SR 8.0 Installation and Migration Guide

Please Read

Important

Read this entire guide. If this guide provides installation or operation instructions, give particular attention to all safety statements included in this guide.

Notices

Trademark Acknowledgments

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: **www.cisco.com/go/trademarks**.

Third party trademarks mentioned are the property of their respective owners.

The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Publication Disclaimer

Cisco Systems, Inc. assumes no responsibility for errors or omissions that may appear in this publication. We reserve the right to change this publication at any time without notice. This document is not to be construed as conferring by implication, estoppel, or otherwise any license or right under any copyright or patent, whether or not the use of any information in this document employs an invention claimed in any existing or later issued patent.

Copyright

Contents

About This Guide

Purpose

This guide provides step-by-step instructions for the following SR 8.0 installation scenarios.

- Initial installation of System Release (SR) 8.0
- Migration of SR 7.x to SR 8.0
- Upgrade to a newer version of SR 8.0

SR 8.0 Features Forklift Upgrade

The upgrade to SR 8.0 involves the migration from Sun Solaris 10 to CentOS Linux. The SR 8.0 upgrade allows engineers to upgrade the system without having to shut the system down until the activation of the new system software.

Cisco engineers have expended great effort to make sure that the upgrade causes minimal system impact. However, there are times during the upgrade where Digital Home Communication Terminals (DHCTs) will not be able to boot and where some functions (Broadcast File System [BFS], billing system control of set-top-boxes [STBs], and so on) are interrupted. These outages will likely go unnoticed by most of your subscribers.

How Long to Complete the Upgrade?

The upgrade to SR 8.0 is to be completed within a maintenance window that usually begins at midnight. Upgrade engineers have determined that a typical site can be upgraded within one 6-hour maintenance window. The maintenance window should begin when you stop system components in ***Migrate Key Files and Database to SR 8.0*** (on page 53).

System Performance Impact

Interactive services are not available and billing transactions will be suspended during the maintenance window.

Audience

This guide is written for field service engineers and system operators who are responsible for creating virtual machines (VMs) and installing or upgrading to SR 8.0.

Read the Entire Guide

Please review this entire guide before beginning the installation. If you are uncomfortable with any of the procedures, contact Cisco Services for assistance.

Important: Complete all of the procedures in this guide in the order in which they are presented. Failure to follow all of the instructions may lead to undesirable results.

Required Skills and Expertise

System operators or engineers who upgrade the Explorer Controller (EC) software need the following skills:

- Advanced knowledge of Linux
  - Experience with the Linux vi editor. Several times throughout the system upgrade process, system files are edited using the Linux vi editor. The Linux vi editor is not intuitive. The instructions provided in this guide are no substitute for an advanced working knowledge of vi.
  - The ability to review and edit cron files
- Knowledge of VMware
- Extensive EC and DBDS system expertise
  - The ability to identify keyfiles that are unique to the site being upgraded
  - The ability to add and remove user accounts

Document Version

This is the first formal release of this document.

Revision History

Date	Revision	Section
20170914	Removed bullet that required SR 8.0 VM hostname to match SR 7.x hostname.	***Install SR 8.0*** (on page 41)
20171130	Added details if deploy-ec script fails during installation.	***Install SR 8.0*** (on page 41)
	Added two new sections in Chapter 7, SR 8.0 Post Upgrade Procedures.	***Configure FTP Users and Start the vsftpd Service*** (on page 82)
		Configuring snmpd Traps on the EC Node (on page 83)
20171228	Added VMware 6.5 to C240 M4 test reference configuration table.	***Hardware Requirements*** (on page 2)
20180228	Add Appendix I to provide the procedures to configure multiple network interfaces. This is required for systems using a multi-home environment on a CentOS platform.	***Configuring Multiple Interfaces in CentOS*** (on page 211)
	Added a step to enable the consul service prior to checking the certificate created on the EC.	***Transferring EC Certificates Created From the Admin Node to the EC*** (on page 46)
	Added SFTP Support section.	***Setting Up SFTP Support*** (on page 74)
20180321	Added section in Chapter 7 to update GQAM code if enabling Multicast CVT support.	***Multicast CVT Support Feature (Optional)*** (on page 110)

1

Planning the Install or Migration

Introduction

This chapter contains information that helps you and Cisco engineers plan the installation or migration to minimize system downtime.

In This Chapter

Site Requirements

Your site requires the following requirements. Ensure that these requirements are met prior to deploying virtual machines.

Hardware Requirements

The following hardware prerequisites are required to deploy virtual machines (VMs) in an SR 8.0 environment.

- Cisco UCS hardware (C240 M3 or C240 M4) with the latest ESXi software installed.

  Important: If you are using a new UCS C240 server, refer to ***Appendix A, Hardware Configuration Procedures for the Cisco UCS C240 Server*** to configure the server. This must be completed prior to deploying the OVA. See ***UCS Hardware and Software Compatibility*** (***https://ucshcltool.cloudapps.cisco.com/public/***) for details.

- Supported EC Server Platform:

Platform	Hard Drives	Memory
Cisco UCS C240 M3	16 X 300 GB	128 GB minimum
Cisco UCS C240 M4	16 X 300 GB	128 GB minimum

  Notes:

  - The procedures in this guide deal primarily with the setup and configuration of the UCS C240 M3 server.
  - To ensure the reliable operation of the UCS and the Explorer Controller, the UCS should be connected to a UPS-protected power source and should be shut down gracefully if there is a risk that the server will lose power. Details on the power requirements for the UCS can be found in the hardware installations guides provided with the servers.

- Cisco UCS hardware should have adequate CPU, Memory, a local disk datastore and a sufficient network for EC Virtual Machines (VMs):

CPUs	Memory (GB)	Hard Disks (GB)	Network Interfaces	Number of Nodes for HA
8	64	1 x 64 (root) 1 x 384 (disk1)	1 x Public 1 x Headend 1 x TED 1 x RepDB	2

- C240 M3 Tested reference configuration:

Configuration	Specification
Server Series	C Series Standalone Server
UCS Release	1.5(3)
Server Model	C240-M3 (SFF)
OS Vendor	VMware
OS	VMware vSphere ESXi 5.5 or later
Component	RAID Adapter
Adapter	LSI 9271-8i /LSI 9271CV- 8i MegaRaid SAS HBA
Adapter Driver	**VMware 5.5**: 6.602.54.00.1vmw

- C240 M4 Tested reference configuration:

Configuration	Specification
Server Series	C Series Standalone Server
UCS Release	2.0(13i)
Server Model	C240-M4 (SFF)
OS Vendor	VMware
OS	VMware vSphere ESXi 5.5 or later
Component	RAID Adapter
Adapter	Cisco 12G SAS Modular Raid Controller
Adapter Driver	■ **VMware 6.5:** 6.611.07.00-1OEM.600.0.0.2768847 ■ **VMware 6.0**: 6.605.08.00-6vmw.600.0.0.2494585 ■ **VMware 5.5 U2**: 6.606.06.00.1vmw

Note: This is the **minimum** tested reference configuration. Refer to the UCS Hardware and Software Compatibility Web page to ensure that your components satisfy these requirements. (http://www.cisco.com/web/techdoc/ucs/interoperability/matrix/matrix.html)

- **EC 8.0 Mapping**:
  - NET0 – vSwitch0 – Corp/Engineering Network

    Important: By default, DHCP is enabled on the eth0 NET0-vSwitch0-Corp network. If DHCP is not available, then a static IP address, netmask and gateway, as well as DNS information is required.
  - NET1 – vSwitch1 – Headend (HE) Network
  - NET2 – vSwitch2 – TED Network
  - NET3 - vSwitch3 - RepDB

    Note: RepDB is configured after the installation/migration to SR 8.0.

Software Requirements

The following software prerequisites are required for an SR 8.0 installation.

- VMware vSphere (5.5 or later) and vCenter infrastructure (software, license, and a running vCenter machine).
  - vSphere Web UI 5.5 is used for examples throughout this guide.
- A vCenter Web UI login or a vSphere ESXi client to connect and perform management tasks.
  - vCenter login must have admin privileges to deploy VMs.
- Admin Node installed (refer to the ***Admin Node Installation Guide***.
- Linux Platform Template saved via vCenter Server (created from a procedure in the ***Admin Node Installation Guide***).
- Admin Node access to copy the following files to your VM:
  - cisco-vcs-deployment-[VERSION].zip
  - ec-system-release-[VERSION].tar
  - cisco-vcs-infra-[VERSION].tar
  - SSL Certificates created for each unique SR 8.0 EC node
  - CSCOlxplat-[VERSION].ova

    Note: The CSCOlxplat OVA is only needed if you are using vSphere ESXi client to deploy VMs rather than the vSphere Web UI.
- Migration and Upgrade Only:
  - You are currently running SR 7.x.
  - EC Backup and Restore scripts available from Cisco.
  - EC Pre-Upgrade Checks TAR file (e.g. ecpuc_8.0.1.tar) available from your customer-specific forum on Cisco's File Exchange Server.

- At least one external Network Time Protocol (NTP) server, version 4.x or later, configured and accessible on the network.
- You have a complete list of all third-party tools and scripts currently in use on the EC.
- You have a complete list of key files and directories where you store site-specific information that you want to keep, such as:
  - EMM files
  - Log files
  - Scripts
  - Service logo files or MSO logo files

  Note: No files on the active EC are deleted as part of this upgrade.
- DTACS 5.0 and DTACS 4.1 are supported.

  Note: If you have a DTACS 4.1 system, refer to Appendix G, ***Procedures Specific to EC 8.0 With a DTACS 4.1 Server*** (on page 199) for instructions to configure SSH keys for the EC 8.0 and DTACS 4.1 servers.

Web Browser Requirements

The Web UIs have been tested and verified against Mozilla Firefox version 50 and ESR version 52.1 browsers. Due to unpredictable results with other browsers, we highly recommend that you only use Mozilla Firefox on your system when you work with the EC.

Java must be enabled in the browser to be able to view the Performance Monitoring graph.

Turn Off Automatic Updates for Mozilla Firefox ESR Only

1. Open the Firefox browser.
2. Click the **Navigation** icon,  , and select **Options**.
3. From the left area, click **Advanced** and then click the **Update** tab.
4. In the Firefox Updates section, click either the **Check for updates but let me choose whether to install them** or the **Never check for updates** option.
5. Click **OK**.

X.509 CA Certificate and Associated Private Key Requirements

Important: During the installation and configuration of the Admin Node, you should have created a root CA, as well as all certificate/key pairs for each node in your NextX system. If you have not created these certificates, refer to Chapters 5 through 6 in the ***Admin Node Installation Guide*** to create them now.

Each EC node in your NextX system requires a NextX X.509 certificate along with an associated private key. The X509 certificates must be signed by a Certification Authority (CA). The CA can be either an external entity or an internal CA.

The NextX X.509 certificates were created when you deployed and configured the Admin Node. In this guide, you will distribute the appropriate certificates from the Admin Node to their respective EC node.

Additional IP Address and NAS Interface Requirements

In addition to inheriting all of the IP address of the existing EC, the SR 8.0 EC will require the following additional IP addresses.

- Temporary IP address (for access to the Admin Node).
- IP address for the Network Attached Storage (NAS) Interface (if a dedicated interface will be used).

  Notes:

  - The UCS/EC does not support backing up to tape. Backups of the key files and the database are performed to the NAS.
  - VM cloning is also an option to save a full file system backup; however, you must have vCenter Server to do so.

About the EC Pre-Upgrade Checks Scripts

The purpose of the EC pre-upgrade checks (EC PUC) scripts is to perform pre-upgrade checks related to the EC that you are migrating or upgrading to SR 8.0 to ensure that it is seamless and successful.

The EC PUC scripts are packaged in the ecpuc_[VERSION].tar file. The tar file must be downloaded from your customer-specific forum on Cisco's File Exchange Server and then saved to a shared (NFS) storage device accessible by the EC.

The EC PUC validates your system for migration eligibility. These scripts should be run two or more weeks prior to your migration/upgrade to allow enough time to resolve any major issues or incompatibilities that may affect your ability to upgrade the EC. The EC PUC should be run again just before your migration/upgrade to validate the system.

Important: The EC PUC scripts must be run on each EC that will be migrated or upgraded.

Important Points About the Upgrade

Performance Impact

Interactive services will not be available and billing transactions will be suspended while you are within the maintenance window, after EC processes are stopped.

Estimated Timeline

Estimated Time to Complete the Upgrade

The upgrade to SR 8.0 features the forklift upgrade, which provides the ability to stage the Cisco UCS server with the upgraded operating system and application software before entering the maintenance window.

Most sites should be able to complete an upgrade within a typical 6-hour maintenance window. However, depending on the size of your system, it could take longer. Key factors are the size of your database and the number of headend elements.

Post-upgrade procedures involve resetting the modulators. Cisco recommends that you never reset more than eight modulators at a time. Refer to the following table for estimated times for resetting the modulators.

Number of Modulators	Minutes (approx. 4 minutes per modulator, 8 at a time)
60	30 to 38
100	50 to 63
150	75 to 94
200	100 to 125
250	125 to 157

Non-Cisco Application Server and/or Third Party Application Servers

If the site you are upgrading supports a non-Cisco application server, contact the vendor of that application server to obtain upgrade requirements, and upgrade and rollback procedures.

If the site you are upgrading runs a third-party software application, contact the supplier of that application to obtain any upgrade requirements.

Important: Make sure that all third-party vendors are aware that the SR 8.0 upgrade is built upon the CentOS 6.8 (x86) software platform.

Plan What Optional Features Will be Supported

Optional Features in SR 8.0

An upgrade can contain additional optional features that you can enable on your system. Some of these features require that you obtain a special license for the feature to be activated; others can simply be activated by Cisco engineers without a special license.

Determine which optional features (licensed or unlicensed) need to be enabled as a result of this upgrade. You can activate these optional features later during the upgrade, while the system processes are down.

If any licensed features are to be enabled as a result of this upgrade, contact Cisco Services to purchase the required license.

Important:

- Any features that have been previously enabled or licensed as part of an earlier upgrade do not have to be re-enabled.
- If the upgraded system that is to support the SRM CAS PowerKEY feature, Cisco Services needs to enable the feature. Contact Cisco Services.
- If this is a new install to SR 8.0 and features need to be enabled, contact Cisco Services.

2

System Release Pre-Upgrade Checks

Important: If this is a new SR 8.0 installation, skip this chapter and go to ***Deploy the EC Virtual Machine*** (on page 23).

This chapter describes the procedures that must be completed prior to migrating or upgrading to SR 8.0.

In This Chapter

Preparing to Run the Pre-Upgrade Checks Script

To upgrade your system to SR 8.0, you will need to execute commands and scripts using both the **root** and **dncs** roles on the EC. For this reason, we recommend opening two xterm windows: one that accesses the EC server as **root** user and one that accesses the EC server as **dncs** user.

Important: Once this procedure is complete, we will refer to executing commands from either the root or the EC terminal window on the EC.

Complete the following steps to open the terminal windows.

Note: These commands are executed on the SR 7.x system.

1. From a terminal window, log into the active EC with your administrative user account.
2. Complete the following steps to change to the **root** role.
   a. Type `sux - root` and press **Enter**.
   b. Enter the **root** password and press **Enter**.
3. Copy the EC pre-upgrade tar file from your local PC to the **/var/tmp** directory on the active EC.

   Command Syntax:

   ```
   scp ecpuc_[VERSION].tar dncsftp@[EC_IP]:/var/tmp
   ```

   Example:

   ```
   # scp ecpuc_8.0.1.tar dncsftp@10.90.47.184:/var/tmp
   ```
4. Open a *second* another terminal window and log into the EC with your Administrator account.
5. Enter the following command to change to the **dncs** role.

   ```
   $ sux - dncs
   ```

   Note: You should now have two terminal windows open. One where you are root and one where you are dncs.
6. Go to the next section in this chapter.

Checking the .profile Exit Status

In this procedure, you will check the exit status when sourcing the dncs user .profile settings. The exit status must be 0 (zero). If the status is not 0 upon exit, there is a problem in the .profile file that will prevent the EC processes from starting after the upgrade.

1 As **dncs** user, type the following command and press **Enter** to source the dncs role .profile settings.

```
$ . ./.profile
```

2 Type the following command and press **Enter** to verify that the exit status from Step 1 is **0** (zero).

```
$ echo $?
```

Result: The system displays the exit status of the command executed in Step 1.

3 Is the exit status **0**?

- If **yes**, go to the next procedure in this chapter.
- If **no**, continue with the next step.

4 Open the dncs user **.profile** file in a text editor and review the file for problems. Check especially for the following condition:

If the last statement (bottom) in the .profile is an "unset" statement, verify that it unsets a variable that was set earlier in the .profile file. If it does not, remark or delete this entry, and repeat Steps 1-3.

Note: If the solution proposed in Step 4 still does not produce an exit status of 0 in the dncs user .profile file, contact Cisco Services for assistance

Checking the EAS Configuration

Before installing the new EC system release software, verify that your EAS equipment is working correctly by testing the system's ability to transmit EAS messages.

- If migrating from SR 7.x, complete all of the procedures in Chapter 5, **Testing the EAS**, of *Configuring and Troubleshooting the Digital Emergency Alert System* (part number 78-4004455-01).
- If upgrading from SR 8.0, refer to the EC Online Help file.

Note: You will check the EAS configuration after the installation of the new software, as well.

Checking dncs_bfsRemote in the dncsSetup File (DSG Systems Only)

Important: This procedure should only be run on systems that use the DOCSIS set-top gateway (DSG) for BFS.

In this section, you will review the dncsSetup file for the dncs_bfsRemote variable setting. This information will be used during post-upgrade procedures if DSG BFS is configured on your system.

1 As the **dncs** role, type the appropriate command and press **Enter**. The output shows the dncs_bfsRemote variable setting in the dncsSetup file.

```
$ grep 'dncs_bfsRemote=' /dvs/dncs/bin/dncsSetup
```

Example Output:

dncs_bfsRemote=dncsatm

2 Does the output show the variable set to **dncsdsg**?

- If **yes**, you must execute the **Modify the dncsSetup File for DSG** procedure in your appropriate system upgrade guide after the migration is complete.

  Note: Do not go to that procedure now. You will get there as a matter of course while following the procedures in your upgrade guide.

- If **no**, you will skip the ***Modify the .profile File for DSG*** (on page 69) procedure in the post-upgrade chapter.

Checking for the IPG_TVDATA_NEW Variable in appservSetup

Note: This procedure is executed on the EC.

Complete the following steps to check for the IPG_TVDATA_NEW variable in the appservSetup file.

1 As **dncs** role, type the following command and press **Enter** to check for the "IPG_TVDATA_NEW" variable:

```
$ grep "IPG_TVDATA_NEW" /dvs/appserv/bin/appservSetup
```

2 Is the variable present?

- If **yes**, record the variable setting. You will need to put this variable back into the appservSetup file after the migration.
- If **no**, continue with the next procedure.

Checking the Number of BFS Sessions

The number of BFS sessions post-upgrade needs to equal the number of pre-upgrade sessions. Use this procedure to determine and record the number of pre-upgrade BFS sessions. Then, after the upgrade, you will determine the number of post-upgrade BFS sessions.

Follow this procedure to check and record the number of pre-upgrade BFS sessions.

1 Press the **Options** button on the front panel of the BFS QAM until the **Session Count** total appears.

Record the **Session Count** total in the space provided. _____

2 As **dncs** role, enter the following command and press **Enter**.

Command Syntax:

```
auditQam -query <QAM IP> <port #>
```

Example:

```
$ auditQam -query 192.0.2.65 16
```

3 Complete the following steps to check the number of BFS sessions directly from the GQAM device.

a Type the following command and press **Enter**.

Command Syntax:

```
telnet [GQAM IP address]
```

Example:

```
$ telnet 192.0.2.65
```

b When prompted, enter the user name and password for the GQAM.

c Press the **Ctrl** and **]** keys simultaneously to go to the telnet prompt.

d Type the following command and press **Enter** twice.

```
telnet> mode ch
```

e Type the following commands and press **Enter** after each to display the GQAM sessions on the specified port.

Example:

```
D9479 GQAM> session
```

```
D9479 GQAM>session

       OUTPUT       ACTIVE       ENCRYPTED      SDV
        PORT       SESSIONS      SESSIONS     SESSIONS

          0          33            0            0
          1           3            3            0
          2           3            3            0
          3           9            9            0
          4           8            8            0
          5          39           39            0
          6           7            7            0
          7           7            7            0
          8           9            9            0
          9          14           13            0
         10           9            9            0
         11           6            6            0
         12           2            2            0
         13           0            0            0
         14           2            2            0
         15           2            2            0
                   --------     --------     --------

       Totals:      153          119            0
```

Command Syntax:

```
print_session_status <port #>
```

Example:

```
D9479 GQAM> print_session_status 0
```

Note: In this example, the BFS sessions are built on GQAM channel 1. The GQAM numbers ports 0 through 15; the EC numbers them 1 through 16.

Result: The system displays the BFS session built upon the specified IP address and port.

4 Do the number of sessions shown in Steps 1 through 3 match the number of sessions built on the BFS QAM?

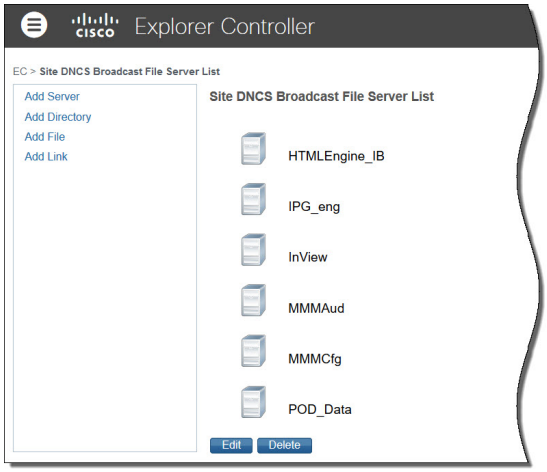
- If **yes**, go to the next procedure in this chapter.
- If **no**, contact Cisco Services for assistance.

Recording Third Party BFS Application Cabinet Data

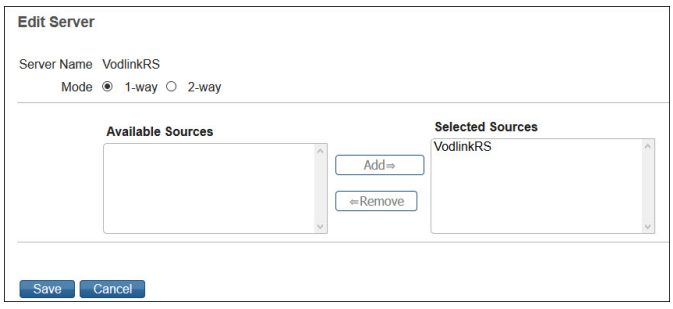
In this procedure, you will record third-party BFS application cabinet data so that you have a record of it in the event that the data is not preserved during the upgrade. Following the upgrade, during post-upgrade activities, you will confirm that this data has been preserved.

Note: You do not need to record this data for all BFS application cabinets, only those that are NOT created by default.

1 From the EC Web UI, click the **Navigation** icon, , and then select **App Interface Modules > BFS Client**. The Site DNCS Broadcast File Server List window opens.



2 Select a third-party application cabinet and select **Edit**. The Edit Server window opens for the selected cabinet.



3 On a sheet of paper, record the **Server Name**, the **Mode** (whether 1-way or 2-way), and the **Selected Source(s)** used to regulate the cabinet.

Note: In this example, the **Server Name** is **VodlinkRS**, the **Mode** is **1-way**, and the **Selected Source** is **VodlinkRS**.

Important: Do not lose this sheet of paper. You will need it when completing post-upgrade instructions.

4. Click **Cancel** to close the Edit Server window.
5. Record all folders, files, and link information in the cabinet, as needed.
6. Repeat Steps 2 through 5 for each third-party BFS application cabinet in the Site DNCS Broadcast File Server List.
7. Close the Site DNCS Broadcast File Server List window when you are finished.

Running the EC PUC

This section describes how to run a system check on the EC to determine if your system is acceptable for an upgrade. If it is, you can continue with the upgrade; if it is not, you must correct any errors that are found and then rerun this procedure

Complete the following steps to execute the ecpuc script on the EC you are upgrading.

Note: The EC PUC tar file should already be downloaded the Admin Node. If it is not yet on the Admin Node, refer to the ***Admin Node Installation Guide*** to download it now.

1 As **root** user, go to the **/var/tmp** directory.

```
# cd /var/tmp
```

2 Enter the following command to extract the EC PUC tar file.

Command Syntax:

```
tar -xvf /var/tmp/ecpuc_[VERSION].tar
```

Example:

```
# tar -xvf /var/tmp/ecpuc_8.0.1.tar
```

Result: The EC PUC scripts and a README file are extracted to a new directory named ECPUC in the /var/tmp directory.

```
# ls -ltr /var/tmp/ECPUC
total 115
-rwxr-xr-x   1 root     dncs       15217 Mar 28 10:05 nondncsatmvasps.sh
-rwxr-xr-x   1 root     dncs       19044 Mar 28 10:05 ecpuc
-rwxr-xr-x   1 root     dncs        1446 Mar 28 10:05 dncsDbCheckBoss
-rwxr-xr-x   1 root     dncs        9017 Mar 28 10:05 del_nummap_dupes
-rwxr-xr-x   1 root     dncs        5998 Mar 28 10:05 checkstrandedseg.sh
-rw-r--r--   1 root     dncs        1051 Mar 28 10:05 README
```

3 Enter the following command to execute the **ecpuc** script. You are prompted to continue.

```
# /var/tmp/ECPUC/ecpuc
```

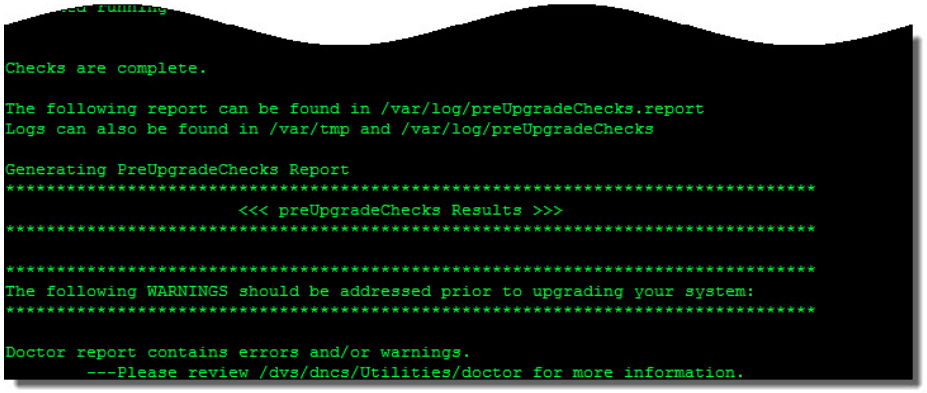
```
*************************** EC preUpgradeChecks ******************************

This program will perform some basic checks to ensure your system is prepared
for an upgrade. User input may be required. Depending on your system, these
checks may take more than 30 minutes to run.

*************************** EC preUpgradeChecks ******************************
Do wish to continue? (y/n):
```

4 Type **y** and press **Enter**. The PUC begins the system checks and includes the following checks:

- Clears all database sessions.
- Runs the doctor report.

5 Did any errors or warnings appear?

Example Output:



- If **yes**, correct the issues and repeat this procedure.
- If **no**, go to the next step.

6 Review the EC PUC log in **/var/log/preUpgradeChecks** directory for any errors or warnings.

Command Syntax:

```
less /var/log/preUpgradeChecks/puclog_[date]_[time]
```

Example:

```
# less /var/log/preUpgradeChecks/puclog_20170704_103158
```

7 Review the doctor output in the **/dvs/dncs/Utilities/doctor** directory for any errors or warnings.

Command Syntax:

```
less /dvs/dncs/Utilities/doctor/report_[most recent].doc
```

Example:

```
# less /dvs/dncs/Utilities/doctor/report_16695.170725_1115.doc
```

8 Review all WARNINGS and ERRORS in the PUC and doctor output prior to upgrading your system.

3

Deploy the EC Virtual Machine

Introduction

Important: If this is a new UCS C240 server, refer to Appendix A, Hardware Configuration Procedures for the Cisco UCS C240 Server to install and configure the server. The procedures in the appendix only need performed once. When you have completed the installation and configuration of the server, return to this chapter.

This chapter provides the procedure to deploy an EC VM from a Linux platform template. This template was created when the Admin Node was built. You will need the password for the admin user that was configured for this template.

Note: If you did not deploy and configure the Admin Node or the Linux platform template, ask your site administrator for the Admin Node IP address, the location and the password for the Linux platform template.

In This Chapter

Deploying the VM From the Linux Platform Template

Important:

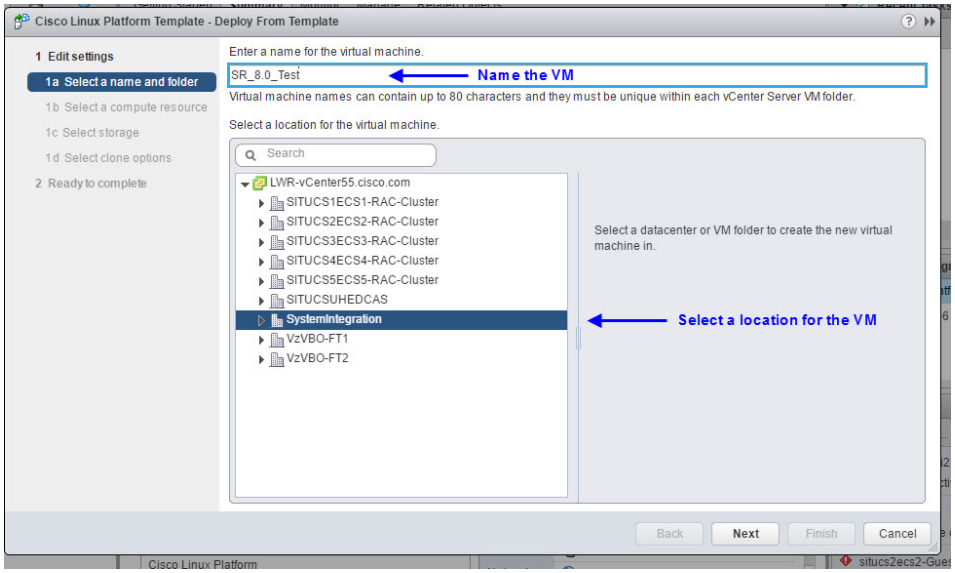
- Execute this procedure for either a new install or a migration.
- If this is a migration, deploy the OVF template on the *secondary* EC.
- If you are deploying the VM from a vSphere ESXi client, go to ***Procedures When Using an ESXi Client*** (on page 205).

Follow these steps to deploy the OVA using vSphere Web UI.

1 From vCenter Web UI, click **VMs and Templates**.

2 Locate and select the CSCOlxplat template that was created from the procedures in the ***Admin Node Installation Guide***.

3 Right-click the template and select **Deploy VM from this Template**. The Deploy From Template window opens.

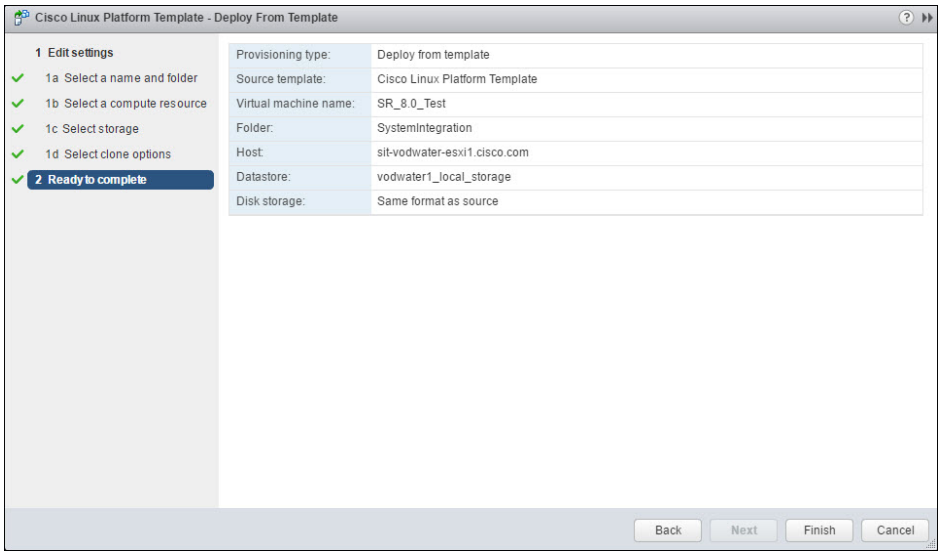


4 In the text box, enter a name for the VM you are creating and then select the datacenter or VM folder where it will be deployed. Click **Next.**

5 Select the compute resource (e.g. cluster, host) where the VM will run and click **Next**.

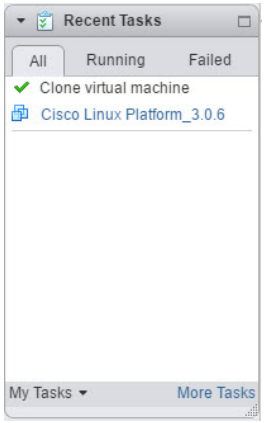
6 From the **Select virtual disk format** dropdown menu, maintain the **Same format as source** default. Then ensure that the appropriate datastore is selected.

7 Click **Next** and then click **Next** again.



8 Review the settings and click **Finish**.

9 Monitor the **Recent Tasks** area to ensure that the VM is created successfully.



Reconfiguring the Virtual Hardware Settings on the VM

Important: Execute this procedure for either a new install or a migration.

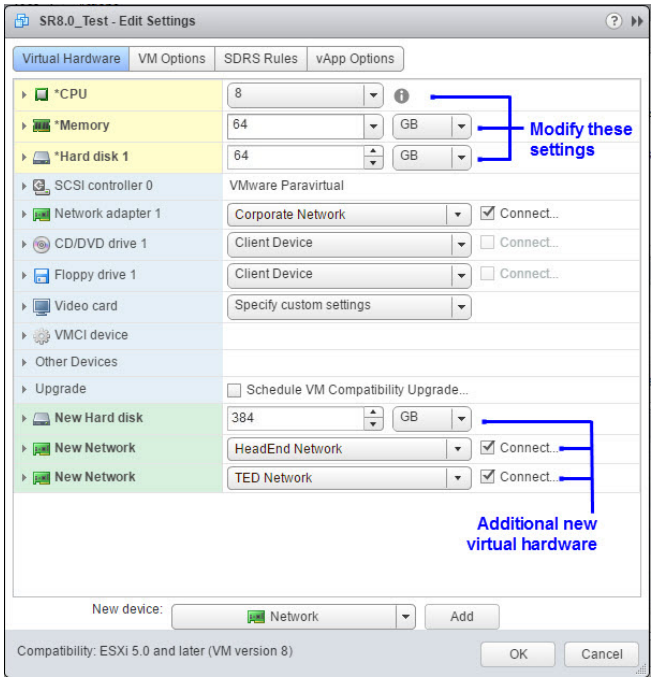
Complete the following steps to modify the virtual hardware configuration on the VM.

1. Click the **Home** icon, , and then click **Hosts and Clusters**.
2. Locate and select the VM you just cloned from the Linux platform template.
3. Right-click the VM and select **Edit Settings**. The Edit Settings window appears.
4. From the **CPU** dropdown menu, select **8**.
5. From the **Memory** entry, modify the memory to **64 GB**.

   Important: Make sure that you change MB to **GB**.
6. From the **Hard disk 1** entry, modify the disk size to **64 GB**.
7. From the **New device** dropdown menu at the bottom of the window, select **New Hard Disk**.
8. Click **Add**. The New Hard Disk entry is added to the list of virtual hardware.
9. Modify the disk size to **384 GB**.
10. From the **New device** dropdown menu, select **Network** and then click **Add**. A New Network entry is added to the bottom of the Virtual Hardware list.
11. From the dropdown menu, select the network label for the headend (i.e. HeadEnd Network).
12. Repeat Steps 10 through 11 and select the network label for the TED Network.

    Important: ***Do not set up a fourth interface at this time*** as there is a known issue in VMware that causes errors between network interfaces during the initial bootup.

Example: Edit Settings window



13 Click **OK**. The Edit Settings window closes and the VM is reconfigured.

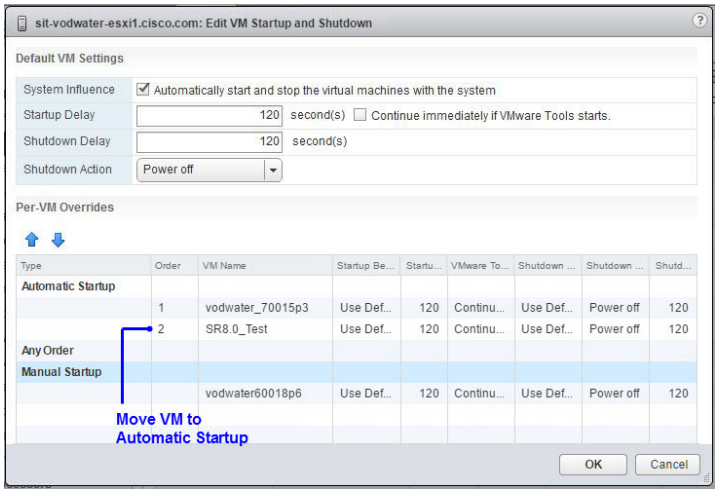
14 Monitor the **Recent Tasks** area to ensure the VM is successfully reconfigured.

Setting the Power Policy

Important: Execute this procedure for either a new install or a migration.

Complete the following steps to set the power policy for the new VM.

1. Select the ESXi host where the VM was created.
2. Click the **Manage** tab.
3. Click the **Settings** tab and from the Virtual Machines dropdown menu, click **VM Startup/Shutdown**.
4. Click **Edit**.
5. Ensure that the **Automatically start and stop the virtual machines with the system** check box is selected.
6. From the **Per-VM Overrides** table, select the VM you just created. The up arrow, , becomes active.
7. Click the up arrow until the VM is moved to the **Automatic Startup** area.



8. Click **OK**. The Edit VM Startup and Shutdown window closes and you are returned to the **Manage** window for the ESXi host.

