Release Notes for Cisco TV CDS 2.1.4

These release notes cover Cisco TV CDS Release 2.1.4.

Revised: October 2011 OL-22676-02

Contents

The following information is in the release notes:

Enhancements

Release 2.1.4 is a maintenance release and consists of resolved caveats and the Bulk Configuration feature. See the "Resolved Caveats" section on page 14 for more information.

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

2.1.3 CDSM Bulk Configuration Import Support for Stream Destinations

In 2.1.3, CDSM GUI will support importing Stream Destination (Configure -> System Level -> Stream Destination) configurations using an XML file. This feature will enable the user to import a set of Stream Destination configurations using an XML file in one step.

Enabling Bulk Import Feature:

In 2.1.3, this feature will be always enabled for Stream Destination Page.

Supported Environments

Release 2.1.4 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 2.1.4 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 2.1.4 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 2.1.4 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 2.1.4.

See the "Related Documentation" section on page 47 for links to the documentation online.

Limitations and Restrictions

There are no limitations nor restrictions in Release 2.1.4.

Important Notes

The section covers the following important notes that apply to this release;

New SSD Driver

There is a new driver for the new solid-state drives (SSDs) that also addresses an issue with the old SSDs.

Old SSD Issue

When an abrupt power loss occurs on an older SSD while the SSD is under load, which can also happen when the SSD is being written to and a power-off shutdown occurs, the result is that the SSD may become corrupted and unusable. If an SSD becomes corrupted in this way it must be replaced.

This driver update provides a fix to prevent the corruption of the SSD when the system is being shutdown. When the system is being shutdown the driver sends a command to the SSD to stop all activity and therefore is protected from corruption.

Note We recommend that this driver update be installed on all systems with SSDs. The driver update is compatible with both the older PV SSDs and the newer PVR SSDs.

New SSDs

New solid-state drives (SSDs) used in the following CDE models require a device driver update for the TV CDS software to recognize the drives:

- CDE220-2S1
- CDE220-2S3
- CDE250-2S5
- CDE250-2S6

A new Generation 2 SSD drive could occur in one of the above newly manufactured CDEs or as a returned merchandise authorization (RMA) SSD drive replacement.

The new SSDs replace the end-of-life (EOL) external 160 GB SSDs. A new SSD drive is a Generation 2 front-mounted SSD. The new SSD model is identified by the title “Intel SSD 320 Series” on the label and has the model number: SSDSA2BW160G3. For more information, see Field Notice 63438 at: http://www.cisco.com/en/US/products/ps7126/prod_field_notices_list.html.

The new driver prevents the corruption of the existing SSDs in the field when a system is shutdown. In the case of receiving any new model of SSDs, the driver must be installed.

Note The new driver is 100 percent backward-compatible with older, pre-existing SSD drives. We recommend that a proactive upgrade of the SSD driver is a good best-practice.

For more information, see the "Updating the Device Drivers for new SSDs" section on page 44.

Thin Pipe Mapping

The CDSM GUI's Thin Pipe Map page allows you to configure low-bandwidth connections between local and remote groups. A local group consists of CDS servers in the same local area network (LAN). A remote group consists of all the CDS servers that are reachable by way of a wide area network (WAN).

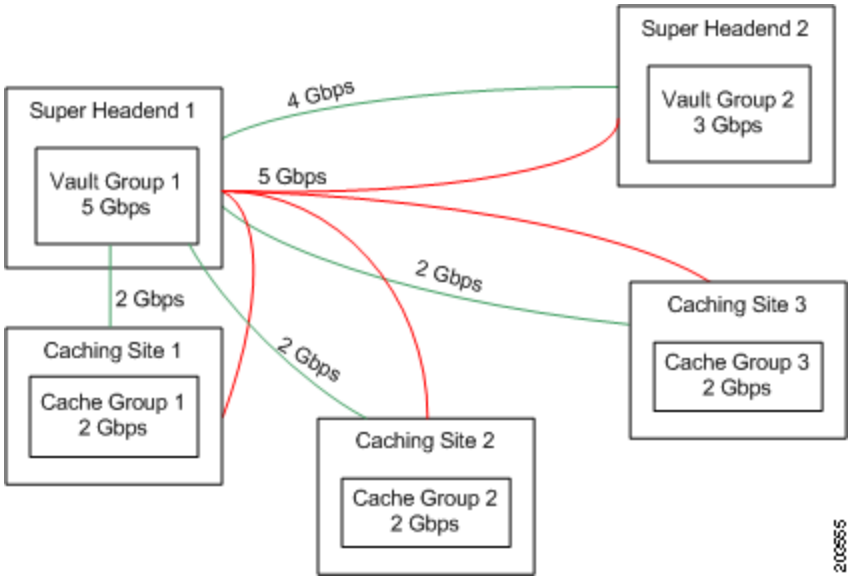
There can be multiple thin pipes configured for each local group. As an example, a site with Caching Nodes organized into a Cache Group could have one 500-Mbps thin pipe going to a site with a Vault Group, and a second 500-Mbps thin pipe going to a location with a Stream Group. The thin pipes are completely independent of each other.

The Thin Pipe Map page also allows for the configuration of thin pipes in a hierarchy, where a remote group must be reached through several pipes. For example, a Cache Group could have a 500 Mbps thin pipe over which it streams to three Stream Groups. Each Stream Group could have separate 100 Mbps thin pipes. In this case, the Cache Group traffic on egress to all Stream Groups is limited to 500 Mbps, while ingress traffic to each Stream Group from this Cache Group is limited to 100 Mbps. In this example, the Cache Group would have four thin pipes configured: one 500 Mbps pipe to all three Stream Groups, and a total of three 100 Mbps pipes, one to each individual Stream Group.

Note In the CDSM, the configured bandwidth for CCP on the Thin Pipe Map page must be the minimum bandwidth reserved for the AF class. The sum of the bandwidths of all physical links configured for CCP among all sites must be less than the bandwidth configured for the AF class reserved for CCP.

As an example, Figure 1 shows the maximum bandwidth available for the various groups in a Virtual Video Infrastructure (VVI) system with two super headends (SHEs), three caching sites, and one streaming site.

Figure 1 Thin Pipe Example



Note The maximum bandwidth available is dictated by the physical link, as well as any network design constraints placed on bandwidth availability. If a switched network has further restrictions, for example, Vault Group 1(VG1) to Vault Group 2 (VG2) and Cache Group 3 (CG3) share a 3 Gbps link on the route between VG1 and the other two sites, then another thin pipe must be configured to specify this 3 Gbps restriction.

Table 1 lists the thin pipe mappings that would be configured for the Vault Group 1 illustrated in Figure 1.

Table 1 Thin Pipe Mappings for Thin Pipe Example

Thin Pipe Map	Remote Group	Bandwidth
Vault Group 1 (VG1)		
VG1toAll	Vault Group 2, Cache Group 1, Cache Group 2, Cache Group 3	5 Gbps
VG1toVG2	Vault Group 2	4 Gbps
VG1toCG1	Cache Group 1	2 Gbps
VG1toCG2	Cache Group 2	2 Gbps
VG1toCG3	Cache Group 3	2 Gbps
Vault Group 2 (VG2)		
VG2toAll	Vault Group 1, Cache Group 1, Cache Group 2, Cache Group 3	4 Gbps
VG2toCG1	Cache Group 1	2 Gbps
VG2toCG2	Cache Group 2	2 Gbps
VG2toCG3	Cache Group 3	2 Gbps
Cache Group 1 (CG1)		
CG1toAll	Vault Group 1, Vault Group 2, Cache Group 2, Cache Group 3	2 Gbps

Table 1 Thin Pipe Mappings for Thin Pipe Example (continued)

Thin Pipe Map	Remote Group	Bandwidth
CG2toSG1	Stream Group 1	3 Gbps
Cache Group 2 (CG2)		
CG2toAll	Vault Group 1, Vault Group 2, Cache Group 1, Cache Group 3	2 Gbps
Cache Group 3 (CG3)		
CG3toAll	Vault Group 1, Vault Group 2, Cache Group 1, Cache Group 3	2 Gbps

The thin pipes configured in Table 1 ensures that the bandwidth for Vault Group 1 never exceeds the maximum bandwidth available for Vault Group 1, which is 5 Gbps. This means that even if all remote groups were requesting cache-fills from Vault Group 1, which would be a maximum throughput of 9 Gbps, the actual maximum bandwidth of cache-fill traffic coming from Vault Group 1 would never exceed 5 Gbps.

Configuring QoS Settings on the CDS Servers

There needs to be a dedicated Differentiated Services (DiffServ) Assured Forwarding (AF) class for the CCP traffic. The Assured Forwarding PHB guarantees a certain amount of bandwidth to an AF class and allows access to extra bandwidth, if available. There are four AF classes, AF1x through AF4x. Within each class, there are three drop probabilities (low, medium, and high).

Note The sum of all bandwidths configured for CCP traffic cannot exceed the bandwidth configured for the AF classes reserved for CCP.

Table 1 lists the DSCP parameters that are configured in the setupfile, the data types that use each parameter, and the required DSCP value for each. The DSCP value can be any number from 0 to 63, but in order for CCP traffic to work properly, the DSCP value must be one of the values listed in Table 2.

Table 2 DSCP Values Configured in Setupfile

DCSP Settings	AF1x Class	AF2x Class	AF3x Class	AF4x Class	Data Types
cache_priority0 _dscp <*value*>	14 (AF13)	22 (AF23)	30 (AF33)	38 (AF43)	Remote smoothing traffic (Vault to Vault) and prefetched traffic (Vault to Caching Node to Streamer must be set for high drop probability.
cache_priority1 _dscp <*value*>	14 (AF13)	22 (AF23)	30 (AF33)	38 (AF43)	Mirroring traffic for creating additional mirrored copies (Vault to Vault) must be set for high drop.
cache_priority2 _dscp <*value*>	14 (AF13)	22 (AF23)	30 (AF33)	38 (AF43)	Repair traffic that is recovering striped data lost because of a drive failure (Vault to Vault) must be set for high drop.
cache_priority3 _dscp <*value*>	14 (AF13)	22 (AF23)	30 (AF33)	38 (AF43)	Mirroring of live ingest traffic (Vault to Vault) must be set for high drop.
cache_priority4 _dscp <*value*>	12 (AF12)	20 (AF22)	28 (AF32)	36 (AF42)	Committed rate traffic (Vault or Caching Node or Streamer to Vault or Caching Node or Streamer) must be set for medium drop.

