DVD Upgrade Installation Guide for System Release 5.0

with Standalone Application Server

Please Read

Important

Please 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. A listing of Cisco's trademarks can be found at **www.cisco.com/go/trademarks**.

CableCARD, M-Card, OCAP, and OpenCable are trademarks of Cable Television Laboratories, Inc.

Rovi is a trademark of Rovi Corporation.

Other 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. (1009R)

Publication Disclaimer

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

Copyright

Contents

About This Guide

Purpose

This guide provides step-by-step instructions for upgrading a Digital Broadband Delivery System (DBDS), with a standalone Application Server, to System Release (SR) 5.0.

Important: If you are upgrading a DBDS with an integrated Application Server to SR 5.0, you need to use *DVD Upgrade Installation Guide for System Release 5.0 with Integrated Application Server* (part number 4035749) as your guide.

SR 5.0 Features Live Upgrade

The upgrade to SR 5.0 features the Solaris Live Upgrade. Through use of the Live Upgrade, engineers can upgrade the system to SR 5.0 without having to shut down the system processes until activation of the new system software.

How Long to Complete the Upgrade?

The upgrade to SR 5.0 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 4.

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 5.0.

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 DNCS 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
- 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

Requirements

Before beginning the upgrade to SR 5.0, be sure that the site you are upgrading meets these requirements:

- The site you are upgrading uses a standalone Application Server.
- You have at least two DVDs labeled similarly to **SR 5.0 DVD** in order to complete the required backups of the database and the filesystem.
- You must have the DBDS Utilities package SAIdbdsut v6.1.0.3 or SAIdbdsutils v6.3.0.16 or later installed on your system.

Recommended Web Browser

When viewing the Web UIs (WUIs) in SR 5.0, Cisco recommends using Firefox version 3.0.7 for Solaris and version 3.6.16 for both Windows, Linux and Mac operating systems.

Notes:

- Cisco engineers tested the WUIs with Firefox 3.0.7 on the Solaris and version 3.6.16 on the Windows, Linux, and Mac operating systems.
- Firefox version 4.0 is not supported.
- Safari, for Windows or Mac, is not supported.

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

If the site you are upgrading supports a non-SA 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 5.0 upgrade is built upon a Solaris 10 software platform.

Supported Server Platforms

The following DNCS server and Application Server hardware platforms are supported by the SR 5.0 release:

DNCS Server

Platform	Hard Drives	Memory
Sun Fire V445	■ 4 X 73 GB ■ 4 X 146 GB	■ 4 GB w/2 CPUs ■ 8 GB w/4 CPUs
Sun Fire V880	■ 6 X 73 GB ■ 12 X 73 GB ■ 6 X 146 GB ■ 12 X 146 GB	■ 4 GB minimum ■ 8 GB minimum ■ 8 GB minimum ■ 16 GB minimum
Sun Fire V890	■ 6 X 146 GB ■ 12 X 146 GB	■ 8 GB minimum ■ 16 GB minimum

Application Server

Platform	Hard Drives	Memory
Sun Fire V240	2 X 36 GB	512 MB minimum
Sun Fire V245	2 X 73 GB	256 MB minimum

Document Version

This is the second formal release of this document. In addition to minor text and graphic changes, the following table provides the technical changes to this document.

Description	See Topic
Procedures for configuring the loadPIMS and BOSS Web Services were added to the guide.	See the following topics: ■ ***Record the Apache Allow and Deny Directives (Optional)*** (on page 26) ■ ***Configuring the loadPIMS and BOSS Web Services*** (on page 143)

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 5.0

SR 5.0 implements enhanced security which changes the way you will interact with and administer the system. Refer to *DNCS System Release 5.0 Security Configuration Guide* (part number 4034689) 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 DNCS.

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 DNCS or the Application Server 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 DNCS or Application Server (telnet, rlogin, rsh, etc.) are disabled by default.

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

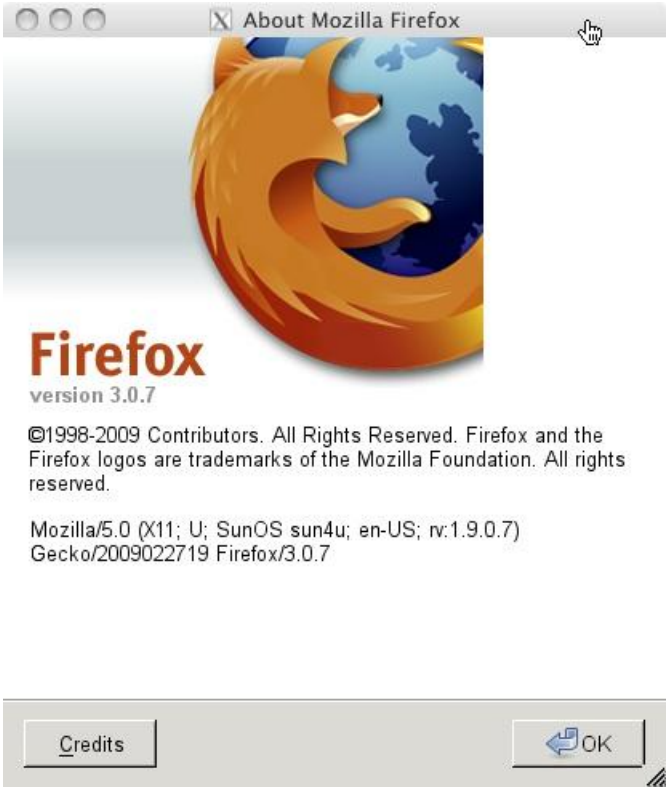
Performance Impact

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

Upgrade Requirements

Before beginning the upgrade to SR 5.0, be sure that the site you are upgrading meets these requirements:

- The site you are upgrading uses a standalone Application Server.
- You have at least two DVDs labeled similarly to **SR 5.0 DVD** in order to complete the required backups of the database and the filesystem.
- You must have the DBDS Utilities package SAIdbdsut v6.1.0.3 or SAIdbdsutils v6.3.0.16 or later installed on your system.
- You must currently be running system release 4.2.0.31p9 or later.
- You must be running version 3.0.x of the Firefox web browser.



Estimated Timeline

The upgrade to SR 5.0 features the Solaris Live Upgrade which provides the ability to "stage" an area on disk 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 5.0 upgrade is built upon a Solaris 10 software platform.

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.

Important: Any features that have been previously enabled or licensed as part of an earlier upgrade do not have to be re-enabled.

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.

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 in ***Run the preUpgradeChecks Script on Each Server in a Standalone System*** (on page 36).

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

2

SR 5.0 Pre-Upgrade Procedures

Introduction

This chapter contains procedures that you should complete before you begin the actual SR 5.0 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 5.0, 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.

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 **su -** and press **Enter**. The **password** prompt appears.
   b. Type the **root** password and press **Enter**.
3. In the second xterm window, type **id** and press **Enter** to verify that you are logged in as dncs user.
   Example:
   ```
   id
   uid=500(dncs) gid=500(dncs)
   ```
4. Is the ID (**uid**) of the second xterm window **dncs**?
   - If **yes**, go to step 5.
   - 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.
   ```
   rsh appservatm
   ```
6. Complete steps 2a and 2b 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 DNCS 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 was 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 step 4.

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

Verify System Communications

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. Type the following command and press **Enter** to run the Doctor Report.
   ```
   doctor -av
   ```
3. Examine the log file created earlier in this chapter 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)
4. Verify that you can manually ping all router interfaces in the system.
5. Type **df -k** and then press **Enter** to verify that you are using no more than 85 percent of the partition capacity of each disk.

   Note: If any disk partition lists a capacity of greater than 85 percent, contact Cisco Services before proceeding.
6. Verify that you can successfully stage a DHCT (OSM and CVT methods).
7. 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**.

8 Verify that you can ping the DHCT.

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

10 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.

11 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

Examine the status of the mirrored disk drives on the Sun Fire V445, V880 or V890 DNCS and the V245 or V240 Application Server, if applicable, prior to the SR 5.0 upgrade.

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 then 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>
.
..
11. c2t5d0 <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 DNCS platform a Sun Fire V880 or V890?

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

```
luxadm  display  FCloop
```

Example:

```
SUNWGS INT FCBPL
Disk Status
Slot  Disks             (Node WWN)
0     On (OK)           500000e0108977d0
1     On (OK)           20000004cf2bf3f1
2     On (OK)           500000e010897d30
3     On (OK)           500000e010898090
4     On (OK)           500000e010894d90
5     On (OK)           2000000c5056c543
6     Not Installed
7     Not Installed
8     Not Installed
```

```
9     Not Installed
10    Not Installed
11    Not Installed
```

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

3 Did the output from step 4 reveal a **Disk Status** of **OK** for all disks?

- If **yes**, continue with step 6.
- If **no**, call Cisco Services for assistance.

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

```
metastat -c
```

Example: The following example shows a Sun Fire V880 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.

```
$ metastat -c
d382              p  2.0GB d520
d381              p  2.0GB d520
d380              p  2.0GB d520
d379              p  2.0GB d520
d378              p  2.0GB d520
d377              p  2.0GB d520
d376              p  2.0GB d520
d375              p  2.0GB d520
d374              p  2.0GB d520
d373              p  2.0GB d520
d372              p  2.0GB d520
d371              p  2.0GB d520
d370              p  2.0GB d520
d369              p  2.0GB d520
d368              p  2.0GB d520
d367              p  2.0GB d520
d366              p  2.0GB d520
d365              p  2.0GB d520
d364              p  2.0GB d520
d363              p  2.0GB d520
d362              p  2.0GB d520
d361              p  2.0GB d520
d360              p  2.0GB d520
d359              p  2.0GB d520
d358              p  2.0GB d520
d357              p  2.0GB d520
d356              p  2.0GB d520
d355              p  2.0GB d520
d354              p  2.0GB d520
d353              p  2.0GB d520
d352              p  2.0GB d520
```

```
d351              p  2.0GB d520
d350              p  1.0GB d520
    d520          m  238GB d720 d420
        d720      s  238GB c2t10d0s0 c2t11d0s0 c2t12d0s0
c2t13d0s0
        d420      s  238GB c1t2d0s0 c2t3d0s0 c2t4d0s0 c2t5d0s0
d507              m  8.0GB d707 d407
    d707          s  8.0GB c2t8d0s5
    d407          s  8.0GB c1t0d0s5
d503              m  8.0GB d403
    d403          s  8.0GB c1t0d0s3
d501              m  8.0GB d701 d401
    d701          s  8.0GB c2t8d0s1
    d401          s  8.0GB c1t0d0s1
d500              m  8.0GB d400
    d400          s  8.0GB c1t0d0s0
d510              m   59GB d710 d410
    d710          s   59GB c2t9d0s0
   d410          s   59GB c1t1d0s0
d703              s  8.0GB c2t8d0s3
d700              s  8.0GB c2t8d0s0
```

5 Examine each device and submirror. Is each device in good working order?

- If **yes**, go to step 6.
- If **no**, call Cisco Services for assistance.

6 Repeat steps 1 through 5 on the Application Server and any LIONN servers on the system.

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.

The list of default key files is located on the installation DVD in the following file:

`/cdrom/cdrom/sai/backup_restore/keyFiles.include`

With SR 5.0 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

On a sheet of paper, create a list of special key files that you will back up. 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/<date_time> 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 after the upgrade, or copy the file to the /dvs/admin/sysinfo/<date_time> directory created by the preUpgradeChecks script.

  Note: 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.

  CAUTION:

  Several files are inadvertently not preserved in the default keyfiles list maintained on the DVD. You will need to add the files listed in the next bullet to your key files list when you are prompted during the Live Upgrade. You can also add them to your kfs.out file if you chose to create this. CR CSCzk46462 addresses this issue.

- If you are using the loadPIMS or BOSS Web services, be certain that the /etc/opts/certs/ path is included in the keyfiles list for the SR 5.0 upgrade.
- Add the following files to your kfs.out file or to the key files list when prompted during the Live Upgrade.
  - dvs/dncs/etc/PopulateGQIBlockList.sh
  - /export/home/dncs/SGFrequencies.dat
  - /dvs/admin/sysinfo
  - /dvs/rfgwftp

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 you 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 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]
   ```
4. Add the /tftpboot/backup.[DNCS version] directory to your list of key files to be backed up.

Check the EAS Configuration—Pre-Upgrade

Checking the EAS Configuration

Before installing the SR 5.0 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 4004455)**.**

Note: You will check the EAS configuration after the installation of the SR 5.0 software, as well.

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.

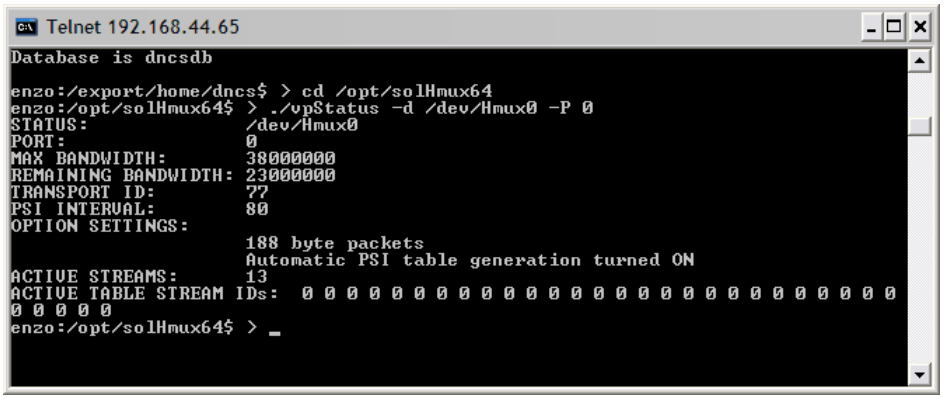
2 Record the **Session Count** total in the space provided. _____

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**, is your system currently running SR 5.0 AND are your BFS sessions Multicast?
  - If **yes**, go to step 4.
  - If **no** (to either condition), go to the next procedure in this chapter.

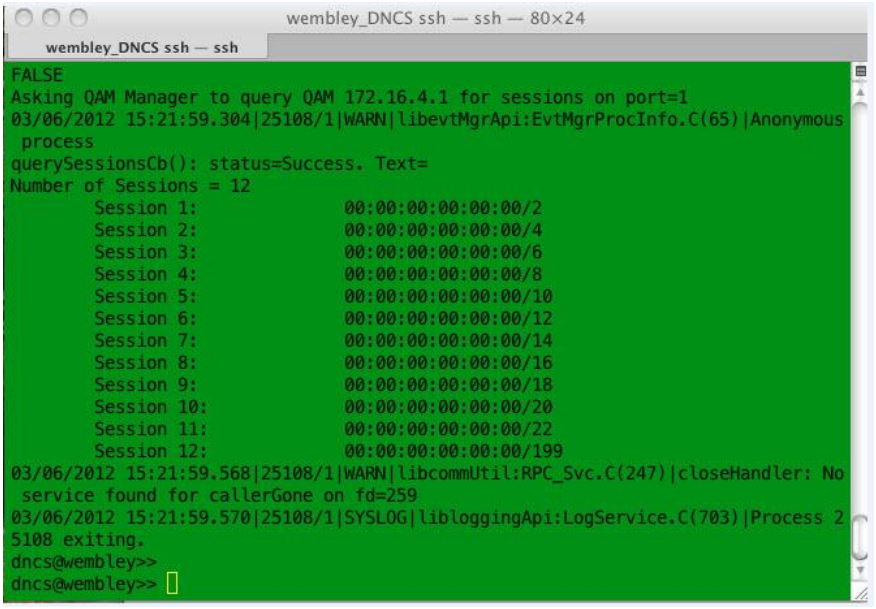
4 Follow these instructions to verify your BFS sessions.

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

```
auditQam -query <GigE Qam IP> <port>
```

Note: Replace <GigE Qam IP> with the IP address of the BFS Gqam. Replace <port> with to port/channel the BFS sessions are built on. In this example the multcast BFS sessions are built on the last channel on the Gqam (port 16).

Example: `auditQam -query 172.16.4.23 16`



b On the DNCS WUI, follow this path: **DNCS->Network Element Provisioning->QAM**.

c Click the **Filter By Field** menu and select **All**.

d Click **Show**. All provisioned QAMs are displayed.

e Click the BFS Gqam. The Edit QAM <qam name> WUI appears.

f In the top left corner, click **Multicast Sessions**. The Multicast Digital Session Definition for <qam name> is WUI appears.

g Verify that the number of multicast sessions match the number on the Gqam.

5 Do the number of **Active Streams** match the number of sessions built on the BFS QAM?

- If **yes**, go to the next procedure in this chapter.
- If **no**, call Cisco Services and inform them about the discrepancy.

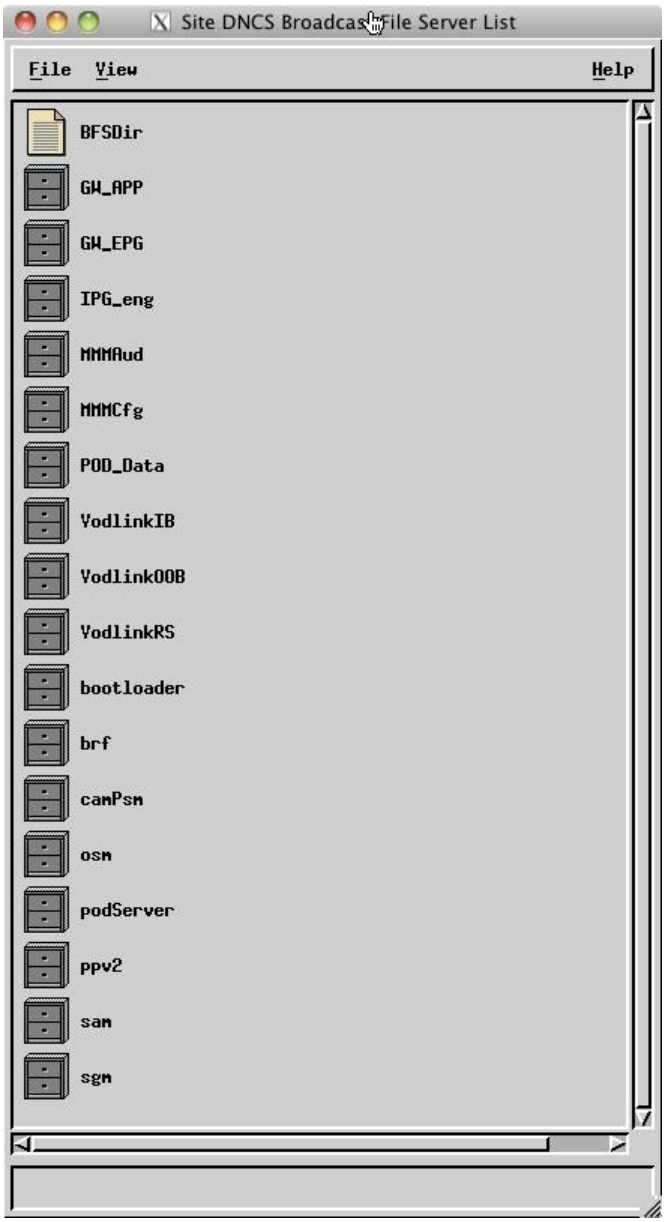
Record Third-Party BFS Application Cabinet Data

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.

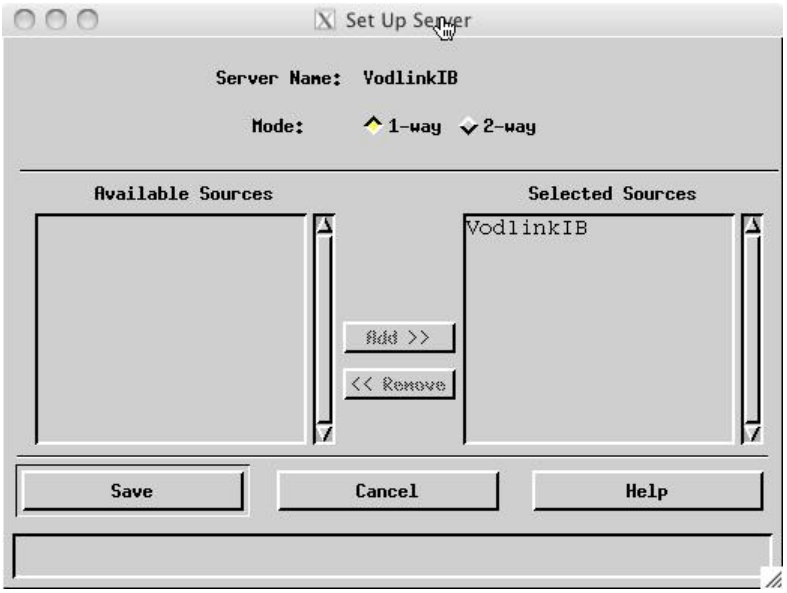
Note: You do not need to record this data for all BFS application cabinets, only those that are NOT created by the DNCS or the Application Server.

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 then click **File** and select **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 Repeat steps 3 through 5 for every third-party BFS application cabinet on the Broadcast File Server List window.

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

Record the Apache Allow and Deny Directives (Optional)

Complete this procedure only if you are using the loadPIMS or BOSS Web services.

In this procedure, you will examine several files for allow and deny directives, which you should record in a manner most convenient for you. You will need this information later, so be certain to record it accurately.

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

2 Type the following command and press **Enter** to open, for viewing, the /etc/apache2/conf/boss.http file.

