CHAPTER 1

Overview of Upgrading and Downgrading the VDS-TV Software

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

Introduction

The Release 4.8 software upgrade for VDS servers (CDSM, VVIM, Streamer, Vault, Caching Node, and ISV) on a 64-bit operating system (OS) is done with the vdsinit script.

The following software upgrade paths are supported for Release 4.84.8:

- Release 2.5.x to Release 3.2.x to Release 4.8
- Release 3.0.x to Release 3.2.x to Release 4.8
- Release 3.2.x to Release 4.8
- Release 3.4.x to Release 4.8
- Release 3.5.x to Release 4.8
- Release 3.7.x to Release 4.8
- Release 3.9.x to Release 4.8
- Release 3.12.x to Release 4.8
- Release 4.2.x to Release 4.8
- Release 4.4.x to Release 4.8

If the VDS is running an earlier software release, you must first upgrade to one of the supported releases before upgrading to Release 4.8.

Downgrade from 4.8 to an image lesser than 3.9.1-ES9

In RTSP deployment downgrading streamers from Release 4.8 to Release lesser than 3.9.1-ES9 (except 3.2.5ES1), have issues in the following scenario:

- Downgrade the **Available and Backup streamer** from 4.8 to an image lesser than 3.9.1-ES9. (For Example 3.5.1).
- Primary Failovers from 4.8 to 3.5.1 streamer.
- Streamer will crash when recreating all the sessions, because the opaque structures are not compatible between 3.5.1 and greater than 3.91 ES9 versions (except 3.2.5ES1).

Workaround

Teardown all sessions in a maintenance window, and perform the downgrade.

Note Due to changes in file system, direct upgrade is supported only from Release 3.2.x to Release 4.8.

Warning **If the supported upgrade paths are not followed, then CServer will have to be started with -c option that will erase all the GOIDS in the disk.**

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 VDS 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 VDS products and the Linux command line and vi editor.

We recommend that an experienced Linux system administrator perform the software upgrade and downgrade. The VDS-TV Release 4.8 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 VDS-TV Software

Upgrading or downgrading a VDS server has the following prerequisites:

- 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-6 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 VDS 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 and Interface Setup page after upgrading a VDS server.

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 VDS server or after recovering a VDS server that has been down for less than an hour, the VDS database performs a complete synchronization. The database synchronization takes about five minutes before the server becomes ready for service. If the VDS 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 VDS Servers

The following list provides information about the VDS-TV Release 4.8 software upgrade:

- Copy the vdsinit script and the VDS-TV ISO image file to the VDS server.
- 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.
- 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.
- Review the file /arroyo/image/tags to see if the installed version on the server is Release 3.2.x or higher.
- To perform a downgrade, the ISO image file, cdsinstall for the VDS-TV release and the backup files created during the upgrade (backup.tgz, and backup_db.tgz) are required.

Upgrade and Downgrade Considerations

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

SNMP Service Disabled after Downgrade

In release 4.4, SNMP is added to services using the chkconfig script while running the vdsinit 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 3.0.1, this support is not available. In releases prior to 3.0.1, 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 vdsconfig script supports changing the baud without manually editing any files.

Software Upgrade

For a software upgrade, the vdsconfig 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 vdsinit script. The vdsinit 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 vdsinit script has completed and the vdsconfig 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 vdsinit 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, vdsconfig script may not be run at all.

New Installations

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

- 9600 baud
- 8 bits
- No parity

After the vdsinit script has completed and the vdsconfig 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 VDS-TV Software Files for Release 4.8

Table 1-1 lists the different files for upgrading and downgrading the CDSM and the CDS servers (Streamers, Caching Nodes, Vaults, and ISVs) to Release 4.8.

Table 1-1 Files for Release 4.8 Software Upgrade

Server	Operating System Upgrade Package	VDS-TV Software Upgrade
CDSM	(64-bit OS already installed)	vdsinit-4.8.1 tv_repo-4.8.1-x86_64.iso
Vault, Caching Node, Streamer, or ISV	tv_full-4.8.1-x86_64.iso	vdsinit-4.8.1 tv_repo-4.8.1-x86_64.iso

The tv_repo-4.8.1-x86_64.iso file is the ISO image file of the Release 4.8 software. This file is used for the CDS servers and the CDSM and VVIM.

The vdsinit script must be downloaded and copied to the CDSMs and VVIMs for upgrading to Release 4.8.

The tv_full-4.8.1-x86_64.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 VDS servers. For more information, see the "Imaging a VDS Server with 64-Bit OS using a DVD" section on page 2-15.

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.

Upgrade Sequence for Different Deployments

This section describes the upgrade sequence for a Virtual Video Infrastructure (VVI) and a Content Delivery System (VDS). A VVI includes of Caching Nodes and split-domain management. A VDS 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 for the SHEs should be upgraded first. 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. 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.

3. 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, use the **cat httpinfo** command to view the /proc/calypso/status/cache/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
```

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

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

5. 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
```

6. 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.

Upgrading a VDS

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

VDS Upgrade Sequence

The following is a suggested order for upgrading a VDS:

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 VDS 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 (VDS). The software downgrade should be performed on the VDS server types in the reverse order of the upgrade sequence—that is, Streamer, CDSM, Caching Nodes, Vault and lastly VVIM.

If all Streamers have been upgraded, we recommend not downgrading any of the Streamers. This also applies to Caching Nodes and Vaults. If all VDS 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 VDS) 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. Repeat tasks 1 and 2 for each Streaming domain.
4. 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
5. Vaults. Downgrade all slave Vaults first, then downgrade the master Vault.
6. VVIMs managing Vaults and Caching Nodes. Downgrade the secondary VVIM before the primary VVIM.

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.

VDS Downgrade Sequence

The following is a suggested order for downgrading a VDS:

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 VDS Server

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

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

Software Upgrade Workflow for a VDS Server

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

1. Get the VDS-TV 4.8 ISO file, vdsinit script file and copy it to the target VDS server.
2. Offload the VDS server.
3. Run the vdsinit script and perform the upgrade.
4. Reboot the server and start the services as per the sequence mentioned in vdsServices.conf.

Software Downgrade Workflow for a VDS Server

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

1. Offload the server.
2. Copy the ISO image file to be downgraded, to the /root directory of the VDS server.
3. Execute the vdstvDowngrade script.
4. Reboot the server and start the services as per the sequence mentioned in /etc/rc.local.