Upgrade an Existing Explorer Controller VM in System Release 6.0

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 upgrade of an existing Explorer Controller (EC) Virtual Machine (VM) in System Release (SR) 6.0.

SR 6.0 Upgrade Features

This upgrade to SR 6.0 allows you to create a new VM, independent of the current VM, on the existing Cisco Unified Computing System (UCS). The SR 6.0 EC upgrade also allows engineers to install the new SR on the new VM without having to shut the system down until the activation of the new system software.

Cisco engineers have expended great effort to ensure that the upgrade causes minimal system impact. However, there will be times during the upgrade where DHCTs will be unable to boot and where some functions (BFS, billing system control of STBs, etc.) will be interrupted. These outages will likely go unnoticed by the vast majority of subscribers.

How Long to Complete the Upgrade?

The upgrade to SR 6.0 is to be completed within a 6-hour maintenance window that usually begins at midnight. All of the planning and preparation work can be done without impacting normal operations (Chapters 2 through 4) and should be completed before the start of the maintenance window. The maintenance window activities begin when you stop system components in Chapter 5.

System Performance Impact

Interactive services will not be available during the maintenance window.

Audience

This guide is written for field service engineers and system operators who are responsible for upgrading an existing SR 6.0 EC.

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 at 1-866-787-3866 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 EC software need the following skills:

- Advanced knowledge of UNIX
  - Experience with the UNIX vi editor. Several times throughout the system upgrade process, system files are edited using the UNIX vi editor. The UNIX 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 DBDS system expertise
  - The ability to identify keyfiles that are unique to the site being upgraded
  - The ability to add and remove user accounts

Installation/Migration Requirements

Before beginning the upgrade to SR 6.0, be sure that the site you are upgrading meets these requirements:

- You have at least one of the following in order to complete the required backups of the database and the file system:
  - The SR 6.0.x ISO image
  - Backup and Restore scripts available from Cisco
- You are currently running SR 6.0.x
- 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.

Recommended Web Browser

The WUIs have been tested and verified against the Mozilla Firefox ESR version 24 browser. Due to unpredictable results with other browsers, we highly recommend that you only use Mozilla Firefox ESR version 24 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.

Important: To prevent automatic updates to the Firefox browser, you must change your update preferences. See **Turn Off Firefox Automatic Updates** (which follows) for instructions.

Turn Off Firefox Automatic Updates

1. Open the Firefox ESR 24 browser.
2. Choose **Firefox > Options > Options** to open the Options window.
3. Click the **Update** tab.
4. In the Firefox updates section, select either the **Check for updates but let me choose whether to install them** or the **Never check for updates** option.
5. Click **OK**.

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

If the site you are upgrading supports a non-Cisco Application Server, contact the vendor of that Application Server in order to obtain upgrade requirements, as well as upgrade and rollback procedures.

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

Important: Be certain that all third-party vendors are aware that the SR 6.0 upgrade is built upon a Solaris 10 (x86) software platform.

Supported Server Platform

The following Cisco UCS server hardware platform is supported by the SR 6.0 release:

EC Server

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

Important: The procedures in this guide deal primarily with the setup and configuration of the UCS C240 M3 server. The SR 6.0 release also supports the UCS C210 M2 server. This server, however, is recommended only for lab environments. If you are setting up a C210 server in a lab, refer to Cisco UCS C210 Server Configuration. This appendix contains details pertinent to the C210 server.

Document Version

This is the first formal release of this document.

1

Planning the Upgrade

Introduction

This chapter contains information that helps system operators and Cisco engineers plan the upgrade in order that system downtime can be minimized.

In This Chapter

Important Points About the Upgrade

Enhanced Security for SR 6.0

SR 6.0 includes the enhanced security which changes the way you will interact with and administer the system. Refer to *Explorer Controller Security Configuration Guide* (part number OL-27574) if you are unfamiliar with the changes implemented as a result of the security enhancements. There are fundamental changes you must be aware of to perform some of the most basic functions on the EC.

Single Sign-on

By default, users are not permitted to have more than one login session. This means that any user using the Secure Shell (SSH) to remotely access the EC or the RNCS EC is not allowed to establish a second connection, even from the same remote system, until the first session has been disconnected. However, the user is not restricted as to the number of remote terminal windows that can be launched from a single SSH session.

Non-Essential Services Disabled by Default

All services that are not essential to the operation and administration of the EC (telnet, rlogin, rsh, etc.) are disabled by default.

Note: FTP and TFTP will continue to be enabled by default.

Performance Impact

Interactive services will not be available while you are within the maintenance window, for example, after EC processes are stopped.

SR 6.0 Upgrade Requirements

Before beginning the upgrade to SR 6.0, be sure that the site you are upgrading meets these requirements:

- You have the SR 6.0.0.x ISO file which includes the ISO image and the backup and restore scripts.
- You have the Solaris 10 x86 Update 11 license and ISO image.
- You are currently running SR 6.0.0.x.
- 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.

Estimated Timeline

The upgrade to SR 6.0 provides the ability to stage a new VM on the Cisco UCS server with the upgraded operating system and application software prior to 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 may involve resetting the modulators. Review the release notes to determine if the modulator code is going to be upgraded. Our engineers recommend that you never reset more than eight modulators at once. 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

Third Party Applications

If the site you are upgrading supports a non-Cisco Application Server, contact the vendor of that Application Server in order to obtain upgrade requirements, as well as upgrade and rollback procedures.

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

Important:

- Be certain that all third-party vendors are aware that the SR 6.0 upgrade is built upon a Solaris 10 (x86) software platform.
- If the site you are upgrading uses a third-party application server, before you start the system processes, you need to comment out the line in the /etc/hosts file that is similar to the following:

```
203.0.113.10    appservatm  appserv_host   ppv_manager_host
vc_server_host  Config_manager_host
```

Plan What Optional Features Will be Supported

An upgrade can contain additional optional features that system operators can elect to enable on their systems. Some of these features require that the system operator obtain a special license for the feature to be activated; others can simply be activated by our engineers without a special license.

Determine what optional features (licensed or unlicensed) need to be enabled as a result of this upgrade. You will 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 your Cisco account representative to purchase the required license. Then coordinate with Cisco Services to have the feature enabled at the proper time during the migration/upgrade.

Important:

- Any features that have been previously enabled or licensed as part of an earlier upgrade do not have to be re-enabled.
- If you are migrating from a GQAM to an RFGW as part of the migration to GigE BFS, you need to have the GQI QAM Support feature on the EC. Contact Cisco Services for this license.

About the preUpgradeChecks Script

The preUpgradeChecks scripts are contained in the EC PUC kit. This kit must be downloaded from the following Cisco URL:

```
https://upload.cisco.com/cgi-
bin/swc/fileexg/main.cgi?CONTYPES=ITE_LT
```

You will download the PUC ISO and the pre-upgrade document, *System Release Pre-Upgrade Checks* (part number OL-32656). The PUC ISO image contains all of the scripts necessary to complete the checks. The document contains the instructions for executing the pre-upgrade checks script.

The preUpgradeChecks script validates your system for upgrade eligibility. The preUpgradeChecks script should be run two or more weeks prior to your upgrade in order to ensure that enough time exists to resolve any major issues or incompatibilities that may affect your ability to upgrade. The preUpgradeChecks script should be run again just before you upgrade to validate the system.

Important: The preUpgradeChecks scripts must be run on each EC that will be upgraded.

2

Creating the New VM and Installing Solaris and Solaris Tools

Introduction

This chapter contains procedures for creating the new VM and installing Solaris and Solaris tools on the new VM.

In This Chapter

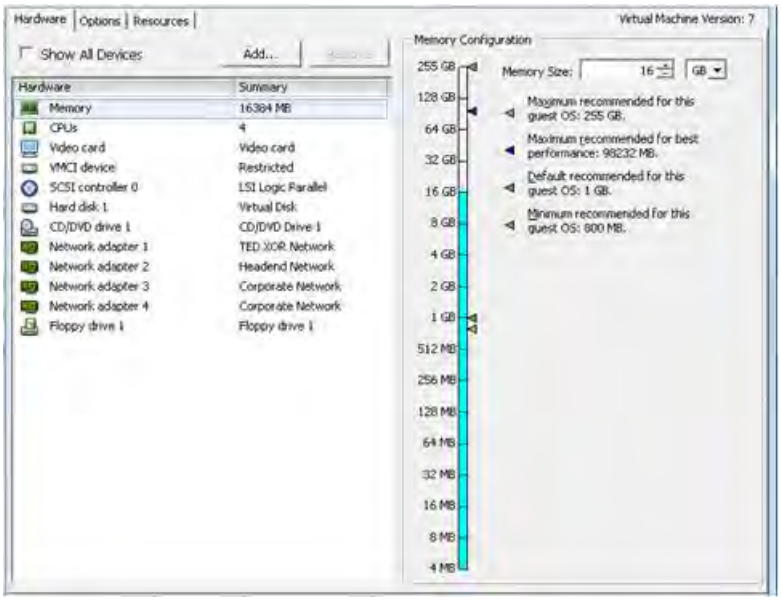
OVA Deployment

Important: You must copy the VMware OVA template file and the JumpStart directory from the SR 6.0 installation ISO image to the vSphere system you will be using to perform this installation.

Follow these steps to copy these files/directories to the vSphere system and to deploy the OVA:

1. Mount the ISO image on the vSphere PC using a third party application, such as PowerISO, or mount on an existing UNIX system for copying over the network.
2. Copy the VMware directory from the ISO to the vSphere PC.
3. Copy the JumpStart directory from the ISO to the vSphere PC.
4. From the **File** menu, choose **Deploy OVF Template**.
5. Click **Browse** and navigate to the **VMwARE** folder you copied to the local machine.
6. Select the **OVA** template and click **Next** twice.
7. In the **Name** field, type the name for the virtual machine (VM) to be created and click **Next**.
8. From the **Configuration** drop-down menu, select the following configuration based on whether the VM is going to be configured as an EC or an RNCS. Then, click **Next.**
   - **EC (240 M3)** — 24 vCPU 96 GB RAM 512 GB HD
   - **RNCS** — 12 vCPU 24 GB RAM 256 GB HD
9. Select **Thick Provisioned Lazy Zeroed** and click **Next**.
10. For the following networks, click the network label and select the corresponding name from the drop-down menu. Examples follow. Your specific network names and configurations will come from the customer-specific network design.
    - VM Network 1 TED XOR Network
    - VM Network 2 Headend Network
    - VM Network 3 Corporate Network
    - VM Network 4 Corporate Network
11. Click **Next**.
12. Verify the settings and click **Finish**.
13. After the **Success** message appears, click **Close** to return to the main menu
14. In the left panel, expand the host inventory by clicking the "**+**" next to the ESXi host.

15 Right-click the new VM and choose **Edit Settings**.



16 From the **Hardware** tab, click **CD/DVD drive 1**.

17 From the **Device Status** area, click **Connect at power on**.

18 From the **Device Type** area, click **Datastore ISO File** and then click **Browse** to navigate to the Solaris ISO image (NFS store).

19 Navigate to the Solaris ISO, select it, and then click **OK**. You are returned to the Hardware > CD/DVD drive 1 window.

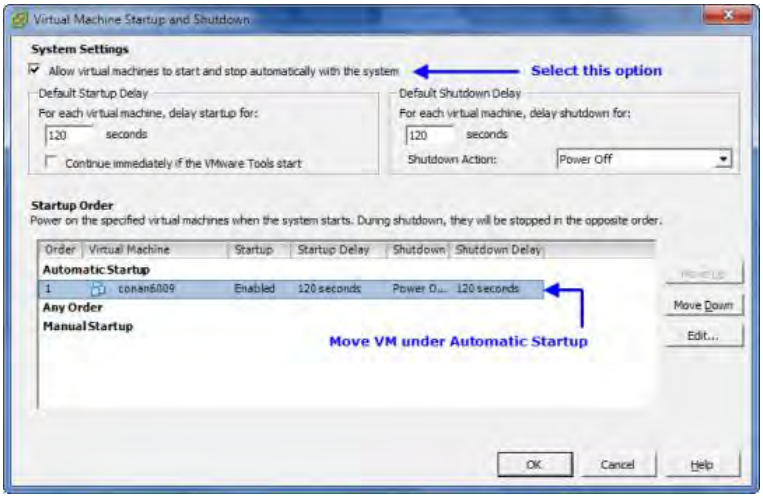
20 Click **OK**.

Note: The system begins reconfiguring the VM. Monitor the status.

