CHAPTER 2

Overview of Upgrading and Downgrading the TV CDS Software

This chapter provides an overview of upgrading and downgrading the CDSM, VVIM, and CDS servers. The chapter covers the following topics:

Note Perform all of the steps in this chapter to upgrade or downgrade TV CDS Release 2.1.x software to Releases 2.2.x, 2.3.x or 2.5.2 software, which requires updating the OS.

Upgrading or downgrading CDS TV Releases 2.2.x, 2.3.x or 2.4.x software to TV CDS Release 2.5.2 software does not require an OS update. To upgrade or downgrade these releases, run the cdsinstall script. There is no need to install the upgrade or downgrade kit.

Introduction

The Release 2.5.2 software upgrade for CDS servers (CDSM, VVIM, Streamer, Vault, Caching Node, and ISV) on a 64-bit operating system (OS) is done with the cdsinstall script.

The following software upgrade paths are supported for Release 2.5.2:

- Release 2.1.x to Release 2.5.2
- Release 2.2.x to Release 2.5.2
- Release 2.3.x to Release 2.5.2
- Release 2.4.x to Release 2.5.2

If the CDS is running Release 2.0 or earlier, you must first upgrade to Release 2.1 before upgrading to Release 2.5.2.

Note The following TV CDS software releases can coexist during an upgrade process, allowing for long upgrade window if necessary:

- For Vaults in a VVI in an ISA environment with SCS, Releases 2.2.1 ES8 and 2.3.3 ES7 software can coexist with the Release 2.5.2 software.
- For Caching Nodes in a VVI in an ISA environment with SCS, Releases 2.2.1 ES9 and 2.3.3 ES7 software can coexist with the Release 2.5.2 software.
- For Streamers in a VVI in an ISA environment with SCS, Releases 2.2.1 ES5 and 2.3.3 ES7 software can coexist with the Release 2.5.2 software.
- For VVI in an RTSP environment with HTTP Streamers, Releases 2.3.2 ES3, 2.4.2 and 2.5.1 software can coexist with the Release 2.5.2 software.
- For CDS (non-VVI) in both ISA and RTSP environments, Releases 2.0.x, 2.1.x, and 2.3.2 software can coexist with the Release 2.5.2 software.

Note Software upgrades and downgrades 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.

Caution Basic understanding of the Linux command line and the vi editor are required for the completion of the software upgrade. Do not attempt the software upgrade if you are unfamiliar with the Cisco CDS products and the Linux command line and vi editor.

We recommend that an experienced Linux system administrator perform the software upgrade and downgrade. The TV CDS Release 2.5.2 software upgrade and downgrade require disk space and network connectivity verification, knowledge of the VNC application (if applicable), and general administration of the remote backup server for archive storage.

Prerequisites for Upgrading or Downgrading the TV CDS Software

Upgrading or downgrading a CDS server has the following prerequisites:

- At least1.8 GB of unused disk space on the / partition for storing and running the upgrade or downgrade kit.
- At least 20 percent unused disk space on the file system for the /boot directory.
- If the /boot_cds directory exists, at least 4.8 GB partition size for the file system and at least 1 GB unused disk space.
- VNC Listener setup defined and operational (We highly recommend using a VNC Listener. See the "VNC Listener" section on page A-9 for more information.)
- Server is operational, which means connected to the network, boot up has completed, all file systems are mounted, and all content drives are operational.
- Any failed content drives should be removed from the server. Upgrading a server with failed content drives may result in a stalled upgrade process, which dramatically increases the amount of time required to perform the upgrade.

- Serial console connected TTYS0 (Not mandatory, but we highly recommend a serial console for monitoring the process).
- Direct physical access in the event of a major failure (for example, power outage) during upgrade.
- Access to a remote server used for backing up each CDS server. The remote Linux server should have enough space to store multiple backups. (The log files that are backed up are not restored.)
- All non-essential files should be archived to a remote location and then removed if the disk space usage is high on all partitions. Any file system at 90 percent capacity should be cleaned up.
- Before upgrading the CDSM or VVIM, all settings on the CDSM Setup page should be recorded. After the CDSM or VVIM is upgraded, all setting on the CDSM Setup page should be verified with the settings that were recorded and resubmitted.

Note After the upgrade procedure starts, do not make any configuration changes until all the servers have been upgraded. The only exceptions to this are submitting the CDSM Setup page after a CDSM or VVIM upgrade, and submitting the Route Tables page after upgrading a CDS server from Release 2.0.

Note The /arroyo/log/archive directory is not preserved. If you want to save the archive, copy it to another server before upgrading the software.

Note During the initialization process of a CDS server or after recovering a CDS server that has been down for less 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.

