



DBDS Backup and Restore Procedures

For System Release 2.2 Through 4.3

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 Acknowledgements

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.

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

© 2006, 2009, 2012 Cisco and/or its affiliates. All rights reserved. Printed in the United States of America.

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

Contents

About This Guide	v
Chapter 1 Release Notes	1
Improvements to the Backup and Restore Procedures	2
Chapter 2 Backup Recommendations	3
System Backup Frequency	4
Tape Considerations	6
Chapter 3 Backup Procedures	9
Check Your Tape Drive Configuration.....	10
Back Up the DNCS or Application Server File System	12
Back Up the Informix Database	17
Back Up the DNCS or Application Server Key Files	21
Chapter 4 Restoration Procedures	27
Restore the DNCS File System	28
Restore the Informix Database.....	36
Restore the Application Server File System	42
Restore the Key Files	49
Chapter 5 Customer Information	55
Appendix A Stopping System Components	57
Stop System Components	58
Appendix B Restarting System Components	61
Restart System Components.....	62

Contents

Appendix C Setting Up an Automated Database Backup	65
Configure the DNCS for an Automatic Database Backup	66
Index	69

About This Guide

Purpose

This guide provides a full set of backup and restore procedures for the Digital Broadband Delivery System (DBDS) databases, as well as for their respective key files and file systems.

Scope

The procedures in this guide for backing up and restoring the Application Server pertain only to the Application Servers on which the SA Resident Application (SARA) runs. System operators who support other application servers should contact their vendor for relevant backup and restore procedures.

Audience

These backup and restore procedures are written for operators who support the following DBDS System Releases (SRs):

- SR 2.2/3.2
- SR 2.5/3.5
- SR 2.6/3.6
- SR 2.7/3.7
- SR 2.8/3.8
- SR 3.3
- CV SR 3.4
- SR 4.0
- SR 4.2
- SR i4.2.1
- SR 4.3

Field service and software installation engineers may also find the information in this guide useful as they assist system operators in installing, troubleshooting, and maintaining their systems.

DBDS Maintenance CD

This guide refers to version 6.0.13 or later of the backup and restore scripts. These scripts may be loaded onto more than one version of the DBDS Maintenance CD. Check with Cisco® Services if you are unsure of the version of backup and restore scripts that are contained on your DBDS Maintenance CD.

Document Version

This is the third formal release of this document. This revision provides backup and restore procedures for SR 2.2 through SR 4.3.

1

Release Notes

Introduction

This chapter lists those change requests (CRs) that were implemented during the development and testing of the backup and restore procedures covered in this guide, as well as the hardware platforms with which the backup and restore scripts are compatible.

Hardware Platform Compatibility

Version 6.0.13 or later of the backup and restore scripts, which is a part of the DBDS Maintenance CD, was tested against the following platforms:

DNCS	Application Server
■ Sun Enterprise 250	■ Sun Blade 150
■ Sun Fire V440	■ Sun Fire V240
■ Sun Fire V445	■ Sun Fire V245
■ Sun Enterprise 450	■ Sun Ultra 2
■ Sun Fire V880	■ Sun Ultra 5
■ Sun Fire V890	

For a complete configuration listing for the System Releases, please contact Cisco Services.

In This Chapter

- Improvements to the Backup and Restore Procedures 2

Improvements to the Backup and Restore Procedures

Interactive Option Added to Database and File System Restoration Scripts

Our engineers have added an interactive option to the `restoreDatabase` and `restoreFileSystems` scripts. Through use of the interactive option, users can now exit from the restoration process before the process has completed. See *Database Restore Script Options* (on page 36) and *File System Restore Script Options* (on page 28) for implementation details.

Physical Restore Option Added to Database Restoration Script

The `restoreDatabase` script has been modified so that it now includes an option to perform only a physical restoration of the database – not both a physical and logical restoration. This option is useful in the Informix High-Availability Data Replication scenario. See *Database Backup Script Options* (on page 18) for implementation details.

2

Backup Recommendations

Introduction

This chapter provides recommendations for the frequency with which system operators should back up the data of their Digital Broadband Delivery System (DBDS). By performing regular backups, system operators are assured that their valuable data will not be lost should they ever experience a failure of a major component of their DBDS system.

System operators can back up their data to either 4-mm data tapes or 8-mm data tapes, depending upon the type of tape drive installed in their DNCS or Application Server. Use the information in this chapter for tape selection and tape cleaning recommendations.

In This Chapter

- System Backup Frequency..... 4
- Tape Considerations..... 6

System Backup Frequency

System operators can ensure the integrity of their data only by adhering to a regular schedule of database and file system backups. The recommendations in this section provide some guidance regarding the frequency with which system backups should occur. Adjust these recommendations, if necessary, according to the size of the system and the frequency with which the data changes.

Full System Backup

A full system backup refers to a backup of the file systems and the database.

System operators should perform a complete system backup prior to making any substantial modification to the system.

In addition, system operators should perform a complete system backup just prior to upgrading to new system software, as well as right after the upgrade. The backup just prior to the upgrade will be used in case the system must be rolled back to the previous release in the event that the upgrade is unsuccessful.

Important: Clearly label the backup tapes and remove them from the working area so that they cannot be accidentally restored to the new release. New and old backups are not compatible.

Informix Database Backup

The Informix database contains all headend configuration information, as well as data needed to provision and authorize Digital Home Communication Terminals (DHCTs). System operators should perform a complete backup of the Informix database once a day. In addition, system operators should perform a complete backup of the database immediately before and after a channel lineup change or a major system configuration change.

Note: Refer to *Setting Up an Automated Database Backup* (on page 65) for a procedure that sets up an automatic database backup. You can use this procedure *ONLY* if your database backup requires one tape.

File System Backup

System operators should perform a complete backup of the DNCS and Application Server file systems once a week.

Important: Beginning with SR 2.2 and SR 3.2, you can now back up the file system of the DNCS and the Application Server without first shutting down the system components. Even though you are no longer required to shut down the system components, our engineers highly recommend that you schedule your file system backups for periods of lowest system activity.

Key Files Backup

The key files need to be backed up only as part of a system upgrade.

Tape Considerations

Two Types of Tape

Consider the following issues when selecting the type of tapes to buy for the backups:

- You can back up your files to either a 4-mm or an 8-mm data tape. The type of tape you choose depends upon the type of tape drive installed on your DNCS or Application Server.
- You can purchase 4-mm tapes or 8-mm tapes in various lengths. Refer to the following chart, compiled by our engineers, for the specifications of the various tapes available for use in your tape drives.

Tape Drive	Tape Length (in meters)	Capacity (normal/compressed) (in Gbytes)	Tapesize (in Kbytes)	Blocksize (in Kbytes)
8 mm	54	2/4	4000000	16
8 mm	112	5/10	10000000	32
8 mm	160	7/14	14000000	128
4 mm DDS	90	2/4	4000000	16
4 mm DDS-2	120	4/8	8000000	32
4 mm DDS-3	125	12/24	24000000	128
4 mm DDS-4	150	20/40	40000000	128
4 mm DAT72	170	36/72	72000000	128

- Buy the largest tapes that your tape drive supports.
Example: Buy 170m DAT72 tapes if you have a DAT72 tape drive; buy 150m DDS-4 tapes if you have a DDS-4 tape drive.
- The backup scripts detect what tape drive your system uses and supplies default parameters in preparation of running the scripts. The operator can override the default values, at the command line, if desired.
- Depending upon the size of your database, you may need more than one tape to do a complete database backup. If you need more than one tape to back up your database, the backup and restore scripts will prompt you to remove the existing tape and to insert a new tape at the appropriate time.

Cleaning Your Tape Drive

Under normal conditions, most tape and tape drive manufacturers recommend that you clean your tape drive after about 30 hours of use. Use only a cleaning cartridge and kit designed for use with your tape drive. Discard your cleaning cartridge after using it for the number of cleaning cycles specified in the cleaning kit documentation.

3

Backup Procedures

Introduction

Use the procedures in this chapter to back up the file system and key files on the DNCS and Application Server, as well as the Informix database on the DNCS.

In This Chapter

- Check Your Tape Drive Configuration..... 10
- Back Up the DNCS or Application Server File System 12
- Back Up the Informix Database 17
- Back Up the DNCS or Application Server Key Files 21

Check Your Tape Drive Configuration

Use this procedure if you need to determine the device name of the tape drive used by your DNCS.

Notes:

- You will only have to complete this procedure once. The device name of your tape drive will not change unless you specifically change the tape drive configuration.
 - Do not have a tape in the tape drive when you complete this procedure.
- 1 If necessary, open an xterm window on the DNCS.
 - 2 Ensure that no tape is currently in your tape drive.
 - 3 Type the following UNIX routine.

Important: Type the routine just as shown by pressing **Enter** at the end of each line.

```
for drive in 0 1 2 3 4 5 6 7
do
mt -f /dev/rmt/$drive status
done
```

Result: The system checks the status of eight possible tape drive configurations and displays the results.

Note: Your system displays results similar to the following illustration.



```
xterm
$ for drive in 0 1 2 3 4 5 6 7
> do
> mt -f /dev/rmt/$drive status
> done
/dev/rmt/0: no tape loaded or drive offline
/dev/rmt/1: No such file or directory
/dev/rmt/2: No such file or directory
/dev/rmt/3: No such file or directory
/dev/rmt/4: No such file or directory
/dev/rmt/5: No such file or directory
/dev/rmt/6: No such file or directory
/dev/rmt/7: No such file or directory
$ █
```

- 4 Examine your results and use the following observations, based upon the example used in step 3, to determine the device name of your tape drive.
 - In the example in step 3, no tape drives are detected in /dev/rmt/1 through /dev/rmt/7 (as indicated by *No such file or directory*). Therefore, you can conclude that /dev/rmt/1 through /dev/rmt/7 are not valid device names for tape drives on the system queried in step 3.
 - In the example in step 3, a tape drive is detected in /dev/rmt/0 and the system accurately notes that no tape is loaded. Therefore, you can conclude that the device name of the tape drive on the system queried in step 3 is /dev/rmt/0.
 - If /dev/rmt/1 is the device name of your tape drive, then *no tape loaded or drive offline* would appear next to /dev/rmt/1.
- 5 Write the device name of your tape drive in the space provided.

Note: You may need to refer to this device name later.

Back Up the DNCS or Application Server File System

Overview

Consider the following points about a backup of the DNCS or Application Server file system.

System Shutdown No Longer Required for File System Backups

System operators no longer have to shut down their system in order to back up the DNCS or Application Server file system. The backup procedures reflect this change.

Important: Even though you are no longer required to shut down the system components, our engineers highly recommend that you schedule all your file system backups for periods of lowest system activity.

