Installation and Migration Guide for 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

© 2015 Cisco and/or its affiliates. All rights reserved.

Information in this publication is subject to change without notice. No part of this publication may be reproduced or transmitted in any form, by photocopy, microfilm, xerography, or any other means, or incorporated into any information retrieval system, electronic or mechanical, for any purpose, without the express permission of Cisco Systems, Inc.

Contents

About This Guide

Purpose

This guide provides step-by-step instructions for the installation and migration of a Digital Broadband Delivery System (DBDS) to System Release (SR) 6.0. This document provides instructions for sites that have an integrated Application Server, as well as for sites that do not.

SR 6.0 Features Forklift Upgrade

The upgrade to SR 6.0 involves migration from Sun Microsystems (Sun) SPARC servers to Cisco's Unified Computing System (UCS). The SR 6.0 upgrade allows engineers to upgrade the system without having to shut the system down until the activation of the new system software.

Cisco engineers have expended great effort to 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, and so on) 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 maintenance window that usually begins at midnight. Upgrade engineers have determined that a typical site can be upgraded within one 6-hour maintenance window. The maintenance window should begin when you stop system components in 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 DBDS to SR 6.0.

Read the Entire Guide

Please review this entire guide before beginning the installation. If you are uncomfortable with any of the procedures, contact Cisco Services 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 DNCS and Explorer Controller (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 4.2.0.x SP4, SR 4.3.x.x, SR 5.0.x.x, or SR 5.1.x.x
- You have infrastructure to support GigE BFS

  Note: This includes router configuration for Multicast, router ports configured for Multicast BFS, and a BFS-capable GQAM. Sites may also have other configuration requirements for GigE BFS.
- Sites running SR 4.2.0.x, SP4, and SR 4.3.x.x have already moved all BFS sessions to a GQAM
- You have the Solaris 10 x86 Update 10 license and ISO
- You have VMware ESXi (5.0u1 or 5.1u1) and vCenter infrastructure (software, license, and a running vCenter machine)

- You have a complete list of all third-party tools and scripts currently in use on the DNCS
- 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 DNCS are deleted as part of this upgrade.

If you use Digital Terminal Adapters (DTAs) in your network, you must upgrade your DTA code to HDDTA 170 v176 (or later) for use with SR 6.0.

Tested Reference Configuration

Server Series	UCS Release	Server Model	OS Vendor	OS	Component	Adapter	Adapter Driver
C Series Standalone Servers	1.5(3)	C240-M3(SFF)	VMware	VMware vSphere ESXi 5.0 U1	RAID Adapter	LSI 9271-8i /LSI 9271CV- 8i MegaRaid SAS HBA	6.506.51.00.1vmw
C Series Standalone Servers	1.5(3)	C240-M3(SFF)	VMware	VMware vSphere ESXi 5.1 U1	RAID Adapter	LSI 9271-8i /LSI 9271CV- 8i MegaRaid SAS HBA	6.506.51.00.1vmw

Note: This is the minimum tested reference configuration. Refer to the UCS HW and SW Interoperability form (http://www.cisco.com/web/techdoc/ucs/interoperability/matrix/matrix.html) to ensure that your components satisfy these requirements.

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 (next in this document) 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.
- 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
```

Supported Server Platform

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

DNCS/EC/RNCS 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, examine ***Cisco UCS C210 Server Configuration*** (on page 189). This appendix contains details pertinent to the C210 server.
- To ensure the reliable operation of the UCS and the Explorer Controller, the UCS should be connected to a UPS-protected power source and should be shut down gracefully if there is a risk that the server will lose power. Details on the power requirements for the UCS can be found in the hardware installations guides provided with the servers.

Other Required Hardware

In order to perform the initial configuration of the UCS hardware you will need the following:

- KVM Cable Adapter (provided with the UCS)
- Standard USB Keyboard
- Monitor with a VGA cable
- A KVM with the appropriate adapters can be used in place of the monitor and keyboard

Correlation to the ASI BFS to RFGW-1 GigE BFS Conversion Configuration Guide

The *ASI BFS to RFGW-1 GigE BFS Conversion Configuration Guide* (part number OL-31477) provides step-by-step instructions for configuring the RF Gateway (RFGW-1) and converting the ASI BFS to the RFGW-1 GigE BFS. This document should be used in conjunction with the installation and migration steps detailed in this guide so that you can configure the RFGW-1 and convert the ASI BFS directly to the RFGW-1 GigE BFS. For now, just obtain the *ASI BFS to RFGW-1 GigE BFS Conversion Configuration Guide* (part number OL-31477). At the appropriate time, you will be instructed to reference it.

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 carries forward the enhanced security which was first introduced in DNCS SR 5.0 and 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.

RBAC

As part of the security enhancements, the system now uses Sun's Role Based Access Control (RBAC) system. This feature converts the "dncs" account to a dncs "role", and you will no longer be able to log on to the system directly as the dncs user. Instead, you will need to create individual accounts with various levels of access to the "dncs" role.

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 xterm 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, and so on) 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, after DNCS processes are stopped.

Estimated Timeline

The upgrade to SR 6.0 features the forklift upgrade, which provides the ability to stage 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 involve resetting the modulators. 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
```

SSP2.3 Compliance

If your site is not SSP2.3 Compliant, you will need to add the following entry to the DNCS .profile file:

```
# VOD variable for systems that are not SSP2.3-compliant

DNCS_DRM_INCLUDE_HE_RSR_VOD=1

export DNCS_DRM_INCLUDE_HE_RSR_VOD
```

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

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 Cisco Services to purchase the required license.

Important:

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

About the preUpgradeChecks Script

This release includes a preUpgradeChecks script that validates your system for upgrade eligibility. The preUpgradeChecks script should be run 2 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. The instructions are found in ***Run the preUpgradeChecks Script on the SPARC DNCS and RNCS*** (on page 31).

Important: The preUpgradeChecks scripts must be run on each server that will be upgraded (for example, DNCS and Remote Network Control Server (RNCS)).

Additional IP Address and NAS Interface Requirements

Sites migrating to GigE BFS, as part of the migration, will need to determine if they will use Multicast or Unicast to deliver BFS to the BFS/Data QAM (GQAM or RFGW).

- For Multicast delivery, you will need to choose a block of addresses, such as 23x.x.x.x.

  Important: This block must not conflict with other services on your network.

- For Unicast, you will need to specify a starting port (1025-65535).

In addition to inheriting all of the IP addresses of the existing DNCS, the UCS server/EC will require the following additional IP addresses.

- CIMC Management IP address
- ESXi Management IP address
- Temporary IP address (for access to the DNCS)
- IP address for the Network Attached Storage (NAS) Interface (if a dedicated interface will be used)

  Note: The UCS/EC does not support backing up to tape. Backups of key files, the filesystem, and the database will be performed to the NAS.

- EC RepDB IP address

  Note: In production environments, it is expected that a primary and secondary EC will be built and that they will be kept synchronized using the Replicated Database (RepDB) process. An interface on each EC needs to be dedicated for this function.

2

SR 6.0 Pre-Upgrade Procedures

Introduction

This chapter contains procedures that you should complete before you begin the actual SR 6.0 upgrade.

In This Chapter

Open a root and dncs xterm Window on the DNCS and an xterm Window on the Application Server

To upgrade your system to SR 6.0, you will need to execute commands and scripts as both **root** and **dncs** user on the DNCS as well as the Application Server. For this reason, we recommend opening a total of three xterm windows: one that accesses the DNCS server as **root** user, one that accesses the DNCS server as **dncs** user, and one that accesses the Application Server.

Note: If you are migrating an SR 5.0 or SR 5.1 system with an integrated Application Server, you do not need to open an extra window for the Application Server.

Important: Once this procedure is complete, we will refer to either the root or the dncs xterm window on the DNCS or the xterm window on the Application Server for the remaining procedures in this document.

Complete the following steps to open the xterm windows.

1. Open three xterm windows on the DNCS system.
2. In one xterm window, change to **root** user by completing the following steps.
   a. Type `sux - root` and press **Enter**. The password prompt appears.
      Note: If you are upgrading from SR 4.x, type `su - root`, instead.
   b. Type the root password and press **Enter**.
3. In the second xterm window, type the following command and press **Enter** to verify that you are logged in as **dncs** user.
   ```
   id
   ```
   Example:
   ```
   uid=500(dncs) gid=500(dncs)
   ```
4. Is the ID (uid) of the second xterm window dncs?
   - If **yes**, go to the next step.
   - If **no**, type the following command and press **Enter**. Then, repeat Steps 3 and 4.
     ```
     sux – dncs
     ```
5. In the third xterm window, type the following command and press **Enter** to access the Application Server, if applicable.
   - On a DNCS prior to SR 5.0, type:
     ```
     rsh appservatm
     ```
   - On a DNCS running SR 5.0 or later, type:
     ```
     siteCmd appservatm ksh
     ```
6. Type the commands from Step 2 to switch to root user in the Application Server xterm window.

Check the .profile Exit Status

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

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

   ```
   . ./.profile
   ```

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

   ```
   echo $?
   ```

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

3. Is the exit status 0?

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

4. Open the dncs user .profile file in a text editor, such as vi. Review the file for problems. Check especially for the following condition:

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

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

Pre-Upgrade System Verification

Use this procedure to verify that an active communication link exists between the DNCS and the various system components. The DNCS must be able to communicate with other system components to ensure a successful system upgrade.

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

1. From the **dncs** xterm window, use the UNIX **cd** command to change to the directory that contains the Doctor Report.
2. Examine the log file and verify that the system was able to ping the following hardware components:
   - The Broadband Integrated Gateway (BIG)

     Note: If the site you are upgrading uses Direct ASI, you may not be able to ping the BIG.
   - All Quadrature Amplitude Modulators (QAMs) in the system
   - The Transaction Encryption Device (TED)
3. Verify that you can manually ping all router interfaces in the system.
4. Type the following command and press **Enter** to verify that you are using no more than 85 percent of the partition capacity of each disk.

   ```
   df -k
   ```

   Note: If any disk partition lists a capacity of greater than 85 percent, contact Cisco Services before proceeding.
5. Verify that you can successfully stage a DHCT (OSM and CVT methods).
6. Complete these steps to perform a slow and fast boot on a test DHCT and Combo-Box (if available) with a working return path (2-way mode):
   a. Boot a DHCT.

      Note: Do not press the power button.

   b. Access the Power On Self Test and Boot Status Diagnostic Screen on the DHCT and verify that all parameters, except UNcfg, display **Ready**.

      Note: UNcfg displays Broadcast.

   c. Wait 5 minutes.

   d. Press the power button on the DHCT. The power to the DHCT is turned on.

   e. Access the Power On Self Test and Boot Status Diagnostic Screen on the DHCT and verify that all parameters, including UNcfg, display **Ready**.
7. Verify that you can ping the DHCT.
8. Verify that the Interactive Program Guide (IPG) displays 7 days of accurate and valid data.

9 Tune to each available channel on a DHCT to confirm that a full channel lineup is present.

Note: Record any anomalies you notice while verifying the channel lineup.

10 For all sites (SARA, Rovi, OCAP), verify that you can define, purchase, and view an IPPV, xOD, and VOD event.

Examine Disks and Mirrored Devices on the SPARC System

Important: If you are upgrading an EC SR 6.0 or later system, you can skip this procedure.

Examine the status of the mirrored disk drives on the Sun Fire V445, V880, or V890 DNCS prior to the upgrade.

This procedure only needs to be performed on Sun SPARC hardware platforms.

CAUTION:

If the disk mirroring functions are not working properly before the upgrade, you may not be able to easily recover from a failed upgrade.

Examining Disks and Mirrored Devices

Follow these instructions to examine the status of the mirrored drives on your system. This procedure should take only a few minutes to complete.

1 In the **root** xterm window, type the following command and press **Enter** to confirm that all disks are present and readable.

```
format  </dev/null
```

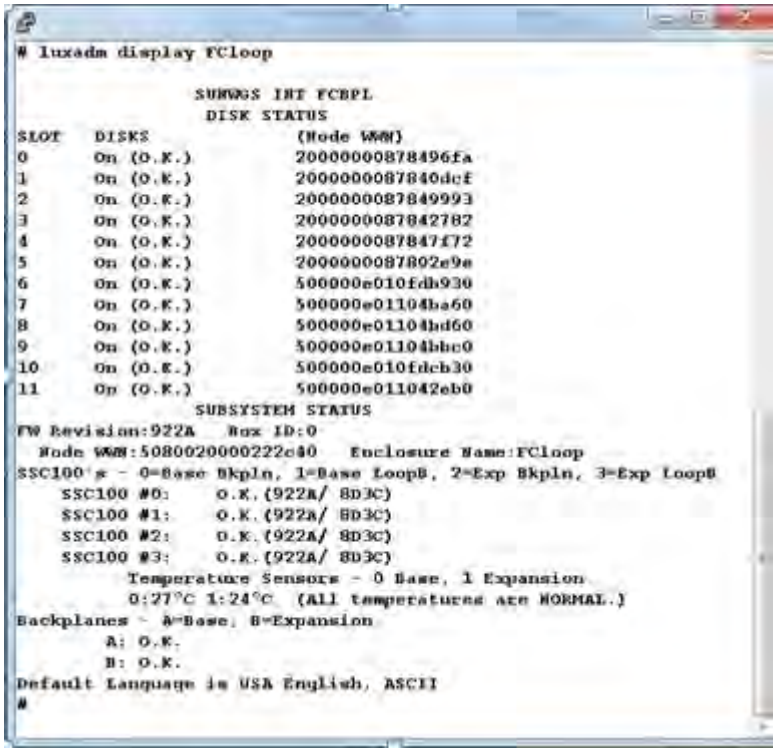
Example: You should see output similar to the following example:

```
AVAILABLE DISK SELECTIONS:
       0. c1t0d0 <SUN72G cyl 14087 alt 2 hd 24 sec 424>
/pci@8,600000/SUNW,qlc@2/fp@0,0/ssd@w500000e0108977d1,0
1. c1t1d0 <SUN72G cyl 14087 alt 2 hd 24 sec 424>
.
..
23. c2t13d0 <SUN72G cyl 14087 alt 2 hd 24 sec 424>
/pci@9,600000/pci@1/SUNW,qlc@4/fp@0,0/ssd@w2200000c5056c543,0
```

2 Is your Sun SPARC platform a Sun Fire V880 or V890?

- If **yes**, type (as root user) the following command and press **Enter** to verify that all slots with disks have a Disk Status of **OK**.

```
luxadm  display  FCloop
```



- If **no**, go to Step 4.

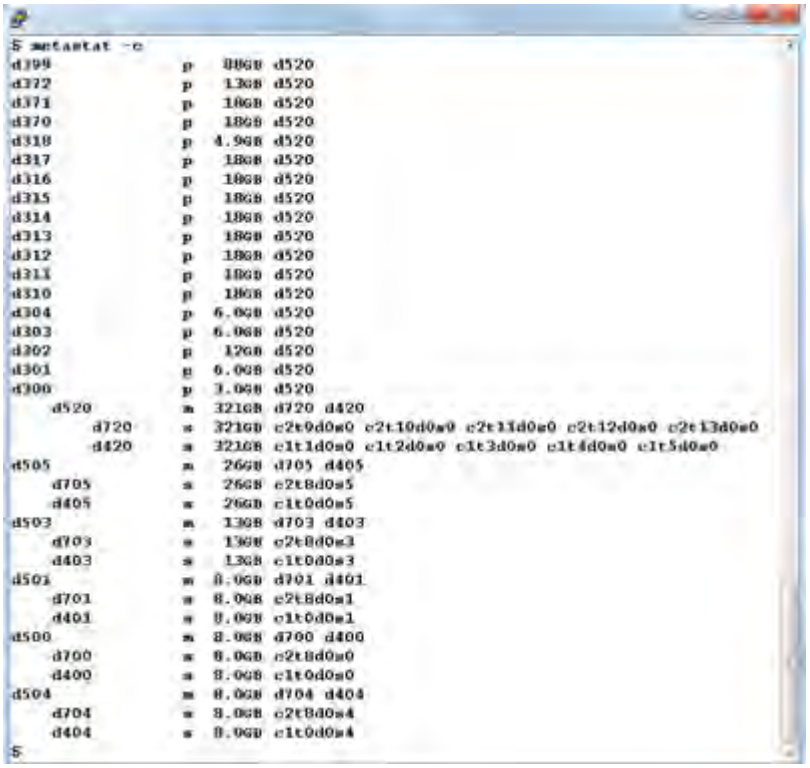
3 Did the output from Steps 1 and 2 reveal that all disks are present?

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

4 Type the following command and press **Enter**. Results similar to the following appear:

```
metastat -c
```

Example: The following example shows a Sun Fire V880 running SR 5.0 software, with a 12 X 73 disk configuration. All devices in this example are in good working order. Any problems with a device would be noted by "**( )**" next to the example.



5 Examine each device and submirror. Do any devices show **maintenance**?

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

6 Repeat Steps 1 through 5 on any LIONN (RNCS) servers on the system.

Important: Although this upgrade will complete successfully with the disks not mirrored, Cisco recommends that the disks be mirrored before attempting this upgrade.

Examine Key Files

The scripts used during the upgrade are designed to back up the key files most likely to be found on the DNCS. Some sites, however, include special key files that are unique to that site, only. As part of the backup, the upgrade scripts ask if you have any special files that you want to be added to the list of files to be backed up. When you answer *yes*, the system offers you an opportunity to add additional files and directories to the default key files list.

Note: This is a comprehensive list containing the names of key files for all system types for a complete key file recovery backup. Some of the files in this comprehensive list will NOT be included in a backup on your current system.

With this release, you may now create a file containing the list of absolute paths to files/directories you want to be added to the default key files list. You only have to supply the path to this file and the upgrade will read the contents of the file and add those paths to the default key files list.

Important: The file we create for this example is called *keyfiles.out*. You can create a file name of your choice to maintain your system key files. The content of your file will differ from the example.

Example file:

```
$ less /export/home/dncs/keyfiles.out
```

/export/home/dncs/network

/export/home/dncs/tmp

/export/home/dncs/keyfiles.out

/dvs/backups/DBbackups

Important: You can save a lot of time if you spend a few minutes identifying those special files now. Work with the system operator to determine if there are any special files or scripts that need to be backed up.

Identify Special Files to be Backed Up

Create a file that contains the list of special key files that will be backed up and restored during the migration. Use the following guidelines when you create the list:

- Make a list of all custom scripts that your system uses.
- Review all system cron files and write down any special cron files that you want to retain after the upgrade.

  Notes:

  - Some of your special cron files may reference custom scripts. Be certain to include those custom scripts on any list of special cron files you want backed up.
  - Call Cisco Services if you are unsure of what cron files you need to back up separately.

- Review all entries in the /etc/vfstab file and record any unique entries that you want to retain after the upgrade.

  Note: The preUpgradeChecks script creates a copy of the vfstab file in the /dvs/admin/sysinfo directory. After the system is upgraded, you can use the entries you recorded or the saved vfstab file to add those unique entries back into the /etc/vfstab file.

- Review all entries in the /etc/dfs/dfstab file and record any unique entries that you want to retain.

  Note: The preUpgradeChecks script creates a copy of the dfstab file in the /dvs/admin/sysinfo directory. After the system is upgraded, you can use the entries you recorded or the saved dfstab file to add those unique entries back into the /etc/dfs/dfstab file.

Do Not Include These Files

When you create your list of special files to be backed up, avoid including the following types of files:

- Any binary files from the /usr/local/bin directory or binary files from any other directory. These binary files may not function after the upgrade and may actually harm the upgrade.
- Library files from the /usr/lib or the /usr/local/lib directories. These library files may not function after the upgrade and may actually harm the upgrade.
- Files in the /dvs/dncs/bin directories. When these files are restored (after the upgrade), they will overwrite the new binary files associated with the upgrade.

  Note: You should not need to back up any files in the /dvs/dncs/bin directories. However, if you have placed a utility in this directory and decide to back it up, our engineers recommend that you copy the utility to /export/home/dncs/scripts/MSOscripts before the upgrade. This directory is a default key file and will always be backed up during an upgrade.

The following is a list of files/directories that should NOT be included in your key files list.

- Solaris operating system binary or library files
- Informix software binary or library files
- Any of the following home directories:
  - /export/home/dncs

- /export/home/dncsSSH
- /export/home/dncsftp
- /export/home/easftp
- /export/home/dbreader
- /export/home/backup
- /export/home/secure
- /export/home/sysadmin
- /export/home/informix

Back Up Modulator Control Files

In the event that you ever need to access the pre-upgrade configuration files of the QAM-family and QPSK modulators, follow these instructions to make a backup copy.

Note: In the following commands, substitute the DNCS version that you are backing up for [DNCS version]

1. From the **root** xterm window on the DNCS, type the following command and press **Enter**:

   ```
   mkdir /tftpboot/backup.[DNCS version]
   ```

2. Type the following command and press **Enter**. The system copies all *.config files to the /tftpboot/backup.[DNCS version] directory.

   ```
   cp -p /tftpboot/*.config /tftpboot/backup.[DNCS version]
   ```

3. Type the following command and press **Enter** to verify that the configuration files were successfully copied to this directory.

   ```
   ls /tftpboot/backup.[DNCS version]
   ```

Copy the Application Server dncs User .profile File to the DNCS

Note: Complete this procedure *only* if your pre-SR 6.0 system uses a Cisco standalone Application Server.

Before migrating your current Application Server to an integrated Application Server environment on the DNCS, we recommend that you copy its existing .profile file to the DNCS. This ensures that, after the upgrade, the Application Server environment variables are correctly added to the DNCS user .profile file. This file will now include environment variables for both the DNCS and the Application Server.

To create a copy of the Application Server .profile file, complete the following procedure.

1 If necessary, open an xterm window on the DNCS.

2 Select one of the following sets of commands based upon the existing version of the DBDS system you are upgrading.

- If your system is currently at SR 4.2 SP4 or SR 4.3.x, type the following commands and press **Enter** in the dncs xterm window.

  a. `cd`

  b. `rcp appservatm:/export/home/dncs/.profile ./appserv.profile`

- If your system is currently at SR 5.0 or SR 5.1, type the following commands and press **Enter** in the dncs xterm window.

  a. `cd`

  b. `scp <username>@appservatm:/export/home/dncs/.profile ./appserv.profile`

  Notes:

  - The command in Step b is one continuous command. Do not press **Enter** until the entire command has been typed.
  - Replace <username> with a valid username, in Step b and in Step d, which follows.

  c. Enter the user password and press **Enter**. The file is copied to the user's home directory.

  d. `sux - dncs`

  e. `cp /export/home/<username>/appserv.profile .`

  f. `ls -l appserv.profile`

  Note: This command confirms the copy command of Step e.

Check the EAS Configuration—Pre-Upgrade

Checking the EAS Configuration

Before installing the DNCS 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)**.**

Note: You will check the EAS configuration after the installation of the DNCS SR 6.0 software, as well.

Check dncs_bfsRemote in the dncsSetup File (DSG Systems Only)

This procedure should only be run on systems that use the DOCSIS set-top gateway (DSG) for BFS. In this section, you will review the /dvs/dncs/bin/dncsSetup file for the dncs_bfsRemote variable setting. This information will be used during post-upgrade procedures if DSG BFS is configured on your system.

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

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

Example: `grep 'dncs_bfsRemote=' /dvs/dncs/bin/dncsSetup`

Sample output: `dncs_bfsRemote=dncsatm`

2 Does the output show the variable set to dncsdsg?

- If **yes**, you must execute the procedures in ***Modify the dncsSetup File for DSG*** (on page 116) after the migration is complete.

  Note: Do not go to Chapter 6 now. You will get there as a matter of course while following the procedures in this document.

- If **no**, you will skip the procedure in ***Modify the dncsSetup File for DSG*** (on page 116).

Check the Number of BFS Sessions

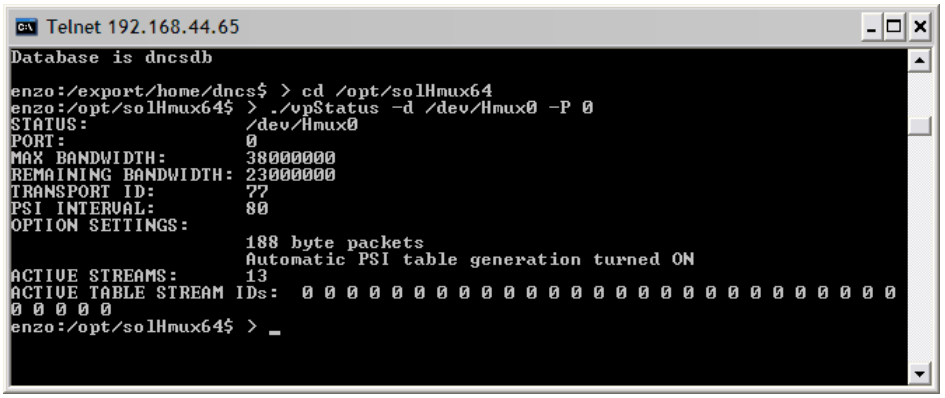
The number of BFS sessions post-upgrade needs to equal the number of pre-upgrade sessions. Use this procedure to determine and record the number of pre-upgrade BFS sessions. Then, after the upgrade, you will determine the number of post-upgrade BFS sessions.

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

1. Press the **Options** button on the front panel of the BFS QAM until the **Session Count** total appears.
2. Record the **Session Count** total in the space provided. _____
3. Does the system you are upgrading use the ASI card?
   - If **yes**, from the **dncs** xterm window, type the following command and press **Enter**.

     `/opt/solHmux64/vpStatus -d /dev/Hmux0 -P 0`

     Example: Output from the command should look similar to the following:

   - If **no**, go to the next step.
4. Type the following command and press **Enter**.

