System Maintenance

This chapter explains how to replace, remove, and add a VDS server, perform a backup and recovery of the configuration and database files, and recover the administrator password. This chapter covers the following topics:

Note If Virtual Video Infrastructure (VVI) with split-domain management is enabled, the CDSM pages associated with the Vaults and Caching Nodes display only on the VVI Manager (VVIM), and the CDSM pages associated with the Streamers display only on the Stream Manager. For more information, see the "Engineering Access Level Pages" appendix in the *Cisco VDS-TV 3.5 ISA Software Configuration Guide* or the *Cisco VDS-TV 3.5 RTSP Software Configuration Guide*.

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

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

Replacing a Server

You may need to replace a VDS server if the server is experiencing unresolvable problems. The procedure to replace a server in the VDS differs based on the type of server being replaced. This section covers the following procedures:

- Replacing a CDSM or VVIM
- Replacing a VDS Server

Note The new replacement server must be the same hardware model as that of the server being replaced.

Replacing a CDSM or VVIM

The procedure to replace a CDSM or VVIM differs based on whether or not there are redundant CDSMs (or VVIMs). With CDSM redundancy, if the primary CDSM becomes unavailable, the secondary CDSM takes over the virtual IP address and the administrator can connect to the secondary CDSM within 15 seconds.

Note These procedures assume the new server has the same software version as the server being replaced.

Before you can replace a server, the new server must have the same Cisco VDS-TV software release as the server being replaced. To verify the software version, use the **cat /arroyo/image/tags** command. For information on upgrading the software, see Chapter 3, "Upgrading to Release 3.5."

Replacing a Redundant CDSM or VVIM

Replacing a redundant CDSM or VVIM involves the following tasks:

1. Shut down the old CDSM or VVIM.
2. Start up the new CDSM which is configured with the same IP address as the old CDSM.
3. Stop the database on the primary CDSM and copy it to the new CDSM.
4. Run the **cdsconfig** script to configure the new CDSM and inform the other CDS servers of the new CDSM.
5. Uncomment all the lines in the rc.local file and reboot the new CDSM.

To replace a redundant CDSM, do the following:

Step 1 Log in to the CDSM being replaced as *root*.

Step 2 Stop Auto Importer if it is enabled on the CDSM being replaced.

a. Check that the Auto Importer process is not running.

```
ps -ef | grep Importer
```

b. If Auto Importer is running, use the **kill** command with the PID.

```
kill - 9 <PID>
```

Step 3 In an ISA deployment, stop the Exporter process if it is enabled on the CDSM being replaced.

a. Check that the Exporter process is not running.

```
ps -ef | grep Exporter
```

b. If the Exporter is running, use the **kill** command with the PID.

```
kill - 9 <PID>
```

Step 4 Stop the database on the CDSM being replaced.

```
# db_shutdown
```

Step 5 Ensure that the database is fully stopped on the CDSM being replaced.

a. Check that the database thread count returns nothing.

```
netstat –an | grep 9999
```

b. Make sure that no process ID (PID) is returned.

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

c. If the database is still up, use the **kill** command with the PID.

```
kill -9 <PID>
```

Step 6 To prevent the CDSM being removed from impacting the CDS network if it boots up again, do the following:

a. On the CDSM being removed, edit the rc.local file and comment out the following lines in the rc.local file

```
#!/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

#/home/stats/statsd -i 10.74.124.103 -s 255.255.255.0 -d eth0

sleep 300
```

b. Log in to the CDSM being replaced as user **isa** and edit the .arroyorc file to remove all entries in the Replication Group members section of the file.

Step 7 Shut down the CDSM being replaced.

```
# poweroff
```

Step 8 You must stop the database on the primary CDSM before copying it to the new CDSM. Log in to the primary CDSM as *root*.

Step 9 Stop Auto Importer if it is enabled on the primary CDSM.

a. Check that the Auto Importer process is not running.

```
ps -ef | grep Importer
```

b. If Auto Importer is running, use the **kill** command with the PID.

```
kill - 9 <PID>
```

Step 10 In an ISA deployment, stop the Exporter process if it is enabled on the primary CDSM.

a. Check that the Exporter process is not running.

```
ps -ef | grep Exporter
```

b. If the Exporter is running, use the **kill** command with the PID.

```
kill - 9 <PID>
```

Step 11 Stop the database on the primary CDSM.

```
# db_shutdown
```

Step 12 Ensure that the database is fully stopped on the primary CDSM.

a. Check that the database thread count returns nothing.

```
netstat –an | grep 9999
```

b. Make sure that no process ID (PID) is returned.

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

c. If the database is still up, use the **kill** command with the PID.

```
kill -9 <PID>
```

Note The new replacement server has already been verified or upgraded to the same Cisco VDS-TV software version as the server it is replacing. This includes running the **cdsinstall** script to install the software; not the **cdsconfig** script.

The new placement CDSM has been configured with the same IP address as the CDSM being replaced.

Step 13 On the new CDSM, use the **scp** command to copy the DATADIR directory from the primary CDSM. For example, if the primary 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 14 On the primary CDSM, start the database again.

```
[root]# su - isa
```

Step 15 On the primary CDSM, start the Auto Importer again if it had been running on the primary CDSM prior to the shutdown of the database.

```
[root]# su - isa -c "cd /home/isa/RTScheduler/Importer; ./ImporterServer -d failover"
[root]# ps -ef | grep Importer
```

Step 16 In an ISA environment, on the primary CDSM, start the Exporter again if it had been running on the primary CDSM prior to the shutdown of the database.

```
[root]# su - isa -c "cd /home/isa/RTScheduler/Exporter; ./ExporterServer >&
/home/isa/RTScheduler/Exporter/ExporterServer.log&"
[root]# ps -ef | grep Exporter
```

Step 17 On the new CDSM, change the ownership of DATADIR from *root:root* to *isa:isa.*

```
# chown -R isa:isa /arroyo/db/DATADIR
```

Step 18 Run the **cdsconfig** script. Answer the following prompts using the same configuration as the CDSM being replaced.

- When the script returns the list of current replication groups, verify that all members have been listed. If any member is missing, at the "Do you want to edit the replication group members?" prompt, enter **Y** for yes, and enter the missing member.
- At the "Do you want to enable CDSM redundancy?" prompt, enter **Y** for yes.
- At the "Is this node getting added to an existing deployment?" prompt, enter **N** for no because the DATADIR has already been copied from the primary CDSM.
- Answer appropriately to the prompts for getting the ID from the first CDSM.

Step 19 Login to the GUI of the new CDSM as a user with Engineering access. The CDSM Setup page is displayed.

Step 20 In the **Installation** drop-down list on the CDSM Setup page, choose either **RTSP** or **ISA** depending on your environment.

Step 21 If Media Scheduler is enabled on the existing CDSM, do the following:

a. Scroll down to the Media Scheduler section of the CDSM Setup page, and click the **ON** radio button next to the **Media Scheduler** field. In the Activation Key field, enter the software access key from your Right to Use Notification for the Content Delivery Application Media Scheduler (CDAMS) product.

b. Scroll down to the **Ingest Manage**r section, and click the **ON** radio button next to the **Ingest Manager** field. In the **Activation key** field, enter the software access key from your Right to Use Notification from the CDAMS product.

Step 22 Verify that all other settings on the CDSM Setup page are the same as on the existing CDSM and click **Submit**.

Step 23 Choose **Maintain > Software > System Configs**. The System Configs page is displayed.

Step 24 Verify the CDS parameters on the System Configs page and click **Submit**.

