



CHAPTER 5

System Maintenance

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

- [Replacing a Server, page 5-2](#)
- [Removing a Server, page 5-7](#)
- [Adding a Server, page 5-10](#)
- [Backup and Recovery, page 5-15](#)
- [Recovering a Lost Administrator Password, page 5-23](#)
- [Disk Maintenance, page 5-24](#)



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 TV CDS 2.4 ISA Software Configuration Guide* or the *Cisco TV CDS 2.4 RTSP Software Configuration Guide*.



Caution

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



Caution

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

Replacing a Server

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

- [Replacing a CDSM or VVIM](#)
- [Replacing a CDS 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 TV CDS 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 2.4.1.”](#)

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. Stop the database on the primary CDSM and copy it to the new CDSM.
3. Run the `cdsconfig` script to configure the new CDSM and inform the other CDS servers of the new CDSM.
4. 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 the database.
- ```
db_shutdown
```
- Step 3** 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.
 

```
pgrep avsdB
```

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

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

- Step 4** You must stop the database before copying it to the new CDSM. Log in to the primary CDSM as *root* and 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.

```
pgrep avbdb
```

- 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 TV CDS software version as the server it is replacing. This includes running the `cdsinstall` script to install the software; not the `cdsconfig` script.

---

- Step 6** On 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 7** On primary CDSM, start the database again.

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

- Step 8** Change the ownership of DATADIR from *root:root* to *isa:isa*.

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

- Step 9** Run the `cdsconfig` script. 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 10** When the `cdsconfig` script finishes, edit the `rc.local` file and uncomment all the command lines. 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. Following is an example with all the lines uncommented:

```
vi /etc/rc.local

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

touch /var/lock/subsys/local

Lines below this one modified by cdsflavconfig (ISA):

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

```

sleep 30

/arroyo/www/bin/apachectl start

sleep 30

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

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

sleep 30

```

**Step 11** Reboot the CDSM.

```
reboot
```

**Step 12** Log in to the GUI of the new secondary CDSM as a user with Engineering access level. The CDSM Setup page is displayed.

**Step 13** Click **Submit** to submit the settings on the CDSM Setup page for the secondary CDSM.

---

## 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.
- 

**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”](#) section on page 5-16.

**Step 5** Shut down the existing CDSM.

```
poweroff
```

**Step 6** On the new CDSM, restore the configuration and database files using the backup that was made from the existing CDSM. For information this procedure, see the [“Performing a Restore on the CDSM”](#) section on page 5-17.



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

---

- Step 7** 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 `DATADIR` has already been copied from the primary CDSM.
- ```
cdsconfig
```
- Step 8** When the `cdsconfig` script completes, edit the `rc.local` file and uncomment all the command lines.
- Step 9** Reboot the new replacement CDSM.
- ```
reboot
```
- Step 10** 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.
- Choose **Maintain > User > Add Users**. The Add Users page is displayed.
  - In the **New User** and **Password** fields, enter the user name and password for this account.
  - From the **Access** drop-down list, choose **Engineering**.
  - 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 11** Verify that the settings on the CDSM Setup page are the same settings that you wrote down for the old CDSM. Click **Submit** to resubmit all the settings.
- Step 12** Choose **Monitor > System Health**, and verify connectivity to all the CDS servers by checking the status of each server. All status boxes should be green.
- 

## Replacing a CDS Server

To replace a Cisco ASR 9000 Series Aggregation Services Router ISM (Integrated Service Module) line card serving as a Vault, Streamer, ISV, or Caching Node, complete the procedures described in this section.

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

- Offload the server and shutdown the processes on the server.
- Back up the configuration to an available Linux server.
- Restore the backup on the new replacement server.
- Log in to the CDSM and complete the configuration.

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.
- Click **Maintain > Servers > Server Offload**. The Server Offload page is displayed.
  - From the **Server IP** drop-down list, choose the IP address or nickname of the server and click **Display**.
  - Choose **Enable** and click **Submit**.
- 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. Check the protocoltiming log.

```
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 by looking at the Active Streams line in the protocoltiming log.