Recommended Frequency

Our engineers recommend that system operators perform a complete system backup at least once a month, just prior to upgrading to new system software, as well as after the upgrade.

Filesystem Backup Script Options

The script that backs up the file system is called **backupFileSystems**. You can run the backupFileSystems script with the following options:

- *-l* – Local-tape-drive. Specifies tape drive to use on local host computer. (for example – /dev/rmt/0h)
- *-r* – Remote-tape-drive. Specifies tape drive on a remote host computer. (for example – sparky:/dev/rmt/0h or 192.168.1.10:/dev/rmt/0h)
- *-B* – Backup directory. Specifies the directory to which the backup of the file system will be saved. The backup directory must be on an NFS-mounted filesystem.
- *-v* – verbose. Verbose output.
- *-t* – tape label. Backup tape label. This must be a unique string with no spaces.
- *-h* – help. Provides a brief description of the valid options.

Failure of File System Backups and the Real-Time, Class Process

Occasionally, the file system backup of the DNCS or the Application Server may fail. If the backup fails, system operators should check whether there are any real-time, class processes that are running. Current file system backup scripts can handle only the `ntpd` process that is running as a real-time class process.

Note: The `ntpd` process is an operating system daemon that sets and maintains system time in synchronization with Internet standard time servers.

If the file system backup fails, system operators should complete the following steps to see if any real-time, class processes are running.

- 1 From an xterm window on the DNCS or the Application Server (depending upon which file system backup failed), type `ps -efc | grep RT` and then press **Enter**. The system reports whether any real-time, class processes are running.
- 2 Are any real-time, class processes running (other than the `ntpd` process)?
 - If **yes** (and the file system backup still failed), call Cisco Services for assistance.
 - If **no**, re-run the procedures to back up the file system. If the backup still fails, call Cisco Services.

Specific Platform Considerations

Before backing up the file system of a Sun Enterprise 450 or Sun Fire V240, V245, V440, V445, V880, or V890 DNCS, our engineers recommend that system operators first check the `dncs` and root user e-mail accounts on the DNCS. The e-mail accounts will reveal whether any metadvice errors exist on the DNCS.

Preparing for the File System Backup

Complete the following steps to prepare for the DNCS or Application Server file system backup.

- 1 Are you backing up a Sun Enterprise 450 or Sun Fire V240, V245, V440, V445, V880, or V890 DNCS?
 - If **yes**, check the `dncs` and root user e-mail accounts on the DNCS for the presence of metadvice errors.

Note: Correct any metadvice errors before proceeding with the backup. Call Cisco Services if you need help in correcting metadvice errors.
 - If **no**, go to step 2.
- 2 If necessary, open an xterm window on the DNCS or the Application Server, whichever server you are backing up.
- 3 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**.

- 4 Insert the CD labeled **DBDS Maintenance CD** into the CD drive of the DNCS or the Application Server, whichever server you are backing up.
- 5 Type **df -n** and then press **Enter**. A list of mounted file systems appears.
Note: The presence of **/cdrom** in the output confirms that the system correctly mounted the CD.
- 6 Choose one of the following options:
 - If you are backing up the file system to tape, go to step 7.
 - If you are backing up the file system to a directory, go to *Backing Up the File System to an NFS-Mounted Directory* (on page 16).
- 7 Label a blank tape with the following information:
[DNCS or Application Server] File System Backup [Date]
[Site Name]
[Software Version]
DBDS Maintenance CD x.x.x
- 8 Choose one of the following options:
 - If you are backing up the file system to a tape in the DNCS or Application Server, go to *Backing Up the DNCS or Application Server File System* (on page 14).
 - If you are backing up the file system to a tape in a remote host computer, go to *Backing Up the File System to a Remote Host Computer* (on page 15).

Backing Up the DNCS or Application Server File System

Complete the following steps under the following circumstances:

- You are backing up the file system of the DNCS to a tape in the DNCS, itself
- You are backing up the file system of the Application Server to a tape in the Application Server, itself

If you are backing up the file system of the Application Server to a tape in the DNCS, go to *Backing Up the File System to a Remote Host Computer* (on page 15).

Note: If you have correctly followed the directions in this chapter, you should be logged in to an xterm window as root user.

- 1 Insert the blank tape into the tape drive of the DNCS or Application Server, whichever server you are backing up, and wait for the green light to stop flashing.
- 2 To back up the file system, type **/cdrom/cdrom0/s3/backup_restore/backupFileSystems -v** and then press **Enter**. The system backs up the DNCS or Application Server file system, ejects the tape, and displays a message when the backup is complete.
- 3 When the backup is complete, remove the tape and store it in a safe place.
- 4 Type **eject cdrom** and then press **Enter**.

Backing Up the File System to a Remote Host Computer

Complete the following steps to back up the DNCS or Application Server file system to a tape in another computer – commonly referred to as a *remote host* computer.

Example: Use this procedure, for instance, if you are backing up the Application Server file system to a tape in the DNCS.

Note: If you have correctly followed the directions in this chapter, you should be logged in to an xterm window as root user.

- 1 Insert the blank tape into the tape drive of the remote host computer.
- 2 At the DNCS or Application Server, whichever server you are backing up, type **rsh [hostname or IP address] pwd** and then press **Enter**.

Notes:

- Substitute the host name or the IP address of the remote host computer for [hostname or IP address].
 - The purpose of this command is to confirm that you can connect (remote shell) to the host computer without being prompted for a password.
- 3 Did the system prompt you for a password or deny you access after executing step 2?
 - If **yes**, call Cisco Services for assistance.
 - If **no**, go to step 4.
 - 4 To back up the DNCS or Application Server file system, type **/cdrom/cdrom0/s3/backup_restore/backupFileSystems -v -r [hostname or IP address]:[tape device]** and then press **Enter**.

Note: Type the entire command on one line.

Examples:

- **/cdrom/cdrom0/s3/backup_restore/backupFileSystems -v -r dnscatm:/dev/rmt/0h**
- **/cdrom/cdrom0/s3/backup_restore/backupFileSystems -v -r 192.168.44.71:/dev/rmt/0h**

Result: The system backs up the file system, ejects the tape, and displays a message when the backup is complete.

- 5 When the backup is complete, remove the tape and store it in a safe place.
- 6 Type **eject cdrom** and then press **Enter**.
- 7 Remove the CD and store it in a safe place.

Backing Up the File System to an NFS-Mounted Directory

The file system can be backed up to a directory that is located on a Network File System (NFS). You must be able to access the NFS directory through the `/net/<remotehost>/<path_to_NFS_directory>` directory structure. In addition, the `/net/<remotehost>/<path_to_NFS_directory>/<hostname>` directory must already exist, and you must have write-access to the directory or the backup will fail.

Important: Procedures for setting up the NFS are beyond the scope of this document. See your System Administrator, if necessary, for help in setting up the NFS.

Complete the following steps to back up the file system to a specified directory on the DNCS or the Application Server.

- 1 Make sure that you have write-access to the NFS-mounted filesystem and backup directory.
- 2 To back up the DNCS or Application Server file system, type `/cdrom/cdrom0/s3/backup_restore/backupFileSystems -v -B /net/<remotehost>/<path_to_NFS_directory>` and then press **Enter**.

Notes:

- The `<remotehost>` represents the hostname of the remote computer which is exporting (or holds) the filesystem into which you will write or back up.
 - The `<path_to_NFS_directory>` represents the directory path on the remote host which holds the backup files.
- 3 When the backup is complete, type `eject cdrom` and then press **Enter**.
 - 4 Complete the following steps to write down the exact path of the directory into which you have written the backup.
 - a Type `cd /net/<remotehost>/<path_to_NFS_directory>` and then press **Enter**.
 - b Type `ls -l` and then press **Enter**.

Result: The output from this command provides a list of all of the backup sets that have been created for the host `<hostname>`.

Note: The name of each backup set includes the date and time that the set was created, similar to `2007_08_2_16_56`. The name with the most current date and time represents the backup that you just completed.
 - c Type `cd <backup_set>` and then press **Enter**.

Note: Substitute the name of the most current backup set for `<backup_set>`.
 - d Type `pwd` and then press **Enter**. The system displays the name and path of the current directory.
 - e In the space provided, write down the results from step d).

Note: You will need this exact path should you ever have to restore the filesystem from the NFS-mounted directory.

Back Up the Informix Database

This section contains the following information:

- Default DNCS tape drive configuration information
- Procedures to back up the Informix database

Our engineers recommend that you back up your Informix database early in the morning or late at night, when system activity is usually at a minimum.

Back up your database *before* your billing system uploads subscriber impulse pay-per-view (IPPV) purchases from your DNCS. By backing up your database *before* your billing system uploads IPPV purchases, you have a record of subscriber purchases in the event that the billing system loses this data.

Avoid backing up your database while you are performing the following system tasks:

- Running the Interactive Program Guide (IPG) Collector
- Loading an Entitlement Management Message (EMM) CD
- Staging DHCTs
- Downloading IPPV events

Default Tape Drive Configuration

The script used by the DNCS to back up the Informix database uses the following default tape drive configuration:

- Tape size: 8000000 KB
- Block size: 32 KB
- Device name: `/dev/rmt/0h`

This tape drive configuration is in use on a majority of systems. Occasionally, however, the tape drive on a system may be configured with a different device name, such as `/dev/rmt/1h`.

Note: The 'h' that appears at the end of device name `/dev/rmt/0h` or `/dev/rmt/1h` indicates that the system is to use a high density format (compressed) when writing to the tape.

If you know that the device name of your tape drive is `/dev/rmt/0h`, you may skip the following procedure, *Checking Your Tape Drive Configuration*, and continue with *Backing Up the Informix Database* (on page 18). However, if you are unsure of the device name of your tape drive, or if you just want to verify that the device name is `/dev/rmt/0h`, complete the following procedure.

Database Backup Script Options

The script that backs up the databases is called **backupDatabase**. You can run the backupDatabase script with the following options:

- **-b** – Blocks. Specifies the block size of the tape device to which the database backup is written.
Note: If **-b** is not specified, the system uses a default tape block size appropriate for your tape drive. If the system is unable to determine your tape drive, the system uses 32.
- **-s** – Size. Specifies the size of the tape device to which the database backup is written.
Note: If **-s** is not specified, the system uses a default tape size appropriate for your tape drive. If the system is unable to determine your tape drive, the system uses 8000000.
- **-l** – Local-tape-drive. Specifies tape drive to use on local host.
(for example – /dev/rmt/0h)
- **-r** – Remote-tape-drive. Specifies tape drive on a remote host.
(for example – sparky: /dev/rmt/0h or 192.168.1.10: /dev/rmt/0h)
- **-c** – check-database. Checks the integrity of the databases. (Does not fix if errors are found.)
- **-n** – non-interactive. Non-interactive, useful when running from cron.
- **-v** – verbose. Verbose output.
- **-h** – help. Provides a brief description of the valid options.