Step 25 Configure NTP on the new CDSM.

a. Set your time zone on the CDSM by copying your time zone file to the /etc/local file. In the following example, the time zone is Asia/Shanghai.

```
#cp   /usr/share/zoneinfo/Asia/Shanghai    /etc/localtime
```

b. Verify that the clock information displayed in the file /etc/sysconfig/clock is correct. The file should display the following information:

```
Zone=time zone
UTC=fale
ARC=false
```

The Zone filed represents the time zone as presented by the zone file under directory /usr/share/zoneinfo. Setting the UTC field to false sets the clock to the local time. Setting the ARC field to false, sets the time to Unix epoch time.

c. Remove all existing lines from the NTP configuration file /etc/ntp.conf and add the NTP server using the command **server** *NTP_Server_IP_Address* **# local clock.** In the following example, the NTP server has an IP address of 10.74.124.189.

```
# server  10.74.124.189   # local clock
```

d. Start the NTP service.

```
# service ntpd start
```

e. Enable the NTP service.

```
# chkconfig ntpd on
```

Step 26 When the **cdsconfig** script completes, edit the rc.local file on the new CDSM and uncomment all the command lines. In an ISA deployment, the **su - isa -c "cd /home/isa/RTScheduler/Exporter...**" command is only used when the MediaX feature sends notifications to a catalog server or similar server. In both an ISA and an RTSP deployment, the **su - isa -c "cd /home/isa/RTScheduler/Importer**; **./ImporterServer -d failover"** command is required when the MediaX Auto Importer is used.

The 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&"

su - isa -c "cd /home/isa/RTScheduler/Importer; ./ImporterServer -d failover

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

sleep 30
```

Step 27 Shut down the database and reboot the new secondary CDSM.

```
# db_shutdown
# ps -ef|grep avsdb
# netstat -an | grep 9999
# reboot
```

Replacing a Standalone CDSM

Note This procedure assumes the new server has the same software version as the server being replaced.

Replacing a standalone CDSM includes the following tasks:

1. Remove the old CDSM from the CDS.
2. Add the new replacement CDSM into the CDS with the same IP address as the old CDSM.

Step 1 Log in to the existing CDSM GUI as a user with Engineering access.

Step 2 Choose **Maintain > Software > CDSM Setup**. The CDSM Setup page is displayed.

Step 3 Write down all the settings on the CDSM Setup page.

Step 4 Back up the configuration and database files on the existing CDSM. For information on this procedure, see the "Performing a Backup on the CDSM or VVIM" section on page 5-27.

Step 5 To prevent the existing CDSM from impacting the CDS network if it boots up again, do the following:

a. On the existing CDSM, edit the rc.local file and comment out the following lines in the rc.local file

```
#!/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

#/home/stats/statsd -i 10.74.124.103 -s 255.255.255.0 -d eth0

sleep 300
```

b. Log in to the CDSM as user **isa** and edit the .arroyorc file to remove all entries in the Replication Group members section of the file.

Step 6 Shut down the existing CDSM.

```
poweroff
```

Step 7 On the new CDSM, restore the configuration and database files using the backup that was made from the existing CDSM. For information on this procedure, see the "Performing a Restore on the CDSM" section on page 5-29.

Note The new replacement server has already been verified or upgraded to the same Cisco VDS-TV software version as the server it is replacing.

Step 8 Run the **cdsconfig** script. At the "Do you want to enable CDSM redundancy?" prompt, enter **N** for no. At the "Is this node getting added to an existing deployment?" prompt, enter **N** for no because the CDSM is not a newly-added CDSM, it is replacing an existing CDSM.

```
cdsconfig
```

Step 9 When the **cdsconfig** script completes, edit the rc.local file and uncomment all the command lines. In an ISA deployment, the **su - isa -c "cd /home/isa/RTScheduler/Exporter..."** command is only used when the MediaX feature sends notifications to a catalog server or similar server. In both an ISA and an RTSP deployment, the **su - isa -c "cd /home/isa/RTScheduler/Importer**; **./ImporterServer -d failover"** command is required when the MediaX Auto Importer is used.

The 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&"

    su - isa -c "cd /home/isa/RTScheduler/Importer; ./ImporterServer -d failover"

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

    sleep 30
```

Step 10 Shut down the database and reboot the newly added CDSM.

```
# db_shutdown
# ps -ef|grep avsdb
# netstat -an | grep 9999
# reboot
```

Step 11 Log in to the new CDSM GUI as a user with Engineering access. If a user account with the Engineering access level does not exist, log in to the CDSM as *admin*, or as another user that has Master access, and add a user with Engineering access.

a. Choose **Maintain > User > Add Users**. The Add Users page is displayed.

b. In the **New User** and **Password** fields, enter the user name and password for this account.

c. From the **Access** drop-down list, choose **Engineering**.

d. Click **Add User**.

Log out of the CDSM, and log in as the user with the Engineering access level. The CDSM Setup page is displayed. If the CDSM Setup page is not displayed, choose **Maintain > Software > CDSM Setup**.

Step 12 In the **Installation** drop-down list, choose either **RTSP** or **ISA** depending on your environment.

Step 13 If Media Scheduler is enabled on existing CDSM, do the following:

a. Scroll down to the Media Scheduler section, and click the **ON** radio button next to the **Media Scheduler** field. In the Activation Key field, enter the software access key from your Right to Use Notification for the CDAMS product.

b. Scroll down to the **Ingest Manage**r section, and click the **ON** radio button next to the **Ingest Manager** field. In the **Activation key** field, enter the software access key from your Right to Use Notification from the CDAMS product.

Step 14 Verify that all other settings are the same as on the existing CDSM and click **Submit**.

Step 15 On the GUI of the new CDSM, choose **Maintain > Software > System Configs**. The System Configs page is displayed.

Step 16 Verify the VDS parameters on the System Configs page and click **Submit**.

Step 17 Choose **Monitor > System Health**, and verify connectivity to all the VDS servers by checking the status of each server. All status boxes should be green.

Replacing a VDS Server

Replacing a Vault, Streamer, ISV, or Caching Node includes the following tasks:

1. Offload the server and shut down the processes on the server.
2. Back up the configuration to an available Linux server.
3. Restore the backup on the new replacement server.
4. Log in to the CDSM and complete the configuration.

Note The replacement server and the server being removed must be of the same server type. Otherwise, remove the old server from the network by following the procedure in the "Removing a Server" section on page 5-13 and then, add the new server to the network by following the procedure in the "Adding a Server" section on page 5-19.

To replace a Vault, Streamer, ISV, or Caching Node, do the following:

Step 1 Using the CDSM GUI, offload the server that is being replaced.

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

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

c. Choose **Enable** and click **Submit**.

When Server Offload is enabled on a server, the server is configured to reject new provisioning; that is, do not allow new ingests on a Vault and do not allow new streams on a Streamer and move existing streams to another Streamer gracefully.

Step 2 Log in to the server as *root*.

Step 3 Ensure the server is fully offloaded.

a. Verify that the TRICKLE_DOWN file exists in the /usr/tmp directory.

b. For a Streamer, check that the protocoltiming log displays a warning message indicating that the server is going offline.

```
tail -f /arroyo/log/protocoltiming.log.20090917
```

You should see the following:

```
Remote vaults 2 caches 0 streamers 1, Adapters fill 4 (1024) stream 4 (1316)
CPU Receive: Ave0+0+0 Cur 0+0+0, Network: 0, Poll: 34 (0 scaled)
Warning: Server is going OFFLINE
```

c. For a Streamer, make sure that all the active streams have moved over to the other Streamers. Check the Active Streams line in the protocoltiming log.

d. For a Vault, make sure that all active ingests on this server have finished. Check that there is no Active Ingest Connections line in the protocoltiming log.

e. Check there is no active traffic on the network interface cards (NICs) using the **/home/stats/ifstats** command.

