Sun N1 System Manager 1.2 Administration Guide

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

Part No: 819–4143
November 2005

051118@13215

Contents

Tables

Figures

Examples

Preface

The Sun N1 System Manager Administration Guide helps system administrators to understand and administer the Sun N1™ System Manager. This book provides detailed examples and procedures to explain how you can use the N1 System Manager to manage users and roles, discover servers to be managed, provision OSs on the servers, install OS and firmware updates, and set up monitoring.

Note – Most of the information in this book focuses on the command-line interface of the N1 System Manager. Instructions are provided when the browser interface can also be used for the same task. Click the Help button in the upper right corner of the browser interface to access the searchable online help system.

Who Should Use This Book

This guide is intended for system administrators who are responsible for managing provisionable servers running the Sun N1 System Manager software. These system administrators are expected to have the following background:

- Knowledge of the Solaris™ Operating System and Red Hat Linux, and the network administration tools provided by each operating system
- Knowledge of network equipment and network devices from a variety of vendors such as Sun Microsystems, Cisco, Foundry, and Extreme
- Knowledge of network device interconnections and cabling
- Knowledge of the Simple Network Management Protocol (SNMP). Some elements of the N1 System Manager use software that is based on SNMP.

Before You Read This Book

Read the following documents:

- *Sun N1 System Manager 1.2 Introduction*
- *Sun N1 System Manager 1.2 Site Preparation Guide*
- *Sun N1 System Manager 1.2 Installation and Configuration Guide*

How This Book Is Organized

Chapter 1 describes the following:

- How to type commands in the N1 System Manager by using the command-line interface and the browser interface
- Session roles and the `n1sh` script file
- Security and how to add, remove, and manage users and roles
- How to backup and recover database and configuration files

Chapter 2 describes the following:

- The discovery process
- How to add provisionable servers to groups
- How to replace failed servers

Chapter 3 describes the following:

- Conceptual and procedural information about how to manage OS installations
- Conceptual and procedural information about performing OS updates
- Conceptual and procedural information about performing firmware updates

Chapter 4 describes the following:

- How to refresh servers and groups
- How to replace servers and groups
- How to rename servers and groups
- How to reboot servers and groups
- How to remove servers and groups

Chapter 5 describes the following:

- An overview of how monitoring works
- How to support monitoring by ensuring key features are installed
- How to switch on monitoring for servers and groups

- How to set and manage thresholds
- How to view and manage jobs
- How to view, manage and create event notifications

Chapter 6 describes how to identify and manage the following possible troubleshooting scenarios:

- Possible problems with server discovery
- Possible problems with security
- Possible problems with OS distributions
- OS deployment failures
- Possible problems with OS updates
- Problems with firmware updates
- Problems after restarting services

Related Books

The following books are useful for installing and using the N1 System Manager.

- *Sun N1 System Manager 1.2 Introduction*
- *Sun N1 System Manager 1.2 Site Preparation Guide*
- *Sun N1 System Manager 1.2 Installation and Configuration Guide*
- *Sun N1 System Manager 1.2 Command Line Reference Manual*
- *Sun N1 System Manager 1.2 Release Notes*

Documentation, Support, and Training

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

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

Typographic Conventions

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

TABLE P–1 Typographic Conventions

Typeface	Meaning	Example
`AaBbCc123`	The names of commands, files, and directories, and onscreen computer output	Edit your `.login` file. Use `ls -a` to list all files. `machine_name% you have mail.`
`AaBbCc123`	What you type, contrasted with onscreen computer output	`machine_name%` **`su`** `Password:`
aabbcc123	Placeholder: replace with a real name or value	The command to remove a file is `rm` *filename*.
AaBbCc123	Book titles, new terms, and terms to be emphasized	Read Chapter 6 in the *User's Guide*. A *cache* is a copy that is stored locally. Do *not* save the file. **Note:** Some emphasized items appear bold online.

Shell Prompts in Command Examples

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

TABLE P–2 Shell Prompts

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

TABLE P–2 Shell Prompts *(Continued)*

Shell	Prompt
Bourne shell and Korn shell for superuser	#

In this book, unless otherwise specified, the term *command line* is used to describe the `n1sh` shell, which uses the `N1-ok>` prompt. The `n1sh` shell is defined as any of the following:

- The shell available from the Command Line pane of the browser interface
- The shell available after typing `n1sh` in a terminal console window on the management server

You can also use N1 System Manager commands from a standard UNIX shell by preceding them with the `n1sh` command.

CHAPTER 1

Managing the N1 System Manager on the Management Server

This chapter provides information about the N1 System Manager user interfaces, security features, user management, and backup and restore procedures for the management server. For an overview of the Sun N1 System Manager features and components, see the *Sun N1 System Manager 1.2 Introduction*.

The main sections in this chapter are as follows:

Introduction to Accessing the N1 System Manager

The two ways to manage a rack of provisionable servers using the N1 System Manager are as follows:

- Command line – The `n1sh` command. The default method is to use the `n1sh` shell, which uses an `N1-ok>` prompt. The shell mode provides a tab completion feature to navigate through all the command options. See the `n1sh` man page for details. Type `man n1sh` from a console in the management server. You don't need to be in the `n1sh` shell to read the `n1sh` man page.
- Browser interface – A web-based user interface that provides a subset of the command line features. The browser interface also includes the `n1sh` shell in the Command Line pane. As you use the browser interface to perform management tasks, the corresponding commands are displayed in the Command Line pane. The

Command Line pane provides the same features as the `n1sh` command in shell mode.

