Sun N1 System Manager 1.3.1 Troubleshooting Guide

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

Part No: 819–6531
July 2006

Contents

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 troubleshooting guidelines and information that you should consider about N1 System Manager that can assist you in troubleshooting.
- Chapter 2 describes problems that can occur during Sun N1 System Manager installation and configuration, their causes, and the solution for each problem.
- Chapter 3 describes problems that can occur during discovery of manageable servers, their causes, and the solution for each problem.
- Chapter 4 describes problems that can occur with manageable server firmware, their causes, and the solution for each problem.
- Chapter 5 describes the most common monitoring problems, their causes, and the solution for each problem.
- Chapter 6 describes problems that can occur with OS distribution creation and deployment, their causes, and the solution for each problem.

- Chapter 7 describes the most common OS update problems, their causes, and the solution for each problem.
- Chapter 8 describes the most common N1 System Manager problems, their causes, and the solution for each problem.
- Chapter 9 provides procedures that are used to resolve more than one N1 System Manager problem.

Related Documentation

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

- *Sun N1 System Manager 1.3.1 What's New*
- *Sun N1 System Manager 1.3.1 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 1.3.1 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*.
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

Guidelines and Considerations

This chapter provides troubleshooting guidelines and information that you should consider about N1 System Manager that can assist you in troubleshooting.

In this book, 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.

Troubleshooting Guidelines and Logs

This section provides generate trouble shooting guidelines.

Tip – Check this manual's index for specific topics and problems.

Installation

Examine the installation log `/var/tmp/installer.log.latest` to determine the cause of the installation failure. Resolutions for the majority of installation problems are provided in this guide.

Configuration

The N1 System Manager configuration utility `n1smconfig` does not generate logs. When `n1smconfig` is run, the current N1 System Manager configuration is displayed. Examine the displayed configuration and ensure that your N1 System Manager management network, provisioning network, and data network are assigned to the correct management server Ethernet ports. Also ensure that all other configuration settings are correct. If configuration needs to be corrected, reconfigure the N1 System Manager as described in "Configuring the N1 System Manager" in *Sun N1 System Manager 1.3 Installation and Configuration Guide*.

Runtime

To determine the cause of an error or a problem, first examine the following items:

- N1 System Manager event logs: Use the command `show log` *log* to display the N1 System Manager event logs. For further information, see "show log" in *Sun N1 System Manager 1.3 Command Line Reference Manual.*.
- Job details: Use the command `show job` to display the N1 System Manager jobs. For further information, see "show job" in *Sun N1 System Manager 1.3 Command Line Reference Manual*.
- Management server system logs: Operating system log locations are dependent on the operating system. Refer to your operating system documentation for the location of the system logs. For example, Solaris OS system logs are stored in the directory `/var/adm/messages`, and Linux system logs are stored in the directory `/var/log`.
- The Windows RIS server debug log `C:\WINDOWS\Debug\binlsvc.log` contains information that might be useful when debugging Windows deployment issues.

Considerations and Constraints

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

- "DHCP Service Conflict With N1 Grid Service Provisioning System" on page 12
- "Discovery and Routers" on page 13
- "Hot-Plugging Sun Blade 8000 Chassis Modules" on page 13
- "Identifying Hardware and OS Threshold Breaches" on page 13
- "N1 System Manager Cannot Be Used to Manage System Management Servers" on page 14
- "Regenerating Security Keys" on page 14

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.

For information about which ports and protocols can be configured, see Appendix A, "Sun N1 System Manager Protocol, Ports, and Features Reference," in *Sun N1 System Manager 1.3 Installation and Configuration Guide*.

Hot-Plugging Sun Blade 8000 Chassis Modules

Because the Sun Blade 8000 chassis systems support hot-pluggable I/O modules, the network boot device list reported by N1 System Manager might be stale if a Sun Blade X8400 Server Blade has not been reset for a very long time. If you select a blade for provisioning using a stale network boot device list and you specify a logical interface using the `load server` command or use the `load server` command defaults, then the interface might not map to the expected physical port. Provisioning will fail if the interface you specify does not map to the correct physical port.

Use either of the two following methods to ensure mapping to proper physical port.

- Best practice: When using the `load server` command to provision a blade, always explicitly specify a physical interface name for the `bootnetworkdevice` and `networkdevice` options. For further information about these options, see Chapter 3, "Provisioning Sun Blade X8400 Server Modules in the Sun Blade 8000 Chassis," in *Sun N1 System Manager 1.3.1 What's New* and "load server" in *Sun N1 System Manager 1.3 Command Line Reference Manual*
- Refresh the network boot device list as follows using either the `n1sh` shell or the N1 System Manager browser interface command line pane.
  1. Type **`reset server`** *server* where *server* is the blade that is to be provisioned.
  2. Type **`set server`** *server* **`refresh`** to refresh the network boot device list.
  3. Type **`show server`** *server* to display the server information.
  4. Choose the logical interface name based on the boot device list shown when using the `load server` command. If you do not specify any options, the first entry in the boot list is used.

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. The event log 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. Because the management server date is out of synchronization, N1 System Manager services might not 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 58.

CHAPTER 2

Installation and Configuration Problems

This chapter lists Sun N1 System Manager problems that can occur during installation and configuration, their causes, and the solution for each problem. The following topics are discussed:

Checkinstall Script Did Not Complete Successfully

If you use the command **`su`** instead of **`su - root`** to log in to the management server to run N1 System Manager installation, the `checkinstall` process will fail. The following message is displayed:

```
/tmp/bm122834/installm1a4XN/checkinstallp1a4XN: /tmp/bm122834/installm1a4XN/checkinstallp1a4XN: cannot open
pkgadd: ERROR: checkinstall script did not complete successfully
```

Always use the command **`su - root`** when instructed to log in as root. The `su` command does not provide the full system `root` account environment, path, and privileges.