```
more /etc/apache2/conf/boss.http
```

3 Record the allow and deny directives listed in the file.

Example: The following is an example of the allow and deny directives that you should record:

```
Allow from 147.191.126.36
Allow from 147.191.126.37
Allow from 147.191.126.38
Allow from 147.191.126.39
Allow from 24.40.12.107
Allow from 24.40.12.108
Allow from 24.40.12.52
Allow from 24.40.13.104
Allow from 24.40.13.105
Deny from 192.168.0.0/16
Deny from 64.0.0.0/8
```

4 Close the file when you are finished.

5 Repeat steps 2 through 4 with the **`/etc/apache2/conf/loadPIMS.https`** file.

Mount the DVD

Depending upon your current Solaris patch set, the DVD may not mount automatically. Use the following chart to determine what method to use to mount the DVD.

DNCS Release	SAIpatch Set	DVD Mount Method
SR 4.2	4.2.1.6 and older	Manually mount
SR 4.2	4.2.1.10	Automount
SR 4.3	4.3.0.1	Manually mount
SR 5.0	10.20100322.2	Automount

Use the appropriate DVD mounting method for your current installation.

Important:

- If you only have one DVD, you will need to complete this procedure each time you move the DVD from one system to another.
- To unmount a DVD, type **cd /** and then type **`umount /cdrom/cdrom`**.

Note: You should have an SR 5.0 DVD for each server that you are upgrading. Repeat this procedure for each DNCS and RNCS server that you are upgrading.

Automount the DVD

Follow these steps to automount the DVD.

1. Inspect the DVD to ensure that it is clean. There should be no smudges on the DVD. Some small, light scratches may be present; this is fine.
2. Insert the system release installation DVD into the CD-ROM drive of the server.
3. Did the DVD automount?
   - If **yes**, continue with the next procedure in this chapter.
   - If **no**, as **root** user, type the following command and press **Enter** to restart the volfs process.

     `svcadm restart volfs`

     Note: If the DVD still does not automount, contact Cisco Support for assistance.

Manually Mount the DVD

Follow these steps to manually mount the DVD.

1. Inspect the DVD to ensure that it is clean. There should be no smudges on the DVD. Some small, light scratches may be present; this is fine.
2. From a **root** xterm window on each server that you are upgrading, type the following command and press **Enter** to stop the Solaris Volume Manager.
   ```
   svcadm -v disable -s volfs
   ```
3. Type the following command and press **Enter** to check for the presence of the DVD drive and to record the disk from the Logical Node entry.
   ```
   rmformat -l
   ```
   Note: The "l" in the command is a lowercase L.
4. Record the disk entry in the space provided. _____
5. Insert the system release installation DVD into the CD-ROM drive of the server.
6. Type the following command and press **Enter** to create the mount point for the DVD.
   ```
   mkdir -p /cdrom/cdrom
   ```
7. Type the following command and press **Enter** to mount the DVD.
   Important: Although the rmformat command shows the device as /dev/rdsk/c0t0d0s2, use /dev/dsk/c0t0d0s0 for the mount command. You may need to replace "c0t0" depending on your hardware. For example, if rmformat shows the logical node as /dev/rdsk/c0t1d0s0, you would use /dev/dsk/c0t1d0s0 with the mount command.
   ```
   mount -F hsfs /dev/dsk/[/dev/dsk/[disk]] /cdrom/cdrom
   ```
   Note: Substitute the appropriate device syntax for c#t#d#s0 from the rmformat -l output you recorded in step 4.
   Example: `mount -F hsfs /dev/dsk/c0t0d0s0 /cdrom/cdrom`
   Troubleshooting Tip: If /cdrom/cdrom is busy, make sure the mount point is not already in use or that you are not already in the /cdrom directory. You cannot mount to cdrom if you are in the directory.
8. Type the following command and press **Enter** to verify that the OS.flar file can be read.
   ```
   dd if=/cdrom/cdrom/sai/flash_archives/OS.flar of=/dev/null
   ```
   Notes:
   - This command may take 15 to 20 minutes to complete.
   - If this command fails, contact Cisco Services for assistance.

Back Up the File Systems and Database

The upgrade scripts do not back up the DNCS and Application Server file systems or database. Prior to beginning the upgrade, back up the file systems and database manually. Based upon the data on your system, the backup could take between one and six hours to complete. Be sure to allow sufficient time for the system to complete the backup before you enter the maintenance window.

Choose one of the following options:

- If you are performing a standard file system backup to tape, complete the instructions that follow.
- If your backup is not standard, then follow the instructions in *DBDS Backup and Restore Procedures For SR 2.2 Through 4.3 User Guide* (part number 4013779) to back up the file systems.

1. Insert the blank DNCS file system tape into the tape drive.
2. From the **root** xterm window, type the following command and press **Enter**. The DNCS file systems are backed up to the tape.
   `/cdrom/cdrom/sai/backup_restore/backupFileSystems -v`
3. When the backup has completed, remove and label the file system tape and then insert the blank database tape.
4. As **root** user type the following command and press **Enter**. You are prompted to **mount tape 1 and press Return**.
   `/cdrom/cdrom/sai/backup_restore/backupDatabase -v`
5. Verify that the database tape is in the tape drive and press **Enter**. The database backup continues.
6. When the backup has completed remove and label the database tape.
7. Does the system you are upgrading have a standalone Application Server?
   - If **yes**, insert the Application Server file system tape in the DNCS tape drive and continue with step 8.
   - If **no** (you are upgrading an integrated Application Server), skip the rest of this procedure.
8. Type the following command (on one line) and press **Enter** to copy the backup_restore directory from the DVD to the Application Server.
   `rcp -r /cdrom/cdrom/sai/backup_restore appservatm:/dvs/backups`
9. Type the following command on the DNCS and press **Enter** to determine what drive number to use.
   `ls /dev/rmt`
   Note: The tape drive number may vary from system to system.

10 On the Application Server, as **root** user, type (on one line) one of the following commands and press **Enter**.

- If your Application Server is a V245 or V240, type the following command.
  `/dvs/backups/backup_restore/backupFileSystems -v -r dncsatm:/dev/rmt/0cn`
- If your Application Server is a Sunblade 150 or an Ultra 5, type the following command.
  `/dvs/backups/backup_restore/backupFileSystems_nomds -v -r dncsatm:/dev/rmt/0cn`

11 When the backup is complete, remove the tape and label it appropriately.

Delete DBDS Process Core File Directories

The DBDS 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 old DBDS software. These core file directories should be deleted before beginning the Live Upgrade. This section provides instructions for deleting the DBDS core files directories.

1. As 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 the standalone Application Server and any LIONN servers on the system. The process core files are located in the following system directories:
   - **DNCS with a supported Application Server: `/dvs/dncs/tmp/corefiles`**
   - **Application Server: `/dvs/appserv/tmp/corefiles`**
   - **LIONN: `/dvs/lionn/tmp/corefiles`**
   - **DNCS with an integrated Application Server: `/dvs/dncs/tmp/corefiles and /dvs/appserv/tmp/corefiles`**

3

SR 5.0 DNCS, RNCS, and Standalone V245/V240 Application Server Upgrade

Introduction

This chapter contains procedures to upgrade the DNCS, RNCS, and the standalone V245/V240 Application Server.

Notice to Installers

Follow these instructions if you are upgrading a system that has a standalone V245 or V240 Application Server.

You should have an SR 5.0 upgrade DVD mounted on each server: DNCS, Application Server, and RNCS, if applicable. You will run the commands in this chapter on all servers being upgraded at the same time. That is, if you have a DNCS and an Application Server with one RNCS, you will run these commands on all three servers simultaneously.

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

Mount the DVD

Depending upon your current Solaris patch set, the DVD may not mount automatically. Use the following chart to determine what method to use to mount the DVD.

DNCS Release	SAIpatch Set	DVD Mount Method
SR 4.2	4.2.1.6 and older	Manually mount
SR 4.2	4.2.1.10	Automount
SR 4.3	4.3.0.1	Manually mount
SR 5.0	10.20100322.2	Automount

Use the appropriate DVD mounting method for your current installation.

Important:

- If you only have one DVD, you will need to complete this procedure each time you move the DVD from one system to another.
- To unmount a DVD, type **cd /** and then type **`umount /cdrom/cdrom`**.

Note: You should have an SR 5.0 DVD for each server that you are upgrading. Repeat this procedure for each DNCS and RNCS server that you are upgrading.

Automount the DVD

Follow these steps to automount the DVD.

1. Inspect the DVD to ensure that it is clean. There should be no smudges on the DVD. Some small, light scratches may be present; this is fine.
2. Insert the system release installation DVD into the CD-ROM drive of the server.
3. Did the DVD automount?
   - If **yes**, continue with the next procedure in this chapter.
   - If **no**, as **root** user, type the following command and press **Enter** to restart the volfs process.

     `svcadm restart volfs`

     Note: If the DVD still does not automount, contact Cisco Support for assistance.

Manually Mount the DVD

Follow these steps to manually mount the DVD.

1. Inspect the DVD to ensure that it is clean. There should be no smudges on the DVD. Some small, light scratches may be present; this is fine.
2. From a **root** xterm window on each server that you are upgrading, type the following command and press **Enter** to stop the Solaris Volume Manager.
   ```
   svcadm -v disable -s volfs
   ```
3. Type the following command and press **Enter** to check for the presence of the DVD drive and to record the disk from the Logical Node entry.
   ```
   rmformat -l
   ```
   Note: The "l" in the command is a lowercase L.
4. Record the disk entry in the space provided. _____
5. Insert the system release installation DVD into the CD-ROM drive of the server.
6. Type the following command and press **Enter** to create the mount point for the DVD.
   ```
   mkdir -p /cdrom/cdrom
   ```
7. Type the following command and press **Enter** to mount the DVD.
   Important: Although the rmformat command shows the device as /dev/rdsk/c0t0d0s2, use /dev/dsk/c0t0d0s0 for the mount command. You may need to replace "c0t0" depending on your hardware. For example, if rmformat shows the logical node as /dev/rdsk/c0t1d0s0, you would use /dev/dsk/c0t1d0s0 with the mount command.
   ```
   mount –F hsfs /dev/dsk/[/dev/dsk/[disk]] /cdrom/cdrom
   ```
   Note: Substitute the appropriate device syntax for c#t#d#s0 from the rmformat –l output you recorded in step 4.
   Example: `mount –F hsfs /dev/dsk/c0t0d0s0 /cdrom/cdrom`
   Troubleshooting Tip: If /cdrom/cdrom is busy, make sure the mount point is not already in use or that you are not already in the /cdrom directory. You cannot mount to cdrom if you are in the directory.
8. Type the following command and press **Enter** to verify that the OS.flar file can be read.
   ```
   dd if=/cdrom/cdrom/sai/flash_archives/OS.flar of=/dev/null
   ```
   Notes:
   - This command may take 15 to 20 minutes to complete.
   - If this command fails, contact Cisco Services for assistance.

Run the preUpgradeChecks Script on Each Server in a Standalone System

Important: If you are migrating to an integrated Application Server, **STOP**. You should be following the instructions in *DVD Upgrade Installation Guide for System Release 5.0 with Integrated Application Server* (part number 4035749).

Running the preUpgradeChecks Script on the DNCS and RNCS

This section describes how to run an automated system check to determine if your system is acceptable for an SR 5.0 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.

CAUTION:

Important: A feature of the preUpgradeChecks script collects system information required to reconstruct the system should the upgrade fail. This information will be saved to the /dvs/admin/sysinfo directory on each server; therefore, make sure you add this file to the default Key Files list when prompted during the live upgrade of the system. **CR122820** addresses this issue.

Notes:

- The Sun Blade 150 and Ultra 5 Application Servers are not supported hardware platforms for SR 5.0 upgrades. You have to either upgrade the server to a supported platform (Sun Fire V245 or V240) or convert to an integrated Application Server before you can continue with the upgrade.
- If your system includes a Sun Blade 150 or an Ultra5 Application Server and you do NOT want to migrate to a supported Application Server, you need to be following the upgrade instructions in *DVD Upgrade Installation Guide for System Release 5.0 with Integrated Application Server* (part number 4035749).

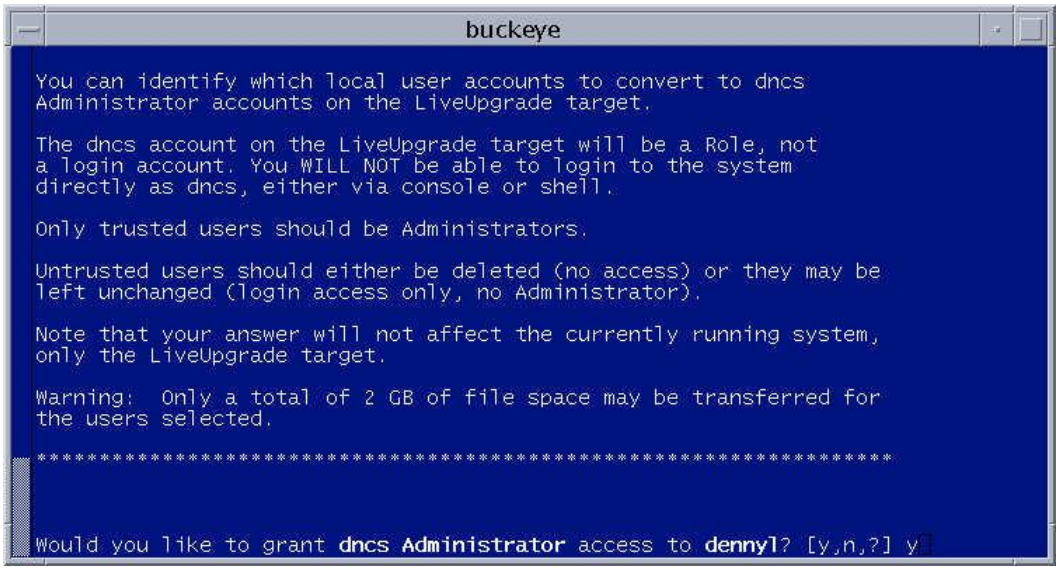
1 From the **root** xterm window, type the following command and then press **Enter.**

```
/cdrom/cdrom/sai/scripts/preUpgradeChecks
```

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

2 Type **y** and press **Enter**. The script validates the system's readiness for an upgrade to SR 5.0 and reports any issues.

Example:



3 Are any 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.

- If **yes**, the **Would you like to grant dncs Administrator access to [username]?** message appears. Go to step 4.

  Important: Do NOT grant Administrator access to the "backup" user account. If your system has a "backup" user account, answer **no** for this user account.
- If **no** (the script continues), skip to step 7.

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

- If **yes**, type **y** and press **Enter**. Go to step 6.
- If **no**, type **n** and press **Enter**. The **Do you want to remove [username] from the upgrade target?** message appears. Go to step 5.

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

- If **yes**, type **y** and press **Enter**. Go to step 6.

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

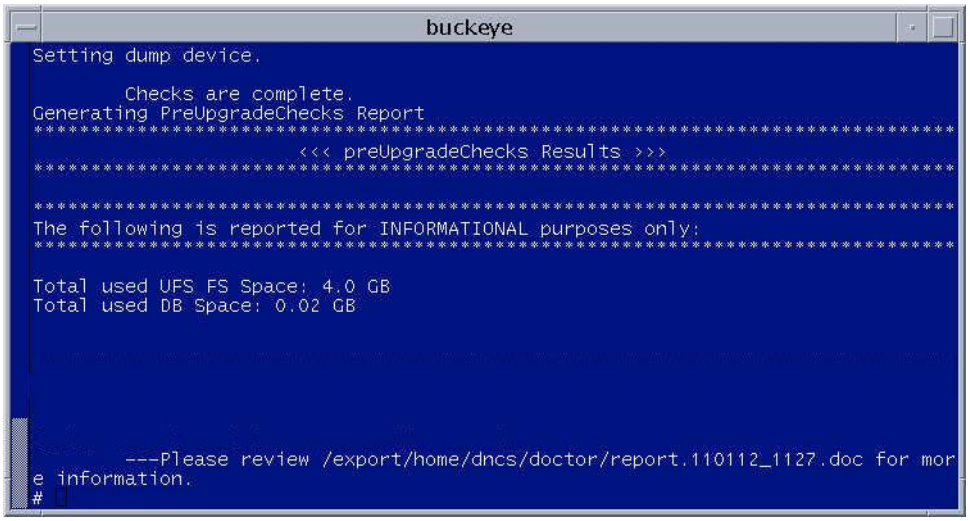
  Note: The /export/home/[username] directory will not be preserved after the upgrade.
- If **no**, type **n** and press **Enter**. Go to step 6.

6 Did the **Would you like to grant dncs Administrator access to [username]?** message re-appear?

- If **yes**, repeat steps 3 through 5 for each user for whom you are prompted to grant dncs Administrator privilege.
- If **no**, go to step 7.

7 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 8.

8 Type the following command and press **Enter** to change directory to the optional_checks directory on the DVD.

```
cd /cdrom/cdrom/sai/scripts/LU/PUC/optional_checks
```

9 Type the following command and press **Enter** to run the checkDupGigeIP scripts.

```
./checkDupGigeIP
```

Note: Review the output the script produces if any duplicates are found. These need to be corrected before upgrading.

10 Type the following command and press **Enter** to run the checkimage.sh script.

```
./checkimage.sh
```

Note: Review the output the script produces. The output file is: /dvs/dncs/tmp/imagecheck.<datetime>. Correct any invalid characters before upgrading.

11 Type the following command and press **Enter** to run the sourceConflicts.sh script.