Table 2 DSCP Values Configured in Setupfile (continued)

DCSP Settings	AF1x Class	AF2x Class	AF3x Class	AF4x Class	Data Types
cache_priority5 _dscp <*value*>	10 (AF11)	18 (AF21)	26 (AF31)	34 AF41)	Lost packet recovery for committed rate traffic (Vault or Caching Node or Streamer to Vault or Caching Node or Streamer) must be set for low drop.
cache_priority6 _dscp <*value*>	10 (AF11)	18 (AF21)	26 (AF31)	34 AF41)	Handles the following data types that must be set for low drop: • High-priority lost packet recovery for committed rate traffic (Vault or Caching Node or Streamer to Vault or Caching Node or Streamer) • iGate and index file transmission (Vault or Caching Node to Streamer) • First part of mirror data going to a new Vault (Vault to Vault)
cache_priority7 _dscp <*value*>	14 (AF13)	22 (AF23)	30 (AF33)	38 (AF43)	Lost packet recovery of mirroring traffic (Vault to Vault) must be set for high drop.
control_dscp <*value*>	10 (AF11)	18 (AF21)	26 (AF31)	34 (AF41)	The control value is for the control traffic and must be set for low drop.
cache_dscp <*value*>	If the cache_priority value is not specified then the cache_dscp value is used for that priority. All cache_priority DSCP values must be set in order for Thin Pipe Mapping to work properly.				
transport_dscp <*value*>	A DSCP value other than those used for the cache_priority settings.				The transport value is for the traffic going from a Streamer to a STB or QAM device.

Currently, the values for the DSCP parameters must be set manually in the setupfile. Log in to each CDS server as *root* and edit the setupfile by adding the parameters described in Table 2. The setupfile file is located in the /arroyo/test directory.

Caution Do not attempt to access the Linux command line unless you are familiar with the CDS, the Linux operating system, and have an understanding of the Linux command line.

Following are the fields that have to be added to the setupfile on each CDS server grouped by AF class. For convenience, you can copy the text of the appropriate settings for the AF class you want to use and paste it into the setupfile.

To configure for class AF1 add the following lines to the setupfile:

```
cache_priority0_dscp 14
cache_priority1_dscp 14
cache_priority2_dscp 14
cache_priority3_dscp 14
cache_priority4_dscp 12
cache_priority5_dscp 10
cache_priority6_dscp 10
cache_priority7_dscp 14
control_dscp 10
```

To configure for class AF2 add the following lines to the setupfile:

```
cache_priority0_dscp 22
cache_priority1_dscp 22
cache_priority2_dscp 22
```

```
cache_priority3_dscp 22
cache_priority4_dscp 20
cache_priority5_dscp 18
cache_priority6_dscp 18
cache_priority7_dscp 22
control_dscp 18
```

To configure for class AF3 add the following lines to the setupfile:

```
cache_priority0_dscp 30
cache_priority1_dscp 30
cache_priority2_dscp 30
cache_priority3_dscp 30
cache_priority4_dscp 28
cache_priority5_dscp 26
cache_priority6_dscp 26
cache_priority7_dscp 30
control_dscp 26
```

To configure for class AF4 add the following lines to the setupfile:

```
cache_priority0_dscp 38
cache_priority2_dscp 38
cache_priority3_dscp 38
cache_priority4_dscp 36
cache_priority5_dscp 34
cache_priority6_dscp 34
cache_priority7_dscp 38
control_dscp 34
```

Changing the Date and Time with NTP

This section provides the details on setting the time and date. Specific NTP configuration details should be obtained from your system administrator.

The clocks on all CDS nodes (vault, streamer, cache and CDSM) in a network must be synchronized in order to retrieve the statistics on the CDSM. Synchronizing the clocks is the final step in the installation process before rebooting the system for each CDS node.

Perform the following steps to change the date and time with NTP:

Step 1 Log in as root.

Step 2 Enable the service by entering the following commands:

```
[root@system]# chkconfig --level 2345 ntpd on
[root@system]# chkconfig --list ntpd
```

You will see the following:

```
ntpd              0:off    1:off    2:on    3:on    4:on    5:on    6:off
```

Step 3 Stop the NTPD service by issuing the following command:

```
[root@system]# service ntpd stop
```

Step 4 If needed, set the timezone by entering the following command and follow the prompts:

```
[root@system]# /usr/bin/tzselect
```

Step 5 Set the system date and time to a date and time close to the NTP server date and time by entering the **date -s** "*date_time_string*" command, for example:

```
[root@system]# date -s "16:55:30 Nov 7, 2009"
```

Step 6 Synchronize the clock to the configured NTP servers by entering the following command:

```
[root@system]# ntpd -q
```

Note If the system clock is off by a significant amount, the command will take considerable time to return.

Step 7 Start the NTPD service by entering the following command:

```
[root@system]# service ntpd start
```

Step 8 Synchronize the hardware clock by entering the following command:

```
[root@system]# /sbin/hwclock --systohc
```

Step 9 Check the NTP synchronization by entering the following command:

```
[root@system]# ntpq -p
```

Step 10 Reboot the CDS system by entering the following command:

```
[root@system]# init 6
```

Open Caveats

This release contains the following open caveats:

Configuration:

- CSCtg88234

  Symptom:

  Submitting System-> Headend Setup page removes the leading zeros in the Service Group Name.

  Condition:

  CDSM Setup:

  - CServer Version > 2.0.x
  - Installation Type - RTSP
  - RTSP Deployment - Event IS
  - Service Group Steering - ON

  Workaround:

  None,

Database

- CSCte72718

  Symptom:

  The error indicates that a PAID to GOID lookup is occurring during a database checkpoint. The lookup times out due to the database being busy with a checkpoint and the error is thrown in c2k log and the messages log. The lookup is retried and the fill is successful.

  Condition:

  CCDN-PS-WCDC-01 kernel: IsaDbCommand error -1 attempting GET PAID_TO_GOID.

  Workaround:

  cServer and Database should communicate with each other to avoid these types of errors.

Ingest

- CSCtg79615

  Symptom:

  CDSM System Snapshot page: Prov. (push) Ingests field is always 0.

  Condition:

  Database content records for Provisioned FTP Push Ingests were not replicated from vaults to CDSM properly. Some fields are zeroed.

  Workaround:

  Check database on vaults directly. Provisioned but not active FTP Push Ingests will have OpState = 3, and AdminState = 2.

ISA

- CSCtg50574

  Symptom:

  If more than a handful (> 10) of barkers streams are created then this issue occurs, but the root cause is not known yet.

  Condition:

  The error is triggered by some unknown issues. It is under investigation and and is trying to be reproduce in the lab.

  Workaround:

  Manually figure out the duplicate barker streams and use the procedure to clean them. The following procedure must be run on both primary and backup setup streamers:

  1. Login as isa to the streamer.
  2. cd StreamsDriver
  3. Edit the run_driver script and type exit at the top line. (This will prevent the streams driver auto-start.)
  4. ./stop_driver

After steps 1-4 are done on both the primary and backup setup streamers , perform the following steps only on the primary setup streamer:

5. cddb
6. Use bsql (select 3, 8, 6) to look for duplicate records.
7. Use bsql to delete the duplicate records (select 3, 8, 3, 1) and quit.
8. Keep the records that you are deleting. The streamId will be used to tear down the duplicate streams.

After steps 5-8 are done then perform the following steps on both streamers:

9. cd /home/isa/StreamsDriver
10. Edit the run_driver file and delete the top line (add on step 3).
11. cdint; tail -f ns_log (make sure StreamsDriver is restarted.)

Finally, perform the following step only on the primary streamer:

12. Use the ./destroy_a_stream script to tear down the duplicate barker streams noted in step 8. Ask the customer to verify the duplicate barker streams are no longer there.

Streamer

- CSCtg36522

  Symptom:

  1.5 vault could not fill content to 2.1.4 streamers.

  Condition:

  During upgrade, cserver version is co-existing on vaults and streamers. It did not happen always.

  Workaround:

  Reboot 2.1.4 streamers.

- CSCtg88135

  Symptom:

  On the simulation test bed, if a stream failed to be transmit-filled from vaults or cache servers to streamers, ResourceManager could not identify it when it is LSCP Timeout.

  Condition:

  This only happens on the simulation test bed, and only happens when the stream failed to be filled. If stream plays to end and transition to Open state, it will be detected by ResourceManager and torn down by Stream Service if it is LSCP Timeout. On the end-to-end system, STB will send Tear Down command to control server if the null stream becomes timeout.

  Workaround:

  Hardly see it on the end-to-end system.

- CSCth00239

  Symptom:

  Small number of packet loss is observed with a packet analyzer.

  Condition:

When streaming 3000+ streams from 80 live ingest streams the packet analyzer reports a few packets that are lost. With the small number of packets lost there is no visual effect observed or degradation of quality.

Workaround:

Stream a lower number of streams per streamer or ingest lower number of live streams per vault.

Upgrade

- CSCth04589

  Symptom:

  While running preupgrade script in 1.5.x, at the end it displays the following message “Please reboot the server and run the script 'upgrade' when the server comes back up”. This message should be changed to indicate that the upgrade script should be run after the OS upgrade.

  Conditions:

  Run preupgrade script on a 1.5.x server

  Workaround:

  None.

Vault

- CSCte77024

  Symptom:

  1.5 vault ingested content failed to remote-mirror to 2.1.4 vault

  Condition:

  During upgrade, the cserver version is co-existing on vaults. Newly ingested content to 1.5 vault cannot be remote mirrored to 2.1.4 vault. It is not a 2.1.4 bug, it is related to 1.5 code.

  Workaround:

  Once 1.5 vault is upgraded to 2.1.4, objects will be mirrored to 2.1.4 vault automatically. Or they do not ingest new content during upgrade.

- CSCtg42458

  Symptom:

  When HD ingest count is over 40 on a Lindenhurst with 8G memory, c2k log shows “ERROR: Out of memory”, video has artifacts for live streaming.

  Condition:

  160 SD ingest count is enforced on a Lindenhurst vault. But equivalent HD ingest has no limitation enforced. It is possible HD ingests are over vault's capacity.

  Workaround:

  Limit HD ingest number at backoffice.

- CSCtg50641

  Symptom:

A bad drive caused receiving mirroring stuck on a vault.

Condition:

A bad drive on the vault and vault is doing disk writes.

Workaround:

Pull the bad drive. Or wait for 5-10 minutes, the bad drive will be kicked off by the cserver.

Video Quality

- CSCte08685

  Symptom:

  Packet loss is observed when 300 live streams for 30 MPEG2 HD live contents.

  Condition:

  – This issue is observed on CDE400 with 8G memory ingesting live contents.
  – This issue is not observed on CDE420 with 12G memory ingesting live contents.

  Workarounds:

  – Reduce stream number.
  – Reduce live content number.

- CSCtf98150

  Symptom:

  Packet loss is observed with 3000 streams for 50/80 MPEG2 SD live contents. There are about 50 packets lost testing on the CDE420.