Configuring DNS

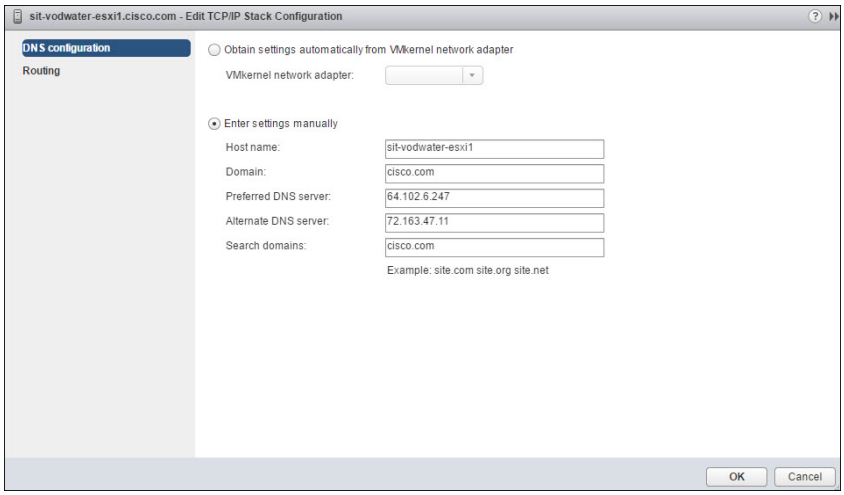
Complete the following procedure to configure DNS for your system.

Note: The Manage window for your ESXi host should still be displayed in your vSphere Web UI.

1 Click the **Networking** tab and then click **TCP/IP configuration**.

2 Click the **pencil** icon, , and then click **DNS configuration**.

3 Click the **Enter settings manually** radio button and then enter the IP address for the **Preferred DNS server** and the **Alternate DNS server**.



4 Click **Routing** from the left area, and if necessary, enter the default gateway in the **VMkernel gateway** text box.

5 Click **OK**.

4

Preparing the System for the Installation or Migration

This chapter contains procedures to prepare the system for the installation or migration to SR 8.0.

Important: Follow the procedures carefully as some procedures will not always pertain to both a new installation and a migration.

In This Chapter

Shutdown the Secondary SR 7.x EC

Important: Complete this procedure if you are performing a migration to SR 8.0. If this is an initial installation or you are creating a secondary VM for Replicated Database, go to ***Power On the New SR 8.0 VM*** (on page 33).

Complete the following procedure on the *secondary* SR 7.x EC.

1 Backup the key files and database on the active SR 7.x EC to your NAS drive using one of the following methods.

Note: Refer to the ***Explorer Controller Backup and Restore User Guide*** (part number OL-27573) for instructions.

- The SR 7.x ISO image
- Backup and Restore scripts available from Cisco
- Cloning the VM

2 Is RepDB enabled on your system?

- If **yes,** refer to Disabling Data Replication to disable it. Then go to the next step.
- If **no**, go to the next step.

3 Select and right-click the *secondary* EC and select **All vCenter Actions > Power > Power Off**. The secondary EC is shut down.

Power on the New SR 8.0 VM

Complete the following steps to power on and log into the new VM.

1 Select and right-click the SR 8.0 VM and select **Power On**.

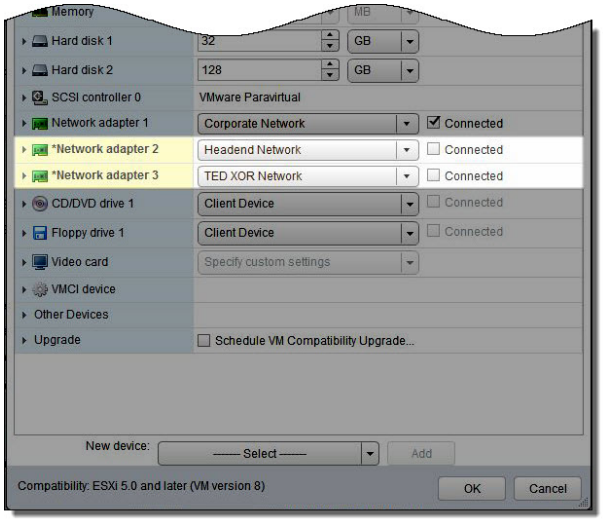
2 Is this a new installation of SR 8.0?

- If **no** and this is a migration, go to the next step.
- If **yes**, go to Step 6.

3 Select and right-click the SR 8.0 VM again and select **Edit Settings**.

4 Unselect the **Connected** box for both the **Network adapter 2** (Headend Network) and the **Network adapter 3** (TED XOR Network) devices.

Important: If you have created a Network adapter 4 interface, ***make sure to delete this interface*** as there is a known issue in VMware when you boot the VM. This issue results in the fourth interface overwriting the MAC address for eth0.



Note: Do ***not*** unselect the **Connect At Power On** box.

5 Click **OK**. Monitor the **Recent Tasks** area until the VM is successfully reconfigured.

6 Right-click the VM and select **Open Console**.

Note: If you are using DHCP, you can use an SSH client to login to the VM.

7 Log into the VM as **admin** user.

Important: You can only log in as admin user on the Cisco Linux platform. Direct root access is not permitted; however, the admin user has full root privileges via the sudo command.

User Name: admin

Password: [password defined for the Linux Platform template]

Important: If you are performing an EC migration, you will use this password to create an admin user in the ***Create an Admin User on the SR 7.x EC*** (on page 52).

8 Do you plan to configure a static IP configuration?

- If **yes**, go to ***Set Up the Network With a Static IP Configuration (Optional)*** (on page 35).
- If **no**, go to ***SR 8.0 Application Installation*** (on page 39).

Set Up the Network With a Static IP Configuration (Optional)

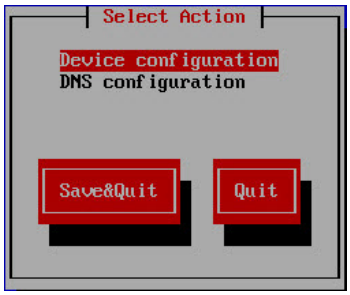
Important: This procedure is only required if you choose to set up your network with a static IP configuration. If you choose to use a DHCP configuration, you can skip this procedure and go to ***SR 8.0 Application Installation*** (on page 39).

By default, eth0 (Corporate Network) will boot up as DHCP. If you wish to change to a static IP, you must manually update ifcfg-eth0, DNS and add static routes.

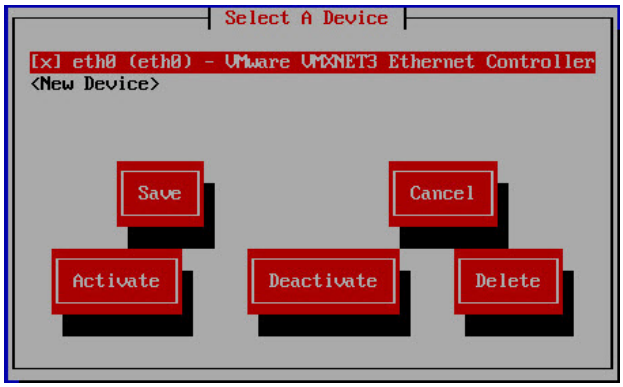
Complete the following procedure to configure a static IP network for the Cisco Linux platform.

1 From the console window, enter the following command to configure the network and DNS settings. The Select Device window displays.

```
[admin@platform ~]$ sudo system-config-network
```



2 Maintain the **Device configuration** selection and press **Enter**. The Select a Device window appears.



3 Maintain the default setting to configure eth0 and press **Enter**.

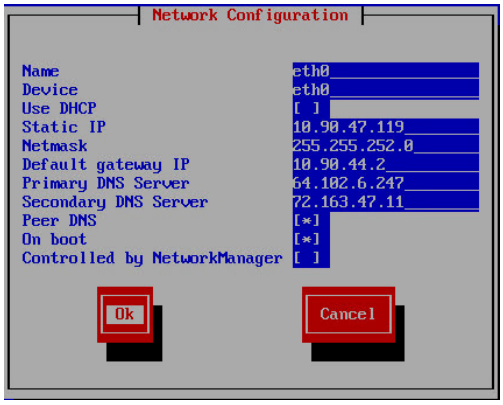
4 Press the **Tab** key until the cursor is in the **Use DHCP** field. Then press the **Spacebar** to unselect this option.

5 Tab to each of the following fields to enter the appropriate values for your system.

- **Static IP**
- **Netmask**
- **Default gateway IP**
- **Primary DNS Server**
- **Secondary DNS Server**

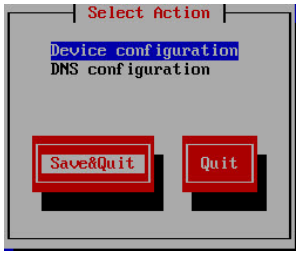
6 Verify that **Peer DNS** is selected.

7 Press the **Tab** key until the cursor is in the **Controlled by NetworkManager** field. Then press the **Spacebar** to unselect this option.



8 Press **Tab** to highlight **Ok** and press **Enter**. The Select A Device window appears.

9 Press **Tab** to highlight **Save** and press **Enter**. The Select Action window appears.



10 Click **Save&Quit**.

11 Enter the following command to edit the **ifcfg-eth0** configuration file.

```
[admin@platform ~]$ sudo vi
/etc/sysconfig/network-scripts/ifcfg-eth0
```

12 Go to the **IPV6INIT** field and change the value from yes to **no**.

13 Go to the **HWADDR** field and delete the entire line.

14 Save and close the file.

15 Restart the network service to update the interface configuration.

```
[admin@platform ~]$ sudo service network restart
```

16 Close the console window.

17 Using an SSH client, log into the VM using the IP address you configured for eth0.

18 Is the EC on the same network as the Admin Node?

- If **yes**, then go to the ***SR 8.0 Application Installation*** (on page 39).
- If **no**, add a route to the EC.

  Note: Only add routes that are required to access the Admin Node and/or the local machine where the Cisco VCS Deployment scripts were downloaded. Please note that any static routes added to /etc/sysconfig/network-scripts/route-eth0 will be overwritten during the deployment of packages.

  Example:

```
[admin@platform ~]$ sudo route add -net 10.90.44.0/24
gw 10.90.47.1 dev eth0
```

19 Can you can ping the Admin Node from the EC.

- If **yes**, go to the next section.
- If **no**, troubleshoot your network or contact your system administrator.

5

SR 8.0 Application Installation

Important: Execute these procedures for either a new install or a migration.

This chapter provides step-by-step instructions for copying the SR 8.0 application (zip file) to your VM and for installing the application.

In This Chapter

Copy the VCS Deployment Zip File to the VM

The cisco-vcs-deployment zip file resides on the Admin Node for your site. In this procedure, you will copy this file to your VM.

Important: You will need the IP address of the Admin Node for this procedure.

1 Enter the following command to change to **root** user.

```
[admin@platform ~]$ sudo -i
[root@platform ~]#
```

Important: At this point, the only user that can log into the system is the **admin** user. When you see the instruction, "As root user", you will need to execute "sudo -i" from the admin user account to become root user.

2 Secure copy (SCP protocol) the **cisco-vcs-deployment** zip file from the Admin Node to the **/var/tmp** directory on the new VM.

Command Syntax: Assumes the zip file is in the /opt/cisco/software/admin_node directory on the Admin Node.

```
scp admin@[Admin_Node_IP]:/opt/cisco/software/admin_node/
cisco-vcs-deployment-1.0.X.zip /var/tmp
```

Example:

```
[root@platform scripts]# admin@10.90.47.106://opt/cisco/software/admin_node/cisco-vcs-d
eployment-1.0.6.zip /var/tmp
The authenticity of host '10.90.47.106 (10.90.47.106)' can't be established.
RSA key fingerprint is 2f:33:59:4f:c4:e8:89:0d:fd:99:aa:57:21:08:8c:ae.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.90.47.106' (RSA) to the list of known hosts.
admin@10.90.47.106's password:
cisco-vcs-deployment-1.0.6.zip                100%   29KB  29.4KB/s   00:00
```

3 On the new VM, change to the **/var/tmp** directory.

```
[root@platform ~]# cd /var/tmp
```

4 Unzip the file using the following command.

```
[root@platform tmp]# unzip cisco-vcs-deployment*.zip
```

5 Enter the following command to change to the **cisco-vcs-deployment-1.0.x/scripts** directory.

```
[root@platform tmp]# cd cisco-vcs-deployment*/scripts
```

6 Verify that the following EC-specific files are present.

- **deploy-ec.sh**
- **ec.envfile**

```
[root@platform scripts]# ls | grep ec
```

7 Stay in this directory and go to the next section.

Install SR 8.0

Important: You will need the IP address of the Admin Node for this procedure.

1 Enter the following command to open the **ec.envfile** file in a text editor.

```
[root@platform scripts]# vi ec.envfile
```

2 Enter values specific to your system.

Important:

- Values are required for each line.
- Go to the end of the file and add a "hostname=" entry and then append the hostname you want to define for the EC.

  Note: If this is a migration from SR 7.x to SR 8.0 and you want to change the hostname to a new hostname, append the new name to the "hostname=" entry. Ensure that you execute the steps in ***Update the site_info Database Table for a Hostname Change*** (on page 70) procedure, post upgrade, or dncsInit.d will not start.

Default ec.envfile

```
admin_node=
cisco_appserver=false
default_gateway=
ec_headend_interface=
ec_headend_ip=
ec_headend_netmask=
lab_setup=false
route_eth0_file=
ted_interface=
```

Example ec.envfile

```
admin_node=10.90.44.70
cisco_appserver=true
default_gateway=204.3.1.206
ec_headend_interface=eth1
ec_headend_ip=204.3.1.193
ec_headend_netmask=255.255.255.240
lab_setup=false
route_eth0_file=/var/tmp/route-eth0
ted_interface=eth2
hostname=vodwater
```

3 Save and close the file.

4 Enter the following command to create the **route-eth0** file in the /var/tmp directory.

Note: If this is a migration, reference the /etc/rc2.d/S85SASpecial and the /etc/rc2.d/S82atminit files on the SR 7.x system to obtain the appropriate routes.

```
[root@platform scripts]# vi /var/tmp/route-eth0
```

Example

```
10.90.0.0/16 via 10.90.44.2 dev eth0
64.100.0.0/16 via 10.90.44.2 dev eth0
64.102.0.0/16 via 10.90.44.2 dev eth0
10.116.0.0/16 via 10.90.44.2 dev eth0
10.84.0.0/16 via 10.90.44.2 dev eth0
10.82.0.0/16 via 10.90.44.2 dev eth0
10.78.192.0/21 via 10.90.44.2 dev eth0
10.143.32.0/23 via 10.90.44.2 dev eth0
172.18.0.0/23 via 10.90.44.2 dev eth0
```

5 Save and close the **route-eth0** file.

6 Execute the following command to deploy the EC application. This will take several minutes.

```
[root@platform scripts]# ./deploy-ec.sh --envfile=ec.envfile
2>&1 | tee /var/log/deploy-ec.out
```

Result: An "ec installation completed" message will display with no errors. The VM will then reboot.

Important: If the deploy-ec.sh script fails, troubleshoot the issue. Once the issue is resolved/recognized, delete this VM and return to ***Deploy the EC Virtual Machine*** (on page 23) to build a new VM.

Example:

```
The system is going down for reboot NOW!
ec installation completed
```

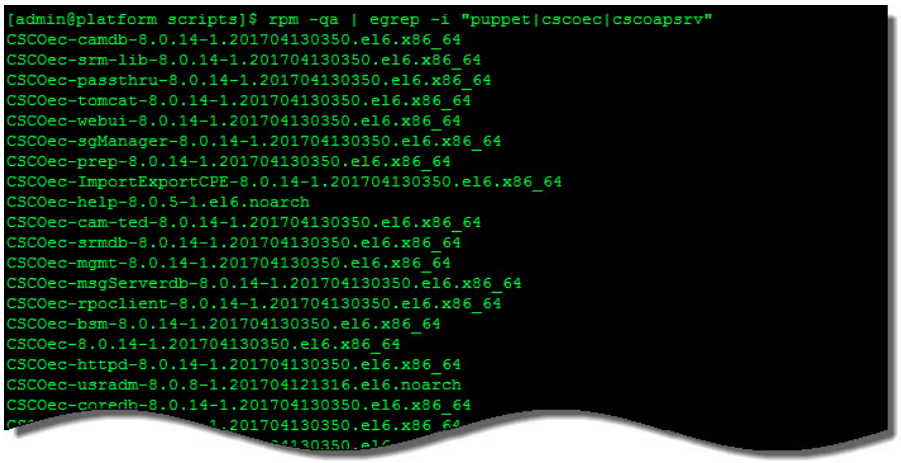
7 From the terminal window, log back into the VM as **admin** user.

8 Verify that the network interfaces are up by entering the following command.

```
[root@vodwater ~]# ifconfig -a
```

9 Enter the following command to verify that the RPM packages are installed.

```
[root@vodwater ~]# rpm -qa | egrep -i
"puppet|cscoec|cscoapsrv"
```



Result: A list of the installed packages are displayed.

10 Do any patches to the installation exist?

- If **yes**, go to ***EC SR 8.0 Patch Installs*** (on page 185). Once the patch is installed, go to the next section in this chapter.
- If **no**, go to the next section.

Transfer HTTPS X.509 Certificates to the EC

Important: The NextX X.509 certificates should have been created for each EC node when you deployed the Admin Node. If they have not yet been created, go to the following chapters in the ***Admin Node Installation Guide*** to create them now.

- Chapter 5: Create Environment Files for NextX Nodes
- Chapter 6: Create NextX X.509 Root CA Certificates

This section includes the procedures to transfer the HTTPS X.509 certificates from the Admin Node to the EC node in your system.

Creating the config.json File on the EC

Complete the following steps to create the config.json file on the EC.

1 As **admin** user on the EC, enter the following command to change to the /etc/consul directory.

```
[admin@vodwater scripts]$ cd /etc/consul
```

2 Enter the following command to copy the client.json.template file to the **config.json** file.

```
[admin@vodwater consul]$ sudo cp client.json.template
config.json
```

3 Enter the following commands to change the permission of the config.json file to **444** and the ownership to **consul:consul**.

```
[admin@vodwater consul]$ sudo chmod 444 config.json
[admin@vodwater consul]$ sudo chown consul:consul config.json
```

4 Enter the following command to verify the permissions and ownership of the config.json file.

```
[admin@vodwater consul]$ ls -ltr | grep config
```

5 **Example Output**:

```
-r--r--r--. 1 consul consul 337 Nov 27 16:55 config.json
```

6 Open the **/etc/consul/config.json** file in a text editor.

```
[admin@vodwater consul]$ sudo vi config.json
```

7 In the "**bind_addr**" line, replace <client_ip> with the IP address of the EC node.

Example:

```
"bind_address": "10.90.181.101",
```

8 Do you plan on building an Explorer Controller Suite (ECS) 3.0 system?

- If **no**, save and close the config.json file and go to ***Transferring EC Certificates Created From the Admin Node to the EC*** (on page 46).

- If **yes**, do not close this file and go to the next step.

  Note: You may need to refer to the **Deploying the Consul VM** section of the *Explorer Controller Suite 3.0 Installation and Upgrade Guide* for assistance.

9 Has a consul encrypt key been generated for your NextX system?

- If **no**, go to the next step.
- If **yes**, retrieve the encrypt key and go to Step 7.

10 From another terminal window, log into the Admin Node and enter the following command to generate the consul encryption key. A key is generated and displayed in the output.

```
[admin@adminnode ~]$ sudo consul keygen
```

Example:

```
nSv70A9cEX28KLfmUgRLHA==
```

Note: Store the key in a safe location as you will need it for all nodes in your NextX system.

11 In the terminal window for the EC, and where the config.json file is open, go to the **"encrypt"** line and replace <output from <`consul keygen`> with the encryption key.

12 In each of **server_ip** entries, substitute the appropriate IP address for the Consul nodes in your NextX system.

- "<server_ip1>" IP Address of Consul 1
- "<server_ip2>" IP Address of Consul 2
- "<server_ip3>" IP Address of Consul 3

Example:

```
{
    "server": false,
    "bind_addr": "10.90.181.106",
    "datacenter": "dc1",
    "data_dir": "/opt/consul/data",
    "encrypt": "nSv70A9cEX28KLfmUgRLHA==",
    "log_level": "INFO",
    "enable_syslog": true,
    "disable_update_check": true,
    "retry_join": [
    "10.90.181.36"
    "10.90.181.37",
    "10.90.181.38"
    ]
```

13 Save and close the **config.json** file.

Transferring EC Certificates Created From the Admin Node to the EC

Important: This procedure must be executed for certificates that were generated from an internal root CA or from an external CA.

Complete the following steps to transfer the appropriate certificate files to the EC node.

Note: You should have two terminal windows open from the previous procedure. One for the EC where you are logged in as root user and one for the Admin Node where you are logged in as admin user.

1 On the Admin Node, enter the following command to go to the **/opt/cisco/ca** directory.

```
[admin@adminnode ~]$ cd /opt/cisco/ca
```

2 Enter the following command and press **Enter** to transfer the appropriate certificate and key pair to the EC.

Command Syntax:

```
sudo ./manageCerts -P [absolute_path_to_cert]
[absolute_path_to_key] [EC_IP]
```

Example:

```
[admin@adminnode ca]$ sudo ./manageCerts -P
/etc/pki/CA/certs/vodwater.domain.pem
/etc/pki/CA/private/vodwater.domain.key 10.90.47.184
```

Notes:

- Replace [cert] with the location of the node certificate file (e.g. /etc/pki/CA/certs/[EC.pem]) on the Admin Node.
- Replace [key] with the location of the node private key file (e.g. /etc/pki/CA/private/[EC.key]) on the Admin Node.
- Replace [IP] with the IP address of the EC, which is the IP address defined as IP.1 in the [hostname].env file for that EC.

3 Were you prompted to verify the SSH RSA key fingerprint?

- If **yes**, type **yes** and press **Enter**. Then go to the next step.
- If **no**, go to the next step.

4 When prompted, enter and then re-enter the EC admin password.

5 When prompted, enter the keystore password and press **Enter**. Make note of this keystore password.

6 When prompted again, re-enter the keystore password and press **Enter**.

7 When prompted, enter the trust store password and press **Enter**. Make note of this trust store password.

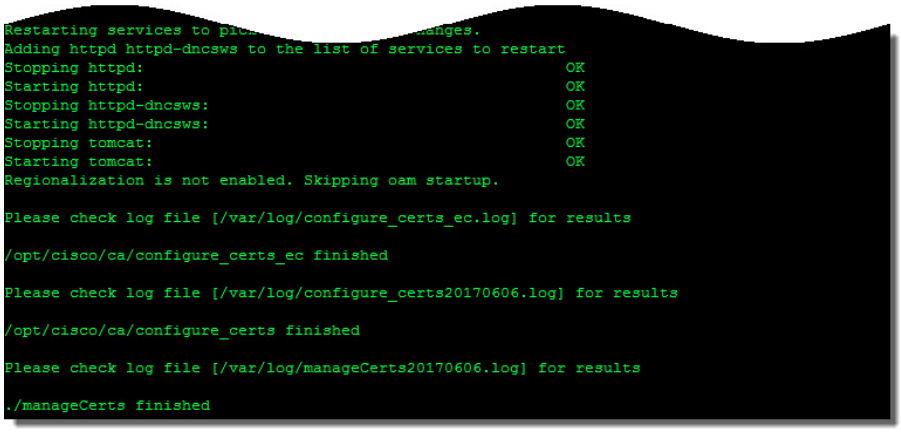
Note: Alternatively press **Enter** to use the keystore passphrase from the previous step.

8 When prompted again, re-enter the trust store password and press **Enter**.

Results:

- The keystore and truststore are generated from the signed SSL certificates on the EC node.
- The SSL certificate is deployed for the HTTPS service.
- Apache and tomcat services are restarted.
- A **./manageCerts finished** message displays.

Example:



9 Go to the next section to verify that the X.509 certificate was successfully configured.

Verifying the EC Certificate Configuration

Complete the following procedure to verify the configuration of the EC certificate.

Note: Once all NextX nodes on your system are configured for certificates, refer to the **Verify Inter-Node Encrypted Communication** procedure in Appendix B of the ***Admin Node Installation Guide***. This procedure allows you to execute encrypted communication checks for all nodes, including the ECs.

1 As **admin** user in the Admin Node terminal window, enter the following command to check the certificate configuration for the EC. A validation of the certificate files occurs.

Command Syntax:

```
sudo ./checkConfig -s [hostname].env
```

Example:

```
[admin@adminnode ca]$ sudo ./checkConfig -s vodwater.env
```

```
==========20170522.214030==========
./checkConfig
Checking all nodes

===Checking node at IP 10.90.47.89 from vodwater.env
mkdir: created directory `check'
mkdir: created directory `check/10.90.47.89'
Validating files in check/10.90.47.89
Checking ec or dtacs at 10.90.47.89
Checking consul config ./etc/consul/config.json
Checking CA cert ./etc/pki/tls/cacert.pem
Checking server client key ./etc/pki/tls/certs/bossclient.key
Checking CA cert ./etc/pki/tls/certs/cacert.pem
Checking CA chain ./etc/pki/tls/certs/cachain.crt
Checking Keystore ./etc/pki/tls/certs/genericKeystore.jks
Found aliases  Alias name: vodwater
Checking Truststore ./etc/pki/tls/certs/genericTruststore.jks
Found aliases  Alias name: caserver
Checking server client key ./etc/pki/tls/certs/ldsclient.key
Checking server client key ./etc/pki/tls/certs/rpoclient.key
Checking server cert ./etc/pki/tls/certs/server.crt
Checking server key ./etc/pki/tls/certs/server.key
Checking server key ./etc/pki/tls/private/server.key
Checking Keystore ./etc/pki/tls/vodwaterKeystore.jks
Found aliases  Alias name: vodwater
Checking Truststore ./etc/pki/tls/vodwaterTruststore.jks
Found aliases  Alias name: caserver
Checking security properties ./opt/cisco/vcs/security.properties
openssl verify -CAfile /opt/cisco/ca/check/10.90.47.89/etc/pki/tls/cacert.pem /opt/cisco/ca/check
/10.90.47.89/etc/pki/tls/certs/server.crt
/opt/cisco/ca/check/10.90.47.89/etc/pki/tls/certs/server.crt: OK

Please check log file [/var/log/checkConfig20170522.log] for results
```

2 Did any errors display?

- If **no**, go to Step 3.
- If **yes**, review the **/var/log/checkConfig[date].log** file to remedy the issue. Then repeat Step 1. When the issues are corrected, go to Step 3.

  Important: Ignore any errors related to the consul and/or the oammgrctrl services. If you are regionalizing your system, the consul service will be started and enabled later in this procedure. The oammgrctrl service is enabled later by default.

3 Do you plan to regionalize the EC to an existing ECS?

- If **yes**, go to the next step.
- If **no**, go to step 18.

4 Is the EC currently regionalized?

- If **yes**, go to the next step.
- If **no**, refer to **Appendix B** in the ***ECS 3.0 Installation and Upgrade Guide*** to regionalize it to the ECS. Then go to the next step.

5 From a terminal window for the EC, enter the following command to view the status of the **consul** service.

```
[admin@vodwater consul]$ service consul status
```

6 Is the **consul** service running?

- If **yes**, go to the next step.
- If **no**, enter the following command to start the service. Then go to the next step.

```
[admin@vodwater ~]$ sudo service consul start
```

7 Enter the following command to enable the **consul** service.

```
[admin@vodwater ~]$ sudo chkconfig consul on
```

8 Enter the following command to verify that the **consul** service is enabled.

```
[admin@vodwater ~]$ sudo chkconfig | grep consul
```

9 Enter the following command to SSH to the *primary* Consul node as **admin** user.

10 Enter the following commands to stop and restart the **consul** service.

```
[admin@consul ~]$ sudo service consul stop
[admin@consul ~]$ sudo service consul start
```

11 Verify that the consul service started successfully.

```
[admin@consul ~]$ sudo service consul status
```

12 Enter the following command to verify that the consul service is running.

```
[admin@consul ~]$ sudo consul monitor
```

Result: Output similar to the following should display.

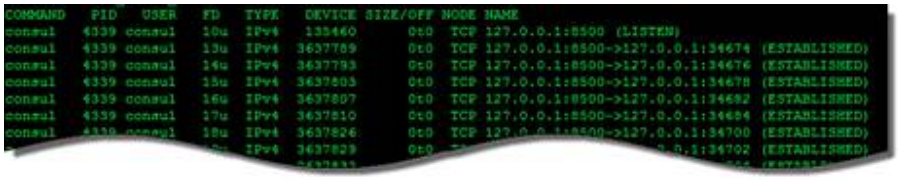
```
2017/04/11 13:15:42 [INFO] agent.rpc: Accepted client:
127.0.0.1:50448
```

Note: Press **Ctrl-C** to exit from the consul monitor.

13 Enter the following command to view a list of open processes/files on port 8500.

```
[admin@consul ~]$ sudo lsof -Pni :8500
```

Example Output:



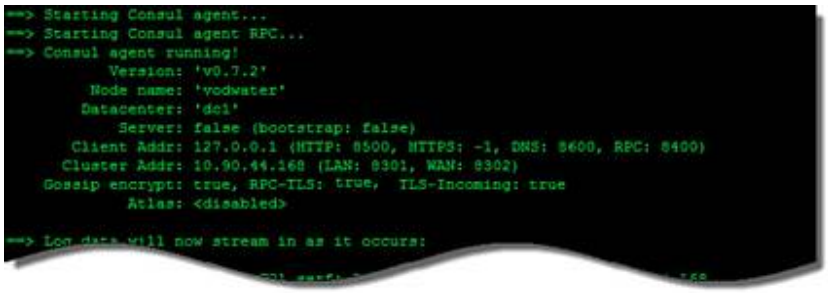
14 Enter the following command to verify that the EC is now in the current list of members that the Consul knows about.

```
[admin@consul ~]$ sudo consul members
```

Example Output:

15 Review the **/var/log/consul/consul.log** file to verify that consul encryption has been successfully enabled.

Example Output:



16 Verify that the following values are all set to **true**.

Note: These three values appear on the same line

- Gossip encrypt
- RPC-TLS
- TLS-Incoming

17 Type **exit** to close the SSH session to the Consul node and return to the EC session.

18 Is this a new installation?

Note: If you just configured a *secondary* host for your system, go to ***Configure and Operate the Replicated Database*** (on page 111).

- If **yes**, go to ***SR 8.0 Post-Upgrade Procedures*** (on page 59).
- If **no** and this is a migration, go to the next chapter, ***Migrate SR 7.x to SR 8.0***.

6

Migrate SR 7.x to SR 8.0

Important: If you are executing a new SR 8.0 installation, skip this section and go to ***SR 8.0 Post-Upgrade Procedures*** on page 59).

This section provides the procedure to migrate an SR 7.x EC running on a Solaris_x86-10 platform to SR 8.0 on a Cisco Linux platform.

In This Chapter

Create an Admin User on the SR 7.x EC

To successfully migrate to SR 8.0, you must create an admin user on the SR 7.x EC. The admin user is used to assist in the migration activities.

Important: This section provides the steps to be completed on the existing SR 7.x system.

1. From a terminal window, log into the SR 7.x EC.
2. As **root** user, execute the following command to create a migration user called **admin**.

   ```
   useradd -c "Cisco Linux Platform Migration User" -s /bin/bash
   -d /export/home/admin -m admin
   ```

3. Enter the following command to set the password for the **admin** user.

   ```
   passwd -r files admin
   ```

4. When prompted for the new password, enter the same password defined for the admin user on the newly deployed SR 8.0 EC.

   Important: The password for the admin user on the SR 7.x and SR 8.0 EC systems must match.

5. When prompted, re-enter the password. A successful message appears.
6. Complete the following steps to allow sudo root access for the admin user.
   a. Enter the following command to edit the **/usr/local/etc/sudoers_config** file.

      ```
      /usr/local/sbin/visudo
      ```

   b. Open a line under the **# User privilege specification** entry in the file and type the following entry.

      ```
      admin ALL=(ALL) NOPASSWD: ALL
      ```

   c. Save and close the file.
7. Complete these steps to verify that the admin user as sudo root access.
   a. In a new terminal window, log into the SR 7.x EC as **admin** user.
   b. When prompted, enter the admin password.
   c. Enter **sudo –i** and press **Enter**. If the command line changes to a root prompt (#), then the admin user has sudo root access.

      Note: If errors appear, verify the entries that you added in the sudoers command performed in Step 6.

Migrate Key Files and Database to SR 8.0

This section provides the procedure to migrate an existing Solaris_x86 SR 7.x EC to the new EC SR 8.0 Linux platform.

Important: If the SR 7.x EC is registered to Explorer Controller Suite (ECS) 2.0, you must first unregionalize and delete the registration. Refer to Appendix B in the ***Explorer Controller Suite 3.0 Installation and Upgrade Guide*** (part number TP-00133) for details.

Descriptions and Options for the Migrate Scripts

Each migration script includes a description and a list of options that may be used along with the script command. Complete the following steps to view the descriptions for each migration script.

1 Enter the following command to view the description of the **migrateKeyFiles** script.

```
[admin@vodwater ~]$ sudo
/opt/cisco/backup_restore/migrateKeyFiles -h
```

```
NAME
     migrateKeyFiles - migrate remote key files

DESCRIPTION
     This script will rsync key files from remote host specified

     Usage: migrateKeyFiles [-vh] [-I keyfiles_include ] [ -E keyfiles_exclude ] [ -S keyf
iles_staging ] [ -F force copy ] -l username -r remote_host

OPTIONS
     The following options are supported:
     -I     Specify the file that lists all the files that need to
            be included in the backup.

     -E     Specify the file that lists all the files that need to
            be excluded from the backup.

     -S     Specify the file that lists all the files that need to
            be moved to the staging dir for reference on remote_host.

     -F     Force copy on SunOS to Linux migration.

     -l     Remote login user.

     -r     Remote host/ip.

     -h     Display this help message then exit.

     -v     Operate verbosely.
```

2 Enter the following command to view the description of the **migrateUsers** script.

```
[admin@vodwater ~]$ sudo
/opt/cisco/backup_restore/migrateUsers -h
```

```
usage: migrateUsers [-h] --source [SRC_HOST]

Migrate Unix and WUI users from Unix host to this Linux host

optional arguments:
  -h, --help           show this help message and exit
  --source [SRC_HOST]  IP address of machine to be migrated
```

3 Enter the following command to view the description of the **migrateDBKF** script.

```
[admin@vodwater ~]$ sudo /opt/cisco/backup_restore/migrateDBKF
-h
```

```
usage: migrateDBKF [-h] --source [SRC_HOST] --db [SYS_TYPE]
                   [-I [INCLUDE_FILE]] [-E [EXCLUDE_FILE]] [-S [EXCLUDE_FILE]]

optional arguments:
  -h, --help            show this help message and exit
  --source [SRC_HOST]   IP address of machine to be migrated
  --db [SYS_TYPE]       [dncs or dtacs] Migrate DTACS or EC and AppSrv database
                        to this machine
  -I [INCLUDE_FILE]     Include file to be used for migrateKeyFiles
  -E [EXCLUDE_FILE]     Exclude file to be used for migrateKeyFiles
  -S [EXCLUDE_FILE]     Staging file to be used for migrateKeyFiles
```

Migrating Key Files

In this section, you will migrate the key files from SR 7.x to SR 8.0. The migration script for the key files will put the key files migration RSA key (kfm_rsa) in place and execute an initial migration of the key files. The specified files or directories will be mapped into a new directory, /disk1/keyfiles_staging, on the SR 8.0 EC.

Complete the following procedure to migrate the key files.

Note: These procedures will be executed on the SR 8.0 EC.

1 As **admin** user, change to the **/opt/cisco/backup_restore** directory.

```
[admin@vodwater ~]$ cd /opt/cisco/backup_restore
```

2 Execute one of the following migrateKeyFiles script as shown below.

Note: Substitute the IP address for the SR 7.x EC for the [SR 7.x IP] entry in the command.

Migrate Default Key Files Command

```
sudo migrateKeyFiles -v -l admin –r [SR 7.x IP]
```

Migrate Default Key Files Example

```
[admin@vodwater backup_restore]$ sudo ./migrateKeyFiles -v -l
admin –r 10.90.46.120
```

Migrate Default and Specific Key Files Command

```
sudo migrateKeyFiles -v -I <PATH/keyfiles_include> -E
<PATH/keyfiles_exclude> -l admin -r [SR 7.x IP]
```

Migrate Default and Specific Key Files Example

```
[admin@vodwater backup_restore]$ sudo ./migrateKeyFiles -v -I
tmp/keyfiles_include -E /tmp/keyfiles_exclude -l admin -r
10.90.46.120
```

3 When prompted, enter **yes** to continue and then press **Enter**.

4 When prompted, enter the admin password and press **Enter**.

5 Re-enter the admin password and press **Enter**. The key files are migrated to the SR 8.0 EC in the /disk1/keyfiles_staging directory. The keyfile migration starts.

6 When the script completes, review the output in the **/var/log/migrateKeyFilesLog**.

7 Enter the following command to go to the **/disk1/keyfiles_staging/etc/apache2/user-conf** directory.

```
[admin@vodwater backup_restore]$ cd
/disk1/keyfiles_staging/etc/apache2/user-conf
```

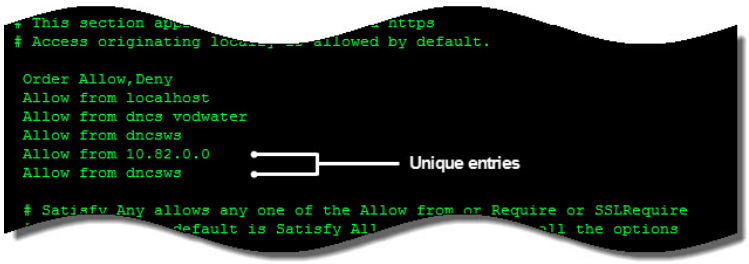
8 Open the **SAIdncs.bossreq.auth.conf** file and navigate to the **Order Allow,Deny** line.

```
[admin@vodwater user-conf]$ sudo less
SAIdncs.bossreq.auth.conf
```

9 Do any unique entries exist?

- If **yes**, go to the next step.
- If **no**, close the file and go to *Migrating Users* (on page 56).

Example with unique entries:



10 Copy any unique entries to a text file.

11 Go to the **/etc/httpd/user-conf** directory.

```
[admin@vodwater user-conf]$ sudo cd /etc/httpd/user-conf
```

12 Open the **CSCOec.loadPIMS.auth.conf** file in a text editor and go to the **Order Allow,Deny** line.

```
[admin@vodwater user-conf]$ sudo vi CSCOec.loadPIMS.auth.conf
```

13 Open a line after the last entry in the **Order Allow,Deny** list.

14 Paste the unique entries into the **CSCOec.loadPIMS.auth.conf** file.

15 Save and close the file.

Migrating Users

In this section, you will migrate the users and their user directories from SR 7.x to SR 8.0. This migration script, migrateUsers, uses the kfm_rsa key created when you executed the migrateKeyFiles script in the previous section.

This script also moves the digest file into place and removes any users who were not selected for migration. The digest is staged in /disk1/keyfiles_staging.

Complete the following procedure to migrate users.

Note: From the previous procedure, you should still be **root** user.

1 If necessary, change back to the **/opt/cisco/backup_restore** directory.

2 Execute the following script to migrate users to the SR 8.0 EC. You will be prompted to confirm or deny the migration of each user, line by line.

