Release Notes for Cisco TV CDS 2.1.1

These release notes cover Cisco TV CDS Release 2.1.1.

Revised: August 2009 OL-19660-02

Contents

The following information is in the release notes:

New Features

Release 2.1 of the Cisco TV CDS introduces the following new features:

- Cisco Virtual Video Infrastructure (VVI)
  - Content Library
  - Content Cache
  - Virtual Video Infrastructure Manager
- Shared Content Store
- Library Site Redundancy
- Local Cache-Fill
- NAT Traversal
- CDSM Redundancy
- New Hardware Configurations Supported
  - Dense Vault: CDE220 (2A)
  - Caching Node: CDE420 (4G)

Cisco Virtual Video Infrastructure (VVI)

The Cisco TV CDS Release 2.1 introduces support for the Virtual Video Infrastructure. The Cisco Virtual Video Infrastructure (VVI), built using proven Cisco Content Delivery System (CDS) technology, provides a highly scalable foundation for storing, managing, and distributing personalized TV and video services across national and transnational video networks.

The main functions offered by the Cisco Virtual Video Infrastructure (VVI) are

- Content Library
- Content Cache
- Virtual Video Infrastructure Manager

Content Library

The Content Library consists of one or two Vault Arrays and is responsible for content acquisition, content adaptation, reliable storage, and content propagation.

Content Acquisition

Offers support for multiple content acquisition protocols for both Asset-based and Real-Time content. Following is a list of the supported control plane protocols in the Cisco TV CDS Release 2.1:

- FSI
- SOAP/XML
- NGOD A3 and A5

Following is a list of the supported data plane protocols in the Cisco TV CDS Release 2.1:

- FTP Pull (asset based acquisition)
- IP Multicast (real-time acquisition)

These interfaces are also supported in the Cisco TV CDS Release 2.0. Enhancements to these interfaces specific to the Cisco TV CDS Release 2.1 are documented in the "Enhancements" section on page 6.

Content Adaptation

This function processes and modifies acquired content for optimized storage and propagation. This process is also responsible for trick-mode files generation.

Reliable Storage

The Content Library persistently stores redundant copies of video assets.

Create copies of assets (mirroring) based on predefined policies to guarantee high availability of content in the case of server-level or component-level failures. See the "Library Site Redundancy" section on page 4 for more information.

Content Propagation

The Content Library is responsible for "filling" the cache in the Streamers with popular content by propagating the required content segments to the Streamers. Cisco Vault application supports an average cache-fill throughput of 6.5 Gbps on a CDE420-4A hardware and 4.7 Gbps on a CDE220-2A hardware platform.

Content Cache

Content Cache is a new Content Delivery Application (CDA) introduced in Cisco TV CDS Release 2.1 It runs on the Caching NOde CDE and acts as an additional cache between the Content Library and the Streamers. Content Cache improves caching efficiency of CDS and lowers the bandwidth required in the backbone of a large, nationwide content delivery network. The Content Cache CDA is responsible for the following functions:

Content Acquisition

Locates asset and request Cache Fill of content from the CDS Content Library in a Cache Miss scenario

Content Caching

Dynamic Content Cache. Aging heuristics take into account content popularity and how long content has been in the cache.

Content Propagation

Provides High-Performance Asset Propagation (Segmented Cache Fill) from Content Library to downstream caches

Offers cache-fill priority capability, which prioritizes cache-filling groups and where each Caching Node could receive their content from (including local Content Libraries)

Supports Cache Fill from local Caching Nodes belonging to the same Caching Node Array.

Supports hierarchical caching tiers with the ability to Fill from a higher tier Caching Node Array rather than directly from the Content Library.

Virtual Video Infrastructure Manager

The Virtual Video Infrastructure Manager (VVIM) is a new Content Delivery Application (CDA) being introduced with the Cisco TV CDS Release 2.1. It allows users to manage the Content Library and Caching functions of the VVI network. The Streaming function in the edge domains (stream domains)

are managed separately by CDS Managers (Stream Managers). VVI Manager and CDS Manager together offer what is known as *split-domain management*, which allows independent scaling of monitoring and reporting capabilities required for each domain. VVI Manager is typically deployed in a redundant configuration for server-level redundancy in managing the VVI network. VVI Manager interacts with the CDS Managers deployed in the edge domains where the CDS Streamers are deployed.

Shared Content Store

This feature offers the ability to ingest content from multiple sites. CDS-Vault Array can interface with multiple Video Back Office (VBO) systems to trigger ingests. Content is ingested only once and shared across multiple regions.

CDSM enhancements to configure multiple ingest sites are also supported in TV CDS Release 2.1.

Library Site Redundancy

The Library Site Redundancy feature ensures that at least one copy of each piece of content that is ingested into a Vault Group will be mirrored to another Vault Group that typically exists in another geographic location. This would guarantee the Content will be available in the case of an outage of any one site.

The TV CDS Release 2.1 will support mirroring across two (2) Vault Arrays.

In addition, the content mirroring with in a Vault Group can still be used to create multiple copies within each Vault Group to protect from server-level and component-level failures.

Library Site Redundancy is configured and managed through the VVI Management system.

