Sun N1 System Manager 1.3 Troubleshooting Guide

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054
U.S.A.

Part No: 819–5143
April 2006

060411@14774

Contents

Tables

Preface

The *Sun N1 System Manager 1.3 Troubleshooting Guide* describes problems and errors that might occur when using the Sun N1™ System Manager system, and provides solutions for those problems.

Who Should Use This Book

This guide is intended for system administrators who are responsible for maintaining the N1 System Manager software and hardware. The system administrators must have extensive knowledge and experience in the following areas:

- The Solaris™, Linux, and Microsoft Windows operating systems, and the network administration tools provided by each operating system
- Network equipment and network devices from a variety of vendors such as Sun and Cisco
- DNS, DHCP, IP addressing, subnetworks, VLANs, SNMP, NFS, TFTP, and mail configuration
- Network device interconnections and cabling
- Linux Kickstart™ installation
- Solaris JumpStart™ installation
- Microsoft Windows Remote Installation Services (RIS)

How This Book Is Organized

- Chapter 1 provides information concerning N1 System Manager operational processes that can assist you in troubleshooting.
- Chapter 2 lists error messages, causes, and resolutions.
- Chapter 3 lists common problems that can occur during installation, configuration, and operation of the N1 System Manager, and provides solutions for each.
- Chapter 4 provides the procedures for resolving N1 System Manager problems.

Related Documentation

This guide is part of a nine-volume implementation reference set. The set should be read in the following order:

- *Sun N1 System Manager 1.3 Release Notes*
- *Sun N1 System Manager 1.3 Introduction*
- *Sun N1 System Manager 1.3 Site Preparation Guide*
- *Sun N1 System Manager 1.3 Installation and Configuration Guide*
- *Sun N1 System Manager 1.3 Discovery and Administration Guide*
- *Sun N1 System Manager 1.3 Operating System Provisioning Guide*
- *Sun N1 System Manager 1.3 Grid Engine Provisioning and Monitoring Guide*
- *Sun N1 System Manager 1.3 Command Line Reference Manual*
- *Sun N1 System Manager 1.3 Troubleshooting Guide*

Documentation, Support, and Training

The Sun web site provides information about the following additional resources:

- Documentation (`http://www.sun.com/documentation/`)
- Support (`http://www.sun.com/support/`)
- Training (`http://www.sun.com/training/`)

Typographic Conventions

The following table describes the typographic conventions that are used in this book.

TABLE P–1 Typographic Conventions

Typeface	Meaning	Example
`AaBbCc123`	The names of commands, files, and directories, and onscreen computer output	Edit your `.login` file. Use `ls -a` to list all files. `machine_name% you have mail.`
`AaBbCc123`	What you type, contrasted with onscreen computer output	`machine_name%` **`su`** `Password:`
aabbcc123	Placeholder: replace with a real name or value	The command to remove a file is `rm` *filename.*

TABLE P–1 Typographic Conventions *(Continued)*

Typeface	Meaning	Example
AaBbCc123	Book titles, new terms, and terms to be emphasized	Read Chapter 6 in the *User's Guide*. A *cache* is a copy that is stored locally. Do *not* save the file. **Note:** Some emphasized items appear bold online.

Shell Prompts in Command Examples

The following table shows the default UNIX® system prompt and superuser prompt for the C shell, Bourne shell, and Korn shell.

TABLE P–2 Shell Prompts

Shell	Prompt
C shell	`machine_name%`
C shell for superuser	`machine_name#`
Bourne shell and Korn shell	`$`
Bourne shell and Korn shell for superuser	`#`

◆ ◆ ◆ CHAPTER 1

General Information

This section provides information concerning N1 System Manager operational processes that can assist you in troubleshooting. The following topics are discussed:

In this manual, the term *manageable server* is used for a server that is accessible by the N1 System Manager network, but has not yet been discovered by the N1 System Manager. A *managed server* is a server that has been successfully discovered by the N1 System Manager and is subsequently managed by the N1 System Manager.

Note – The topics in this chapter and subsequent chapters are organized alphabetically.

DHCP Service Conflict With N1 Grid Service Provisioning System

If you are using both the N1 System Manager and the Sun N1™ Service Provisioning System with the OS provisioning plug-in, you must choose which product you want to use for OS deployment for a given target set of servers. Based on the product chosen for OS deployment, you must ensure that the DHCP service supplied by the other product is manually shut down (as the `root` user) using operating system commands. Failure to shut the service down might result in unreliable behavior of OS deployment operations as well as potential network related problems.

Discovery and Routers

Discovery of manageable servers works across routers if the network services used by the discovery process are not blocked by a firewall. Network services used by the discovery process can include SSH, IPMI, Telnet and SNMP.

Identifying Hardware and OS Threshold Breaches

If the value of a monitored hardware health attribute, or OS resource utilization attribute breaches a threshold value, an event log is immediately created, which indicates that the threshold has been breached. The event log is available from the browser interface. A symbol appears among the monitored data table in the browser interface to indicate that a threshold has been breached, as shown in the graphic at "To Retrieve Threshold Values for a Server" in *Sun N1 System Manager 1.3 Discovery and Administration Guide*.

Alternatively, use the `show log` command to verify that the event log has been generated:

```
N1-ok> show log
Id            Date                       Severity    Subject     Message
.
.
10            2005-11-22T01:45:02-0800   WARNING     Sun_V20z_XG041105786
A critical high threshold was violated for server Sun_V20z_XG041105786: Attribute cpu0.vtt-s3 Value 1.32

13            2005-11-22T01:50:08-0800   WARNING     Sun_V20z_XG041105786
A normal low  threshold was violated for server Sun_V20z_XG041105786: Attribute cpu0.vtt-s3 Value 1.2
```

If monitoring traps are lost, a particular threshold status may not be refreshed for up to `30` hours, although the overall status can still be refreshed every `10` minutes.

N1 System Manager Cannot Be Used to Manage System Management Servers

Do not use the N1 System Manager to manage servers that have system management software installed on them such as Sun Management Center, Sun Control Station, and any other system management applications including the N1 System Manager.

Regenerating Security Keys

The N1 System Manager uses strong encryption techniques and common agent container security keys to ensure secure communication between the management server and each managed server.

The security keys used by the N1 System Manager must be identical across all servers. Under normal operation, the security keys used by the keys can be left in their default configuration. You should regenerate the security keys if any of the following cases occur:

- The root password of the management server has been exposed or compromised.
- The system date on the management server has been changed using the `date` command. This raises the risk that because the management server date is out of synchronization, no N1 System Manager services will start the next time that the N1 System Manager is restarted.

In each of the above cases, the security keys must be regenerated, and the N1 System Manager management daemon restarted, as described in "To Regenerate Common Agent Container Security Keys" on page 45.

◆ ◆ ◆ CHAPTER 2

Error Messages

This section lists Sun N1 System Manager error messages and resolutions for each error.

Installation and Configuration Error Messages

This section provides error messages that might be displayed during installation and configuration of the N1 System Manager.

```
[alert] httpd: Could not determine the server's fully
 qualified domain name, using 129.123.111.12 for ServerName
 scs-httpd: Fri Nov 19 12:47:34 PST 2004 : Daemon started (pid=1473 1485 1486..
```

Cause: The system cannot determine the server's fully qualified domain name because the system file `/etc/resolv.conf` is not configured correctly.

Solution: Update the `/etc/resolv.conf` file as directed by "To Update the `/etc/resolv.conf` File" on page 50.

```
Error waiting for SPS to start.
```

Cause: Incorrect entry in the `/etc/hosts` file.

Solution: Update the `/etc/hosts` as directed by "To Update the `/etc/hosts` File" on page 49.

```
Fatal error: Command failed for target 'Makefile'
```

Example:

```
Writing Makefile for Locale::gettext
Makefile out-of-date with respect to
/usr/perl5/5.8.4/lib/i86pc-solaris-64int/Config.pm
/usr/perl5/5.8.4/lib/i86pc-solaris-64
int/CORE/config.h
Cleaning current config before rebuilding Makefile...
make -f Makefile.old clean > /dev/null 2>&1 || /bin/sh -c true
/usr/bin/perl Makefile.PL
Writing Makefile for Locale::gettext
```

```
==> Your Makefile has been rebuilt. <==
==> Please rerun the make command. <==
false
*** Error code 255
make: Fatal error: Command failed for target ‘Makefile’
```

Cause: The system date is incorrect.

Solution: Set the system date.

Run Time Error Messages

This section provides error messages that might be displayed when starting N1 System Manager or trying to connect to N1 System Manager.

`An exception occurred trying to update` *SP-IPaddress*`.`
`Please refer to the log file for more information.`

Cause: Firmware versions 2.2 and above for the Sun Fire V20z servers do not support the PIC firmware upgrade. The upgrade of PIC firmware will fail, and the job step will show the above error message.

Solution: Do not load PIC firmware to the Sun Fire V20z servers.