```
./sourceConflicts.sh
```

Note: Review the output the script produces. The output file is: /tmp/sourceConflicts.<pid>.out. Correct any invalid source conflicts before upgrading.

12 Type the following command and press **Enter** to run the MultiSpace script.
```
./MultiSpace -C
```
Note: Review the output the script produces. Log files are located in /var/log/preUpgradeChecks/MultiSpace. If any entries with multiple spaces are found, they must be corrected before upgrading.

13 Type the following command and press **Enter** to run the dup_smpkgauth script.
```
./dup_smpkgauth -C
```
Notes:

- This script can take from 20 minutes to over an hour to run, depending upon the size of the sm_pkg_auth table.
- Review the output the script produces. Log files are located in /var/log/preUpgradeChecks/smpkgauth. If any duplicate are found, they must be corrected before upgrading.

14 If you have RNCS server(s) to upgrade, repeat this procedure on each RNCS server.

Running the preUpgradeChecks on the Sun Fire V245 or V240 Application Server

This section describes how to run an automated system check on the Application Server to determine if your system is acceptable for an SR 5.0 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.

CAUTION:

A feature of the preUpgradeChecks script collects system information required to reconstruct the system should the upgrade fail. This information will be saved to the /dvs/admin/sysinfo directory on each server; therefore, make sure you add this file to the default Key Files list when prompted during the live upgrade of the system. **CR122820** addresses this issue.

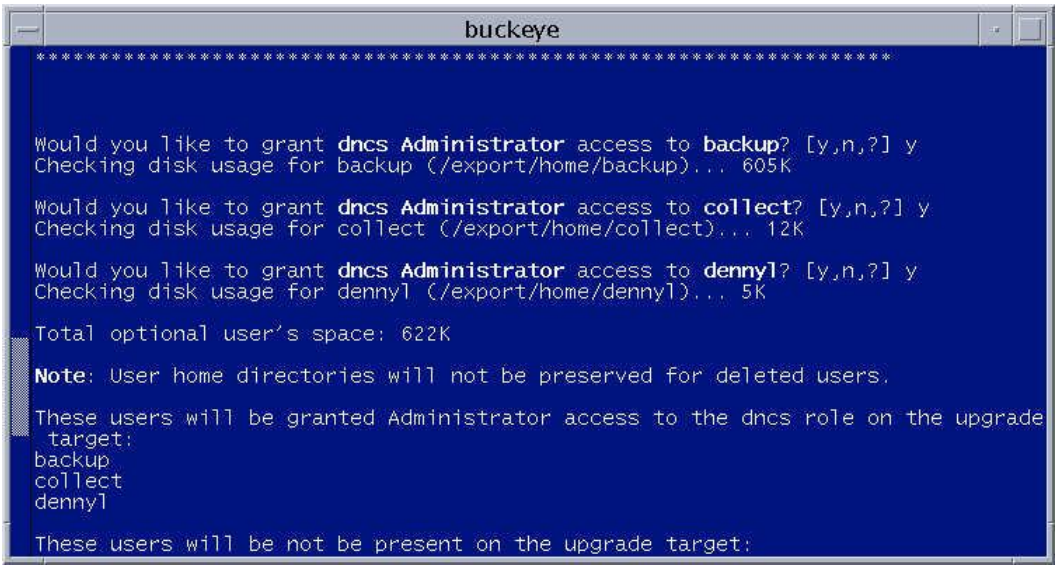
Important: This procedure must be performed and the system check must "pass" in order to continue with this upgrade.

1 From the **root** xterm window on the Application Server, type the following command and press **Enter** to set up the proper environment.
```
. /dvs/appserv/bin/appservSetup
```

2 Type the following command and press **Enter.**
```
/cdrom/cdrom/sai/scripts/preUpgradeChecks
```
Result: The **Do you wish to continue?** message appears.

3 Type **y** and press **Enter**. The script validates the system's readiness for an upgrade to SR 5.0 and reports any issues.

Example:



4 Have you created user accounts on your 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.

- If **yes**, the **Would you like to grant dncs Administrator access to [username]?** message appears. Go to step 5.
- If **no**, go to step 8.

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

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

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

- If **yes**, type **y** and press **Enter**. Go to step 7.

  Notes:

  – If there is a "backup" user account, answer **yes** to remove the home directory for this user.

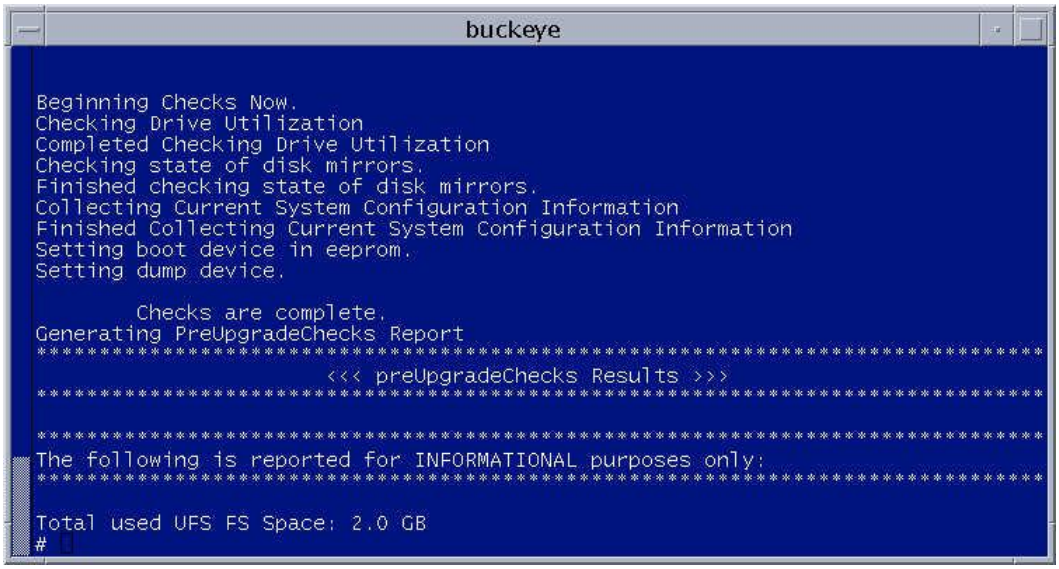
  – The /export/home/[username] directory will not be preserved after the upgrade.
- If **no**, type **n** and press **Enter**. Go to step 7.

7 Did the **Would you like to grant dncs Administrator access to [username]?** message re-appear?

- If **yes**, repeat steps 4 through 6 for each user for whom you are prompted to grant dncs Administrator privileges.
- If **no**, go to step 8.

8 Did any errors or warnings appear?

Example:



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

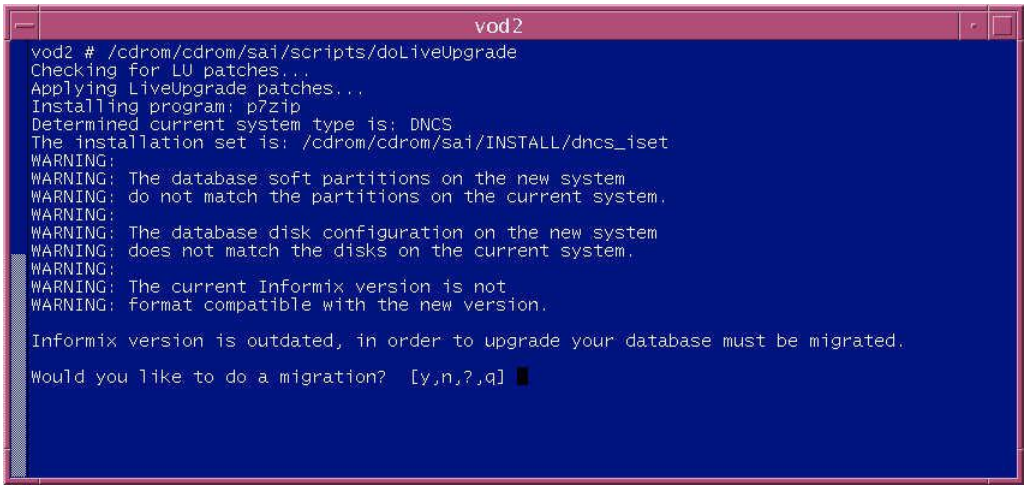
  Note: If errors continue to persist or if you need assistance with correcting an issue, contact Cisco Services.

- If **no**, continue with the next procedure of this chapter.

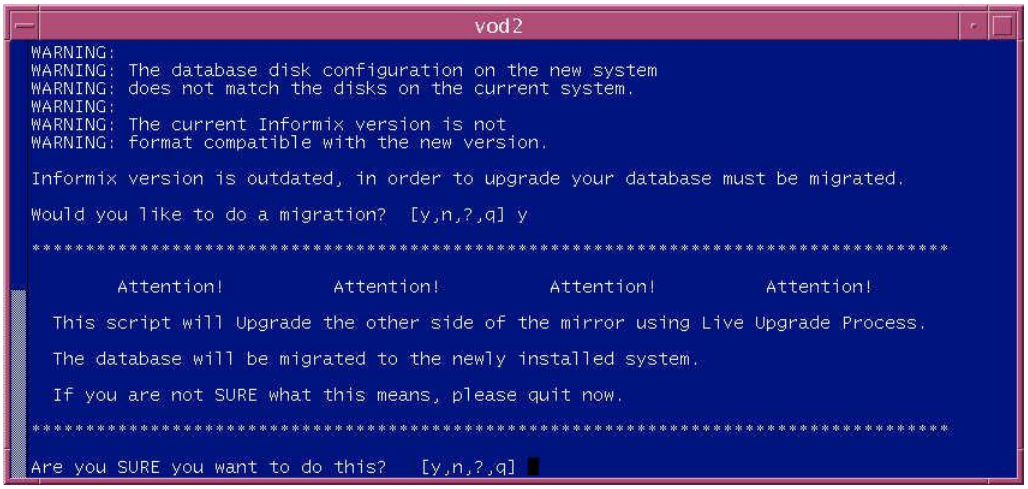
Upgrade the DNCS

1 From the **root** xterm window, type the following command and press **Enter**. The screen updates with messages detailing progress through the Live Upgrade and displays the **Would you like to do a migration?** message.

`/cdrom/cdrom/sai/scripts/doLiveUpgrade`



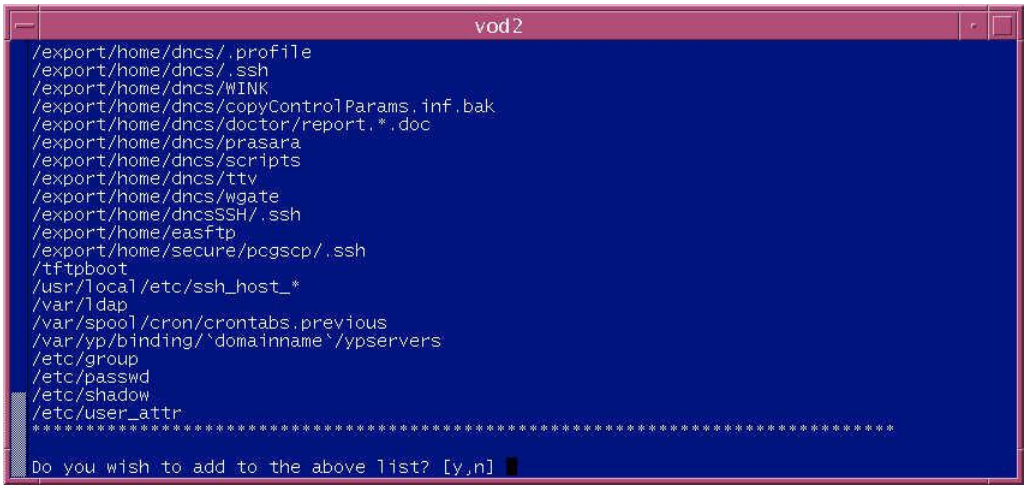
2 Type **y** and then press **Enter**. The **Are you SURE you want to do this?** message appears.



3 Type **y** and then press **Enter**. The system executes the following tasks:

- Detaches non database-mirrors
- Creates temporary file systems
- Updates system configuration files
- Extracts the image

  Note: This will take approximately 20 minutes.
- Displays the default key file list and the **Do you wish to add to the above list?** message



4 Do you have additional files or directories to add?

Important: We recommend that you add **/dvs/admin/sysinfo** to your additional key files and directories list because this file contains system and network information that is important for post-installation procedures, as well as to reconstruct the system should an upgrade fail. **CR 122820** addresses this issue.

- If **yes**, type **y** and then press **Enter**. Then, add the absolute path of 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**.

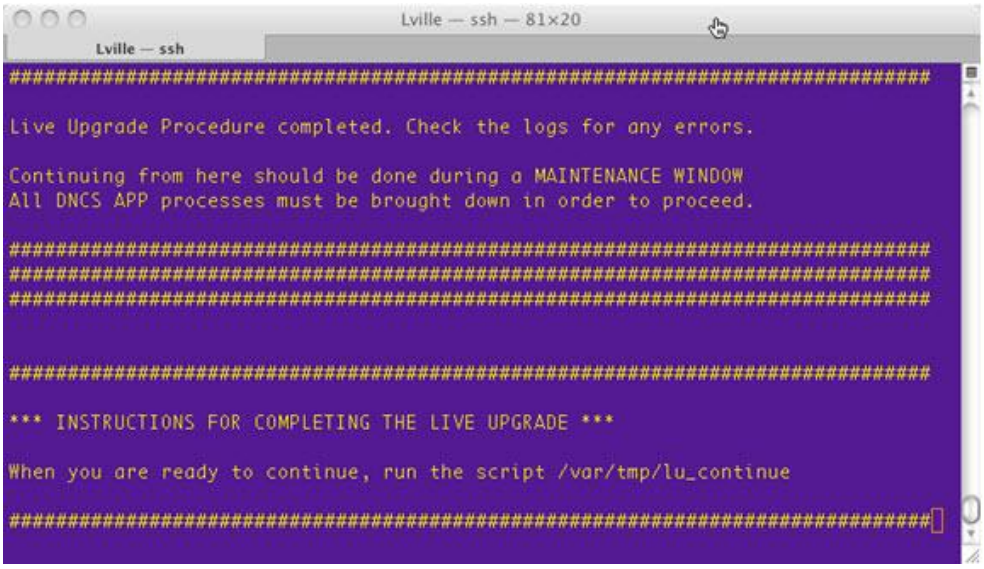
5 Do you have files or directories that you want to delete from the list?

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

  Note: 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.

6 Type **y** and press **Enter**. The key files are backed up and the screen updates with the following message.



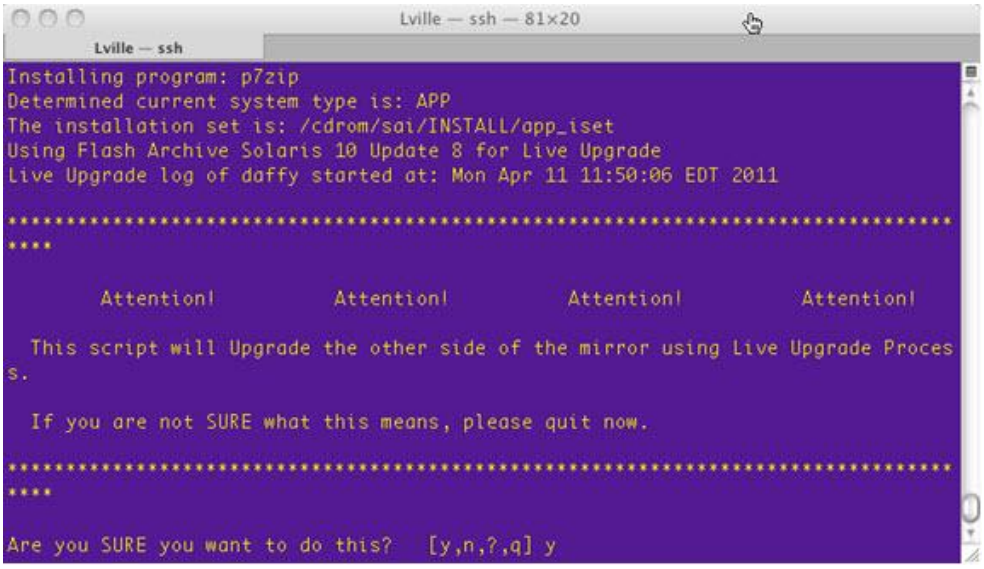
Important: Do *not* proceed with the lu_continue script until you are in a maintenance window.

Upgrade the Standalone Application Server

Follow these instructions to upgrade a standalone Sun Fire V240 or V245 Application Server.

1 From the **root** xterm window on the Application Server, type the following command and press **Enter**. The screen updates with messages about progress through the Live Upgrade and displays a **Are you sure you want to do this?** message.

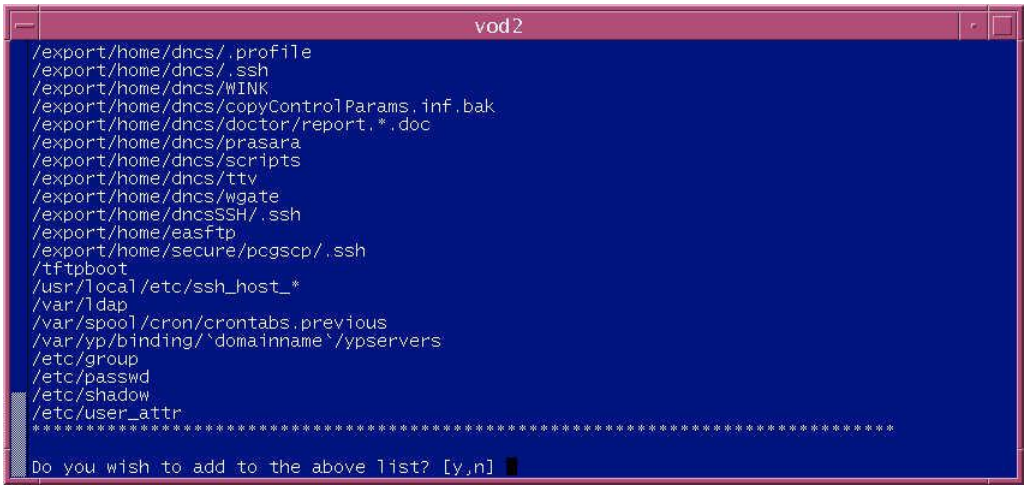
`/cdrom/cdrom/sai/scripts/doLiveUpgrade`



2 Type **y** and press **Enter**. The system executes the following tasks:

- Detaches non database-mirrors
- Creates temporary file systems
- Updates system configuration files
- Extracts the image

  Note: This will take approximately 20 minutes.
- Displays the default key file list and the **Do you wish to add to the above list?** message



3 Do you have additional files or directories to add?

Important: We recommend that you add **/dvs/admin/sysinfo** to your additional key files and directories list because this file contains system and network information that is important for post-installation procedures, as well as to reconstruct the system should an upgrade fail. **CR 122820** addresses this issue.

- If **yes**, type **y** and then press **Enter**. Then, add the absolute path of 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**.

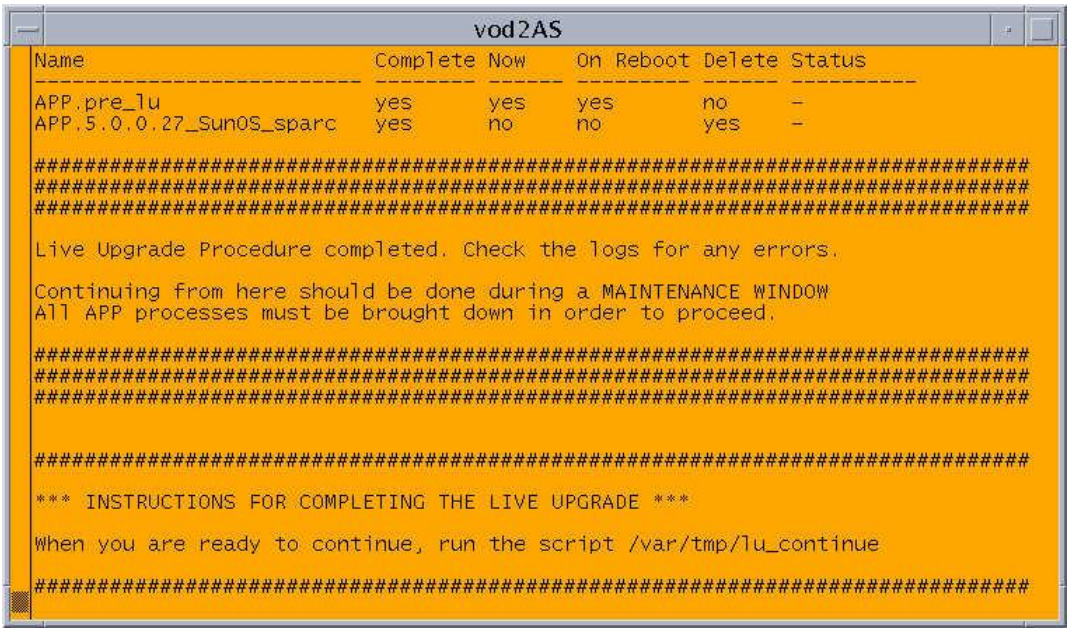
4 Do you have files or directories that you want to delete from the list?

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

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

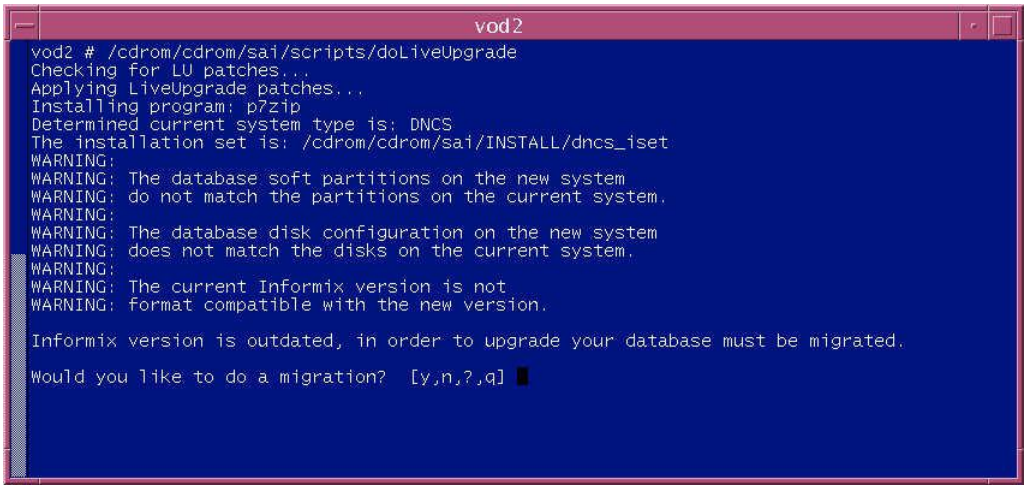
- If **no**, type **n** and press **Enter**. Add the absolute path of the needed files or directories.

Result: The key files are backed up and the screen updates with the following message.

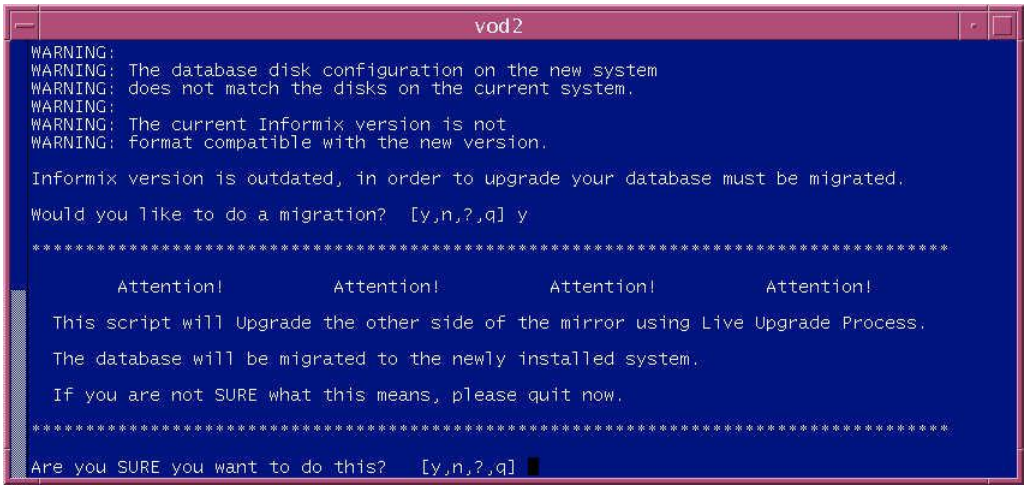


Upgrade the RNCS

1 From the **root** xterm window on the RNCS, type the following command and press **Enter**. The screen updates with messages detailing progress through the Live Upgrade and displays the **Would you like to do a migration?** message.
`/cdrom/cdrom/sai/scripts/doLiveUpgrade`



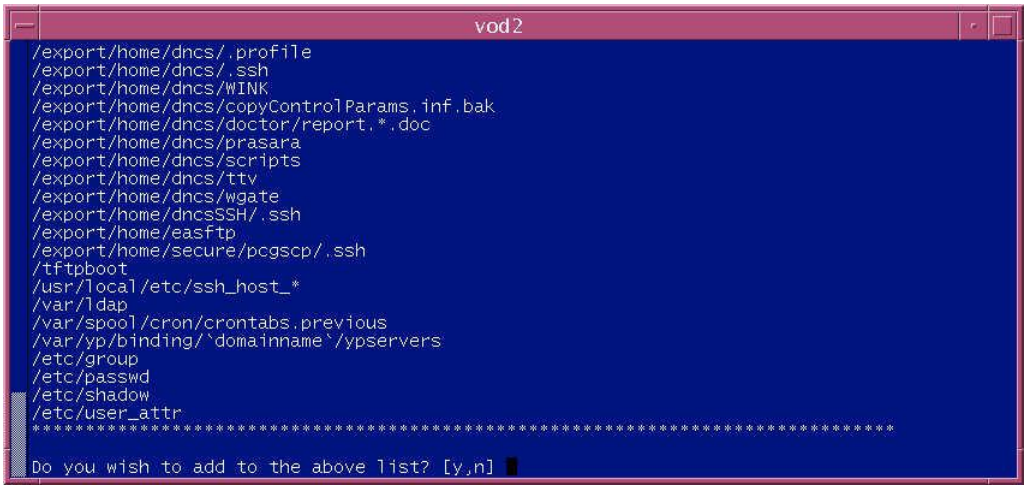
2 Type **y** and then press **Enter**. The **Are you SURE you want to do this?** message appears.



3 Type **y** and then press **Enter**. The system executes the following tasks:

- Detaches non database-mirrors
- Creates temporary file systems
- Updates system configuration files
- Extracts the image

  Note: This will take approximately 20 minutes.
- Displays the default key file list and the **Do you wish to add to the above list?** message



4 Do you have additional files or directories to add?

Important: We recommend that you add **/dvs/admin/sysinfo** to your additional key files and directories list because this file contains system and network information that is important for post-installation procedures, as well as to reconstruct the system should an upgrade fail. **CR 122820** addresses this issue.

- If **yes**, type **y** and then press **Enter**. Then, add the absolute path of 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**.

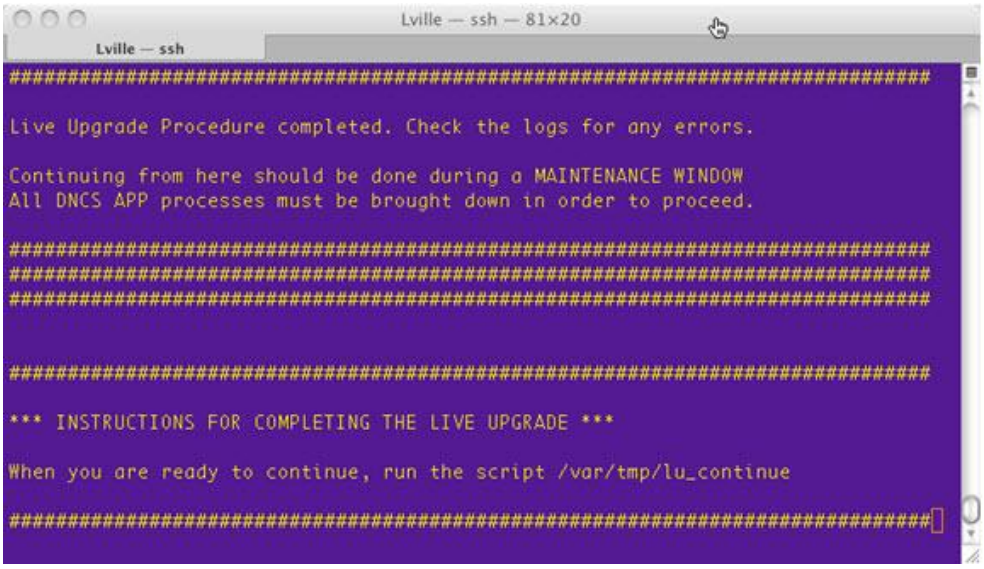
5 Do you have files or directories that you want to delete from the list?

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

  Note: 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.

6 Type **y** and press **Enter**. The key files are backed up and the screen updates with the following message.



Important: Do *not* proceed with the lu_continue script until you are in a maintenance window.

CAUTION:
You need to be in a maintenance window to complete the remaining procedures associated with this upgrade.

4

Maintenance Window Activities

Introduction

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

In This Chapter

Stop System Components

Maintenance Window

CAUTION:

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

Suspend Billing Transactions

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

Stop All Third-Party Utilities

All third-party utilities should be stopped for the upgrade to succeed. Consult with the system operator about which third-party utilities may be running on the system and then 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 the next procedure, ***Stopping the System Components*** (on page 53).

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 6-8 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 From the BIG List window, select the **BIG** and then click **File** and select **Delete**. A confirmation window appears.

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

15 Close the BIG List window.

Stopping the System Components

Follow these instructions to stop the system components.

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** Type the following command and press **Enter**. The initd process on the Application Server is shut down.
     ```
     appKill
     ```
   - **c** Type the following command and press **Enter** to determine if the processes have stopped. The processes are stopped when there are no processes listed in the output.
     ```
     pgrep -fl dvs
     ```
   - **d** Change to **root** user on the 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 processes have stopped. The processes are stopped when there are no processes listed in the output.
   ```
   siteCmd [lionn hostname]pgrep -fl dvs
   ```

   d From the **root** 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
   ```