  Conditions:

  This issue is observed on both the CDE420 with 32G memory and CDE400 with 8G memory.

  Workarounds:

  – Reduce the stream number.
  – Reduce the live content number.

- CSCtg36215

  Symptom:

  Macroblocking for up to a second after a transition from FF or REW to 1x Play.

  Conditions:

  – Content must be encrypted with PowerKey.
  – Trick speed must be higher than 4x.
  – Minimum ARM time (from ECM control word insertion into stream to first use) must be less than two seconds (the default is around one second).

  Workarounds:

  – Reduce the trick speed to 4x.
  – Increase the minimum ARM time higher (to two seconds for 8x tricks) and reingest assets.
  – Upgrade the streamer to a version with this bug fixed, no reingest required.

Resolved Caveats

The following caveats have been resolved since Cisco TV CDS Release 2.1.4. Not all resolved issues are mentioned here. The following list highlights associated with customer deployment scenarios.

CacheGateway

- CSCte10296

  Symptom:

  The Streamer is unable to get content from the Cache Gateways when the Provide ID is 20 characters in length.

Cache Management

- CSCtd93467

  Symptom:

  When sending a name-to-GOID lookup request to the library node from the cache node, there was no library node online. In this case, the requesting server synthesizes a response, but the response contains no response data, only a response status. The fix is to ensure that we do not de-reference the response data pointer unless the response status indicates success.

CDSM

- CSCte78915

  Symptom:

  The CDSM file system can become full and all logging stops.

Configuration

- CSCte05319

  Symptom:

  You cannot configure an SOP in the CDSM GUI with a name longer than 20 characters, and the GUI also does not allow any special characters in the SOP name.

- CSCtf94376

  Symptom:

  Service Group values greater than 32bit signed into (2147483647) get changed to 2147483647 prior to being set in the database.

File Systems

- CSCtf26647

  Symptom:

  Objects do not stream properly after upgrading from 1.5.x to 2.x. Fragmented objects on the 1.5 server (Streamer or Vault) may become unusable after an upgrade to 2.x as they are marked as “data downloads” after the upgrade is completed.

Ingest

- CSCsw43707

  Symptom:

  A Gen II vault KDB during live ingest.

- CSCtb61737

  Symptom:

  The active ingest content gets stuck after the ingest port is down for a long time. This problem occurs only if the link that has the current ingest going on (management or ingest interface) goes down. The thread in the application waiting for the response from the FTP server never comes out and remains hung until service is restarted.

ISA

- CSCtd95374

  Symptom:

  Connections on the Sectamus server are timing out when there is no response from the master vault received within 3 seconds. A portion of the RTA titles that are ingested at the top of the hour will fail and will not be available to be viewed.

- CSCte37026

  Symptom:

  When adding 60 feed live ingestion (FTP push ingest; the vault acts as an FTP server), after ingesting for some time we found the content store factory in the master vault is restarted.

- CSCtf23352

  Symptom:

  The defragmentation or local smoothing of large objects can lead to a stuck polling loop, which excessively consumes the CPU.

Network

- CSCte25648

  Symptom:

There is a time comparison that is intended to make sure that the receiving server does not send out the cancel message on a stream it does not want at a rate faster than 5ms between packets (200 packets per second maximum).

Scalability

- CSCtd23968

  Symptom:

  Streamer runs out of capacity when starting more than 300 unique fill streams.

statsd

- CSCte81804

  Symptom:

  The statsd fails to generate a setup file for ISA non-scs deployments.

Streamer

- CSCtb98330

  Symptom:

  After a network outage, when control primary and control backup stream servers resync, the backup primary may KDB if it is required to process rapid commands given from a remote control. This happens when the user pushes the buttons several times a second.

- CSCtd73159

  Symptom:

  If the Igate read fails with a read failure, when retrying reading the igate the read always fails because the flag in the read rate that indicates that a read failure has occurred is never reset.

- CSCtd94314

  Symptom:

  When IGate mem on streamer reaches 720M, streams cannot be set up and “IGate memory limit exceeded 0 1 0 0 0 0 0 0 0 0” is kept printing in the Streamer protocoltiming.log.

- CSCte44722

  Symptom:

  A new tunable is required to adjust the delay before a failing stream.

- CSCte82068

  Symptom:

  2.1 NGOD cannot play live-ingested content.

- CSCtg23764

  Symptom:

There are several paths in the cost request code where the CostingAgent may reference a stream after it has already been destroyed. One of these paths was previously fixed as part of CSCta12859 but was subsequently broken again by CSCtb95669.

Utilities

- CSCtg25603

  Symptom:

  The avs_clist tool is printing out the wrong GOID length creating a clone list. When running the avs_clist on 1.5.1.5.4, the clone list has problems with the GOID length. Also the cloned vault can delete a remote GOID.

Vault

- CSCtd04537

  Symptom:

  When removing a copy, the loop exceeds the bound of a global array.

- CSCtd67685

  Symptom:

  Asset fails to ingest. Asset being ingested has to be coded with more than one setting for the aspect ratio, and in violation of both our VOD encoding specs and the MPEG-2 specification Part 1.

- CSCtd92730

  Symptom:

  If any of the remote vaults are rebooted, the FTP control connections from the master vault to the remote vault are left in the EST state on the master side. The master content store considers them as a good connection and sends the PASV command through it, but the send fails and causes the ingest to fail.

- CSCte05010

  Symptom:

  If an error occurs during the RTA ingest (ftp-push) request (PASV failed or STOR failed), the connection between the master and the remote vault are closed by the remote vault and there are chances that the file desc goes into an error and causes the poll thread to spin on it until the file desc is reused by the system for other ingests.

  The window for the thread spinning over CPU is small if the file desc number is small (such as 10, 11) but it could be bigger if the file desc number is big enough that system takes time to reuse it.

- CSCtf11781

  Symptom:

  A softlockup is caused by an infinite loop when more than ten servers exist in one array.

- CSCtg29316

  Symptom:

  A malformed vaultcloner file can cause the cloner to delete content on the cloner.

Installing and Configuring the TV CDS 2.1 Software

This section includes the following topics:

For a CDS for an ISA environment or RTSP environment, see the software installation procedures included in the *Cisco Content Delivery Engine 110 Hardware Installation Guide* and the *Cisco Content Delivery Engine 205/220/420 Hardware Installation Guide*. See the "Related Documentation" section on page 47 for information on accessing these documents.

It is a good idea to read through this entire section before performing the install or upgrade procedure.

Note If the CDS does not have 2.1.4 as the preferred release to deploy, before starting this procedure download the TV CDS 2.1.4 software and transfer it to the CDS. Enter the following command to verify the system version:

uname -r

If the response to this command has "cdstv.2.1.4.b30" in the output, the system has the TV CDS 2.1.4 software. If 2.1.4 is not on the system, see the "Getting a Software File from Cisco.com" section on page 35 to obtain the TV CDS software needed for your deployment.

Release 2.1 introduces two features that require additional information when configuring the CDS servers and the CDSM:

- Virtual Video Infrastructure
- CDSM Redundancy

Virtual Video Infrastructure

Release 2.1 introduces the Virtual Video Infrastructure with Caching Nodes. With the VVI, there is the option to centrally manage all the servers or to use the split-domain management. Split-domain management has two managers:

- Virtual Video Infrastructure Manager (VVIM) manages the Vaults and Caching Nodes
- Stream Manager manages the Stream Domain of Streamers

You can have multiple Stream Domains that are each managed by a separate Stream Manager. Centrally managed VVIs are only supported in an RTSP environment. A VVI in an ISA environment must use split-domain management, as well as Shared Content Store and CCP Streamers. For more information about Shared Content Store and CCP Streamers, see the *Cisco TV CDS ISA 2.1 Software Configuration Guide*. Each of the VVI configurations has a different installation process.

Note In an ISA environment, split-domain management and Shared Content Store requires that both the VVIM and Stream Manager be configured with the ISA settings in order to successfully communicate with the BMS. Use the VVIM to configure the Shared ISA settings (Shared ISA Settings page), and use the Stream Manager to configure the individual ISA Stream Service settings (VHO ISA Settings).

CDSM Redundancy

Release 2.1 also introduces CDSM redundancy. All CDS servers keep track of both CDSM IP addresses. Each CDSM keeps track of the other CDSM IP address, as well as the virtual IP address that is used to access the CDSM. When running the cdsconfig script on each CDS server, you need to add each CDSM

as a replication member. The CDSM that is chosen as the primary is accessed by using the virtual IP address. When running the cdsconfig script on each CDSM, you are prompted for the virtual IP address and subnet mask. When running the cdsconfig script on a Stream Manager, you are asked if this is the first CDSM that is getting added to the domain. For more information on the CDSM Redundancy feature, see the *Cisco TV CDS ISA 2.1 Software Configuration Guide* or the *Cisco TV CDS RTSP 2.1 Software Configuration Guide*.

Following is an overview of the procedure to add a second CDSM:

1. As part of the installation process of the CDS servers and CDSM (or VVIM and Stream Manager in split-domain management), the cdsconfig script prompts you to add replication members. Along with adding all the CDS servers, add the second CDSM (VVIM or Stream Manager in split-domain management) as a replication member.
2. When installing the second CDSM (VVIM or Stream Manager in split-domain management), along with adding all the CDS servers as replication members, add the first CDSM (VVIM or Stream Manager in split-domain management) as a replication member.
3. Reboot the CDSMs (VVIMs or Stream Managers in split-domain management) after the cdsconfig script completes in order to start the statsd process for the virtual IP address on each CDSM (VVIM or Stream Manager in split-domain management).

Note During the initialization process of a CDS server or after recovering a CDS server that has been down for more than an hour, the CDS database performs a complete synchronization. The database synchronization takes about five minutes before the server becomes ready for service. If the CDS server is down for a much longer time than an hour, the database synchronization takes longer than five minutes. The **netstat** command does not show the interfaces as up until the synchronization has completed.

Preparing the CDEs for the TV CDS Software

Before performing the software installation and initial configuration, you must correctly install the CDEs and connect the cables as described in the *Cisco Content Delivery Engine 110 Hardware Installation Guide* and the *Cisco Content Delivery Engine 205/220/420 Hardware Installation Guide*. See the "Related Documentation" section on page 47 for information on accessing these documents.

Note As part of the hardware installation of the CDEs, check to make sure all I/O cards are properly and firmly seated, and all cables are firmly connected.

