Sun N1 System Manager 1.3 Installation and Configuration Guide

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

Part No: 819–5135
April 2006

Sun Microsystems, Inc. has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more U.S. patents or pending patent applications in the U.S. and in other countries.

U.S. Government Rights – Commercial software. Government users are subject to the Sun Microsystems, Inc. standard license agreement and applicable provisions of the FAR and its supplements.

This distribution may include materials developed by third parties.

Parts of the product may be derived from Berkeley BSD systems, licensed from the University of California. UNIX is a registered trademark in the U.S. and other countries, exclusively licensed through X/Open Company, Ltd.

Sun, Sun Microsystems, the Sun logo, the Solaris logo, the Java Coffee Cup logo, docs.sun.com, N1, Sun Fire, JDK, Netra, Sun Enterprise Java, and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc. Netscape Navigator and Mozilla is a trademark or registered trademark of Netscape Communications Corporation in the United States and other countries.

The OPEN LOOK and Sun™ Graphical User Interface was developed by Sun Microsystems, Inc. for its users and licensees. Sun acknowledges the pioneering efforts of Xerox in researching and developing the concept of visual or graphical user interfaces for the computer industry. Sun holds a non-exclusive license from Xerox to the Xerox Graphical User Interface, which license also covers Sun's licensees who implement OPEN LOOK GUIs and otherwise comply with Sun's written license agreements.

Products covered by and information contained in this publication are controlled by U.S. Export Control laws and may be subject to the export or import laws in other countries. Nuclear, missile, chemical or biological weapons or nuclear maritime end uses or end users, whether direct or indirect, are strictly prohibited. Export or reexport to countries subject to U.S. embargo or to entities identified on U.S. export exclusion lists, including, but not limited to, the denied persons and specially designated nationals lists is strictly prohibited.

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

Sun Microsystems, Inc. détient les droits de propriété intellectuelle relatifs à la technologie incorporée dans le produit qui est décrit dans ce document. En particulier, et ce sans limitation, ces droits de propriété intellectuelle peuvent inclure un ou plusieurs brevets américains ou des applications de brevet en attente aux Etats-Unis et dans d'autres pays.

Cette distribution peut comprendre des composants développés par des tierces personnes.

Certaines composants de ce produit peuvent être dérivées du logiciel Berkeley BSD, licenciés par l'Université de Californie. UNIX est une marque déposée aux Etats-Unis et dans d'autres pays; elle est licenciée exclusivement par X/Open Company, Ltd.

Sun, Sun Microsystems, le logo Sun, le logo Solaris, le logo Java Coffee Cup, docs.sun.com, N1, Sun Fire, JDK, Netra, Sun Enterprise Java et Solaris sont des marques de fabrique ou des marques déposées de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pays. Toutes les marques SPARC sont utilisées sous licence et sont des marques de fabrique ou des marques déposées de SPARC International, Inc. aux Etats-Unis et dans d'autres pays. Les produits portant les marques SPARC sont basés sur une architecture développée par Sun Microsystems, Inc. Netscape Navigator et Mozilla sont des marques de Netscape Communications Corporation aux Etats-Unis est dans d'autres pays.

L'interface d'utilisation graphique OPEN LOOK et Sun a été développée par Sun Microsystems, Inc. pour ses utilisateurs et licenciés. Sun reconnaît les efforts de pionniers de Xerox pour la recherche et le développement du concept des interfaces d'utilisation visuelle ou graphique pour l'industrie de l'informatique. Sun détient une licence non exclusive de Xerox sur l'interface d'utilisation graphique Xerox, cette licence couvrant également les licenciés de Sun qui mettent en place l'interface d'utilisation graphique OPEN LOOK et qui, en outre, se conforment aux licences écrites de Sun.

Les produits qui font l'objet de cette publication et les informations qu'il contient sont régis par la legislation américaine en matière de contrôle des exportations et peuvent être soumis au droit d'autres pays dans le domaine des exportations et importations. Les utilisations finales, ou utilisateurs finaux, pour des armes nucléaires, des missiles, des armes chimiques ou biologiques ou pour le nucléaire maritime, directement ou indirectement, sont strictement interdites. Les exportations ou réexportations vers des pays sous embargo des Etats-Unis, ou vers des entités figurant sur les listes d'exclusion d'exportation américaines, y compris, mais de manière non exclusive, la liste de personnes qui font objet d'un ordre de ne pas participer, d'une façon directe ou indirecte, aux exportations des produits ou des services qui sont régis par la legislation américaine en matière de contrôle des exportations et la liste de ressortissants spécifiquement designés, sont rigoureusement interdites.

LA DOCUMENTATION EST FOURNIE "EN L'ETAT" ET TOUTES AUTRES CONDITIONS, DECLARATIONS ET GARANTIES EXPRESSES OU TACITES SONT FORMELLEMENT EXCLUES, DANS LA MESURE AUTORISEE PAR LA LOI APPLICABLE, Y COMPRIS NOTAMMENT TOUTE GARANTIE IMPLICITE RELATIVE A LA QUALITE MARCHANDE, A L'APTITUDE A UNE UTILISATION PARTICULIERE OU A L'ABSENCE DE CONTREFACON.

060411@14774

Contents

Tables

Preface

The *Sun N1 System Manager 1.3 Installation and Configuration Guide* describes the requirements for installing and configuring the Sun N1™ System Manager software on your management server.

Who Should Use This Book

This guide is intended for system administrators who are responsible for installing 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
- DNS, DHCP, IP addressing, subnetworks, VLANs, SNMP, TFTP, NFS, Microsoft Remote Installation Services (RIS), and mail services

How This Book Is Organized

- Chapter 1 describes how to install, configure, and tune the N1 System Manager.
- Chapter 2 provides the guidelines and procedures for tuning the N1 System Manager on a management server for the first time.
- Chapter 3 describes how to upgrade an existing N1 System Manager 1.2 installation to N1 System Manager 1.3
- Chapter 4 describes how to uninstall the N1 System Manager software.
- Appendix A provides cross references of the protocols, ports, and features used by the N1 System Manager management server and managed servers.

Related Documentation

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

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

Documentation, Support, and Training

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

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

Typographic Conventions

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

TABLE P–1 Typographic Conventions

Typeface	Meaning	Example
`AaBbCc123`	The names of commands, files, and directories, and onscreen computer output	Edit your `.login` file. Use `ls -a` to list all files. `machine_name% you have mail.`

`AaBbCc123`	What you type, contrasted with onscreen computer output	`machine_name%` **`su`**
		`Password:`

aabbcc123	Placeholder: replace with a real name or value	The command to remove a file is `rm` *filename*.

TABLE P–1 Typographic Conventions *(Continued)*

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

Shell Prompts in Command Examples

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

TABLE P–2 Shell Prompts

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

CHAPTER 1

Installing and Configuring the Sun N1 System Manager Software

This chapter provides the procedures for installing and configuring the Sun N1 System Manager software on the management server. If a previous version of N1 System Manager is installed on your management server, upgrade the N1 System Manager as described in Chapter 3.

The N1 System Manager configuration process can be run at any time to reconfigure the N1 System Manager. For example, you would run the configuration process if you wanted to change how unknown and changed host keys for SSH operations are processed. You would also run the configuration process to set up N1 System Manager for Windows operating system provisioning if you have added a RIS server.

The following topics are discussed:

- "N1 System Manager Installation Prerequisites" on page 11
- "Installing the Sun N1 System Manager 1.3 Software" on page 13
- "Configuring the N1 System Manager" on page 17
- "Configuring SSH Unknown and Changed Host Key Policies" on page 29

Note – The term manageable server is used in this manual for any server that has not been discovered by the N1 System Manager and is subsequently not monitored or managed by the N1 System Manager. The term managed server is used for any server that has been discovered by the N1 System Manager and is monitored and managed by the N1 System Manager.

N1 System Manager Installation Prerequisites

The following prerequisites must be met before you can install the N1 System Manager software:

- The hardware must be connected and configured as described in Chapter 2, "Sun N1 System Manager System and Network Preparation," in *Sun N1 System Manager 1.3 Site Preparation Guide*.

- An OS version appropriate for the management server hardware type must be installed on the N1 System Manager management server, as described in Chapter 3, "Installing and Configuring an OS on the Management Server," in *Sun N1 System Manager 1.3 Site Preparation Guide*.
- If you plan to provision windows to managed servers, you should install and configure a Microsoft Remote Installation Services (RIS) server before installing and configuring N1 System Manager. For further information, see "Setting Up a Windows Remote Installation Services Server" in *Sun N1 System Manager 1.3 Site Preparation Guide*.

  If you install a RIS server after completing N1 System Manager installation and configuration, you can add the RIS server to your N1 System Manager network by running the N1 System Managerconfiguration process as described in "Configuring the N1 System Manager" on page 17.

Two methods of installing the Sun N1 System Manager are available:

- If the server you have selected for the management server has a DVD drive installed, you can install the Sun N1 System Manager software from the installation DVD-ROM as described in "To Install the N1 System Manager Software" on page 14.
- If the server you have selected for the management server does not have a DVD drive installed, you must download, unpack, and mount the N1 System Manager installation ISO image as described next in "To Download and Mount the Sun N1 System Manager Installation ISO Image" on page 12.

▼ To Download and Mount the Sun N1 System Manager Installation ISO Image

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

2. **(Optional) Download and install the Sun Download Manager.**

   Downloads of large files using web browsers can sometimes fail. For this reason, use the Sun Download Manager to download the N1 System Manager installation ISO image. For instructions about how to download and install the Sun Download Manager, go to `http://www.sun.com/download/sdm/index.xml`.

