NN42020-502

Multimedia Communication Portfolio

Multimedia Communication Server

Backup and Recovery Guide

MCS 5100 3.5 Standard 5.0 August 2006

NORTEL

Finding the latest updates on the Nortel web site

The content of this documentation was current at the time the product was released. To check for updates to the latest documentation and software for MCS 5100, click one of the following links:

Link to	Takes you directly to the
Latest Software	Nortel page for MCS 5100 software located at www130.nortelnetworks.com/cgi-bin/eserv/cs/main.jsp?cscat=SOFTWARE&resetFilter=1&tranProduct=12482
Latest Documentation	Nortel page for MCS 5100 documentation located at www130.nortelnetworks.com/cgi-bin/eserv/cs/main.jsp?cscat=DOCUMENTATION&resetFilter=1&tranProduct=12482

How to get help

This section explains how to get help for Nortel products and services.

Getting help from the Nortel web site

The best way to get technical support for Nortel products is from the Nortel Technical Support web site:

www.nortel.com/support

This site provides quick access to software, documentation, bulletins, and tools to address issues with Nortel products. From this site, you can:

- download software, documentation, and product bulletins
- search the Technical Support Web site and the Nortel Knowledge Base for answers to technical issues
- sign up for automatic notification of new software and documentation for Nortel equipment
- open and manage technical support cases

Getting help over the phone from a Nortel Solutions Center

If you do not find the information you require on the Nortel Technical Support web site, and you have a Nortel support contract, you can also get help over the phone from a Nortel Solutions Center.

In North America, call 1-800-4NORTEL (1-800-466-7835).

Outside North America, go to the following web site to obtain the phone number for your region:

www.nortel.com/callus

Getting help from a specialist by using an Express Routing Code

To access some Nortel Technical Solutions Centers, you can use an Express Routing Code (ERC) to quickly route your call to a specialist in your Nortel product or service. To locate the ERC for your product or service, go to:

www.nortel.com/erc

Getting help through a Nortel distributor or reseller

If you purchased a service contract for your Nortel product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller.

Overview

This chapter is organized as follows:

Functional description

The purpose of this document is to provide procedures for backing up specific core Multimedia Communication Server (MCS) servers, and recovering the software (both server and MCS component-level software) on MCS servers when a specific hardware failure occurs. The recovery procedures range from the ability to recover software after minor server failures, to recovery of hardware and software after catastrophic server failures.

In addition, this document covers the backup and recovery procedures for accounting files located on the MCS server hosting the Accounting Module component. The backup and recovery of accounting files is designed as a method of providing restoration of accounting files in the event that they can not be transferred to an Operations Support System (OSS) through the normal process. For more information on the normal process of retrieving accounting files, please refer to *MCS Accounting Module Basics (NN10279-111)*.

General backup information

Some recovery procedures involve the restoration of backups made of the MCS servers or the Oracle database, depending on the server having the failure and the type of hardware failure which occurred. In the event of a catastrophic server failure (where the server hardware must be entirely replaced), backups of the corresponding MCS server are restored as part of the recovery process. If the Database Module resided on the server which had the failure, then a backup of the Oracle database would also have to be restored after the MCS server backup is restored.

Backups of the MCS servers involve taking a snapshot of both the third party (non-Nortel) and component software, as well as other required data, which is deployed to the associated server. The software and data included within a MCS server backup consists of the following:

- All operating system (OS) software and patches installed on the server.
- All third party (non-Nortel) software and patches installed on the server.
- All MCS component software deployed to the server.
- All logs and operational measurements (OMs) residing on the server.

  Note: Although the log information is captured during the backup of an MCS server, this data is not supplied through the restore process. This is due to the fact that the data contained within the backup would be out-of-date and provide no useful purpose after the restore.

- All configuration data for the server and MCS component software.
- All component data files (excluding accounting files and data stored in the Oracle database).

Backups of the Oracle database consist of all the provisioning and configuration data that is stored within the Oracle database.

ATTENTION

Backups of the MCS servers are highly recommended in certain situations based on the software resident on the server. These situations include when the Solaris Operating System on any MCS server is updated, the Oracle software on the server running the Oracle database is updated, and when an MCS software maintenance release for the Management Module is deployed to a server.

General recovery information

Part of the recovery process is the replacement of hardware components after detecting that there is an issue. Prior to replacing any hardware, it is strongly recommended that the hardware support vendor/distributor, or the next level of support, be consulted.

CAUTION

Prior to performing any hardware replacement, it is important to determine whether any support or warranty contracts are in place. If such support/warranty agreements are not utilized during the replacement, then the support/warranty agreement for the hardware may be voided.

The recovery process is different based on both the type of hardware server and the type of MCS server having the failure. The following table shows the different types of MCS servers covered within this document.

MCS Server Type	Description
Application Server	A server (either Sun Netra 140x, Sun Netra 240, or Sun Fire v100) which can have the following type of MCS components deployed to it: • SIP Application Module • Provisioning Module • H.323 Gatekeeper • IP Client Manager • Web Client Manager • iPlanet Monitor • UFTP Base Software
Management/ Accounting Server	A server (either Sun Netra 140x, Sun Netra 240, or Sun Fire v100) which can have the following type of MCS components deployed to it: • Management Module • Accounting Module • Database Module/Oracle database (only in Micro System configuration) • Oracle Monitor (only in Micro System configuration)
Database Server	A server (either Sun Netra 140x, Sun Netra 240, or Sun Fire v100) which can have the following type of MCS components deployed to it: • Database Module/Oracle database • Oracle Monitor
AudioCodes PRI Gateway	AudioCodes server which provides the PRI interface to the PSTN for the MCS network.

For information on the recovery processes for servers where the RTP Media Portal is deployed, please refer to *MCS RTP Media Portal Basics (NN10265-111)*. For information on the recovery process for servers where the Media Application Server (MAS) is deployed, refer to any of the following documents:

- *MAS Application Server Ad Hoc Audio Conferencing Service Guide (NN10297-111)*
- *MAS Application Server Meet Me Audio Conferencing Service Guide (NN10303-111)*
- *MAS Application Server IM Chat Service Guide (NN10380-113)*
- *MAS Application Server Music On Hold Service Guide (NN10378-113)*
- *MAS Application Server Announcements Service Guide (NN10379-113)*

Appropriate backup procedures required for successful recovery of those servers are also covered within the corresponding documents.

The complexity of the recovery process for the different MCS servers is dependent on the degree of the hardware failure. In the event of a catastrophic disk failure, the recovery process involves the restoration of a previously made backup of an MCS server. Whereas, for minor hardware issues, only a simple reboot of the server is required.

Prerequisite material for recovery procedures

For a faster recovery time, it is strongly recommended that the following information and material be accessible during the recovery process:

- Completed customer-specific information (CSI) that was used during the initial installation. Refer to the *Network Deployment and Engineering Guide* (NN10313-191) for more on CSI and system requirements.
- List of all IP Address and nodenames for servers and deployed components.
- List of all accounts and passwords.
- List of all Veritas license keys for MCS servers.
- Applicable MCP 3.5 software installation CDs.
- Most recent backup of the MCS servers.

> ***Note:*** For information on how to perform backups of the MCS servers, please refer to Backup of MCP Solaris servers on page 25.

- Most recent backup of the Primary Oracle database.

  Note: For information on how to regularly schedule backups of the Oracle database, please refer to Scheduling regular Oracle database backups on page 33.

- Relevant third party documentation. Veritas is required for 1400 Management Server and Database Server configurations. DiskSuite is used by all other configurations.
  - — *Netra t 1400/1405 Service and System Reference Manual*

    Note: This document is available from the following web site: www.sun.com/documentation/

  - — *Solstice DiskSuite 4.2 User's Guide*

    Note: This document is available from the following web site: www.sun.com/documentation/

  - — *VERITAS Volume Manager for Solaris Administrator's Reference Guide*
- Location of the server hosting a DDS4 tape drive to be used for MCS server backup and restore procedures. When the tape drive is located remotely, the IP address of the hosting server is also required.
- PuTTY VT 100 terminal Emulator tool. This tool is a freeware configuration tool which is recommended for setting up sessions to the MCS servers.

  Note: This tool can be downloaded from the following web site: www.chiark.greenend.org.uk/~sgtatham/putty/

Backup scheduling

The typical DDS4 tape drive streams at 330 MB/min, which is approximately 5.5 MBps. This is easily manageable if the backup is to local tape, which is the case for the T140x Management/Accounting servers, as well as the preferred option for the T140x Database server.

However, the application servers (which include all other MCP components running on a Solaris platform), the V100s, and the N240s do not have a local tape drive and thus perform remote tape operations. As half of the maximum available bandwidth of the sending and receiving servers' network interfaces is consumed during backup and restore operations, these operations should be scheduled for low traffic periods to avoid impacting operational traffic.

As the main task of the server backup is to backup base software (i.e., the operating system, third-party software), server backups should be performed infrequently. Thus, a backup of a MCP Solaris Server should occur when:

- Solaris operating system has been patched.
- Oracle patch has been applied (Database Server only).
- A maintenance release has been installed or deployed (Management Server only).

The backup of the Oracle database should be performed nightly.

Duration

Determine how much data will be involved in the backup or restore operation in order to estimate the length of time required for the operation. Use Unix commands to determine the size of the partitions as shown below, depending on the type of server on which the operation is performed.

	Management/Accounting Server	
Disk Partition	**Application Server**	**Database Server**
/	X	X
/opt	X	X
/var	X	X
/IMS	X	X
/backup		X

Backup requires approximately 20 minutes per GB when using a USB tape drive, and approximately eight minutes per GB for a SCSI tape device.

Restore requires approximately 35 minutes per GB, regardless of which type of tape drive is used.

Estimates for backup and restore are rough as there are multiple factors that can affect the time required to complete the operation. As backups can be performed while the machine is live, system activity may slow the operation. If a backup or restore occurs across a network, network traffic can affect the time required to complete the operation.

ATTENTION

As multiple factors can affect the amount of time required to complete a backup or restore operation, estimates are rough. There is no guarantee customers will complete the operations within the estimated times.

Hardware

This documentation covers hardware and software recovery for the Sun Netra t140x, Sun Netra 240, Sun Fire V100, and AudioCodes servers. The standard platform configuration for these servers within the MCS network is described in the following table.

Table 1 Standard configuration of servers

Server type	standard configuration
Sun Netra t140x	4 GB RAM 4 x Ultra Sparc 2 Processors 2 x 36GB Ultra SCSI Disk Drives (4 x 36 GB Database Server) 1 x Internal 32X CD-ROM Drive (bootable) DDS4 tape drive (on the Management/Accounting and Database servers)
Sun Netra 240	2 x 1.2 GHz Hz UltraSPARC IIIi processors 1MB Internal Cache 4 Gigabyte Memory 1 x DVD – ROM Drive 2 x 73GB Disk 10K RPM Ultra160SCSI 4 x 10/100/1000 BASE-T Ethernet Ports 2 x USB Ports, OHCI-1.0 Compliant Interfaces, supporting dual speeds of 12 and 1.5 Mbits/sec each 1 x TIA/EIA-232-F (RJ45) Serial Port (Console + ALOM shared) 1 x TIA/EIA-232-F asynchronous (DB9) Serial Port

Table 1 Standard configuration of servers

Server type	standard configuration
Sun Fire V100	UltraSparc IIe processor @ 550Mhz 512 Kb external cache 1 GB RAM 2 IDE, 40Gb hard disks, @ 7000RPM 24X CD-ROM 2 10/100 Base-T Ethernet ports 2 USB ports

For backup and restore of the MCS servers and accounting files, the addition of a DDS4 or USB type tape drive is required. The type of tape drive is dependent on the hardware server where the tape drive is being connected.

> ***Note:*** For MCS networks using the Sun Netra t140x platform configuration, the Management/Accounting and Database type servers already contain a DDS4 tape drive.

The Seagate Travan 40 USB 2.0 20/40 GB tape drive with the media tape model STTM40 is the only supported USB tape drive for the Sun Fire V100 and Netra 240 servers.

Tools and utilities

The following tools and utilities are required in order to perform the recovery or backup procedures documented:

- PuTTY VT 100 terminal Emulator tool
- Terminal Server
- System Management Console
- Oracle Enterprise Manager (OEM) Console

Physical access or IP connectivity is assumed.

Backup of accounting records

This chapter is organized as follows:

Backup of accounting records overview

There are two separate procedures used to backup MCP accounting records: one is used when the tape device resides on the server with the accounting records being backed up, and the other is used for a remote host.

Restrictions and limitations

The backup of accounting records has the following restrictions:

- Only DDS4 and USB tape drives are supported for backup of the accounting records.

  Follow the manufacturer's recommendations for tape and tape drive use.
- The recommended USB tape drive is the Seagate Travan 40 USB 2.0 20/40 GB tape drive, with the media tape model STTM40.
- Only one backup file is allowed per tape.
- Tapes can be overwritten but not appended.

Backup log files

The backup script (**mcp_backup_billing.pl**) generates a log file with every execution. Review this log file to ensure the backup was successful. The log file is stored in the directory:

```
/export/home/sysadmin/bkup_restore
```

The generated log file is named:

```
mcp_backup_billing.pl.log.<dayTimeStamp>
```

where
`<dayTimeStamp>` is YYYY_MM_DD_HH:MM:SS. For example:
mcp_backup_billing.pl.log.2004_03_05_21:49:50

If the data being backed up is larger than what one tape can accommodate, the user will be prompted to enter the next tape at the appropriate time. Below is an example of the output displayed when additional tapes are required during a backup.

```
DUMP: End-of-tape detected
DUMP: 91.41% done, finished in 0:04
DUMP: Change Volumes: Mount volume `#2' on
`<ip_address>:/dev/rmt/0cn'
DUMP: NEEDS ATTENTION: Is the new volume (#2) mounted
on `<ip_address>:/dev/rmt/0cn' and ready to go?:
("yes" or "no")
```

Before you begin

Before you begin the backup of accounting records, review the following:

- Requirements for accounting record backups
- Utilization of a USB tape drive
- Required setup of an MCP server acting as a remote host

Requirements for accounting record backups

The following is a list of actions or requirements that need to be fulfilled prior to performing a backup.

- Local or remote DDS4 tape drive.
- DDS4 tape in tape drive.

  For USB drives this will be a 20 GB tape, for SCSI drives it will be a 12 GB tape.
- Live 100Mbps Ethernet connection for remote backup.
- List of all accounts and passwords.
- For remote backup or restore operation all servers involved should be running at full duplex. This includes the server being backed up, the tape server, and any intermediate node(s) in the network. All MCP servers should be set to auto negotiate. Failure to perform the backup at full duplex will result in backup times ten times the normal.

If you are uncertain whether the servers are running at full duplex, contact your next level of support.

Utilization of a USB tape drive

Add a tape drive

If using a USB Tape Drive for the backup, perform the following steps when connecting a USB tape drive to the server:

Procedure 1 Adding a tape drive

1 Login as **root** on the server where the tape drive is being connected and enter the following command:

```
/etc/init.d/volmgt stop
```

2 Connect the USB Tape Drive to port 0.

3 Enter the following command:

```
/etc/init.d/volmgt start
```

4 Turn on the Tape Drive and insert a tape.

Remove a tape drive

If using a USB Tape Drive for the backup, perform the following steps when disconnecting a USB tape drive to the server:

Procedure 2 Removing a tape drive

1 Login as **root** on the server where the tape drive is being removed, and enter the following command:

```
/etc/init.d/volmgt stop
```

2 Remove the USB Tape Drive.

Required setup of an MCP server acting as a remote host

The following commands are required to setup access to a remote MCP server with a tape drive acting as the remote host.

If the remote tape drive is NOT on an MCP server, then the steps below can be ignored. However, you must ensure that remote shell operations are enabled (from the server to be backed up) on the remote tape drive server.

To perform the commands in the steps listed below, the user can login as **root** (or **sysadmin** as shown below).

Procedure 3 Setting up an NCP server as a remote host

1 Ensure the MCP server with the accounting records has proper access to MCP server with the tape drive (remote host).

2 Login to the MCP server with the tape drive (remote host) as sysadmin.

```
sysadmin
```

3 Execute the following script on the remote host:

```
sudo /usr/local/bin/mcp_enable_remote_sh.pl
<MCP_Server_IP>
```

Where
`<MCP_Server_IP>` is the IP address of the server with the accounting records being backed up.

The above script enables the execution of remote shell commands from the MCP server with the accounting records.

4 Log off as **sysadmin**.

exit

5 Login to the server with the accounting records as **root**.

6 Verify access to the tape server has been setup correctly, execute the command from the server with the accounting records:

```
rsh  -l  sysadmin  <Tape_Server_IP>  df -k
```

Where
`<Tape_Server_IP>` is the IP of the remote host with the tape drive.

If you see the output of the **df –k** command, then the target system is setup for the backup procedure. If not, contact your next level of support.

7 After the backup procedure has completed, logon as **sysadmin** on the remote host and execute the following command:

```
sudo /usr/local/bin/mcp_disable_remote_sh.pl
```

This command disables ability to execute remote shell commands.

Required server access

Access to the server can be through:

- A secure telnet session (SSH) through the server's network interface. Note, if this is used and the telnet session dies, the associated process (accounting records backup in this case) will die as well.

- Telnet session through a terminal server to the server's serial console interface for T140x and V100 servers, or through a telnet session to the NetMgmt port for N240s.

Login to the NetMgmt Port of the 240

The procedure to log into the NetMgmt Port of a Sun Netra 240 server is described below.

Procedure 4 Logging in to the NetMgmt Port

1 Telnet to the NetMgmt port IP. This is a regular, not secure, telnet.

2 Login as **admin**.

user name: **admin**
admin password: **<admin_pswd>**

Where
<admin_pswd> is the admin password set during the N 240 server installation.

A successful login gets you to the sc prompt.

3 Enter the following at the sc prompt.

```
console -f
```

This brings up console login prompt.

4 Login as either **sysadmin** or **root**.

5 When finished and ready to exit the console session, you MUST enter a "**#.**" to return back to the sc prompt. Failure to type "**#.**" will lock up the console port.

```
"#."
```

You will return to the **sc** prompt.

Backing up accounting records to a local tape drive

Use this procedure to backup accounting records to a local tape drive.

Procedure 5 Backing up accounting records

1 Label the DDS4 tape with the server name and current date.

2 Insert the DDS4 tape into the tape drive of the server being backed up.

3 Login as **sysadmin**.

```
sysadmin
```

4 Execute the backup script

```
sudo /usr/local/bin/mcp_backup_billing.pl
```

5 When the backup is complete, remove the tape from the drive.

The backup operation time will depend on type of MCP server and the amount of data on the server.

6 Review the log file generated by the backup script to ensure the backup was successful. The log file is stored in the directory:

```
/export/home/sysadmin/bkup_restore
```

7 Logoff the server.

8 Store the tape in a safe, dry location.

Backing up accounting records to a remote tape drive

Use this procedure to backup accounting records to a remote tape drive. IP addresses are required as part of the backup script. Use the machine logical IP address, not the physical IP address. If the servers are in a dual configuration, use the IP address of the network where the server containing the tape drive is on. If you are uncertain of the logical IP address, contact your next level of support.

Ensure all nodes involved have their network interfaces set to full duplex mode before beginning the remote backup. This includes both the server with the accounting records being backed up, the server with the tape, and any intermediate node(s) in the network being traversed. All MCP servers are set to auto negotiate. If the nodes they are communicating with are set to auto negotiate, then they will be set to full duplex. If a server involved in the backup is not running at full duplex, the backup times will increase to ten times the normal. If you are uncertain whether all nodes are set to full duplex, contact your next level of support.

Procedure 6 Backing up accounting records

1 Label the DDS4 tape with the appropriate server name and current date.

2 Select a tape host (a remote server with a tape drive).

3 Insert the DDS4 tape into the tape drive of the remote tape server host.

4 Login to the MCP Server host to be backed up as **sysadmin**.

```
sysadmin
```

5 Execute the backup script

```
sudo /usr/local/bin/mcp_backup_billing.pl
<Tape_Server_IP>
```

where
`<Tape_Server_IP>` is the IP address of the host that the tape drive resides on.

6 When the backup is complete, remove the tape from the drive.

The backup operation time will depend on type of MCP server and the amount of data on the server.

7 Review the log file generated by the backup script to ensure the backup was successful. The log file is stored in the directory:

```
/export/home/sysadmin/bkup_restore
```

8 Logoff the server.

9 After the backup or restore procedure has completed, execute the following command on the remote host, to disable the execution of remote shell commands on the tape server host:

```
sudo /usr/local/bin/mcp_disable_remote_sh.pl
```

See the procedure Required setup of an MCP server acting as a remote host for more details

10 Store the tape in a safe, dry location.

Backup of MCP Solaris servers

This chapter is organized as follows:

Backup of MCP Solaris servers overview

Backup procedures for the Sun Solaris nodes are the same across the platform. They all involve tape transactions, to a local or remote tape drive, depending on the server.

There are two separate procedures used to backup MCP Solaris servers: one is used when the tape device resides on the server being backed up, and the other is used for a remote host. The list of partitions that are backed up varies based on server type.

Restrictions and limitations

The backup of MCP Solaris servers has the following restrictions and limitations.

- Only DDS4 and USB tape drives are supported for backup operations.

  Follow the manufacturer’s recommendations for tape and tape drive use.
- Only one backup file is allowed per tape.
- Tapes can be overwritten, but not appended.
- Scheduling of delayed backup operations is NOT supported.

- The backup script does not include the contents of the Oracle database.
- System logs and alarms cannot be generated by the backup operations performed from the Command Line Interface (CLI).

Backup log files

The backup script (**mcp_backup.pl**) generates a log file with every execution. Review this log file to ensure the backup was successful. The log file is stored in the directory:

```
/export/home/sysadmin/bkup_restore
```

The generated log file is named:

```
mcp_backup.pl.log.<dayTimeStamp>
```

where
`<dayTimeStamp>` is YYYY_MM_DD_HH:MM:SS. For example:
mcp_backup.pl.log.2004_03_05_21:49:50

If the data being backed up is larger than what one tape can accommodate, the user will be prompted to enter the next tape at the appropriate time. Below is an example of the output displayed when additional tapes are required.

```
DUMP: End-of-tape detected
DUMP: 91.41% done, finished in 0:04
DUMP: Change Volumes: Mount volume `#2' on
`<ip_address>:/dev/rmt/0cn'
DUMP: NEEDS ATTENTION: Is the new volume (#2) mounted
on `<ip_address>:/dev/rmt/0cn' and ready to go?:
("yes" or "no")
```

Before you begin

Before you begin the backup of a MCP Solaris server, review the following:

- Requirements for MCP Solaris server backups
- Utilization of a USB tape drive
- Required setup of an MCP server acting as a remote host

Requirements for MCP Solaris server backups

The following is a list of actions or requirements that need to be fulfilled prior to performing a backup.

- DDS4 tape drive

  For USB Tape drives, the recommended tape drive is the Seagate Travan 40 USB 2.0 20/40 GB tape drive with the media tape model STTM40.

  The tape drive can be local or remote for backup. It does not have to be within MCP network but must be attached to a Solaris machine that is visible to the server doing backup operations.

- DDS4 tape in tape drive.

  For USB drives this will be a 20 GB tape, for SCSI drives it will be a 12 GB tape.

- Live 100Mbps Ethernet Connection for remote backup.
- If backup using a remote tape drive, IP address of tape server.
- List of all accounts and passwords.
- For remote backup operations, all servers involved should be running at full duplex. This includes the server being backed up, the tape server, and any intermediate node(s) in the network. All MCP servers should be set to auto negotiate. Failure to perform the backup at full duplex will result in backup times ten times the normal. If you are uncertain whether the servers are running at full duplex, contact your next level of support.

Utilization of a USB tape drive

Add a tape drive

If using a USB Tape Drive for the backup, perform the following steps when connecting a USB tape drive to the server.

Procedure 7 Adding a tape drive

1 Login as **root** on the server where the tape drive is being connected and enter the following command:

```
/etc/init.d/volmgt stop
```

2 Connect the USB Tape Drive to port 0.

3 Enter the following command:

```
/etc/init.d/volmgt start
```

4 Turn on the Tape Drive and insert a tape.

Remove a tape drive

If using a USB Tape Drive for the backup, perform the following steps when disconnecting a USB tape drive to the server.

Procedure 8 Removing a tape drive

1 Login as **root** on the server where the tape drive is being removed, and enter the following command:

```
/etc/init.d/volmgt stop
```

2 Remove the USB Tape Drive.

Required setup of an MCP server acting as a remote host

The following commands are required to setup access to a remote MCP server with a tape drive acting as the remote host.