General Software Upgrade and Downgrade Information for CDS Servers

The following list provides information about the TV CDS Release 2.5.2 software upgrade:

- Copy the upgrade kit and the TV CDS ISO image file to the CDS server. The TV CDS ISO image file is copied after the upgrade is performed.
- Upgrade and downgrade procedures are not for imaging a server to the same state as a brand new system.
- Upgrade can take approximately one hour. The minimum time to perform an upgrade has been 25 minutes; however, servers in different network deployments may require additional time. This time is also based on no failures during the upgrade (that is, power loss or other major failures).
- All configuration information concerning the network should be recorded before upgrading the software.
- Upgrade can be monitored (recommended) from a VNC Listener. During the stage 2 boot process of the upgrade, a window is provided to the user to see the operations taking place on the server. Using the VNC Listener provides the additional ability to triage issues through the serial console if there is a failure during the upgrade.
- The previous **preupgrade** and **upgrade** scripts provided with the TV CDS software should not be used in conjunction with the upgrade and downgrade kits.

- Log files are backed up during the upgrade and downgrade procedures. However, if the log file backup process fails, it is not considered a fatal error and the procedure continues.
- File systems preserved across the OS upgrade are those associated with the following directories: /boot, /arroyo/db, and /boot_cds (if it exists). The upgrade procedure creates the /boot_cds directory if it does not exist.
- Backups are created in /arroyo/db directory. After the upgrade, the administrator performing the upgrade is responsible for removing these files when they are no longer needed.
- CDS servers received from Cisco that will be installed into a Release 2.5.x deployment need to be upgraded with this upgrade kit. Review the file /arroyo/image/tags to see if the installed version on the server is Release 2.5 or higher. See the "Upgrading a New CDS Server to Release 2.5.2" section on page 3-19 for more information.
- To perform a downgrade, the ISO image file for the TV CDS release and the backup files created during the upgrade (backup.tgz, and backup_db.tgz) are required. To downgrade the CDS server, these files must be copied to an accessible server.

Upgrade and Downgrade Considerations

The following sections contain considerations for the upgrade and downgrade procedures.

Thin Pipe Map Configuration

If the CDSM/VVIM is upgraded to release 2.5.2 and the servers are running an earlier version of the software, old thin pipes are not displayed in the GUI, but are displayed in the CDSM/VVIM's and other servers' database.

The setup file on the servers still has thin pipes configured in the old version. Even if new thin pipes are created in the GUI in 2.5.2, the statsd on the servers ignores them and they are not written to the setup file.

If the servers are also upgraded to release 2.5.2, when the Thin Pipe Map page or the Server Setup page is submitted, any 2.5.2 pipe configurations are applied on the servers.

If the servers are downgraded to a earlier version than 2.5.2 and the CDMS is running 2.5.2, the GUI displays the 2.5.2 thin pipes. When the Server Setup page is submitted, any old thin pipes are applied to the servers.

Note In versions prior to 2.5.2, the servers must be rebooted for thin pipe configurations take effect.

Once the VVIM/CDSM is also downgraded to an earlier version, all thin pipe configuration are consistent in the GUI and the servers.

Note Delete all 2.5.2 thin pipes before downgrading the CDSM/VVIM.

New Server Offload State

Because of the new server offload state, the normal recommended upgrade order (CDSM first, Streamers second) may require a special tunable to have the Streamers offload before upgrade. This is because the new Server Offload states on the CDSM that have been upgraded are not recognized by the Streamer that has not been upgraded yet.

SNMP Service Disabled after Downgrade

In release 2.5.2, SNMP is added to services using the chkconfig script while running the cdsinstall script. So, SNMPD is started on reboot. SNMP service can also be started, stopped or restarted using the **service snmpd start/ stop/restart** command.

Once the server is downgraded to any version before 2.5.2, this support is not available. In releases prior to 2.5.2, SNMP can be started by running the cdsconfig script to generate rc.local. This adds the line **nice -n 19 /usr/local/sbin/snmpd** to the rc.local and SNMP starts on reboot. SNMP can also be started manually by executing **nice -n 19 /usr/local/sbin/snmpd** on the server after the downgrade procedure has completed.

Baud Setting

Most installations required the baud of 9600 bits per second (bps). The cdsinstall script and the cdsconfig script support changing the baud without manually editing any files.