Note: Substitute the IP address for the SR 7.x EC for the <EC7.x IP> entry in the command.

Migrate Users Command

```
sudo ./migrateUsers --source <EC7.x IP>
```

Migrate Users Example

```
[admin@vodwater backup_restore]$ sudo ./migrateUsers --source
10.90.46.120
```

3 When prompted to migrate a user, enter **y** or **n**, as appropriate. The default is **n**.

Note: If you are prompted to migrate a dncssse user, enter **n** as this was used for SDV tools.

Result: Once you have responded to all user prompts, each user's home directory is present in **/home/<user>/migrated_home**.

Migrating the Database and Key Files

Important: Cisco recommends completing this procedure during a Maintenance Window due to the following:

- The migrateDBKF script will stop all EC processes on the SR 7.x system.
- All billing transactions and updates to the active SR 7.x EC will be suspended.

In this section, you will migrate the database from the SR 7.x EC to the SR 8.0 EC. This migration script, migrateDBKF, automates a remote database unload of the database(s) and then runs migrateKeyFiles to bring the database(s) over to the local machine. Any new files related to key files are also migrated.

When the migration completes, the migrateDBKF script loads the database(s).

Important: Processes will be stopped on the *primary* EC when running this script. Therefore, perform this procedure in a maintenance window, as services will be impacted.

1 Type the following command to migrate the database and any new keyfiles.

Important: Substitute the IP address for the SR 7.x EC for the [SR 7.x IP] entry in the command.

Migrate Database and Key Files Command

```
sudo ./migrateDBKF --source [SR 7.x IP] --db dncs
```

Migrate Database and Key Files Example

```
[admin@vodwater backup_restore]$ sudo ./migrateDBKF --source
10.90.46.120 --db dncs
```

2 When prompted to proceed with the migration, enter **y** and press **Enter**.

Note: This could take up to an hour depending on the size of the database.

3 When the DBKF migration completes, type the following command as root user to shutdown the SR 7.x EC.

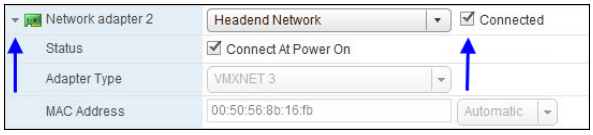
```
# shutdown –y –g0 –i0
```

4 Go to the next chapter.

Update the EC Network Configuration

1. From the vCenter Web UI, right-click the SR 8.0 EC and select **Edit Settings**. The Edit Settings window appears.
2. From the Virtual Hardware area, click the pointer next to **Network adapter 2** and select **Connected**.

   Note: If you are using vSphere ESXi client, refer to ***Modifying the Device Status for an Ethernet Adapter*** (on page 208).



3. Repeat Step 2 for **Network adapter 3**.
4. Click **OK**.
5. In the EC terminal window, type the following command to restart the network service.

   ```
   [root@vodwater ~]# service network restart
   ```

6. Verify that you can ping the headend network and the TED device.

7

SR 8.0 Post-Upgrade Procedures

Complete the procedures in this section to verify that the system is fully functional and to complete the upgrade.

Important: If any of the tests in this chapter fail, troubleshoot the system to the best of your ability. If you are unable to resolve the failure, contact Cisco Services.

In This Chapter

Creating User Accounts

This section describes the types of user accounts that you can create on the EC, while also including the steps to create an Administrator user account.

User Account Types

The following user accounts can be created on the EC.

- **Regular User**
  - Can log into the operating system
  - Cannot read or write EC application files
  - Cannot execute EC application executable files
  - Cannot switch to the dncs user
- **Operator**
  - Can log into the operating system
  - Can read but cannot write EC application files
  - Cannot execute EC application executable files
  - Cannot switch to the dncs user
- **Administrator**
  - Can log into the operating system
  - Can read but not write EC application files
  - Cannot execute EC application executable files
  - Can switch to the dncs user — once switched to the dncs user:
    - Can read and write EC application files
    - Can execute EC application executable files

Accessing the root and dncs User Accounts

Important:

- Role-Based Access Control (RBAC) is no longer supported. Please follow the steps below to switch between different user accounts.
- The **ecadmin/dtacsadmin** user is used in examples for all Cisco DBDS documents pertaining to EC 8.0 and DTACS 5.0.
- Commands run as **root** user are shown with a **#** symbol.

  Example:

  ```
  [root@vodwater ~]#
  ```

- Commands run as a **admin**, **dncs**, or any **Administrator** user are shown with a **$** symbol.

  Example:

  ```
  [admin@vodwater ~]$
  [ecadmin@vodwater ~]$
  [dncs@vodwater ~]$
  ```

Once the EC/DTACS application installation is complete, you can only log in with the **admin** user account. The admin account is created by default during the installation, and is granted privileges to access the root user account, as root login is not permitted. These privileges allow the admin user to execute root commands by preceding the command with "sudo". For example, if you want to modify a network configuration file, the command will resemble the following:

Example: Executing a root command as admin user:

```
[admin@vodwater ~]$ sudo vi
/etc/sysconfig/network-scripts/ifcfg-eth0
```

As **admin** user, you can also change to the root user account by entering the following command.

Important: For any procedure in this guide that states "As root user", you must be logged into a terminal window as admin user and switch to the root user.

Command Syntax: Changing to root user:

```
[admin@vodwater ~]$ sudo –i
```

Any ***Administrator*** account that you create using the useradmin script (see the next section) has privileges to log into the EC/DTACS from a terminal window. Administrator accounts do not have privileges to access the root user account, but should be used to access the dncs user account.

Important: Do not access the dncs user account using the root user account.

To switch to the **dncs** user, type the following command from the terminal window where you are logged in as an Administrative user.

Important: For any procedure that states "As dncs user", you need to execute this command from the terminal window where you are logged in with your Administrator account.

Command Syntax: Changing to the dncs user:

```
[ecadmin@vodwater ~]$ sudo su – dncs
```

Note: Throughout all Cisco DBDS documentation, the **ecadmin/dtacsadmin** user is used as an example.

Overview:

Terminal Window Logged in as:	Use Account to change to:	Command to execute:
admin	root	sudo -i
[Administrator] **Example:** ecadmin	dncs	sudo su - dncs

Creating an Administrative User Account

Important: It is highly recommended that you create an Administrator user account to access the dncs user account. It is best practice ***not*** to use the admin or root user account to access the dncs account.

Complete the following steps to create an Administrator account called "ecadmin". This user account, along with any other Administrative user accounts you create, will be used to sudo to the dncs account, which includes the ability to stop and start system processes.

1 As **admin** user, type the following command to create the **ecadmin** user account on the EC. The USER ADMINISTRATION MENU appears.

```
[admin@vodwater ~]$ sudo /dvs/admin/useradmin
```

2 Enter **a** to add a new user and press **Enter**.

3 Type **y** to confirm that you want to add a user and press **Enter**.

4 Select one of the following user types:

- Add Regular User
- Add Operator
- Add Administrator

5 Type **3** to define this user as an Administrative user and press **Enter**.

6 Enter a username called **ecadmin** and press **Enter**.

7 Type **y** to confirm the action and press **Enter** to continue. You are prompted for the password.

8 Enter a password for the user and press **Enter**.

Note: The password must contain upper and lower case letters, a special character, and a number.

9 Re-type the password and press **Enter**. You are then prompted to enter a password to access the Web UI.

10 Enter a password for this user to access the Web UI.

Note: You can set this password to anything you want. We suggest that you set it to the same password your user login password.

11 Re-enter the password for the Web UI and press **Enter**. You are returned to the User menu.

12 Continue adding users for your system, as needed.

13 When you have finished adding users, type **q** to exit the menu.

14 Type **q** again to exit the USER ADMINISTRATION MENU.

15 Are you using LDAP or NIS?

- If **no**, and you are storing passwords locally, go to the next step.
- If **yes**, go to Step 18.

16 Enter the following command to reset the password for the **ecadmin** user.

```
[admin@vodwater ~]$ sudo passwd ecadmin
```

17 When prompted, enter the password, and then when prompted again, re-enter the password. A confirmation will display.

Note: Enter the same password that you used when creating the ecadmin user with the USER ADMINISTRATION MENU.

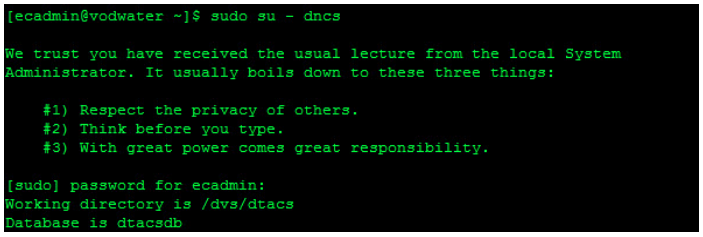
```
Changing password for user ecadmin.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

18 Open a new terminal window to the EC and login as **ecadmin**.

19 Type the following command to verify that you can change to the **dncs** user.

```
[ecadmin@vodwater ~]$ sudo su - dncs
```

20 When prompted, enter the password for the **ecadmin** user.



Note: You should now have two terminal windows open; one as admin user and one as ecadmin user (use to su to dncs).

Set the manage_dncsLog Script Log Retention Variables

In this procedure, you will review and, if necessary, set variables in the manage_dncsLog script. These variables determine the number of days the DBDS core files and logs are kept. DBDS core files and logs can be very large and, under extreme conditions, can be created very rapidly.

Note: If this is an EC migration, you must complete this procedure as the manage_dncsLog script variables are not currently migrated.

The variables are:

- `DAYS_SAVELOGS_KEPT=10`
- `DAYS_COREFILES_KEPT=10`
- `DAYS_CORELOGDIRS_KEPT=10`

As listed above, the default value for each variable is 10 days. DBDS process logs are only saved when the logLvl +ZIP is enabled.

Notes:

- The logLvl command sets logging levels. The +ZIP switch enables the save-log option.
- Cisco recommends that logLvl +ZIP only be enabled when you are attempting to capture logs for processes that are exhibiting a problem. Once sufficient logs have been captured, this should be disabled (-ZIP).

These variables are set to minimize the possibility that core files and logs fill the file system and cause system outages. If you determine that the DBDS logs and/or core files should be kept for a longer or shorter period, follow these instructions to set the variables.

1. As **dncs** user, open the **/dvs/dncs/etc/manage_dncsLog** file in a text editor.
   ```
   [dncs@vodwater ~]$ vi /dvs/dncs/etc/manage_dncsLog
   ```
2. Locate the **DAYS_SAVELOGS_KEPT** variable and change the value to the appropriate number of days.
3. Locate the **DAYS_CORELOGDIRS_KEPT** variable and change the value to the appropriate number of days.
4. Locate the **DAYS_COREFILES_KEPT** variable and change the value to the appropriate number of days.
5. Save and close the file.

Update the osmAutoMux.cfg File

Important: If your system is not using the osmAutoMux file, you can skip this procedure.

The osmAutoMux.cfg file configuration file must include a headend map entry (HEMAP). If this entry is not present in the osmAutomux.cfg file, the code version table (CVT) will not be generated for remote BFS QAMs.

The following line must be added to the osmAutoMux.cfg file:

```
HEMAP|1|200
```

Note: 1 is the local headend ID and 200 is the sample headend ID.

Follow these steps to add the HEMAP entry to the osmAutoMux.cfg file.

1. As **dncs** user, enter the following command to change to the **/dvs/dvsFiles/OSM** directory.

   ```
   [dncs@vodwater ~]$ cd /dvs/dvsFiles/OSM
   ```

2. Edit the **osmAutoMux.cfg** file in a text editor.

   ```
   [dncs@vodwater OSM]$ vi /dvs/dvsFiles/OSM/osmAutoMux.cfg
   ```

3. Add the following entry to the end of the file.

   ```
   HEMAP|1|200
   ```

4. Save and close the file.

Modify the dncs User .profile File

In this section, review and adjust the .profile file for the following items:

- Variables that are required for Emergency Alert Messages (EAM).
- If your site is not SSP2.3 Compliant, you need to add the following entry to the DNCS .profile file as **dncs** user.

Note: If you have completed the procedures to this point, you should be logged in as **dncs** user.

1 As **dncs** user, go to the /home/dncs directory.

```
[dncs@vodwater ~]$ cd /home/dncs
```

2 Open the **.profile** file in a text editor.

```
[dncs@vodwater dncs]$ vi .profile
```

3 Go to the end of the file and add the following content.

```
# VOD variable for systems that are not SSP2.3-compliant
DNCS_DRM_INCLUDE_HE_RSR_VOD=1
export DNCS_DRM_INCLUDE_HE_RSR_VOD
```

Note: If you are not sure what this means, or how to do this, contact Cisco Services.

4 Save and close the file.

Add the DrmCheckVodZeroScrIp Environment Variable in the .profile File

Important: This section applies to systems that include a VOD server that is running in a single element environment with direct connections to the MPEG source.

Complete the following procedure to add the DrmCheckVodZeroScrIp environment variable with a value of 1 to the dncs user .profile file.

Note: If you have completed the procedures to this point, you should be logged in as **dncs** user.

1 As **dncs** user, go to the **/home/dncs** directory.

```
[dncs@vodwater ~]$ cd /home/dncs
```

2 Open the **.profile** file in a text editor.

```
[dncs@vodwater ~]$ vi .profile
```

3 Move to the end of the file and add the following entries:

```
# VOD Server
 DrmCheckVodZeroScrIp=1; export DrmCheckVodZeroScrIp
```

4 Save and close the .profile file.

Modify the .profile File for DSG

Important: If your system was not configured for DSG BFS, you can skip this procedure.

In this procedure, you will update your system to use DSG BFS.

Note: If you have completed the procedures to this point, you should be logged in as **dncs** user.

1 Type **cd** to return to the root directory for the **dncs** user.

```
[dncs@vodwater dncs]$ cd
```

2 Enter the following command to see if the dncs_bfsRemote=dncsdsg entry exists.

```
[dncs@vodwater ~]$ less .profile | grep dncs_bfsRemote
```

3 Did **export dncs_bfsRemote=dncsdsg** display in the output?

- If **yes**, you have completed this procedure.
- If **no**, enter the following command to open the .profile file in a text editor.

```
[dncs@vodwater ~]$ vi .profile
```

4 Add the following entry.

```
export dncs_bfsRemote=dncsdsg
```

5 Save and close the file.

6 Type the following commands to restart system processes.

```
[dncs@vodwater ~]$ appStop
[dncs@vodwater ~]$ dncsStop
```

Note: Wait until all processes are stopped before restarting processes.

```
[dncs@vodwater ~]$ dncsStart
[dncs@vodwater ~]$ appStart
```

7 Type **exit** to log out of the dncs session. You are returned to the ecadmin session.

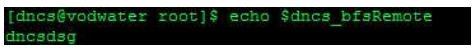
8 Enter the following command to change back to **dncs** user.

```
[ecadmin@vodwater ~]$ sudo su - dncs
```

9 Enter the following command to verify the **bfsRemote** setting. The output should be **dncsdsg**.

```
[dncs@vodwater ~]$ echo $dncs_bfsRemote
```

Example Output:



Update the site_info Database Table for a Hostname Change

Important: If this is a new install or a migration from SR <previous_version> to SR 8.0 in which the hostname of the SR <previous_version> and SR 8.0 system is the same, you can skip this procedure.

Complete this procedure only if your SR 8.0 system was a migration from SR <previous_version> in which the hostname was changed to a new hostname when you defined the ec.envfile in ***Install SR 8.0*** (on page 41).

Note: For this procedure, we will assume the SR <previous_version> hostname is "dncs" and the hostname that was added to the ec.envfile is "vodwater".

1 As **root** user, enter the following command to verify the current hostname for the SR 8.0 system.

Note: The output of this command should be the same as the "hostname=" value in the /var/tmp/cisco-vcs-deployment-1.0.*/scripts/ec.envfile.

```
[root@vodwater ~]# hostname
```

Example Output:

```
vodwater
```

2 Enter the following command to source the environment.

```
[root@vodwater ~]# . /dvs/dncs/bin/dncsSetup
```

3 Enter the following command to access the dncs database. A database prompt appears.

```
[root@vodwater ~]# dbaccess dncsdb -
>
```

4 Enter the following command to view the output of the **site_info** table.

```
> select * from site_info;
```

Example Output:

```
site_id             1
site_name           DNCS
bfs_sess_mac_addr   00:00:00:00:00:00
site_ip_address     10.253.3.1
site_mac_address    00:00:00:00:00:00
site_hostname       dncs
site_status         1
oob_flow_ipaddr
gda
gda_port            0
```

5 Does the **site_hostname** entry match the output from Step 1?

- If **yes**, go to Step 9.
- If **no**, go to the next step.

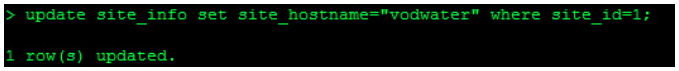
6 Enter the following command and press **Enter** to update the **site_hostname** entry. You are returned to the database prompt.

Command Syntax:

```
update site_info set site_hostname="[new_hostname]" where
site_id=[site_id value];
```

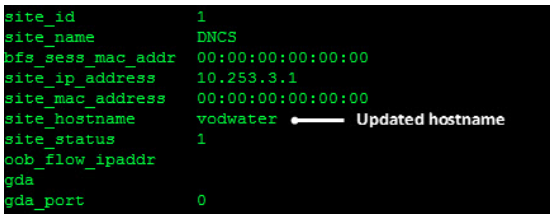
Example:

```
> update site_info set site_hostname="vodwater" where
site_id=1;
```



7 Repeat Step 4 to verify that the **site_hostname** was successfully updated in the site_info table.

Example Output:



8 Press **Ctrl+C** to exit the database.

9 Enter the following command to verify the IP address for the **dncsatm** entry.

```
[root@vodwater ~]# less /etc/hosts | grep dncsatm
```

Example Output:

```
10.253.3.1      dncsatm dncs_host
```

10 Does the site_ip_address entry match the dncsatm IP address from the output of Step 4?

- If **yes**, you have completed this procedure.
- If **no**, go to the next step.

11 Enter the following command to access the dncs database. A database prompt appears.

```
[root@vodwater ~]# dbaccess dncsdb -
```

12 Enter the following command and press **Enter** to update the **site_ip_address** entry. You are returned to the database prompt.

Command Syntax:

```
update site_info set site_ip_address="[new_dncsatm_IP]" where
site_id=[site_id value];
```

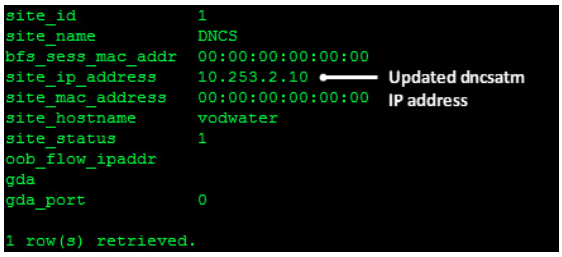
Example:

```
> update site_info set site_ip_address="10.253.2.10" where
site_id=1;
```

13 Enter the following command to verify that the **site_ip_address** entry was successfully updated in the site_info table.

```
> select * from site_info;
```

Example Output:



14 Press **Ctrl+C** to exit the database.

Add IPG_TVDATA_NEW to appservSetup

Important: Only execute this procedure if you use TVDATA for IPG.

Note: At this point, all EC processes should be stopped and the dncsInitd and appInitd processes have been killed.

Was the IPG_TVDATA_NEW variable found in the appservSetup file during pre-upgrade checks?

- If **yes**, as **dncs** user add the variable to the **/home/dncs/.profile** file exactly as it was in the old system.

  Note: This variable should have been saved and recorded in ***Checking for the IPG_TVDATA_NEW Variable in appservSetup*** (on page 16).

- If **no**, continue with the next procedure.

Setting Up SFTP Support

Important: Only complete the procedures in this section if SFTP support is required at your site.

This section describes how to add an SFTP user for SFTP support. It also includes procedures to restrict SFTP to a single home directory.

Note: The SFTP user you create can also be used to communicate with an AGI Adapter provided you have configured an AGI Adapter.

Creating a User for SFTP Support

Complete the following procedure to create an SFTP user.

1 As **admin** user, enter the following command to create an SFTP user. The USER ADMINISTRATION MENU displays.

```
[admin@vodwater ~]$ sudo /dvs/admin/useradmin
```

2 Type **a** and press **Enter**.

3 When prompted to add a new user, type **y** and press **Enter**.

4 Type **1** and press **Enter** to add a regular user.

5 At the **New Username** prompt, type a name for this user (for example, sftpuser1).

6 When prompted to continue to add this user, type **y** and press **Enter**.

7 At the **New password** prompt, enter a new password (for example, sftpuser1) and press **Enter**.

8 At the **Retype a new password** prompt, re-enter the password and press **Enter**.

9 Type **q** to exit from adding any other users.

10 Type **q** to exit the USER ADMINISTRATION MENU. You are returned to an admin prompt.

11 Enter the following command to reset the password for the SFTP user.

Command Syntax:

```
sudo passwd [SFTP-username]
```

Example:

```
[admin@vodwater ~]$ sudo passwd sftpuser1
```

12 When prompted, enter the same or a new password for the SFTP user.

13 When prompted to re-enter the password, re-enter it.

Important: By default, the password for the SFTP user will expire in 91 days. Your system administrator must decide the password expiration policies for the SFTP user.

Creating a Directory for SFTP File Transfers

Complete the following steps to create a directory that restricts SFTP access to a single home directory. The directory you create and all directories above it *must* be owned by root and have write permissions only for root.

Note: This directory must be created under /dvs.

1 Enter the following command to create a directory in **/dvs**.

Command Syntax:

```
sudo mkdir /dvs/[SFTP-home-directory]
```

Example:

```
[admin@vodwater ~]$ sudo mkdir /dvs/sftpuser1
```

2 Enter the following command to set the ownership of the new SFTP home directory to **root:root**.

Command Syntax:

```
sudo chown root:root /dvs/[SFTP-home-directory]
```

Example:

```
[admin@vodwater ~]$ sudo chown root:root /dvs/sftpuser1
```

3 Enter the following command to update the permissions of the SFTP home directory to **0755**.

Command Syntax:

```
sudo chmod 0755 /dvs/[SFTP-home-directory]
```

Example:

```
[admin@vodwater ~]$ sudo chmod 0755 /dvs/sftpuser1
```

4 Enter the following command to create an upload directory under the new SFTP home directory and then change its ownership to the SFTP user with a directory permission of **0700**.

Command Syntax:

```
sudo mkdir /dvs/[SFTP-username]/[upload-directory]
sudo chown [SFTP-username]:[SFTP-username]
/dvs/[SFTP-username]/[upload-directory]
chown root:root /dvs/[SFTP-home-directory]
```

Example:

```
[admin@vodwater ~]$ sudo mkdir /dvs/sftpuser1/uploads
[admin@vodwater ~]$ sudo chown sftpuser1:sftpuser1
/dvs/sftpuser1/uploads
[admin@vodwater ~]$ sudo chmod 0700 /dvs/sftpuser1/uploads
```

Restricting SFTP Access to a Single Directory

Complete the following steps to restrict SFTP access to a single directory.

1 Open the **/etc/ssh/sshd_config** file in a text editor.

```
[admin@vodwater ~]$ sudo vi /etc/ssh/sshd_config
```

2 Go to the end of the file and add the following content:

Command Syntax:

```
Match User [SFTP-username]
ForceCommand internal-sftp
PasswordAuthentication yes
ChrootDirectory /dvs/[SFTP-home-directory]
PermitTunnel no
AllowAgentForwarding no
AllowTcpForwarding no
X11Forwarding no
```

Example:

```
Match User sftpuser1
ForceCommand internal-sftp
PasswordAuthentication yes
ChrootDirectory /dvs/sftpuser1
PermitTunnel no
AllowAgentForwarding no
AllowTcpForwarding no
X11Forwarding no
```

3 Enter the following command to restart the **sshd** service.

```
[admin@vodwater ~]$ sudo systemctl restart sshd
```

Verifying the SFTP Configuration

Complete the following steps to verify the SFTP configuration.

1 Enter the following command to verify that you cannot complete an SSH request as SFTP user.

Command Syntax:

```
sudo ssh [SFTP-username]@localhost
```

Example:

```
[admin@vodwater ~]$ sudo ssh sftpuser1@localhost
```

2 Enter the following command to verify that you can successfully execute an SFTP file transfer.

Command Syntax:

```
sudo sftp[SFTP-username]@localhost
```

Example:

```
[admin@vodwater ~]$ sudo sftp sftpuser1@localhost
```

3 When prompted, enter the password for the SFTP user. You are connected to local host and an sftp prompt displays.

4 At the **sftp>** prompt, type `dir`. Your SFTP upload directory should display. You should be able to read and write into the directory.

Example:

```
sftp> dir
uploads
sftp>
```

5 Attempt a file transfer to the directory.

Remove Old BFS Entries

In this procedure, you will remove old BFS entries in the /dvs/dvsFiles/BFS_REMOTE directory.

1 As **dncs** user, type the following command and press **Enter** to change to the **/dvs/dvsFiles/BFS_REMOTE** directory:

```
[dncs@vodwater ~]$ cd /dvs/dvsFiles/BFS_REMOTE
```

2 Type the following command and press **Enter** to check for old entries.

```
[dncs@vodwater ~]$ ls
```

3 Did the output from step 2 reveal any files or directories?

- If **yes**, type the following command and press **Enter** to remove these files or directories:

  ```
  [dncs@vodwater BFS_REMOTE]$ rm -rf *
  ```

- If **no**, type the following command and press **Enter** to leave the /dvs/dvsFiles/BFS_REMOTE directory:

  ```
  [dncs@vodwater ~]$ cd
  ```

Stop and Disable Unneeded Processes

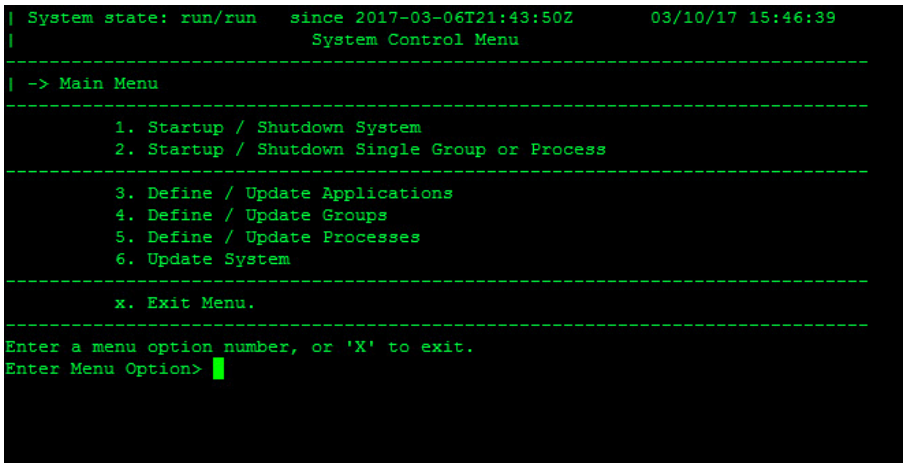
After the upgrade completes and the processes are started, all processes will be running (green). If your system includes dncs processes that were not running or enabled before the upgrade, they should be stopped and/or disabled after the upgrade.

Example: The example used throughout this procedure involves stopping and disabling the saManager process.

1 As **dncs** user, type `dncsStart` and press **Enter**.

2 Type the following command and press **Enter**. The dncs System Control Menu appears.

```
[dncs@vodwater ~]$ dncsControl
```



3 Type `2` (Startup/Shutdown Single Group of Process) and press **Enter**.

4 Type `1` (dncs) and press **Enter**.

5 Type `e` (Display Groups) and press **Enter**.

6 Type `14` and press **Enter**.

7 Type `e` (Display Process Entries) and press **Enter**.

8 Type `1` (saManager) and press **Enter**.

9 To stop the process, type `1` (stopped) and press **Enter**. The process status changes to red in the Process Status tree.

10 Do you want to disable the process?

Note: Disabling the process removes the process from the Process Status tree.

- If **yes**, type `1` (saManager) and press **Enter**, then type `4` (disabled) and press **Enter**. The saManager process is removed from the Process Status tree. Then go to Step 11.
- If **no**, go to Step 11.

11 Repeat this procedure to stop/disable other processes, as needed.

Important: Once you get to step 7, the entries may change to view the appropriate display group.

12 To exit the dncsControl window, type `X` (Return to Menu) until the dncsControl window closes.

13 Type the following commands and press **Enter** to stop and kill the dncs processes:

```
dncsStop
```

Important: Wait for all processes to stop before executing the next command.

```
dncsKill
```

Add External Database Listener for Third Party Application Servers

Important: This procedure is required if the site being upgraded uses a third-party application server.

1 As **admin** user, change to the following directory.

```
[admin@vodwater ~]$ cd /opt/cisco/informix/server/etc
```

2 Enter the following command to open the **sqlhosts** file in a text editor and add the following line to the end of the file.

```
[admin@vodwater ~]$ sudo vi sqlhosts
```

3 Go to the end of the file and add the following entry.

```
dncsatmDbServer  onsoctcp   dncsatm   sqlexec
```

4 Save and close the file.

5 Enter the following command to open the open the **onconfig** file in a text editor.

```
[admin@vodwater ~]$ sudo vi onconfig
```

6 Go to the DBSERVERALIASES entry and add **dncsatmDbServer** to the end of the line.

Example:

```
DBSERVERALIASES demo_on,localhost_tcp, dncsatmDbServer
```

7 Type the following commands, pressing **Enter** after each, to restart Informix:

```
[admin@vodwater ~]$ sudo service informix stop
[admin@vodwater ~]$ sudo service informix start
[admin@vodwater ~]$ sudo service informix status
```

8 Type the following command and press **Enter** to ensure that the Informix listener is running on the dncsatm interface or whatever external interface was previously configured, as well as on the loopback interface:

```
[admin@vodwater ~]$ sudo netstat -an |grep 9088
```

Result: Output should be similar to the following example:

```
tcp        0   0 172.16.3.131:9088     0.0.0.0:*    LISTEN
tcp        0   0 127.0.0.1:9088        0.0.0.0:*    LISTEN
```

Configure FTP Users and Start the vsftpd Service

Important: Complete this procedure only if the FTP service is required on your system.

The vfstpd daemon (very secure FTP daemon) is the default FTP server used in CentOS.

For security reasons, the vsftpd service does not run at initial install/bootup. The following procedure must be performed must be performed to configure FTP users, provide FTP access to the users and to start the vfstp service.

1 As **admin** user, enter the following command to open the **/etc/vsftpd/user_list** file in a text editor.

```
[admin@vodwater ~] $ sudo vi /etc/vsftpd/user_list
```

2 Add an entry for the **easftp** and **dncsftp** users.

3 Save and close the file.

4 Enter the following command to start the **vsftpd** service.

```
[admin@vodwater ~]$ sudo service vsftpd start
```

5 Enter the following command to verify that the service has started.

```
[admin@vodwater ~]$ service vsftpd status
```

6 Enter the following command to set the vsftpd service to start automatically at bootup.

```
[admin@vodwater ~]$ sudo chkconfig vsftpd on
```

Configuring snmpd Traps on the EC Node

Important: This section should *only* be completed if the EC is or will be regionalized to an ECS.

Complete the following steps to update the snmpd configuration file to configure alarm forwarding to the VCS Console for the following services:

- dncsInitd
- appInitd
- tomcatmon
- httpd
- httpd-dncsws
- oammgr
- consul

1 As **admin** user, enter the following command to update the **snmpd.conf** file in a text editor.

```
[admin@vodwater ~]$ sudo vi /etc/snmp/snmpd.conf
```

2 Go to the end of the file and add the following content.

```
# Monitor consul process and send traps


view systemview included .1.3.6.1.4.1.1429 #cisco
view systemview included .1.3.6.1.4.1.2021 #ucd
rwcommunity cisco
rocommunity public
proc dncsInitd 1 1
proc appInitd 1 1
proc tomcatmon 1 1
proc httpd
proc httpd-dncsws
proc oammgr 1 1
proc consul 1 1


monitor -r 5 -u admin -i -o .1.3.6.1.4.1.2021.2.1.2.1 -o
.1.3.6.1.4.1.2021.2.1.101.1 "EC application h
as stopped." -o .1.3.6.1.4.1.2021.2.1.100.1 .1.3.6.1.4.1.2021.2.1.100.1 != 0
monitor -r 5 -u admin -i -o .1.3.6.1.4.1.2021.2.1.2.1 -o
.1.3.6.1.4.1.2021.2.1.101.1 "EC application i
s running." -o .1.3.6.1.4.1.2021.2.1.100.1 .1.3.6.1.4.1.2021.2.1.100.1 == 0
```

```
monitor -r 5 -u admin -i -o .1.3.6.1.4.1.2021.2.1.2.2 -o
.1.3.6.1.4.1.2021.2.1.101.2 "AppServer has stopped." -o
.1.3.6.1.4.1.2021.2.1.100.2 .1.3.6.1.4.1.2021.2.1.100.2 != 0

monitor -r 5 -u admin -i -o .1.3.6.1.4.1.2021.2.1.2.2 -o
.1.3.6.1.4.1.2021.2.1.101.2 "AppServer is running." -o
.1.3.6.1.4.1.2021.2.1.100.2 .1.3.6.1.4.1.2021.2.1.100.2 == 0


monitor -r 5 -u admin -i -o .1.3.6.1.4.1.2021.2.1.2.3 -o
.1.3.6.1.4.1.2021.2.1.101.3 "EC Tomcat service has stopped." -o
.1.3.6.1.4.1.2021.2.1.100.3 .1.3.6.1.4.1.2021.2.1.100.3 != 0

monitor -r 5 -u admin -i -o .1.3.6.1.4.1.2021.2.1.2.3 -o
.1.3.6.1.4.1.2021.2.1.101.3 "EC Tomcat service is running." -o
.1.3.6.1.4.1.2021.2.1.100.3 .1.3.6.1.4.1.2021.2.1.100.3 == 0


monitor -r 5 -u admin -i -o .1.3.6.1.4.1.2021.2.1.2.4 -o
.1.3.6.1.4.1.2021.2.1.101.4 "EC HTTP service has stopped." -o
.1.3.6.1.4.1.2021.2.1.100.4 .1.3.6.1.4.1.2021.2.1.100.4 != 0

monitor -r 5 -u admin -i -o .1.3.6.1.4.1.2021.2.1.2.4 -o
.1.3.6.1.4.1.2021.2.1.101.4 "EC HTTP service is running." -o
.1.3.6.1.4.1.2021.2.1.100.4 .1.3.6.1.4.1.2021.2.1.100.4 == 0


monitor -r 5 -u admin -i -o .1.3.6.1.4.1.2021.2.1.2.5 -o
.1.3.6.1.4.1.2021.2.1.101.5 "EC HTTP-DNCSWS service has stopped." -o
.1.3.6.1.4.1.2021.2.1.100.5 .1.3.6.1.4.1.2021.2.1.100.5 != 0

monitor -r 5 -u admin -i -o .1.3.6.1.4.1.2021.2.1.2.5 -o
.1.3.6.1.4.1.2021.2.1.101.5 "EC HTTP-DNCSWS service is running." -o
.1.3.6.1.4.1.2021.2.1.100.5 .1.3.6.1.4.1.2021.2.1.100.5 == 0


monitor -r 5 -u admin -i -o .1.3.6.1.4.1.2021.2.1.2.6 -o
.1.3.6.1.4.1.2021.2.1.101.6 "OAM service has stopped." -o
.1.3.6.1.4.1.2021.2.1.100.6 .1.3.6.1.4.1.2021.2.1.100.6 != 0

monitor -r 5 -u admin -i -o .1.3.6.1.4.1.2021.2.1.2.6 -o
.1.3.6.1.4.1.2021.2.1.101.6 "OAM service is running." -o
.1.3.6.1.4.1.2021.2.1.100.6 .1.3.6.1.4.1.2021.2.1.100.6 == 0


monitor -r 5 -u admin -i -o .1.3.6.1.4.1.2021.2.1.2.7 -o
.1.3.6.1.4.1.2021.2.1.101.7 "Consul process has stopped." -o
.1.3.6.1.4.1.2021.2.1.100.7 .1.3.6.1.4.1.2021.2.1.100.7 != 0

monitor -r 5 -u admin -i -o .1.3.6.1.4.1.2021.2.1.2.7 -o
.1.3.6.1.4.1.2021.2.1.101.7 "Consul process is running." -o
.1.3.6.1.4.1.2021.2.1.100.7 .1.3.6.1.4.1.2021.2.1.100.7 == 0


trapsess -v 2c -c public localhost:162
```

3 Save and close the file.

4 Enter the following command to restart the snmpd process.

```
[admin@vodwater ~]$ sudo service snmpd restart
```

Restart Apache and Tomcat Services

Complete the following procedure to restart Apache and Tomcat services. These services must be running to access the EC Web UI.

1 As **admin** user, enter the following commands to restart the Apache and Tomcat services.

```
[admin@vodwater ~]$ sudo service tomcat restart
[admin@vodwater ~]$ sudo service httpd-dncsws restart
[admin@vodwater ~]$ sudo service httpd restart
```

Example:

```
Stopping tomcat:                                           [  OK  ]
Starting tomcat:                                           [  OK  ]
[root@vodwater ~]# service httpd-dncsws restart
Stopping httpd-dncsws:                                     [  OK  ]
Starting httpd-dncsws:                                     [  OK  ]
[root@vodwater ~]# service httpd restart
Stopping httpd:                                            [  OK  ]
Starting httpd:                                            [  OK  ]
```

2 Enter the following commands to verify that the Apache and Tomcat services are running. A message stating that the service is running should appear.

```
[admin@vodwater ~]$ sudo service tomcat status
[admin@vodwater ~]$ sudo service httpd-dncsws status
[admin@vodwater ~]$ sudo service httpd status
```

Example:

```
tomcat (pid 30927) is running...                           [  OK  ]
[root@vodwater ~]# service httpd-dncsws status
httpd-dncsws (pid  31029) is running...
[root@vodwater ~]# service httpd status
httpd (pid  31113) is running...
```

Note: If a service fails to start, please contact Cisco Services.

Start the EC Processes

Important: Execute this procedure for either a new install or a migration.

1 As **dncs** user, type the following command to start dncs processes.

```
[dncs@vodwater ~]$ dncsStart
```

2 If you have installed the application server, type the following command to start the application server processes.