Command failed for target 'Makefile'

If the management server system date is incorrect, N1 System Manager installation will fail. The following message is written to the installation log file `/var/tmp/installer.log.lates`:

```
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'
```

Set the management server system date and rerun the N1 System Manager install.

DHCP Startup Failed

If N1 System Manager has not been configured, DHCP will not start. The error message `Starting dhcpd: [Failed]` is displayed during management server reboot.

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*.

Error Waiting for *Component* To Start

If the management server `/etc/hosts` file does not contain a domain name for the management server, or contains an incorrect domain name, then N1 System Manager components will fail to start. The following message is displayed:

```
Error waiting for component to start
```

where *component* is the name of the N1 System Manager component that failed to start.

Update the `/etc/hosts` file as described in “To Update the `/etc/hosts` File” on page 62.

HTTPD Cannot Determine Server’s Domain Name

If the management server `/etc/resolve.conf` file is not configured correctly, then N1 System Manager cannot start HTTPD services. The following message is displayed:

```
[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..
```

Update the `/etc/resolv.conf` file as described in “To Update the `/etc/resolv.conf` File” on page 63.

HTTPS Connection to the Management Server Is Refused

If the management server file `/etc/resolve.conf` is not configured correctly, any attempt to connect to themanagement server web server using the URL format `https://`*management-server-name* will fail and display the following error message.

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

Update the `/etc/resolv.conf` file as described in "To Update the `/etc/resolv.conf` File" on page 63.

Management Server IP Address Resolves to 127.0.0.1

If the `/etc/hosts` file does not contain an IP address and server name assignment for the management server, the management server IP address will resolve to 127.0.0.1. Assign the management server IP address and name as described in "To Update the `/etc/hosts` File" on page 62.

◆ ◆ ◆ CHAPTER 3

Discovery Problems

This chapter lists Sun N1 System Manager problems that can occur during discovery of manageable servers, their causes, and the solution for each problem. The following topics are discussed:

- "Cannot Discover a Manageable Server" on page 19
- "Unable to Log In to a Managed Server Management Processor" on page 22

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:

- "Incorrect Firmware Is Installed on the Managed Server" on page 19
- "Maximum Number of SNMP Destinations Has Been Exceeded" on page 20
- "RSC Servers Must Be Powered Off for Discovery to Succeed" on page 20
- "V20z or V40z Discovery Fails With `Error Cannot Open IPMI Session`" on page 21

Incorrect Firmware Is Installed on the Managed Server

The managed server firmware version might be less than the minimum supported version.

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 Destinations Has Been Exceeded

The service processor of the Sun Fire V20z and V40z servers has a limit of three SNMP destinations. If there are more than three SNMP destinations for a V20z or a V40z server, 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.

Perform the following steps to view the service processor SNMP destinations and then delete at least one SNMP destination:

1. Log into the V20z or V40z service processor `admin` account using SSH.
2. To display the server's current SNMP destinations, type the command **`sp get snmp-destinations`**.

   The SNMP destinations appear in the output.

   If there are more than three SNMP destinations, you must delete SNMP destinations until there are no more than three SNMP destinations.
3. To delete an SNMP destination on the service processor, use the command **`sp delete`** *snmp-destination* where *snmp-destination* is the SNMP destination to be deleted..

   Use the delete command with caution because some other management software might 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. Always use the `delete server` command when removing a manageable server.

RSC Servers Must Be Powered Off for Discovery to Succeed

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-based 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 cannot be 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.

V20z or V40z Discovery Fails With `Error Cannot Open IPMI Session`

Discovery cannot open an IPMI session to a Sun Fire V20z or a V40z server if the IPMI password on the V20z or V40z is missing or has been reset.

To reset the IPMI password and then discover the server, proceed as follows:

1. Open a terminal window and log in to the V20z or V40z service processor admin account using SSH.
2. Type the command **ipmi get channels** followed by the command **ipmi reset -a** to reset the IPMI password. You are prompted to confirm the new password.

   For example, assume the server management processor IP address is *10.0.5.3*, and that the default `ssh` account name `admin` and the default password `admin` have not been changed:

   ```
   bash-3.00# ssh -l admin 10.0.5.3
   admin@10.0.5.3's password:

   Sun Microsystems
   IPMI v2.0 Service Processor

   Version:  V2.4.0.6
   localhost $
   localhost $ ipmi get channels
   Channel Status
   lan     enabled
   sms     enabled
   localhost $ ipmi reset -a
   localhost $
   localhost $ ipmi enable channel lan
   Password: example
   Confirm password: example
   ```
3. Rerun discovery from the N1 System Manager commandline interface for the V20z or V40z, using the IPMI password you specified.

For example:

```
N1-ok > discover 10.0.5.3 ssh=admin/admin ipmi=/example
```

Unable to Log In to a Managed Server Management Processor

If the service processor account and password are not known, reset the service processor accounts to the factory defaults as described by the hardware documentation.

CHAPTER 4

Managed Server Firmware Problems

This chapter lists problems that can occur with manageable server firmware, their causes, and the solution for each problem. The following topics are discussed:

- "Cannot Determine the Firmware Version on a Managed Server" on page 24
- "Exception Occurs When Updating Sun Fire V20z Firmware" on page 25
- "Firmware Update for a Sun Fire V20z or Sun Fire V40z Fails" on page 25

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. If it has been set, see 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 described in 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*.

  If you cannot access the management processor, reset the manageable server to the factory defaults as described in 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, 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 described in the server's hardware documentation. For example, to view all of the firmware for an ALOM-enabled server, log in to 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 described in the hardware documentation.

Exception Occurs When Updating Sun Fire V20z Firmware

Starting with Sun Fire V20z Firmware Version 2.2, the firmware versions do not support the PIC firmware upgrade. The upgrade of PIC firmware will fail, and the job step will show the following error message.