Step 4 In an ISA environment, stop the database and statsd processes using the following commands:

```
# db_shutdown
# ps -ef | grep statsd
# kill -9 ID
```

Step 5 In an RTSP environment, stop the database using the following commands:

```
# su -isa
# arroyo stop
```

Step 6 Ensure the database and statsd are fully stopped.

a. Check that the database thread count returns nothing.

```
netstat -an | grep 9999
```

b. Check that the statsd process returns nothing.

```
ps -aef | grep statsd
```

Step 7 Back up the configuration and database files. See "Performing a Backup on a VDS Server" section on page 5-31 for more information.

Step 8 On the VDS server being replaced, to prevent the VDS server from impacting the VDS network if it boots up again, comment out all of the lines in the /etc/rc.local file and edit the .arroyorc file to remove all entries in the Replication Group members section of the file.

Step 9 Using the CDSM GUI, shut down the server.

a. Click **Maintain > Servers > Server Shutdown**.

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

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

Step 10 Log in to the new server as user *root*.

Note The new replacement server has already been verified or upgraded to the same Cisco VDS-TV software version as the server it is replacing. This includes running the **cdsinstall** script to install the software; not the **cdsconfig** script.

Step 11 Restore the configuration and database files that were backed up to the Linux server. See "Performing a Restore on a VDS Server" section on page 5-33 for more information.

Step 12 Run the **cdsconfig** script to rewrite the rc.local file for the VDS server. The script prompts display default values in brackets that are taken from the configuration you restored. To accept the default, press **Enter**. If the default value is incorrect, enter the correct value and press **Enter**.

```
[root]# cdsconfig

ATTENTION!!!
If a new image is installed on this server, a reboot is required before running cdsconfig.
If a reboot is already performed, please continue.
Otherwise, please exit and execute cdsconfig after rebooting the server

Do you want to continue ? (yes/no) [y]: y
Enter management interface [eth0]: Enter

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]: 3

Backing up old scripts /etc/sysconfig/network-scripts
Writing new ifcfg-ethx scripts

Enter a hostname [Streamer-51]: Enter
Enter the number of the eth interface that connects to the gateway [0]: Enter
Enter the default gateway IP address [10.74.124.1]: 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
    ..............
   16. CDE110-2C-1
```

```
   17. CDE205-1C1-C
   18. CDE220-2A-C
   .................
   32. CDE420-4G-C
   33. CDE420-4G-F
Choice [3]: 3

Please select a device role:
    1. streamer
Choice [1]: 1
Is this Server going to get added to a Stream Domain in a CDN Split Domain Management
Environment ? (yes/no) [y]: n
Please enter a Group ID(Array ID) [5356]: Enter
Please enter a server ID [51]: Enter
Enter Stream Control interface (Hit 'Enter' to skip): Enter
Writing new configuration to /home/isa/.arroyorc
Current replication group members:
  vault         10.74.124.55
  vault         10.74.124.54
  streamer      10.74.124.21
  controller    10.74.124.175
Do you want to edit the replication group members? (yes/no) [n]: n
Configuring ISA ecosystem
Is this node getting added to an existing deployment ? (yes/no) [y]: n
Database is running.
Starting statsd
Run svrinit to seed database? (yes/no) [n]: n
Is this an IPTV deployment with Dual CAS? (yes/no) [n]: n
Writing rc.local
ISA ecosystem configuration finished
cdsconfig finished, please use CDSM to complete configuration
```

Step 13 Edit the rc.local file and uncomment all command lines.

Step 14 Reboot the server.

```
reboot
```

Step 15 Using the CDSM, disable the server offload.

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

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

c. Choose **Disable** and click **Submit**.

When Server Offload is enabled on a server, the server is configured to reject new provisioning; that is, do not allow new ingests on a Vault and do not allow new streams on a Streamer and move existing streams to another Streamer gracefully.

Step 16 Using the CDSM GUI, verify the server is online.

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

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

Removing a Server

You can remove a server if the server is experiencing unresolvable problems or when the network address or configuration has changed and you need to add the server back into the VDS network using a new address or configuration.

This section documents the following procedures:

- Removing a CDSM
- Removing a VDS Server

Removing a CDSM

Note A CDSM should only be removed if there are redundant CDSMs because at least one CDSM must be operational at all times.

To remove a CDSM, do the following:

Step 1 Log in to the CDSM to be removed as *root*.

Step 2 Stop Auto Importer if it is enabled on the CDSM being removed.

a. Check that the Auto Importer process is not running.

```
ps -ef | grep Importer
```

b. If Auto Importer is running, use the **kill** command with the PID.

```
kill - 9 <PID>
```

Step 3 In an ISA deployment, stop the Exporter process if it is enabled on the CDSM being removed.

a. Check that the Exporter process is not running.

```
ps -ef | grep Exporter
```

b. If the Exporter is running, use the **kill** command with the PID.

```
kill - 9 <PID>
```

Step 4 Stop the database on the CDSM being removed.

```
# db_shutdown
```

Step 5 Ensure that the database is fully stopped on the CDMS being removed.

a. Check that the database thread count returns nothing.

```
netstat -an | grep 9999
```

b. Make sure that no process ID (PID) is returned.

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

c. If the database is still up, use the **kill** command with the PID.

```
kill -9 <PID>
```

Step 6 On the primary CDSM, do the following:

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

b. Edit the .arroyorc file and remove the CDSM entry, which is the controller entry in the Replication Group Members section.

c. If the Auto Importer is running on the primary CDSM, stop this process.

```
[isa]# ps -ef | grep Importer
[isa]# kill -9 <PID>
```

d. In an ISA environment, if the Exporter is running on the primary CDSM, stop this process.

```
[isa]# ps -ef | grep Exporter
[isa]# kill -9 <PID>
```

e. Stop the database on the primary CDSM.

```
[root]# db_shutdown
[root]# ps -ef|grep avsdb
[root]# netstat -an | grep 9999
```

f. Restart the database on the primary CDSM.

```
[root]# su - isa
```

g. If the Auto Importer was running on the primary CDSM, wait five minutes until the database has restarted, and restart the Auto Importer processes.

```
[root]# su - isa -c "cd /home/isa/RTScheduler/Importer; ./ImporterServer -d failover"
[root]# ps -ef | grep Importer
```

h. In an ISA environment, if the Exporter process was running on the primary CDSM, restart the Exporter processes.

```
[root]# su - isa -c "cd /home/isa/RTScheduler/Exporter; ./ExporterServer >&
/home/isa/RTScheduler/Exporter/ExporterServer.log&"
[root]# ps -ef | grep Exporter
```

Step 7 On each VDS server in the system, do the following:

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

b. Edit the .arroyorc file and remove the CDSM entry, which is the controller entry in the Replication Group Members section.

c. In an RTSP environment, stop the database and all applications on the VDS server.

```
[isa]# arroyo stop
[isa]# arroyo status
```

d. In an ISA environment, stop the database on the VDS server.

```
[root]# db_shutdown
[root]# ps -ef|grep avsdb
[root]# netstat -an | grep 9999
```

e. In an RTSP environment, restart the database and applications on Vaults using the following commands:

```
[isa]# arroyo start avsdb
[isa]# arroyo start fsi aim
[isa]# arroyo status
```

f. In an RTSP environment, restart the database and applications on Streamers using the following commands:

```
[isa]# arroyo start avsdb
[isa]# arroyo start rtsp
[isa]# arroyo status
```

g. In an ISA environment, restart the database on the VDS server using the following commands:

```
[root]# su - isa
[isa]# exit
[root]# ps -ef|grep avsdb
```

Step 8 Log in to the remaining CDSM as *root* and remove the statsd line in the /etc/rc.local file. This line is only for redundant CDSMs.

Step 9 Stop the statsd process.

```
# ps -ef | grep statsd
# kill -9 ID
```

Step 10 To verify that the statsd process has stopped, try accessing the remaining CDSM by the virtual IP address that was used for CDSM redundancy. If successful, shut down the virtual IP address by using the **ifconfig eth0:1 down** command.