If the remote tape drive is NOT on an MCP server, then the steps below can be ignored. However, you must ensure that remote shell operations are enabled (from the server to be backed up) on the remote tape drive server.

Procedure 9 Setting up an MCP server as a remote host

1 Ensure the MCP server being backed up has proper access to the MCP server with the tape drive (remote host) using the **ping** command. Sample output follows:

```
ping 47.47.47.47
47.47.47.47. is alive
```

2 Login to the MCP server with the tape drive (remote host) as **sysadmin**.

```
sysadmin
```

3 Execute the following script on the remote host:

```
sudo /usr/local/bin/mcp_enable_remote_sh.pl
<MCP_Server_IP>
```

Where
`<MCP_Server_IP>` is the IP address of the server being backed up.

The above script enables the execution of remote shell commands from the MCP server being backed up.

4 Log off as **sysadmin**.

exit

5 Login to the MCP server being backed up as **root**.

6 Verify access to the tape server has been setup correctly, execute the command from the server being backed up:

```
rsh  -l  sysadmin  <Tape_Server_IP>  df –k
```

Where
<Tape_Server_IP> is the IP of the remote host with the tape drive.

If you see the output of the **df –k** command, then the target system is setup for the backup procedure. If not, contact your next level of support.

7 After the backup procedure has completed, logon to the remote host as **sysadmin** and execute the following command:

```
sudo /usr/local/bin/mcp_disable_remote_sh.pl
```

This command disables ability to execute remote shell commands.

Required server access

Access to the server can be through:

- A secure telnet session (SSH) through the server's network interface. Note, if this is used and the telnet session dies, the associated process (backup in this case) will die as well.
- Telnet session through a terminal server to the server’s serial console interface for T140x and V100 servers, or through a telnet session to the NetMgmt port for N240s.

Login to the NetMgmt Port of the 240

The procedure to log into the NetMgmt Port of a Sun Netra 240 server is described below.

Procedure 10 Logging in to the NetMgmt Port

1 Telnet to the NetMgmt port IP. This is a regular, not secure telnet.

2 Login as **admin** and provide the admin password.

user name: **admin**
admin password: **<admin_pswd>**

Where
<admin_pswd> is the admin password set during the N 240 server installation.

A successful login gets you to the **sc** prompt.

3 Enter the following at the sc prompt.

```
console -f
```

This brings up console login prompt.

4 Login as either as sysadmin, root, or oracle, depending on the procedures being performed.

5 When finished and ready to exit the console session, you MUST enter a "**#.**" to return back to the sc prompt. Failure to type "**#.**" will lock up the console port.

```
"#."
```

You will return to the **sc** prompt.

Backup of an MCP Solaris Server to a local tape drive

Use this procedure to backup the MCP Solaris server to a local tape drive.

Procedure 11 Backing up an MCP Solaris server to a local tape drive

1 Label the DDS4 tape with the server name and current date.

2 Insert the DDS4 tape into the tape drive of the server being backed up.

3 Login using **sysadmin**.

```
sysadmin
```

4 Execute the backup script

```
sudo /usr/local/bin/mcp_backup.pl
```

5 When the backup is complete, remove the tape from the drive.

The backup operation time will depend on type of MCP server and the amount of data on the server.

6 Review the log file generated by the backup script to ensure the backup was successful. The log file is stored in the directory

```
/export/home/sysadmin/bkup_restore
```

7 Logoff the server.

8 Store the tape in a safe, dry location.

Backup of an MCP Solaris Server to a remote tape drive

Use this procedure to backup an MCP Solaris server to a remote tape drive. IP addresses are required as part of the backup script. Use the machine logical IP address, not the physical IP address.

If the servers are in a dual configuration, use the IP address of the network where the server containing the tape drive is on.

Procedure 12 Backing up an MCP Solaris server to a remote tape drive

1. Label the DDS4 tape with the appropriate server name and current date.
2. Select a tape host (a remote server with a tape drive).
3. Insert the DDS4 tape into the tape drive of the remote tape server host.
4. Login to the MCP Server host to be backed up as **sysadmin**.

   ```
   sysadmin
   ```

5. Execute the backup script

   ```
   sudo /usr/local/bin/mcp_backup.pl
   <Tape_Server_IP>
   ```

   where
   `<Tape_Server_IP>` is the IP address of the host that the tape drive resides on.

6. When the backup is complete, remove the tape from the drive.

   The backup operation time will depend on type of MCP server and the amount of data on the server.

7. Review the log file generated by the backup script to ensure the backup was successful. The log file is stored in the directory:

   ```
   /export/home/sysadmin/bkup_restore
   ```

8. Logoff the server.
9. After the backup procedure has completed, execute the following command on the remote host as **sysadmin** to disable the execution of remote shell commands on the tape server host:

   ```
   sudo /usr/local/bin/mcp_disable_remote_sh.pl
   ```

10. Store the tape in a safe, dry location.

Backup of the Oracle database

This chapter is organized as follows:

Scheduling regular Oracle database backups

The Database functionality supports the ability to backup the Oracle database using the Oracle Enterprise Manager (OEM) Console.

> **ATTENTION**
> It is recommended that the Oracle database be backed up daily, whether it is a redundant configuration or not. If there is no redundancy in the network, there is no replication process. Thus, a backup of the data is even more important.

Recovery of an Oracle database restores the database to the last point in time when the database (or secondary database within a redundant architecture) was backed up. All changes made to the database since that last point in time will be lost.

The monitoring of backups is recommended. Indication that a backup is in progress and its status is available from the OEM console through the Active and History screens. Both include a status column, displayed when the Show Targets is selected. Sample output showing the status of an active backup follows:

```
Submitted: The job has been submitted to the job
target running an Intelligent Agent.

Scheduled: The job has been successfully delivered to
the Intelligent Agent and is scheduled for execution.
```

```
Started: The job execution has started. After the job
executes, the job execution is displayed in the Job
History page. If this is the last scheduled execution
of the job, the job is removed from the Active Jobs
page. Otherwise, the job remains in the Active Jobs
page and has the status of Scheduled. Unless you view
the Active Jobs page at the exact time that the job
is executing, you would not seethe Running status.
```

Sample output showing the status of a failed backup follows:

```
Status of job is one of the following:
Completed: The job has executed successfully.
Failed: The job execution has failed.
Deleted: The job has been deleted.
```

For more information regarding backup failure and procedures for viewing details of the failure, refer to *MCS Database Module Basics (NN10267-111)*.

Creating an Export/Import Oracle database backup job

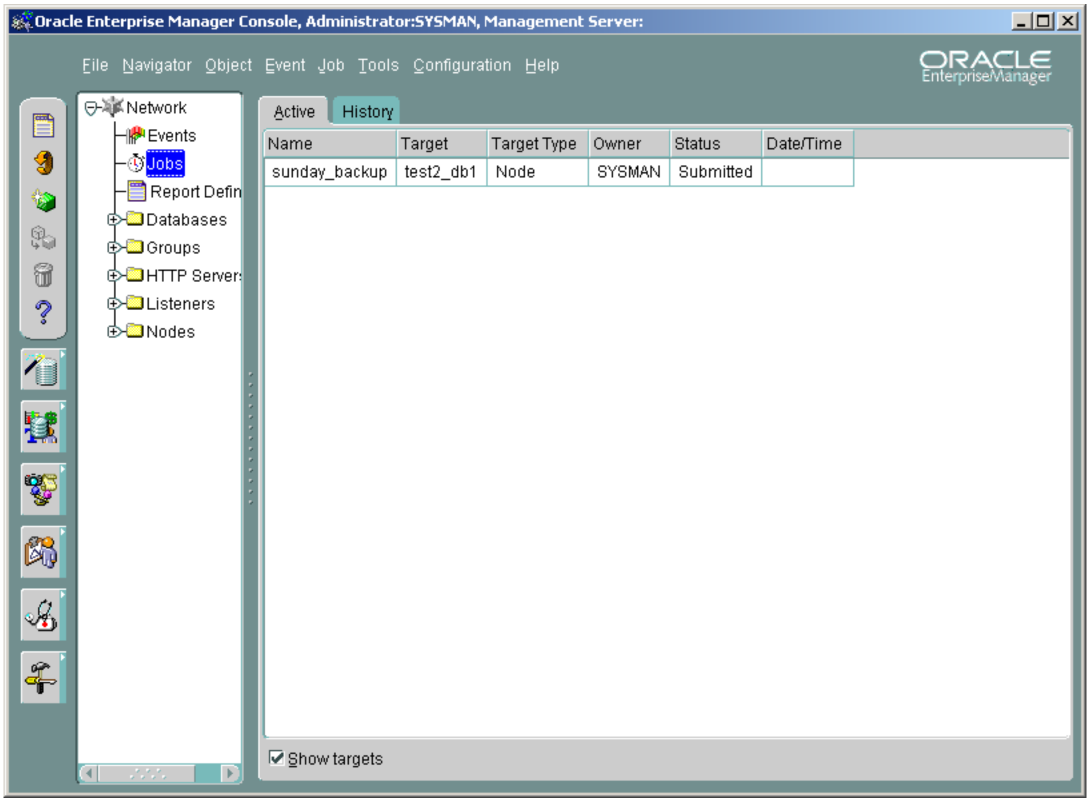
Use the following procedure to create backup jobs from the OEM Console using the Export/Import backup method:

> ***Note:*** When a scheduled backup job is run, the approximate export time is 25 MegaBytes of data per minute.

Procedure 13 Set general backup properties

1 From the **Network** tree, select **Jobs**.

The **Jobs > Active** pane displays the list of active backup jobs that have been scheduled.

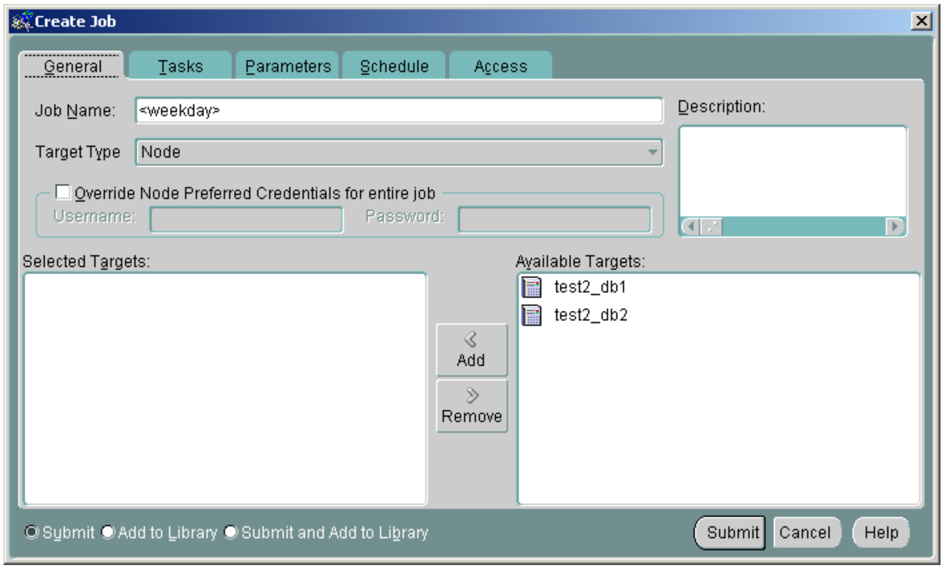

Oracle Enterprise Manager Console, Administrator:SYSMAN, Management Server:
File Navigator Object Event Job Tools Configuration Help
ORACLE Enterprise Manager
Network
Events
Jobs
Report Defin
Databases
Groups
HTTP Server
Listeners
Nodes
Active
History

Name	Target	Target Type	Owner	Status	Date/Time
sunday_backup	test2_db1	Node	SYSMAN	Submitted	

☑ Show targets

2 From the **Job** menu, select **Create Job**.

The **Create Job > General** pane opens.



Job Name: <weekday>

Target Type Node

□ Override Node Preferred Credentials for entire job

Username: Password:

Description:

Selected Targets:

Available Targets:
test2_db1
test2_db2

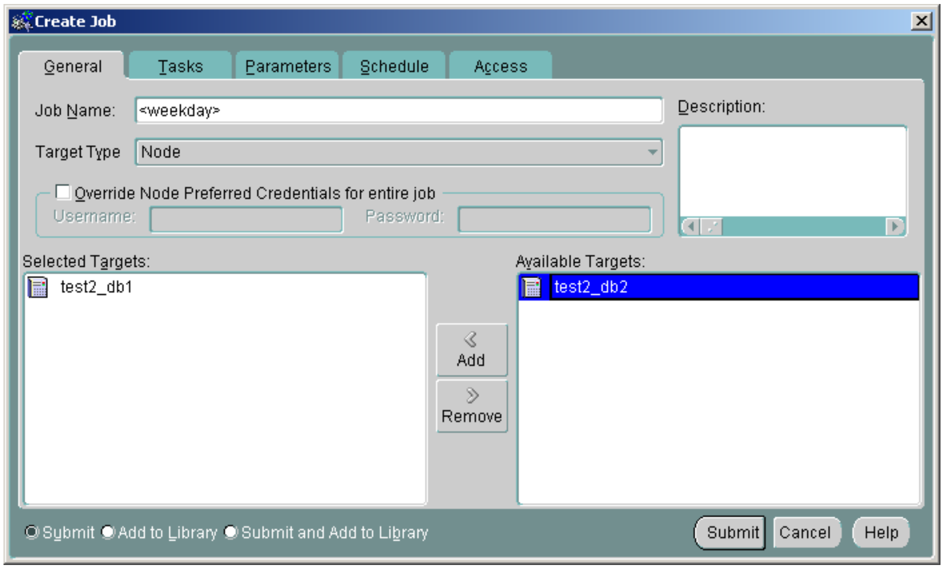
● Submit ○ Add to Library ○ Submit and Add to Library

3 In the **Job Name** box, type **<weekday>**, where **weekday** is the day of the week the job should be run.

4 Under **Target Type**, select **Node**.

5 In the **Available Targets** box, select the node name where the primary Oracle database resides and click **Add**.

The target node name which was selected moves into the **Selected Targets** list.



Create Job

Job Name: <weekday>

Target Type Node

□ Override Node Preferred Credentials for entire job

Username:

Password:

Description:

Selected Targets: test2_db1

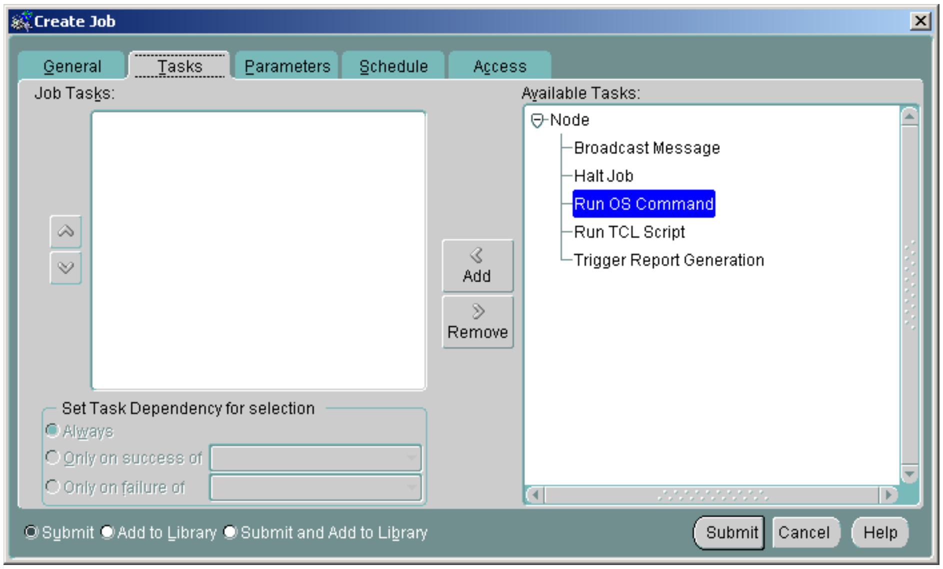
Available Targets: test2_db2

● Submit ○ Add to Library ○ Submit and Add to Library

Set backup task properties

6 Click the **Tasks** tab.

The **Create Job > Tasks** pane opens.



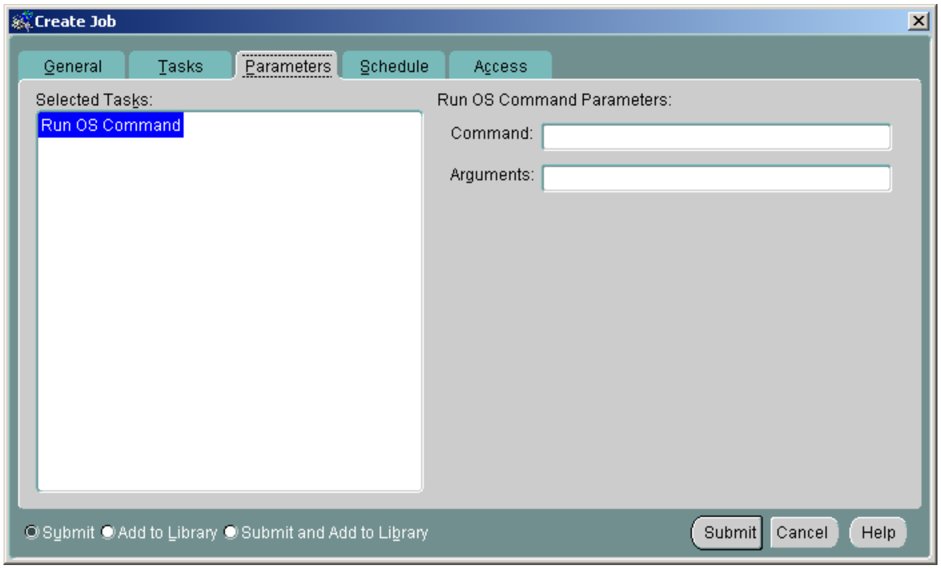
7 Select **Run OS Command** from the **Available Tasks** pane and click **Add**.

The **Run OS Command** task is added to the **Job Tasks** pane.

Define backup parameters

8 Click the **Parameters** tab.

The **Create Job > Parameters** pane opens.



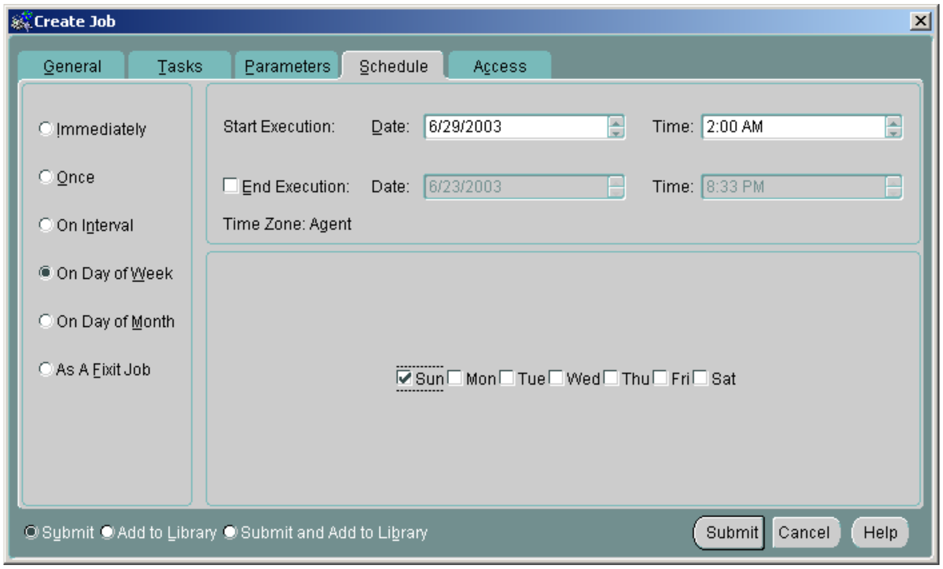
9 In the **Command** box, enter the following command: **/IMS/imssipdb/data/db_schema/backup/export_imsdb1.sh**

10 In the **Arguments** box, enter the following argument format: **<db_type> <name_of_backup> <media_type>** where **db_type** is PRIMARY (or SECONDARY, when within a redundant architecture), **name_of_backup** is the name of the backup file, and **media_type** is DISK or TAPE.

Schedule backup frequency

11 Click the **Schedule** tab.

The **Create Job** > **Schedule** pane opens.



○ Immediately
○ Once
○ On Interval
● On Day of Week
○ On Day of Month
○ As A Fixit Job

Start Execution: Date: 6/29/2003 Time: 2:00 AM

□ End Execution: Date: 6/23/2003 Time: 8:33 PM

Time Zone: Agent

☑ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat

● Submit ○ Add to Library ○ Submit and Add to Library

12 Select **On Day of Week**. Next, select the day of the week on which the backup should run.

> ***Note:*** A backup job should be created for each day of the week.

13 Choose a default start time during off-peak hours. The recommended time is 2:00 a.m.

Submit and add the backup job to the library

14 Once all of the above steps are completed, do the following:

a Select the **Submit and Add to Library** option.

b Click the **Submit and Add** button to save the backup.

The **Create Job** dialog box closes and the new backup job appears in the **Active > Jobs** tab.

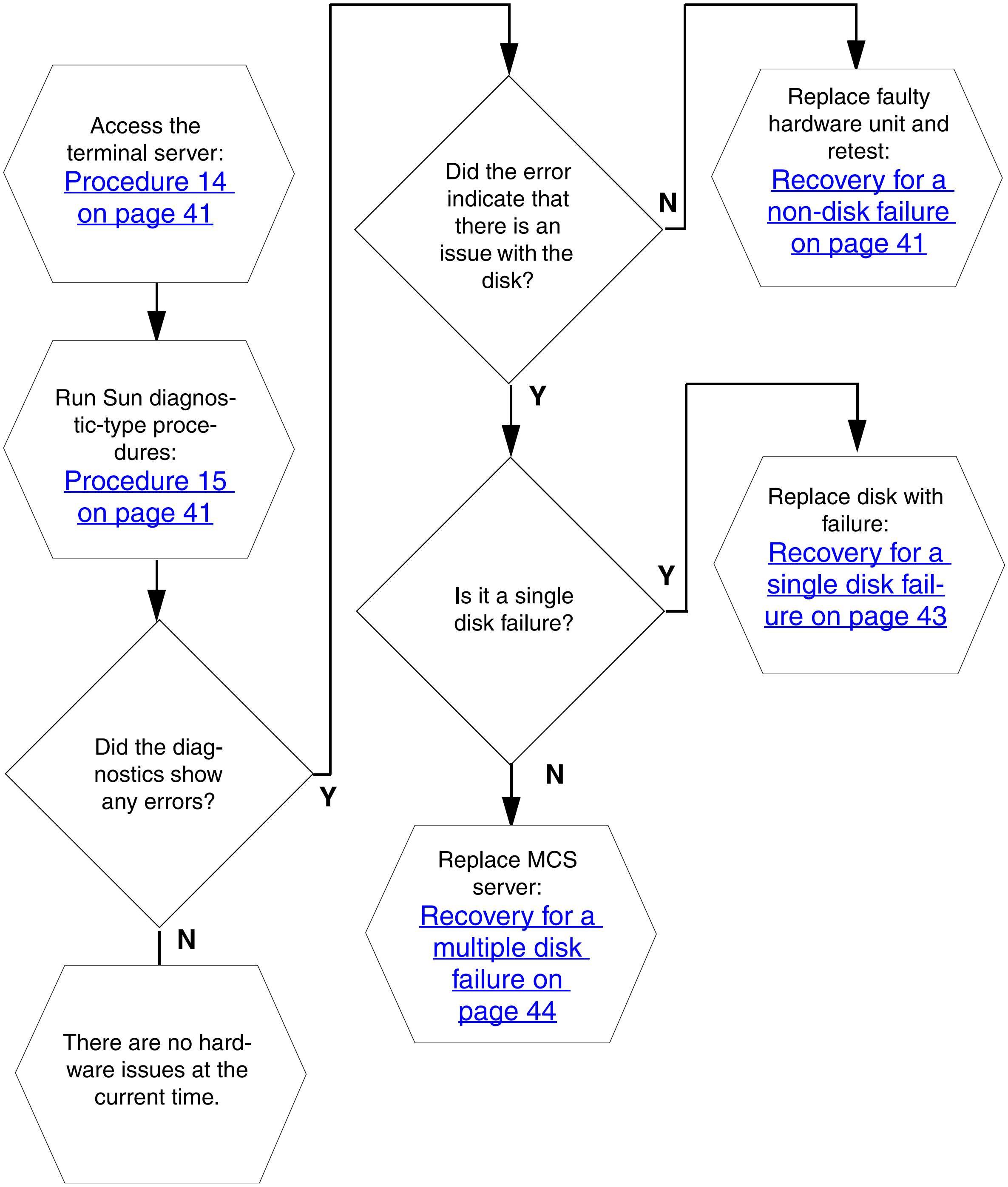
Recovery for Sun Netra t140x servers

This chapter is organized as follows:

Determining existence of hardware problems

The first step is to determine if or where a failure has occurred. Figure 1, Flow for determining existence of a hardware problem, on page 40 walks through the steps required to determine the existence of any hardware failures on an MCS server using the Sun Netra t140x platform.