The `n1sh` command provides two other ways to issue management commands. The `n1sh -e` option, or UNIX® command mode, enables you to type management commands one at a time within a UNIX shell. The `n1sh -f` option enables you to specify a custom script of management commands to run. See the `n1sh` man page for details. Type `man n1sh` from a console in the management server. You don't need to be in the `n1sh` shell to read the `n1sh` man page.

Command Line Tips

This section contains a few tips to help you use the N1 System Manager command line interface.

General Syntax

Here is the general syntax for a N1 System Manager command:

command object [*object-value*] [*object* [*object-value*]]* [*attribute*[=][*attribute-value*]]* [*keyword*]*

- *command* – The action taken on the objects.
- *object* – A system-defined object that is fundamental to the operation being performed. The target of the operation is usually the first object in the command's syntax.
- *object-value* – A value for the object, which is usually user-defined. Values containing spaces must be enclosed within quotes.
- *attribute* – A system–defined and optional object that affects the way the operation is performed.
- *attribute–value* – A user-defined value for the attribute. Values containing spaces must be enclosed within quotes.
- *keyword* – A system-defined attribute without a value.

For simplification purposes, the attribute term is usually used to describe both objects and keywords.

User-Defined Names

As a general rule, the command line interface allows the following character syntax for user-defined names, such as OS profile or role names: [A-Za-z][A-Za-z0-9._\-]*.

`id` Keyword

The `id` keyword is an optional keyword that can be used on the N1 System Manager command line before some attribute values, typically for the *server* attribute value. The purpose of this keyword is to provide an attribute value that may be the same name as a reserved keyword (for example, a server named `all`).

Equal Sign

The equal sign (=) can be optionally used between attributes and attribute values on the N1 System Manager command line. For example, the following commands are equivalent:

```
N1-ok> set role MyRole description myDescription
N1-ok> set role MyRole description=myDescription
```

The equal sign variant is not shown in the command line help.

Script Comments

When creating a customized `n1sh` script, you can specify the comment character (#) at the beginning of the line to indicate that the rest of the line should be ignored. See "To Run a Script of N1 System Manager Commands" on page 31 for details.

Multiple Attribute Values

Where allowed, multiple attribute values can be specified as a comma–separated list on the N1 System Manager command line. For example:

```
N1-ok> set server serverA,serverB,serverC locator on
```

In the command line help, multiple attribute values are shown using the following syntax notation: `set server <server>[,<server>...]`

Quotation Marks

Single and double quotation marks are supported on the N1 System Manager command line. If needed, either type of quotation mark can be escaped using the backslash character. For example:

```
N1-ok> set role myRole description "Some Role that I've made up"
N1-ok> set role myRole description='Some Role that I\'ve made up'
```

Special Characters

Depending on the shell you are using to run `n1sh` in UNIX command mode, some special characters may need to be escaped. For example, in the `bash` shell, quotes need to be escaped with the backslash character, like this:

```
$ n1sh set role MyRole description=\"Some Role that \\\"Paul\\\" made up\"
```

See your specific shell's documentation for detailed information on escaping special characters.

In the `n1sh` shell mode, you do not have to escape special characters, so the same command described above would look like this:

```
N1-ok> set role MyRole description="Some Role that \"Paul\" made up"
```

Hiding Passwords

You can enter a question mark (?) for any password attribute value if you do not want the password to display in the command line. Once you enter the command, you are prompted for the password. Examples include the `rootpassword` and `agentssh` attributes.

▼ To Access the N1 System Manager Command Line

The following procedure describes how to access the N1 System Manager command line (the `n1sh` shell) as a valid user from a remote system. You can also access the command line directly on the management server.

Before You Begin

During management server configuration, the superuser (`root`) account is set up with all the system default roles added to it (`Admin`, `ReadOnly`, and `SecurityAdmin`). If you want to log in as a valid user other than the superuser account, see "To Add an N1 System Manager User" on page 38.

Steps

1. **Log in to the management server from a remote system.**

   ```
   $ ssh -l user-name management-server
   ```

   Where *user-name* is a valid N1 System Manager user, and *management-server* is the host name or IP address of the management server.

   You are prompted for a password.

2. **Type a password for the user account.**

   The `N1-ok>` prompt is displayed and you are logged in with your default N1 System Manager role, unless you use the `-r` option to specify a role for login.

3. **If the `N1-ok>` prompt does not display, type the following command to access the command line:**

   ```
   # /opt/sun/n1gc/bin/n1sh [-r role-name]
   ```

   The superuser (`root`) user account typically does not have its login configured to automatically log in to the `n1sh` shell.

4. **(Optional) To switch to a different N1 System Manager role that has been added to your user account, type the following command:**

   `N1-ok>` **`set session role`** *role*

   See "set session" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.

▼ To Access the N1 System Manager Browser Interface

The following procedure describes how to log in to the N1 System Manager browser interface through the Sun Web Console.

Before You Begin

During management server configuration, the superuser (`root`) account is set up with all the system default roles added to it (`Admin`, `ReadOnly`, and `SecurityAdmin`). If you want to log in as a valid user other than the superuser account, see "To Add an N1 System Manager User" on page 38.