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 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 processes have stopped. The processes are stopped when there are no processes listed in the output.
   ```
   pgrep -fl dvs
   ```
   Note: The following entries will always appear in the output of this command and indicate that it is safe to proceed with the next procedure in this chapter.
   – /usr/sbin/dtrace -qws /dvs/dncs/etc/app_crash/app_crash_global.d
   – /dvs/dncs/bin/dncsResMon

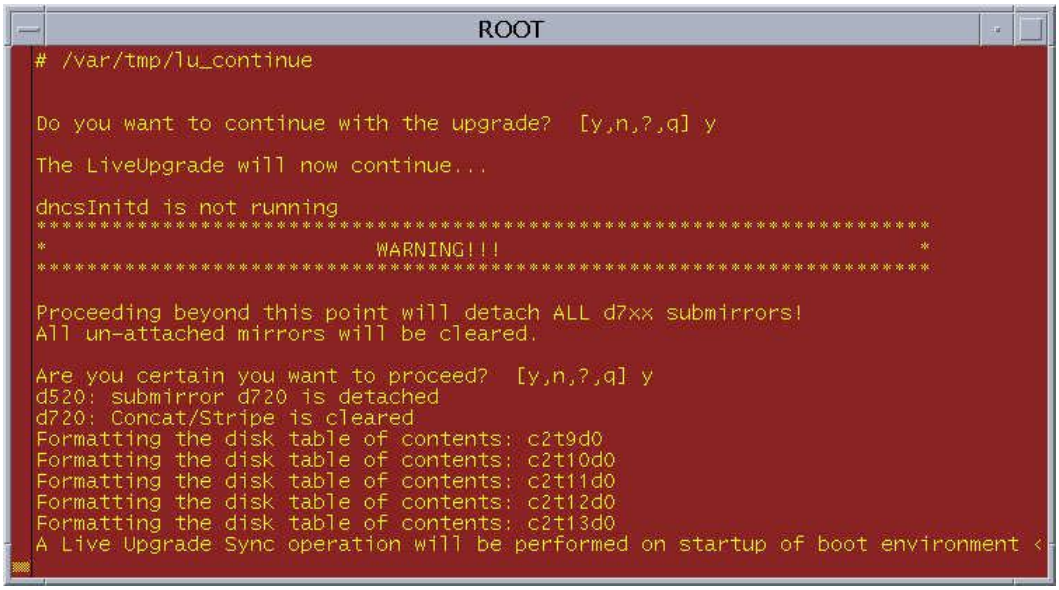
   d From the **root** xterm window, type the following command and press **Enter** to disable cron jobs.
   ```
   svcadm –v disable –s cron
   ```

Continue with the SR 5.0 Upgrade of the DNCS

1 From the **root** xterm window, type the following command on the DNCS and press **Enter**. The **Do you want to continue with the upgrade?** message appears.
`/var/tmp/lu_continue`

2 Type **y** and then press **Enter**. The **Are you certain you want to proceed?** message appears.

3 Type **y** and press **Enter**. The system detaches the database mirrors.
Important: Do *not* type *init 6* to reboot the DNCS until the lu_continue script has been run on all of the servers on the system.



4 Type **lustatus** to verify the new boot environment is set to **Active On Reboot**. The system displays a message similar to the following:

5 Choose one of the following options:

- If you are upgrading an RNCS, go to ***Continue with the RNCS Upgrade*** (on page 57).
- If you are upgrading a standalone Application Server, go to ***Continue with the V245/V240 Standalone Application Server Upgrade*** (on page 56).

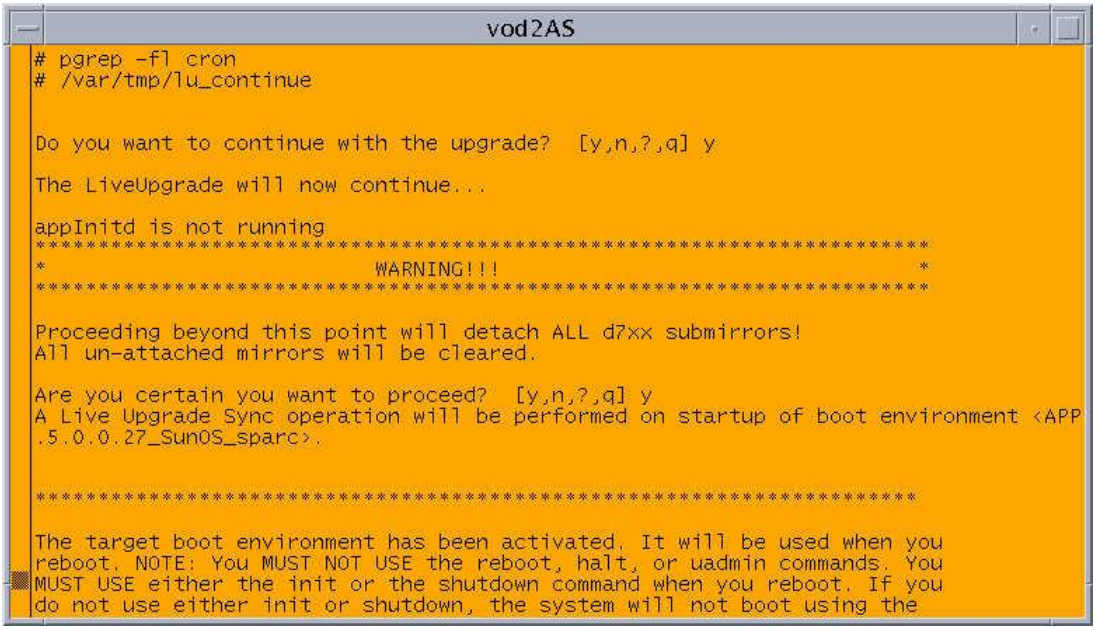
Continue with the V245/V240 Standalone Application Server Upgrade

Important: Complete this procedure only if you are continuing to use a standalone Application Server. If you are migrating to an integrated Application Server, skip this procedure.

1 From the **root** xterm window on the Application Server, type the following command and press **Enter**. The **Do you want to continue with the upgrade?** message appears.

```
/var/tmp/lu_continue
```

2 Type **y** and press **Enter**. The **Are you certain you want to proceed?** message appears.



3 Type **y** and press **Enter**.

Important: Do *not* type *init 6* to reboot the Application Server.

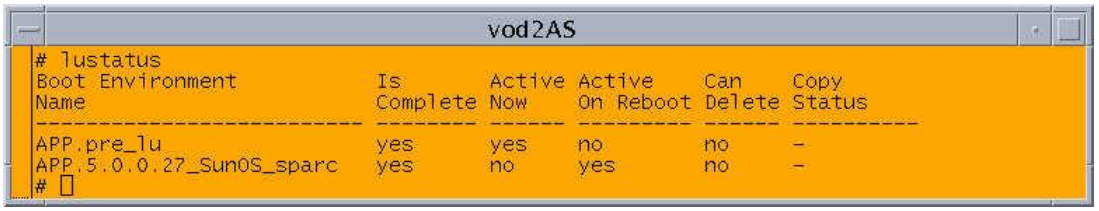
Results:

- A live upgrade operation is executed upon startup of the boot environment.
- The target boot environment is activated.

4 Type the following command and press **Enter** to verify that the new boot environment is set to **Active On Reboot**.

```
lustatus
```

Result: The system displays output similar to the following:



Continue with the RNCS Upgrade

1. From the **root** xterm window on the RNCS, type the following command and press **Enter**. The **Do you want to continue with the upgrade?** message appears.
   `/var/tmp/lu_continue`
2. Type **y** and press **Enter**.
3. Type **y** and press **Enter**.

   Important: Do *not* type *init 6* to reboot the Application Server.

   Results:

   - A live upgrade operation is executed upon startup of the boot environment.
   - The target boot environment is activated.
4. Type the following command and press **Enter** to verify that the new boot environment is set to **Active On Reboot**.
   `lustatus`

   Result: The system displays a message similar to the following:

```
Boot Environment           Is        Active   Active    Can    Copy
Name                       Complete   Now    On Reboot Delete  Status
-------------------------- --------   ------ --------- ------ ----------
RNCS.pre_lu                  yes       yes      no        no      -
RNCS.5.0.0.x_SunOS_sparc     yes       no       yes       no      -
```

Shut Down and Reboot the Servers

Follow these instructions to reboot the servers.