Figure 1 Flow for determining existence of a hardware problem


Access the terminal server: Procedure 14 on page 41
Run Sun diagnostic-type procedures: Procedure 15 on page 41
Did the diagnostics show any errors?
Y
N
There are no hardware issues at the current time.
Did the error indicate that there is an issue with the disk?
N
Y
Replace faulty hardware unit and retest: Recovery for a non-disk failure on page 41
Is it a single disk failure?
Y
N
Replace disk with failure: Recovery for a single disk failure on page 43
Replace MCS server: Recovery for a multiple disk failure on page 44

Procedure 14 Access Terminal Server

At the administrator workstation

1 Open a PuTTY telnet session to the MCS server using the IP Address of the terminal server for the problematic server and the port number to connect to the console.

2 When prompted to login, login and then type the following: **init 0**

Procedure 15 Run Sun diagnostic-type procedures

From the telnet session

1 Execute the diagnostic procedures as described in the *Netra t 1400/1405 Service and System Reference Manual* at www.sun.com/documentation/. Execute any actions suggested within the procedure.

Recovery for a non-disk failure

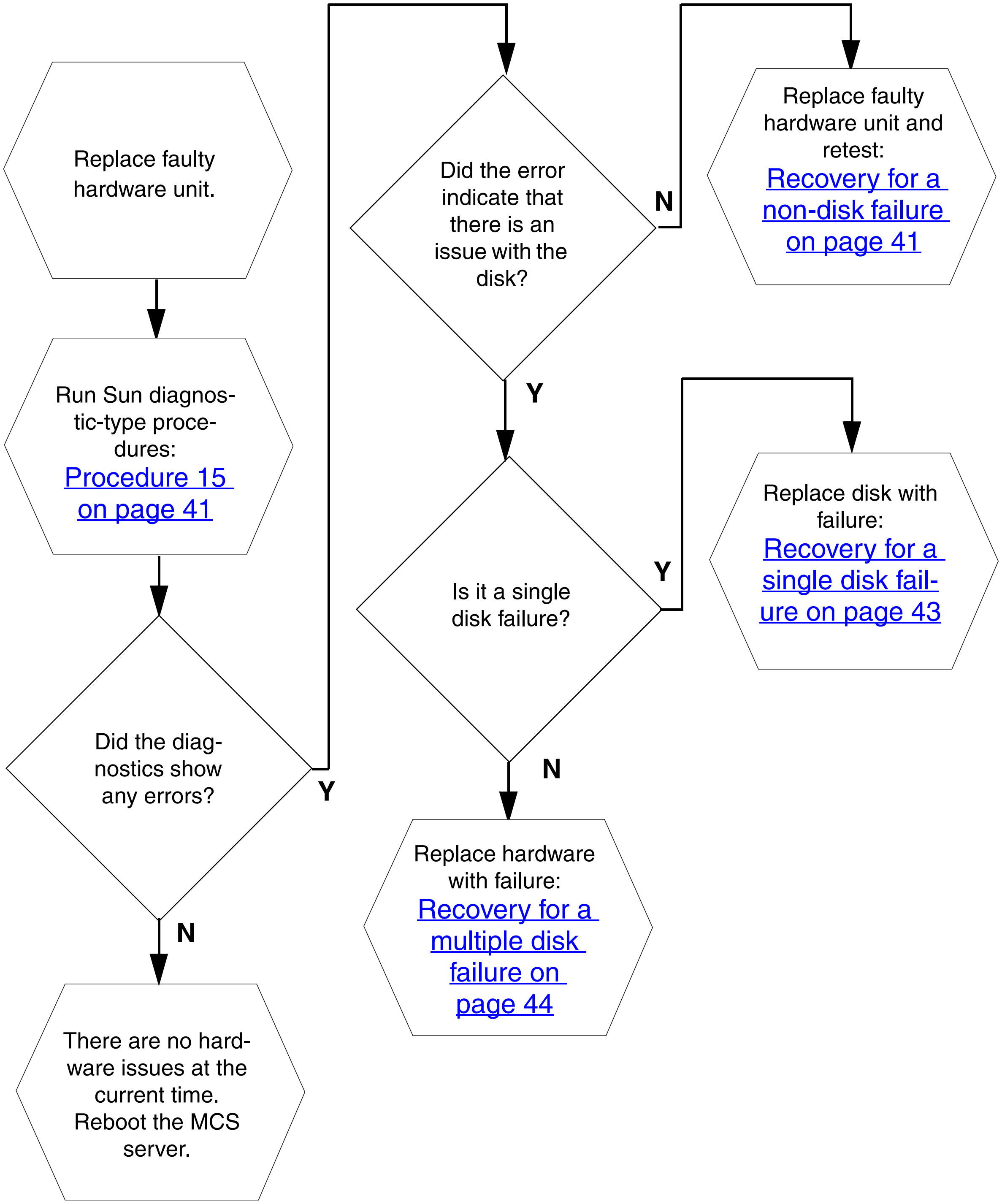
In the event of a hardware failure that is not due to a disk failure, the general process is to replace the faulty hardware component, re-test to make sure there are no other hardware issues, and then reboot the MCS server.

CAUTION

Prior to performing any hardware replacement, it is important to determine whether any support or warranty contracts are in place. If such support/warranty agreements are not utilized during the replacement, then the support/warranty agreement for the hardware may be voided.

The flow for this process is shown in Figure 2, Flow for recovering from a non-disk failure, on page 42.

Figure 2 Flow for recovering from a non-disk failure


Replace faulty hardware unit.
Run Sun diagnostic-type procedures: Procedure 15 on page 41
Did the diagnostics show any errors?
Y
N
There are no hardware issues at the current time. Reboot the MCS server.
Did the error indicate that there is an issue with the disk?
N
Replace faulty hardware unit and retest: Recovery for a non-disk failure on page 41
Y
Is it a single disk failure?
Y
Replace disk with failure: Recovery for a single disk failure on page 43
N
Replace hardware with failure: Recovery for a multiple disk failure on page 44

Recovery for a single disk failure

In the event of a single disk hardware failure, the general process is to replace the disk which had the failure.

CAUTION

Prior to performing any hardware replacement, it is important to determine whether any support or warranty contracts are in place. If such support/warranty agreements are not utilized during the replacement, then the support/warranty agreement for the hardware may be voided.

Disk replacement involves referencing the following documentation based on what type of MCS server had the failure:

- "Boot Problems" within Chapter 7 "Troubleshooting the System" of the *Solstice DiskSuite 4.2 User's Guide* at www.sun.com/documentation/

  Note: The following common items should be noted when using the above referenced document:

  — The replacement disk must be partitioned to match the known good disk prior to running the procedures within the document referenced above.

  — If performing the procedure "How to recover from Boot Device Failure," use **disk1** as the alternate boot device.

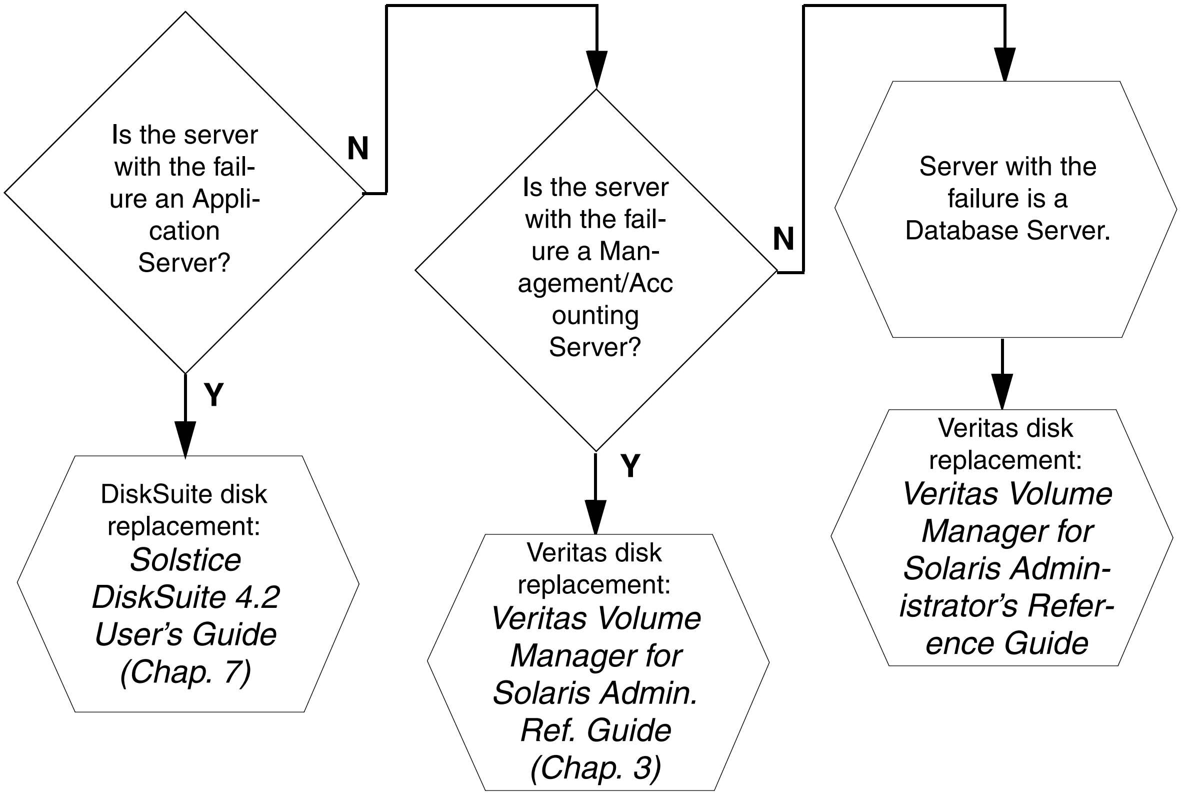
  — When calling commands (e.g. metadb, metastat, metareplace, etc.), use the **which** command to determine the path necessary to run the command.

  — If performing the procedure "How to recover from Insufficient State Database Replicas," it is important to verify the status of all mirrors/submirrors afterward.

- "Replacing Disks" within Chapter 3 "Disks and Disk Groups" of the *Veritas Volume Manager for Solaris Administrator's Reference Guide*.

For information on when to reference the above documentation, please refer to the flow for this process shown in Figure 3, Flow for recovering after a single disk failure, on page 44.

Figure 3 Flow for recovering after a single disk failure


Is the server with the failure an Application Server?
N
Y
DiskSuite disk replacement: *Solstice DiskSuite 4.2 User's Guide (Chap. 7)*
Is the server with the failure a Management/Accounting Server?
N
Y
Veritas disk replacement: *Veritas Volume Manager for Solaris Admin. Ref. Guide (Chap. 3)*
Server with the failure is a Database Server.
Veritas disk replacement: *Veritas Volume Manager for Solaris Administrator's Reference Guide*

Recovery for a multiple disk failure

In the event of a catastrophic disk failure, a new server is required and a restore of a previous backup of the MCS server must be performed. Figure 4 on page 45 through Figure 9 on page 50 provide the steps required to recover from this type of failure scenario.

Should both servers running redundant databases fail, these steps must be repeated for both servers with the primary database being restored first.

Figure 4 Flow for recovering after a multiple disk failure

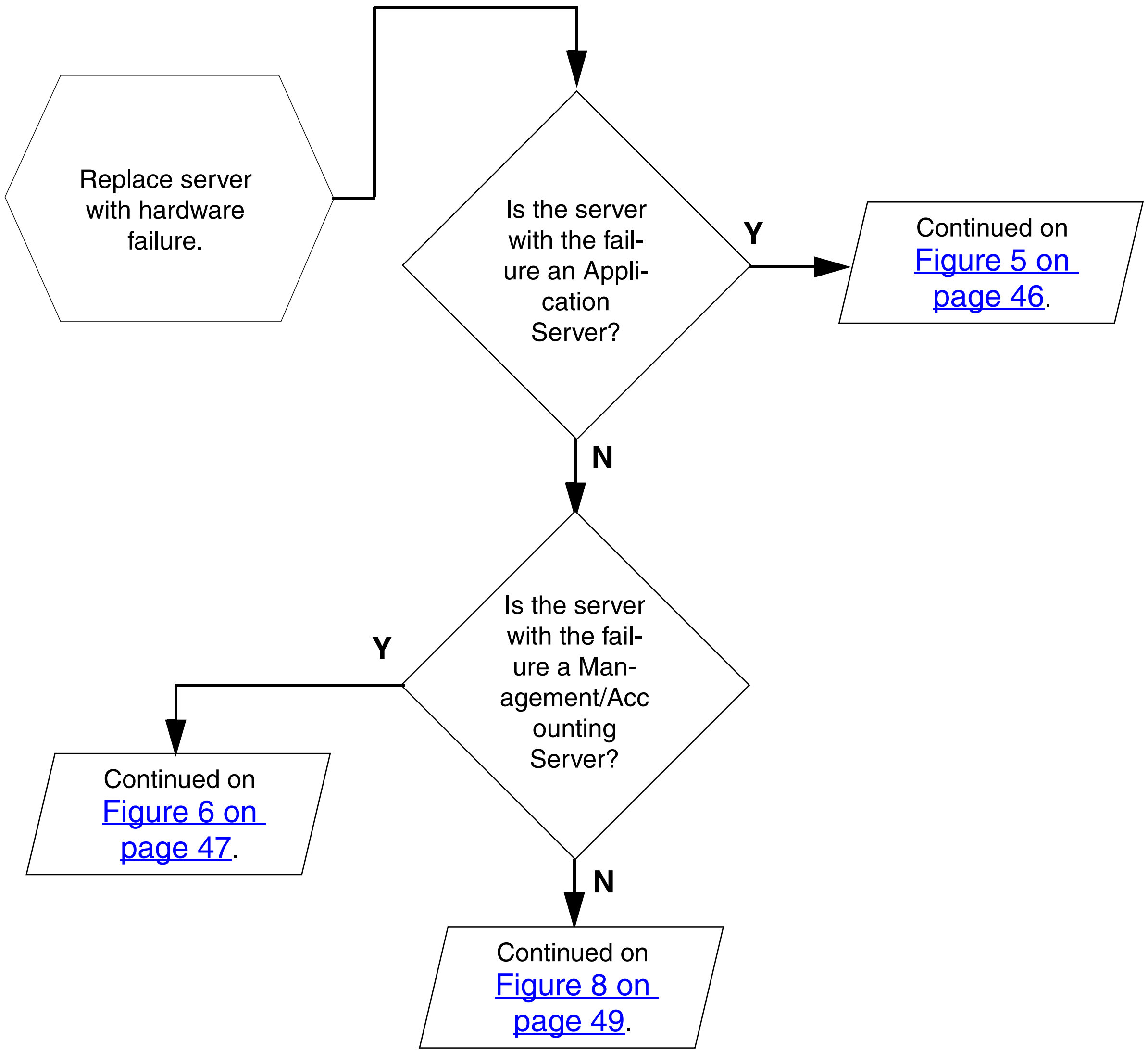

Replace server with hardware failure.
Is the server with the failure an Application Server?
Y
Continued on Figure 5 on page 46.
N
Is the server with the failure a Management/Accounting Server?
Y
Continued on Figure 6 on page 47.
N
Continued on Figure 8 on page 49.

Figure 5 Flow for recovering an Application server after a multiple disk failure

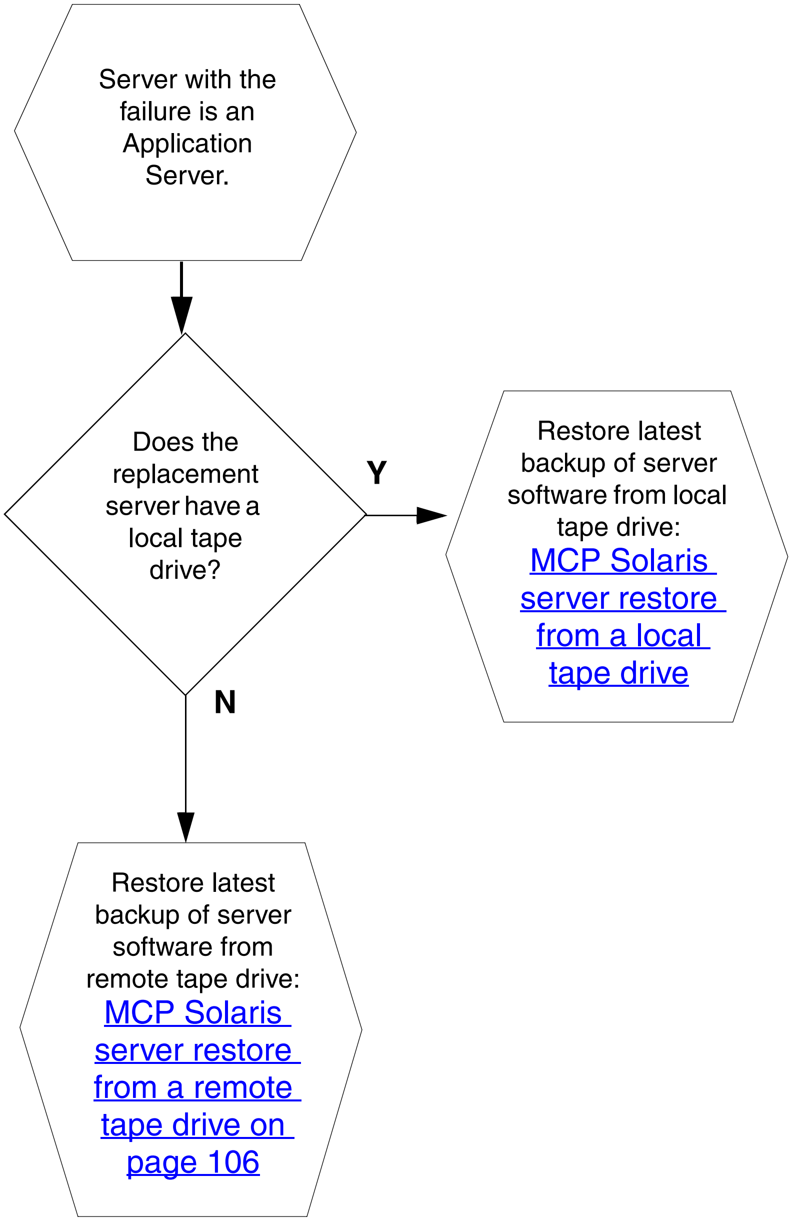

Server with the failure is an Application Server.
Does the replacement server have a local tape drive?
Y
Restore latest backup of server software from local tape drive:
MCP Solaris server restore from a local tape drive
N
Restore latest backup of server software from remote tape drive:
MCP Solaris server restore from a remote tape drive on page 106

Figure 6 Flow for recovering a Management/Accounting server after a multiple disk failure

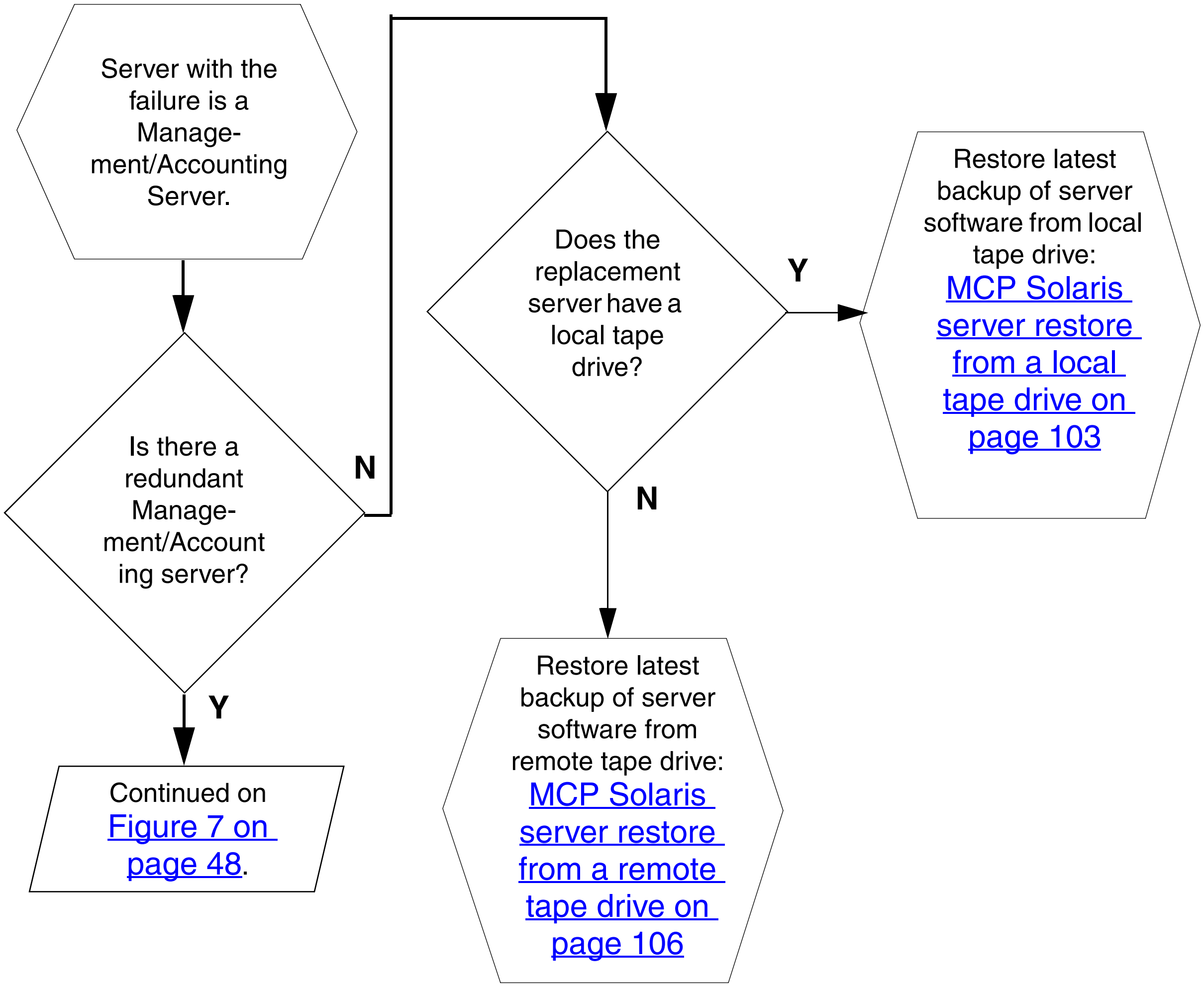

Server with the failure is a Management/Accounting Server.
Is there a redundant Management/Accounting server?
N
Y
Continued on Figure 7 on page 48.
Does the replacement server have a local tape drive?
Y
N
Restore latest backup of server software from local tape drive: MCP Solaris server restore from a local tape drive on page 103
Restore latest backup of server software from remote tape drive: MCP Solaris server restore from a remote tape drive on page 106

Figure 7 Flow for recovering a redundant Management/Accounting server after a multiple disk failure