`Connect to` *management server url:443* `failed (Connection refused)`

Description: When entering the Sun N1 System Manager server URL using the format `https://`*servername*, where *servername* is the name of the management server, the above error message is displayed.

Cause: The system file `/etc/resolv.conf` is not configured correctly.

Solution: Update the `/etc/resolv.conf` as directed by “To Update the `/etc/resolv.conf` File” on page 50.

`Starting dhcpd: [Failed]`

Description: `dhcpd` fails to start during system boot. This message is normal if Sun N1 System Manager configuration has not been performed.

Solution: Configure the N1 System Manager system as described in “Configuring the N1 System Manager” in *Sun N1 System Manager 1.3 Installation and Configuration Guide*.

◆ ◆ ◆ CHAPTER 3

Common Problems

This chapter provides a list of issues and problems that might occur during installation, configuration, and operation of the N1 System Manager, and provides solutions for each.

The following topics are discussed:

Base Management Installation for a Managed Server Fails

Installing the base management feature support might fail due to stale SSH entries on the management server. If the `add server feature` command fails and no true security breach has occurred, note the name and IP address of the management server, and then remove the entry for that server as described in "To Update the `ssh_known_hosts` File" on page 50.

Cannot Determine the Firmware Version on a Managed Server

If the firmware version cannot be reported by the N1 System Manager, one or all of the following situations might be the cause:

- The IP address of the manageable server's management processor has not been set, and thus the server cannot be discovered.

  Check whether the management processor IP address has been set and, if it has been set, whether it is accessible by the N1 System Manager.

  If the management processor IP address is not correct, assign an IP address to the processor as directed by the hardware documentation.

  If the IP address is correct, go to the next item in this list.

- The manageable server's management processor account credentials (login account and password) are not recognized by the N1 System Manager. Check the credentials used by the N1 System Manager, and then try accessing the manageable server's management processor account. For information about the processor accounts, see "SPARC Architecture Manageable Server Credentials" in *Sun N1 System Manager 1.3 Site Preparation Guide* and "x86 Architecture Manageable Server Credentials" in *Sun N1 System Manager 1.3 Site Preparation Guide*.g

  If you cannot access the management processor, reset the manageable server to the factory defaults as directed by the hardware documentation, and reassign an IP address to the manageable server's management processor. When you have completed resetting the manageable server, run discovery on the server as described in "SP-Based Discovery" in *Sun N1 System Manager 1.3 Discovery and Administration Guide*.

  If discovery is successful, verify the managed server's firmware version as described in "To List the Firmware Updates Installed on a Managed Server" in *Sun N1 System Manager 1.3 Operating System Provisioning Guide*.

  If the firmware version still cannot be reported by the N1 System Manager, you need to manually check the managed server's firmware by logging into the service processor on the managed server and running a specific service processor command as directed by the server's hardware documentation. For example, to view all of the firmware for an ALOM-enabled server, log into the service processor and type the following command:

```
showsc version -v
Advanced Lights Out Manager v1.5.3
SC Firmware version: 1.5.3
SC Bootmon version: 1.5.3

SC Bootmon Build Release: 02
SC bootmon checksum: 4F888E28
SC Bootmon built Jan  6 2005, 17:05:24

SC Build Release: 02
SC firmware checksum: 6FFB200D

SC firmware built Jan  6 2005, 17:05:12
```

```
SC firmware flashupdate MAY 25 2005, 01:33:55

SC System Memory Size: 8 MB

SC NVRAM Version = b

SC hardware type: 0
```

Compare the service processor firmware versions to the supported firmware versions. See "Manageable Server Firmware Requirements" in *Sun N1 System Manager 1.3 Site Preparation Guide*, and update the firmware to a supported version as directed by the hardware documentation.

Cannot Discover a Manageable Server

Failure to discover a manageable server can be caused by many different issues. This section provides guidelines and references to help you resolve each issue.

The following topics are discussed:

Discovery of RSC Servers

Manageable servers based on the Remote System Control (RSC) technology, such as Sun Fire V490 and V890 series servers, must be powered off before they can be discovered by N1 System Manager. RSC servers must remain powered off until discovery is complete and discovery has been confirmed by using the `show server` command.

Note – The first time the `show server` command is used to identify a newly discovered RSC server, the command can take up to 5 minutes to complete.

The console of an RSC server must not be in use when being discovered. These servers must also be bench configured prior to discovery. For details on bench configuration of RSC servers, see "Preparing RSC-based Manageable Servers" in *Sun N1 System Manager 1.3 Site Preparation Guide*.

If the RSC manageable server was not powered off before being discovered by N1 System Manager, the server MAC address is not detected. Subsequent attempts to load an OS on the server fail with the following message:

```
Operation failed
```

In this case, stop the managed server:

```
N1-ok> stop server server force true
```

Refresh the managed server to retrieve the server's MAC address:

```
N1-ok> set server server refresh
```

This command can take up to 5 minutes to complete. Once complete, an OS can be provisioned on to the RSC server using N1 System Manager.

Incorrect Firmware is Installed on the Managed Server

The managed server firmware might be too old.

Verify the firmware version and, if necessary, update the firmware. For a list of qualified firmware versions, see "Manageable Server Firmware Requirements" in *Sun N1 System Manager 1.3 Site Preparation Guide*.

Maximum Number of SNMP Connections has been Exceeded

If discovery fails, the target server has reached its maximum number of SNMP connections if the following is contained in the job output:

```
Error. The limit on the number of SNMP destinations has been exceeded.
```

The service processor of the Sun Fire V20z and V40z server has a limit of three SNMP destinations. To see the current SNMP destinations, perform the following steps:

1. Log into the service processor using SSH.
2. Run the following command:

   ```
   sp get snmp-destinations
   ```

The SNMP destinations appear in the output.

If there are three destinations for a V20z or a V40z, discovery will fail. The failure occurs because the N1 System Manager adds another snmp-destination to the service processor during discovery.

The SNMP destinations can be configured in a service processor by N1 System Manager or some other management software. You can delete entries from the SNMP destinations if you know that the SNMP destination entry is no longer needed. This would be the case if you discovered the target server using N1 System Manager on one management server and then decided to not use that management server without deleting the server. You can use the `sp delete snmp-destination` command on the service processor if you need to delete an entry. Use the delete command with caution because some other management software may need the entry for monitoring. A manageable

server's SNMP destination is deleted, however, when the server is deleted from the N1 System Manager using the `delete server` command. It is best practice always to use the `delete server` command when removing a manageable server.

Firmware Update for a Sun Fire V20z or Sun Fire V40z fails

Cause: Auto-negotiate link speed has not been enabled on the management network switch.

Solution: Enable auto-negotiate link speed on the management network switch for all management network connections.

Job IDs are Missing After Power Cycling the Management Server

If the N1 System Manager management server is rebooted or power cycled while jobs are running, the `show jobs` command will not list the jobs that were running when the management server was power cycled. Subsequent jobs will start at a higher job number, and the list of jobs produced by the `show jobs` command will display a gap in the job numbers. This can occur if there is a power loss, or if the management server was manually power cycled.

To avoid this problem, wait until all jobs have completed, then stop the N1 System Manager and wait for all processes to stop before rebooting or powering off the management server.

Management Server IP Address Resolves to 127.0.0.1

Cause: The `/etc/hosts` file does not contain an IP address and server name assignment for the management server.

Solution: Update the `/etc/hosts` file as described in "To Update the `/etc/hosts` File" on page 49.

Management Server Reboots During Discovery

Cause: The IP address range specified for discovery includes the management server IP addresses. The discovery process has discovered the management server and attempted to configure the management server as a managed server, which causes the management server/

Solution 1: Specify an IP address range for discovery that does not include the management server IP addresses.

Solution 2: Run `n1smconfig`, and when prompted whether to specify a range of IP addresses for the DHCP server to use:

- Type **`y`** to configure the IP addresses that are to be used for discovery.
- Specify a range of IP addresses that does not include the management server IP addresses.

For further information, see "To Configure the N1 System Manager" in *Sun N1 System Manager 1.3 Installation and Configuration Guide*.

N1 System Manager Services do not Start After Reboot or Restart

If you reboot the management server, and the N1 System Manager services do not restart, you must regenerate security keys as described in "Regenerating Security Keys" on page 15.

If you stop and then start the N1 System Manager and the services do not restart you must regenerate security keys as described in "Regenerating Security Keys" on page 15.

Management Features Unavailable on Manageable Servers After Rebooting

When the `load server` or `load group` command is used to install software on the manageable server, the manageable server's `networktype` attribute could be set to `dhcp`. This setting means that the server uses DHCP to get its provisioning network IP address. If the system reboots and obtains a different IP address than the one that was used for the `agentip` parameter during the `load` command or `add server` commands, then the following features may not work:

- The OS Monitoring content of the `show server` command. (No OS monitoring)
- The `load server update` and `load group update` commands
- The `start server command` command
- The `set server threshold` command
- The `set server refresh` command

In this case, use the `set server agentip` command to correct the server's agent IP address. See "To Modify the Agent IP for a Server" in *Sun N1 System Manager 1.3 Discovery and Administration Guide* for details.