1. From the **root** xterm window on the Application Server, type the following command and press **Enter**. The Application Server shuts down to the **ok** prompt.
   ```
   shutdown -y -g0 -i0
   ```
2. If an RNCS server(s) exists on this system, type the following command and press **Enter** in the **root** xterm window on the DNCS to shut down the RNCS server(s).
   ```
   siteCmd [lionn hostname] shutdown -y -g0 -i0
   ```
3. From the **root** xterm window on the DNCS, type the following command and press **Enter**. The DNCS reboots several times and installs the new DNCS software packages.
   ```
   init 6
   ```
   Notes:
   - When upgrading from SR 4.2.0.x to SR 5.0, the initial reboot may ask for NFS4 information. Accept the default values and press **F2**. A confirmation message appears. Press **F2** again. The upgrade continues.
   - After the final reboot, the DNCS boots to the CDE login screen.
4. After the DNCS CDE login screen is displayed, type the following command on the Application Server and press **Enter**. The Application Server boots several times and installs the Application Server packages.
   ```
   boot
   ```
5. After the DNCS CDE login screen is displayed, type the following command on the RNCS and press **Enter**. The RNCS boots several times and installs the RNCS packages
   ```
   boot
   ```
6. If necessary, repeat step 5 for each RNCS server on your system.

Log into the Upgraded DNCS

This section describes how to log into the DNCS after the live upgrade completes.

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

1 From the CDE login window, type **root** and press **Enter**. You are prompted for the root password.

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.

3 Click **OK**. An xterm window appears and prompts you to enter a new root password.

Important: Place your mouse cursor in the xterm window displayed in the top left corner of the screen.

4 Enter the new password and press **Enter**. You are prompted to re-enter the new password.

5 Re-enter the password and press **Enter**. The CDE login reappears.

6 Log on to the DNCS as **root** user.

7 When prompted to select a desktop environment, select the **CDE** desktop.

8 Click **OK**. The display environment appears.

9 Open two xterm windows on the DNCS. Both xterm windows will be **root** xterm windows.

10 In one of the xterm windows, type the following command and press **Enter** to change to **dncs** user in the xterm window.

```
sux - dncs
```

11 Type the following command and press **Enter** to kill the dncsInitd process.

```
dncsKill
```

12 The **dncs** user password must be reset. You may reset it to the original password if you wish. From the root xterm window, type the following command and press **Enter** to reset the dncs user password.

```
passwd -r files dncs
```

13 Type the password for the **dncs** user and then press **Enter**. You are prompted to re-enter the password.

14 Re-type the password for the **dncs** user and press **Enter**.

15 Does this system include a standalone Application Server?

- If **yes**, go to ***Log into the Upgraded V245/V240 Application Server*** (on page 60).
- If **no**, select one of the following options.
  - If your system includes an RNCS, go to ***Log into the Upgraded RNCS*** (on page 61).
  - If your system does not include an RNCS, go to ***Run the setupAS Script on the DNCS*** (on page 62).

Log into the Upgraded V245/V240 Application Server

This section describes how to log into the upgraded *standalone* Application Server after the live upgrade completes.

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

1. From the CDE login window, type **root** and press **Enter**. You are prompted for the root password.
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.
3. Click **OK**. An xterm window appears and prompts you to enter a new root password.

   Important: Place your mouse cursor in the xterm window displayed in the top left corner of the screen.
4. Enter the new password and press **Enter**. You are prompted to re-enter the new password.
5. Re-enter the password and press **Enter**. The CDE login reappears.
6. Log on to the Application Server as **root** user.
7. When prompted to select a desktop environment, select the **CDE** desktop.
8. Click **OK**. The display environment appears.
9. Open two root xterm windows on the Application Server by typing the following command and pressing **Enter**. Then, enter the **root** password when prompted.

   ```
   su -
   ```
10. In the second xterm window on the Application Server, type the following command and press **Enter** to switch to **dncs** user.

    ```
    sux - dncs
    ```
11. As **dncs** user, type the following command and press **Enter** to kill the appInitd process.

    ```
    appKill
    ```
12. The **dncs** user password must be reset. You may reset it to the original password if you wish. From the **root** xterm window, type the following command and press **Enter** to reset the **dncs** user password.

    ```
    passwd -r files dncs
    ```
13. Type the password for the **dncs** user and then press **Enter**. You are prompted to re-enter the password.
14. Re-type the password for the **dncs** user and press **Enter**.

Log into the Upgraded RNCS

1. Log into the RNCS via the ALOM port 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.
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 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. You may reset it to the original password.

   ```
   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**.

Run the setupAS Script on the DNCS

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

Important: The setupAS script must be run on systems that include either a standalone or an integrated Application Server.

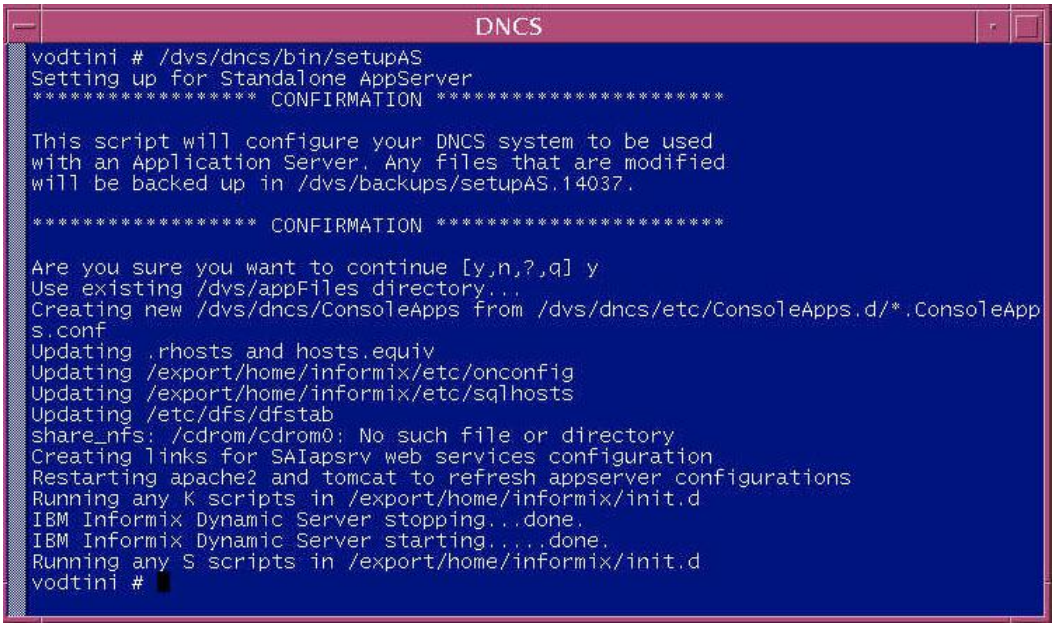
1 From the **root** xterm window on the DNCS, type the following command and press **Enter** to run the setupAS script.

```
setupAS
```

2 Did the **Are you SURE you want to continue?** message appear?

- Type **y** and press **Enter**. The script configures the DNCS to operate with the Application Server.

  Example: DNCS with standalone Application Server



- If **no**, call Cisco Services for assistance.

Add Unique Entries to the dfstab File (Optional)

You should only have to perform this procedure if you are using a third party Application Server. After running the setupAS script, complete the following steps to compare the pre-upgrade dfstab file with the post-upgrade dfstab file and make any necessary modifications to the /etc/dfs/dfstab file.

Important: You must be **root** user to make any modifications to the /etc/dfs/dfstab file.

1. Open a third xterm window on the DNCS and change to **root** user.

   Note: You should now have three xterm windows on the DNCS. You are root user in two, and dncs user in the third.
2. In one **root** xterm window, type the following command and press **Enter** to change to the /dvs/admin/sysinfo/[date_time] directory.

   ```
   cd /dvs/admin/sysinfo[date_time]
   ```

   Note: Replace [date_time] with the directory name of the date and time that the preUpgradeChecks script was run.
3. In the same **root** xterm window, type the following command and press **Enter** to open the dfstab file for review.

   ```
   less dfstab
   ```
4. In the second **root** xterm window type the following command and press **Enter** to open the /etc/dfs/dfstab file.

   ```
   less /etc/dfs/dfstab
   ```
5. Compare the two files. Does the pre-upgrade dfstab file contain any unique entries other than the 3 default entries?
   - If **yes**, in a **root** xterm window, 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 the DNCS, 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.

1. Open a third xterm window on the DNCS and change to **root** user.

   Note: You should now have three xterm windows on the DNCS. You are root user in two, and dncs user in the third.

2. In one **root** xterm window, type the following command and press **Enter** to change to the /dvs/admin/sysinfo/[date_time] directory.

   ```
   cd /dvs/admin/sysinfo[date_time]
   ```

   Note: Replace [date_time] with the directory name that indicates when the preUpgradeChecks script was run.

3. In the same **root** xterm window, type the following command and press **Enter** to open the vfstab file for review.

   ```
   less vfstab
   ```

4. In the second **root** xterm window type the following command and press Enter to open the /etc/vfstab file.

   ```
   less /etc/vfstab
   ```

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

   - If **yes**, in a **root** xterm window, complete these steps.
     a. Open the /etc/vf 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 (Standalone Application Servers and RNCS Servers Only)

Important: If you upgraded a system with an integrated Application Server and no RNCS servers, skip this procedure and go to ***SR 5.0 Post Upgrade Procedures*** (on page 69).

After the upgrade you will have to create the private/public keys between any independent servers on the system (for example, RNCS servers or a standalone Application Server). This is necessary due to the Enhanced Security enabled in this system release. The DNCS must also exchange keys with the RNCS servers.

Important: If your are upgrading an existing SR 5.0 system, private and public keys are backed up and restored as key files. Skip this procedure.

1 From a **root** xterm window on the DNCS, 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 Application Server 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 Application Server. *appservatm*, as shown in the following example, is only an example.

Example: `appservatm`

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

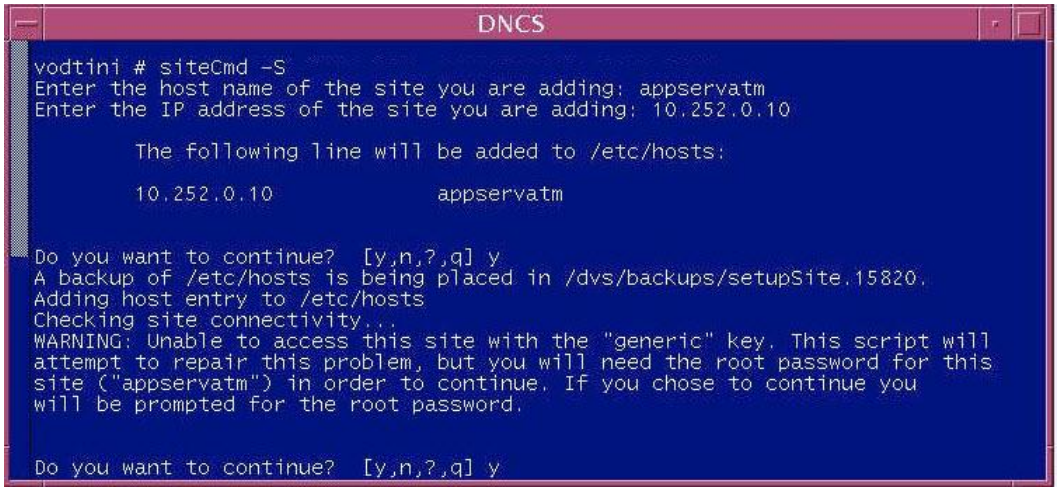
Important: Be sure you enter the actual IP address of the Application Server. *10.253.0.10*, as shown in the following example, is only an example.

Example: `10.253.0.10`

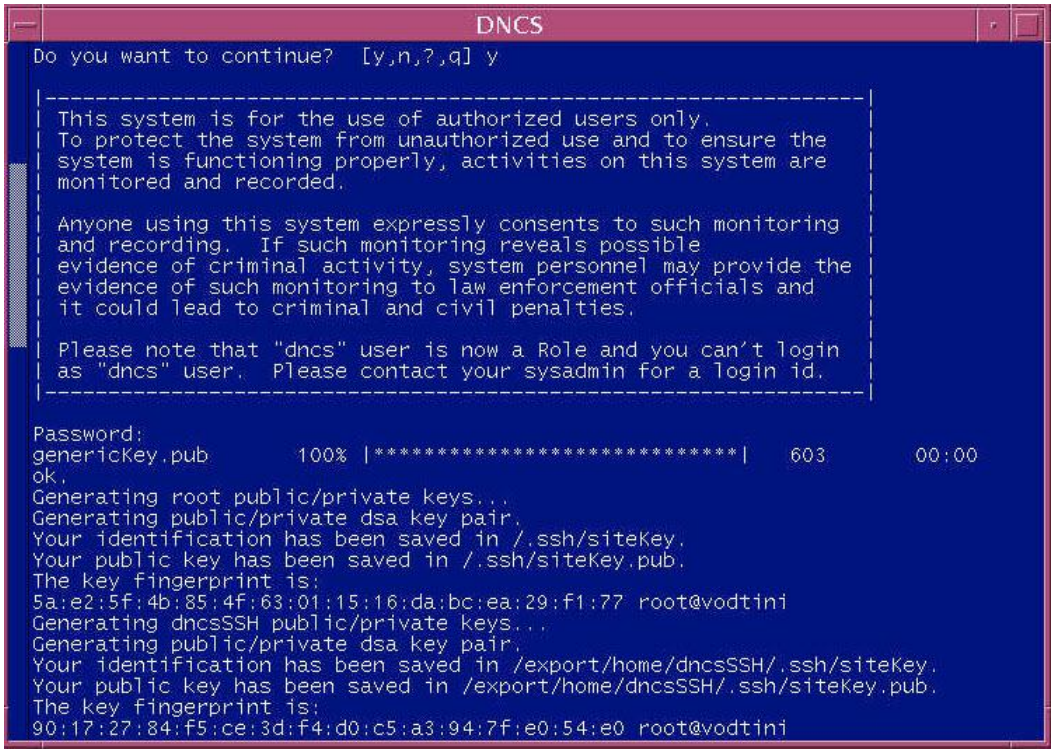
4 Type **y** and then press **Enter**.

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 Application Server.



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.

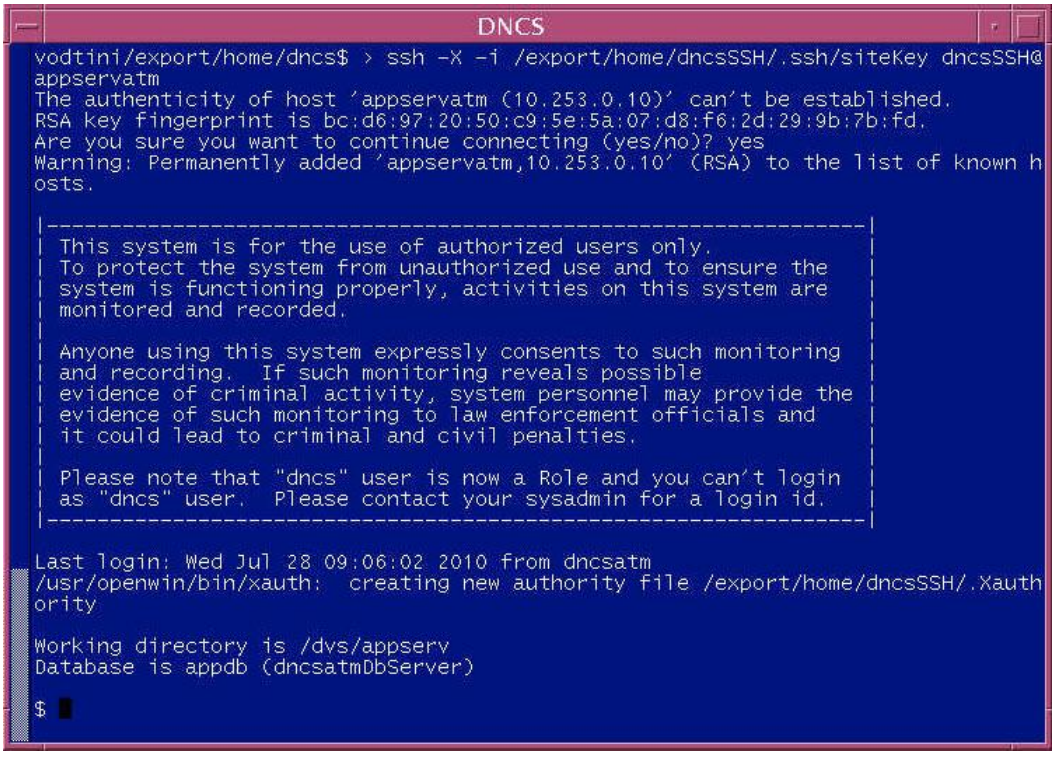


6 Type the following command and press **Enter**.

```
sux - dncs
```

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

ssh -X -i /export/home/dncsSSH/.ssh/siteKey dncsSSH@appservatm



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

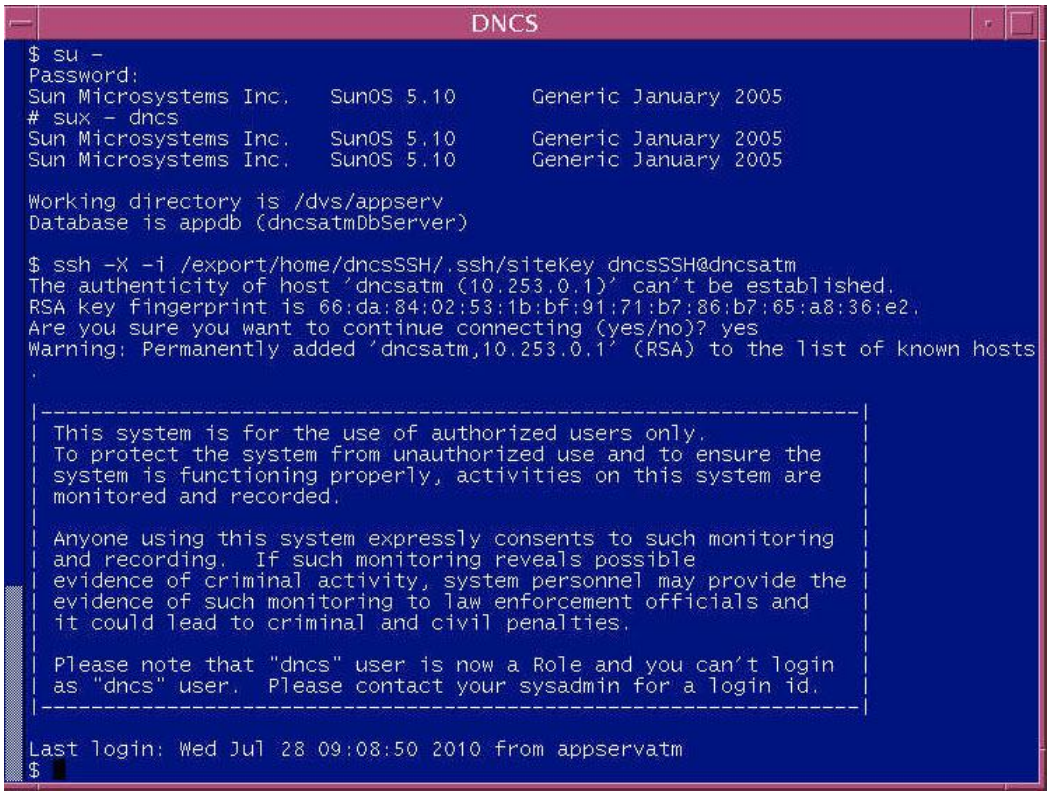
9 Type the **root** password and then press **Enter**.

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 DNCS 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 DNCS and the host for the DNCS 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.

14 Repeat steps 1 through 13 for each RNCS server on your system.

Note: Be sure to insert the hostname and IP address of each RNCS server when prompted.

5

SR 5.0 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

Beginning with SR 5.0.0.x, you can no longer log onto the DNCS or Application Server directly as the dncs user. Instead, you must create individual user accounts for each user that will access these servers.

In this section you will create a default user account named **ciscousr** on the DNCS and Application Server, as well as user accounts directed by the customer.

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

Creating User Accounts on the DNCS, Application Server, and RNCS

Note: The user will be required to change their password during their first successful login session.

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 (web UI). 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 web UIs can be the same password that was defined for the user account.

11 Re-type the password to access the web UI 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 Because the default expiration date for a new user account is 0, type the following command and press **Enter**.