Backing Up the Informix Database

Use this procedure to back up the DNCS and Application Server databases to the DNCS.

Notes:

- The DNCS, the Application Server, and Spectrum can be running while you back up the Informix database.
 - It may take up to 30 minutes to back up a typical database with approximately 100,000 DHCTs.
- 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 If necessary, insert the CD labeled **DBDS Maintenance CD** into the CD drive of the DNCS.

- 4 Type **df -n** and then press **Enter**. A list of the mounted filesystems appears.
Note: The presence of **/cdrom** in the output confirms that the system correctly mounted the CD.
- 5 Label your backup tape with the following information:
[DNCS or Application Server] Database Backup [Day of the Week]
[Site Name]
[Software Version]
DBDS Maintenance CD x.x.x
[Tape #]
Notes:
 - Customize the label with the day of the week, site name, and software version for the site you are backing up.
 - If your database backup requires more than one tape, be sure to note the tape number on the label.
- 6 Insert the tape into the tape drive of the DNCS and wait until the green light stops flashing.
Important: Be sure that you are using different tapes for each day of the week, as recommended in the Introduction to this chapter.
- 7 Type **./dvs/dnCS/bin/dnCSSetup** and then press **Enter**. The system establishes the root user environment.
Important: Be sure to type the dot, followed by a space, prior to typing **/dvs**.
- 8 Choose one of the following options.
 - If you are using the standard tape drive configuration listed in *Check Your Tape Drive Configuration* (on page 10), go to step 9.
 - If you are using a custom tape drive configuration, go to step 10.
- 9 If you are using the standard tape drive configuration, type **/cdrom/cdrom0/s3/backup_restore/backupDatabase -v** and then press **Enter**; then, go to step 11.
Result: The system displays the following message:
Please mount tape 1 on /dev/rmt/0h and then press Return to continue.

- 10 If you are using a custom tape drive configuration, type `/cdrom/cdrom0/s3/backup_restore/backupDatabase -v -b [blocksize] -s [tapesize]` and then press **Enter**.

Notes:

- The [blocksize] refers to the blocksize that corresponds to your tape from the chart in *Tape Considerations* (on page 6).
- The [tapesize] refers to the tapesize that corresponds to your tape from the chart in *Tape Considerations* (on page 6).

Example:

```
/cdrom/cdrom0/s3/backup_restore/backupDatabase -v -b 128 -s 14000000
```

Result: The system displays the following message:

Please mount tape 1 on /dev/rmt/0h and then press Return to continue.

- 11 Press **Enter**. The system backs up your Informix database.

Notes:

- The system prompts you to insert additional tapes if your backup requires more than one tape.
- A **Successfully completed the database backup** message appears when the backup has completed successfully.
- If the database backup was not successful, the system displays an error message. Call Cisco Services at 1-800-283-2636 for assistance in resolving the error message.

- 12 Type **eject cdrom** and then press **Enter**.

- 13 Remove the CD and tape(s) and store them in a safe place.

Back Up the DNCS or Application Server Key Files

Overview

Consider the following points about a backup of the DNCS or Application Server key files.

Recommended Frequency

The key files consist of those files required to boot the DNCS or Application Server. The script that backs up the file system also backs up the key files. For this reason, system operators need to back up the key files only when preparing for a system upgrade.

Key Files Backup Script Options

The script that backs up the DNCS and Application Server key files is called **backupKeyFiles**. You can run the backupKeyFiles script with the following options:

- **-I** – Key_files_include. Specifies the file that lists all the files that need to be included in the backup.
- **-E** – Key_files_exclude. Specifies the file that lists all the files that need to be excluded from the backup.
- **-l** – Local-tape-drive. Specifies tape drive to use on local host computer. (for example – /dev/rmt/0h)
- **-r** – Remote-tape-drive. Specifies tape drive on a remote host computer. (for example – sparky:/dev/rmt/0h or 192.168.1.10:/dev/rmt/0h)
- **-B** – Backup_Directory. Specifies the backup directory to which the key files should be saved (in tar format).

Important: The system creates a file named KeyFiles.tar in the specified directory. If you wish to back up both the DNCS and the Application Server key files at the same time, be sure to specify different directories for both sets of key files, or one backup will overwrite the other.

- **-v** – verbose. Verbose output.
- **-A** – Alternate Root Directory. Specify the Alternate Root Directory where the key files should be restored. This is useful during a Live Upgrade (UniPack upgrades) when you may want to back up key files from one root directory and restore them to another root directory. The Alternate Root Directory must contain the /usr/sbin/tar directory, or the backup script will fail to execute correctly.

- `-h` – help. Provides a brief description of the valid options.

Notes:

- The `-I` and `-E` options are independent of one another; any one of them may be used. If neither the `-I` or `-E` option is specified, then the default `Keyfiles.include` or `Keyfiles.exclude` files, which exist in the current directory, are used.
- If either the `-I` or `-E` option is included, the absolute path must be specified.
- The `-I` and `-r` options are mutually exclusive of one another; only one of them can be used.
- The `-B` option cannot be used if either the `-l` or `-r` option is used.

Preparing for the Key Files Backup

Complete the following steps to prepare to back up the DNCS or Application Server key files.

- 1 If necessary, open an xterm window on the DNCS or Application Server, depending on which server you are backing up.
- 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 Insert the CD labeled **DBDS Maintenance CD** into the CD drive of the DNCS or Application Server, depending on which server you are backing up.
- 4 Type `df -n` and then press **Enter**. A list of the mounted filesystems appears.

Note: The presence of `/cdrom` in the output confirms that the system correctly mounted the CD.

- 5 Label a blank tape with the following information:

[DNCS or Application Server] Key Files Backup [Date]
[Site Name]
[Software Version]
DBDS Maintenance CD x.x..x

Note: Customize the date, site name, and software version for the site you are backing up.

- 6 Choose one of the following options:
 - If you are backing up the key files to a tape in the DNCS or Application Server, go to *Backing Up the Key Files to Tape* (on page 23).
 - If you are backing up the key files to a tape in a remote host computer, go to *Backing Up the Key Files to a Remote Host Computer* (on page 23).
 - If you are backing up the key files to another directory, go to *Backing Up the Key Files to an NFS-Mounted Directory* (on page 24).

Backing Up the Key Files to Tape

Complete the following steps under these circumstances:

- You are backing up the key files of the DNCS to a tape in the DNCS, itself
- You are backing up the key files of the Application Server to a tape in the Application Server, itself

If you are backing up the key files of the Application Server to a tape in the DNCS, use the procedure in *Backing Up the Key Files to a Remote Host Computer* (on page 23), instead.

Note: If you have correctly followed the directions in this chapter, you should be logged in to an xterm window as root user.

- 1 Insert the blank tape into the tape drive of the DNCS or Application Server, whichever server you are backing up, and wait for the green light to stop flashing.
- 2 Type `/cdrom/cdrom0/s3/backup_restore/backupKeyFiles -v` and then press **Enter**. The system backs up the DNCS or Application Server key files and displays a message when the backup is complete.
- 3 When the backup is complete, eject the tape and store it in a safe place.
- 4 Type `eject cdrom` and then press **Enter**.
- 5 Remove the CD and store it in a safe place.

Backing Up the Key Files to a Remote Host Computer

Complete the following steps to back up the DNCS or Application Server key files to a tape in another computer—commonly referred to as a *remote host* computer.

Example: Use this procedure, for instance, if you are backing up the Application Server key files to a tape in the DNCS.

Note: If you have correctly followed the directions in this chapter, you should be logged in to an xterm window as root user.

- 1 Insert the blank tape into the tape drive of the remote host computer.
- 2 At the DNCS or Application Server, whichever server you are backing up, type `rsh [hostname or IP address] pwd` and then press **Enter**.

Notes:

- Substitute the host name or the IP address of the remote host computer for [hostname or IP address].
- The purpose of this command is to confirm that you can connect (remote shell) to the host computer without being prompted for a password.

- 3 Did the system prompt you for a password or deny you access after executing step 2?
 - If **yes**, call Cisco Services for assistance.
 - If **no**, go to step 4.

- 4 To back up the DNCS or Application Server key files, type `/cdrom/cdrom0/s3/backup_restore/backupKeyFiles -v -r [hostname or IP address]:[tape device]` and then press **Enter**.

Note: Type the entire command on one line.

Examples:

- `/cdrom/cdrom0/s3/backup_restore/backupKeyFiles -v -r dnscatm:/dev/rmt/0h`
- `/cdrom/cdrom0/s3/backup_restore/backupKeyFiles -v -r 192.168.44.71:/dev/rmt/0h`

Result: The system backs up the DNCS or Application Server key files, ejects the tape, and displays a message when the backup is complete.

- 5 When the backup is complete, remove the tape and store it in a safe place.
- 6 Type **eject cdrom** and then press **Enter**.
- 7 Remove the CD and store it in a safe place.

Backing Up the Key Files to an NFS-Mounted Directory

The key files can be backed up to a directory that is located on a Network File System (NFS). You must be able to access the NFS directory through the `/net/<remotehost>/<path_to_NFS_directory>` directory structure. In addition, the `/net/<remotehost>/<path_to_NFS_directory>/<hostname>` directory must already exist, and you must have write-access to the directory or the backup will fail.

Procedures for setting up the NFS are beyond the scope of this document. See your System Administrator, if necessary, for help in setting up the NFS.

Complete the following steps to back up the key files to a specified directory on the DNCS or the Application Server.

- 1 Make sure that you have write-access to the NFS-mounted filesystem and backup directory.
- 2 To back up the DNCS or Application Server key files, type `/cdrom/cdrom0/s3/backup_restore/backupKeyFiles -v -B /net/<remotehost>/<path_to_NFS_directory>` and then press **Enter**.

Notes:

- The `< remotehost >` represents the hostname of the remote computer which is exporting (or holds) the filesystem into which you will write or back up.
- The `< path_to_NFS_directory >` represents the directory path on the remote host which holds the backup files.

- 3 When the backup is complete, type **eject cdrom** and then press **Enter**.
- 4 In the space provided, write down the exact path of the directory into which you have written the backup.

Note: The path for the backup file you just created is /net/<remotehost>/<path_to_NFS_directory>/<hostname >. The file name is **KeyFiles.tar**.

Note: You will need this exact path should you ever have to restore the key files from the NFS-mounted directory.

4

Restoration Procedures

Introduction

Use the procedures in this section to restore the file system and key files on the DNCS and the Application Server, as well as the Informix database on the DNCS.

Important: If you are performing a full system restoration, be certain to complete these procedures in the order presented in this chapter.