Step 11 To prevent the CDSM being removed from impacting the VDS network if it boots up again, do the following:

a. On the CDSM being removed, edit the rc.local file and comment out the following lines in the rc.local file

```
#!/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

#/home/stats/statsd -i 10.74.124.103 -s 255.255.255.0 -d eth0

sleep 300
```

b. Log in to the CDSM as user **isa** and edit the .arroyorc file to remove all entries in the Replication Group members section of the file.

Step 12 Shut down the CDSM being removed.

```
#poweroff
```

Removing a VDS Server

Removing a Vault, Streamer, ISV, or Caching Node includes the following tasks:

1. Offload the server, shut down the processes on the server, and deregister the server.
2. Remove the server entry from the .arroyorc file on each VDS server.
3. Shut down the server and remove it from the CDSM.

To permanently remove a Vault, Streamer, Caching Node, or ISV, do the following:

Step 1 Using the CDSM GUI, offload the server that you want to remove.

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

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

c. Choose **Enable** and click **Submit**.

When Server Offload is enabled on a server, the server is configured to reject new provisioning; that is, do not allow new ingests on a Vault and do not allow new streams on a Streamer and move existing streams to another Streamer gracefully.

Step 2 Log into the server as *root*.

Step 3 Ensure that the server is fully offloaded.

a. Verify that the TRICKLE_DOWN file exists in the /usr/tmp directory.

b. For a Streamer, check that the protocoltiming log displays a warning message indicating that the server is going offline.

```
tail -f /arroyo/log/protocoltiming.log.20090917
```

You should see the following:

```
Remote vaults 2 caches 0 streamers 1, Adapters fill 4 (1024) stream 4 (1316)
CPU Receive: Ave0+0+0 Cur 0+0+0, Network: 0, Poll: 34 (0 scaled)
Warning: Server is going OFFLINE
```

c. For a Streamer, make sure that all the active streams have moved over to the other Streamers. Check the Active Streams line in the protocoltiming log.

d. For a Vault, make sure that all active ingests on this server have finished. Check that there is no Active Ingest Connections line in the protocoltiming log.

e. Check there is no active traffic on the network interface cards (NICs) using the **/home/stats/ifstats** command.

Step 4 If the server is a member of a group, remove the server from the group.

a. From the VDS GUI, click **Configure > Array Level > Stream/Vault/Cache Groups Setup**. The Group Configure page is displayed.

b. From the **Select Stream/Vault/Cache Group** drop-down list, choose the group ID and click **Display**.

c. From the **New Group** drop-down list, choose **None** for the VDS server and click **Submit**.

Step 5 Stop the statsd process.

```
# ps -ef | grep statsd
# kill -9 ID
```

Step 6 Ensure the statsd process is fully stopped. Check that the statsd process returns nothing.

```
ps -aef | grep statsd
```

Note If statsd is running when the **svrinit_15** command is used, the VDS server still shows up in the CDSM GUI as a phantom server. Stop the statsd process, then use the **svrinit_15** command, and the phantom server is removed. The database must still be running on the VDS server at the time of using the **svrinit_15** command.

Step 7 Use the **svrinit_15** command to deregister the server by using the -d option.

```
# cd/home/stats
# ./svrinit_15 -d -i <IP address of CDS being removed> -s <netmask> -h <hostname> -g
<gateway>
```

Step 8 In an RTSP environment, stop the database and applications on the VDS server being removed using the following commands:

```
[isa]# arroyo stop
[isa]# arroyo status
```

Step 9 In an ISA environment, stop the database on the VDS server being removed using the following command:

```
# db_shutdown
```

Step 10 Ensure that the database is fully stopped.

a. Check that the database thread count returns nothing.

```
netstat –an | grep 9999
```

b. Make sure that no process ID (PID) is returned.

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

c. If the database is still up, use the **kill** command with the PID.

```
kill -9 <PID>
```

Step 11 On each CDSM, do the following:

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

b. Edit the .arroyorc file and remove the server entry under the Replication Group Members section.

a. Stop the Auto Importer process if it is running using the following commands:

```
#ps -ef|grep Importer
#kill -9 PID
```

b. In an ISA environment, stop the Exporter process if it is running.

```
#ps -ef|grep Exporter
#kill -9 PID
```

c. Shut down the database.

```
#db_shutdown
```

d. Ensure that the database has fully stopped.

```
netstat –an | grep 9999
ps -ef|grep avsdb
kill -9 <PID>
```

e. Restart the database on the CDSM.

```
[root]# su - isa
```

f. Restart the Auto Importer process if it had been running.

```
[root]# su - isa -c "cd /home/isa/RTScheduler/Importer; ./ImporterServer -d failover"
[root]# ps -ef | grep Importer
```

g. In an ISA environment, on the primary CDSM, start the Exporter again if it had been running on the CDSM prior to the shutdown of the database.

```
[root]# su - isa -c "cd /home/isa/RTScheduler/Exporter; ./ExporterServer
/home/isa/RTScheduler/Exporter/ExporterServer.log&"
[root]# ps -ef | grep Exporter
```

Step 12 On each VDS server, do the following:

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

b. Edit the .arroyorc file and remove the server entry under the Replication Group Members section.

c. Stop the database and applications.

In an RTSP environment, use the following commands:

```
#su - isa
#arroyo stop
```

In an ISA environment, use the following commands:

```
# db_shutdown
```

d. Restart the database and applications.

For a Vault in an RTSP environment, use the following commands:

```
[root]# su - isa
[isa]# arroyo start avsdb
[isa]# arroyo start fsi aim
[isa]# arroyo status
```

For a Streamer in an RTSP environment, use the following commands:

```
[root]# su - isa
[isa]# arroyo start avsdb
[isa]# arroyo start rtsp
[isa]# arroyo status
```

In an ISA environment, use the following commands:

```
[root]# su - isa
[isa]# exit
[root]# ps -ef|grep avsdb
```

Step 13 On the VDS server being removed, to prevent the VDS server from impacting the VDS network if it is boots up again, comment out all of the lines in the /etc/rc.local file and edit the .arroyorc file to remove all entries in the Replication Group members section of the file.

Step 14 Shut down the VDS server.

```
[isa]# arroyo stop all
[isa]# exit
[root]# poweroff
```

Step 15 Log in to the CDSM GUI and verify that the VDS server is not displayed in the System Health Monitor page.

If the removed VDS server displays in the System Health Monitor page, do the following:

a. Log in to the CDSM as *root*.

b. Edit the .arroyorc file, record the server ID and group ID of the CDSM, then change the server ID and group ID entry for the CDSM to be the same as the server ID and group ID as the removed server.

c. Run the **./svrinit_15** command. This manually removes the VDS server.

```
# cd/home/stats
# ./svrinit_15 -d -i <IP address of CDS being removed> -s <netmask> -h <hostname> -g
<gateway>
```

d. Edit the .arroyorc file again and change the server ID and group ID entry back to the CDSM values.

Adding a Server

The procedure to add a server in the VDS is different depending on the type of server being added. This section provides information on the following procedures:

- Adding a Second CDSM
- Adding a VDS Server

Adding a Second CDSM

Note All VDS servers and CDSM that are part of the same system as the CDSM you are adding must be online for the database synchronization to work properly.

Note The database synchronization copies database information from all existing VDS servers and the existing CDSM, with the exception of Stream Report data. If you require a copy of Stream Report data, copy the database on the existing CDSM to the new CDSM. The copy is performed during a maintenance window on the existing CDSM.

To implement the CDSM Redundancy feature, do the following:

Step 1 Log in to the new CDSM as *root* .

Note The new replacement server has already been verified or upgraded to the same Cisco VDS-TV software version as the server it is replacing. This includes running the **cdsinstall** script to install the software; not the **cdsconfig** script.