Before you run the initial configuration script, you should gather the following information:

- IP address and subnet mask of the CDE management interface—Typically the eth0 interface is used for the management interface.
- IP address of the default gateway interface—This is the address of the interface on the router that is directly attached to the CDE management (eth0) interface.
- Hostname for the CDE—Name for the device host.
- Group ID—A unique user-defined value. All servers (ssv [ISV], Vault, Streamer, controller [CDSM]) that are part of the same CDS system (managed by one CDSM) have the same group ID. This group ID should be unique across an enterprise.
- Server ID—A unique user-defined value. The ID must be unique for each CDS device.

Note ISA VVI generates a range for the streamers to use in the Stream Domain. When configuring a streamer, choose a server ID in a range.

However, RTSP VVI does not generate a range for the server ID.

- Replication group members—The CDS devices that will be replication group members and the IP address of each member. The servers to include in a replication group depends on the network design for the CDS.

Note With the exception of the server you are configuring, all CDS devices (VVIMs, Stream Managers, ISVs, Vaults, and Streamers) that are members of the replication group should be configured at this time. The server you are configuring is not configured as a replication group member.

  - In simple cases, because all CDS servers share information with each other, all servers are in each other's replication group.
  - In more complex cases, only a subset of the servers are included in a replication group. As an example, if Streamers only talk to the CDSM, Vaults, and Streamers within *a specific Streamer group*, then the Streamers replication group includes only these devices.

In both the CDS and VVI, all Vaults and Streamers are identified by an array ID, a group ID, and a server ID. In the CDSM GUI, the array ID identifies servers that are part of the same system, the group ID identifies servers that are part of the same group (Vault Group or Stream Group), and the server ID is a unique number that identifies the server. Table 1-3 lists the CDSM GUI ID names and maps them to the CServer names in the setupfile and .arroyorc files.

Table 1-3 ID Names in the CDSM GUI and CServer Files

CDSM GUI ID Name	CServer Files ID Name
Array ID on the Array Name page	groupid
Group ID on the Server-Level pages	groupid
Stream Group ID on the Server Setup page	arrayid
Cache Group ID on the Server Setup page	arrayid
Vault Group ID on the Server Setup page	arrayid
Stream Group ID on the Configuration Generator page	arrayid

Connecting to the Serial Port on the CDE

The RJ-45 serial ports on the Cisco CDEs front and back panels can be used for administrative access to the CDE through a terminal server. Terminal emulation software must be configured as follows:

- Bits per second: 115200
- Data bits: 8
- Parity: none
- Stop bits: 1
- Hardware flow control: ON

VVI with Split-Domain Management Installation Procedure

Note New CDEs ship with the Linux operating system, the TV CDS 2.0 software, and both the cdsinstall and cdsconfig scripts. Before starting the procedures in this section, you need to download the TV CDS 2.1 ISO image file and the cdsconfig script from the Cisco software download website, and upgrade the software on your new CDE to Release 2.1. For more information, see the "Upgrading from Release 2.0 to Release 2.1.4" section on page 35.

The order in which you install and configure the CDEs for VVI is very important. The VVIM (Vault/Cache CDSM) and all the Vaults and Caching Nodes in the VVIM domain must be installed and configured first and brought online before the Streamer domain is configured. A high-level view of the installation order follows:

Step 1 Install and configure the VVIM.

a. Follow the "Installing and Configuring the VVIM" procedure.

b. Log in to the VVIM as a user that has the engineering access level and configure the VVIM Setup page. For more information, see the "Getting Started" chapter in either the *Cisco TV CDS ISA 2.1 Software Configuration Guide* or the *Cisco TV CDS RTSP 2.1 Software Configuration Guide*.

Step 2 Install and configure each Vault and Caching Node in the VVIM domain.

a. Follow the "Installing and Configuring the Vaults, Caching Nodes, or Streamers" section on page 28.

b. Log in to the VVIM and configure each Vault and Caching Node using the "VVI Workflow" section in the "Getting Started" chapter in the *Cisco TV CDS ISA 2.1 Software Configuration Guide* or the *Cisco TV CDS RTSP 2.1 Software Configuration Guide*.

Note In an ISA environment, the ISA services cannot be started until the Stream Manager is up and at least one Streamer in a Stream Domain has had the VHO Setup and VHO ISA Setup settings configured.

Step 3 Install and configure the Stream Manager.

a. Follow the "Installing and Configuring the Stream Manager" section on page 25.

b. Log in to the Stream Manager as a user that has the engineering access level and configure the CDSM Setup page. For more information, see the "Getting Started" chapter in either the *Cisco TV CDS ISA 2.1 Software Configuration Guide* or the *Cisco TV CDS RTSP 2.1 Software Configuration Guide*.

Step 4 Install and configure each Streamer completely. Make sure the Streamer is configured completely and displaying in the Stream Manager's System Health Monitor page before moving on to the next Streamer.

a. Follow the "Installing and Configuring the Vaults, Caching Nodes, or Streamers" section on page 28.

b. Log in to the Stream Manager and configure each Streamer using the "VVI Workflow" section in the "Getting Started" chapter in the *Cisco TV CDS ISA 2.1 Software Configuration Guide* or the *Cisco TV CDS RTSP 2.1 Software Configuration Guide*.

Step 5 Repeat Step 3 and Step 4 for each Stream Domain.

Step 6 Add any redundant CDSM to either the VVIM or Stream Managers. See the "CDSM Redundancy" section on page 18 for more information.

Note During the running of the cdsconfig script, the Stream Manager communicates with the VVIM to get a range of group IDs and server IDs to use in the Stream Domain. If the Stream Manager is unable to connect to the VVIM, the VVIM administrator can manually generate the IDs and send the information to the Stream Manager installer for manual entry. For more information, see the *Cisco TV CDS ISA 2.1 Software Configuration Guide* or the *Cisco TV CDS RTSP 2.1 Software Configuration Guide*.

Installing and Configuring the VVIM

To install the TV CDS software and initially configure the VVIM, do the following:

Step 1 If the Cisco CDE110 is not powered on, press the front panel power switch on the server.

The operating system boots.

Step 2 Log in as *root* with the password *rootroot*.

Step 3 So that your password for root is not the default password, use the **passwd** command to change the password used.

Step 4 To install the TV CDS software, issue the following command and, depending on your deployment type, choose 1 (CDSM):

```
[root]# ./cdsinstall
```

The following prompt is displayed:

```
Continuing first-time installation after kickstart using image //CDS-TV.iso
Select Deployment Type (ctrl-c to quit):
  1) CDSM
1
CDSM Selected

... Output omitted ...

Unmounting /mnt/cdrom
inst.sh completed, removing .iso image
```

```
================================================
Configure the system for initial installation
================================================
```

Step 5 To run the initial configuration script, issue the **cdsconfig** command. In the prompts displayed by the script, the default values in brackets are taken from the configuration that you just completed.

- If a default value is correct, press **Enter** to accept that value.
- If a default value is incorrect, enter the correct value and press **Enter**.

```
[root]# cdsconfig

Please ensure an IP address and netmask are configured for
  management interface eth0:

Select an option or an interface to re-configure/disable:
    1. eth0     ip:172.22.97.162    mask:255.255.255.128  bcast:172.22.97.255
    2. Configure another interface
    3. Done
Choice [3]: 3
Backing up old scripts in /etc/sysconfig/network-scripts
Writing new ifcfg-ethX scripts

Enter a hostname [cdsm162]: Enter
Enter the number of the eth interface that connects to the gateway [0]: Enter
Enter the default gateway IP address [172.22.97.129]: Enter
Backing up /etc/sysconfig/network
Writing new /etc/sysconfig/network
Backing up /etc/hosts
Writing new /etc/hosts
Restarting network services, this may take a minute:
Shutting down interface eth0:                              [  OK  ]
Shutting down loopback interface:                          [  OK  ]
Bringing up loopback interface:                            [  OK  ]
Bringing up interface eth0:                                [  OK  ]
Network services restarted; may take a few seconds to establish connectivity
Reboot for hostname changes to take effect
Network configuration complete

Please choose your platform from the following list of valid platforms:
    1. 2U-SCSI-1
    2. 3U-SCSI-1
    3. 3U-SCSI-10
    4. 3U-SCSI-11
    5. 2U-SATA-1
    6. 2U-SATA-2
    7. 2U-SATA-10
    8. 2U-SATA-11
    9. 4U-SATA-1
   10. 4U-SATA-2
   11. 4U-SATA-3
   12. 4U-SATA-10
   13. 4U-SATA-11
   14. 4U-SATA-12
   15. CDE100-2C-1
   16. CDE110-2C-1
Choice: 16

Please select a role for this CDSM:
    1. CDS Manager (single domain)
    2. VVI Manager (split domain for Vault and Caching node)
    3. CDS Manager (split domain for Streamers)
Choice: 2
```

```
Please enter a group ID: 12345
Please enter a server ID [62]: 162
Writing new configuration to /home/isa/.arroyorc

No existing replication group information found
Do you want to configure replication group members now? (yes/no) [y]: y

There are currently no replication group members.
Do you want to add another replication group member? (yes/no) [y]: y
```

Note With the exception of the server you are configuring, all CDS devices (VVIMs, Stream Managers, ISVs, Vaults, Caching Nodes, and Streamers) that are members of the replication group should be configured at this time. The server you are configuring is not configured as a replication group member.

In the following example, the configuration of the CDS devices shows generalized input values. Option 5, cdsmgw, is the Stream Manager. Add the Stream Manager as a replication group member. This is for ISA only; this is not required for RTSP.

```
Select a role for the new replication group member:
    1. ssv
    2. Vault
    3. cache
    4. Streamer
    5. cdsmgw

Choice: device_role (1, 2, 3, 4, 5 or 6)
Enter an IP address for new CDS_device: IP_Address

Current replication group members:
device_role IP_Address

Do you want to add another replication group member? (yes/no) [n]: n
Configuring CDSM
Database is running.
Do you want to enable CDSM Redundancy ? (yes/no) [y]:
CDSM Virtual IP [172.22.99.106]:
Subnet Mask [255.255.254.0]:
Writing rc.local
CDSM configuration finished
cdsconfig finished, please use CDSM to complete configuration

[root]#
```

Step 6 View the contents of the hidden file /home/isa/.arroyorc and make sure that the file contains the following line:

dbdomsock /tmp/isadb

If the preceding line is not in the file, use a text editor to add the line. Close and save the .arroyorc file.

Step 7 To ensure that the AVS database (avsdb) and the Apache web server are started, issue the following commands and verify that a process ID exists for avsdb:

```
[root]# su - isa     //==== start avsdb
[isa]$ pgrep avsdb
28794                //==== verify avsdb process is running
[isa]$ exit
logout
[root]# /arroyo/www/bin/apachectl start   //==== start apache server
httpd: Could not reliably determine the server's fully qualified domain name, using
172.22.97.162 for ServerName
```

```
[root]#
```

Step 8 To verify that VVIM is operational, point your web browser to the Cisco CDE110 that hosts the VVIM by entering the IP address using the following format:

```
http://VVIM_ip_address
```

The VVIM Login page is displayed.