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

When updating Sun Fire V20z firmware, do not load PIC firmware to the Sun Fire V20z servers.

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

If the Auto-negotiate link speed feature on the management network switch has not been enabled for all management network connections, V20z and V40z firmware updates will fail. Refer to your switch documentation and enable the auto-negotiate link speed feature.

CHAPTER 5

Monitoring Problems

This chapter describes the most common monitoring problems, their causes, and the solution for each problem. The following topics are discussed:

Adding OS Monitoring to a Managed Server On Which Base Management is Installed Fails

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 OS 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
  ```

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

To resolve, do one of the following:

- 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 58

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 managed server. Remove the entry for that server as described in "To Update the `ssh_known_hosts` File" on page 63.

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 10 minutes, a transient network problem might be occurring. However if the status remains `unknown` or `unreachable` for more than 30 minutes, monitoring might have failed. This failure 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 whether a problem exists 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 in the `known_hosts` file on the management server. 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` file as described in "To Update the `ssh_known_hosts` File" on page 63. Then, retry the `add` command.

Sun Blade X8400 Server Blade is not Displayed In Its Chassis Group and is Displayed as a Separate Managed Server

Under certain circumstances, a Sun Blade X8400 server blade will not be listed in its chassis group, but will be listed as a separate managed server with the status `unreachable`.

This problem can be caused by any one or more of the following situations:

- The Sun Blade X8400 server blade has been removed from the Sun Blade X8000 chassis
- The Sun Blade X8400 server blade SP is not accessible by N1 System Manager due to SP problems, IP address reassignment, or other management network problems

To resolve this problem:

- Ensure the IP address assigned to the Sun Blade X8400 server blade is correct.
- Ensure that the Sun Blade X8400 server blades can be accessed using `ssh`.
- Physically check the blade, and if necessary, power cycle the blade SP. If the blade SP has hung, you will need to go to the blade to power cycle the SP.

After you have verified that the Sun Blade X8400 server blade is accessible using N1 System Manager and standard access protocols, refresh the server blade using either of the following two methods:

- Type **`set server`** *server id* **`refresh`** in the N1 System Manager browser interface command line prompt where *server id* is either the Sun Blade X8400 server blade IP address or the name you have assigned to the Sun Blade X8400 server blade.
- Type **`n1sh set server`** *server id* **`refresh`** in a root login terminal window on the management server where *server id* is either the Sun Blade X8400 server blade IP address or the name you have assigned to the Sun Blade X8400 server blade.

CHAPTER 6

OS Distribution and Deployment Problems

This chapter lists problems that can occur with OS distribution creation and deployment, their causes, and the solution for each problem. OS distribution creation and OS deployment failures can be caused by many different issues as described in this section. 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 "RSC Servers Must Be Powered Off for Discovery to Succeed" on page 20.
- 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 OS Deployment Job Times Out or Stops" on page 39.
- OS profiles that install only the Solaris OS Core System Support will fail to deploy. The entire Solaris OS distribution must be deployed.See "Solaris OS Profile Installation Fails" on page 39.
- The target server cannot access DHCP information or mount distribution directories. See "Invalid Management Server Netmask" on page 34.
- The management server cannot access files during a Load OS operation. See "Restarting NFS to Resolve `Boot Failed` Errors" on page 38.
- The Linux OS deployment stops. See "Linux OS Deployment Stops" on page 35.
- The Red Hat OS deployment fails. See "Red Hat Linux OS Profile Creation Fails" on page 38.
- If OS deployment still fails, the problem might be the managed server. Perform the following steps to troubleshoot the managed server.

  Refer to the managed server documentation for the server-specific access methods and BIOS access commands.

  1. Access the service processor of the managed server by using Telnet, SSH, or by opening the serial console.
  2. Access the managed server BIOS. The command used to access the server BIOS depends on the type of server and its service processor type.
  3. Enter the BIOS command required to power-cycle the managed server. Make sure that the power-on self test completes correctly, and that the Preboot Execution Environment (PXE) boot starts.
  4. Check whether the OS profile specifications for disk partitions, resources, and scripts are configured correctly.
  5. Redeploy the OS distribution to the managed server and monitor the deployment process.
  6. Verify whether the deployment was successful by listening for DHCP broadcasts from the managed server ETH0 and ETH1 ports by doing a network packet dump using the operating system specific tools such as `snoop`, `tcpdump`, or `ethereal`.

Possible Causes for Windows Distribution and Deployment Failure

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 63.
- 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 the Linux OS 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 managed server's disk.
- The operating system name has to be exactly the name given when using the `risetup.exe` command. For example, `D:\RemoteInstall\Setup\English\Images\`*OS-name* where *OS-name* is the name of the OS.

  The OS architecture type must be specified correctly. For example, a 64–bit OS image should be stored in the RIS server directory `D:\RemoteInstall\Setup\English\Images\`*OS-name*`\amd64`.
- You created the directory `C:\N1SM` already exists on the RIS server before running `n1smconfig`, and `n1smconfig` displays the error `INFO : Error when trying to configure RIS server`. To resolve this issue, log in to the RIS server and delete the `C:\N1SM` directory, then run `n1smconfig` again. The `C:\N1SM` directory is created on the RIS server by `n1smconfig`.
- You have upgraded from N1 System Manager 1.3 to N1 System Manager 1.3.1. Delete and re-add the RIS server as described in "Windows Deployment Fails after Upgrade from N1 System Manager 1.3 to 1.3.1" on page 40.

Deploying Solaris OS 9 Update 7 or Previous Distributions From a Linux OS Management Server Fails

The inability to deploy Solaris OS 9 Update 7 and previous Solaris OS 9 distributions to manageable servers from a Linux OS 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 OS 9 distribution. The instructions differ according to the management and patch server configuration scenarios listed in the following table. The patch is not required if you are deploying Solaris OS 9 Update 8 or later.

TABLE 6–1 Task Map for Patching a Solaris OS 9 Distribution

Management Server	Patch Server	Task
Red Hat 3.0 u2	Solaris OS 9 on x86 platform	"Creating and Using a Solaris OS 9 x86 Patch Server to Patch Solaris OS 9 Update 7 Distributions" on page 64
Red Hat 3.0 u2	Solaris OS 9 on SPARC platform	"Creating and Using a Solaris OS 9 SPARC Patch Server to Patch Solaris OS 9 Update 7 Distributions" on page 68