21 When the **Status** indicates **Completed**, go to the next procedure in this chapter.

Set the Power Policy

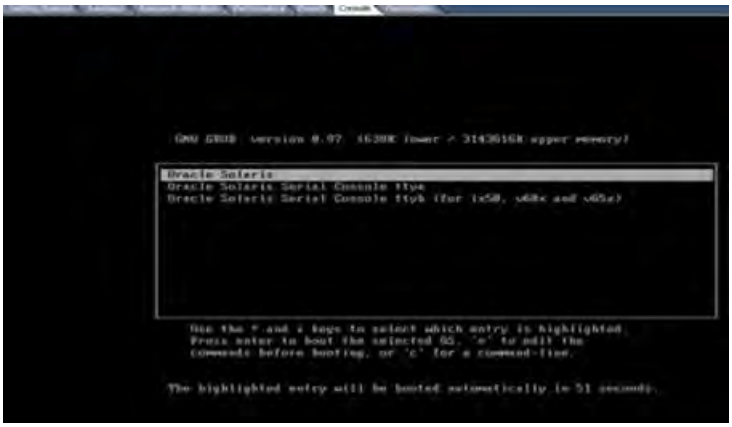
1. Click the ESXi Host.
2. In the **Configuration tab** choose **Virtual Machine Startup/Shutdown** from the **Software** menu.
3. Click **Properties** (located at the top right of the Startup Order window).
4. Check the **Allow virtual machines to start and stop automatically with the system** checkbox.
5. Highlight the VM and click **Move Up** until it is under **Automatic Startup**.



6. Click **OK**.

Solaris x86 Installation

1. Right-click the new virtual machine and choose **Power > Power On**.
2. Click the **VM**, click the **Console** tab and click inside the console window to gain focus. The Grub menu opens with the Oracle Solaris option selected by default.



3. Press **e** to edit.
4. Press **e** again to edit the kernel boot line.
5. Use the left arrow key to move the cursor back to the space that follows the word "unix," and type the following:

   ```
   - install nowin
   ```

   Important:

   - There is a space before and after the "-" in the new string.
   - There is a space that follows the word *nowin*.
   - Do not change any other settings.
6. Press **Enter** to return to the GNU GRUB page that shows the highlighted kernel boot line.
7. Press **Ctrl** and **Alt** to regain control of the mouse.
8. From the toolbar, click the **Floppy Disk** and choose **Floppy drive 1 > Connect to floppy image on a local disk**.
9. Browse to the **JumpStart** folder that was copied from the application DVD onto your local disk, and double-click the **.flp** image.
10. Click in the **Console** window to regain focus.
11. Press **b** to boot, wait for the Solaris OS to boot, and press **F2** in the **Solaris Installation Program** box to continue.
12. Press **F2** in the **Identify This System** box to begin identification.
13. When prompted, choose the **Region**, **Country**, and **Time Zone**, and press **F2** to confirm. The installation resumes.
14. During installation, press **Ctrl** and **Alt** to regain the mouse.

15 Right-click on the VM and select **Edit Settings**, click the **Options** tab.

16 Click **Boot Options** and click the check box in the **Force BIOS Setup** area.

17 Click **OK**.

18 Monitor the Solaris installation progress.

19 When the installation completes, type the following command and press **Enter** to reboot the system:

```
init 6
```

Result: The system goes into the BIOS mode.

20 Type **Ctrl** and **Alt** to regain the mouse.

21 Right-click the VM and choose **Edit Settings**.

22 Click the **Hardware** tab.

23 Click **CD/DVD drive 1**.

24 From the **Device Type** area, click **Client Device**.

25 Click **OK**.

26 From the toolbar, click the **Floppy Disk** and click **Disconnect from <file>**.

27 When prompted to confirm the disconnection, click **Yes**.

28 When the **Disconnected** message appears, click **OK** to acknowledge it.

29 Refocus on the Console and go to the **Boot** section. In the BIOS boot options tab, re-order the boot order as follows:

CD-ROM Drive

Hard Drive

Note: Use the arrow keys to maneuver around. Press the **Shift** and **+** keys to move the device up in the list.

30 Use the arrow keys to move to **Exit** and press **Enter**. The Set Up Confirmation window opens.

31 Highlight **Yes** and press **Enter** to confirm. The Solaris boot menu appears and the system boots to multiuser mode.

VM Solaris Tools

1. Regain control of the mouse.
2. Right-click the VM that was just deployed and click **Guest > Install/Upgrade VMware Tools**, and click **OK**.
3. Click on the Console window and log into Solaris using the default root password:
   ```
   2g3n3r!c
   ```
4. Type the following command and press **Enter**:
   ```
   df -h
   ```
5. Ensure that the VMware tools were mounted under /cdrom/vmwaretools.
6. Type the following command and press **Enter**:
   ```
   cd /tmp
   ```
7. Type the following command and press **Enter**.
   ```
   gzcat /cdrom/vmwaretools/vmware* | tar xvf -
   ```
8. Type the following command and press **Enter**:
   ```
   cd vmware*
   ```
9. Type the following command and press **Enter**:
   ```
   ./vmware-install.pl -d
   ```
10. Type the following command and press **Enter** to reboot the Solaris guest VM:
    ```
    init 6
    ```

3

SR 6.0 Application Installation and Migration

Introduction

This chapter includes the procedures to install the new SR 6.0 image onto the destination (new) VM using the SR 6.0 ISO.

Note: To ensure a successful system upgrade, it is important that you follow the instructions described in this chapter in the order given.

In This Chapter

Application Installation

SR 6.0 currently supports three product types:

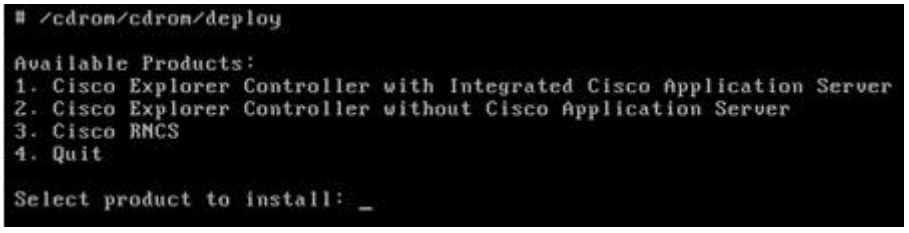
- Cisco Explorer Controller with an Integrated Application Server
- Cisco Explorer Controller with no Application Server
- Cisco RNCS

During the installation of the EC, the key files and database are migrated from the target VM.

SR 6.0 Installation and Migration on the New VM

Important: If the Replicated Database is enabled on the system you are upgrading, refer to *Configuring and Operating the Replicated Database Package on the Explorer Controller* (part number OL-27794), to disable it on both the primary and secondary systems.

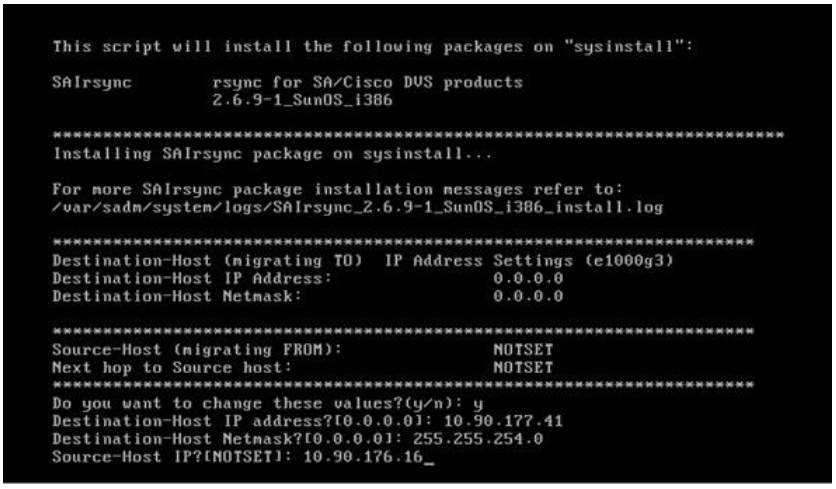
1. Enable **root ssh** on the current (target) VM and restart the SSH service by completing these steps:
   a. Type the following command and press **Enter**.
      `vi /etc/ssh/sshd_config`
   b. Find "PermitRootLogin no" and change it to "yes", save, and quit.
   c. Type the following command and press **Enter** to restart the ssh daemon.
      `svcadm restart ssh`
2. Return to the new VM to which you are migrating and mount the ISO image using the procedure in Mounting and Unmounting Using VMware.
3. Refocus on the console window and log in as **root**, with default password, **2g3n3r!c** (if not already logged in as root).
4. Type the following command and press **Enter**. The Available Products menu opens.
   `/cdrom/cdrom/deploy`



5. Enter the appropriate number corresponding to the product you are installing.
6. Choose **Install and Migrate Data**. The Migration Network Interface configuration opens.

7 At the **Do you want to change these values?** message, press **y** and press **Enter** to change the temporary IP settings.

Note: Consult with your Network Administrator to obtain the temporary IP and netmask data (interface e1000g3), and the existing EC or RNCS EC IP data.



8 Enter the VM temporary IP address for the new VM.

9 Enter the VM netmask of the temporary interface for the new VM.

10 Enter the IP address of the EC or RNCS EC from which you are going to migrate data. A **Do you wish to continue?** message appears.

11 Press **y** and **Enter** to continue with the migration. Another **Are you sure you want to continue?** message appears.

12 Press **yes** and **Enter** to continue. You are prompted for the root password for the current VM.

13 Enter the **root** password of the remote host and press **Enter** to accept the RSA keys. You are prompted a second time for the root password.

Result: The default key files list opens. You are asked if you want to add to the keyfiles list or accept the defaults.

14 Enter the **root** password of the current VM and press **Enter**.

15 Do you have additional files or directories to add?

- If **yes**, type **y** and press **Enter**. Then, enter the absolute path to the needed files or directories.

  Note: If you have a file containing the absolute path to additional key files, you can use the following format to read in the entire list from the file: **@/<path of file>**

  Example: `@/export/home/dncs/keyfiles.out`

- If **no**, type **n** and press **Enter**.

16 Do you have files or directories that you want to delete from the list?

- If **yes**, type **y** and press **Enter**.

Note: Then, type the number of the entry you want to delete. Type **0** when you are finished.

- If **no**, type **n** and press **Enter**.

Result: The **Do you want to continue?** message appears.

17 Type **y** and press **Enter**. The key files are backed up and the installation continues.

Important: If the deploy script fails and if you are able to correct the problem that caused the deploy script to fail, you can restart the deploy script with the *-r* option, which will attempt to recover the script at the point where it failed.

Example: `/cdrom/cdrom/deploy -r`

18 Go to ***Maintenance Window Activities*** (on page 21) when the installation has completed.

4

Maintenance Window Activities

Introduction

Be certain that you are within a maintenance window before you begin the procedures in this chapter.

In This Chapter

Stop System Components

Maintenance Window

CAUTION:

You need to be in a maintenance window to complete the remaining procedures in this chapter, as well as in the following chapter.

Suspend Billing Transactions

If you have not already done so, contact the billing vendor and ask that all transactions be suspended until after the upgrade is complete.

Stop All Third Party Utilities

All third-party utilities should be stopped for the upgrade to succeed. Consult with the system operator about which third party utilities may be running on the system and stop them.

Important: If third party utilities are not stopped, the upgrade may fail.

Stopping the System Components and Migrating the Database and Key Files

Follow these instructions to migrate the database from an existing system.

1. From the dncs remote terminal window on the current EC, complete the following steps to stop the Application Server processes:
   a. Type the following command and press **Enter**. The Application Server processes stop.
      ```
      appStop
      ```
   b. Type the following command and press **Enter**. The initd process on the Application Server is shut down.
      ```
      appKill
      ```
2. If applicable, from the **dncs** window, use the **siteCmd** command to access the RNCS EC and complete the following steps:
   a. Type the following command and press **Enter**. The RNCS EC processes stop.
      ```
      siteCmd [lionn hostname] lionnStop
      ```
   b. Type the following command and press **Enter**. The initd process on the LIONN shuts down.
      ```
      siteCmd [lionn hostname] lionnKill
      ```

c Type the following command and press **Enter** to determine if the processes have stopped. The processes are stopped when there are no processes listed in the output.

```
siteCmd [lionn hostname] pgrep -fl dvs
```

d From the **root** remote terminal window, type the following commands, pressing **Enter** after each, to disable the RNCS cron jobs:

```
ssh –X dncs@[lionn hostname]
su -
svcadm –v disable –s cron
exit
exit
```

3 Close all WUIs.

4 From the **dncs** remote terminal window on the current EC, complete these instructions:

a Type the following command and press **Enter**. The EC processes stop.

```
dncsStop
```

b Type the following command and press **Enter**. The initd process on the EC is shut down.

```
dncsKill
```

c Type the following command and press **Enter** to determine if the processes have stopped. The processes are stopped when there are no processes listed in the output.

```
pgrep -fl dvs
```

Note: The following entries will always appear in the output of this command and indicate that it is safe to proceed with the next procedure in this chapter:

- /usr/sbin/dtrace -qws /dvs/dncs/etc/app_crash/app_crash_global.d
- /dvs/dncs/bin/dncsResMon
- /dvs/cmd2000/bin/cmd2000 -startFile
- /dvs/cmd2000/dvsFiles/cmd2k.conf

d If the output from the command in step 4c shows that processes are running, type the following command in the root terminal window and press **Enter** to stop those processes.