3. **Download and unpack the N1 System Manager installation ISO image to the management server.**

   Refer to your N1 System Manager eFulfillment documentation and email for your download location, and download the ISO image appropriate for the operating system you have installed on your management server:

   - `n1sm-1.3-ga-linux-x86-iso.zip`
   - `n1sm-1.3-ga-solaris-x86-iso.zip`
   - `n1sm-1.3-ga-solaris-sparc-iso.zip`

4 **Unpack the N1 System Manager installation ISO image zip file.**

Type `unzip` *ISO-image-name*`.zip`, where *ISO-image-name* is the name of the N1 System Manager installation ISO image zip file that you downloaded.

5 **Create a mount point directory for the installation ISO image on the management server and mount the ISO image.**

Assume you have saved the N1 System Manager installation ISO image in the management server root directory as `n1sm-install.iso`, and that the ISO image is to be mounted on the mount point directory named `/n1sminstall`. You would then create the mount point directory and mount the ISO image as follows:

- Solaris:

  ```
  # mkdir /n1sminstall
  # lofiadm -a /n1sm-install.iso
  /dev/lofi/1
  # mount -F hsfs -o ro /dev/lofi/1 /n1sminstall/
  ```

  If your management server has other `lofi` devices installed, the `lofiadm -a /n1sm-install.iso` command displays a different `lofi` device, for example `/dev/lofi/2`. Use the name of the displayed `lofiadmin -a` command in the `mount -F` command.

- Linux:

  ```
  # mkdir /n1sminstall
  # mount -o loop,ro /n1sm-install.iso /n1sminstall
  ```

Next Steps Install the Sun N1 System Manager software as described in the next section.

Installing the Sun N1 System Manager 1.3 Software

This section provides the procedure for installing N1 System Manager 1.3 software on the management server for the first time.

- If N1 System Manager 1.2 is installed on your management server, upgrade your management server to version1.3 as described in Chapter 3.
- If N1 System Manager 1.1 is installed on your management server, you must first upgrade to N1 System Manager 1.2 before you can upgrade to version 1.3.

The N1 System Manager software installation process might require up to two hours to complete depending on your network configuration.

⚠ **Caution –** Dedicate the management server only to N1 System Manager software. Do not install other applications on the management server.

▼ To Install the N1 System Manager Software

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

2. **Change directory to the N1 System Manager installation source.**

   If you are installing from the N1 System Manager DVD, change directory as follows.

   - Solaris SPARC-based management server:

     ```
     # cd /cdrom/n1_system_mngr/Solaris_sparc/Product/installer
     ```

   - Solaris x86-based management server:

     ```
     # cd /cdrom/n1_system_mngr/Solaris_x86/Product/installer
     ```

   - Linux x86-based management server:

     ```
     # cd /cdrom/n1_system_mngr/Linux_x86/Product/installer
     ```

   If you are installing from an N1 System Manager installation ISO image, substitute your mount point directory name for `/cdrom` in the path names.

3. **Type `./install` to start the installation process**

   The Software Evaluation Agreement appears.

4. **Choose whether to accept the agreement and continue installation.**

   Read the agreement carefully. Type **y** to continue installation, or type **n** to exit the installation.

   When you continue installation, the installation script checks for required Perl modules. When this process completes, the N1SM Installer process checks whether a prior version of N1 System Manager 1.2 is installed on your management server.

   Note – If version 1.2 is installed, the installation process displays the following message and then exits.

   ```
   Version 1.2 is already installed
   Invoke installer with -u option to upgrade
   ```

   If the above message is displayed, upgrade your management server as described in Chapter 3

The appearance of the N1SM Installer menu and the components installed by the N1SM installer depend on the operating system installed on the management server as shown by the following examples.

- Solaris 10 Based Management Server

```
         N1SM Installer (version 1.3 on SunOS)

 1. Install OS packages.                         [Not Completed]
 2. Install Expect.                              [Not Completed]
 3. Install IPMI tool.                           [Not Completed]
 4. Install JDK 1.5.                             [Not Completed]
 5. Install service provisioning components.     [Not Completed]
 6. Install OS provisioning components.          [Not Completed]
 7. Copy DHCP configuration file.                [Not Completed]
 8. Install user interface components.           [Not Completed]
 9. Install service container components.        [Not Completed]
10. Install N1 System Manager.                   [Not Completed]


Non-interactive install in progress

Executing current step:  Install OS packages...
```

- Linux Based Management Server

```
         N1SM Installer (version 1.3 on Linux)

 1. Check that required RPM packages are present.    [Not Completed]
 2. Install IPMI tool.                               [Not Completed]
 3. Install JDK 1.5.                                 [Not Completed]
 4. Install Python.                                  [Not Completed]
 5. Install service provisioning components.         [Not Completed]
 6. Install OS provisioning components.              [Not Completed]
 7. Copy DHCP configuration file.                    [Not Completed]
 8. Install user interface components.               [Not Completed]
 9. Install service container components.            [Not Completed]
10. Install N1 System Manager.                       [Not Completed]


Non-interactive install in progress.
```

The installation process runs each step in sequence. When a step completes successfully, the status of the step is updated to Completed.

If a step fails, you are notified, and the status remains Not Completed or is changed to Partially Run. Exit the installation process and examine the log file `/var/tmp/installer.log.latest` to determine the cause of the failure. Correct the problem and then run the installation process again.

You are informed when the installation process completes, and are then prompted to run the configuration utility:

```
N1SM installation is complete
Run the n1smconfig utility to configure N1SM.
```

- If you have installed Red Hat Enterprise Linux (RHEL) 3.0 AS Update 2, Update 3, or Update 4 on the management server and have installed RPMs other than those from RHEL 3.0 AS Update 2 through Update 4, you might be warned after Step 1 of the install completes that the RPMs might not work with the N1 System Manager. A list of the expected RPMs is displayed, followed by a list of the RPMs that were found. You are informed that this is only a warning and may continue with the install by pressing c. This option is in addition to options currently available for when an installation step fails (t to try again or x to exit.)
- If you installed RedHat Enterprise Linux AS Update 3 or later, the following message might be displayed after installation of the service container components completes:

  ```
  This installer has determined that some rpms currently
  installed on this system have later versions than those currently
  required by N1SM. If you encounter any problems related to these
  substitutions, you might need to obtain and install the exact version
  of the software required by the installer before re-installing N1SM.
  ```

- If you have installed Red Hat Enterprise Linix AS 4.0, Update 1, and did not disable SELinux during installation, the following message is displayed:

```
Failed Step:  Install OS provisioning components.
The following is a portion of the installer
log which may indicate the cause of the error.
If this does not indicate the cause of the
error, you will need to view the full log
file. More information on how to do that is
available below.
* * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *

WARNING: This version of N1 System Manager does not support SELinux fully enabled.
If SELinux is enabled, disable it by exiting the installer and performing these steps:
 1) At the Operating System prompt, type ’setenforce 0’
 2) Edit the file /etc/selinux/config and set ’SELINUX=disabled’
Then restart the N1 System Manager installer.
* * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
Please fix the problem and then try this step again.
For a full log of the failed install see the file: /var/tmp/installer.log.14427.

t. Try this step again (correct the failure before proceeding)
x. Exit
Enter selection: (t/x)
```

Disable SELinux as instructed.

Next Steps Configure the N1 System Manager system as directed in the next section, "Configuring the N1 System Manager" on page 17.

Configuring the N1 System Manager

This section provides the procedures for stopping and starting the N1 System Manager and for configuring the N1 System Manager system.

Initial configuration is performed by running the `n1smconfig` command. You can also reconfigure the N1 System Manager at any time by running the `n1smconfig` command again, for example, if you later add a RIS server to your production N1 System Manager environment.

If you have already installed and configured N1 System Manager, running `n1smconfig` again and accepting the changes will, in most cases, stop and then restart the N1 System Manager. To minimize impact, a good practice is to schedule the reconfiguration, and then stop N1 System Manager before running `n1smconfig`. The following table lists the commands to start and stop N1 System Manager.

TABLE 1–1 Starting and Stopping N1 System Manager

Starting N1 System Manager:
On a Solaris management server, type **`svcadm enable n1sm`**
On a Linux management server, type **`/etc/init.d/n1sminit start`**
Stopping N1 System Manager:
On a Solaris management server, type **`svcadm disable n1sm`**
On a Linux management server, type **`/etc/init.d/n1sminit stop`**

▼ To Configure the N1 System Manager

Before You Begin The N1 System Manager software must be successfully installed as described in "Installing the Sun N1 System Manager 1.3 Software" on page 13, or successfully upgraded as described in Chapter 3.

Note – You must have at least a provisioning network or a management network connected to the management server. If your network configuration provides only a management network or only a provisioning network to the management server, then you are running a restricted N1 System Manager. N1 System Manager provides two default security roles with specific privileges assigned for the restricted mode of operation. See "Managing Roles" in *Sun N1 System Manager 1.3 Discovery and Administration Guide* and "Restricted Mode Capabilities" in *Sun N1 System Manager 1.3 Discovery and Administration Guide*.

---

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

2 **If you are reconfiguring N1 System Manager, stop N1 System Manager.**

- On a Solaris management server, type **`svcadm disable n1sm`**.
- On a Linux management server, type **`/etc/init.d/n1sminit stop`**.

3 **Type `n1smconfig` to start the configuration process.**

- If you are running `n1smconfig` for the first time, the current N1 System Manager configuration settings are displayed, followed by a description of the provisioning network and a list of the network interfaces that have been detected.
- If you are rerunning `n1smconfig`, only configuration settings that can be changed are displayed.

You are asked whether you want to continue. Type **`y`** to continue.