OS Distributions and Deployment

OS distribution creation and OS deployment failures can be caused by many different issues. This section provides guidelines and references to help you resolve each issue.

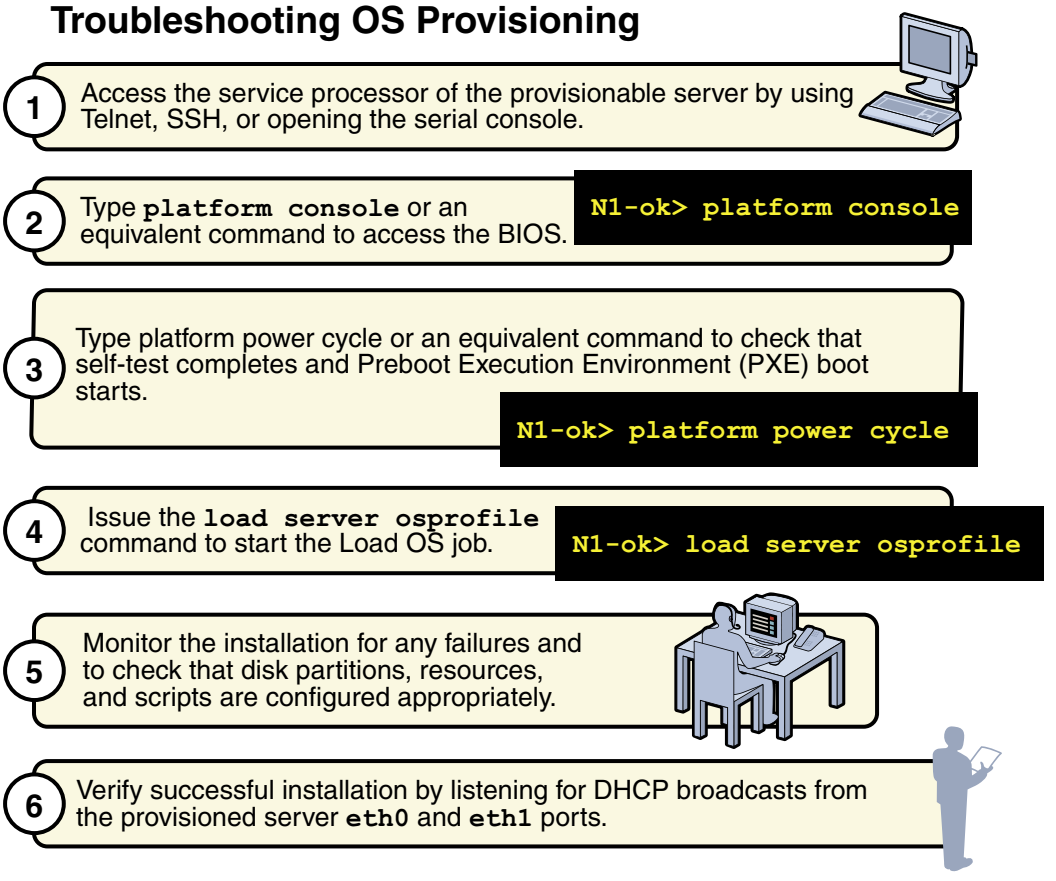
The following topics are discussed:

Possible Causes for Distribution and Deployment Failure

OS deployments might fail or fail to complete if any of the following conditions occur:

- The target RSC technology server was not powered off before discovery was run. RSC servers must remain powered off until discovery is complete and discovery has been confirmed by using the `show server` command. See "Discovery of RSC Servers" on page 21.
- Partitions are not modified to suit a Sun Fire V40z or SPARC V440 server. See "To Modify the Default Solaris OS Profile for a Sun Fire V40z or a SPARC V440 Server" in *Sun N1 System Manager 1.3 Operating System Provisioning Guide*.
- Scripts are not modified to install the driver needed to recognize the Ethernet interface on a Sun Fire V20z server. See "To Modify a Solaris 9 OS Profile for a Sun Fire V20z Server With a K2.0 Motherboard" in *Sun N1 System Manager 1.3 Operating System Provisioning Guide*.
- DHCP is not correctly configured. See "Solaris Deployment Job Times Out or Stops" on page 26.
- OS profile installs only the Solaris Core System Support distribution group. See "Solaris OS Profile Installation Fails" on page 27.
- The target server cannot access DHCP information or mount distribution directories. See "Invalid Management Server Netmask" on page 29.
- The management server cannot access files during a Load OS operation. See "Restarting NFS to Resolve `Boot Failed` Errors" on page 31.
- The Linux deployment stops. See "Linux Deployment Stops" on page 28.
- The Red Hat deployment fails. See "Red Hat Linux OS Profile Creation Fails" on page 28.

Use the following graphic as a guide to troubleshooting best practices. The graphic describes steps to take when you initiate provisioning operations. Taking these steps will help you troubleshoot deployments with greater efficiency.



Solaris Deployment Job Times Out or Stops

If you attempt to load a Solaris OS profile and the OS Deploy job times out or stops, check the output in the job details to ensure that the target server completed a PXE boot. For example:

```
PXE-M0F: Exiting Broadcom PXE ROM.
      Broadcom UNDI PXE-2.1 v7.5.14
     Copyright (C) 2000-2004 Broadcom Corporation
     Copyright (C) 1997-2000 Intel Corporation
     All rights reserved.
CLIENT MAC ADDR: 00 09 3D 00 A5 FC  GUID: 68D3BE2E 6D5D 11D8 BA9A 0060B0B36963
     DHCP.
```

If the PXE boot fails, the `/etc/dhcpd.conf` file on the management server might have not been set up correctly by the N1 System Manager.

Note – The best diagnostic tool is to open a console window on the target machine and then run the deployment. See "Connecting to the Serial Console for a Managed Server" in *Sun N1 System Manager 1.3 Discovery and Administration Guide*.

If you suspect that the `/etc/dhcpd.conf` file was configured incorrectly, complete the following procedure to modify the configuration.

▼ To Modify the Network Interface Configuration

1. **Log in to the management server as root.**
2. **Inspect the `dhcpd.conf` file for errors.**

   ```
   # vi /etc/dhcpd.conf
   ```

3. **If errors exist that need to be corrected, run the following command:**

   ```
   # /usr/bin/n1smconfig
   ```

   The `n1smconfig` utility appears.

4. **Modify the provisioning network interface configuration.**

   See "Configuring the N1 System Manager" in *Sun N1 System Manager 1.3 Installation and Configuration Guide* for detailed instructions.

5. **Load the OS profile on the target server.**

Solaris OS Profile Installation Fails

OS profiles that install only the Core System Support distribution group do not load successfully. Specify `"Entire Distribution plus OEM Support"` as the value for the `distributiongroup` parameter. Doing so configures a profile that will install the needed version of SSH and other tools that are required for servers to be managed by the N1 System Manager.

Deploying Solaris OS 9 Update 7 or Lower from a Linux Management Server Fails

The inability to deploy Solaris 9 Update 7 or lower OS distributions to servers from a Linux management server is usually due to a problem with NFS mounts. To solve this problem, you need to

apply a patch to the mini-root of the Solaris 9 OS distribution. The instructions differ according to the management and patch server configuration scenarios in the following table. The patch is not required if you are deploying Solaris 9 Update 8 or later.

TABLE 3–1 Task Map for Patching a Solaris 9 Distribution

Management Server	Patch Server	Task
Red Hat 3.0 u2	Solaris 9 OS on x86 platform	"To Patch a Solaris 9 OS Distribution by Using a Solaris 9 OS on an x86 Patch Server" on page 51
Red Hat 3.0 u2	Solaris 9 OS on SPARC platform	"To Patch a Solaris 9 OS Distribution by Using a Solaris 9 OS on a SPARC Patch Server" on page 54

Red Hat Linux OS Profile Creation Fails

Building Red Hat OS profiles on the N1 System Manager might require additional analysis to avoid failures. If you have a problem with a custom OS profile, perform the following steps while the problem deployment is still active.

1. Log into the management server as `root`.
2. Run the following script:

```
# cat /var/opt/sun/scs/share/allstart/config/ks*cfg > failed_ks_cfg
```

The `failed_ks_cfg` file will contain all of the KickStart parameters, including those that you customized. Verify that the parameters stated in the configuration file are appropriate for the current hardware configuration. Correct any errors and try the deployment again.

Linux Deployment Stops

If you are deploying a Linux OS and the deployment stops, check the console of the target server to see if the installer is in interactive mode. If the installer is in interactive mode, the deployment timed out because of a delay in the transmission of data from the management server to the target server. This delay usually occurs because the switch or switches connecting the two machines has `spanning tree` enabled. Either turn off `spanning tree` on the switch or disable `spanning tree` for the ports that are connected to the management server and the target server.