The following browsers are supported:

- Mozilla™ 1.4 or later (Solaris, Linux, or Microsoft Windows version)
- Internet Explorer 6 or later (Microsoft Windows version)

Accessibility features in the N1 System Manager browser interface include descriptions of images and tables, keyboard navigation, and tool tips.

Note – When the cursor is positioned at the `N1-ok>` prompt in the Command Line pane, the arrow keys can be used to view only the previous command typed or the next command in the history. To move the cursor to the top of the Command Line pane, press Shift+Tab and then press the up arrow key. To move focus from the Command Line pane to other areas of the browser interface, press Shift+Tab twice.

Help text near the top of most screens describes the purpose of that screen. Brief help text also appears beneath entry fields and associated check boxes, radio buttons, and text entry fields.

Steps

1. **Log in to the Sun Web Console on the management server through the following URL:**

   `http://`*management-server*

   where *management-server* is the host name or IP address of the management server.

   The browser is automatically redirected to the `https://`*management-server*`:6789` URL, and the Sun Web Console login page is displayed.

2. **Log in to the Sun Web Console by using your N1 System Manager user name and password.**

   The Sun Web Console launch page is displayed.

3. **Click the Sun N1 System Manager link to launch the Sun N1 System Manager browser interface.**

   The browser interface is displayed, and you are logged in with your default N1 System Manager role. See "Access the N1 System Manager" in *Sun N1 System Manager 1.2 Introduction* for an overview of the browser interface.

4. **(Optional) To switch to a different N1 System Manager role that has been added to your user account, type the following command in the Command Line pane:**

   ```
   N1-ok> set session role role
   ```

   See "set session" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.

▼ To Show Your Current Session Role

Your role might affect your ability to access certain features of the N1 System Manager. By default, you are logged into the N1 System Manager with your default role.

See "Managing Roles" on page 42 for more details about roles.

Steps

1. **Log in to the N1 System Manager.**

   See "To Access the N1 System Manager Command Line" on page 28 for details.

2. **Show your current session role.**

   ```
   N1-ok> show session
   ```

▼ To Switch Your Session Role

If you have more than one role, you can switch between multiple roles to perform tasks that require specific privileges.

See "Managing Roles" on page 42 for more details about roles and privileges.

Steps

1. **Log in to the N1 System Manager.**

   See "To Access the N1 System Manager Command Line" on page 28 for details.

2. **Switch to a different session role.**

   ```
   N1-ok> set session role role
   ```

See "set session" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.

▼ To Exit the N1 System Manager Command Line

Step ● **Exit the N1 System Manager command line.**

```
N1-ok> exit
```

The `n1sh` shell is terminated.

▼ To Run a Script of N1 System Manager Commands

The following procedure describes how to run a custom script of N1 System Manager commands that are saved in a file. Return codes are returned for each command. Also, you can specify a comment character (#) at the beginning of the line to indicate that the rest of the line should be ignored.

Steps

1. **Log in to the N1 System Manager.**

   See "To Access the N1 System Manager Command Line" on page 28 for details.

   If the `n1sh` shell is your default login shell on the management server, you must change this configuration. Otherwise, you won't be able to run the `n1sh` command and use the script option.

2. **Run a custom script that contains the N1 System Manager commands.**

   ```
   # /opt/sun/n1gc/bin/n1sh -f filename
   ```

   where *filename* is a fully qualified path to the custom script file.

Example 1–1 `n1sh` Custom Script File

The following example shows an `n1sh` script file, which can be run with the `n1sh -f` command.

```
# n1sh custom script

show group all

create group RACK1
create group RACK2
create group RACK3
create group RACK4
create group RACK5
```

```
add group RACK1 server SERVER1
add group RACK1 server SERVER2

add group RACK2 server SERVER3
add group RACK2 server SERVER4


add group RACK3 server SERVER5
add group RACK3 server SERVER6

add group RACK4 server SERVER7
add group RACK4 server SERVER8

add group RACK4 server SERVER9
add group RACK4 server SERVER10

add group RACK5 server SERVER11
add group RACK5 server SERVER12

show group all
```

Introduction to N1 System Manager User Security

This section provides information about how to set up and manage user security for the N1 System Manager.

The following tasks are used to manage N1 System Manager users:

- "To Add an N1 System Manager User" on page 38
- "To Delete an N1 System Manager User" on page 39
- "To Set a User's Default Role" on page 40
- "To Show a User's Default Role" on page 41
- "To Add a Role to a User" on page 41
- "To Remove a Role From a User" on page 41
- "To List the Roles Added to a Specific User" on page 42

The following tasks are used to manage N1 System Manager roles:

- "To Create a Role" on page 43
- "To Delete a Role" on page 43
- "To Add a Privilege to a Role" on page 44
- "To Remove a Privilege From a Role" on page 44
- "To List the Available Roles" on page 44
- "To List Privileges Added to a Role" on page 45
- "To List the Roles Added to All Users" on page 45

- "To List the Available Privileges" on page 45

The N1 System Manager provides a user account system that allows users to have role-based access to its main features (commands and browser interface areas) through a predefined, fixed set of privileges. A *privilege* is a predefined set of permissions enabling a user to perform operations within the N1 System Manager, such as installing OS distributions or deleting jobs. A *role* is a set of privileges to which a user has access. The N1 System Manager provides three system default roles, but customized roles can be created depending on your needs.