- If you are running `n1smconfig` for the first time, you are prompted to specify the interface that is to be used by the provisioning network.
- If you are rerunning `n1smconfig`, you are notified that the DHCP range may be modified only when modifying the provisioning interface. You are then asked whether you want to modify the interface or DHCP range used for the provisioning network. Type **`y`** to continue.

You are then prompted to specify the interface that is to be used by the provisioning network.

4 **Specify the interface to be used by the provisioning network.**

- If you do not have a provisioning network, type **`none`**.

  Without a provisioning network, the N1 System Manager operates in a restricted mode.

  A description of the management network appears, followed by a list of the network interfaces that have been detected. You are then prompted to specify the interface that is to be used by the management network. Go to Step 6.
- If you do have a provisioning network, type the interface name, for example, `eth1`, `hme0`, `bge1`, and so on, depending on the machine architecture and installed OS.

You are asked whether you want to specify a range of IP addresses for the DHCP server to use.

5 **Choose whether to configure the DHCP server address range.**

- If you choose to configure the DHCP IP address range, the range of IP addresses you provide will be allocated for assignment to the manageable servers for loading operating systems and updates over the provisioning network.
- If you choose not to configure the DHCP IP address range, then you must specify static addressing when using the N1 System Manager `load` operation for OS profiles.

Note – The management server provides DHCP services only for the provisioning network. The management server does not provide DHCP services for the data network. If you plan to dynamically configure IP services on the data network, you must provide an external DHCP server for the data network. You must not have another DHCP server on the provisioning network.

- Type **n** if you do not want to specify a range of IP addresses.

  A description of the management network is displayed, followed by the network interfaces that have been detected. You are then prompted to specify the interface for the management network. Go to Step 6.
- Type **y** if you want to specify a range of IP addresses for the DHCP server to use for the provisioning network.

Caution –

- If the management network port address is on the same subnet as the provisioning network, ensure that the management server IP addresses are not within the range of the IP addresses you specify for the DHCP address range. This rule ensures that the DHCP server does not assign a duplicate IP address to a client that does not resolve using the DHCP client clause.
- Ensure that you specify an IP address range that does not include the management server IP addresses. If the management server IP addresses are within the range of addresses used for discovery, then the discovery process will discover the management server and reboot the management server.

You are prompted to type the starting DHCP IP address. Type the starting IP address for the DHCP server to use.

You are prompted to type the ending IP address. Type the ending IP address for the DHCP server to use.

You are then prompted to configure the DNS name servers and search list entries. Go to Step 6.

6 Specify the interface to be used by the management network.

- If you do not have a management network, type **none**.

  Without a management network, the N1 System Manager operates in a restricted mode.
- If you do have a management network, type the interface name.

You are then prompted to configure the DNS name servers and search list entries.

7 Choose whether to configure the name servers.

- Type **y** if you want to configure the name servers and domain search list. You are prompted for the name server addresses. Go to Step 8.
- Type **n** if you accept the displayed name servers and domain search list. You are asked whether you want to configure the SMTP server for event notification. Go to Step 10.

8 Configure the name servers.

Type the IP addresses of the name servers, separated by a single space. For example:

```
129.111.111.11 129.111.111.22
```

You are prompted to enter the search domain suffix list.

9 **Specify the search domains.**

Type the names of the domains that are to be used for DNS search separated by a single space. For example:

```
location-one.company.com location-two.company.com location-three.company.com
```

You are asked whether you want to configure the SMTP server for event notification.

10 **Choose whether to configure SMTP for event notification.**

SMTP must be configured if you want the N1 System Manager to receive event notifications from ALOM-based managed servers. To determine which manageable servers are ALOM-based, see "Manageable Server Requirements" in *Sun N1 System Manager 1.3 Site Preparation Guide*.

- Type **y** if you want to configure the SMTP server. You are prompted for the name of the SMTP server, or the IP address of the SMTP server. Go to Step 11.
- Type **n** if you do not want to configure the SMTP server. You are asked whether you want to modify logging configuration. Go to Step 12.

11 **Specify the SMTP server name or IP address.**

Type either the fully qualified SMTP server name, or the IP address for the SMTP server. For example:

```
smtp.mycompany.com
```

or

```
129.111.222.33
```

You are asked whether you want to modify logging event configuration.

12 **Modify logging event configuration**

- Type **y** if you want to configure logging. Information about logging configuration appears. Go to Step 13.
- Type **n** if you do not want to configure logging. The configuration process displays information about OS deployment and job time out configuration. You are then asked whether you want to modify job time out configuration. Go to Step 16.

13 **Configure logging.**

Press Return to accept the default of "ALL" or type the specifications as directed. You are prompted to enter the event logging severity value.

14 **Specify the event logging severity value.**

Take one of the following actions:

- Type **q** to exit event logging severity specification. The event logging severity level is not set. You are then asked whether you want to modify job time out configuration. Go to Step 16.

- Press Return to accept the default value of 0, or type the number corresponding to one of the following event severity levels:
  - 0 = unknown
  - 1 = other
  - 2 = information
  - 3 = warning
  - 4 = minor
  - 5 = major
  - 6 = critical
  - 7 = fatal

The configuration process displays information about log entry retention. You are prompted for the number of days to retain event log entries.

15 Specify the number of days to retain event log entries.

Press return to accept the default of 365 days, or type the number of days that event log entries are to be retained.

The configuration process displays information about OS deployment and job time out configuration. You are then asked whether you want to modify job time out configuration.

16 Choose whether to modify job time out configuration.

Some OS distributions are very large, and might take longer than the default time when provisioning a server. If you plan to provision large OS distributions, increase the time out values.

- Type **y** if you want to modify job time out configuration.

  A description of job and step time out values appears. Type the new time out values when prompted.
- Type **n** if you do not want to modify time out configuration.

You are asked whether to enable N1 System Manager (N1SM) startup at each boot.

17 Choose whether to start the N1 System Manager system at each boot.

- Type **y** to start the N1 System Manager system each time the system boots.
- Type **n** if you want to start the N1 System Manager system manually after the management server has been rebooted. You are notified that you can start the N1 System Manager manually.

You are asked whether you want to enable auto-login to the ILOM Web GUI on managed servers that offer the auto-login feature.

18 Choose whether to enable the managed server ILOM GUI auto-login feature.

The Sun Fire™ X4100 and Sun Fire X4200 servers provide a web GUI for performing various system administration tasks such as connecting remote devices and performing system monitoring.

- If you enable the ILOM GUI auto-login feature, then you will automatically be logged onto the Sun Fire X4100 or X4200 web GUI when you click the managed server's Open Web Console link in the N1 System Manager browser interface.
- If you do not enable the auto-login feature, you are prompted for the password when you click the Open Web Console link. For further information, see *To Open the Sun ILOM Web GUI for a Sun Fire X4000 Series Server* in the N1 System Manager online help after you have installed or upgraded the N1 System Manager.

Caution – Enabling the Web Console (Sun ILOM Web GUI) automatic login feature for Sun Fire X4100 and X4200 managed servers exposes the server's service processor credentials to users who can view the web page source for the ILOM on the management network login page.

- Type **y** to enable the auto-login feature.
- Type **n** if you do not want to enable the auto-login feature.

  You are asked whether you want to modify the SSH policies for changed and unknown host keys.

19 Choose whether to modify SSH policies.

Note – Accepting changed or unknown host keys for SSH operations can expose N1 System Manager to security risks, but will allow more N1 System Manager operations to succeed.

- Type **n** if you do not want to modify SSH policies.

  Note – You can modify the SSH policies at any time after initial configuration as described in "Configuring SSH Unknown and Changed Host Key Policies" on page 29.

  The following SSH policies are applied for changed and unknown host keys.

  – Accept changed host keys for Management IP address: yes
  – Accept changed host keys for Platform IP address: yes
  – Accept unknown host keys for Management IP address: yes
  – Accept unknown host keys for Platform IP address: yes

  If your are running `n1smconfig` for the first time, the configuration process then displays information about ALOM-based manageable server mail alerts. If you are reconfiguring N1 System Manager, the current ALOM email alert settings are displayed. Go to Step 21.

- Type **y** if you want to modify SSH policies.

  You are asked whether you want to accept changed host keys to management IP addresses.

a. Choose whether to accept changed host keys for SSH operations to management IP addresses.

- Type **n** if you do not want N1 System Manager to accept changed host keys for management IP addresses.

- Type **y** to accept changed host keys for the management IP addresses.

You are asked whether to accept changed host keys to platform IP addresses.

b. **Choose whether to accept changed host keys for SSH operations to platform IP addresses.**

- Type **n** if you do not want N1 System Manager to accept changed host keys for platform IP addresses.
- Type **y** to accept changed host keys for the platform IP addresses.

You are asked whether to accept unknown host keys to management IP addresses.

c. **Choose whether to accept unknown host keys for SSH operations to management IP addresses.**

- Type **n** if you do not want N1 System Manager to accept changed host keys for management IP addresses.
- Type **y** to accept changed host keys for the management IP addresses.

You are asked whether to accept unknown host keys to platform IP addresses.

d. **Choose whether to accept unknown host keys for SSH operations to platform IP addresses.**

- Type **n** if you do not want N1 System Manager to accept changed host keys for platform IP addresses.
- Type **y** to accept changed host keys for the platform IP addresses.

The next step depends on the operating system installed on the management server.

- If you are configuring a Solaris-based management server, you are then asked whether you want to enable the SSHv1 protocol so that you can access the serial console on managed servers. Go to Step 20.
- If you are configuring a Linux-based management server, the configuration process then displays information about ALOM-based manageable server mail alerts. If you are reconfiguring N1 System Manager, the current ALOM email alert settings are displayed. Go to Step 21.