Invalid Management Server Netmask

If the target server cannot access DHCP information or mount the distribution directories on the management server during a Solaris OS 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*.

Linux OS Deployment Stops

If you are deploying a Linux OS and the deployment stops, check the console of the target server to see whether 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, a problem might exist with your network.

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

Management Server Reboots During `load os` Operations

If the IP address range specified for discovery includes the management server IP addresses, and the management server service processor port is connected to the management network, the discovery process discovers the management server. Subsequently, it is possible that a `load os` operation that includes the discovered management server will attempt to load an OS to the management server, thus causing the management server to reboot.

Solution:

1. Disconnect the management server's service processor port from the management network.
2. Delete the management server from the list of discovered servers in N1 System Manager.

Mount Point Issues

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

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

If OS deployment fails on a Sun Fire V20z or a V40z server 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 be directed to the service processor, reboot the service processor. To reboot the service processor, log in to the service processor and run the `sp reboot` command.

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

OS Deployment Fails on a Sun Blade X8400 Server Blade That Has Correct Firmware

Provisioning an OS distribution to a Sun Blade™ X8400 server blade will fail if the following conditions are met:

- You specify only the `bootnetworkdevice` or the `networkdevice` option when using the `load server` command
- The `bootnetworkdevice` or the `networkdevice` value you have specified maps to a port other than `e1000g0` when deploying a Solaris OS distribution, or to a port other than `eth0` when deploying a Linux OS distribution.

To provision an OS distribution to a Sun Blade X8400 server blade, use either of the following two methods:

- Explicitly state both the `bootnetworkdevice` and the `networkdevice` options when using the `load server` command
- Do not specify either the `bootnetworkdevice` or the `networkdevice` options, thereby accepting the default network boot options

For further information about the `bootnetworkdevice` and the `networkdevice` options, see Chapter 3, "Provisioning Sun Blade X8400 Server Modules in the Sun Blade 8000 Chassis," in *Sun N1 System Manager 1.3.1 What's New*

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 example 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*.

Red Hat Linux OS Deployment Fails on a Sun Blade X8400 Server Blade With Factory-Default Firmware or After a Firmware Update

Linux OS deployment fails after some Sun Blade X8400 server blade BIOS firmware upgrades and on factory default blades. Some BIOS firmware upgrades may cause CMOS checksum errors, prompting you to restore the default CMOS settings after the server blade resets. The default BIOS settings will not work with Linux.

To resolve this problem:

1. Connect to the server blade service processor by either logging directly into the SP, or by using `connect server` from the N1 System Manager browser interface.

2. Press F2 during the boot sequence to enter the BIOS setup.
3. Press F9 to load the optimal defaults.
4. Navigate to Advanced settings.
   a. Choose ACPI Configuration.
   b. Choose Advanced ACPI Configuration.
   c. Set `ACPI MCFG Table Select:` to `No`.
5. Navigate back to Advanced settings.
6. Set `AMD PowerNow Select` to `Enabled`.
7. Press F10 to save the settings and reboot.

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 in to 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.

Restarting NFS to Resolve `Boot Failed` Errors

`Boot Failed` messages occur when the management server cannot access files during a Load OS operation, and appear similar to the following example.

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

Note – The message differs depending on the OS that is being deployed.

Stale NFS file handles are the most common cause of this problem. Log in to the management server as root (**`su - root`**) and restart NFS.

- On a Solaris OS management server, type **`svcadm nfs restart`**
- On a Linux OS management server, type **`/etc/init.d/nfs restart`**

Solaris OS 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 erroneous network interface connection entries, which can occur if incorrect information is specified during the N1 System Manager configuration process.

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, perform the following steps to modify the configuration.

1. Log in to the management server as root (**`su - root`**).
2. Inspect the `dhcpd.conf` file for errors.
3. If errors exist that need to be corrected, stop N1 System Manager and rerun the configuration process as described in "Configuring the N1 System Manager" in *Sun N1 System Manager 1.3 Installation and Configuration Guide*. Ensure that you specify the correct management server Ethernet port for the N1 System Manager management network and provisioning network.
4. When the configuration process has completed and N1 System Manager has restarted, 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. This setting 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.

SuSE OS Profile Fails to Load on a Sun Fire V20z or Sun Fire V40z

Loading a SuSE OS profile on a Sun Fire X4000 series server modifies the associated SuSE OS distribution, which makes the SuSE OS distribution unusable by Sun Fire V20z and V40z servers.

To avoid this problem, you must create separate SuSE Linux Enterprise Server 9 OS and SuSE Linux Enterprise Server 9 SP1 OS distributions profiles for the Sun Fire V20z and V40z servers, and for the Sun Fire X4000 series servers.

Windows Deployment Fails after Upgrade from N1 System Manager 1.3 to 1.3.1

The N1 System Manager 1.3 to 1.3.1 does not upgrade the scripts and drivers in the Windows RIS server `C:\N1SM` directory. To upgrade the RIS server for N1 System Manager 1.3.1 you must perform the following tasks:

1. Delete the `C:\N1SM` directory on the RIS server
2. Delete the RIS server from N1 System Manager
3. Re-add the RIS server to N1 System Manager

The following procedure provides the specific steps required to update the RIS server for N1 System Manager 1.3.1.

▼ To Update the RIS Server After Upgrading to N1 System Manager 1.3.1

1 **Log in to the RIS server using an account with administrative privileges.**

Delete the `C:\N1SM` directory.

If you specified a different file directory on the RIS server when running N1 System Manager 1.3 `n1smconfig`, delete that directory.

The `C:\N1SM` will be recreated on the RIS server when you re-add the RIS server to N1 System Manager.

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

3 **Delete the RIS server from N1 System Manager as follows.**

a. **Type `n1smconfig`.**

The current N1 System Manager configuration is displayed.

Tip – Print the current configuration to use as reference in the following steps.

You are notified that only options that can be changed will be displayed.

b. **Type y to continue.**

Respond to each prompt as appropriate for your network and N1 System Manager configuration.

c. **Type `y` when prompted** `Add, Delete, or Modify Windows RIS server? ([n]/y)`

The current RIS server configuration is displayed again, for example:

```
Add, Delete, or Modify Windows RIS server? ([n]/y) y
CURRENT RIS Servers:
ID: 1
        Name: default
        HostName:
        IP: 192.168.0.100
        Subnet_Address: 192.168.0.0
        OSP_Location: C:\\\\N1SM
        RIS_Share_Path: D:\\RemoteInstall
        Active_dir_domain: mularis.sfbay.sun.com
        Active_dir_user: n1smuser
        ssh_user: n1smuser

Delete this RIS server? ([n]/y)
```

d. **Type y to delete the RIS server from N1 System Manager.**

Respond to the remaining prompts as appropriate for your network and N1 System Manager configuration.

4 **Add the RIS server to N1 System Manager as follows.**

a. **Type `n1smconfig`.**

The current N1 System Manager configuration is displayed.

You are notified that only options that can be changed will be displayed.

b. **Type y to continue.**

Respond to each prompt as appropriate for your network and N1 System Manager configuration.

c. **Type `y` when prompted** `Add, Delete, or Modify Windows RIS server? ([n]/y).`

Respond to each prompt, specifying the values that were displayed in Step 3 substep Step a.

After RIS server configuration is completed, respond to the remaining prompts as appropriate for your network and N1 System Manager configuration.

CHAPTER 7

OS Update Problems

This chapter describes the most common OS update problems, their causes, and the solution for each problem. The following topics are discussed:

OS Update Creation Fails

The file name that is specified when you create a new OS update must be unique. The combination of the internal package name, version, release, and file name that make up the OS update 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, a later attempt to uninstall the OS update will fail. See "OS Update Uninstall on a Managed Server Fails" on page 44.

The default `admin` file setting used for Solaris OS 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 OS system to view the man page.

For Solaris OS 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*.

OS Update Uninstall on a Managed Server Fails

If you cannot uninstall an OS update that was installed on a managed server using an `adminfile`, the package file name does not match the name of the package. Log in to the managed server and use the `pkginfo` command to display the package name, and compare the package name to the name of the package file.

For example:

```
# ls package file name
   package-file-name
   # pkginfo -d ./package-file-name
   application package-name        package-information
   # pkginfo -d ./package-name | /usr/bin/awk '{print $2}'
   package-name
---
   # cp package-file-name  new-file-name
   # pkginfo -d ./new-file-name
   application package-name        package-information
   5# pkginfo -d ./new-file-name | /usr/bin/awk '{print $2}'
   package-name
```

If the name of the package file is not the same as the package name , 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`.

Solaris OS Update Deployment Failures

This section provides solutions for the following categories of failures that can occur during Solaris OS update deployment:

- "Failures That Occur Before the Job is Submitted" on page 45
- "Load Update Job Failures" on page 45
- "Unload Update Job Failures" on page 46
- "Stop Job Failures for Load and Unload Update" on page 46
- "Unload Server and Unload Group Failures" on page 47

Failures That Occur Before the Job is Submitted

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

`Target server is not initialized`

Solution: Check whether 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 whether 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 whether 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.

Load Update Job Failures

The following are possible causes for Load Update job failures:

`error: Failed dependencies:`

`A prerequisite package should be installed`

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

Solution: For a Solaris OS 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 preinstallation or postinstallation 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.

Unload Update Job Failures

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

```
N1-ok> unload server server update update
```

Always check whether the package is targeted to the correct architecture.

Note – The N1 System Manager does not distinguish 32-bit from 64-bit for the Solaris OS on either the x86 or SPARC platforms, 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 whether the architecture of the patch matches the architecture of the OS. 32–bit packages will run under a 64–bit operating system, but this mismatch will decrease performance.

Stop Job Failures for Load and Unload Update

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

If you stop a Load Update or Unload Update job and the job does not stop, manually ensure that the following processes are 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:

Unload Server and Unload Group Failures

The following are possible causes for failures related to the 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 OS 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 uninstall 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, type **`n1sh stop job`** *job-ID* to stop the job.

Next, find the PID of the PKG and use the `pkill` command to kill the process. For example:

```
# ps -ef |grep pkgadd
root 1235 913 0 Jun 07 ? 0:0 pkgadd
# pkill 1235
```

Last, run the `unload` command again.

Linux OS Update Deployment Failures

This section provides solutions for the following categories of failures that can occur during Linux OS update deployment:

Failures that Occur Before the Job is Submitted

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

`Target server is not initialized`

Solution: Check whether the `add server feature osmonitor` command was issued and whether 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 whether 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 whether 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.

Load Update Job Failures

The following are possible causes for Load Update job failures:

`error: Failed dependencies:`

`A prerequisite package should be installed`

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

Solution: Use an RPM tool to address and resolve Linux OS RPM dependencies.

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

`ERROR: ... script did not complete successfully`

Solution: Check the preinstallation or postinstallation 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.

Unload Update Job Failures

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

```
N1-ok> unload server server update update
```

Stop Job Failures for Load and Unload Update

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, ...
```

Unload Server and Unload Group Failures

The following are possible causes for failures related to the 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 uninstall 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, type **`n1sh stop job`** *job-ID* to stop the job.