Software Upgrade

For a software upgrade, the cdsconfig script may not need to be run. If the baud rate is currently11520 and the user needs to change it to 9600, the user needs to create the /etc/cdsbaud9600 file before running the cdsinstall script. The cdsinstall script searches for the cdsbaud9600 file, and sets the baud to 9600 if the file is found; otherwise, the baud is set to 115200. After the cdsinstall script has completed and the cdsconfig script prompts the user as follows:

```
Serial Console BAUD speed is configured as '9600'. Do you wish to change it (yes/no) [n]:
y
Please select the speed:
1. 9600
2. 115200
Choice:
```

For CDE250s, the /etc/cdsbaud9600 file need not be created as the BAUD rate is set to 9600 by default on upgrade (through the cdsintall script). For other servers, the /etc/cdsbaud9600 file must be created if the user wants to change the BAUD speed to 9600 on upgrade. If the BAUD speed was manually changed in the grub.conf and inittab files, it is not changed during upgrade. For software upgrades, cdsconfig script may not be run at all.

New Installations

For a new installation, the cdsinstall script still requires the following settings on the terminal server serial port:

- 9600 baud
- 8 bits

- No parity

After the cdsinstall script has completed and the cdsconfig script prompts the user as follows:

```
Serial Console BAUD speed is configured as '9600'. Do you wish to change it (yes/no) [n]:
y
Please select the speed:
1. 9600
2. 115200
Choice:
```

Getting the Cisco TV CDS Software Files for Release 2.5.2

Table 2-1 lists the different files for upgrading and downgrading the CDSM and the CDS servers (Streamers, Caching Nodes, Vaults, and ISVs) to Release 2.5.2.

Table 2-1 Files for Release 2.5 Software Upgrade

Server	Operating System Upgrade Package	TV CDS Software Upgrade
CDSM	(64-bit OS already installed)	cdsinstall CDS-TV-2.5.2.iso
Vault, Caching Node, Streamer, or ISV	cdstv-2.5.2-b169-x86_64-os-kit.sh cdstv-2.5.2-b169-i386-os-kit.sh CDS-TV-2.5.2-DVD-OS.iso	CDS-TV-2.5.2.iso

The CDS-TV-2.5.2.iso file is the ISO image file of the Release 2.5.2 software. This file is used for the CDS servers and the CDSM and VVIM.

The **cdsinstall** script must be downloaded and copied to the CDSMs and VVIMs for upgrading to Release 2.5.2.

The cdstv-2.5.2-b169-x86_64-os-kit.sh and cdstv-2.5.2-b169-i386-os-kit.sh files are the self-extracting upgrade and downgrade kits only for the CDS servers. For more information, see the "Upgrade and Downgrade Kits for CDS Servers" section on page 2-13.

The CDS-TV-2.5.2-DVD-OS.iso file is an ISO image file that can be burned to a DVD for recovering from an upgrade or used for a clean install of the CDS servers. For more information, see the "Imaging a CDS Server with 64-Bit OS using a DVD" section on page 3-21.

Note When upgrading to Release 2.5.2 software from Release 2.3.3 using the 2.5.2-ISO-Image, you receive the following error messages when you run the 2.3.3 version of the cdsinstall file for the first time:

```
./cdsupgrade.sh: line 52: $LOGFILENAME: ambiguous redirect
./cdsupgrade.sh: line 59: $LOGFILENAME: ambiguous redirect
./cdsupgrade.sh: line 52: $LOGFILENAME: ambiguous redirect
./cdsupgrade.sh: line 59: $LOGFILENAME: ambiguous redirect
```

When you receive these messages, wait for all them to print out, then the installation continues. Once the installation is complete, the new cdsinstall file is copied to the server. If you are using the new cdsinstall file to install the 2.5.2 image, you do not receive the error messages. It is suggested that you copy the 2.5.2 cdsinstall from the CCO software repository and upgrade the software from 2.3.3-ESx to 2.5.2.

Keep the 2.3.3 version of the cdsinstall file, which will be used for an image downgrade by entering the following command:

```
# mv cdsinstall cdsinstall.233
```

When running the CDS-TV-2.5.2.iso file, always select **1** to install the image on any type of server: VVIM, CDSM, Vault, Cache Node, or Streamer.

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://www.cisco.com/cisco/software/navigator.html

The Select a Product page is displayed. The page displays a Navigator for browsing Cisco products.

Step 2 Log in to Cisco.com using your designated username and password.

Step 3 Click **Products > Video and Content Delivery > Content Delivery Systems > Content Delivery Applications > Cisco TV Streamer Application**.

The Download Software page is displayed, listing the available software releases s for the TV Streamer application.

Step 4 Click the software release you want. The page refreshes and the software image files are displayed.

Step 5 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.

Step 6 Click **Download Now** to download the file, or click **Add to cart** to select more image files before downloading them. The Download Cart page is displayed.