20 **Choose whether to enable the SSHv1 protocol on a Solaris-based management server.**

SSHv1 is required to enable managed server remote serial console access from a Solaris-based N1 System Manager browser interface. For more information, see To *Open the Serial Console for a Server* in the N1 System Manager online help after you have installed or upgraded the N1 System Manager.

Caution – The following SSHv1 security issues should be considered:

- The applet used for the serial console access from the browser interface does not provide a certificate-based authentication of the applet. The applet uses SSHv1 only for communication back to the management server, and requires that SSHv1 is enabled for themanagement server. Users concerned about this issue can use the serial console feature from the command line through the `connect` command.
- SSH fingerprints used during connections from the management server to the provisioning network interfaces on the managed servers are automatically acknowledged by the N1 System Manager software, which might make the managed servers vulnerable to man-in-the middle attacks.

- **Type y to enable SSHv1.**

  If you later want to disable SSHv1:

  a. **Stop the N1 System Manager.**

  b. **Edit the file** `/etc/ssh/sshd_config`**.**

  c. **Change the line** `Protocol 2,1` **to** `Protocol 2`**.**

  d. **Delete the line** `HostKey /etc/ssh/ssh_host_rsa1_key`**.**

  e. **Start the N1 System Manager.**

- **Type** `n` **if you do not want to enable SSHv1.**

You are asked whether you want to use the N1 System Manager internal email server to receive ALOM email alerts.

If your are running `n1smconfig` for the first time, the configuration process then displays information about ALOM-based manageable server mail alerts. If you are reconfiguring N1 System Manager, the current ALOM email alert settings are displayed.

21 **Choose whether to use the N1 System Manager internal email server to receive ALOM email alerts.**

ALOM-based managed servers use email to send hardware monitoring alerts to theN1 System Manager.

You can use the secure N1 System Manager internal email server, which requires only that port 25 is not in use, or you can use an existing mail server which must be accessible by the N1 System Manager and configured for use by the N1 System Manager.

To determine whether port 25 has been assigned to a process, open a terminal window and type the command **`grep 25 /etc/services`**. To determine if port 25 is in use, type the command **`netstat -an | grep 25`**. If port 25 is in use, refer to your operating system documentation to disable the process using port 25.

Note – Using an existing email server exposes N1 System Manager to denial of service attacks and other email-based security risks.

- Type **y** if you want to use the secure N1 System Manager internal email server.

  You are prompted to add, delete, or modify the Windows RIS (Remote Installation System) server. Go to Step 24.

- Type **n** if you want to use an existing email server.

  The current external email server values are displayed, and you asked whether you want to change the settings.

22 **Choose whether to change the external email server settings.**

- Type **n** if you do not want to change the email settings.

  You are prompted to add, delete, or modify the Windows RIS (Remote Installation System) server. Go to Step 24.

- Type **y** if you want to change any of the displayed email settings.

  You are prompted to specify each of the ALOM email alert settings as described in the next step.

23 **Specify the ALOM email alert settings.**

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

Press Enter or Return to accept the default value of Inbox, or type the name of an email folder.

You are prompted for email alert IP address.

b. **Specify the mail server IP address.**

- If you have installed and enabled an email server on the management server, type the IP address of the management servers 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 the server on which the email server is installed.

You are prompted for the email alert mail address.

c. **Specify the email address to which alerts are to be sent.**

Type the full email address. For example: `n1smadmin@company.com`

You are prompted for the email account password.

d. **Specify the account password.**

Type the password for the external email account.

You are prompted for the email alert protocol.

e. **Specify the email alert protocol.**

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

You are prompted for the email alert user name.

f. **Specify the email alert user name.**

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

For example: `n1smadmin`

The mail settings you have specified are displayed, and you are asked whether you want to accept the settings.

g. **Choose whether to accept the 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 mail folder.
- Type **`y`** to accept the email alert settings.

  You are whether to add, delete, or modify the Windows RIS (Remote Installation System) server.

24 Choose whether to Add, Delete, or Modify the Windows RIS server.

If you plan to provision a Windows operating system to one or more managed servers, you must install and configure a separate Windows RIS server that is accessible to the provisioning network. For further information, see "Setting Up a Windows Remote Installation Services Server" in *Sun N1 System Manager 1.3 Site Preparation Guide*.

If you install a RIS server after completing N1 System Manager installation and configuration, you can add the RIS server to your N1 System Manager network by running `n1smconfig` again.

- Type **`n`** if you do not want to add, delete, or modify a Windows RIS server for use by the N1 System Manager.

  You are asked whether you want to enable OS discovery. Go to Step 26.
- Type **`y`** if you want to add, delete, or modify a Windows RIS server for use by the N1 System Manager.

  You are prompted for the RIS server subnet address.

25 Configure the Windows RIS Server.

a. **Specify the RIS server SSH access user name.**

Type the RIS server SSH account user name.For example: **`n1smssh`**.

The user account you specify must already exist on the RIS server.

You are prompted for the RIS server SSH access user password.

b. **Specify the RIS server SSH access user password.**

   Type the password for the RIS server SSH user account. Type the password again when are prompted to re-enter the SSH access password.

   You are prompted for the RIS share path.

c. **Specify the RIS share path.**

   The RIS share path is the drive letter and directory name on the RIS server in which the RIS software is installed. For example: `D:\RemoteInstall`.

   You are prompted for the RIS provisioning file location.

d. **Specify the RIS provisioning file location.**

   The provisioning file location is the drive letter and directory path which the configuration process will create on the RIS server, and to which N1 System Manager will copy scripts for use by the RIS server. For example: `C:\N1SM`.

   You are prompted for the RIS netmask.

e. **Specify the RIS netmask.**

   Press Return or Enter to accept the default netmask value 255.255.255.0, or type a different netmask value.

   You are prompted for the RIS language.

f. **Specify the RIS language.**

   Press Return or Enter to accept the default language value English, or type the name of a different language.

   To view a list of valid languages, select Regional and Language Options from the Microsoft Windows Control Panel on your RIS server to display the Regional and Language Options panel. Click the Regional Options tab, and then click the arrow to the right of the displayed language. The list of languages is displayed.

   You are prompted for the RIS host name.

g. **Specify the RIS host name.**

   Type the host name of the RIS server. For example: *risserver*.

   You are prompted for the RIS host IP address.

h. **Specify the RIS host IP address.**

   Type the RIS host IP address.

   You are prompted for the RIS active directory user name.

i. **Specify the RIS active directory user name.**

   Type the name of the active directory user account, for example `n1smadmin`. If the active directory user account does not exist on the RIS server, the configuration process will create the user account.

   You are prompted for the active user directory account password.

j. **Specify the RIS active directory password.**

   Type the password for the RIS server active directory user account password. Type the password again when are prompted to re-enter the active directory password.

   You are prompted for the RIS active directory domain.

k. **Specify the RIS active directory domain name.**

   Type the active directory domain name that you specified during setup of Active Directory on your RIS server For example: *servername.company.com*.

   The RIS settings you have specified are displayed, and you are asked whether you want to apply the settings.

l. **Choose whether to use the RIS settings you have specified.**

   - Type **n** if you want to change any of the displayed settings. The RIS configuration process restarts, and you are asked whether to add, delete, or modify the Windows RIS server. Go to the beginning of Step 25.
   - Type **y** to apply the displayed settings.

The settings are applied, and you are asked whether you want to enable OS discovery.

26 **Choose whether to enable OS discovery.**

If you enable OS discovery, you can discover manageable servers by the operating system running on the manageable servers.

- Type **n** if you do not want to enable OS discovery.
- Type **y** if you want to enable OS discovery.

You are asked if you want to modify the default password of the plan and jobs execution server.

27 **Choose whether to modify the plan and jobs execution server password.**

Changing the execution server password increases security, and modifies the service provisioning password.

- Type **n** if you do not want to change the password.
- Type **y** if you want to change the password.

  You are prompted to type the new password or to accept the displayed default. Type a new password or accept the default.

All of the settings you have specified are displayed, and you are asked whether you want to apply the settings.

28 **Review the proposed settings.**

- Type **y** to apply the settings.

  The settings are applied.

  - If you not previously run `n1smconfig`, you are prompted to press Enter to start the N1 System Manager.
  - If you have previously run `n1smconfig`, you are asked whether you want to restart N1 System Manager. Type **y** to restart N1 System Manager, or type **n** to exit to the command prompt.
- Type **n** if the settings are not correct.

  You are notified that you must reconfigure and apply settings for the N1 System Manager to work properly. The configuration process then exits to the system prompt. To configure the N1 System Manager, run the `n1smconfig` command again.

Next Steps Prepare the N1 System Manager system for production as described in Chapter 2

Configuring SSH Unknown and Changed Host Key Policies

This section provides the procedure for changing SSH policies for changed and unknown host keys.

▼ To Change SSH Policies

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

2 **Stop N1 System Manager.**

- On a Solaris management server, type **`svcadm disable n1sm`**.
- On a Linux management server, type **`/etc/init.d/n1sminit stop`**.

Wait for all N1 System Manager processes to stop.

3 **Change the management IP address policies as follows:**

- Unknown host keys:
  - To accept unknown host keys, type **`n1smconfig -ssh_unk_man_ip=y`**.
  - To reject unknown host keys, type **`n1smconfig -ssh_unk_man_ip=n`**.
- Changed host keys:
  - To accept changed host keys, type **`n1smconfig -ssh_cha_man_ip=y`**.
  - To reject changed host keys, type **`n1smconfig -ssh_cha_man_ip=n`**.