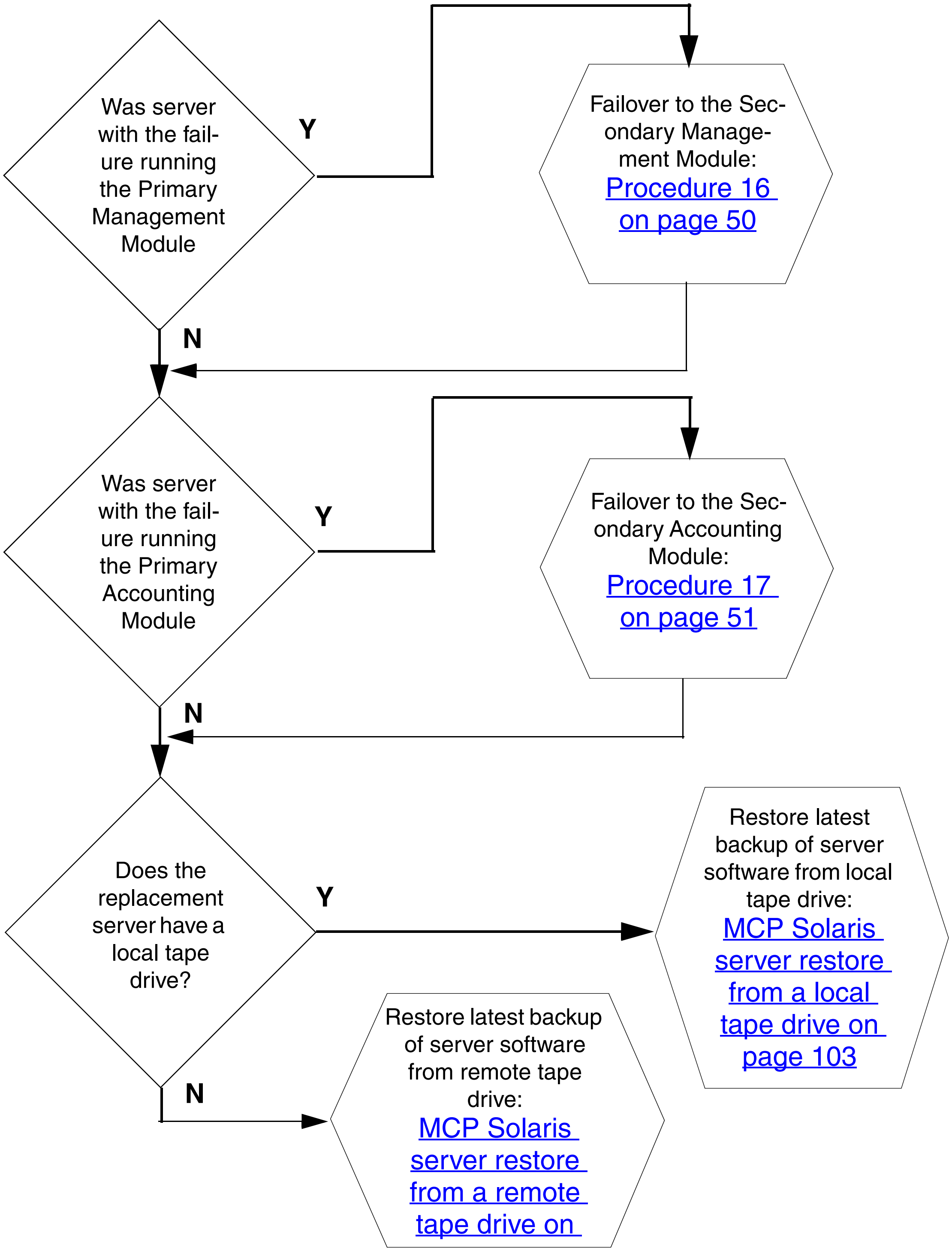

Was server with the failure running the Primary Management Module
Y
Failover to the Secondary Management Module: Procedure 16 on page 50
N
Was server with the failure running the Primary Accounting Module
Y
Failover to the Secondary Accounting Module: Procedure 17 on page 51
N
Does the replacement server have a local tape drive?
Y
Restore latest backup of server software from local tape drive: MCP Solaris server restore from a local tape drive on page 103
N
Restore latest backup of server software from remote tape drive: MCP Solaris server restore from a remote tape drive on

Figure 8 Flow for recovering a Database server after a multiple disk failure

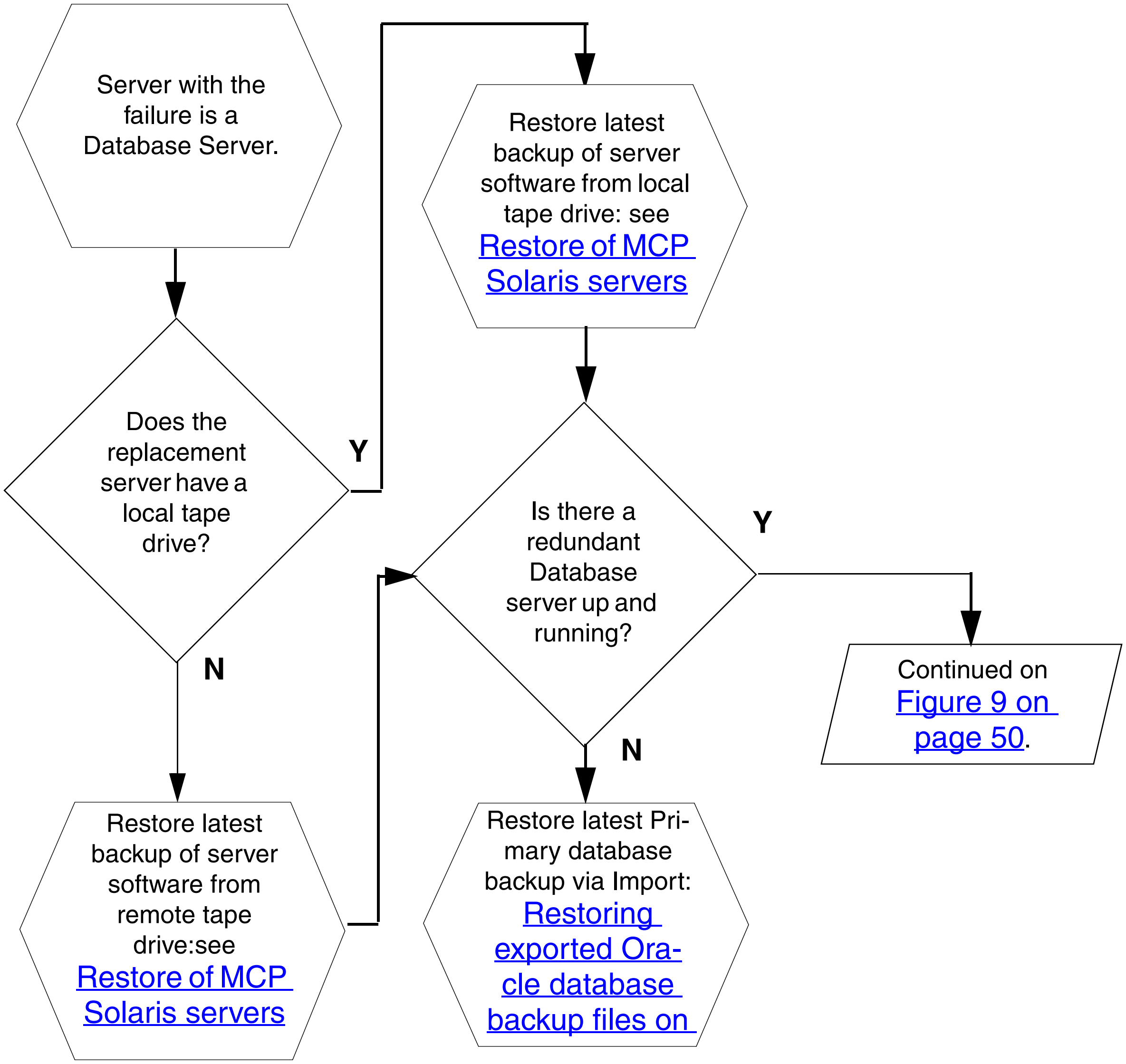
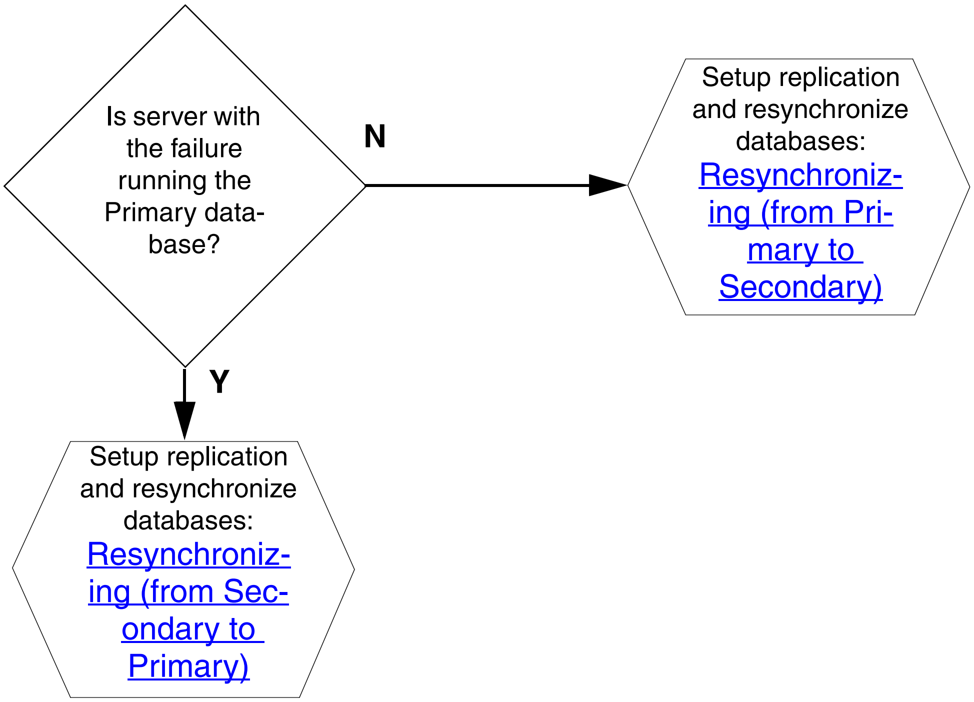

Server with the failure is a Database Server.
Does the replacement server have a local tape drive?
Y
N
Restore latest backup of server software from local tape drive: see Restore of MCP Solaris servers
Restore latest backup of server software from remote tape drive:see Restore of MCP Solaris servers
Is there a redundant Database server up and running?
Y
N
Continued on Figure 9 on page 50.
Restore latest Primary database backup via Import: Restoring exported Oracle database backup files on

Figure 9 Flow for recovering a redundant Oracle database after a multiple disk failure


Is server with the failure running the Primary database?
N
Y
Setup replication and resynchronize databases:
Resynchronizing (from Primary to Secondary)
Setup replication and resynchronize databases:
Resynchronizing (from Secondary to Primary)

Procedure 16 Starting the cold standby Management Module

from the administrator's workstation

1 Log into the server hosting the secondary SysMgr component.

IP Address: <physical address of server>

Login ID: **sysadmin**

2 Navigate to the directory with the failover script.

```
cd /IMS/mgmtsvr/bin
```

3 Execute the failover startup script to start SysMgr processes and take ownership of the logical IP address.

```
sudo Failover.pl start sysmgr
```

When the startup is finished, the screen will display the name and path of the log file associated with this event.

Procedure 17 Starting the cold standby Accounting Module instance

From the administrator workstation

1 Establish a remote login session to the server hosting the cold standby Accounting Module. Log in as **sysadmin**.

2 Type

cd /IMS/acctmgr/bin

3 Use the **sudo** command to execute the Failover script using the following syntax:

sudo Failover.pl start acctmgr

The process will be stopped, the logical IP will be assigned for this machine and the Accounting Module process restarted.

Restoring exported Oracle database backup files

> **CAUTION**
>
> Only trained personnel should perform the following task.

Use the following procedure to restore files created using the Export/Import backup method:

Note 1: Stop all network components that connect to the Oracle database before performing this procedure. After the procedure is completed, start all network components to return them to their previous state.The following components connect to the database: Oracle Monitor, Provisioning Module, SIP Application Module, IP Client Manager, Web Client Manager, and Management Module.

Note 2: The approximate import time, when recovering a database, is 100 MegaBytes of data per hour.

Procedure 18 Restoring an exported Oracle database

On the server hosting the primary database

a Shut down the primary database as follows:

- **i** Log in as **root**.
- **ii** Execute the following commands:

  cd /etc/init.d

  ./dbora stop

b Set up a clean database as follows:

- **i** Log in as **oracle**.
- **ii** Execute the following commands:

  cd /export/home/oracle/bin

  ./**restore_empty_db**

c Start up the primary database as follows:

- **i** Log in as **root**.
- **ii** Execute the following commands:

  cd /etc/init.d

  ./dbora start

d Restore the primary database as follows:

- **i** Log in as **oracle** to the server hosting the primary database.
- **ii** Execute the following commands:

  cd /IMS/imssipdb/data/db_schema/backup

  ./**import_imsdb1.sh PRIMARY <name_of_backup> <media_type>**

  where **name_of_backup** is the name of the backup file and **media_type** can be a DISK or TAPE where the backup is located.

  > ***Note:*** If restoring the database from disk, the **name_of_backup** file must be located within the **/backup/orabackup** directory.

Resynchronizing (from Primary to Secondary)

The following procedure should be used when the secondary database must be synchronized with the data from the primary database. In this way, the secondary database is updated with the most current data which is resident in the primary database.

Procedure 19 Drop replication:

1 Log in as **oracle** to the server hosting the primary database.

2 Execute the following commands:

```
cd /IMS/imssipdb/data/db_schema/util
./remove_replication.sh
```

Procedure 20 Deploying the database to the secondary database server:

1 Log in as **nortel** to the management server.

2 Execute the following commands:

```
dbdeploy.pl
```

3 When prompted about replication, type **N**

4 When prompted for type of deployment, select **Install files only**

5 When prompted for the primary database, provide the IP address of the secondary database.

Procedure 21 Prepare to replicate the database:

1 Log in as **oracle** to the server hosting the primary database.

2 Execute the following commands:

cd /export/home/oracle/bin/upgrade/logs

pwd (verify that path displayed is the same as path listed in above **cd** command)

rm *

cd /export/home/oracle/bin/upgrade

./prepare_replication.sh

3 If you see the message “ERROR at line 1: ORA-00955: name is already used by an existing object.”, do the following:

a Login to the Secondary database as **oracle**.

b Execute the following commands:

```
cd /export/home/oracle/bin
./restore_empty_db
```

c Restart this procedure.

4 When prompted to restart the database, type **Y**.

Procedure 22 Perform a backup of the primary database

During the backup process, copy data transactions that occur to the secondary database. Once the backup is complete, start queueing these data transactions to the primary database:

1. Log in as **oracle** to the server hosting the primary database.
2. Execute the following commands:

   cd /export/home/oracle/bin/upgrade

   ./add_secondary_db.sh

Procedure 23 Setting up replication

Setup replication:

1. Log in as **oracle** to the server hosting the secondary database.
2. Execute the following commands:

   cd /export/home/oracle/bin/upgrade

   ./activate_secondary_db.sh <primary_DB_hostname>

   Note: The activate_secondary_db.sh script uses Secure FTP to transfer the backup (taken above) from the primary database to the secondary database. If this is the first time Secure FTP has been used on this server, the administrator will be prompted to confirm the authenticity of the host with the following question: The authenticity of host … can't be established. RSA key fingerprint … Are you sure you want to continue connecting (yes/no)? Type **yes** in response.
3. When prompted for the "`oracle@<hostname> password`", enter the oracle password for the primary database
4. When prompted to restart the database, type **Y**.

Procedure 24 Turning off archiving logs on primary database

Turn off archiving logs on primary database:

1. Log in as **oracle** to the server hosting the primary database.
2. Execute the following commands:

   cd /export/home/oracle/bin

   ./archivallogctl off
3. When prompted to restart the database, type **Y**.

Procedure 25 Clean up the primary and secondary databases

Clean up the primary and secondary databases:

1. Log in as **oracle** to the server hosting the primary database.
2. Execute the following commands:

   cd /export/home/oracle/bin/upgrade

   ./clean.sh
3. Repeat this procedure on the server hosting the secondary database.

Procedure 26 Reconfigure the database SNMP agent

Re-configure the database SNMP agent:

1. Log in as **root** to the server hosting the secondary database.
2. Execute the following commands:

   cd /export/home/oracle/bin

   ./config_snmp

Procedure 27 Undeploy database from secondary database server

Undeploy database from the secondary database server:

1. Log in as **nortel** to the server hosting the secondary database.
2. Execute the following commands:

   dsmundeploy -load <DB_load> -node <secondary_DB_IP>

Resynchronizing (from Secondary to Primary)

The following procedure should be used when the primary database must be synchronized with the data from the secondary database. In this way, the primary database is updated with the most current data which is resident in the secondary database.

Procedure 28 Dropping replication

Drop replication:

1. Log in as **oracle** to the server hosting the primary database.
2. Execute the following commands:

   cd /IMS/imssipdb/data/db_schema/util

./remove_replication.sh

Procedure 29 Deploying the database to the secondary database server

Deploy database to the secondary database server:

1 Log in as **nortel** to the management server.

2 Execute the following commands:

dbdeploy.pl

When prompted about replication, type **N**

When prompted for type of deployment, select **Install Files only**

when prompted for the primary database, provide the IP address of the secondary database.

Procedure 30 Prepare to replicate the database

Prepare to replicate the database:

1 Log in as **oracle** to the server hosting the secondary database.

2 Execute the following commands:

cd /export/home/oracle/bin/upgrade/logs

pwd (verify that path displayed is the same as path listed in above **cd** command)

rm *

cd /export/home/oracle/bin/upgrade

./prepare_replication_at_secondary.sh

When prompted to restart the database, type **Y**.

Procedure 31 Perform a backup of the secondary database

Perform a backup of the secondary database:

1 Log in as **oracle** to the server hosting the secondary database.

2 Execute the following commands:

cd /export/home/oracle/bin/upgrade

./add_primary_db.sh

Procedure 32 Setting up replication

Setup replication:

1 Log in as **oracle** to the server hosting the primary database.

2 Execute the following commands:

```
cd /export/home/oracle/bin/upgrade
./activate_primary_db.sh <secondary_DB_hostname>
```

> ***Note:*** The activate_primary_db.sh script uses Secure FTP to transfer the backup (taken above) from the secondary database to the primary database. If this is the first time Secure FTP has been used on this server, the administrator will be prompted to confirm the authenticity of the host with the following question: The authenticity of host … can't be established. RSA key fingerprint … Are you sure you want to continue connecting (yes/no)? Type **yes** in response.

When prompted for the "`oracle@<hostname> password`", enter the oracle password for the secondary database

When prompted to restart the database, type **Y**.

Procedure 33 Turning off archiving logs on secondary database

Turn off archiving logs on secondary database:

1 Log in as **oracle** to the server hosting the secondary database.

2 Execute the following commands:

```
cd /export/home/oracle/bin
./archivallogctl off
```

When prompted to restart the database, type **Y**.

Procedure 34 Cleaning up the primary and secondary databases

Clean up the primary and secondary databases:

1 Log in as **oracle** to the server hosting the primary database.

2 Execute the following commands:

```
cd /export/home/oracle/bin/upgrade
./clean.sh
```

3 Repeat this procedure on the server hosting the secondary database.

Procedure 35 Reconfiguring the database SNMP agent

Re-configure the database SNMP agent:

1 Log in as **root** to the server hosting the primary database.

2 Execute the following commands:

```
cd /export/home/oracle/bin
./config_snmp
```

Procedure 36 Undeploy database from secondary database server

Undeploy database from secondary database server:

1. Log in as **nortel** to the server hosting the secondary database.
2. Execute the following commands:

   ```
   dsmundeploy -load <DB_load> -node <secondary_DB_IP>
   ```

Recovery for Sun Netra 240 server

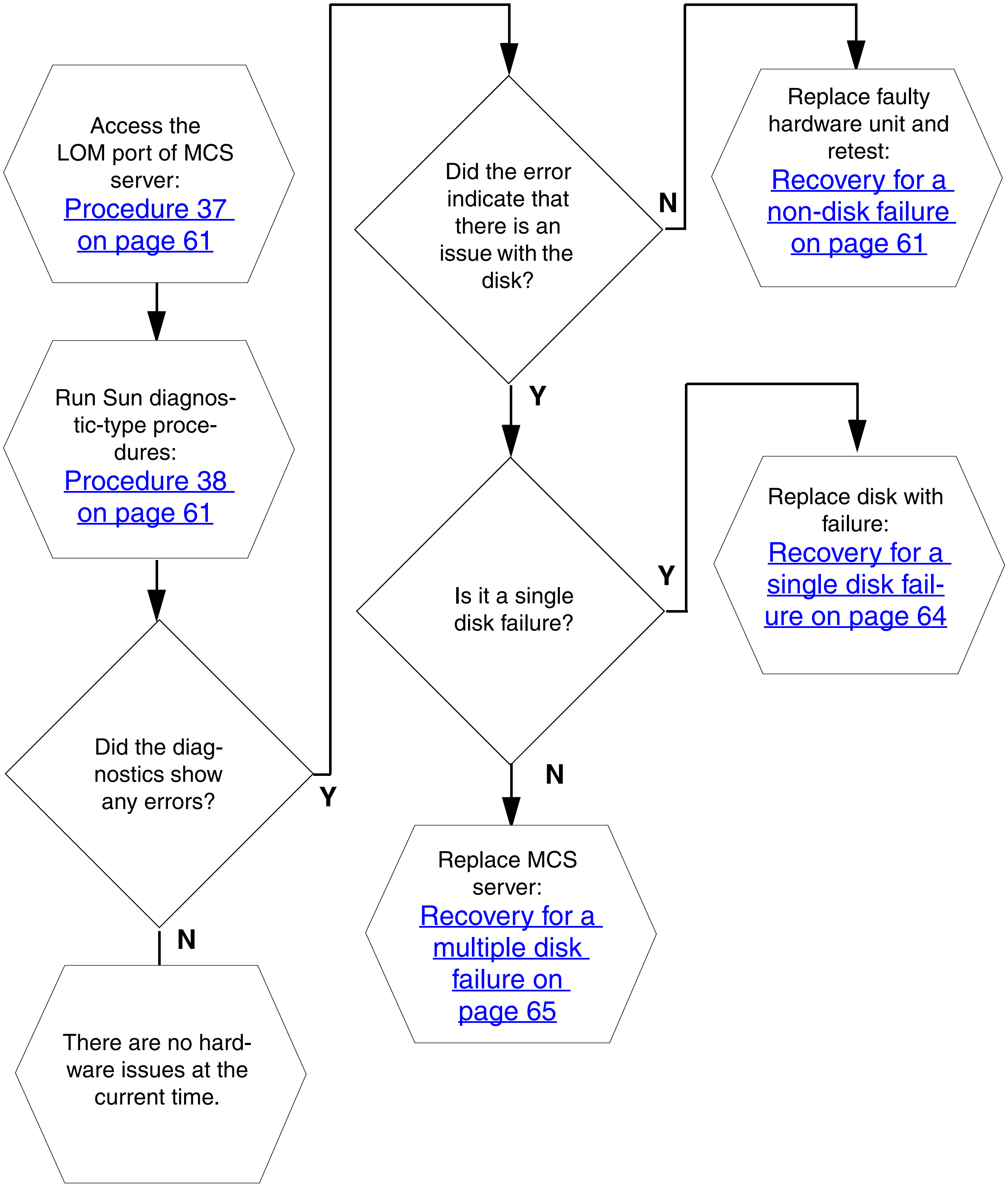
This chapter is organized as follows:

Determining existence of hardware problems

The first step is to determine if or where a failure has occurred. Figure 10, Flow for determining existence of a hardware problem, on page 60 walks through the steps required to determine the existence of any hardware failures on an MCS server using the Sun Netra 240 platform.

Should both servers running redundant databases fail, these steps must be repeated for both servers with the primary database being restored first.

Figure 10 Flow for determining existence of a hardware problem


Access the LOM port of MCS server: Procedure 37 on page 61
Run Sun diagnostic-type procedures: Procedure 38 on page 61
Did the diagnostics show any errors?
Y
N
There are no hardware issues at the current time.
Did the error indicate that there is an issue with the disk?
N
Y
Replace faulty hardware unit and retest: Recovery for a non-disk failure on page 61
Is it a single disk failure?
Y
N
Replace disk with failure: Recovery for a single disk failure on page 64
Replace MCS server: Recovery for a multiple disk failure on page 65

Procedure 37 Access LOM (Lights Out Management) port

1 Telnet to the NetMgmt port IP. This is a regular, not secure telnet.

2 Login as **admin**.

user name: **admin**
admin password: **<admin_pswd>**

Where
<admin_pswd> is the admin password set during the N 240 server installation.

A successful login gets you to the **sc** prompt.

3 Enter the following at the sc prompt.

```
console -f
```

This brings up console login prompt.

4 Login as either **sysadmin**, **root**, or **oracle** depending on the procedures being performed.

5 When finished and ready to exit the console session, you MUST enter a “**#.**" to return back to the **sc** prompt. If you Failure to type "**#.**" that will lock up the console port.

```
“#.”
```

You will return to the **sc** prompt.

Procedure 38 Run Sun diagnostic-type procedures

From the telnet session

1 Execute the diagnostic procedures as described in the *Sun Fire Netra 240 Administrative Guide*. Execute any actions suggested within the procedure.