Local Cache-Fill

This new feature allows a Caching NOde to fill content from another Caching NOde. Similarly, a Streamer can also fill content from another Streamer when this capability is enabled. This improves effective cache gain and reduces backbone traffic. It also adds additional resiliency to the system in cases where connectivity is lost between sites.

NAT Traversal

In the IPTV universe it is very common for subscriber premises to have a NAT (Network Address Translator) device deployed. The NAT device maps internal private IP addresses into external public IP addresses. More commonly only one external IP address is presented publicly, while multiple internal IP addresses are mapped to different port numbers on the same external IP address. Another functional behavior of the NAT is in-bound filtering. The NAT device drops packets to an IP address/port pair for which no mapping is active.

Traversal of the NAT for bidirectional protocols such as TCP is straightforward. However protocols such as SIP or RTSP which convey the destination address of a media stream are problematic, since the NAT typically does not inspect L7 signaling and extract the address for future reference. Further complicating NAT traversal is the variety of behaviors exhibited by NAT devices. In some cases these behaviors are dynamic and change over time. One type of NAT behavior is very open and allows all

inbound packets to be forwarded. Another type restricts the forwarding to any port on an IP address that has previously been learned or authorized. The most restrictive (symmetrical NAT) only forwards packets from an IP address and port number tuple that has been previously learned or authorized.

The Cisco TV CDS Release 2.1 introduces support for STUN and ICE protocols on the CDS TV Streamers and will enable delivery of unicast video to STBs deployed behind NAT devices.

Both on-vpath (Session Set Up initiated from the STB to the Video server that will also deliver the video) and off-vpath (Session Set Up initiated from the STB to a Session Manager device separated from the Video server that will also deliver the video) type deployment are supported.

CDSM Redundancy

The Cisco TV CDS Release 2.1 introduces support for Active-Standby 1+1 server level redundancy for the CDS Manager and VVI Manager applications. A floating, virtual IP address is used for all external interfaces (web browsers, APIs, and so on) to the management application. The CDS servers (Vault, Caching Node, Streamer, and ISV) participate in replication with both the primary and secondary CDSMs. However, the CDS servers can only retain up to one hour of reporting data, so if a CDSM is down for over an hour, when the CDSM recovers, it will only be able to get the last hour of reporting data from each CDS server, which means the reporting data will not be synchronized between the primary and secondary CDSMs.

New Hardware Configurations Supported

The Cisco TV CDS Release 2.1 introduces support for the following new hardware configurations:

Dense Vault: CDE220 (2A)

In particular the following Copper and Fiber models and respective CDE Bundle PIDs are supported

CDE220 Model	CDE Bundle PID
CDE220-2A-C	CB-32-12A1T-2QTX
CDE220-2A-F	CB-32-12A1T-4DSX

Caching Node: CDE420 (4G)

In particular the following Copper and Fiber models and respective CDE Bundle PIDs are supported.

CDE220 Model	CDE Bundle PID
CDE420-4G-C	CB-32-24S450-3QTX
CDE420-4G-F	CB-32-24S450-3QSX

See the CDE Datasheet for details on these CDEs.

Enhancements

The enhancements in the Cisco TV CDS Release 2.1 software are the following?

- Non-blocking FTP pull
- FSI Ingest Redundancy
- Disable Trick-mode on playlist
- CDSM 2.1 Enhancements
- SNMP MIB Enhancements
- Trick-mode History with time range
- Multiple R2 Connections
- Low Bandwidth Links (Thin Pipes)

Table below describes the enhancements introduced with the Cisco TV CDS Release 2.1.

Enhancements	Descriptions	Category
Non-blocking FTP pull	This feature adds the following capabilities to the content acquisition function of the Cisco CDS Vault applications: • Allows starting cache-fill from the Content Library immediately after FTP pull acquisition has started. • Provide an interface to check the transfer status, including the bit-rate, the number of bytes transferred and percentage complete • Provide an interface to detect link failure during ingestion. • Provide an interface to cancel or abort an ongoing FTP transfer.	Content Acquisition
FSI Ingest Redundancy	The feature achieves live ingest redundancy by creating two recording copies on separate ingest Vaults, so that the backup recording can switch into service, under certain error conditions	Reliability
Disable trick modes on playlist	Release 2.1 introduces several enhancements needed for the OpenStream integration to support playlists containing advertisements. • OpenStream sets up playlists with VOD assets interspersed with advertisements. For proper accounting of the advertisements, OpenStream requires CDS to disable trick plays for specific segments in the playlist and also publish all trick events on the session. • CDS supports an API to allow OpenStream to notify, at session setup time, which segments are restricted, specifically that trick plays need to be disabled. • CDS also publishes stream play and trick events at the time of session teardown and on-demand through an API to OpenStream.	Content Acquisition
Trick-mode Events (TME) Enhancement	The default value for TME is disabled. TME must be enabled during installation time if the backoffice is OpenStream version 4.0 or higher, and "Trick Mode Events" reports are to be generated in the backoffice. If Shared Content Store is enabled, then the TME setting affects all VHOs, and has to be enabled from the CDSM "Shared ISA Setup" page. Once it is enabled on the VVI, it remains enabled for all VHOs.	Content Acquisition