**Step 4** Stop the database and statsd processes.

```
db_shutdown
pgrep statsd | xargs kill
```

**Step 5** 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 6** Back up the configuration and database files. See [“Performing a Backup on a CDS Server” section on page 5-19](#) for more information.

**Step 7** 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 8** Log in to the new server as user *root*.




---

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

---

**Step 9** Restore the configuration and database files that were backed up to the Linux server. See [“Performing a Restore on a CDS Server” section on page 5-21](#) for more information.

**Step 10** Run the cdsconfig script to rewrite the rc.local file for the CDS 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
```

```
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

Use detected platform: A9K-ISM-100? (yes/no) [y]: y

Writing new configuration to /home/isa/.arroyorc

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

Started avssdb, verify with "arroyo status"
Starting statsd
Run svrinit to seed database? (yes/no) [n]: n
Writing /etc/rc.local
cdsconfig finished, please use CDSM to complete configuration

```

- Step 11** Using the CDSM, disable the server offload.
- Click **Maintain > Servers > Server Offload**. The Server Offload page is displayed.
  - From the **Server IP** drop-down list, choose the IP address or nickname of the server and click **Display**.
  - Choose **Disable** and click **Submit**.
- Step 12** Using the CDSM GUI, verify the server is online.
- Click **Monitor > System Health**. The System Health Monitor page is displayed.
  - 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 CDS network using a new address or configuration.

This section documents the following procedures:

- [Removing a CDSM](#)
- [Removing a CDS 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 as *root*.
- Step 2** Stop the database.

```
db_shutdown
```

**Step 3** 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.

```
pgrep avsdb
```

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

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

**Step 4** On each CDS 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. Restart the database on each server.

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

**Step 5** 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 6** Stop the `statsd` process.

```
pgrep statsd | xargs kill
```

**Step 7** 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 8** Reboot the CDSM.

```
reboot
```

## Removing a CDS Server

To remove a Cisco ASR 9000 Series Aggregation Services Router ISM (Integrated Service Module) line card serving as a Vault, Streamer, ISV, or Caching Node, complete the procedures described in this section.

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 CDS 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**.

**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. Check the protocoltiming log.

```
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.

**Step 4** Stop the statsd process.

```
pgrep statsd | xargs kill
```

**Step 5** 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 CDS 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 CDS server at the time of using the **svrinit\_15** command.

**Step 6** 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 7** Stop the database process.

```
db_shutdown
```

**Step 8** Ensure the database is fully stopped. Check that the database thread count returns nothing.

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

**Step 9** On each CDS server in the system, 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. Restart the database on each server. The following commands are for servers in an RTSP environment. For ISA environments, only enter the **su - isa** command.

```
[root]# su - isa
[isa]# arroyo start avbdb
```

**Step 10** Shut down the CDS server.

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

**Step 11** Log in to the CDSM GUI and verify that the CDS server is not displayed in the System Health Monitor page.

If the removed CDS 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 CDS 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 CDS is different depending on the type of server being added. This section provides information on the following procedures:

- [Adding a Second CDSM](#)
- [Adding a CDS Server](#)

## Adding a Second CDSM



### Note

All CDS 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.

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 TV CDS software version as the server it is replacing. This includes running the `cdsinstall` script to install the software; not the `cdsconfig` script.

**Step 2** Stop the database on the existing CDSM.

```
[root]# db_shutdown
```

**Step 3** 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.

```
pgrep avbdb
```

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

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

- Step 4** 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 5** Change the ownership of DATADIR from *root:root* to *isa:isa*.

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

- Step 6** Run the **cdsconfig** script and 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.

- Step 7** When the **cdsconfig** script completes, edit the **rc.local** file and uncomment all the command lines. The **su - isa -c “cd /home/isa/RTScheduler/Exporter...”** command is only used when the MediaX feature needs to send notifications to a catalog server or similar type of server. Following is an example with all the lines uncommented:

```
vi /etc/rc.local
```

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

touch /var/lock/subsys/local

Lines below this one modified by cdsflavconfig (ISA):

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

sleep 30

/arroyo/www/bin/apachectl start

sleep 30

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

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

sleep 30
```

- Step 8** Reboot the CDSM.