Next, find the PID of the RPM and use the `pkill` command to kill the RPM process. For example:

```
# ps -ef |grep rpm-name
root 1235 913 0 Jun 07 ? 0:0 rpm-name
# pkill 1235
```

Then run the `unload` command again.

CHAPTER 8

N1 System Manager Problems

This chapter describes the most common N1 System Manager problems, their causes, and the solution for each problem. The following topics are discussed:

- "N1 System Manager Services Do Not Start After Reboot or Restart" on page 51
- "Management Features Unavailable on Managed Servers After Rebooting" on page 51
- "Job IDs are Missing After Power Cycling the Management Server" on page 52
- "Solaris OS Management Server Unable To Start Jobs" on page 52

N1 System Manager Services Do Not Start After Reboot or Restart

If you reboot the management server, or if you stop and restart the N1 System Manager, and the services do not start, you must regenerate security keys as described in "Regenerating Security Keys" on page 14.

Management Features Unavailable on Managed Servers After Rebooting

When the `load server` or `load group` command is used to install software on the managed server, the managed 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` command, then the following features might 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.

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 gap can occur due to a power loss, or if the management server was manually power cycled.

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

Solaris OS Management Server Unable To Start Jobs

If `IPv6` is enabled on a Solaris OS Management Server, N1 System Manager jobs will not start, and the n1sh user interface is not available. `IPv6` must be disabled for N1 System Manager to function correctly. Perform the following procedure to ensure that `IPv6` is disabled.

▼ To Disable `IPv6` on a Solaris OS Management Server

1 **Log in to the management server as root (`su - root`).**

2 **Type `ifconfig -a6` to determine whether `IPv6` is enabled.**

The `IPv6` status is displayed. If `IPv6` is enabled, the status contains the text `UP` and `RUNNING`. For example:

```
# ipconfig -a6
lo0: flags=2000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv6> mtu 8252 index 1
        inet6 ::1/128
eri0: flags=2000841<UP,RUNNING,MULTICAST,IPv6> mtu 1500 index 2
```

3 Disable IPv6

To disable IPv6, you must rename the IPv6 interface files in the /etc directory and then reboot the system as follows.

a. Type `ls /etc/hostname6.*` to list the IPv6 interfaces. For example:

```
# ls /etc/hostname6.*
/etc/hostname6.eri0 /etc/hostname6.eri1  /etc/hostname6.eri2
```

b. For each file listed in Step a, rename the file as follows:

```
# mv /etc/hostname6.interface  disabled./etc/hostname6.interface
```

where *interface* is the interface used such as eri0, lo0, bge0 and so on.

4 Reboot the management server.

CHAPTER 9

Common Procedures

This section provides procedures that are used to resolve more than one N1 System Manager problem.

The following topics are discussed:

- "Downloading ALOM 1.5 Firmware Updates" on page 55
- "Downloading V20z and V40z Server Firmware Updates" on page 56
- "Regenerating Common Agent Container Security Keys" on page 58
- "Resetting Email Accounts for ALOM-based Managed Servers" on page 58
- "Updating Management Server System Files" on page 62
- "Using a Managed Server to Patch Solaris OS 9 Distributions" on page 64

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 (`su - 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 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 unpack 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 (`su - 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 and 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 and 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 (`su - root`) on the management server.**

2 **Stop N1 System Manager.**

- On a Solaris OS 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 processes 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 OS management server, type **`svcadm enable n1sm`**.
- On a Linux management server, type **`/etc/init.d/n1sminit start`**.

  Wait for all processes 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, the following problems might exist:

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

To resolve the first three issues, log in to the management server as root (**su - root**) and run the command `n1smconfig -A` to start the email reconfiguration process. Then do one of the following actions:

- 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 59

To resolve the last issue, proceed as described by "To Reset Email Accounts for ALOM-based Managed Servers" on page 61

▼ To Configure the ALOM Email Alert Settings

1 **Log in as root (`su - 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 **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 **Type the name of an email folder for the alert account, for example,** `inbox`**.**

You are prompted for the email protocol

6 **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.**

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 Verify ALOM Server Email

This procedure provides the steps required to determine why ALOM server email alerts are not received by N1 System Manager. Failure to receive email alerts from ALOM servers might be caused by the following problems:

- The management server, or some other chosen server that can be accessed by the N1 System Manager, might not been configured correctly as an email server
- Email configuration has been invalidated due to other issues such as network error or domain name change

1 Verify that email sent from the ALOM server can be received by the designated email server.

Configure an independent mail client, such as Mozilla, with the same mail server IP, username and password.

2 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 reset the email accounts for the server.

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.

3 Verify that the N1 System Manager has access to the designated email server.

Use the `telnet` command to access an ALOM server, and execute the `showsc` command. Make sure the following parameters and values are set as shown:

- `if_emailalerts` value is set to `true`
- `mgt_mailhost` variable is set to the designated mail server's IP address.
- `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, reset the email account as described in "To Reset Email Accounts for ALOM-based Managed Servers" on page 61.

▼ To Reset Email Accounts for ALOM-based Managed Servers

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.

Before You Begin Confirm that the problem is related to the fact that email alerts are not being received for the server as described in "To Verify ALOM Server Email" on page 60.

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.

- **For an individual server, 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.**

- **For an individual 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 (`su - 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 (`su - 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 (`su - 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 Solaris OS 9 Distributions

Solaris OS 9 update 7 or earlier distributions on the management server must be patched before being deployed to manageable servers. The patches described are necessary to enable N1 System Manager to provision Solaris OS 9 update 7 and earlier versions to managed server. The procedures in this section are not required for Solaris OS 9 update 8.