In This Chapter

■ Restore the DNCS File System	28
■ Restore the Informix Database	36
■ Restore the Application Server File System	42
■ Restore the Key Files	49

Restore the DNCS File System

Overview

Consider the following points about the restoration of the DNCS file system.

Prerequisite

You need the tape from your most recent backup of the file system before restoring the file system.

Important: Be sure your tapes are write-protected before you use them to restore the system.

File System Restore Script Options

The script that restores the DNCS file system is called **restoreFileSystems**. You can run the `restoreFileSystems` script with the following options:

- `-l` – Local-tape-drive. Specifies tape drive to use on local host computer. (for example – `/dev/rmt/0h`)
- `-r` – Remote-tape-drive. Specifies tape drive on a remote host computer. (for example – `sparky:/dev/rmt/0h` or `192.168.1.10: /dev/rmt/0h`)
- `-B` – Backup directory. Specifies the directory that contains the backup from which the file system will be restored. The backup directory must be on an NFS-mounted filesystem.
- `-v` – verbose. Verbose output.
- `-i` – interactive. Runs the restoration script in interactive mode.
- `-h` – help. Provides a brief description of the valid options.

Note: The `-l`, `-r`, and `-B` options are mutually exclusive of one another; only one of them can be used.

Preparing to Restore the DNCS File System

Complete the following steps to prepare to restore the DNCS file system.

Important: You need to know the IP address and the netmask of the DNCS in order to complete this procedure.

- 1 Follow the procedures in *Stopping System Components* (on page 57) to stop the system components.
- 2 Open an xterm window on the DNCS.

- 3 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**.
- 4 Insert the CD labeled **DBDS Maintenance CD** into the CD drive of the DNCS.
- 5 Type **shutdown -y -g0 -i0** and then press **Enter** on *both* the DNCS and the Application Server. The system halts all processes and an **ok** prompt appears.
- 6 At the ok prompt on the DNCS, type **boot cdrom - SAsShell** and then press **Enter**. The DNCS boots into the OpenWindows environment.

Notes:

- When the system boots into the OpenWindows environment, it searches its non-volatile RAM for configuration information.
 - If the system is unable to locate its configuration information (a rare occurrence), it prompts you for the information it needs through the Solaris Installation menu.
- 7 In the process of booting, did the Solaris Installation menu appear?
 - If **yes**, go to step 8.
 - If **no** (the system successfully found the configuration information it needed), go to step 9.
 - 8 Complete the following steps on the Solaris Installation menu, as requested.

Note: The System Identification windows may not require you to configure all of the following items. Configure only those items that the system presents.

 - a At the Solaris Installation menu, select **Continue**.
 - b At the Identify This System menu, select **Continue**.
 - c At the Hostname menu, type the hostname of the DNCS and then select **Continue**.
 - d At the IP Address menu, type the IP address of the DNCS and then select **Continue**.
 - e At the NIS menu, select **None** and then click **Continue**.
 - f At the Subnets menu, select **Yes** at the System part of subnet question and then select **Continue**.
 - g At the Netmask menu, type the netmask of the DNCS and then select **Continue** (or just select Continue to accept the default value of 255.255.255.0).
 - h At the IPv6 menu, choose **No** and then select **Continue**. The Confirm Information window opens that allows you to review all of the configuration information you have just submitted.

- i Review the data on the Confirm Information window and correct anything that needs to be changed; then, select **Continue**.
 - j At the Name Service window, select **None** and then select **Continue**. The Confirm Information window reappears.
 - k Review the data on the Confirm Information window and correct anything that needs to be changed; then select **Continue**. An xterm window opens.
- 9 Choose one of the following options:
- If you are using the tape drive of the DNCS to restore the file system, insert your most recent file system backup tape into the tape drive of the DNCS.
 - If you are using the tape drive of a remotely located computer to restore the file system, insert your most recent file system backup tape into the tape drive of the remotely located computer.
- 10 Type **cd /tmp/cdrom/backup_restore** and then press **Enter**. The /tmp/cdrom/backup_restore directory becomes the working directory.
- 11 Choose one of the following options:
- If you are restoring from an NFS-mounted directory, go to *Preparing to Restore the DNCS File System from an NFS-Mounted Directory* (on page 30).
 - If you are using the tape drive of the DNCS to restore the file system, go to *Restoring the DNCS File System* (on page 31).
 - If you are using the tape drive of a remotely located computer to restore the file system, go to *Restoring the DNCS File System from a Remote Host Computer* (on page 32).

Preparing to Restore the DNCS File System from an NFS-Mounted Directory

To prepare for the restoration of the DNCS file system from an NFS-mounted directory, complete the following steps.

- 1 Type **mkdir /tmp/<remotehost>** and then press **Enter**. The system creates the /tmp/<remotehost> directory.
Note: The <remotehost> represents the hostname of the remote computer that holds the file system which you used for the backup.
- 2 Configure the appropriate interface to the NFS files server.
Example: **# ifconfig ce0 inet 192.168.2.20 netmask 255.255.255.0 up**
- 3 Type **mount <remotehost>: /<path_to_NFS_directory> /tmp/<remotehost>** and then press **Enter**.
Note: The <path_to_NFS_directory> represents the directory path on the remote host that holds the backup files.
- 4 Type **ls** and then press **Enter**. Look for the hostname of the DNCS.

- 5 Type `cd /tmp/remotehost/<hostname>/<date_time_stamp>` and then press **Enter**. The specified directory becomes the working directory.
- 6 Go to *Restoring the DNCS File System from an NFS-Mounted Directory* (on page 34).

Restoring the DNCS File System

Complete the following steps if you are restoring the file system of the DNCS from a tape in the DNCS.

Note: If you have correctly followed the directions in this chapter, you should be logged in to an xterm window as root user.

- 1 Type `/restoreFileSystems -v` and then press **Enter**. The system restores the DNCS file system and displays a message when the restoration is complete.
- 2 When the restoration is complete, remove the tape and store it in a safe place.
- 3 Type `/usr/sbin/shutdown -y -i0 -i6` and then press **Enter**. The DNCS reboots and the Common Desktop Environment (CDE) login window appears.

Note: The Enterprise 450, the Sun Fire V880, and the Sun Fire V890 DNCS will reboot a few times as part of the restoration process.

- 4 Log on to the CDE as **root** user.
- 5 Follow the *Restore the Informix Database* (on page 36) procedures to restore the Informix database. After restoring the Informix database, go to step 6.

Important: The final few steps in restoring the Informix database require that you eject the DBDS Maintenance CD and restart the system components. Stop right before you eject the CD and restart the system components.

- 6 Have you just restored the file system of an Enterprise 450, Sun Fire V440, V445, V880, or V890 DNCS?

- If **yes**, go to step 7; you now need to enable disk mirroring.

Note: The DBDS Maintenance CD should still be in the CD drive of the DNCS and you should still be logged in as root user to an xterm window.

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

- 7 Type `/cdrom/cdrom0/s3/backup_restore/mirrState -a` and then press **Enter**. The system displays the following message:

WARNING!

Proceeding beyond this point will Attach all Controller 2 submirrors.

Are you certain you want to proceed?

- 8 Type **y** and then press **Enter**. The system enables the disk mirroring functions on the DNCS.

Note: Depending upon your system configuration, it may take up to an hour for all of the data to become mirrored.

- 9 Are you restoring the file system of an Enterprise 450 DNCS?
 - If **yes**, type `/cdrom/cdrom0/s3/sai/scripts/Media/add_hotspares` and then press **Enter**. The system creates hot spare disks and associates them with the metadevices.
 - If **no**, go to step 10.
- 10 Type **eject cdrom** and then press **Enter**. The system ejects the CD.
- 11 Click the right mouse button on the DNCS and select **Log Out**. The root user logs off and the CDE window returns.
- 12 Log on to the CDE window as **dncs** user.
- 13 Does the Application Server display an **ok** prompt?
 - If **yes**, type **boot** and press **Enter** at the ok prompt on the Application Server; then, log on to the Application Server as dncs user.
 - If **no**, go to step 14.
- 14 Follow the procedures in *Restarting System Components* (on page 61) to restart Spectrum, the DNCS, and the Application Server.

Restoring the DNCS File System from a Remote Host Computer

Complete the following steps to restore the DNCS file system from a tape in another computer – commonly referred to as a *remote host* computer.

Note: If you have correctly followed the directions in this chapter, you should be logged on to an xterm window as root user.

- 1 Type `/tmp/cdrom/backup_restore/restoreFileSystems -v -r [hostname or IP address]:[tape device]` and then press **Enter**. The system restores the DNCS file system and displays a message when the restoration is complete.

Notes:

- Substitute the hostname or IP address of the remotely located computer for [hostname or IP address].
- Type the command on one line.

Example:

```
/tmp/cdrom/backup_restore/restoreFileSystems -v -r 192.168.44.71:/dev/rmt/0h
```

- 2 When the restoration is complete, eject the tape and store it in a safe place.
- 3 Type `/usr/sbin/shutdown -y -i0 -i6` and then press **Enter**. The DNCS reboots and the Common Desktop Environment (CDE) login window appears.

Note: The Sun Enterprise 450 and the Sun Fire V440, V445, V880, or V890 DNCS will reboot a few times as part of the restoration process.

- 4 Log on to the CDE as **root** user.

- 5 Follow the *Restore the Informix Database* (on page 36) procedures to restore the Informix database.

Note: After restoring the Informix database, go to step 6.

Important: The final few steps in restoring the Informix database require that you eject the DBDS Maintenance CD and restart the system components. Stop right before you eject the CD and restart the system components.
- 6 Have you just restored the file system of an Enterprise 450, Sun Fire V880, or Sun Fire V890 DNCS?
 - If **yes**, go to step 7; you now need to enable disk mirroring.

Note: The DBDS Maintenance CD should still be in the CD drive of the DNCS and you should still be logged in as root user to an xterm window.
 - If **no**, go to step 10.
- 7 Type `/cdrom/cdrom0/s3/backup_restore/mirrState -a` and then press **Enter**. The system displays the following message:

WARNING!
Proceeding beyond this point will Attach all Controller 2 submirrors.
Are you certain you want to proceed?
- 8 Type **y** and then press **Enter**. The system enables the disk mirroring functions on the DNCS.

Note: Depending upon your system configuration, it may take up to an hour for all of the data to become mirrored.
- 9 Are you restoring the file system of an Enterprise 450 DNCS?
 - If **yes**, type `/cdrom/cdrom0/s3/sai/scripts/Media/add_hotspares` and then press **Enter**. The system creates hot spare disks and associates them with the metadevices.
 - If **no**, go to step 10.
- 10 Type `eject cdrom` and then press **Enter**. The system ejects the CD.
- 11 Click the right mouse button on the DNCS and select **Log Out**. The root user logs off and the CDE window returns.
- 12 Log on to the CDE as **dncs** user.
- 13 Does the Application Server display an **ok** prompt?
 - If **yes**, type **boot** and press **Enter** at the ok prompt on the Application Server; then, log on to the Application Server as **dncs** user.
 - If **no**, go to step 14.
- 14 Follow the procedures in *Restarting System Components* (on page 61) to restart Spectrum, the DNCS, and the Application Server.