If `spanning tree` is already disabled and OS deployment stops, there may be a problem with your network.

Note – For Red Hat installations to work with some networking configurations, you must enable `spanning tree`.

Windows Deployment Fails

Provisioning a Windows distribution to a managed server can fail for several reasons:

- The Windows operating system might not be compatible with the managed server. For a list of qualified servers, see "Manageable Server Requirements" in *Sun N1 System Manager 1.3 Site Preparation Guide*.
- The SSH entries for that managed server on the management server `known_hosts` file might be stale or obsolete. Determine the management server name and IP address, and then remove the entry for that managed server from the `known_hosts` as described in "To Update the `ssh_known_hosts` File" on page 50.
- The product key is unique to each release of the Windows OS. To ensure that the correct product key applies, either modify the OS profile to include the correct product key or use the *productkey* attribute on the `load server` command.
- If you encounter a TFTP error when loading the OS profile, the GUID is likely incorrect. To find the GUID of a system, use the Pre-Boot eXecution Environment (PXE) to boot the system.
- If Linux was installed previously on the managed server, Windows will ask about partitions the first time that you try to install Windows on the system. To resolve this issue, delete the partitions on the console, or wipe out the first part of the disk before you install Windows.

Invalid Management Server Netmask

If the target server cannot access DHCP information or mount the distribution directories on the management server during a Solaris 10 deployment, you might have network problems caused by an invalid netmask. The console output might be similar to the following:

```
Booting kernel/unix...
  krtld: Unused kernel arguments: 'install'.
  SunOS? Release 5.10 Version Generic 32-bit
  Copyright 1983-2005 Sun Microsystems, Inc.  All rights reserved.
  Use is subject to license terms.
  Unsupported Tavor FW version: expected: 0003.0001.0000, actual: 0002.0000.0000
  NOTICE: tavor0: driver attached (for maintenance mode only)
  Configuring devices.
  Using DHCP for network configuration information.
  Beginning system identification...
  Searching for configuration file(s)...
  Using sysid configuration file /sysidcfg
```

```
Search complete.
Discovering additional network configuration...
Completing system identification...
Starting remote procedure call (RPC) services: done.
System identification complete.
Starting Solaris installation program...
Searching for JumpStart directory...
/sbin/dhcpinfo: primary interface requested but no primary interface is set
not found
Warning: Could not find matching rule in rules.ok
Press the return key for an interactive Solaris install program...
```

To fix the problem, set the management server netmask value to `255.255.255.0`. See "To Configure the N1 System Manager" in *Sun N1 System Manager 1.3 Installation and Configuration Guide*.

OS Distribution Creation Fails with a Copying Files Error

If the creation of an OS distribution fails with a copying files error, check the size of the ISO image and ensure that it is not corrupted. You might see output similar to the following in the job details:

```
bash-3.00# /opt/sun/n1gc/bin/n1sh show job 25
Job ID:   25
Date:     2005-07-20T14:28:43-0600
Type:     Create OS Distribution
Status:   Error (2005-07-20T14:29:08-0600)
Command:     create os RedHat file /images/rhel-3-U4-i386-es-disc1.iso
Owner:    root
Errors:   1
Warnings: 0

Steps
ID     Type             Start
Completion                 Result
1      Acquire Host     2005-07-20T14:28:43-0600
2005-07-20T14:28:43-0600   Completed
2      Run Command      2005-07-20T14:28:43-0600
2005-07-20T14:28:43-0600   Completed
3      Acquire Host     2005-07-20T14:28:46-0600
2005-07-20T14:28:46-0600   Completed
4      Run Command      2005-07-20T14:28:46-0600
2005-07-20T14:29:06-0600   Error 1

Errors
Error 1:
Description: INFO   : Mounting /images/rhel-3-U4-i386-es-disc1.iso at
```

```
/mnt/loop23308
INFO   : Version is 3ES, disc is 1
INFO   : Version is 3ES, disc is 1
INFO   : type redhat ver: 3ES
cp: /var/opt/SUNWscs/data/allstart/image/3ES-bootdisk.img: Bad address
INFO   : Could not copy PXE file bootdisk.img
INFO   : umount_exit: mnt is: /mnt/loop23308
INFO   : ERROR: Could not add floppy to the Distro

Results
Result 1:
Server:   -
Status:   -1
Message:  Creating OS rh30u4-es failed.
```

In the above case, try copying a different set of distribution files to the management server. See "To Copy an OS Distribution From CDs or a DVD" in *Sun N1 System Manager 1.3 Operating System Provisioning Guide* or "To Copy an OS Distribution From ISO Files" in *Sun N1 System Manager 1.3 Operating System Provisioning Guide*.

Mount Point Issues

Distribution copy failures might also occur if there are file systems on the `/mnt` mount point. Move all file systems off of the `/mnt` mount point before attempting `create os` command operations.

OS Deployment Fails on a V20z or V40z With `internal error` Message

If OS deployment fails on a V20z or a V40z with the `internal error occurred` message provided in the job results, direct the platform console output to the service processor. If the platform console output cannot simply be directed to the service processor, reboot the service processor. To reboot the service processor, log on to the service processor and run the `sp reboot` command.

To check the console output, log on to the service processor, and run the `platform console` command. Examine the output during OS deployment to resolve the problem.

Restarting NFS to Resolve `Boot Failed` Errors

```
Error: boot: lookup /js/4/Solaris_10/Tools/Boot failed boot: cannot open
kernel/sparcv9/unix
```

Solution: The message differs depending on the OS that is being deployed. If the management server cannot access files during a Load OS operation, it might be caused by a network problem. To possibly correct this problem, try restarting NFS.

On a Solaris system, type the following:

```
# svcadm nfs restart
```

On a Linux system, type the following:

```
# /etc/init.d/nfs restart
```

Monitoring Problems

This section describes the most common monitoring problems, their causes, and solutions.

Basic Monitoring

If monitoring is enabled as described in "Enabling and Disabling Monitoring" in *Sun N1 System Manager 1.3 Discovery and Administration Guide*, and the status in the output of the `show server` or `show group` commands is `unknown` or `unreachable`, then the server or server group is not being reached successfully for monitoring. If the status remains `unknown` or `unreachable` for less than `30` minutes, it is possible that a transient network problem is occurring. However if the status remains `unknown` or `unreachable` for more than `10` minutes, it is possible that monitoring has failed. This could be the result of any of the following issues.

- The base monitoring agent on the managed server has stopped running.
- The managed server has been powered off or been unplugged.
- The managed server IP address or name has been changed independently of N1 System Manager.

If monitoring traps are lost, a particular threshold status may not be refreshed for up to `30` hours, although the overall status should still be refreshed every `10` minutes.

A time stamp is provided in the monitoring data output. The relationship between this time stamp and the current time can also be used to judge if there is an error with the monitoring agent.

OS Monitoring

It can take 5 to 7 minutes before all OS monitoring data is fully initialized. You may see that CPU idle is at `0.0`%, which causes a Failed Critical status with OS usage. This should clear up within 5-7 minutes after adding or upgrading the OS monitoring feature to the managed server. At that point, OS monitoring data should be available for the managed server by using the `show server` *server* command. For further information, see "To Add the OS Monitoring Feature" in *Sun N1 System Manager 1.3 Discovery and Administration Guide*

Adding the base management feature to a managed server might fail due to stale or obsolete SSH entries for that managed server on the management server `known_hosts` file. If the `add server server-name feature osmonitor agentip` command fails and no true security breach has occurred, remove the entry for that managed server from the `known_hosts` as described in "To Update the `ssh_known_hosts` File" on page 50. Then, retry the `add` command.

ALOM-based Managed Server Notifications are not Displayed

The ports of some models of manageable servers use the Advanced Lights Out Manager (ALOM) standard. These servers, detailed in "Manageable Server Requirements" in *Sun N1 System Manager 1.3 Site Preparation Guide*, use email instead of SNMP traps to send notifications about hardware events to the management server. For information about other events, see "Managing Event Log Entries" in *Sun N1 System Manager 1.3 Discovery and Administration Guide* and "Setting Up Event Notifications" in *Sun N1 System Manager 1.3 Discovery and Administration Guide*.

If there are no notifications about hardware events from ALOM architecture manageable servers, it could mean that all managed servers are all healthy. If you are using an external mail service instead of the internal secure N1 System Manager mail service, it is possible that the external mail service has not been configured correctly as an email server, or that email configuration has been invalidated due to other issues such as network error or domain name change.

To resolve, either:

- Reconfigure the N1 System Manager by running `n1smconfig`, and choose the secure internal N1 System Manager mail service.
- Check and reset your external email server configuration. See "Resetting Email Accounts for ALOM-based Managed Servers" on page 46

OS Updates

This section describes the most common OS update problems, their causes, and solutions.