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

   Example: `auditQam –query 192.0.2.65 16`
5. Is BFS on a GQAM?
   - If **yes**, complete these instructions.
     a. Type the following command and press **Enter**.
        `telnet [GQAM IP address]`
     b. Press the **Ctrl** and **]** keys simultaneously to go to the telnet prompt.
     c. Type the following command and press **Enter** twice.
        `mode ch`
     d. Type the following commands and press **Enter** after each to display the GQAM sessions on the specified port.
        `session`
        `print_session_status <port #>`

Example:

```
session
print_session_status 15
```

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

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

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

6 Do the number of sessions shown in Steps 3, 4, and 5 match the number of sessions built on the BFS QAM?

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

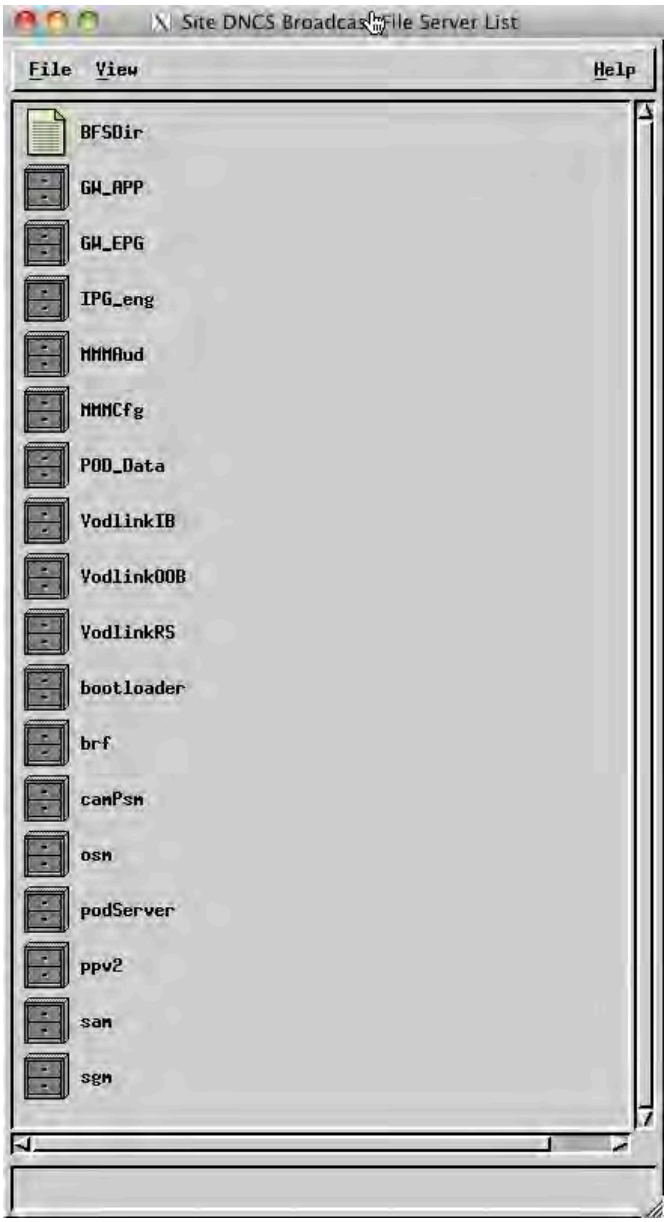
Record Third Party BFS Application Cabinet Data

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

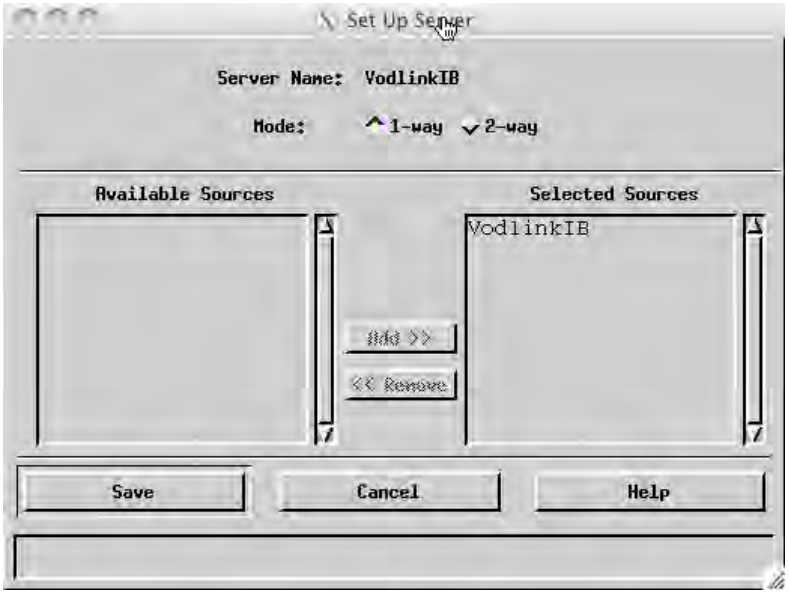
Note: You do not need to record this data for all BFS application cabinets, only those that are NOT created by the DNCS or the Application Server.

1 From the DNCS Administrative Console, click the **Application Interface Modules** tab.

2 Click **BFS Client**. The Broadcast File Server List window opens.



3 Highlight a third party application cabinet and click **File > Open**. The Set Up Server window opens for the selected cabinet.



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

Note: In the example used in Step 3, the **Server Name** is **VodlinkIB**, the **Mode** is **1-way**, and the **Selected Source** is **VodlinkIB**.

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

5 Click **Cancel** to close the Set Up Server window.

6 Record all folders, files, and link information in the cabinet.

7 Repeat this procedure from step 3 for each third-party BFS application cabinet in the Broadcast File Server List.

8 Close the Broadcast File Server List window when you are finished.

Delete DBDS corefiles Directories

The corefiles directory is located on /disk2. The /disk2 directory is a default key file directory. However, there is no need to back up and restore the contents of the corefiles directory. These are old core files that pertain to the errors that occurred with the previous software. These corefiles directories should be deleted before beginning the Live Upgrade. This section provides instructions for deleting old core files.

1. As the **root** user, type the following command and press **Enter** to change to the /dvs/[DBDS system]/tmp/corefiles directory:

   `cd /dvs/<DBDS system>/tmp/corefiles`

   Example: `cd /dvs/dncs/tmp/corefiles`

2. Type the following command and press **Enter** to delete all of the directories:

   `rm -r *`

3. Repeat Steps 1 and 2 on any LIONN servers on the system. The process core files are located in the following system directories:

   - **DNCS:** `/dvs/dncs/tmp/corefiles`
   - **LIONN:** `/dvs/lionn/tmp/corefiles`

Run the preUpgradeChecks Script on the SPARC DNCS and RNCS

This section describes how to run an automated system check on the SPARC DNCS and the RNCS to determine if your system is acceptable for an SR 6.0 upgrade. If it is, you can continue with the upgrade; if it is not, you must correct any errors that are found and then rerun this procedure.

1. Ensure that the SR 6.0 PUC ISO image is locally accessible to the system, or else available via a network shared drive.
2. If necessary, mount the ISO image using the lofiadm utility. See ***Mounting and Unmounting Using the lofiadm Utility*** (on page 187) for details.
3. From the **root** xterm window, select the appropriate command for the type of Application Server you are currently using.
   - If you are currently using a Cisco Application Server, type the following command and press **Enter**.

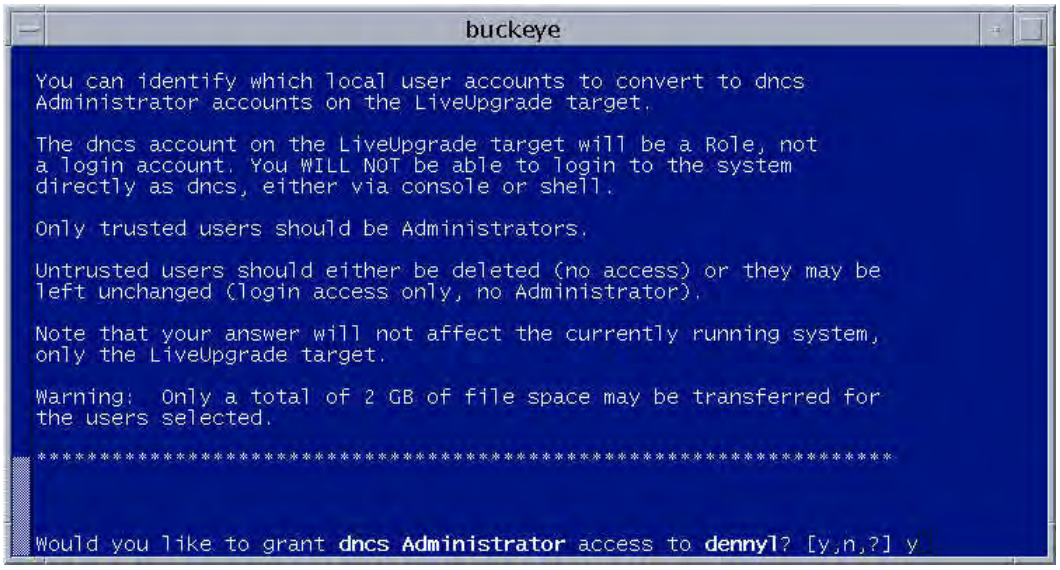
     ```
     /cdrom/cdrom/sai/scripts/preUpgradeChecks
     ```
   - If you are currently using a non-Cisco Application Server (MDN/ODN, Rovi Corp, and so on), type the following command and press **Enter**.

     ```
     /cdrom/cdrom/sai/scripts/preUpgradeChecks -A
     ```

   Result: The **Do you wish to continue?** message appears.
4. Type **y** and press **Enter**. The script checks for unique user accounts defined on this system.

   Important: If you are upgrading an existing SR 5.0 or SR 5.1 system, you will be asked if you want to "remove" < username > from the upgrade target. If you want to retain the user, answer **n** to this question. If you answer **y**, the user will not be present on the upgraded system.

Example:



5 Examine the message displayed on the screen after you have completed step 4.

- If the message **Would you like to grant Administrator access ... ?** appears, go to step 6.
- If the message **Do you want to remove ... ?** appears, go to step 7.
- If there are no unique users, go to step 9.

6 Do you want to grant dncs Administrator access to this user?

- If **yes**, type **y** and press **Enter**. Go to step 8.
- If **no**, type **n** and press **Enter**. The **Do you want to remove [username] from the upgrade target?** message appears. Go to Step 7.

7 Do you want to remove this user from the upgrade target?

- If **yes**, type **y** and press **Enter**. Go to step 8.

  Important: If there is a "backup" user account, answer **yes** to remove the home directory of this user.

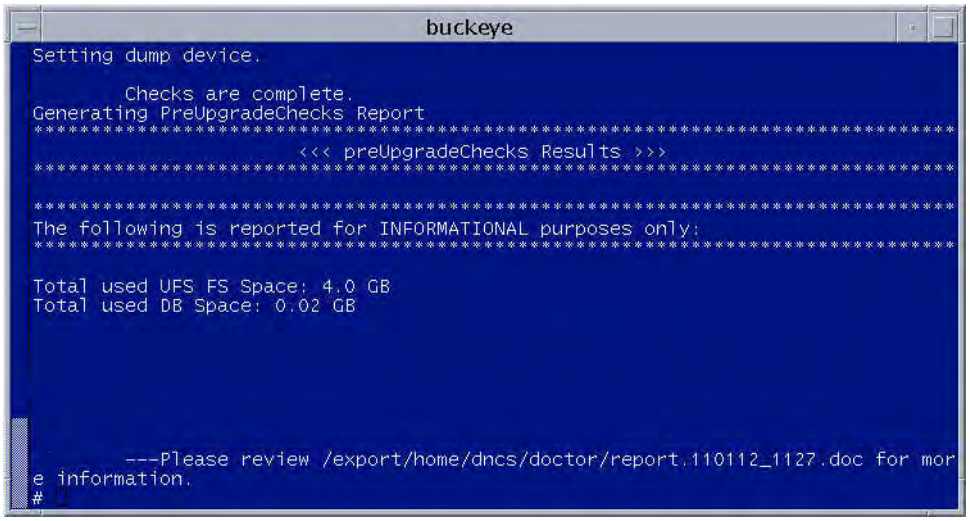
  Note: The /export/home/[username] directory will not be preserved after the upgrade.
- If **no**, type **n** and press **Enter**. Go to step 8.

8 Were you prompted for another username?

- If **yes**, repeat steps 5 through 8 for each username.
- If **no**, go to step 9.

9 Did any errors or warnings appear?

Example:



- If **yes**, correct these issues and repeat this procedure.

  Note: If errors continue to persist or if you need assistance with correcting an issue, contact Cisco Services.

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

10 Review the preUpgradeChecks logs in /var/log/preUpgradeChecks. Pay special attention to the puclog_<datetime> file and review the results of running the checkasi.sh script. If any bfshosts are using ASI (inbandmode 83), these bfshosts will be converted to Ethernet (inbandmode 69) as part of the upgrade.

Important:

- SR 6.0 does not support ASI BFS. The upgrade database migration, will change the *inbandmode* of each entry in the bfshost table from ASI (83) to GigE (69).
- If the preUpgradeChecks script found duplicate entries in the sm_pkg_auth table, these duplicates *must be* removed during the Maintenance Window after stopping system processes. This procedure is documented in ***Remove Duplicate sm_pkg_auth Entries*** (on page 88).

Run the del_nummap_dupes Script

Run this script to find and delete duplicate entries in the pdsernummap table.

Note: If the output from this script includes serial numbers that you are unable to validate, call Cisco Services if you are uncomfortable making the decision to delete duplicate entries.

1. Type the following command and press **Enter**. The script creates a log file in /var/log/preUpgradeChecks. If any duplicate entries are found, they are displayed in the script output and logged to /var/log/preUpgradeChecks.

   ```
   /cdrom/cdrom/sai/scripts/LU/PUC/optional_fixes/del_nummap_dupes -l
   ```

   Note: The "-l" is a lower case L.

2. Change to the /var/log/preUpgradeChecks directory and review the log file.
3. Did you find duplicate entries?
   - If **yes**, follow these steps to edit the /var/log/preUpgradeChecks/del_nummap_dupes_<datatime>.list file:
     a. If necessary, change to the /var/log/preUpgradeChecks directory.
        ```
        cd /var/log/preUpgradeChecks
        ```
     b. Type the following command and press **Enter**:
        ```
        cp del_nummap_dupes_<datatime>.list serialnum.del
        ```
     c. Open the serialnum.del file with a text editor.
        ```
        vi serialnum.del
        ```
     d. Delete the header and blank lines.
     e. Delete the entries that are correct and that you want to keep.
     f. Delete the MAC address for each serial number. This should leave only the serial numbers to be removed in the file.
     g. Save the file and exit the editor.
     h. Type the following command and press **Enter** to delete the duplicates:
        ```
        /cdrom/cdrom/sai/scripts/LU/PUC/optional_fixes/del_nummap_dupes -d serialnum.del
        ```
     i. Review the new del_nummap_dupes_<datetime>.log file for any errors.
     j. Repeat Step 1.
   - If **no**, this procedure is complete. Go to the next procedure in this chapter.
4. Did you find any **new** duplicate entries?
   - If **yes**, repeat step 3 to remove these new duplicate entries.
   - If **no**, go to the next procedure in this chapter.

Remove Expired eam Table Entries

In this procedure, you will execute the rmexpiredeam.sh script to remove expired eam table entries. Follow these steps to review and, if necessary, remove eam table entries.

1. Use the instructions in ***Mounting and Unmounting ISO Images*** (on page 185) to mount the SRDVD ISO.
2. As **dncs** user, enter the following command to list expired eam table entries:
   ```
   /cdrom/cdrom/sai/scripts/LU/PUC/other_scripts/rmexpiredeam.sh -l
   ```
   Note: The "-l" in this command is a lower-case L.
3. Did the script return any values?
   - If **yes**, continue with the next step.
   - If **no**, you are finished with this procedure. Go to the next procedure.
4. As **dncs** user, enter the following command to remove the expired eam table entries:
   ```
   /cdrom/cdrom/sai/scripts/LU/PUC/other_scripts/rmexpiredeam.sh -r
   ```
5. As the **root** user, enter the following command to ensure that eam entries have been removed:
   ```
   /cdrom/cdrom/sai/scripts/LU/PUC/other_scripts/rmexpiredeam.sh -l
   ```
   Note: The "-l" in this command is a lower-case L.
6. Did the script return any values?
   - If **yes**, contact Cisco Services.
   - If **no**, you are finished with this procedure.

Check for Node Set Names with Leading Blanks

In this procedure, you will execute the checknodesetname.sh script to find any Node Set names in the node_set table that have a leading blank space in the name. With the Web UI, leading blanks are not permitted in the node_set_name.

1. If necessary, use the instructions in ***Mounting and Unmounting ISO Images*** (on page 185) to mount the SRDVD ISO.
2. As **root** user, type the following command and press **Enter**. The script creates a log file in the /var/log/preUpgradeChecks directory.

   ```
   /cdrom/cdrom/sai/scripts/LU/PUC/other_scripts/checknodesetname
   s.sh -C
   ```

   Note: The log file has the following format:
   checknodesetname_MMDDYYYhhmmss.log
3. Review the log file for any node sets with leading blanks. If any node sets have leading blanks, the node name must be changed so that the leading blank spaces are removed. You will do this in the following step.
4. Did the log file reveal node sets with leading blank spaces?
   - If **yes**, change the node_set_name using the Node Set GUI.
   - If **no**, you are finished with this procedure.

Check for QAM Names with Trailing Blanks

In this procedure, you will check for QAM modulator names that have a trailing blank space in the name. QAM names with a trailing space can cause errors when adding QAM multicast source definitions. Follow the steps in this procedure to check for and remove trailing spaces.

1. If necessary, use the information in ***Mounting and Unmounting ISO Images*** (on page 185) to mount the SRDVD ISO.
2. As the **root** user, enter the following command to change directories to the script location:

   ```
   cd /cdrom/cdrom/sai/scripts/LU/PUC/optional_fixes
   ```
3. Type the following command and press **Enter**. The script checks each QAM name for a trailing space.

   ```
   ./checkqamnames.sh -C
   ```

   Note: The -C argument checks for QAM names with trailing spaces. It generates the following report in /var/log/preUpgradeChecks:

   checkqamnames_mmddyyyyhhmmss.log
4. Did the script find any QAM names that contained trailing spaces?
   - If **yes**, type the following command and press **Enter**. The script removes the trailing spaces from the QAM names.

     ```
     ./checkqamnames.sh -F
     ```
   - If **no**, go to the next procedure.
5. Review the output log: fixqamnames_mmddyyyyhhmmss.log.
6. Repeat step 3 to verify that there are no QAM names with trailing spaces.

Add the IPG Collector Entries to the /etc/hosts Files

If you are upgrading from a DNCS with a standalone Application Server, you must manually add the IPG Collector IP and hostname entries into the DNCS /etc/hosts file. This allows for the successful collection of IPG data, post-upgrade.

1 From an xterm window on the DNCS, switch to **root** user by completing these steps:

   a Type `su -` and press **Enter**.

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

2 Type the following command and press **Enter**. The ftphost entries in the ipgcollectconfig table of the appdb are displayed.

```
dbaccess appdb - <<E
select ftphost, description from ipgcollectconfig;
E
```

Sample output:

```
Database selected.


ftphost         ftp.tmstv.com
description  English Collector


ftphost         198.51.100.99
description   Spanish Collector
```

Note: In this example, the system shows two IPG Collectors that are provisioned. One uses a hostname; the other uses an IP address.

3 From an xterm window on the standalone Application Server, type the following command and press **Enter** for each IPG Collector. The ftphost entry in the /etc/hosts file is displayed.

```
grep 'ftp.tmstv.com' /etc/hosts
```

Sample output: `198.51.100.77 ftp.tmstv.com`

Note: IPG Collectors that use an IP address may not have an entry in the Application Server /etc/hosts file.

4 Does the output from step 3 show the ftphost as an IP address?

- If **yes**, does the output from Step 3 display an entry for each IPG Collector?
  - If **yes**, go to step 6.
  - If **no**, you need to add each unique entry to the Application Server /etc/hosts file. Go to step 5.
- If **no**, go to step 5 to add each entry to the Application Server /etc/hosts.

5 As **root** user, add the IP address and a hostname for each missing IPG provider (ftphost) to the Application Server /etc/hosts file.

Notes:

- Adding the IP address and a hostname to the Application Server /etc/hosts file should not cause any problems. You are simply associating the IP address to a hostname. The hostname should reflect one or all of the following: IPG Collector description (spa_ipg_collect), IPG content provider (ftp.tmstv.com), or source machine (IPG_File_Drop_Box).

  Example: `198.51.100.99  spa_ipg_collect`

- If all IPG Collectors use the same IP address or hostname, only one entry is necessary in the /etc/hosts file.

Important: This file is tab-separated. Use the tab key between the IP address and the hostname.

6 As **root** user on the DNCS, add each IPG Collector IP address and hostname to the /etc/hosts file.

Notes:

- Based on this scenario, when finished, you should have two new entries in the DNCS and Application Server /etc/hosts files. The entries should look similar to the following:

  ```
  198.51.100.77     ftp.tmstv.com
  198.51.100.99     spa_ipg_collect
  ```

- Adding the IP and a hostname to the DNCS / etc/hosts file is required. It should not cause any problems. You are simply associating the IP address to a hostname. The hostname should reflect the IPG description (such as spa_ipg_collect), or source.

  Example: `198.51.100.99  spa_ipg_collect`

- If all IPG Collectors use the same IP address/hostname, only one entry is necessary in the /etc/hosts files.

Important: This file is tab-separated. Use the tab key between the IP address and the hostname.

7 If you are converting ASI BFS directly to an RFGW-1, go to *ASI BFS to RFGW-1 GigE BFS Conversion Configuration Guide* (part number OL-31477). See the section **Correlation to the Installation and Migration Guide for SR 6.0**.

Gather Information for BFS ASI to GigE Conversion

Complete this procedure only if your system is still using ASI for BFS. If your system is using GigE BFS (multicast or unicast), skip this procedure.

SR 6.0 does not support ASI BFS. When migrating from a SPARC platform to the UCS and SR 6.0, you must convert the existing ASI to GigE BFS during the post upgrade procedure, ***ASI to GigE BFS Conversion*** (see "***ASI to GigE BFS Conversion***" on page 126). In this section, you will gather the information required to complete this procedure.

Note: Systems that have enabled the Distributed DNCS may have multiple Site IDs, depending upon the number of RNCS/LIONN systems deployed. You must gather the following information for each site that will convert from ASI to GigE BFS.

Gather the following information and write it down next to the appropriate field.

- Site ID:

  Notes:

  - For systems running SR 4.2, SR 4.3, or SR 5.0 without an RNCS, the Site ID can be obtained from the database table *site_info*. The following commands should be executed to obtain the Site ID:

    1. `dbaccess dncsdb –`
    2. `select * from site_info;`
    3. Press the **Ctrl** and **c** keys simultaneously to exit.

  - For systems running SR 5.1 and older releases that include an RNCS, the Site ID can be obtained from the RNCS Site WUI.

- GQAM ID where the GigE BFS is to be built:

  Note: The GQAM ID is obtained from the database table *pdcaqam*. The following commands should be executed to obtain the GQAM ID:

  1. `dbaccess dncsdb -`
  2. `select qam_name, qam_id from pdcaqam where qam_name="[QAM Name]";`

     Note: The [QAM Name] is the name of the GQAM where GigE BFS sessions will be built. If the QAM name includes alpha characters, it must be enclosed in quotes. Do NOT include brackets when entering the command.
  3. Press the **Ctrl** and **c** keys simultaneously to exit.

- GQAM output TSID:
- GQAM input port:
- Multicast or Unicast BFS

- If Multicast, the base Multicast IP address (23x.a.b.c):
- If Unicast, the base Unicast port (1025 - 65535):

Important: If you are migrating ASI BFS directly to RFGW-1, go to *ASI BFS to RFGW-1 GigE BFS Conversion Configuration Guide* (part number OL-31477). See the section **Correlation to the Installation and Migration Guide for SR 6.0**.

Upgrades From SR 5.0 or SR 5.1 to SR 6.0

If you are upgrading from SR 5.0 or SR 5.1, and have not already moved ASI BFS to a GQAM, follow these instructions to enable the GQAM for BFS.

1. Open the QAM WUI.
2. Open the GQAM upon which you will build the GigE BFS.
3. Click **BFS Capability**.
4. Save the configuration.

3

Hardware Configuration Procedures for the Cisco UCS C240 Server

Introduction

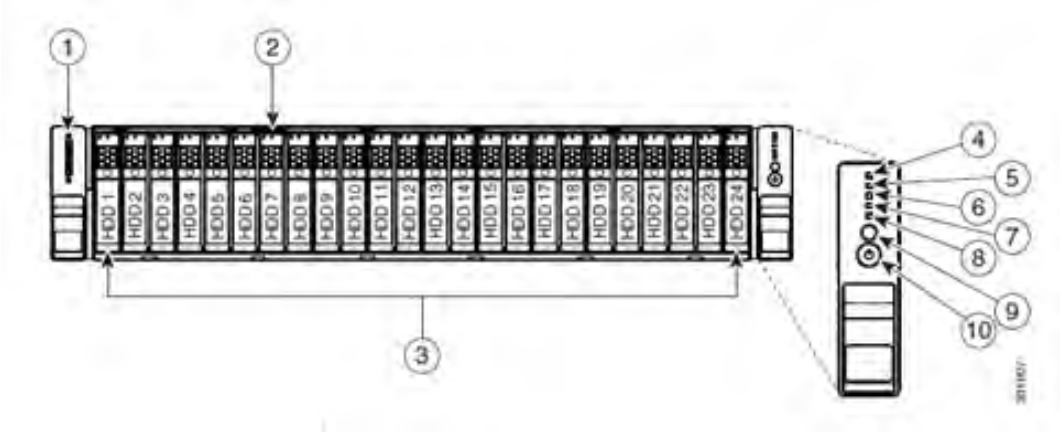
This chapter contains procedures for configuring Cisco's UCS C240 server for use with System Release 6.0.

Important: You can skip this chapter if you are performing a VM to VM migration.