`kill -9 PID` (where PID is the process ID(s) of the running process(es))

Note: Kill all processes except those identified in the note in step 4c.

e If the EC has been Regionalized, type the following command and press **Enter**. This will show if the oammgrctrl process is running.

```
pgrep -fl oam
```

f Is the oammgr process running?

- If **yes**, type the following command, as **root** user, and press **Enter** to stop the process:

  ```
  /etc/init.d/oammgrctrl stop
  ```

- If **no**, continue with step 4 h.

g Type the following command and press **Enter** to verify that the oammgr process is no longer running:

```
pgrep -fl oam
```

Note: If the oammgr process is still running, execute the oammgrctrl stop command again. If the process still does not stop, contact Cisco Services for assistance.

h From the **root** remote terminal window, type the following command and press **Enter** to disable cron jobs:

```
svcadm -v disable -s cron
```

5 Within the vSphere console, move the new VM's /etc/hostname.e1000g[0-2] files to backup files.

Example: `mv /etc/hostname.e1000g0 /etc/hostname.e1000g0.bak`

Note: If the system has other network interfaces configured (e1000g4, etc.), move these files to .bak also.

6 Does this system include a Replicated Database?

- If **yes**, go to step 7.
- If **no**, go to step 10.

7 Enter the following command to copy the /etc/hostname.e1000g3 file to a backup file.

```
cp -p /etc/hostname.e1000g3 /etc/hostname.e1000g3.bak
```

8 Open the /etc/hostname.e1000g3 file in a text editor and modify it so it will reference the temporary IP address and netmask defined when the deploy script was executed.

Example:

```
192.0.2.92 netmask 255.255.254.0 broadcast
```

9 Save and close the file.

10 Type the following command and press **Enter** on the new VM. The VM reboots.

```
shutdown -y -g0 -i6
```

11 If necessary, repeat step 5 for the new RNCS VM for /etc/hostname.e1000g[1-2].

12 Log in to the new VM, and if necessary, the new RNCS VM as **root** user.

13 Type the following command and press **Enter** to ensure that the ISO is still mounted on the system:

```
df -h
```

14 Is the ISO still mounted?

- If **yes**, go to step 17.

- If **no**, continue with step 15.

15 Type the following commands and press **Enter** to bounce the volfs process.

```
svcadm –v disable –s volfs
svcadm –v enable –rs volfs
```

16 Repeat steps 13 and 14.

17 Type the following commands and press **Enter** after each on the current VM and the new VM. The apache Tomcat processes stop.

```
svcadm disable http
svcadm disable apache-tomcat
svcadm disable http-dncsws
```

18 Type the following command on the current VM and press **Enter** to check for active database sessions:

```
showActiveSessions
```

19 Are there active sesisons?

- If **yes**, type the following command and press **Enter** to kill active database sessions:

  ```
  killActiveSessions
  showActiveSessions
  ```

  Note: If active sessions are still present, repeat this step. If active sessions are still present, contact Cisco Service for assistance.

- If **no**, continue with step 20.

20 Type the following command and press **Enter** to export the database from the remote EC:

```
/cdrom/cdrom/migrate
```

Result: The system displays the current network values.

21 At the **Do you wish to continue?** prompt, type **y** and press **Enter**. The **Are you sure you want to continue connecting?** message appears.

22 Type **yes** and press **Enter** to continue. The system prompts you for the root password for the target (current) VM.

23 Type the current EC **root** password and press **Enter**. You are prompted for the **root** password again.

24 Type the EC root password and press **Enter**. The migration begins.

Important: If the migration script fails and if you are able to correct the problem that caused the migration script to fail, you can restart the migration script with the *–r* option, which will attempt to recover the script at the point where it failed.

Example: `/cdrom/cdrom/migrate –r`

25 Once the database migration is complete, move the /etc/hostname.<int>.bak files to their original names.

Example: `mv /etc/hostname.e1000g0.bak /etc/hostname.e1000g0`

26 Does the system include a Replicated Database?

- If **yes**, enter the following command to move the RepDB hostname file to hostname.e1000g3.

  ```
  mv /etc/hostname.e1000g3.bak /etc/hostname.e1000g3
  ```

- If **no**, enter the following command to remove the hostname.e1000g3 file from the system.

  ```
  rm /etc/hostname.e1000g3
  ```

27 Type the following commands and press **Enter** after each to delete the following files:

```
rm /var/tmp/deployIp*
rm  /var/tmp/dncsip*
```

28 If necessary, repeat step 22 for the new RNCS VM for /etc/hostname.e1000g[1-2].bak.

Shut Down and Reboot the Servers

Follow these instructions to reboot the servers:

1. If an RNCS EC exists on this system, type the following command and press **Enter** in the **root** remote terminal window on the existing EC to shut down the EC server(s):

   ```
   siteCmd [lionn hostname] shutdown -y -g0 -i0
   ```

2. Type the following command and press **Enter** to shut down the target (current) VM:

   ```
   shutdown -y -g0 -i0
   ```

3. From vSphere, select the target (current) VMs you shut down, right-click, and click **Power > Power Off**.

4. Does the system include the Replicated Database?

   - If **yes**, repeat steps 2 and 3 on the **standby** VM.
   - If **no**, continue with the next step.

5. From vSphere, click the new VM and click **Console**. Then, type the following command and press **Enter** to reboot the new VM:

   ```
   shutdown -y -g0 -i6
   ```

6. If you are installing on and migrating an RNCS VM, complete steps 2 through 5 on the RNCS EC.

Important: The remaining procedures in this chapter can be performed in the **VM Console** tab in vSphere/vCenter or from a **root** and/or **dncs** remote terminal window on the new VM.

Log into the New Explorer Controller

Perform this procedure in remote terminal windows on the new VM by logging into the EC with your user account:

1. Open a remote terminal window to the new VM and log in with your user account. Then, type `sux -` and press **Enter** to log into the EC as the **root** user. The system prompts for the root password.
2. Type the **root** password and press **Enter**.
3. Type the following command and press **Enter** to change to the **dncs** user:

   ```
   sux - dncs
   ```

4. Type the following commands and press **Enter** (after each command) to kill the dncsInitd process:

   a `dncsKill`

   b `appKill`

5. Type **exit** and press **Enter** to log out as the dncs user.
6. Does this system include an RNCS EC?
   - If **yes**, go to ***Log into the New RNCS Explorer Controller*** (on page 29).
   - If **no**, go to ***Post-Upgrade Check for the 3010 Listening Interface*** (on page 30).

Log into the New RNCS Explorer Controller

Only perform this procedure if you have installed and migrated an RNCS EC. Perform this procedure in the **VM Console** tab.

1. Log into the RNCS EC as the **root** user.
2. Type the **root** password and press **Enter**.

Post-Upgrade Check for the 3010 Listening Interface

The 3010 listening port must be running for the Informix database to receive its connections and go online. To ensure that this port is running, complete the following steps:

1. In the **root** EC remote terminal window, type the following command and press **Enter**:

   ```
   netstat -an |grep 3010
   ```

   Example: Output should be similar to the following:

   ```
   127.0.0.1.3010          *.*              0     0 49152     0
   LISTEN
   ```

2. Is the 3010 listening port running?
   - If **yes**, you have completed this procedure.
   - If **no**, continue with step 3.
3. If you are not already **root** user, change to **root** user (`su -`).
4. Type the following command and press **Enter**:

   ```
   grep 3010 /etc/services
   ```

5. Is the 3010 port present in the /etc/services file?
   - If **yes**, skip to step 7.
   - If **no**, continue with step 6.
6. Open a text editor and add the following to the end of the /etc/services file:

   ```
   informixOnline      3010/tcp
   ```

7. Type the following command and press **Enter** to confirm that Informix is running:

   ```
   onstat -
   ```

   Example: Output should be similar to the following:

   ```
   IBM Informix Dynamic Server Version 11.70.FC4 -- On-Line -- Up
   08:09:44 -- 7759872 Kbytes
   ```

Run the setupAS Script on the EC

Important:

- This procedure is not required if your system is an EC without an Application Server.
- This procedure is not required if your system is an EC using a third party Application Server (MDN/ODN, Rovi Corporation, and so on).

After the installation has completed, you must run the setupAS script to configure the EC system to operate with the integrated Cisco Application Server.

As the **root** user on the EC, type the following command and press **Enter** to run the setupAS script. The script configures the EC to operate with the Application Server.

```
setupAS
```

Add Unique Entries to the dfstab File

Important: You must be the **root** user to make any modifications to the /etc/dfs/dfstab file. Perform this procedure as the **root** user on the EC.

1. Type the following command and press **Enter** to change to the /dvs/admin/sysinfo directory:

   ```
   cd /dvs/admin/sysinfo
   ```

2. Type the following command and press **Enter** to open the dfstab file for review:

   ```
   less dfstab
   ```

3. Type the following command and press **Enter** to open the /etc/dfs/dfstab file:

   ```
   less /etc/dfs/dfstab
   ```

4. Compare the two files. Does the pre-upgrade dfstab file contain any unique entries?

   - If **yes**, complete these steps:
     - **a** Open the /etc/dfs/dfstab file in a text editor.
     - **b** Add all exact unique entries found in the pre-upgrade dfstab file into the /etc/dfs/dfstab file.
     - **c** Save and close the /etc/dfs/dfstab file.
     - **d** Type the following command and press **Enter** to share these new entries:

       ```
       shareall
       ```

   - If **no**, you have completed this procedure.

Add Unique Entries to the vfstab File (Optional)

After upgrading the EC, a new vfstab file is installed and saved to the /etc directory. Complete the following steps to inspect the vfstab file and add any unique entries:

Important: You must be the **root** user to make any modifications to the /etc/vfstab file. Perform this procedure as the **root** user on the EC.

1. Type the following command and press **Enter** to change to the /dvs/admin/sysinfo directory:

   ```
   cd /dvs/admin/sysinfo
   ```

2. Type the following command and press **Enter** to open the vfstab file for review:

   ```
   less vfstab
   ```

3. Type the following command and press **Enter** to open the /etc/vfstab file:

   ```
   less /etc/vfstab
   ```

4. Compare the two files. Does the pre-upgrade vfstab file contain any unique entries compared to the post-upgrade vfstab file?

   - If **yes**, complete these steps:
     - **a** Open the /etc/vfstab file in a text editor.
     - **b** Add all exact unique entries found in the pre-upgrade vfstab file into the /etc/vfstab file.
     - **c** Save and close the /etc/vfstab file.
     - **d** Create any mount points that do not already exist.
     - **e** Type the following command and press **Enter** to mount these new entries:

       ```
       mountall
       ```

   - If **no**, you have completed this procedure.

Create the Private and Public Keys (RNCS EC Servers Only)

Important:

- If you have a DTACS server, you will configure it post-upgrade in ***(Apx C) Configuring DTACS on an SR 6.0 System Vm to VM*** (on page 79).
- If you upgraded a system that did not include an RNCS EC, skip this procedure and go to ***SR 6.0 Post Upgrade Procedures*** (on page 37).

You will have to create the private/public keys between any independent servers on the system (for example, RNCS EC servers). This is necessary due to the Enhanced Security in SR 6.0. The EC must exchange keys with the RNCS EC servers.

Perform this procedure as **root** user on the EC.

1 Type the following command and press **Enter**. The **Enter the host name of the site you are adding** message appears.

```
siteCmd -S
```

2 Type the host name of the RNCS EC and press **Enter**. The **Enter the IP address of the site you are adding** message appears.

Important: Be sure you enter the actual host name of the RNCS EC.