The following table lists the system default roles that are automatically provided by the N1 System Manager. These system default roles cannot be modified.

TABLE 1–1 System Default Roles

Role	Privileges	Description
`Admin`	All privileges except `SecurityAdmin` privileges	This role has all the privileges available on the N1 System Manager except those required for role management, which is provided by the `SecurityAdmin` role.
`ReadOnly`	All read-only (`*Read`) privileges except `SecurityAdmin` privileges	This role allows the user to view only status (read-only) information about the N1 System Manager.
`SecurityAdmin`	`RoleRead`, `RoleWrite`, `UserRead` , `UserWrite`, `PrivilegeRead`	This role only has the privileges required to perform role management operations, such as creating roles, adding privileges to roles, and adding roles to users.

When you install the Sun N1 System Manager software, the management server's superuser (`root`) account has all three system default roles automatically added to it, and the `Admin` role is the account's default role.

Users with the `SecurityAdmin` role (security administrators) are allowed to create new roles as needed in their organization, which includes adding one or more privileges to those roles. Security administrators can also add roles to users.

For example, you might need to restrict specific users to perform only OS update management on the provisionable servers. A security administrator could create a new role, called `OSUpdateAdmin`, and add the following privileges to it: `GroupRead`, `JobRead`, `LogRead`, `ServerDeployUpdate`, `ServerRead`, `UpdateRead`, and `UpdateWrite`. See Table 1–2 for details about privileges. Then, the security administrator would add that role to those specific users. If `OSUpdateAdmin` is the only role added to the users, the users would not be able to access any part of the N1 System Manager other than the OS update management feature.

Note – Non-root users with only the `SecurityAdmin` role are not allowed to extend their own privilege set, either by adding new privileges to the `SecurityAdmin` role (which cannot be modified) or by adding new roles to their own user account. See "Security Administrator Rules" on page 37 for more details.

The following table lists the set of predefined privileges that may be added to roles. To display an abbreviated form of this list, use the `show privilege` command.

TABLE 1–2 N1 System Manager Privileges

Command	Privileges Required
`add group`	`GroupRead`
	`GroupWrite`
`add osprofile`	`OSProfileWrite`
`add role`	`RoleWrite`
`add server`	`ServerWrite`
`connect server`	`ServerConsole`
`create firmware`	`FirmwareWrite`
`create group`	`GroupRead`
	`GroupWrite`
`create notification`	`NotificationRuleRead`
	`NotificationRuleWrite`
`create os`	`OSWrite`
`create osprofile`	`OSProfileWrite`
`create role`	`RoleWrite`
`create update`	`UpdateRead`
	`UpdateWrite`
`create user`	`UserWrite`
`delete firmware`	`FirmwareRead`
	`FirmwareWrite`
`delete group`	`GroupRead`
	`GroupWrite`
`delete job`	`JobWrite`

TABLE 1–2 N1 System Manager Privileges *(Continued)*

Command	Privileges Required
delete notification	NotificationRuleRead
	NotificationRuleWrite
delete os	OSWrite
delete osprofile	OSProfileWrite
delete role	RoleWrite
delete server	ServerWrite
delete update	UpdateRead
	UpdateWrite
discover	Discover
	JobRead
load group	GroupRead
	FirmwareRead
	FirmwareWrite
	ServerDeployFirmware
	ServerDeployOS
	ServerDeployUpdate
	UpdateRead
load server	FirmwareRead
	FirmwareWrite
	ServerDeployFirmware
	ServerDeployOS
	ServerDeployUpdate
remove group	GroupRead
	GroupWrite
remove osprofile	OSProfileWrite
remove role	RoleWrite
set firmware	FirmwareRead
	FirmwareWrite
set group	GroupRead
	GroupWrite

TABLE 1–2 N1 System Manager Privileges *(Continued)*

Command	Privileges Required
`set group` *group* `refresh`	`ServerRead`
`set notification`	`NotificationRuleRead`
	`NotificationRuleTest`
	`NotificationRuleWrite`
`set os`	`OSWrite`
`set osprofile`	`OSProfileWrite`
`set role`	`RoleWrite`
`set server`	`ServerExecute`
`set server` *server* `refresh`	`ServerRead`
	`ServerWrite`
`show firmware`	`FirmwareRead`
`show group`	`GroupRead`
`show job`	`JobRead`
`show log`	`LogRead`
`show notification`	`NotificationRuleRead`
`show privilege`	`RoleRead`
`show role`	`RoleRead`
`show os`	`OSRead`
`show osprofile`	`OSProfileRead`
	`UpdateRead`
`show server`	`ServerRead`
`show update`	`UpdateRead`
`show user`	`UserRead`
`start group`	`ServerExecute`
	`ServerPower`
`start notification`	`NotificationRuleRead`
	`NotificationRuleTest`
`start server`	`ServerPower`
	`ServerExecute`

TABLE 1–2 N1 System Manager Privileges *(Continued)*

Command	Privileges Required
`stop job`	`JobWrite`
`stop group`	`ServerExecute`
	`ServerPower`
`stop server`	`ServerExecute`
	`ServerPower`
`unload group`	`GroupRead`
	`ServerDeployUpdate`
	`UpdateRead`
`unload server`	`ServerDeployUpdate`
	`UpdateRead`

For more information about these commands, see the *Sun N1 System Manager 1.2 Command Line Reference Manual*.