The following topics are discussed:

OS Update Creation Fails

The name that is specified when you create a new OS update must be unique. The OS update to be created also needs to be unique. That is, in addition to the uniqueness of the file name for each OS update, the combination of the internal package name, version, release, and file name also needs to be unique.

For example, if `test1.rpm` is the source for an RPM named `test1`, another OS update called `test2` cannot have the same file name as `test1.rpm`. To avoid additional naming issues, do not name an OS update with the same name as the internal package name for any other existing packages on the manageable server.

You can specify an `adminfile` value when you create an OS update. For the Solaris OS update packages, a default `admin` file is located at `/opt/sun/n1gc/etc/admin`.

```
mail=
   instance=unique
   partial=nocheck
   runlevel=nocheck
   idepend=nocheck
   rdepend=nocheck
   space=quit
   setuid=nocheck
   conflict=nocheck
   action=nocheck
   basedir=default
   authentication=nocheck
```

If you use an `adminfile` to install an OS update, ensure that the package file name matches the name of the package. If the file name does not match that of the package, and an `adminfile` is used to install the OS update, uninstallation will fail. See "OS Update Uninstallation Failures" on page 39.

The default `admin` file setting used for Solaris package deployments in the N1 System Manager is `instance=unique`. If you want to report errors for duplicated packages, change the `admin` file setting to `instance=quit`. This change causes an error to appear in the Load Update job results if a duplicate package is detected.

See the `admin(4)` man page for detailed information about `admin` file parameter settings. Type `man -s4 admin` as root user on a Solaris system to view the man page.

For Solaris packages, a response file might also be needed. For instructions on how to specify an `admin` file and a `response` file when you create an OS update, see "To Copy an OS Update" in *Sun N1 System Manager 1.3 Operating System Provisioning Guide*.

Solaris OS Update Deployment Failures

This section describes troubleshooting scenarios and possible solutions for the following categories of failures during Solaris OS update deployment:

- Failures that occur before the job is submitted
- Load Update job failures
- Unload Update job failures
- Stop Job failures for Load Update

In the following `unload` command, the *update* could be either the *update* name in the list that appears when you type `show update all` list, or the update could be the actual package name on the target server.

```
N1-ok> load server server update update
```

Always check the package is targeted to the correct architecture.

Note – The N1 System Manager does not distinguish 32-bit from 64-bit for the Solaris (x86 or SPARC) OS, so the package or patch might not install successfully if it is installed on an incompatible OS.

If the package or patch does install successfully, but performance decreases, check that the architecture of the patch matches the architecture of the OS.

The following are common failures that can occur before the job is submitted:

`Target server is not initialized`
Solution: Check that the `add server feature osmonitor` command was issued and that it succeeded.

`Another running job on the target server`
Solution: Only one job is allowed at a time on a server. Try again after the job completes.

`Update is incompatible with operating system on target server`
Solution: Check that the OS type of the target server matches one of the update OS types. Type `show update update-name` at the `N1–ok>` prompt to view the OS type for the update.

`Target server is not in a good state or is powered off`
Solution: Check that the target server is up and running. Type `show server server-name` at the `N1–ok>` prompt to view the server status. Type `reset server server-name force` to force a reboot.

The following are possible causes for Load Update job failures:

Sometimes, Load Update jobs fail because either the same package already exists or because a higher version of the package exists. Ensure that the package does not already exist on the target server if the job fails.

`error: Failed dependencies:`

`A prerequisite package and should be installed.`
Solution: For a Solaris system, configure the `idepend=` parameter in the `admin` file.

`Preinstall or postinstall scripts failure: Non-zero status`

`pkgadd: ERROR: ... script did not complete successfully`
Solution: Check the pre-installation or post installation scripts for possible errors to resolve this error.

`Interactive request script supplied by package`
Solution: This message indicates that the `response` file is missing or that the setting in the `admin` file is incorrect. Add a `response` file to correct this error.

patch-name `was installed without backing up the original files`
Solution: This message indicates that the Solaris OS update was installed without backing up the original file. No action needs to be taken.

`Insufficient diskspace`
Solution: Load Update jobs might fail due to insufficient disk space. Check the available disk space by typing `df -k`. Also check the package size. If the package size is too large, create more available disk space on the target server.

The following are stop job failures for loading or unloading update operations:

If you stop a Load Update or Unload Update job and the job does not stop, manually ensure that the following process is killed on the management server:

```
# ps -ef |grep swi_pkg_pusher
ps -ef |grep pkgadd, pkgrm, scp, ...
```

Then, check any processes that are running on the manageable server:

```
# ps -ef |grep pkgadd, pkgrm, ...
```

The following are common failures for Unload Server and Unload Group jobs:

The rest of this section provides errors and possible solutions for failures related to the following commands: `unload server server-name update update-name` and `unload group group-name update update-name`.

`Removal of <SUNWssmu> was suspended (interaction required)`
Solution: This message indicates a failed dependency for uninstalling a Solaris package. Check the `admin` file setting and provide an appropriate `response` file.

`Job step failure without error details`

Solution: This message might indicate that the job was not successfully started internally. Contact a Sun Service Representative for more information.

`Job step failure with vague error details: Connection to 10.0.0.xx`

Solution: This message might indicate that the uninstallation failed because some packages were not fully installed. In this case, manually install the package in question on the target server. For example:

To manually install a `.pkg` file, type the following command:

```
# pkgadd -d pkg-name -a admin-file
```

To manually install a patch, type the following command:

```
# patchadd -d patch-name -a admin-file
```

Then, run the `unload` command again.

`Job hangs`

Solution: If the job appears to hang, stop the job and manually kill the remaining processes. For example:

To manually kill the job, type the following command:

```
# n1sh stop job job-ID
```

Then, find the PID of the PKG and kill the process, by typing the following commands:

```
# ps -ef |grep pkgadd
# pkill pkgadd-PID
```

Then run the `unload` command again.

Linux OS Update Deployment Failures

This section describes troubleshooting scenarios and possible solutions for the following categories of failures during Linux OS update deployment:

- Failures that occur before the job is submitted
- Load Update job failures
- Unload Update job failures
- Stop Job failures for Load Update

In the following `unload` command, the *update* could be either the *update* name in the list that appears when you type `show update all` list, or the update could be the actual package name on the target server.

`N1-ok> load server` *server* `update` *update*

The following are common failures that can occur before the job is submitted:

`Target server is not initialized`
Solution: Check that the `add server feature osmonitor` command was issued and that it succeeded.

`Another running job on the target server`
Solution: Only one job is allowed at a time on a server. Try again after the job completes.

`Update is incompatible with operating system on target server`
Solution: Check that the OS type of the target server matches one of the update OS types. Type `show update update-name` at the `N1–ok>` prompt to view the OS type for the update.

`Target server is not in a good state or is powered off`
Solution: Check that the target server is up and running. Type `show server server-name` at the `N1–ok>` prompt to view the server status. Type `reset server server-name force` to force a reboot.

The following are possible causes for Load Update job failures:

Sometimes, Load Update jobs fail because either the same package already exists or because a higher version of the package exists. Ensure that the package does not already exist on the target server if the job fails.

`error: Failed dependencies:`

`A prerequisite package should be installed`
Solution: Use an RPM tool to address and resolve Linux RPM dependencies.

`Preinstall or postinstall scripts failure: Non-zero status`

`ERROR: ... script did not complete successfully`
Solution: Check the pre-installation or post installation scripts for possible errors to resolve this error.

`Insufficient diskspace`
Solution: Load Update jobs might fail due to insufficient disk space. Check the available disk space by typing `df -k`. Also check the package size. If the package size is too large, create more available disk space on the target server.

The following are stop job failures for loading or unloading update operations:

If you stop a Load Update or Unload Update job and the job does not stop, manually ensure that the following process is killed on the management server:

```
# ps -ef |grep swi_pkg_pusher
ps -ef |grep rpm
```

Then, check any processes that are running on the manageable server:

```
# ps -ef |grep rpm, ...
```

The following are common failures for Unload Server and Unload Group jobs:

The rest of this section provides errors and possible solutions for failures related to the following commands: `unload server server-name update update-name` and `unload group group-name update update-name`.

`Job step failure without error details`
Solution: This message might indicate that the job was not successfully started internally. Contact a Sun Service Representative for more information.

`Job step failure with vague error details: Connection to 10.0.0.xx`
Solution: This message might indicate that the uninstallation failed because some RPMs were not fully installed. In this case, manually install the package in question on the target server. For example:

To manually install an RPM, type the following command:

```
# rpm -Uvh rpm-name
```

Then, run the `unload` command again.

`Job hangs`
Solution: If the job appears to hang, stop the job and manually kill the remaining processes. For example:

To manually kill the job, type the following command:

```
# n1sh stop job job-ID
```

Then, find the PID of the RPM and kill the process, by typing the following commands:

```
# ps -ef |grep rpm-name
# pkill rpm-PID
```

Then run the `unload` command again.