```
[dncs@vodwater ~]$ appStart
```

3 From a supported Web browser, use the following URL syntax to access the EC Web UI.

URL Syntax:

```
https://EC IP address]
```

Example:

```
https://10.90.47.20
```

4 Login to the EC Web UI using the **ecadmin** account credentials or any other administrator account you created in ***Creating User Accounts*** (on page 61).

5 Monitor the processes as they come up. Green indicators replace red indicators as the application processes start. All processes should turn green shortly.

Note: All process logs are located in /dvs/dncs/tmp for dncs processes and /dvs/appserv/tmp for application server processes.

6 Provision the system as needed.

Note: Refer to the ***SR 8.0 EC Online Help*** for assistance.

Verify the Number of BFS Sessions

The number of BFS sessions after the upgrade needs to be the same as the number of BFS sessions before the upgrade. The procedures in this section guide you through the steps that are required in validating the number of BFS sessions.

Verifying the Number of Recovered BFS Sessions

1. Press the **Options** button on the front panel of the BFS QAM until the **Session Count** total appears.
2. Does the **Session Count** total equal the number of sessions you recorded in *Checking the Number of BFS Sessions* (on page 17)?
   - If **yes**, skip to step 6.
   - If **no**, telnet to the GQAM modulator where BFS sessions are built.

     Example: `telnet 192.51.100.29`

     Note: The login ID and password are both `Gqam`. If you make a typing error, follow these steps to recover.

     a. Press **Ctrl +]** to return to the telnet prompt.
     b. Type `mode ch` and press **Enter** twice. The system returns you to the GQAM.
3. Type the following command and press **Enter**. The system displays the sessions that are set up on the GQAM port.

   Command Syntax:

   ```
   print_session_status <port number>
   ```

   Example:

   ```
   D9479 GQAM> print_session_status 0
   ```

   Note: Port numbers on the GQAM are 0 through 15. If your sessions are built on port 1 in the QAM Web UI, it is port 0 on the GQAM.
4. Locate Session ID **00:00:00:00:00:00:2**. Is this session **Active**?
   - If **yes**, go to step 6.
   - If **no**, go to the next step.
5. If the session is not in a **CREATE_TABMAN_WAITING** or **PAT_ASSEMBLY** state, troubleshoot this matter using your established escalation procedures. If you cannot resolve the problem, contact Cisco Services for assistance.
6. Does the **Session State** field of Session ID **00:00:00:00:00:00:2** show **PAT_ASSEMBLY**?
   - If **yes**, go to *Tear Down BFS and OSM Sessions* (on page 88).
   - If **no**, troubleshoot this matter using your established escalation procedures.

     Note: Call Cisco Services if you are unable to resolve the issue.

7 Press **Ctrl +]** to return to the telnet prompt and then type `quit` to exit the telnet session. You are returned to the root prompt.

8 As **dncs** user, type the following command and press **Enter**. The BFS session count is displayed.

Command Syntax:

```
auditQam –query [BFS QAM IP address] [port #]
```

Example:

```
[dncs@vodwater ~]$ auditQam –query 209.165.202.129 1
```

Important: Make sure to use the IP address of the BFS QAM in your system when running this procedure.

```
Number of Sessions = 12
        Session 1:    00:00:00:00:00:02/2
        Session 2:    00:00:00:00:00:02/4
        Session 3:    00:00:00:00:00:02/6
        Session 4:    00:00:00:00:00:02/8
        Session 5:    00:00:00:00:00:02/10
        Session 6:    00:00:00:00:00:02/12
        Session 7:    00:00:00:00:00:02/14
        Session 8:    00:00:00:00:00:02/16
        Session 9:    00:00:00:00:00:02/18
        Session 10:   00:00:00:00:00:02/20
        Session 11:   00:00:00:00:00:02/22
        Session 12:   00:00:00:00:00:02/199
```

Tear Down BFS and OSM Sessions

Complete this procedure ONLY if the number of recovered BFS sessions does not match the number of pre-upgrade BFS sessions. Complete these steps to tear down the BFS and OSM sessions to return the BFS session count to the expected number of sessions.

1 From the home page of the EC Web UI (displays the processes), click the button next to **bfsServer**.

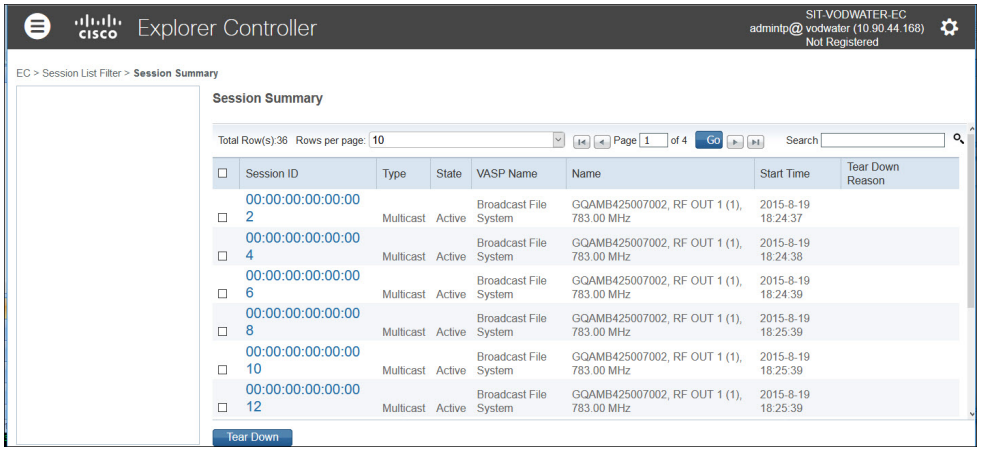
2 Click **Stop**. The bfsServer process stops and turns red.

3 Scroll down the process list and click the button next to **osm**.

4 Click **Stop**. The osm process stops and turns red.

5 Click the **Navigation** button,  , and then select **Utilities > Session List**. The Session List Filter page opens.

6 Select the BFS QAM from the QAMs list and then click **Display**. The Session Summary page appears.



7 Does the system have more than 10 BFS sessions?

- If **yes**, change the **Rows per page** field to a value that will include all sessions.
- If **no**, continue with the next step.

8 Click the check box next to **Session ID** in the top row. This selects **ALL BFS** sessions displayed on this page.

9 Click **Tear Down** at the bottom of the page. All BFS sessions are torn down.

10 Click **EC** from the left-most portion of the window to display the home page of the EC WUI.

11 Click the **bfsServer** button and then click **Start**. The bfsServer process starts and turns green.

12 Click the **osm** button and then click **Start**. The osm process starts and turns green.

Note: Wait about 10 minutes for the BFS sessions to build.

13 Repeat Steps 5 through 6 to display the current BFS session list.

14 Are all the BFS Sessions present and active?

- If **yes**, continue with the next step.
- If **no**, contact Cisco Services for assistance.

15 Press the **Options** button on the front panel of the BFS QAM modulator until the **Session Count** total appears.

16 Does the **Session Count** total now equal the number of sessions you recorded in the ***Checking the Number of BFS Sessions*** (on page 17) procedure?

- If **yes**, continue with the next step.
- If **no**, contact Cisco Services for assistance.

17 As **dncs** user, type the following command and press **Enter**. The BFS session count is displayed.

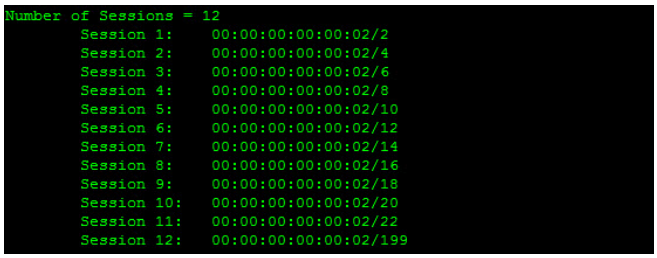
Command Syntax:

```
auditQam –query [BFS QAM IP address] [port #]
```

Example:

```
[dncs@vodwater ~]$ auditQam –query 209.165.202.129 1
```

Important: Be sure to use the IP address of the BFS QAM in your system when running this procedure.



18 Does the **Session Count** total equal the number of sessions you recorded in the ***Checking the Number of BFS Sessions*** (on page 17)?

- If **yes**, continue with the next step.
- If **no**, contact Cisco Services for assistance.

19 Telnet to the GQAM modulator where BFS sessions are built.

Example:

```
[dncs@vodwater ~]$ telnet 198.51.100.29
```

Note: The login ID and password are both `Gqam`. If you make a typing error, follow these steps to recover.

a Press **Ctrl** + **]** to return to the telnet prompt.

b Type `mode ch` and press **Enter** twice.

20 Type the following command and press **Enter**. The system displays the sessions that are set up on the GQAM port.

Command Syntax:

```
print_session_status <port number>
```

Example:

```
D9479 GQAM> print_session_status 0
```

Note: Port numbers on the GQAM are 0 through 15. If your sessions are built on port 1 in the QAM WUI, it is port 0 on the GQAM.

21 Locate Session ID **00:00:00:00:00:00:2**. Is this session in the **CREATE_TABMAN_WAITING** state?

- If **yes**, go to next step.
- If **no**, troubleshoot this matter using your established escalation procedures.

  Note: Call Cisco Services if you are unable to resolve the issue.

22 Does the Program State field of Session ID **00:00:00:00:00:00:2** show **PAT_ASSEMBLY**?

- If **yes**, go to the next procedure in this chapter.
- If **no**, troubleshoot this matter using your established escalation procedures.

  Note: Call Cisco Services if you are unable to resolve the issue.

Reset the Modulators

The SR 8.0 installation updates your modulator code. When you reset the modulators, the modulators upgrade by downloading these versions of software from the EC. Only reset those modulators that do not already have the latest version of code.

You have the following methods available when you reset modulators:

- You can use the traditional method of resetting modulators through the EC Web UI.
- You can reset the modulators (except the QAM and QPSK modulators) through the front panel of the modulators. The QAM modulator resets through the power switch on the back panel.
- You can use the auditQam utility to reset the QAM family of modulators through the command line of the EC.

Important Notice Regarding the Reset of QAM Modulators

On occasion, for testing purposes, default configuration files for headend components are changed. For example, a site might substitute a file called gqam.config.464, instead of gqam.config, for the GQAM configuration file. If the site you have upgraded uses a custom configuration file, and if you are now ready to use the default configuration file again, you need to update the configuration file settings for your headend equipment.

The following list includes the default configuration files for the QAM-family of devices:

- QAM — /var/lib/tftpboot/qam.config
- GQAM — /var/lib/tftpboot/gqam.config
- GOQAM —/var/lib/tftpboot/goqam.config
- MQAM — /var/lib/tftpboot/mqam.config

CAUTION:

Failure to update the configuration file(s) results in the device remaining in the uniquely specified configuration. The device will not load new code. Instead, it will continue to load the code specified in the custom configuration file.

If the headend device fails to load the code you intended it to receive, check to see if either a unique file was specified in the EC Web UI or in the /var/lib/tftpboot file before contacting Cisco Services for assistance.

Which Reset Method to Use

Resetting the QAM-family of modulators from the EC Web UI or the front panel can be time consuming. If you have several modulators to reset, consider using the auditQam utility. The auditQam utility takes, as an argument, the IP address of the modulator that you want to reset. While the auditQam utility script runs, you are free to complete other upgrade-related tasks.

To reset modulators, go to one of the following sections:

- ***Resetting Modulators Through the EC WUI*** (on page 93)
- ***Resetting Modulators Through the Modulator Panel*** (on page 95)
- ***Resetting Modulators Through the auditQam Utility*** (on page 97)

Resetting Modulators Through the EC WUI

When you reset the modulators, the modulators download their new SR 8.0 code. Follow these instructions to reset the modulators through the EC WUI.

Important: Never reset more than four modulators at a time or the EC may become overloaded. The following instructions alert you to this important point at the appropriate step.

1 Follow these instructions to record the Session Count, the Program Count, and the IP address of your modulators.

Note: Skip this step for any modulator used for video-on-demand (VOD).

a Press the **Options** button on the front panel until the Session Count total appears.

b Record the Session Count on a piece of paper.

Note: Press the **RF Select** button to access each component of the MQAM and GQAM.

c Press the **Options** button on the front panel until the **Program Count** total appears.

d Record the Program Count on a piece of paper.

Note: Press the **RF Select** button to access each component of the MQAM and GQAM.

e Press the **Options** button on the front panel until the **IP address** appears.

f Record the IP address on a piece of paper.

Note: Press the RF Select button to access each component of the MQAM and GQAM.

g Repeat these steps for all of your modulators.

2 From the EC Web UI, click the **Navigation** button,  , and then select **Network Element Provisioning > QAM**.

3 Click **QAM**.

Result: The QAM List window opens.

4 Click **By Field** and select **All**.

5 Click **Show**. All provisioned QAM modulators on the system can now be accessed.

Note: If the **Security Warning** dialog box opens, click **Continue**.

6 From the QAM List window, choose a modulator.

Note: Refer to the QAM Type column to differentiate between types of modulators.

7 Click **Reset** at the bottom of the page. A confirmation message appears.

8 Click **OK** in the confirmation message.

Result: The modulator resets.

9 Repeat steps 6 through 8 for up to three additional modulators and then go to the next step.

Important: Never reset more than four modulators at a time as it may overload the EC.

Note: In step 11, you will have the opportunity to reset additional modulators.

10 Wait a few minutes and as dncs user, enter the following command to ping modulator you just reset.

Command Syntax:

```
ping [IP address of modulator]
```

Example:

```
[dncs@vodwater ~]$ ping 192.10.2.4
```

Important: Make sure to use the actual IP address for the specific modulators in your system when running this command.

Note: It may take up to 5 minutes for each modulator to reset.

11 Do you have additional modulators to reset?

- If **yes**, repeat steps 6 through 10 as many times as necessary until all of your modulators have been reset, and go to the next step.
- If **no**, go to the next step.

12 Did you record the Program Count and the Session Count for each modulator not used for VOD?

- If **yes**, repeat step 1 to verify that the Program Count and Session Count totals match what you recorded before resetting the modulators, and go to the next step.

  Important: If the Program Count and Session Count totals do not match what you recorded prior to resetting the modulators, call Cisco Services for assistance.

- If **no**, go to the next step.

13 Go to *Reset QPSK Modulators* (on page 98).

Resetting Modulators Through the Modulator Panel

When you reset the modulators, the modulators download the new SR 8.0 code. Follow these instructions to reset the modulators through the modulator panel.

1 Follow these instructions to record the **Session Count**, the **Program Count**, and the **IP address** of your modulators:

  Note: Skip this step for any modulator used for video-on-demand (VOD).

  a Press the **Options** button on the front panel until the **Session Count** total appears.

  b Record the **Session Count** on a piece of paper.

  c Press the **Options** button on the front panel until the **Program Count** total appears.

  d Record the **Program Count** on a piece of paper.

  e Press the **Options** button on the front panel until the **IP address** appears.

  f Record the **IP address** on a piece of paper.

  Note: Press the **RF Select** button to access each component of the MQAM and GQAM.

  g Repeat these steps 1a through 1f for all QAM, MQAM, and/or GQAM modulators.

2 Choose one of the following options:

- To reset an MQAM or GQAM modulator, go to the next step.
- To reset a QAM modulator, go to step 4.

3 To reset an MQAM or GQAM modulator, follow these instructions:

  a Press the **Options** button on the front panel until the **Reset** option appears.

  b Follow the instructions that appear alongside the Reset option.

  c Go to step 5.

4 To reset a QAM modulator, turn off the power switch on the back of the QAM modulator, wait a few seconds, and turn it back on.

5 Repeat steps 3 and 4 for up to three additional modulators, and then go to the next step.

Important: Never reset more than four modulators at once, or you may overload the EC.

Note: In step 7, you have the opportunity to reset additional modulators.

6 Wait a few minutes and as dncs user, enter the following command to ping each modulator that you reset.

Command Syntax:

```
ping [IP address of modulator]
```

Example:

```
[dncs@vodwater ~]$ ping 192.10.2.4
```

Note: It may take up to 5 minutes for each modulator to reset.

7 Do you have additional modulators to reset?

- If **yes**, repeat steps 3 through 6 as many times as necessary until all of your modulators have been reset, and then go to the next step.
- If **no**, go to the next step.

8 Did you record the **Program Count** and the **Session Count** for each modulator not used for VOD?

- If **yes**, repeat step 1 to verify that the **Program Count** and **Session Count** totals match what you recorded before resetting the modulators, and then go to next step.

  Important: If the **Program Count** and **Session Count** totals do not match what you recorded prior to resetting the modulators, call Cisco Services, for assistance.
- If **no**, go to the next step.

9 Go to ***Reset QPSK Modulators*** (on page 98).

Resetting Modulators Through the auditQam Utility

The *reset* option of the auditQam utility allows upgrade engineers to reset a modulator from the command line of the EC, a process that is usually quicker than resetting the modulator through the EC Web UI or modulator panel. If you have only a few modulators to reset, you can just type the IP address of the modulator as an argument to the `auditQam -reset` command. If you have many modulators to reset, consider creating a script. Instructions and guidelines for both situations follow.

Resetting a Few Modulators

If you want to reset only a few modulators, complete this procedure for each modulator:

1 As **dncs** user, type the following command and press **Enter.**

Command Syntax:

```
auditQam -reset [qam ip address or mqam ip address]
```

Example:

```
[dncs@vodwater ~]$ auditQam -reset 209.165.202.129
```

Result: The system shuts down and reinitializes the modulator.

Note: The system also performs an audit to ensure that the session list for the modulator matches the session list from the EC.

2 Repeat step 2 for each QAM modulator on your system.

Resetting Many QAM and MQAM Modulators

You frequently do not have time to manually reset hundreds of modulators from the EC Web UI. To save time, you can create a script that runs automatically. Refer to the following example for a sample script:

```
auditQam  -reset  192.0.2.1
sleep 1
auditQam  -reset  192.0.2.2
sleep 1
auditQam  -reset  192.0.2.3
sleep 1
auditQam  -reset  192.0.2.4
```

Important: Resetting a QAM interrupts all active sessions on the QAM for up to 10 minutes. Complete this task during a maintenance period whenever possible. Do not reset more than four modulators at a time.

Reset QPSK Modulators

Important Notice Regarding the Reset of QPSK Modulators

On occasion, for testing purposes, default configuration files for headend components are changed. For example, a site might substitute a file called qpskC70.config, instead of qpsk.config, for the QPSK configuration file. If the site you have upgraded uses a custom configuration file, and if you are now ready to use the default configuration file again, you need to update the configuration file settings for your headend equipment.

The default configuration file for the QPSK modulator is **/var/lib/tftpboot/qpsk.config**.

CAUTION:

Failure to update the configuration file(s) results in the device remaining in the uniquely specified configuration. The device will not load new code. Instead, it will continue to load the code specified in the custom configuration file.

If the headend device fails to load the code you intended it to receive, check to see if either a unique file was specified in the Web UI or in the /etc/bootptab file before contacting Cisco Services for assistance.

Resetting QPSK Modulators

Complete the following steps to reset your QPSK modulators.

Notes:

- You do not have to reset the QPSK modulators if the system you are upgrading is already operating with the new version of QPSK modulator code.
- You can also reset QPSK modulators through the back panel by turning the modulator off, waiting a few seconds, and turning it back on.

1. From the EC Web UI, click the **Navigation** button,  , and then select **Network Element Provisioning > QPSK**.
2. Use the **Filter > By Field** dropdown menu to select an option to display the appropriate QPSKs on the system. Then click **Show**.
3. Click the button next to the appropriate QPSK modulator.
4. Click **Reset** at the bottom of the Web UI window. A confirmation message appears.
5. Click **OK** to confirm the reset. The QPSK modulator resets.
6. Wait about 15 minutes and repeat steps 3 through 5 until all of your QPSK modulators have been reset.

CentOS cron and anacrontab Overview

By default, CentOS includes the following three installed cron packages:

- cronie-[VERSION].x86_64
- cronie-anacron-[VERSION].x86_64
- crontabs-[VERSION].noarch

Both cron and anacron are daemons that can schedule execution of recurring tasks to a certain point in time defined by the user.

The main difference between cron and anacron is that cron assumes that the system is running continuously. If your system is off and you have a job scheduled during this time, the job will not be executed.

On the other hand, anacron is designed for systems that are not running 24x7. For it to work, anacron uses time-stamped files to find out when the last time its commands were executed. Also, anacron can only run a job once a day, but cron can run as often as every minute.

For example, assume there is a power failure or scheduled maintenance on your system from 3:00AM to 5:00AM. cron.daily is set by default to run at 3:45AM. In this case, cron could not perform tasks such as logrotate. However, with anacron, this daemon takes over the task and runs the cron job after the machine is up again (i.e. at 5:00AM).

For additional info about anacron, please refer to the man pages by entering the following command as admin user: `man anacron`

cron and anacron Features

cron Features:

- Minimum granularity is in minutes (i.e. jobs can be scheduled to be run every minute).
- Can be scheduled by any normal user (not restricted for the super user).
- Expects systems to be running 24x7.

  Note: If a job is scheduled and the system is down during that time, the job is not executed.
- Desirable when a job needs executed at an exact hour and minute

anacron Features

- Minimum granularity is only daily.
- Can be used only by the super user.

  Note: Workarounds exist to enable use by normal users.
- Does not expect system to be running 24x7.

  Note: If a job is scheduled and the system is down during that time, the job executed when the system comes back up.
- Desirable when a job does not need executed at a precise hour and minute of the day.

Default cron Jobs in SR 8.0

The following list identifies the default cron jobs in this release.

- /etc/cron.daily/cups
- /etc/cron.daily/doctor.cron file
  (/etc/cron.daily/doctor.cron is not owned by any package)
- /etc/cron.daily/logrotate
- /etc/cron.daily/makewhatis.cron
- /etc/cron.daily/mlocate.cron
- /etc/cron.daily/prelink
- /etc/cron.daily/readahead.cron
- /etc/cron.daily/tmpwatch
- /etc/cron.d/raid-check
- /etc/cron.d/sysstat
- /etc/cron.hourly/0anacron
- /etc/cron.monthly/readahead-monthly.cron

Verifying the crontab Entries Managed by cron

Verifying the crontab Entries

After upgrading, inspect the crontab file in the keyFiles.staging directory on the EC.

Important: All EC 7.x cron jobs are not migrated over to cron. They are only copied to the staging directory.

Examining the CED.in Entry

Our engineers developed the dbOptimizer program to delete EMMs that are no longer needed by DHCTs. dbOptimizer runs as a cron job. The cron job can be found in /etc/cron.d/dbOptimizers.

Most EMMs are assigned to DHCTs during the staging process when DHCTs are prepared for deployment in the homes of subscribers. These EMMs are also stored in the database of the EC. When a DHCT has been successfully staged, those EMMs associated with the staging process are no longer needed and should be removed from the EC database. The dbOptimizer program is configured to run by default each Saturday at 4 AM.

The /dvs/dncs/bin/CED.in file in the EC contains a value that represents a number of *days*. The dbOptimizer program is designed to delete unneeded EMMs that are older than the number of days specified in the CED.in file.

In this procedure, you will examine and change, if necessary, the number of days specified in the CED.in file.

Note: Our engineers recommend the default value of 90 days.

1 As **admin** user on the EC, type the following command and press **Enter**. The system displays the number of days that EMMs are retained. EMMs older than this number of days are deleted by the dbOptimizer program when it runs each Saturday.

```
[admin@vodwater ~]$ sudo cat /dvs/dncs/bin/CED.in
```

2 Are you satisfied by the number of days specified by the CED.in file?

- If **yes**, go to the next section.
- If **no**, go to the next step to edit the CED.in file.

3 Type the following command and press **Enter**. The system changes the value stored in the CED.in file.

Command Syntax:

```
echo [new # of days] > /dvs/dncs/bin/CED.in
```

Example:

```
[admin@vodwater ~]$ sudo echo 90 > /dvs/dncs/bin/CED.in
```

Verify the crontab Entries

Adding Custom crontab Entries

Important: The dncs user can no longer manage cron entries. In EC 7.x, the dncs user could manage the timing of tools such as clearDbSessions, manage_SDVLog, dbOptimizer, manage_pim_files, and updatedsteffyear.sh as they were a part of the dncs cron. In EC 8.0, these tools are managed in /etc/cron.d and the files are owned by root. This limits the ability of a dncs/ec administrator from modifying them to suit site needs. BR CSCve78465 addresses this issue.

Examine old crontab entries for each user on the DBDS system (dncs, root, informix). Then consult with the system operator to determine whether any of these old entries should be retained. If necessary, add the required crontab entries to the current crontab file.

Important:

- Be careful when migrating cron entries as some cron jobs in SR 8.0 reside in /etc/cron* directories and not just those in the crontab file itself. For example, dbOptimizer is in the crontab file in SR 7.0 but in the /etc/cron.d/dbOptimizer file in SR 8.0.
- Do not add RepDB cron jobs as these are added when enabling RepDB.

Note: If you migrate a crontab entry that is also present in one of the /etc/cron* directories, you will likely cause the cron job to run more often than you intended.

1. As **root** user, enter the following command to change to the crontabs directory.

   ```
   [root@vodwater ~]# cd
   /disk1/keyfiles_staging/var/spool/cron/crontabs
   ```

2. Type the following command to open the **root** crontab file.

   ```
   [root@vodwater crontabs]# less root
   ```

   Result: The system displays the contents of the pre-upgrade root crontab file.

3. In another terminal window as **root** user, type the following command and press **Enter**. The system displays the contents of the current root crontab file.

   ```
   [root@vodwater crontabs]# crontab -l
   ```

4. Compare the pre-upgrade and post-upgrade crontab entries. If the pre-upgrade crontab file contains site-specific, unique entries, consult with the system operator regarding whether those entries are still needed.

5 Are there unique crontab entries that need to be retained?

- If **yes**, complete the following steps to update the root crontab file:
  - **a** Type the following command and press **Enter** to copy the root crontab file to **/tmp/root.cron**.
    ```
    [root@vodwater crontabs]# crontab -l > /tmp/root.cron
    ```
  - **b** Type the following command and press **Enter** to edit the **root.cron** file.
    ```
    [root@vodwater crontabs]# vi /tmp/root.cron
    ```
  - **c** Add any unique entries to the **/tmp/root.cron** file and then save and close the file.

    Note: Some directory paths have changed from SR 7.x to SR 8.0. Make sure you verify the paths.

    Important: Be careful when migrating cron entries as some cron jobs in SR 8.0 reside in /etc/cron* directories and not just those in the crontab file itself. For example, dbOptimizer is in the crontab file in SR 7.0 but in the /etc/cron.d/ directory in SR 8.0.
  - **d** Type the following command and press **Enter**. The edited /tmp/root.cron file becomes the new root crontab file.
    ```
    [root@vodwater crontabs]# crontab /tmp/root.cron
    ```
  - **e** Type the following command and press **Enter** to verify that the crontab file properly contains the unique entries.
    ```
    [root@vodwater crontabs]# crontab -l
    ```
- If **no**, go to step 6.

6 Type the following command and press **Enter** to change to the informix user.
```
[root@vodwater ~]# su informix
```

7 Repeat steps 2 through 5 for the informix crontab file.

8 Type `exit` and press **Enter** to close the informix user session and return to the root user session.

9 As **dncs** user, repeat steps 2 through 5 for the dncs crontab file.

10 Enter the following command to verify that cron is running.
```
[admin@vodwater crontabs]$ service crond status
```
Example Output:
```
crond (pid  4682) is running...
```
Note: If cron is not running, enter the following command to start crond as **admin** user,
```
[admin@vodwater crontabs]$ sudo service crond start
```
Example Output:
```
Starting crond:                OK
```

Verify the Upgrade

Go to Appendix B, ***System Verification Procedures*** (on page 165) to verify the upgrade.

Set the Clock on the TED (Optional)

1. In a **root** remote terminal window, type `date` and press **Enter**. The system date and time appear.
2. Write down the system date and time in the space provided.

   System Date: _____

   System Time: _____
3. What type of TED is installed at the site you are upgrading?
   - If it is a TED-FX, type the following command and press **Enter**:

     `telnet dncsted`
   - If it is a TED-3 or TED-4, type the following command and press **Enter**:

     `ssh dncsted`
4. Login as **root** user and press **Enter**. Then enter the password when prompted. You are logged onto the TED as root user.
5. Type `date` and press **Enter**. The TED date and time appear.
6. Compare the time results from step 1 with step 5. Do the date, time, and timezone on the EC and TED match?
   - If **yes**, go to step 9.
   - If **no**, go to the next step.
7. At the prompt, type `date [mmddhhmm]` and press **Enter**.

   Example: `date 07172017`

   Notes:
   - The format for the date command is:
     - `mm` - month
     - `dd` - day
     - `hh` - hours in 24 hour format
     - `mm` - minutes
   - The command can be modified to include the year, the seconds, or both the year and seconds.

   Examples:
   - The **date 073123162017** includes the year.
   - The **date 07132316.30** includes the seconds.
   - The **date 071323162017.30** includes the year and seconds.

8 Type `date` again and press **Enter**. Verify that the correct time now appears.

9 Type `/sbin/clock -r` and press **Enter**. The time on the hardware clock appears.

10 Type `/sbin/clock -w` and press **Enter**. This command writes the system time to the TED hardware clock.

11 Type `/sbin/clock -r` and press **Enter**. Verify the time is synchronized between the system and the TED hardware clock.

12 Type `exit` and press **Enter** to log out of the TED.

Confirm Third-Party BFS Application Cabinet Data

In this procedure, you will check to make sure that all third-party BFS application cabinet data is present following the upgrade.

Note: You need the sheet of paper that you used to record third-party BFS application cabinet data when you completed ***Recording Third Party BFS Application Cabinet Data*** (on page 19).

1 From the EC Web UI, click the **Navigation** button, and then select **App Interface Modules > BFS Client**. The Site DNCS Broadcast File Server List window appears.

2 Refer to the sheet of paper that you used when you completed ***Recording Third Party BFS Application Cabinet Data*** (on page 19). Are there any third-party BFS application cabinets that were present before the upgrade and are now missing after the upgrade?

- If **yes**, create a cabinet for each of the missing third-party applications using the Broadcast File Server List window that is open.
  - **a** Click **Add Server**. The Add Server window opens.
  - **b** Click the **Server Name** dropdown arrow and select the appropriate server.
  - **c** Click the appropriate **Mode** checkbox (**1-way** or **2-way**).
  - **d** From the **Available Sources** area, select the appropriate source.
  - **e** Click **Add** to move it to the **Selected Sources** column.
  - **f** Click **Save**.
  - **g** Repeat these steps for any additional third-party BFS application cabinets that are missing.
- If **no** (there are no missing third-party BFS application cabinets), continue with the next step.

3 Highlight each of the third-party application cabinets listed on the sheet of paper, in turn, and click **Edit**. The Edit Server window opens for the selected cabinet.

4 Examine the **Mode** field for the selected cabinet and verify that the correct mode (**1-way** or **2-way**) is checked.

5 Verify that the correct **Selected Sources** are present for the selected cabinet.

6 Click **Cancel** to close the Edit Server window when you are finished.

Enabling RADIUS and LDAP (Optional)

To enable RADIUS or LDAP on your system, refer to ***Configuring RADIUS and LDAP Support Configuration Guide for Explorer Controller 8.0 and DTACS 5.0***.

Multicast CVT Support Feature (Optional)

If you plan to enable the Multicast CVT (Code Version Table) feature on the EC, the GQAM code must be version 4.7.0. If it is not version 4.7.0, you must download v4.7.0 to the GQAMs by resetting these devices.

Complete the following procedure to download the GQAM code from the EC to the GQAMs and to enable the Multicast CVT feature.

Important: Update the GQAM code ***prior*** to enabling the Multicast CVT feature.

1 Verify if v4.7.0 has been download to the GQAMs on the system.

- If the GQAM code is v4.7.0, go to Step 3.
- If the GQAM code is ***not*** v4.7.0, go to the next step.

2 Reset the GQAMs using one of the following methods.

Note: For detailed steps to reset your GQAMs, refer to ***Reset the Modulators*** (on page 92).

- From the EC Web UI
- From the front panel of the modulators
- From the command line using the auditQam utility

3 When the reset completes, contact Cisco Services to enable the Multicast CVT feature.

8

Configure and Operate the Replicated Database

The Replicated Database package, sometimes referred to as RepDB, is comprised of the following two components:

- The IBM Informix Dynamic Server Data Replication for the database.
- The rsync utility — a fast and versatile remote file-copying tool for user-defined files.

Data replication allows a copy of the database from a primary server to be maintained on a secondary server. When activated, the primary database server continuously replicates data between itself and the secondary server by sending copies of the logical-log transactions to the secondary database server.

The rsync utility allows a copy of selected files and directories from a primary server to be maintained on a secondary server. When activated, the rsync utility periodically synchronizes the primary server to the secondary server.

In This Chapter

Prerequisites for RepDB

Important: Your system environment must have a second UCS platform with VMware installed and an EC 8.0 virtual machine configuration.

- ESXi host standalone license or vCenter server license.
- VMware ESXi (5.5 or later) and vCenter infrastructure (software, license and a running vCenter machine).
- vCenter login must have admin privileges to deploy and clone VMs.
- Network connectivity between the operational EC and the new virtual machine.
- Use the existing network ports (vSwitches) that were defined when installing or migrating the SR 8.0 EC.
  - EC 8.0 Mapping
    - NET0 – vSwitch0 – Corp/Engineering Network

      Important: By default, DHCP is enabled on the eth0 NET0-vSwitch0-Corp network. If DHCP is not available, then static an IP address, netmask, gateway, and DNS information is required.
    - NET1 – vSwitch1 – Headend (HE) Network
    - NET2 – vSwitch2 – TED Network
    - NET3 - vSwitch3 - RepDB

Overview of the Replicated Database Package

This section describes the Replicated Database package and lists some of the advantages and limitations associated with the package. This section also introduces the hardware platforms that are compatible with the Replicated Database, as well as the system release software requirements.

RepDB Package and Components

The RepDB package consists of the following two components:

- The IBM Informix Dynamic Server Data Replication for the database.
- The rsync utility — a fast and versatile remote file-copying tool for user-defined files.

The data replication component allows a copy of the Informix database to be maintained on another server. When the data replication component is active on a system, data is copied between a primary database server and a secondary database server. The primary database server continuously replicates data between itself and the secondary server by sending copies of the logical-log transactions to the secondary database server.

The remote file copying component allows a copy of user-defined files to be maintained on another server. When RepDB is enabled, remote file copying becomes active as a cron entry is added to the root crontab file. According to the cron entry, files and directories are periodically synchronized from the primary server to the secondary server.

Advantages of RepDB

The following are some of the advantages of enabling the Replicated Database on a system:

- Service-impacting events are reduced on the primary server by allowing third-party database query tools to access the secondary database server.
- The secondary server provides a flexible platform for developing new tools. Furthermore, if the secondary server has access to the Digital Broadband Delivery System (DBDS), it can be used by third-party tools that require both database and network access.
- The secondary server, at the operator's command, can be converted to the primary server, if needed.

Limitations of the Replicated Database

RepDB includes the following inherent limitations:

- The Replicated Database is read-only. The Replicated Database cannot be used for database backups because a database backup is considered a write process.
- There is a minor time delay between changes made to the primary database and those changes being reflected on the secondary server.
- Automatic failover — the ability to re-route users and applications to the Replicated Database with minimal interruption — is not supported. Failover requires manual intervention.
- Regular backups of the primary database server are still required. Database corruption in the primary server, if it occurs, will be copied to the secondary server while the Replicated Database is active.

Replicated Database and Failover

The Replicated Database package contains tools that maintain a synchronized file system between the primary and secondary server. It also contains tools that assist in the conversion of the secondary server to a live server, if necessary. Therefore, using this configuration, the secondary server has the capability to become the active server.

Note: For failover procedures, refer to the ***Replicated Database Operator's Guide***.

To achieve this configuration, the secondary server must meet the following conditions:

- Run the same system release software and Linux OS version as the primary server.
- Exactly match the hardware configuration of the primary server.

In addition, both the primary and secondary servers must include the following conditions:

- Both servers must be a UCS C240 M3 or UCS C240 M4 server.
- Both servers require network connectivity to one another, as well as to the network.
- In environments with a single TED, the operator will need to physically connect the TED to the secondary server as part of the failover process.

Setup Replicated Database

Important: If you are using a vSphere ESXi client to deploy VMs, refer to ***Setting Up RepDB Using an ESXi Client*** (on page 209).

This section provides instructions to set up RepDB by cloning the primary VM into a secondary VM. Review the following two methods to determine how you will clone the *primary* VM.

Note: Cisco recommends cloning the VM during a maintenance window (primary VM shutdown).

- **Cloning when the Primary VM is shutdown**
  - Cloning occurs during a maintenance window
  - Billing Transactions and all EC updates are suspended during the cloning process
  - Go to ***Cloning When the Primary VM is Shutdown*** (on page 115)
- **Cloning while the Primary VM is powered on and running**
  - Cloning may cause EC performance issues depending on the size of the system
  - The primary EC will be processing transactions without the interruption of interactive services
  - Go to ***Cloning While the Primary VM is Running*** (on page 117)

Cloning When the Primary VM is Shutdown

Important: If a Network adapter 4 interface exists, right-click the VM in vSphere and select Edit Settings. Then ***delete this interface*** before you clone the VM as there is a known issue in VMware. The fourth interface will be re-added later.

Complete the following steps to clone HOSTA while the *primary* VM is shutdown.

Note: In this example, HOSTA is the *primary* EC.

1 As **admin** user on the *primary* EC, edit the **/etc/hosts** file to include the primary and secondary RepDB entries.

Note: You may substitute other names for HOSTA and HOSTB if you desire. However, these are the names that will be used throughout this guide.

```
[admin@berlin ~]$ sudo vi /etc/hosts
```

2 Save and close the file.

3 Enter the following command to verify the RepDB entries.

```
[admin@berlin ~]$ less /etc/hosts | grep -i host
```

Example Output:

```
172.16.3.131   HOSTA
172.16.3.132   HOSTB
```

4 As **dncs** user, enter the following commands stop system processes.

```
[dncs@vodwater ~]$ appStop
[dncs@vodwater ~]$ appKill
[dncs@vodwater ~]$ dncsStop
[dncs@vodwater ~]$ dncsKill
```

5 Stop all billing transactions and updates to the *primary* EC.

6 As **admin** user, type the following command to shutdown the *primary* EC.

```
[admin@berlin ~]$ sudo shutdown -h now
```

7 From the VMware vSphere Web UI, right-click the *primary* server and select **Clone to Virtual Machine**. The Clone Existing Virtual Machine window appears.

8 From the **Enter a name for the virtual machine** text box, enter a name for the *secondary* host.

9 Select the appropriate datastore and then click **Next**.

10 Select the compute resource (e.g., cluster, ESXi host) where the VM is to be cloned. A compatibility check occurs.

11 Once the compatibility check succeeds, click **Next**. The Select storage window appears.

12 Ensure the following settings exist and then click **Next**. The Select clone option window appears.

- The "Select virtual disk format" field is set to **Same format as source**.
- The correct datastore is selected.

13 Click **Next** again.

14 Review the settings and then click **Finish**.

15 Monitor the **Recent Tasks** area to verify that the cloned VM completed successfully.

16 When the VM clone completes, select and right-click the *primary* VM and select **Power On**.

17 From a terminal window, login as **ecadmin**.

18 As **dncs** user, enter the following commands to start the system processes.