Security Administrator Rules

The following list provides important rules for N1 System Manager security administrators:

- You can securely configure a non-root N1 System Manager user to have only security administrator privileges by adding only the `SecurityAdmin` role to the user. Such users cannot extend their own privilege set, either by adding new privileges to the `SecurityAdmin` role (which cannot be modified) or by adding new roles to their own user account.
- You cannot configure the `root` user to have only security administrator privileges.
- You cannot configure a user to have only security administrator privileges if the user has the `SecurityAdmin` role and a custom role added to it. Such users could use their `SecurityAdmin` privileges to add any privileges to the custom role and therefore extend their privilege set.

Managing Users

You can set up new N1 System Manager users at any time. When you install the Sun N1 System Manager software, the management server's superuser (`root`) account has all three system default roles automatically added to it, and the `Admin` role is the account's default role.

The following table provides a quick reference to all the tasks and associated commands used to manage users.

TABLE 1–3 Managing Users Quick Reference

Task	Command Syntax
"To Add an N1 System Manager User" on page 38	`# useradd -s n1sh user` `# n1sh create user` *user* `role` *role*
"To Delete an N1 System Manager User" on page 39	`# n1sh delete user` *user* `# userdel`
"To Set a User's Default Role" on page 40	`set user` *user* `defaultrole` *defaultrole*
"To Show a User's Default Role" on page 41	`show user` *user*
"To Add a Role to a User" on page 41	`add user` *user* `role` *role*
"To Remove a Role From a User" on page 41	`remove user` *user* `role` *role*
"To List the Roles Added to a Specific User" on page 42	`show user` *user*

For more information about these commands, see the *Sun N1 System Manager 1.2 Command Line Reference Manual*.

▼ To Add an N1 System Manager User

Before You Begin

You must be superuser (`root`) to add a new user account to the management server's operating system. The rest of the task must be performed by a user with the `SecurityAdmin` role, such as the superuser account used in this task.

When you create a new user for the N1 System Manager, you can also configure the user's login shell to be either a UNIX® shell or the `n1sh` shell. If the user's login is configured with the `n1sh` shell, the user automatically logs into the `n1sh` shell (`N1-ok>` prompt) when logging in to the management server.

Steps

1. **Log in to the management server as superuser from a remote system.**

   ```
   $ ssh -l root management-server
   ```

   See "To Access the N1 System Manager Command Line" on page 28 for details.

2. **Add a new user account to the management server using the `useradd` command.**

   Provide the following configuration details:

   - Use the `useradd -s` option to configure the user's shell to automatically log into the `n1sh` shell. For example: `useradd -s /opt/sun/n1gc/bin/n1sh`
   - Use the `passwd` command to set the user's password.
   - Add `/opt/sun/n1gc/bin` to the user's path in order to access the `n1sh` command.

   See the management server's `useradd` man page for more information.

3. **Add the user to the N1 System Manager with one or more roles.**

   ```
   # n1sh -r SecurityAdmin create user user role role[,role...]
   ```

   The `-r` option enables you to run the `n1sh` command with the `SecurityAdmin` role, which is required for this step. See "create user" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details. You can also use the `add user` command to later add more roles.

▼ To Delete an N1 System Manager User

Before You Begin

You must be superuser (root) to delete an existing user account from the management server's operating system. The rest of the task must be performed by a user with the `SecurityAdmin` role, such as the superuser account used in this task.

Steps

1. **Log in to the management server as superuser from a remote system.**

   ```
   $ ssh -l root management-server
   ```

   See "To Access the N1 System Manager Command Line" on page 28 for details.

2. **Delete the user from the N1 System Manager.**

   ```
   # n1sh -r SecurityAdmin delete user user
   ```

   The `-r` option enables you to run the `n1sh` command with the `SecurityAdmin` role, which is required for this step. See "delete user" in *Sun N1 System Manager 1.2 Command Line Reference Manual*.

3. **(Optional) Delete the user account from the management server by using the management server's `userdel` command.**

▼ To Set a User's Default Role

Users are automatically logged in to the N1 System Manager with their default role.

Note – The default role for the `root` user is automatically set to `Admin` after you reboot the management server or if you restart the N1 System Manager. It is still possible to set the `root` user's default role to a different role, but this is not a permanent assignment.

Steps

1. **Log in to the N1 System Manager.**

   See "To Access the N1 System Manager Command Line" on page 28 for details.

2. **Show which roles are added to the user.**

   ```
   N1-ok> show user user
   ```

   You must have the `SecurityAdmin` role's privileges to run this command. See "show user" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.

3. **Set a user's default role.**

   ```
   N1-ok> set user user defaultrole defaultrole
   ```

   See "set user" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.

Example 1–2 Setting a User's Default Role

The following example shows setting the `SecurityAdmin` role as the default role for the `root` user.

```
N1-ok> show user root

Name:         root
Default Role: Admin
Roles:        SecurityAdmin, ReadOnly, Admin


N1-ok> set user root defaultrole SecurityAdmin
```

▼ To Show a User's Default Role

Steps

1. **Log in to the N1 System Manager.**

   See "To Access the N1 System Manager Command Line" on page 28 for details.