Restoring the DNCS File System from an NFS-Mounted Directory

Complete the following steps to restore the file system from a specified backup directory on the DNCS.

- 1 Type `/tmp/cdrom/backup_restore/restoreFileSystems -v -B <path_to_NFS_directory>` and then press **Enter**.

Note: Substitute the full directory path that you recorded in step 4 e) of *Backing Up the File System to an NFS-Mounted Directory* (on page 16).

- 2 When the restoration is complete, type `/usr/sbin/shutdown -y -i0 -i6` and then press **Enter**. The DNCS reboots and the Common Desktop Environment (CDE) login window appears.

Note: The Sun Enterprise 450 and Sun Fire V440, V445, V880, or V890 DNCS will reboot a few times as part of the restoration process.

- 3 Log on to the CDE as **root** user.
- 4 Follow the *Restore the Informix Database* (on page 36) procedures to restore the Informix database. After restoring the Informix database, go to step 6.

Important: The final few steps in restoring the Informix database require that you eject the DBDS Maintenance CD and restart the system components. Stop right before you eject the CD and restart the system components.

- 5 Have you just restored the file system of an Enterprise 450, Sun Fire V440, V445, V880, or V890 DNCS?

- If **yes**, go to step 6; you now need to enable disk mirroring.

Note: The DBDS Maintenance CD should still be in the CD drive of the DNCS and you should still be logged in as root user to an xterm window.

- If **no**, go to step 9.

- 6 Type `/cdrom/cdrom0/s3/backup_restore/mirrState -a` and then press **Enter**. The system displays the following message:

WARNING!

Proceeding beyond this point will Attach all Controller 2 submirrors.

Are you certain you want to proceed?

- 7 Type **y** and then press **Enter**. The system enables the disk mirroring functions on the DNCS.

Note: Depending upon your system configuration, it may take up to an hour for all of the data to become mirrored.

- 8 Are you restoring the file system of an Enterprise 450 DNCS?

- If **yes**, type `/cdrom/cdrom0/s3/sai/scripts/Media/add_hotspares` and then press **Enter**. The system creates hot spare disks and associates them with the metadevices.

- If **no**, go to step 9.

- 9 Type **eject cdrom** and then press **Enter**. The system ejects the CD.
- 10 Click the right mouse button on the DNCS and select **Log Out**. The root user logs off and the CDE window returns.
- 11 Log on to the CDE window as **dncs** user.
- 12 Does the Application Server display an **ok** prompt?
 - If **yes**, type **boot** and press **Enter** at the ok prompt on the Application Server; then, log on to the Application Server as dncs user.
 - If **no**, go to step 13.
- 13 Follow the procedures in *Restarting System Components* (on page 61) to restart Spectrum, the DNCS, and the Application Server.

Restore the Informix Database

This section contains information that guides you through the process of restoring the Informix database.

Prevent the Loss of Data

When you restore the database, you restore it with data that was present in the database at the time of the backup. Unless you coordinate the restore procedures with your billing vendor, you run the risk of losing data that was transmitted to your system since the time of the backup. By adhering to the following guidelines, you can minimize the risk that you will lose data when you restore the database.

Follow these guidelines when restoring the database:

- Before restoring the database, contact your billing vendor and request that the billing vendor send no more transactions until the restoration is complete.
- If your system is still functional at the time of the restore, request that the billing vendor download from the DNCS the latest set of IPPV billing transactions before you start the restoration process. This way, you have the most current record of subscriber IPPV purchases.
- After completing the restoration of the database, contact the billing vendor and request that the billing vendor re-transmit all transactions since the date of the backup tape you used. For example, have the billing vendor re-transmit transactions relating to DHCT service levels, PPV event definitions, and package authorizations.

Database Restore Script Options

The script that restores the databases is called **restoreDatabase**. You can run the `restoreDatabase` script with the following options:

- `-l` – Local-tape-drive. Specifies tape drive to use on local host.
(for example – `/dev/rmt/0h`)
- `-r` – Remote-tape-drive. Specifies tape drive on a remote host.
(for example – `sparky: /dev/rmt/0h` or `192.168.1.10: /dev/rmt/0h`)
- `-c` – check-database. Checks the integrity of the databases. (Does not fix if errors are found.)
- `-v` – verbose. Verbose output.

- *-p* – physical-restore. Performs only a physical restoration of the database and does not restore the logical logs.
Important: This option must be used *only* on the secondary Informix server before activating the Replicated Database.
- *-i* – interactive. Runs the restoration in interactive mode.
- *-h* – help. Provides a brief description of the valid options.

How Many Tapes Are in the Backup?

You may have used more than one backup tape when you backed up the Informix database. Refer to one of the following procedures based on whether you used more than one backup tape:

- If you used *only* one tape to back up the Informix database, refer to the *Restoring the Informix Database Using One Backup Tape* (on page 37) procedure to restore the database.
- If you used *more than one* tape to back up the Informix database, refer to the *Restoring the Informix Database Using More Than One Backup Tape* (on page 39) procedure to restore the database.

Restoring the Informix Database Using One Backup Tape

Complete the following steps to restore the DNCS and Application Server databases using only one backup tape.

Note: You need the tape from your most recent database backup in order to restore the Informix database.

Important: Be sure your tape is write-protected before you use it to restore the database.

- 1 If necessary, follow the procedures in *Stopping System Components* (on page 57) to stop Spectrum, the Application Server, and the DNCS.
- 2 If necessary, open an xterm window on the DNCS.
- 3 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**.
- 4 Have you just restored the DNCS file system?
 - If **yes**, go to step 5.
 - If **no**, go to step 6.

- 5 Complete the following steps. (You have just restored the DNCS file system.)
 - a Type `./dvs/dnCS/bin/dnCSSetup` and then press **Enter**. The system establishes the root user environment.

Important: Be sure to type the dot, followed by a space, prior to typing `/dvs`.
 - b Type `/export/home/informix/bin/formatDbSpace.sh` and then press **Enter**. The system formats the database partitions.
- 6 Insert the CD labeled **DBDS Maintenance CD** into the CD drive of the DNCS.
- 7 Type `df -n` and then press **Enter**. A list of the mounted filesystems appears.

Note: The presence of `/cdrom` in the output confirms that the system correctly mounted the CD.
- 8 Insert your most recent copy of the DNCS database backup tape into the tape drive of the DNCS and wait for the green light on the tape drive to stop flashing.
- 9 Type `/cdrom/cdrom0/s3/backup_restore/restoreDatabase -v` and then press **Enter**. The **Is there more than 1 tape in this backup? [Y/N]** message appears.
- 10 Type `n` and then press **Enter**. The system displays a message about ensuring that the backup tape is in the drive.
- 11 Press **Enter**. The system restores the database.
- 12 When the **Successfully restored the database** message appears, remove the tape and store it in a safe place.
- 13 Complete the following steps to eject the CD.
 - a Type `cd /` and then press **Enter**.
 - b Type `/etc/init.d/informix stop` and then press **Enter**. The system stops the Informix oninit processes.
 - c Type `eject cdrom` and then press **Enter**.
 - d Type `/etc/init.d/informix start` and then press **Enter**. The system restarts the Informix oninit processes.
- 14 Remove the CD and store it in a safe place.
- 15 Type `exit` and then press **Enter** to log out the root user.
- 16 Prior to restoring the Informix database, did you restore the file system on the DNCS?
 - If **yes**, return to one of the following sections:
 - Step 6 in *Restoring the DNCS File System* (on page 31)
 - Step 6 in *Restoring the DNCS File System from a Remote Host Computer* (on page 32)
 - Step 5 in *Restoring the DNCS File System from an NFS-Mounted Directory* (on page 34).
 - If **no**, go to step 17.
- 17 Follow the procedures in *Restarting System Components* (on page 61) to restart Spectrum, the DNCS, and the Application Server.

Restoring the Informix Database Using More Than One Backup Tape

Complete the following steps to restore the DNCS and Application Server databases using more than one backup tape.

Note: You need the tapes from your most recent database backup in order to restore the Informix database.

Important: Be sure your tapes are write-protected before you use them to restore the database.

- 1 If necessary, follow the procedures in *Stopping System Components* (on page 57) to stop Spectrum, the Application Server, and the DNCS.
- 2 If necessary, open an xterm window on the DNCS.
- 3 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**.
- 4 Have you just restored the DNCS file system?
 - If **yes**, go to step 5.
 - If **no**, go to step 6.
- 5 Complete the following steps. (You have just restored the DNCS file system.)
 - a Type **./dvs/dnCS/bin/dnCSSetup** and then press **Enter**. The system establishes the root user environment.

Important: Be sure to type the dot, followed by a space, prior to typing **/dvs**.
 - b Type **/export/home/informix/bin/formatDbSpace.sh** and then press **Enter**. The system formats the database partitions.
- 6 Insert the CD labeled **DBDS Maintenance CD** into the CD drive of the DNCS.
- 7 Type **df -n** and then press **Enter**. A list of the mounted filesystems appears.

Note: The presence of **/cdrom** in the output confirms that the system correctly mounted the CD.
- 8 Type **/cdrom/cdrom0/s3/backup_restore/restoreDatabase -v** and then press **Enter**.
- 9 When the **Is there more than 1 tape in this backup? [Y/N]** message appears, type **y** and then press **Enter**. The system displays a message about ensuring that the *last* backup tape is in the tape drive.

Note: You are instructed to load the *last* tape because a configuration file is appended to the final tape in the backup series during the backup procedure.
- 10 Insert the *last* tape from your most recent database backup and press **Enter**.

Results:

- The system examines the configuration file.
- The system displays a message similar to the following:
Please mount tape 1 on [device name] and press Return to continue.