Step 2 Run the **cdsconfig** script. The following are some user prompts to be aware of when running the **cdsconfig** script. :

- When the script returns the list of current replication groups, verify that all members have been listed. If any member is missing, at the "Do you want to edit the replication group members?" prompt, enter **Y** for yes, and enter the missing member.
- At the "Is this node getting added to an exiting deployment?" prompt, enter **Y** for yes to dynamically add this CDSM.
- At the "Do you want to enable CDSM redundancy?" prompt, enter **Y** for yes. You are prompted for the virtual IP address and netmask that is used to access the CDSM. Answer appropriately to the prompts related to getting the ID from the first CDSM.

If you do not require Stream Report data to be copied to the new CDSM, go to Step 14.

Step 3 Login in to the existing CDSM as *root*.

Step 4 Stop Auto Importer if it is enabled on the existing CDSM.

a. Check that the Auto Importer process is not running.

```
ps -ef | grep Importer
```

b. If Auto Importer is running, use the **kill** command with the PID.

```
kill - 9 <PID>
```

Step 5 In an ISA deployment, stop the Exporter process if it is enabled on the existing CDSM.

a. Check that the Exporter process is not running.

```
ps -ef | grep Exporter
```

b. If the Exporter is running, use the **kill** command with the PID.

```
kill - 9 <PID>
```

Step 6 Stop the database on the existing CDSM.

```
[root]# db_shutdown
```

Step 7 Ensure that the database is fully stopped.

a. Check that the database thread count returns nothing.

```
netstat -an | grep 9999
```

b. Make sure that no process ID (PID) is returned.

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

c. If the database is still up, use the **kill** command with the PID.

```
kill -9 <PID>
```

Step 8 Stop the database on the new CDSM and verify that the database has fully stopped using the procedure outline in Step 6 to Step 7.

Step 9 On the new CDSM, use the **scp** command to copy the DATADIR directory from the existing 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 10 Change the ownership of DATADIR from *root:root* to *isa:isa.*

```
# chown -R isa:isa /arroyo/db/DATADIR
```

Step 11 Start the database on the existing CDSM.

```
# su -isa
```

Step 12 On the existing CDSM, start the Auto Importer again if it had been running prior to shutting down the database.

```
[root]# su - isa -c "cd /home/isa/RTScheduler/Importer; ./ImporterServer -d failover"
[root]# ps -ef | grep Importer
```

Step 13 In an ISA environment, on the existing CDSM, start the Exporter again if it had been running prior to shutting down the database.

```
[root]# su - isa -c "cd /home/isa/RTScheduler/Exporter; ./ExporterServer >&
/home/isa/RTScheduler/Exporter/ExporterServer.log&"
[root]# ps -ef | grep Exporter
```

Step 14 On the new CDSM, start the Apache server by running the following command:

```
/arroyo/www/bin/apachectl start
```

Step 15 Log in to the GUI on the new CDSM as a user with Engineering access level. The CDSM Setup page is displayed.

Step 16 In the **Installation** drop-down list, choose either **RTSP** or **ISA** depending on your environment.

Step 17 If Media Scheduler is enabled on existing CDSM, do the following:

a. Scroll down to the Media Scheduler section, and click the **ON** radio button next to the **Media Scheduler** field. In the Activation Key field, enter the software access key from your Right to Use Notification for the CDAMS product.

b. Scroll down to the **Ingest Manage**r section, and click the **ON** radio button next to the **Ingest Manager** field. In the **Activation key** field, enter the software access key from your Right to Use Notification from the CDAMS product.

Step 18 Verify that all other settings are the same as on the existing CDSM and click **Submit**.

Step 19 On the GUI of the new CDSM, choose **Maintain > Software > System Configs**. The System Configs page is displayed.

Step 20 Verify the CDS parameters on the System Configs page and click **Submit**.

Step 21 Configure NTP on the new CDSM.

a. Set your time zone on the CDSM by copying your time zone file to the /etc/local file. In the following example, the time zone is Asia/Shanghai.

```
#cp   /usr/share/zoneinfo/Asia/Shanghai    /etc/localtime
```

b. Verify that the clock information displayed in the file /etc/sysconfig/clock is correct. The file should display the following information

```
Zone=time zone
UTC=fale
ARC=false
```

Timezone represents zone as presented by the zone flie under directory /usr/share/zoneinf. Setting UTC to lase sets the clock to the local time. Setting ARC to false, sets the time to Unix epoch time.

c. Remove all existing lines from the NTP configuration file /etc/ntp.conf and add the NTP server using the command **server** *NTP_Sever_IP_Address* **# local clock.** In the following example, the NTP server has an IP address of 10.74.124.189.

```
# server  10.74.124.189   # local clock
```

d. Start the NTP service.

```
# service ntpd start
```

e. Turn on the NTP service.

```
# chkconfig ntpd on
```

Step 22 When the **cdsconfig** script finishes, edit the rc.local file on the new CDSM and uncomment all the command lines. In an ISA deployment, the **su - isa -c "cd /home/isa/RTScheduler/Exporter...**" command is only used when the MediaX feature sends notifications to a catalog server or similar server. In both an ISA and an RTSP deployment, the **su - isa -c "cd /home/isa/RTScheduler/Importer**; ./**ImporterServer -d failover"** command is required when the MediaX Auto Importer is used.

The 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&"

    su - isa -c "cd /home/isa/RTScheduler/Importer; ./ImporterServer -d failover"

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

    sleep 30
```

Step 23 Shut down the database and reboot the newly added CDSM.

```
# db_shutdown
# ps -ef|grep avsdb
# netstat -an | grep 9999
# reboot
```

Step 24 On the existing CDSM, run the **cdsconfig** script to enable redundancy.

Step 25 When the **cdsconfig** script completes, edit the rc.local file and uncomment all the command lines.

Step 26 Reboot the existing CDSM.

The CDSM Redundancy feature is configured.

Adding a VDS Server

Note All VDS servers and CDSMs that are part of the same system as the VDS server you are adding must be online for the database synchronization to work properly.

To add a Vault, Streamer, Caching Node, or ISV to an existing VDS, do the following:

Step 1 Log into the new server as user *root*.

Note The new replacement server has already been verified or upgraded to the same Cisco VDS-TV software version as the server it is replacing. This includes running the **cdsinstall** script to install the software; not the **cdsconfig** script.

Step 2 Make sure the only interface that is configured is the management interface. If other interfaces are configured (for example, the ingest interface), the adding a server procedure fails.

```
ifconfig -a | more
```

If other interfaces are configured on this VDS server, manually shut them down by using the **ifconfig eth# down** command, where eth# is the interface name (for example, eth1).

Step 3 Run the **cdsconfig** script to configure the VDS server, create the rc.local file, and edit the .arroyorc file on every VDS server in the same system. The script prompts display default values in brackets. To accept the default, press **Enter**. If the default value is incorrect, enter the correct value and press **Enter**.

Note The **cdsconfig** script detects all configured interfaces. When adding a new VDS server, only the management interface should be configured. The script provides the ability to disable the other interfaces. You must disable all other interfaces and leave only the management interface configured for the **cdsconfig** script to complete successfully.