```
[dncs@vodwater ~]$ dncsStart
[dncs@vodwater ~]$ appStart
```

19 Go to ***Configuring the Secondary Host After Cloning*** (on page 118).

Cloning While the Primary VM is Running

Important: If a Network adapter 4 interface exists, right-click the VM in vSphere and select Edit Settings. Then ***delete this interface*** before you clone the VM as there is a known issue in VMware. The fourth interface will be re-added later.

Complete the following steps to clone HOSTA while the *primary* VM is running.

Note: In this example, HOSTA is the *primary* EC.

1. As **admin** user on the *primary* EC, edit the **/etc/hosts** file to include the primary and secondary RepDB entries.

   Note: You may substitute other names for HOSTA and HOSTB if you desire. However, these are the names that will be used throughout this guide.

   ```
   [admin@berlin ~]$ sudo vi /etc/hosts
   ```

2. Save and close the file.
3. Enter the following command to verify the RepDB entries.

   ```
   [admin@berlin ~]$ less /etc/hosts | grep -i host
   ```

   Example Output:

   ```
   172.16.3.131   HOSTA
   172.16.3.132   HOSTB
   ```

4. From the VMware vSphere Web UI, right-click the *primary* server and select **Clone to Virtual Machine**. The Clone Existing Virtual Machine window appears.
5. From the **Enter a name for the virtual machine** text box, enter a name for the *secondary* host.
6. Select the appropriate datastore and then click **Next**.
7. Select the compute resource (e.g., cluster, ESXi host) where the VM is to be cloned. A compatibility check occurs.
8. Once the compatibility check succeeds, click **Next**. The Select storage window appears.
9. Ensure the following settings exist and then click **Next**. The Select clone option window appears.
   - The "Select virtual disk format" field is set to **Same format as source**.
   - The correct datastore is selected.
10. Click **Next** again.
11. Review the settings and then click **Finish**.
12. Monitor the **Recent Tasks** area to verify that the cloned VM completed successfully.
13. When the VM clone completes, go to the next section.

Configuring the Secondary Host After Cloning

1 From the vSphere Web UI, right-click the *secondary* VM and select **Edit Settings**.

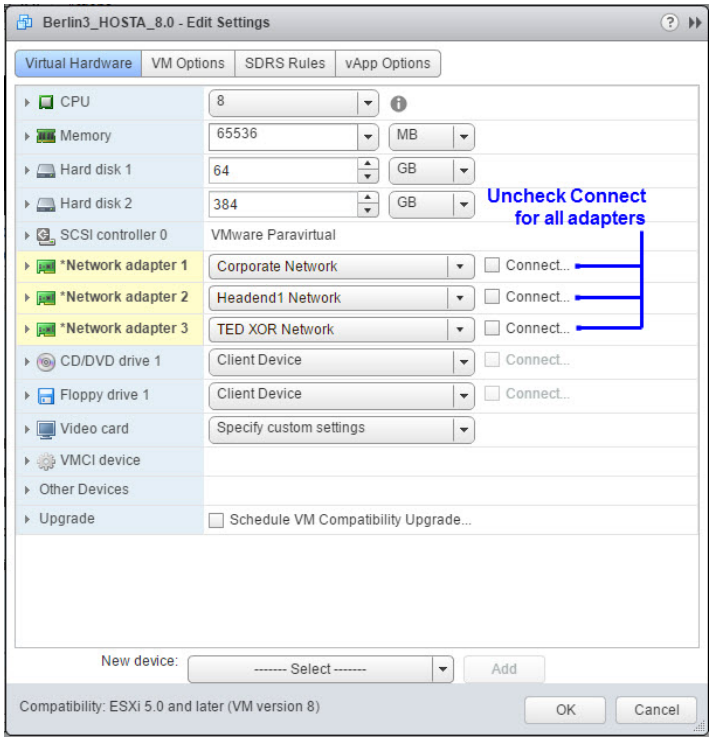
2 Uncheck the **Connect** box for all of the network adapters.

3 Does a **Network adapter 4** entry exist?

- If **yes**, go to Step 4.
- If **no**, go to Step 6.

4 Hover the mouse on the **Network adapter 4** entry. An "X" icon appears to the far right on that line.

5 Click the "X" to delete Network adapter 4.



6 Click **OK**.

7 Monitor the **Recent Tasks** area until the *secondary* VM is successfully reconfigured.

8 Right-click the *secondary* VM and select **Power On**.

9 Right-click the *secondary* VM again and click **Open Console**.

10 In the console window, login as **admin** user.

11 Enter the following command to delete the **70-persistent-net.rules** file.

```
[admin@berlin ~]$ sudo rm
/etc/udev/rules.d/70-persistent-net.rules
```

12 When prompted to confirm the removal of the file, type **y**.

```
[root@berlin rules.d]# rm /etc/udev/rules.d/70-persistent-net.rules
rm: remove regular file `/etc/udev/rules.d/70-persistent-net.rules'? y
[root@berlin rules.d]#
```

13 Enter the following command to verify that the interfaces are mapped correctly.

```
[admin@berlin ~]$ ls -latr
/etc/sysconfig/network-scripts/ifcfg*
```

14 Does an **ifcfg-eth3** file exist?

- If **yes**, go to the next step.
- If **no**, and the interfaces are mapped correctly, go to Step 17.

```
-rw-r--r--. 1 root root 118 Jun 13 16:53 /etc/sysconfig/network-scripts/ifcfg-eth1
-rw-r--r--. 1 root root 113 Jun 13 16:53 /etc/sysconfig/network-scripts/ifcfg-lo:1
-rw-r--r--. 1 root root 119 Jun 13 16:53 /etc/sysconfig/network-scripts/ifcfg-eth2
-rw-r--r--. 1 root root 214 Jun 13 20:52 /etc/sysconfig/network-scripts/ifcfg-eth0
-rw-r--r--. 1 root root 254 Jun 13 20:52 /etc/sysconfig/network-scripts/ifcfg-lo
```

15 Enter the following command to delete the **ifcfg-eth3** file.

```
[admin@berlin ~]$ sudo rm
/etc/sysconfig/network-scripts/ifcfg-eth3
```

16 When prompted to confirm the deletion of the file, enter **y** and press **Enter**.

17 Do you want the *secondary* VM accessible remotely and/or the Admin Node to only be reachable on the Corporate Network?

- If **yes**, go to Step 18.
- If **no**, you have completed this procedure. Go to ***Configure RepDB*** (on page 121).

18 Enter the following command to open the **ifcfg-eth0** file in a text editor.

```
[admin@berlin ~]$ sudo vi
/etc/sysconfig/network-scripts/ifcfg-eth0
```

19 From the **IPADDR** line, modify the IP address, as it should be unique to the IP address of the primary VM.

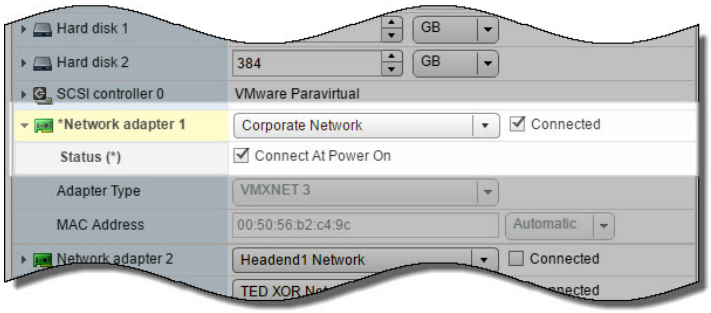
20 Save and close the file.

21 Open the **/etc/hosts** file in a text editor and update the IP to the IP address you configured in Step 19.

22 Save and close the file.

23 From the vSphere Web UI, right-click the *secondary* VM and select **Edit Settings**.

24 From the **Network adapter 1** (corporate network) row, click the **Connected** and **Connect At Power On** boxes and then click **OK**.



25 From the console window, type **reboot** to reboot the *secondary* server.

26 From a terminal window, log into the *secondary* VM as **admin** user.

27 Enter the following command to verify that the interfaces are mapped properly.

```
[admin@berlin ~]$ ifconfig -a
```

28 Go to ***Configure RepDB*** (on page 121).

Configure RepDB

Complete the following procedures to configure the RepDB network on the primary and the secondary servers.

Adding the RepDB Network Adapter on the Primary and Secondary VMs

Complete the following procedure to add a network adapter for RepDB to the primary and the secondary EC.

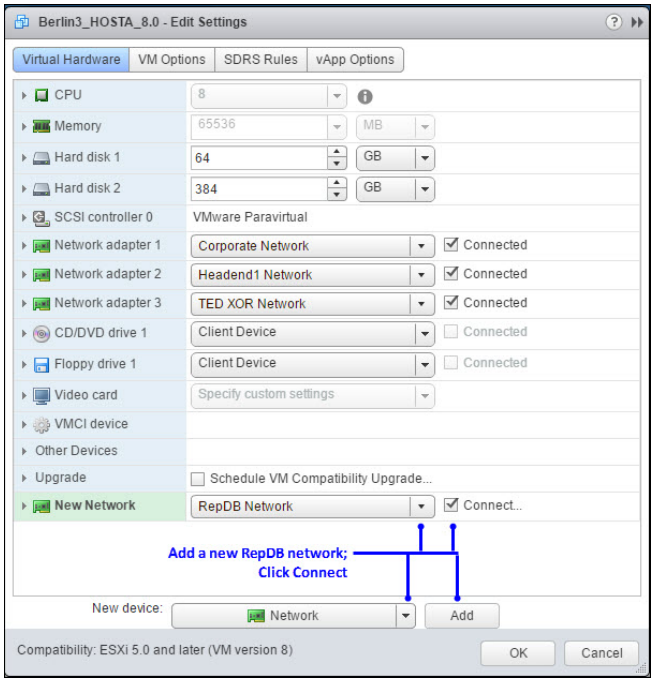
1 From the vSphere Web UI, right-click the *primary* VM and select **Edit Settings**.

2 From the **New device** dropdown menu, select **Network** and then click **Add**. A New Network entry is added to the Virtual Hardware list.

3 From the **New Network** dropdown menu, select the appropriate replicated database network label.

4 Ensure the **Connect** check box is selected.

Example: Primary EC



5 Click **OK**. The VM is reconfigured.

6 Monitor the **Recent Tasks** area until the task is completed.

7 Right-click the *secondary* VM and select **Edit Settings**.

8 From the **New device** dropdown menu, select **Network** and then click **Add**. A New Network entry is added to the list of Virtual Hardware.

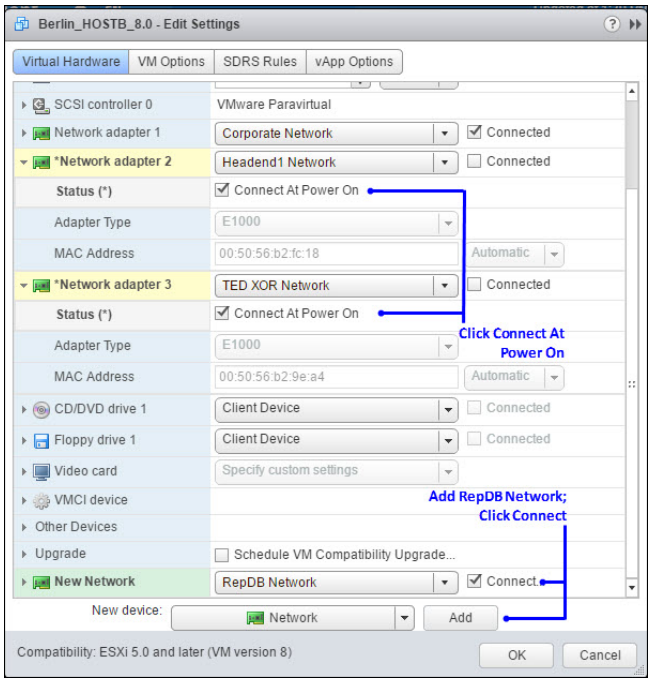
9 From the **New Network** dropdown menu, select the appropriate replicated database network label.

10 Ensure the **Connect** check box is selected.

11 Click the arrow adjacent to **Network adapter 2** and **Network adapter 3**. The configuration for each adapter displays.

12 For each adapter, click the **Connect At Power On** check boxes.

Example: Secondary EC



13 Click **OK**. The VM is reconfigured.

14 Monitor the **Recent Tasks** area until the task is completed.

15 Did you upgrade from SR 8.0.x to SR 8.0.y?

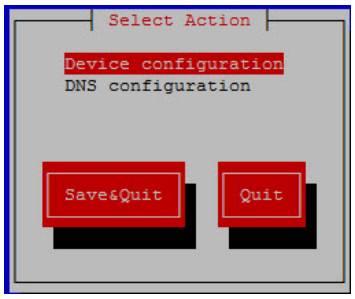
- If **no**, go to the next section.
- If **yes**, go to *Enabling RepDB* (on page 127).

Creating an Interface Configuration File for RepDB

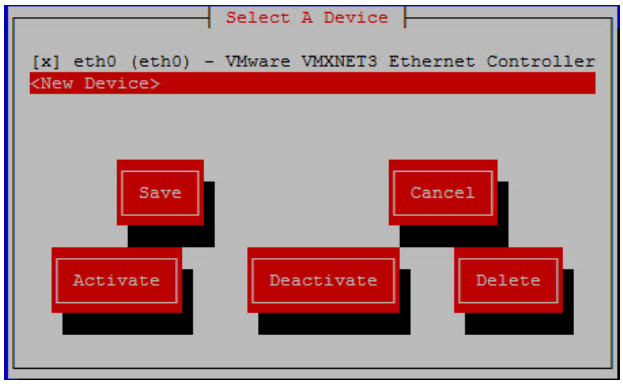
Complete the following steps to add a network interface for RepDB.

1 As **admin** user on the *primary* EC, enter the following command to configure the RepDB (eth3) interface. The Select Action window displays.

```
[admin@berlin ~]$ sudo system-config-network
```

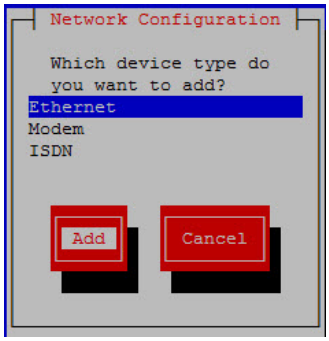


2 With Device configuration selected, press **Enter**. The Select a Device window displays.



3 Press the down arrow key on your keyboard to highlight **<New Device>** and then press **Enter**. The Network Configuration window displays.

4 With **Ethernet** highlighted, press the **Tab** key until **Add** is highlighted; then press **Enter**.



5 In the **Name** text box, type **eth3** and then press **Tab**.

6 In the **Device** text box, type **eth3** and then press **Tab** twice.

7 In the **Static IP** field, type the IP address for the RepDB interface and then press **Tab**.

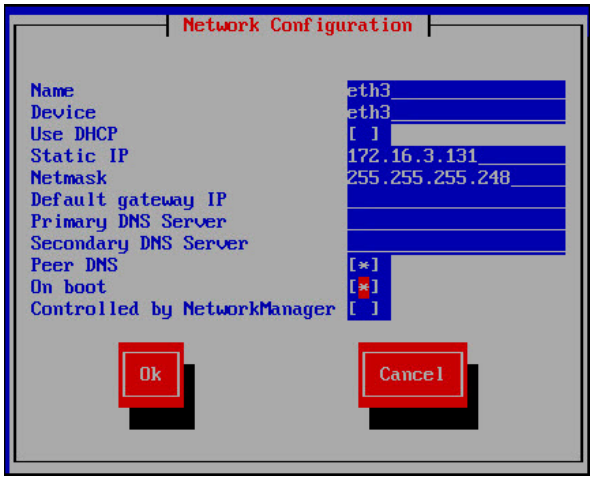
8 In the **Netmask** field, type the netmask for the RepDB interface.

9 Press the **Tab** key until your cursor is in the **Peer DNS** field.

10 Press the **spacebar** to select this option. An asterisk, *, appears in the field.

11 Press the **Tab** key until your cursor is in the **On boot** field.

12 Press the **spacebar** to select this option. An asterisk, *, appears in the field.



13 Press the **Tab** key until the **Ok** button is highlighted and then press **Enter**. You are returned to the Select a Device window.

14 Press the **Tab** key until **Save** is highlighted and then press **Enter**. You are returned to the Select Action window.

15 Press the **Tab** key until **Save&Quit** is highlighted and then press **Enter**. The network configuration menu closes and you are returned to the admin user prompt.

16 Open the **ifcfg-eth3** file in a text editor.

```
[admin@berlin ~]$ sudo vi
/etc/sysconfig/network-scripts/ifcfg-eth3
```

17 Delete the **HWADDR** line.

18 Save and close the file.

19 Enter the following command to bring the eth3 interface up.

```
[admin@berlin ~]$ sudo /etc/sysconfig/network-scripts/ifup
eth3
```

20 Repeat Steps 1 through 19 on the *secondary* EC.

Note: Make sure you define the IP address for the *secondary* EC.

21 Test the connection between the hosts.

On HOSTA

```
[admin@berlin ~]$ ping HOSTB
```

On HOSTB

```
[admin@berlin ~]$ ping HOSTA
```

22 Can the two hosts ping each other?

- If **yes**, go to the next procedure.
- If **no**, go back over the steps in this procedure to review configurations and settings.

Setting Up SSH Login Between the EC Servers Without a Password

Complete this procedure to setup password-less SSH access between the primary and the secondary EC. This will enable RepDB features to function properly.

1 As **admin** user on the *primary* EC, enter the following command to generate SSH keys for the admin user.

Note: The keys will be saved as id-rsa-pub (public) and id-rsa (private) files in the /export/admin/.ssh directory.

```
[admin@berlin ~]$ ssh-keygen
```

2 When prompted for the location to save the key, press **Enter** to accept the default.

3 Did an **Overwrite (y/n)?** message display?

- If **yes**, enter **y** and press **Enter**. Then go to the next step.
- If **no**, go to the next step.

4 When prompted for the passphrase, press **Enter** to leave this field empty.

5 When prompted to re-enter the passphrase, press **Enter**. The public and private keys are generated and saved in the **/home/admin/.ssh** directory.

```
[admin@berlin ~]$ ssh-keygen <-----generate keys
Generating public/private rsa key pair.
Enter file in which to save the key (/home/admin/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/admin/.ssh/id_rsa.
Your public key has been saved in /home/admin/.ssh/id_rsa.pub.
The key fingerprint is:
b4:7e:0c:43:b6:07:be:e1:f2:13:ee:22:59:74:42:13 admin@berlin
The key's randomart image is:
+--[ RSA 2048]----+
|      E.         |
|      o          |
|     . .=        |
|      o=.+       |
|     . oS .      |
|      .o.B       |
|     o..+.o      |
|    o .oo.       |
|     . oo.       |
+-----------------+
```

6 Enter the following command to copy the keys to the *secondary* EC.

Note: The authorized_keys file is saved in the /home/admin/.ssh directory on the remote server.

Command Syntax:

```
ssh-copy-id [secondary_hostname]
```

Example:

```
[admin@berlin ~]$ ssh-copy-id HOSTB
```

7 When prompted to connect to the *secondary* VM, type **yes**.

8 When prompted for the password for the *secondary* VM, enter the password for that host.

```
[admin@berlin ~]$ ssh-copy-id HOSTB <-----Copy the keys to HOSTB
The authenticity of host 'hostb (172.16.3.132)' can't be established.
RSA key fingerprint is 07:a7:d6:24:ca:6d:38:1f:8b:0d:06:83:77:cb:f5:fc.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'hostb,172.16.3.132' (RSA) to the list of known hosts.

|---------------------------------------------------------------------|
| This system is for the use of authorized users only.                |
| To protect the system from unauthorized use and to ensure the       |
| system is functioning properly, activities on this system are       |
| monitored and recorded.                                             |
|                                                                     |
| Anyone using this system expressly consents to such monitoring      |
| and recording.  If such monitoring reveals possible                 |
| evidence of criminal activity, system personnel may provide the     |
| evidence of such monitoring to law enforcement officials and        |
| it could lead to criminal and civil penalties.                      |
|                                                                     |
| Please contact your system administrator for a login id.            |
|---------------------------------------------------------------------|

admin@hostb's password:
Now try logging into the machine, with "ssh 'HOSTB'", and check in:

  .ssh/authorized_keys

to make sure we haven't added extra keys that you weren't expecting.
```

9 Enter the following command on the *primary* host to test the password-less SSH connection to the secondary host.

```
[admin@berlin ~]$ ssh HOSTB
```

Result: You are logged into the *secondary* host without having to enter a password.

10 Type **exit** to close the session.

11 Repeat Steps 1 through 10 on the *secondary* EC.

Enabling RepDB

Complete the following steps to enable RepDB.

1. As **admin** user on the *primary* EC, enter the following command to change to the **/opt/cisco/repdb** directory.

   ```
   [admin@berlin ~]$ cd /opt/cisco/repdb
   ```

2. Enter the following command to configure RepDB.

   ```
   [admin@berlin repdb]$ sudo ./configRepDb
   ```

   Note: This can take up to 30 minutes or more, depending on the size of the database.

3. When prompted for the hostname of the *primary* node, enter the hostname (i.e. HOSTA) of the *primary* system's RepDB interface.

4. When prompted for the hostname of the *secondary* node, enter the hostname (i.e. HOSTB) of the *secondary* system's RepDB interface.

   Result: The system returns the hostnames and IP addresses for each system, as defined by the entries in the /etc/hosts file.

   ```
   [admin@berlin repdb]# sudo ./configRepDb
   Please enter the hostname for the repdb interface on the active node
   Primary hostname: HOSTA

   Please enter the hostname for the repdb interface on the standby node
   Secondary hostname: HOSTB

   Primary: HOSTA
   Primary IP:172.16.3.131
   Secondary: HOSTB
   Secondary IP:172.16.3.132

   Continue with these host settings? (y/n): y
   ```

5. Verify that the entries are correct and when prompted to continue, type **y**.

   Results: The RepDB environment is set up on the primary and the secondary hosts.

6. When prompted to run formatDbSpace on the *secondary* EC, type **y** and press **Enter**. The database setup begins and, if active database sessions are found, you are prompted to kill them.

7. Were you prompted to kill active database sessions?

   - If **yes**, type **y** and press **Enter**. Then go to the next step.
   - If **no**, go to the next step.

8 Observe the output and verify that Database Replication is successfully enabled on both systems and a **Replication has been SUCCESSFULLY ENABLED** message displays.

```
################################################################################
# NOTICE * NOTICE * NOTICE * NOTICE * NOTICE * NOTICE * NOTICE * NOTICE * #
################################################################################
Enabling database replication on HOSTA.
Successfully enabled Database Replication on HOSTA.
################################################################################
# NOTICE * NOTICE * NOTICE * NOTICE * NOTICE * NOTICE * NOTICE * NOTICE * #
################################################################################
Enabling database replication on HOSTB.
Successfully enabled Database Replication on HOSTB.
Created file /etc/no_system_start on the system.
Completed all tasks.
Database Replication has been ENABLED for the secondary server.

Replication has been SUCCESSFULLY ENABLED.
```

9 As **root** user, source the environment variables.

10 Type the following command and press **Enter** on the *primary* server. The output should indicate that the database is **On-Line (Prim)** and data replication is paired to the secondary server.

```
[root@berlin repdb]$ onstat -g dri
```

```
IBM Informix Dynamic Server Version 12.10.FC4W1XK -- On-Line (Prim) -- Up 00:25:37 -- 200
24820 Kbytes

Data Replication at 0x856ed028:
  Type          State        Paired server        Last DR CKPT (id/pg)    Supports Proxy
 Writes
  primary       on           HOSTBDbServer               13 / 11         NA

  DRINTERVAL   5
  DRTIMEOUT    15
  DRAUTO       0
  DRLOSTFOUND  /opt/cisco/informix/server/cisco/etc/dr.lostfound
  DRIDXAUTO    0
  ENCRYPT_HDR  1
  Backlog      5
  Last Send    2017/03/17 10:46:45
  Last Receive 2017/03/17 10:46:45
  Last Ping    2017/03/17 10:46:36
  Last log page applied(log id,page): 13,293
```

11 Repeat Step 9 on the *secondary* EC. The output should indicate that the database is **Read-Only (Sec)** and is paired to the primary server.

```
IBM Informix Dynamic Server Version 12.10.FC4W1XK -- Read-Only (Sec) -- Up 00:16:17 -- 20
024820 Kbytes

Data Replication at 0x856f2028:
  Type          State        Paired server        Last DR CKPT (id/pg)    Supports Proxy
 Writes
  HDR Secondary on           HOSTADbServer               13 / 11         N

  DRINTERVAL   5
  DRTIMEOUT    15
  DRAUTO       0
  DRLOSTFOUND  /opt/cisco/informix/server/cisco/etc/dr.lostfound
  DRIDXAUTO    0
  ENCRYPT_HDR  1
  Backlog      0
  Last Send    2017/03/17 10:52:55
  Last Receive 2017/03/17 10:52:55
  Last Ping    2017/03/17 10:52:43
  Last log page applied(log id,page): 0,0
```

12 Go to the next section to verify that RepDB is functioning properly.

Post RepDB Verifications

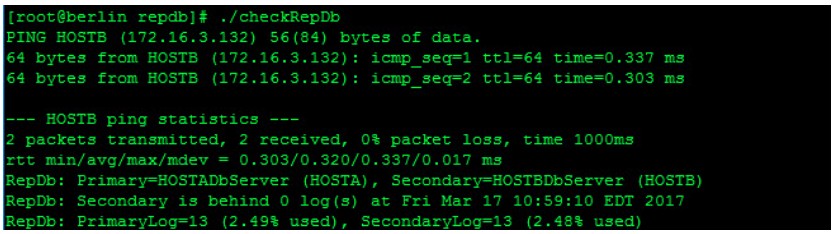
Verifying That RepDB is Running

Complete the following steps to verify that Data Replication from the primary server to the secondary server is functioning properly.

1 As **root** user, type the following command on the *primary* server.

```
[root@berlin repdb]# /opt/cisco/repdb/checkRepDb
```

Result: The system returns the status of the secondary server, the names of the primary and secondary servers, and the number of logs the secondary server is behind.



2 Repeat Step 1 on the *secondary* server.

Note: Ensure that you change to the /opt/cisco/repdb directory on the *secondary* server to run the checkRepDb script.

Verifying Remote File Copying

When the Replicated Database is enabled on the *primary* system, remote file copying is activated and key files are synced from the primary server to the secondary server.

Complete the following steps to verify that a cron job to sync key files between the remote servers is present and that the key file synchronization is functioning properly.

1 As **root** user, enter the following command to verify that the cron job is present on the *primary* host.

Note: This command synchronizes the key files twice an hour.

```
[root@berlin repdb]# crontab -l
```

Command Syntax:

```
15,45 * * * * /opt/SAIrepdb/syncKeyFiles -l [PRIMARY HOSTNAME]
-r [SECONDARY HOSTNAME] -n > /var/log/syncKeyFiles.out 2>&1
```

Example Output:

```
15,45 * * * * /opt/SAIrepdb/syncKeyFiles -l HOSTA -r HOSTB
-n > /var/log/syncKeyFiles.out 2>&1
```

2 Type the following command to verify the last modification time of the output from the syncKeyFiles crontab entry. The date and time should be several minutes after the passage of the syncKeyFiles cron event.

```
[root@berlin repdb]# ls -l /var/log/syncKeyFiles.out
```

3 Type the following command to view the output from the crontab entry. The status of the primary and secondary VMs and the ssh/scp between the servers is displayed.

```
[root@berlin repdb]# cat /var/log/syncKeyFiles.out
```

4 Review the KeyFiles2Sync log file to further check the status of the key file sync,

```
[root@berlin repdb]# less /var/log/KeyFiles2Sync.log
```

Editing the Key Files Sync File Lists

Complete these steps on the *primary* server to edit the list of files in the KeyFiles2Sync and the KeyFiles2Exclude files.

1 Type the following command on the *primary* server to edit the KeyFiles2Sync.list file in a text editor.

```
[root@berlin repdb]# vi /opt/cisco/repdb/KeyFiles2Sync.list
```

2 Add or delete any unique files, as needed.

Important:

- Do not add system-specific files, such as /etc/* or /dev/*, to this list. These files have the potential to disrupt the Replicated Database environment.
- Be certain to use absolute path names.
- When synchronizing links, do not add both the link and its target to the list. Instead, add only the link. Links are followed such that both the link and the file to which it points are synchronized.

3 Save and close the file.

4 Type the following command on the *primary* server to edit the KeyFiles2Exclude.list file in a text editor.