3 Type the IP address of the RNCS EC and press **Enter**. The **Do you want to continue?** message appears.

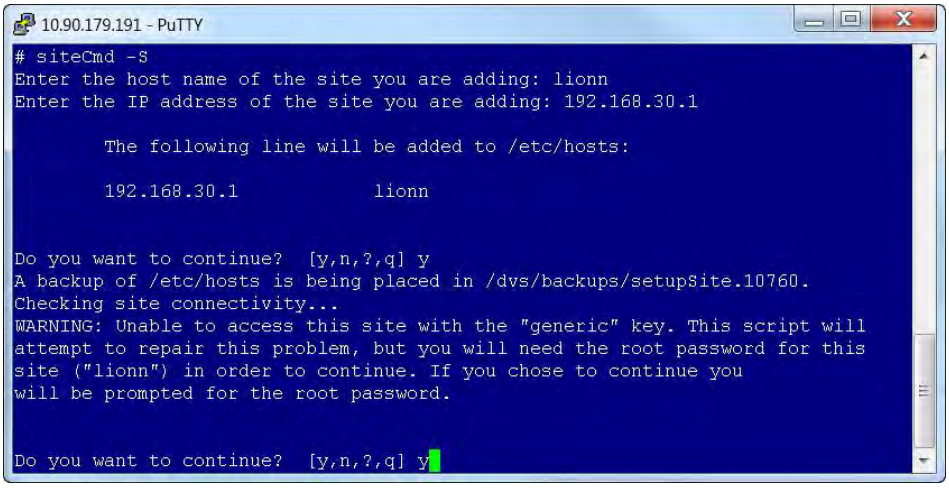
Important: Be sure you enter the actual IP address of the RNCS EC.

4 Type **y** and press **Enter**.

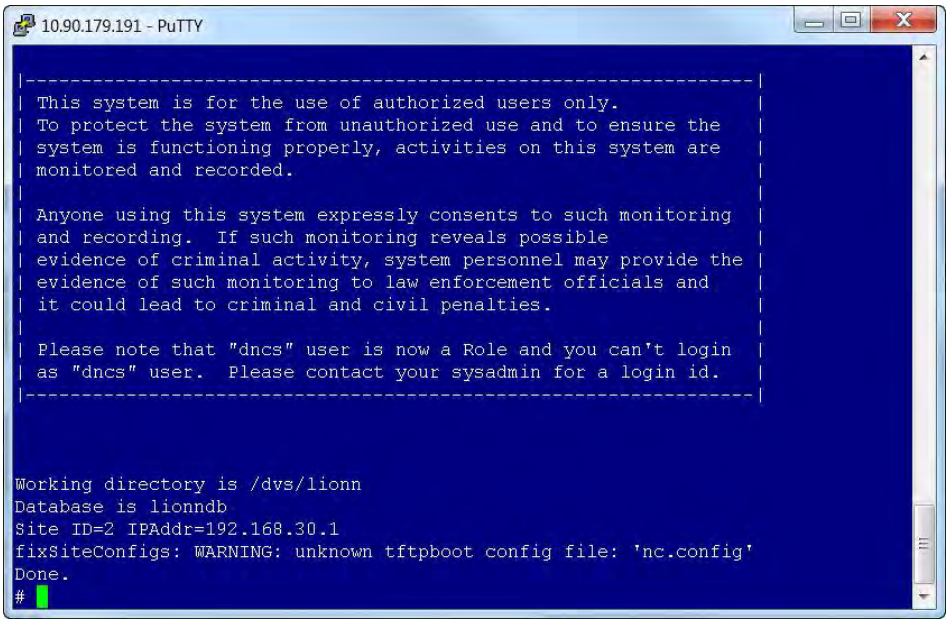
Results:

- A message appears about the system backing up and adding an entry to the /etc/hosts file.

- The **Do you want to continue?** message appears and you are prompted for the root password of the RNCS EC.



5 At the prompt for the root password, type the **root** password and press **Enter**. The system displays a series of messages about generating various keys and a **Done** message appears.



6 Type the following command and press **Enter**:

```
sux - dncs
```

7 Type the following command and press **Enter**. The system logs you on to the RNCS EC as dncsSSH user. You are now connected to the RNCS EC and the host for the RNCS EC is permanently added to the list of known hosts.

```
ssh -X -i /export/home/dncsSSH/.ssh/siteKey  dncsSSH@[RNCS EC hostname]
```

Note: Replace [RNCS EC hostname] with the actaul hostname of the RNCS EC.

Example: `ssh -X -i /export/home/dncsSSH/.ssh/siteKey dncsSSH@rncs1`

8 Type `su -` and press **Enter**. The password prompt opens.

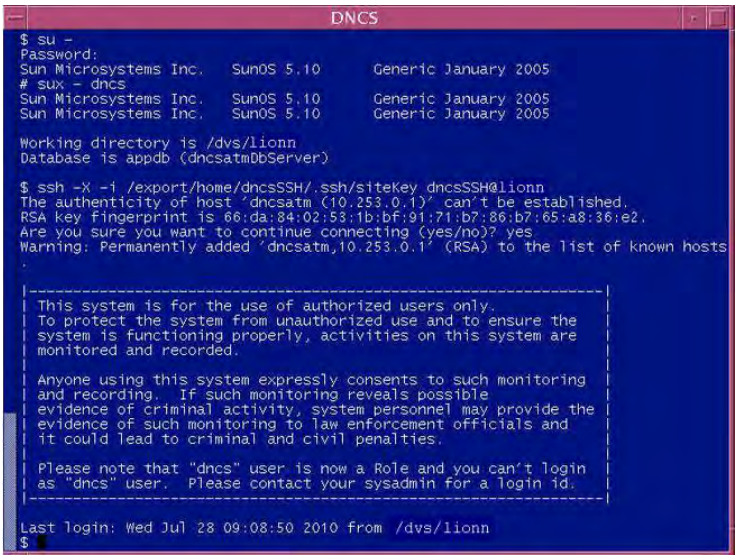
9 Type the **root** password and press **Enter**.

10 Type the following command and press **Enter**:

`sux - dncs`

11 Type the following command and press **Enter**. The system logs you on to the EC as dncsSSH user, and the **Are you sure you want to continue connecting?** message appears.

`ssh -X -i /export/home/dncsSSH/.ssh/siteKey dncsSSH@dncsatm`



12 Type `yes` and press **Enter**. You are now connected to the EC and the host for the EC is permanently added to the list of known hosts.

13 Type `exit` and press **Enter** until the remote terminal window closes. This ensures that you are not still logged on as dncsSSH user.

5

SR 6.0 Post Upgrade Procedures

Introduction

Complete the procedures in this chapter 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

Install Patches and Emergency Patches

If the release came with patches and/or emergency patches (EP), install them now. Each patch and EP comes with a README file with instructions on it that describe how to install the software. Follow the instructions in the README file to install all patches and EPs released with this code.

Note: Your patch might be released as an ISO image. See ***Mounting and Unmounting ISO Images*** (on page 95), if needed.

Enable Optional and Licensed Features

If you have properly followed the instructions in this chapter, the system processes should currently be stopped. Now is the time to enable the optional features you have chosen as part of this upgrade. Contact Cisco Services to have the licensed or optional features enabled on your network.

If you are migrating from a QAM to an RFGW as part of the migration to GigE BFS, you need to have GQI QAM Support licensed on the EC. Contact Cisco Services to enable this feature.

Modify the dncsSetup File for DSG

Only perform this procedure if the system was configured for DSG BFS pre-upgrade. In this procedure, you will modify the /dvs/dncs/bin/dncsSetup file and change the dncs_bfsRemote variable to dncsdsg.

1. Change to the **root** user.
2. Open the /dvs/dncs/bin/dncsSetup file with an editor.

   Example: `vi /dvs/dncs/bin/dncsSetup`
3. Find the dncs_bfsRemote entry and change `dncsatm` to `dncsdsg`. Then, save and close the file.
4. Log out of the EC completely.
5. Log into the EC with an Administrator account.
6. Change to dncs user.

   ```
   sux - dncs
   ```
7. Does the system include an RNCS EC?
   - If **yes**, go to ***Run fixSiteConfigs on the RNCS EC*** (on page 42).
   - If **no**, go to ***Remove Old BFS Entries*** (on page 43).

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 should have been killed.

Was the IPG_TVDATA_NEW variable found in the appservSetup file durning Pre-Upgrade Checks?

- If **yes**, add the variable to the appservSetup file exactly as it was in the old system.
- If **no**, continue with the next procedure.

Run fixSiteConfigs on the RNCS EC

Only perform this procedure if the site you are upgrading includes an RNCS EC system. If the site you are upgrading does not have an RNCS EC, skip this procedure and go to the next procedure in this chapter.

This procedure fixes the /tftpboot config files for headend components. It also sets the AlarmServerIpAddr entries to the correct IP address for the RNCS EC.

1 As **root** user on the RNCS EC, type the following command and press **Enter**:

```
fixSiteConfigs
```

Sample output:

```
# fixSiteConfigs
     fixSiteConfigs: Fixing config files in
lionn1:/tftpboot...
     fixSiteConfigs: modified: goqam.config
     fixSiteConfigs: modified: gqam.config
     fixSiteConfigs: Ignoring platform file 'inet-config'
    fixSiteConfigs: modified: mqam.config
     fixSiteConfigs: WARNING: unknown tftpboot config file:
'nc.config'
    fixSiteConfigs: no mods needed: nc.config
     fixSiteConfigs: modified: qam.config
     fixSiteConfigs: modified: qpsk.config
     fixSiteConfigs: modified: scsmqam.config
     fixSiteConfigs: 6 of 9 tftpboot config files were
modified
```

2 Type the following command and press **Enter**:

```
cd /tftpboot
```

3 Verify that each of the .config files contains the correct IP addresses.

Notes:

- The QAM config files contain two IpAddr variables, RpcServerIpAddr and AlarmServerIpAddr. These entries should have the following IP addresses assigned:

  ```
  RpcServerIpAddr = [dncsatm IP Address]
  AlarmServerIpAddr = [RNCS IP Address]
  ```

- If these variables do NOT have the correct IP address assigned, contact Cisco Services for assistance.
- Ignore any *inet-config* and *nc.config* warnings.

Remove Old BFS Entries

In this procedure, you will remove old BFS entires in the /dvs/dvsFiles/BFS_REMOTE directory. Follow these instructions to remove old BFS_REMOTE entries:

1. If necessary, open a remote terminal window on the EC.
2. Complete the following steps to log on to the remote terminal window as the **root** user:
   a. Type `sux - root` and press **Enter**. The password prompt opens.
   b. Type the root password and press **Enter**.
3. Type the following command and press **Enter** to change to the /dvs/dvsFiles/BFS_REMOTE directory:
   ```
   cd /dvs/dvsFiles/BFS_REMOTE
   ```
4. Type the following command and press **Enter** to check for old entries:
   ```
   ls
   ```
5. Did the output from step 4 reveal any files or directories?
   - If **yes**, type the following command and press **Enter** to remove these files or directories:
     ```
     rm -r *
     ```
   - If **no**, type the following command and press **Enter** to leave the /dvs/dvsFiles/BFS_REMOTE directory:
     ```
     cd
     ```

Stop and Disable Unneeded Processes

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

To stop and disable a process, complete the following procedure:

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

Important: If you have completed all procedures to this point, you should already have the following windows open from a remote PC, Mac, or other system:

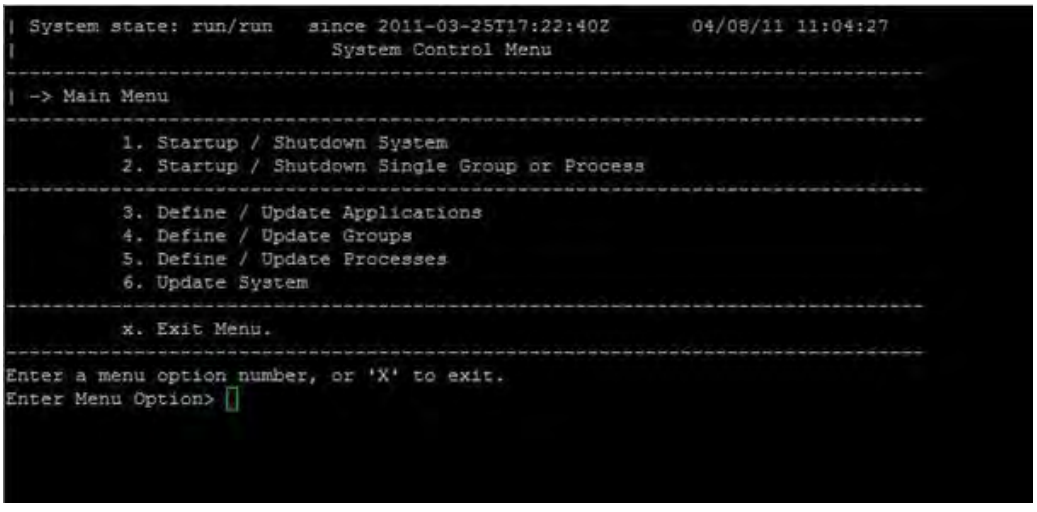
- An xterm, putty, or remote terminal window logged into the EC
- Firefox logged into the EC Administrative Console

If they are not open, from a PC, Mac or other system, open them now and log in using an Administrator user account.