```
passwd -r files [username]
```

14 When prompted, type a password for this user account and press **Enter**.

Note: You can enter the same password that was used to create the account.

15 Re-type the password when prompted and press **Enter**.

16 Open the user's **.profile** file in a UNIX text editor.

Example: `vi /export/home/ciscousr/.profile`

17 Add the following lines to the .profile file:

```
export PATH=$PATH:/usr/ucb
export PS1="$LOGNAME@`hostname`:$PWD>”
set -o vi
```

18 Save and close the user's .profile file.

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

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

21 When prompted to select a desktop environment, select the CDE desktop.

22 Switch to **root** user and repeat steps 1 through 21 to create additional user accounts.

23 Repeat steps 1 through 22 for each server on your system.

Install Patch Software

If you received any patches, or emergency patches (EP), install them now. Any patch or EP CD should have a README file explaining how to install it. Follow the instructions in the README file.

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.

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. From the **root** xterm window on the DNCS, 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 osmAutomux.cfg file.

1. From the **root** xterm window on the DNCS, open the **osmAutomux.cfg** file in a text editor.

   Example: vi 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

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 5.0, 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 From the dncs xterm window, 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 2 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 DNCS and then log back into the DNCS.

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. From the **dncs** xterm window, 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.

Run fixSiteConfigs on the RNCS

Only perform this procedure if the site you are upgrading has an RNCS system. If the site you are upgrading does not have an RNCS, 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.

1 In a **root** xterm window on the RNCS, 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 assitance.
- Ignore any *inet-config* and *nc.config* warnings.

Configure Remote Access to the DNCS Web Interface

If you wish to configure remote access to the DNCS web interface through a Web browser, refer to *DNCS System Release 5.0 Security Configuration Guide* (part number 4034689).

Remove Old BFS_REMOTE Entries

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

1. If necessary, open an xterm window on the DNCS.
2. Complete the following steps to log on to the xterm window as **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 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
     ```
6. Go to the next procedure in this chapter.

Restart System Processes

Important: Note these important points:

- 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.
- Be certain that you are dncs user. Do not start the processes as root user.
- Be certain to start the DNCS, Application Server, and RNCS processes as applicable.
- The Administrative Console has been replaced with a new Digital Network Control System web interface using the FireFox browser.

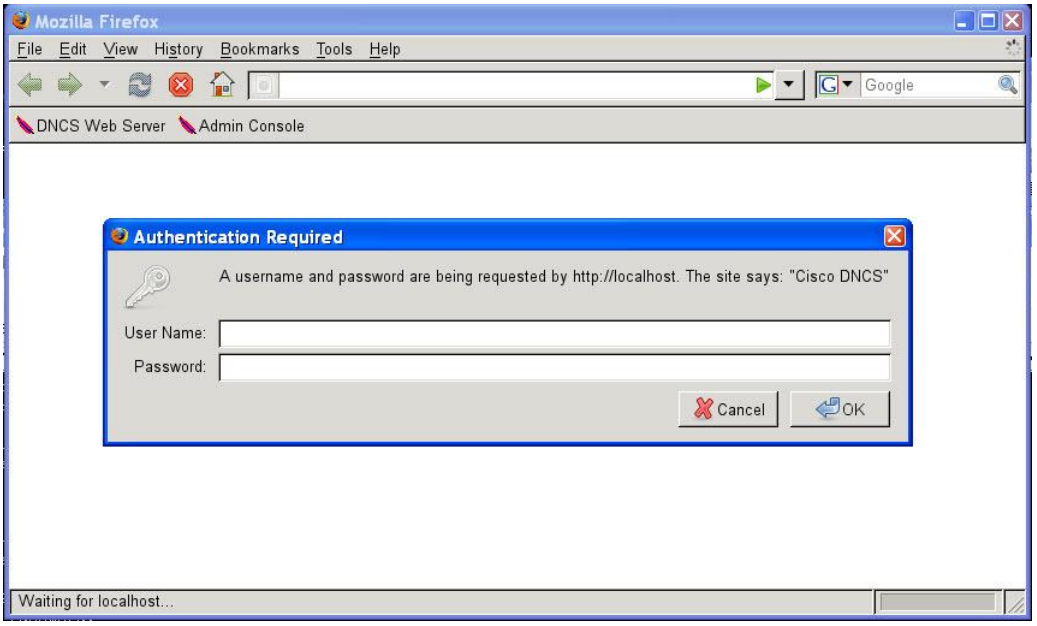
Restarting the DNCS

1. Did you create the **ciscousr** user account or any other user account?
   - If **yes**, skip to step 4.
   - If **no**, go to ***Create User Accounts on the Upgraded Servers*** (on page 71). After creating at least one Administrator account, continue with step 2 of this procedure.
2. Log on to the DNCS as one of the Administrative User accounts that you created in ***Create User Accounts on the Upgraded Servers*** (on page 71).
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. From a dncs xterm window, type the following command and press **Enter**.
   ```
   dncsStart
   ```

5 From the **dncs** xterm window type the following command and press **Enter** to start the FireFox Digital Network Control System web interface.

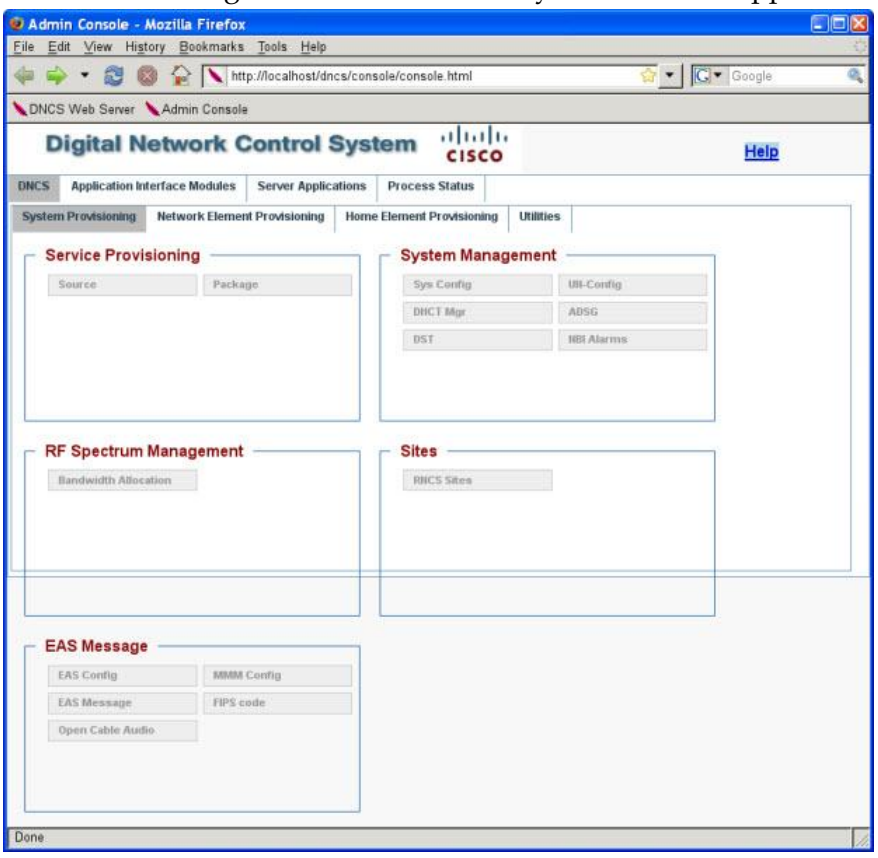
```
admincon
```

Result: An Authentication Requested dialog box appears.

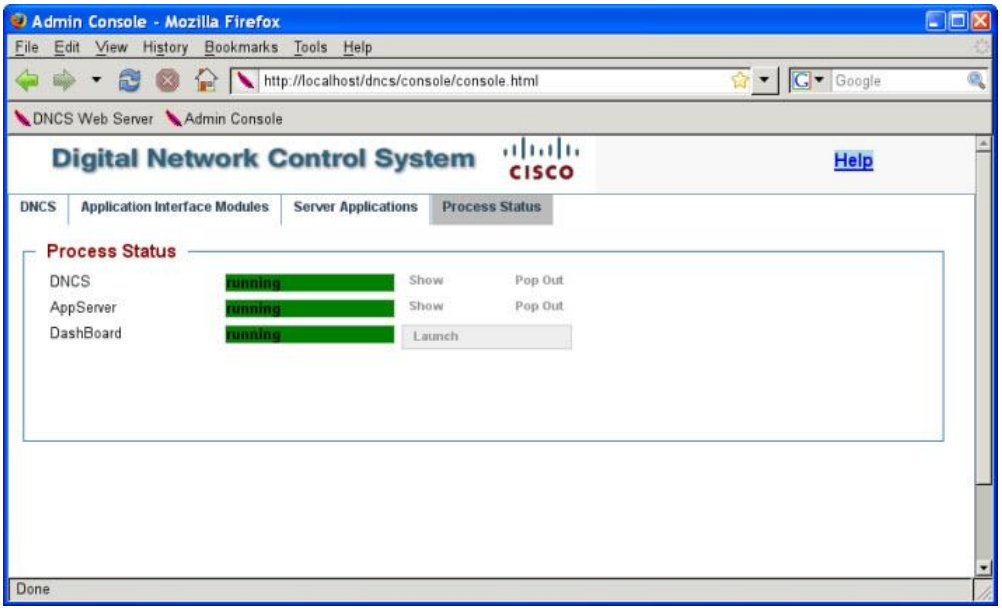


6 Type your user name (for example, **ciscousr**), and then type the password you defined to access the web UIs

7 Click **OK**. The Digital Network Control System window appears.



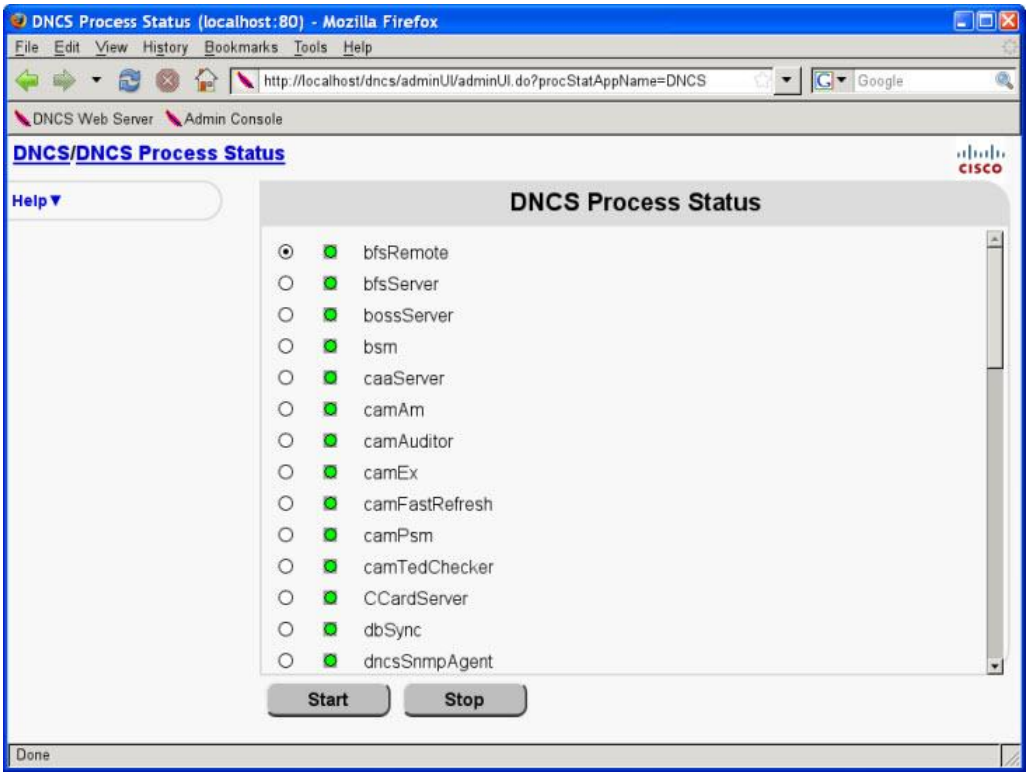
8 From the Digital Network Control System window, click **Process Status**.



9 Click **Show** from the **DNCS** row.

Results:

- The DNCS Process Status window appears.
- Green indicators replace red indicators as the DNCS processes start.



10 From the **dncs** xterm window on the DNCS, type the following command and press **Enter**. The dncsControl utility window opens.

```
dncsControl
```

11 Type **2** (for Startup/Shutdown Single Element Group) and then press **Enter**. The dncsControl window updates to list the available applications for Startup/Shutdown.

12 Type **1** (for dncs) and press **Enter**. The dncsControl window updates to list the goal states.

13 Type **e** (for Display Groups) and press **Enter**. The dncsControl window updates to list the status of all of the processes and servers running on the DNCS.

14 Wait for the dncsControl window to list the current status (**Present State**) of all processes and servers as **running**.

Notes:

- The dncsControl window updates automatically every few seconds, or you can press **Enter** to force an update.
- The indicators on the dncsControl window all become green when the processes and servers have restarted.

Restarting the Standalone Application Server

This section provides procedures for restarting either a SARA server or a third-party server in a standalone Application Server environment. Choose the procedure that pertains to your system.

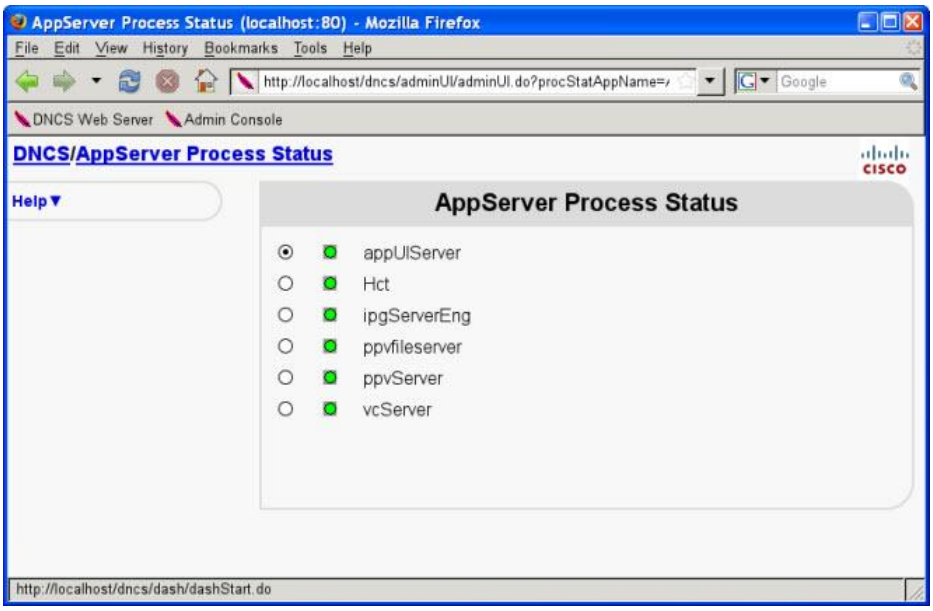
Restarting the Application Server at SARA Sites

1. On the standalone Application Server, open a second xterm window and type the following command to switch to **dncs** user.
   ```
   sux - dncs
   ```
2. Type the following command and press **Enter** to start the Application Server processes.
   ```
   appStart
   ```
3. Type the following command and then press **Enter**. The appControl window opens.
   ```
   appControl
   ```
4. Select option **2** (for Startup/Shutdown Single Group or Process) and press **Enter**. The appControl window updates to list the available applications for Startup/Shutdown.
5. Select option **1** (for appserv) and press **Enter**. The appControl window updates to list the goal states.
6. Select option **e** (for Display Groups) and press Enter. The system displays a list of Application Server processes and their current status.
7. When the appControl window indicates that the current state (**Present State**) of each process is **running**, follow the on-screen instructions to close the Applications Control window.

8 To see Application Server processes start and to monitor their progress, complete these steps.

a From the Digital Network Control System window, click **Process Status**.

b Click **Show** from the **AppServer** row. The AppServer Process Status window appears.



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

1 From the **dncs** xterm window on the DNCS, type the following command and press **Enter**. The LIONN processes start.

```
siteCmd [hostname] lionnStart
```

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

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

Stop and Disable Unneeded DNCS Processes

After the SR 5.0 upgrade completes and the DNCS processes are started, all processes will be running (green). If your system included DNCS processes that were not running or enabled before the upgrade they should be stopped and/or disabled after the upgrade.

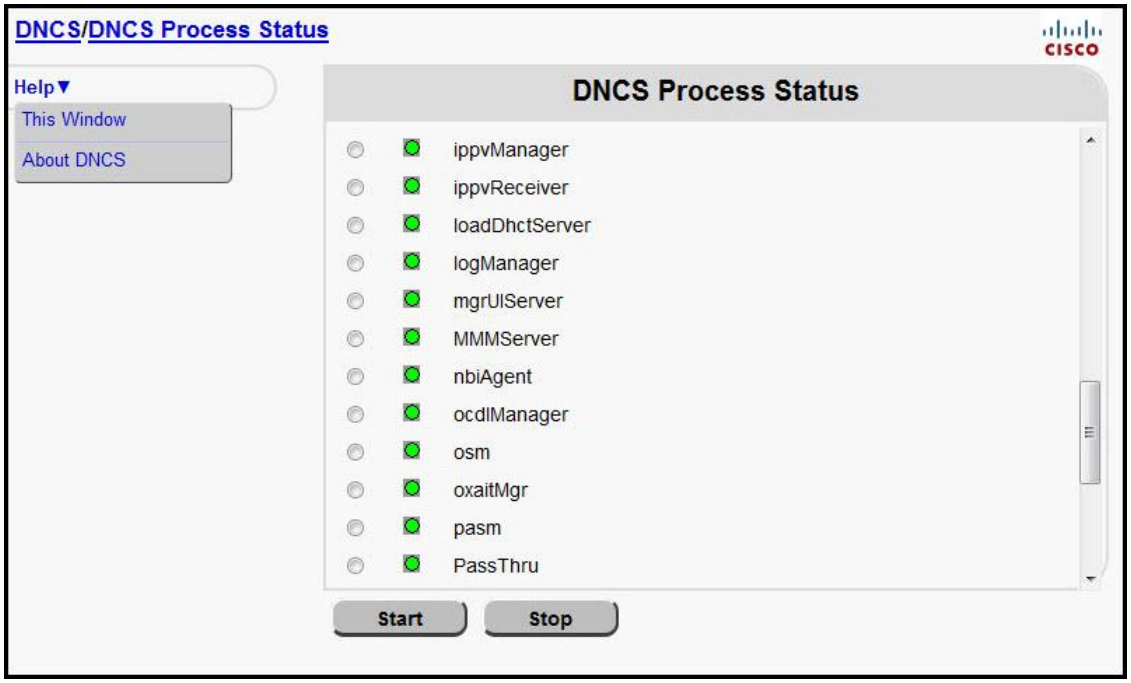
To stop and disable a DNCS process, complete the following procedure.

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

1 If your DNCS Administrative Console has not yet launched, go to a dncs xterm window and type the following command and press **Enter** to open the console.