```
[root@berlin repdb]# vi /opt/cisco/repdb/KeyFiles2Exclude.list
```

5 Add or delete any unique files, as needed.

6 Save and close the file.

9

Customer Information

If You Have Questions

If you have technical questions, call Cisco Services for assistance. Follow the menu options to speak with a service engineer.

Access your company's extranet site to view or order additional technical publications. For accessing instructions, contact the representative who handles your account. Check your extranet site often as the information is updated frequently.

A

Hardware Configuration Procedures for the Cisco UCS C240

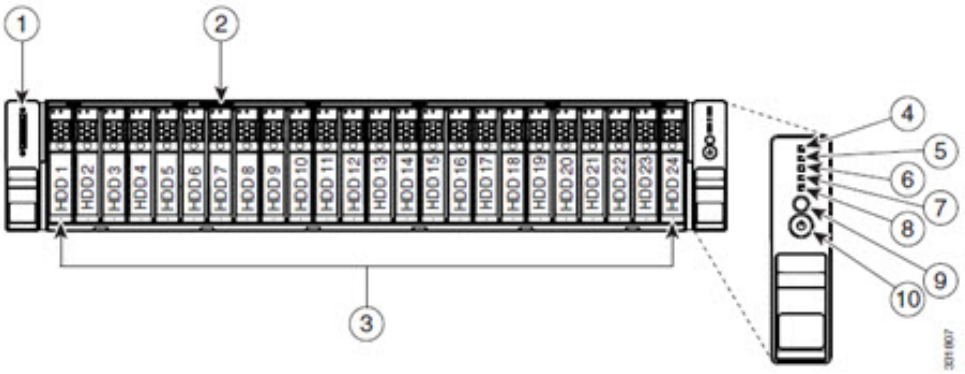
Introduction

This chapter contains procedures for configuring Cisco's UCS C240 M3 and UCS C240 M4 server for use with System Release 8.0.

In This Appendix

Hardware Diagram of the Cisco UCS C240 M3 Server

Chassis Front View

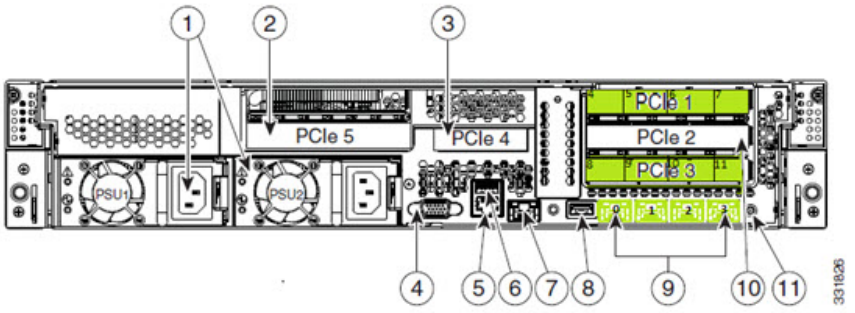


Slot	Description	Slot	Description
1	KVM connector (Used with KVM cable that provides two USB, one VGA, and one serial connector)	6	Temperature status LED
2	Asset tag (serial number)	7	Fan status LED
3	Drives (up to 24 2.5-inch hot-swappable drives)	8	System status LED
4	Network link activity LED	9	Identification button/LED
5	Power supply status LED	10	Power button/power status LED

Chassis Rear View

Important: Make sure that the network cards are installed in the slots shown in this diagram.

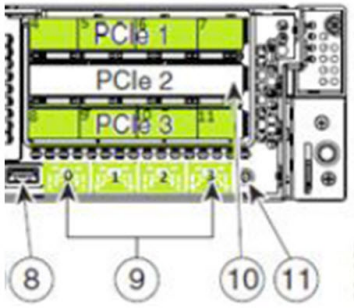
Note: Only the essential features of the rear panel are shown. A more detailed image follows.



Slot	Description	Slot	Description
1	Power supplies (up to two)	7	One RJ-45 10/100/1000 Ethernet dedicated management port
2	Standard-profile PCIe slot on riser 2: PCIe 5 - full height, 3/4-length, x16 lane width, x24 connector, GPU ready	8	USB 2.0 port
3	Low-profile PCIe slot on riser: PCIe 4 - half-height, 3/4-length, x8 lane width, x16 connector, no NCSI support	9	Quad 1-GB Ethernet ports (LAN1, LAN2, LAN3, LAN4)
4	VGA video connector	10	Standard-profile PCIe slots on riser 1 (three): ■ PCIe 1-full-height, half-length, x8 lane width, x8 connector ■ PCIe 2-full-height, half-length, x16 lane width, x24 connector (supports Cisco Virtual Interface Card (VIC) ■ PCIe 3-full-height, half-length, x8 lane width, x16 connector

Slot	Description	Slot	Description
5	Serial connector (RJ-45)	11	Rear identification button/LED
6	USB 2.0 port		

Detailed View of PCI Ports



- Top row contains ports 0, 1, 2, 3
- Middle row contains ports 4, 5, 6, 7
- Bottom row contains ports 8, 9, 10, 11

Tested Reference Configuration

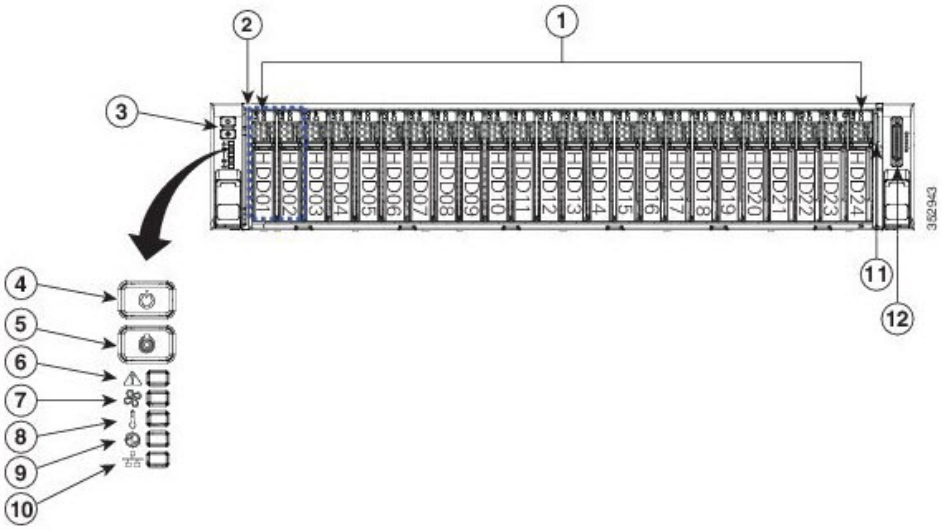
Network ports are numbered and marked as green. Cables should be run to the below designated ports.

- NIC Ports 1 and 7 — ESXi Management
- NIC Ports 8 and 4 — Headend network
- NIC Ports 9 and 5 — Corporate network
- NIC Ports 10 and 6 — RepDB network
- NIC Ports 2 and 11 — Headend 2 network (DSG)
- NIC Port 0 — TED crossover
- NIC Port 3 — Open

  Important: The DOCSIS Set-Top Gateway (DSG) network is only used if you have the licensed feature. Otherwise, these ports are unused at this time.

Hardware Diagram of the Cisco UCS C240 M4 Server

Chassis Front View

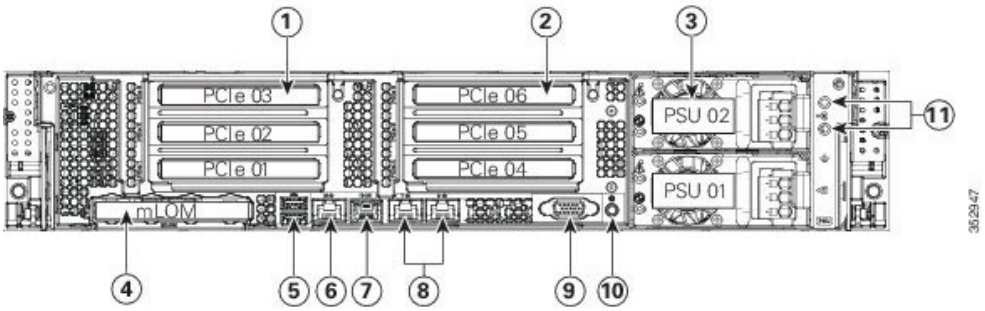


Slot	Description	Slot	Description
1	Drive bays 1-24 supports SAS/SATA drives	7	Fan status LED
2	Drive bays 1 and 2 supports NVMe PCIe SSDs and SAS/SATA drives	8	Temperature status LED
3	Operations panel buttons and LEDS Drives (up to 24 2.5-inch hot-swappable drives)	9	Power supply status LED
4	Power button/power status LED	10	Network link activity LED
5	Identification button/LED	11	Pull-out asset tag (serial number)
6	System status LED	12	KVM connector (Used with KVM cable that provides two USB, one VGA, and one serial connector)

Chassis Rear View

Important: Make sure that the network cards are installed in the slots shown in this diagram.

Note: Only the essential features of the rear panel are shown. A more detailed image follows.



Slot	Description	Slot	Description
1	PCIe riser 1 (slots 1, 2, 3*) * Slot 3 not present in all versions.	7	Serial port (RJ-45 connector)
2	PCIe riser 2 (slots 4, 5, 6)	8	Dual 1-Gb Ethernet ports (LAN1, LAN2)
3	Power supplies (DC power supply shown)	9	VGA video port (DB-15 connector)
4	Modular LAN-on-motherboard (mLOM) card slot	10	Rear Unit Identification button/LED
5	USB 3.0 ports (two)	11	Grounding-lug holes (for DC power supplies)
6	1-GB dedicated management port		

PCI Ports

- Bottom row contains ports 0, 1
- Top left row contains ports 2, 3, 4, 5
- Top right row contains ports 6, 7, 8, 9

Tested Reference Configuration

Network ports are numbered and marked as green. Cables should be run to the below designated ports.

- NIC Ports 1 and 7 — ESXi Management
- NIC Ports 8 and 4 — Headend network
- NIC Ports 9 and 5 — Corporate network
- NIC Ports 10 and 6 — RepDB network
- NIC Ports 2 and 11 — Headend 2 network (DSG)
- NIC Port 0 — TED crossover
- NIC Port 3 — Open

  Important: The DOCSIS Set-Top Gateway (DSG) network is only used if you have the licensed feature. Otherwise, these ports are unused at this time.

Hardware Requirements for a New UCS Install

The following hardware is required to install a new UCS server. This is in addition to the hardware requirements defined in ***Hardware Requirements*** (on page 2).

- KVM Cable Adapter (provided with the UCS)
- Standard USB Keyboard
- Monitor with a VGA cable
- A KVM with the appropriate adapters can be used in place of the monitor and keyboard

Cisco UCS C240 Server CIMC Configuration

Important:

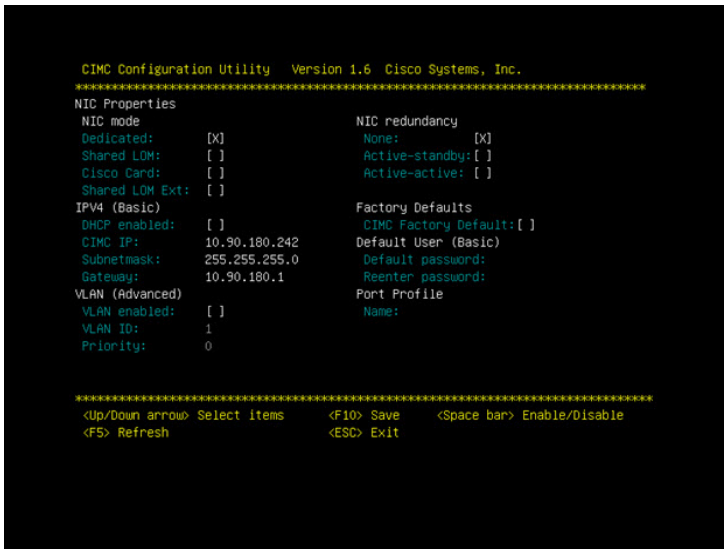
- This procedure is used for both the C240 M3 and C240 M4 servers and only needs to be performed once — when you initially install the server.
- Make sure that you use configuration data that pertains to the system that you are migrating. The screen-capture in Step 5 is to be referenced as an example only.

1. Obtain the ***UCS C240 Quick Start Guide***. This guide is shipped with the server.
2. Follow the instructions in the ***UCS C240 Quick Start Guide*** through step 5.
3. Press the **Power** button to power on the UCS C240 server.
4. Press **F8** at the Cisco screen. The server boots to the CIMC Configuration Utility window.

   Important: Note the BIOS Version on the Cisco splash screen as the system is booting.
5. Use the information in the CIMC Configuration Utility window to complete the configuration.

   Note: In addition to the information in the CIMC Configuration Utility window, make sure to obtain the network IP address for the CIMC interface.

   Important: The following image is an example only. Do not use the IP address, netmask, or gateway in the image.



6. Enter a default password and re-enter it at the prompt. Store this password in a safe place for future use.
7. Press **F10** to save changes.
8. Press **Esc** to exit. The EFI shell prompt may appear.

Cisco UCS C240 Host Configuration

Important:

- This procedure only needs to be performed once — when you initially install the UCS C240 server.
- The CIMC firmware and BIOS version (noted in step 4 of ***Cisco UCS C240 Server CIMC Configuration*** (on page 141)) should be at or higher than the minimum required version found in the **Tested Reference Configuration** chart in the Preface. If it is not, contact Cisco Support for assistance in upgrading the firmware and the BIOS.

RAID Configuration

Important: This procedure only needs to be performed once — when you initially install the UCS C240 server.

Go to the appropriate section to configure RAID on your UCS hardware.

- *Configuring RAID for UCS C240 M3 Servers* (on page 143)
- *Configuring RAID for UCS C240 M4 Servers* (on page 150)

Configuring RAID for UCS C240 M3 Servers

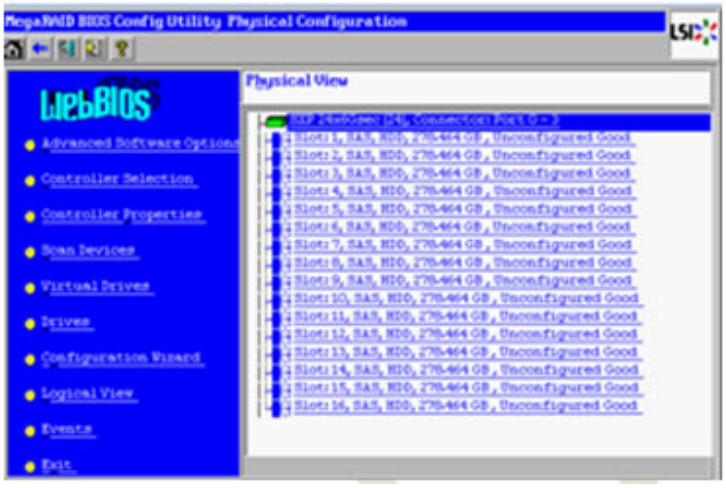
Important: This procedure only needs to be performed once — when you initially install the UCS C240 server.

The UCS hardware RAID configuration for this system release consists of a RAID 10 (14x300GB disks) for the OS disk, and two global hotspares (2X300 GB disks). This section details the steps necessary to create these volumes and hot spares.

1 Press **Ctrl-Alt-Del** to reboot the server.

2 Watch the reboot process closely. After the disks are displayed, observe the boot messages and press **Ctrl-R** when prompted to access the WebBIOS (RAID Configuration Utility). After a few minutes, a **Start** button appears.

3 Click **Start** to configure RAID. The MegaRAID BIOS Config Utility main menu appears.



4 Click the **Configuration Wizard** link in the left pane of the utility menu.

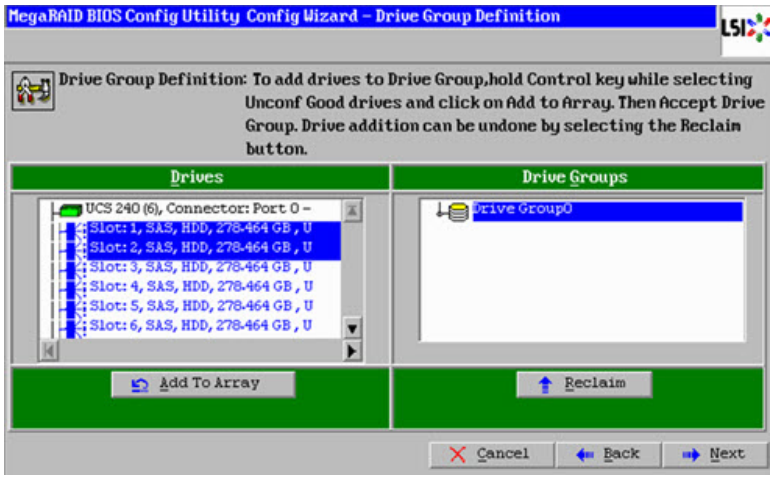
5 Click **New Configuration** and click **Next**. The utility prompts you to clear the existing configuration.

6 Click **Yes**.

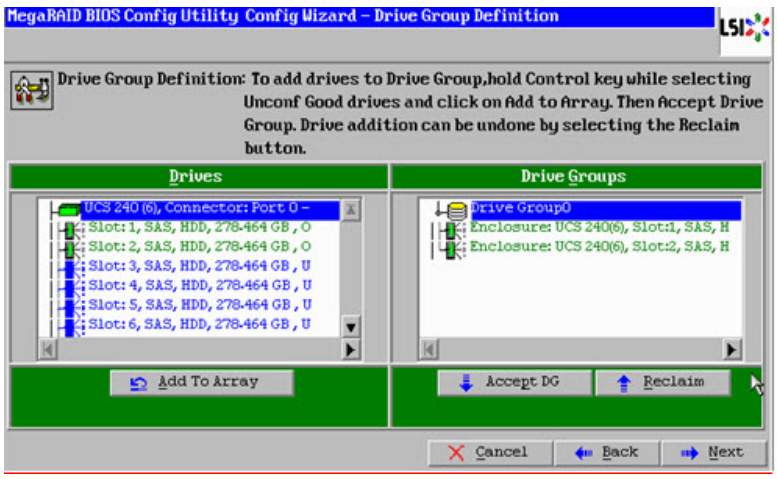
7 Click **Manual Configuration** and click **Next**. The Drive Group Definition screen appears.

Note: Within the drives panel, there is a list of all 16 hard drives. Create 7 drive groups (0-6), each consisting of 2 disks (1 and 2, 3 and 4, and so on). Drives 13 and 14 are your final drive group.

8 Select the **Slot 1** disk, and while pressing the **Ctrl** key, click the **Slot 2** disk to highlight both disks.



9 Click **Add to Array** to form **Drive Group (0)**.



10 Click **Accept DG**.

11 Repeat steps 8 through 10 for the following drive pairs:

Slots 3 and 4

Slots 5 and 6

Slots 7 and 8

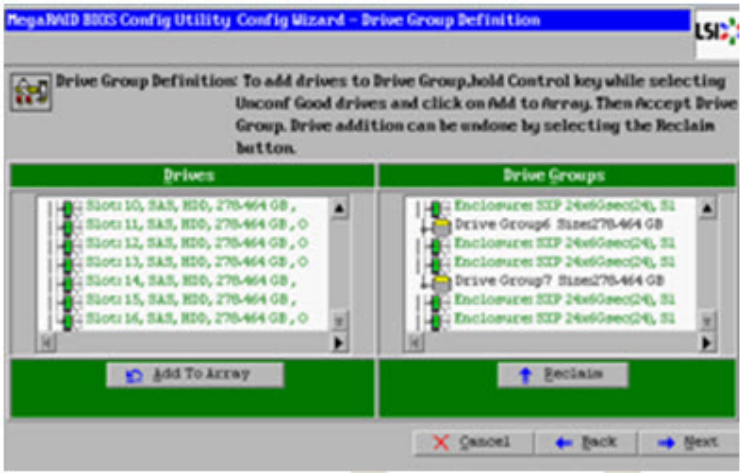
Slots 9 and 10

Slots 11 and 12

Slots 13 and 14

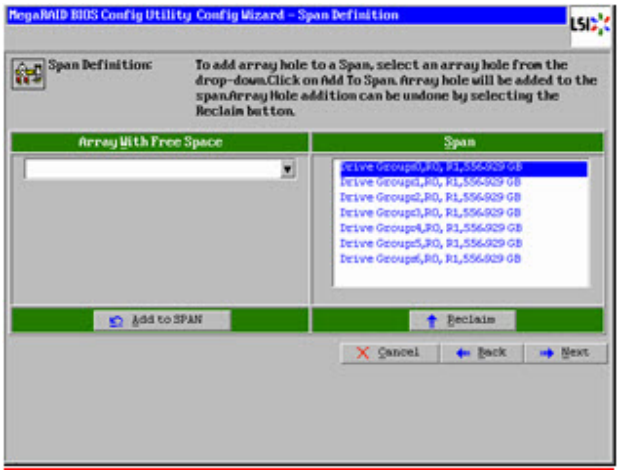
Result: The system creates a drive group for each pair.

Note: When you complete this step, you should have 7 drive groups (0 - 6).

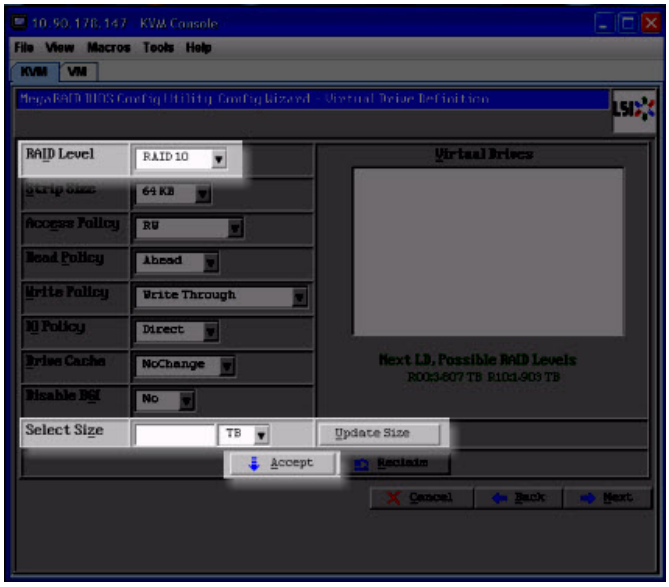


12 Click **Next** and select **Drive Group 0**.

13 Select each drive group, one by one, and click **Add to SPAN** to add all drive groups to the span list.

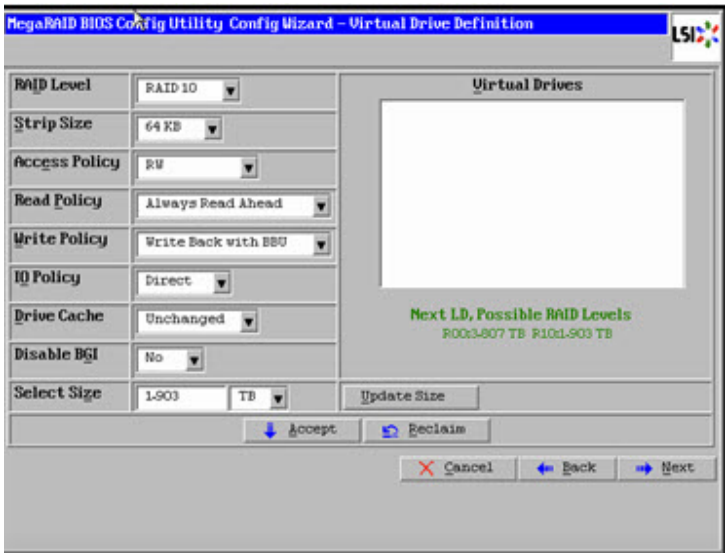


14 Click **Next**. The Virtual Drive Definition window appears.



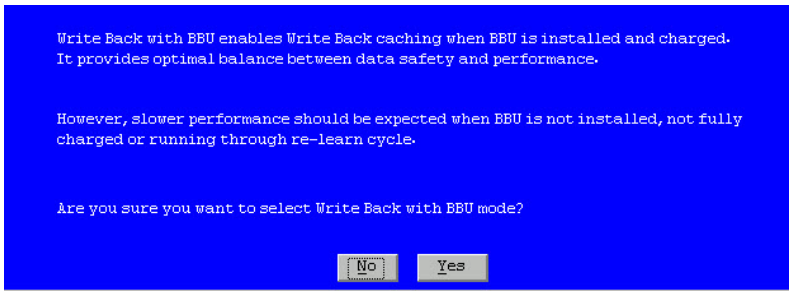
15 Select **RAID 10** from the RAID Level drop-down menu.

16 Click **Update Size**. The maximum allowed size for the selected RAID level populates the **Select Size** field.

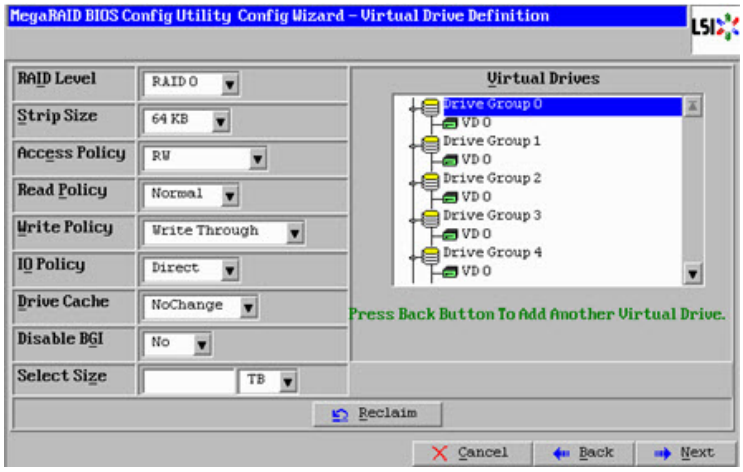


17 Record the **Select Size** here: _____

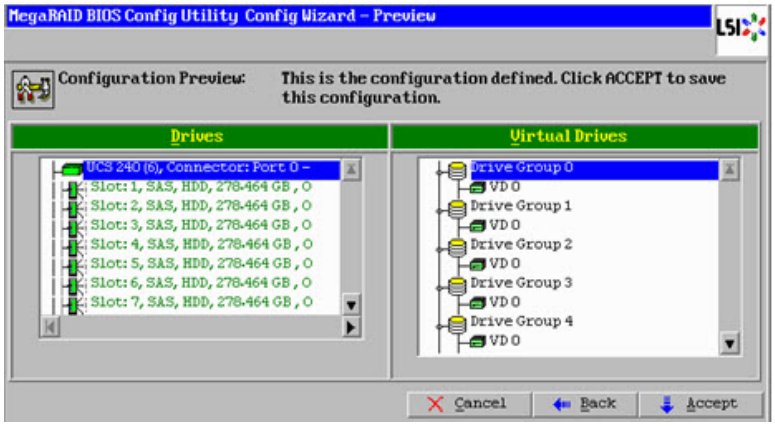
18 Click **Accept**. The Write Policy window appears.



19 Click **Yes** to confirm the default write policy. The total list of Vdisks created from Drive Groups 0-6 appears.

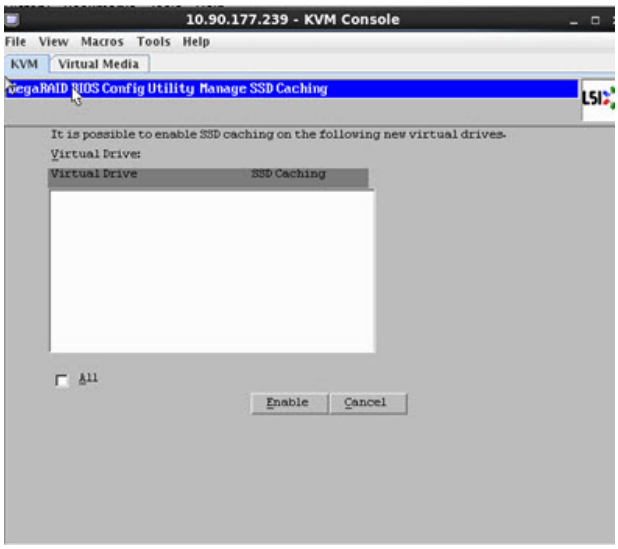


20 Click **Next**.

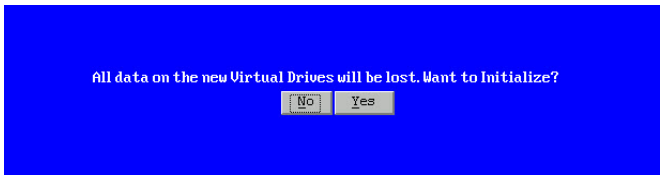


21 Examine the configuration preview to verify that the virtual drives match the previous list and click **Accept**. The system prompts to confirm saving the configuration.

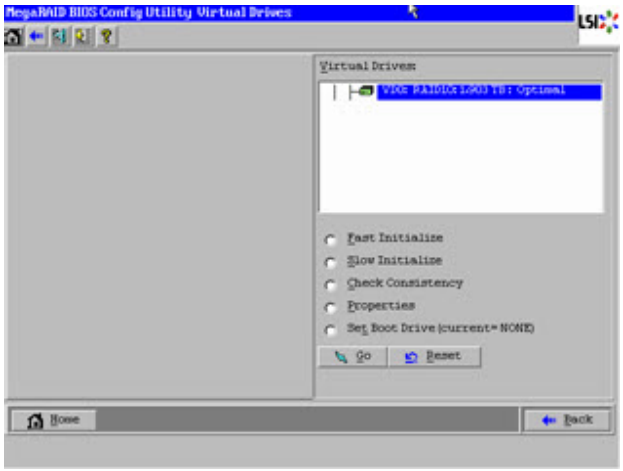
22 Click **Yes**. A warning message appears and indicates that you may lose data.



Note: After canceling the previous screen, you are prompted to initialize the new virtual drives.

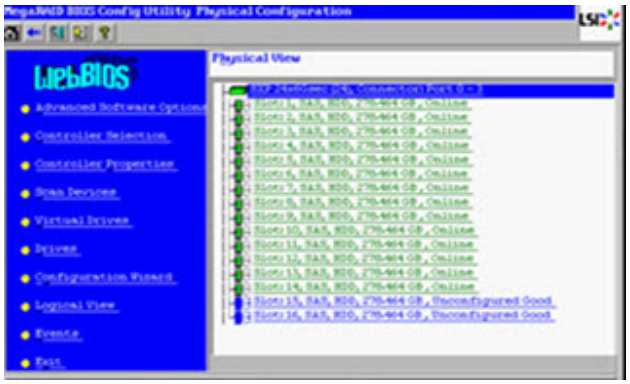


23 Click **Yes** to initialize. The Virtual Drive VD0 is displayed.



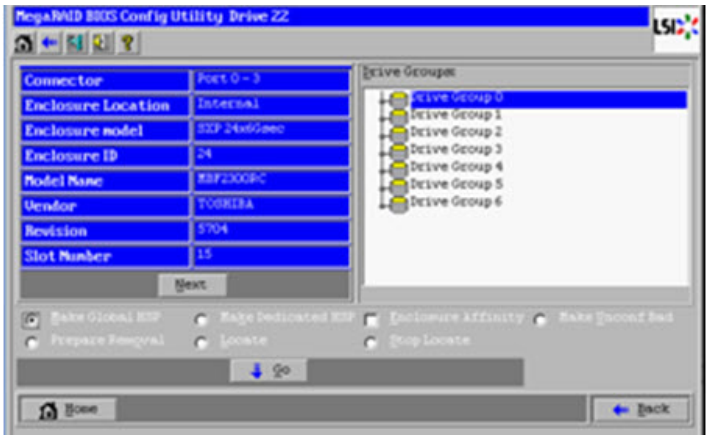
24 Click **Home**. The Raid Configuration utility main menu appears.

25 Click the **Physical View** from the left pane if it is not currently displayed.



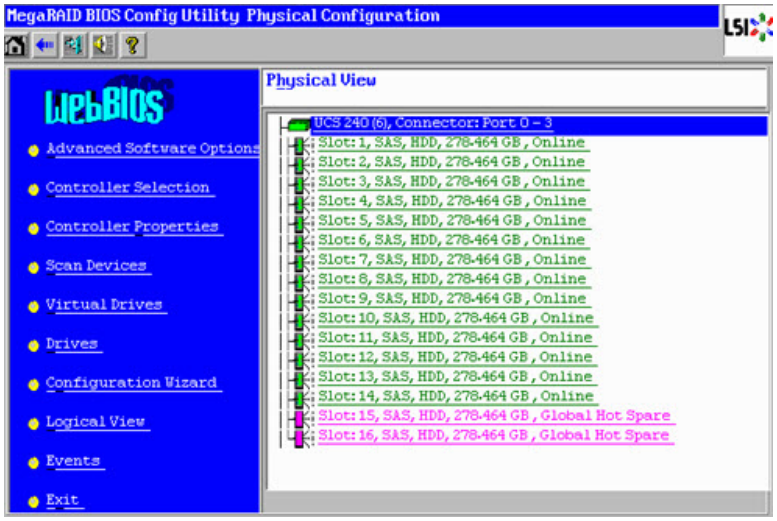
26 Click the drive on Slot 15 in the Physical View.

27 Click the option **Make Global HSP** and click **Go** to save.



28 Click **Back** and repeat steps 26 and 27 for the drive in Slot 16.

29 Click **Home** and select the **Physical View** (if it is not displayed by default).



30 Verify that the drives in Slot 15 and 16 are visible as Global Hotspares.

31 From the Main Menu, click **Exit** to exit the RAID Configuration Utility.

32 Click **Yes** to confirm exiting the utility.

Important: At this point, you may be prompted to reboot the computer. **Do NOT reboot**. It is very important that you do not reboot the computer at this time.

Configuring RAID for UCS C240 M4 Servers

Complete the following steps to configure RAID for a C240 M4 UCS server.

1 Power on the Cisco UCS C240 M4 server.

Note: If the server is already powered on, reboot the server.

2 On boot up, press **CTRL+R** to enter the Cisco 12G SAS Modular Raid Controller BIOS Configuration Utility.

3 Press **CTRL+N** and then click the **PD Mgmt** tab.

4 Use the **UP** or **DOWN** arrow keys to move between the disks.

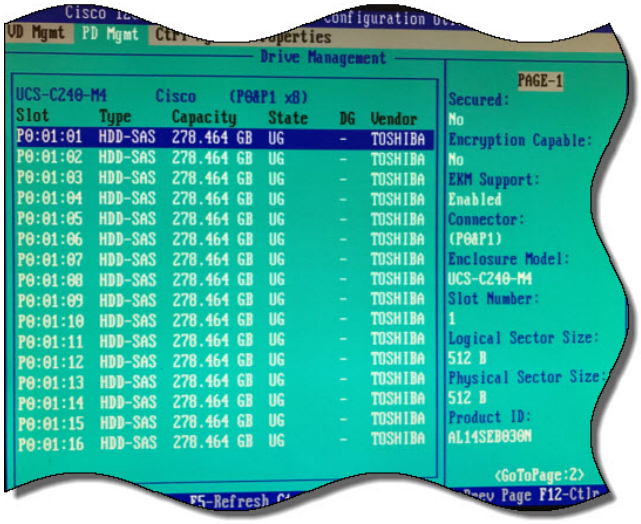
5 Complete the following steps to change the disks from Just a Bunch Of Disks (JBOD) to **Unconfigured Good (UG)**.

a Select the first disk and press **F2**.

b Select **Make unconfigured good**.

c When prompted to confirm the change, click **Yes** and press **Enter**. The state of the drive will change from JBOD to UG.

d Repeat Steps 4a through 4c for the remaining drives.



6 Go back to the **VD Mgmt** tab and press **CTRL+P**.

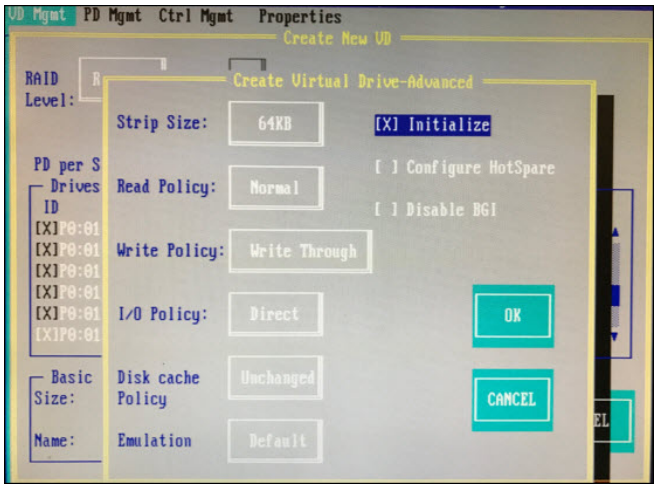
7 Select **No Configuration Present** and press **Enter**.

8 Configure the following:

- **a** From the RAID Level area, select **RAID-10**.
- **b** From the Secure VD area, select **No**.
- **c** From PD per Span area, enter **2**.
- **d** From the Drives area, use the UP or DOWN arrow to highlight the appropriate drive and press **Enter**. An **X** displays next to the drive to indicate that it is selected.
- **e** Repeat Step 8d to select the next drive that will make up this drive pair.

9 Click **Advanced** option and highlight the **Initialize** option.

10 Press **Enter**. An **X** is inserted next to Initialize to indicate that it is selected.



11 Click **Ok**.

12 Click **Ok** to close the Advanced window. The Configuration window is displayed.

13 Click **Ok** and system will now initialize the RAID-10 array. Wait for the initialization to complete.

14 Click **Ok** after the Confirmation window indicates that the initialization is complete.

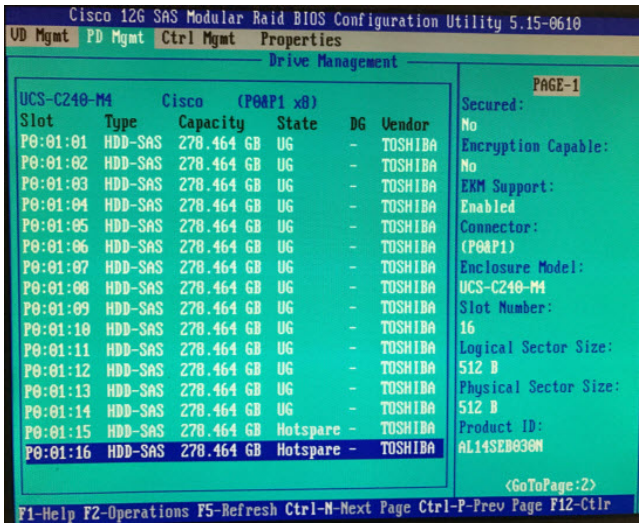
15 Click **CTRL+N** to return to the **PD Mgmt** window.

16 From the PD Mgmt window, use the **UP** or **DOWN** arrows to highlight drive **P0:01:15**.

17 Press **F2** and then select **Make Global HS**.

Note: The state of the drive changes from **UG** to **Hotspare**.

18 Press **ESC** and then repeat Steps 16 through 17 for drive **P0:01:16**.



19 Press **ESC** and click **Ok** to exit the utility.

20 Click the **Macros** tab and select **Static Macros > CTRL+ALT+DEL** to reboot the server.

Note: The server must be rebooted for the changes to go into effect.

ESXi Installation

Important: This procedure is written for both the C240 M3 and C240 M4 servers and only needs to be performed if you are executing an initial installation or moving to new hardware.

Before You Begin

Note: The Firefox browser is not officially supported for accessing the UCS C240 M3/C4 CIMC application.

1. Use a Web browser to open the CIMC application, using the IP address configured in ***Cisco UCS C240 Server CIMC Configuration*** (on page 141).
2. Log onto the server using the admin password or the password that you set in ***Cisco UCS C240 Server CIMC Configuration*** (on page 141).

Power Policy

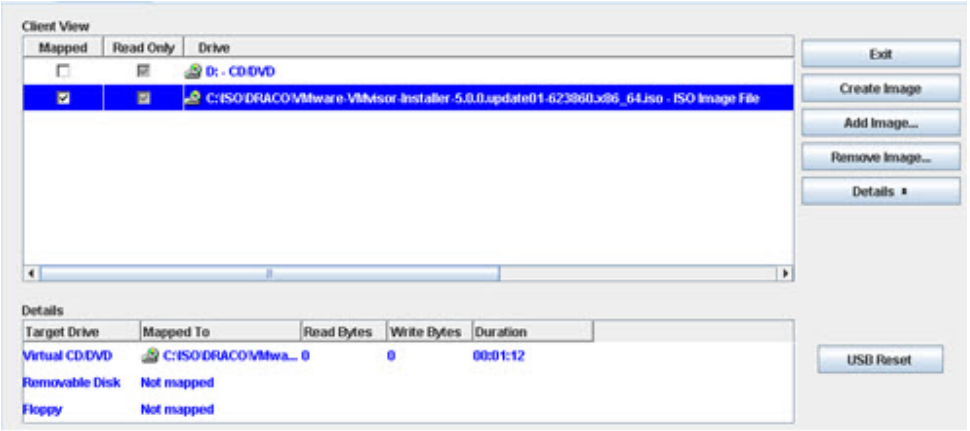
1. Click **Power Policies**.
2. Choose **Restore Last State** from the menu.
3. Click **Save Changes**.
4. Click **Summary** on the Server tab in the CIMC.
5. Click **Launch KVM Console** from the Server Summary window.
6. Select open using java viewer in the dialog box. The KVM Console is displayed.

Installing ESXi

Important: Before beginning this procedure, make sure that you have downloaded or copied the VMware ISO image to the local hard drive that is running the CIMC application.

1. Follow these instructions to mount the ESXi ISO image.
   a. Click the **Virtual Media** tab in the KVM Console.
   b. Click **Add Image**.
   c. Browse to the location of the VMware ISO image and select **Open**.

d Click the **Mapped** box next to the added image.



e Click the **KVM** tab in the KVM Console.

2 Select **Macros** and then the **Ctrl-Alt-Del** option from the KVM menu bar to reboot the server.

Note: Later versions of firmware may refer to **Static Macros**.

3 Press **F2** when the Cisco screen is displayed to enter the system setup.

4 Navigate to the **Boot Options** tab.

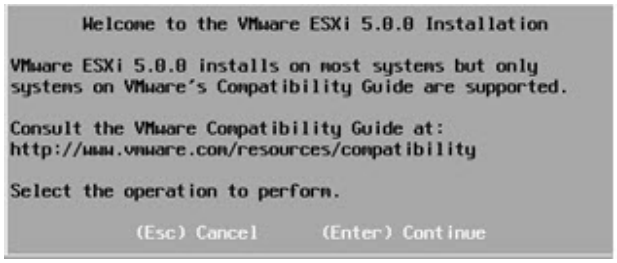
5 Make the following selections:

- Boot Option 1 — RAID Adapter
- Boot Option 2 — Virtual CD/DVD
- Disable remaining boot options

6 Press **F10** to save the settings and reset system.

7 Click **Yes** to save the settings and reset the system.

8 Wait for the ESXi installer to load. After the ESXi load completes, a **Welcome** message appears.



9 When prompted, press **Enter** to continue.

10 When prompted, press **F11** to accept the license agreement.

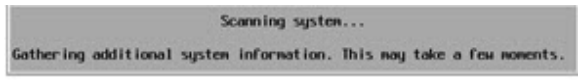
Note: This action selects the disk. Select the disk that matches the size of the Virtual Disk that was recorded in RAID Configuration, Step 17.

11 Press **Enter** to continue.

12 Select the appropriate keyboard layout (for example, **US default**) and press **Enter**.

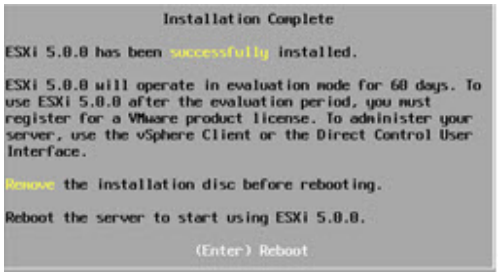
13 Enter and confirm a new **root** password for the ESXi host.

14 Press **Enter** to continue.



15 Press **F11** to confirm the installation on the selected disk. The ESXi installation begins and a progress bar appears.

16 When the installation completion screen is displayed, press **Enter** to reboot. The ISO is un-mapped and the system boots to the VMware ESXi window.

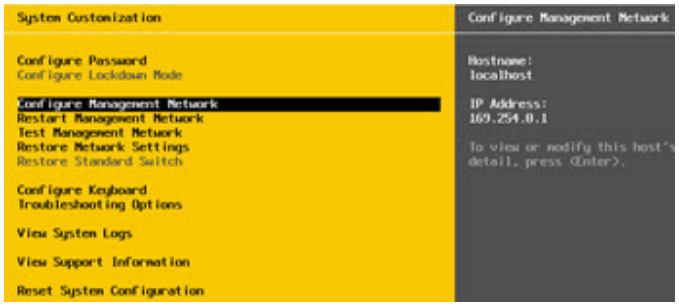


Important: Let the system boot into ESXi. If you press F2 too early (during boot-up), the BIOS configuration screen appears, which is not what you want.

17 Press **F2** to customize the system.

18 Log in as **root** user. The System Customization window appears.

19 Navigate to **Configure Management Network** and press **Enter**.

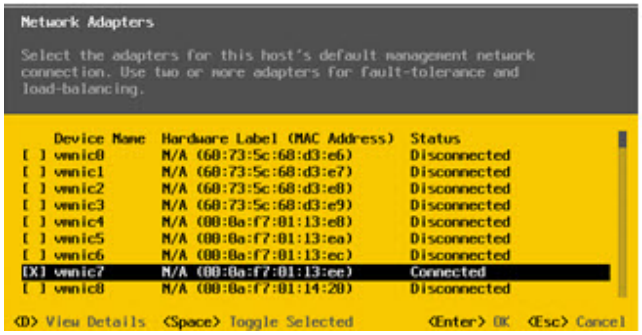


20 Select **Network Adapters** and press **Enter**.

21 To select a vmnic, highlight the line you want and press the **Spacebar**.

Note: For the UCS 240 server, enable nic 1 and 7; disable the others. These nics are for ESXi access.

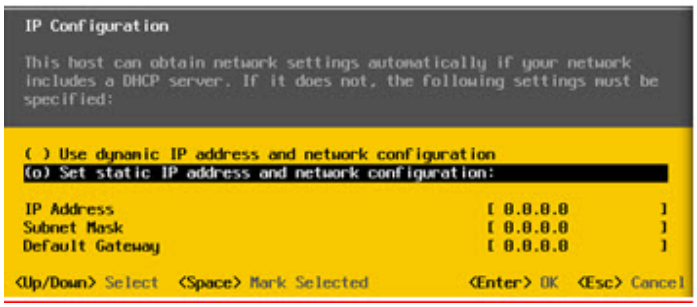
22 Verify that the devices you enabled in step 21 show a **Connected** status.



23 Press **Enter**. The system returns to the Configure Management Network window.

24 Select **IP Configuration** and press **Enter** to set/modify the IP address.

25 Use the arrow keys to highlight **Set static IP address** and press the **Spacebar**.



26 Provide the following information to configure the ESXi server:

- IP Address
- Subnet Mask
- Gateway

27 Press **Enter** to accept the changes.

28 Use the arrow keys to highlight **DNS configuration** and then press **Enter**.

29 Provide the following information.

- Primary DNS IP address
- Secondary DNS IP address (optional)
- Hostname

30 Press **Enter** to accept and return.

31 Press **Esc** to exit and press **Y** to accept the changes when prompted.

32 Select **Test Management Network** and press **Enter** to navigate to the Test Management Network dialog.

33 Press **Enter** to begin a ping test.

34 After the ping test is complete, press **Enter** to exit the test dialog.

35 See the site Network Administrator to verify addressing and cabling.

36 Scroll to **Troubleshooting Options** and press **Enter**.

37 Select **Enable SSH** and press **Enter**. The right-hand panel mode should indicate **SSH is Enabled**.

38 Press **Esc** to exit.

39 Press **Esc** to log out and disconnect the KVM.

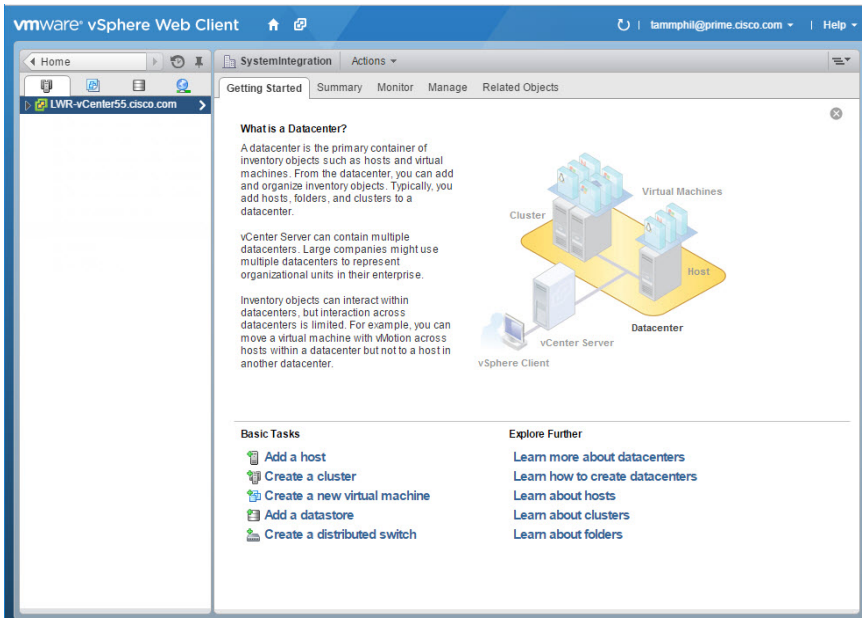
40 Click **File/Exit** to close the KVM console.

Configure the Host System

Important: This procedure is written for the C240 M3 and C240 M4 servers and only needs to be performed once — when you initially install the UCS C240 server.

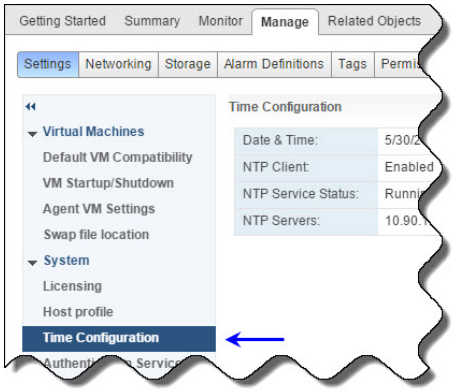
You must have a Windows, Linux, or Mac OS system with vSphere installed to complete the installation and migration of SR 8.0.

1. Provide the IP address, username, and password for the new ESXi host to the vCenter administrator. Once the administrator licenses the new host, you can able to access it through vCenter.
2. Use the VMware vSphere Web Client to connect to the vCenter server by providing the IP address, username and password for authentication.
3. Click **Hosts and Clusters**. The Host and Clusters view displays.



4. Drill down in the dropdown list to locate and select the new ESXi host.
5. Click the **Manage** tab and then click the **Settings** menu button to begin configuring resources.

6 From the **System** dropdown list on the left pane, click **Time Configuration** to modify the date and time.



7 Click **Edit**. The Edit Time Configuration window displays.

8 Complete the following steps to update the date and time.

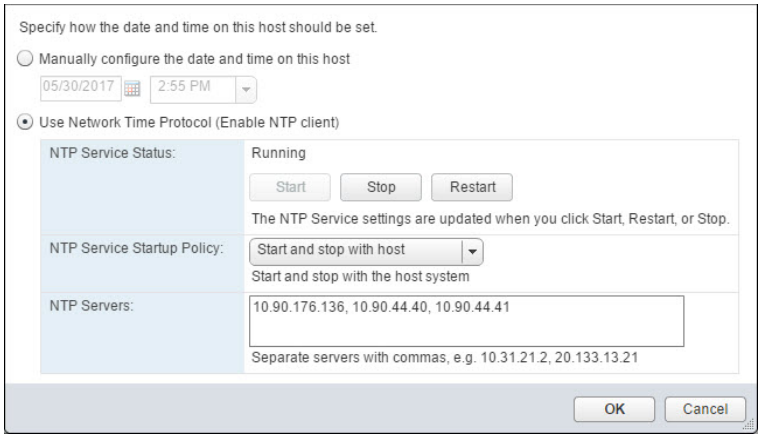
a Click **Use Network Time Protocol (Enable NTP client)**.

b From the NTP Server Startup Policy area, select **Start and stop with host**.

c From the NTP Servers area, enter the IP Addresses for your NTP servers separated by a comma.

d From the NTP Service Status area, click **Restart**.

e Verify that that NTP Service Status indicates **Running** and then click **OK**. You are returned to the Settings window.



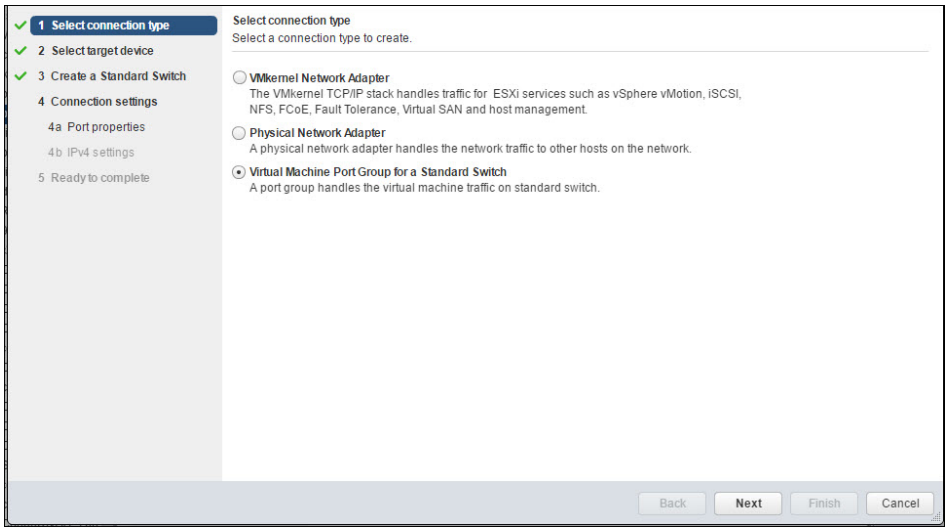
9 From the top area of the window, click the **Networking** tab and then click **Virtual Switches**.

10 From the Virtual switches area, select **vSwitch0**. The Standard switch: vSwitch0 (VM Network) area displays in the lower section of the window.

11 From the Virtual switches area, click the **Remove selected standard switch** icon, ✖.

12 When prompted to remove the switch, click **Yes**.

13 From the Virtual switches area, click the **Add host networking** icon, , to configure the network adapters for your system. The Add Networking > Select connection type window displays.



14 Select **Virtual machine Port Group for a Standard Switch** and click **Next**. The Select target device window displays.

15 Select **New standard switch** and then click **Next**. The Create a Standard Switch window displays.

16 Click the **Add adapters** icon, . The Add Physical Adapters to the Switch window displays.

17 From the Network Adapters area, select the appropriate adapter for the Management network (i.e. vmnic1) and then click **OK**. You are returned to the previous screen where the new network adapter is added to the Active adapters list.

Note: Refer to the following chart to help you configure the network host system settings.

Network	UCS 240-M3	UCS 240-M4
ESXi Management	1, 7	1, 7
Headend network	4, 8	4, 8
Corporate network	5, 9	5, 9
RepDB network	10, 6	10, 6
Headend 2 network (DSG)	2, 11	2,11
TED crossover	0	0

18 Click the **Add adapters** icon again,  , and select the second network adapter for the vSwitch. Then click **OK**.

19 From the Create a Standard Switch window, click **Next** and then click **OK**. The Connection settings window displays.

20 From the **Network label** text box, change the label name to a name that is appropriate for the network adapter (e.g. Management Network). Then click **Next**. The Ready to complete window displays.

Note: The vSwitch labels used in this document are suggested labels only. You can name this and the remaining vSwitches to reflect your system configuration.

21 Click the **Use static IPv4 settings** radio button and then enter the **IPv4 address** and **Subnet** mask. Click **Next**.

22 Review the settings and click **Finish**.

23 Monitor the **Recent Tasks** area to confirm that the network configuration completed successfully.

24 Repeat Steps 13 through 23 to create the Headend Network on vSwitch1.

Notes:

- Use the chart in Step 17 to configure the proper headend network adapters for your system.
- When entering the Network label, make sure you enter a name that identifies the network as the headend.

25 Repeat Steps 13 through 23 to configure the following networks shown in the network design that was created for the customer.

The following examples are for reference only.

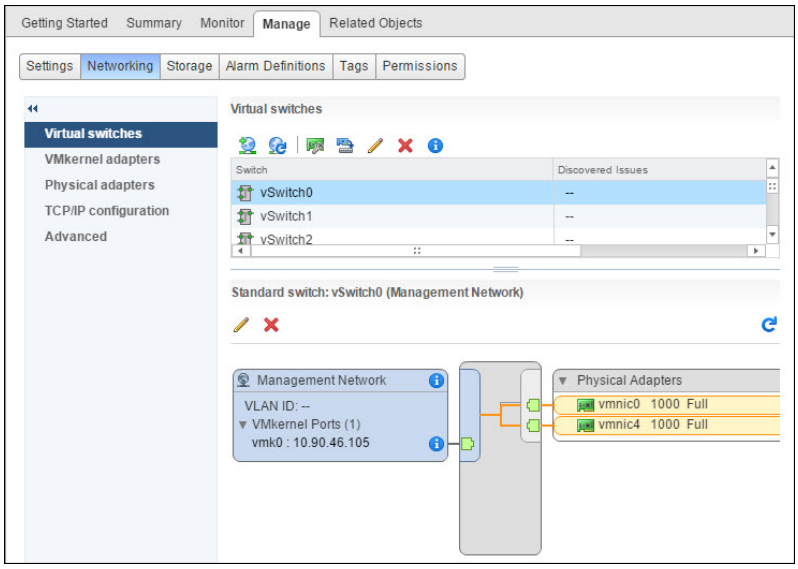
- **Corporate Network —** For corporate and back office access. This is created under **vSwitch 2.**
- **TED XOR Network —** For direct crossover connectivity with the TED. This is created under **vSwitch3.**
- **RepDB Network —** For direct connectivity to the RepDB interface when RepDB is an enabled feature. This is created under **vSwitch4**.

  Note: This network is optional and should be configured only if you are using RepDB.
- **Headend 2 Network —** This vSwitch may be used for DSG or other network requirements. This is created under **vSwitch5**.

  Note: This network is optional and should be configured only if needed.

26 To review the networking for each vSwitch, click on a vSwitch from the Virtual switches area. The Networking diagram is displayed.

Example for vSwitch0:



27 To configure the **Storage Configuration**, click the **Storage** tab.

28 From the left area of the window, click **Storage Devices**.

29 Select **datastore1** and click the **Updates the SCSI LUN display name of the selected device**, , icon.

30 In the **Name** text box, rename the device to **<hostname>_local_storage1**. Click **OK**.

Note: Cisco engineers have seen some issues when the datastore name contains blank spaces. Do not include spaces when you rename the datastore.

31 If necessary, create an NFS mapping to the location of the Linux platform image.

a Right-click the ESXi host and select **New Datastore**. The New Datastore window displays and lists the Location where the new datastore will reside.

b Click **Next**.

c Select **NFS** and click **Next**.

d In the Datastore name field, replace the name with something that describes your datastore.

e In the Server field, enter the name or IP address of the server.

f In the Folder field, enter path to the folder you want to access.

g Click the **Mount NFS as read-only** check box. and then click **Next**.

h Verify the settings and click **Finish**.

B

System Verification Procedures

Introduction

Use these procedures to verify that an active communication link exists between the EC and DHCTs. The EC must be able to communicate with DHCTS to have a successful system upgrade.

In This Appendix

Verify the System Upgrade

Verifying the System Upgrade

Important: If any of the following tests fail, troubleshoot the system to the best of your ability. If you are unable to resolve the failure, contact Cisco Services for assistance.

1 As **dncs** user, type the following command and press **Enter**:

```
[dncs@vodwater ~]$ cd /dvs/dncs/Utilities/doctor
```

2 Type the following command and press **Enter**. This command runs the Doctor report.

```
[dncs@vodwater ~]$ doctor -vn
```

3 When the Doctor report completes, review it to ensure that communications exist among all DBDS elements.

4 Type the following command and press **Enter** to verify that you are using no more than 85 percent of the partition capacity of each disk:

```
[dncs@vodwater ~]$ df -k
```

Important: If any disk partition lists a capacity greater than 85 percent, contact Cisco Services before proceeding.

5 Stage at least one new DHCT to your site's specifications. After staging the DHCT, verify the following:

- The DHCT receives 33 or 34 EMMs.
- The DHCT successfully receives its Entitlement Agent.

6 Complete these steps to perform a slow and fast boot on a test DHCT and Combo-Box (if available) with a working return path (2-way mode):

a Boot a DHCT.

Note: Do not press the power button.

b Access the Power On Self Test and Boot Status Diagnostic Screen on the DHCT and verify that all parameters, except UNcfg, display **Ready**.

Note: UNcfg displays Broadcast.

c Wait 5 minutes.

d Press the power button on the DHCT. The power to the DHCT is turned on.

e Access the Power On Self Test and Boot Status Diagnostic Screen on the DHCT and verify that all parameters, including UNcfg, display **Ready**.

7 Verify that you can ping the DHCT.

8 Verify that the Interactive Program Guide (IPG) displays 7 days of accurate and valid data.

9 Tune to each available channel on a DHCT to confirm that a full channel lineup is present.

Note: Record any anomalies you notice while verifying the channel lineup.

10 For all sites, verify that you can define, purchase, and view an IPPV, xOD, and VOD event.

Verify the Channel Map After the Upgrade

Verify that the channel map associated with various types of DHCTs in the headend is accurate for each specific hub. If you notice that the channel map is not accurate, complete the following steps.

Delete the sam File Server

1 Have you confirmed that there are inaccuracies in the channel map of various DHCTs?

- If **yes**, go to the next step.
- If **no**, check the channel map associated with various types of DHCTs in the headend for each specific hub.

  Note: Complete the procedures in this section only if the channel maps are not accurate.

2 From the EC Web UI, click the **Navigation** button and then select **App Interface Modules > BFS Client**. The Site DNCS Broadcast File Server List window opens.

3 Highlight the **sam** file server.

4 Click **File > Delete**. A confirmation message appears.

5 Click **Yes** and press **Enter**. The system deletes the sam file server.

Bounce the saManager Process

1 From the EC Web UI Process Status window, click the button next to the **saManager** process.

2 Click **Stop**. In a few minutes, the indicator for the saManager process changes from green to red.

Note: Do not go to the next step until the indicator has changed from green to red.

3 Click the button next to the **saManager** process again.

4 Click **Start**. In a few minutes, the indicator for the saManager process changes from red to green.

Save the Channel Map Web UIs

1 Wait the length of time of the SAM Configuration Update Timer.

Note: You can find this value on the SAM Configuration window.

2 Examine again the channel maps for the DHCTs.

- If the channel maps are accurate, you are finished with this procedure.
- If the channel maps are still inaccurate, go to the next step.

3 Open the Channel Map user interface for each applicable channel map, and click **Save**.

Note: Do not make any changes on the Web UI; simply click **Save**.

4 Wait again the length of time of the SAM Configuration Update Timer.

5 Examine each channel map again for accuracy.

Checking the EAS Configuration

After installing the SR 8.0 software, verify that your EAS equipment is working correctly by testing the system's ability to transmit EAS messages. Refer to **Conduct EAS Tests** in the ***EC 8.0 Online Help***.

C

SR 8.0 Rollback Procedures

Introduction

The SR 8.0 rollback procedures are intended for field service engineers who encounter problems while upgrading an existing digital system to SR 8.0. Prior to executing the SR 8.0 rollback procedures, contact Cisco Services.

In This Appendix

Activate the Old System Release

1 As **dncs** user, type the following commands to stop all system components.

```
[dncs@vodwater ~]$ appStop
[dncs@vodwater ~]$ dncsStop
[dncs@vodwater ~]$ appKill
[dncs@vodwater ~]$ dncsKill
```

2 As **admin** user, type the following command to shut down and power off the VM.

```
[admin@vodwater ~]$ sudo shutdown -h now
```

3 From the vSphere Web UI, right-click the VM and select **All vCenter Actions > Power > Power Off**.

4 From the vSphere Web UI, right-click the SR 7.x EC and select **Power On**.

5 Log onto the SR 7.x EC as an administrative user.

6 Change to **dncs** user.

```
$ sux - dncs
```

7 Type the following command and press **Enter** to start the EC processes:

```
$ dncsStart
```

8 Type the following command and press **Enter** on the application server to start the application server processes:

```
$ appStart
```

9 Return to procedures at the beginning of this appendix to verify system functionality.

D

SR 8.0 Upgrade

This appendix provides the procedures to upgrade your system to a new version of SR 8.0.

In This Appendix

SR 8.0 Upgrade Prerequisites

The following prerequisites are required prior to performing the EC SR 8.0 upgrade.

- **Admin Node**
  - Refer to Appendix C in the ***Admin Node User's Guide*** for the procedure to upgrade the software repos.

    Important: The software repos ***must*** be updated before starting the EC upgrade.
- **EC System**
  - Refer to ***System Verification Procedures*** (on page 165) to verify that the active system is operating without any issues.
  - Refer to ***Post RepDB Verifications*** (on page 129) to execute a file sync and Replicated Database check.
  - Verify available disk space on the primary and secondary ESXi hosts for cloning the new VMs (i.e. for a standard C240 installation, the EC requires 512 GB of disk space).
  - The secondary VM must have access to the Admin Node.

Preparing for the Upgrade

Complete the following steps on the EC system to prepare the primary and secondary servers for the upgrade.

1 Stop all billing interfaces.

2 Disable RepDB on the *primary* and *secondary* servers.

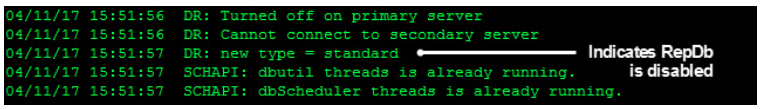
a As **admin** user on the *primary* server, type the following command.

```
[admin@berlin repdb]$ sudo ./RepDb -d
```

b When prompted, type **y**. Data replication is disabled.

c Type the following command to verify that data replication is disabled.

```
[admin@berlin repdb]$ sudo onstat -m
```



d Repeat Steps 2a through 2c on the *secondary* server.

3 Go to the next section.

Upgrading the Secondary VM

Cloning the Secondary VM

Important: If you are using an ESXi client then you cannot clone the secondary VM. Refer to ***Procedures When Using an ESXi Client*** (on page 205) to deploy a new secondary VM.

1 As **admin** user, enter the following command to shut down the *secondary* server.

```
[admin@berlin ~]$ sudo shutdown -h now
```

2 From the vSphere Web UI, right-click the *secondary* VM and select **All vCenter Actions > Power > Power Off**.

3 Monitor the **Recent Tasks** area until the task completes.

4 Right-click the *secondary* VM and select **Clone to Virtual Machine** to create a backup of the original VM. The Clone to Virtual Machine window appears.

5 In the **Enter a name for the virtual machine** text box, type a name to reflect the VM.

Note: In this example, we will use Berlin3_HOSTB_8.0-upgrade_20170622

6 Select the datacenter where the cloned VM will be built. Then click **Next**.

7 Select the ESXi host and verify that the compatibility is validated in the **Compatibility** area of the window. Then click **Next**.

8 Select the storage destination which should be the same as the VM that is being cloned. Then click **Next**.

9 Click **Next** again and then click **Finish**.

10 Monitor the cloning of the VM in the **Recent Tasks** area and when it successfully completes, go to the next step.

11 From the vSphere Web UI, right-click the cloned VM and select **Edit Settings**.

12 Hover your cursor in the **Network adapter 4** (RepDB) line. An X icon, ⊗, appears.

13 Click the ⊗ icon to delete Network adapter 4.

14 Do any remaining Network Adapters share an IP address with the *primary* VM?

- If **yes**, click the check mark out of the **Connected** box. Then go to the next step.
- If **no**, go to the next step.

15 Click **OK**.

16 Right-click the cloned VM and select **Power On**.

17 Right-click the cloned VM and select **Open Console**.

18 Login as **admin** user.

19 Type the following command to delete the **70-persistent-net.rules** file.

```
[admin@berlin ~]$ sudo rm
/etc/udev/rules.d/70-persistent-net.rules
```

20 When prompted to confirm the deletion of the file, type **y**.

21 Enter the following command to reboot the EC.

```
[admin@berlin ~]$ sudo shutdown -r now
```

22 When the VM completes the boot process, login and check the network connectivity and verify that you can ping the Admin Node.

Note: If the VM has a unique IP address for eth0, you can log into the VM from a terminal window.

```
[admin@berlin ~]$ ifconfig -a
[admin@berlin ~]$ ping [Admin Node IP]
```

Upgrading the Software on the New Secondary EC

1 As **dncs** user, type the following commands and press **Enter** (after each command) to kill the Initd processes.

```
[dncs@berlin ~]$ appKill
[dncs@berlin ~]$ dncsKill
```

2 As **admin** user, type the following command to see if CSCOec-lic-8.0.x package is installed on the system.

```
[admin@berlin ~]$ rpm -qa | grep -i cscoec-lic
```

3 Is the **CSCOec-lic** package installed on your system?

- If **yes**, go to Step 4.
- If **no**, go to Step 5.

4 Enter the following command to remove the **cscoec-lic** package.

Command Syntax:

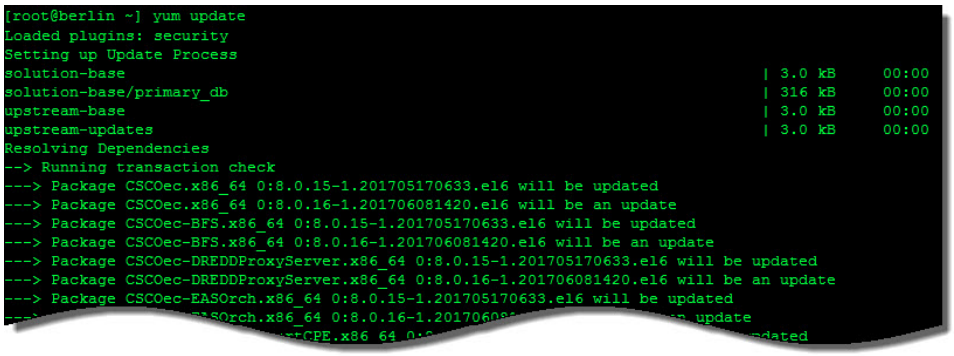
```
rpm -e CSCOec-lic-[version]
```

Example:

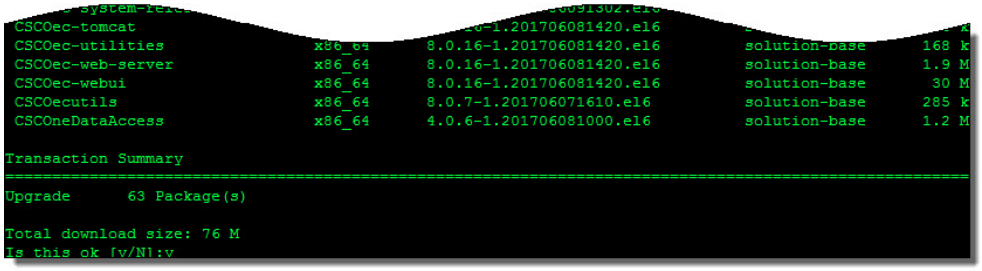
```
[admin@berlin ~]$ sudo rpm -e
CSCOec-lic-8.0.17-1.201706230635.el6.x86_64
```

5 Type the following command to upgrade the EC software. A verification of the repos occurs and a check is done to verify which packages need upgraded.

```
[admin@berlin ~]$ sudo yum update
```



6 Once the packages are resolved and a list of the packages to upgrade is displayed, you are prompted to confirm the download of the packages.



7 Type **y** and press **Enter**. The update of the packages begins and, when complete, a **Complete!** message displays.

8 Did the yum update complete successfully?

- If **yes**, go to Step 9.
- If **no**, go to Step 10.

9 Enter the following command to reboot the server. Then go to the next section in this appendix.

```
[admin@berlin ~]$ sudo shutdown -r now
```

10 Log back into the EC.

11 Review the following log for any error messages.

```
[admin@berlin ~]$ sudo less /var/log/yum.log
```

12 If errors exist and you cannot determine the issue, execute one of the following options.

- Contact Cisco Services.
- Rollback the upgrade.

  Note: To rollback the upgrade, go to the next step.

13 Type the following command to shutdown the VM

```
[admin@berlin ~]$ sudo shutdown -h now
```

14 From the vSphere Web UI, right-click the VM and select **All vCenter Actions > Power > Power Off**.

15 Monitor the **Recent Tasks** area to verify that the VM successfully powered off.

16 Right-click the original VM and select **Power On**.

Shutting Down the Primary VM

1 As **dncs** user. enter the following commands to stop system processes on the *primary* EC.

```
[dncs@berlin ~]$ appStop
[dncs@berlin ~]$ dncsStop
[dncs@berlin ~]$ appKill
[dncs@berlin ~]$ dncsKill
```

2 As **admin** user, type the following command to shutdown the *primary* EC.

```
[admin@berlin ~]$ sudo shutdown -h now
```

3 Monitor the **Recent Tasks** area until the task completes.

Updating IP Addresses on the Secondary VM

Important: If the primary and secondary ECs use the same IP address for the corporate network (i.e. eth0), then skip this section.

1 On the active *secondary* EC, enter the following command to copy the **ifcfg-eth0** file to a new file.

```
[admin@berlin ~]$ sudo cp
/etc/sysconfig/network-scripts/ifcfg-eth0
/etc/sysconfig/network-scripts/orig.ifcfg-eth0
```

2 Open the **/etc/sysconfig/network-scripts/ifcfg-eth0** in a text editor and update the IP address.

```
[admin@berlin ~]$ sudo vi
/etc/sysconfig/network-scripts/ifcfg-eth0
```

3 Save and close the file.

4 Execute the following commands to restart the network interface.

```
[admin@berlin ~]$ sudo /etc/sysconfig/network-scripts/ifdown
eth0
[admin@berlin ~]$ sudo /etc/sysconfig/network-scripts/ifup
eth0
```

5 Repeat Steps 1 through 4 for any other interface that uses a unique IP address.

Note: Make sure to substitute the appropriate file name for ifcfg-eth0.

6 Enter the following command to verify that the IP addresses are correct for each interface.

```
[admin@berlin ~]$ ifconfig -a
```

Reconfiguring the Network Adapters on the Secondary VM

Complete the following steps to reconfigure the network adapters on the secondary VM.

1 From the vSphere Web UI, right-click the *active secondary* VM and select **Edit Settings**.

2 Click the **Connect** box for all network adapters.

3 Click **OK**.

4 Monitor the **Recent Tasks** area to confirm that the task successfully completes.

Starting Processes on the Secondary VM

1 As **dncs** user, type the following commands to start system processes on the *active secondary* EC.

```
[dncs@berlin ~]$ dncsStart
[dncs@berlin ~]$ appStart
```

2 Type the following command to verify that system processes have started.

```
[dncs@berlin ~]# pgrep -fl dvs
```

3 Log into the EC Web UI and verify that processes are coming up and eventually go green.

Note: This server is now the active *primary* EC in the system.

Verifying the Functionality of the Upgraded EC

Go to ***System Verification Procedures*** (on page 165) verify the functionality of your new *active* EC.

Note: If your EC is functioning properly, go to the next section to upgrade the original *primary* server.

Upgrading the Original Primary VM

Cloning the Original Primary VM

Important: If you are using an ESXi client then you cannot clone this VM. Refer to ***Procedures When Using an ESXi Client*** (on page 205) to deploy a new VM.

Note: This server has already been shutdown.

1. Right-click the *original primary* VM and select **Clone to Virtual Machine**. The Clone to Virtual Machine window appears.
2. In the **Enter a name for the virtual machine** text box, type a name to reflect the VM.

   Note: In this example, we will use Berlin3_HOSTA_8.0-upgrade_20170622
3. Select the datacenter where the cloned VM will be built. Then click **Next**.
4. Select the ESXi host and verify that the compatibility is validated in the **Compatibility** area of the window. Then click **Next**.
5. Select the storage destination which should be the same as the VM that is being cloned. Then click **Next**.
6. Click **Next** again and then click **Finish**.
7. Monitor the cloning of the VM in the **Recent Tasks** area. When it successfully completes, go to the next step.
8. From the vSphere Web UI, right-click the new, cloned VM and select **Edit Settings**.
9. Hover your cursor in the **Network adapter 4** (RepDB) line. An X icon, ⊗, appears.
10. Click the icon to delete the network adapter for RepDB.
11. Do any of the other Network adapters share an IP address with the new active VM in the system?
    - If **yes**, click the check mark out of the **Connected** box. Then go to the next step.
    - If **no**, go to the next step.
12. Click **OK**.
13. Right-click the VM and select **Power On**.
14. Right-click the VM again and select **Open Console**.
15. Login to the VM as **admin** user.
16. As **admin** user, type the following command to delete the **70-persistent-net.rules** file.

```
[admin@berlin ~]$ sudo rm
/etc/udev/rules.d/70-persistent-net.rules
```

17 When prompted to confirm the deletion of the file, type **y**.

18 Enter the following command to reboot the EC.

```
[admin@berlin ~]$ sudo shutdown -r now
```

19 When the VM completes the boot process, login as **admin** user.

20 Enter the following commands to check the network connectivity and to verify that you can ping the Admin Node.

```
[admin@berlin ~]$ ifconfig -a
[admin@berlin ~]$ [Admin Node IP]
```

Upgrading the Software on the New EC

Note: This will become the new secondary EC in the system you are upgrading.

1 As **dncs** user, enter the following commands to kill the **Initd** processes.

```
[dncs@berlin ~]$ appKill
[dncs@berlin ~]$ dncsKill
```

2 As **admin** user, type the following command to see if the **CSCOec-lic** package is installed on the system.

```
[admin@berlin ~]$ rpm -qa | grep -i cscoec-lic
```

3 Is the **CSCOec-lic** package installed on your system?

- If **yes**, go to Step 4.
- If **no**, go to Step 5.

4 Enter the following command to remove the **cscoec-lic** package.

Command Syntax:

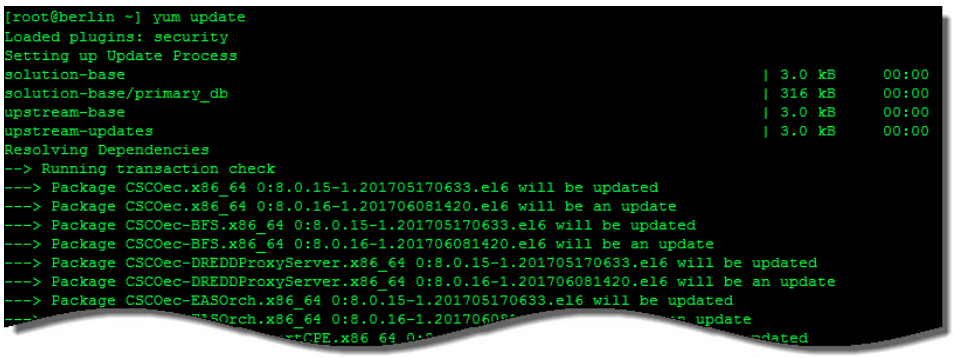
```
sudo rpm -e CSCOec-lic-[version]
```

Example:

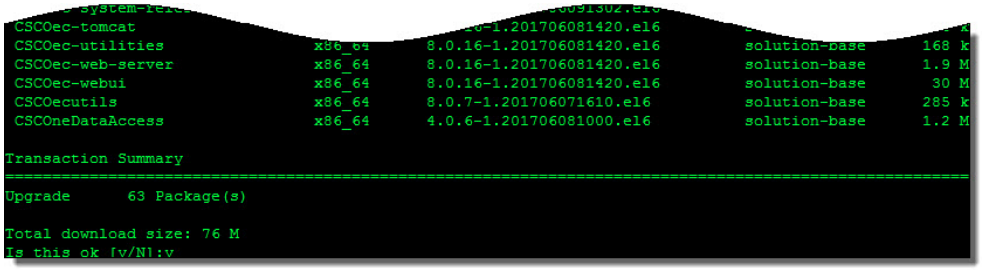
```
[admin@berlin ~]$ sudo rpm -e
CSCOec-lic-8.0.17-1.201706230635.el6.x86_64
```

5 Type the following command to upgrade the EC software. A verification of the repos occurs and a check is done to verify which packages need upgraded.

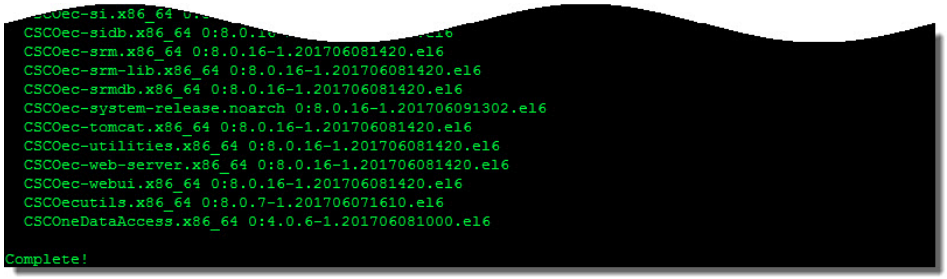
```
[admin@berlin ~]$ sudo yum update
```



6 Once the packages are resolved and a list of the packages to upgrade is displayed, you are prompted to confirm the downloading of the packages.



7 Enter **y** and press **Enter**. The update of the packages begins and, when complete, a **Complete!** message displays.



8 Did the yum update complete successfully?

- If **yes**, go to Step 9.
- If **no**, go to Step 10.

9 Enter the following command to reboot the server. Then go to the next section in this appendix.

```
[admin@berlin ~]$ sudo shutdown -r now
```

10 Log back into the EC and review the following log to see if any error messages exist.

```
[root@berlin ~]# less /var/log/yum.log
```

11 If errors exist and you cannot determine the issue, execute one of the following options.

- Contact Cisco Services.
- Rollback the upgrade.

  Note: To rollback the upgrade, go to the next step.

12 Type the following command to shutdown the VM

```
[admin@berlin ~]$ sudo shutdown -h now
```

13 From the vSphere Web UI, right-click the VM and select **All vCenter Actions > Power > Power Off**.

14 Monitor the **Recent Tasks** area to verify that the VM successfully powered off.

15 Right-click the original VM host and select **Power On**.

Enabling RepDB on the Upgraded System

To enable RepDB on the upgraded system, refer to the following two sections in Chapter 7, ***Configure and Operate the Replicated Database***.

- ***Adding the RepDB Network Adapter on the Primary and Secondary VMs*** (on page 121)
- ***Enabling RepDB*** (on page 127)

E

EC SR 8.0 Patch Installs

This section describes the procedures to install a patch to the primary and secondary ECs in your NextX system.

The format for an EC patch is: **CSCOec-patch-[VERSION].[DATE].[PLATFORM].rpm**

The version for the first CSCOec-patch package is always "-2" (i.e. CSCOec-patch-8.0.19**.-2**.[VERSION].[DATE].[PLATFORM].rpm). The version for any future patches is numbered incrementally (i.e. CSCOec-patch-8.0.19-**3**.[VERSION].[DATE].[PLATFORM].rpm).

In addition, each new patch is a cumulative patch, as it will include all patches previous to the current package version.

In This Appendix

Preparing for a Patch Upgrade

Complete the following steps prior to executing the patch upgrade.

1 Are you using vSphere Web UI or vSphere client?

- If **yes**, clone your *primary* system to create a full system backup.
- If **no** and you are using an ESXi client, back up the database and key files to an NFS mount.

Note: For details about cloning and system backups, refer to the ***Backup and Restore User Guide for EC 8.0 and DTACS 5.0*** document.

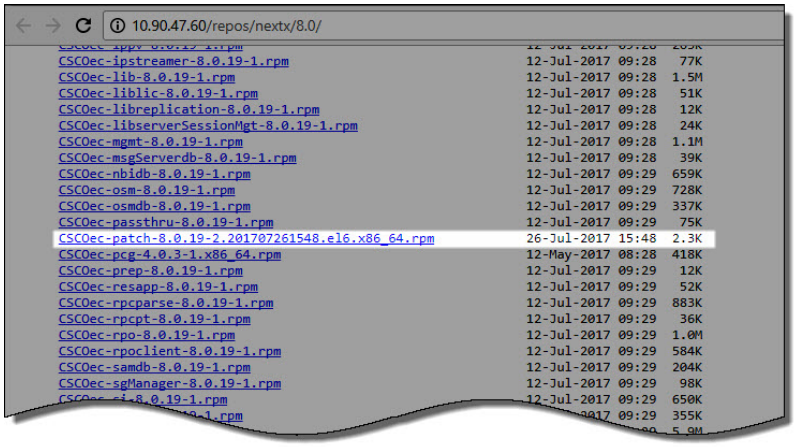
2 From a Web browser, enter the following command to verify that the patch has been deployed on the Admin Node that is associated with your system.

URL Syntax:

`http://[Admin_Node_IP]/repos/nextx/8.0/`

Example:

`http://10.90.47.60/repos/nextx/8.0/`



3 Is the **CSCOec-patch** RPM present?

- If **yes**, go to the next section.
- If **no**, refer to the **Updating the Application Packages Repo** section in the ***Admin Node Installation Guide*** to update the NextX repo with the patch software.

Installing an EC Patch

A patch install to your primary and secondary servers requires you to disable and deactivate Replicated Database prior to the installation. This is because upgraded database transactions on the primary server should not flow to the secondary server until it has been patched as well.

Complete the following procedure to install a patch to your system.

1 As **admin** user, enter the following command to disable RepDB on *the* primary server.

```
[dncs@vodwater ~]$ sudo /opt/cisco/repdb/RepDb -d
```

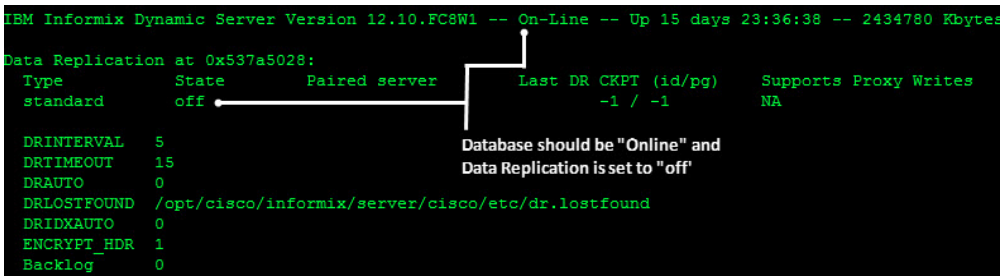
2 Enter the following command to deactivate RepDB on *the* primary server.

```
[dncs@vodwater ~]$ sudo /opt/cisco/repdb/RepDb -D
```

3 Repeat Steps 1 through 2 on the *secondary* server.

4 As **root** user, enter the following command on both the *primary* and *secondary* servers to verify that RepDB is disabled.

```
[root@vodwater ~]# onstat -g dri
```



5 As **dncs** user on the *primary* server, enter the following commands to stop processes.

```
[dncs@vodwater ~]$ appStop
[dncs@vodwater ~]$ dncsStop
[dncs@vodwater ~]$ appKill
[dncs@vodwater ~]$ dncsKill
```

6 Enter the following command to verify if a **CSCOec-patch** package is currently installed on the EC?