Note Make note of the MD5 checksum value to verify the MD5 checksum after download. You can copy and paste the value into a text file for easy reference.

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

Step 8 Read the agreement and click **Agree**. The Download Software page is displayed.

Step 9 Choose a download option, either **Download Manager Option** or **Non Java Download Option**. A new window displays the filename of the ISO image file.

Step 10 Click **Download**. the File Download dialog box is displayed.

Step 11 Click **Save**. The Save As dialog box is displayed.

Step 12 Navigate to the location where you want to save the file and click **Save**. The file downloads.

Note If you are using a Windows system to get the upgrade kit from http://www.cisco.com, and you plan to use the **scp** command to copy it to the CDS server, make sure the Windows system does not corrupt the kit when copying it to the CDS server.

Upgrade Sequence for Different Deployments

This section describes the upgrade sequence for a Virtual Video Infrastructure (VVI) and a Content Delivery System (CDS). A VVI includes of Caching Nodes and split-domain management. A CDS consists of Streamers and Vaults, or ISVs.

Upgrading a VVI

This section describes the software upgrade sequence for a Virtual Video Infrastructure (VVI). The upgrade sequence for a VVI in an ISA environment and a VVI in an RTSP environment are the same, except the Caching Nodes are upgraded in a specific order in the RTSP environment.

ISA Environment

A VVI in an ISA environment has the following network design:

- Multiple video hub offices (VHOs) and multiple sites per VHO
- Shared Content Store
- ISA with Stream Destination
- Vault Group Redundancy
- Caching Nodes (VVI)
- Split-domain management (VVIM and Stream Manager [CDSM])
- CDSM Redundancy

RTSP Environment

A VVI in an RTSP environment with NGOD deployment and HTTP Streamers has the following network design:

- Multiple Stream Groups
- Multiple Source Output Ports
- Vault Group Redundancy
- Caching Nodes (VVI)
- Split-domain management (VVIM and Stream Manager [CDSM])
- CDSM Redundancy

VVI Upgrade Sequence

The following is a suggested order for upgrading a VVI:

1. VVIM of the first Stream Domain (VHO1 in ISA environment). Upgrade the secondary VVIM, then upgrade the primary VVIM.

The primary and secondary VVIM can be determined by entering the **ifconfig -a | more** command. The primary has the following output:

```
eth0:1    Link encap:Ethernet HWaddr 00:11:00:00:00:00
          inet addr:172.22.98.54 Bcast:172.22.99.255 Mask:255.255.254.0
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          Memory:b8820000-b8840000
```

The primary VVIM has device eth0:1. The secondary VVIM does not have the virtual IP address as up.

2. Streamers in the first Stream Domain. If the Streamers are in multiple Stream Groups (sites), 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 each Stream Group, upgrade the Streamers in the following order:
   a. Available Streamers
   b. Backup Streamer
   c. Primary Streamer

   To identify the Streamers, use the following command:

```
# cat /proc/calypso/status/streamer/resiliencyinfo
    Streamer Resiliency Info:
        Service Address: 172.22.98.50
        Control Service: Primary
```

3. Repeat tasks 1 and 2 for each Stream Domain in the VVI. Upgrade the secondary CDSM, followed by the primary CDSM, then upgrade the Streamers in the Control site (available Streamers first, backup Streamer second, and primary Streamer last), followed by the Streamers in the Setup/Control site.

Note A Stream Manager can manage multiple VHOs (ISA) or Stream Groups (RTSP). Always upgrade the Stream Manager first, then upgrade the Streamers in each VHO (or Stream Group) managed by this CDSM.

4. Caching Nodes. There is no specific order for upgrading the Caching Node in an ISA environment, but to guarantee nonstop services, keep at least one Caching Node online at all times at each site.

   Upgrade the Caching Nodes in an RTSP environment in the following order:
   a. Available Caching Nodes
   b. Backup Caching Node
   c. Primary Caching Node

   To identify the Caching Nodes in Release 2.1.x, view the /var/log/debugmessages file. The following messages indicate the Caching Node was assigned the role of backup:

```
Mar 17 14:53:50 cc_c36 kernel: Backup HTTP Locate Port on service address 192.169.87.100
Mar 17 14:53:50 cc_c36 kernel: Starting backup service for HTTP Locate Port address
192.169.87.100
Mar 17 14:53:50 cc_c36 kernel: Stopped being primary during synchronization to backup for
service address 192.169.87.100
```