4. **Change the platform IP address policies as follows:**

   - Unknown host keys:
     - To accept unknown host keys, type **`n1smconfig -ssh_unk_pla_ip=y`**.
     - To reject unknown host keys, type **`n1smconfig -ssh_unk_pla_ip=y`**.
   - Changed host keys:
     - To accept changed host keys, type **`n1smconfig -ssh_cha_pla_ip=y`**.
     - To reject changed host keys, type **`n1smconfig -ssh_cha_pla_ip=y`**.

5. **Start N1 System Manager.**

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

◆ ◆ ◆ CHAPTER 2

Preparing for Production

This chapter provides guidelines and procedures for tuning the N1 System Manager.

This chapter discusses the following topics:

Security Considerations

The following list provides security considerations that you should be aware of when you are using the N1 System Manager.

- The Java™ Web Console that is used to launch the N1 System Manager's browser interface uses self-signed certificates. These certificates should be treated with the appropriate level of trust by clients and users.
- The terminal emulator applet that is used by the browser interface for the serial console feature does not provide a certificate-based authentication of the applet. The applet also requires that you enable SSHv1 for the management server. For certificate-based authentication or to avoid enabling SSHv1, use the serial console feature by running the `connect` command from the `n1sh` shell.
- SSH fingerprints that are used to connect from the management server to the provisioning network interfaces on the manageable servers are automatically acknowledged by the N1 System Manager software. This automation might make managed servers vulnerable to "man-in-the middle" attacks.
- The Web Console (Sun ILOM Web GUI) autologin feature for Sun Fire X4100 and Sun Fire X4200 servers exposes the server's service processor credentials to users who can view the web page source for the Login page. To avoid this security issue, disable the autologin feature by running the `n1smconfig` utility. See "Configuring the N1 System Manager" on page 17 for details.

Performance Guidelines

To ensure the best performance in your N1 System Manager environment, adhere to the following guidelines and recommendations:

- Before you run discovery, tune the N1 System Manager as described in "To Increase the N1 System Manager Performance" on page 32.
- Maximize the number of managed servers per group, and run operations against groups instead of against a large number of individual servers. Running operations on a group minimizes the number of groups you need to manage and minimizes the number of jobs you need to submit in order to accomplish a given task.

N1 System Manager Performance Tuning

Tune the N1 System Manager for maximum performance based on the number of managed servers you plan to manage. The following procedure should be done before you run discovery.

▼ To Increase the N1 System Manager Performance

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

2. **Linux only: Update the NFS file.**

   a. **Edit the file `/etc/sysconfig/nfs` file and add the following line:**

   ```
   RPCNFSDCOUNT=32
   ```

   b. **Save and close the file.**

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

3. **Update the `package.cache.xml` file.**

   Edit the `/opt/sun/n1gc/lib/package.cache.xml` file and locate the line containing `attribute name="FirmwareInfos"`. Update the line to read as follows:

   ```
   <attribute name="FirmwareInfos" refresh-interval="-1" delay="none" persistent="true"/>
   ```

   This instruction ensures that the first invocation of the `show server` command after a restart of the N1 System Manager does not take a long time to complete.

4. **Stop N1 System Manager.**

   - On a Solaris management server, type **`svcadm disable n1sm`**
   - On a Linux management server, type **`/etc/init.d/n1sminit stop`**

   Wait for all N1 System Manager processes to stop.

5 **Start N1 System Manager.**

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

Next Steps If you have updated an earlier version of N1 System Manager to version 1.3, you can now use N1 System Manager 1.3.

If you have completed a first-time install of N1 System Manager 1.3, perform the following tasks:

- Log in to the N1 System Manager as described in "Accessing the N1 System Manager Through the Command Line" in *Sun N1 System Manager 1.3 Discovery and Administration Guide*.
- Define the N1 System Manager users as described in "Managing Users" in *Sun N1 System Manager 1.3 Discovery and Administration Guide*.
- Define the N1 System Manager roles as described in "Managing Roles" in *Sun N1 System Manager 1.3 Discovery and Administration Guide*.
- Run discovery to locate and identify the manageable servers as described in "SP-Based Discovery" in *Sun N1 System Manager 1.3 Discovery and Administration Guide* .
- Create the operating system distributions for the managed servers as described in "Managing UNIX OS Distributions" in *Sun N1 System Manager 1.3 Operating System Provisioning Guide*.
- Create the operating system profiles for the managed servers as described in "Managing OS Profiles" in *Sun N1 System Manager 1.3 Operating System Provisioning Guide*.
- Install the operating system distributions on the managed servers as described in "Installing the UNIX OS on Managed Servers" in *Sun N1 System Manager 1.3 Operating System Provisioning Guide*.
- Back up your N1 System Manager installation as described in Chapter 3, "Backing Up and Restoring," in *Sun N1 System Manager 1.3 Discovery and Administration Guide*.

For problem resolution procedures, see *Sun N1 System Manager 1.3 Troubleshooting Guide*.

Management Server Rehosting

Rehosting is the process of relocating an installed and configured N1 System Manager management server to a new network. The new network may have a completely different configuration, in which case the management server's network settings must be changed.

Conditions in which you need to rehost the management server are as follows:

- The N1 System Manager is installed and configured on a management server in a test environment, and the management server is now ready to be moved to the production environment.
- The N1 System Manager is installed and configured on a management server in a production environment, and is being relocated to a new network.

Rehosting the N1 System Manager management server is comprised of three major tasks:

- Disabling N1 System Manager start on reboot
- Reconfiguring operating system Files
- Reconfiguring the management server

Note – N1 System Manager 1.3 does not support managed server rehosting.

Disabling N1 System Manager Start on Reboot

Caution – You must disable the N1 System Manager Start on Reboot feature before you rehost your management server.

If you change the hostname or IP address of the management server and then reboot the server, and N1 System Manager is configured to start at boot, then N1 System Manager could start with an invalid hostname or IP address or hostname.

1. Type**`ps -ef | grep [Nn]1`** to display the N1 System Manager processes that might be running
2. Type **`kill -9`** *PID* where *PID* is the process ID of the N1 System Manager process

The following task must be performed before you make any rehosting changes to the management server.

▼ To Disable N1 System Manager Start on Reboot

1 Log in as root on the management server.

2 Stop N1 System Manager.

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

Wait for all process to stop, then type **`ps -ef | grep [Nn]1`** to display any N1 System Manager processes that might be running.

To stop any remaining N1 System Manager processes, type **`kill -9`** *PID* where *PID* is the process ID of the N1 System Manager process.

3 Type `n1smconfig` to run the configuration process.

Step through the configuration process and accept the displayed values. Do not change any value *except* when asked whether to Enable N1SM to start at each boot.

4 **When asked** `Enable N1SM to start at each boot? (n/[y])`**, type** **`n`.**

Step through the rest of the configuration process and accept the displayed values. Type **`n`** when asked whether to restart N1SM.

5 **Ensure all N1 System Manager process have stopped as described in Step 2.**

Next Steps Reconfigure the management server system files as described in the next section.

Reconfiguring Operating System Files

This section provides the procedures for reconfiguring the operating system files. This must be done before you reconfigure the N1 System Manager.

▼ To Reconfigure Solaris Operating System Files for Rehosting

Before You Begin Ensure that the N1 System Manager Start on Reboot feature has been disabled as described in "Disabling N1 System Manager Start on Reboot" on page 34.

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

2 **Edit the file `/etc/hosts` and change the displayed hostname and IP address to the new hostname and IP address.**

3 **Edit the file `/etc/nodename` and change the displayed hostname to the new hostname.**

4 **Edit the `/etc/hostname.`*port type* where *port type* is the name of the Ethernet port type.**

The port type name is dependent on the underlying hardware, for example `/etc/hostname.bge0` or `/etc/hostname.hme0`.

Change the displayed hostname to the new hostname.

5 **Power down the management server.**

6 **Connect the management server to the new network.**

7 **Reboot the management server.**

When the management server has completed rebooting, ensure that no N1 System Manager processes are running.

Next Steps Reconfigure the N1 System Manager system files as described in "Reconfiguring the Management Server" on page 36.

▼ To Reconfigure Linux Operating System Files for Rehosting

Before You Begin Ensure that the N1 System Manager Start on Reboot feature has been disabled as described in "Disabling N1 System Manager Start on Reboot" on page 34.

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

2. **Edit the file `/etc/hosts` and change the displayed hostname and IP address to the new hostname and IP address.**

3. **Edit the file `/etc/sysconfig/network` and change the displayed hostname to the new hostname.**

4. **Edit each `/etc/sysconfig/network-scripts/ifcfg-`*ethx* where *ethx* is the name of the Ethernet port type.**

   For example `/etc/sysconfig/network-scripts/ifcfg-eth0` and `/etc/sysconfig/network-scripts/ifcfg-eth1`.

   Change the displayed IP address to the new IP address. If your management server uses separate Ethernet ports for the management and provisioning networks, ensure that you specify the correct IP address to each port.

5. **Power down the management server.**

6. **Connect the management server to the new network.**

7. **Reboot the management server.**

   When the management server has completed rebooting, ensure that no N1 System Manager processes are running.

Next Steps Reconfigure the N1 System Manager system files as described in the next section.

Reconfiguring the Management Server

This section provides the procedure for reconfiguring N1 System Manager on the management server.

▼ To Reconfigure the Management Server For Rehosting

Before You Begin Operating system files must be reconfigured for rehosting as described in "Reconfiguring Operating System Files" on page 35.