Note: In this procedure, we will disable saManager.

1. Change to the **dncs** user.
2. At the command prompt, as dncs user, type **dncsStart** and press **Enter**.
3. Type the following command and press **Enter**. The dncsControl window opens.

   `dncsControl`



4. Type `2` (Startup/Shutdown Single Group of Process) and press **Enter**.
5. Type `1` (dncs) and press **Enter**.
6. Type `e` (Display Groups) and press **Enter**.
7. Type `14` and press **Enter**.
8. Type `e` (Display Process Entries) and press **Enter**.

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

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

11 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.
- If **no**, go to step 12.

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

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

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

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

```
dncsStop
dncsKill
```

Important: Wait for all processes to stop before executing 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.
- If you have a DTACS server, you must perform the tasks in ***(Apx C) Configuring DTACS on an SR 6.0 System Vm to VM*** (on page 79) to configure the DTACS server.
- This procedure is not necessary if the site being upgraded uses the Cisco Application Server, or does not have a DTACS server. Skip this procedire and go to Restart System Processes, next in this document.
- The steps in this procedure need to be run as the **root** user.

1 With a text editor, add the following line to the /export/home/informix/etc/sqlhosts file:

```
dncsatmDbServer   ontlitcp   dncsatm   informixOnline
```

2 With a text editor, amend the following line in the /export/home/informix/etc/onconfig file by adding the dncsatmDbServer entry:

Example: DBSERVERALIASES demo_on,localDbServer, `dncsatmDbServer`

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

```
/etc/rc2.d/S98informix stop
/etc/rc2.d/S98informix start
```

4 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:

```
netstat -an |grep 3010
```

Result: Output should be similar to the following example:

```
127.0.0.1.3010    *.*    0      0 49152      0 LISTEN
203.0.113.1.3010    *.*   0      0 49152      0 LISTEN
```

Restart System Processes

Important: Note these important points:

- From this point on, you should be logged into the EC remotely from a PC, Mac, or other system.
- You should be using Putty, xterm, or remote terminal software, depending on the remote system you are using.
- You should be remotely logged in to the EC with an Administrator user account created in previous procedures.
- Do not overlook this procedure. This procedure restarts system processes. You must restart the system processes at this time. If you fail to restart the system processes, you will delay completion of the upgrade.
- If the site you are upgrading uses a third party application server, before you start the system processes, you need to comment out the line in the /etc/hosts file that is similar to the following:

  ```
  203.0.113.10  appservatm  appserv_host   ppv_manager_host
  vc_server_host  Config_manager_host
  ```

- Be certain that you are the dncs user. Do not start the processes as the root user.
- Be certain to start the EC, Application Server, and RNCS EC processes as applicable.

Starting EC Processes on the VM

1. Log onto the EC using your Administrator user account.
2. Type the following command and press **Enter** to change to the dncs role:

   ```
   sux - dncs
   ```

   Note: Type the dncs user password when prompted.
3. Type the following command and press **Enter**:

   ```
   dncsStart
   ```
4. Type the following command and press **Enter** to start the Application Server processes:

   ```
   appStart
   ```
5. If applicable, type the following command and press **Enter** to start LIONN processes:

   ```
   siteCmd [hostname] lionnStart
   ```
6. If applicable, type the following command and press **Enter** to confirm that the LIONN processes started successfully:

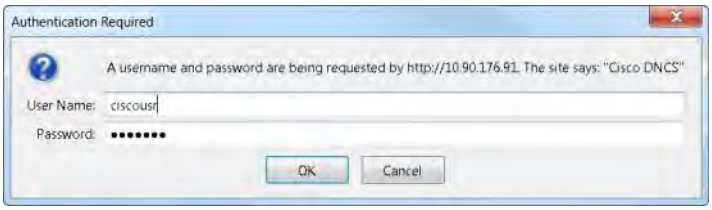
   ```
   siteCmd [hostname] pgrep -fl dvs
   ```

7 In a supported Web browser, type the following address:

`<VM IP address>/dncs`

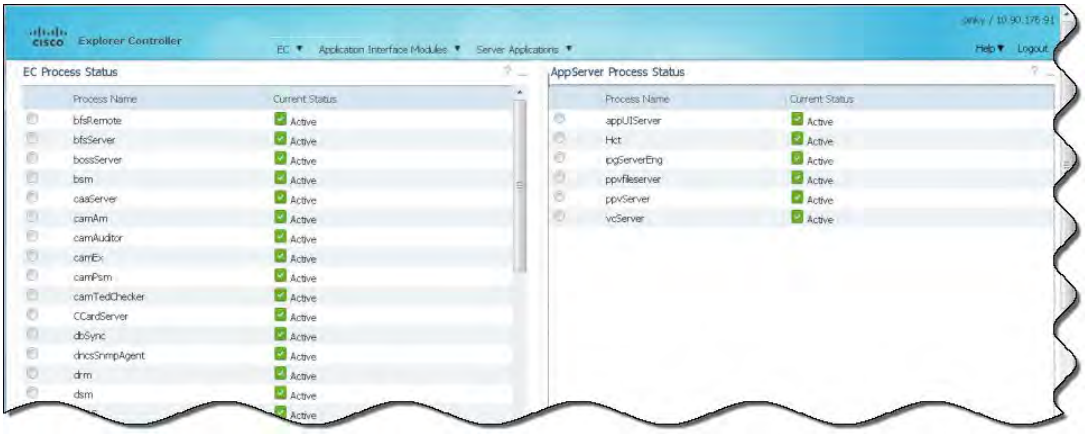
Example: `192.0.2.44/dncs`

Result: The Authentication Required dialog box opens.



8 Type your user name (for example, **ciscousr**), and type the password you defined to access the WUIs.

9 Click **OK**. The Cisco Explorer Controller window opens.



10 Monitor the processes as they come up. Green indicators replace red indicators as the EC processes start. All processes should turn green in short order.

Restarting the Application Server at Rovi Corporation Sites

If necessary, refer to the documents supplied by Rovi to restart the Rovi server.

Restarting the Time Warner Mystro Application Server

If necessary, refer to the documents supplied by Mystro to restart the MDN.

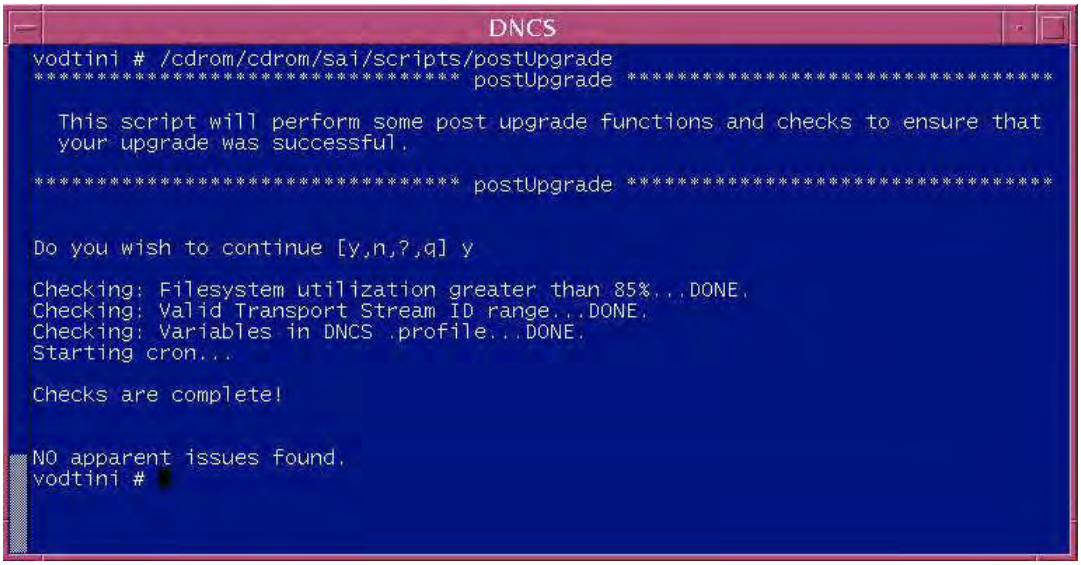
Run the postUpgrade Script on Each Upgraded Server

For each upgraded server, a post-install script is run to verify the system upgrade. This script also restarts cron jobs, as well as performing other tasks required to complete the upgrade.

1 As the **root** user on each appropriate server, type the following command and press **Enter**. A confirmation message appears.

```
/cdrom/cdrom/sai/scripts/postUpgrade
```

2 Type `y` and press **Enter**.



3 Repeat steps 1 and 2 for each upgraded server.

4 Do you have a DTACS server?

- If **yes**, go to ***(Apx C) Configuring DTACS on an SR 6.0 System Vm to VM*** (on page 79) to configure the DTACS server. Then return to *Verify the Number of BFS Sessions*, next in this document.
- If no, go to *Verify the Number of BFS Sessions*, next in this document.

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 **RF Sel** button on the front panel of the BFS GQAM until the appropriate port number is accessed. The sessions on that port open.
2. Does the **Session Count** total equal the number of sessions you recorded in Check the Number of BFS Sessions?
   - If **yes**, skip to step 6.
   - If **no**, telnet to the GQAM modulator where BFS sessions are built.

     Example: `telnet 192.0.2.30`

     Note: Enter the login ID and password for the GQAM. If you make a typing error, follow these steps to recover:

     a. Press the **Ctrl** and **]** keys simultaneously 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.

   `print_session_status <port number>`

   Note: Port numbers on the GQAM are 0-15. If your sessions are built on port 16 in the QAM WUI, it will be port 15 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 step 5.
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 51).
   - If **no**, troubleshoot this matter using your established escalation procedures.

     Note: Call Cisco Services if you are unable to resolve the issue.
7. Type the following command and press **Enter**. The BFS session count is displayed.

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

   Example: auditQam –query 192.0.2.20 2

Important: Be 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 in order to return the BFS session count to the expected number of sessions.

1. Open the EC WebUI. The EC Process Status window opens.
2. Click the radio button next to **bfsServer**.
3. Click **Stop**. The bfsServer process stops and turns red.
4. Scroll down the process list and click the radio button next to **osm**.
5. Click **Stop**. The osm process stops and turns red.
6. Click **EC > Utilities > Session List**. The Session List Filter page opens.
7. Select the **BFS GQAM** from the QAMs list.
8. Click **Display** at the bottom of the page. The Session Summary page opens.

   Result: Data for each BFS session appears under the **Session Summary** heading:

   Total row(s) — This shows the total number of BFS sessions the system has

   Rows per page — The default is 10 per page

   Page — This shows the current page

   Search — Allows you to search the page
9. Does the system have more than 10 BFS sessions?
   - If **yes**, change the **Rows per page** field to include all sessions.
   - If **no**, continue with step 10.

10 Click the button on the left next to **Session ID** in the top row. This selects **ALL BFS** sessions displayed on this page.

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

12 Click **EC** from the left-most portion of the window to open the EC Process Status.

13 Click the **bfsServer** radio button.

14 Click **Start**. The bfsServer process starts and turns green.

15 Scroll to the **osm** service and click its radio button.

16 Click **Start**. The osm process starts and turns green.

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

17 Click the **EC** drop-down arrow, navigate to **Utilities**, and select **Session List**. The Session List Filter page opens.

18 Select the **BFS QAM** from the QAMs list.

19 Click **Display** at the bottom of the page. The Session Summary page opens.

20 Are all the BFS Sessions present and active?

- If **yes**, continue with step 21.
- If **no**, contact Cisco Services for assistance.

21 Press the **RF Sel** button on the front panel of the BFS GQAM modulator until the port with the BFS sessions displays.

22 Does the **Session Count** total now equal the number of sessions you recorded in the Check the Number of BFS Sessions procedure?