   To identify the Caching Nodes in Release 2.5.x, use the **cat httpinfo** command to view the /proc/calypso/status/httpinfo file. The following example indicates that Caching Node 35 is the primary and Caching Node 36 is the backup:

```
# cat httpinfo
```

```
C2 Protocol Info:
 Locate Port Service:
    IPv4 Address: 192.169.87.100
    Primary Server: 35 local
    Backup Server: 36
    Time Offset: 0 usec
 Local Transfer Ports:
    192.169.87.10: Up: Allocated 0bps
    192.169.87.11: Up: Allocated 0bps
    192.169.87.12: Up: Allocated 0bps
```

5. Vaults. Upgrade all slave Vaults first, then upgrade the master Vault.

   The master and slave Vault can be determined by entering the **ifconfig -a | more** command. The master has the following output:

```
eth0:1    Link encap:Ethernet HWaddr 00:11:00:00:00:00
          inet addr:172.22.98.54 Bcast:172.22.99.255 Mask:255.255.254.0
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          Memory:b8820000-b8840000
```

   The master Vault has device eth0:1. The slave Vault does not have the virtual IP address as up.

Upgrading a CDS

This section describes the software upgrade sequence for a Content Delivery System (CDS) as opposed to a VVI. The upgrade sequence for a CDS in an ISA environment and a CDS in an RTSP environment are the same.

CDS Upgrade Sequence

The following is a suggested order for upgrading a CDS:

1. CDSM. Upgrade the secondary CDSM, then upgrade the primary CDSM.
2. Streamers. If the Streamers are in multiple Stream Groups (sites), 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 each Stream Group, upgrade the Streamers in the following order:
   a. Available Streamers
   b. Backup Streamer
   c. Primary Streamer

   To identify the Streamers, use the following command:

```
# cat /proc/calypso/status/streamer/resiliencyinfo
    Streamer Resiliency Info:
        Service Address: 172.22.98.50
        Control Service: Primary
```

3. Vaults. Upgrade all slave Vaults first, then upgrade the master Vault.

Note If the CDS consists of a CDSM and ISVs, upgrade the CDSM first followed by the ISVs.

Downgrade Sequence for Different Deployments

This section describes the downgrade sequence for a Virtual Video Infrastructure (VVI) and a Content Delivery System (CDS). The software downgrade should be performed on the CDS server types in the reverse order of the upgrade sequence—that is, Vaults, then Caching Nodes, then Streamers, and lastly CDSMs.

If all Streamers have been upgraded, we recommend not downgrading any of the Streamers. This also applies to Caching Nodes and Vaults. If all CDS servers of a specific type (Streamer, Caching Node, Vault, or ISV) have all been upgraded, we recommend not downgrading the software.

Note Before downgrading the software, any problems encountered as a result of the upgrade should be understood first. Downgrading a system (VVI or CDS) may result in loss of configuration changes and loss of content that was ingested since the upgrade. Contact Cisco support before downgrading your system.

VVI Downgrade Sequence

The following is a suggested order for downgrading a VVI:

1. Streamers in the first Stream Domain. Downgrade the Control site first, followed by the Setup/Control site. In each Stream Group, downgrade the Streamers in the following order:
   a. Available Streamers
   b. Backup Streamer
   c. Primary Streamer
2. CDSMs in the first Stream Domain. Downgrade the secondary CDSM before the primary CDSM.
3. Caching Nodes. There is no specific order for downgrading the Caching Nodes in an ISA environment, but to guarantee nonstop services, keep at least one Caching Node online at all times at each site.

   Downgrade the Caching Nodes in an RTSP environment in the following order:
   a. Available Caching Nodes
   b. Backup Caching Node
   c. Primary Caching Node
4. Vaults. Downgrade all slave Vaults first, then downgrade the master Vault.
5. VVIMs managing Vaults and Caching Nodes. Downgrade the secondary VVIM before the primary VVIM.
6. Repeat tasks 4 to 5 for each Stream Domain.

If the Streamers at a Setup/Control site have not been upgraded, just downgrade the Streamers at a Control site. If the Streamers at a Setup/Control site have been upgraded, downgrade these Streamers first, then downgrade the Control site Streamers.

Note Before downgrading a CDSM or VVIM, delete any sites and thin pipes that were defined in the Release 2.5.2 installation from the VVIM and CDSM.

CDS Downgrade Sequence

The following is a suggested order for downgrading a CDS:

1. Vaults. Downgrade all slave Vaults first, then downgrade the master Vault.
2. Streamers. Downgrade the Control site first, followed by the Setup/Control site. In each Stream Group, downgrade the Streamers in the following order:
   a. Available Streamers
   b. Backup Streamer
   c. Primary Streamer
3. CDSM. Downgrade the secondary CDSM before the primary CDSM.