- 11 Remove the tape that is currently in the tape drive.
- 12 Insert the *first* tape from your most recent database backup and press **Enter**.
Results:
 - The system displays archive information from the tape.
 - The message **Continue restore? (y/n)** appears.
- 13 Type **y** and then press **Enter**. The **Do you want to back up the logs? (y/n)** message appears.
- 14 Type **n** and then press **Enter**.
Results:
 - The system begins restoring the database.
 - The **Please mount tape 2 on [device name] and press Return to continue** message appears after several minutes.
- 15 Remove the first tape and insert the second tape from your most recent database backup and then press **Enter**.
Results:
 - The restoration of the database continues.
 - If there is another tape in the backup series, the system will prompt you to insert the next tape.
- 16 Repeat step 15 for as many backup tapes that are in the backup series.
- 17 When the **Restore a level 1 archive? (y/n)** message appears, type **n** and then press **Enter**.
- 18 When the **Do you want to restore log tapes? (y/n)** message appears, type **n** and then press **Enter**.
- 19 When the **DNCS Informix partition restore completed and verified** message appears, remove the final tape and store it in a safe place.
- 20 Complete the following steps to eject the CD.
 - a Type **cd /** and then press **Enter**.
 - b Type **/etc/init.d/informix stop** and then press **Enter**. The system stops the Informix oninit processes.
 - c Type **eject cdrom** and then press **Enter**.
 - d Type **/etc/init.d/informix start** and then press **Enter**. The system restarts the Informix oninit processes.
- 21 Remove the CD and store it in a safe place.
- 22 Type **exit** and then press **Enter** to log out the root user.

- 23** Prior to restoring the Informix database, did you restore the file system on the DNCS?
- If **yes**, return to one of the following sections:
 - Step 6 in *Restoring the DNCS File System* (on page 31)
 - Step 6 in *Restoring the DNCS File System from a Remote Host Computer* (on page 32)
 - Step 5 in *Restoring the DNCS File System from an NFS-Mounted Directory* (on page 34)
 - If **no**, go to step 24.
- 24** Follow the procedures in *Restarting System Components* (on page 61) to restart the DNCS, the Application Server, and Spectrum.

Restore the Application Server File System

Overview

Consider the following points about the restoration of the Application Server file system.

Prerequisite

You need the tape from your most recent backup of the file system before restoring the file system.

Important: Be sure your tapes are write-protected before you use them to restore the system.

File System Restore Script Options

The script that restores the Application Server file system is called **restoreFileSystems**. You can run the `restoreFileSystems` script with the following options:

- `-l` – Local-tape-drive. Specifies tape drive to use on local host computer. (for example – `/dev/rmt/0h`)
- `-r` – Remote-tape-drive. Specifies tape drive on a remote host computer. (for example – `sparky:/dev/rmt/0h` or `192.168.1.10:/dev/rmt/0h`)
- `-B` – Backup directory. Specifies the directory that contains the backup from which the file system will be restored. The backup directory must be on an NFS-mounted filesystem.
- `-v` – verbose. Verbose output.
- `-i` – interactive. Runs the restoration script in interactive mode.
- `-h` – help. Provides a brief description of the valid options.

Note: The `-l`, `-r`, and `-B` options are mutually exclusive of one another; only one of them can be used.

Preparing to Restore the Application Server File System

Complete the following steps to prepare to restore the Application Server file system.

Important: You need to know the IP address and the netmask of the Application Server in order to complete this procedure.

- 1 Follow the procedures in *Stopping System Components* (on page 57) to stop the system components.
- 2 Open an xterm window on the Application Server.
- 3 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**.
- 4 Insert the CD labeled **DBDS Maintenance CD** into the CD drive of the Application Server.
- 5 Type **shutdown -y -g0 -i0** and then press **Enter** on the Application Server. The system halts all processes on the Application Server and an **ok** prompt appears.
- 6 At the **ok** prompt, type **boot cdrom - SAsHell** and then press **Enter**. The Application Server boots into the OpenWindows environment.

Notes:

- When the system boots into the OpenWindows environment, it searches its non-volatile RAM for configuration information.
 - If the system is unable to locate its configuration information (a rare occurrence), it prompts you for the information it needs through the Solaris Installation menu.
 - If you are restoring a Sun Fire V240 or V245 Application Server, you may be asked if you want to install a *DNCS Demo*. Type **n** and press **Enter**.
- 7 Did your system display the following message?
Not enough memory for a Graphical installation. Graphical installation requires 288 MB of memory. Found 256 MB of memory. Reverting to text-based installation.
 - If **yes**, just skip to step 10. If the Application Server you are restoring has less than 256 MB of memory, the server will be unable to boot into the OpenWindows environment.
 - If **no**, go to step 8.
 - 8 In the process of booting, did the Solaris Installation menu appear?
 - If **yes**, go to step 9.
 - If **no** (the system successfully found the configuration information it needed), go to step 10.

- 9 Complete the following steps on the Solaris Installation menu.
 - a At the Solaris Installation menu, select **Continue**.
 - b At the Identify This System menu, select **Continue**.
 - c At the Hostname menu, type the hostname of the Application Server and then select **Continue**.
 - d At the IP Address menu, type the IP address of the Application Server and then select **Continue**.
 - e At the Subnets menu, select **Yes** at the System part of subnet question and then select **Continue**.
 - f At the Netmask menu, type the netmask of the Application Server and then select **Continue** (or just select Continue to accept the default value of 255.255.255.0).
 - g At the IPv6 menu, choose **No** and then select **Continue**. The Confirm Information window opens that allows you to review all of the configuration information you have just submitted.
 - h Review the data on the Confirm Information window and correct anything that needs to be changed; then, select **Continue**.
 - i At the Name Service window, select **None** and then select **Continue**. The Confirm Information window reappears.
 - j Review the data on the Confirm Information window and correct anything that needs to be changed; then select **Continue**. An xterm window opens.
- 10 Choose one of the following options:
 - If you are using the tape drive of the Application Server to restore the file system, insert your most recent file system backup tape into the tape drive of the Application Server.
 - If you are using the tape drive of a remotely located computer to restore the file system, insert your most recent file system backup tape into the tape drive of the remotely located computer.
 - If you are restoring your file system from a backup directory that is located on the NFS, go to *Preparing to Restore the Application Server File System from an NFS-Mounted Directory* (on page 45).
- 11 Type `cd /tmp/cdrom/backup_restore` and then press **Enter**. The `/tmp/cdrom/backup_restore` directory becomes the working directory.
- 12 Choose one of the following options:
 - If you are using the tape drive of the Application Server to restore the file system, go to *Restoring the Application Server File System* (on page 45).
 - If you are using the tape drive of a remotely located computer to restore the file system, go to *Restoring the Application Server File System from a Remote Host Computer* (on page 46).

Preparing to Restore the Application Server File System from an NFS-Mounted Directory

To prepare for the restoration of the Application Server file system from an NFS-mounted directory, complete the following steps.

- 1 Type **mkdir /tmp/<remotehost>** and then press **Enter**. The system creates the /tmp/<remotehost> directory.
Note: The <remotehost> represents the hostname of the remote computer that holds the file system which you used for the backup.
- 2 Configure the appropriate interface to the NFS files server.
Example: **# ifconfig ce0 inet 192.168.2.20 netmask 255.255.255.0 up**
- 3 Type **mount <remotehost>: /<path_to_NFS_directory>/tmp/<remotehost>** and then press **Enter**.
Note: The <path_to_NFS_directory> represents the directory path on the remote host that holds the backup files.
- 4 Type **ls** and then press **Enter**. Look for the hostname of the Application Server.
- 5 Type **cd /tmp/remotehost/<hostname>/<date_time_stamp>** and then press **Enter**. The specified directory becomes the working directory.
- 6 Go to *Restoring the Application Server File System from an NFS-Mounted Directory* (on page 47).

Restoring the Application Server File System

Complete the following steps if you are restoring the file system of the Application Server from a tape in the Application Server.

Note: If you have correctly followed the directions in this chapter, you should be logged in to an xterm window as root user.

- 1 Type **/restoreFileSystems -v** and then press **Enter**. The system restores the Application Server file system and displays a message when the restoration is complete.
- 2 When the restoration is complete, remove the tape and store it in a safe place.
- 3 Type **/usr/sbin/shutdown -y -i0 -i6** and then press **Enter**. The Application Server reboots and the Common Desktop Environment (CDE) login window appears.
- 4 Log on to the CDE as **root** user.

- 5 Have you just restored the file system of a Sun Fire V240 or V245 Application Server?
 - If **yes**, type `/cdrom/cdrom0/s3/backup_restore/mirrState -a` and then press **Enter**. The system displays the following message:
WARNING!
Proceeding beyond this point will Attach all Controller 2 submirrors.
Are you certain you want to proceed?
 - If **no**, go to step 7.
- 6 Type **y** and then press **Enter**. The system enables the disk mirroring functions on the Application Server.

Note: Depending upon your system configuration, it may take up to an hour for all of the data to become mirrored.
- 7 Type **eject cdrom** and then press **Enter**. The system ejects the CD.
- 8 Click the right mouse button on the Application Server and select **Log Out**. The root user logs off and the CDE window returns.
- 9 Log on to the CDE window as **dncs** user.
- 10 Type **boot** and press **Enter** at the ok prompt on the Application Server; then, log on to the Application Server as dncs user.
- 11 Follow the procedures in *Restarting System Components* (on page 63) to restart Spectrum, the DNCS, and the Application Server.

Restoring the Application Server File System from a Remote Host Computer

Complete the following steps to restore the Application Server file system from a tape in another computer—commonly referred to as a *remote host* computer.

Example: Use this procedure, for instance, if you are restoring the Application Server file system from a tape in the DNCS.

Note: If you have correctly followed the directions in this chapter, you should be logged on to an xterm window as root user.

- 1 Type `/tmp/cdrom/backup_restore/restoreFileSystems -v -r [hostname or IP address]:[tape device]` and then press **Enter**. The system restores the Application Server file system and displays a message when the restoration is complete.

Notes:

- Substitute the hostname or IP address of the remotely located computer for [hostname or IP address].
- Type the command on one line.

Example:

`/tmp/cdrom/backup_restore/restoreFileSystems -v -r 192.168.44.71:/dev/rmt/0h`

- 2 When the restoration is complete, eject the tape and store it in a safe place.

- 3 Type `/usr/sbin/shutdown -y -i0 -i6` and then press **Enter**. The Application Server reboots and the Common Desktop Environment (CDE) login window appears.
- 4 Log on to the CDE as **root** user.
- 5 Have you just restored the file system of a Sun Fire V240 or V245 Application Server?
 - If **yes**, type `/cdrom/cdrom0/s3/backup_restore/mirrState -a` and then press **Enter**. The system displays the following message:
WARNING!
Proceeding beyond this point will Attach all Controller 2 submirrors.
Are you certain you want to proceed?
 - If **no**, go to step 7.
- 6 Type **y** and then press **Enter**. The system enables the disk mirroring functions on the Application Server.
- 7 Type `eject cdrom` and then press **Enter**. The system ejects the CD.
- 8 Click the right mouse button on the Application Server and select **Log Out**. The root user logs off and the CDE window returns.
- 9 Log on to the CDE as **dncs** user.
- 10 Type **boot** and press **Enter** at the ok prompt on the Application Server; then, log on to the Application Server as **dncs** user.
- 11 Follow the procedures in *Restarting System Components* (on page 61) to restart Spectrum, the DNCS, and the Application Server.