Enhancements	Descriptions	Category
CDSM 2.1 Enhancements	CDSM was enhanced in Release 2.1 to support the following features: • Cisco Virtual Video Infrastructure (VVI) • Shared Content Store (SCS) • Library Site Redundancy • Local Cache-Fill (Streamers) • NAT Traversal • CDSM Redundancy • New Hardware Configuration • Ingest Resiliency and Non-Blocking FTP • Trick-Mode Enhancements for Playlists • Multiple R2 Connections	Usability
SNMP MIBs	In Release 2.1, CDS MIB is renamed from "arroyo" to "ciscoCdsTV" and several new object groups were added to support read-only access to device configurations and to add additional monitoring attributes. The following object groups are supported in TV CDS 2.1 MIB: • cdstvNotificationGroup: SNMP Trap definitions (Disk up/down, MSA Event traps) • cdstvCacheStatsGroup: Cache-fill and disk read statistics • cdstvStreamStatsGroup: Active Stream and Unique Stream statistics • cdstvDiskMonitorGroup: Disk Monitoring statistics • cdstvServicesMonitorGroup: Software services monitoring • cdstvMSAEventGroup: MSA Events information • cdstvInterfaceSetupGroup: Server Interface configuration • cdstvServerSetupGroup: Server setup (hostname, and so on) • cdstvRoutingTableSetupGroup: Routing Table setup • cdstvDNSBindingGroup: DNS Setup • cdstvRTSPSetupGroup: RTSP configuration settings • cdstvFSISetupGroup: FSI configuration settings • cdstvISAConfigGroup: ISA configuration settings • cdstvHostServiceGroup: Information about objects providing Host Service • cdstvBandwidthManagerGroup: Bandwidth manager settings • cdstvIngestManagerGroup: Ingest Manager settings • cdstvAuthenticationManagerGroup: Authentication manager settings • cdstvIngestTuningGroup: Configured Trick Play settings	Manageability
Trick mode History	Added Trick-mode History reporting for a specified time-frame	Manageability

Enhancements	Descriptions	Category
Multiple R2 Connections	As defined in the NGOD architecture, RT interface is the connection between On-Demand Resource Manager (ODRM) and Streaming Service, and is used for session control (setup and teardown). CDS previously supported only one ODRM connection per Setup Server (which is allowed per NGOD spec). However, some implementations of ODRM are limited to a maximum of 3000 streams. This artificially reduces effective stream capacity of CDS Streamers (can only support 3000 streams in a Stream Group). To solve this, CDS introduced in Release 2.1, support for multiple R2 connects per Stream Group (specifically, multiple VM CA servers connect to one Setup server).	Streaming
Low Bandwidth Connections (Thin Pipe)	In some video networks, the communication lines between super headend sites, or between super headend sites and regional sites, have low bandwidth. This feature allows the operator to set limits on the maximum bandwidth used for mirroring and cache-fill operations.	Performance

Supported Environments

Release 2.1 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 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 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 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.

See the "Related Documentation" section on page 50 for links to the documentation online.

Limitations and Restrictions

There are no limitations nor restrictions in Release 2.1.

Open Caveats

This release contains the following open caveats:

Caching Node

- CSCta26804

    Symptom:

    Streams are dropped when a Caching Node is brought down.

    Conditions:

    With two Caching Nodes running, bring down one Caching Node and a number of streams on the surviving Caching Node are dropped.

    Workaround:

    None.

CDSM

- CSCso77551

    Symptom:

    When scheduling a day's events for a channel, error messages are displayed in the scheduler complaining about events in the past, even for already scheduled event.

    Conditions:

    Schedule all the events in a channel by clicking the channel name. Make sure that here are some schedule events before the current time.

    Workaround:

    NONE. This message is harmless and can be ignored.

- CSCsu67090

    Symptom:

    When DNS Settings are configured and then deleted, they are not removed from the hosts. /etc/resolv.conf

    Conditions:

Create DNS settings through the CDSM and then delete them.

Workaround:

Statsd will regenerate these configurations when it is restarted. Restart statsd or reboot server to have the deleted settings removed.

- CSCsv28319

  Symptom:

  When host entries are created and then deleted, they are not removed from the /etc/hosts.

  Conditions:

  Create host entries through the CDSM and then delete them.

  Workaround:

  Edit the /etc/hosts file manually.

- CSCsz81489

  Symptom:

  When host entries are created and then deleted, they are not removed from the /etc/hosts.

  Conditions:

  Create host entries through the CDSM and then delete them.

  Workaround:

  Edit the /etc/hosts file manually to remove the incorrect records.

- CSCta34676

  Symptom:

  A port used for stream, cache or cache/stream is rejected for use by cserver.

  Conditions:

  An Ethernet port used for stream, cache or cache-fill is in 100Mbps and not 1Gbps. Ports that are unable to negotiate 1Gbps are rejected by the cserver, however, on the GUI they are not listed as red or down, because the port is up.

  Workaround:

  Check ethernet switch configurations to validate the port can negotiate 1Gbps. Secondly replace the ethernet cable to see if there is a problem with that.