If the Streamers at a Setup/Control site have not been upgraded, just downgrade the Streamers at a Control site. If the Streamers at a Setup/Control site have been upgraded, downgrade these Streamers first, then downgrade the Control site Streamers.

If the system consists of ISVs and CDSMs, downgrade the ISVs first followed by the CDSMs.

Upgrade and Downgrade Workflow for a CDS Server

The procedure to upgrade or downgrade a CDS server is more complicated than for a CDSM or VVIM. This section covers the following topics:

- Software Upgrade Workflow for a CDS Server
- Software Downgrade Workflow for a CDS Server

Note Use the CDS-TV-2.5.2.iso file to upgrade to the 2.5.2 TV CDS ISO image, or use a specific version of the file to install a previous version of the TV CDS ISO image (for example, use CDS-TV-2.3.3.iso file to install CDS TV Release 2.3.3 software.

Software Upgrade Workflow for a CDS Server

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

1. Get the upgrade kit from http://www.cisco.comand copy it to the target CDS server.
2. Compare the MD5 checksum from http://www.cisco.com to the file on the target CDS server.
3. Extract the files from the upgrade kit.
4. Offload the CDS server.
5. Run the upgrade utility and script to perform the upgrade. A server backup is created and can be copied to another server during the upgrade.
6. Update (move) the rc.local file and reboot the server.

Software Downgrade Workflow for a CDS Server

A high-level view of the software downgrade workflow is as follows:

1. Make original backup of CDS server available.
2. Get the downgrade kit from http://www.cisco.com and copy to the target CDS server.
3. Compare the MD5 checksum from http://www.cisco.com to the file on the target CDS server.
4. Extract the files from the downgrade kit.
5. Run the downgrade utility and script to perform the downgrade. A server backup is created and can be copied to another server during the downgrade.
6. Restore the original backup of the configuration (this is not the backup from the previous step).
7. Update (move) the rc.local file and reboot the server.

Upgrade and Downgrade Kits for CDS Servers

The upgrade and downgrade kits are self-extracting bash scripts with the necessary files to perform the OS upgrade or downgrade. The names of the kits have the release version in the name. For example, the upgrade and downgrade kits for Release 2.5.2 are the following:

- cdstv-2.5.2-b169-x86_64-os-kit.sh (to upgrade to Release 2.2 or greater 64bit OS)
- cdstv-2.5.2-b169-i386-os-kit.sh (to downgrade to Release 2.0 or 2.1 32bit OS)

Kit Extraction and Content

Use the following commands to copy the kit to /root on the target CDS server and run the self-extracting script:

```
ssh <target_CDS_server_ip_address> -l root
scp -p <remote_server_IP-address>:<kit_location>/cdstv-2.5.2-b169-x86_64-os-kit.sh /root
cd /root
./cdstv-2.5.2-b169-x86_64-os-kit.sh
```

There should be no errors during the extraction of the files in the kit. After extracting the kit, verify that there are no errors before proceeding. If an error message is displayed or if “cdstv-os-5.1-x86_64.iso: OK” is not displayed as the last line for the upgrade kit extraction or “cdstv-os-5.1-i386.iso: OK” is not deployed as the last line for the downgrade kit extraction, the kit may have had errors in downloading. Download and extract the kit again.

Following is an example of the output displayed for a corrupted kit:

```
[root@bd_strm_1 ~]# ./cdstv-2.5.2-b169-x86_64-os-kit.sh --help
CDS-TV Remote Upgrade Kit Self-Extracting Script

Extracting files into /root (extracting the ISO file may take a few minutes):
cds_remote_upgrade/./
cds_remote_upgrade/./backup_cfg.sh
cds_remote_upgrade/./ks_remote_template.cfg
cds_remote_upgrade/./restore_cfg.sh
cds_remote_upgrade/./backup.list
cds_remote_upgrade/./cdstv-os-5.1-x86_64.iso

gzip: stdin: invalid compressed data--format violated
tar: Unexpected EOF in archive
```

```
tar: Unexpected EOF in archive
tar: Error is not recoverable: exiting now

ISO file checksum checking (may take a few minutes):
Found SHA1 checksum file:
dirname: missing operand
Try `dirname --help' for more information.
basename: missing operand
Try `basename --help' for more information.
```

Whenever a tar failure like the above occurs, the kit is corrupted. Download and extract the kit again.

Note If disk space on the "/" partition is an issue, the kit file can be removed after it is extracted to free up disk space.