OS Update Uninstallation Failures

If you cannot uninstall an OS update that was installed with an `adminfile`, check that the package file name matches the name of the package. To check the package name:

```
bash-2.05# ls FOOi386pkg
   FOOi386pkg
   bash-2.05# pkginfo -d ./FOOi386pkg
```

```
   application FOOi386pkg     FOO Package for Testing
   bash-2.05# pkginfo -d ./FOOi386pkg | /usr/bin/awk '{print $2}'
   FOOi386pkg
---
   bash-2.05# cp FOOi386pkg Foopackage
   bash-2.05# pkginfo -d ./Foopackage
   application FOOi386pkg     FOO Package for Testing
   bash-2.05# pkginfo -d ./Foopackage | /usr/bin/awk '{print $2}'
   FOOi386pkg
   bash-2.05#
```

If the name is not the same, rename the `adminfile` in the manageable server's `/tmp` directory to match the name of the package and try the `unload` command again. If the package still exists, remove it from the manageable server by using `pkgrm`.

Unable to Log On to a Managed ServerManagement Processor

Cause: The service processor account and password are not known.

Solution: Reset the service processor accounts to the factory defaults as described by the hardware documentation

◆ ◆ ◆ CHAPTER 4

Problem Resolution Procedures

This section provides the procedures for resolving N1 System Manager problems. Many of the procedures provide solutions for more than one problem.

The following topics are discussed:

Checking for OS Monitoring Agents

Adding the OS monitoring feature to a managed server that has the base management feature installed might fail. The following job output shows the error:

```
N1-ok> show job 61
Job ID: 61
Date: 2005-08-16T16:14:27-0400
Type: Modify OS Monitoring Support
Status: Error (2005-08-16T16:14:38-0400)
Command: add server 192.168.2.10 feature osmonitor agentssh root/rootpasswd
Owner: root
Errors: 1
Warnings: 0

Steps
ID Type Start Completion Result
1 Acquire Host 2005-08-16T16:14:27-0400 2005-08-16T16:14:28-0400 Completed
2 Run Command 2005-08-16T16:14:28-0400 2005-08-16T16:14:28-0400 Completed
```

```
3 Acquire Host 2005-08-16T16:14:29-0400 2005-08-16T16:14:30-0400 Completed
4 Run Command 2005-08-16T16:14:30-0400 2005-08-16T16:14:36-0400 Error

Results
Result 1:
Server: 192.168.2.10
Status: -3
Message: Repeate attempts for this operation are not allowed.
```

This error indicates that SSH credentials have previously been supplied and cannot be altered. To avoid this error, issue the `add server feature osmonitor` command without `agentssh` credentials for instructions.

Use the `grep` command as follows to determine whether the OS monitoring agents were successfully installed.

- To verify the Solaris feature, type the following commands:

```
# pkginfo |grep n1sm

sparc:   SUNWn1smsparcag-1-2
solx86:  SUNWn1smx86ag-1-2
# ps -ef |grep -i esd
root 23817     1  0 19:57:59 ?       0:01 esd - init agent -dir
 /var/opt/SUNWsymon -q
```

- To verify the Linux feature, type the following commands:

```
# rpm -qa | grep n1sm-linux-agent

 # ps -ef | grep -i esd
 root 1940 1 0 Jan28 ? 00:00:14 esd - init agent -dir
 /var/opt/SUNWsymon -q
```

Downloading ALOM 1.5 Firmware Updates

This section provides detailed information to help you download and prepare the firmware versions that are required to discover Sun servers that use ALOM 1.5.

▼ To Download and Prepare ALOM 1.5 Firmware

1 Log in as root to the N1 System Manager management server.

The `N1–ok` prompt appears.

2. **Create directories into which the ALOM firmware update zip files are to be saved.**

   Create separate directories for each server type firmware download. For example:

   ```
   # mkdir ALOM-firmware
   ```

3. **In a web browser, go to** `http://jsecom16.sun.com/ECom/EComActionServlet?StoreId=8`**.**

   The downloads page appears.

4. **To download the ALOM 1.5 firmware zip file, log in and navigate to the ALOM 1.5, All Platforms/SPARC, English, Download.**

   Download the file to the directory you created for the ALOM firmware in Step 2.

5. **Change to the directory where you downloaded the ALOM firmware file and untar the file.**

   ```
   bash-3.00# tar xvf ALOM_1.5.3_fw.tar
   x README, 9186 bytes, 18 tape blocks
   x copyright, 93 bytes, 1 tape blocks
   x alombootfw, 161807 bytes, 317 tape blocks
   x alommainfw, 5015567 bytes, 9797 tape blocks
   ```

   The files are extracted.

Next Steps

- Copy the firmware updates to the N1 System Manager as described in "To Copy a Firmware Update" in *Sun N1 System Manager 1.3 Operating System Provisioning Guide*.
- Update the firmware on a single server or server group manageable server as described in "To Load a Firmware Update on a Server or a Server Group" in *Sun N1 System Manager 1.3 Operating System Provisioning Guide*.

Downloading V20z and V40z Server Firmware Updates

This section provides detailed information to help you download and prepare the firmware versions that are required to discover Sun Fire V20z and V40z servers.

▼ To Download and Prepare Sun Fire V20z and V40z Server Firmware

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

   The `N1–ok` prompt appears.

2. **Create directories into which the V20z and V40z firmware update zip files are to be saved.**

   Create separate directories for each server type firmware download. For example:

   ```
   # mkdir V20z-firmware V40z-firmware
   ```

3 In a web browser, go to `http://www.sun.com/servers/entry/v20z/downloads.html`.

The Sun Fire V20z/V40z Server downloads page appears.

4 Download the Sun Fire V20z Server 2.4.0.8 NSV patch file.

The download Welcome page appears. Type your username and password, and then click Login.

The Terms of Use page appears. Read the license agreement carefully. You must accept the terms of the license to continue and download the firmware. Click Accept and then click Continue.

The Download page appears. Several downloadable files are displayed.

5 To download the V20z firmware zip file, click V20z BIOS and SP Firmware, English (nsv-v20z-bios-fw_V2.4.0.8.zip).

Save the file to the directory that you created for the V20z firmware in Step 2.

6 To download the V40z firmware zip file, click V40z BIOS and SP Firmware, English (nsv-v40z-bios-fw_V2.4.0.8.zip).

Save the file to the directory you created for the V40z firmware in Step 2.

7 Change to the directory where you downloaded the V20z firmware file.

a. Type `unzip nsv-v20z-bios-fw_V2.4.0.8.zip` to unpack the zip file.

The `sw_images` directory is extracted.

The following files in the `sw_images` directory are used by the N1 System Manager to update V20z manageable server firmware:

- Service Processor:

  `sw_images/sp/spbase/V2.4.0.8/install.image`

- BIOS

  `sw_images/platform/firmware/bios/V1.34.6.2/bios.sp`

8 Change to the directory where you downloaded the V40z firmware zip file.

a. Type `unzip nsv-v40z-bios-fw_V2.4.0.8.zip` to unpack the zip file.

The `sw_images` directory is extracted.

The following files in the `sw_images` directory are used by the N1 System Manager to update V40z manageable server firmware:

- Service Processor:

  `sw_images/sp/spbase/V2.4.0.8/install.image`

- BIOS:

  `sw_images/platform/firmware/bios/V1.34.6.2/bios.sp`

Next Steps

- Copy the firmware updates to the N1 System Manager as described in "To Copy a Firmware Update" in *Sun N1 System Manager 1.3 Operating System Provisioning Guide*.
- Update the firmware on a single server or server group manageable server as described in "To Load a Firmware Update on a Server or a Server Group" in *Sun N1 System Manager 1.3 Operating System Provisioning Guide*.

Regenerating Common Agent Container Security Keys

This section provides the procedure for regenerating the N1 System Manager security keys.

▼ To Regenerate Common Agent Container Security Keys

1 Log in as root on the management server.

2 Stop N1 System Manager.

- On a Solaris management server, type **`svcadm disable -s n1sm`**.
- On a Linux management server, type **`/etc/init.d/n1sminit stop`**. Wait for all process to stop.

Wait for all process to stop before continuing.

3 Regenerate security keys using the `create-keys` subcommand.

If the management server is running Linux:

```
# /opt/sun/cacao/bin/cacaoadm create-keys --force
```

If the management server is running the Solaris OS:

```
# /opt/SUNWcacao/bin/cacaoadm create-keys --force
```

4 Restart the N1 System Manager.

- On a Solaris management server, type **`svcadm enable n1sm`**.
- On a Linux management server, type **`/etc/init.d/n1sminit start`**. Wait for all process to stop.