Step 9 Enter **admin** as the username and **admin** as the password and press **Login**.

If you are unable to log in with the username *admin* and the password *admin*, do the following:

a. Run the following command as *root* on the Cisco CDE110 that hosts VVIM:

```
[root]# /home/stats/runonce
```

b. Log in to the VVIM with the username *admin* and the password *admin*.

The VVIM Setup page is displayed.

Step 10 Use the VVIM to complete the configuration. For information on the other configuration tasks, see one of the following:

- For an ISA deployment, see the "Getting Started" chapter in the *Cisco TV CDS 2.1 ISA Software Configuration Guide*.
- For an RTSP deployment, see the "Getting Started" chapter in the *Cisco TV CDS 2.1 RTSP Software Configuration Guide*.

Once the VVIM has been installed and initially configured, install and initially configure the Vaults and Caching Nodes that are part of this VVIM domain. See the "Installing and Configuring the Vaults, Caching Nodes, or Streamers" section on page 28 for more information. When all the servers in the VVIM domain have been configured and are listed on the VVIM's System Health Monitor page, install and configure the Stream Manager. See the "Installing and Configuring the Stream Manager" section on page 25 for more information.

Installing and Configuring the Stream Manager

To install the TV CDS software and initially configure the Stream Manager, do the following:

Step 1 If the Cisco CDE110 is not powered on, press the front panel power switch on the server.

The operating system boots.

Step 2 Log in as *root* with the password *rootroot*.

Step 3 So that your password for root is not the default password, use the **passwd** command to change the password used.

Step 4 To install the TV CDS software, issue the following command and, depending on your deployment type, choose 1 for CDSM:

```
[root]# ./cdsinstall
```

The following prompt is displayed:

```
Continuing first-time installation after kickstart using image //CDS-TV.iso
Select Deployment Type (ctrl-c to quit):
  1) CDSM
1
```

```
CDSM Selected

... Output omitted ...

Unmounting /mnt/cdrom
inst.sh completed, removing .iso image

================================================
Configure the system for initial installation
================================================
```

Step 5 To run the initial configuration script, issue the **cdsconfig** command. In the prompts displayed by the script, the default values in brackets are taken from the configuration that you just completed.

- If a default value is correct, press **Enter** to accept that value.
- If a default value is incorrect, enter the correct value and press **Enter**.

```
[root]# cdsconfig

Please ensure an IP address and netmask are configured for
  management interface eth0:

Select an option or an interface to re-configure/disable:
    1. eth0     ip:172.22.97.162    mask:255.255.255.128  bcast:172.22.97.255
    2. Configure another interface
    3. Done
Choice [3]: 3
Backing up old scripts in /etc/sysconfig/network-scripts
Writing new ifcfg-ethX scripts

Enter a hostname [cdsm162]: Enter
Enter the number of the eth interface that connects to the gateway [0]: Enter
Enter the default gateway IP address [172.22.97.129]: Enter
Backing up /etc/sysconfig/network
Writing new /etc/sysconfig/network
Backing up /etc/hosts
Writing new /etc/hosts
Restarting network services, this may take a minute:
Shutting down interface eth0:                              [  OK  ]
Shutting down loopback interface:                          [  OK  ]
Bringing up loopback interface:                            [  OK  ]
Bringing up interface eth0:                                [  OK  ]
Network services restarted; may take a few seconds to establish connectivity
Reboot for hostname changes to take effect
Network configuration complete

Please choose your platform from the following list of valid platforms:
    1. 2U-SCSI-1
    2. 3U-SCSI-1
    3. 3U-SCSI-10
    4. 3U-SCSI-11
    5. 2U-SATA-1
    6. 2U-SATA-2
    7. 2U-SATA-10
    8. 2U-SATA-11
    9. 4U-SATA-1
   10. 4U-SATA-2
   11. 4U-SATA-3
   12. 4U-SATA-10
   13. 4U-SATA-11
   14. 4U-SATA-12
   15. CDE100-2C-1
   16. CDE110-2C-1
```

```
Choice: 16

Please select a role for this CDSM:
    1. CDS Manager (single domain)
    2. VVI Manager (split domain for Vault and Caching node)
    3. CDS Manager (split domain for Streamers)
Choice: 3
Is this Streaming Domain going to use CCP as Cache Fill Protocol? (yes/no) [y]: Y
Is this the first CDS Manager getting added to this domain? (yes/no) [y]:
Enter the name of this Stream Domain: StreamDomain1
Enter the IP address of the VVIM: 172.22.99.109

Retrieved Server ID '1001' from '172.22.99.109'
Please enter a group ID: 12345
```

Note The group ID should be the same group ID as the VVIM. This group ID is the ID of the array. The VVIM assigns the server ID to the Stream Manager.

```
Writing new configuration to /home/isa/.arroyorc

No existing replication group information found
Do you want to configure replication group members now? (yes/no) [y]: y

There are currently no replication group members.
Do you want to add another replication group member? (yes/no) [y]: y
```

Note With the exception of the server you are configuring, all CDS devices (VVIMs, Stream Managers, ISVs, Vaults, and Streamers) that are members of the replication group should be configured at this time. The server you are configuring is not configured as a replication group member.

In the following example, the configuration of the CDS devices shows generalized input values. Option 5, vvimgw, is the VVIM. Add the VVIM as a replication group member.

Note Select a role for the new replication group member:

```
    1. ssv
    2. Vault
    3. cache
    4. Streamer
    5. vvimgw

Choice: device_role (1, 2, 3, 4, 5 or 6)
Enter an IP address for new CDS_device: IP_Address

Current replication group members:
device_role IP_Address

Do you want to add another replication group member? (yes/no) [n]: n
Configuring CDSM
Database is running.
Do you want to enable CDSM Redundancy ? (yes/no) [y]:
CDSM Virtual IP [172.22.99.106]:
Subnet Mask [255.255.254.0]:
Writing rc.local
CDSM configuration finished
cdsconfig finished, please use CDSM to complete configuration
```

```
[root]#
```

Step 6 View the contents of the hidden file /home/isa/.arroyorc and make sure that the file contains the following line:

dbdomsock /tmp/isadb

If the preceding line is not in the file, use a text editor to add the line. Close and save the .arroyorc file.

Step 7 To ensure that the AVS database (avsdb) and the Apache web server are started, issue the following commands and verify that a process ID exists for avsdb:

```
[root]# su - isa     //==== start avsdb
[isa]$ pgrep avsdb
28794                //==== verify avsdb process is running
[isa]$ exit
logout
[root]# /arroyo/www/bin/apachectl start   //==== start apache server
httpd: Could not reliably determine the server's fully qualified domain name, using
172.22.97.162 for ServerName

[root]#
```

Step 8 To verify that Stream Manager is operational, point your web browser to the Cisco CDE110 that hosts Stream Manager by entering the IP address using the following format:

`http://`*`Stream_Manager_ip_address`*

The Stream Manager Login page is displayed.

Step 9 Enter **admin** as the username and **admin** as the password and press **Login**.

If you are unable to log in with the username admin and the password admin, do the following:

a. Run the following command as *root* on the Cisco CDE110 that hosts Stream Manager:

```
[root]# /home/stats/runonce
```

b. Log in to the Stream Manager with the username *admin* and the password *admin*.

The CDSM Setup page is displayed.

Step 10 Use the Stream Manager to complete the configuration. For information on the other configuration tasks, see one of the following:

- For an ISA deployment, see the *Cisco TV CDS 2.1 ISA Software Configuration Guide*.
- For an RTSP deployment, see the *Cisco TV CDS 2.1 RTSP Software Configuration Guide*.

Installing and Configuring the Vaults, Caching Nodes, or Streamers

To install the TV CDS software and initially configure each Vault, Caching Node, or Streamer, do the following:

Step 1 Power on the CDE by pressing the Power button on the front of the CDE.

Step 2 Log in as **root** with the password **rootroot**.

So that your password for root is not the default password, use the **passwd** command to change the password used.

Step 3 Install the TV CDS software on the CDE by entering the following command and, depending on your deployment type, choose **1** for an ISA deployment and **2** for an RTSP/FSI deployment:

```
[root]# ./cdsinstall
```

You should see something similar to this:

```
Continuing first-time installation after kickstart using image //CDS-TV.iso
Select Deployment Type (ctrl-c to quit):
  1) ISA
  2) RTSP/FSI
1
ISA Selected
Mounting //CDS-TV.iso at /mnt/cdrom
Calling inst.sh for isa
Killing running processes: statsd

Un-taring isa-base.tgz
Calling forprod.sh
Removing RTSP-specific files
Installing ISA-specific files (existing files backed up to .file)
ISA installation complete

Starting fixperms.sh
   Loading File List
   Processing File List
Ending fixperms.sh
Unmounting /mnt/cdrom
inst.sh completed, removing .iso image
```

Step 4 If you are installing a version of software different then what is currently on the CDS-TV system, an example of the cdsinstall command to enter is:

```
[root]# ./cdsinstall CDS-TV-2.1.4.iso
```

You must reboot the system after running the install script. When the system has rebooted, login as root and continue with Step 5.

Step 5 Enter the following command to configure CDS:

```
[root]# cdsconfig
```

You should see something similar to this:

```
Please ensure an IP address and netmask are configured for
  management interface eth0:

Select an option or an interface to re-configure/disable:
    1. eth0     ip:172.22.99.237    mask:255.255.254.0    bcast:172.22.99.255
    2. Configure another interface
    3. Done
Choice [3]:
```

Step 6 Enter **1** and press **Enter**.

Step 7 You are asked if you want to disable interface eth0. Enter **N** for no and press **Enter**.

Step 8 Enter the IP address for eth0 when prompted.

Step 9 Enter the netmask for eth0 when prompted.

Step 10 Enter the broadcast address for eth0 when prompted. You should see something similar to this:

```
Select an option or an interface to re-configure/disable:
    1. eth0     ip:172.22.99.238    mask:255.255.254.0    bcast:172.22.99.255
    2. Configure another interface
```

```
    3. Done
Choice [3]:
```

Step 11 Enter **2** to configure another interface or **3** to complete this step and press **Enter**. You should see something similar to this:

```
Backing up old scripts in /etc/sysconfig/network-scripts
Writing new ifcfg-ethX scripts
```

Step 12 Enter a hostname when prompted.

Step 13 Enter the number of the Ethernet interfaces that connect to the gateway when prompted.