Upgrade Kit Content

The following files are extracted when you run the upgrade kit script:

```
./cdstv-2.5.2-b169-x86_64-os-kit.sh
CDS-TV Remote Upgrade Kit Self-Extracting Script

Extracting files into /SHARE/upgrade/tmp (extracting the ISO file may take a few minutes):
cds_remote_upgrade/./
cds_remote_upgrade/./backup_cfg.sh
cds_remote_upgrade/./ks_remote_template.cfg
cds_remote_upgrade/./restore_cfg.sh
cds_remote_upgrade/./backup.list
cds_remote_upgrade/./cds_upg_report.sh
cds_remote_upgrade/./cds_remote_iso_install
cds_remote_upgrade/./restore.list
cds_remote_upgrade/./check_tcp_port.pl
cds_remote_upgrade/./iso.sha1sum
cds_remote_upgrade/./cdsinstall
cds_remote_upgrade/./cdstv-os-5.1-x86_64.iso
cds_remote_upgrade/./version
cds_remote_upgrade/./cdsmodify.sh

ISO file checksum checking (may take a few minutes):
Found SHA1 checksum file:./cds_remote_upgrade/iso.sha1sum
cdstv-os-5.1-x86_64.iso: OK
```

Remote upgrade files are extracted to the./cds_remote_upgrade directory.

Downgrade Kit Content

The following files are extracted when you run the downgrade kit script:

```
./cdstv-2.5.2-b169-i386-os-kit.sh
CDS-TV Remote Downgrade Kit Self-Extracting Script

Extracting files into /SHARE/upgrade/tmp (extracting the ISO file may take a few minutes):
cds_remote_upgrade/./
cds_remote_upgrade/./backup_cfg.sh
cds_remote_upgrade/./ks_remote_template.cfg
cds_remote_upgrade/./restore_cfg.sh
cds_remote_upgrade/./backup.list
cds_remote_upgrade/./cds_upg_report.sh
cds_remote_upgrade/./cds_remote_iso_install
```

```
cds_remote_upgrade/./restore.list
cds_remote_upgrade/./cdstv-os-5.1-i386.iso
cds_remote_upgrade/./check_tcp_port.pl
cds_remote_upgrade/./iso.sha1sum
cds_remote_upgrade/./DOWNGRADE
cds_remote_upgrade/./cdsinstall
cds_remote_upgrade/./version
cds_remote_upgrade/./cdsmodify.sh

ISO file checksum checking (may take a few minutes):
Found SHA1 checksum file:./cds_remote_upgrade/iso.sha1sum
cdstv-os-5.1-i386.iso: OK
```

Remote downgrade files are extracted in the ./cds_remote_upgrade directory.

Important Kit Utilities

Both the upgrade and downgrade kits include the following important scripts:

- cds_remote_iso_install Details—Performs the upgrade or downgrade
- cds_upg_report.sh Details—Collects the upgrade logs
- backup_cfg.sh Details—Creates a backup of the CDS server
- restore_cfg.sh Details—Restores the configuration from a backup

cds_remote_iso_install Details

The **cds_remote_iso_install** script performs the upgrade or the downgrade. Depending on the kit extracted, the script has different options.

Upgrade Kit Options

```
Usage: cds_remote_iso_install [--check | --help | --upgrade [UPGRADE_OPTIONS]]
   --help    : show the script usage
   --check   : check the partitions setup but do not perform upgrade
   --upgrade : start remote upgrade process
  UPGRADE_OPTIONS := [iso-file <FILE> | baud-rate <RATE> | vnc-listener <HOST IP[:PORT]> ]
                     iso-file <FILE> : ISO image file
                     baud-rate <RATE> : serial line baud rate
                     vnc-listener <HOST IP[:PORT]> : vnc listener IP[:port]
```

Downgrade Kit Options

```
Usage: cds_remote_iso_install [--check | --help | --downgrade [DOWNGRADE_OPTIONS]]
   --help    : show the script usage
   --check   : check the partitions setup but do not perform upgrade
   --downgrade : start remote downgrade process
 DOWNGRADE_OPTIONS := [iso-file <FILE> | baud-rate <RATE> | vnc-listener <HOST IP[:PORT]>]
                      iso-file <FILE> : ISO image file
                      baud-rate <RATE> : serial line baud rate
                      vnc-listener <HOST IP[:PORT]> : vnc listener IP[:port]
```

Note Under normal circumstances, the **iso-file** and **baud-rate** options should not be used. Use of a VNC Listener is highly recommended. See "VNC Listener" section on page A-9 for more information.

--check Option

The **--check** option can be used at any time. Before upgrading or downgrading a CDS server, use the **--check** option to verify that all necessary prerequisites are met. The **--check** option checks the following:

- TV CDS processes states (running or not running)
- Required system partitions and minimum unused disk space required for each partition
- VNC Listener status

Note The TV CDS processes do not need to be manually stopped. The cds_remote_iso_install **--upgrade** and **--downgrade** options stop all processes before performing the OS upgrade or downgrade.