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

2. **Ensure the N1 System Manager is not running.**

3 **Type `n1smconfig` to start the reconfiguration process.**

4 **Respond to each of the configuration prompts according to the requirements of the network to which the N1 System Manager management server is being rehosted.**

For configuration details, see "Configuring the N1 System Manager" on page 17.

CHAPTER 3

Upgrading the Sun N1 System Manager Software

This chapter provides the procedure for upgrading your N1 System Manager 1.2 management server to N1 System Manager 1.3. If you are upgrading from Sun N1 System Manager version 1.1 to version 1.3, you must first upgrade your version 1.1 N1 System Manager to version 1.2 as described in Chapter 3, "Upgrading the Sun N1 System Manager Software," in *Sun N1 System Manager 1.2 Installation and Configuration Guide*

The following topics are discussed:

- "Upgrading to Sun N1 System Manager 1.3" on page 39
- "Removing the N1 System Manager Version 1.2 `n1gc` Account" on page 42
- "Updating Managed Servers For Use by the Grid Engine" on page 42

Note –

- **Security warning:** Managed servers on which the Solaris operating system has been deployed by N1 System Manager have a user account named `n1gc`. The `n1gc` user account is no longer needed and should be removed as described in "Removing the N1 System Manager Version 1.2 `n1gc` Account" on page 42.
- If you are going to use managed servers with the Grid Engine, and if the OS monitoring or base management features have been enabled for the managed servers, then update the servers for Grid Engine deployment as described in "Updating Managed Servers For Use by the Grid Engine" on page 42

Upgrading to Sun N1 System Manager 1.3

This section provides the procedure for upgrading N1 System Manager 1.2 on the management server to N1 System Manager 1.3.

▼ To Upgrade the Sun N1 System Manager Software

Before You Begin Back up your N1 System Manager installation as described in Chapter 3, "Backing Up and Restoring," in *Sun N1 System Manager 1.3 Discovery and Administration Guide*.

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

2. **Stop all N1 System Manager processes.**

   - On a Solaris management server, type **`svcadm disable n1sm`**
   - On a Linux management server, type **`/etc/init.d/n1sminit stop`**

   Wait for all N1 System Manager processes to stop.

3. **Change directory to the N1 System Manager installation source.**

   If you are installing from the N1 System Manager DVD, change directory as follows.

   - Solaris SPARC-based management server:

     ```
     # cd /cdrom/n1_system_mngr/Solaris_sparc/Product/installer
     ```

   - Solaris x86-based management server:

     ```
     # cd /cdrom/n1_system_mngr/Solaris_x86/Product/installer
     ```

   - Linux x86-based management server:

     ```
     # cd /cdrom/n1_system_mngr/Linux_x86/Product/installer
     ```

   If you are installing from an N1 System Manager installation ISO image, substitute your mount point directory name for `/cdrom` in the path names.

4. **Type `./install -u` to start the upgrade installation process**

   The Software Evaluation Agreement appears.

5. **Choose whether to accept the agreement and continue installation.**

   Read the agreement carefully. Type **`y`** to continue installation, or type **`n`** to exit the installation.

   When you continue the upgrade, the upgrade script checks for required Perl modules. When this process completes, the upgrade process then checks the component versions on the management server against the application versions in the N1 System Manager 1.3 installation media. The N1SM Installer upgrade menu then appears, listing which components are up to date, and for which components an upgrade is available.

   The appearance of the N1SM Upgrade menu, and the list of components to be upgraded depends on the operating system installed on the management server as shown by the following examples.

   – Solaris 10 Based Management Server

```
             N1SM Upgrade (version 1.2 to 1.3 on SunOS)

  1. Install IPMI tool.                             [Up to Date]
  2. Install JDK 1.5.                               [Up To Date]
  3. Install service provisioning components.       [Upgrade Available]
  4. Install OS provisioning components.            [Upgrade Available]
  5. Install user interface components.             [Upgrade Available]
  6. Install service container components.          [Up to Date]
  7. Install N1 System Manager.                     [Upgrade Available]


 Non-interactive install in progress

 Executing current step:  Install OS packages...
```

- Linux Based Management Server

```
                  N1SM Upgrade (version 1.2 to 1.3 on Linux)

  1. Install IPMI tool.                             [Up To Date]
  2. Install JDK 1.5.                               [Up To Date]
  3. Install Python.                                [Up To Date]
  4. Install service provisioning components.       [Upgrade Available]
  5. Install OS provisioning components.            [Upgrade Available]
  6. Install user interface components.             [Upgrade Available]
  7. Install service container components.          [Up To Date]
  8. Install N1 System Manager.                     [Upgrade Available]


 Non-interactive upgrade in progress.

 Executing current step:  Install IPMI tool...
```

The installation process runs each step in sequence. When a step completes successfully, the status of the step is changed to `[Up to Date]`.

If a step fails, you are notified, and the status remains `[Upgrade Available]` or is changed to `[Partially Run]`. Exit the installation process and examine the log file `/var/tmp/installer.log.latest` to determine the cause of the failure. Correct the problem and then run the upgrade process again.

When the upgrade process completes, all running N1 System Manager processes are stopped and restarted, and then you are informed that the N1 System Manager upgrade process is complete.

The installation process then exits. You are prompted to run the `n1smconfig` utility. N1 System Manager 1.3 provides several new features that must be configured before you restart the N1 System Manager. Run `n1smconfig` as directed in "Configuring the N1 System Manager" on page 17.

Next Steps Remove the N1 System Manager Version 1.2 `n1gc` account as described in the next section.

Removing the N1 System Manager Version 1.2 `n1gc` Account

Managed servers on which the Solaris operating system has been deployed by N1 System Manager have a user account named `n1gc`. The `n1gc` user account is no longer needed and should be removed. Removal of the `n1gc` user account does not affect N1 System Manager 1.3 functionality.

The method used for removal of the `n1gc` user account depends on whether base management is enabled for the managed server.

- If base management is enabled, remove the `n1gc` user account as follows from. the N1 System Manager command line:
  - For a single managed server, type:

    ```
    start server server command "/usr/sbin/userdel n1gc"
    ```
  - For a group of managed servers, type:

    ```
    start group groupip command "/usr/sbin/userdel n1gc"
    ```

  For information about the base management feature, see "Adding and Upgrading Base Management and OS Monitoring Features" in *Sun N1 System Manager 1.3 Discovery and Administration Guide*
- If base management is not enabled, refer to your operating system documentation for user account removal procedures.

Updating Managed Servers For Use by the Grid Engine

If you are going to use managed servers on which the OS monitoring or base management features have been enabled, the features must be updated before the managed servers can be used by the Grid Engine.

- To update the OS monitoring feature on managed servers:
  - For a single managed server, type:

    ```
    add server server feature osmonitor upgrade=true
    ```
  - For a group of managed servers, type:

    ```
    add group group feature osmonitor upgrade=true
    ```
- To update the base management feature on managed servers:
  - For a single managed server, type:

    ```
    add server server feature basemanagement upgrade=true
    ```
  - For a group of managed servers, type:

    ```
    add group group feature basemanagement upgrade=true
    ```

For information about the base management and OS monitoring features, see "Adding and Upgrading Base Management and OS Monitoring Features" in *Sun N1 System Manager 1.3 Discovery and Administration Guide*

◆ ◆ ◆ CHAPTER 4

Uninstalling the Sun N1 System Manager Software

This chapter provides the procedures for uninstalling the N1 System Manager software from the management server.

Before you uninstall the N1 System Manager, back up your N1 System Manager installation as described in Chapter 3, “Backing Up and Restoring,” in *Sun N1 System Manager 1.3 Discovery and Administration Guide*.

Uninstalling the Sun N1 System Manager Software

This section provides the procedures for uninstalling the N1 System Manager software.

▼ To Uninstall the N1 System Manager Software

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

2 **Stop all N1 System Manager processes.**

See Table 1–1 for operating system dependent commands.

Wait for the message `N1 services stopped` to appear before continuing.

3 Type `/n1gc-setup/installer/install -e` to uninstall the N1 System Manager software.

Depending on the operating system installed on the management server, one of the following menus appears.

```
          N1SM Installer (SunOS)

 1. Uninstall OS packages.                          [Not Uninstalled]
 2. Uninstall Expect.                               [Not Uninstalled]
 3. Uninstall IPMI tool.                            [Not Uninstalled]
 4. Uninstall JDK 1.5.                              [Not Uninstalled]
 5. Uninstall service provisioning components.      [Not Uninstalled]
 6. Uninstall OS provisioning components.           [Not Uninstalled]
 7. Uninstall user interface components.            [Not Uninstalled]
 8. Uninstall service container components.         [Not Uninstalled]
 9. Uninstall N1 System Manager.                    [Not Uninstalled]


Non-interactive uninstall in progress

Executing current step:  Install OS packages...

                N1SM Installer (Linux)


 1. Uninstall empty directories.                     [Not Uninstalled]
 2. Uninstall IPMI tool.                             [Not Uninstalled]
 3. Uninstall JDK 1.5.                               [Not Uninstalled]
 4. Uninstall Python.                                [Not Uninstalled]
 5. Uninstall service provisioning components.       [Not Uninstalled]
 6. Uninstall OS provisioning components.            [Not Uninstalled]
 7. Uninstall user interface components.             [Not Uninstalled]
 8. Uninstall service container components.          [Not Uninstalled]
 9. Uninstall N1 System Manager.                     [Not Uninstalled]




Non-interactive uninstall in progress.
```

The uninstall process begins uninstalling the N1 System Manager software and components in reverse order. When the uninstall process completes, the message `N1SM is uninstalled` appears.