```
[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:172.22.99.237    mask:255.255.254.0    bcast:172.22.99.255
    2. Configure another interface
    3. Done
Choice [3]: 3

Backing up old scripts /etc/sysconfig/network-scripts
Writing new ifcfg-ethx scripts

Enter a hostname: hostname
Enter the number of the eth interface that connects to the gateway [eth0]:
Enter the default gateway: gateway

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

Please choose your platform from the following list of valid platforms:
    1. 2U-SCSI-1
    2. 1. 2U-SCSI-1
    2. 3U-SCSI-1
    3. 3U-SCSI-10
    ............
   16. CDE110-2C-1
   17. CDE205-1C1-C
   18. CDE220-2A-C
   ..............
   32. CDE420-4G-C
   33. CDE420-4G-F
Choice: server_platform

Please select a device role:
    1. ssv
    2. vault
    3. cache
    4. streamer
Choice: device_role
```

Step 4 The **cdsconfig** script asks for information about your VDS to get a server ID and group ID for the new VDS server. Answer the questions correctly for your system to make sure the correct server ID and group ID are applied. If the device role is a Streamer, you have the option to enter the Stream Control interface through the script, or later through the CDSM GUI.

Step 5 The **cdsconfig** script prompts you to add the replication group members. Add all the VDS servers, including CDSMs, that share information with this server.

```
Do you want to edit the replication group members (yes/no) [n]: y
```

Note With the exception of the server you are configuring, all VDS servers (VVIMs, Stream Managers, CDSMs, 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.

Step 6 If this is an RTSP deployment, you are asked if it is an NGOD deployment and what NPT syntax is used for the deployment.

```
Configuring RTSP ecosystem
Is this an NGOD deployment (yes/no):

Choose NPT Syntax:
    1. NGOD
    2. NGOD_SC
    3. Standard
Choice [NGOD]:3

Writing /home/isa/bss/scripts/arroyo-env.sh
Writing /home/isa/bss/scripts/arroyo-site-env.sh
```

```
Setting Sttributes for AVSRTSPServer
```

Step 7 In an RTSP deployment, the **cdsconfig** script asks if you want to enable Redirect Server. Answer no (**N**) to disable the Redirect Server.

```
Do you want to enable Redirect Server ? (yes/no) [y]: no
```

Step 8 The **cdsconfig** script asks if the server is being added to an existing deployment. Answer yes (**Y**) to synchronizes the database on the new server with the database on all the other CDS servers.

```
Is this node getting added to an existing deployment ? (yes/no) [y]:y

Starting database sync...

...Output omitted

Database sync completed.
Started avsdb, verify with "arroyo status"
Starting statsd
```

Note The time it takes to synchronize the database is proportional to the size of the database. Database synchronization could take up to 30 minutes for 90,000 content objects.

Step 9 The **cdsconfig** script asks if you want to run svrinit to seed the database. Enter **Y** for yes to run svrinit to seed the database or **N** for no. Enter the IP address, netmask, hostname, and gateway of this VDS server when prompted. These are the same settings as you configured for the eth0 interface at the beginning of the **cdsconfig** script.

Note You must seed the database whenever you are adding a new VDS server to a network or installing the VDS-TV software on a VDS server. Wait until all e database connections are established before entering the management IP address, management netmask, hostname, and gateway of this VDS server.

```
Run svrinit to seed database? (yes/no) [n]: y
Running svrinit
Please enter an IP address for svrinit: mgmt_ip_address
Please enter a netmask for svrinit: mgmt_netmask
Please enter a hostname for svrinit: hostname
Please enter a gateway for svrinit:gateway
Writing /etc/rc.d/rc.local
RTSP ecosystem configuration finished
cdsconfig finished, please use CDSM to complete configuration
```

If you receive an error message indicating the database is unavailable and cannot be set up, enter the following commands to initialize the database tables for a VDS server in an ISA environment:

```
[root]# su - isa
[isa]# exit
[root]# /home/stats/svrinit_15 -h <hostname> -i <ip address> -s <mask-ip address> -g
<gateway>
```

Enter the following commands to initialize the database tables for a VDS server in an RTSP environment:

```
[root]# su - isa
[isa]# arroyo start avsdb
[isa]# exit
```

```
[root]# /home/stats/svrinit_15 -h <hostname> -i <ip address> -s <mask-ip address> -g
<gateway>
```

Note If this server has, at some point, been part of a Cisco VDS array before this configuration, clean out /arroyo/db by deleting *.db *.idx and all replication IP address files. Also, in an ISA deployment, delete all /persist directories found in the directories under /home/isa/Streaming and /home/isa/ContentStore.

Step 10 Verify connectivity to the CDSM. Using the CDSM GUI, choose **Monitor > System Health**. The System Health Monitor page is displayed.

The status boxes for the server should all be green. The services status box may be yellow because some services may not be running.

Step 11 To complete the server configuration, log in to the CDSM GUI and go through the **Configure > Server Level** pages for the new server.

Note In RTSP deployments, if you need to enable the Redirect Server in Release 3.5, run the **cdsconfig** script and answer yes (**Y**) at the following prompt:

```
Do you want to enable Redirect Server ? (yes/no) [y]
```

Backup and Recovery

This section provides information on the following procedures:

- Preparation for a Backup
- Performing a Backup on the CDSM or VVIM
- Performing a Restore on the CDSM
- Performing a Backup on a VDS Server
- Performing a Restore on a VDS Server

Note Any VDS server or another Linux server on the network can be used as a backup server as long as it has the /arroyo/backup directory and is accessible through SSH. The CDSM backup files require approximately 50 MB of disk space. The backup files for each VDS server (Streamer, Vault, or ISV) require approximately 1 MB each of disk space.

Preparation for a Backup

Before performing backup or restore on any server in the VDS, follow these precautionary steps:

Step 1 On the Linux server used to store the backup files, create the /arroyo/backup directory.

Step 2 Before performing the CDSM backup, collect the configuration information on the system.

a. Collect the following configuration settings on each server and write them down:

- Management IP address
- Gateway IP address Network mask
- Network mask
- Stream and cache interface IP address
- Streamer ID
- Stream Group ID
- QAM Gateways
- Route tables
- Name Service IP address (ISA only)
- Ingest IP address
- Service Groups

Note This is a precautionary step, because the configuration is saved in the backup file created.

b. Log in to the CDSM with Engineering access. The CDSM setup page is displayed.

c. Write down the settings for every field on the CDSM Setup page.

Note Backup and restore 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.

Performing a Backup on the CDSM or VVIM

Before you back up the CDSM or VVIM, make sure you have collected the configuration information and created the backup directory on a Linux server. See the "Preparation for a Backup" section on page 5-26 for more information. Backing up the configuration and database files on the CDSM or VVIM includes the following tasks:

1. Stop the database and shut down the processes on the CDSM or VVIM.
2. Run the **preupgrade** script to back up the configuration and database files.
3. Verify the tar file has been copied to the Linux server.
4. Reboot the CDSM or VVIM.

To back up the CDSM or VVIM, do the following:

Step 1 Log in to the CDSM or VVIM server as *root*.

Step 2 Stop Auto Importer if it is enabled on the CDSM.

a. Check that the Auto Importer process is not running.

```
ps -ef | grep Importer
```

b. If Auto Importer is running, use the **kill** command with the PID.

```
kill - 9 <PID>
```

Step 3 In an ISA deployment, stop the Exporter process if it is enabled on the CDSM.

a. Check that the Exporter process is not running.

```
ps -ef | grep Exporter
```

b. If the Exporter is running, use the **kill** command with the PID.

```
kill - 9 <PID>
```

Step 4 Enter the following command to stop the database on a CDSM.

```
# db_shutdown
```

Step 5 Enter the following command to stop the database on a VVIM.

```
# su - isa
Database is running.
$ cd /arroyo/db
$ ./stop_db
$ exit
```

Step 6 Ensure that the database is fully stopped.

a. Check that the database thread count returns nothing.

```
netstat –an | grep 9999
```

b. Make sure that no process ID (PID) is returned.

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

c. If the database is still up, use the **kill** command with the PID.

```
kill -9 <PID>
```

Step 7 If the CDSM or VVIM is redundant, shut down the statsd process and ensure that the process has stopped.

```
# ps -ef | grep statsd
# kill -9 PID
# ps -aef | grep statsd
```

Step 8 Shut down the Apache server and ensure the server is shut down.