Recovery for a non-disk failure

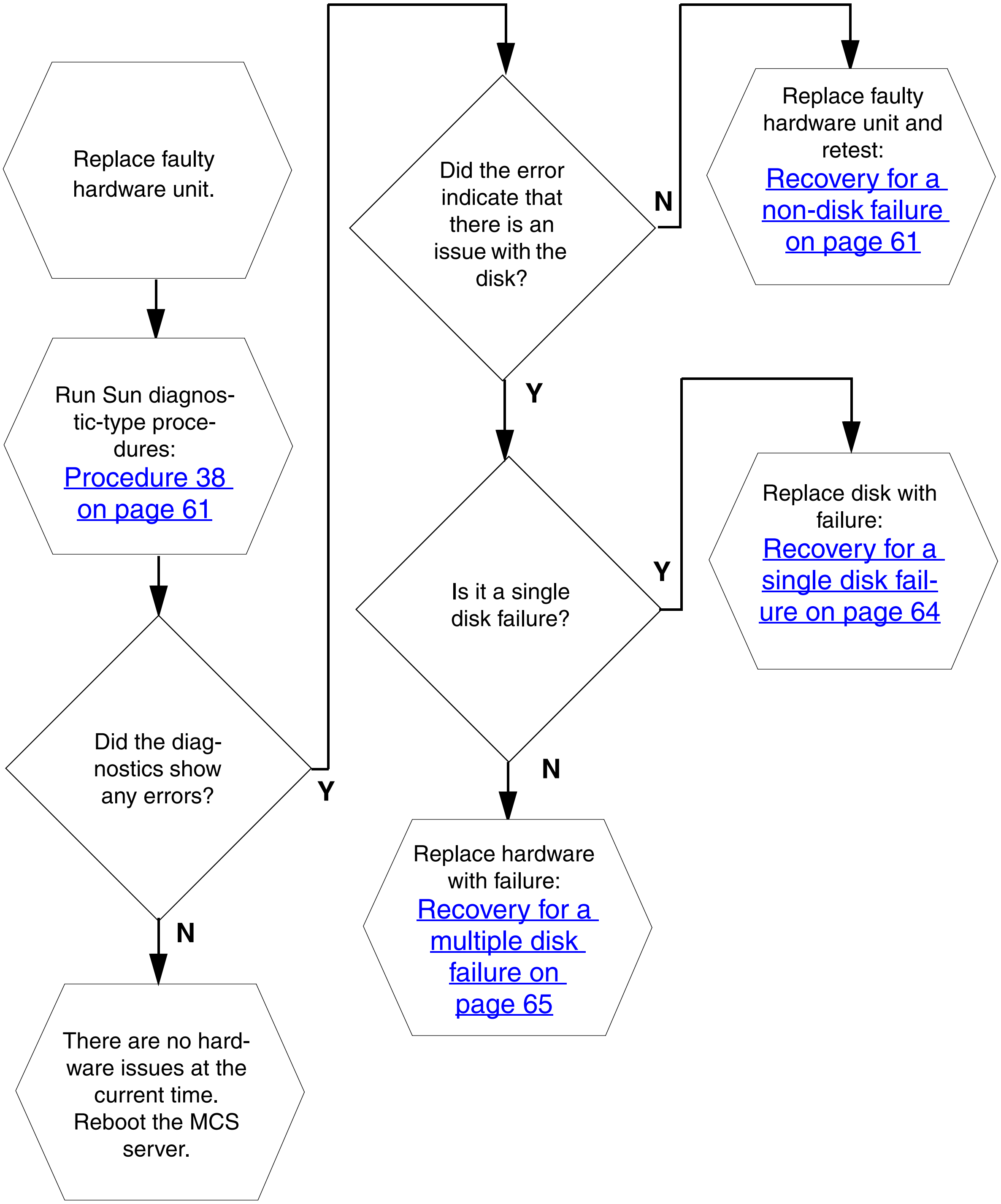
In the event of a hardware failure that is not due to a disk failure, the general process is to replace the faulty hardware component, re-test to make sure there are no other hardware issues, and then reboot the MCS server.

CAUTION

Prior to performing any hardware replacement, it is important to determine whether any support or warranty contracts are in place. If such support/warranty agreements are not utilized during the replacement, then the support/warranty agreement for the hardware may be voided.

The flow for this process is shown in Figure 11, Flow for recovering from a non-disk failure, on page 63.

Figure 11 Flow for recovering from a non-disk failure


Replace faulty hardware unit.
Run Sun diagnostic-type procedures:
Procedure 38 on page 61
Did the diagnostics show any errors?
Y
N
There are no hardware issues at the current time. Reboot the MCS server.
Did the error indicate that there is an issue with the disk?
N
Replace faulty hardware unit and retest:
Recovery for a non-disk failure on page 61
Y
Is it a single disk failure?
Y
Replace disk with failure:
Recovery for a single disk failure on page 64
N
Replace hardware with failure:
Recovery for a multiple disk failure on page 65

Recovery for a single disk failure

In the event of a single disk hardware failure, the general process is to replace the disk.

CAUTION

Prior to performing any hardware replacement, it is important to determine whether any support or warranty contracts are in place. If such support/warranty agreements are not utilized during the replacement, then the support/warranty agreement for the hardware may be voided.

Disk replacement involves referencing the following documentation based on what type of MCS server had the failure:

- “Boot Problems” within Chapter 7 “Troubleshooting the System” of the *Solstice DiskSuite 4.2 User’s Guide* at www.sun.com/documentation/.

  Note: The following common items should be noted when using the above referenced document:

  — The replacement disk must be partitioned to match the known good disk prior to running the procedures within the document referenced above.

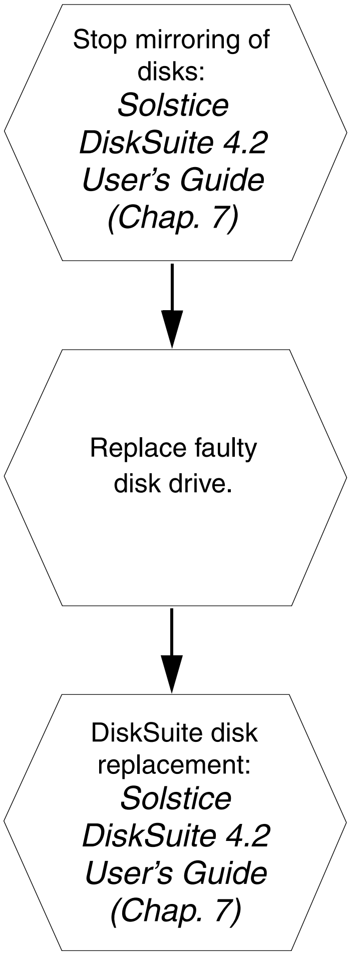
  — If performing the procedure “How to recover from Boot Device Failure,” use **disk1** as the alternate boot device.

  — When calling commands (e.g. metadb, metastat, metareplace, etc.), use the **which** command to determine the path necessary to run the command.

  — If performing the procedure “How to recover from Insufficient State Database Replicas,” it is important to verify the status of all mirrors/submirrors afterward.

For information on when to reference the above documentation, please refer to the flow for this process shown in Figure 12, Flow for recovering after a single disk failure, on page 65.

Figure 12 Flow for recovering after a single disk failure


Stop mirroring of disks:
Solstice DiskSuite 4.2 User's Guide (Chap. 7)
Replace faulty disk drive.
DiskSuite disk replacement:
Solstice DiskSuite 4.2 User's Guide (Chap. 7)

Recovery for a multiple disk failure

In the event of a catastrophic disk failure, a new server is required and a restore of a previous backup of the MCS server must be performed. Figure 13 on page 66 through Figure 18 on page 71 provide the steps required to recover from this type of failure scenario.

Figure 13 Flow for recovering after a multiple disk failure

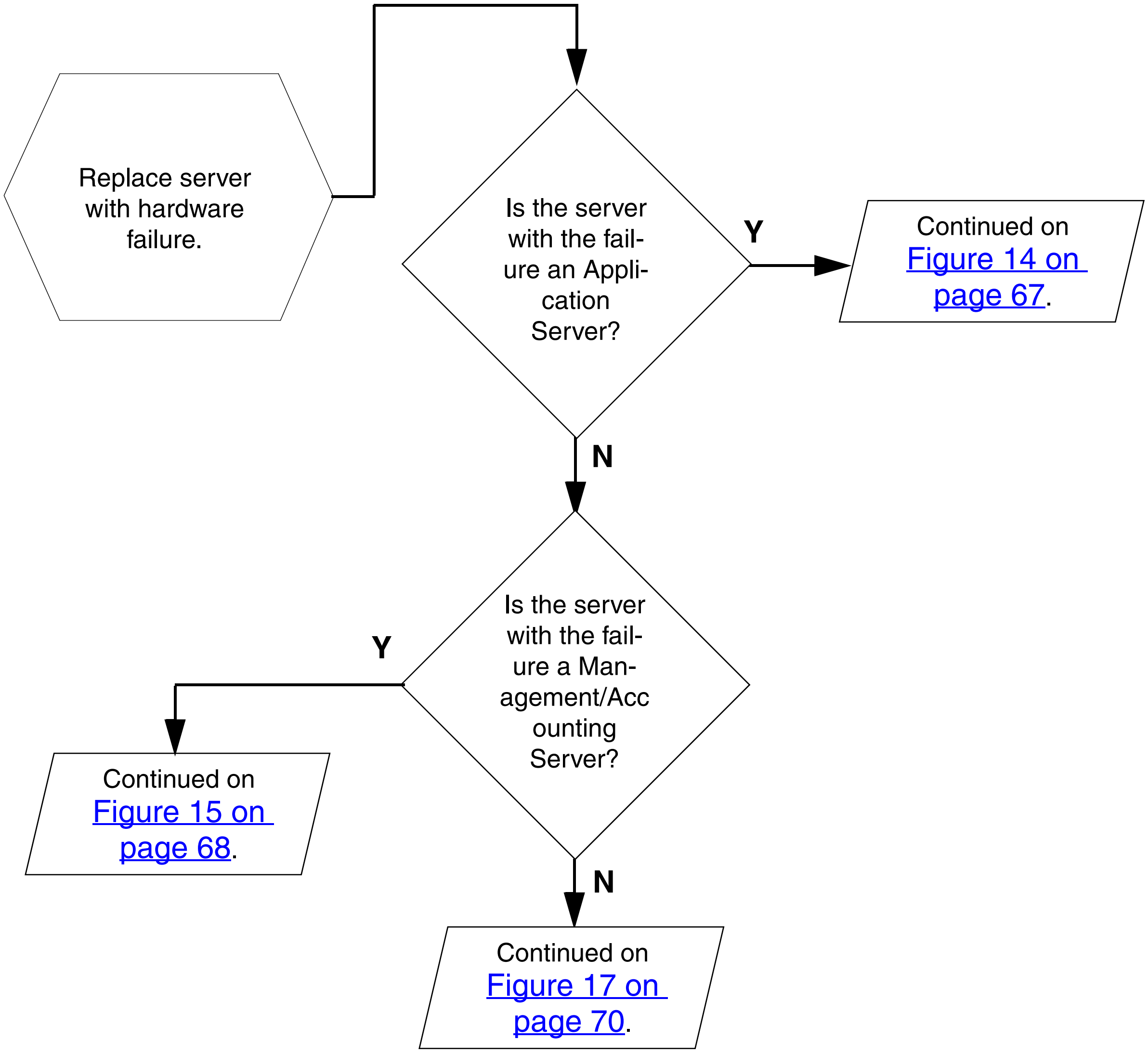

Replace server with hardware failure.
Is the server with the failure an Application Server?
Y
Continued on Figure 14 on page 67.
N
Is the server with the failure a Management/Accounting Server?
Y
Continued on Figure 15 on page 68.
N
Continued on Figure 17 on page 70.

Figure 14 Flow for recovering an Application server after a multiple disk failure

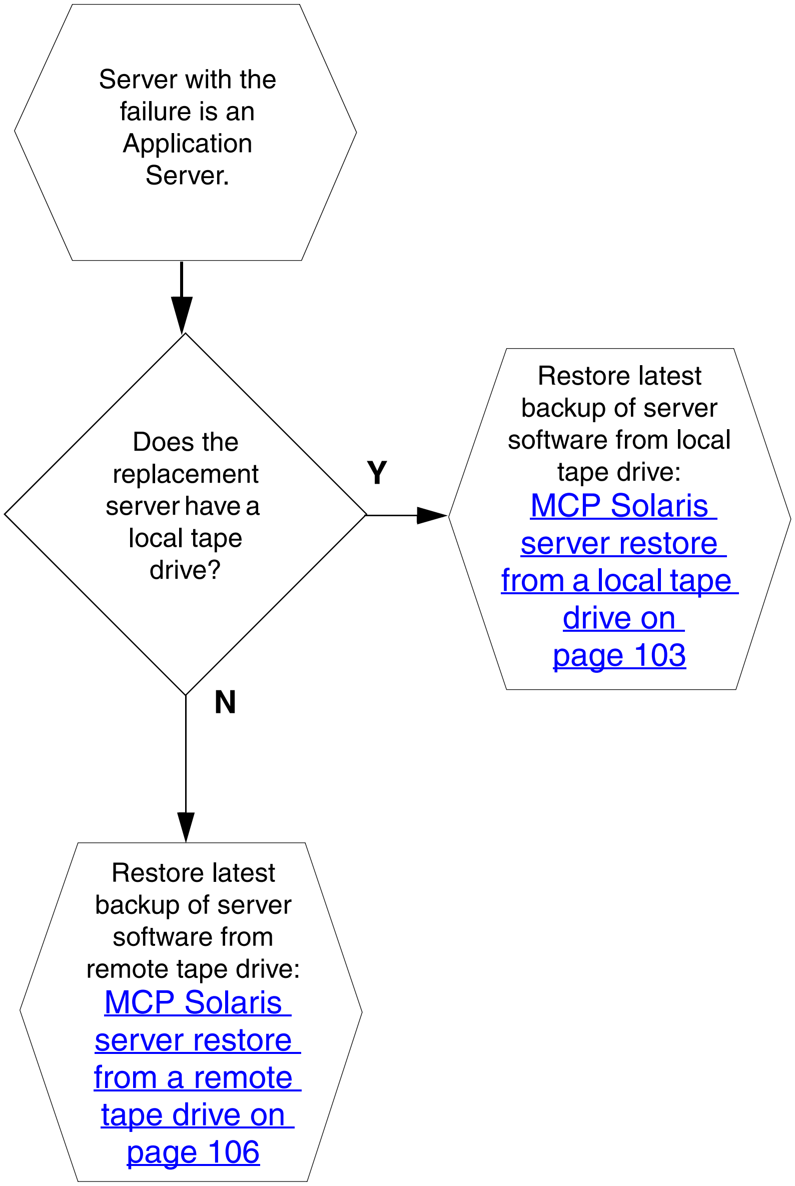

Server with the failure is an Application Server.
Does the replacement server have a local tape drive?
Y
Restore latest backup of server software from local tape drive:
MCP Solaris server restore from a local tape drive on page 103
N
Restore latest backup of server software from remote tape drive:
MCP Solaris server restore from a remote tape drive on page 106

Figure 15 Flow for recovering a Management/Accounting server after a multiple disk failure

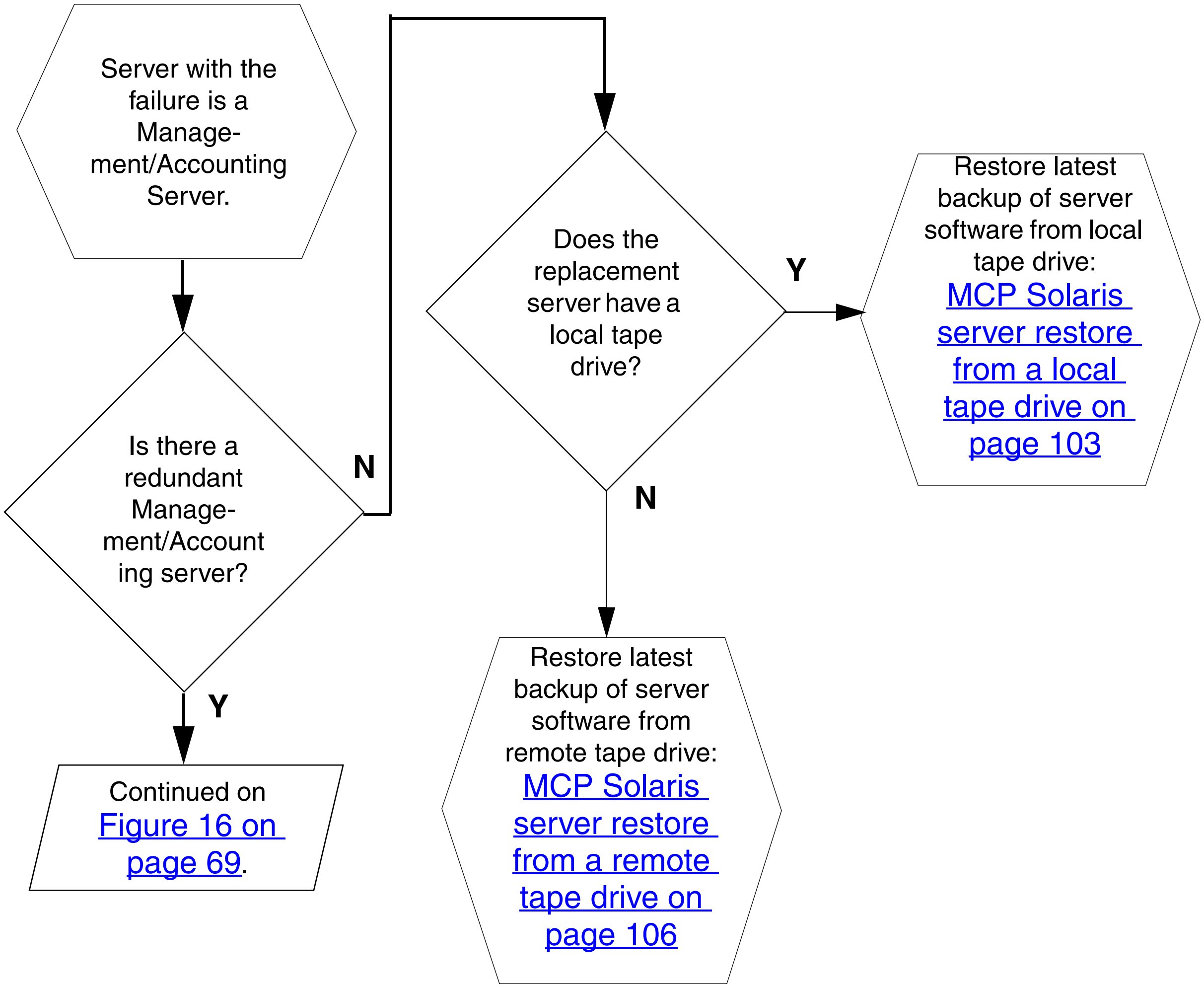

Server with the failure is a Management/Accounting Server.
Is there a redundant Management/Accounting server?
N
Y
Continued on Figure 16 on page 69.
Does the replacement server have a local tape drive?
Y
N
Restore latest backup of server software from local tape drive: MCP Solaris server restore from a local tape drive on page 103
Restore latest backup of server software from remote tape drive: MCP Solaris server restore from a remote tape drive on page 106

Figure 16 Flow for recovering a redundant Management/Accounting server after a multiple disk failure

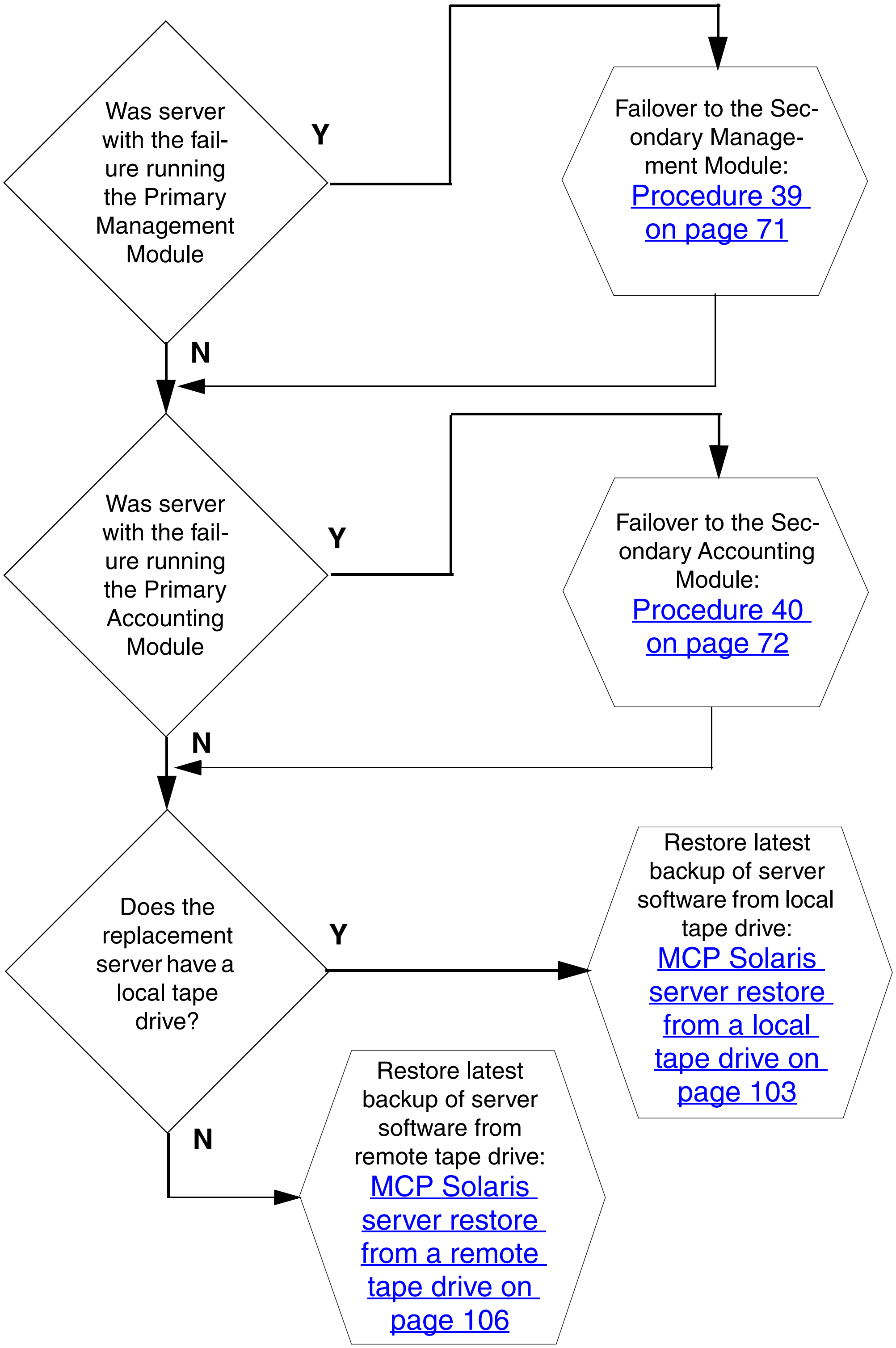

Was server with the failure running the Primary Management Module
Y
N
Failover to the Secondary Management Module: Procedure 39 on page 71
Was server with the failure running the Primary Accounting Module
Y
N
Failover to the Secondary Accounting Module: Procedure 40 on page 72
Does the replacement server have a local tape drive?
Y
N
Restore latest backup of server software from local tape drive: MCP Solaris server restore from a local tape drive on page 103
Restore latest backup of server software from remote tape drive: MCP Solaris server restore from a remote tape drive on page 106