- CSCta60580

  Symptom:

  When DNS Settings are configured and then deleted, they are not removed from the hosts /etc/resolv.conf

  Conditions:

  Create DNS settings through the CDSM and then delete them.

  Workaround:

  Statsd will regenerate these configurations when it is restarted. Restart statsd or reboot server to have the deleted settings removed.

- CSCtb20761

  Symptom:

Restarting the SNMP service from CDSM does not seem to work.

Conditions:

Using the restart button on CDSM fails to restart the snmp daemon.

Workaround:

kill -HUP the daemon (if configuration changes are made) or kill and restart the daemon directly.

Database

- CSCta98395

  Symptom:

  CDSM database crashes when scheduling events through the GUI.

  Conditions:

  This issue can happen when an excessive number of events (e.g. 5 min. events for 24 hours a day 7 days a week on several channels) is requested to be scheduled.

  Workaround:

  Reduce the number of scheduled events per channel per day.

- CSCtb09704

  Symptom:

  CDSM database crashes when recording events.

  Conditions:

  This issue can happen when an excessive number of events (e.g. 5 min. events for 24 hours a day 7 days a week on several channels) is being processed for recording.

  Workaround:

  Reduce the number of scheduled events per channel per day.

- CSCsz66661

  Symptom:

  As part of the live ingest process, two copies of a content are created to provide redundancy. If ingest is successful, the backup copy is deleted. However, it is found that, under load situations, DB synchronization sequence might be out-of-order, and some backup copy DB entries are not removed correctly from all Vaults.

  Conditions:

  This can occur in RTSP/FSI deployments supporting live capture with ingest resiliency enabled. Mostly occurs under high performance/load scenarios.

  Workaround:

  Manually delete the residue backup content records.

RTSP

- CSCsx72598

  Symptom:

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

Conditions:

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

Workaround:

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

- CSCtb38508

Symptom:

Ampersand escape sequence in FSI request will not be taken as "&" in attributes.

Conditions:

Requests that include the special character of ampersand.

Workaround:

No workaround. Requests might avoid this special character.

Vault

- CSCta47772

Symptom:

If all the Vaults in the group are set to offloaded state, then new ingests are still accepted on the master Vault.

Conditions:

All Vaults in the group are set to offloaded state.

Workaround:

Do not issue new ingest requests if Vaults are offloaded.

- CSCta95302

Symptom:

Ingest fails during certain network failure cases.

Conditions:

cserver returns INGEST_NOT_STARTED to FSI because the FTP data connection is not established immediately.

Workaround:

Ingest the package again.

Ingest Manager

- CSCsz84213

Symptom:

AIM GetPackageStatus returns wrong status.

Conditions:

If an UpdatePackage operation fails, subsequent GetPackageStatus operations would return the wrong status for this package.

Workaround:

No good workaround. One way is to do a successful UpdatePackage or remove the package and ingest it again.

ISA

- CSCtb12469

    Symptom:

    The issue is introduced because of adding new feature redundant CDSM. There are multiple entries in the /home/isa/.arroyorc file for controller. The isa scripts does not parse the multiple controller IPs correctly so caused this issue. The /home/isa/isa.cfg shows multiple IP listed in the ControllerIP like (e.g. ControllerIP = 192.168.0.100 192.168.0.101).

    Conditions:

    Adding multiple controller IPs in the /home/isa/.arroyorc file on each Streamers.

    Workaround:

    The /home/isa/.arroyorc should have only 1 controller ip. If redundant CDSM are mandatory than there is no work around.

CServer

- CSCsz66255

    Symptom:

    This problem is introduced because of supporting new feature in the 2.1. The new feature allows to disable the (+ffx) speed for an asset in the playlist at the stream setup time. If an asset is repeated in the playlist by once or more and the same asset still allows to play +ffx speed in other segments then to disable the +ffx speed does not take effect.

    Conditions:

    This problem occurs only in very specific conditions.

    1. It has to be playlist setup.

    2. There should a flag set to disable the +ffx speeds of an asset in the playlist.

    3. The same asset that has set to disable the +ffx speeds also repeated in the playlist without disabling the +ffx speeds.

    Workaround:

    1. The asset that does disable the +ffx speeds in the play list should not be repeated in the list.

    2. If it is repeated in the playlist then it should have the same policies to enable or disable the +ffx speeds.

- CSCtb14959

    Symptom:

Log file is not create when disk runs out of space.

Conditions:

When a disk runs out of space and the log file is rolling over to a new file, the new log file creation fails because there is no disk space.

Workaround:

Delete some content so the disk will have room to create the new log file.

- CSCtb00703

Symptom:

Assert enters debugger.

Conditions:

File system contains large objects 8GB or bigger.

Workaround:

Do not create large objects.

- CSCtb17542

Symptom:

Cache/Fill NICs on Vaults show up as malfunctioning adapters in the protocoltiming logfile.

Conditions:

A combination of reduced cache/fill NICs (3 or less), high fill load (in the 1000s), and active local evaluators (local smoothing, defrag).

Workaround:

Turn off local evaluators by default, and run local evaluators at non-peak time. A couple of scripts (avs_stopLocalEvaluators and avs_startLocalEvaluators) are available to properly stop and start the local evaluators. These scripts can be incorporated in a cron job to run local evaluators at non-peak time.