In This Chapter

Hardware Diagram of the Cisco UCS C240 Server

Chassis Front View

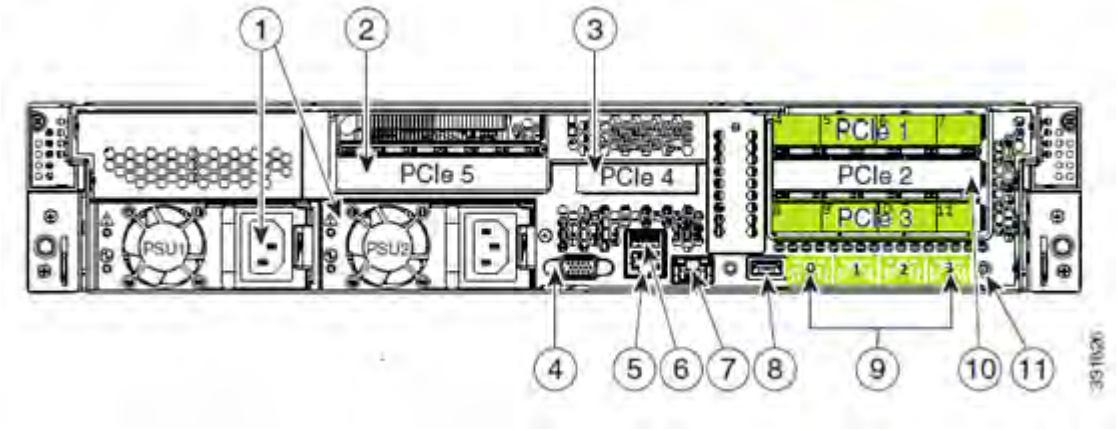


Slot	Description	Slot	Description
1	KVM connector (Used with KVM cable that provides two USB, one VGA, and one serial connector)	6	Temperature status LED
2	Asset tag (serial number)	7	Fan status LED
3	Drives (up to 24 2.5-inch hot-swappable drives)	8	System status LED
4	Network link activity LED	9	Identification button/LED
5	Power supply status LED	10	Power button/power status LED

Chassis Rear View

Important: Be certain that the network cards are installed in the slots shown in this diagram.

Note: Only the essential features of the rear panel are shown. A more detailed image follows.



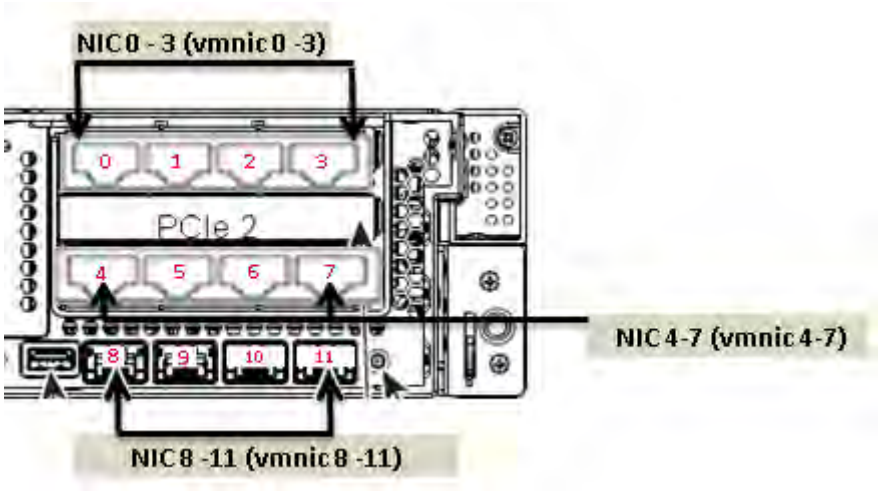
Slot	Description	Slot	Description
1	Power supplies (up to two)	7	One RJ-45 10/100/1000 Ethernet dedicated management port
2	Standard-profile PCIe slot on riser 2: PCIe 5 - full height, 3/4-length, x16 lane width, x24 connector, GPU ready	8	USB 2.0 port
3	Low-profile PCIe slot on riser: PCIe 4 - half-height, 3/4-length, x8 lane width, x16 connector, no NCSI support	9	Quad 1-GB Ethernet ports (LAN1, LAN2, LAN3, LAN4)
4	VGA video connector	10	Standard-profile PCIe slots on riser 1 (three): ■ PCIe 1-full-height, half-length, x8 lane width, x8 connector ■ PCIe 2-full-height, half-length, x16 lane width, x24 connector (supports Cisco Virtual Interface Card (VIC) ■ PCIe 3-full-height, half-length, x8 lane width, x16 connector
5	Serial connector (RJ-45)	11	Rear identification button/LED

6	USB 2.0 port

Detailed View of PCI Ports

C240M3 Installation Using ESXi5.5 and Later

This figure shows the mapping of the physical NIC to the VM NIC (vmnic).



Note: Use the data in this chart to help you configure the network host system settings.

Network Type	VMNIC Instance
ESXi Management	vmnic-3, vmnic-9
Headend Network	vmnic-4, vmnic-0
Corporate Network	vmnic-5, vmnic-1
RepDB Network	vmnic-6, vmnic-2
Headend2 Network (DSG)	vmnic-7, vmnic-10
TED Crossover	vmnic-8

Tested Reference Configuration with ESIX-5.5

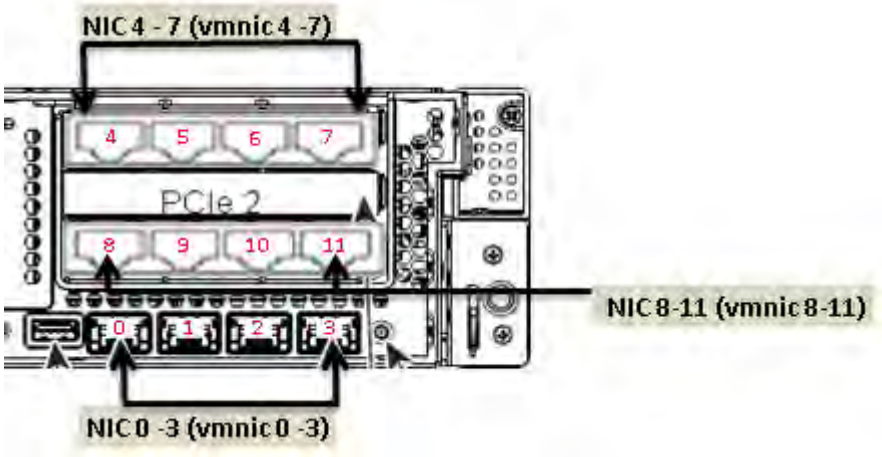
This reference configuration was tested with ESIX-5.5 Patch Release 201407001 (build 1892795).

- NIC Ports 3 and 9 — ESXi Management
- NIC Ports 4 and 0 — Headend network
- NIC Ports 5 and 1 — Corporate network
- NIC Ports 6 and 2 — RepDB network
- NIC Ports 7 and 10 — Headend 2 network (DSG)

- NIC Port 8 — TED crossover
- NIC Port 11 — Open

C240M3 Installation Using Previous Versions of ESXi

This figure shows the mapping of the physical NIC to the VM NIC (vmnic).



Note: Use the data in this chart to help you configure the network host system settings.

Network Type	VMNIC Instance
ESXi Management	vmnic-1, vmnic-7
Headend Network	vmnic-8, vmnic-4
Corporate Network	vmnic-9, vmnic-5
RepDB Network	vmnic-10, vmnic-6
Headend2 Network (DSG)	vmnic-2, vmnic-11
TED Crossover	vmnic-0

Tested Reference Configuration with Prior ESXi Releases

Network ports are numbered and marked as green. Cables should be run to the following designated ports.

- NIC Ports 1 and 7 — ESXi Management
- NIC Ports 8 and 4 — Headend network
- NIC Ports 9 and 5 — Corporate network
- NIC Ports 10 and 6 — RepDB network
- NIC Ports 2 and 11 — Headend 2 network (DSG)
- NIC Port 0 — TED crossover

- NIC Port 3 — Open

  Important: The DOCSIS Set-Top Gateway (DSG) network is only used if you have the licensed feature. Otherwise, these ports are unused at this time.

Cisco UCS C240 Server CIMC Configuration

Important:

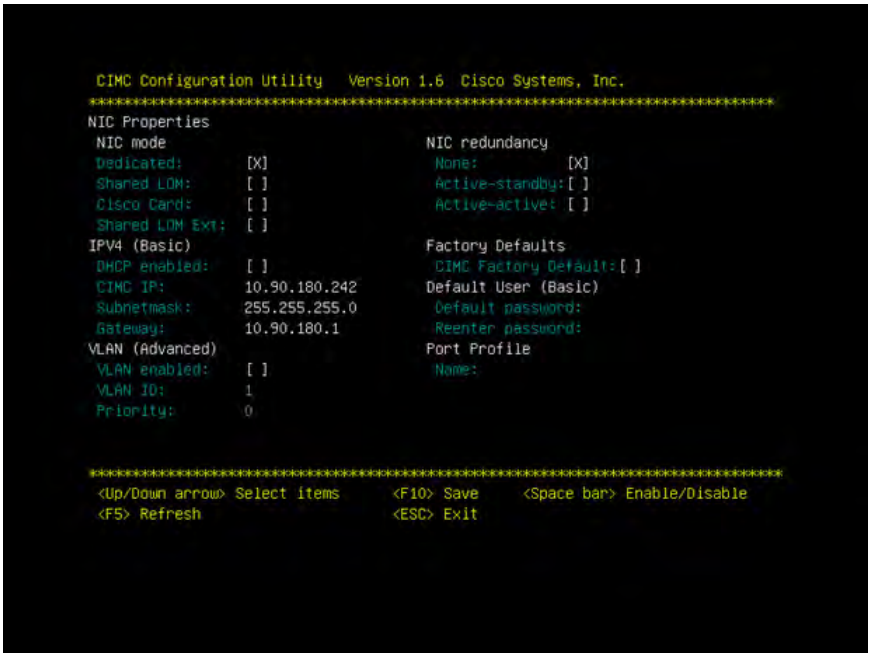
- This procedure only needs to be performed once — when you initially install the UCS C240 server.
- Be sure that you use configuration data that pertains to the system that you are migrating. The screen-capture at Step 5 is to be referenced as an example, only.

1. Obtain the UCS C240 Quick Start Guide. This guide is shipped with the server.
2. Follow the instructions in the UCS C240 Quick Start Guide through Step 5.
3. Press the **Power** button to power on the UCS C240 server.
4. Press **F8** at the Cisco splash screen. The server boots to the CIMC Configuration Utility window.

   Important: Note the BIOS Version on the Cisco splash screen as the system is booting.
5. Use the information in the CIMC Configuration Utility window to complete the configuration.

   Note: In addition to the information in the CIMC Configuration Utility window, be sure to obtain the network IP address for the CIMC interface.

   Important: The following image is an example only. Do not use the IP address, netmask, or gateway in the image.



6. Enter a default password and then re-enter it at the prompt. Store this password in a safe place for future use.
7. Press **F10** to save changes.

8 Press **Esc** to exit. The EFI shell prompt may appear.

Cisco UCS C240 Host Configuration

Important:

- This procedure only needs to be performed once — when you initially install the UCS C240 server.
- The CIMC firmware and BIOS version (noted in Step 4 of ***Cisco UCS C240 Server CIMC Configuration*** (on page 49)) should be at or higher than the minimum required version found in the **Tested Reference Configuration** chart in the Preface. If it is not, contact Cisco Support for assistance in upgrading the firmware and the BIOS.

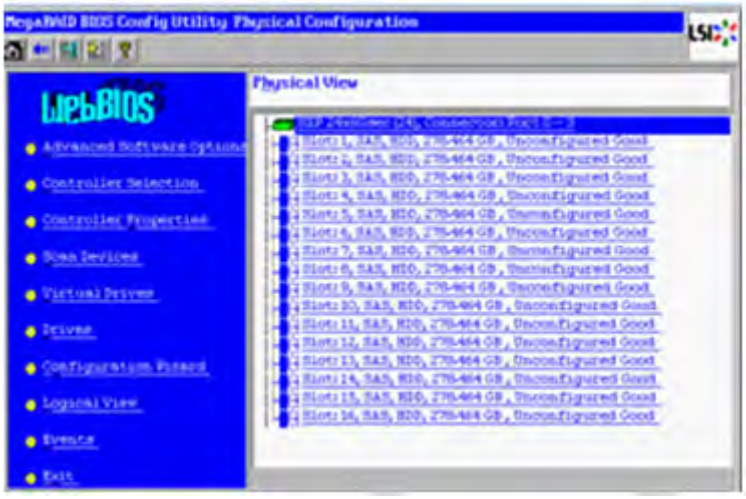
RAID Configuration

Important: This procedure only needs to be performed once — when you initially install the UCS C240 server.

The UCS hardware RAID configuration for this system release consists of a RAID 10 (14x300GB disks) for the OS disk, and two global hotspares (2X300 GB disks). This section details the steps necessary to create these volumes and hot spares.

1. Press **Ctrl-Alt-Del** to reboot the server.
2. Watch the reboot process closely. After the disks are displayed, observe the boot messages and press **Ctrl-H** when prompted to access the WebBIOS (RAID Configuration Utility). After a few minutes, a **Start** button appears.

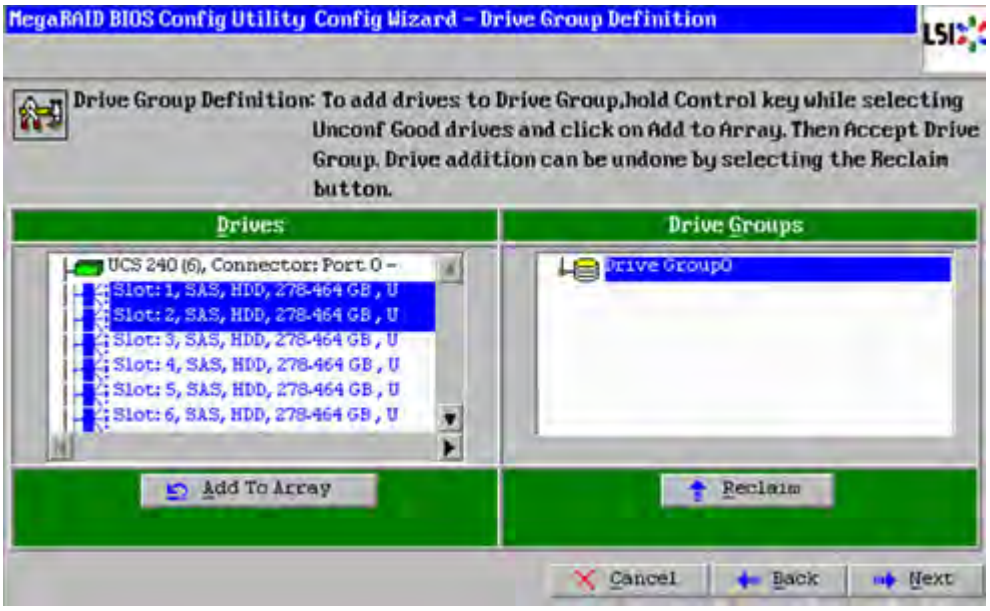
3. Click **Start** to configure RAID. The MegaRAID BIOS Config Utility main menu appears.



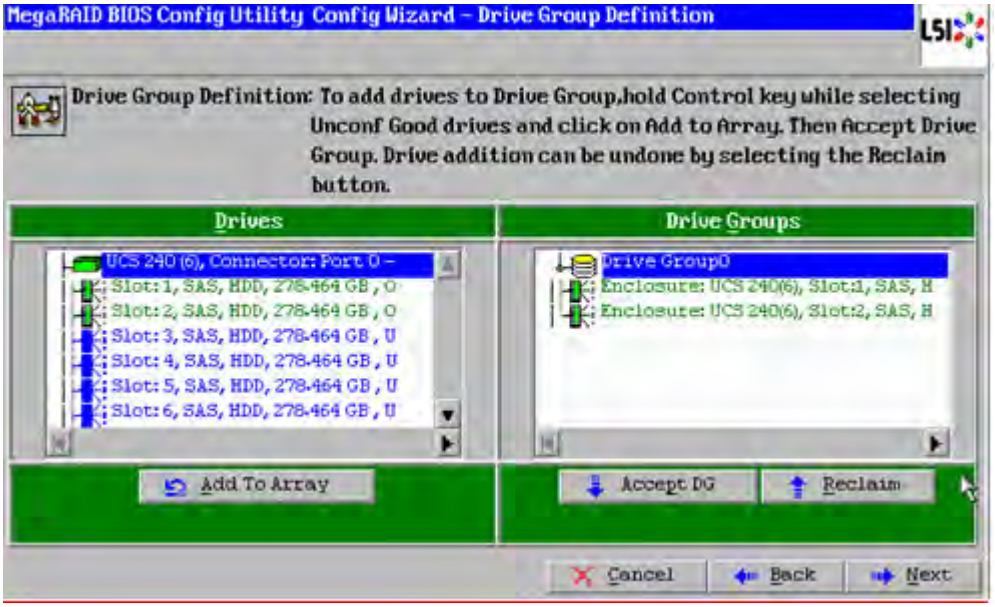
4. Click the **Configuration Wizard** link in the left pane of the utility menu.
5. Click **New Configuration** and then click **Next**. The utility prompts you to clear the existing configuration.
6. Click **Yes**.
7. Click **Manual Configuration** and then click **Next**. The Drive Group Definition screen appears.

   Note: Within the drives panel, there is a listing of all 16 hard drives. Create 7 drive groups (0-6), each consisting of 2 disks (1 and 2, 3 and 4, and so on). Drives 13 and 14 will be your final drive group.

8 Select the **Slot 1** disk, and while pressing the **Ctrl** key, click the **Slot 2** disk to highlight both disks.



9 Click **Add to Array** to form **Drive Group (0)**.



10 Click **Accept DG**.

11 Repeat Steps 9 through 11 for the following drive pairs:

Slots 3 and 4

Slots 5 and 6

Slots 7 and 8

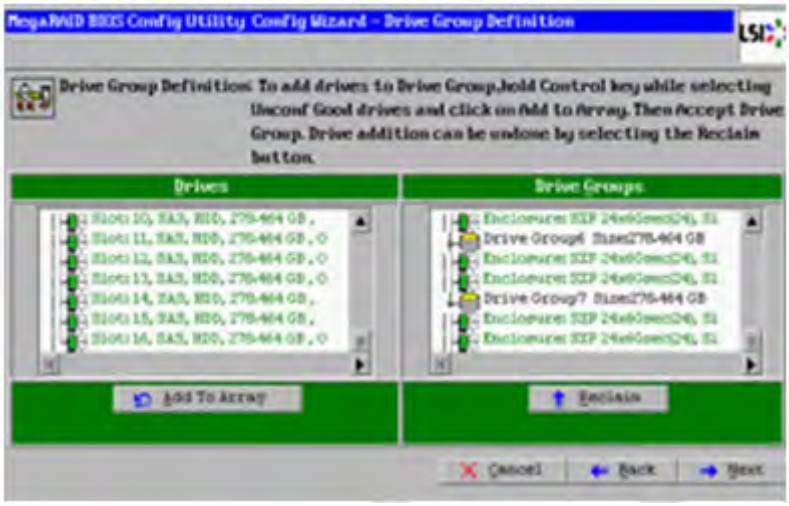
Slots 9 and 10

Slots 11 and 12

Slots 13 and 14

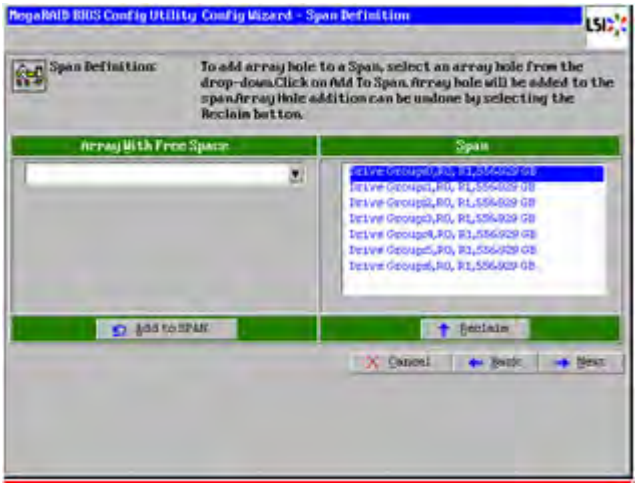
Result: The system creates a drive group for each pair.

Note: When you complete this step, you should have 7 drive groups (0 - 6).

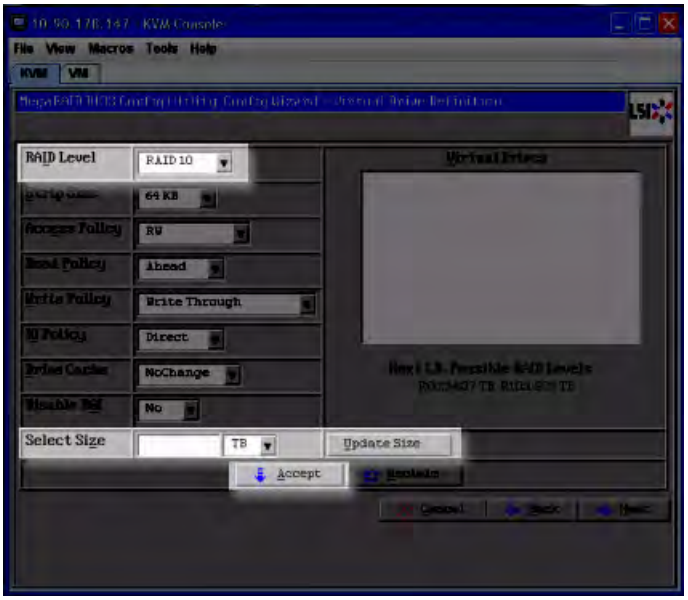


12 Click **Next** and then select **Drive Group 0**.

13 Select each drive group, one by one, and then click **Add to SPAN** to add all drive groups to the span list.

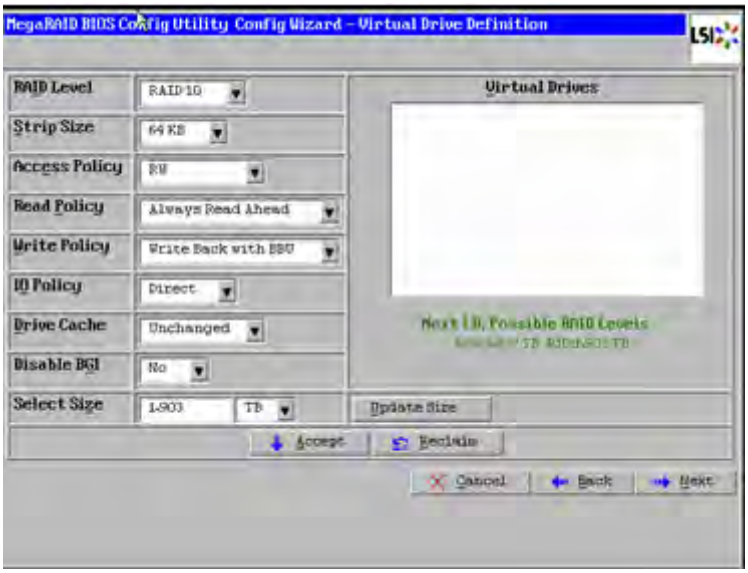


14 Click **Next**. The Virtual Drive Definition window appears.



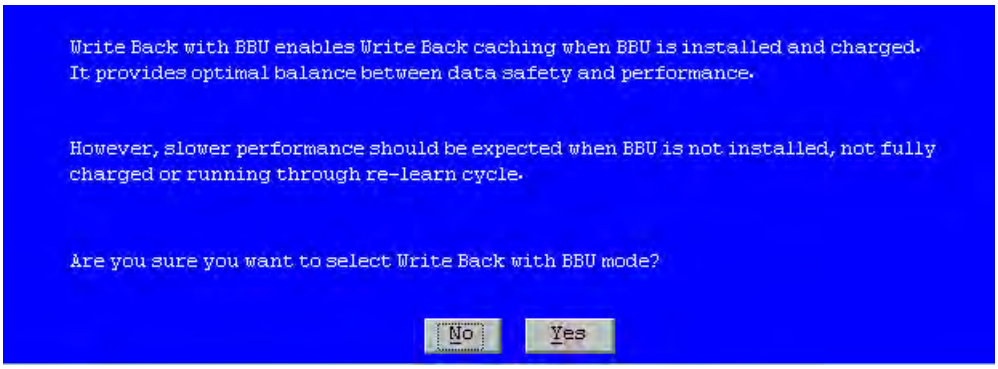
15 Select **RAID 10** from the RAID Level drop-down menu.