- If **yes**, continue with step 29.
- If **no**, contact Cisco Services for assistance.

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

```
auditQam –query [BFS QAM IP address] [Port Number]
```

Example: auditQam –query 192.0.2.20 2

Important: Be 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
```

24 Does the **Session Count** total equal the number of sessions you recorded in the Check the Number of BFS Sessions procedure?

- If **yes**, continue with step 31.
- If **no**, contact Cisco Services for assistance.

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

Example: `telnet 192.0.2.30`

Note: Enter the login ID and password for the GQAM. If you make a typing error, follow these steps to recover.

a Press the **Ctrl** and **]** keys simultaneously to return to the telnet prompt.

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

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

`print_session_status <port number>`

Note: Port numbers on the GQAM are 0-15. If your sessions are built on port 16 in the QAM WUI, it will be port 15 on the GQAM.

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

- If **yes**, go to step 28.
- If **no**, troubleshoot this matter using your established escalation procedures.

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

28 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 6.0 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 WebUI.
- 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 mqam250.config, instead of mqam.config, for the MQAM 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 — /tftpboot/qam.config
- GQAM — /tftpboot/gqam.config
- GOQAM — /tftpboot/goqam.config
- MQAM — /tftpboot/mqam.config
- CAQAM — /tftpboot/caqam.config

CAUTION:

Failure to update the configuration file(s) will result 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 WebUI or in the /etc/bootptab file before contacting Cisco Services for assistance.

Which Reset Method to Use

Resetting the QAM-family of modulators from the EC WUI or the front panel can be time-consuming. If you have many modulators to reset, consider using the new 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, engineers are free to complete other upgrade-related tasks.

Note:

- Instructions for resetting modulators through the EC WUI are found in Resetting Modulators Through the EC WUI.
- Instructions for resetting modulators through the front panel are found in Resetting Modulators Through the Modulator Panel.
- Instructions for resetting modulators through the auditQam utility are found in ***Resetting Modulators Through the auditQam Utility*** (on page 58).

Resetting Modulators Through the EC WebUI

When you reset the modulators, the modulators download their new SR 6.0 code. Follow these instructions to reset the modulators through the EC WebUI:

Important: Never reset more than four modulators at once 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 that is 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 Steps a through f for all of your modulators.

2 Open a remote terminal window on the EC.

3 From the EC WebUI, click the **EC** drop-down menu and navigate to **Network Element Provisioning**. Then select **QAM**.

4 Click **QAM**.

Result: The QAM List window appears.

5 Click **By Field** and select **All**.

6 Click **Show**. All provisioned QAM modulators on the system can now be accessed.

Note: If the **Security Warning** dialog box opens, click **Continue**.

7 From the QAM List window, choose a modulator.

Note: Refer to the QAM Type column to differentiate between types of modulators.

8 Click **Reset** at the bottom of the page. A confirmation message appears.

9 Click **OK** in the confirmation message.

Result: The modulator resets.

10 Repeat Steps 7 through 9 for up to three additional modulators, and then go to Step 11.

Important: Never reset more than four modulators at once, or you may overload the EC.

Note: In Step 12, you will have the opportunity to reset additional modulators.

11 Wait a few minutes and then type **ping [IP address]** and press **Enter** to ping each modulator you just reset.

Example: ping 192.10.2.4

Important: Be sure to use the actual IP address for the specific modulators in your system when running this command.

Result: The ping command displays a message similar to **Device is alive** when the modulator has been reset.

Note: It may take up to 5 minutes for each modulator to reset.

12 Do you have additional modulators to reset?

- If **yes**, repeat Steps 7 through 11 as many times as necessary until all of your modulators have been reset, and then go to Step 13.
- If **no**, go to Step 13.

13 Did you record the Program Count and the Session Count for each modulator not used for VOD, as specified in Step 1?

- 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 ***Reset QPSK Modulators*** (on page 60).

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 ***Reset QPSK Modulators*** (on page 60).

Resetting Modulators Through the Modulator Panel

When you reset the modulators, the modulators download their new SR 6.0 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 that is 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 steps a through f for all of your QAM, MQAM, and/or GQAM modulators.

2. Choose one of the following options:

   - To reset an MQAM or GQAM modulator, go to step 3.
   - 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 then turn it back on.

5. Repeat steps 3 and 4 for up to three additional modulators, and then go to step 6.

   Important: Never reset more than four modulators at once, or you may overload the DNCS.

   Note: In step 7, you will have the opportunity to reset additional modulators.

6. Wait a few minutes and then from an xterm window on the DNCS, type ping [IP address] and press **Enter** to ping each modulator you just reset.

Example: ping 192.0.2.4

Result: The ping command displays a message similar to **Device is alive** when the modulator has been reset.

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 step 8.
- If **no**, go to step 8.

8 Did you record the Program Count and the Session Count for each modulator not used for VOD, as specified in Step 1?

- 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 ***Reset QPSK Modulators*** (on page 60).

  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 ***Reset QPSK Modulators*** (on page 60).

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 WebUI 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 From the **dncs** remote terminal window on the EC, type the following command and press **Enter** to change to **dncs** user:

```
sux - dncs
```

2 Type the following command and press **Enter**:

```
auditQam  -reset  [qam ip address or mqam ip address]
```

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.

3 Repeat step 2 for each QAM modulator on your system.

Resetting Many QAM and MQAM Modulators

Upgrade engineers frequently do not have time to manually reset hundreds of modulators from the EC WebUI. To save time, engineers 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 /tftpboot/qpsk.config.

CAUTION:

Failure to update the configuration file(s) will result 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 GUI or in the /etc/bootptab file before contacting Cisco Services for assistance.

Resetting QPSK Modulators

Use these instructions 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 on.

1. From the EC WUI, click **EC > Network Element Provisioning > QPSK**.
2. Use the **Filter > By Field** filter to select an option to see the appropriate QPSKs on the system. Click **Show**.
3. Click the radio button next to the appropriate QPSK modulator.
4. Click **Reset** at the bottom of the WUI. A confirmation message appears.
5. Click **OK** on the confirmation message. The QPSK modulator resets.
6. Wait about 15 minutes and repeat steps 3 through 5 until all of your QPSK modulators have been reset.

   Important: Our engineers recommend that you wait about 15 minutes before resetting the next modulator.

Verify the crontab Entries

Verifying the crontab Entries

After upgrading, inspect the crontab file to verify that it contains an entry for dbOptimizer, and that it contains no entry for camEmmDeleter. Follow these instructions to inspect the crontab file.

1 From the **dncs** remote terminal window, type `cd` and press **Enter**. The home directory of /export/home/dncs becomes the working directory.

2 Type `crontab -l` and press **Enter**. The system lists the entries in the crontab file.

Note: The 'l' is a lowercase L.

3 Does the crontab file include an entry for **dbOptimizer**?

- If **yes**, go to ***Examining the CED.in Entry*** (on page 61).
- If **no**, call Cisco Services for assistance.

Examining the CED.in Entry

Our engineers developed the dbOptimizer program to delete EMMs that are no longer needed by DHCTs. 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 From the **root** remote terminal window on the EC, type the following command and press **Enter**. The system displays the number of days that EMMs will be retained. EMMs that are older than this number of days will be deleted by the dbOptimizer program when it runs each Saturday.

```
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 ***Adding Custom crontab Entries*** (on page 62).
- If **no**, go to step 3 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.

```
echo <new # of days>  >  /dvs/dncs/bin/CED.in
```

Example: To set the value to our recommended default value of 90 days, type the following command and press **Enter**.

```
echo 90 > /dvs/dncs/bin/CED.in
```

4 Type `exit` and press **Enter** to log out the root user.

Adding Custom crontab Entries

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.

1 If you do not already have two **root** remote terminal windows available, open another remote terminal window on the EC and change to root user by typing `sux - root` and pressing **Enter** (enter root password when prompted).

Note: You should now have three remote terminal windows open on the EC. Two of them are for the root user and one is for the dncs user.

2 Follow these instructions in one of the **root** remote terminal windows:

Note: This remote terminal window will contain the pre-upgrade crontab entries for each user.

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

```
cd /dvs/admin/sysinfo/crontabs
```

b Type the following command and press **Enter**:

```
less root
```

Result: The system displays the contents of the pre-upgrade root crontab file.

3 In the second **root** remote terminal window, type the following command and press **Enter**. The system displays the contents of the current root crontab file.

```
crontab -l  root
```

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**, follow these instructions:
  a Type the following command and press **Enter**. The system copies the root crontab file to /tmp/root.cron.

```
crontab -l > /tmp/root.cron
```

  b Type the following command and press **Enter**:

```
vi /tmp/root.cron
```

  c Add any unique entries to the /tmp/root.cron file and save the file.

d Type the following command and press **Enter**. The edited /tmp/root.cron file becomes the new root crontab file.

```
crontab /tmp/root.cron
```

e Type the following command and press **Enter** to verify that the crontab file properly contains the unique entries.

```
crontab -l root
```

- If **no**, go to step 6.

6 Type the following command and press **Enter** to change to the informix user:

```
sux - informix
```

7 Repeat steps 2 through 5 for the Informix crontab file.

Note: Replace "root" with "informix" in each command.

8 Type `exit` and press **Enter** to log off as informix user.

9 Type the following command and press **Enter** to change to the dncs user:

```
sux - dncs
```

10 Repeat steps 2 through 5 for the dncs crontab file.

Note: Replace "root" with "dncs" in each command.

11 Type **exit** and press **Enter** in both remote terminal windows.

Verify the Upgrade

Go to ***System Verification Procedures*** (on page 71) to verify the upgrade.

Set the Clock on the TED (Optional)

Complete these steps to set the clock on the TED:

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**:

     `rsh -l root dncsted`
   - If it is a TED-3 or TED-4, type the following command and press **Enter**:

     `ssh -l root dncsted`

   Note: The "l" is a lowercase L in each instance.
4. Type the **root** password and press **Enter**. You are logged on to 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 DNCS and TED match?
   - If **yes**, go to step 9.
   - If **no**, go to step 7.
7. At the prompt, type `date [mmddhhmm]` and press **Enter**.

   Example: `date 07132316`

   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 073123162001** includes the year.
   - The **date 07132316.30** includes the seconds.
   - The **date 071323162001.30** 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.

13 Type `exit` and press **Enter** to log out the root user.

Confirm Third Party BFS Application Cabinet Data

In this procedure, you will check to ensure that all third party BFS application cabinet data is present following the upgrade.

Note: You will need the sheet of paper that you used to record third-party BFS application cabinet data when you completed Record Third Party BFS Application Cabinet Data.

1. From the EC WUI, click **Application Interface Modules > BFS Client**. The Site DNCS Broadcast File Server List window opens.
2. Refer to the sheet of paper that you used when you completed Record Third Party BFS Application Cabinet Data. 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 already open.
     a. Click **Add Server**. The Add Server window opens.
     b. Click the arrow next to the Server Name field and select the appropriate server.
     c. Click to highlight the correct **Mode** (**1-way** or **2-way**).
     d. Click to highlight the appropriate **Available Source**. Then click **Add** to move it to the **Selected Sources** column.
     e. Click **Save**.
     f. Repeat steps a through e for any additional third party BFS application cabinets that are missing.
   - If **no** (there are no missing third-party BFS application cabinets), continue with step 4.
3. Highlight each of the third-party application cabinets listed on the sheet of paper, in turn, and click **Edit**. The Set Up 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 Site DNCS Broadcast File Server List window when you are finished.

Enable RADIUS and LDAP (Optional)

To enable RADIUS or LDAP on your system, refer to *Configuring RADIUS and LDAP Support Configuration Guide for Explorer Controller* (part number OL-27571) .

6

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

System Verification Procedures

Introduction

Use this procedure to verify that an active communication link exists between the EC and DHCTs. The EC must be able to communicate with DHCTS to ensure a successful system upgrade.

In This Appendix

Verify the System Upgrade

Complete these steps to verify a successful upgrade to SR 6.0:

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 the **dncs** user, type the following command and press **Enter**:

   ```
   cd /dvs/dncs/Utilities/doctor
   ```

2. Type the following command and press **Enter**. This command runs the Doctor Report. Review the Doctor Report to ensure that communications exist among all DBDS elements.

   ```
   doctor -vn
   ```

3. 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:

   ```
   df -k
   ```

   Important: If any disk partition lists a capacity greater than 85 percent, contact Cisco Services before proceeding.