```
# /arroyo/www/bin/apachectl stop
   httpd: Could not reliably determine the server's fully qualified domain name, using
   10.74.115.120 for ServerName

# pgrep httpd
```

Step 9 Log on to the Linux server where the backup files are to be placed and verify that the /arroy/backup directory exists. If the backup folder does not exist, create it.

```
# mkdir /arroyo/backup
```

Step 10 To back up the configuration and database files to the available Linux server, run the **preupgrade** script. You are prompted for the IP address of the backup server, which is the server you are using to store the backup files.

```
# cd /home/upgrade/2_2
# ./preupgrade
```

```
Starting Backup of configuration and database files
   Checking that all processes are stopped on the system
   Checking that cserver is not running on the system
   Starting Backup of files to: /root/cdsm218
   Backup of files completed.
   Creating Tarball of backed up files
   Tarball of backed up files created successfully

!! IMPORTANT : Make sure that the directory /arroyo/backup is created on the machine to
back up !!
IP Address of machine to backup configuration/database files?: 171.71.51.99
root@171.71.51.99's password:
cdsm218.tgz                                                                    100%
47MB 687.3KB/s   01:11
Tarball uploaded to 171.71.51.99

Scripts executed successfully !!!
Please reboot the server and run the script 'upgrade' when the server comes back up.
```

Note Do not reboot the server and run the **upgrade** script at this time.

Step 11 Ensure that the tar file was copied to the backup server in the /arroyo/backup directory.

Step 12 Reboot the CDSM or VVIM.

```
reboot
```

Performing a Restore on the CDSM

Before you can restore a backup, you need to create the backup. See "Performing a Backup on the CDSM or VVIM" section on page 5-27. Restoring the configuration and database files on the CDSM includes the following tasks:

1. Stop the database and shut down the processes on the CDSM.
2. Run the **upgrade** script to restore the configuration and database files.
3. Check that the settings in the .arroyorc file are correct.
4. Reboot the CDSM.

Note Before running the **upgrade** script, make sure you can ping the backup server where the backup configuration and database files are stored. You are prompted for the IP address of the backup server.

To restore a backup, do the following:

Step 1 Log in to the CDSM server as *root*.

Step 2 Stop Auto Importer if it is enabled on the CDSM.

a. Check that the Auto Importer process is not running.

```
ps -ef | grep Importer
```

b. If Auto Importer is running, use the **kill** command with the PID.

```
kill - 9 <PID>
```

Step 3 In an ISA deployment, stop the Exporter process if it is enabled on the CDSM.

a. Check that the Exporter process is not running.

```
ps -ef | grep Exporter
```

b. If the Exporter is running, use the **kill** command with the PID.

```
kill - 9 <PID>
```

Step 4 Stop the database.

```
# db_shutdown
```

Step 5 Ensure that the database is fully stopped.

a. Check that the database thread count returns nothing.

```
netstat –an | grep 9999
```

b. Make sure that no process ID (PID) is returned.

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

c. If the database is still up, use the **kill** command with the PID.

```
kill -9 <PID>
```

Step 6 Shut down the Apache server and ensure the server is shut down.

```
# /arroyo/www/bin/apachectl stop
    httpd: Could not reliably determine the server's fully qualified domain name, using
    10.74.115.120 for ServerName

# pgrep httpd
```

Step 7 If the CDSM is redundant, shut down the statsd process and ensure that the process has stopped.

```
# ps -ef | grep statsd
# kill -9 ID
# ps -aef | grep statsd
```

Step 8 To restore the database from a backup, delete or rename the existing CDSM database.

If this is a new server and the database has not been seeded (run **svrinit_15** step in the **cdsconfig** script), there is no database to delete, so this step can be skipped.

To delete the database use the **rm -rf DATADIR** command.

To rename the database use the **mv DATADIR DATADIR-***new-name* command. For example, the following command renames the database to DATDIR-2.2:

```
# cd /arroyo/db
# mv DATADIR DATADIR-2.2
```

Step 9 Restore the CDSM configuration and database files from the backup by running the **upgrade** script.

```
# cd /home/upgrade/2_2/
# ./upgrade

Restoring backup of configuration and database files
   Checking that all processes are stopped on the system
   Checking that cserver is not running on the system
Please enter the hostname of this device : cdsm218
   Collect cdsm218.tgz from server with backup data
```

```
IP Address of machine containing configuration/database files?: 171.71.51.99
The authenticity of host '171.71.51.99 (171.71.51.99)' can't be established.
RSA key fingerprint is 09:0f:95:9e:0b:ff:ec:ce:1a:cb:3f:39:0d:ce:d4:36.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '171.71.51.99' (RSA) to the list of known hosts.
root@171.71.51.99's password:
cdsm218.tgz                                                                   100%
48MB   1.1MB/s   00:43
   Untarring cdsm218.tgz
   This installation appears to be a 1.5.1.X --> 2.x Upgrade.  Database Conversion
   is required to continue.

   Upgrading database ...
DB->Cursor: Successful return: 0
DB->Cursor: Successful return: 0
DB->Cursor: Successful return: 0
Done.
Scripts executed successfully. Please follow these steps below :
1. Customize and Uncomment the service start commands in /etc/rc.local
2. Reboot the servers.
```

Step 10 Check the .arroyorc file to make sure that the configuration settings are correct.

Step 11 Check the rc.local file to make sure that the services will start on boot up.

Step 12 Check the /etc/hosts file to make sure the host settings are correct.

Step 13 Check the /etc/sysconfig/network file to make sure the network settings are correct.

Step 14 Check the /etc/sysconfig/network-scripts/ifcfg-eth0 file to make that the Management IP address is set correctly.

Step 15 Reboot the CDS:M

```
reboot
```

Performing a Backup on a VDS Server

Before you back up the VDS server, make sure you have collected the configuration information and created the backup directory on a Linux server. See the "Preparation for a Backup" section on page 5-26 for more information. Backing up the configuration and database files includes the following tasks:

1. Offload the server and shut down the processes on the server.
2. Comment out all the command lines in the rc.local file and reboot the VDS server.
3. Run the **preupgrade** script to backup the configuration and database files.
4. Verify that the tar file has been copied to the Linux server.
5. Edit the rc.local file and uncomment all the command lines.
6. Reboot the VDS server, wait for it to come online, and disable the Server Offload.

To perform a backup on a Vault, Caching Node, Streamer, or ISV, 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 the IP address of the server and click **Display**.

c. Choose **Enable** and click **Submit**.

When Server Offload is enabled on a server, the server is configured to reject new provisioning; that is, do not allow new ingests on a Vault and do not allow new streams on a Streamer and move existing streams to another Streamer gracefully.

Step 2 Log in to the VDS server as *root*.

Step 3 Ensure that the server is fully offloaded.

a. Verify that the TRICKLE_DOWN file exists in the /usr/tmp directory.

b. For a Streamer, check that the protocoltiming log displays a warning message indicating that the server is going offline.

```
tail -f /arroyo/log/protocoltiming.log.20090917
```

You should see the following:

```
Remote vaults 2 caches 0 streamers 1, Adapters fill 4 (1024) stream 4 (1316)
CPU Receive: Ave0+0+0 Cur 0+0+0, Network: 0, Poll: 34 (0 scaled)
Warning: Server is going OFFLINE
```

c. For a Streamer, make sure that all the active streams have moved over to the other Streamers. Check the Active Streams line in the protocoltiming log.

d. For a Vault, make sure that all active ingests on this server have finished. Check that there is no Active Ingest Connections line in the protocoltiming log.

e. Check there is no active traffic on the network interface cards (NICs) using the **/home/stats/ifstats** command.

Step 4 In an ISA environment, stop the database and statsd processes using the following commands:

```
# db_shutdown
# ps -ef | grep statsd
# kill -9 ID
```

Step 5 In an RTSP environment, stop the database using the following command:

```
# su -isa
# arroyo stop
```

Step 6 Ensure the database and statsd processes are fully stopped.

a. Check that the database thread count returns nothing.