Step 14 Enter the default gateway IP address when prompted. You should see something similar to this:

```
Backing up /etc/sysconfig/network
Writing new /etc/sysconfig/network
Backing up /etc/hosts
Writing new /etc/hosts
Shutting down interface eth0:  [  OK  ]
Shutting down loopback interface:  [  OK  ]
PCI: Enabling device 0000:0e:00.0 (0000 -> 0003)
PCI: Enabling device 0000:0e:00.1 (0000 -> 0003)
Restarting network services, this may take a minute:
Shutting down loopback interface:  [  OK  ]
Bringing up loopback interface:  [  OK  ]
Bringing up interface eth0:  [  OK  ]
Network services restarted; may take a few seconds to establish connectivity
Reboot for hostname changes to take effect
Network configuration complete
Use detected platform: CDE420-4A-C ? (yes/no) [y]: y
Use detected platform: CDE420-4A-C ? (yes/no) [y]: y
```

Step 15 Enter the role for the CDE you are configuring and press **Enter**. The role options listed below shows all the options for the CDE220 and CDE420, but the options displayed by the cdsconfig script are determined by the platform selected.

```
Please select a device role:
    1. ssv
    2. Vault
    3. cache
    4. Streamer
```

Step 16 Enter the group ID when prompted.

Step 17 Enter the server ID when prompted.

Step 18 If the device role selected is a Streamer, you have the option to enter the Stream Control interface. Designating an interface as a stream control interface allows you to separate stream control traffic from stream traffic. You should see something similar to this:

```
Enter Stream Control interface (Hit 'Enter' to skip): eth1
Writing new configuration to /home/isa/.arroyorc

No existing replication group information found
Do you want to configure replication group members now? (yes/no) [y]: yes
There are currently no replication group members.
Do you want to add another replication group member? (yes/no) [y]: y
```

Note With the exception of the server you are configuring, all CDS devices (VVIMs, Stream Managers, ISVs, Vaults, and Streamers) that are members of the replication group should be configured at this time. The server you are configuring is not configured as a replication group member.

In the following example, the configuration of the CDS devices shows generalized input values. The option for the VVIM and Stream Manager is called "Controller." Add the VVIM and Stream Manager as a replication group members, as well as the Vaults, Caching Nodes, and Streamers.

```
Select a role for the new replication group member:
    1. ssv
    2. Vault
    3. cache
    4. Streamer
    5. Controller
```

Step 19 Enter the role for the CDE you are adding to the replication group and press **Enter**.

Step 20 Enter an IP address for the CDE when prompted. You should see something similar to this:

```
Current replication group members:
  Vault         172.22.99.239
Do you want to add another replication group member? (yes/no) [n]:
```

Step 21 Enter **Y** for yes to add another CDE to the system or **N** for no and press **Enter**. If you entered Y, you are prompted to select a role and enter the IP address. If you entered N, you should see something similar to this:

```
Configuring ISA ecosystem
/home/isa/Berkeley/status_db:
dbstatus: Subscript out of range.
Starting statsd
Run svrinit to seed database? (yes/no) [n]: y
```

Step 22 Enter **Y** for yes to run svrinit to seed the database or **N** for no and press **Enter**.

Note Always enter **Y** because you must seed the database whenever you are adding a new CDE to a network, or installing the TV CDS software on a CDE.

a. Enter the IP address of the CDE for svrinit when prompted.

b. Enter the netmask for svrinit when prompted.

c. Enter the hostname for svrinit when prompted. You should see something similar to this:

```
Writing rc.local
ISA ecosystem configuration finished
cdsconfig finished, please use CDSM to complete configuration
[root@v238 ~]#
```

If you receive an error message saying the database is unavailable and cannot set things up, enter the following command to initialize the database tables:

```
[root]# su - isa (For ISA deployments only.)
[isa]# exit
[root]# /home/stats/svrinit_15 -h <hostname> -i <ip address> -s <mask-ip address>
```

Note For ISA deployments only, if avsdb is not running, enter the **`su - isa`** command as user root before entering the **`/home/stats/svrinit_15...`** command above.

Note The database synchronization takes about five minutes before the server becomes ready for service. If the database is very large, it could take longer than five minutes to seed the database. In this case, wait awhile longer and retry the **svrinit_15** command.

Step 23 Verify connectivity to the VVIM or Stream Manager by performing the following steps:

a. Point your web browser to the device that hosts the VVIM or Stream Manager by entering the IP address:

```
http://XXX.XXX.XXX.XXX
```

The VVIM or CDSM Login page is displayed.

b. Enter **admin** as the username and **admin** as the password and click **Login**.

The System Health Monitor page is displayed showing the devices and their IP address.

The TV CDS software installation is complete.

Upgrading to Release 2.1

This section includes the following topics:

Note Release 2.1.4 supports software upgrades only from Release 1.5.1.x, Release 2.0, and Release 2.1.3for CDS ISA and CDS RTSP environments. Upgrades for VVI are only supported for new systems installed with Release 2.1.3.

Release 2.1 introduces the ability to route interfaces to different subnets. After upgrading the TV CDS software to Release 2.1, any servers with incompatible routes are listed in red on the Route Tables page. You can review the Route Table configuration for each of these servers, modify or delete the routes, and click **Submit** to apply the changes. The routes are converted to the Release 2.1 format and the server is listed in black. When all servers with incompatible routes are fixed, the warning message is removed and the entry in the system alarm drop-down list in the GUI banner is removed.

Release 2.1 also introduces the ability to configure up to 16 DNS servers on each of the System Level, Array Level, and Server Level DNS pages. After upgrading the TV CDS software to Release 2.1, any DNS entries need to be resubmitted. When all DNS entries are resubmitted, the warning message is removed and the entry in the system alarm drop-down list in the GUI banner is removed.

Note During the initialization process of a CDS server or after recovering a CDS server that has been down for more than an hour, the CDS database performs a complete synchronization. The database synchronization takes about five minutes before the server becomes ready for service. If the CDS server

is down for a much longer time than an hour, the database synchronization takes longer than five minutes. The netstat command will not show the interfaces as up until the synchronization has completed.

Note Downgrading from Release 2.1 to Release 2.0 is a manual process, requiring a reload of the old database files. Any changes made to configuration or content after upgrading to Release 2.1 are lost.

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

1. Upgrade CDSM to Release 2.1
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 2.1 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.

Upgrading from Release 1.5.1.x

Note Because the software upgrade to Release 2.1 includes upgrading the operating system, a Cisco technician will perform the upgrade. The procedures described in this section are informational only. (EDCS-760974)

The Cisco technician will have the following items to upgrade your software to Release 2.1:

- 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-2.1.4.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 2.1 software.
6. Run the post-install script. This fixes the disk partitions.
7. Install the TV CDS Release 2.1 software and nattily 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 CDS server.
4. Install the Red Hat Enterprise Linux 5 (32-bit) operating system.
5. Insert the CD-ROM with the TV CDS Release 2.1 software.
6. Install the TV CDS Release 2.1 software and initially configure the CDS server.
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.

Note For ISA services to run as high priority (-16) on the vault, set the ISA permissions to "ISA hard priority -16" in the /etc/security/limit.conf file. Then restart the inetd service by entering the following command.

```
# killall -HUP inetd
```

If this is not done, you will receive the error "setpriority: Permission denied" in the ns_log when ISA services are starting up. The ISA services will still be up but the default priority will be (0).

Upgrading from Release 2.0 to Release 2.1.4

Upgrading the CDSM and CDS servers from Release 2.0 to Release 2.1.4 involves the following steps:

1. Download the ISO image file from the Cisco software download website.
2. Copy the file to each server.
3. For Streamers and Vaults, enable the Offload Server option.
4. Run the cdsinstall script.
5. For Streamers and Vaults, disable the Offload Server option.

Note Because Release 2.1 introduces the ability to route interfaces to different subnets, the route table information for each server needs to be recorded before upgrading the TV CDS software. Log in to the CDSM, go the **Configure > Server Level > Route Table** page and write down the Route Table information for each CDS server.

After upgrading the TV CDS software to Release 2.1, any servers with incompatible routes are listed in red on the Route Tables page. You can review the Route Table configuration for each of these servers, modify or delete the routes using the information you recorded, and click **Submit** to apply the changes. For more information, see either the *Cisco TV CDS 2.1 ISA Software Configuration Guide* or the *Cisco TV CDS 2.1 RTSP Software Configuration Guide*.

The following procedures are covered in this section:

- Getting a Software File from Cisco.com, page 35
- Upgrade the Software on the CDSM, page 36
- Upgrade the Software on Each Streamer and Vault, page 37

Getting a Software File from Cisco.com

To get a software file from Cisco.com, do the following:

Step 1 Launch your web browser and enter the following URL:

http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=268438145

The Log In page is displayed.

Step 2 Log in to Cisco.com using your designated username and password. The Video and Content Delivery page is displayed, listing the available software products.

Step 3 Click **Content Delivery Systems**. The Downloads page is displayed.

Step 4 Click the **Cisco Content Delivery Applications** folder to expand it, and click the **Cisco TV Application**. The page refreshes and the software releases are displayed.

Step 5 Click the software release you want. The page refreshes and the software image files are displayed.

Step 6 Click the link for the software image file you want.

- If this is the first time you have downloaded a file from Cisco.com, the Cisco Systems Inc., Encryption Software Usage Handling and Distribution Policy is displayed. Read the policy, fill in the unfilled fields, and click **Accept**.
- If you previously filled out the Encryption Software Usage and Handling and Distribution form, the form does not display again.

The Download page is displayed with the information about the software image file and a Download link.

Step 7 Click **Download**. The Cisco End User Software License Agreement is displayed.

Step 8 Read the agreement and click **Agree**. The File Download dialog box is displayed.

Step 9 Click **Save**. The Save As dialog box is displayed.

Step 10 Navigate to the location where you want to save the file and click **Save**. The file downloads.

Upgrade the Software on the CDSM

Note The software upgrade procedure for the CDSM requires that the cdsinstall script exists on the server in the /root directory. All CDEs that shipped with Release 2.0 have the cdsinstall script. All CDEs that were upgraded to Release 2.0 from a previous release do not have the cdsinstall script. If necessary, download the cdsinstall script from the Cisco.com website. See the "Getting a Software File from Cisco.com" section on page 35 for more information on downloading a file from Cisco.com.

To upgrade the software on the CDSM, do the following:

Step 1 Log in to the CDSM Linux operating system as *root*.