- CSCsx17185

Symptom:

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

Conditions:

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

Workaround:

If possible reingest the content.

- CSCsx53364

Symptom:

Cache-fill transfers from a cache node of a non-cached asset has additional start delay time.

Conditions:

The additional delay is incurred due to starting and processing of cache-fill from Vault server to cache node.

Workaround:

There is no workaround. The net-effect to the consumer is additional stream start delay time around 400ms.

- CSCsx93294

  Symptom:

  Null streams may be played when more than 2432 streams are played on a Streamer

  Conditions:

  If more than 2432 streams are played those streams in some cases may play null streams.

  Workaround:

  The sure workaround is not to play more than 2432 streams per Streamer. This does not happen in all cases but if it does reduce the number of streams below 2432.

- CSCta26804

  Symptom:

  When there are multiple cache severs at a site, the failure of one cache server may cause another cache server to drop some of its active streams.

  Conditions:

  This can occur if the surviving cache server does not have enough capacity to immediately take over the streams from the failed cache server.

  Workaround:

  Keep the load on the cache servers at a level where the surviving cache server can pickup the streams from the failed cache server.

- CSCta27376

  Symptom:

  Deleted content could still be present on the mirroring Vaults.

  Conditions:

  This happens in the FSI environment if a mirroring Vault is disabled when the deletion takes place. The deletion of the object would not be reflected on the disabled Vault even after that Vault is brought back up (though the corresponding entry in the content database would be deleted, making that object an orphan).

  Workaround:

  Clean up orphaned objects manually with the scripts provided.

- CSCta38890

  Symptom:

  The maximum number of unique streams that can be filled from a Vault and played simultaneously is less than the number supported on the 2.0 release by 19 streams

  Conditions:

  The Streamer must be streaming at maximum load with the maximum number of unique streams and with none of the content located in the Streamer's disk cache, so that every stream is filling the content from the Vault. This problem only occurs when using standard size network frames to fill content from the Vault.

  Workaround:

Play some streams from content that is already in the Streamer disk cache, or play multiple streams on some of the content, or use jumbo size network frames to fill content from the Vault.

- CSCta93989

  Symptom:

  Soft lockups were detected on CPU3.

  Conditions:

  The network cards on the server were receiving large number of packets before cserver was fully initialized and loaded.

  Workaround:

  Make sure there are no bombardments of network packets to servers that are not online.

- CSCtb15493

  Symptom:

  When a device is placed in "Repair Mode" due to poor performance, device errors, or device resets, the evaluators are paused. The paused evaluators prevent the storage system from completing its load-balancing or resiliency tasks. This bug prevents a device from leaving the repair mode. Although the system may appear to remain operational it will not achieve the expected level of performance or resiliency.

  A device in this state will post repeated messages to /var/log/debugmessages similar to the following: "cdd:err: csd10: IO error 0x2 - ok : ok : CHECK_CONDITION".

  Conditions:

  This condition is the result of a rare device failure mode wherein the device does not return error context with an initial failure event. The missing context renders the driver unable to accurately interpret the error condition and the device remains in repair mode.

  Workaround:

  The offending device can be removed and replaced. In this example, the offending device is 'csd10'. Echoing this device name to /proc/cds/cdd/remove_device will logically remove the device from the system.

  ```
  echo csd10 > /proc/cds/cdd/remove_device
  ```

  After this the device will no longer hold off the evaluators. The device can now be physically removed from the box and replaced. A new device can simply be re-inserted and it will be discovered automatically.

- CSCtb30715

  Symptom:

  This bug will cause the system to Page-Fault and enter the debugger.

  Conditions:

  This condition is due to a failing device or possibly intermittent communication errors.

  Workaround:

  Remove or replace the offending device.

- CSCtb32108

  Symptom:

  Directory write did not complete in the allocated time because polling process was running too slowly for a short time

  Conditions:

  Freeing memory was taking too much time

  Workaround:

- This is not easily reproducible. Problem is self-correcting.CSCtb33516

  Symptom:

  The c2k log file on a Streamer contains many "play-callback" entries reporting READ_FAILURE errors for a given stream. Eventually, the stream stops responding to stream play commands.

  Conditions:

  This issue occurs when a site using separate Streamer and content-store servers (as opposed to integrated Streamer-Vaults) attempts to playback live content close to the live point in a given stream. This occurs in CDS 2.1.1 and prior versions.

  Workaround:

  The following command can be used to force fast-forward play commands to return an NPT that is no closer than 3 seconds to the live point of the stream:

  ```
  echo bb8 > /proc/calypso/tunables/cm_closetolivedelay
  ```

- CSCsz34225

  Symptom:

  When the network is partitioned so that the primary and backup Streamers cannot communicate with each other, some streams by become stuck and stop playing.

  Conditions:

  This problem may occur when the Streamer which is in the role of setup primary is also control backup, and the Streamer which is in the role of control primary is also setup backup. This is not a typical configuration. To create this configuration requires that the setup service address and the control service address be separate addresses and not be shared. In addition it requires that some servers in the Streamer array are configured to host both the control service address and the setup service address, while other servers in the Streamer array are configured to host the control service address but are not configured to host the setup service address.