Resetting Email Accounts for ALOM-based Managed Servers

If you have configured a separate mail server and account for the N1 System Manager to receive hardware event notifications, and the N1 System Manager is not receiving hardware event notifications from ALOM architecture manageable servers, it is possible that:

1. The mail server is not configured correctly
2. The email configuration has been invalidated by a mail server IP address change
3. The email configuration has been invalidated by a mail server domain name change
4. The manageable servers email account has been compromised or corrupted.

To resolve issues 1 through 3, log on to the management server as root and run the command `n1smconfig -A` to start the email reconfiguration process, and then either:

- Configure N1 System Manager to use the secure N1 System Manager internal mail service instead of a separate mail service or server.
- If you are using an external mail service , configure the ALOM email alert settings as described in "To Configure the ALOM Email Alert Settings" on page 46

To resolve issue 4, proceed as described by "To Reset Email Accounts for ALOM-based Managed Servers" on page 47

▼ To Configure the ALOM Email Alert Settings

1 Log in as root to the management server management server.

2 Type `n1smconfig -A` to start the ALOM email alert settings configuration process.

You are notified that proper settings are required to send email alerts, and the existing values are displayed. You are then asked whether to modify the email alert settings.

3 Choose whether to modify the email alert settings.

- Type **`n`** to accept the displayed settings. The email alert configuration process exits to the system prompt.
- Type **`y`** to modify the email alert configuration.

  You are prompted for the email alert user name.

4 Specify the email alert user name.

Type the account name that is to be used for the email alerts.

For example: `n1smadmin`

You are prompted for the email alert folder.

5 Specify the email folder in which the email alerts are to be stored.

Type the name of an email folder for the alert account, for example, `inbox`

You are prompted for the email protocol

6 Specify the email alert protocol.

Type the name of the email protocol used by the management server. Valid entries are `pop3` or `imap`.

You are prompted for the email alert user account password.

7 Type the password for the email alert user account.

Type the password for the email alert user account.

You are prompted for the email alert user account email address.

8 Type the user account email address.

For example: `n1smadmin@company.com`

You are prompted for the IP address of the email server.

9 Specify the IP address of the email server.

- If you have installed and enabled an email server on the management server, type the IP address of the management server management network interface.
- If you have installed and enabled an email server on a different machine that is accessible by the management server management network interface, type the IP address of that machine.

The values you have specified are displayed, and you are asked whether you want to use the values.

10 Choose whether to accept the displayed email alert settings.

- Type **n** if the settings are not correct. The ALOM email alert settings process is restarted, and you are prompted to specify the email alert user name.
- Type **y** to use the displayed email alert settings.

  The settings are displayed again, and you are asked whether you want to apply the settings.

  Type **y** to apply the settings, or type **n** to exit to the command prompt.

▼ To Reset Email Accounts for ALOM-based Managed Servers

Before You Begin This procedure provides the steps required to replace a compromised or corrupt ALOM email account on a managed server. The ALOM email addresses should be reserved for use only by the N1 System Manager.

Confirm that the problem is related to the fact that email alerts are not being received for the server. It is possible that the management server, or some other chosen server that can be accessed by the N1 System Manager, has not been configured correctly as an email server, or that email configuration has been invalidated due to other issues such as network error or domain name change.

Before trying the following procedure, verify that email sent from the ALOM server can be received by the designated email server, by configuring an independent mail client, such as Mozilla, with the same mail server IP, username and password. Then use the `telnet` command to access an ALOM server, and execute the `resetsc -y` command to generate a warning message. Check if the mail client is able to receive the ALOM warning message. If it is, you do not need to follow this procedure.

See "SP-Based Discovery" in *Sun N1 System Manager 1.3 Discovery and Administration Guide* for information about default `telnet` login and passwords for servers.

Before trying the following procedure, verify also that the N1 System Manager has access to the designated email server by using the `telnet` command to access an ALOM server, and executing the `showsc` command. Make sure the following parameters/values are set as shown:

- The `if_emailalerts` value is set to `true`
- The `mgt_mailhost` variable is set to the designated mail server's IP address.
- The `mgt_mailalert(1)` variable is set to the email address to which alerts must be sent.

If you do not see these settings, or if you see incorrect values for the `mgt_mailalert` email address, follow this procedure.

1 Log in to the N1 System Manager.

See "To Access the N1 System Manager Command Line" in *Sun N1 System Manager 1.3 Discovery and Administration Guide* for details.

2 Switch off monitoring for ALOM-based manageable servers.

Set the `monitored` attribute to `false` by using the `set server` command.

```
N1-ok> set server server monitored false
```

In this example, *server* is the name of the ALOM-based manageable server for which you want to reset the email account. Executing this command disables monitoring of the server.

- **If the ALOM-based servers are in the same group, use the `set group` command to switch off monitoring for the server group.**

  ```
  N1-ok> set group group monitored false
  ```

  In this example, *group* is the name of the group of ALOM-based manageable servers for which you want to reset email accounts. Executing this command disables monitoring of the server group.

3 Change the email address for the server using the `n1smconfig` command with the `–A` option.

ALOM-based servers support email addresses of up to `33` characters in length.

Note – If you *manually configured* ALOM-based servers to send event notifications by email to other addresses, using the `telnet` command and the `setsc mgt_mailalert` command, those addresses will not be changed by running the `n1smconfig` command.

4 Switch on monitoring for the ALOM-based manageable server.

Set the `monitored` attribute to `true` by using the `set server` command.

```
N1-ok> set server server monitored true
```

- **If the ALOM-based servers are in the same group, use the `set group` command to switch on monitoring for the server group.**

  ```
  N1-ok> set group group monitored true
  ```

  In this example, *group* is the name of the group of ALOM-based manageable servers for which you want to reset email accounts. Executing this command enables monitoring of the server group.

Updating Management Server System Files

This section provides the procedures for configuring the management server system files.

▼ To Update the `/etc/hosts` File

1 Log in as root on the management server.

2 Edit `/etc/hosts` and ensure that the entries are similar to the following example:

```
# Do not remove the following line, or various programs
# that require network functionality will fail.
127.0.0.1           localhost
111.222.333.44      machine-name loghost
```

where *111.222.333.44* is the IP address of the N1 System Manager server, and *machine-name* is the name of the N1 System Manager management server.

For example, if the machine name is `n1manager`, and the assigned IP address for `eth0` is `129.123.111.12`, then the `/etc/hosts` file should contain the following settings:

```
# Do not remove the following line, or various programs
# that require network functionality will fail.
127.0.0.1          localhost.localdomain localhost
129.123.111.12     n1manager loghost
```

You must reboot the system after updating the `/etc/hosts` file.

▼ To Update the `ssh_known_hosts` File

The management server `/etc/opt/sun/n1gc/ssh_known_hosts` file contains the name, IP address, and encrypted access keys for SSH-accessible servers. A stale or obsolete entry for a server in the `/etc/opt/sun/n1gc/ssh_known_hosts` file prevents SSH access to that server. The solution is to remove the entry for server from the `/etc/opt/sun/n1gc/ssh_known_hosts` file as follows.

1. **Note the name and IP address of the inaccessible server.**
2. **Log in as root on the management server.**
3. **Edit the `/etc/opt/sun/n1gc/ssh_known_hosts` file and delete the entry for the inaccessible server.**

▼ To Update the `/etc/resolv.conf` File

- **Edit `/etc/resolv.conf` and ensure that the entries are similar to the following:**

  `nameserver` *server 1 IP address*
  `nameserver name` *server 2 IP address*
  `nameserver name` *server 3 IP address*
  `domain` *your-domain-name*
  `search` *your-domain-name*

  For example, assume the IP address of the first DNS server is 129.123.111.12, the second DNS server is 129.123.111.24, and the third DNS server is 129.123.111.36. If your company domain name is `mydomain.com`, then the `/etc/resolv.conf` file would contain the following lines.

```
nameserver 129.123.111.12
nameserver name 129.123.111.24
nameserver name 129.123.111.36
domain mydomain.com
search mydomain.com
```

▼ To Disable Managed Server Automatic Configuration

The following procedure disables the automatic configuration of manageable servers during discovery.

1. **Log in as root on the management server.**
2. **Edit the `/etc/opt/sun/n1gc/domain.properties` file and add the following line to the file:**

   `com.sun.hss.domain.internal.discovery.initializeDevice=false`

   The N1 System Manager system must be restarted for auto configuration disabling to take effect. Note that once auto configuration is disabled, any servers in a factory default state cannot be

discovered until their SSH and IPMI accounts are configured. For further information, see "Setting Up Manageable Servers" in *Sun N1 System Manager 1.3 Site Preparation Guide*.

Using a Managed Server to Patch OS Distributions

When you are using a patch server to perform the following tasks, you need to have root access to both the management server and the manageable server at the same time. For some tasks, you need to first patch the manageable server, then mount the management server and patch the distribution.

▼ To Patch a Solaris 9 OS Distribution by Using a Solaris 9 OS on an x86 Patch Server

This procedure describes how to patch a Solaris 9 OS distribution in the N1 System Manager. The steps in this procedure need to be performed on both the patch server and the management server. The patches described are necessary for the N1 System Manager to be able to provision Solaris OS 9 update 7 and below. This procedure is not required for Solaris OS 9 update 8 and above.