To patch your Solaris OS 9 update 7 or earlier distributions, you first create either an x86 based or SPARC based Solaris 9 patch server using an available managed server. You then use the patch server to patch your Solaris 9 update 7 distributions on the management server, after which you can provision the patched distributions to managed servers.

This section provides the procedures for creating and using a patch server to patch your Solaris OS 9 update 7 or earlier distributions. The following topics are discussed:

- "Creating and Using a Solaris OS 9 x86 Patch Server to Patch Solaris OS 9 Update 7 Distributions" on page 64
- "Creating and Using a Solaris OS 9 SPARC Patch Server to Patch Solaris OS 9 Update 7 Distributions" on page 68

Note – The procedures in this section require that you have created at least one Solaris OS 9 update 7 or earlier distribution on the management server. For instructions on how to create an OS distribution, 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*.

Creating and Using a Solaris OS 9 x86 Patch Server to Patch Solaris OS 9 Update 7 Distributions

This section provides the procedures for creating a Solaris OS 9 x86 patch server, and then using the patch server to patch the Solaris OS 9 distributions on the management server. The following topics are discussed:

- "To Create a Solaris OS 9 x86 Patch Server" on page 65
- "To Patch the Solaris x86 OS on the Patch Server" on page 65
- "To Configure and Restart NFS on the Management Server" on page 66
- "To Patch the Solaris OS 9 Distribution on the Management Server" on page 66
- "To Reconfigure and Restart NFS on the Management Server" on page 67
- "To Update the Solaris 9 x86 OS Distribution `bootenv.rc` File" on page 67

Caution – The procedures are sequentially dependent, and must be followed in the above order.

▼ To Create a Solaris OS 9 x86 Patch Server

Before You Begin At least one Solaris OS 9 update 7 or earlier distribution on the management server. For instructions on how to create an OS distribution, 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*

1. **Select an unused x86 managed server to become the x86 patch server.**

   The following steps refer to the selected managed server as the x86 patch server.

2. **Install the Solaris x86 OS on the x86 patch server.**

   If the OS distribution to be provisioned is Solaris x86 OS 9 update 7, then install Solaris x86 OS 9 update 7 on the x86 patch server.

   If the OS distribution is a version earlier than Solaris x86 OS 9 update 7, then install that version of the Solaris OS on the x86 patch server.

3. **Log in as root (`su - root`) to the x86 patch server.**

4. **Create a `/patch` directory on the x86 patch server.**

5. **Download and unzip the patches from `http://sunsolve.sun.com` to the `/patch` directory on the x86 patch server as follows:**

   - **For a Solaris OS 9 on x86 distribution, download and unzip the following patches into the `/patch` directory: 117172-17 and 117468-02.**

   - **For a Solaris OS 9 on SPARC distribution, download and unzip the following patches into the `/patch` directory: 117171-17, 117175-02, and 113318-20. .**

Next Steps Patch the Solaris x86 OS on the patch server as described in the next procedure.

▼ To Patch the Solaris x86 OS on the Patch Server

Before You Begin Create the Solaris x86 OS patch server as described in "To Create a Solaris OS 9 x86 Patch Server" on page 65.

1. **Log in as root (`su - root`) on the patch server.**

2. **Type `reboot -- -s` to reboot the Solaris 9 patch server to single-user mode.**

3. **In single-user mode, change to the `/patch` directory.**

4 **Install the Solaris x86 OS patches.**

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

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

Next Steps Configure and restart NFS on the management server as described in the next procedure.

▼ To Configure and Restart NFS on the Management Server

Before You Begin Patch the Solaris OS on the patch server as described in "To Patch the Solaris x86 OS on the Patch Server" on page 65.

1 **Log in as root (`su - root`) on the management server server.**

2 **Edit the** `/etc/exports` **file and change** `/js *(ro,no_root_squash)` **to** `/js *(rw,no_root_squash)`**.**

3 **Save and close the** `/etc/exports` **file.**

4 **Type `/etc/init.d/nfs restart` to restart NFS.**

Next Steps Patch the Solaris x86 OS distribution on the management server as described in the next procedure.

▼ To Patch the Solaris OS 9 Distribution on the Management Server

Before You Begin Configure and restart NFS on the management server as described in "To Configure and Restart NFS on the Management Server" on page 66.

1 **Log in as root (`su - root`) on the management server server.**

2 **Type `n1sh show os all` to list all OS distributions on the management server.**

Note the ID of the Solaris OS 9 update 7 or earlier distribution. The Solaris OS 9 update 7 distribution ID is used in place of *DISTRO-ID* in the following steps.

3 **Mount the Solaris 9 OS distribution on the management server.**

Type **`mount -o rw`** *management-server-IP*:**`/js/`***DISTRO-ID* **`/mnt`** where *management-server-IP* is the IP address of the management server, and *DISTRO-ID* is the ID of the Solaris OS 9 update 7 or earlier distribution that is to be patched.

4 **Patch the distribution on the management server.**

a. **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.

b. **Type `unmount /mnt` to unmount the management server.**

Next Steps Reconfigure and restart NFS on the management server as described in the next procedure.

▼ To Reconfigure and Restart NFS on the Management Server

Before You Begin Patch the Solaris OS 9 distribution on the management server as described in "To Patch the Solaris OS 9 Distribution on the Management Server" on page 66.

1 **Log in as root (`su - root`) on the management server server.**

2 **Edit the `/etc/exports` file and change `/js *(rw,no_root_squash)` to `/js *(ro,no_root_squash)`.**

Save and close the file.

3 **Type `/etc/init.d/nfs restart` to restart NFS.**

Next Steps Update the Solaris 9 OS distribution as described in the next procedure.

▼ To Update the Solaris 9 x86 OS Distribution `bootenv.rc` File

Before You Begin Reconfigure and restart NFS on the management server as described in "To Reconfigure and Restart NFS on the Management Server" on page 67.