  Workaround:

  When a Streamer array is being configured to support both setup and control services, use a single service address to share both of these functions. If you need to use two separate service addresses for setup and control, then making sure that each server that is a configured to host the control service addresses is also configured to host the setup service address.

- CSCta98972

  Symptom:

  Warning message on system console.

  Conditions:

  Unclear. We would need to drop the system into the debugger when this condition is detected to determine why this is happening.

Workaround:

Just ignore these messages.

- CSCtb28920

Symptom:

The c2k log file on a streamer contains many "play-callback" entries reporting READ_FAILURE errors for a given stream. Eventually, the stream stops responding to stream play commands.

Conditions:

This issue occurs when a site using separate streamer and content-store servers (as opposed to integrated streamer-vaults) attempts to playback live content close to the live point in a given stream. This occurs in CDS 2.1.1 and prior versions.

Workaround:

The following command can be used to force fast-forward play commands to return an NPT that is no closer than 3 seconds to the live point of the stream:

```
echo bb8 > /proc/calypso/tunables/cm_closetolivedelay
```

- CSCtb24004

Symptom:

The system will page-fault and enter the debugger.

Conditions:

The cause of this rare event is a race condition in the process of a device becoming "SICK" due to excessive errors or resets.

Workaround:

There is no workaround.

- CSCtb24037

Symptom:

Assert enters the debugger because the system runs out of memory.

Conditions:

System mis-configured such that the mirroring bandwidth is unable to keep up with the ingest traffic for an extended period of time. In this case, the ingest traffic was many times greater than the thin pipe limitations imposed on the mirroring traffic while attempting to ingest 15,000 assets.

Workaround:

Properly configure mirroring bandwidth to be able to keep up with the ingest traffic. Keep in mind that when trick modes are generated this traffic also needs to be mirrored, not just the 1X object.

- CSCsw79171

Symptom:

When a vault is server offloaded, the protocol timing log will not specifically state that the server has been offloaded.

Conditions:

The offload functionality on vaults does not specifically notify the cache server component that it should be placed offline as its managed by the back office integration application. As a result the informational message is not displayed in the cserver logs.

Workaround:

There is no workaround for the issue.

- CSCta98830

  Symptom:

  Network congestion causes streams to be dropped.

  Conditions:

  When the network does not have enough bandwidth to deliver the data for the streams that have been committed, streams will be dropped.

  Workaround:

  Engineer the network so that there is enough bandwidth to deliver the streams that are committed or use a Pipe Bandwidth rule to limit the number of streams that can be committed through the network path.

- CSCsw50536

  Symptom:

  When there are multiple vaults at a site, the failure of one vault may cause another vault to drop some of the active fill streams to streamers

  Conditions:

  This can occur if the surviving vault does not have enough capacity to immediately take over the streams from the failed vault.

  Workaround:

  Keep the load on the vaults at a level where the surviving vault can pickup the streams from the failed cache server.

- CSCsw87409

  Symptom:

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

  Conditions:

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

  Workaround:

  The workaround is to increase the number of Streamers to stream the live content.

- CSCsx17357

  Symptom:

  Streams lost packets.

  Conditions:

  Test conditions removing and adding disks while live ingesting.

  Workaround:

- Do not remove/reinsert drives.CSCsx18109

  Symptom:

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

Conditions:

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

Workaround:

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

- CSCsx61185

Symptom:

The Protocol Timing Log reports messages similar to the following: "Device 15 average seek time of 116ms is greater than 100ms"

Conditions:

These messages can occur for a variety of reasons and they are not necessarily an indication of eminent failure. Should a device persist in poor performance then the device will eventually be abandoned by the system.

Workaround:

None.

- CSCsy90305

Symptom:

Cannot handle intermediary network path failures.

Conditions:

Network failures occur.

Workaround:

Correct instability in network.

- CSCta19793

Symptom:

Some objects are not able to be written to disk. This warning message appears incessantly in the protocol timing log.

Conditions:

An objects is sufficiently fragmented such that the data cannot be successfully striped to the available disk drives.

Workaround:

None. However, the known conditions that cause objects to get into this state (highly fragmented) have been fixed.

- CSCta26321

Symptom:

Not all streams recover when a Streamer fails

Conditions:

If there are two Streamers in an array and one of the Streamers (A) is running near capacity (~2500 streams) and the other one (B) is idle, if the A crashes, not all the streams that were running will fail over and continue to play.

Workaround:

Balance the work loads between the Streamers so that they both handle the load and don't run them at full capacity but leave enough headroom so that fail overs can occur.

- CSCta34840

Symptom:

Number of streams can become unbalanced on the NIC streaming ports if ports cables are unplugged and replugged in reverse order.

Conditions:

Unplug ports 10, 11, 12, and 13, and replug them back in this order, 13, 12, 11, 10. NIC port 13 will have more streams than the other ports.

Workaround:

As the system accepts new stream requests and destroys other ones, the system will re-balance itself over time.

- CSCta79178

Symptom:

Some media objects with no corresponding database entries are found to be present on the disk.