Restoring the Application Server File System from an NFS-Mounted Directory

Complete the following steps to restore the file system from a specified backup directory on the Application Server.

- 1 Type `/tmp/cdrom/backup_restore/restoreFileSystems -v -B <path_to_NFS_directory>` and then press **Enter**.
Note: Substitute the full directory path that you recorded in step 4 e) of *Backing Up the Application Server File System to an NFS-Mounted Directory* (on page 16).
- 2 When the restoration is complete, type `/usr/sbin/shutdown -y -i0 -i6` and then press **Enter**. The Application Server reboots and the Common Desktop Environment (CDE) login window appears.
- 3 Log on to the CDE as **root** user.

- 4 Have you just restored the file system of a Sun Fire V240 or V245 Application Server?
 - If **yes**, type `/cdrom/cdrom0/s3/backup_restore/mirrState -a` and then press **Enter**. The system displays the following message:
WARNING!
Proceeding beyond this point will Attach all Controller 2 submirrors.
Are you certain you want to proceed?
 - If **no**, go to step 6.
- 5 Type **y** and then press **Enter**. The system enables the disk mirroring functions on the Application Server.
- 6 Type **eject cdrom** and then press **Enter**. The system ejects the CD.
- 7 Click the right mouse button on the Application Server and select **Log Out**. The root user logs off and the CDE window returns.
- 8 Log on to the CDE window as **dncs** user.
- 9 Type **boot** and press **Enter** at the ok prompt on the Application Server; then, log on to the Application Server as dncs user.
- 10 Follow the procedures in *Restarting System Components* (on page 61) to restart Spectrum, the DNCS, and the Application Server.

Restore the Key Files

Overview

Consider the following points about the restoration of the DNCS or Application Server key files.

Prerequisite

You need the tape from your most recent backup of the key files before restoring the key files.

Important: Be sure your tapes are write-protected before you use them to restore the key files.

System Shutdown Required

In order to restore the DNCS or Application Server key files, system operators must shut down Spectrum, the DNCS, and the Application Server.

Key Files Restore Script Options

The script that restores the DNCS or Application Server key files is called **restoreKeyFiles**. You can run the `restoreKeyFiles` script with the following options:

- `-l` – Local-tape-drive. Specifies tape drive to use on local host computer. (for example – `/dev/rmt/0h`)
- `-r` – Remote-tape-drive. Specifies tape drive on a remote host computer. (for example – `sparky:/dev/rmt/0h` or `192.168.1.10: /dev/rmt/0h`)
- `-v` – verbose. Verbose output.
- `-h` – help. Provides a brief description of the valid options.

Note: The `-l` and `-r` options are mutually exclusive of one another; only one of them can be used.

Preparing to Restore the Key Files

Complete the following steps to prepare to restore the DNCS or Application Server key files.

- 1 Follow the procedures in *Stopping System Components* (on page 57) to stop Spectrum, the Application Server, and the DNCS.
- 2 If necessary, open an xterm window on the DNCS or the Application Server, depending upon which server you are restoring.

- 3 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**.
- 4 Insert the CD labeled **DBDS Maintenance CD** into the CD drive of the DNCS or Application Server, depending upon which server you are restoring.
- 5 Type **df -n** and then press **Enter**. A list of the mounted filesystems appears.

Note: The presence of **/cdrom** in the output confirms that the system correctly mounted the CD.
- 6 Choose one of the following options:
 - If you are going to restore the key files from a tape in the DNCS or Application Server, insert your most recent key files backup tape into the tape drive of the DNCS or Application Server, depending upon which server you are restoring, and wait for the green light to stop flashing.
 - If you are going to restore the key files from a tape in a remote host computer, insert your most recent key files backup tape into the tape drive of the remote host computer.
- 7 Choose one of the following options:
 - If you are using the tape drive of the DNCS or Application Server to restore the key files, go to *Restoring the DNCS or Application Server Key Files* (on page 51).
 - If you are using the tape drive of a remotely located computer to restore the key files, go to *Restoring the Key Files from a Remote Host Computer* (on page 52).
 - If you are restoring the key files from a file on an NFS-mounted directory, go to *Restoring the Key Files from an NFS-Mounted Directory* (on page 53).

Restoring the DNCS or Application Server Key Files

Complete the following steps under these circumstances:

- You are restoring the key files of the DNCS from a tape in the DNCS, itself
- You are restoring the key files of the Application Server from a tape in the Application Server, itself

If you are restoring the key files of the Application Server from a tape in the DNCS, use the procedure in *Restoring the Key Files from a Remote Host Computer* (on page 52), instead.

Note: If you have correctly followed the directions in this chapter, you should be logged in to an xterm window as root user.

- 1 Type `/cdrom/cdrom0/s3/backup_restore/restoreKeyFiles -v` and then press **Enter**. The system restores the DNCS or Application Server key files and displays a message when the restoration is complete.
- 2 When the restoration is complete, eject the tape and store it in a safe place.
- 3 Type `eject cdrom` and then press **Enter**.
- 4 Remove the CD and store it in a safe place.
- 5 Are you restoring the key files of the DNCS?
 - If **yes**, go to step 6.
 - If **no** (you are restoring the key files of the Application Server), type `/usr/sbin/shutdown -y -g0 -i6` and press **Enter**; then, go to step 7.
Result: The Application Server reboots.
- 6 Complete the following steps if you are restoring the key files of the DNCS.
 - a From an xterm window on the Application Server, type `su -` and then press **Enter**.
 - b Type the root password and then press **Enter**.
 - c On the Application Server, type `/usr/sbin/shutdown -y -g0 -i0` and then press **Enter**. The Application Server shuts down and the **ok** prompt appears.
 - d On the DNCS, type `/usr/sbin/shutdown -y -g0 -i6` and then press **Enter**. The DNCS reboots.
 - e Log on to the CDE of the DNCS as **dncs** user.
- 7 Is the Application Server still at the **ok** prompt?
 - If **yes**, go to step 8.
 - If **no**, go to step 9.

- 8 Complete the following steps to reboot the Application Server.
 - a Type **boot** and then press **Enter**. The Application Server reboots.
 - b Log on to the CDE of the Application Server as **dncs** user.
- 9 Follow the instructions in *Restarting System Components* (on page 61) to restart Spectrum, the DNCS, and the Application Server.

Restoring the Key Files from a Remote Host Computer

Complete the following steps to restore the DNCS or Application Server key files from a tape in another computer – commonly referred to as a *remote host* computer.

Example: Use this procedure, for instance, if you are restoring the Application Server key files from a tape in the DNCS.

Note: If you have correctly followed the directions in this chapter, you should be logged in to an xterm window as root user.

- 1 Type `/cdrom/cdrom0/s3/backup_restore/restoreKeyFiles -v -r [hostname or IP address]:/dev/rmt/0h` and then press **Enter**.

Note: Type the command on one line.

Examples:

- `/cdrom/cdrom0/s3/backup_restore/restoreKeyFiles -v -r dnccatm:/dev/rmt/0h`
- `/cdrom/cdrom0/s3/backup_restore/restoreKeyFiles -v -r 192.168.44.71:/dev/rmt/0h`

Result: The system restores the DNCS or Application Server key files and displays a message when the restoration is complete.

- 2 When the restoration is complete, eject the tape and store it in a safe place.
- 3 Type **eject cdrom** and then press **Enter**.
- 4 Remove the CD and store it in a safe place.
- 5 Are you restoring the key files of the DNCS?
 - If **yes**, go to step 6.
 - If **no** (you are restoring the key files of the Application Server), type `/usr/sbin/shutdown -y -g0 -i6` and press **Enter**; then, go to step 7. The Application Server reboots.

- 6 Complete the following steps if you are restoring the key files of the DNCS.
 - a From an xterm window on the Application Server, type **su -** and then press **Enter**.
 - b Type the root password and then press **Enter**.
 - c On the Application Server, type **/usr/sbin/shutdown -y -g0 -i0** and then press **Enter**. The Application Server shuts down and the **ok** prompt appears.
 - d On the DNCS, type **/usr/sbin/shutdown -y -g0 -i6** and then press **Enter**. The DNCS reboots.
 - e Log on to the CDE of the DNCS as **dncs** user.
- 7 Is the Application Server still at the **ok** prompt?
 - If **yes**, go to step 8.
 - If **no**, go to step 9.
- 8 Complete the following steps to reboot the Application Server.
 - a Type **boot** and then press **Enter**. The Application Server reboots.
 - b Log on to the CDE of the Application Server as **dncs** user.
- 9 Follow the instructions in *Restarting System Components* (on page 61) to restart Spectrum, the DNCS, and the Application Server.

Restoring the Key Files from an NFS-Mounted Directory

Complete the following steps to restore the key files from a specified backup directory on the DNCS or the Application Server.

- 1 From an xterm window, where you are logged on as root user, type **cd /** and then press **Enter**.
- 2 Type **/usr/bin/tar xvf <backup_directory>/KeyFiles.tar** and then press **Enter**.
Note: Substitute the full directory path that you recorded in step 4 of *Backing Up the Key Files to an NFS-Mounted Directory* (on page 24).
- 3 Type **eject cdrom** and then press **Enter**.
Note: Remove the CD and store it in a safe place.
- 4 Are you restoring the key files of the DNCS?
 - If **yes**, go to step 5.
 - If **no** (you are restoring the key files of the Application Server), follow these instructions.
 - a Type **/usr/sbin/shutdown -y -g0 -i6** and then press **Enter**. The Application Server reboots.
 - b Go to step 6.

- 5 Complete the following steps if you are restoring the key files on the DNCS.
 - a From an xterm window on the Application Server, type **su -** and then press **Enter**.
 - b Type the root password and then press **Enter**.
 - c On the Application Server, type **/usr/sbin/shutdown -y -g0 -i0** and then press **Enter**. The Application Server shuts down and the **ok** prompt appears.
 - d On the DNCS, type **/usr/sbin/shutdown -y -g0 -i6** and then press **Enter**. The DNCS reboots.
 - e Log on to the DNCS as **dncs** user.
- 6 Is the Application Server at the **ok** prompt?
 - If **no**, go to step 7.
 - If **yes**, follow these instructions.
 - a Type **boot** and then press **Enter**. The Application Server reboots.
 - b Log on to the Application Server as **dncs** user.
- 7 Follow the instructions in *Restarting System Components* (on page 61) to restart Spectrum, the DNCS, and the Application Server.

5

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

Stopping System Components

Introduction

Use the procedures in this appendix to stop the Spectrum Network Management Service (Spectrum), the Application Server, and the DNCS.