2. **Show a user's default role.**

   ```
   N1-ok> show user user
   ```

   See "show user" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.

Example 1–3 Showing a User's Default Role

The following example shows that the `root` user has the `Admin` default role.

```
N1-ok> show user root

Name:         root
Default Role: Admin
Roles:        SecurityAdmin, ReadOnly, Admin
```

▼ To Add a Role to a User

Steps

1. **Log in to the N1 System Manager.**

   See "To Access the N1 System Manager Command Line" on page 28 for details.

2. **Add one or more roles to a user.**

   ```
   N1-ok> add user user role role[,role...]
   ```

   See "add user" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details. You can use the `show role all` command to list all of the valid roles.

▼ To Remove a Role From a User

Steps

1. **Log in to the N1 System Manager.**

   See "To Access the N1 System Manager Command Line" on page 28 for details.

2. **Remove one or more roles from a user.**

   ```
   N1-ok> remove user user role role[,role...]
   ```

   See "remove user" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details. You can use the `show user` *user* command to list all the roles currently added to the user.

▼ To List the Roles Added to a Specific User

Steps

1. **Log in to the N1 System Manager.**
   See "To Access the N1 System Manager Command Line" on page 28 for details.
2. **List the roles that are added to a user.**

   ```
   N1-ok> show user user
   ```

   See "show user" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.

Example 1–4 Listing the Roles that are Added to a Specific User

The following example shows that the `root` user currently has the `SecurityAdmin`, `ReadOnly`, and `Admin` roles.

```
N1-ok> show user root

Name:         root
Default Role: Admin
Roles:        SecurityAdmin, ReadOnly, Admin
```

Managing Roles

Table 1–1 lists the system default roles that are automatically provided by the N1 System Manager. These system default roles cannot be modified. However, you can create customized roles for your users to fit your organizational and business needs.

The following table provides a quick reference to all the tasks and associated commands used to manage roles.

TABLE 1–4 Managing Roles Quick Reference

Task	Command Syntax
"To Create a Role" on page 43	`create role` *role* `privilege` *privilege*
"To Delete a Role" on page 43	`delete role` *role*
"To Add a Privilege to a Role" on page 44	`add role` *role* `privilege` *privilege*
"To Remove a Privilege From a Role" on page 44	`remove role` *role* `privilege` *privilege*

TABLE 1–4 Managing Roles Quick Reference *(Continued)*

Task	Command Syntax
"To List the Available Roles" on page 44	`show role all`
"To List Privileges Added to a Role" on page 45	`show role` *role*
"To List the Roles Added to All Users" on page 45	`show user all`
"To List the Available Privileges" on page 45	`show privilege all`

For more information about these commands, see the *Sun N1 System Manager 1.2 Command Line Reference Manual*.

▼ To Create a Role

Steps

1. **Log in to the N1 System Manager.**

   See "To Access the N1 System Manager Command Line" on page 28 for details.

2. **Create a new role with one or more privileges.**

   `N1-ok>` **`create role`** *role* `[`**`description`** *description*`]` `privilege` *privilege*`[,`*privilege*`...]`

   Use the `show privileges all` command to list all of the valid privileges or see Table 1–2.

   See "create role" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details. You can also use the `add role` command to later add privileges to the role.

▼ To Delete a Role

Before You Begin

A role cannot be deleted if it is currently added to one or more users. If you try to delete a role that is being used, an error occurs. To successfully delete a role, an authorized user must first remove the role from all users and then attempt the role deletion.

Use the `show role all` command to list all of the valid roles.

Steps

1. **Log in to the N1 System Manager.**

   See "To Access the N1 System Manager Command Line" on page 28 for details.

2. **Delete a role.**

   ```
   N1-ok> delete role role
   ```

   See "delete role" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.

▼ To Add a Privilege to a Role

Before You Begin Use the `show privilege all` command to list all of the valid privileges or see Table 1–2.

Steps

1. **Log in to the N1 System Manager.**
   See "To Access the N1 System Manager Command Line" on page 28 for details.

2. **Add one or more privileges to a role.**

   ```
   N1-ok> add role role privilege privilege[,privilege...]
   ```

   See "add role" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.

Tip – If you want to add most of the privileges to a role, you can use the `all` option to add all the privileges and then use the `remove role` command to remove the unneeded privileges.

▼ To Remove a Privilege From a Role

Before You Begin Use the `show role` *role* command to list all of the privileges currently added to a role.

Steps

1. **Log in to the N1 System Manager.**
   See "To Access the N1 System Manager Command Line" on page 28 for details.

2. **Remove one or more privileges from a role.**

   ```
   N1-ok> remove role role privilege privilege [,privilege...]
   ```

   See "remove role" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.

▼ To List the Available Roles

Steps

1. **Log in to the N1 System Manager.**
   See "To Access the N1 System Manager Command Line" on page 28 for details.

2. **List the available roles.**

```
N1-ok> show role all
```

▼ To List Privileges Added to a Role

Before You Begin Use the `show role all` command to list all of the valid roles.

Steps

1. **Log in to the N1 System Manager.**

   See "To Access the N1 System Manager Command Line" on page 28 for details.

2. **List the privileges that are added to a role.**

   ```
   N1-ok> show role role
   ```

   See "show role" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.