Conditions:

This issue happens when there is mirroring going on during the ingest process and the network connectivity to the mirroring vault is lost. In addition, the ingest needs to fail (for example, due to an external factor such as the FTP server from where the file is downloaded goes down) for this problem to show up.

Workaround:

None.

- CSCta95296

Symptom:

When on a stream is paused and then play is resumed, the play will resume in the wrong location.

Conditions:

When a stream is paused and the Streamer crashes while the stream is paused, the stream will fail over to another Streamer. When this happens the stream that was paused will begin playing in the wrong location when resumed by the viewer.

Workaround:

Rewind or fast forward to the correct location and begin playing the stream.

- CSCta95322

Symptom:

When doing a rewind on a stream it will start rewinding in the wrong location.

Conditions:

When a stream is being rewound and the Streamer crashes, the stream will fail over to another Streamer. When this happens the stream that was rewinding will begin playing in the wrong location.

Workaround:

Rewind or fast forward to the correct location and begin playing the stream.

- CSCtb02690

  Symptom:

  Macroblocks on 1x jumps.

  Conditions:

  When doing 1x jumps VOO-style

  Workaround:

  In work.

- CSCtb10402

  Symptom:

  File fails to ingest and there are error messages printed to the c2k log regarding the "problem goid".

  Conditions:

  This issue is apparent when more than 20 parallel ingest requests are submitted.

  Workaround:

  Ensure that the number of parallel ingests are less than 20. The issue will not happen if ingests are done in a serial fashion.

- CSCtb28713

  Symptom:

  The Streamer hosting the setup service can crash if given a malformed content bundle to replace the content bundle of a stream which is already playing

  Conditions:

  The back end office issues an update content bundle command to replace the content bundle for a stream which is already playing, and the new content bundle is malformed. The reasons that a content bundle may be malformed are 1) it contains no play ranges, 2) A play range has an ending NPT that is before the starting NTP, or 3) the content to be played has a stream rate of 0 Mbps.

  Workaround:

  Do not use the update content bundle functionality, or verify that the content to be played is valid before using update content bundle.

- CSCtb34869

  Symptom:

  Presence for a object is not correct for a short time.

  Conditions:

  Drive is in Repair mode

  Workaround:

  Problem self corrects.

- CSCtb37797

  Symptom:

  Assert enters debugger.

  Conditions:

  Large number of evaluators scheduled (this was caused by a mis-configuration where the mirroring traffic could not keep up with the ingest traffic).

Workaround:

Avoid conditions that schedule large number of one-shot evaluators.

- CSCsz88494

    Symptom:

    Potential visible artifacts at stream transition point.

    Conditions:

    Faulty network conditions or overloaded servers.

    Workaround:

    None.

- CSCtb32568

    Symptom:

    Occasionally, the length of an FTP Out object is too short when the content must be filled from a remote Vault.

    Conditions:

    The issue is unlikely to occur on a fully-operational, standard multi-Vault configuration. If one or more Vaults has several non-operational drives, the error condition is more likely to occur. The issue can occur even if only one object at a time is requested.

    Workaround:

    Verify the content output length matches the length recorded during ingest. If not, repeat the FTP-Out operation. If any disk drives are non-operational, return them to fully-operational state. Request the FTP-Out operation from a Vault that contains an entire local copy of the desired content.

- CSCta33730

    Symptom:

    FTP Out operations starting at other than the beginning of the content do not match data at the corresponding offset in the original (pre-ingest) content if the content was ingested with rate standardization enabled.

    Conditions:

    This issue occurs when rate stabilization is enabled.

    Workaround:

    Start all FTP Out operations at offset zero and download the entire content. Once a local copy of the content has been retrieved, use local file management tools to extract the portion of the content that was desired.

Resolved Caveats

The following caveats have been resolved since Cisco TV CDS Release 2.1. Not all resolved issues are mentioned here. The following list highlights associated with customer deployment scenarios.

CServer

- CSCtb15650

  Symptom:

  Under certain conditions FTP out would crash the server.

- CSCtb02347

  Symptom:

  Vault rejecting streams.

- CSCta99011

  Symptom:

  Remote smoothing is on by default and could not be disabled for 2 hours after the server comes up. .

- CSCta96653

  Symptom:

  The play server was kicking off a lot the streams when server was going offline.

- CSCta07239

  Symptom:

  The symptoms of this bug are varied and are usually the result of memory corruption.

- CSCsz95781

  Symptom:

  Server KDB because of a failed assert that checks the sanity of TCP session state.

- CSCsz93799

  Symptom:

  Cache server might not service certain destinations because of invalid bandwidth accounting.

- CSCsz79814

  Symptom:

  Cache server would assert / KDB when processing messages from security port scanner.

- CSCsz70532

  Symptom:

  Cache server would crash when processing a C2 request with an invalid length PAID.

- CSCsz56557

  Symptom:

  Streamer, Vault or Cache would page fault when processing invalid C2 network packets sent from security port scanner.

- CSCsz33510

  Symptom:

  Drives used for CDS-TV caching (Streamers, caches, and Vaults) may falsely get removed during a network partitioning event.

- CSCsz33478

  Symptom:

  ARP replies are missed on the cache/fill network.