4 Reboot the management server before performing further tasks.

APPENDIX A

Sun N1 System Manager Protocol, Ports, and Features Reference

The tables in this appendix provide summaries of the protocols, ports, features, and services of the N1 System Manager management server, the managed servers, and the configuration options for each.

TABLE A–1 Management Server Protocol, Ports, and Features Reference and Ports

DHCP	
Network access	Provisioning Network
Default port	67, 68 (server)
Router and Firewall Configuration	DHCP Relay required in routed networks.
Port Configurable?	no
Feature That Maps to the Port	Responds to DHCP requests from managed servers during netboot.
Enable or Disable?	The DHCP service is enabled by the N1 System Manager during the netboot phase of OS deployment and is disabled thereafter.
Authentication	None
Data encryption	None
FTP	
Network access	Management Network
Default port	TCP:21 (server)
Router and Firewall Configuration	No
Port Configurable?	No
Feature That Maps to the Port	Firmware Management for ALOM based systems
Enable or Disable?	Indirectly through manual assertion

TABLE A–1 Management Server Protocol, Ports, and Features Reference and Ports *(Continued)*

Authentication	Randomly generated user and password account on the N1 System Manager server. Not user configurable
Data encryption	No
HTTP	
Network access	Provisioning Network
Default port	80 (server)
Router and Firewall Configuration	No
Port Configurable?	No
Feature That Maps to the Port	Required during disk-full OS Deployment of Red Hat Enterprise Linux and SUSE Linux Enterprise Server.
Enable or Disable?	No
Authentication	User ID and password
Data encryption	No
HTTP	
Network access	Management Network
Default port	TCP:80 (client)
Router and Firewall Configuration	No
Port Configurable?	No
Feature That Maps to the Port	Launch of Web Console for the Sun Fire T1000 and T2000 managed servers from within the N1 System Manager browser interface.
Enable or Disable?	Yes. Use the `n1smconfig` to enable or disable, which will shutdown and restart the N1 System Manager.
Authentication	User ID and password
Data encryption	No.
HTTPS	
Network access	Corporate Network
Default port	6789 (server)
Router and Firewall Configuration	No
Port Configurable?	Port 6789 is registered by the N1 System Manager browser interface. Override is not recommended
Feature That Maps to the Port	Serves content to the N1 System Manager browser interface.

TABLE A–1 Management Server Protocol, Ports, and Features Reference and Ports *(Continued)*

Enable or Disable?	Port must be exclusively owned by the N1 System Manager browser interface and cannot be disabled while the N1 System Manager is running.
Authentication	PAM based Authentication done by the N1 System Manager browser interface component.
Data encryption	Yes, through certificates
ICMP	
Network access	Provisioning Network
Default port	5813 (client)
Router and Firewall Configuration	No
Port Configurable?	Well known port. Override is not recommended.
Feature That Maps to the Port	Network monitoring of a running OS on managed servers.
Enable or Disable?	No
Authentication	None
Data encryption	No
ICMP	
Network access	Management Network
Default port	5813 (client)
Router and Firewall Configuration	No
Port Configurable?	Well known port. Override is not recommended.
Feature That Maps to the Port	Network monitoring of service processor interfaces
Enable or Disable?	No
Authentication	None
Data encryption	No
IPMI	
Network access	Management Network
Default port	TCP:623 (client)
Router and Firewall Configuration	No
Port Configurable?	No
Feature That Maps to the Port	Discovery using IPMI based service processor

TABLE A–1 Management Server Protocol, Ports, and Features Reference and Ports *(Continued)*

Enable or Disable?	Indirectly through manual assertion
Authentication	User/password
Data encryption	No
JDBC	
Network access	Local host
Default port	5434 (server)
Router and Firewall Configuration	Not applicable
Port Configurable?	Yes. Modify the file `/opt/sun/N1_Service_Provisioning_System_5.1/server/postgres/data/postgresql.conf`
Feature That Maps to the Port	Service provisioning Postgres database server
Enable or Disable?	No
Authentication	User/password
Data encryption	No
JDBC	
Network access	Local host
Default port	5434 (client)
Router and Firewall Configuration	Not applicable
Port Configurable?	Yes. Modify the file `/etc/opt/sun/cacao/modules/servicescommonmodule.xml`
Feature That Maps to the Port	Service provisioning Postgres database server client
Enable or Disable?	No
Authentication	User ID and password
Data encryption	No
JDBC	
Network access	Local host
Default port	5433 (server)
Router and Firewall Configuration	Not applicable
Port Configurable?	Yes. Modify the file `/var/opt/sun/scs/data/db/mgmt/postgresql.conf`

TABLE A–1 Management Server Protocol, Ports, and Features Reference and Ports *(Continued)*

Feature That Maps to the Port	SCS Postgres database server
Enable or Disable?	No
Authentication	User/password
Data encryption	No
JDBC	
Network access	Local host
Default port	5433 (client)
Router and Firewall Configuration	Not applicable
Port Configurable?	Yes. Modify the file `/etc/opt/sun/cacao/modules/servicescommonmodule.xml`
Feature That Maps to the Port	SCS Postgres Database client
Enable or Disable?	No
Authentication	User ID and password
Data encryption	None
JMXMP	
Network access	localhost
Default port	10162 (server)
Router and Firewall Configuration	No
Port Configurable?	No
Feature That Maps to the Port	Used by all features. This port is opened by the common agent container Mbean Server.
Enable or Disable?	Port 10162 must be owned exclusively by the common agent container and cannot be disabled while the N1 System Manager is running.
Authentication	PAM based authentication for `UnknownClient` connection requests.
Data encryption	Yes
JMXMP	
Network access	localhost
Default port	10162 (client)
Router and Firewall Configuration	No
Port Configurable?	Yes. By editing `cacao.properties`.

TABLE A–1 Management Server Protocol, Ports, and Features Reference and Ports *(Continued)*

Feature That Maps to the Port	Used by the N1 System Manager browser interface component to connect to the common agent container Mbean server using the `JMX UnknownClient` connection.
Enable or Disable?	No
Authentication	PAM
Data encryption	Yes
JMXMP	
Network access	localhost
Default port	10163 (server)
Router and Firewall Configuration	No
Port Configurable?	Yes. By editing `cacao.properties`.
Feature That Maps to the Port	Used by the N1 System Manager `n1sh` command line interface to connect to the common agent container `CommandStream` adaptor using the JMX `WellknownClient` connection.
Enable or Disable?	No
Authentication	Yes. Public key based.
Data encryption	Yes
JMXMP	
Network access	localhost
Default port	10163 (client)
Router and Firewall Configuration	No.
Port Configurable?	Yes, by modifying `cacao.properties`.
Feature That Maps to the Port	Used by the N1 System Manager `n1sh` command line interface to establish the `WellKnownClient` connection to CSA in the common agent container `MbeanServer`.
Enable or Disable?	No
Authentication	Key based authentication
Data encryption	Yes
NFS	
Network access	Provisioning Network
Default port	TCP/UDP:2049 (server)

TABLE A–1 Management Server Protocol, Ports, and Features Reference and Ports *(Continued)*

Router and Firewall Configuration	No
Port Configurable?	Well-know port. Override is not recommended
Feature That Maps to the Port	Used by the N1 System Manager to export file systems during disk-full OS deployment process for Solaris only.
Enable or Disable?	Must always be running if OS deployment is a desired feature. NFS is not automatically enabled or disabled by the N1 System Manager.
Authentication	None
Data encryption	No
SMTP	
Network access	Management Network
Default port	TCP:25 (server)
Router and Firewall Configuratio	No
Port Configurable?	No
Feature That Maps to the Port	Email alert based detection of hardware monitoring threshold violations for ALOM based managed servers
Enable or Disable?	Yes. Set *monitored=false* using the N1 System Manager, but not independent of OS monitoring.
Authentication	Email account user and password configured manually prior to installation
Data encryption	None
SNMP V1	
Network access	All
Default port	UDP:8089 (server)
Router and Firewall Configuration	No
Port Configurable?	Yes. By editing the configuration file entry as root user. Requires restart of the N1 System Manager to activate.
Feature That Maps to the Port	SNMP read requests for info Management Information Base (MIB) OIDs from external SNMP Managers
Enable or Disable?	The SNMP agent is active as long as the N1 System Manager is running. The SNMP agent cannot be disabled at N1 System Manager startup time or while the N1 System Manager is running.
Authentication	SNMP V1 Community string. Community strings are passed in clear text and are not configurable.

TABLE A–1 Management Server Protocol, Ports, and Features Reference and Ports *(Continued)*

Data encryption	None
SNMP V1	
Network access	All
Default port	UDP:162 (server)
Router and Firewall Configuration	No
Port Configurable?	Yes. By running the `create notification` CLI command.
Feature That Maps to the Port	Send SNMP traps to external SNMP trap listeners per OIDS in the trap MIB.
Enable or Disable?	Cannot be directly disabled at startup time or while the N1 System Manager is running. Can be indirectly disabled by denying privileges to create SNMP Notification Rules in the N1 System Manager.
Authentication	None
Data encryption	None
SNMP V1	
Network access	Management Network
Default port	UDP:162 (server)
Router and Firewall Configuration	No
Port Configurable?	No.
Feature That Maps to the Port	Trap based detection of hardware monitoring threshold violations for the Sun Fire V20z, V40z, X2100, X4100, and X4200.managed servers.
Enable or Disable?	Yes. Set *monitored=false* using the N1 System Manager, but not independent of OS monitoring.
Authentication	None
Data encryption	None
SNMP V1	
Network access	Provisioning Network
Default port	UDP:161 (client)
Router and Firewall Configuration	No
Port Configurable?	Yes. Edit the file `/etc/opt/sun/ n1gc/agent.properties` as root and insert the property `com.sun.hss.agent.snmpAgentPort=`*port number* where *port number* is the new port number. You must configure the port on each managed node agent manually. AnN1 System Manager restart is required.