4. Stage at least one new DHCT to the system operator's specifications. After staging the DHCT, verify the following:

   - The DHCT receives 33 or 34 EMMs
   - The DHCT successfully receives its Entitlement Agent

5. 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**.

6. Verify that you can ping the DHCT.

7. Verify that the Interactive Program Guide (IPG) displays 7 days of accurate and valid data.

8. 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.

9 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 step 2.
- 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 WUI, click **Application 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 WUI Process Status window, click the radio 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 radio 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 WebUIs

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 step 3.

3 Open the Channel Map user interface for each applicable channel map, and click **Save**.

Note: Make no changes on the WUI; just click **Save**.

4 Wait again the length of time of the SAM Configuration Update Timer.

5 Examine each channel map again for accuracy.

Check the EAS Configuration—Post Upgrade

Checking the EAS Configuration

After installing the SR 6.0 software, verify that your EAS equipment is working correctly by testing the system's ability to transmit EAS messages. 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).

After completing the procedures in Chapter 5, **Testing the EAS**, of the *Configuring and Troubleshooting the Digital Emergency Alert System, For Use With All System Releases* guide, verify that you can generate an EAS message for the Emergency Alert Controller (EAC), itself.

B

SR 6.0 Rollback Procedures

Introduction

The SR 6.0 rollback procedures are intended for field service engineers who encounter problems while upgrading an existing digital system to SR 6.0. Prior to executing the SR 6.0 rollback procedures however, contact Cisco Services.

In This Appendix

Activate the Old System Release

1. From the **root** remote terminal window, type `sux - dncs` and press **Enter** to change to the dncs user.
2. Type the following command and press **Enter** to stop Application Server processes:

   ```
   appStop
   ```
3. If necessary, type the following command and press **Enter** to stop RNCS EC processes:

   ```
   siteCmd [hostname] lionnStop
   ```
4. Type the following command and press **Enter** to stop EC processes:

   ```
   dncsStop
   ```
5. Type `exit` and press **Enter** to return to the root window.
6. If applicable, type the following command and press **Enter** to shut down the RNCS EC:

   ```
   siteCmd [hostname] shutdown -y -g0 -i0
   ```
7. Type the following command and press **Enter** to shut down the EC:

   ```
   shutdown -y -g0 -i0
   ```
8. From vSphere, right-click the VM and click **Power > Power Off**.
9. From vSphere, right-click the old VM, and click **Power > Power On**.
10. Log in with your user account to the VM you just powered-on and switch to the **dncs** user.
11. Enter the dncs password when prompted.
12. Type the following commands, pressing **Enter** after each, to start all processes, as needed:
    - `dncsStart`
    - `appStart`
    - `siteCmd [hostname] lionnStart`
13. Return to Appendix A, ***System Verification Procedures*** (on page 71), to verify system functionality.

C

Configuring DTACS on an SR 6.0 System

Introduction

Important: If DTACS was already set up to run on the system, skip this procedure.

This appendix provides procedures that allow the Digital Transport Adapter Control System (DTACS) server to communicate with the EC through the SSH protocol in order to enable database synchronization.

In This Appendix

Open a Remote Terminal Window on the EC and DTACS Servers

To configure the DTACS server to run on an SR 6.0 system, you will need to add or modify specific configurations and files on both the DTACS server and the EC. For this reason, we recommend opening two **root** remote terminal windows: one that accesses the EC server and one that accesses the DTACS server.

Important: Once this procedure is completed, we will refer to either the root remote terminal window on the DTACS or the EC server for the remaining procedures in this appendix.

Complete the following steps to open two **root** remote terminal windows on each server:

1. Open two remote terminal windows on the EC system.
2. In one remote terminal window, complete the following steps to log in as **root** user on the EC:
   a. Type `su -` and press **Enter**. You are prompted to enter your password.
   b. Type the **root** password and press **Enter**. The root prompt appears.
3. In the other remote terminal window, access your DTACS server by entering the following command and pressing **Enter**:

   ```
   ssh -X [userID]@[dtacsIP]
   ```

   Notes:

   - Substitute your user ID that was created on your DTACS server for [userID].
   - Substitute the IP address for the DTACS server for [dtacsIP].
   - Do not include any brackets in the command.
4. In the DTACS window, type `su -` and press **Enter** to change to **root** user.
5. Enter the password when prompted.

Create the dncsSSH User on the DTACS Server

Important: All steps in this procedure take place in the **root** remote terminal window on the DTACS server.

1 Type the following command and press **Enter**:

```
grep dncsSSH /etc/passwd
```

2 Does the dncsSSH user exist?

- If **yes**, skip the rest of this procedure and go to the next procedure in this chapter.
- If **no**, continue with step 3.

3 In the **root** remote terminal window on the DTACS server, open the **/etc/ssh/sshd_config** file in a text editor.

4 Edit the **PermitRootLogin no** entry to the following:

```
PermitRootLogin yes
```

5 Save and close the sshd_config file.

6 Type the following command and press **Enter** to restart the SSH service:

```
svcadm restart ssh
```

7 To create the dncsSSH user, type the following command and press **Enter**:

Note: The following command is a single command and should be typed as a single entry. Type the entire command before pressing **Enter**.

```
useradd -c "DNCS SSH Account" -e "" -f 0 -d
/export/home/dncsSSH -g dtacs -m -s /bin/ksh dncsSSH
```

8 Type the following command and press **Enter**:

Note: The following command is a single command and should be typed as a single entry. Type the entire command before pressing **Enter**.

```
usermod -K type=normal -K profiles=All -K
lock_after_retries=no dncsSSH
```

Remove the appservatm Entry from the DTACS /etc/hosts File

In this procedure, you will check for an appservatm entry in the /etc/hosts file of the DTACS. This entry is not needed, and can cause issues with the booting of the DTA if it is present. Follow these instructions to check for this entry and to delete it if it is present:

1. Type the following command and press **Enter** on the DTACS server to check for the existence of an appservatm entry in the /etc/hosts file:

   ```
   grep appservatm /etc/hosts
   ```

2. Is there an appservatm entry in the /etc/hosts file?
   - If **yes**, as the **root** user on the DTACS server, open the /etc/hosts file and delete the entry.
   - If **no**, go to the next procedure in this appendix.

Add DTACS as a Trusted Host on the EC Server

Important: All steps in this procedure take place in the **root** remote terminal window on the EC server.

1 In the **root** remote terminal window on the EC server, verify the name of the DTACS server by typing the following command and pressing **Enter**:

```
grep [dtacsIP] /etc/hosts
```

2 Locate the dtacs entry and record the first entry that follows the IP address for DTACS in the space provided.

Host Name of DTACS Server: _____

Example: In the following example, the output shows that the hostname of the DTACS server is **dtacshost**.

```
# grep 203.0.113.2 /etc/hosts
203.0.113.2  dtacshost  dtacs
```

Notes:

- The first name listed after the IP address is the hostname of the DTACS server; the other names are aliases.
- This is only an example. The IP address and entries for dtacs may differ in your /etc/hosts file.

3 Add the following entries into the hosts.equiv file, where [dtacshost] is the entry you recorded in step 2:

```
[dtacshost] dtacs
[dtacshost] dncs
[dtacshost] root
```

Important: Substitute the hostname you recorded in step 2 for [dtacshost]. Do not include the brackets.

4 Save and close the file.

Create the Private and Public Keys Between the EC and DTACS Servers

This procedure includes the steps that add the private/public keys between the EC and DTACS server. This procedure is necessary because of the Enhanced Security feature enabled in this system release.

1 Record the hostname for the DTACS server that you identified in step 2 of the ***Add DTACS as a Trusted Host on the EC Server*** (on page 83) in the space provided.

Host Name of DTACS Server: _____

2 In the **root** remote terminal window of the DTACS server, open the **/export/home/informix/etc/sqlhosts** file in a text editor.

3 Open a new line at the end of the file and add the following entry:

```
dncsatmDbServer ontlitcp dncsatm informixOnline
```

4 Save and close the sqlhosts file on the DTACS server.

5 In the **root** remote terminal window of the EC server, open the **/export/home/informix/etc/sqlhosts** file in a text editor.

6 Open a new line at the end of this file and add the following entry:

```
dncsatmDbServer ontlitcp dncsatm informixOnline
```

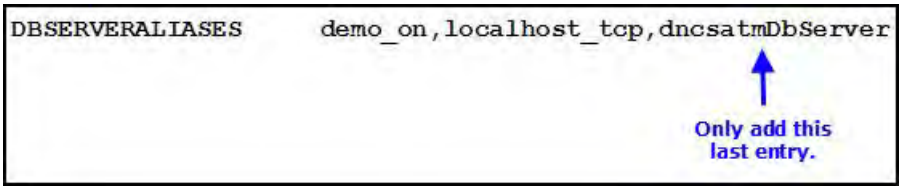
7 Save and close the file on the EC server.

8 In the **root** remote terminal window of the EC server, open the **/export/home/informix/etc/onconfig** file in a text editor.

9 Add **dncsatmDbServer** to the end of the **DBSERVERALIAS** variable in the onconfig file.

Important: This is an example; the entries for DBSERVERALIASES may differ on your system. Ensure that dncsatmDbServer is the last entry in this line.

Example:



10 In the **root** remote terminal window on the EC server, type the following command and press **Enter** to start the Informix listener for the dncsatmDbServer:

```
onmode -P start dncsatmDbServer
```

11 In the **root** remote terminal window on the EC server, type the following command and press **Enter**. The **Enter the host name of the site you are adding** message appears.

```
siteCmd -S
```

12 Type the hostname of the DTACS server (recorded in step 2) and press **Enter**. The **Enter the IP address of the site you are adding** message appears.

Example: `dtacshost`

Note: Replace the hostname in this example with the actual hostname for your DTACS server (recorded in step 2).

13 Type the IP address of the DTACS server (used in step 1) and press **Enter**. The **Do you want to continue?** message appears.

Example: `203.0.113.2`

Note: Replace the IP address in this example with the actual IP address for your DTACS server (used in step 1).

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

Results:

- A message appears that states that the system is backing up and adding an entry to the /etc/hosts file.
- The **Do you want to continue?** message appears and you are prompted for the root password of the DTACS server.

15 When prompted, type the **root** password for the DTACS server and press **Enter**. The system displays a series of messages about generating various keys and a **Done** message appears when it is finished.

16 Type the following command and press **Enter** to change to the **dncs** user:

Note: You should still be working in the **root** remote terminal window of the EC server.

```
sux - dncs
```

17 Type the following command and press **Enter**:

```
ssh -X -i /export/home/dncsSSH/.ssh/siteKey dncsSSH@[DTACS hostname]
```

Note: ubstitute the hostname of your DTACS server (recorded in step 1) for [DTACS hostname]. Do not include the brackets.

Result: The system logs you on to the DTACS server as dncsSSH user. You are now connected to the DTACS server and the host for the DTACS server is permanently added to the list of known hosts on the EC.

18 Type `su -` and press **Enter**. The password prompt appears.

19 Type the **root** password for the DTACS server and press **Enter**.

20 Type the following command and press **Enter** to change to the **dncs** user:

```
sux - dncs
```

21 Type the following command and press **Enter**:

```
ssh -X -i /export/home/dncsSSH/.ssh/siteKey dncsSSH@dncsatm
```

Result: The system logs you on to the EC as dncsSSH user and the **Are you sure you want to continue connecting?** message appears.

Note: If an error message appears about **conflicting keys**, open the known_keys file, and delete the entry that corresponds to the dncsatm. Then, save the file and repeat this step.

22 Type `y` and press **Enter**. You are now connected to the EC. The hostname for the EC is permanently added to the list of known hosts on the DTACS server.

23 Type `exit` and press **Enter** until the remote terminal windows close and you are entirely logged out as dncsSSH user on the DTACS and the EC servers. Your current window should be the root user in the EC remote terminal window.

Revise the sshd_config File on the DTACS Server

Important: All steps in this procedure take place in the **root** remote terminal window of the DTACS server.

1. Open the /etc/ssh/sshd_config file in a text editor.
2. Edit the **PermitRootLogin yes** entry to the following:

   ```
   PermitRootLogin no
   ```

3. Save and close the sshd_config file.
4. Type the following command and press **Enter** to restart the SSH service:

   ```
   svcadm restart ssh
   ```

Verify User Ownership and Group Permissions

Important:

- All steps in this procedure take place in the **root** remote terminal window of the DTACS server.
- The examples in the following steps may differ from the output on your system; however, they should be similar.
- Do not change the group ID for any group.