Figure 17 Flow for recovering a Database server after a multiple disk failure

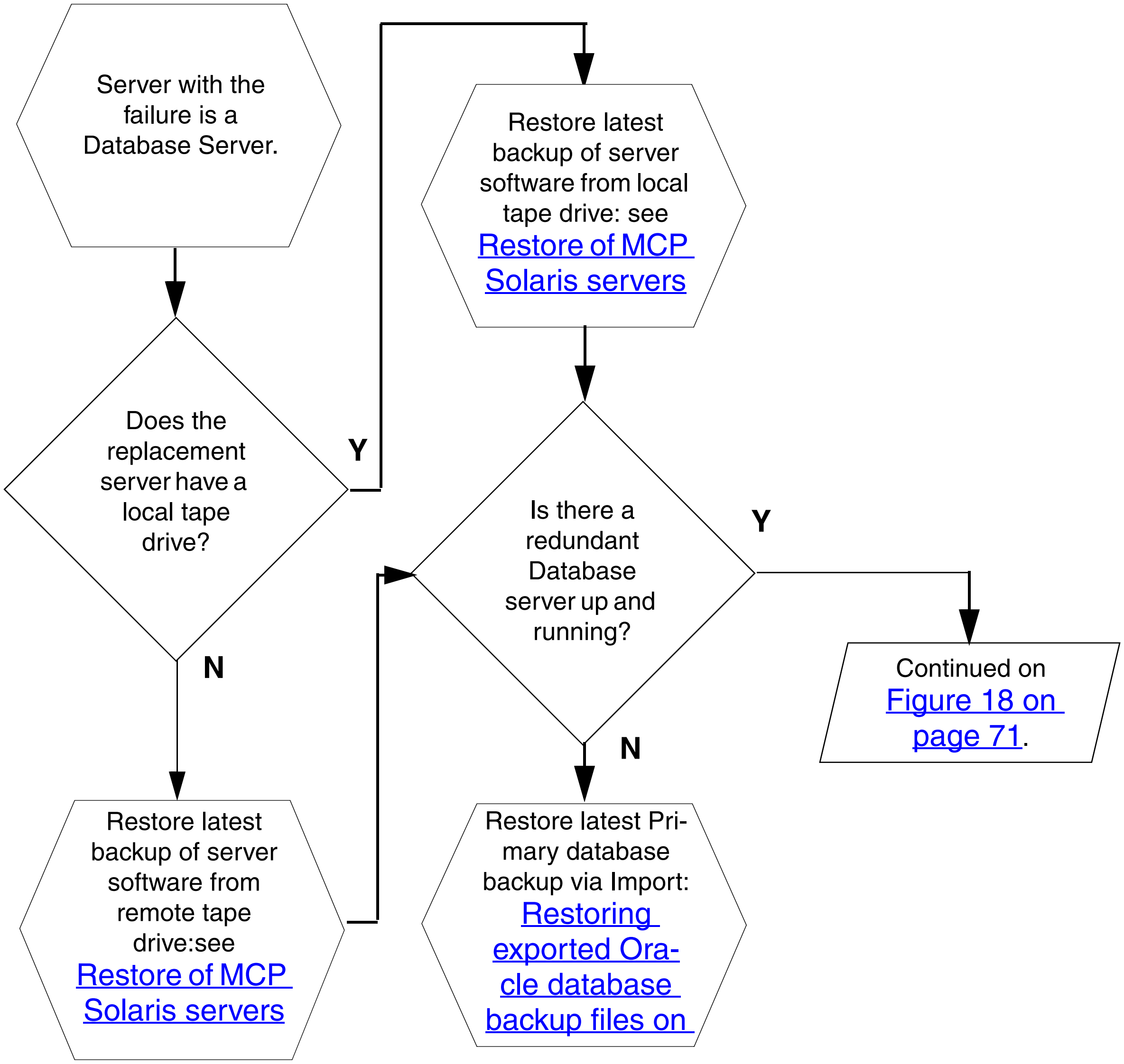
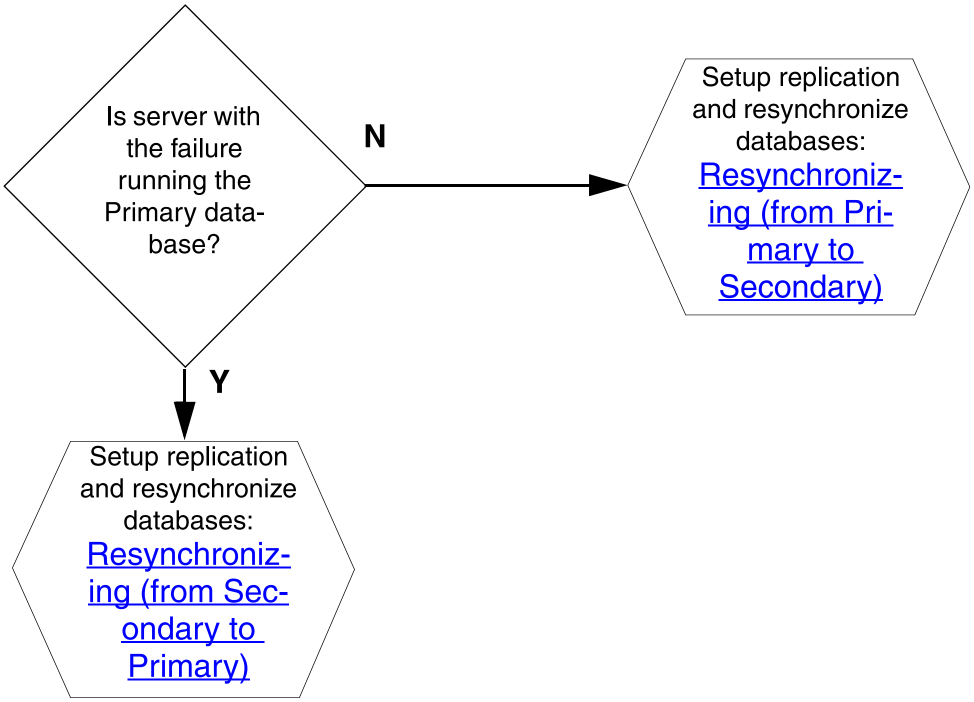

Server with the failure is a Database Server.
Does the replacement server have a local tape drive?
Y
N
Restore latest backup of server software from local tape drive: see Restore of MCP Solaris servers
Restore latest backup of server software from remote tape drive:see Restore of MCP Solaris servers
Is there a redundant Database server up and running?
Y
N
Continued on Figure 18 on page 71.
Restore latest Primary database backup via Import: Restoring exported Oracle database backup files on

Figure 18 Flow for recovering a redundant Oracle database after a multiple disk failure


Is server with the failure running the Primary database?
N
Setup replication and resynchronize databases:
Resynchronizing (from Primary to Secondary)
Y
Setup replication and resynchronize databases:
Resynchronizing (from Secondary to Primary)

Procedure 39 Starting the cold standby Management Module instance

from the administrator's workstation

1 Log onto the server hosting the secondary SysMgr component.

IP Address: <physical address of server>

Login ID: **sysadmin**

2 Navigate to the directory with the failover script.

```
cd /IMS/mgmtsvr/bin
```

3 Execute the failover startup script to start SysMgr processes and take ownership of the logical IP address.

```
sudo Failover.pl start sysmgr
```

When the startup is finished, the screen will display the name and path of the log file associated with this event.

Procedure 40 Starting the cold standby Accounting Module instance

From the administrator workstation

1 Establish a remote login session to the server hosting the cold standby Accounting Module. Log in as **sysadmin**.

2 type: **cd /IMS/acctmgr/bin**

3 Use the sudo command to execute the Failover script using the following syntax:

type: **sudo Failover.pl start acctmgr**

The process will be stopped, the logical IP will be assigned for this machine and the Accounting Module process restarted.

Restoring exported Oracle database backup files

> **CAUTION**
>
> Only trained personnel should perform the following task.

Use the following procedure to restore files created using the Export/Import backup method:

Note 1: Stop all network components that connect to the Oracle database before performing this procedure. After the procedure is completed, start all network components to return them to their previous state.The following components connect to the database: Oracle Monitor, Provisioning Module, SIP Application Module, IP Client Manager, Web Client Manager, and Management Module.

Note 2: The approximate import time, when recovering a database, is 100 MegaBytes of data per hour.

Procedure 41 Restoring an exported Oracle database

On the server hosting the primary database

1 Shut down the primary database as follows:

a Log in as **root**.

b Execute the following commands:

```
cd /etc/init.d
./dbora stop
```

2 Set up a clean database as follows:

a Log in as **oracle**.

b Execute the following commands:

```
cd /export/home/oracle/bin
./restore_empty_db
```

3 Start up the primary database as follows:

a Log in as **root**.

b Execute the following commands:

```
cd /etc/init.d
./dbora start
```

4 Restore the primary database as follows:

a Log in as **oracle** to the server hosting the primary database.

b Execute the following commands:

```
cd /IMS/imssipdb/data/db_schema/backup
./import_imsdb1.sh PRIMARY <name_of_backup>
<media_type>
```

where **name_of_backup** is the name of the backup file and **media_type** can be a DISK or TAPE where the backup is located.

> ***Note:*** If restoring the database from disk, the name_of_backup file must be located within the /backup/orabackup directory.

Resynchronizing (from Primary to Secondary)

The following procedure should be used when the secondary database must be synchronized with the data from the primary database. In this way, the secondary database is updated with the most current data which is resident in the primary database.

Procedure 42 Dropping replication

Drop replication:

1 Log in as **oracle** to the server hosting the primary database.

2 Execute the following commands:

```
cd /IMS/imssipdb/data/db_schema/util
./remove_replication.sh
```

Procedure 43 Deploying database to secondary database server

Deploy database to the secondary database server:

1 Log in as **nortel** to the management server

2 Execute the following commands:

dbdeploy.pl

3 When prompted about replication, type **N**

4 When prompted for the type of deployment, select **Install files only**

5 When prompted for the primary database, provide the IP address of the secondary database.

Procedure 44 Preparing to replicate the database

Prepare to replicate the database:

1 Log in as **oracle** to the server hosting the primary database.

2 Execute the following commands:

cd /export/home/oracle/bin/upgrade/logs

pwd (verify that path displayed is the same as path listed in above **cd** command)

rm *

cd /export/home/oracle/bin/upgrade

./prepare_replication.sh

3 If the message “ERROR at line 1:ORA-00955: name is already used by an existing obect”, execute the following:

a Log in to the secondary database as **oracle**

b Execute the following commands:

cd /export/home/oracle/bin

./restore_empty_db

c Restart this procedure.

4 When prompted to restart the database, type **Y**.

Procedure 45 Backing up the primary database

Perform a backup of the primary database. During the backup process, copy data transactions that occur to the secondary database. Once the backup is complete, start queueing these data transactions to the primary database:

1. Log in as **oracle** to the server hosting the primary database.
2. Execute the following commands:

   cd /export/home/oracle/bin/upgrade

   ./add_secondary_db.sh

Procedure 46 Setting up replication

Setup replication:

1. Log in as **oracle** to the server hosting the secondary database.
2. Execute the following commands:

   cd /export/home/oracle/bin/upgrade

   ./activate_secondary_db.sh <primary_DB_hostname>

   > ***Note:*** The activate_secondary_db.sh script uses Secure FTP to transfer the backup (taken above) from the primary database to the secondary database. If this is the first time Secure FTP has been used on this server, the administrator will be prompted to confirm the authenticity of the host with the following question: The authenticity of host … can't be established. RSA key fingerprint … Are you sure you want to continue connecting (yes/no)? Type **yes** in response.

   When prompted for the "`oracle@<hostname> password`", enter the oracle password for the primary database.

   When prompted to restart the database, type **Y**.

Procedure 47 Turning off archiving logs on primary database

Turn off archiving logs on primary database:

1. Log in as **oracle** to the server hosting the primary database.
2. Execute the following commands:

   cd /export/home/oracle/bin

   ./archivallogctl off

   When prompted to restart the database, type **Y**.

Procedure 48 Cleaning up the primary and secondary databases

Clean up the primary and secondary databases:

1. Log in as **oracle** to the server hosting the primary database.
2. Execute the following commands:

   cd /export/home/oracle/bin/upgrade

   ./clean.sh
3. Repeat this procedure on the server hosting the secondary database.

Procedure 49 Reconfiguring the database SNMP agent

Re-configure the database SNMP agent:

1. Log in as **root** to the server hosting the secondary database.
2. Execute the following commands:

   cd /export/home/oracle/bin

   ./config_snmp

Procedure 50 Undeploy database from secondary database server

Undeploy the database from the secondary database server:

1. Log in as **nortel** to the server hosting the secondary database.
2. Execute the following commands:

   dsmundeploy -load <DB_load> -node <secondary_DB_IP>

Resynchronizing (from Secondary to Primary)

The following procedure should be used when the primary database must be synchronized with the data from the secondary database. In this way, the primary database is updated with the most current data which is resident in the secondary database.

Procedure 51 Dropping replication

Drop replication:

1. Log in as **oracle** to the server hosting the primary database.
2. Execute the following commands:

   cd /IMS/imssipdb/data/db_schema/util

   ./**remove_replication.sh**

Procedure 52 Deploying database to the secondary database server

Deploy database to the secondary database server:

1 Log in as **nortel** to the management server.

2 Execute the following commands:

```
dbdeploy.pl
```

When prompted about replication, type **N**.

When prompted for type of deployment, select **Install Files only.**

When prompted for the primary database, provide the IP address of the secondary database.

Procedure 53 Preparing to replicate the database

Prepare to replicate the database:

1 Log in as **oracle** to the server hosting the secondary database.

2 Execute the following commands:

```
cd /export/home/oracle/bin/upgrade/logs
```

pwd (verify that path displayed is the same as path listed in above **cd** command)

```
rm *
cd /export/home/oracle/bin/upgrade
./prepare_replication_at_secondary.sh
```

When prompted to restart the database, type **Y**.

Procedure 54 Performing a backup of the secondary database

Perform a backup of the secondary database:

1 Log in as **oracle** to the server hosting the secondary database.

2 Execute the following commands:

```
cd /export/home/oracle/bin/upgrade
./add_primary_db.sh
```

Procedure 55 Setting up replication

Setup replication:

1 Log in as **oracle** to the server hosting the primary database.

2 Execute the following commands:

cd /export/home/oracle/bin/upgrade

./activate_primary_db.sh <secondary_DB_hostname>

> ***Note:*** The activate_primary_db.sh script uses Secure FTP to transfer the backup (taken above) from the secondary database to the primary database. If this is the first time Secure FTP has been used on this server, the administrator will be prompted to confirm the authenticity of the host with the following question: The authenticity of host … can't be established. RSA key fingerprint … Are you sure you want to continue connecting (yes/no)? Type **yes** in response.

When prompted for the "`oracle@<hostname> password`", enter the oracle password for the secondary database.

When prompted to restart the database, type **Y**.

Procedure 56 Turning off archiving logs on secondary database

Turn off archiving logs on secondary database:

1. Log in as **oracle** to the server hosting the secondary database.
2. Execute the following commands:

   cd /export/home/oracle/bin

   ./archivallogctl off

   When prompted to restart the database, type **Y**.

Procedure 57 Cleaning up the primary and secondary databases

Clean up the primary and secondary databases:

1. Log in as **oracle** to the server hosting the primary database.
2. Execute the following commands:

   cd /export/home/oracle/bin/upgrade

   ./clean.sh
3. Repeat this procedure on the server hosting the secondary database.

Procedure 58 Reconfiguring the database SNMP agent

Re-configure the database SNMP agent:

1. Log in as **root** to the server hosting the primary database.
2. Execute the following commands:

   cd /export/home/oracle/bin

```
./config_snmp
```

Procedure 59 Undeploying database from secondary database server

Undeploy database from secondary database server:

1 Log in as **nortel** to the server hosting the secondary database.

2 Execute the following command:

```
dsmundeploy -load <DB_load> -node <secondary_DB_IP>
```

Recovery for Sun Fire v100 server

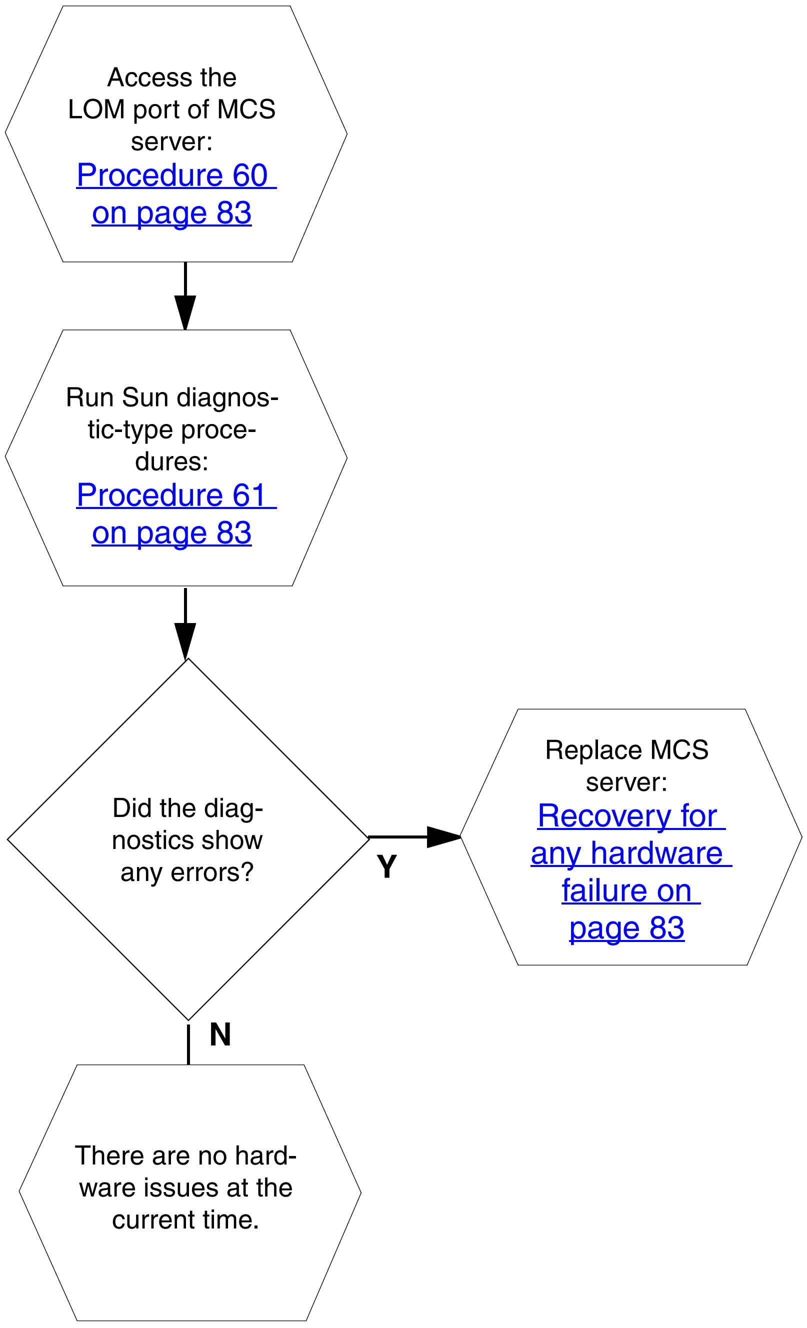
This chapter is organized as follows:

Determining existence of hardware problems

The first step is to determine if or where a failure has occurred. Figure 19, Flow for determining existence of a hardware problem, on page 82 walks through the steps required to determine the existence of any hardware failures on an MCS server using the Sun Fire v100 platform.

Should both servers running redundant databases fail, these steps must be repeated for both servers with the primary database being restored first.

Figure 19 Flow for determining existence of a hardware problem


Access the LOM port of MCS server: Procedure 60 on page 83
Run Sun diagnostic-type procedures: Procedure 61 on page 83
Did the diagnostics show any errors?
Y
Replace MCS server: Recovery for any hardware failure on page 83
N
There are no hardware issues at the current time.

Procedure 60 Access Terminal Server

At the administrator workstation

1 Open a PuTTY telnet session to the MCS server using the IP Address of the terminal server for the problematic server and the port number to connect to the console.

2 When prompted to login, login and then type the following: **init 0**

Procedure 61 Run Sun diagnostic-type procedures

From the telnet session

1 Execute the diagnostic procedures as described in the *Sun Fire v100 Administrative Guide*. Execute any actions suggested within the procedure.

Recovery for any hardware failure

In the event of any hardware failure, a new server is required and a restore of a previous backup of the MCS server must be performed. Figure 20 on page 84 through Figure 25 on page 89 provide the steps required to recover from this type of failure scenario.

Figure 20 Flow for recovering after a multiple disk failure

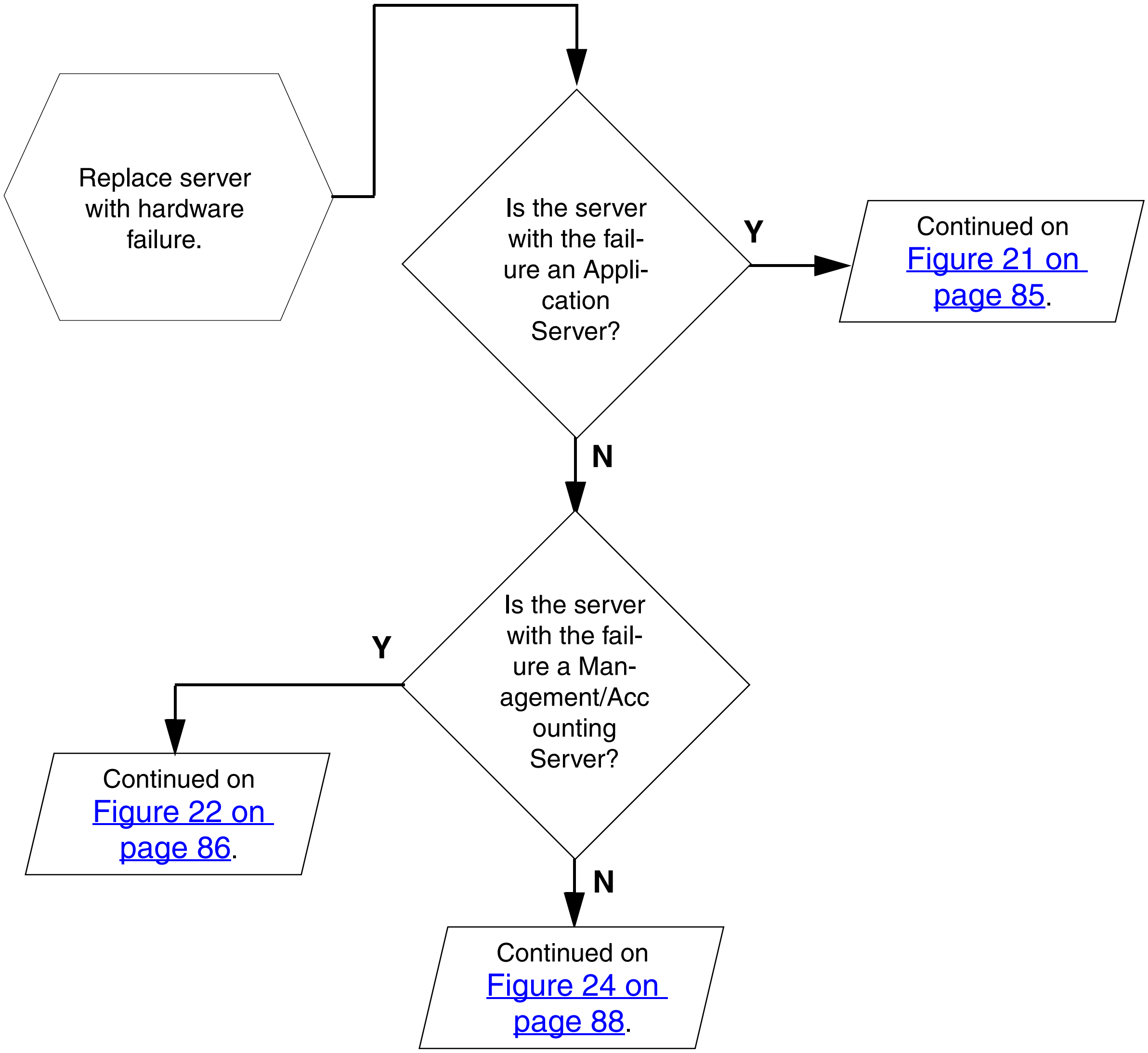

Replace server with hardware failure.
Is the server with the failure an Application Server?
Y
Continued on Figure 21 on page 85.
N
Is the server with the failure a Management/Accounting Server?
Y
Continued on Figure 22 on page 86.
N
Continued on Figure 24 on page 88.