```
netstat -an | grep 9999
```

b. Check that the statsd process returns nothing.

```
ps -aef | grep statsd
```

Step 7 Edit the rc.local file so that it does not start any service; that is, comment out all command lines.

Step 8 Reboot the server.

```
reboot
```

Step 9 Run the **preupgrade** script. The **preupgrade** script is located in the /home/upgrade/2_2 directory.

```
# ./preupgrade

Starting Backup of configuration and database files
   Checking that all processes are stopped on the system
   Checking that cserver is not running on the system
   Starting Backup of files to: /root/s66
   Backup of files completed.
```

```
   Creating Tarball of backed up files
   Tarball of backed up files created successfully

!! IMPORTANT : Make sure that the directory /arroyo/backup is created on the machine to
back up !!
IP Address of machine to backup configuration/database files?: 171.71.51.99
The authenticity of host '171.71.51.99 (171.71.51.99)' can't be established.
RSA key fingerprint is 09:0f:95:9e:0b:ff:ec:ce:1a:cb:3f:39:0d:ce:d4:36.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '171.71.51.99' (RSA) to the list of known hosts.
root@171.71.51.99's password:
s66.tgz              100%
|*****************************************************************************|  1078 KB
00:00
Tarball uploaded to 171.71.51.99

Scripts executed successfully !!!
Please reboot the server and run the script 'upgrade' when the server comes back up.
```

Step 10 Ensure that the tar file was copied to the backup server in the /arroyo/backup directory.

Step 11 Edit the rc.local file and uncomment all the command lines.

Step 12 Reboot the server.

```
reboot
```

Step 13 Using the CDSM, disable the server offload.

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

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

c. Choose **Disable** and click **Submit**.

When Server Offload is enabled on a server, the server is configured to reject new provisioning; that is, do not allow new ingests on a Vault and do not allow new streams on a Streamer and move existing streams to another Streamer gracefully.

Step 14 Using the CDSM GUI, verify that the server has come online.

a. Choose **Monitor > System Health**. The System Health Monitor page is displayed.

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

Performing a Restore on a VDS Server

Before you can restore a backup, you need to create the backup. See "Performing a Backup on a VDS Server" section on page 5-31. Restoring the configuration and database files includes the following tasks:

1. Offload the server and shut down the processes on the server.
2. Comment out all the command lines in the rc.local file and reboot the VDS server.
3. Delete or rename the database.
4. Run the **upgrade** script to restore the configuration and database files.
5. Edit the rc.local file and uncomment all the command lines.
6. Reboot the VDS server, wait for it to come online, and disable the Server Offload.

Note Before running the **upgrade** script, make sure you can ping the backup server where the backup configuration and database files are stored. You are prompted for the IP address of the backup server.

To perform a restore on a Vault, Caching Node, Streamer, or ISV, 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 the IP address of the server and click **Display**.

c. Choose **Enable** and click **Submit**.

When Server Offload is enabled on a server, the server is configured to reject new provisioning; that is, do not allow new ingests on a Vault and do not allow new streams on a Streamer and move existing streams to another Streamer gracefully.

Step 2 Log in to the VDS server as *root*.

Step 3 Ensure that the server is fully offloaded.

a. Verify that the TRICKLE_DOWN file exists in the /usr/tmp directory.

b. For a Streamer, check that the protocoltiming log displays a warning message indicating that the server is going offline.

```
tail -f /arroyo/log/protocoltiming.log.20090917
```

You should see the following:

```
Remote vaults 2 caches 0 streamers 1, Adapters fill 4 (1024) stream 4 (1316)
CPU Receive: Ave0+0+0 Cur 0+0+0, Network: 0, Poll: 34 (0 scaled)
Warning: Server is going OFFLINE
```

c. For a Streamer, make sure that all the active streams have moved over to the other Streamers. Check the Active Streams line in the protocoltiming log.

d. For a Vault, make sure that all active ingests on this server have finished. Check that there is no Active Ingest Connections line in the protocoltiming log.

e. Check there is no active traffic on the network interface cards (NICs) using the **/home/stats/ifstats** command.

Step 4 In an ISA environment, stop the database and statsd processes using the following commands:

```
# db_shutdown
# ps -ef | grep statsd
# kill -9 ID
```

Step 5 In an RTSP environment, stop the database and using the following command:

```
# su -isa
# arroyo stop
```

Step 6 Ensure the database and statsd processes are fully stopped.

a. Check that the database thread count returns nothing.

```
netstat -an | grep 9999
```

b. Check that the statsd process returns nothing.

```
ps -aef | grep statsd
```

Step 7 Edit the rc.local file so that it does not start any service; that is, comment out all command lines.

Step 8 Reboot the server.

```
# reboot
```

Step 9 To restore the configuration and database files from a backup, delete or rename the existing database.

Note If this is a new server and the database has not been seeded (run **svrinit_15** step in the **cdsconfig** script), there is no database to delete, so this step can be skipped.

To delete the database use the **rm -rf DATADIR** command. To rename the database use the **mv DATADIR DATADIR-ORIG** command.

Step 10 Restore the configuration and database files from the backup by running the **upgrade** script.

```
# cd /home/upgrade/2_2/
# ./upgrade

Restoring backup of configuration and database files
   Checking that all processes are stopped on the system
   Checking that cserver is not running on the system
Please enter the hostname of this device : s66
   Collect s66.tgz from server with backup data

IP Address of machine containing configuration/database files?: 171.71.51.99
The authenticity of host '171.71.51.99 (171.71.51.99)' can't be established.
RSA key fingerprint is 09:0f:95:9e:0b:ff:ec:ce:1a:cb:3f:39:0d:ce:d4:36.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '171.71.51.99' (RSA) to the list of known hosts.
root@171.71.51.99's password:
s66.tgz
100% 1079KB   1.1MB/s   00:01
   Untarring s66.tgz
   Copying database files ...
Scripts executed successfully. Please follow these steps below :
1. Customize and Uncomment the service start commands in /etc/rc.local
2. Reboot the servers.
```

Step 11 Edit the rc.local file and uncomment all the command lines.

Step 12 Reboot the server.

```
reboot
```

Step 13 Using the CDSM, disable the server offload.

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

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

c. Choose **Disable** and click **Submit**.

When Server Offload is enabled on a server, the server is configured to reject new provisioning; that is, do not allow new ingests on a Vault and do not allow new streams on a Streamer and move existing streams to another Streamer gracefully.

Step 14 Using the CDSM GUI, verify that the server has come online.

a. Choose **Monitor > System Health**. The System Health Monitor page is displayed.

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

Recovering a Lost Administrator Password

If an administrator password is forgotten, lost, or misconfigured, you must reset the password on the server.

Note There is no way to recover a lost administrator password. You must reset the password to a new one.

To reset the password, do the following:

Step 1 Log into the server as *root*.

Step 2 Enter the following command:

```
/home/stats/resetpw
```

Step 3 Log in to the CDSM with the username *admin* and the password *admin*.

Step 4 Reset the admin password by following the steps detailed in the "Editing User Settings" section on page 7-3 in the *Cisco VDS-TV 3.5 ISA Software Configuration Guide* or the *Cisco VDS-TV 3.5 RTSP Software Configuration Guide*.

Disk Maintenance

The hard disk drives on the CDE110, CDE205 and CDE220 are hot-swappable. For the procedure outlining the steps for removing and replacing a hard disk drive, see Removing and Replacing a Hard Disk Drive in the *Cisco Content Delivery Engine 110 Hardware Installation Guide* and "Installing External Storage Drives" in the *Cisco Content Delivery Engine 205/220/250/420 Hardware Installation Guide*.