Perform this procedure to verify that the ownership for dncs, dtacs, and dncsSSH users are correct on the DTACS server and also to verify that the dncs user belongs to the dtacs group and the dtacs user belongs to the dncs group:

1 Type the following command and press **Enter** to verify directory ownership for the dncsSSH, dncs, and dtacs users:

```
ls –ltr /export/home
```

Example: Output should be similar to the following example:

```
# ls –ltr /export/home
  .
  .
  .
drwxr-x---   3 dncsSSH  dtacs     512 Feb 22 15:30 dncsSSH
drwxr-x---   6 dncs     dncs      512 Feb 23 07:25 dncs
drwxr-xr-x   7 dtacs    dtacs     512 Mar  3 10:19 dtacs
```

2 Type the following command and press **Enter** to verify that the dncs user belongs to the dtacs group:

```
groups dncs
```

Example: Output should be:

```
dncs dtacs
```

3 Type the following command and press **Enter** to verify that the dtacs user belongs to the dncs group:

```
groups dtacs
```

Example: Output should be:

```
dtacs dncs
```

Test dbSync on the DTACS Server

Important: All steps in this procedure take place in the **root** remote terminal window of the DTACS server.

Complete the following procedure to ensure that the DTACS database successfully syncs with the DNCS database:

1. In the root remote terminal window of the DTACS server, type the following command and press **Enter** to switch to the **dncs** user:

   ```
   sux - dncs
   ```

2. Type the following command and press **Enter** to establish the correct DTACS environment:

   ```
   . /dvs/dtacs/bin/dtacsSetup
   ```

   Note: Make sure there is a space between the period (**.**) and the forward slash (**/**).

3. Type the following command and press **Enter** to verify that you can access the DNCS database:

   ```
   dbaccess dncsdb@dncsatmDbServer -
   ```

   Example: Output should be similar to the following example:

   ```
   $ dbaccess dncsdb@dncsatmDbServer -
       Database selected
       >
   ```

4. Press the **Ctrl** and **c** keys simultaneously to exit from the dbaccess utility.
5. Type the following command and press **Enter** to initiate a synchronization of the DTACS database:

   ```
   dtacsdbsync -S
   ```

6. Did a **Dbsync Succeeded** message appear at the end of the script?
   - If **yes**, the synchronization was successful. Go to step 7.
   - If **no**, contact Cisco Services for assistance.
7. Click the **Sys Config** button on the Web UI console. The DTA Control System Configuration window opens.
8. Click **Sync Db** to initiate the DTACS database synchronization process.
9. Did a **DB Sync request processed successfully** message appear?
   - If **yes**, the synchronization was successful.
   - If **no**, contact Cisco Services for assistance.

D

Setting Up the Network Time Protocol on Solaris Servers and Clients

Introduction

The instructions in this appendix describe how to set up the Network Time Protocol (NTP) on Solaris 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, if desired.

Note: Obtain the primary and any secondary NTP source IP addresses from the system operator.

1. If necessary, open a remote terminal window on the EC.
2. Complete the following steps to log on to the xterm window as the **root** user.
   a. Type `su -` and press **Enter**. The password prompt appears.
   b. Type the root password and press **Enter**.
3. Type the following command and press **Enter** to initialize the /etc/inet/ntp.conf file as a server:
   ```
   /dvs/platform/libexec/install_ntp -s
   ```
4. Open the `etc/inet/ntp.conf` file in a text editor.
5. Replace the contents of the ntp.conf file with the following:
   ```
   server [Primary Time Source IP Address] prefer
   server [Secondary Time Source IP Address]
   server 127.127.1.0
   driftfile /etc/ntp.drift
   ```
6. Save and close the ntp.conf file.
7. Type the following command and press **Enter**.
   ```
   svcs | grep ntp
   ```
8. Did the output from step 7 show *ntp*?
   - If **yes**, continue with step 9.
   - If **no**, type the following command and press **Enter**. Then, go to step 9.
     ```
     svcadm enable ntp
     ```
9. Type the following command and press **Enter** to restart the NTP service:
   ```
   svcadm restart ntp
   ```
10. Type the following command and press **Enter** to check the status of the NTP:
    ```
    ntpq -p
    ```
    Result: You should see output similar to the following:
    ```
        remote           refid      st t when poll reach   delay   offset
    disp
    ==============================================================
    ====
    *PrimNTPSvr 198.51.100.44 3 u   53   64   37  0.37  -2.320
    438.31
    ```

```
LOCAL(0)     LOCAL(0)        5 l   49   64   37  0.00   0.000
438.35
```

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.

11 Type `exit` and press **Enter** to log out the root user.

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. An example is the RNCS EC.

1. If necessary, open a remote terminal window on the client.
2. Complete the following steps to log on to the xterm window as the **root** user.
   a. Type `su -` and press **Enter**. The password prompt appears.
   b. Type the root password and press **Enter**.
3. Type the following command and press **Enter** to initialize the /etc/inet/ntp.conf file as a client:

   ```
   /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 wish to change this setting, you can use a text editor to edit the ntp.conf file.
4. Type the following command and press **Enter** to restart the NTP service:

   ```
   svcadm restart ntp
   ```
5. Type the following command and press **Enter** to check the status of the NTP:

   ```
   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.
6. Type `exit` and press **Enter** to log out the root user.

E

Mounting and Unmounting ISO Images

Introduction

The instructions in this appendix describe how to mount and unmount an ISO image. Two methods for each are provided:

- Mounting and unmounting using VMware
- Mounting and unmounting using the lofiadm utility

In This Appendix

Mounting and Unmounting Using VMware

Mount the ISO Image

1. In an xterm window, as the **root** user, type the following command and press **Enter** to unmount any ISO image that may be mounted:

   ```
   eject cd
   ```

2. Right-click the VM and select **Edit Settings**. The Edit Settings window opens.
3. Click **CD/DVD drive 1**.
4. On the right side, in the **Device Type** area, choose **Client Device** and click **OK**.
5. Repeat Steps 2 and 3.
6. In the **Device Type** area, click **Datastore ISO File** and then click **Browse** to navigate to the ISO image.
7. Select the ISO image and click **OK**.
8. On the right side, in the **Device Status** area, click **Connected** and **Connect at power on**. Then, click **OK**.
9. In an xterm window as the **root** user, enter the following commands to restart the volfs process:

   ```
   svcadm restart volfs
   df –h
   ```

   Note: The ISO image should be mounted at /cdrom/cdrom.
10. In an xterm window, type the following command and press **Enter** to verify that the ISO system release is correct:

    ```
    less /cdrom/cdrom/sai/TOC | grep “System Release”
    ```

    Example:

    ```
    less /cdrom/cdrom/sai/TOC | grep "System Release"
    D::SRDVD::6.0.0.22_SunOS_i386::System Release 6.0 DVD
    ```

    Note: If the ISO image does not mount, contact Cisco Services for assistance.

Unmount the ISO Image

To unmount the ISO image, type the following command and press **Enter**:

```
eject cd
```

Mounting and Unmounting Using the lofiadm Utility

From within the Solaris operating system, users can mount and unmount ISO images for reading with the lofiadm utility.

This procedure is valid for mounting the PUC and SRDVD ISO files. Follow this procedure to mount either ISO file. When mounting the PUC on a SPARC system, this is the procedure you will use.

Mount the ISO Image

1. Type the following command and press **Enter** to verify that nothing is currently mounted by the volume manager:

   ```
   eject cd
   ```

2. Type the following command and press **Enter** to create the mount point.

   Important: Only execute this step if the /cdrom/cdrom directory does not already exist.

   ```
   mkdir -p /cdrom/cdrom
   ```

3. Type the following command and press **Enter**. Note the lofi device name that is returned.

   ```
   lofiadm -a <path_to_ISO>/<ISO_filename>
   ```

   Example:

   ```
   lofiadm -a
   /net/aurora/ccm_archive/release/integrate/system_release_dvd/7
   .0.0.9_SunOS_i386/PUC_7.0.0.9_SunOS_i386.iso
   ```

   Note: This is a lengthy command. Do not press Enter until the entire command has been typed.

4. Type the following command and press **Enter**, using the device name from step 3.

   ```
   mount -F hsfs <lofi_device_name> /cdrom/cdrom
   ```

   Example:

   ```
   mount -F hsfs /dev/lofi/1 /cdrom/cdrom
   ```

Unmount the ISO Image

1. Type the following command and press **Enter** to unmount the image:

   ```
   umount /cdrom/cdrom
   ```

2. Type the following command and press **Enter** to delete the device created when you mounted the image:

   ```
   lofiadm -d <lofi_device_name>
   ```

Example: `lofiadm -d /dev/lofi/1`

F

Registration of EC with the ECS

Introduction

Use the information in this appendix to register an EC device with the Explorer Controller Suite (ECS).

Important: To register an EC to an ECS, you must have an operating ECS on your network.

In This Appendix

Enable Regionalization on the EC

Contact Cisco Services for installation of the SAIlic package and for the enabling of the Regionalization feature.

Configure the EC System for Regionalization

1. Access the EC WUI by entering the following address in a Firefox Web browser. The Explorer Control WUI opens.

   `http://[EC_IP]/dncs`

   Example: `http://102.0.2.135/dncs`

   Note: The rpOrch process will be yellow (Recovering) in the EC Process Status WUI.

2. Click **EC > System Provisioning > Regionalization Configuration**. The Regionalization Configuration WUI opens.

3. Enter the appropriate values for the following fields:

   - **EC ID** — A unique ID that identifies a specific EC

     Note: It is recommended that the EC hostname is used as the EC ID.

   - **Primary EC Description** — (Optional) Text to describe the EC, such as location (for example, LWR, SJC)

     Note: This is useful in identifying where the primary EC is physically located. Cisco recommends that you use a location code for your primary EC's location. If the primary EC crashes and the secondary EC crashes, as well, the description of the secondary EC will be moved to the description of the primary EC by the Replicated Database process.

   - **EC Management URL Scheme** — Select how the EC Administration Console URL is accessed, either http or https

   - **EC Management URL** — (Read Only) Calculated by the EC and populated after pressing **Save**

     Note: This is displayed for informational purposes, only.

- **Standby EC Description —** If a standby/secondary EC is present, you can optionally enter a description to identify the standby EC

  Notes:

  – This is useful in identifying where the secondary EC is physically located. Cisco recommends that you use a location code (for example, ATL, SJC, and so on).

  – Leave this field empty if there is no standby EC configured. If the primary EC crashes and the secondary EC becomes the primary EC, this description field moves to the **Primary EC Description** field by the RepDb process.

- **Standby EC Timezone —** (Optional) Defines the timezone where the standby EC is located

  Note: Leave this field empty if there is no standby EC configured.

- **Standby EC IP —** The IP address of the standby EC, if a standby EC exists

  Note: Leave this field empty if there is no standby EC configured.

- **ECS Group ID —** Enter the ECS group ID

  Example: `rac1ecs1`

- **Pending Registration Timeout —** The timeout period for which the registration request stays pending if not acknowledged by the ECS. If a response is not received within this period, the request will time out and the operator has to click the **Retry** button.

- **Management Console Controller IP —** The IP address or hostname of the Videoscape Control Suite Management Node

  Example: `192.0.2.84`

- **Management Console Controller Port —** Port on which the Management Console Controller restful interface is listening. It is usually 8200, which is the default.

- **BOA URL —** Contains the protocol (http/https), destination host (and optional port), as well as the URL string to proxy BOSS requests to the BOA when regionalization is enabled. It is usually `http://boa-ip:8080`.

- **BOA Timeout —** How long the cloud proxy waits for a response from BOA before timing out

4 Click **Save**. The following results occur in the lower area of the WebUI:

- **Registration Status** indicates the current status of the EC registration (a successful registration will indicate **Registered**)

- **Status Comment** indicates the current state of the EC registration (if registration is successful to the ECS, the comment displays **Successfully Registered**)

- **Last Updated Time i**ndicates the time in which the EC was successfully registered to the ECS

5 Go to **ECS (https://IP)** and click **Message Infrastructure > Service Infrastructure > Service Instance**. Service Instances are present for the EC host you registered.

6 From the ECS WUI, click **Services > ECS Management > Dashboard**.

7 Click the **Network Element Management** tab.

8 Click **Network Element Access Management**.

9 From the **User** area, select a user that you want to have the ability to access (log in to) the EC (Network Element).

10 From the **Network Element(s)** area, select all ECs to which you want access.

11 Click **Save**.

12 Repeat steps 9 through 11 for another user, if necessary.

Index

S

T

V

W

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 2015

Part Number OL-29862-01