Step 2 Copy the ISO image file to the CDSM. For example, if the ISO image file (CDS-TV-2.1.4.iso) is stored in a directory (images) on a server (172.22.98.111), the following command is used:

```
# scp 172.22.98.111:/images/2.1/CDS-TV-2.1.4.iso /root
```

Step 3 If the CDSM was upgraded to Release 2.0 from a previous release, copy the cdsinstall script to the CDSM.

```
# scp 172.22.98.111:/images/2.1/cdsinstall /root
```

Step 4 Upgrade the CDS software on the CDSM by entering the following command, and when prompted, enter the deployment type.

```
# ./cdsinstall CDS-TV-2.1.4.iso

Select Deployment Type (ctrl-c to quit):
  1) ISA
  2) RTSP/FSI
  3) CDSM
  4) CDSM with ISA
```

```
--- Output omitted ---
```

Step 5 Reboot the CDSM.

```
# reboot
```

Step 6 Verify that the database is running on the CDSM.

```
ps -ef | grep avsdb
```

Upgrade the Software on Each Streamer and Vault

Perform this procedure for each Vault and Streamer in the CDS.

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.

Note When upgrading from Release 2.0.x to Release 2.1.x in an RTSP environment, because of database changes, the CDSM server offload function does not work correctly. You need to offload the CDS servers manually by entering the following command:

For Vaults:

- touch /var/tmp/TRICKLE_DOWN

For Streamers:

- touch /var/tmp/TRICKLE_DOWN
- echo 1 > /proc/calypso/tunables/offline

To upgrade the software on a Vault or Streamer, do the following:

Step 1 Using the CDSM GUI, offload the server.

a. Click **Maintain > Servers > Server Offload**. The Server Offload page is displayed.

b. From the **Server IP** drop-down list, choose a server's IP address or nickname and click **Display**. The server type and ID, as well as the array ID, are displayed.

c. Select **Enable** and click **Submit**.

Step 2 Check the CDSM to verify that the stream count on the offline server is zero.

a. Using the CDSM, click **Monitor > Server Level > NIC Monitor**.

b. From the **Server IP** drop-down list, choose a server and click **Display**.

c. Click **Graph Ports** to view any stream traffic.

Step 3 Log in to the Vault or Streamer Linux operating system as *root*.

Step 4 Copy the ISO image file to the CDS server. For example, if the ISO image file (CDS-TV-2.1.4.iso) is stored in a directory (images) on a server (172.22.98.111), the following command is used:

```
# scp 172.22.98.111:/images/2.1/CDS-TV-2.1.4.iso /root
```

Step 5 If the CDS server was upgraded to Release 2.0 from a previous release, copy the cdsinstall script to the CDS server.

```
# scp 172.22.98.111:/images/2.1/cdsinstall /root
```

Step 6 Upgrade the CDS software on the CDS server by entering the following command, and when prompted, enter the deployment type.

```
# ./cdsinstall CDS-TV-2.1.4.iso

Select Deployment Type (ctrl-c to quit):
  1) ISA
  2) RTSP/FSI
  3) CDSM
  4) CDSM with ISA

    --- Output omitted ---
```

Step 7 Using the CDSM GUI, reboot the server.

a. Click **Maintain > Servers > Server Restart**. The Server Restart page is displayed.

b. From the **Server IP** drop-down list, choose the IP address of the server and click **Display**.

c. From the **Restart** drop-down list, choose Yes and click **Submit**.

Step 8 Using the CDSM GUI, wait for the server to come online.

a. Click Monitor > System Health. The System Health page is displayed.

b. The colored boxes for the server should all be green.

Step 9 Using the CDSM GUI, disable Server Offload.

a. Click **Maintain > Servers > Server Offload**. The Server Offload page is displayed.

b. From the **Server IP** drop-down list, choose a server's IP address or nickname and click **Display**. The server type and ID, as well as the array ID, are displayed.

c. Select **Disable** and click **Submit**.

Step 10 Repeat this procedure for the rest of the Vaults and Streamers.

Upgrading from Release 2.1.3 to Release 2.1.4

Note Before upgrading to Release 2.1.4, log in to the CDSM, choose **Configure > Server Level > RTSP Server**, select the IP address of a Streamer and write down the settings for the SOP fields for each Streamer.

Upgrading the CDSM and CDS servers from Release 2.1.3 to Release 2.1.4 involves the following steps:

1. Download the ISO image file from the Cisco software download website.
2. Copy the file to each server.

3. For Streamers and Vaults, enable the Offload Server option.
4. Run the cdsinstall script.
5. For Streamers and Vaults, disable the Offload Server option.

The following procedures are covered in this section:

- Getting a Software File from Cisco.com, page 35
- Upgrade the Software on the CDSM, page 36
- Upgrade the Software on Each Streamer and Vault, page 37

Upgrading a VVI from Release 2.1.3 to Release 2.1.4

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

1. Upgrade VVIM to Release 2.1.4. Follow the "Upgrade the Software on the CDSM " procedure on page 40.
2. Upgrade the Super Headends (SHEs) one at a time. Within one SHE, upgrade the slave Vault and finish with the master Vault. To identify the slave Vault, log in to the Vault as *isa*, change to the /home/isa/IntegrationTest directory and run the following command:

```
[isa@vault220 ~/IntegrationTest]$ ./show_calypso_services
************************************************************
********** ContentStore (SLAVE) Services Status ************
************************************************************
ContentStoreSlave ======> Running
************************************************************
************************************************************
************************************************************
```

   Follow the "Upgrade the Software on Each Streamer and Vault" procedure on page 41. When all SHEs are upgraded, there will be Vaults running Release 2.1.4 coexisting with Caching Nodes and Streamers running Release 2.1.3.
3. Upgrade each video hub office (VHO) one at a time. Within one VHO, upgrade the CDS servers and CDSM in the following order:
   a. Caching Nodes (Follow the "Upgrade the Software on Each Streamer and Vault" procedure on page 41.)
   b. Stream Manager (Follow the "Upgrade the Software on the CDSM " procedure on page 40.)
   c. 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). Follow the "Upgrade the Software on Each Streamer and Vault" procedure on page 41.
   d. Repeat for every Streamer on the site starting with the "Available" Streamers, followed by the "Backup" Streamer, and ending with the "Primary" Streamer. To identify the Streamers, use the following command:

```
[root@s65 root]# cat /proc/calypso/status/streamer/resiliencyinfo
    Streamer Resiliency Info:
        Service Address: 172.22.98.50
        Control Service: Primary
```

Note The Release 2.1.3 software can coexist with the Release 2.1.4 software. Therefore, long upgrade windows are possible.

Getting a Software File from Cisco.com

To get a software file from Cisco.com, do the following:

Step 1 Launch your web browser and enter the following URL:

http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=268438145

The Log In page is displayed.

Step 2 Log in to Cisco.com using your designated username and password. The Video and Content Delivery page is displayed, listing the available software products.

Step 3 Click **Content Delivery Systems**. The Downloads page is displayed.

Step 4 Click the **Cisco Content Delivery Applications** folder to expand it, and click the **Cisco TV Application**. The page refreshes and the software releases are displayed.

Step 5 Click the software release you want. The page refreshes and the software image files are displayed.

Step 6 Click the link for the software image file you want.

- If this is the first time you have downloaded a file from Cisco.com, the Cisco Systems Inc., Encryption Software Usage Handling and Distribution Policy is displayed. Read the policy, fill in the unfilled fields, and click **Accept**.
- If you previously filled out the Encryption Software Usage and Handling and Distribution form, the form does not display again.

The Download page is displayed with the information about the software image file and a Download link.

Step 7 Click **Download**. The Cisco End User Software License Agreement is displayed.

Step 8 Read the agreement and click **Agree**. The File Download dialog box is displayed.

Step 9 Click **Save**. The Save As dialog box is displayed.

Step 10 Navigate to the location where you want to save the file and click **Save**. The file downloads.

Upgrade the Software on the CDSM

Note The software upgrade procedure for the CDSM requires that the cdsinstall script exists on the server in the /root directory. All CDEs that shipped with Release 2.0 have the cdsinstall script. All CDEs that were upgraded to Release 2.0 from a previous release do not have the cdsinstall script. If necessary, download the cdsinstall script from the Cisco.com website. See the "Getting a Software File from Cisco.com" section on page 35 for more information on downloading a file from Cisco.com.

To upgrade the software on the CDSM, do the following:

Step 1 Log in to the CDSM Linux operating system as *root*.

Step 2 Copy the ISO image file to the CDSM. For example, if the ISO image file (CDS-TV-2.1.4.iso) is stored in a directory (images) on a server (172.22.98.111), the following command is used:

```
# scp 172.22.98.111:/images/2.1/CDS-TV-2.1.4.iso /root
```

Step 3 If the cdsinstall script is not found in the /root directory on the CDSM, copy the cdsinstall script to the CDSM.

```
# scp 172.22.98.111:/images/2.1/cdsinstall /root
```

Step 4 Upgrade the CDS software on the CDSM by entering the following command, and when prompted, enter the deployment type.

```
# ./cdsinstall CDS-TV-2.1.4.iso

Select Deployment Type (ctrl-c to quit):
  1) ISA
  2) RTSP/FSI
  3) CDSM
  4) CDSM with ISA

    --- Output omitted ---
```

Step 5 Reboot the CDSM.

```
# reboot
```

Step 6 Verify that the database is running on the CDSM.

```
ps -ef | grep avsdb
```

Upgrade the Software on Each Streamer and Vault

Perform this procedure for each Vault and Streamer in the CDS.

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.

To upgrade the software on a Vault or Streamer, do the following:

Step 1 Using the CDSM GUI, offload the server.

a. Click **Maintain > Servers > Server Offload**. The Server Offload page is displayed.

b. From the **Server IP** drop-down list, choose a server's IP address or nickname and click **Display**. The server type and ID, as well as the array ID, are displayed.

c. Select **Enable** and click **Submit**.

Step 2 Check the CDSM to verify that the data traffic on the offline server is zero.

a. Using the CDSM, click **Monitor > Server Level > NIC Monitor**.

b. From the **Server IP** drop-down list, choose a server and click **Display**.

c. Click **Graph Ports** to view any data traffic.

Step 3 Log in to the Vault or Streamer Linux operating system as *root*.

Step 4 Copy the ISO image file to the CDS server. For example, if the ISO image file (CDS-TV-2.1.4.iso) is stored in a directory (images) on a server (172.22.98.111), the following command is used:

```
# scp 172.22.98.111:/images/2.1/CDS-TV-2.1.4.iso /root
```

Step 5 If the cdsinstall script is not found in the /root directory on the CDS server, copy the cdsinstall script to the CDS server.

```
# scp 172.22.98.111:/images/2.1/cdsinstall /root
```

Step 6 Upgrade the CDS software on the CDS server by entering the following command, and when prompted, enter the deployment type.

```
# ./cdsinstall CDS-TV-2.1.4.iso

Select Deployment Type (ctrl-c to quit):
  1) ISA
  2) RTSP/FSI
  3) CDSM
  4) CDSM with ISA

    --- Output omitted ---
```

Step 7 Using the CDSM GUI, reboot the server.

a. Click **Maintain > Servers > Server Restart**. The Server Restart page is displayed.

b. From the **Server IP** drop-down list, choose the IP address of the server and click **Display**.

c. From the **Restart** drop-down list, choose Yes and click **Submit**.