16 Click **Update Size**. The maximum allowed size for the selected RAID level populates the **Select Size** field.

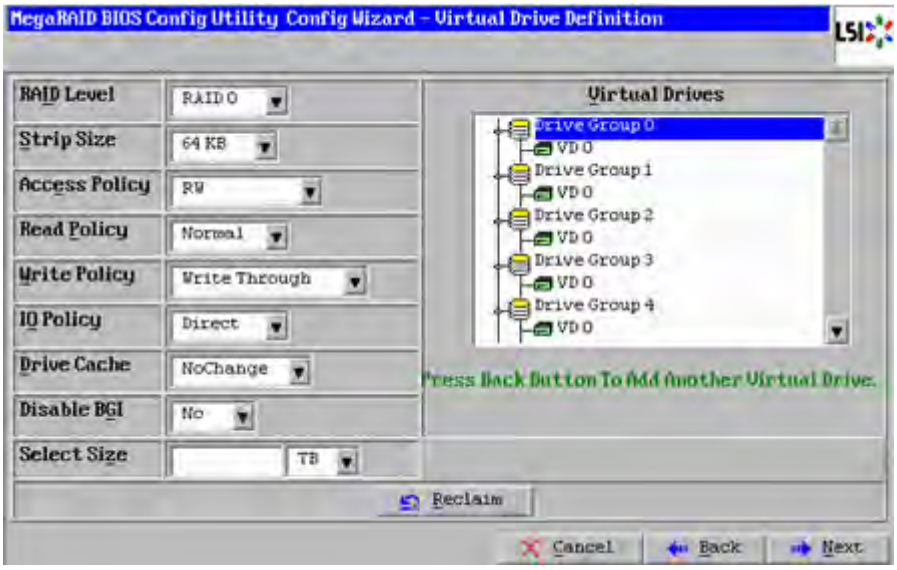


17 Record the **Select Size** here: _____

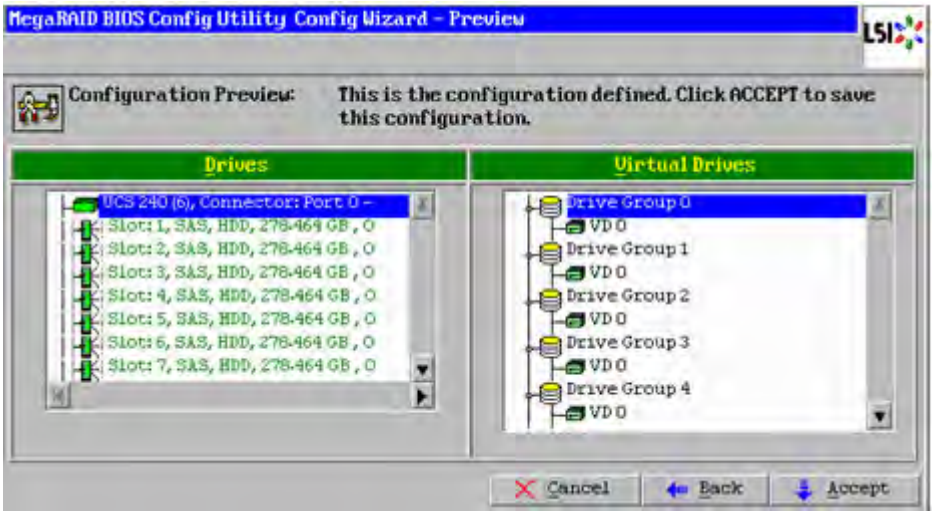
18 Click **Accept**. The Write Policy window appears.



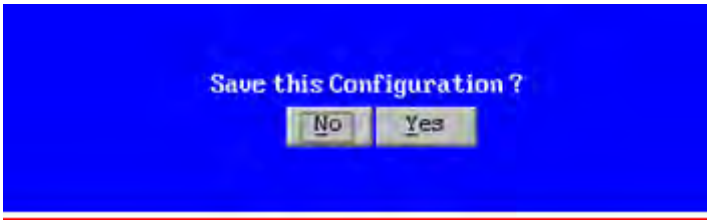
19 Click **Yes** to confirm the default write policy. The total list of Vdisks created from Drive Groups 0-6 appears.



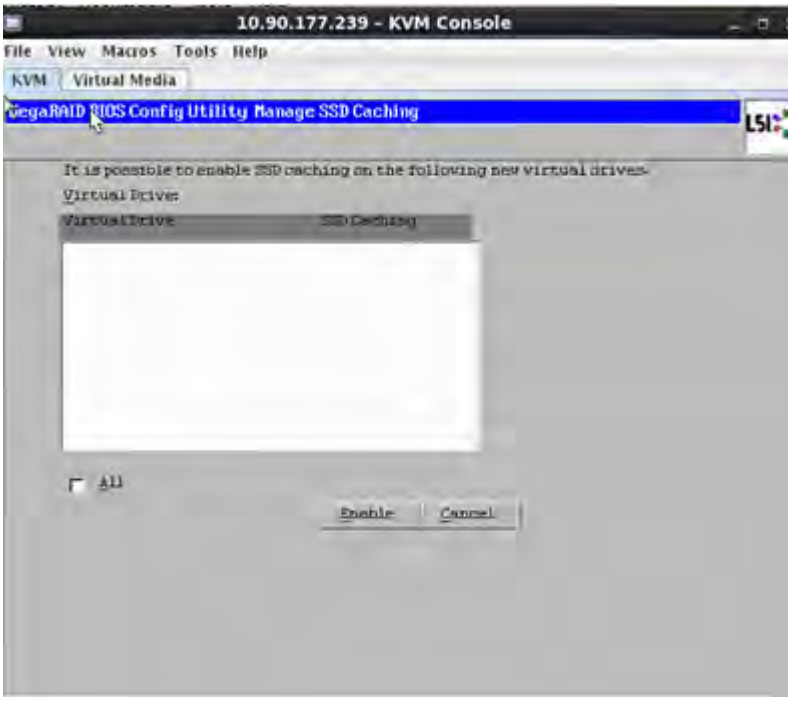
20 Click **Next**.



21 Examine the configuration preview to verify that the virtual drives match the previous list and select **Accept**. The system prompts to confirm saving the configuration.

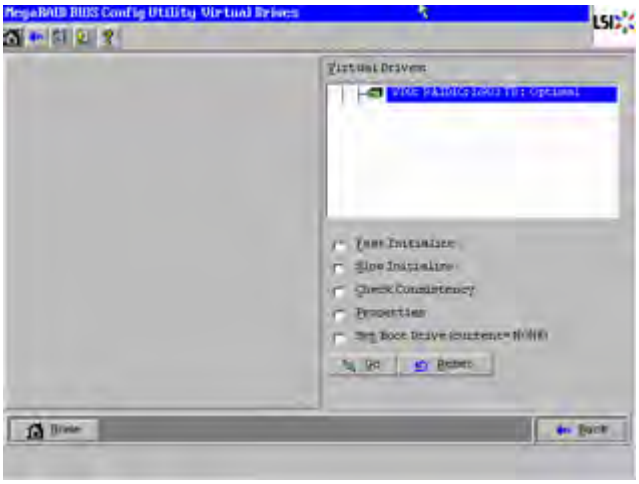


22 Click **Yes**. A warning message appears and indicates that you may lose data.



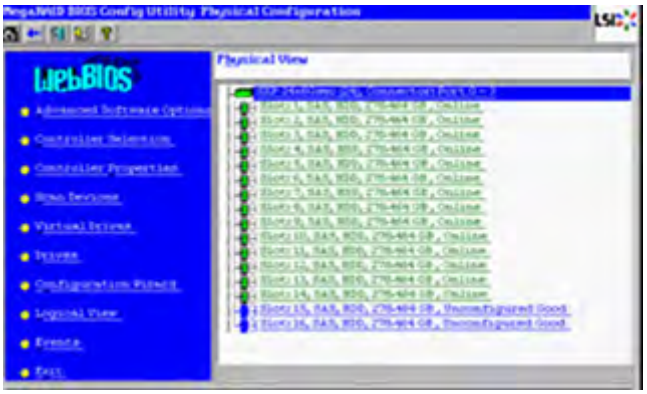
Note: After canceling the previous screen, you are prompted to initialize the new virtual drives.

23 Click **Yes** to initialize. The Virtual Drive VD0 is displayed.



24 Click **Home**. The Raid Configuration utility main menu appears.

25 Click the **Physical View** from the left pane if it is not currently displayed.

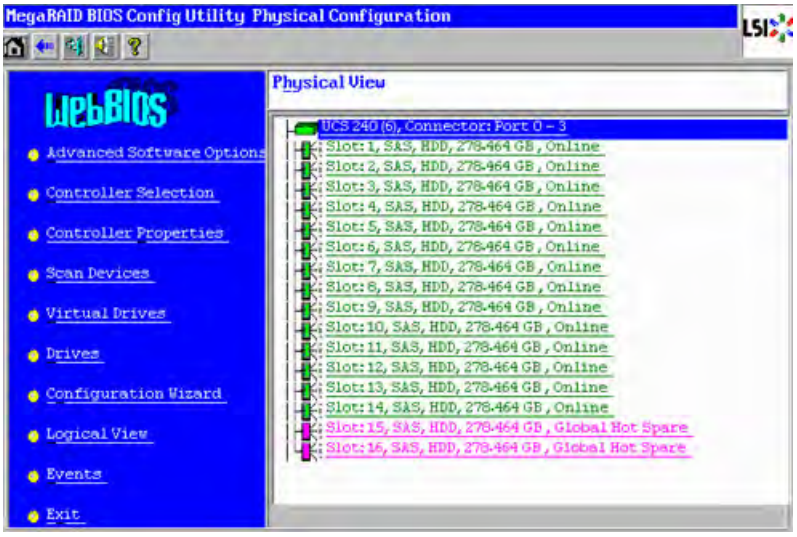


26 Click the drive on Slot 15 in the Physical View.

27 Click the option **Make Global HSP** and then click **Go** to save.

28 Click **Back** and then repeat Steps 26 and 27 for the drive in Slot 16.

29 Click **Home** and select the **Physical View** (if it is not displayed by default).



30 Verify that the drives in Slot 15 and 16 are visible as Global Hotspares.

31 From the Main Menu, click **Exit** to exit the RAID Configuration Utility.

32 Click **Yes** to confirm exiting the utility.

Important: At this point, you may be prompted to reboot the computer. Do NOT reboot. It is very important that you do not reboot the computer at this time.

ESXi Installation

Important: This procedure only needs to be performed once — when you initially install the UCS C240 server.

Before You Begin

Note: The Firefox browser is not officially supported for accessing the UCS C240 M3 CIMC application.

1. Use a web browser to open the CIMC application, using the IP address configured in ***Cisco UCS C240 Server CIMC Configuration*** (on page 49).
2. Log on to the server using the admin password or the password that you set in *Cisco UCS C240 Server CIMC Configuration*.

Power Policy

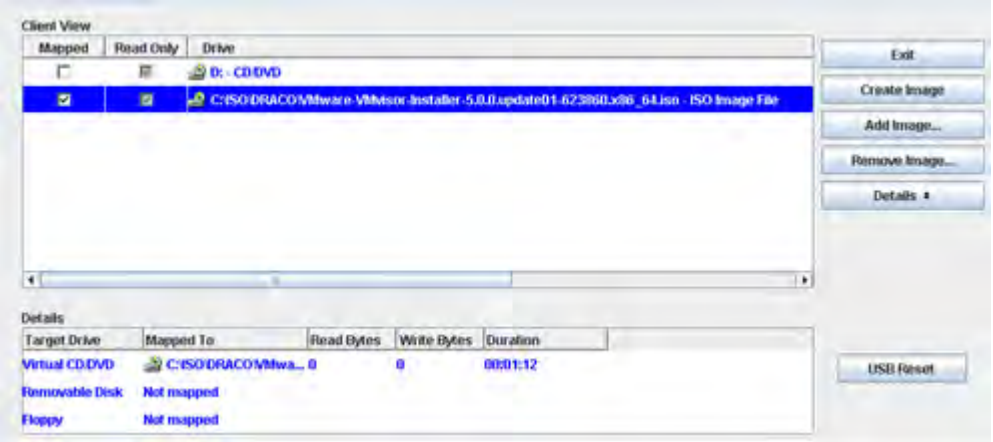
1. Click **Power Policies**.
2. Choose **Restore Last State** from the menu.
3. Click **Save Changes**.
4. Click **Summary** on the Server tab in the CIMC.
5. Click **Launch KVM Console** from the Server Summary window.
6. Select open using java viewer in the dialog box. The KVM Console is displayed.

Installing ESXi

Important: Before beginning this procedure, be sure that you have downloaded or copied the VMware ISO image to the local hard drive that is running the CIMC application.

1. Follow these instructions to mount the ESXi ISO image.
   a. Click the **Virtual Media** tab in the KVM Console.
   b. Click **Add Image**.
   c. Browse to the location of the VMware ISO image and select **Open**.

d Click the **Mapped** box next to the added image.



e Click the **KVM** tab in the KVM Console.

2 Select **Macros** and then the **Ctrl-Alt-Del** option from the KVM menu bar to reboot the server.

Note: Later versions of firmware may refer to **Static Macros**.

3 Press **F2** when the Cisco splash screen is displayed to enter the system setup.

4 Navigate to the **Boot Options** tab.

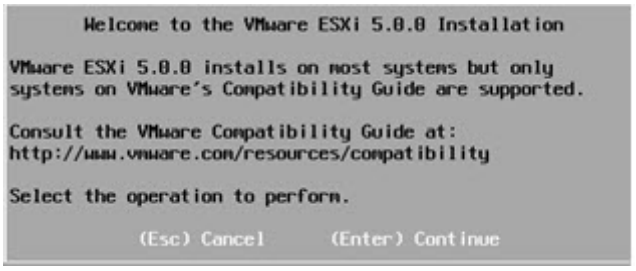
5 Make the following selections:

- Boot Option 1 — RAID Adapter
- Boot Option 2 — Virtual CD/DVD
- Disable remaining boot options

6 Press **F10** to save the settings and reset system.

7 Click **Yes** to save the settings and reset the system.

8 Wait for the ESXi installer to load. After the ESXi load completes, a **Welcome** message appears.



9 When prompted, press **Enter** to continue.

10 When prompted, press **F11** to accept the license agreement.

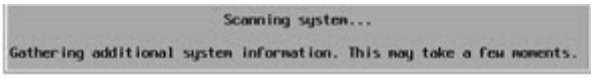
Note: This action selects the disk. Select the disk that matches the size of the Virtual Disk that was recorded in ***RAID Configuration*** (on page 52), Step 17.

11 Press **Enter** to continue.

12 Select the appropriate keyboard layout (for example, **US default**) and press **Enter**.

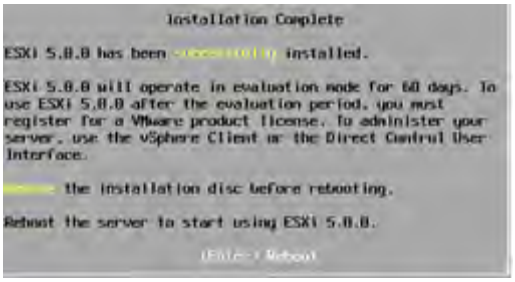
13 Enter and confirm a new **root** password for the ESXi host.

14 Press **Enter** to continue.



15 Press **F11** to confirm the installation on the selected disk. The ESXi installation begins and a progress bar appears.

16 When the installation completion screen is displayed, press **Enter** to reboot. The ISO is un-mapped and the system boots to the VMware ESXi window.



Important: Let the system boot all of the way into ESXi. If you press F2 too early (during boot-up), the BIOS configuration screen appears, which is not what you want at this point.

17 Press **F2** to customize the system.

18 Log in as **root** user. The System Customization window appears.

19 Navigate to **Configure Management Network** and press **Enter**.

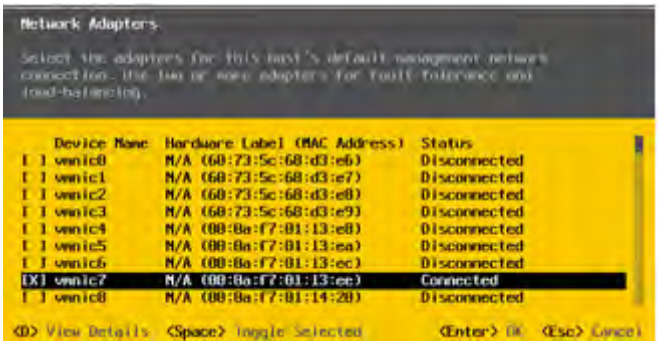
20 Select **Network Adapters** and press **Enter**.

21 To select a vmnic, highlight the line you want and press the **Spacebar**.

- For the UCS 240 server, enable nic 1 and 7; disable the others.

  Note: These nics are for ESXi access.

22 Verify that the devices you enabled in Step 21 show a **Connected** status.



23 Press **Enter**. The system returns to the Configure Management Network window.

24 Select **IP Configuration** and press **Enter** to set/modify the IP address.

25 Use the arrow keys to highlight **Set static IP address** and press the **Spacebar**.

26 Provide the following information to configure the ESXi server:

- IP Address
- Subnet Mask
- Gateway

27 Press **Enter** to accept the changes.

28 Use the arrow keys to highlight **DNS configuration** and then press **Enter**.

29 Provide the following information.

- **Primary DNS IP address**
- **Secondary DNS IP address** (optional)
- **Hostname**

30 Press **Enter** to accept and return.

31 Press **Esc** to exit and press **Y** to accept the changes when prompted.

32 Select **Test Management Network** and then press **Enter** to navigate to the Test Management Network dialog.

33 Press **Enter** to begin a ping test.

34 After the ping test is complete, press **Enter** to exit the test dialog.

35 See the site Network Administrator to verify addressing and cabling.

36 Scroll to **Troubleshooting Options** and then press **Enter**.

37 Select **Enable SSH** and press **Enter**. The right-hand panel mode should indicate **SSH is Enabled**.

38 Press **Esc** to exit.

39 Press **Esc** to log out and disconnect the KVM.

40 Click **File/Exit** to close the KVM console.

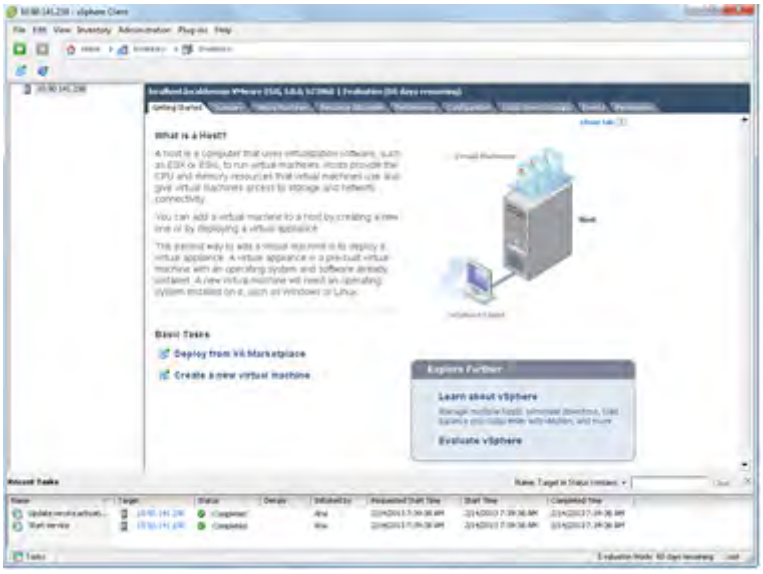
Use VMware vSphere to Configure the Host System

Important: This procedure only needs to be performed once — when you initially install the UCS C240 server.

You must have a Windows, Linux, or Mac OS system with vSphere installed to complete the installation and migration of SR 6.0.

1. Provide the IP address, username, and password for the new ESXi host to the vCenter administrator. Once the administrator licenses the new host, you will be able to access it through vCenter.
2. Use the VMware vSphere Client to connect the vCenter server. Provide the IP Address, username, and password for authentication.
3. If you are using vCenter and the Home view is displayed, click on **Hosts and Clusters**, and then highlight the new ESXi host in the left pane to begin configuring resources.

   Result: vSphere should go to the Inventory display. If not, click **Inventory** to display the ESXi Host.



4. Click the **Configuration** tab.
5. From the **Software** menu, choose **Time Configuration** to modify the date and time.
6. Click **Properties** and enter the correct date and time.
7. Click **NTP Client Enabled**.
8. Click **Options** and click **Start and Stop with host**.
9. Click **NTP Settings** and then click **Add**.
10. Enter the **NTP Server Address** and click **OK**.

11 Select **Restart NTP Service** to apply changes and click **OK**.

12 Verify that **NTP Client Enabled** is enabled and click **OK**.

13 From the **Hardware** menu, select **Networking**. Switch vSwitch 0 is displayed.

14 Select **Properties** for vSwitch 0.

15 Select **VM Network** and click **Remove**. You are prompted to confirm this request.

16 Click **Yes**.

17 Click the **Network Adapters** tab and click **Add**.

18 Refer to the appropriate location to configure the proper management network adapter for your system:

- ***C240M3 Installation Using ESXi5.5 and Later*** (on page 46)
- ***C240M3 Installation Using Previous Versions of ESXi*** (on page 47)

19 Click **Next** after selecting the proper network adapter.

20 Verify the adapter selection and click **Next**.

21 Click **Finish** to close the wizard.

22 Click **Close** to return to the **Configuration** tab.

23 Click **Add Networking**.

24 Select **Virtual Machine** and then click **Next**.

25 Refer to the charts referenced in step 18 to configure the proper Headend network adapters for your system.

26 Click **Next**.

27 Label the network as **Headend Network**.

Note: The vSwitch labels used in this document are suggested labels, only. You may name this and the remaining vSwitches to reflect your system configuration.

28 Click **Next** and click **Finish**.

29 Repeat these procedures to configure the following networks shown in the network design that was created for the customer.

Note: The vSwitch labels used in this document are suggested labels, only. You may name this and the remaining vSwitches to reflect your system configuration.

The following examples are for reference, only.

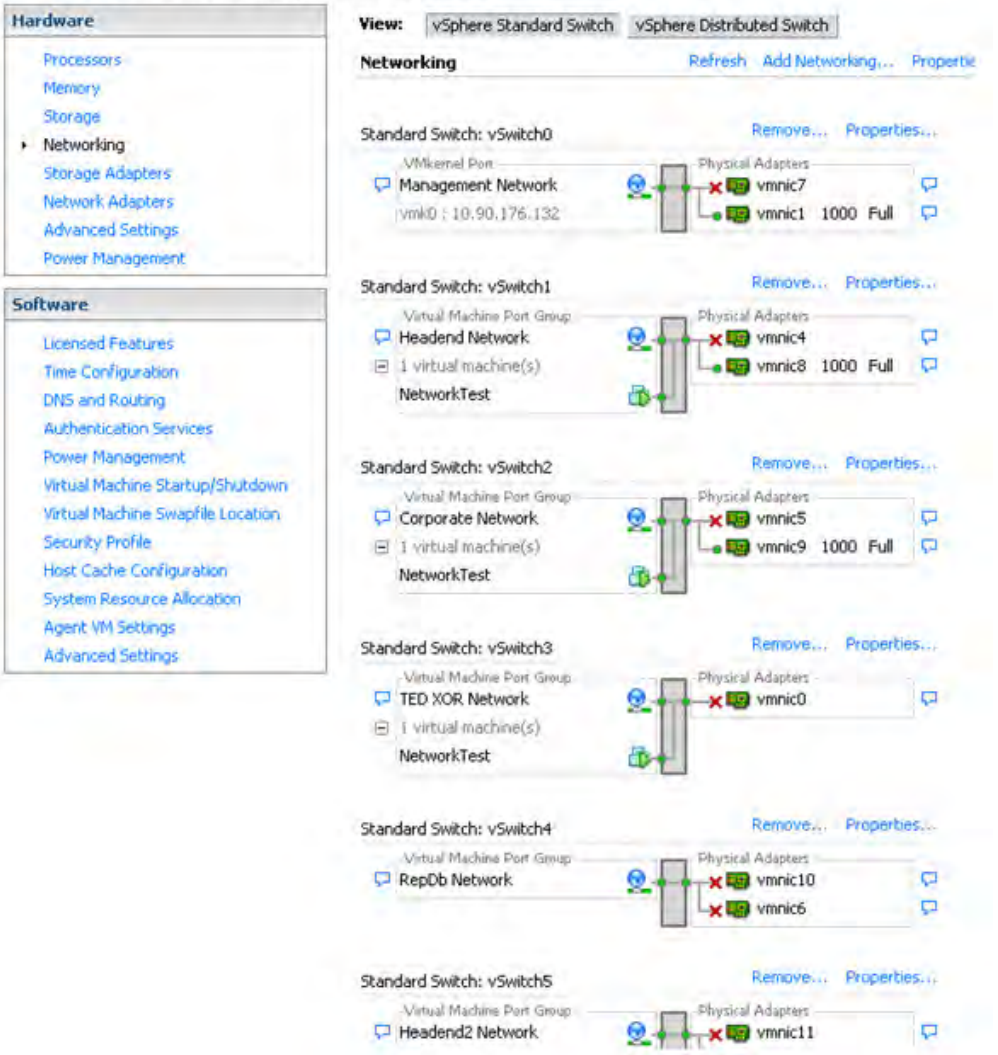
- **Corporate Network —** For corporate and back office access. This is created under **vSwitch 2.**
- **TED XOR Network —** For direct crossover connectivity with the TED. This is created under **vSwitch3.**
- **RepDB Network —** For direct connectivity to the RepDB interface when RepDB is an enabled feature. This is created under **vSwitch4**.

  Note: This network is optional and should be configured only if you are using RepDB.

- **Headend 2 Network** — This vSwitch may be used for DSG or other network requirements. This is created under **vSwitch5**.

  Note: This network is optional and should be configured only if needed.

Example Networking Configuration



30 To configure the **Storage Configuration**, click **Storage** from the **Hardware** menu.

31 Highlight **datastore1** and select **Properties**.

32 Click **Rename** and rename to **<hostname>_local_storage1**. Click **OK**.

Note: Cisco engineers have seen some issues when the datastore name contains blank spaces. Do not include spaces when you rename the datastore.

33 Verify the changes and click **Close**.

34 If necessary, create an NFS mapping to the location of the Solaris image.

Note: The server and path are site-specific. The customer should have the Solaris 10 (x86) ISO file on an NFS server accessible by the Virtual Machine (VM).

a Click **Add Storage**.

b Select **Network File System** and click **Next**.

c Input the server name or IP address, folder, select **Read Only**, and input a datastore name.

d Click **Next**.

e Verify the settings and click **Finish**.