```
reboot
```

- Step 9** On the existing CDSM, run the **cdsconfig** script to enable redundancy.

- Step 10** When the **cdsconfig** script completes, edit the **rc.local** file and uncomment all the command lines.

- Step 11** Reboot the existing CDSM.

The CDSM Redundancy feature is configured.

## Adding a CDS Server



### Note

All CDS servers and CDSMs that are part of the same system as the CDS 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 CDS, 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 TV CDS 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 CDS 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 CDS server, create the `rc.local` file, and edit the `.arroyorc` file on every CDS 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 CDS 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
```

```
Do you want to disable interface eth0? (yes/no) [n]: n
```

```
Enter an IP address for eth0: IP_Address
```

```
Enter a netmask for eth0: netmask
```

```
Enter a broadcast address for eth0: broadcast_address
```

```

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:
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
Use detected platform: A9K-ISM-100? (yes/no) [y]: y

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

```

**Step 4** The `cdsconfig` script asks for information about your CDS to get a server ID and group ID for the new CDS 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 CDS 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 CDS 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 Stributes for AVSRTSPServer
```

- Step 7** The cdsconfig script asks if the server is getting added to an existing deployment. Answer yes (Y) to synchronize 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 avfdb, 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 8** 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 CDS server when prompted. These are the same settings as you configured for the eth0 interface at the beginning of the cdsconfig script.




---

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

---

```
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 CDS 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 CDS server in an RTSP environment:

```
[root]# su - isa
[isa]# arroyo start avfdb
[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 CDS array before this configuration, clean out /home/isa/Berkeley by deleting \*.db \*.idx and all replication ip address files. Also, delete all /persist directories found in the directories under /home/isa/Streaming and /home/isa/ContentStore.

**Step 9** 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.

## Backup and Recovery

This section provides information on the following procedures:

- [Preparation for a Backup](#)
- [Performing a Backup on the CDSM](#)
- [Performing a Restore on the CDSM](#)
- [Performing a Backup on a CDS Server](#)
- [Performing a Restore on a CDS Server](#)



**Note** Any CDS 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 CDS 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 CDS, 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 CDS and stream demands are the lowest.

## Performing a Backup on the CDSM

Before you back up the CDSM, 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 5-15](#) for more information. Backing up the configuration and database files on the CDSM includes the following tasks:

1. Stop the database and shutdown the processes on the CDSM.
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.

To back up the CDSM, do the following:

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

**Step 2** Stop the database.

```
db_shutdown
```

**Step 3** 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.

```
pgrep avsdB
```

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

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

**Step 4** If the CDSM is redundant, shut down the statsd process and ensure that the process has stopped.

```
pgrep statsd | xargs kill
ps -aef | grep statsd
```

**Step 5** 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 6** 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.

```
./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 7** Ensure that the tar file was copied to the backup server in the /arroyo/backup directory.

**Step 8** Reboot the CDSM.

```
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” section on page 5-16](#). Restoring the configuration and database files on the CDSM includes the following tasks:

1. Stop the database and shutdown 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 the database.

```
db_shutdown
```

**Step 3** 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.

```
pgrep avsdB
```

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

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

**Step 4** 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 5** If the CDSM is redundant, shut down the statsd process and ensure that the process has stopped.

```
pgrep statsd | xargs kill
```

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

**Step 6** 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-ORIG** command.

To rename the database use the **mv DATADIR DATADIR-new-name** command. For example, the following command renames the database to *DATDIR-2.4*:

```
cd /arroyo/db
```

```
mv DATADIR DATADIR-2.4
```

**Step 7** 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 8** Check the `.arroyorc` file to make sure that the configuration settings are correct.

**Step 9** Reboot the CDSM

```
reboot
```

## Performing a Backup on a CDS Server

Before you back up the CDS 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 5-15](#) for more information. Backing up the configuration and database files includes the following tasks:

1. Offload the server and shutdown the processes on the server.
2. Comment out all the command lines in the `rc.local` file and reboot the CDS 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 CDS 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**.

**Step 2** Log in to the CDS 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. Check the protocoltiming log.