```
admincon
```

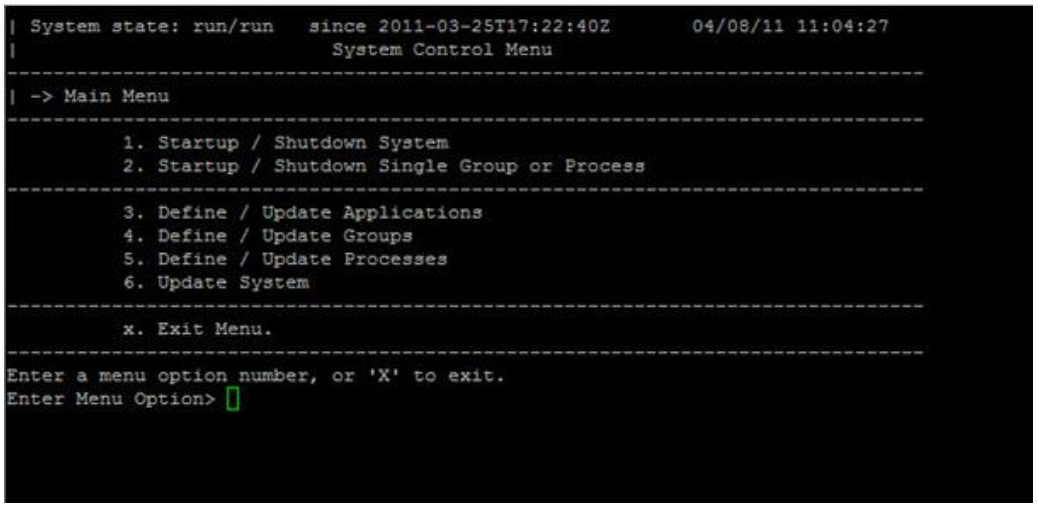
2 Click **Process Status** and then click **Show** to view the DNCS Process Status window.



Note: In this example, the ocdlManager process is running (green).

3 From the **dncs** xterm window, 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 **6** (DNCS DSM, BSM, SiMa) and press **Enter**.

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

9 Type **6** (ocdlManager) and press **Enter**.

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

11 Do you want to disable the process?

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

- If **yes**, type **6** (ocdlManager) and press **Enter** and then type **4** (disabled) and press **Enter**. The ocdlManager process is removed from the DNCS 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 DNCS display group.

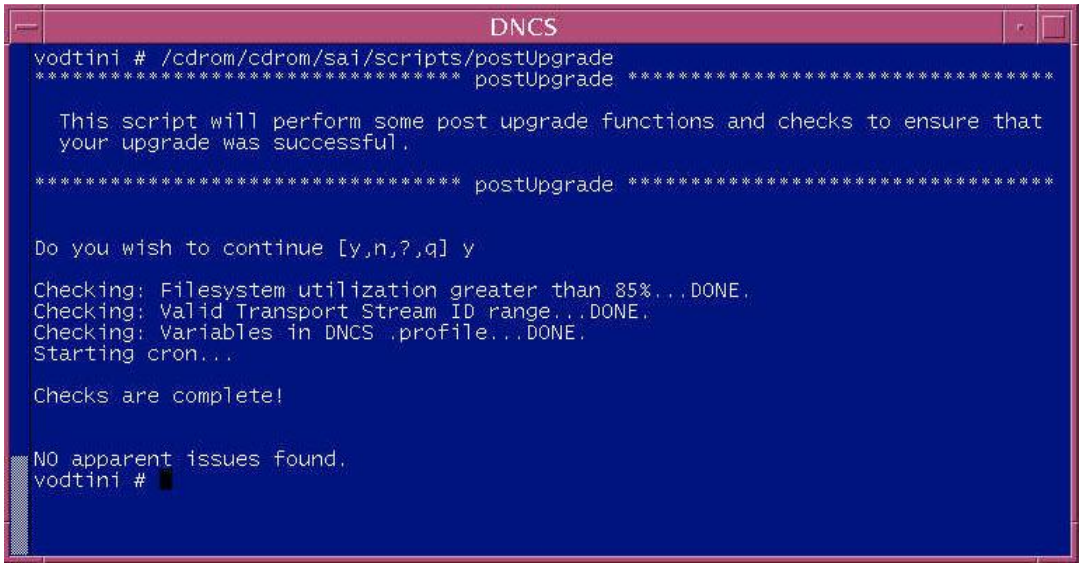
13 To exit the dncsControl window, type **X** (Return to Menu) until the dncsControl window closes.

Run the postUpgrade Script on Each Upgraded Server

For the DNCS, Application Server, and any RNCS server, a post-install script is run to verify the system upgrade. This script also restarts cron jobs and sets the dump device to d501 (swap).

1 From the **root** xterm window 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 Does your system include a standalone Application Server?

- If **yes**, repeat steps 1 and 2 on the Application Server.
- If **no**, go to step 4.

4 Does your system include any RNCS servers?

- If **yes**, repeat steps 1 and 2 for each RNCS server.
- If **no**, you have completed this procedure.

Verify the Number of BFS Sessions

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

Verifying the Number of Recovered BFS Sessions

1. Press the **Options** button on the front panel of the BFS QAM until the **Session Count** total appears.
2. Does the **Session Count** total equal the number of sessions you recorded in *Check the Number of BFS Sessions* (on page 22)?
   - If **yes**, skip to step 6.
   - If **no**, access the craft port of the BFS QAM using whatever terminal emulator software you prefer.
3. Type **print_session_status** and then press **Enter**. The system displays the sessions that are set up on the BFS QAM.
4. Locate Session ID **00:00:00:00:00:00:2**. Is this session in the **CREATE_TABMAN_WAITING** state?
   - If **yes**, go to step 5.
   - If **no**, troubleshoot this matter using your established escalation procedures.

     Note: Call Cisco Services if you are unable to resolve the issue.
5. Does the Program State field of Session ID **00:00:00:00:00:00:2** show **PAT_ASSEMBLY**?
   - If **yes**, go to *Tear Down BFS and OSM Sessions* (on page 93).
   - If **no**, troubleshoot this matter using your established escalation procedures.

     Note: Call Cisco Services if you are unable to resolve the issue.
6. In the **dncs** xterm window type the following command and press **Enter**. The BFS session count is displayed.

   auditQam –query [BFS QAM IP address] 2

   Example: auditQam –query 172.16.4.20 2

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

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

```
Session 10:   00:00:00:00:00:02/20
Session 11:   00:00:00:00:00:02/22
Session 12:   00:00:00:00:00:02/199
```

7 Is the system using an ASI BFS?

- If **yes**, in the dncs xterm window, type the following command and press **Enter** to display the number of **Active Streams** on the ASI card.
  /opt/solHmux64/vpStatus -d /dev/Hmux0 -P 0
  Example:
  ```
  STATUS: /dev/Hmux0
  PORT: 0
  MAX BANDWIDTH: 38800000
  REMAINING BANDWIDTH: 25800000
  TRANSPORT ID: 110
  PSI INTERVAL: 80
  OPTION SETTINGS:
  188 byte packets
  Automatic PSI table generation turned ON
  ACTIVE STREAMS: 12
  ACTIVE TABLE STREAM IDs: 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
  0 0 0
  0 0 0 0 0 0 0
  ```
- If **no**, and your system is using Multicast, follow this procedure to verify the number of Multicast sessions.
  a On the DNCS WUI, follow this path: **DNCS**->**Network Element Provisioning**->**QAM**.
  b Click the **Filter By Field** menu and select **All**.
  c Click **Show**. All provisioned QAMs are displayed.
  d Click the BFS GQAM. The Edit QAM <qam name> WUI appears.
  e In the top left corner, click **Multicast Sessions**. The Multicast Digital Session Definition for <qam name> is WUI appears.
  f Verify that the number of multicast sessions match the number on the GQAM.

8 Do the number of sessions match the number of pre-upgrade sesssions?

- If **yes**, continue with ***Reset the Modulators*** (on page 97).
- If **no**, execute the procedures in ***Tear Down BFS and OSM Sessions*** (on page 93).

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 Digital Network Control System WebUI.

2 Click **Process Status**. The Process Status page appears.

3 Click **DNCS**. The DNCS Process Status page appears.

4. Click **bfsServer** on the left side of the page.
5. Click **Stop** at the bottom of the page. The bfsServer process stops and turns red.
6. Click **osm** on the left side of the page.
7. Click **Stop** at the bottom of the page. The osm process stops and turns red.
8. Click **DNCS** in the top left corner of the page. The Digital Network Control System page appears.
9. Click **Utilities**. The Application Tools page appears.
10. Click **Session List**. The Session List Filter page appears.
11. Select the **BFS QAM** from the QAMs list.
12. 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 of number of pages

    Search — Allows you to search the page
13. 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 14.
14. Click the button on the left next to **Session ID** in the top row. This selects **ALL BFS** sessions displayed on this page.
15. Click **Tear Down** at the bottom of the page. All BFS sessions are torn down.
16. Select the **Process Status** page.
17. Click **bfsServer** on the left side of the page.
18. Click **Start** at the bottom of the page. The bfsServer process starts and turns green.
19. Click **osm** on the left side of the page.
20. Click **Start** at the bottom of the page. The osm process starts and turns green.

    Note: Wait about 10 minutes for the BFS sessions to build.
21. Click **DNCS** in the top left corner of the page. The Digital Network Control System page appears.
22. Click **Utilities**. The Application Tools page appears.
23. Click **Session List**. The Session List Filter page appears.
24. Select the **BFS QAM** from the QAMs list.
25. Click **Display** at the bottom of the page. The Session Summary page appears.
26. Are all the BFS Sessions present and active?
    - If **yes**, continue with step 27.
    - If **no**, contact Cisco Services for assistance.
27. Press the **Options** button on the front panel of the BFS QAM modulator until the **Session Count** total appears.

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

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

29 In the **dncs** xterm window type the following command and press **Enter**. The BFS session count is displayed.

```
auditQam –query [BFS QAM IP address] 2
```

Example: auditQam –query 172.16.4.20 2

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

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

30 Does the **Session Count** total equal the number of sessions you recorded in the ***Check the Number of BFS Sessions*** (on page 22) procedure?

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

31 Is the system using an ASI BFS?

- If **yes**, in the dncs xterm window, type the following command and press **Enter** to display the number of **Active Streams** on the ASI card.
  /opt/solHmux64/vpStatus -d /dev/Hmux0 -P 0
  Example:
  ```
  STATUS: /dev/Hmux0
  PORT: 0
  MAX BANDWIDTH: 38800000
  REMAINING BANDWIDTH: 25800000
  TRANSPORT ID: 110
  PSI INTERVAL: 80
  OPTION SETTINGS:
  188 byte packets
  Automatic PSI table generation turned ON
  ACTIVE STREAMS: 12
  ACTIVE TABLE STREAM IDs: 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
  0 0 0
  0 0 0 0 0 0 0
  ```
- If **no**, and your system is using Multicast, follow this procedure to verify the number of Multicast sessions.
  a On the DNCS WUI, follow this path: **DNCS->Network Element Provisioning->QAM**.
  b Click the **Filter By Field** menu and select **All**.
  c Click **Show**. All provisioned QAMs are displayed.
  d Click the BFS GQAM. The Edit QAM <qam name> WUI appears.
  e In the top left corner, click **Multicast Sessions**. The Multicast Digital Session Definition for <qam name> is WUI appears.
  f Verify that the number of multicast sessions match the number on the GQAM.

32 Does the number of **Active Streams** match the output from step 31?

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

Reset the Modulators

The SR 5.0 installation updates your modulator code. When you reset the modulators, the modulators upgrade by downloading these versions of software from the DNCS. 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 DNCS GUI.
- 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 DNCS.

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 DNCS GUI 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 DNCS GUI 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 DNCS GUI are found in ***Resetting Modulators Through the DNCS Web UI*** (on page 98).
- Instructions for resetting modulators through the front panel are found in ***Resetting Modulators Through the Modulator Panel*** (on page 100).
- Instructions for resetting modulators through the auditQam utility are found in ***Resetting Modulators Through the auditQam Utility*** (on page 101).

Resetting Modulators Through the DNCS Web UI

When you reset the modulators, the modulators download their new SR 5.0 code. Follow these instructions to reset the modulators through the DNCS web UI.

Important: Never reset more than four modulators at once or the DNCS 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 an xterm window on the DNCS.
3. From the DNCS web UI, click **Network Element Provisioning**.

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, select 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** on 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 DNCS.

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 172.16.4.4

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 Click **DNCS** (top left of window) to return to the Digital Network Control System main page.

14 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 103).

  Important: If the Program Count and Session Count totals do not match what you recorded prior to resetting the modulators, call Cisco Services.
- If **no**, go to ***Reset QPSK Modulators*** (on page 103).

Resetting Modulators Through the Modulator Panel

When you reset the modulators, the modulators download their new SR 5.0 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 172.16.4.4

   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 103).

  Important: If the Program Count and Session Count totals do not match what you recorded prior to resetting the modulators, call Cisco Services.
- If **no**, go to ***Reset QPSK Modulators*** (on page 103).

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 DNCS, a process that is usually quicker than resetting the modulator through the DNCS GUI 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** xterm window on the DNCS, 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 DNCS.

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 DNCS GUI. To save time, engineers can create a script that runs automatically. Refer to the following example for a sample script.

```
auditQam  -reset  123.123.123.123
sleep 1
auditQam  -reset  123.123.123.124
sleep 1
auditQam  -reset  123.123.123.125
sleep 1
auditQam  -reset  123.123.123.126
```

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 DNCS 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 then turning it on.

1. From the Digital Network Control System web UI, select the **Network Element Provisioning**.
2. Click **QPSK**. The QPSK List window opens.
3. Select a QPSK modulator.
4. Click **Reset** at the bottom of the web UI. A confirmation message appears.
5. Click **OK** on the confirmation message. The QPSK modulator resets.
6. Wait about 15 minutes and then 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.
7. Click **DNCS** (at the top left corner of the web UI) to close the QPSK List window.

Verify the crontab Entries

After upgrading the DNCS, 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 Does the crontab file include an entry for **dbOptimizer**?

- If **yes**, go to *Examining the CED.in Entry* (on page 104).
- 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 DNCS. When a DHCT has been successfully staged, those EMMs associated with the staging process are no longer needed and should be removed from the DNCS database. The dbOptimizer program is configured to run by default each Saturday at 4 AM.

The /dvs/dncs/bin/CED.in file in the DNCS 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** xterm window on the DNCS, type the following command and then 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 105).
- If **no**, go to step 3 to edit the CED.in file.

3 Type the following command and then 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 then press **Enter**.

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

4 Type **exit** and then 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** xterm windows available, open another xterm window on the DNCS and change to root user by typing **su –** and pressing **Enter** (enter root password when prompted).

Note: You should now have three xterm windows open on the DNCS. Two of them are root user and one is dncs user.

2 Follow these instructions in one of the **root** xterm windows.

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

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

```
cd   /dvs/admin/sysinfo/[date]/crontabs
```

Note: Substitute the date of the most recent network directory for [date] in the command for /dvs/admin/sysinfo/[date]/crontabs.

b Type the following command and then press **Enter**.

```
less  root
```

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

3 In the second **root** xterm window, type the following command and then 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 then press **Enter**. The system copies the root crontab file to /tmp/root.cron.
    ```
    crontab -l > /tmp/root.cron
    ```
  - **b** Type the following command and then press **Enter**.
    ```
    vi  /tmp/root.cron
    ```
  - **c** Add any unique entries to the /tmp/root.cron file and then save the file.
  - **d** Type the following command and then press **Enter**. The edited /tmp/root.cron file becomes the new root crontab file.
    ```
    crontab /tmp/root.cron
    ```
  - **e** Type the following command and then 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 then press **Enter**.
```
vi informix
```

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

8 Type the following command and press Enter.
```
vi dncs
```

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

10 Type **exit** and press **Enter** in both xterm windows.

Verify the Upgrade

Go to Appendix A, ***System Verification Procedures*** (on page 119), 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** xterm window, type **date** and then 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, type the following command and press **Enter**.
  `ssh -l root dncsted`

Note: The "l" is a lowercase L in each instance.

4 Type in 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 then 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 24)

1. From the DNCS Administrative Console, click the **Application Interface Modules** tab.
2. Click **BFS Client**. The Broadcast File Server List window opens.
3. Refer to the sheet of paper that you used when you completed ***Record Third-Party BFS Application Cabinet Data*** (on page 24). 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 Set Up Server window opens.
     b. Click the arrow next to the Server Name field and select the appropriate server.
     c. Click to highlight the correct **Mode** (**1-way** or **2-way**).
     d. Click to highlight the appropriate **Available Source**. Then click **Add** to move it to the **Selected Sources** column.
     e. Click **Save**.
     f. Repeat steps a through e for any additional third-party BFS application cabinets that are missing.
   - If **no** (there are no missing third-party BFS application cabinets), continue with step 4.
4. 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.
5. Examine the **Mode** field for the selected cabinet and verify that the correct mode (**1-way** or **2-way**) is checked.
6. Verify that the correct **Selected Sources** are present for the selected cabinet.
7. Click **Cancel** to close the Broadcast File Server List window when you are finished.

Authorize Access to the DNCS Administrative Console

If your pre-SR 5.0 system contained existing pre-upgrade user accounts and you "granted Administrative access" to the user during preUpgradeChecks, you have to authorize these users to access the DNCS Administrative Console.

Use this procedure to authorize web access to the Administrative Console for any existing OS username.

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