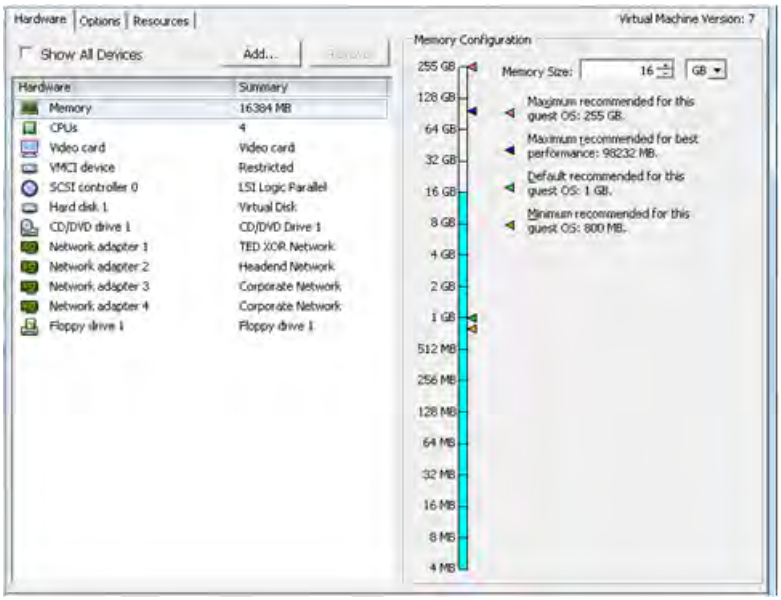
OVA Deployment

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.

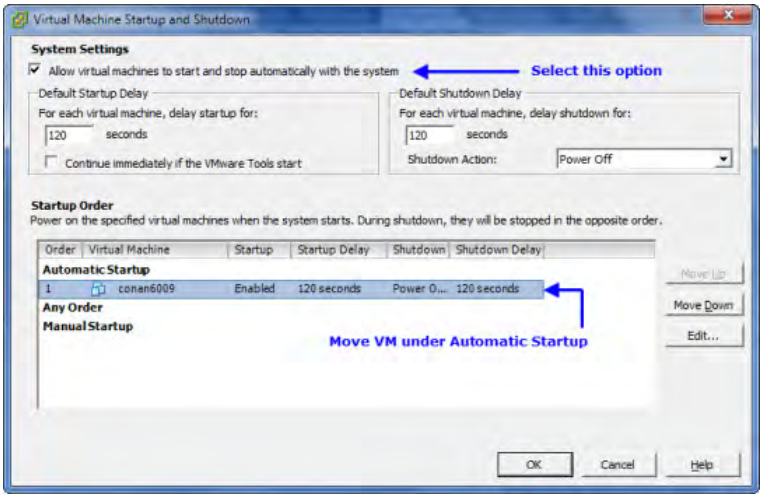
20 Click **OK**.

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

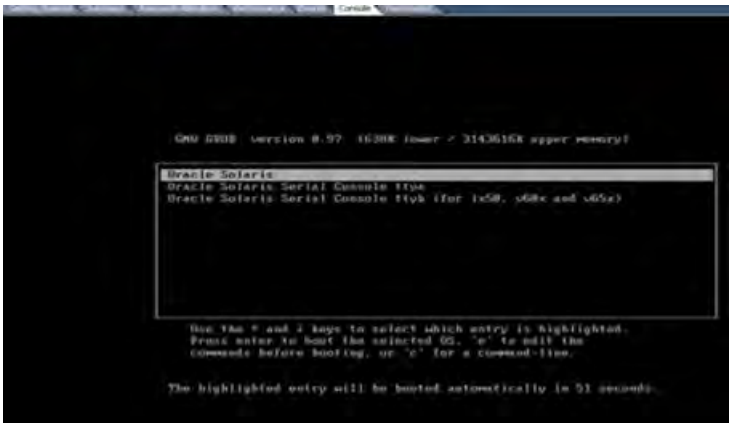
1. Click the ESXi Host.
2. In the **Configuration tab** choose **Virtual Machine Startup/Shutdown** from the **Software** menu.
3. Click **Properties** (located at the top right of the Startup Order window).
4. Check the **Allow virtual machines to start and stop automatically with the system** checkbox.
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`

4

SR 6.0 Application Installation and Migration

Introduction

This chapter includes the procedures to install or migrate a system to SR 6.0 using the SR 6.0.0.x ISO file.

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

Important: In SR 6.0, the DNCS is no longer recognized. Instead, the system is referred to as the Explorer Controller (EC). The RNCS is referred to as the RNCS EC.

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 a SPARC system.

To install the SR 6.0 application, refer to the procedures in one of the following sections.

- See Initial Installation of SR 6.0 for new installs
- See ***Installation and Migration to SR 6.0*** (on page 80) for installs with data migration

Initial Installation of SR 6.0

Important: This procedure is for performing an *INITIAL INSTALLATION* of SR 6.0 on the UCS platform. You must have completed all of the procedures in chapter 3 before continuing.

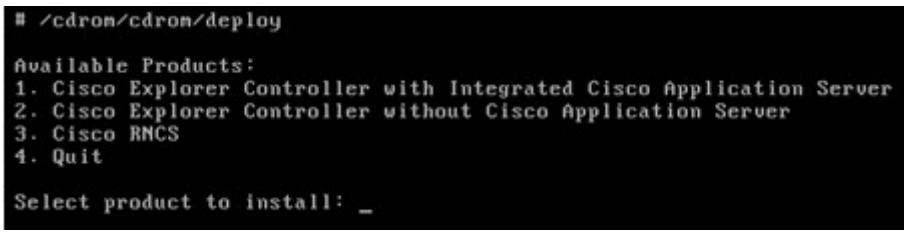
1. Press **Ctrl** and **Alt** to regain control of the mouse.
2. Mount the SRDVD 6.0 ISO image using the procedure in ***Mounting and Unmounting Using VMware*** (on page 186).
3. Refocus (click) in the Console window and log in as **root** with default password, 2g3n3r!c.
4. Type the following command and press **Enter** to verify that the ISO is mounted as /cdrom/cdrom.

   ```
   df -k
   ```

   Note: If the ISO does not mount, type the following command and press **Enter**. Then, repeat Step 4.

   ```
   svcadm refresh volfs
   ```
5. Type the following command and press **Enter** to begin the application installation. The Available Products menu appears.

```
/cdrom/cdrom/deploy
```



6 Enter the number that corresponds to the product you want to install.

7 Select **Install**. The default IP configuration appears.

8 Confirm or update the default IP configuration, as needed.

Note: Obtain IP addresses from your Network Administrator.

9 When you have confirmed the IP configuration, type `c` and press **Enter** to begin the software installation.

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`

10 Once the installation is complete, type the following command and press **Enter** to reboot.

```
shutdown –y –g0 –i6
```

11 Skip to ***Log into the New Explorer Controller*** (on page 93).

Configure Remote Access to the EC Web Interface

In this procedure you will configure the EC for web access. You should be familiar with the UNIX vi text editor or another text editor for this procedure. Follow these steps to configure the EC for web access.

1 If you have not created any user accounts, follow the ***Create User Accounts on the Upgraded Servers*** (on page 105) procedure to create a valid user account.

2 Open the /etc/hosts file with a text editor and make the following changes:

- **a** On the dncs entry (IP address of 192.168.1.1), delete the EC "hostname" and "dncsws" aliases.
- **b** Add the following entry to the end of the file:

  ```
  127.0.0.2      loopback2 dncsws
  ```

- **c** Add the "dncseth" alias to the line containing the hostname of the EC.
- **d** Save and close the file.

3 Type the following command and press **Enter** to create the /etc/hostname.lo0:1 interface:

```
cat loopback2 > /etc/hostname.lo0:1
```

4 Open the /etc/apache2/user-conf/httpd.ports file with a text editor.

5 Add the following entry to the bottom of the file:
```
Listen dncseth:80
```
6 Save and close the file.
7 Type the following command and press Enter to reboot the EC:
```
shutdown -y -g0 -i6
```
8 Open Firefox and enter the IP address/dncs in the URL field and press **Enter**. You will be prompted for login credentials.
9 Enter a valid user name and password. You are logged in to the EC WebUI.
10 Begin system provisioning.

Installation and Migration to SR 6.0

Important: If the Replicated Database is enabled on the system you are upgrading, heed the following statements:

- Refer to *Configuring and Operating the Replicated Database Package on the Explorer Controller* (part number OL-27794), to disable RepDB on both the primary and secondary systems.
- Record the name of the /etc/hostname. file for the RepDB interface. This interface will be moved to the /etc/hostname.e1000g3 file, post-migration.

In this procedure, you will migrate from an existing SPARC DBDS system to the UCS Draco platform. Follow these steps to deploy the SR 6.0 packages on the UCS platform.

1 Enable **root ssh** on the system that **will be migrated** 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 Verify that the network cable to the Corporate network is connected.
4 Refocus on the console window and log in as **root**, with default password, `2g3n3r!c` (if not already logged in as root).
5 Type the following command and press **Enter**. The Available Products menu appears.

```
/cdrom/cdrom/deploy
```

```
# /cdrom/cdrom/deploy

Available Products:
1. Cisco Explorer Controller with Integrated Cisco Application Server
2. Cisco Explorer Controller without Cisco Application Server
3. Cisco RNCS
4. Quit

Select product to install: _
```

6 Enter the appropriate number corresponding to the product you are installing.

7 Select **Install and Migrate Data**. The Migration Network Interface configuration appears.

8 At the **Do you want to change these values?** message, type **y** and then 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 DNCS or RNCS IP data.

```
This script will install the following packages on "sysinstall":

SAIrsync        rsync for SA/Cisco DVS products
                2.6.9-1_SunOS_i386

**********************************************************************
Installing SAIrsync package on sysinstall...

For more SAIrsync package installation messages refer to:
/var/sadm/system/logs/SAIrsync_2.6.9-1_SunOS_i386_install.log

**********************************************************************
Destination-Host (migrating TO)  IP Address Settings (e1000g3)
Destination-Host IP Address:                0.0.0.0
Destination-Host Netmask:                   0.0.0.0

**********************************************************************
Source-Host (migrating FROM):               NOTSET
Next hop to Source host:                    NOTSET
**********************************************************************
Do you want to change these values?(y/n): y
Destination-Host IP address?[0.0.0.0]: 10.90.177.41
Destination-Host Netmask?[0.0.0.0]: 255.255.254.0
Source-Host IP?[NOTSET]: 10.90.176.16_
```

9 Enter the VM temporary IP address of the VM.

10 Enter the VM netmask of the temporary interface of the VM.

11 Enter the IP address of the DNCS or RNCS from which you are going to migrate data.

12 If the DNCS and UCS are on separate subnets, enter the gateway to the DNCS or RNCS when prompted. A **Do you want to continue?** message appears.

13 Type **y** and press **Enter** to continue with the migration. Another **Are you sure you want to continue?** message appears.

14 Type **yes** and press **Enter** to continue. You are prompted for the SPARC root password.

15 Enter the **root** password of the remote host and press **Enter** to accept the RSA keys.

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

16 Do you have additional files or directories to add?

- If **yes**, type **y** and then press **Enter**. Then, add 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**.

17 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.

18 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`

19 Go to ***Maintenance Window Activities*** (on page 83) when the installation has completed.

5

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.

Delete a BIG and its PAT Sessions

This procedure describes how to delete a BIG that is configured on your system, and to delete any sessions associated with the BIG.

Important: If you have not converted from a BIG to ASI, skip this section. If you have converted from a BIG to ASI, perform the following procedure.

Deleting a BIG and BIG PAT Sessions

1. From the DNCS Administrative Console, click the **Network Element Provisioning** tab and then click **BIG**. The BIG List window appears.
2. Does a BIG exist in the BIG List window?
   - If **yes**, go to Step 3.
   - If **no**, skip the rest of this section and go to ***Stopping the System Components and Migrating the Database and Key Files*** (on page 86).
3. Double-click the **BIG**. The Set Up BIG window appears.
4. Is the Administrative State set to Offline?
   - If **yes**, go to Step 5.
   - If **no**, click **Offline** and then click **Apply**. Go to Step 5.
5. Click **PAT Configuration**. The BIG PAT window appears.

6 Are there any entries in the PAT Configuration table?

- If **yes**, continue with Step 7.
- If **no**, skip to Step 11.

7 Select the first entry in the BIG PAT window and click **Delete Entry**. A confirmation window appears.

8 Click **Yes** to confirm the deletion of this entry. An Information message appears and informs you that all BFS sessions must be torn down and rebuilt for the deletion to take effect.

Notes:

- The Information message only appears for the first entry you delete.
- Although you must respond to this question, you do not need to tear down and rebuild these sessions because you will delete the BIG later in this procedure.

9 Click **OK**.

10 Repeat Steps 6-9 until you have deleted every entry in the BIG PAT window and then go to Step 11.

11 From the BIG PAT window, click **Close**.

12 From the Set Up BIG window, click **Apply** and then click **Save**.

13 In the Set up BIG window, click **Cancel**. The Set up BIG window closes.

14 From the BIG List window, select the **BIG** and then click **File** and select **Delete**. A confirmation window appears.

15 Click **Yes** to confirm the deletion of the BIG.

16 Close the BIG List window.

Prepare for GigE BFS if Moving BFS Sessions to a GQAM

Important:

- If you are upgrading an SR 4.2 or SR 4.3 site, skip this procedure. You should have already moved ASI BFS from the CAQAM to a GQAM. The QAM GUI in these releases do not have the "BFS Capable" button.
- If you are moving ASI BFS to an RFGW, skip this procedure.

In this procedure, you will enable a GQAM for BFS in preparation for migrating the existing ASI BFS to GigE BFS.

1 Open the QAM WUI.

2 Click **By Field** and select **QAM Type**. By default, the **By Value** field should be populated with **GQAM**.

3 Does the **By Value** field contain **GQAM**?

- If **yes**, continue with Step 4.

- If **no**, choose **GQAM** from the drop-down menu.

4 Select the GQAM that will be used for Multicast BFS and open it.

5 Select the **BFS Capable** setting and save the QAM.

6 Close the QAM WUI.

Stopping the System Components and Migrating the Database and Key Files

Follow these instructions ONLY if you are migrating the database from an existing system. If this is an initial installation of SR 6.0, skip this procedure and go to ***Log into the New Explorer Controller*** (on page 93).

1 In the Application Server xterm window, type **exit** and press **Enter** to switch to the **dncs** user.

2 Complete the following steps to stop the processes on the Application Server.

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

```
appStop
```

b Wait for all processes to stop, and then type the following command and press **Enter**. The initd process on the Application Server is shut down.

```
appKill
```

Note: All process are stopped when appInitd is the only process remaining.

c Change to **root** user on the standalone Application Server and type the following command and press **Enter** to disable cron jobs.

```
svcadm –v disable –s cron
```

3 If applicable, from the **dncs** window, use the **siteCmd** command to access the RNCS and complete the following steps.

a Type the following command and press **Enter**. The RNCS 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 RNCS processes have stopped. The processes are stopped when there are no RNCS processes listed in the output.

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

d From the **root** xterm 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
```

4 Close all GUIs and WUIs.

5 From the **dncs** xterm window on the DNCS, complete these instructions.

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

```
dncsStop
```

b Wait for all processes to stop, and then type the following command and press **Enter**. The initd process on the DNCS is shut down.

```
dncsKill
```

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

– If the site is running CMD2000, the following may also be seen:

/dvs/cmd2000/bin/cmd2000 -startFile
/dvs/cmd2000/dvsFiles/cmd2k.conf

d If the output from the command in Step 5c shows that processes are running, then, from a root xterm window, type the following command and press **Enter** to stop those processes.

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

e From the **root** xterm window, type the following command and press **Enter** to disable cron jobs.

```
svcadm –v disable –s cron
```

Remove Duplicate sm_pkg_auth Entries

Execute this procedure on the system you are upgrading only if the preUpgradeChecks script found duplicate entries in the sm_pkg_auth table.

In this procedure, you will execute two scripts.

- The checkfordups.sh script verifies that duplicate entries are in the sm_pkg_auth table.
- The deldupsmpkgauth.sh script removes the duplicate entries.

Important: Duplicate entries in the sm_pkg_auth table cause the database conversion to fail.

1. Did the preUpgradeChecks script find duplicate entries in the sm_pkg_auth table?
   - If **no**, you are finished with this procedure.
   - If **yes**, go to Step 2.
2. Type the following command and press **Enter**. The checkfordups.sh script verifies duplicate entries in the table.

   ```
   /cdrom/cdrom/sai/INSTALL/dncsapp_iset/packages/SAIdncs/reloc/dncs/bin/checkfordups.sh -c
   ```

   Note: If duplicates are found, the script creates a file in the /var/log/preUpgradeChecks directory with the checkfordups__sm_pkg_auth__sm_pkg_aut9008_idx format.
3. Type the following command and press **Enter** to change to the preUpgradeChecks script directory.

   ```
   cd /var/log/preUpgradeChecks
   ```
4. Type the following command and press **Enter**. A file is created in /tmp containing the pkg_name and sm_serial_num duplicates.

   ```
   cat checkfordups__sm_pkg_auth__sm_pkg_aut9008_idx.log | awk -F'|' '{print $2"|"$3}' > /tmp/smpkgauth_dups.out
   ```

   Note: This is a single command. Do not press Enter until you have typed the entire comand. Entries in this file must be pipe (|) delimited.
5. Type the following command and press **Enter** to change to the /tmp directory.

   ```
   cd /tmp
   ```
6. Type the following command and press **Enter**. You are prompted to enter the file name containing the duplicate entries.

   ```
   /cdrom/cdrom/sai/INSTALL/dncsapp_iset/packages/SAIdncs/root/PUC/optional_fixes/deldupsmpkgauth.sh -d
   ```

   Note: This is a single command. Do not press Enter until you have typed the entire command.

7 Enter the file name created in Step 4 and press **Enter**. The script removes the duplicate entries.

8 Type the following command and press **Enter** to verify that there are no more duplicate entries.

```
/cdrom/cdrom/sai/INSTALL/dncsapp_iset/packages/SAIdncs/reloc/dncs/bin/checkfordups.sh -c
```

Note: This is a single command. Do not press Enter until you have typed the entire command.

9 Were more duplicate entries found?

- If **yes**, repeat this procedure.
- If **no**, you are finished with this procedure.

Migrate the Database and Key Files and Complete the Package Installation

Important: If this is an initial installation of SR 6.0, skip this procedure and go to *Log into the New Explorer Controller* (on page 93).

In this procedure, you will reboot the VM and execute the migration script to complete the migration from the SPARC to the UCS platform. Follow these instructions ONLY if you are migrating the database from an existing system.

Important: If you have RNCS systems, perform this procedure, as well, on each RNCS system.

1. Type the following command and press **Enter** on the new VM. The VM reboots.
   ```
   shutdown -y -g0 -i6
   ```
2. Log into the VM as **root** user.
3. Type the following command to ensure the ISO is still mounted on the system.
   ```
   df -h
   ```
4. Is the ISO still mounted?
   - If **yes**, go to Step 7.
   - If **no**, go to Step 5.
5. Enter the following commands to bounce the volfs process.
   ```
   svcadm -v disable -s volfs
   svcadm -v enable -rs volfs
   ```
6. Repeat Steps 3 and 4.
7. Type the following command and press **Enter** to export the database from the remote DNCS and install the headend components.
   ```
   /cdrom/cdrom/migrate
   ```
   Result: The system displays the current network values.

   Important: Be sure to execute this command on the RNCS, too.
8. At the **Do you wish to continue?** prompt, type **y** and press **Enter**. The **Are you sure you want to continue connecting?** message appears.
9. Type **yes** and press **Enter** to continue. The system prompts you for the SPARC system root password.
10. Type the SPARC DNCS or RNCS **root** password and press **Enter**.

    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`
11. Once the database migration is complete, the /etc/hostname.<interface> files must be moved prior to the final reboot.

Notes:

- The RNCS does not have a TED. The network interface e1000g0 is not used on the RNCS.
- The interface files from the SPARC DNCS may be platform- or site-specific. The examples that follow do not necessarily reflect the actual file names on the SPARC DNCS.

a Move the TED interface file to hostname.e1000g0.

Example: `mv /etc/hostname.ce0 /etc/hostname.e1000g0`

b Move the dncsatm file to hostname.e1000g1.

Example: `mv /etc/hostname.ce1 /etc/hostname.e1000g1`

c Move the corp/dncseth file to hostname.e1000g2.

Example: `mv /etc/hostname.ce2 /etc/hostname.e1000g2`

d Does the system include RepDB?

– If **yes**, move the RepDB interface file to hostname.e1000g3

– If **no**, enter the following command to remove the hostname.e1000g3 interface:

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

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

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

13 If you are installing and migrating an RNCS, complete this procedure on each RNCS.

Shut Down and Reboot the Servers

Follow these instructions to reboot the servers.

1. From the **root** xterm window on the SPARC Application Server, type the following command and press **Enter**. The SPARC Application Server shuts down to the **ok** prompt.

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

2. When the Application Server shuts down to an **ok** prompt, power the server off.
3. If any SPARC RNCS server(s) exist on this system, type the following command and press **Enter** in the **root** xterm window on the DNCS to shut down the SPARC RNCS server(s).

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

4. Follow these steps to shut down the SPARC DNCS, move the network cables, and reboot the new VM
   a. Type the following command on the SPARC DNCS and press **Enter** to shut it down.

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

   b. Make sure all network cables are in place and are connected to the EC.
   c. Type the following command on the new VM and press **Enter** to reboot it. This will now become the active system.

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

5. If you are installing on and migrating an RNCS VM, complete Step 4 on the RNCS.

Important: The remaining procedures in this chapter will be performed in the **VM Console** tab in vSphere/vCenter.

Log into the New Explorer Controller

Perform this procedure in the **VM Console** tab. The procedures in the remainder of the chapter will be performed in the **VM Console** tab in vSphere/VCenter.

Important: You can no longer directly log into the EC as dncs user.

1. Type **root** and press **Enter** to log into the EC as root user. The system prompts for the root password.
2. Type the **root** password and press **Enter**. The system prompts you to enter a new password.

   Note: If this is an initial installation, the default root password is `2g3n3r!c`.
3. Enter the new password and press **Enter**. You are prompted to re-enter the new password.
4. Re-enter the password and press **Enter**. The system changes the root password.
5. Log onto the EC as **root** user, using the new password.
6. The **dncs** user password must be reset. Type the following command and press **Enter** to reset the dncs user password.

   Note: This step is not required when upgrading from SR 5.0 or a newer release. You can skip to Step 9.

   ```
   passwd -r files dncs
   ```
7. Type the password for the **dncs** user and then press **Enter**. You are prompted to re-enter the password.
8. Re-type the password for the **dncs** user and press **Enter**
9. Type the following command and press **Enter** to change to **dncs** user.

   ```
   sux - dncs
   ```
10. Type the following commands and press **Enter** (after each command) to kill the dncsInitd process.

    a `dncsKill`

    b `appKill`
11. Type **exit** and press **Enter** to log out the dncs user.
12. Does this system include an RNCS EC?
    - If **yes**, go to ***Log into the New RNCS Explorer Controller*** (on page 94).
    - If **no**, go to ***Post-Upgrade Check for the 3010 Listening Interface*** (on page 95).

Log into the New RNCS Explorer Controller

Only perform this procedure if you have installed and migrated a SPARC RNCS Server. Perform this procedure in the **VM Console** tab.

1. Log into the RNCS EC as **root** user.
2. Type the **root** password and press **Enter**. A message appears informing you that the current password has expired and that you need to create a new password for the root account.

   Note: If this is an initial install, the default root password is `2g3n3r!c`.
3. Type the new password and press **Enter**. You are prompted to re-enter the new password.
4. Re-type the new password and press **Enter**.
5. Log into the RNCS EC as **root** user using the new password.
6. Type the following command and press **Enter** to reset the dncs user password.

   Note: The dncs user password must be reset.

   ```
   passwd –r files dncs
   ```
7. Type the password for the **dncs** user and then press **Enter**. You are prompted to re-enter the password.
8. Re-type the password for the **dncs** user 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. Perform this procedure in the VM Console tab.

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

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

   Example: Output should be similar to the following:

   ```
   209.165.202.129.3010          *.*             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 8.
   - 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 restart Informix.

   ```
   oninit
   ```

8. 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:

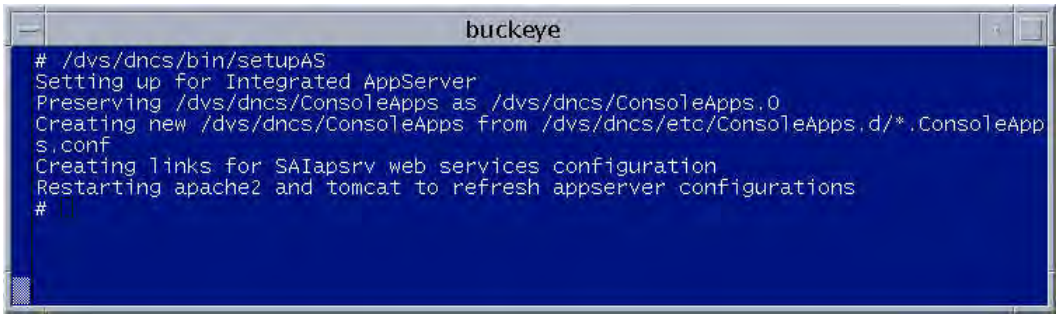
- Perform this procedure in the **VM Console** tab.
- This procedure is not required if your system is an EC without an Application Server.
- This procedure is not required if your system is an EC using a third party Application Server (MDN/ODN, Rovi Corporation,and so on).

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

Important: Only execute this command on an EC. Do not execute it on an RNCS.

As **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 (Optional)

Important: You must be **root** user to make any modifications to the /etc/dfs/dfstab file. Perform this procedure in the **VM Console** tab.

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 other than the 3 default entries?

   - If **yes**, complete these steps.
     - **a** Open the /etc/dfs/dfstab file in a text editor.
     - **b** Add the exact unique entry 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, 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 **root** user to make any modifications to the /etc/vfstab file. Perform this procedure in the VM Console tab.

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 the exact unique entry 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 upgraded a system with an integrated Application Server and no RNCS servers, skip this procedure and go to ***SR 6.0 Post Upgrade Procedures*** (on page 103).

After the upgrade, 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 enabled in this system release. The EC must exchange keys with the RNCS EC servers.

Perform this procedure in the **VM Console** tab.

1 As the **root** user, 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 then 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.