- CSCsy84731

  Symptom:

  When a stream destination is configured for multiple stream arrays using the same priority, streams for the destination are only directed to Streamers in a single array.

- CSCsy55855

  Symptom:

  Vault endlessly attempting to fill content from another Vault. The DataRecovery agent is always actively trying to repair one or more objects without success.

- CSCsy55642

  Symptom:

  The RTSP server stops responding to new requests.

- CSCsy49208

  Symptom:

  At random times SCSI drives attached to the same controller are removed from the system.

- CSCsy45529

  Symptom:

  Streamer would get stuck continually trying to fill non-existent content.

- CSCsy24110

  Symptom:

  A corrupted link list caused the server to crash.

- CSCta53368

  Symptom:

  Vault goes into kernel debugger mode (KDB) during ingest.

- CSCta46430

  Symptom:

  Soft lockup on Vaults after switch reload during ingest.

- CSCta32268

  Symptom:

  Newly ingested content is unavailable for streaming after the Vault is rebooted.

CDSM

- CSCta67651

  Symptom:

  Unable to Delete QAM in CDSM GUI.

- CSCsr81309

  Symptom:

  When adding qams the system does not automatically use the configuration created for them.

- CSCsy90332

  Symptom:

  Unable to restart the RTSP services.

- CSCta49789

  Symptom:

  Cache Group Locator page displays Vault/Cache Domain CDSM IP as the name of the VVIM IP field.

- CSCta49783

  Symptom:

  The Stream to Cache Map is not updating correctly.

- CSCta46208

  Symptom:

  PDF files are not updated for Release 2.1 on the Manuals page in the CDSM.

- CSCta43940

  Symptom:

  When adding a new Cache Group and pressing **Enter** instead of clicking **Submit**, the CDSM jumps to the System Health Monitor page.

- CSCta38261

  Symptom:

  An error message on the CDSM states the database is not available.

- CSCta10489

  Symptom:

  Slave CDSM may show server as being offline when it is online.

- CSCsx63423

  Symptom:

  The System Health Monitor page does not reflect the threshold settings correctly for disk capacity.

Database

- CSCsz57980

  Symptom:

  The database appears hung or crashes when doing resynchronization activities.

Configuration

- CSCsz89756

  Symptom:

  STBs or the BackOffice can have difficulty connecting to setup or control ip addresses.

Vault

- CSCta32181

  Symptom:

  Some trick-mode files are lost after removing a disk drive during ingest.

Installation

- CSCsz43324

  Symptom:

  CDSM display for the Fiber Servers port mapping is not correct in versions > 2.0 .

Installing and Configuring the TV CDS 2.1 Software

This section includes the following topics:

- Preparing the CDEs for the TV CDS Software, page 29
- VVI with Split-Domain Management Installation Procedure, page 30

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 50 for information on accessing these documents.

> **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" section on page 44.

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 50 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** If you are installing a VVI system with split-domain management, the server ID for Streamers in a Stream Domain is generated by the Stream Manager.

- 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 1-1 lists the CDSM GUI ID names and maps them to the CServer names in the setupfile and .arroyorc files.

Table 1-1 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" section on page 44.

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 38.

     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 35.

     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 38.

     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 28 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 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 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.

```
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 38 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 35 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 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 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
  3) CDSM
  4) CDSM with ISA
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   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 5   Enter **1** and press **Enter**.

Step 6   You are asked if you want to disable interface eth0. Enter **N** for no and press **Enter**.

Step 7   Enter the IP address for eth0 when prompted.

Step 8   Enter the netmask for eth0 when prompted.

Step 9   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 10   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 11   Enter a hostname when prompted.

Step 12   Enter the number of the Ethernet interfaces that connect to the gateway when prompted.

Step 13   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 14 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 15 Enter the group ID when prompted.

Step 16 Enter the server ID when prompted.

Step 17 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 the 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 18 Enter the role for the CDE you are adding to the replication group and press **Enter**.

Step 19 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 20 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 21 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 22 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 supports software upgrades only from Release 1.5.1.x and Release 2.0 for CDS ISA and CDS RTSP environments. Upgrades to VVI is not supported.

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-2.1.1.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.

> ✎
> **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

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.

Upgrading from Release 2.0

Upgrading the CDSM and CDS servers from Release 2.0 to Release 2.1 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

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 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-2.1.1.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-2.1.1.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-2.1.1.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 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 CDSM. For example, if the ISO image file (CDS-TV-2.1.1.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-2.1.1.iso /root
```

Step 5 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 6 Upgrade the CDS software on the CDSM by entering the following command, and when prompted, enter the deployment type.

```
# ./cdsinstall CDS-TV-2.1.1.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 35.

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.

Documentation Updates

The following documents have been added for this release:

- *Cisco TV CDS 2.1 ISA Software Configuration Guide*
- *Cisco TV CDS 2.1 RTSP Software Configuration Guide*
- *Cisco TV CDS 2.1 API Guide*

The following documents have been updated for this release:

- *Cisco Content Delivery Engine 205/220/420 Hardware Installation Guide*
- *Cisco Content Delivery System 2.x Documentation Roadmap*

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.