Figure 21 Flow for recovering an Application server after a multiple disk failure

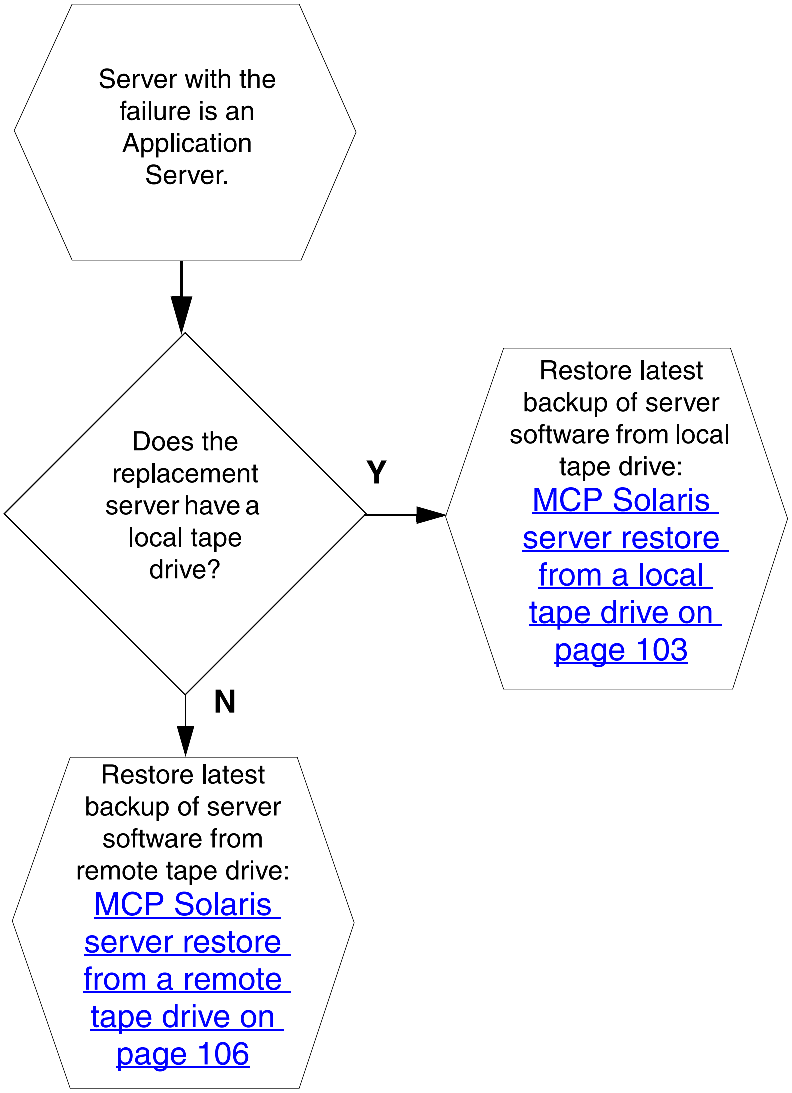

Server with the failure is an Application Server.
Does the replacement server have a local tape drive?
Y
Restore latest backup of server software from local tape drive: MCP Solaris server restore from a local tape drive on page 103
N
Restore latest backup of server software from remote tape drive: MCP Solaris server restore from a remote tape drive on page 106

Figure 22 Flow for recovering a Management/Accounting server after a multiple disk failure

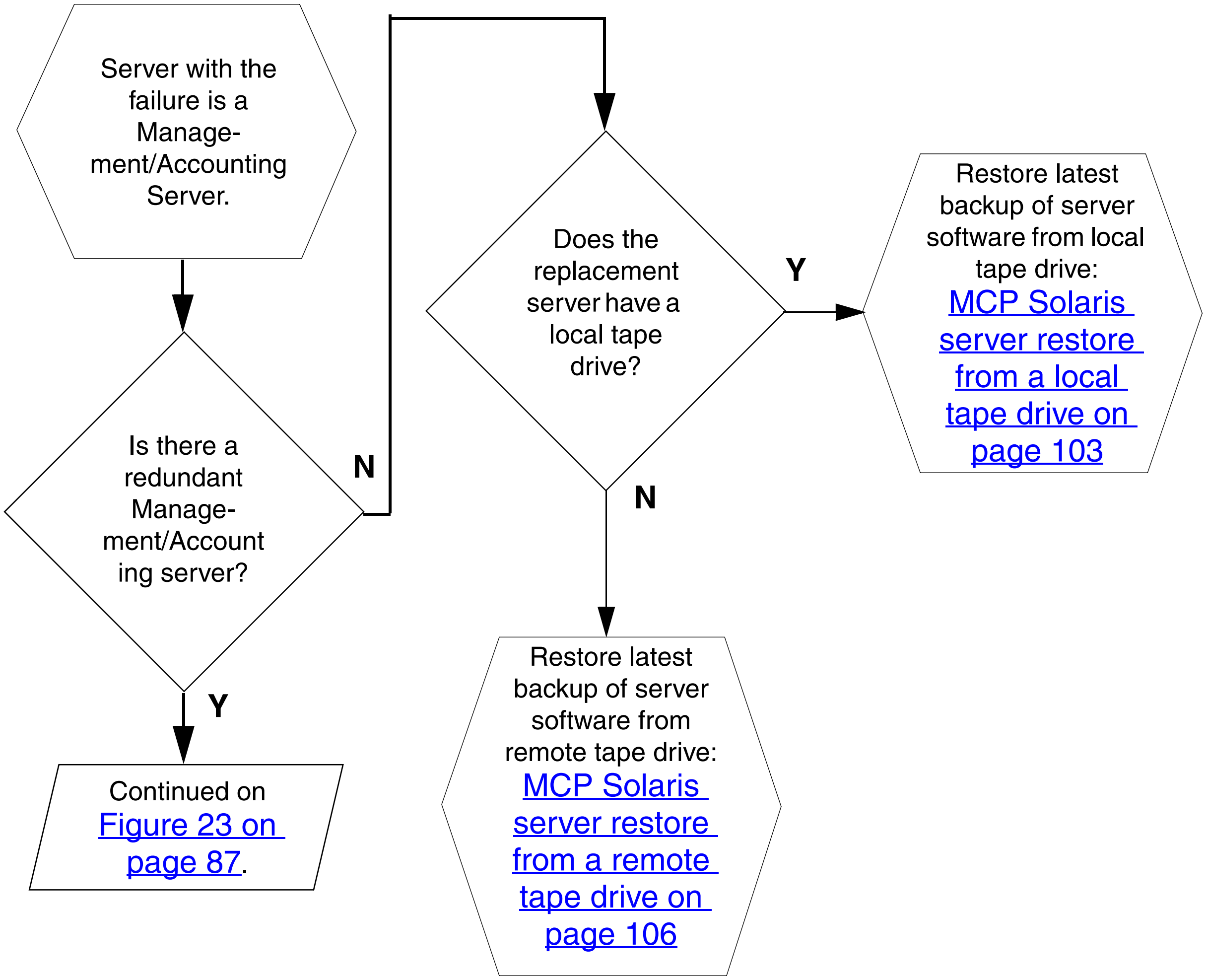

Server with the failure is a Management/Accounting Server.
Is there a redundant Management/Accounting server?
N
Y
Continued on Figure 23 on page 87.
Does the replacement server have a local tape drive?
Y
N
Restore latest backup of server software from local tape drive: MCP Solaris server restore from a local tape drive on page 103
Restore latest backup of server software from remote tape drive: MCP Solaris server restore from a remote tape drive on page 106

Figure 23 Flow for recovering a redundant Management/Accounting server after a multiple disk failure

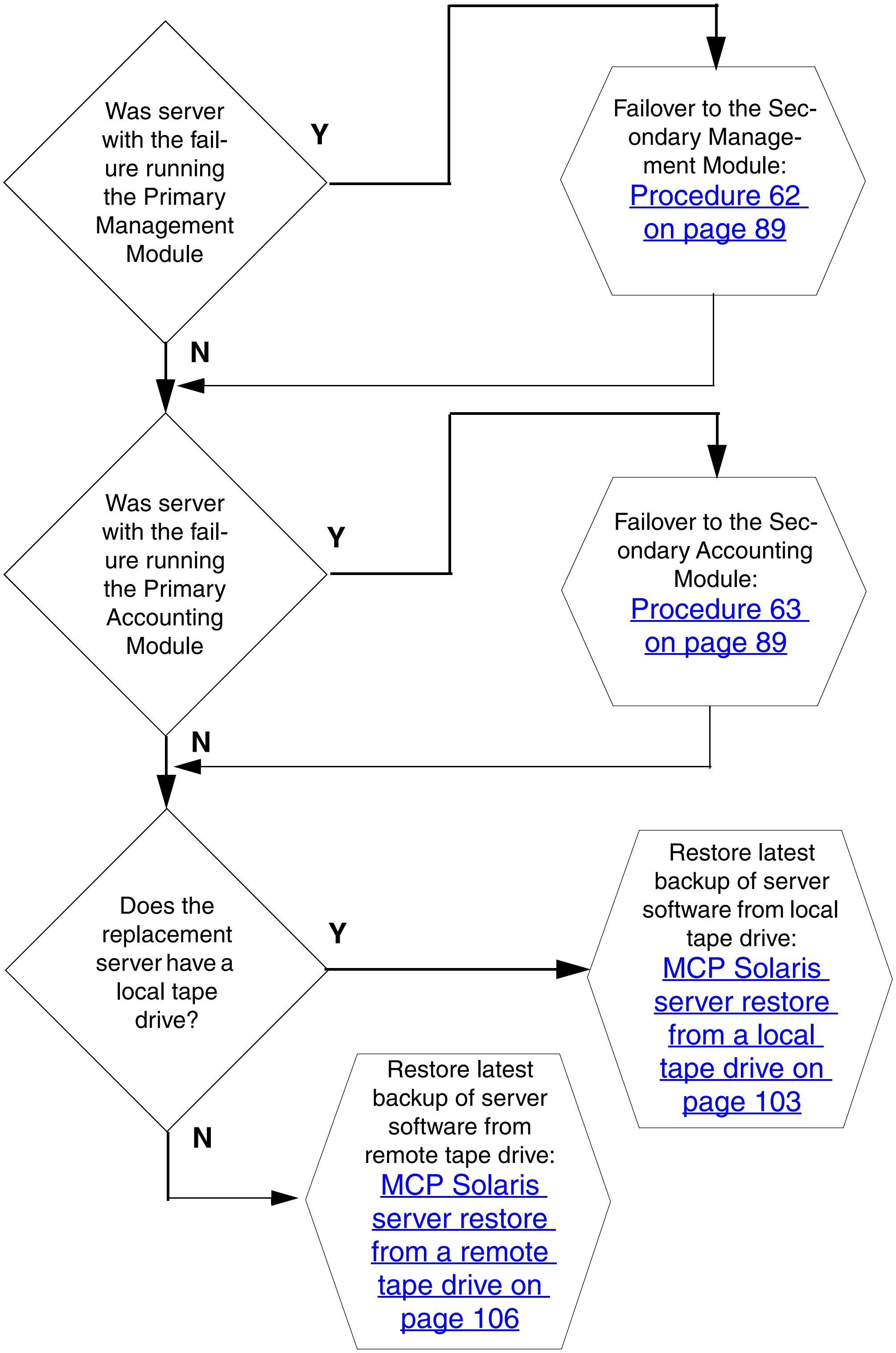

Was server with the failure running the Primary Management Module
Y
N
Failover to the Secondary Management Module: Procedure 62 on page 89
Was server with the failure running the Primary Accounting Module
Y
N
Failover to the Secondary Accounting Module: Procedure 63 on page 89
Does the replacement server have a local tape drive?
Y
N
Restore latest backup of server software from local tape drive: MCP Solaris server restore from a local tape drive on page 103
Restore latest backup of server software from remote tape drive: MCP Solaris server restore from a remote tape drive on page 106

Figure 24 Flow for recovering a Database server after a multiple disk failure

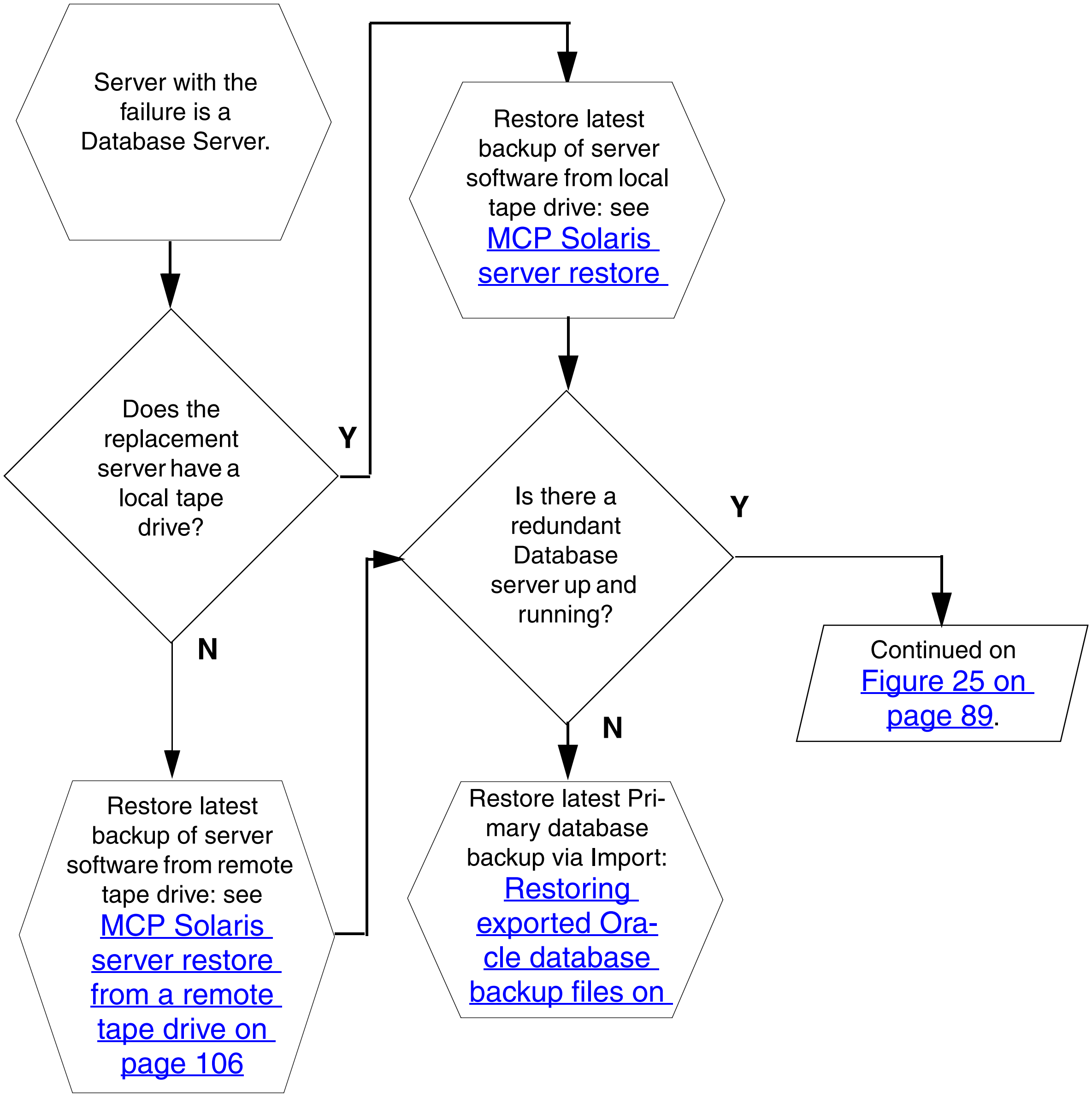
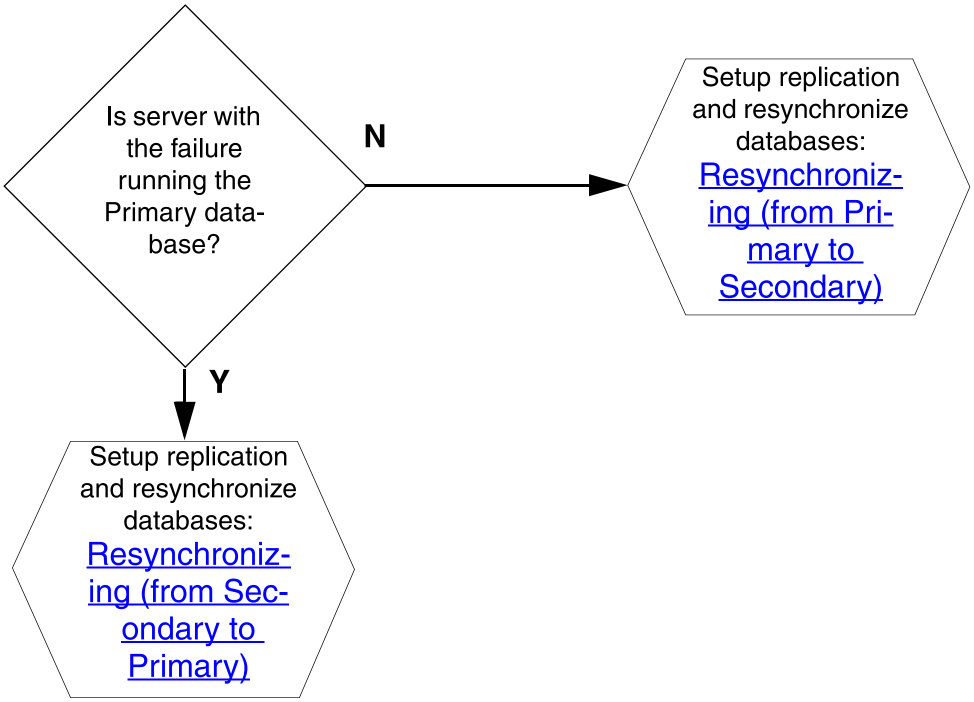

Server with the failure is a Database Server.
Does the replacement server have a local tape drive?
Y
N
Restore latest backup of server software from local tape drive: see MCP Solaris server restore
Is there a redundant Database server up and running?
Y
N
Continued on Figure 25 on page 89.
Restore latest backup of server software from remote tape drive: see MCP Solaris server restore from a remote tape drive on page 106
Restore latest Primary database backup via Import: Restoring exported Oracle database backup files on

Figure 25 Flow for recovering a redundant Oracle database after a multiple disk failure


Is server with the failure running the Primary database?
N
Setup replication and resynchronize databases: Resynchronizing (from Primary to Secondary)
Y
Setup replication and resynchronize databases: Resynchronizing (from Secondary to Primary)

Procedure 62 Starting the cold standby Management Module instance

from the administrator's workstation

1 Log onto the server hosting the secondary SysMgr component.

IP Address: <physical address of server>

Login ID: **sysadmin**

2 Navigate to the directory with the failover script.

```
cd /IMS/mgmtsvr/bin
```

3 Execute the failover startup script to start SysMgr processes and take ownership of the logical IP address.

```
sudo Failover.pl start sysmgr
```

When the startup is finished, the screen will display the name and path of the log file associated with this event.

Procedure 63 Starting the cold standby Accounting Module

instance

From the administrator workstation

1 Establish a remote login session to the server hosting the cold standby Accounting Module. Log in as **sysadmin**.

2 type: **cd /IMS/acctmgr/bin**

3 Use the sudo command to execute the Failover script using the following syntax:

type: **sudo Failover.pl start acctmgr**

The process will be stopped, the logical IP will be assigned for this machine and the Accounting Module process restarted.

Restoring exported Oracle database backup files

> **CAUTION**
>
> Only trained personnel should perform the following task.

Use the following procedure to restore files created using the Export/Import backup method:

> ***Note 1:*** Stop all network components that connect to the Oracle database before performing this procedure. After the procedure is completed, start all network components to return them to their previous state.The following components connect to the database: Oracle Monitor, Provisioning Module, SIP Application Module, IP Client Manager, Web Client Manager, and Management Module.
>
> ***Note 2:*** The approximate import time, when recovering a database, is 100 MegaBytes of data per hour.

Procedure 64 Restoring an exported Oracle database

On the server hosting the primary database

1 Shut down the primary database as follows:

a Log in as **root**.

b Execute the following commands:

```
cd /etc/init.d
./dbora stop
```

2 Set up a clean database as follows:

a Log in as **oracle**.

b Execute the following commands:

```
cd /export/home/oracle/bin
./restore_empty_db
```

3 Start up the primary database as follows:

a Log in as **root**.

b Execute the following commands:

```
cd /etc/init.d
./dbora start
```

4 Restore the primary database as follows:

a Log in as **oracle** to the server hosting the primary database.

b Execute the following commands:

```
cd /IMS/imssipdb/data/db_schema/backup
./import_imsdb1.sh PRIMARY <name_of_backup>
<media_type>
```

where **name_of_backup** is the name of the backup file and **media_type** can be a DISK or TAPE where the backup is located.

> ***Note:*** If restoring the database from disk, the name_of_backup file must be located within the /backup/orabackup directory.

Resynchronizing (from Primary to Secondary)

The following procedure should be used when the secondary database must be synchronized with the data from the primary database. In this way, the secondary database is updated with the most current data which is resident in the primary database.

Procedure 65 Resynchronizing (from Primary to Secondary)

Drop replication:

1 Log in as **oracle** to the server hosting the primary database.

2 Execute the following commands:

```
cd /IMS/imssipdb/data/db_schema/util
./remove_replication.sh
```

Deploying the database to the secondary database server

Deploy the database to the secondary database server:

1 Log in as **nortel** to the management server.

2 Execute the following command:

dbdeploy.pl

3 When prompted about replication, type **N**

4 When prompted for type of deployment, select **Install Files only**

5 When prompted for the primary database, provide the IP address of the secondary database.

Prepare to replicate the database:

1 Log in as **oracle** to the server hosting the primary database.

2 Execute the following commands:

cd /export/home/oracle/bin/upgrade/logs

pwd (verify that path displayed is the same as path listed in above **cd** command)

rm *

cd /export/home/oracle/bin/upgrade

./prepare_replication.sh

3 If the message "ERROR at line 1:ORA-00955: name is already used by an existing object", then perform the following steps:

a Log on to the secondary database as **oracle**.

b Execute the following commands:

cd /export/home/oracle/bin

./restore_empty_db

c Restart this procedure

When prompted to restart the database, type **Y**.

Perform a backup of the primary database.

During the backup process, copy data transactions that occur to the secondary database. Once the backup is complete, start queueing these data transactions to the primary database:

4 Log in as **oracle** to the server hosting the primary database.

5 Execute the following commands:

```
cd /export/home/oracle/bin/upgrade
./add_secondary_db.sh
```

Setup replication:

1 Log in as **oracle** to the server hosting the secondary database.

2 Execute the following commands:

```
cd /export/home/oracle/bin/upgrade
./activate_secondary_db.sh <primary_DB_hostname>
```

> ***Note:*** The activate_secondary_db.sh script uses Secure FTP to transfer the backup (taken above) from the primary database to the secondary database. If this is the first time Secure FTP has been used on this server, the administrator will be prompted to confirm the authenticity of the host with the following question: The authenticity of host … can't be established. RSA key fingerprint … Are you sure you want to continue connecting (yes/no)? Type **yes** in response.

When prompted for the "`oracle@<hostname> password`", enter the oracle password for the primary database

When prompted to restart the database, type **Y**.

Turn off archiving logs on primary database:

1 Log in as **oracle** to the server hosting the primary database.

2 Execute the following commands:

```
cd /export/home/oracle/bin
./archivallogctl off
```

When prompted to restart the database, type **Y**.

Clean up the primary and secondary databases:

1 Log in as **oracle** to the server hosting the primary database.

2 Execute the following commands:

```
cd /export/home/oracle/bin/upgrade
./clean.sh
```

3 Repeat this procedure on the server hosting the secondary database.

Re-configure the database SNMP agent:

1 Log in as **root** to the server hosting the secondary database.

2 Execute the following commands:

cd /export/home/oracle/bin

./config_snmp

Undeploy database from secondary database server:

1 Log in as **nortel** to the server hosting the secondary database.

Execute the following command:

dsmundeploy -load <DB_load> -node <secondary_DB_IP>

Resynchronizing (from Secondary to Primary)

The following procedure should be used when the primary database must be synchronized with the data from the secondary database. In this way, the primary database is updated with the most current data which is resident in the secondary database.

Procedure 66 Resynchronizing (from Secondary to Primary)

Drop replication:

1 Log in as **oracle** to the server hosting the primary database.

2 Execute the following commands:

cd /IMS/imssipdb/data/db_schema/util

./remove_replication.sh

Deploy database to the secondary database server:

1 Log in as **nortel** to the management server.

2 Execute the following commands:

dbdeploy.pl

When prompted about replication, type **N**

When prompted for type of deployment, select **Install Files only**

When prompted for the primary database, provide the IP address of the secondary database.

Prepare to replicate the database:

1 Log in as **oracle** to the server hosting the secondary database.

2 Execute the following commands:

cd /export/home/oracle/bin/upgrade/logs

pwd (verify that path displayed is the same as path listed in above **cd** command)

rm *

cd /export/home/oracle/bin/upgrade

./prepare_replication_at_secondary.sh

When prompted to restart the database, type **Y**.

Perform a backup of the secondary database:

1 Log in as **oracle** to the server hosting the secondary database.

2 Execute the following commands:

cd /export/home/oracle/bin/upgrade

./add_primary_db.sh

Setup replication:

1 Log in as **oracle** to the server hosting the primary database.

2 Execute the following commands:

cd /export/home/oracle/bin/upgrade

./activate_primary_db.sh <secondary_DB_hostname>

> ***Note:*** The activate_primary_db.sh script uses Secure FTP to transfer the backup (taken above) from the secondary database to the primary database. If this is the first time Secure FTP has been used on this server, the administrator will be prompted to confirm the authenticity of the host with the following question: The authenticity of host ... can't be established. RSA key fingerprint ... Are you sure you want to continue connecting (yes/no)? Type **yes** in response.