1 **Log in as root (`su - root`) on the management server server.**

2 **Change directory to `/js/`*distro-id*`/Solaris_9/Tools/Boot/boot/solaris`.**

3 **Type `ln -s ../../tmp/root/boot/solaris/bootenv.rc .` to re-create the `bootenv.rc` link.**

The Solaris OS 9 on x86 distribution is ready for deployment to x86 manageable server.

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.

Creating and Using a Solaris OS 9 SPARC Patch Server to Patch Solaris OS 9 Update 7 Distributions

This section provides the procedures for creating a Solaris OS 9 SPARC patch server, and then using the patch server to patch the Solaris OS 9 distributions on the management server. The following topics are discussed:

- "To Create a Solaris OS 9 SPARC Patch Server" on page 68
- "To Patch the Solaris SPARC OS on the Patch Server" on page 69
- "To Configure and Restart NFS on the Management Server" on page 69
- "To Patch the Solaris OS 9 Distribution on the Management Server" on page 70
- "To Reconfigure and Restart NFS on the Management Server" on page 70
- "To Update the Solaris 9 SPARC OS Distribution bootenv.rc File" on page 71

Caution – The procedures are sequentially dependent, and must be followed in the above order.

▼ To Create a Solaris OS 9 SPARC Patch Server

Before You Begin Create at least one Solaris OS 9 update 7 or earlier distribution on the management server. For instructions on how to create an OS distribution, 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*

1 **Select an unused SPARC managed server to become the x86 patch server.**

The following steps refer to the selected managed server as the x86 patch server.

2 **Install the Solaris SPARC OS on the x86 patch server.**

If the OS distribution to be provisioned is Solaris SPARC OS 9 update 7, then install Solaris SPARC OS 9 update 7 on the SPARC patch server.

If the OS distribution is a version earlier than Solaris SPARC OS 9 update 7, then install that version of the Solaris OS on the SPARC patch server.

3 **Log in as root (su - root) to the SPARC patch server.**

4 **Create a /patch directory on the SPARC patch server.**

5 **Download and unzip the patches from `http://sunsolve.sun.com` to the `/patch` directory on the SPARC patch server as follows:**

- **For a Solaris OS 9 on x86 distribution, download and unzip the following patches into the `/patch` directory: 117172-17 and 117468-02.**
- **For a Solaris OS 9 on SPARC distribution, download and unzip the following patches into the `/patch` directory: 117171-17, 117175-02, and 113318-20. .**

Next Steps Patch the Solaris OS on the patch server as described in "To Patch the Solaris SPARC OS on the Patch Server" on page 69.

▼ To Patch the Solaris SPARC OS on the Patch Server

Before You Begin Create the Solaris SPARC OS patch server as described in "To Create a Solaris OS 9 SPARC Patch Server" on page 68.

1 **Log in as root (`su - root`) on the patch server.**

2 **Type `reboot -- -s` to reboot the Solaris 9 patch server to single-user mode.**

3 **In single-user mode, change to the `/patch` directory.**

4 **Install the Solaris SPARC OS patches.**

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

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

Next Steps Configure and restart NFS on the management server as described in the next procedure.

▼ To Configure and Restart NFS on the Management Server

Before You Begin Patch the Solaris SPARC OS on the patch server as described in "To Patch the Solaris SPARC OS on the Patch Server" on page 69.

1 **Log in as root (`su - root`) on the management server server.**

2 **Edit the `/etc/exports` file and change `/js *(ro,no_root_squash)` to `/js *(rw,no_root_squash).`**

3 **Save and close the `/etc/exports` file.**

4 **Type `/etc/init.d/nfs restart` to restart NFS.**

Next Steps Patch the Solaris OS 9 distribution on the management server as described in the next procedure.

▼ To Patch the Solaris OS 9 Distribution on the Management Server

Before You Begin Configure and restart NFS on the management server as described in "To Configure and Restart NFS on the Management Server" on page 69.

1. **Log in as root (`su - root`) on the management server server.**

2. **Type `n1sh show os all` to list all OS distributions on the management server.**

   Note the ID of the Solaris OS 9 update 7 or earlier distribution. The Solaris OS 9 update 7 distribution ID is used in place of *DISTRO-ID* in the following steps.

3. **Mount the Solaris 9 OS distribution on the management server.**

   Type **`mount -o rw`** *management-server-IP*:**`/js/`***DISTRO-ID* **`/mnt`** where *management-server-IP* is the IP address of the management server, and *DISTRO-ID* is the ID of the Solaris OS 9 update 7 or earlier distribution that is to be patched.

4. **Patch the distribution on the management server.**

   a. **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.

   b. **Type `unmount /mnt` to unmount the OS distribution.**

Next Steps Reconfigure and restart NFS on the management server as described in the next procedure.

▼ To Reconfigure and Restart NFS on the Management Server

Before You Begin Patch the Solaris OS 9 distribution on the management server as described in "To Patch the Solaris OS 9 Distribution on the Management Server" on page 70.

1. **Log in as root (`su - root`) on the management server server.**

2 **Edit the /etc/exports file and change /js *(rw,no_root_squash) to /js *(ro,no_root_squash).**

Save and close the file.

3 **Type `/etc/init.d/nfs restart` to restart NFS.**

Next Steps Update the Solaris 9 OS distribution bootenv.rc file as described in the next procedure.

▼ To Update the Solaris 9 SPARC OS Distribution bootenv.rc File

1 **Log in as root (`su - root`) on the management server server.**

2 **Change directory to /js/*distro-id*/Solaris_9/Tools/Boot/boot/solaris.**

3 **Type `ln -s ../../tmp/root/boot/solaris/bootenv.rc .` to re-create the bootenv.rc link.**

The Solaris OS 9 on x86 distribution is ready for deployment to x86 manageable server.

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.

Index