Example 1–5 Listing Privileges Added to a Role

The following example shows that the `SecurityAdmin` role has five privileges added to it.

```
N1-ok> show role SecurityAdmin

Name:       SecurityAdmin
Privileges: UserWrite, RoleWrite, RoleRead, PrivilegeRead, UserRead
```

▼ To List the Roles Added to All Users

Steps

1. **Log in to the N1 System Manager.**

   See "To Access the N1 System Manager Command Line" on page 28 for details.

2. **List the roles that are added to all users.**

   ```
   N1-ok> show user all
   ```

▼ To List the Available Privileges

Steps

1. **Log in to the N1 System Manager.**

   See "To Access the N1 System Manager Command Line" on page 28 for details.

2. **List the available privileges.**

   ```
   N1-ok> show privilege all
   ```

Backing Up and Restoring N1 System Manager Database and Configuration Files

This section provides the following procedures:

These procedures describe how to back up and restore the N1 System Manager database and configuration files. Successful completion of these procedures enables you to do the following:

- Swap management server and management server-related hardware without losing the N1 System Manager database and configuration files.
- Replicate the database and configuration files from one N1 System Manager installation to another installation.

▼ To Back Up the N1 System Manager Database and Configuration Files

This procedure describes how to back up the database and configuration files from a running management server.

The N1 System Manager service is restarted several times during this process. Therefore, perform these steps only when the N1 System Manager is not currently running jobs.

Do not change the configuration or OS usage of the provisioned servers during the period between the backup and restore procedures.

Before You Begin

Identify a server with similar hardware and network configurations as that of the original management server.

Steps

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

   See "To Access the N1 System Manager Command Line" on page 28 for details.

2. **Run the `n1smbackup.sh` script.**

   For example:

```
# /opt/sun/n1gc/bin/n1smbackup.sh
This program will back up Sun N1SM on this Linux/SunOS machine.

The N1SM services will be restarted and N1SM will be interrupted during
the process.

All files related to N1SM, including network interface
configuration, will be backed up. Therefore, it is recommended
that these files are restored to an identical hardware setup.

Verify that N1SM does not have outstanding jobs before proceeding.

The backup process will take about 8 minutes.

Would you like to continue? [y/N] y

Backing up configuration files (done)
Backing up SCS database (done)
Backing up SPS database (done)
N1SM restarted.
N1SM backup completed. Backup saved to file
/var/tmp/n1smbackup/n1smbackup.tgz.
```

   The backup file and the `/var/tmp/n1smbackup` directory are created.

3. **Save the `/var/tmp/n1smbackup/n1smbackup.tgz` file to a safe location, for example, to CD media, FTP, or NFS.**

Next Steps "To Restore the N1 System Manager Database and Configuration Files" on page 47

▼ To Restore the N1 System Manager Database and Configuration Files

This procedure describes how to restore the database and configuration files to a newly installed management server.

The N1 System Manager service is restarted several times during this process. Therefore, perform these steps only when the N1 System Manager is not currently running jobs.

These steps require that the N1 System Manager is not yet installed on the server. Also, preferably, a new installation of either Linux or the Solaris OS is installed on the server.

The `n1smbackup.sh` script backs up only the N1SM database and configuration files. The actual OS files are not backed up. After running `n1smrestore.sh`, OS distributions and OS profiles that exist in the database will need to be deleted and recreated.

Before You Begin

- Follow the instructions in "To Back Up the N1 System Manager Database and Configuration Files" on page 46 to backup the database and configuration files.
- Identify a server with similar hardware and network configurations as that of the original management server.
- Install an operating system and the N1 System Manager software on the replacement management server before starting the procedure. See Chapter 3, "Installing and Configuring an OS on the Management Server," in *Sun N1 System Manager 1.2 Site Preparation Guide*, and the *Sun N1 System Manager 1.2 Installation and Configuration Guide* for details.

Steps

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

   See "To Access the N1 System Manager Command Line" on page 28 for details.

2. **Run the `n1smconfig` utility.**

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

   The current system configuration appears, and lists the network interfaces. You are then asked to enter the interface for the provisioning network.

3. **Specify the port for the provisioning network interface.**

   The available interfaces are listed in the prompt. Type the interface name that is to be used for the provisioning interface, for example `eth0`, `hme0`, `bge0` and so on depending on the machine architecture and installed OS.

4. **Answer the remaining questions in the `n1smconfig` utility.**

   Note that the remaining answers given in `n1smconfig` will be overwritten by the following steps in this procedure. But, it is important to provide the answers and to apply the new settings in order to complete the restore process.

5. **Create the `/var/tmp/n1smbackup` directory on the management server.**

   ```
   # mkdir /var/tmp/n1smbackup
   ```

6. **Copy the `n1smbackup.tgz` backup file to the `/var/tmp/n1smbackup` directory.**

7. **Restore the N1 System Manager database and configuration files:**

   ```
   # /opt/sun/n1gc/bin/n1smrestore.sh -f /var/tmp/n1smbackup/n1smbackup.tgz

   This program will restore Sun N1SM from backup files.

   The N1SM services will be restarted and N1SM will be interrupted during
   the process.

   All files related to N1SM, including network interface
   configuration, will be restored. Therefore, it is recommended
   that these files are restored to an identical hardware setup.
   ```

```
The restore process will take about 8 minutes.

Would you like to continue? [y/N] y

Restoring configuration files (done)
Restoring SCS database (done)
Restoring SCS database (done)
N1SM restarted.
N1SM restore completed.
Run n1smconfig and verify that N1SM settings are correct.
```

8. **Verify that the N1 System Manager configuration settings are still valid or modify them as appropriate.**

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

9. **Verify that the N1 System Manager is working as expected, using the browser interface or `n1sh` command line.**

   See "To Access the N1 System Manager Command Line" on page 28 for details.