To see an example of the output for the **-- check** option, see the "Upgrade Script with the Check Option" section on page A-10.

If there are error or warning messages related to the minimum required disk space, the locations that have been identified should be cleaned up. Use the following Linux commands to find the areas that need cleaning up:

- ***df –k***—Provides the partition space usage
- ***du –sk ****—Provides the space used by everything in the current directory

For example, if /boot is full, run the following commands to view the files in the /boot directory.

```
cd /boot
du -sk *
```

Note When cleaning out /boot, do not remove the vmlinuz kernels defined in the /boot/grub/grub.conf file. Doing so prevents the system from booting when the system is halted or rebooted.

Following is an example of the output from the above commands:

```
42      config-2.6.18-53.el5.cdstv.2.1.3.b1
48      config-2.6.18-53.el5.cdstv.2.1.3.b1
65      config-2.6.18-53.el5PAE
240     grub
2427    initrd-2.6.18-53.el5.cdstv.2.1.3.b1.img
2527    initrd-2.6.18-53.el5.cdstv.2.1.4.b1.img
2626    initrd-2.6.18-53.el5.cdstv.2.1.3.b1kdump.img
2626    initrd-2.6.18-53.el5.cdstv.2.1.4.b1kdump.img
2397    initrd-2.6.18-53.el5PAE.img
12      lost+found
5090    ssd_mod_initrd.img
88      symvers-2.6.18-53.el5PAE.gz
788     System.map-2.6.18-53.el5.cdstv.2.1.3.b1
796     System.map-2.6.18-53.el5.cdstv.2.1.4.b1
887     System.map-2.6.18-53.el5PAE
1656    vmlinuz-2.6.18-53.el5.cdstv.2.1.3.b1
1706    vmlinuz-2.6.18-53.el5.cdstv.2.1.4.b1
1756    vmlinuz-2.6.18-53.el5PAE
```

If the TV CDS software installed is Release 2.1.4, the Release 2.1.3 related files can be removed.

--upgrade or --downgrade Option

The **--upgrade** and **--downgrade** options are used to start the upgrade or downgrade process. The cds_remote_iso_install can be run with just these options or can include the "vnc-listener <ip>:<port>" as well.

When the cds_remote_iso_install runs for the first time, the prerequisite checks are performed and if any TV CDS processes are running, you are asked to reboot the CDS server. Before rebooting the server, make sure there are no ingests or active streams. The CDS server should have the **Server Offload** option enabled. Log in to the CDSM or VVIM, choose **Maintain > Servers > Server Offload**, select the IP address of the server, choose **Enable**, and click **Submit**.

cds_upg_report.sh Details

When an upgrade is performed, there are several log files that are created during different phases of the upgrade. The **cds_upg_report.sh** script archives all the these log files into a tgz file, which can be sent to a Cisco support engineer requesting this information. All details in the archive are kept confidential.

To see an example of the output for the **cds_upg_report.sh** script, see the "CDS Upgrade Report Script" section on page A-11.

backup_cfg.sh Details

The **backup_cfg.sh** script creates the same backup as the **cds_remote_iso_install** script. The following tar gzip archives are created by this script and the **cds_remote_iso_install** script with the specified filenames:

- Configuration— <*host*>_<*cds version*>_<*datestamp*>_backup.tgz
- Database— <*host*>_<*cds version*>_<*datestamp*>_backup_db.tgz
- Log— <*host*>_<*cds version*>_<*datestamp*>_backup_log.tgz

The archive files are created in the /arroyo/db. directory.

Note The /arroyo/log/archive directory is not backed up by any scripts provided with either upgrade or downgrade kits.

To see an example of the output for the **backup_cfg.sh** script, see the "Backup Script—Configuration and Database" section on page A-12.

Note The list of files being backed up with this utility and the **cds_remote_iso_install** script are listed in the kit package file backup.list.

restore_cfg.sh Details

The **restore_cfg.sh** script restores the configuration files that was backed up using the backup_cfg.sh or **cds_remote_iso_install** scripts. This script is used if a system is downgraded. The script expects the following filenames of the two required archives:

- Configuration archive: <*host*>_<*cds version*>_<*datestamp*>_backup.tgz
- Database archive: <*host*>_<*cds version*>_<*datestamp*>_backup_db.tgz

If either of these files do not exist, the configuration is not restored.

To see an example of the output for the **restore_cfg.sh** script, see the "Restore Script—Configuration and Database" section on page A-13.

Note The list of files being restored by this utility are listed in the kit package file restore.list.