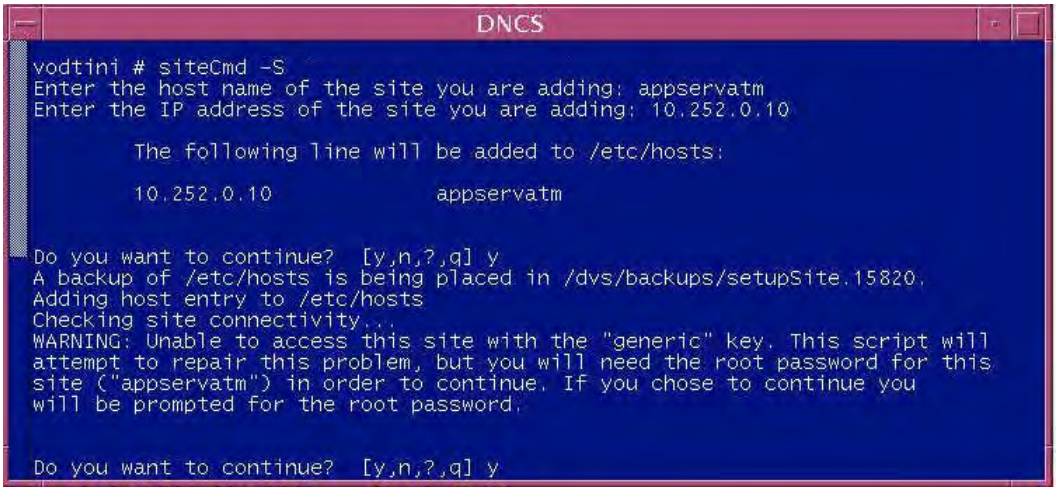
3 Type the IP address of the RNCS EC and then press **Enter**. The **Do you want to continue?** message appears.

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

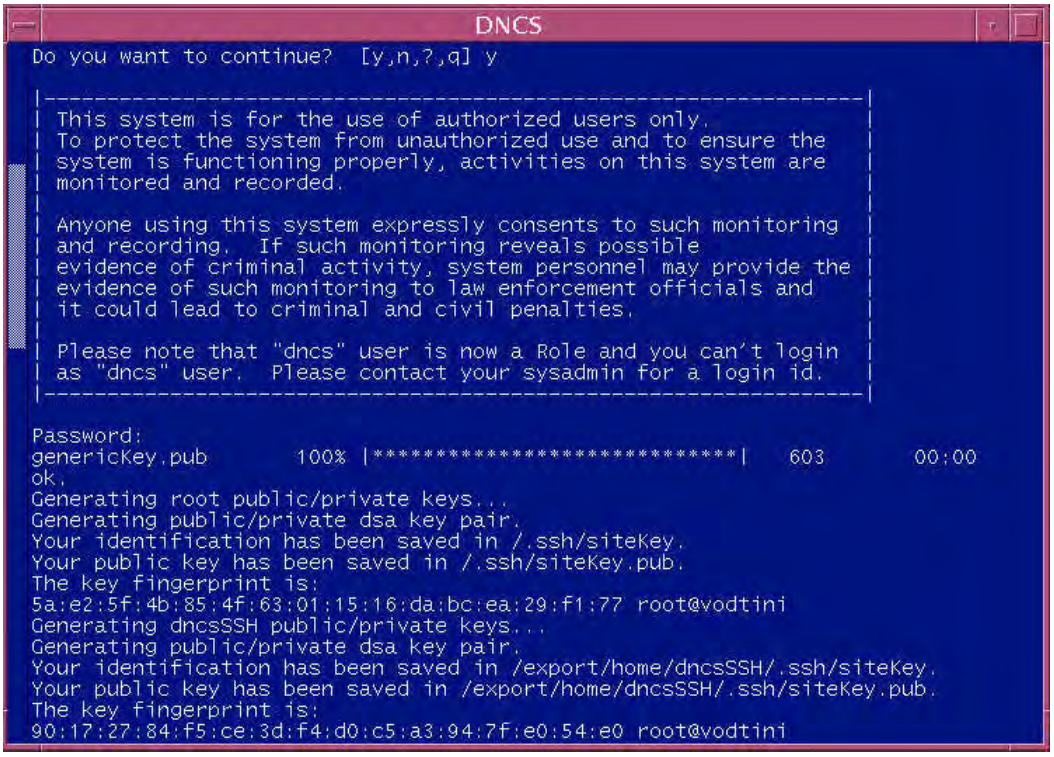
4 Type **y** and then press **Enter**.

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.



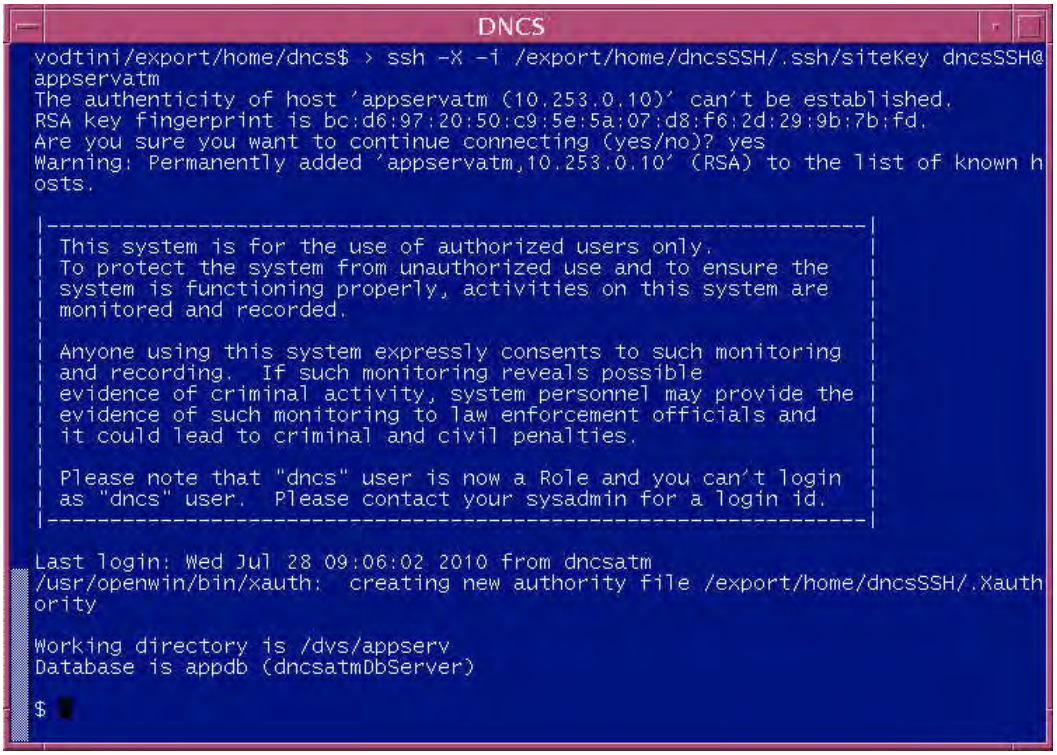
6 Type the following command and press **Enter**.

```
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 hostname]
```

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



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

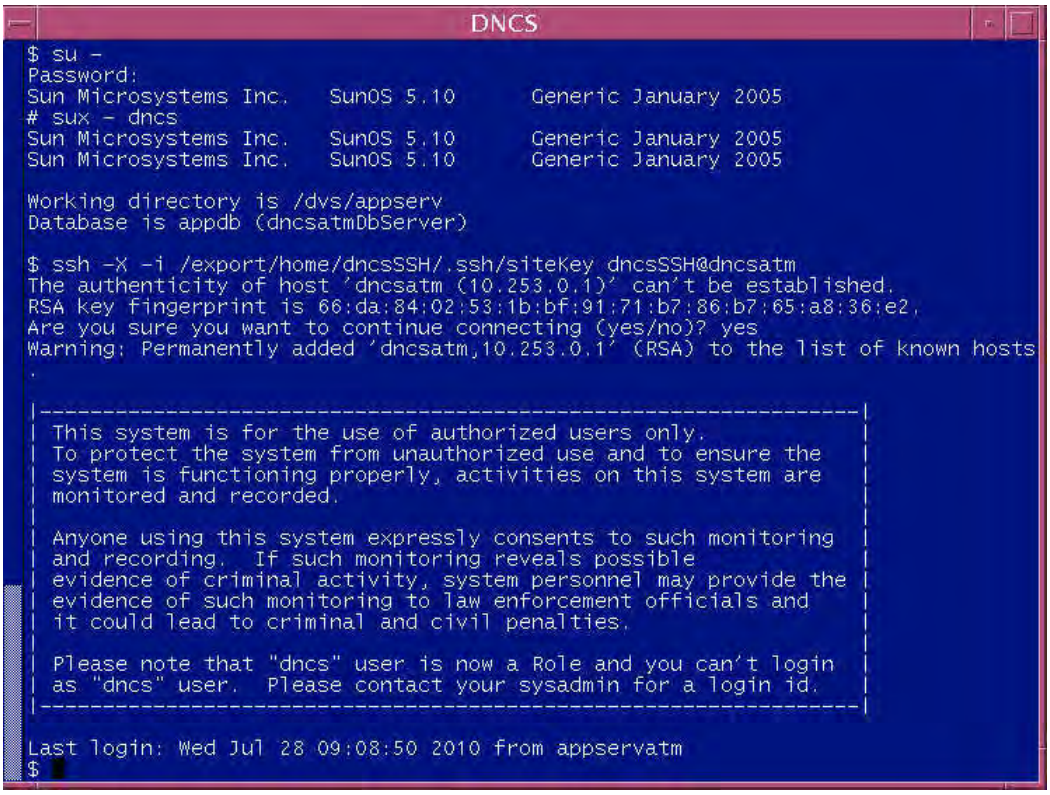
9 Type the **root password** and press **Enter**.

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 then 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 xterm window closes. This ensures that you are not still logged on as dncsSSH user.

6

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

Create User Accounts on the Upgraded Servers

Logging into the EC or RNCS EC servers is only permitted using individual user accounts. You cannot log in as dncs user. This section includes a procedure to create user accounts and provides the steps to create a default user account on the EC and/or RNCS EC, named ciscousr.

Important: Before creating a **ciscousr** account, you must first gain permission from the site. This user account will be used by Cisco personnel, post upgrade, to access the system should the site require assistance. The site will maintain control of the user password and should change the password temporarily each time Cisco assistance is requested. After Cisco assistance is no longer needed for the particular issue, the site should reset the password.

User Account Defaults

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

Creating User Accounts on the EC and RNCS EC

In this procedure, you will create a user account. All users created will be required to change their password during their first successful login session.

Note: If you are migrating from SR 5.0 or SR 5.1, you should already have created your users. You may skip this procedure or add new users, if needed.

1. Open an xterm window on the appropriate server.
2. Log into the server as **root**.
3. Type the following command and press **Enter**.
   `/dvs/admin/create_users`
   Result: The following menu appears:

```
# /dvs/admin/create_users

--------------------
Choose Type of User to Add
--------------------
1: Add Regular User (has no DNCS privileges)
2: Add Operator (has DNCS read privileges)
3: Add Administrator (has DNCS read & write privileges)
Please enter choice or 'Q' to exit: 3
```

4. Select one of the following user types:
   - Add Regular User
   - Add Operator
   - Add Administrator

   Note: For this example, type 3 to create an Administrator account called **ciscousr**.
5. Type the name of the new user account and press **Enter**.
   Notes:
   - The user name must be between 6 and 8 alphanumeric characters.
   - The user name cannot contain special characters.

   Result: The **Do you wish to continue adding this user Y/N?** message appears.
6. Type **y** (for yes) and press **Enter**.
7. Type the **password** for the user and press **Enter**.
8. Re-type the **password** for the user and press **Enter**.
9. Did you create an Administrative user?

- If **yes**, you are prompted to create a password that enables this user to access the Administrative Console (WUI). Go to Step 10.

```
Setting WebUI password for ciscousr now.
  NOTE: The user will not be required to change this password. At this point,
        the WebUI and system passwords will diverge. To update the WebUI
        password, use the htdigest command as specified in the release
        documentation.
Adding user ciscousr in realm Cisco DNCS
New password:
Re-type new password:
```

- If **no**, go to Step 13.

10 Type a password for the user you created and press **Enter**.

Note: The password to access the WUIs can be the same password that was defined for the user account.

11 Re-type the password to access the WUI and press **Enter**. The create_users menu appears.

12 Enter a number to create another user or type **q** to exit the menu. For this example, type **q** and press **Enter**.

13 When you are finished creating the Administrator user account, log out of the server.

14 Log back on to the server as the Administrator user you created in the previous steps.

Note: When you log into a newly created account, you will be prompted to change the initial password. Follow the on-screen instructions to change the password.

15 Switch to **root** user and repeat Steps 1 through 14 to create additional user accounts.

16 If you have upgraded any RNCS EC servers, repeat Steps 1 through 15 on each upgraded RNCS EC.

Important: After creating Administrator accounts on the EC, you may open terminal or xterm windows on a PC, laptop, or other remote systems to access the EC. You must use SSH to log into the EC remotely. The following example shows a typical session to the EC.

Example: `ssh -X ciscousr@[IP address]`

Note: Replace [IP address] with the actual IP address of the EC and RNCS EC, if applicable.

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 185), 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.

Set the manage_dncsLog Script Log Retention Variables

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

The variables are:

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

As shown in the preceding example, the default value is 10 days. DBDS process logs are only saved when the logLvl +ZIP is enabled.

Notes:

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

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

1. As **root** user on the EC, open the **/dvs/dncs/etc/manage_dncsLog** file with a text editor.
2. If desired, locate the **DAYS_LOGDIRS_KEPT** variable and change the value to the desired number of days.
3. If desired, locate the **DAYS_COREFILES_KEPT** variable and change the value to the desired number of days.
4. Save and close the file.

Update the osmAutomux.cfg File

For systems that use the osmAutomux.cfg file, beginning with the SR 5.0 release, this configuration file must include a headend map entry (HEMAP). If this entry is not present in the osmAutomux.cfg file, the code version table (CVT) will not get generated for remote BFS QAMs.

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

```
HEMAP|1|200
```

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

Follow these steps to add the HEMAP entry to the /dvs/dvsFiles/OSM/osmAutoMux.cfg file.

1. As **root** user on the EC, open the **osmAutomux.cfg** file in a text editor.

   Example: `vi /dvs/dvsFiles/OSM/osmAutoMux.cfg`

2. Add the following entry to the end of the file:

   `HEMAP|1|200`

3. Save and close the file.

Modify the DNCS dncs User .profile File

In this section, we will modify the dncs user .profile file. We will review and adjust the .profile file for the following items:

- Variables that are no longer needed
- New variables required for SR 5.x installations
- Review the Application Server .profile file and add unique Application Server variables to the dncs user .profile
- If your site is not SSP2.3 Compliant, you will need to add the following entry to the DNCS .profile file:

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

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

The following procedures guide you through the process.

Delete the SYSTEM_AVG_EMM_PACKETS Entry from the dncs User .profile File

The SYSTEM_AVG_EMM_PACKETS variable is the average number of EMMs per STB sent by the emmDistributor process. Setting this variable to 10 or 11 keeps the number of packets required to deliver the EMMs to the desired value of 3 per STB. In SR 6.0, the average packets value is set to 3 by default so this environmental variable is not needed. To delete this variable from the dncs user .profile file, follow these instructions.

1. As the **dncs** user, search for the variable by typing the following command and pressing **Enter**.

   ```
   grep SYSTEM_AVG_EMM_PACKETS /export/home/dncs/.profile
   ```

2. Did the above command return the variable?
   - If **yes**, open the .profile file in a text editor and go to the next step.
   - If **no**, the variable is not set. Skip the rest of this procedure.
3. Locate the **SYSTEM_AVG_EMM_PACKETS** entry, move the cursor to the beginning of the entry, and press the **d** key twice.

   Result: The SYSTEM_AVG_EMM_PACKETS entry is deleted.

   Note: The SYSTEM_AVG_EMM_PACKETS variable may be enabled on two lines as follows:

   SYSTEM_AVG_EMM_PACKETS=5

   export SYSTEM_AVG_EMM_PACKETS

If this is the case, be sure to delete both lines from the .profile file.

4 Save and exit the file by typing **:qw**.

5 Log out of the EC and then log back in to the EC.

Add the DrmCheckVodZeroScrIp Environment Variable in the .profile File

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

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

1 As the **dncs** user, open the .profile file in a text editor.

2 Move to the end of the file and add the following entry:

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

3 Save and close the .profile file.

4 Log out and then log back in as **dncs** user.

Add Unique Application Server .profile Entries to the dncs User .profile File

In this procedure, you will review the .profile file copied from the Application Server during the pre-upgrade procedures and add any unique Application Server environment variables to the dncs user .profile file of the EC.

Important: Skip this procedure if your system does not include a Cisco integrated Application Server.

1 Open a window to the EC and log in with an Administrator account.

2 Open a second window to the EC and log in using another Administrator account.

3 In both windows, type the following command and press **Enter** to change to the dncs user role.

```
sux - dncs
```

4 Type the **dncs** user password and press **Enter**.

5 In one window, open the dncs user's .profile file in a text editor.

Example: `vi .profile`

6 In the other window, type the following command and press **Enter** to review the .profile file copied over from the Application Server.

```
less appserv.profile
```

7 Review the appserv.profile file for unique Application Server-related environment variables that are set. Exclude system variables like MAIL, PATH, and so on.

Examples: The following list includes some unique environment variables that you may find.

```
PPV_ADV_WIND_START_INTVL=600
PPV_ADV_WIND_END_INTVL=900
PPV_IB_SRC_ID2=22
PPV_IB_SRC_ID1=8
PPV_OB_SRC_ID=7
```

8 Did you find any unique environment variables?

- If **yes**, continue with Step 9.
- If **no**, skip the rest of this procedure and go to the next procedure in this chapter.

9 Follow these instructions to add the unique environment variables to the .profile file (the file open in the first xterm window).

a Move the cursor to the bottom of the .profile file.

b Add the following commented line.

```
# Application Server Environment Variables
```

Important: The "#" symbol is required. It identifies the line as a comment.

c Add each unique environment variable that you found in the appserv.profile file to the dncs user .profile file.

Important: The new variables that you add should NOT be commented. The examples that follow show two ways of accomplishing this.

Example 1:

```
export PPV_ADV_WIND_START_INTVL=600
export PPV_ADV_WIND_END_INTVL=900
```

Example 2:

```
PPV_IB_SRC_ID2=22
PPV_IB_SRC_ID1=8
PPV_OB_SRC_ID=7
export PPV_IB_SRC_ID2 PPV_IB_SRC_ID1 PPV_OB_SRC_ID
```

10 Save the .profile file and exit from the text editor.

11 Type **exit** and press **Enter** in the second window (the one in which the appserv.profile file is open).

Result: The system exits from the less utility.

12 In a window, type the following command and press **Enter** to log back in as **dncs** user.

```
sux - dncs
```

13 Type the following command and press **Enter** to review the dncs user enabled environment variables.

```
env | less
```

14 Are all the new Application Server environment variables that were added present and correct?

- If **yes**, go to the next procedure in this chapter.
- If **no**, repeat this procedure.

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 118).
   - If **no**, go to ***Remove Old BFS Entries*** (on page 120).

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.

Configure Remote Access to the EC Web Interface

In this procedure, you will configure remote access to the EC Web interface through a Web browser. Follow this procedure to enable remote WebUI access to the EC.

Important: To enable SSL access, see *Explorer Controller Security Configuration Guide* (part number OL-27574).

1. In an xterm window, as the **root** user, type the following command and press **Enter**. The working directory becomes /etc/apache2/user-conf.

   ```
   cd /etc/apache2/user-conf
   ```

2. Open the **httpd.ports** file in a text editor.
3. Move to the bottom of the file. Is there a "Listen 0.0.0.0:8045" entry?
   - If **yes**, delete that entry and continue with the next step.
   - If **no**, continue with the next step.
4. Edit the httpd.ports file and add a new Listener at the bottom of the file. The entry will consist of the network interface IP address, or "dncseth" and the port that will be used to access the WebUI. There are two different options to consider:
   - **Option 1 —** Make sure that "dncseth" is an alias to the interface IP address in the /etc/hosts file. Add the following entry at the end of the httpd.ports file:

     Example: `Listen dncseth:80`
   - **Option 2 —** Use the interface IP address. If using the interface IP address, you must complete the following steps:
     a. Add the following to the **dncs** user .profile file:
     `BOSS_BOA_RESPONSE_HOST_NAME=<hostname>`

     Example: `BOSS_BOA_RESPONSE_HOST_NAME=system1`
     b. Log off as the dncs user and log back in to source the variable.
     c. Add the following to the end of the httpd.ports file:
     `Listen <IP>:80`

     Example: `Listen 198.51.100.17:80`
5. Save and exit the httpd.ports file.
6. Type the following command and press **Enter** to restart the http service:

   ```
   svcadm restart http
   ```

7. Open the Web browser and enter the IP address in the URL field and then press **Enter**. The Authentication window is displayed.

   Example: `198.51.100.17/dncs`
8. In the Authentication window, enter a valid Administrator login and password and then click **OK**. You are logged in to the EC WebUI.

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
     ```

Run the updateipmcast.sh Script

In this procedure, you will execute the updateipmcast.sh script to update the ipmulticastconn table after converting ASI BFS to GigE. In most cases the script will run and not update anything. However, some sites may have manually created some BFS sessions for a device that sets the source IP address to something other then the dncsatm IP address. Once ASI BFS has been converted to GigE BFS, these sources can now use the dncsatm IP address. This script finds and changes the sourceipaddress entry in the ipmulticastconn table to the dncsatm IP address.

1. Mount the SRDVD ISO image using the instructions in ***Mounting and Unmounting ISO Images*** (on page 185).
2. Type the following command and press **Enter** to change the directory.

   ```
   cd /cdrom/cdrom/sai/scripts/LU/PUC/other_scripts
   ```
3. Type the following command and press **Enter**. The script lists any sourceipaddress entries that need to be changed.

   ```
   ./updateipmcast.sh -U
   ```

   Results: The script runs and displays the EC version and source IP addresses (dotted and decimal). You are prompted to press **Enter** to continue.
4. Press **Enter** to continue.

   Result: The screen updates and either displays that no updates were performed, or that **ipaddresses** need to be updated.
5. Are updates needed?
   - If **no**, you are finished with this procedure.
   - If **yes**, the **Do you want to perform the update?** message is displayed. Continue with Step 5.
6. Type **y** and press **Enter**.

   Results: A restoration file is created and you are prompted to press **Enter** to begin the update.
7. Press **Enter**. The ipmulticastconn sourceipaddress are updated.
8. Review the /tmp/updateipmcast_<date>_update.log file. Verify that the updates completed successfully.
9. Type the following command and press **Enter** to verify that the ipmulticastconn table entries were updated.

   ```
   dbaccess dncsdb -
   select sourceipaddress from ipmulticastconn where
   session_oid=<session_oid from the update log file>;
   ```

   Example:

   ```
   select sourceipaddress from ipmulticastconn where
   session_oid=15247;
   ```

Sample Output:

```
session_oid 15247
resrc_num -32764
alloc_time 2013-08-22 11:46:07
rel_time
resrc_state 3
resrc_view 2
assoc_tag -32767
sourceudpport 10099
sourceipaddress 184287237
sourceipaddress2 0
sourceipaddress3 0
sourcemacaddress 00:00:00:00:00:00
mcastdestudpport 0
mcastdestipaddress -402587387
memberipaddress -1408105449
```

Note: The sourceipaddress should now be correct. Convert the decimal IP to a dotted-decimal IP to verify the correct IP (use the convertIP utility for this).

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.

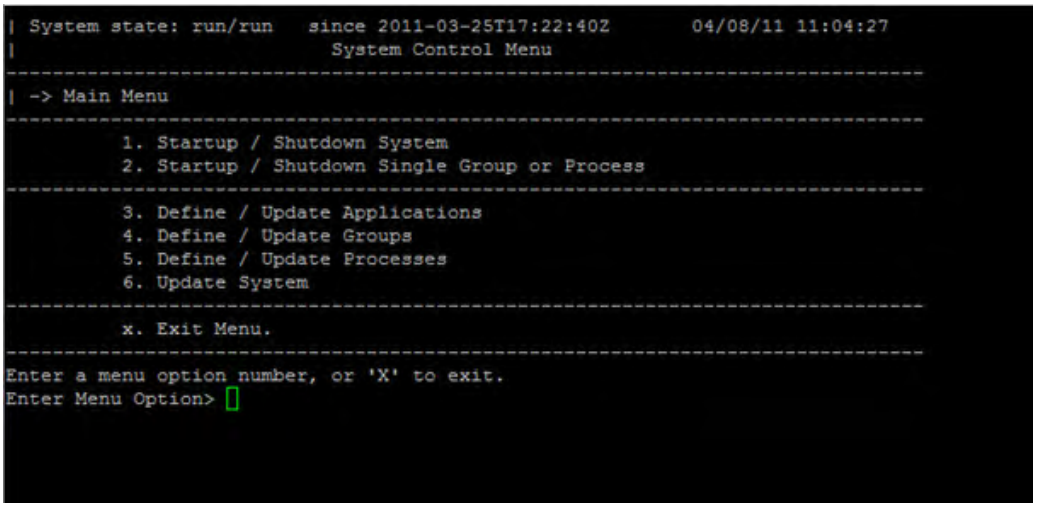
Important: If you have completed all procedures to this point, you should already have the following windows open from a remote PC, Mac, or other system:

- 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 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
```

ASI to GigE BFS Conversion

Systems upgrading from SR 4.3 and older do not support the GigeE Ethernet BFS. Most of these systems are configured to use the ASI card in Sun SPARC platforms. This procedure collects information from the site to be upgraded and converts existing ASI BFS sources to GigE Ethernet BFS sources.

Important: If you are migrating the QAM ASI BFS directly to RFGW-1, refer to *ASI BFS to RFGW-1 GigE BFS Conversion Configuration Guide* (part number OL-31477) to convert QAM ASI BFS to the RFGW-1.

Once you have completed the conversion procedure, return to this document, Chapter 6, ***Run the postUpgrade Script on Each Upgraded Server*** (on page 134), to complete the migration.

Notes:

- If your system is running SR 5.0 or later (newer), and has already been converted to GigE BFS, skip this procedure and continue with the next procedure in this chapter.
- If the upgrade engineer has completed all necessary pre-upgrade tasks, ASI BFS should have been moved to a GQAM. If this has not been done, contact Cisco Services for assistance in enabling a GQAM for BFS.

You have two choices of Ethernet configuration, Multicast or Unicast. You must supply the following information:

- The Site ID
- The Output TSID
- The GQAM ID
- The QAM input port
- The session type (1:Multicast 2:Unicast)
- Based upon the session type, the base multicast IP address (23x.a.b.c) or the unicast IP address and UDP port (1025-65535)

  Note: You will be prompted for each octet of the IP address.

  Important:

  - If you are migrating from an SR 4.3.x.x or older DNCS release, and converting from a CAQAM to an RFGW-1, you will use *ASI BFS to RFGW-1 GigE BFS Conversion Configuration Guide* (part number OL-31477) to complete this procedure.
  - When you have finished the procedure in OL-31477, return to ***Run the postUpgrade Script on Each Upgraded Server*** (on page 134), in this document, to complete the migration.

1 Are you converting the BFS from a CAQAM to an RFGW-1?

- If **yes**, use *CAQAM to RFGW-1 Broadcast File System (BFS) Migration* (OL-31477) to complete this conversion.

  Note: Once you have completed the CAQAM to RFGW-1 conversion, return to this document and continue with **Run the updateipmcast.sh Script**, next in this chapter.

- If **no**, you are converting ASI BFS to a GQAM; continue with Step 2.

2 From what DBDS version did you migrate?

- SR 5.0 or SR 5.1 (both with ASI BFS), go to Step 3.
- SR 4.3.2.x or earlier with BFS sessions built on a GQAM, go to Step 3.
- SR 4.3.2.x or earlier with BFS sessions still built on a CAQAM or an MQAM, follow these instructions.

  a As **dncs** user, type the following command and press **Enter**. The dncsdb database opens.