```
[dncs@vodwater ~]$ rpm -qa | grep -i CSCOec-patch
```

7 Does a **CSCOec-patch** package exist on the system?

- If **no**, enter the following command. The script sets up the install process and verifies dependencies; and then displays an **Is this ok [y/N]** message.

  Note: If this is the first time you are installing an EC patch, enter the full package name in the installation command.

  Command Syntax:

  ```
  sudo yum install CSCOec-patch-[VERSION].[DATE].[PLATFORM]
  ```

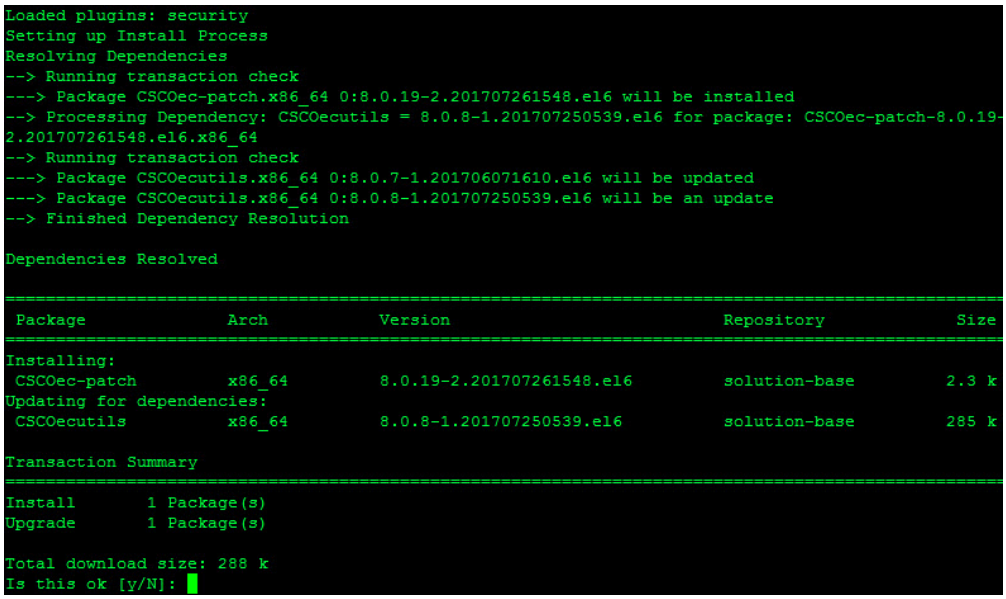
  Example:

  ```
  [admin@vodwater ~]$ sudo yum install
  CSCOec-patch-8.0.19-2.201707261548.el6.x86_64
  ```

- If **yes** and you are installing a newer CSCOec-patch, enter the following command. The script sets up the install process and verifies dependencies; and then displays an **Is this ok [y/N]** message.

  Note: If a previous patch is present, enter only the patch name with an asterisk (*). The asterisk is a wildcard and installs the most current version of the EC patch that is in the NextX repo.

  ```
  [admin@vodwater ~]$ sudo yum update CSCOec-patch*
  ```



8 Type **y** and press **Enter**. The installation continues and when finished, a **Complete!** message displays.

Note: The output from this particular patch install indicates that the CSCOec-patch and the CSCOecutils packages were downloaded and installed. Subsequent patch installs will contain different RPMs as required.

```
ecutils                                                                    539.el6

Transaction Summary
================================================================================
Install       1 Package(s)
Upgrade       1 Package(s)

Total download size: 288 k
Is this ok [y/N]: y
Downloading Packages:
(1/2): CSCOec-patch-8.0.19-2.201707261548.el6.x86_64.rpm   | 2.3 kB     00:00
(2/2): CSCOecutils-8.0.8-1.rpm                             | 285 kB     00:00
--------------------------------------------------------------------------------
Total                                          6.2 MB/s | 288 kB     00:00
Running rpm_check_debug
Running Transaction Test
Transaction Test Succeeded
Running Transaction
  Updating   : CSCOecutils-8.0.8-1.201707250539.el6.x86_64                 1/3
Post Install complete
  Installing : CSCOec-patch-8.0.19-2.201707261548.el6.x86_64               2/3
  Cleanup    : CSCOecutils-8.0.7-1.201706071610.el6.x86_64                 3/3
  Verifying  : CSCOec-patch-8.0.19-2.201707261548.el6.x86_64               1/3
  Verifying  : CSCOecutils-8.0.8-1.201707250539.el6.x86_64                 2/3
  Verifying  : CSCOecutils-8.0.7-1.201706071610.el6.x86_64                 3/3

Installed:
  CSCOec-patch.x86_64 0:8.0.19-2.201707261548.el6

Dependency Updated:
  CSCOecutils.x86_64 0:8.0.8-1.201707250539.el6

Complete!
```

9 Enter the following command to verify that the **CSCOec-patch** package successfully installed, as well as any other packages.

Command Syntax:

```
rpm –qa | egrep "[package_name_1] | [package_name_2]
[package_name_n]"
```

Example:

```
[admin@vodwater ~]$ rpm -qa | egrep -i "CSCOec-patch|ecutils"
CSCOecutils-8.0.8-1.201707250539.el6.x86_64
CSCOec-patch-8.0.19-2.201707261548.el6.x86_64
```

10 Enter the following command to query the patch package and view the release date, the version, other installed packages, and the issues corrected in the patch.

Command Syntax:

```
rpm -q --changelog CSCOec-patch-[VERSION].[DATE].[PLATFORM]
```

Example:

```
[admin@vodwater ~]$ rpm -q --changelog
CSCOec-patch-8.0.19-2.201707261548.el6.x86_64
* Tue Jul 25 2017 - 8.0.19-2
CSCOecutils-8.0.8-1.rpm

- CSCvf16242 cvtChecker script fails to execute
- CSCvf16318 Utility script version should be correct and uniform
```

11 Enter the following command to reboot the server.

```
[admin@vodwater ~]$ sudo shutdown –r now
```

12 Log back into the server and, as **dncs** user, enter the following commands to start processes.

```
[dncs@vodwater ~]$ dncsStart
[dncs@vodwater ~]$ appStart
```

13 Verify server functionality.

14 Is your server functioning properly?

- If **yes**, and you successfully installed the patch on the *primary* EC, go to the next step.
- If **yes** and you successfully installed the patch on the *primary* and the *secondary* EC servers, go to Step 16.
- If **no**, troubleshoot the system. If you cannot remedy the issue, contact Cisco Services.

  Note: You can also choose to uninstall the patch. Refer to the next section for details.

15 Repeat Steps 6 through 14 on the *secondary* system.

16 Refer to ***Configure RepDB*** (on page 121) to re-enable replicated database on your system.

Uninstalling an EC Patch

Complete the following steps to uninstall an EC patch. This procedure also downgrades any packages that were installed/upgraded as dependencies to the patch installation.

Note: Replicated Database should still be disabled.

1 As **dncs** user on the *primary* server, enter the following commands to stop processes.

```
[dncs@vodwater ~]$ appStop
[dncs@vodwater ~]$ dncsStop
[dncs@vodwater ~]$ appKill
[dncs@vodwater ~]$ dncsKill
```

2 Enter the following command to verify the current version of the **CSCOec-patch**.

```
[dncs@vodwater ~]$ rpm -qa | grep -i CSCOec-patch
```

```
CSCOec-patch-8.0.19-2.201707261548.el6.x86_64
```

3 As **admin** user, enter the following command to obtain the **ID** of the CSCOec-patch installation.

```
[admin@vodwater ~]$ sudo yum history package-list
CSCOec-patch\*
```

```
Loaded plugins: security
ID     | Action(s)      | Package
-------------------------------------------------------------------------------
    69 | Install        | CSCOec-patch-8.0.19-2.201707261548.el6.x86_64      EE
history package-list
```

4 From the **ID** column, record the ID number for the CSCOec-patch installation.

ID Number _____

5 Enter the following command to uninstall/downgrade the patch using the ID number you recorded in the previous step. An **Is this ok [y/N]** message displays.

Command Syntax:

```
sudo yum history undo [ID_number]
```

Example:

```
[admin@vodwater ~]$ sudo yum history undo 69
```

```
Resolving Dependencies
--> Running transaction check
---> Package CSCOec-patch.x86_64 0:8.0.19-2.201707261548.el6 will be erased
---> Package CSCOecutils.x86_64 0:8.0.7-1.201706071610.el6 will be a downgrade
---> Package CSCOecutils.x86_64 0:8.0.8-1.201707250539.el6 will be erased
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================
 Package              Arch           Version                      Repository          Size
================================================================================
Removing:
 CSCOec-patch         x86_64         8.0.19-2.201707261548.el6    @solution-base      0.0
Downgrading:
 CSCOecutils          x86_64         8.0.7-1.201706071610.el6     solution-base       285 k

Transaction Summary
================================================================================
Remove        1 Package(s)
Downgrade     1 Package(s)

Total download size: 285 k
Is this ok [y/N]:
```

6 Type **y** and press **Enter**. The downgrade proceeds, and when finished, a **Complete!** message displays.

Note: In this example, the script deletes the CSCOec-patch and downgrades the CSCOecutils package. When you execute this script for subsequent patch installs, it deletes and/or removes different RPMs as required.

```
Downloading Packages:
CSCOecutils-8.0.7-1.rpm                                    | 285 kB     00:00
Running rpm_check_debug
Running Transaction Test
Transaction Test Succeeded
Running Transaction
  Installing : CSCOecutils-8.0.7-1.201706071610.el6.x86_64                  1/3
Post Install complete
  Erasing    : CSCOec-patch-8.0.19-2.201707261548.el6.x86_64                2/3
  Cleanup    : CSCOecutils-8.0.8-1.201707250539.el6.x86_64                  3/3
  Verifying  : CSCOecutils-8.0.7-1.201706071610.el6.x86_64                  1/3
  Verifying  : CSCOecutils-8.0.8-1.201707250539.el6.x86_64                  2/3
  Verifying  : CSCOec-patch-8.0.19-2.201707261548.el6.x86_64                3/3

Removed:
  CSCOec-patch.x86_64 0:8.0.19-2.201707261548.el6      CSCOecutils.x86_64 0:8.0.8-1.201707250539.el6

Installed:
  CSCOecutils.x86_64 0:8.0.7-1.201706071610.el6

Complete!
```

7 Enter the following command to verify the current versions of the patches and any other packages that were downgraded.

Note: If this was the first time a CSCOec-patch was installed, no output is displayed for this package.

Command Syntax:

```
rpm –qa | egrep "[package_name_1] | [package_name_2]
[package_name_n]"
```

Example:

```
[admin@vodwater ~]$ rpm -qa | egrep -i "CSCOec-patch |
ecutils"
```

```
[admin@vodwater ~] rpm -qa | egrep -i "CSCOec-patch|ecutils"
CSCOecutils-8.0.7-1.201706071610.el6.x86_64
```

8 Enter the following command to reboot the server.

```
[admin@vodwater ~]$ sudo shutdown –r now
```

9 Log back into the server and, as **dncs** user, enter the following command to start processes.

```
[dncs@vodwater ~]$ dncsStart
[dncs@vodwater ~]$ appStart
```

10 Verify EC functionality.

11 Is your EC functioning properly?

- If **yes**, go to the next step.
- If **no**, refer to the ***Backup and Restore User Guide for EC 8.0 and DTACS 5.0*** to restore your system.

12 Refer to ***Configure RepDB*** (on page 121) to re-enable replicated database on your system.

F

Setting Up the Network Time Protocol on Servers and Clients

Introduction

The instructions in this appendix describe how to set up the Network Time Protocol (NTP) on servers and clients.

In This Appendix

Configure NTP on the Server

By default, the EC is configured to use the internal clock for timing. Follow these instructions to configure the EC to obtain timing from an external NTP server.

Note: Obtain the primary and any secondary NTP source IP addresses from the system operator.

1 As **admin** user, enter the following command to edit the **/etc/inet/ntp.conf** file in a text editor.

```
[admin@vodwater ~]$ sudo vi /etc/ntp.conf
```

2 Go to the end of the file and enter the IPs for your NTP servers in the following format.

Syntax:

```
server [NTP IP 1] iburst
server [NTP IP 2] iburst
```

Example:

```
server 10.90.44.40 iburst
server 10.90.44.41 iburst
```

3 Press **Enter** twice and then enter the following:

```
# Driftfile.
driftfile /var/lib/ntp/drift
```

4 Save and close the **ntp.conf** file.

5 Type the following command and press **Enter**.

```
[admin@vodwater ~]$ sudo service ntpd status
```

6 Did the output from step 5 show ntpd running?

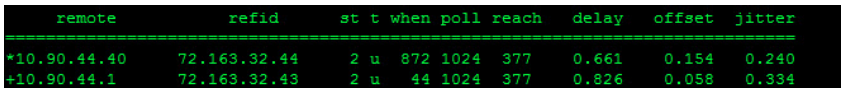
- If **yes**, continue with the next step.
- If **no**, type the following command and press **Enter**. Then, go to the next step.

  ```
  [admin@vodwater ~]$ sudo service ntpd start
  ```

7 Type the following command and press **Enter** to check the status of the NTP:

```
[admin@vodwater ~]$ sudo ntpq -p
```

Result: You should see output similar to the following:



```
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*10.90.44.40     72.163.32.44     2 u  872 1024  377    0.661    0.154   0.240
+10.90.44.1      72.163.32.43     2 u   44 1024  377    0.826    0.058   0.334
```

Note: It takes the NTP daemon a few minutes to decide which server will be the primary server after the ntp server is restarted. An asterisk appears next to the source that is being referenced.

Configure NTP on the Client

Follow these instructions to configure NTP on the new client.

Note: A "client" can be any device that uses the EC server to configure its time.

1 If necessary, open a remote terminal window on the client.

2 As **admin** user, type the following command and press **Enter** to initialize the /etc/ntp.conf file as a client:

```
[admin@vodwater ~]$ sudo /dvs/platform/libexec/install_ntp -c
```

Note: The default settings for the client ntp.conf file use the host "dncs_host" as the time server. If you want to change this setting, use a text editor to edit the ntp.conf file.

3 Type the following command and press **Enter** to restart the NTP service:

```
[admin@vodwater ~]$ sudo service ntpd restart
```

4 Type the following command and press **Enter** to check the status of the NTP service:

```
ntpq
```

Result: You should see output similar to the following:

```
remote    refid         st t when poll reach delay offset    disp
==============================================================
*ISDS     198.51.100.44  4 u   39   64    7  0.30  -9.535 1939.02
LOCAL(0)  LOCAL(0)       5 l   41   64    7  0.00   0.000 1937.99
```

Note: It takes the NTP daemon a few minutes to decide which server will be the primary server after the ntp server is restarted. An asterisk appears next to the source that is being referenced.

G

EC 8.0 Procedures Specific to DTACS 4.1

This appendix provides procedures specific to EC 8.0 systems that include DTACS 4.1 servers. These procedures must be completed for the EC and DTACS servers to communicate to one another.

In This Appendix

Configuring the SSH Key Exchange Between EC 8.0 and DTACS 4.1 Systems

Complete the following procedure to configure and execute the SSH key exchange between the EC 8.0 and DTACS 4.1 server.

1 Complete the following steps as **admin** user on the ***EC 8.0*** system.

a Type the following command to change to the **dncsSSH** user.

```
[admin@vodwater ~]$ sudo su - dncsSSH
```

b Enter the following command to generate an rsa key for the dncsSSH user.

```
[dncsSSH@vodwater ~]$ ssh-keygen -t rsa -N "" -f
/home/dncsSSH/.ssh/siteKey
```

```
Generating public/private rsa key pair.
Your identification has been saved in /home/dncsSSH/.ssh/siteKey.
Your public key has been saved in /home/dncsSSH/.ssh/siteKey.pub.
The key fingerprint is:
7f:83:06:5f:e2:de:e8:51:92:b2:f9:95:4d:65:00:fc dncsSSH@conan1
The key's randomart image is:
+--[ RSA 2048]----+
|          ....   |
|           .  . |
|            .  o|
|           .  Eo |
|        S + o .  |
|         O * +   |
|        o B = .  |
|         + * .   |
|          .= .   |
+-----------------+
```

c Enter the following command to create the **/home/dncsSSH/.ssh/siteConfig** file with the content **StrictHostKeyChecking no**.

```
[dncsSSH@vodwater ~]$ echo StrictHostKeyChecking no >
/home/dncsSSH/.ssh/siteConfig
```

d Enter the following command to add **PasswordAuthentication no** to the **/home/dncsSSH/.ssh/siteConfig** file.

```
[dncsSSH@vodwater ~]$ echo PasswordAuthentication no >>
/home/dncsSSH/.ssh/siteConfig
```

e Enter the following command to verify the contents of the **/home/dncsSSH/.ssh/siteConfig** file.

```
[dncsSSH@vodwater ~]$ cat /home/dncsSSH/.ssh/siteConfig
```

```
StrictHostKeyChecking no
PasswordAuthentication no
```

f Type `exit` to return to the **admin** user session.

g Enter the following command to change the ownership of the **/home/dncsSSH/.ssh/site*** directories to **dncs:dncs**.

```
[admin@vodwater ~]$ sudo chown dncs:dncs
/home/dncsSSH/.ssh/site*
```

h Enter the following command to securely copy the **siteKey.pub** file to the DTACS 4.1 system.

```
[admin@vodwater ~]$ sudo scp /home/dncsSSH/.ssh/siteKey.pub
root@dtacs:/export/home/dncsSSH/.ssh/siteKey.pub.EC8
```

2 Complete the following steps as **root** user on the ***DTACS 4.1*** system.

a Enter the following command to change to the **dncsSSH** user.

```
# su - dncsSSH
```

b Enter the following command to generate an rsa key for the dncsSSH user.

```
$ ssh-keygen -t rsa -N "" -f
/export/home/dncsSSH/.ssh/siteKey
```

c Enter the following command to create the **/home/dncsSSH/.ssh/siteConfig** file with the content **StrictHostKeyChecking no**.

```
$ echo StrictHostKeyChecking no >
/export/home/dncsSSH/.ssh/siteConfig
```

d Enter the following command to add **PasswordAuthentication no** to the **/home/dncsSSH/.ssh/siteConfig** file.

```
$ echo PasswordAuthentication no >>
/export/home/dncsSSH/.ssh/siteConfig
```

e Type `exit` to return to the **root** user session.

f Enter the following command to change the ownership of the **/home/dncsSSH/.ssh/site*** directories to **dncs:dncs**.

```
# chown dncs:dncs /export/home/dncsSSH/.ssh/site*
```

g Enter the following command to securely copy the **siteKey.pub** file to the EC 8.0 system.

```
# sudo scp /export/home/dncsSSH/.ssh/siteKey.pub
admin@dncsatm:/tmp/siteKey.pub.DTACS
```

h Enter the following command to SSH to the EC 8.0 system as **admin** user and copy the **siteKey.pub.DTACS** file to the **/home/dncsSSH/.ssh** directory.

```
# ssh admin@dncsatm sudo cp /tmp/siteKey.pub.DTACS
/home/dncsSSH/.ssh/siteKey.pub.DTACS
```

i Enter the following command to change to the **/export/home/dncsSSH/.ssh** directory.

```
# cd /export/home/dncsSSH/.ssh
```

j Enter the following command to redirect the contents of the **siteKey.pub.DTACS** to a new file named **authorized_keys2**.

```
# cat siteKey.pub.EC8 > authorized_keys2
```

3 As **admin** user on the ***EC 8.0*** system, complete the following steps.

a Change the ownership of the **/home/dncsSSH/.ssh/siteKey.pub.DTACS** file to **dncs:dncs**.

```
[admin@vodwater ~]$ sudo chown dncs:dncs
/home/dncsSSH/.ssh/siteKey.pub.DTACS
```

b Enter the following command to change to the **/home/dncsSSH/.ssh** directory.

```
[admin@vodwater ~]$ cd /home/dncsSSH/.ssh
```

c Enter the following command to redirect the content of the **siteKey.pub.DTACS** file to a new file named **authorized_keys2**.

```
[admin@vodwater ~]$ sudo cat siteKey.pub.DTACS >
authorized_keys2
```

d Enter the following command to transfer the **siteKey** file to the DTACS 4.1 system.

```
[admin@vodwater ~]$ sudo ssh -X -i
/home/dncsSSH/.ssh/siteKey dncsSSH@dtacs
```

4 As **root** user on the ***DTACS 4.1*** system, enter the following command to transfer the **siteKey** to the SR 8.0 system.

```
# ssh -X -i /export/home/dncsSSH/.ssh/siteKey dncsSSH@dncsatm
```

Modifying Database-related Files on the EC 8.0 and DTACS 4.1 Systems

Complete the following procedure to modify database-related files on the EC 8.0 and DTACS 4.1 servers.

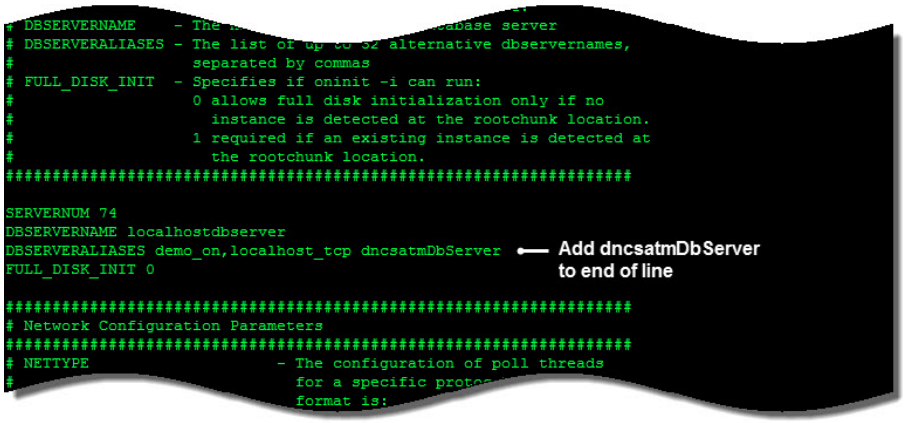
1 Complete the following steps as **admin** user on the ***EC 8.0*** server to update database-related files.

a Enter the following command to edit the **/opt/cisco/informix/server/etc/onconfig** in a text editor.

```
[admin@vodwater ~]$ sudo vi
/opt/cisco/informix/server/etc/onconfig
```

b Go to the DBSERVERALIASES line and add **dncsatmDbServer** to the end of the line.

Example:



c Save and close the **onconfig** file.

d Enter the following command to edit the **/opt/cisco/informix/server/etc/sqlhosts** in a text editor.

```
[admin@vodwater ~]$ sudo vi
/opt/cisco/informix/server/etc/sqlhosts
```

e Add the following line to the end of the file.

```
dncsatmDbServer      onsoctcp      dncsatm     sqlexec
```

f Save and close the **sqlhosts** file.

g As **root** user, enter the following command to source the environment.

```
[root@vodwater ~]# . /dvs/dncs/bin/dncsSetup
```

h Enter the following command to start the database.

```
[root@vodwater ~]# onmode -P start dncsatmDbServer
```

i Enter the following command to add the following dtacs entries to the **/etc/hosts.equiv** file.

Note: The dtacs entry (first entry in each row) must be the same as the first entry for dtacs in the /etc/hosts file.

```
[root@vodwater ~]# vi /etc/hosts.equiv
```

Example:

```
dtacs  dtacs
dtacs  dncs
dtacs  root
```

2 Complete the following steps as **root** user in the ***DTACS 4.1*** to update database-related files.

a Enter the following command to edit the **/etc/services** file in a text editor.

```
# vi /etc/services
```

b Add the following entries into the **services** file.

```
sqlexec 9088/tcp # IBM Informix SQL Interface
sqlexec 9088/udp # IBM Informix SQL Interface
```

c Save and close the file.

d Open the **/export/home/informix/etc/sqlhosts** file in a text editor.

```
# vi /export/home/informix/etc/sqlhosts
```

e Add the following line to the end of the **sqlhosts** file.

```
dncsatmDbServer     ontlitcp    dncsatm   sqlexec
```

f Save and close the file.

g As **dncs** user, enter the following command to source the dtacs environment.

```
$ . /dvs/dtacs/bin/dtacsSetup
```

h Enter the following command to verify that you can access the database. A **Database selected** output should appear and you should be at a **>** prompt.

```
$ dbaccess dncsdb@dncsatmDbServer -
```

i Press **Ctrl+C** to exit the database.

j Enter the following command to test the database sync. If successful, a **Sync DB request processed successfully** message will display.

```
$ /dvs/dtacs/bin/dtacsdbsync -S
```

H

Procedures When Using an ESXi Client

This appendix describes various procedure when deploying and reconfiguring VMs using a vSphere client.

In This Appendix

Deploy and Configure a VM Using an ESXi Client

Deploying a Virtual Machine Using an ESXi Client

Complete the following steps to deploy a VM from the ESXi client.

1. Log on to the ESXi client.
2. Select the appropriate ESXi host and click **File > Deploy OVF Template**. The Source window displays.
3. Click **Browse** and navigate to the directory where the Cisco platform OVA resides.
4. Select the OVA and click **Open**. The absolute path to the OVA is added to the text box in the Source Window.
5. Click **Next**. The OVF Template Details window displays.
6. Review the details and click **Next**. The End User License Agreement displays.
7. Review the license agreement and click **Accept**. Then click **Next**. The Name and Location window display.
8. From the **Name** text box, type a name that describes the VM.
9. Click **Next**. The Deployment Configuration window displays.
10. From the **Configuration** dropdown, select **4 CPU 8GB RAM 20GB DISK** and then click **Next**. The Storage window displays.
11. Select the appropriate storage device and click **Next**. The Disk Format window displays.
12. Maintain the default selection, **Thick Provisioned Lazy Zeroed** and click **Next**. The Network Mapping window displays.
13. For the source network, click the dropdown in the **Destination Networks** column and select the corporate network.
14. Click **Next**. The Ready to Complete window displays.
15. Click **Finish**. The VM deployment starts. A window opens that shows the progress of the deployment, and when it completes, a **Completed Successfully** message appears.

Reconfiguring the Virtual Network Using an ESXi Client

Complete the following steps to reconfigure the virtual hardware for the SR 8.0 VM using an ESXi client.

1. Select and right-click the new SR 8.0 VM. The Edit Settings window displays.
2. Click **Memory** and modify the value to **64 GB**.

   Note: Make sure you change MB to **GB**.
3. Click **CPUs** and then from the **Number of virtual sockets** dropdown list, select **8**.
4. Select **Hard disk 1** and modify the **Provisioned Size** to **64** GB.
5. Click the **Add** button. The Device Type window opens.
6. Select **Hard Disk** and then click **Next**.
7. Maintain the **Create a new virtual disk** selection and click **Next**.
8. Change the Disk Size to **384** and maintain all other default selections. Then click **Next**.
9. Click **Next** again. The Ready to Complete window displays.
10. Review the options and then click **Finish**. The new hard disk is added to the virtual machine list.
11. Click the **Add** button again and select **Ethernet Adapter**. Then click **Next**.
12. Maintain the VMXNET 3 adapter type and from the **Network** label dropdown menu, select the label that represents the **Headend** network. Then click **Next**. The Ready to Complete window displays.
13. Review the details and then click **OK**. The VM is reconfigured.
14. Review the options and then click **Finish**. The new Ethernet adapter is added to the virtual machine list.
15. Repeat Steps 11 through 14 to create another Ethernet Adapter with the label defined for the **TED** interface.

Setting the Power Policy Using a vSphere Client

1. Click the **ESXi** Host and then click the **Configuration** tab.
2. From the **Software** area, click **Virtual Machine Startup/Shutdown**.
3. Click **Properties** (located at the top right of the Startup Order window).
4. Check the **Allow virtual machines to start and stop automatically with the system** checkbox.
5. Highlight the VM and click **Move Up** until it is under **Automatic Startup**.
6. Click **OK**.

Modifying the Device Status for an Ethernet Adapter

During various procedures, you are directed to enable or disable the Connected and/or the Connected at power on options for the device status of an Ethernet adapter.

To modify these settings using the vSphere client, complete the following steps.

1. From the vSphere client, select and right-click the appropriate VM.
2. Click **Edit Settings**. The Virtual Machine Properties window opens.
3. Select the appropriate Network adapter. Details for the network adapter appear in the right area of the window.
4. From the **Device Status** section, execute either or both of the following steps, as needed.
   a. Click/unclick the **Connected** check box.
   b. Click/unclick the **Connect at power on** check box.
5. Click **OK** to save the setting.

Setting Up RepDB Using an ESXi Client

Complete the following procedure to set up RepDB using an ESXi client. Because the client only has a connection to a specific ESXi host, you cannot utilize the cloning feature. Instead, you will deploy a secondary VM.

1 As **admin** user on the *primary* EC, edit the **/etc/hosts** file to include the primary and secondary RepDB entries.

Note: You may substitute other names for HOSTA and HOSTB if you desire. However, these are the names that will be used throughout this guide.

```
[admin@berlin ~]$ sudo vi /etc/hosts
```

2 Save and close the file.

3 Enter the following command to verify the RepDB entries.

```
[admin@berlin ~]$ less /etc/hosts | grep -i host
```

Example Output:

```
172.16.3.131   HOSTA
172.16.3.132   HOSTB
```

4 Go to the following sections, in order, to deploy a secondary VM.

- ***Deploy and Configure a VM Using an ESXi Client*** (on page 206)
- ***Power on the New SR 8.0 VM*** (on page 33)
- ***Set Up the Network With a Static IP Configuration (Optional)*** (on page 35)
- ***SR 8.0 Application Installation*** (on page 39)

5 When you have completed these procedures, go to ***Adding the RepDB Network Adapter Using an ESXi Client*** (on page 209).

Adding the RepDB Network Adapter Using an ESXi Client

Complete the following steps to add a network adapter for RepDB on the primary and the secondary ECs.

1 From the vSphere ESXi client, right-click the *primary* VM and then select **Edit Settings**.

2 Just above the **Hardware** area, select the **Add...** button. The Device Type window displays.

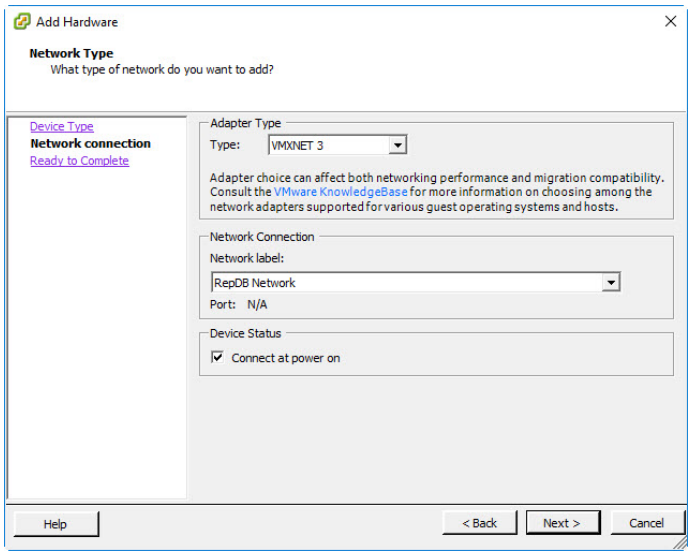
3 Select **Ethernet Adapter** and click **Next**.

4 From the **Type** dropdown menu, select **VMXNET 3**.

5 From the **Network label** dropdown, select the label for your RepDB network (e.g. RepDB Network).

6 Ensure the **Connect at power on** check box is selected and then click **Next**. The Ready to Complete window displays.

Example: Primary EC



7 Review the settings and if they are correct, click **Finish**. You are returned to the Edit Settings Window and the new NIC is listed in the Hardware area.

8 Click **OK**. The *primary* VM is reconfigured.

9 Right-click the *secondary* VM and then select **Edit Settings**.

10 Just above the **Hardware** area, select the **Add...** button. The Device Type window displays.

11 Select **Ethernet Adapter** and click **Next**.

12 From the **Type** dropdown menu, select **VMXNET 3**.

13 From the **Network label** dropdown, select the label for your RepDB network (e.g. RepDB Network).

14 Ensure the **Connect at power on** check box is selected and then click **Next**. The Ready to Complete window displays.

15 Review the settings and if they are correct, click **Finish**. You are returned to the Edit Settings Window and the new NIC is listed in the Hardware area.

16 Click **Network adapter 2** and select the **Connect at power on** checkbox.

17 Click **Network adapter 3** and select the **Connect at power on** checkbox.

18 Click **OK**. The *secondary* VM is reconfigured.

19 Monitor the **Recent Tasks** area until the task successfully completes.

20 Go to ***Creating an Interface Configuration File for RepDB*** (on page 123).

I

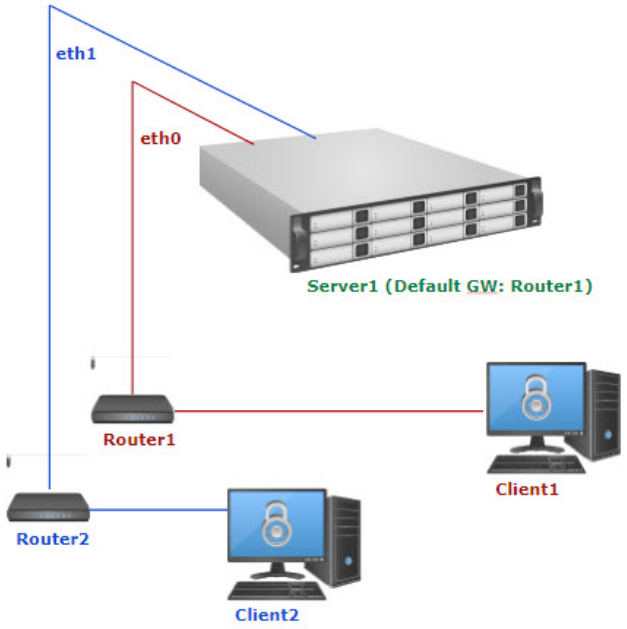
Configure Multiple Interfaces in a CentOS Environment

The instructions in this appendix describe how to configure multiple network interfaces in a CentOS environment.

In This Appendix

Background

RedHat distributions, including CentOS, do not allow multi-homed (multiple interfaces) servers to reply through a different interface from where the request came in. The following illustration demonstrates this issue:



- Client1 attempts to reach eth0.
- Server1 receives the request via eth0.
- Server1 tries to respond back using Router2 (default GW) but fails as Router2 is only accessible via a different interface from where the request originated (eth0).

Solution to this Issue

The solution to this issue relies on having two default gateways, one per interface. Refer to the next section for an example to configure two default gateways and two unique routing tables for each eth0 and eth1 network interface in your system.

Configuring Multiple Interfaces in CentOS

Complete the following procedure to configure multiple interfaces in your environment

Notes:

- Multiple default gateways work only for incoming traffic. Traffic initiated by the server still relies on its global default gateway and static routes.
- The following example includes two interfaces, eth0 and eth1, and two routing tables, table 1 for eth0, and table 2 for eth1.

  Example: Network Interface Configuration

  Important: Make sure to substitute the values for your system for the eth0 and eth1 interfaces, as well as for the global default gateway.

	IP Address/Mask Bits	Gateway
eth0	10.90.167.208/24	10.90.167.1
eth2	10.253.6.2/24	10.253.6.254
Global Default Gateway	N/A	10.253.6.254

1. As **admin** user, enter the following command to open the **/etc/sysconfig/network** file in a text editor.

   ```
   [admin@NextXvm ~]$ sudo vi /etc/sysconfig/network
   ```

2. Is the value for the **GATEWAY** field set to the global default gateway?
   - If **no**, update the value to the default global gateway. Then save and close the file.

     Example Input:

     ```
     NETWORKING=yes
     NOZEROCONF=yes
     RES_OPTIONS="rotate timeout:1 attempts:1"
     GATEWAY=10.253.6.254       #Global default gateway
     ```

   - If **yes**, close the file.

3 Enter the following command to configure the routes for the **eth0** interface (for example, from the previous table).

```
[admin@NextXvm ~]$ sudo vi
/etc/sysconfig/network-scripts/route-eth0
```

Note: In this example, the static route, 10.82.0.0.16 is used for traffic initiated from the server.

Example Input:

```
10.82.0.0/16 via 10.90.167.1  #(Optional) Specific unicast static route
for table 1
10.90.167.0/24 dev eth0 table 1
default via 10.90.167.1 dev eth0 table 1
```

4 Save and close the file.

5 Enter the following command to configure the routes for the **eth1** interface (table 2).

```
[admin@NextXvm ~]$ sudo vi
/etc/sysconfig/network-scripts/route-eth1
```

Example Input:

```
224.0.0.0/4 dev eth1  #(Optional) Specific multicast static route for
table 2
10.90.47.0/24 dev eth0  #(Optional) Specific unicast static route for
table 2
10.253.6.0/24 dev eth 1 table 2
default via 10.253.6.254 dev eth1 table 2
default via 10.253.6.254 dev eth1 table 254 #Traffic initiated from the
node
```

6 Save and close the file.

7 Enter the following command to create a rules file for the **eth0** interface.

```
[admin@NextXvm ~]$ sudo vi
/etc/sysconfig/network-scripts/rule-eth0
```

Example Input:

```
iif eth0 table 1
from 10.90.167.208 table 1
```

8 Save and close the file.

9 Enter the following command to create a rules file for the **eth1** interface.

```
[admin@NextXvm ~]$ sudo vi
/etc/sysconfig/network-scripts/rule-eth1
```

Example Input:

```
iif eth1 table 2
from 10.253.6.2 table 2
```

10 Save and close the file.

11 Enter the following command to reboot the server.

```
[admin@NextXvm ~]$ sudo shutdown –r now
```

12 When the server boots up, login as **admin** user.

Testing the Setup of the Network Interfaces

Complete the following procedure to test the setup of the network interfaces.

1 As **admin** user, enter the following command to check the rules defined for your network.

```
[admin@NextXvm ~]$ ip rule
```

Example Output:

```
0:      from all lookup local
32762:  from 10.253.6.2 lookup 2
32763:  from all iif eth1 lookup 2
32764:  from 10.90.167.208 lookup 1
32765:  from all iif eth0 lookup 1
32766:  from all lookup main
32767:  from all lookup default
```

2 Enter the following commands to verify the routing tables defined for your network.

```
[admin@NextXvm ~]$ ip route show table 1
```

Example Output:

```
10.90.167.0/24 dev eth0 scope link
default via 10.90.167.1 dev eth0
```

```
[admin@NextXvm ~]$ ip route show table 2
```

Example Output:

```
10.253.6.0/24 dev eth1 scope link
default via 10.253.6.254 dev eth1
```

```
[admin@NextXvm ~]$ ip route show table 254
```

Note: The routing table 254 is the default routing table.

Example Output:

```
10.253.6.0/24 dev eth1 proto kernel scope link src 10.253.6.2
10.90.167.0/24 dev eth0 proto kernel scope link src 10.90.167.208
default via 10.253.6.254 dev eth
```

3 Were the rules and routing tables set up correctly?

- If **yes**, you have completed this procedure.
- If **no**, refer to ***Configuring Multiple Interfaces in CentOS*** (on page 211) to make sure your network is configured correctly.

Index

E

H

I

L

M

N

O

P

R

S

T

U

V

W

X

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA

http://www.cisco.com
Tel: 408 526-4000
800 553-6387
Fax: 408 527-0883

March 2018

Part Number TP-00140