Step 8 Using the CDSM GUI, wait for the server to come online.

a. Click Monitor > System Health. The System Health page is displayed.

b. The colored boxes for the server should all be green.

Step 9 Using the CDSM GUI, disable Server Offload.

a. Click **Maintain > Servers > Server Offload**. The Server Offload page is displayed.

b. From the **Server IP** drop-down list, choose a server's IP address or nickname and click **Display**. The server type and ID, as well as the array ID, are displayed.

c. Select **Disable** and click **Submit**.

Step 10 Repeat this procedure for the rest of the Vaults and Streamers.

Adding a Second CDSM

To implement the CDSM Redundancy feature available in Release 2.1, do the following after upgrading all existing servers to Release 2.1:

Step 1 If the Cisco CDE110 is not powered on, press the front panel power switch on the server.

The operating system boots.

Step 2 Log in as *root* with the password *rootroot*.

Note So that your password for root is not the default password, use the **passwd** command to change the password used.

Step 3 Run the **cdsinstall** script and select your deployment type, choose 3 (CDSM) or 4 (CDSM w/ ISA).

```
[root]# ./cdsinstall
```

The following prompt is displayed:

```
Continuing first-time installation after kickstart using image //CDS-TV.iso
Select Deployment Type (ctrl-c to quit):
  1) ISA
  2) RTSP
  3) CDSM
  4) CDSM with ISA
3
CDSM Selected

... Output omitted ...

Unmounting /mnt/cdrom
inst.sh completed, removing .iso image

================================================
Configure the system for initial installation
================================================
```

Step 4 Copy the DATADIR directory from the existing CDSM to the new CDSM. For example, if the existing CDSM has an IP address of 172.22.98.109, the following command is used:

```
# scp -r 172.22.98.109:/arroyo/db/DATADIR /arroyo/db
```

Step 5 Run the **cdsconfig** script and answer "Y" to the "Do you want to enable CDSM redundancy?" prompt. Answer appropriately for the prompts for getting the ID from the first CDSM.

For more detail about the cdsconfig script, see the "Installing and Configuring the Stream Manager" section on page 25.

Step 6 When the cdsconfig script completes, edit the rc.local file and uncomment all the command lines. The su - isa -c "cd /home/isa/RTScehduler/Exporter..." command is only used for the MediaX feature when notifications need to be exported to a catalog server or similar. Following is an example with all the lines uncommented.

```
# vi /etc/rc.local
    #!/bin/sh
    #
    # This script will be executed *after* all the other init scripts.
    # You can put your own initialization stuff in here if you don't
    # want to do the full Sys V style init stuff.

    touch /var/lock/subsys/local

    # Lines below this one modified by cdsflavconfig (ISA):

    su - isa -c "cd /home/isa/IntegrationTest"

    sleep 30

    /arroyo/www/bin/apachectl start

    sleep 30
```

```
su - isa -c "cd /home/isa/RTScheduler/Exporter; ./ExporterServer >&
/home/isa/RTScheduler/Exporter/ExporterServer.log&"


/home/stats/statsd -i 172.11.99.100 -s 255.255.255.0 -d eth0

sleep 30
```

Step 7 Reboot the CDSM.

```
# reboot
```

Step 8 On each CDS server and the first CDSM, do the following:

a. Log in to the server as user ***isa***.

b. Edit the .arroyorc file and add the new CDSM as a replication member. Following is an example of the .arroyorc file.

```
$ vi /home/isa/.arroyorc
# Local settings
    self 2
    groupid 400
    serverid 141
    partno 3U-SCSI-10
    mirroring 0
    mgmtif 0
    ingestif 1

# Database Params
    dbdomsock /tmp/isadb
    dbnetport 9999

# Replication Group Members
    Vault 111.0.110.40
    controller 111.0.110.42
```

c. Restart the database.

```
[root]# su - isa (For ISA deployments only.)
[isa]# exit
[root]# /home/stats/svrinit_15 -h <hostname> -i <ip address> -s <mask-ip address>
```

Note For ISA deployments only, if avsdb is not running, enter the **su - isa** command as user root before entering the **/home/stats/svrinit_15...** command above.

Updating the Device Drivers for new SSDs

The SSD driver update is for new SSDs and to address an issue with older SSDs. For more information, see the "Important Notes" section on page 3.

If a CDE requires an SSD replacement, the device driver must be updated. The device driver must be updated before replacing the SSD. If a new CDE is being added to the CDS, after upgrading the TV CDS software, the device driver must be updated. New SSDs are not recognized with the proper attributes until the device driver is updated.

Note The new driver is 100 percent backward-compatible with older, pre-existing SSD drives. We recommend that a proactive upgrade of the SSD driver is a good best-practice.

To view a list of TV CDS software releases this device driver applies to see the defect, CSCtr29064, in the Bug Tool Kit ((http://tools.cisco.com/Support/BugToolKit/).

Note When using the **cdsinstall** script to install the software image file, install the driver package after the **cdsinstall** script is complete.

To install the device driver update package, do the following:

Step 1 Download the cdstv_x.y.z_CSCtr29064.bin driver update package to the /root directory of the CDE. The filename is cdstv_x.y.z_CSCtr29064.bin,where x.y.z denotes the software release.

Note The driver update package includes support for all applicable software releases, so any cdstv_x.y.z_CSCtr29064.bin file installs correctly and can be used to update the drivers for any applicable release.

Following is the md5 checksum for the cdstv_x.y.z_CSCtr29064.bin driver update package:

```
89684e2094d841b236ba1d83e958df9b cdstv_x.y.z_CSCtr29064.bin
```

The driver update package is a self-extracting, self-installing package.

Step 2 Change the permissions on the CDE. As user *root*, enter the following command:

```
# chmod 755 /root/cdstv_x.y.z_CSCtr29064.bin
```

Step 3 Install the device driver update. As user *root* user enter the following commands:

```
# cd /root
# ./cdstv_x.y.z_CSCtr29064.bin
```

The package installs the device driver.

Step 4 To verify that the package has been installed on the CDE, view the /etc/cisco-version-history file, and verify that the string “cdstv_CSCtr29064” has been added to this version-history file.

Step 5 To verify that the driver has been updated and will be used by the CDS server, enter the following commands:

```
cd /lib/module/`uname -r`
/sbin/modinfo -F version csd.ko cdd_sys.ko
```

The updated driver files report the same version for both driver files in the format of x.y.z.1, where x.y.z is the version of the TV CDS software (for example, 2.3.3.1).

Step 6 Reboot the CDS server.

```
# reboot
```

Note Rebooting a Vault server does not interrupt stream services, but causes current ingests to fail. If your CDS does not have stream failover, rebooting a Streamer without offloading it interrupts all stream services. If possible, you should perform functions that require a system restart during times when the least number of users are actively connected to your system.

A new SSD drive is a Generation 2 front-mounted SSD. The new SSD model is identified by the title "Intel SSD 320 Series" on the label and has the model number: SSDSA2BW160G3. For more information, see Field Notice 63438 at: http://www.cisco.com/en/US/products/ps7126/prod_field_notices_list.html.

The following command provides information on the external SSDs that are the new drive model:

```
# find /sys/devices -name "model" | xargs grep SSDSA2BW16
/sys/devices/pci0000:80/0000:80:05.0/0000:87:00.0/host3/port-3:7/end_device-3:7/target3:0:7/3:0:7:0/model:INTEL SSDSA2BW16
/sys/devices/pci0000:80/0000:80:05.0/0000:87:00.0/host3/port-3:6/end_device-3:6/target3:0:6/3:0:6:0/model:INTEL SSDSA2BW16
/sys/devices/pci0000:80/0000:80:05.0/0000:87:00.0/host3/port-3:5/end_device-3:5/target3:0:5/3:0:5:0/model:INTEL SSDSA2BW16
/sys/devices/pci0000:80/0000:80:05.0/0000:87:00.0/host3/port-3:4/end_device-3:4/target3:0:4/3:0:4:0/model:INTEL SSDSA2BW16
/sys/devices/pci0000:80/0000:80:05.0/0000:87:00.0/host3/port-3:3/end_device-3:3/target3:0:3/3:0:3:0/model:INTEL SSDSA2BW16
```

To view all SSD models currently supported by the Cisco TV CDS software, enter the following command:

```
# find /sys/devices -name "model" | xargs grep SSDSA
```

The older SSD model is INTEL SSDSA2M160.

Rolling Back the SSD Driver Update

If for any reason you need to revert to the older SSD driver, with the TV CDS software running on the CDS server, do the following:

Step 1 Change to the drivers directory.

```
cd /lib/module/`uname -r`
```

Step 2 To save the updated driver (optional), enter the following command:

```
cp csd.ko csd.ko.update
cp cdd_sys.ko cdd_sys.ko.update
```

Step 3 Rename the backed up driver files to the driver filenames. The "previous_version" is the version number of the driver update.

```
cp csd.ko_bkup_<previous_version> csd.ko
cp cdd_sys.ko_bkup_<previous_version> cdd_sys.ko
```

Step 4 Verify the driver versions by using the following command:

```
/sbin/modinfo -F version csd.ko cdd_sys.ko
```

The drivers before the driver update have a version in the format of a.b.c and the two drivers do not necessarily have the same version number.

Step 5 Reboot the CDS server.

Related Documentation

Refer to the following documents for additional information about the Cisco TV CDS 2.1:

- *Cisco TV CDS 2.1 ISA Software Configuration Guide*

  http://www.cisco.com/en/US/docs/video/cds/cda/tv/2_1/configuration/isa_guide/tv_cds_2_1_isa_cfguide.html

- *Cisco TV CDS 2.1 RTSP Software Configuration Guide*

  http://www.cisco.com/en/US/docs/video/cds/cda/tv/2_1/configuration/rtsp_guide/tv_cds_2_1_rtsp_cfguide.html

- *Cisco TV CDS 2.1 API Guide*

  http://www.cisco.com/en/US/docs/video/cds/cda/tv/2_1/developer_guide/tv_cds_2_1_apiguide.html

- *Cisco Content Delivery System 2.x Documentation Roadmap*

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

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

  http://www.cisco.com/en/US/docs/video/cds/cde/cde205_220_420/installation/guide/cde205_220_420_hig.html

- *Cisco Content Delivery Engine 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*

  http://www.cisco.com/en/US/docs/video/cds/cde/installation/guide/CDE_Install_Book.html

- *Regulatory Compliance and Safety Information for Cisco Content Delivery Engines*

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

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

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

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

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

Obtaining Documentation and Submitting a Service Request

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

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

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