  ```
  dbaccess dncsdb -
  ```

  b Type the following command and press **Enter** to change the GQAM bfscapability setting from 0 to 1.

  ```
  update pdcaqam set bfscapability=1 where qam_id=[GQAM ID];
  ```

  Note: Replace [GQAM ID] with the actual GQAM ID. Do not type the brackets.

  Example:

  ```
  update pdcaqam set bfscapability=1 where qam_id=106;
  ```

  c Type the following command and press **Enter** to verify the change.

  ```
  select * from pdcaqam where qam_id = [GQAM ID];
  ```

  Example: `select * from pdcaqam where qam_id=106;`

  ```
  oid 7087d9079b660007e2000001
  Availbandwidth 155000000
  site_id 1
  ipaddr 172.16.4.23
  ipsubnetmask 255.255.255.0
  mykeycert c442b402997f0062cb000001
  macaddress 00:23:BE:61:86:D6
  qam_fpanel_lock 0
  qam_alarm_cutoff 0
  qam_id 106
  qam_enabled 1
  qam_name ConanGQAM
  busystate 0
  configfile gqam.config
  bfscapability 1
  overhead 0
  ```

```
modeltype 3
defaultgateway 172.16.4.254
coreencryptionmode 0
ca_mode 0
eis_wellknownport
pidmappingmode 0
failtoblack 1
qamhe_he_id 3
thirdparty_enc_mod 0
redundgbepresent 0
crypto_period 5
optimctrl 61
1 row(s) retrieved.
```

d Is the bfscapability field set to 1?

- If **yes**, press the **Ctrl** and **C** keys simultaneously to exit from the database. Then, continue with Step 2.
- If **no**, troubleshoot the issue or call Cisco Services for assistance.

3 As **dncs** user, type the following command and press **Enter**. The script begins to collect information.

```
/dvs/dncs/bin/genupdatesourcesql.sh -G
```

4 At the prompt to provide the Site ID from the list provided, enter the **Site ID** and press **Enter**.

5 At the prompt for the QAM ID value, enter the QAM ID value associated with the GQAM you want to serve as the BFS QAM and press **Enter**.

6 At the prompt for the Output TSID value, enter the QAM output port associated with the desired output TSID value on which you want the BFS sessions created and press **Enter**.

7 At the prompt for the QAM input port value, enter the QAM port number (1-96; the GQAM is usually port 5) and press **Enter**.

8 At the prompt for choosing Multicast or Unicast, enter the number (1: Multicast 2: Unicast) for the type of session you want to set up and press **Enter**.

9 Did you select Multicast?

- If **yes**, you are prompted to enter each octet of the IP address. Enter each octet one at a time and press **Enter**.
- If **no**, you are prompted to enter the UDP port number. Enter the UDP port number and press **Enter**.

  Note: For Unicast, you are only prompted for the first octet of the base IP address.

10 Press **Enter** after you have provided all of the information.

Result: The script creates another script (/dvs/dncs/tmp/updateSource_1.sql) that contains the SQL statements to convert the ASI BFS to the GigE Ethernet sources you have chosen.

Note: The script creates a log file in /tmp/genupdatesourcesql_<mmddyyyyhhmmss>.log. Review this log for any issues.

11 Review the contents of the /dvs/dncs/tmp/updateSource_1.sql script. If you want to change any of the settings, run the script again and provide the correct information.

Note: This overwrites the original SQL script.

12 Type the following command and press **Enter** to make the updateSource_1.sql script executable.

```
chmod 750 /dvs/dncs/tmp/updateSource_1.sql
```

13 Type the following command and press **Enter** to execute the updateSource_1.sql script.

```
dbaccess dncsdb </dvs/dncs/tmp/updateSource_1.sql>/dev/null
```

Note: This script modifies the bfssource table in the EC database, updating the values to your specifications.

14 Do you have an RNCS EC to convert ASI to GigE BFS?

- If **yes**, repeat Steps 1-13 for each RNCS EC.
- If **no**, go to the next procedure in this chapter.

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

Important: If you converted ASI BFS directly to RFGW-1, the EC processes should already be started. Skip this procedure and go to ***Run the postUpgrade Script on Each Upgraded Server*** (on page 134).

1. Did you create the **ciscousr** user account or any other user account?
   - If **yes**, go to Step 2.
   - If **no**, go to ***Create User Accounts on the Upgraded Servers*** (on page 105). After creating at least one Administrator account, continue with Step 2 of this procedure.
2. Log onto the EC as one of the Administrative User accounts that you created in ***Create User Accounts on the Upgraded Servers*** (on page 105).
3. Type the following command and press **Enter** to change to the dncs role.

   ```
   sux - dncs
   ```

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

   ```
   dncsStart
   ```

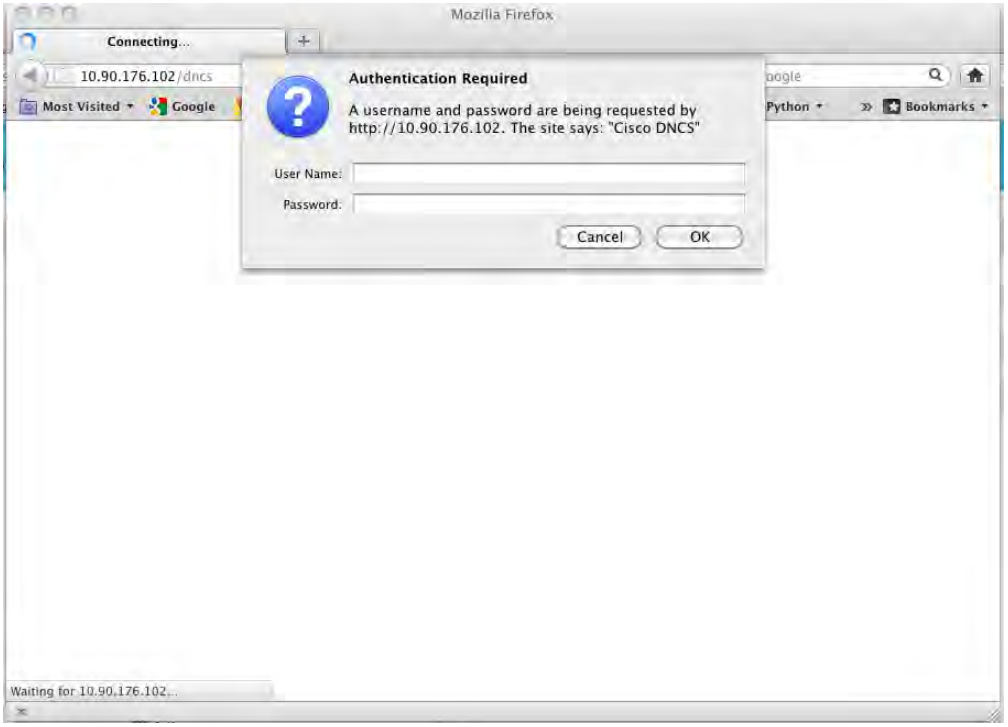
5 Open the Firefox web browser on a PC, Mac, or other system with a supported version of Firefox.

6 In the URL window, type the following:

`<EC IP address>/dncs`

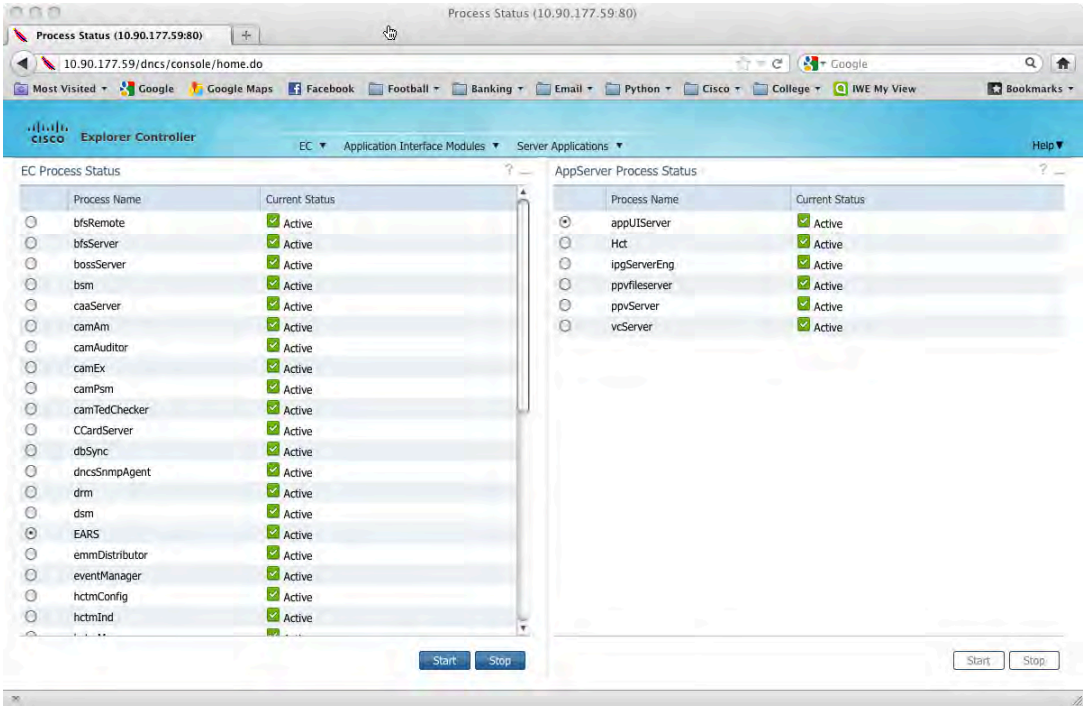
Example: 198.51.100.17/dncs

Result: The Authentication Required dialog box opens.



7 Type your user name (for example, **ciscousr**), and then type the password you defined to access the web UIs.

8 Click **OK**. The Cisco Explorer Controller window appears.



9 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.

Start the Application Processes on the EC

This section provides procedures for starting the Application Server processes on an EC that was migrated to use an integrated Application Server.

1 Type the following command and press **Enter** to start the Application Server processes.

```
appStart
```

2 Monitor the processes as they come up. Green indicators replace red indicators as the application 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.

Restarting the RNCS EC

1. As the **dncs** user on the EC, type the following command and press **Enter**. The LIONN processes start.

   ```
   siteCmd [RNCS EC hostname] lionnStart
   ```

2. Type the following command and press **Enter** to confirm that the LIONN processes started successfully.

   ```
   siteCmd [RNCS EC hostname] pgrep –fl dvs
   ```

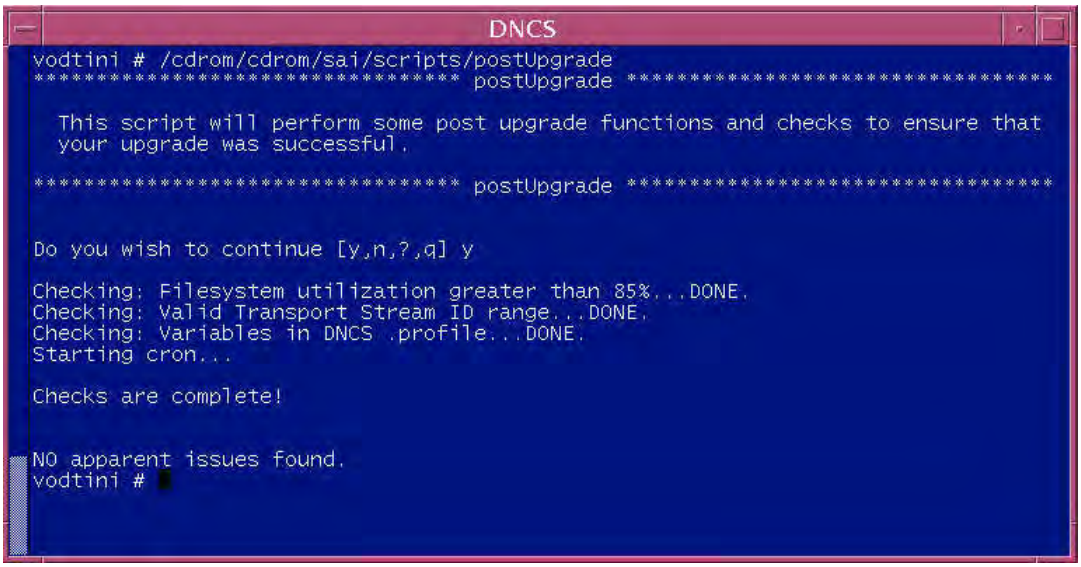
Run the postUpgrade Script on Each Upgraded Server

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 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

Important: If you have moved ASI BFS sessions to an RFGW, you have already verified the number of BFS sessions. You can skip this procedure.

1. Press the **Options** button on the front panel of the BFS QAM until the **Session Count** total appears.
2. Does the **Session Count** total equal the number of sessions you recorded in ***Check the Number of BFS Sessions*** (on page 26)?
   - If **yes**, skip to Step 6.
   - If **no**, telnet to the GQAM modulator where BFS sessions are built.

     Example: telnet 192.51.100.29

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

     a Press 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 then 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 **00:00:00:00:00:00:00:2**. 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 **00:00:00:00:00:00:00:2** show **PAT_ASSEMBLY**?
   - If **yes**, go to ***Tear Down BFS and OSM Sessions*** (on page 136).
   - 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 209.165.202.129

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 appears.

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

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

8 Click **Display** at the bottom of the page. The Session Summary page appears.

Result: Output similar to the following 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 display 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 appears.

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

22 Does the **Session Count** total now equal the number of sessions you recorded in the ***Check the Number of BFS Sessions*** (on page 26) 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 172.16.4.30 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*** (on page 26) 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 198.51.100.29

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

a Press 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 then 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.

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 143).

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 145).

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 145).

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 145).

  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 145).

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** xterm window, type **cd** and then press **Enter**. The home directory of /export/home/dncs becomes the working directory.

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

Note: The 'l' is a lowercase L.

3 If applicable, the dncs user crontab file should now include all of the ipgCollector entries that were on the standalone Application Server before the upgrade. Verify that these entries are present in the dncs user crontab file.

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

- If **yes**, go to ***Examining the CED.in Entry*** (on page 146).
- 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 147).
- 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 159) 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*** (on page 28).

1. From the EC WebUI, click the **Interface Modules** drop-down arrow and then click **BFS Client**. The Site DNCS Broadcast File Server List window appears.
2. Refer to the sheet of paper that you used when you completed ***Record Third Party BFS Application Cabinet Data*** (on page 28). 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 **New 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 3.
3. Highlight each of the third-party application cabinets listed on the sheet of paper, in turn, and then 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 Broadcast File Server List window when you are finished.

Add dncs Role to Users Granted Administrator Access

If your pre-SR 6.0 system contained existing user accounts that were granted Administrative access, you must assign the "dncs" roll to these users. Adding the "dncs" roll to a user also creates the WebUI account for the user. This enables the user to access the WebUI for SR 6.0 systems. Users assigned the "dncs" roll have permission to add, delete, and make changes in all EC WebUIs.

1. As **root** user on the EC, type the following command and press **Enter**. The useradmin menu appears.

   ```
   /dvs/admin/useradmin
   ```

2. Enter the letter corresponding to **Add a Role** and press **Enter**. The system prompts for the user login name.
3. Enter the login name of the user to whom you want to assign the role. The system prompts for the role you want to assign to the user.

   Note: At this time, the only available role is **dncs**.

4. Enter the role and press **Enter**. A confirmation message appears.
5. Type **y** and press **Enter**. The system prompts for a WebUI password for the user.
6. Enter, then re-enter the password at the prompt. The system assigns the dncs role and creates the WebUI account for the user.

   Note: The WebUI login name will be the same as the user's system login. That is, if the user is *testers1* the WebUI login will also be *testers1*.

7. Have the user verify the following functions.
   - The user can log into the EC.
   - The user can change to the dncs user.
   - The user can access the WebUI.

Disable the Default ciscousr Account

If you created the default ciscousr account in ***Create User Accounts on the Upgraded Servers*** (on page 105), you may now disable this account, change the password, or delete the user account to restrict access to the system.

To perform this procedure, refer to *Explorer Controller Security Configuration Guide* (part number OL-27574).

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) .

7

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

Follow this procedure to restore the system software that was in place prior to the unsuccessful upgrade to SR 6.0.

1 Write down the version of the system release you are trying to restore.

_____

2 Follow these steps to disable the GigE BFS sources.

a Choose **Application Interface Modules > BFS Admin**. The BFS Administration WebUI appears.

b Does the system have an RNCS?

– If **yes**, select the **DNCS** and click **Select** at the bottom of the page. The DNCS BFS Host WebUI appears.

– If **no**, go to Step 2c.

c Click **BFS Sources**. The BFS Source WebUI appears.

d Click **Source ID** to sort the IDs in reverse order (high to low).

e Beginning with the highest-numbered, enabled, in-band BFS source number, click the box next to it and then click **Edit**.

Note: You only need to disable the in-band BFS Sources. In-band BFS Sources have even numbered Source IDs.

f Next to **Data Pump**, click **Stop** and then click **Save**.

g Click **OK**.

h Repeat Steps c through g for all remaining enabled, in-band BFS Source IDs.

i Does the system have an RNCS EC?

– If **yes**, repeat Step 2, selecting the **RNCS**.

– If **no**, go to Step 3.

3 Type the following commands, pressing **Enter** after each, to stop all system components.

```
appStop
dncsStop
appKill
dncsKill
```

4 If the system has an RNCS EC, type the following commands and press **Enter** after each to stop the RNCS EC components.

```
siteCmd [RNCS EC IP] lionnStop
siteCmd [RNCS EC IP] lionnKill
```

5 Follow these steps to shut down and power off the VM.

a Type the following command and press **Enter** to shut down the VM.

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

b Right-click the VM and select **Power/Power off**.

c If the system has an RNCS, repeat Steps 5a and 5b for the RNCS VM.

6 Boot the SPARC DNCS.

7 Log onto the SPARC DNCS as **dncs** user.

Note: If the system is SR 5.0 or SR 5.1, log in as an administrator user and change to the dncs user.

8 Type the following command and press **Enter** to start the DNCS processes.

```
dncsStart
```

9 Type the following command and press **Enter** on the Application Server to start the Application Server processes.

```
appStart
```

10 Type the following command and press **Enter** on the DNCS to start the processes on the RNCS.

```
siteCmd <RNCS hostname> lionnStart
```

11 Return to Appendix A, ***System Verification Procedures*** (on page 159), to verify system functionality.

C

Configuring DTACS on an SR 6.0 System

Introduction

Important: If you are upgrading an *existing* SR 6.0 system *and* 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 DNCS through the SSH protocol in order to enable database synchronization.

In This Appendix

Open an xterm Window on the DNCS 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 xterm 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 xterm window on the DTACS or the DNCS server for the remaining procedures in this appendix.

Complete the following steps to open two **root** xterm windows on each server.

1. Open two xterm windows on the DNCS system.
2. In one xterm window, complete the following steps to log in as **root** user on the DNCS.
   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 xterm 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; then 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 DNCS Server

Important: All steps in this procedure take place in the **root** xterm window on the DNCS server.

1. In the **root** xterm window on the DNCS 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 DNCS and DTACS Servers

This procedure includes the steps that add the private/public keys between the DNCS 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 DNCS Server*** (on page 173) in the space provided.

Host Name of DTACS Server: _____

2 In the **root** xterm 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** xterm window of the DNCS 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
```

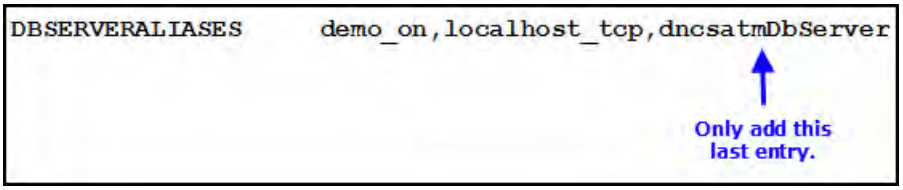
7 Save and close the file on the DNCS server.

8 In the **root** xterm window of the DNCS 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** xterm window on the DNCS server, type the following command and press **Enter** to start the Informix listener for the dncsatmDbServer.

```
onmode –P start dncsatmDbServer
```

11 In the **root** xterm window on the DNCS 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 then 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 then 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** xterm window of the DNCS server.

```
sux - dncs
```

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

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

Note: Substitute 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 DNCS.

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 DNCS 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 DNCS. The hostname for the DNCS is permanently added to the list of known hosts on the DTACS server.

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

Cisco UCS C210 Server Configuration

Introduction

The Cisco UCS C210 server is used mainly for lab exercises in the SR 6.0 environment. It is not intended to be used on production systems.

The information in this appendix helps lab technicians configure the C210 server for use in the lab.

In This Appendix

Cisco UCS C210 Server Details

Supported Server Platform

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

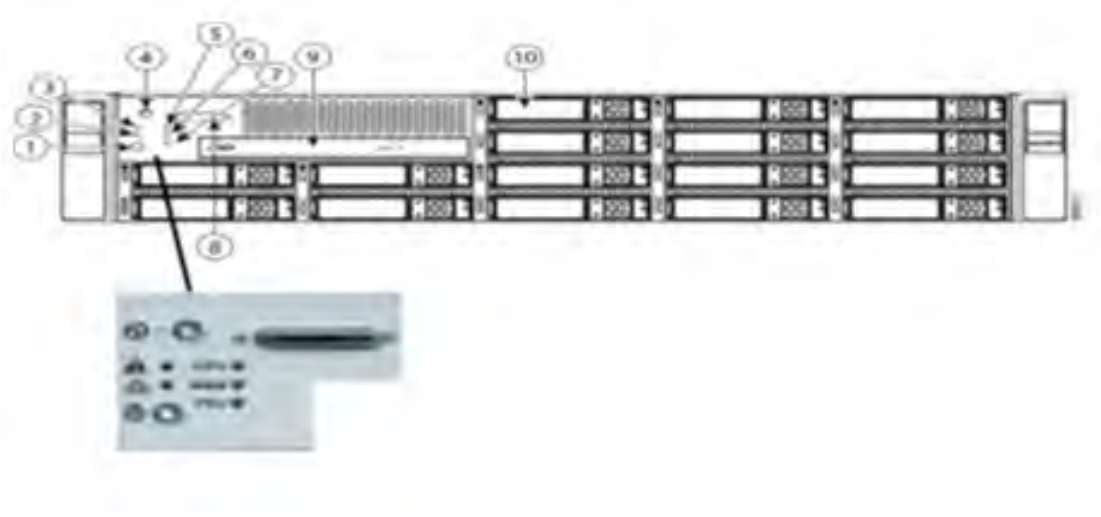
EC / RNCS EC Server

Platform	Hard Drives	Memory
Cisco UCS C210 M2 (Recommended for labs, only)	■ 16 X 300 GB	■ 32 GB minimum

Hardware Diagram of the Cisco UCS C210 Server (Lab Use)

Note: The Cisco UCS C210 server is suited primarily for lab use.

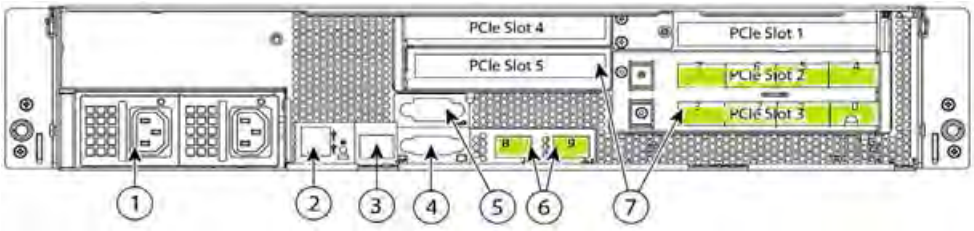
Chassis Front View



Slot	Description	Slot	Description
1	Locator LED/Locator button	6	Memory fault LED
2	Network activity LED	7	Power supply fault LED
3	System fault LED	8	Console connector (with supplied KVM cable, provides DB15 video, DB9 serial, and two USB 2.0 connectors)
4	Power button/Power status LED	9	DVD-RW drive (optional)
5	CPU fault LED	10	Hard drives (up to 16 2.5" HDD)

Chassis Rear View

Important: Some sites receive their SR 6.0 systems unassembled. Therefore, it is most important to ensure that network cards are installed in the slots shown in the following diagram:



Slot	Description	Slot	Description
1	Power supply (up to 2)	5	Serial connector (DB9)
2	USB 2.0 connectors (2)	6	10/100/1000 Megabit Ethernet ports (2)
3	10/100 Ethernet management port (RJ-45)	7	Standard-profile PCIe card slots (five total)
4	Video connector (DB15 VGA)		

Tested Reference Configuration

Network ports are numbered and marked as green. Cables should be run to the following designated ports.