```
/usr/apache2/bin/htdigest /etc/apache2/user-
conf/SAIdncs.digest "Cisco DNCS" [username]
```

Notes:

- This is a single command. Do not press **Enter** until the entire command has been typed.
- Substitute the user account name for [username]. Do not type the brackets in the command.

2 Type the new web interface password for the user and press **Enter**.

3 Type the new password again and press **Enter**. The system compares the two password entries.

4 Did the **They don't match, sorry** message appear?

- If **yes**, the two passwords you entered did not match. Go back to step 3 and re-type the command.
- If **no**, the system prompt is returned. You are finished with this procedure.

Disable the Default ciscousr Account

If you created the default ciscousr account in ***Create User Accounts on the Upgraded Servers*** (on page 71), 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 *DNCS System Release 5.0 Security Configuration Guide* (part number 4034689).

Post-Upgrade Procedure for Sites That Use the loadPIMS and BOSS Web Services

If the site you are upgrading uses the loadPIMS or BOSS Web services, go to ***Configuring the loadPIMS and BOSS Web Services*** (on page 143), and complete the procedures in that appendix.

Then, when you are finished, return to this post-upgrade chapter and continue with ***Enable RADIUS and LDAP (Optional)*** (on page 114).

Enable RADIUS and LDAP (Optional)

To enable RADIUS or LDAP on your system, refer to *Enable RADIUS and LDAP Support in a DBDS for SR 5.0 Configuration Guide* (part number 4017610).

6

Commit the Upgrade

Introduction

Follow the procedure in this chapter only if you have upgraded a Sun Fire V880 or V890 DNCS or a Sun Fire V240 or V245 Application Server during the upgrade to SR 5.0.

Important: Be sure that you complete this procedure during the current maintenance window on the night of the server upgrade. If you wait until the following night to complete this procedure, the server will operate an entire day without its disk-mirroring functions in place.

Important Note to Consider

You should follow the procedure in this chapter only under one of the following circumstances:

- You are satisfied with the upgrade and want to commit the system changes

  Note: Rolling back an upgrade after completing the procedure in this chapter is time consuming and takes more effort.

- You have rolled back from an unsuccessful upgrade and want to synchronize the mirrors

In This Chapter

Attach Mirrors

Before starting this procedure, inform the system operator that completing this procedure commits the upgrade. Any attempt to roll back from the upgrade after the mirrors are attached will take up to 4 hours to complete. Additionally, the rollback procedure cannot be performed during the current night and will have to be performed during a maintenance window tomorrow.

Attaching Mirrors

Follow this procedure to run a script that attaches submirrors to their respective mirrors and creates all necessary hot spare disks.

1. Insert the SR 5.0 DVD into the DVD drive of the applicable server.
2. Type the following command and press **Enter**. A list of the mounted filesystems appears.
   ```
   df  -n
   ```
   Note: The presence of **/cdrom** in the output confirms that the system correctly mounted the DVD.
3. In a **root** xterm window on the DNCS, type the following command and press **Enter**. A confirmation message appears.
   ```
   /cdrom/cdrom/sai/scripts/attach_mirrors
   ```
4. Type **y** and then press **Enter**. The system executes a script that attaches submirrors to their respective mirrors and creates all necessary hot spare disks.
   Note: It may take several hours to execute the attach_mirrors script.
5. When disk mirroring completes, type the following command and press **Enter**.
   ```
   eject cdrom
   ```
6. Repeat steps 1 through 5 to attach the mirrors on any other applicable server.

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 DNCS and DHCTs. The DNCS 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 5.0.

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. In a **dncs** xterm window, 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 (SARA, Aptiv, OCAP™), 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, then 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 DNCS Administrative Console, select the **Application Interface Modules** tab.
3. Click **BFS Client**. The BFS Client Sites window opens.
4. Double-click the DNCS site. The Site [DNCS] Broadcast File Server List window appears.
5. Highlight the **sam** file server.
6. Click **File** and then select **Delete**. A confirmation message appears.
7. Click **Yes** and then press **Enter**. The system deletes the sam file server.

Bounce the saManager Process

1. On the DNCS Control window, highlight the **saManager** process.
2. Click **Process** and then select **Stop Process**. 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. On the DNCS Control window, highlight the **saManager** process again.
4. Click **Process** and then select **Start Process**. In a few minutes, the indicator for the saManager process changes from red to green.

Save the Channel Map WUIs

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 then 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 5.0 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 4004455).

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

Disabling the SAM Process on a Rovi Corporation Server

Introduction

The procedure in this appendix describes how to disable the SAM process on a Rovi Corporation server.

In This Appendix

Disable the SAM Process on Rovi Corporation Systems

Important: Skip this procedure if the site you are upgrading does not use the Rovi Corporation application server.

If the site you are upgrading uses the Rovi Corporation application server, you need to disable the SAM process before you restart the DNCS. Follow these instructions to disable the SAM process.

1. From the DNCS Administrative Console Status window, click **Process Status**. The Process Status window opens.
2. From the **DNCS** row, click either **Show** or **Pop Out**. The DNCS process status appears.
3. From the **dncs** xterm window on the DNCS, type **dncsControl** and then press **Enter**. The DNCS Control window opens.
4. Type **4** (for Define/Update Groups) and then press **Enter**. The window updates to list all applications.
5. Type **1** (for DNCS) and press **Enter**. The window updates to list a series of element groups.
6. Type **14** (for DNCS SA Manager) and then press **Enter**. The window updates to list the elements in the group.
7. Type **1** (for /dvs/dncs/bin/saManager) and then press **Enter**. The first in a series of confirmation messages appears.
8. Press **Enter** at each confirmation message to accept the default setting until a message about **cpElmtExecCtrlStatus** appears.

   Note: In total, you should see about six confirmation messages.
9. At the cpElmtExecCtrlStatus message, type **2** (for Disabled) and then press **Enter**. A confirmation message appears.
10. Type **y** and then press **Enter**. The message **Element Definition was Modified** appears.
11. Follow the onscreen instructions to exit from the DNCS Control window.

C

SR 5.0 Rollback Procedures for the DVD Upgrade

Introduction

The SR 5.0 rollback procedures are intended for field service engineers who encounter problems while upgrading an existing digital system to SR 5.0. Prior to executing the SR 5.0 rollback procedures, contact Cisco Services at 1-866-787-3866.

In This Appendix

Activate the Old System Release

Important: If you have already run the procedure under ***Attach Mirrors*** (on page 116), then use the procedures to restore the DNCS and Application Server file systems and the Informix database in *DBDS Backup and Restore Procedures For SR 2.2 Through 4.3 User Guide* (part number 4013779). Complete the procedures in this appendix for any other upgrade path.

Follow this procedure to restore the system software that was in place prior to the unsuccessful upgrade to SR 5.0.

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

_____

2 If necessary, stop all system components.

Example: For instance, as **dncs** user, type **appStop** to stop the Application Server processes and type **dncsStop** to stop the DNCS processes.

3 From the **root** xterm window on the DNCS, type the following command and then press **Enter**. The system resets the default boot device to the original disk.

```
eeprom  boot-device=disk:a
```

4 Type the following command and then press **Enter**. The system reboots and activates the old software.

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

Important: Do not use the *reboot* or *halt* command to reboot the server.

5 Log on to the DNCS as **dncs** user.

6 Log on to an xterm window as **root** user.

7 Mount the DVD.

8 Follow the ***Attach Mirrors*** (on page 116) procedure.

9 Repeat steps 1 through 8 for any Application Server or RNCS server(s) that need to be restored to their original system release.

Restore the Old System Release After a DNCS Upgrade Reboot Failure

In rare circumstances, the DNCS upgrade may fail due to a hardware failure or some other issue while the software is installing as part of a reboot. The Application Server and/or RNCS should still be shut down to the boot prompt (**ok**) at this point in the upgrade. If the DNCS upgrade should fail during the reboots, and you have to roll the DNCS back to the pre-upgrade disks, you will also have to roll the Application Server and/or RNCS back to the pre-upgrade disks.

Note: Depending upon what the failure was and when it occurred, you will either be at a boot prompt (**ok**) or an Administrative prompt (**#**).

Follow this procedure to restore the system software that was in place prior to an unsuccessful upgrade to SR 5.0.

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

_____

2 Depending upon the prompt that is displaying, choose one of the following options to reset the boot device to the old system release.

- If you are at the boot prompt (**ok**), type the following command and press **Enter**.

  ```
  setenv boot-device disk:a
  ```

- If you are at the Administrative prompt (**#**), type the following command and press **Enter**.

  ```
  eeprom boot-device=disk:a
  ```

3 Depending upon the prompt that is displaying, choose one of the following options to boot/reboot the system.

- If you are at the boot prompt (**ok**), type the following command and press **Enter**.

  ```
  boot
  ```

- If you are at the Administrative prompt (**#**), type the following command and press **Enter**.

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

4 Complete the ***Attach Mirrors*** (on page 116) procedure.

5 Repeat steps 2 and 3 for any Application Server or RNCS server(s) that needs to be restored to the original system release.

D

Configuring DTACS on an SR 5.0 System

Introduction

Important: If you are upgrading an *existing* SR 5.0 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 a DNCS SR 5.0 system, you will need to add or modify specific configurations and files on both the DTACS server and the DNCS. For this reason, we recommend opening two **root** xterm windows: one that accesses the DNCS 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** xterm window on the DTACS server.

1. Type the following command and press **Enter**.
   ```
   grep dncsSSH /etc/hosts
   ```
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** xterm 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 **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 10.253.0.2 /etc/hosts
10.253.0.2    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 135) in the space provided.

Host Name of DTACS Server: _____

2 Does your system include an Integrated Application Server?

- If **yes**, the Informix listener must be added to to various files on the DTACS and the DNCS Servers. Skip to step 6.
- If **no**, go to step 3.

3 In the DTACS xterm window, open the **/export/home/informix/etc/sqlhosts** file in a text editor.

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

```
dncsatmDbServer ontlitcp dncsatm informixOnline
```

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

6 In the DNCS xterm window, open the **/export/home/informix/etc/sqlhosts** file in a text editor.

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

```
dncsatmDbServer ontlitcp dncsatm informixOnline
```

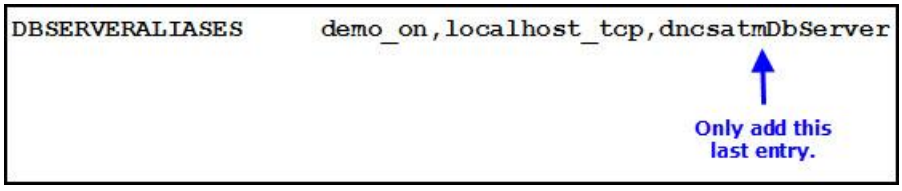
8 Save and close the file on the DNCS server.

9 In the DNCS xterm window, open the **/export/home/informix/etc/onconfig** file in a text editor.

10 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:



11 In the DNCS xterm window, type the following command and press **Enter** to start the Informix listener for the dncsatmDbServer.

```
onmode -P start dncsatmDbServer
```

12 In the DNCS xterm window, type the following command and press **Enter**. The **Enter the host name of the site you are adding** message appears.
```
siteCmd -S
```

13 Type the hostname of the DTACS server (recorded in step 1) 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 1).

14 Type the IP address of the DTACS server (recorded in step 2) and then press **Enter**. The **Do you want to continue** message appears.

Example: `10.253.0.2`

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

15 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.

16 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.

17 Type the following command and press **Enter** to change to the **dncs** user.

Note: You should still be working in the DNCS xterm window
```
sux - dncs
```

18 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: In the DNCS xterm window, 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.

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

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

21 Type the following command and press **Enter** to change to the **dncs** user.
```
sux - dncs
```

22 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.

23 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.

24 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** xterm 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** xterm 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** xterm 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 xterm 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 To test the dbSync command from the Web UI, type **exit** and then press **Enter** to exit from the **dncs** user.

8 Type the following command and press **Enter** to change to the **dtacs** user.

```
sux - dtacs
```

9 Type the following command and press **Enter** to launch the DTACS Administrative Console.

```
dtacsWUIStart
```

10 Click the **Sys Config** button on the Web UI console. The DTA Control System Configuration window appears.

11 Click **Sync Db** to initiate the DTACS database synchronization process.

12 Did a **DB Sync request processed successfully** message appear?

- If **yes**, the synchronization was successful.
- If **no**, contact Cisco Services for assistance.

E

Configuring the loadPIMS and BOSS Web Services

Introduction

This appendix contains post-upgrade procedures for sites that use the loadPIMS and BOSS Web services.

In This Appendix

Post-Upgrade Procedures for the loadPIMS and BOSS Web Services

Add Back the Apache Allow and Deny Directives

Important: This procedure, as well as the remaining procedures in this appendix, are to be completed after the SR 5.0 upgrade.

In ***Record the Apache Allow and Deny Directives (Optional)*** (on page 26), you recorded allow and deny directives from the following files:

- /etc/apache2/conf/boss.http
- /etc/apache2/conf/loadPIMS.https

In this procedure, you will add these directives to two different files.

- Allow and deny directives from the /etc/apache2/conf/boss.http file will be added to the /etc/apache2/user-conf/SAIdncs.loadPIMS.auth.conf file.
- Allow and deny directives from the /etc/apache2/conf/loadPIMS.https file will be added to the /etc/apache2/user-conf/SAIdncs.bossreq.auth.conf file.

1 Open an xterm window on the DNCS as **root** user.

2 Type the following command and press **Enter** to make a backup copy of the original /etc/apache2/user-conf/SAIdncs.loadPIMS.auth.conf file.
```
cp /etc/apache2/user-conf/SAIdncs.loadPIMS.auth.conf
/etc/apache2/user-conf/SAIdncs.loadPIMS.auth.conf.orig
```

3 Type the following command and press **Enter** to make a backup copy of the original /etc/apache2/user-conf/SAIdncs.bossreq.auth.conf file.
```
cp /etc/apache2/user-conf/SAIdncs.bossreq.auth.conf
/etc/apache2/user-conf/SAIdncs.bossreq.auth.conf.orig
```

4 Open the /etc/apache2/user-conf/SAIdncs.loadPIMS.auth.conf in a text editor.
Example: `vi /etc/apache2/user-conf/SAIdncs.loadPIMS.auth.conf`

5 Insert the directives into the file below where the default entries are located.

Example: The following example contains the default entries for the /etc/apache2/user-conf/SAIdncs.loadPIMS.auth.conf file:

```
# This section applies to both http and https
# Access originating locally is allowed by default.
Order Allow,Deny
Allow from localhost
Allow from dncs dncs
Allow from dncsws

# Short instructions for creating and setting a user password
# See /httpd.apache.org for a full list of supported options.
#
```

Note: Your recorded allow and deny directives from the /etc/apache2/conf/boss.http file should go between the following two lines:

```
Allow from dncsws
# Short instructions for creating and setting a user password
```

6 Save and close the file when you are finished.

7 Open the /etc/apache2/user-conf/SAIdncs.bossreq.auth.conf file in a text editor.

Example: `vi /etc/apache2/user-conf/SAIdncs.bossreq.auth.conf`

8 Insert the directives into the file below where the default entries are located.

Example: The following example contains the default entries for the /etc/apache2/user-conf/SAIdncs.bossreq.auth.conf file.

```
# This section applies to both http and https
# Access originating locally is allowed by default.

Order Allow,Deny
Allow from localhost
Allow from dncs dncs
Allow from dncsws

# Satisfy Any allows any one of the Allow from or Require or SSLRequire
```

Note: Your recorded allow and deny directives from the /etc/apache2/conf/loadPIMS.https file should go between the following two lines:

`Allow from dncsws` and

```
# Satisfy Any allows any one of the Allow from or Require or SSLRequire
```

9 Save and close the file when you are finished.

Summarize the Apache Directives (Optional)

It is possible to summarize directives for individual hosts on the same network to single directives per network.

For example, assume you have the following directives:

```
Allow from 147.191.126.36
Allow from 147.191.126.37
Allow from 147.191.126.38
Allow from 147.191.126.39
Allow from 24.40.12.107
Allow from 24.40.12.108
Allow from 24.40.12.52
Allow from 24.40.13.104
Allow from 24.40.13.105
Deny from 192.168.0.0/16
Deny from 64.0.0.0/8
```

The two Deny directives are written in CIDR format and represent any IP address between 192.168.0.1 and 192.168.255.254 (for the former), as well as IP addresses between 64.0.0.1 and 64.255.255.254 (for the latter).

There are a few addresses from the 147.191.126.x networks and the 24.40.x.x networks. To summarize the addresses in the 147.191.126.x networks, assume a 24 bit subnet mask (255.255.255.0). The single directive would be:

```
Allow from 147.191.126.0/24
```

To summarize the 24.40.x.x networks, assume a 16 bit subnet mask (255.255.0.0). This directive would be:

```
Allow from 24.40.0.0/16
```

In this example, you would only need to add the following 4 directives to represent the same 11 directives:

```
Allow from 147.191.126.0/24
Allow from 24.40.0.0/16
Deny from 192.168.0.0/16
Deny from 64.0.0.0/8
```

It is important to verify with your network administrator that your summarized directives are appropriate for your network. In the proceeding example, we have simplified the config files, but we have opened up access to the PIMS and BOSS Web services to larger numbers of IP addresses. With the original directives, only 9 hosts were allowed to connect:

```
147.191.126.36
147.191.126.37
147.191.126.38
147.191.126.39
24.40.12.107
24.40.12.108
24.40.12.52
24.40.13.104
24.40.13.105
```

With these new directives, we are allowing requests from 65,788 hosts. The **24.40.0.0/16** directive allows 65,534 hosts (24.40.0.1 - 24.40.255.254) and the **147.191.126.0/24** directive allows 254 additional hosts (147.191.126.1 - 147.191.126.254).

Configure Apache to Listen for Web Service Requests

Determine the Hostname(s) of Network Interfaces to Receive Web Service Requests from PIMS Servers

Chose one server IP address in each unique network identified in the allow directives previously recorded. Complete the following procedure for each server IP address in order to determine the DNCS network interface on which Web service requests will be received.

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

Note: We will use IP address 24.40.13.104 in this example.

```
traceroute 24.40.13.104
```

Result: Output similar to the following should appear.

```
traceroute: Warning: Multiple interfaces found; using 192.168.2.1 @ ce1
traceroute to 24.40.13.104 (24.40.13.104), 30 hops max, 40 byte packets
 1  cisco (192.168.2.254)  0.522 ms  0.286 ms  0.252 ms
```

Example: In this sample output, *ce1* represents the network interface; its IP address is *192.168.2.1*.

Important: It is possible that servers in different networks will make requests to different DNCS interfaces. Contact your Network Administrator if you are not sure of the interface on which traffic from the PIMS servers will be received.

2 Examine the /etc/hostname.[interface] file that corresponds to the network interface identified in step 1.

```
cat /etc/hostname.ce1
```

Example: `dncseth netmask 255.255.255.0 broadcast +`

Note: The first column of the output represents the hostname of the network interface. In this example, the hostname is *dncseth*.

Verify the /etc/hosts File

1 Type the following command and press **Enter** to open the /etc/hosts file.

```
more /etc/hosts
```

2 Verify that the dncsws hostname does not appear on any line other than the *loopback2 127.0.0.2* line.

3 Verify that all hostnames appear on only one line.

4 Verify that the identified hostnames are associated with the correct IP address in this file.

Add a Listen Directive to the httpd.ports File for Each Network Interface

1 Open the httpd.ports file in a text editor.

2 To add a Listen directive, add one line per interface identified in the /etc/apache2/user-conf/httpd.conf file. Add this to the end of the file.

```
Listen [hostname]:80
```

Note: Replace [hostname] with one of the hostnames identified in ***Determine the Hostname(s) of Network Interfaces to Receive Web Service Requests from PIMS Servers*** (on page 147).

Example: `Listen dncseth:80`

3 Save and close the file.

4 Repeat this procedure for each network interface that you have identified.

Add a Listen Directive to the ssl.ports File for Each Network Interface

1 Open the ssl.ports file in a text editor.

2 To add a Listen directive, add one line per interface identified in the /etc/apache2/user-conf/ssl.conf file. Add this to the end of the file.

```
Listen [hostname]:443
```

Note: Replace [hostname] with one of the hostnames identified in ***Determine the Hostname(s) of Network Interfaces to Receive Web Service Requests from PIMS Servers*** (on page 147).

Example: `Listen dncseth:443`

3 Save and close the file.

4 Repeat this procedure for each network interface that you have identified.

Apply the Configuration Changes

Restart Apache

You need to be **root** user in an xterm window on the DNCS to run these commands.

1. Type the following command and press **Enter**.
   `svcadm -v disable -st http`
2. Type the following command and press **Enter**.
   `svcadm refresh http`
3. Type the following command and press **Enter**.
   `svcadm -v enable -s http`
4. Type the following command and press **Enter**.
   svcadm -v disable -st http-**`dncsws`**
5. Type the following command and press **Enter**.
   `svcadm refresh http-dncsws`
6. Type the following command and press **Enter**.
   `svcadm -v enable -s http-dncsws`

Verify that the Apache Instances are Running Correctly

Run the following command as **root** user in an xterm window on the DNCS.

`svcs -xv`

Results:

- The command produces no output if the Apache instances are running correctly.
- The command displays a detailed list of services in a degraded state if there are issues.

What's Next?

Return to the SR 5.0 post-upgrade procedures and the ***Enable RADIUS and LDAP (Optional)*** (on page 114) procedure.

Cisco Systems, Inc.
5030 Sugarloaf Parkway, Box 465447
Lawrenceville, GA 30042

678 277-1120
800 722-2009
www.cisco.com

May 2012 Printed in United States of America Part Number 4042225 Rev B