When prompted for the "`oracle@<hostname> password`", enter the oracle password for the secondary database

When prompted to restart the database, type **Y**.

Turn off archiving logs on secondary database:

1 Log in as **oracle** to the server hosting the secondary database.

2 Execute the following commands:

cd /export/home/oracle/bin

./archivallogctl off

When prompted to restart the database, type **Y**.

Clean up the primary and secondary databases:

1 Log in as **oracle** to the server hosting the primary database.

2 Execute the following commands:

```
cd /export/home/oracle/bin/upgrade
./clean.sh
```

3 Repeat this procedure on the server hosting the secondary database.

Re-configure the database SNMP agent:

1 Log in as **root** to the server hosting the primary database.

2 Execute the following commands:

```
cd /export/home/oracle/bin
./config_snmp
```

Undeploy database from secondary database server:

1 Log in as **nortel** to the server hosting the secondary database.

2 Execute the following commands:

```
dsmundeploy -load <DB_load> -node <secondary_DB_IP>
```

Restore of MCP Solaris servers

This chapter describes the procedures required to restore a Solaris server, regardless of the Sun server model. This chapter is organized as follows:

- MCP Solaris server restore overview
- Before you begin
- Required server access
- MCP Solaris server restore from a local tape drive
- MCP Solaris server restore from a remote tape drive

MCP Solaris server restore overview

Restore procedures for the Sun Solaris nodes are similar across the platform. They all involve tape transactions, to a local or remote tape drive, depending on the server.

There are two separate procedures used to restore MCP Solaris servers: one is used when the tape device resides on the server being backed up, and the other when is used for a remote host. The list of partitions that are backed up varies based on server type. The time required to complete the operation can vary depending on these and other factors.

If the system being restored is a database server (or a dbcombo), refer to the appropriate section below depending on the configuration:

- For Sun Netra t140x platform, refer to Restoring exported Oracle database backup files on page 51.
- For Sun Netra 240 platform, refer to Restoring exported Oracle database backup files on page 72.
- Sun Fire v100 platform, refer to Restoring exported Oracle database backup files on page 90.

If the server being restored has a Provisioning Module installed, the Provisioning Module must be restarted after the restore to clear an alarm that is raised by the iPlanet Monitor component. See the *MCS System Management Console User Guide (NN10273-111)* for information on restarting a component.

Restrictions and limitations

The restore of MCP Solaris servers has the following restrictions and limitations:

- Only DDS4 and USB tape drives are supported for restore operations.

  Follow the manufacturer's recommendations for tape and tape drive use.
- The restore script does not include the contents of the Oracle database.
- Although the backup process implemented by this feature includes logs and OMs, that data will normally be out of date and of limited value. Therefore it is not included in the restore process.
- Logs and alarms cannot be generated by the restore operations performed from the Command Line Interface (CLI).
- Does not contain billing information.
- Restore operations for Sun Fire V100 and Netra 240 servers will always be done across the network because those servers cannot access the USB port when booted from CD.
- The restore operation will fail if the new drives are a different size or model from the old drives that were backed up.
- Information stored off for a particular server, is specific to that server. So, for example, you cannot use a backup of a primary DB to restore a secondary DB.

Restore log files

The script used for the restore operation (**mcp_recover.pl**) generates a log file with every execution. Review this log file after every restore to ensure the restore was successful. The log file is stored in the local directory:

```
/export/home/sysadmin/bkup_restore
```

The filename is:

```
mcp_recover.pl.log.<dayTimeStamp>
```

Where
`<dayTimeStamp>` is YYYY_MM_DD_HH:MM:SS. For example:
`mcp_recover.pl.log.2004_03_05_21:49:50`

Please note that based on the configuration of the time zone on the server, the timestamps written to the log file may have an ”offset” from the time shown on the server once the restore is completed (e.g. the restore has completed and the server has been rebooted). This “difference/offset” is caused when the default time zone from the SUN Install CD1 does not match the configured time zone on the server when it was backed up.

During the restore operation of a MCP Solaris Server, if the data being restored is larger than what one tape can accommodate, the user will be prompted to enter the next tape at the appropriate time. Below is an example of the output displayed when additional tapes are required during a restore:

extract file
./me/pool9/Files/B/UAS06.zip.bLfCbwYvd5YvveYtkOYinAZgoLi

Mount volume 2
then enter `volume name (default: /dev/rmt/0cn)`

Before you begin

Before you begin the restore of a MCP Solaris server, review the following:

- Requirements for MCP Solaris server restores
- Utilization of a USB tape drive
- Required setup of an MCP server acting as a remote host

Requirements for MCP Solaris server restores

The following are a list of actions or requirements that need to be fulfilled prior to performing a restore operation

- DDS4 tape drive

  For USB Tape drives, the recommended tape drive is the Seagate Travan 40 USB 2.0 20/40 GB tape drive with the media tape model STTM40.

  Tape drive can be local or remote for T140x restores. Only the Database and Management/Accounting servers have a local tape drive in the T140x platform. V100 and N240 restores require a remote tape drive. Tape drive does not have to be within MCP network but must be attached to a Solaris machine that is visible to the server doing restore operations.

- DDS4 tape in tape drive. For USB drives this will be a 20 GB tape, for SCSI drives it will be a 12 GB tape.

  This requires physical access to the tape drive.
- Live 100Mbps Ethernet Connection for remote restore.
- IP address of tape server if using a remote tape drive.
- Sun Solaris Installation CD-ROM in CD-ROM drive.

  This requires physical access to the both the CD and CD drive.
- Server address information.
- List of all accounts and passwords.
- For restore of an Netra 240 server, physical access to the server's serial port is required, if no terminal server is available

Utilization of a USB tape drive

Add a tape drive

If using a USB Tape Drive for the backup, perform the following steps when connecting a USB tape drive to the server:

1 Login as **root** on the server the tape drive is being connected to and enter the following command:

```
/etc/init.d/volmgt stop
```

2 Connect the USB Tape Drive to port 0.

3 Enter the following command:

```
/etc/init.d/volmgt start
```

4 Turn on the Tape Drive and insert a tape.

Remove a tape drive

If using a USB Tape Drive for the backup, perform the following steps when disconnecting a USB tape drive to the server:

1 Login as **root** on the server where the tape drive is being removed, and enter the following command:

```
/etc/init.d/volmgt stop
```

2 Remove the USB Tape Drive.

Required setup of an MCP server acting as a remote host

The following commands are required to setup access to a remote MCP server with a tape drive acting as the remote host.

If the remote tape drive is NOT on an MCP server, then the steps below can be ignored. However, you must ensure that remote shell operations are enabled (from the server to be backed up) on the remote tape drive server.

1 Ensure the MCP server being restored has proper access to the MCP server with the tape drive (remote host).

2 Login to the MCP server with the tape drive (remote host) as **sysadmin**.

```
sysadmin
```

3 Execute the following script on the remote host:

```
sudo /usr/local/bin/mcp_enable_remote_sh.pl
<MCP_Server_IP>
```

Where
<MCP_Server_IP> is the IP address of the server being restored.

The above script enables the execution of remote shell commands from the MCP server being restored.

4 Log off as **sysadmin**.

exit

5 Login to the MCP server being restored as **root**.

6 Verify access to the tape server has been setup correctly, execute the command from the server being restored:

```
rsh  -l  sysadmin  <Tape_Server_IP>  df -k
```

Where
<Tape_Server_IP> is the IP of the remote host with the tape drive.

If you see the output of the **df –k** command, then the target system is setup for the restore procedure. If not, contact your next level of support.

7 After the restore procedure has completed, logon to the remote host as **sysadmin** and execute the following command:

```
sudo /usr/local/bin/mcp_disable_remote_sh.pl
```

This command disables ability to execute remote shell commands.

Required server access

During a system restore, the server's operating system is executing in a limited capacity. Access to each given server type must be obtained in the following manner:

V100 – LOM port

T140x - Console port

N240 – Serial port

In addition, when a terminal server is connected to a T140x or a V100, a telnet session through the terminal server to the T140x serial console interface or V100 LOM interface can be used.

If a restore is being performed on a new server, it is important that the server come up to the menu selection before sending a **break** to the system – which gets the user to the **ok** prompt. To verify the server has initialized correctly, after the **boot cdrom –s** command has finished execution, the user should be in the **/tmp/root** directory. Execute the **pwd** system command to ensure this is true.

Login to the NetMgmt of the 240

The procedure to log into the NetMgmt of a Sun Netra 240 server is described below.

1 Telnet to the NetMgmt IP. This is a regular, not secure telnet.

2 Login as **admin**.

user name: **admin**
admin password: **<admin_pswd>**

Where
<admin_pswd> is the admin password set during the N 240 server installation.

A successful login gets you to the sc prompt.

3 Enter the following at the sc prompt.

```
console -f
```

This brings up console login prompt.

4 Login as either as **sysadmin**, **root**, or **oracle** depending on the procedures being performed.

5 When finished and ready to exit the console session, you MUST enter a "**#.**" to return back to the sc prompt. If you Failure to type "**#.**" that will lock up the console port.

```
"#."
```

You will return to the **sc** prompt.

MCP Solaris server restore from a local tape drive

Use this procedure to restore an MCP server from a local tape drive. For deployments with Netra t140x, this procedure is only applicable for the servers hosting the Database and Management/Accounting components.

1 Select the proper DDS4 tape. This tape should be the most recent backup tape for this server.

2 Insert the tape into the tape drive of the server being restored.

3 Verify the server is at the ok prompt.

```
ok
```

If not, then login as root and get the server to the ok prompt.

4 Insert the Sun Solaris Install CD 1 into the CD-ROM drive.

5 From the console window – at the **ok** prompt type:

```
setenv auto-boot? false
boot -r
setenv auto-boot? true
```

6 Type the following at the **ok** prompt.

```
boot cdrom -s
```

This operation will boot the server into single user mode. When this command completes, ensure you are in the **/tmp/root** directory.

7 Acquire the recovery data, which resides in the first file set on the backup tape.

a Ensure the Tape has been rewound by executing the following command:

```
mt -f /dev/rmt/0cn rewind
```

b Enter the following:

```
ufsrestore rvfs /dev/rmt/0cn 1
```

This begins retrieving the recovery file set, using the local tape drive for restoration.

c If the **ufsrestore** program asks for permission to owner/mode permissions, type **n** and press **Enter**.

d "not found on volume" messages may display. This is a normal condition when performing a system restore and does not indicate an error.

e The **ufsrestore** program creates the following directory which contains the recovery data and scripts:

```
mcp_recov
```

f The **ufsrestore** program exits.

8 Run the recovery script.

```
mcp_recov/mcp_recover.pl
```

The data will be restored from the local tape drive. The restore operation time will vary depending on the type of MCP server and the amount of data being restored.

9 The recovery script reads the Meta-data from the tape backup and displays the information below to the user. The user is then prompted to confirm this is the correct tape to perform the restore with. If the tape is the correct one, press **Enter** to continue with the restore.

Date => date backup was performed

SvrType => "Mgmt/Acct/DB Combo", "App Server", "DB Server", or "Mgmt/Acct Server"

Platform => "V100", "1400", "1405", or "Netra 240"

VolMgr => "DiskSuite" or "Veritas"

Hostname => hostname of server that was backed up

IP Address => IP address associated with the hostname of the server that was backed up

10 The script will prompt the user with the question

```
Is the system being restored a new system, or a
restore of an existing system? Answer Y, if this
is a new system and thus a new Veritas license
key will be required.  (Y/N)?"
```

If the system being restored is the original server being restored, (i.e. the original system/CPU that was backed up) answer **N**. If the system being restore is a different system (i.e. not the original system/CPU backup), answer **Y**.

11 Remove the CD from the CD-ROM drive.

12 The recovery script will now format the disks and restore the file systems.

13 Once the restore of the file systems completes, the script will prompt you to reboot the machine.

Follow the instructions that are displayed to the screen for the reboot process.

14 When you select **Y** to the reboot, it takes you to the **ok** prompt where you need to type **boot disk -r** to boot from the disk.

15 If you answered **no** in the step 10, proceed to step 17. Otherwise, the system will prompt you to enter a valid Veritas License Key. The license key entered must be keyed to the CPU/system being restored. The Veritas License Key must be the correct license key, otherwise Veritas installation will fail, resulting in a restore failure.

16 The recovery process now runs through the installation of the Veritas Volume Manager. Note this process is lengthy, however, it is fully automated and requires no operator intervention.

17 The recovery process now runs through the steps involved in setting up the metadevices, mirroring the disk, and restoring additional partitions. Eventually the system comes up and the system will take you back to the login prompt. Note this stage of the restore is a lengthy process.

18 The restore procedure should be completed at this point.

19 Review the log file which is generated by the recover script, to ensure the restore was successful. The log file is stored in the directory:

```
/export/home/sysadmin/bkup_restore
```

Note that for the restore of a database server there will be two log files in this directory, because the restore is a two-step process with the restore script being executed at two different points in time.

20 Logoff from the server.

21 Verify the correct load for the MCP components has been restored. See the procedure Verify and restore correct load for the MCP components for more information.

22 Press the eject button on tape drive, retrieve tape, and store the tape in safe, dry place.

23 If the server hosted the Oracle Database, it will now have to be restored.

If the server hosted the Provisioning Module, the Provisioning Module must now be restarted. See the *System Management Console User Guide (NN10273-111)* for information on restarting a component.

MCP Solaris server restore from a remote tape drive

Use this procedure to restore an MCP server from a remote tape drive.

1 Select the proper DDS4 tape. This tape should be the most recent backup tape for this server.

2 Insert the tape into the tape drive of the selected tape host server.

3 On tape server host type the following command:

```
mt -f /dev/rmt/0cn rewind
```

4 Verify the server being restored is at the ok prompt.

If not, then login as root and get the server to the ok prompt.

5 Insert the Sun Solaris Install CD1 into the CD-ROM drive of the server being restored.

6 From the console window – at the ok prompt enter

```
setenv auto-boot? false
```

```
boot -r
```

```
setenv auto-boot? true
```

7 At the ok prompt enter

```
boot cdrom -s
```

This operation will boot the server into single user mode. When this command completes, ensure you are in the directory

`/tmp/root directory.`

8 To configure the network interface:

a Determine network interface accessible to tape host. Use the physical IP address for the restore process, because it is the only interface enabled.

b Enter the following to activate the interface

```
ifconfig <tape_if> <ipaddr> netmask <netmask>
broadcast <broadcast> up
```

Where
`<tape_if>` is the name of the primary network interface in

the IPMP group. The interfaces defined for each given server type are:
V100 = dmefe0
Netra 240 = bge0
Netra T140x = qfe2
`<ipaddr>` is the physical IP address for the **<tape_if>**
`<netmask>` is the network mask for the corresponding network
`<broadcast>` is the broadcast address for that subnet

c If the server being restored and the server containing the tape drive are not on the same subnet, enter the following to add the default route

```
route add default <gateway>
```

Where
`<gateway>` is the IP address of the network gateway for the subnet.

9 Acquire the recovery data, which resides in the first file set on the backup tape.

a Enter the following to retrieve the recovery file set

```
ufsrestore rvfs sysadmin@<Tape_Server_IP>:
/dev/rmt/0cn 1
```

Where
`<Tape_Server_IP>` is the IP address of the selected tape host.

b If the ufsrestore program asks for permission to owner/mode permissions enter n and press Enter.

c A “not found on volume” messages may be displayed. This is a normal condition when performing a system restore and does not indicate an error.

d The ufsrestore program creates the following directory which contains the recovery data and scripts.

```
mcp_recov
```

e The ufsrestore program exits.

10 Enter the following to begin system recovery

```
mcp_recov/mcp_recover.pl <Tape_Server_IP>
```

11 The recovery script reads the Meta-data from the tape backup and displays the information below to the user. The user is then prompted to confirm this is the correct tape to perform the restore with. If the tape is the correct one, press Enter to continue with the restore.

Date => date backup was performed

SvrType => "Mgmt/Acct/DB Combo", "App Server", "DB Server", or "Mgmt/Acct Server"

Platform => "V100", "1400", "1405", or "Netra 240"

VolMgr => “DiskSuite” or “Veritas”

Hostname => hostname of server that was backed up

IP Address => IP address associated with the hostname of the server that was backed up

12 If the MCP server being restored is not a T140x Database server or a T140x Management/Accounting server, proceed to step 13. Otherwise, the script will prompt the user with the question

```
Is the system being restored a new system, or a
restore of an existing system?  Answer Y, if
this is a new system and thus a new Veritas
license key will be required.  (Y/N)?
```

If the system being restored is the original server being restored, (i.e. the original system/CPU that was backed up) answer “N”. If the system being restore is a different system (i.e. not the original system/CPU backup), answer “Y”.

13 Remove the CD from the CD-ROM drive.

14 After formatting the disks, the script recovers each partition. Once this is done, the system prompts you to reboot the machine. Follow the instructions you see on the screen when you are running the script.

15 When you select Y to the reboot, the system takes you to the ok prompt. At this point, you need to type **boot disk –r** or **boot disk0** to boot from the disk.

boot disk –r =>T140x Management/Accounting Server or T140x Database Server

boot disk0 => for all other Servers

16 If you answered **no** in the step 12, proceed to step 17. Otherwise, the system will prompt you to enter a valid Veritas License Key. The license key entered must be keyed to the CPU/system being restored. The Veritas License Key must be the correct license key, otherwise Veritas installation will fail, resulting in a restore failure. Once the valid License Key is entered, the recovery process runs through the installation of the

Veritas Volume Manager. Note this process is lengthy, however, it is fully automated and requires no operator intervention

17 The recovery process now runs through the steps involved in setting up the metadevices and mirroring the disk. Eventually the system comes up and the system will take you back to the login prompt.

18 Perform step 5 in the procedure Required setup of an MCP server acting as a remote host.

19 The restore procedure should be completed at this point.

20 Review the log file which is generated by the recover script, to ensure the restore was successful. The log file is stored to the directory

```
/export/home/sysadmin/bkup_restore
```

For the restore of a database server there will be two log files in this directory, because the restore is a two-step process with the restore script being executed at two different points in time.

21 Logoff from the machine.

22 Verify the correct load for the MCP components has been restored. See the procedure Verify and restore correct load for the MCP components for more information.

23 Press the eject button on tape drive, retrieve tape, and store the tape in safe place.

24 If the server hosted the Oracle Database, it will now have to be restored.

If the server hosted the Provisioning Module, the Provisioning Module must now be restarted. See the *System Management Console User Guide (NN10273-111)* for information on restarting a component.

Verify and restore correct load for the MCP components

Since server backups are performed infrequently, the version of the component software/configuration that is restored to the server may not be the current (up-to-date) version shown on the System Management Console. Use the following procedure to verify the correct load is on the restored server.

1 Login to the “restored” server as **root**.

2 Query the server for a list of the current version of the component(s) deployed on the server.

```
/opt/sb/dsm2/bin/dsmquery
```

Ignore the “action” component if it exists on the server.

3 If the version of the component installed on the restored server does not match the version shown on the System Management Console, then the component needs to be updated from the System Management Console.

If the required version is not part of the DSM pool on the server hosting the Management Module, then:

a Restore any required DSM pools to the server hosting the Management Module(s). This will be required if a maintenance releases was installed after the server was backed up.

b Update the Management Module (SysMgr) processes, using the mgmtdeploy.pl script.

See the Management Module Basics document for information on performing Management Module updates.

4 Upgrade all the non-SysMgr components on the restored server(s).

See the *System Management Console User Guide (NN10273-111)* for information on updating component software versions.

Recovery for AudioCodes server

In the event of any hardware failure, a new AudioCodes server is required. A complete re-installation and commissioning of the AudioCodes PRI gateway software is required (using the same server name and IP configuration as the original install). For procedures on how to install and commission the AudioCodes PRI Gateway, please refer to the AudioCodes documentation.

Resolving backup and restore error scenarios

This chapter describes error scenarios that might be experienced during backup and restore activities:

- Invalid IP address entered for ufsrestore command
- Restoring from multiple tapes
- Error installing USB Tape Drive
- Telnet session failure during a backup
- Tape drive failure during a backup
- Lost connectivity during backup/restore to remote tape drive

Invalid IP address entered for ufsrestore command

When the backup/restore scripts are executed, an informative message is displayed when an invalid IP address is entered to “backup to”/”restore from”.

```
/usr/local/bin/mcp_backup.pl 100.10.10.20  <Tape
Server IP>

no answer from 100.10.10.20

10:22:27 ERROR: System, 100.10.10.20,could not be
pinged.

10:22:27 Remote Backup verification failed, aborting
backup process

Logs are written to
/export/home/sysadmin/bkup_restore/mcp_backup…
```

However, the very first step of the restore process has the user execute (manually) an **ufsrestore** command. If the user enters an incorrect IP address at this point, the user can expect to see the following output:

```
ufsrestore rfsv sysadmin@100.10.10.20:/dev/rmt/0cn 1
Fri Feb 6 17:06:14 CST 2004

120.120.13.26: Connection timed out
before Fri Feb  6 17:11:03 CST 2004
```

The command will need to be re-executed with the correct IP address.

Restoring from multiple tapes

When restoring from multiple tapes, if the user presses return before the “next tape” has been inserted into the tape drive, the restore process must be started over. To get out of this situation, when prompted to mount an incorrect volume (e.g. “Mount volume 3” when it should be tape 2) continue to press enter until a "Read error" is displayed, at which point answer **n**, and the restore will abort.

Below is a sample of the output that is displayed to the user for this case.

```
Mount volume 2
then enter volume name (default: /dev/rmt/0cn)
```

<User accidentally presses enter before next tape is inserted>

```
Mount volume 3
then enter volume name (default: /dev/rmt/0cn)
```

<Continue pressing enter until a “Read error” is generated>

```
Read error while
restoring./me/loads/pool9/Files/B/UAS06.zip.bLfCbwY
vd5YvveYtkOYinAZgoLi

continue? [yn] n

Verify volume and initialize maps

Media read error: I/O error

rest*: No such file or directory

12:49:35 Failed to Restore /IMS/imssipdb directory,
aborting restore process
```

```
Logs are written to
/export/home/sysadmin/bkup_restore/mcp_recover.pl.l
og
```

Error installing USB Tape Drive

If the steps documented in section Utilization of a USB tape drive fail, then the server must be rebooted to recognize the USB Tape drive.To perform this activity, use the following steps:

1 Login as **root**

2 Execute the command

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

Telnet session failure during a backup

If a telnet session is being used (through the server's network interface) to perform a backup, and the telnet session dies, the associated backup process will die as well. In addition, when using a Telnet Session, the user will not see any of the "system logs" that can be printed to the Console port (when other "system" type issues occur).

Tape drive failure during a backup

If something happens to the tape drive (turned off USB tape drive) during a backup, something similar to the following is displayed to the screen:

```
DUMP: write: I/O error
DUMP: write error 8320 blocks into volume 1
DUMP: Do you want to restart?: ("yes" or "no")
```

The user should answer **no** to this prompt, so that the script will terminate (and another backup can be started). When the user answers **no** the following is displayed to the screen:

```
DUMP: The ENTIRE dump is aborted.
19:29:15
 **************************************************************

19:29:15  An error occurred during one (or more) dump
commands=>

19:29:15    DUMP: Do you want to restart?: ("yes" or "no")  DUMP:
The ENTIRE dump is aborted.

19:29:15  DO NOT USE THIS BACKUP - a RESTORE USING THIS
BACKUP WILL FAIL
19:29:15  Fix the associated problem, and perform another backup
```

```
19:29:15 ****************************************************************

19:29:15 Dump command(s) failed.  Aborting backup.

 Logs are written to
/home/sysadmin/bkup_restore/mcp_backup.pl.log….
```

Lost connectivity during backup/restore to remote tape drive

If a cable is inadvertently disconnected between the server being backed up and the remote Tape drive (which causes connectivity to be lost between the two servers), or either of the two servers lose power, within 20 minutes the user should see a message printed to the screen that says:

```
DUMP: Lost connection to remote host.
```

However, the underlying system command (**usfdump** - which the **mcp_backup.pl** script invokes to perform the backup) does not time out to return control back to the **mcp_backup** script. Therefore, the script does not terminate when this error occurs. To get out of this situation (and start a new backup), press Cntrl-c to break out of the **ufsdump** system command, and then the **mcp_backup.pl** script will terminate and a log file is generated showing that there was a lost connection.

Multimedia Communication Portfolio

Multimedia Communication Server

Backup and Recovery Guide

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks.

Publication number: NN42020-502
Product release: MCS 5100 3.5
Document version: Standard 5.0
Date: August 2006