Consider opening two terminal windows to complete the steps. The following steps first guide you through patching the patch server and then provide steps for patching the distribution.

Before You Begin

- Create a Solaris 9 OS distribution on the management server. See "To Copy an OS Distribution From CDs or a DVD" in *Sun N1 System Manager 1.3 Operating System Provisioning Guide* or "To Copy an OS Distribution From ISO Files" in *Sun N1 System Manager 1.3 Operating System Provisioning Guide*. Type `show os os-name` at the command line to view the ID of the OS distribution. This number is used in place of *DISTRO_ID* in the instructions.
- Install the Solaris 9 OS on x86 platform software on a machine that is not the management server.
- Create a `/patch` directory on the Solaris 9 x86 patch server.
- For a Solaris OS on x86 distribution, download and unzip the following patches into the `/patch` directory on the Solaris 9 OS on x86 patch server: 117172-17 and 117468-02. You can access these patches from `http://sunsolve.sun.com`.
- For a Solaris OS on SPARC distribution, download and unzip the following patches into the `/patch` directory on the Solaris 9 OS on x86 patch server: 117171-17, 117175-02, and 113318-20. You can also access these patches from `http://sunsolve.sun.com`.

1 Patch the Solaris 9 OS on x86 patch server.

a. Log in as root.

```
% su
password:password
```

The root prompt appears.

b. Reboot the Solaris 9 patch server to single-user mode.

```
# reboot -- -s
```

c. In single-user mode, change to the patch directory.

```
# cd /patch
```

d. Install the patches.

```
# patchadd -M . 117172-17
# patchadd -M . 117468-02
```

Tip – Pressing Control+D returns you to multiuser mode.

---

2 Prepare to patch the distribution on the management server.

a. Log in to the management server as root.

```
% su
password:password
```

The root prompt appears.

b. Edit the `/etc/exports` file.

```
# vi /etc/exports
```

c. Change `/js *(ro,no_root_squash)` to `/js *(rw,no_root_squash)`.

d. Save and close the `/etc/exports` file.

e. Restart NFS.

```
# /etc/init.d/nfs restart
```

3 Patch the distribution that you copied to the management server.

a. Log in to the Solaris 9 patch server as root.

```
% su
password:password
```

The root prompt appears.

b. Mount the management server.

```
# mount -o rw management-server-IP:/js/DISTRO_ID /mnt
```

c. Install the patches by performing one of the following actions:

- **If you are patching an x86 distribution, type the following commands:**

```
# patchadd -C /mnt/Solaris_9/Tools/Boot/ -M /patch 117172-17
# patchadd -C /mnt/Solaris_9/Tools/Boot/ -M /patch 117468-02
```

- **If you are patching a SPARC distribution, type the following commands:**

```
# patchadd -C /mnt/Solaris_9/Tools/Boot/ -M /patch 117171-17
# patchadd -C /mnt/Solaris_9/Tools/Boot/ -M /patch 117175-02
# patchadd -C /mnt/Solaris_9/Tools/Boot/ -M /patch 113318-20
```

Note – You will receive a partial error for the first patch installation. Ignore this error.

d. Unmount the management server.

```
# unmount /mnt
```

4 Restart NFS on the management server.

a. Edit the `/etc/exports` **file.**

```
# vi /etc/exports
```

b. Change `/js *(rw,no_root_squash)` **to** `/js *(ro,no_root_squash).`

c. Restart NFS.

```
# /etc/init.d/nfs restart
```

NFS is restarted.

The Solaris 9 OS on SPARC distribution is ready for deployment to target servers.

5 Fix the Solaris 9 OS on x86 distribution.

a. Change to `/js/<distro_id>/Solaris_9/Tools/Boot/boot/solaris.`

```
# cd /js/<distro_id>/Solaris_9/Tools/Boot/boot/solaris
```

b. Re-create the `bootenv.rc` **link.**

```
# ln -s ../../tmp/root/boot/solaris/bootenv.rc .
```

The Solaris 9 OS on x86 distribution is ready for deployment to target servers.

Troubleshooting If you want to patch another distribution, you might have to delete the `/patch/117172-17` directory and re-create it using the `unzip 117172-17.zip` command. When the first distribution is patched, the `patchadd` command makes a change to the directory that causes problems with the next `patchadd` command execution.

This patch is not needed for the Solaris 9 update 8 build 5 OS and beyond. Versions of the Solaris OS from Solaris 9 9/05 `s9x_u8wos_05`, therefore, do not require this patch.

▼ To Patch a Solaris 9 OS Distribution by Using a Solaris 9 OS on a SPARC Patch Server

This procedure describes how to patch a Solaris 9 OS distribution in the N1 System Manager. The steps in this procedure need to be performed on the manageable server and the management server. Consider opening two terminal windows to complete the steps. The following steps first guide you through patching the manageable server and then provide steps for patching the distribution.

Before You Begin

- Create a Solaris 9 OS distribution on the management server. See "To Copy an OS Distribution From CDs or a DVD" in *Sun N1 System Manager 1.3 Operating System Provisioning Guide* or "To Copy an OS Distribution From ISO Files" in *Sun N1 System Manager 1.3 Operating System Provisioning Guide*. Type `show os os-name` at the command line to view the ID of the OS distribution. This number is used in place of *DISTRO_ID* in the instructions.
- Install the Solaris 9 OS on SPARC software on a machine that is not the management server. See "To Load an OS Profile on a Server or a Server Group" in *Sun N1 System Manager 1.3 Operating System Provisioning Guide*.
- Create a `/patch` directory on the Solaris 9 SPARC patch server.
- For a Solaris OS on x86 distribution, download and unzip the following patches into the `/patch` directory on the Solaris 9 OS on x86 patch server: 117172-17 and 117468-02. You can access these patches from `http://sunsolve.sun.com`.
- For a Solaris OS on SPARC distribution, download and unzip the following patches into the `/patch` directory on the Solaris 9 OS on x86 patch server: 117171-17, 117175-02, and 113318-20. You can access these patches from `http://sunsolve.sun.com`.

1 Set up and patch the Solaris 9 OS on SPARC machine.

a. Log in to the Solaris 9 machine as root.

```
% su
password:password
```

b. Reboot the Solaris 9 machine to single-user mode.

```
# reboot -- -s
```

c. In single-user mode, change to the patch directory.

```
# cd /patch
```

d. Install the patches.

```
# patchadd -M . 117171-17
# patchadd -M . 117175-02
# patchadd -M . 113318–20
```

Tip – Pressing Control+D returns you to multiuser mode.

2 Patch the distribution that you copied to the management server.

a. Log in to the Solaris 9 machine as root.

```
% su
password:password
```

b. Mount the management server.

```
# mount -o rw management-server-IP:/js/DISTRO_ID /mnt
```

c. Install the patches by performing one of the following actions:

- **If you are patching a Solaris OS on x86 software distribution, type the following commands:**

```
# patchadd -C /mnt/Solaris_9/Tools/Boot/ -M /patch 117172-17
# patchadd -C /mnt/Solaris_9/Tools/Boot/ -M /patch 117468-02
```

- **If you are patching a Solaris OS on SPARC software distribution, type the following commands:**

```
# patchadd -C /mnt/Solaris_9/Tools/Boot/ -M /patch 117171-17
# patchadd -C /mnt/Solaris_9/Tools/Boot/ -M /patch 117175-02
# patchadd -C /mnt/Solaris_9/Tools/Boot/ -M /patch 113318-20
```

Note – You will receive a partial error for the first patch installation. Ignore this error.

d. Unmount the management server.

```
# unmount /mnt
```

3 Restart NFS on the management server.

a. Edit the `/etc/exports` **file.**

```
# vi /etc/exports
```

b. Change `/js *(rw,no_root_squash)` **to** `/js *(ro,no_root_squash)`**.**

c. Restart NFS.

```
# /etc/init.d/nfs restart
```

NFS is restarted.

The Solaris 9 OS on SPARC distribution is ready for deployment to target servers.

4 Fix the Solaris 9 OS on x86 distribution.

a. Change to `/js/<distro_id>/Solaris_9/Tools/Boot/boot/solaris`**.**

```
# cd /js/<distro_id>/Solaris_9/Tools/Boot/boot/solaris
```

b. Re-create the `bootenv.rc` **link.**

```
# ln -s ../../tmp/root/boot/solaris/bootenv.rc .
```

The Solaris 9 OS on x86 distribution is ready for deployment to target servers.

Troubleshooting If you want to patch another distribution you might have to delete the `/patch/117172-17` directory and re-create it using the `unzip 117172-17.zip` command. When the first distribution is patched, the `patchadd` command makes a change to the directory that causes problems with the next `patchadd` command execution.

Index

S

T

U

V

W