- NIC Ports 0 and 4 — ESXi Management
- NIC Ports 1 and 5 — Headend network
- NIC Ports 2 & 6 — Corporate network, used for migration
- NIC Port 8 — TED crossover
- NIC Ports 3 and 7 — DSG network

  Important: The DOCSIS Set-Top Gateway (DSG) network is only used if you have the licensed feature. Otherwise, these ports are unused at this time.

Cisco UCS C210 Server CIMC Configuration (Lab Use)

This procedure references steps in the Cisco UCS C210/200 Quick Start guide. Especially for lab use, be certain that you are referencing the correct guide. The C210/200 Quick Start guide goes to Steps 6a and 6b.

Note: The Cisco UCS C210 server is suited primarily for lab use.

- Cisco UCS C210 Server CIMC Configuration (Lab Use) (this procedure)
- ***Cisco UCS C210 Host Configuration (Lab Use)*** (on page 195)
- ***Cisco UCS C210 Firmware Upgrade (Lab Use)*** (on page 196)
- ***ESXi Installation for the C210 Server*** (on page 197)
- ***Use VMware vSphere to Configure the Host System*** (on page 203)

If the UCS C210 platform has already been configured, go directly to ***OVA Deployment When Using a UCS C210 Server*** (on page 206).

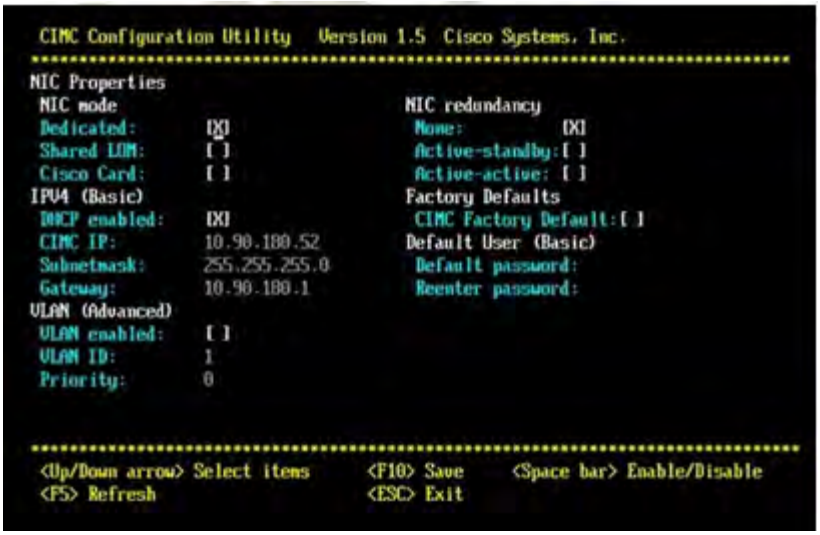
1 Obtain the Cisco UCS C210/200 Quick Start guide. This guide should have shipped with the server and is contained in the box in which the server shipped.

2 In the Cisco UCS C210/200 Quick Start guide, complete the steps through 6a to set up the hardware.

Important: Do not complete Step 6b.

Setting	Value	Step in Quick Start Guide
NIC Mode	Dedicated	3c
IPV4 (Basic)	Disable DHCP Enter IP information	3e
Set NIC Redundancy	None	3d
Change Default User Password	Unique password	3f

3 Press **F8** at the Cisco splash screen. The server boots to the CIMC Configuration Utility window. Use the chart in Step 2 to complete the configuration.



4 Press **F10** to save your changes.

5 Press **Esc** to exit the utility.

Cisco UCS C210 Host Configuration (Lab Use)

1. Use a web browser to open the CIMC application, using the IP address configured in ***Cisco UCS C210 Server CIMC Configuration (Lab Use)*** (on page 193).
2. Log on to the server using the admin password or the password that you set in the previous section.
3. Click **Power Policies**.
4. Select **Restore Last State**.
5. Click **Save Changes**.

Cisco UCS C210 Firmware Upgrade (Lab Use)

Note: The Cisco UCS C210 server is suited primarily for lab use.

Refer to the Cisco UCS C210 hardware guide to upgrade the firmware.

Important:

- This procedure is one example of various methods to upgrade the Cisco UCS C210 firmware.
- To upgrade from CD, download the firmware from this website, and then burn it to a CD:

  http://www.cisco.com/cisco/software/release.html?mdfid=283862069&flowid=25882&softwareid=283850974&release=1.4%283k%29&relind=AVAILABLE&rellifecycle=&reltype=latest
- Cisco engineers have tested firmware version 1.4.3.c.

To install the firmware from CD, follow these instructions:

1. Insert the firmware CD into the CD drive of the Cisco UCS C210 server.
2. Press **Ctrl** + **Alt** + **Delete** to reboot the server. The system reboots from the firmware CD.
3. Type **y** and press **Enter** to accept the license agreement. The Firmware menu is displayed.
4. Type **8** (All of the above) and press **Enter**. The firmware upgrade begins and displays the following message.

   Current running version of the LOM is equal to the version to be updated. Do you want to continue?
5. Type **y** and press **Enter**. The firmware upgrade continues and the message **Press any key to continue** appears.
6. Press any key to continue the upgrade.

   Note: When the firmware upgrade completes the Firmware menu once again appears.
7. Type **10** to save the current CMC settings. The firewall installs.
8. When the system begins to reboot, eject the DVD when the Platform Hardware Check begins.

   Important: If you do not eject the firmware DVD before the system boot, it starts the firmware upgrade again.
9. Watch the reboot process closely. After the disks are displayed, observe the boot messages and press **Ctrl** + **H** when prompted to access the WebBIOS (RAID Configuration Utility). After a few minutes, a **Start** button appears.

ESXi Installation for the C210 Server

Before You Begin

Note: The Firefox browser is not officially supported for accessing the UCS C210 CIMC application.

1. Use a web browser to open the CIMC application, using the IP address configured in ***Cisco UCS C210 Server CIMC Configuration (Lab Use)*** (on page 193).
2. Log on to the server using the admin password or the password that you set in *Cisco UCS C210 Server CIMC Configuration (Lab Use)*.

Power Policy

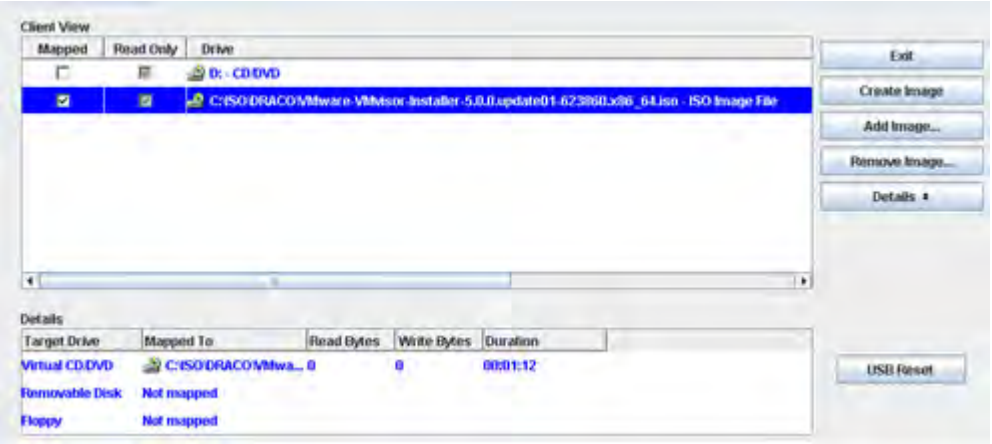
1. Click **Power Policies**.
2. Select **Restore Last State** from the menu.
3. Click **Save Changes**.
4. Click **Summary** on the Server tab in the CIMC.
5. Click **Launch KVM Console** from the Server Summary window.
6. Select **Open using java viewer** in the dialog box. The KVM Console is displayed.
7. Select **Macros**, and then choose **Ctrl-Alt-Del** from the menu bar.

Installing ESXi

Important: Before beginning this procedure, be sure that you have downloaded or copied the VMware ISO image to the local hard drive that is running the CIMC application.

1. Follow these instructions to mount the ESXi ISO image:
   a. Click the **Virtual Media** tab in the KVM Console.
   b. Click **Add Image**.
   c. Browse to the location of the VMware ISO image and click **Open**.

d Click the **Mapped** box next to the added image.



e Click the **KVM** tab in the KVM Console.

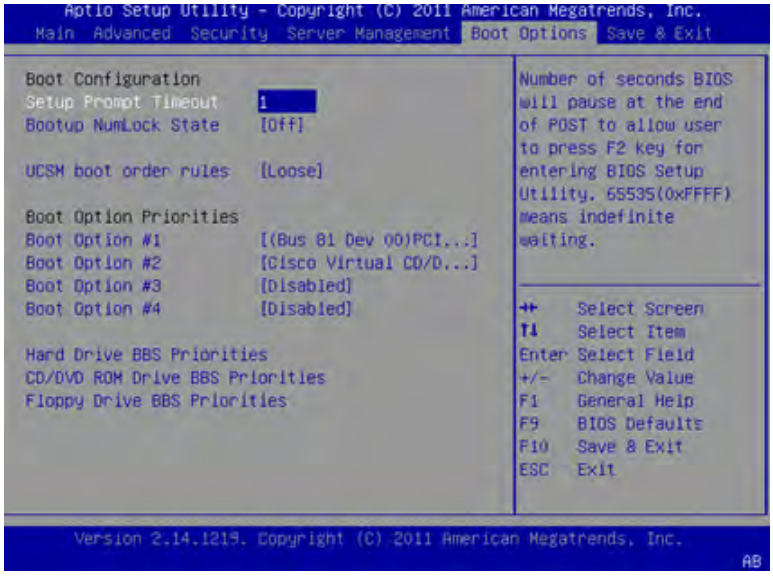
2 Click **Macros** and then choose the **Ctrl-Alt-Del** option from the KVM menu bar to reboot the server.

3 Press **F2** when the Cisco splash screen is displayed to enter the system setup.

4 Navigate to the **Boot Options** tab.

5 Make the following selections:

- Boot Option 1 — (Bus 11 Dev 00) PCI RAID Adapter
- Boot Option 2 — Cisco Virtual CD/DVD
- Disable remaining boot options



6 Press **F10** to save the settings and reset system.

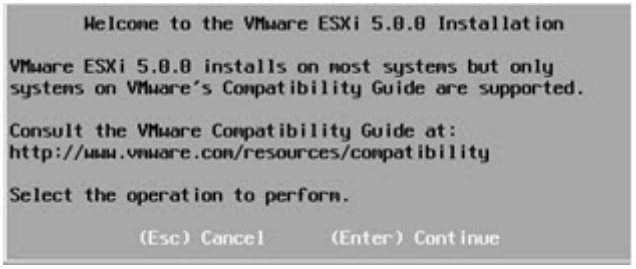
7 Click **Yes** to save the settings and reset the system.

Note: If the **Invalid configuration detected** message appears, you can ignore it.

8 Did a media message appear?

- If **yes**, click the **Macro** tab and select **Ctrl-Alt-Del** to reset the system. Then go to Step 9.
- If **no**, the reboot continued. Go to Step 9.

9 Wait for the ESXi installer to load. After the ESXi load completes, a **Welcome** message appears.



10 When prompted, press **Enter** to continue.

11 When prompted, press **F11** to accept the license agreement.

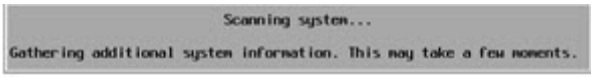
Note: This action selects the disk. There should only be one disk to select.

12 Press **Enter** to continue.

13 Select the appropriate keyboard layout (ex. US default) and press **Enter**.

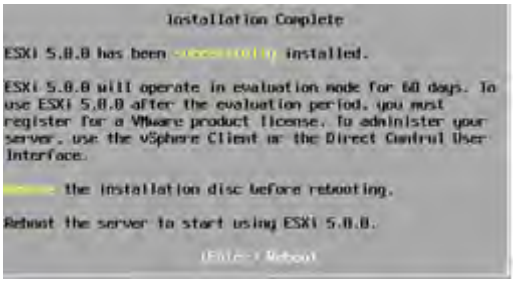
14 Enter and confirm a new **root** password for the ESXi host.

15 Press **Enter** to continue.



16 Press **F11** to confirm the installation on the selected disk. The ESXi installation begins and a progress bar appears.

17 When the installation completion screen is displayed, press **Enter** to reboot. The ISO is un-mapped and the system boots to the VMware ESXi window.



Important: Let the system boot all of the way into ESXi. If you press F2 too early (during boot-up), the BIOS configuration screen appears, which is not what you want at this point.

18 Press **F2** to customize the system.

19 Log in as the **root** user. The System Configuration window appears.

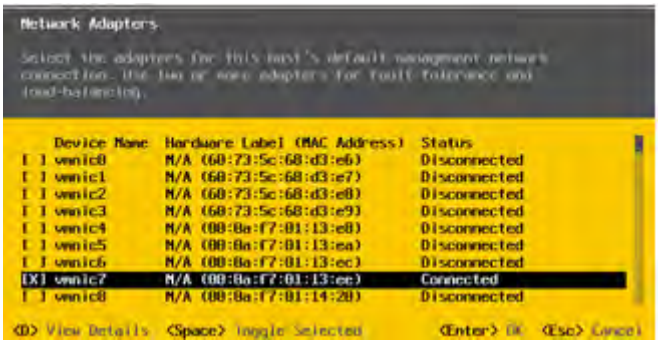
20 Navigate to **Configure Management Network** and press **Enter**.

21 Choose **Network Adapters** and press **Enter**.

22 To select a vmnic, highlight the line you want and press the **Spacebar**.

- For the UCS 210 server, enable nic 0; disable the others.

23 Verify that the device you enabled in Step 22 shows a **Connected** status.



24 Press **Esc** to go back.

Note: If you made changes, you may need to press **Esc** to go back, save the changes, then go back into the Network Adapters window to see your device as Connected.

25 Select **IP Configuration** and press **Enter** to set/modify the IP address.

26 Use the arrow keys to highlight **Set static IP address** and press the **Spacebar**.

27 Provide the following information to configure the ESXi server:

- IP Address
- Subnet Mask
- Gateway

28 Press **Enter** to accept the changes and return.

29 Use the arrow keys to highlight **DNS configuration** and then press **Enter**.

30 Provide the following information.

- **Primary DNS IP address**
- **Secondary DNS IP address** (optional)
- **Hostname**

31 Press **Enter** to accept and return.

32 Press **Esc** to exit and press **Y** to accept the changes when prompted.

33 Select **Test Management Network** and then press **Enter** to navigate to the Test Management Network dialog.

34 Press **Enter** to begin a ping test.

35 After the ping test is complete, press **Enter** to exit the test dialog.

36 See the site Network Administrator to verify addressing and cabling.

37 Scroll to **Troubleshooting Options** and then press **Enter**.

38 Select **Enable SSH** and press **Enter**. The right-hand panel mode should indicate **SSH is Enabled**.

39 Press **Esc** to exit.

40 Press **Esc** to log out and disconnect the KVM.

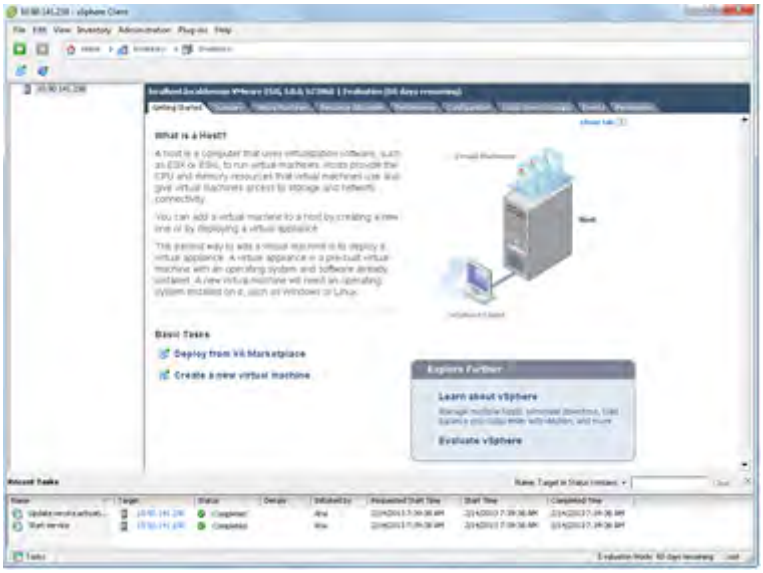
41 Click **File/Exit** to close the KVM console.

Use VMware vSphere to Configure the Host System

You must have a Windows, Linux, or Mac OS system with vSphere installed to complete the installation and migration of SR 6.0.

1. Provide the IP address, username, and password for the new ESXi host to the vCenter administrator. Once the administrator licenses the new host, you will be able to access it through vCenter.
2. Use the VMware vSphere Client to connect the vCenter server. Provide the IP Address, username and password for authentication.
3. If you are using vCenter and the Home view is displayed, click on **Hosts and Clusters**, and then highlight the new ESXi host in the left pane to begin configuring resources.

   Result: vSphere should go to the Inventory display. If not, click **Inventory** to display the ESXI Host.



4. Click the **Configuration** tab.
5. From the **Software** menu, choose **Time Configuration** to modify the date and time.
6. Click **Properties** and enter the correct date and time.
7. Click **NTP Client Enabled**.
8. Click **Options** and then click **Start and Stop with host**.
9. Click **NTP Settings** and then click **Add**.
10. Enter the **NTP Server Address** and click **OK**.
11. Select **Restart NTP Service** to apply changes and click **OK**.
12. Verify that **NTP Client Enabled** is enabled and click **OK**.

13 From the **Hardware** menu, select **Networking**. Switch vSwitch 0 is displayed.

14 Select **Properties** for vSwitch 0.

15 Select **VM Network** and click **Remove**. You are prompted to confirm this request.

16 Click **Yes**.

17 Click the **Network Adapters** tab and then click **Add**.

18 Refer to the chart that follows to configure the proper Management network adapter for your system. Click **Next** after selecting the proper network adapter.

Note: Use the data in this chart to help you configure the network host system settings.

Network	UCS 210 (Lab only)
Management	0, 4
Headend	1, 5
Corporate	2, 6
TED	8
DSG	3, 7

19 Verify the adapter selection and then click **Next**.

20 Click **Finish** to close the wizard.

21 Click **Close** to return to the **Configuration** tab.

22 Click **Add Networking**.

23 Select **Virtual Machine** and then click **Next**.

24 Refer to the chart in Step 18 to configure the proper Headend network adapters for your system.

25 Click **Next**.

26 Label the network as **Headend Network**.

27 Click **Next** and then click **Finish**.

28 Repeat these procedures to configure the following networks shown in the network design that was created for the customer:

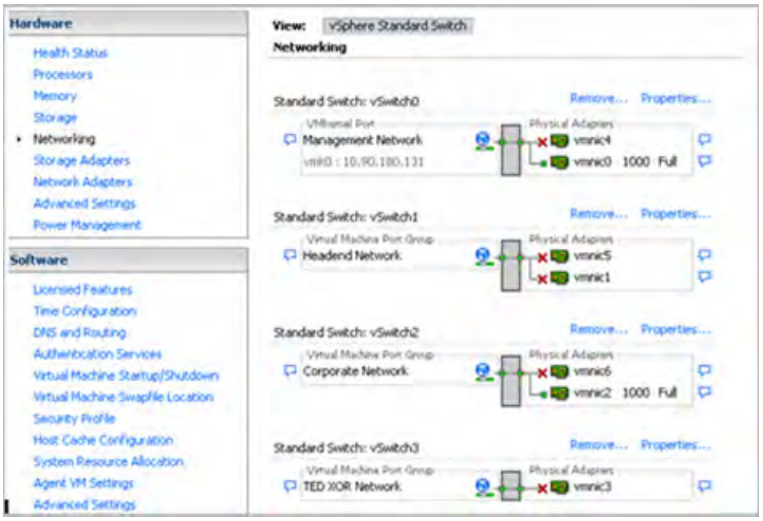
Note: The following examples are for reference, only.

- **Corporate Network —** For corporate and back office access. This is created under **vSwitch 2.**
- **TED XOR Network —** For direct crossover connectivity with the TED. This is created under **vSwitch3.**
- **RepDB Network —** For direct connectivity to the RepDB interface when RepDB is an enabled feature. This is created under vSwitch4.

  Note: This network is optional and should be configured only if you are using RepDB.

- **DSG Network —** For direct connectivity to the DSG interface when DSG is an enabled feature. This is created under vSwitch5.

  Note: This network is optional and should be configured only if you are using DSG.



29 To configure the **Storage Configuration**, click **Storage** from the **Hardware** menu.

30 Highlight **datastore1** and select **Properties**.

31 Click **Rename** and rename to **<hostname>_local_storage1**. Click **OK**.

32 Verify the changes and click **Close**.

33 If necessary, create an NFS mapping to the location of the Solaris image.

Note: The server and path are site-specific. The customer should have the Solaris 10 (x86) ISO file on an NFS server accessible by the Virtual Machine (VM).

Example: The directory path for the Solaris image on the aurora server is `192.0.2.55:/ccm_archive/release/integrate/PlatformOS`

a Click **Add Storage**.

b Select **Network File System** and click **Next**.

c Input the server name or IP address, folder, select **Read Only**, and input a datastore name.

d Click **Next**.

e Verify the settings and click **Finish**.

OVA Deployment When Using a UCS C210 Server

Complete the procedures in ***OVA Deployment*** (on page 70), except in Step 8, choose the following configuration for an EC or an RNCS EC:

- **EC** — 12 vCPU 48 GB RAM 512 GB HD
- **RNCS EC** — 12 vCPU 24 GB RAM 256 GB HD

G

Registration of the 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 enabling of the Regionalization feature.

Important: You must have the Explorer Controller Suite (ECS) configured and installed with ECS software to register an EC.

Configure the EC System for Regionalization

1 As the **root** user, use a text editor to edit the `/etc/apache2/user-config/80.auth.conf` file on the EC and add an "Allow for boa" entry.

Example:

```
ident "@(#) %full_filespec: 80.auth.conf,2:ascii:Da=1%"
<Location/>
# Order Allow,Deny
# Allow from localhost
# Allow from dncs
# Allow from dncseth
# Allow from 198.51.100.99/24
# Allow from 198.51.100.77/24
# Allow from all
Allow from boa
# ErrorDocument 403 "<html><head><title>Error
403</title></head><body><h2>SECURI
TY WARNING</h2>Web connections are only allowed from
localhost.</body></html>"
</html>"
</Location>
```

Note: Uncomment the "<Location/>" and "</Location>" lines. Do not uncomment any other lines.

2 Access the EC WebUI by entering the following address in a Firefox Web browser. The Explorer Control WUI appears.

`http://[EC_IP]/dncs`

Example: `198.51.100.17/dncs`

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

3 Choose **EC > System Provisioning > Regionalization Configuration**. The Regionalization Configuration WebUI appears.

4 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 (such as: LWR, SJC)

  Note: This is useful in identifying where the primary EC is physically located.

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

  Important: You cannot edit this field. Initially, it is blank.

- **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.

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

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

  Notes:

  – This is useful in identifying where the secondary EC is physically located.

  – 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 CMC Management Node

  Example: `198.51.100.84`

- **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

5 Click **Save**. The following results occur in the lower area of the WUI:

- **Registration Status** changes to **Registered**
- **Status Comment** changes to **Successfully Registered**
- **Last Updated Time** updates to the time it was successfully registered

6 Go to the ECS (https://ECS Management IP) and choose **Message Infrastructure > Service Infrastructure > Service Instance**. Verify that all ECID-related Service Instances are IS (In Service).

- [ECID]-oam
- [ECID]-register
- [ECID]-rpo
- [ECID]-boss

7 From the ECS WUI, choose **Service > ECS Management > Dashboard**. The network element for the EC you registered should have an icon with a green checkmark in it. This indicates that the EC (Network Element) is online.

Important: If you provisioned any Standby fields in the EC Regionalization Configuration WUI, the Standby Network Element will be present but will be Offline. Also, a [hostname-Stdby] Service Instance is created but is OOS.

8 Were any of the Standby fields provisioned?

- If **yes**, an [ECID]-stdby-oam SI will be present and will be OOS.

- If **no**, there are no further SIs present.

9 To put the [ECID]-stdby-oam in an IS state, open an xterm window and access the secondary server as the **root** user. Then enter the following commands:

   a `/etc/init.d/dncsInit start`

   b `/etc/init.d/oammgrctrl start`

10 Go back to the ECS Service Instance WUI and refresh the window. The [ECID]-stdby-oam SI should now be IS.

11 From the ECS Dashboard, click the **Network Element Management** tab and then the **Network Element Access Management** tab.

12 From the **User** list, select the user to whom you want to give EC access.

13 In the **Network Element(s)** list, select those ECs to which this user will be granted access.

   Note: You can use the **Shift** or **Ctrl** keys to select more than one user.

14 Click **Save**.

15 Repeat Steps 12 through 14 to add Network Element access to any other user, as needed.

Index

E

G

H

I

L

M

O

P

R

S

T

U

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

This document includes various trademarks of Cisco Systems, Inc. Please see the Notices section of this document for a list of the Cisco Systems, Inc., trademarks used in this document.

Product and service availability are subject to change without notice.

© 2014, 2015 Cisco and/or its affiliates. All rights reserved.

March 2015

Part Number OL-27168-02