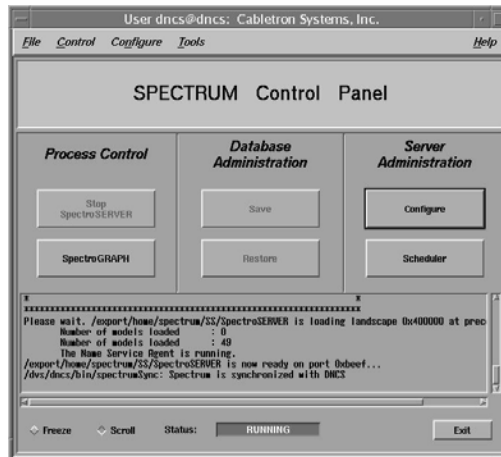
In This Appendix

- Stop System Components 58

Stop System Components

Stopping Spectrum

- 1 From the DNCS Administrative Console Status window, click **Control** in the NMS section of the window. The Select Host to run on window appears.
- 2 Select the appropriate **Host Machine** and then click **OK**. The Spectrum Control Panel appears.



- 3 Click **Stop SpectroSERVER**. A confirmation message appears.
- 4 Click **OK** at the confirmation message. The Status message on the Spectrum Control Panel shows **Inactive**.
- 5 Click **Exit** on the Spectrum Control Panel. A confirmation message appears.
- 6 Click **OK** at the confirmation message. The Spectrum Control Panel closes.

Stopping the Application Server

This section provides procedures for stopping either a SARA Server or a third-party server. Choose the procedure that pertains to your system.

Stopping the Application Server at SARA Sites

- 1 Press the middle mouse button on the Application Server and select **App Serv Stop**.
- 2 From an xterm window on the Application Server, type **appControl** and then press **Enter**. The Applications Control window appears.

- 3 Type **2** (for Startup/Shutdown Single Element Group), and then press **Enter**. The system displays all Application Server processes.
Note: The system updates the display periodically, or you can press **Enter** to force an update.
- 4 When the **Curr Stt** (Current State) field of the Applications Control window indicates that all of the Application Server processes have stopped, follow the on-screen instructions to close the Applications Control window.

Stopping the Application Server at Aptiv Sites

- 1 Press the middle mouse button on the Application Server and select **Passport Stop**.
- 2 From an xterm window on the Application Server, type **CheckServices** and then press **Enter**. A list of drivers appears.
Note: Each driver is associated with an Application Server process.
- 3 Wait until the word **No** appears next to each driver.
Note: If the word **No** does not appear next to each driver within a minute or two, repeat steps 2 and 3 again.

Stopping the DNCS

Complete these steps to stop the DNCS.

- 1 At the DNCS, press the middle mouse button and then select **DNCS Stop**.
Note: If a confirmation message appears, click **OK**.
- 2 From an xterm window on the DNCS, type **dncsControl** and then press **Enter**.
Result: The DnCS Control window appears.
- 3 Type **2** (for Startup/Shutdown Single Element Group), and then press **Enter**.
Result: The system displays all DNCS processes.
Note: The system updates the display periodically, or you can press **Enter** to force an update.
- 4 When the **Curr Stt** (Current State) field of the DnCS Control window indicates that all of the DNCS processes have stopped, follow the on-screen instructions to close the DnCS Control window.

What's Next?

Return to the instructions you were following when you were instructed to stop the system components.

B

Restarting System Components

Introduction

Use the procedures in this appendix to restart Spectrum, the DNCS, and the Application Server.

In This Appendix

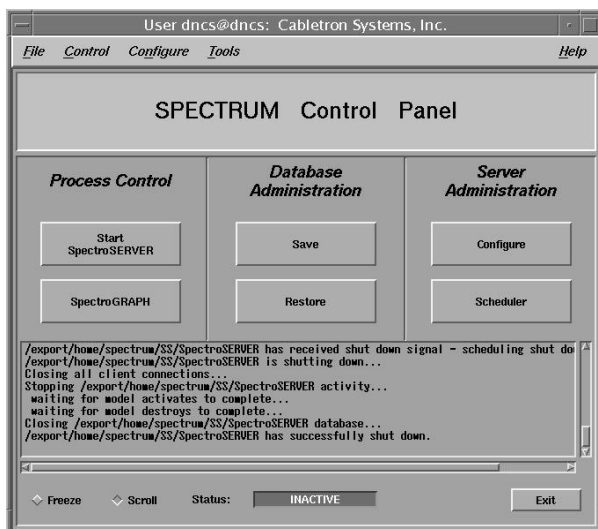
- Restart System Components 62

Restart System Components

Restarting Spectrum

Important: Skip this procedure if you are using DBDS Alarm Manager instead of Spectrum.

- 1 From the DNCS Administrative Console Status window, click **Control** in the NMS section of the window. The Select Host to run on window opens.
- 2 Select the appropriate **Host Machine**, and then click **OK**. The Spectrum Control Panel window opens.



- 3 On the Spectrum Control Panel window, click **Start SpectroSERVER**. The Spectrum Network Management System starts.
- 4 On the Spectrum Control Panel window, click **Exit**. A confirmation message appears.
- 5 Click **OK** on the confirmation message. The Spectrum Control Panel window closes.

Restarting the DNCS

- 1 Click the middle mouse button on the DNCS and select **DNCS Start**. The DNCS processes start.
- 2 Click the middle mouse button on the DNCS and select **Administrative Console**. The DNCS Administrative Console opens.
- 3 From the DNCS Administrative Console Status window, click **DNCS Control**.

Results:

- The DNCS Control window opens.
 - Green indicators begin to replace red indicators on the DNCS Control window.
- 4 From an xterm window on the DNCS, type **dncsControl** and then press **Enter**. The Dncs Control utility window opens.
 - 5 Type **2** (for Startup / Shutdown Single Element Group) and then press **Enter**. The Dncs Control window updates to list the status of all of the processes and servers running on the DNCS.
 - 6 Wait for the Dncs Control window to list the current status (Curr Stt) of all the processes and servers as **running**.

Notes:

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

Restarting the Application Server

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

Restarting the Application Server at SARA Sites

- 1 Press the middle mouse button on the Application Server and select **App Serv Start**.
- 2 From an xterm window on the Application Server, type **appControl** and then press **Enter**. The Applications Control window opens.
- 3 Select option **2** on the Applications Control window. The system displays a list of Application Server processes and their current status.

Note: The system updates the display periodically, or you can press **Enter** to force an update.

- 4 When the Application Control window indicates that the current state (**Curr Stt**) of each process is running, follow the on-screen instructions to close the Applications Control window.

Restarting the Application Server at Aptiv Sites

Complete the following steps to verify that the Passport resident application has started on the Application Server, and then to start it, if necessary.

- 1 Open an xterm window on the Application Server.
- 2 Type **CheckServices** and then press **Enter**. A list of drivers appears.
Note: Each driver is associated with an Application Server process.
- 3 Does the word **Yes** appear next to each driver, indicating that the process has started?
 - If **yes**, you have completed this procedure.
 - If **no**, go to step 4.
- 4 Press the middle mouse button, and then select **Passport Start**.
- 5 When the word **Yes** appears next to each driver, go to step 6.
- 6 Follow the on-screen instructions to close the window containing the list of drivers associated with the Passport resident application.

C

Setting Up an Automated Database Backup

Introduction

You can perform an automatic nightly backup of the database by using the cron script, backupDatabase.

Note: A cron script is an automated process that operates at predefined time intervals. You may sometimes hear a cron script referred to as a cron job.

System operators can later check messages that pertain to the execution of the backupDatabase script by examining the /var/log/backupDatabaselog file.

To configure your system to execute the backupDatabase script, add an entry to the crontab file on the Application Server. Use the instructions in this appendix to configure your system to execute the backupDatabase script.

In This Appendix

- Configure the DNCS for an Automatic Database Backup 66

Configure the DNCS for an Automatic Database Backup

Copying the Backup/Restore Scripts to the DNCS

Complete the following steps to copy the backup and restore scripts from the CD to the DNCS/ISDS.

- 1 Insert the DBDS Maintenance CD into the CD drive of the DNCS/ISDS.
- 2 Type `cp -pr /cdrom/cdrom0/s3/backup_restore /usr/local` and then press **Enter**.

Editing the crontab

Complete the following steps to configure your nightly backup of the Informix database on the DNCS.

- 1 From an xterm window on the DNCS, log in as **root** user.
- 2 Type `crontab -l > /tmp/root.crontab` and then press **Enter**. The system redirects the contents of the crontab into root.crontab.

Note: The 'l' in crontab -l is a lowercase L.

Important: While you can edit the crontab directly, we recommend that you first redirect the contents of the crontab to root.crontab so you can recover the original crontab if necessary.

- 3 Type `vi /tmp/root.crontab` and then press **Enter**. The system opens root.crontab for editing using the UNIX vi editor.
- 4 Add the following lines to the end of root.crontab, based upon your tape drive configuration:

- If you have a *standard* tape drive configuration, add the following entry to the end of the root.crontab file:

```
#cron to automatically back up the database  
0 2 * * * (. /dvs/dnCS/bin/dnCSSetup;  
/usr/local/backup_restore/backupDatabase -n)
```

- If you have a custom tape drive configuration, add the following entry to the end of the root.crontab file:

```
#cron to automatically back up the database  
0 2 * * * (. /dvs/dnCS/bin/dnCSSetup;  
/usr/local/backup_restore/backupDatabase -n -b [blocksize] -s [tapesize])
```

Note: This command will back up the DNCS database at 2 a.m. everyday. To learn more about the various fields in the command you just entered, type **man crontab** and then press **Enter** at an xterm window on the DNCS.

- 5 Save the file and exit the vi editor.
- 6 Type **crontab /tmp/root.crontab** and then press **Enter**. The system automatically backs up your DNCS database everyday.

Important Notes to the System Operator

The system will eject the tape after each backup. Remember to insert a blank tape into the tape drive of the DNCS each day. Our engineers recommend that you store your daily tapes offsite to protect against loss or damage.

Index

B

- backupDatabase
 - options • 18
- backupFileSystems
 - options • 12
- backupKeyFiles
 - options • 21

D

- data loss, prevention • 36
- data tapes, types • 3, 6

I

- interactive option • 2

P

- physical restore option • 2

R

- real-time, class processes • 13
- replicated database • 2
- restoreDatabase
 - restoreDatabase, options • 36
- restoreFileSystems
 - options • 28
- restoreKeyFiles
 - restoreKeyFiles, options • 49

S

- supported hardware platforms • 1
 - special platform considerations • 13
- supported system releases • v

V

- version, backup and restore scripts • v



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

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

This document includes various trademarks of Cisco Systems, Inc. Please see the Notices section of this document for a list of the Cisco Systems, Inc. trademarks used in this document.

Product and service availability are subject to change without notice.

© 2006, 2009, 2012 Cisco and/or its affiliates. All rights reserved.

April 2012 Printed in USA

Part Number 4013779 Rev C