TABLE A–1 Management Server Protocol, Ports, and Features Reference and Ports *(Continued)*

Feature That Maps to the Port	OS Monitoring
Enable or Disable?	Yes. Do not add the `osmonitor` feature
Authentication	SNMP V1 community string that is configurable using the N1 System Manager
Data encryption	No
SNMP V1	
Network access	Provisioning Network
Default port	UDP:8162 (server)
Router and Firewall Configuration	No
Port Configurable?	Yes. Edit the configuration file as root user and configure the port on each managed node using the N1 System Manager. AnN1 System Manager restart is required.
Feature That Maps to the Port	Trap based detection of OS monitoring threshold violations
Enable or Disable?	Yes. Set *monitored=false* using the N1 System Manager, but not independent of hardware monitoring.
Authentication	None
Data encryption	None
SNMP V3	
Network access	Provisioning Network
Default port	UDP:161 (client)
Router and Firewall Configuration	No
Port Configurable?	Yes. Edit the file `/etc/opt/sun/ n1gc/agent.properties` as root and insert the property `com.sun.hss.agent.snmpAgentPort=`*port number* where *port number* is the new port number. You must configure the port on each managed node agent manually. AnN1 System Manager restart is required.
Feature That Maps to the Port	OS monitoring thresholds configuration
Enable or Disable?	Yes. Do not add the `osmonitor` feature
Authentication	SNMP User-based Security Model (USM) user ID and password that is configurable using the N1 System Manager.
Data encryption	Yes
SSH	
Network access	Provisioning Network

TABLE A–1 Management Server Protocol, Ports, and Features Reference and Ports *(Continued)*

Default port	TCP:22 (server)
Router and Firewall Configuration	No
Port Configurable?	Well known port. Override is not recommended.
Feature That Maps to the Port	Required to enable remote login by authorized users who want to launch the `n1sh` command line interface.
Enable or Disable?	May be disabled and enabled at the OS level by the root user. Restart of the N1 System Manager is not required.
Authentication	PAM
Data encryption	Yes
SSH	
Network access	Provisioning Network
Default port	TCP:22 (client)
Router and Firewall Configuration	No
Port Configurable?	Well known port. Override is not recommended.
Feature That Maps to the Port	1. OS monitoring 2. Package deployment 3. Remote command
Enable or Disable?	Yes. Do not add the base management feature.
Authentication	User password and key based
Data encryption	Yes
SSH	
Network access	Management Network
Default port	TCP:22 (client)
Router and Firewall Configuration	No
Port Configurable?	No
Feature That Maps to the Port	1. Discovery 2. Firmware management 3. Hardware monitoring 4. Netboot control for Sun Fire V20z and V40z systems using the service provisioning command line interface for AMD based systems
Enable or Disable?	Indirectly through manual assertion

TABLE A–1 Management Server Protocol, Ports, and Features Reference and Ports *(Continued)*

Authentication	User ID and password specified during discovery
Data encryption	Yes
TELNET	
Network access	Management Network
Default port	TCP:23 (client)
Router and Firewall Configuration	No
Port Configurable?	No
Feature That Maps to the Port	1. Discovery 2. Power Management 3. Hardware monitoring 4. Firmware management 5. Netboot control using the service processor command line interface for for ALOM based systems
Enable or Disable?	Indirectly through manual assertion
Authentication	User/password, configurable during discovery
Data encryption	No
TFTP	
Network access	Management Network
Default port	UDP: Random (server)
Router and Firewall Configuration	No
Port Configurable?	Not applicable
Feature That Maps to the Port	Firmware Management for the Sun Fire V20z and V40z
Enable or Disable?	Indirectly through manual assertion
Authentication	None
Data encryption	No

TABLE A–2 Managed Server Protocol, Ports, and Features Reference

DHCP	
Network access	Provisioning Network

TABLE A–2 Managed Server Protocol, Ports, and Features Reference *(Continued)*

Default port	67, 68 (client)
Router and Firewall Configuration	DHCP Relay required in routed networks
Port Configurable?	Well known port. Override is not recommended.
Feature That Maps to the Port	Broadcasts DHCP requests during netboot
Enable or Disable?	No
Authentication	None
Data encryption	None
FTP	
Network access	Management Network
Default port	TCP:21 (client)
Router and Firewall Configuration	No
Port Configurable?	No
Feature That Maps to the Port	Firmware Management for ALOM based systems
Enable or Disable?	Indirectly through manually deleting account on the service processor
Authentication	Randomly generated user and password account on the N1 System Manager server. Not user configurable
Data encryption	None
HTTP	
Network access	Provisioning Network
Default port	80 (client)
Router and Firewall Configuration	No
Port Configurable?	No
Feature That Maps to the Port	Required during disk-full OS deployment of Red Hat Enterprise Linux and SUSE Linux Enterprise Server.
Enable or Disable?	No
Authentication	None
Data encryption	None
ICMP	

TABLE A–2 Managed Server Protocol, Ports, and Features Reference *(Continued)*

Network access	Management Network
Default port	5813 (server)
Router and Firewall Configuration	No
Port Configurable?	Well known port. Override is not recommended.
Feature That Maps to the Port	Network monitoring of service processor interfaces for AMD and SPARC based systems.
Enable or Disable?	No
Authentication	None
Data encryption	None
IPMI	
Network access	Management Network
Default port	TCP: 623 (server)
Router and Firewall Configuration	No
Port Configurable?	No
Feature That Maps to the Port	1. Discovery 2. Power operations 3. Hardware monitoring 4. Service processor and BIOS firmware management 5. Netboot control using IPMI based service processor for AMD based systems
Enable or Disable?	Indirectly by manually deleting account on SP
Authentication	None
Data encryption	None
NFS	
Network access	Provisioning Network
Default port	2049 (client)
Router and Firewall Configuration	No
Port Configurable?	Well known port. Override is not recommended.
Feature That Maps to the Port	Mounts remote file systems during disk-full OS Deployment process for Solaris and Linux only.

TABLE A–2 Managed Server Protocol, Ports, and Features Reference *(Continued)*

Enable or Disable?	No
Authentication	None
Data encryption	None
SNMP V1	
Network access	Provisioning Network
Default port	TCP:161 (server)
Router and Firewall Configuration	No
Port Configurable?	Yes. See SNMP V1 in Table A–1.
Feature That Maps to the Port	OS monitoring
Enable or Disable?	Yes. See SNMP V1 in Table A–1.
Authentication	SNMP V1 Community String. Configurable using `n1smconfig`
Data encryption	None
SNMP V1	
Network access	Management Network
Default port	UDP:162 (client)
Router and Firewall Configuration	No
Port Configurable?	Yes. See SNMP V1 in Table A–1.
Feature That Maps to the Port	Trap based detection of hardware monitoring threshold violations
Enable or Disable?	Yes. See SNMP V1 in Table A–1.
Authentication	None
Data encryption	None
SNMP V1	
Network access	Provisioning Network
Default port	UDP:8162 (client)
Router and Firewall Configuration	No
Port Configurable?	Yes. See SNMP V1 in Table A–1.
Feature That Maps to the Port	Trap based detection of OS monitoring threshold violations

TABLE A–2 Managed Server Protocol, Ports, and Features Reference *(Continued)*

Enable or Disable?	Yes. See SNMP V1 in Table A–1.
Authentication	None
Data encryption	None
SNMP V3	
Network access	Provisioning Network
Default port	TCP:161 (server)
Router and Firewall Configuration	No
Port Configurable?	Yes. See SNMP V3 in Table A–1.
Feature That Maps to the Port	OS monitoring threshold configuration
Enable or Disable?	Yes. See SNMP V3 in Table A–1.
Authentication	SNMP USM user ID and password. Configurable using `n1smconfig`.
Data encryption	None
SSH	
Network access	Management Network
Default port	TCP: 22 (server)
Router and Firewall Configuration	No
Port Configurable?	No
Feature That Maps to the Port	1. Discovery 2. Firmware management 3. Hardware monitoring 4. Netboot control for the V20z and V40z systems using the service processor command line interface for AMD based systems
Enable or Disable?	Indirectly by manually deleting account on service processor
Authentication	User account and password configured manually on service processor
Data encryption	Yes
SSH	
Network access	Provisioning Network

TABLE A–2 Managed Server Protocol, Ports, and Features Reference *(Continued)*

Default port	TCP: 22 (client)
Router and Firewall Configuration	No
Port Configurable?	Well known port. Override not recommended.
Feature That Maps to the Port	1. OS Monitoring 2. Package deployment 3. Remote command
Enable or Disable?	Yes. Custom install script
Authentication	User password and key based
Data encryption	Yes
TELNET	
Network access	Management Network
Default port	TCP:23 (server)
Router and Firewall Configuration	No
Port Configurable?	No
Feature That Maps to the Port	1. Discovery 2. Power Management 3. Hardware monitoring 4. Firmware management 5. Netboot control using the service processor command line interface for ALOM based systems
Enable or Disable?	Indirectly by manually deleting account on the service processor
Authentication	User ID and password, specified during discovery
Data encryption	None
TFTP	
Network access	Management Network
Default port	UDP:Random (client)
Router and Firewall Configuration	No
Port Configurable?	Not applicable
Feature That Maps to the Port	Firmware management for Sun Fire V20z and V40z systems

TABLE A–2 Managed Server Protocol, Ports, and Features Reference *(Continued)*

Enable or Disable?	No
Authentication	None
Data encryption	None

Index