```
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.

- Step 4** Stop the database and statsd processes.

```
db_shutdown
pgrep statsd | xargs kill
```

- Step 5** 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 6** Edit the rc.local file so that it does not start any service; that is, comment out all command lines.

- Step 7** Reboot the server.

```
reboot
```

- Step 8** 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 9** Ensure that the tar file was copied to the backup server in the /arroyo/backup directory.

- Step 10** Edit the rc.local file and uncomment all the command lines.

- Step 11** Using the CDSM GUI, reboot the server.
- Click **Maintain > Servers > Server Restart**. The Server Restart page is displayed.
  - From the **Server IP** drop-down list, choose the IP address of the server and click **Display**.
  - From the **Restart** drop-down list, choose **Yes** and click **Submit**.
- Step 12** Using the CDSM GUI to verify that the server has come online.
- Choose **Monitor > System Health**. The System Health Monitor page is displayed.
  - The status boxes for the server should all be green.
- Step 13** Using the CDSM, disable the server offload.
- Click **Maintain > Servers > Server Offload**. The Server Offload page is displayed.
  - From the **Server IP** drop-down list, choose the IP address or nickname of the server and click **Display**.
  - Choose **Disable** and click **Submit**.

## Performing a Restore on a CDS Server

Before you can restore a backup, you need to create the backup. See [“Performing a Backup on a CDS Server” section on page 5-19](#). Restoring the configuration and database files includes the following tasks:

- Offload the server and shutdown the processes on the server.
- Comment out all the command lines in the rc.local file and reboot the CDS server.
- Delete or rename the database.
- Run the upgrade script to restore the configuration and database files.
- Edit the rc.local file and uncomment all the command lines.
- Reboot the CDS 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.
- Click **Maintain > Servers > Server Offload**. The Server Offload page is displayed.
  - From the **Server IP** drop-down list, choose the IP address of the server and click **Display**.
  - Choose **Enable** and click **Submit**.
- Step 2** Log in to the CDS server as *root*.
- Step 3** Ensure that the server is fully offloaded.
- Verify that the TRICKLE\_DOWN file exists in the /usr/tmp directory.
  - Check the protocoltiming log.

```
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.

**Step 4** Stop the database and statsd processes.

```
db_shutdown
pgrep statsd | xargs kill
```

**Step 5** 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 6** Edit the rc.local file so that it does not start any service; that is, comment out all command lines.

**Step 7** Reboot the server.

```
reboot
```

**Step 8** 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 9** 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
This installation appears to be a 1.5.1.X --> 2.x Upgrade. Database Conversion
is required to continue.
```

```
Upgrading database ...
Database is running.
```

```
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** Edit the rc.local file and uncomment all the command lines.
- Step 11** Using the CDSM GUI, reboot the server.
- Click **Maintain > Servers > Server Restart**. The Server Restart page is displayed.
  - From the **Server IP** drop-down list, choose the IP address of the server and click **Display**.
  - From the **Restart** drop-down list, choose **Yes** and click **Submit**.
- Step 12** Using the CDSM GUI to verify that the server has come online.
- Choose **Monitor > System Health**. The System Health Monitor page is displayed.
  - The status boxes for the server should all be green.
- Step 13** Using the CDSM, disable the server offload.
- Click **Maintain > Servers > Server Offload**. The Server Offload page is displayed.
  - From the **Server IP** drop-down list, choose the IP address or nickname of the server and click **Display**.
  - Choose **Disable** and click **Submit**.

## 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/runonce
```
- 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 TV CDS 2.4 ISA Software Configuration Guide* or the *Cisco TV CDS 2.4 RTSP Software Configuration Guide*.

Disk Maintenance

The hard disk drives on the CDE110 and CDE220 are hot-swappable. For the procedure outlining the steps for removing and replacing a hard disk drive, see *Cisco Content Delivery Engine 110 Hardware Installation Guide* and *Cisco Content Delivery Engine 205/220/420 Hardware Installation Guide*.