10. **(Optional) Remove any OS distributions or OS profiles that exist on the management server before creating new OS distributions and OS profiles.**

```
N1-ok> show os all
ID      Name                  Type          Version
2       s10                   solaris       solaris10x86

N1-ok> show osprofile
ID      Name                        Distribution
2       s10                         s10

N1-ok> delete osprofile s10
N1-ok> delete os s10
N1-ok> show os
No items found.
N1-ok> show osprofile
No items found.
```

Next Steps You will need to copy new OS distributions and create new OS profiles. See "Copying OS Distributions and Flash Archives" on page 74 and "To Create an OS Profile" on page 83.

CHAPTER 2

Discovering, Grouping, and Replacing Servers in the Sun N1 System Manager

This chapter describes how to use the Sun N1 System Manager discovery process to initiate server management and how to group and replace provisionable servers. These topics are described in the following sections:

Discovering Servers

This section describes how to use the discovery process to add servers to the N1 System Manager.

Note – Before you can perform any of the management activities in this section, physical servers must be cabled and prepared according to the instructions in Chapter 2, "Sun N1 System Manager System and Network Preparation," in *Sun N1 System Manager 1.2 Site Preparation Guide*.

The N1 System Manager performs active discovery of servers. The IP address of the server's system controller or service processor must be assigned as a prerequisite for discovery. You can initiate discovery of servers by specifying a range of IP addresses to search for servers. However, there is no broadcast-based mechanism for discovery in the N1 System Manager.

Servers must also comply with the following revisions of firmware to be discovered. See "Downloading V20z and V40z Server Firmware Updates" on page 226 and "Downloading ALOM 1.5 Firmware Updates" on page 228 for instructions or refer to Sun System Handbook documentation for your provisionable server.

Provisionable Server Type	Minimum	Best Practice
Netra 240 and 440 ALOM	1.4	1.5.3
Sun Fire T1000 ALOM	6.1.0	6.1.0
Sun Fire T2000 ALOM	6.0.1	6.0.1
Sun Fire V20z and V40z SP	Service Processor: 2.1.0.5	Service Processor: 2.3.0.11
Sun Fire V20z BIOS	1.27.4	1.33.5.2
Sun Fire V40z BIOS	1.27.4	2.33.5.2
Sun Fire V210, V240, and V440 ALOM	1.4	1.5.3
Sun Fire X2100 SP	4.0.9	4.11
Sun Fire X2100 BIOS	1.0.0	1.0.3
Sun Fire X4100 and X4200	1.0	1.0

The Discovery job uses a Service Access Point (SAP) to access server capabilities. A *SAP* is generically defined as an IP address, protocol, and security credentials.

If you do not specify the Secure Shell (SSH) and Intelligent Platform Management Interface (IPMI) accounts and passwords, the discovery process assumes that the following credentials are configured on the provisionable servers:

TABLE 2–1 SPARC Architecture Provisionable Server Default Credentials

Type	Telnet Login	Telnet Password
Netra 240 and 440	admin	admin
Sun Fire V210, V240, and V440	admin	admin
Sun Fire T1000 and T2000	admin	admin

TABLE 2–2 x86 Architecture Provisionable Server Default Credentials

Type	SSH Login	SSH Password	IPMI Login	IPMI Password	SNMP Read Community String
Sun Fire V20z and V40z	admin	admin	-	admin	public
Sun Fire X2100	-	-	Admin	admin	-
Sun Fire X4100 and X4200	root	changeme	root	changeme	public

Note – Automatic configuration of credentials is supported for Sun Fire V20z and V40z servers if they are in the factory default state. See "Setting Up Provisionable Servers" in *Sun N1 System Manager 1.2 Site Preparation Guide*.

If you do specify the login accounts and passwords, the discovery process configures the user-specified credentials. If only one credential is specified, the missing credential is configured with one of the defaults specified.

If you want to disable autoconfiguration, add the following line to the `/etc/opt/sun/n1gc/domain.properties` file before you run discovery:

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

The N1 System Manager must be restarted for the disabling of autoconfiguration to take effect. Note that after autoconfiguration is disabled, any servers in the factory default state cannot be discovered until their SSH and IPMI accounts are configured. For further information, see *Sun N1 System Manager 1.2 Site Preparation Guide*.

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

▼ To Discover New Servers

You must discover servers to manage them with the N1 System Manager. This procedure describes how to use the browser interface to initiate and track discovery. Example 2–1 at the end of this procedure provides the command-line equivalent.

Note – Discovered servers are automatically monitored for hardware health.

Before You Begin

- Before you discover a new hardware component, read Chapter 2, "Sun N1 System Manager System and Network Preparation," in *Sun N1 System Manager 1.2 Site Preparation Guide*.

Steps

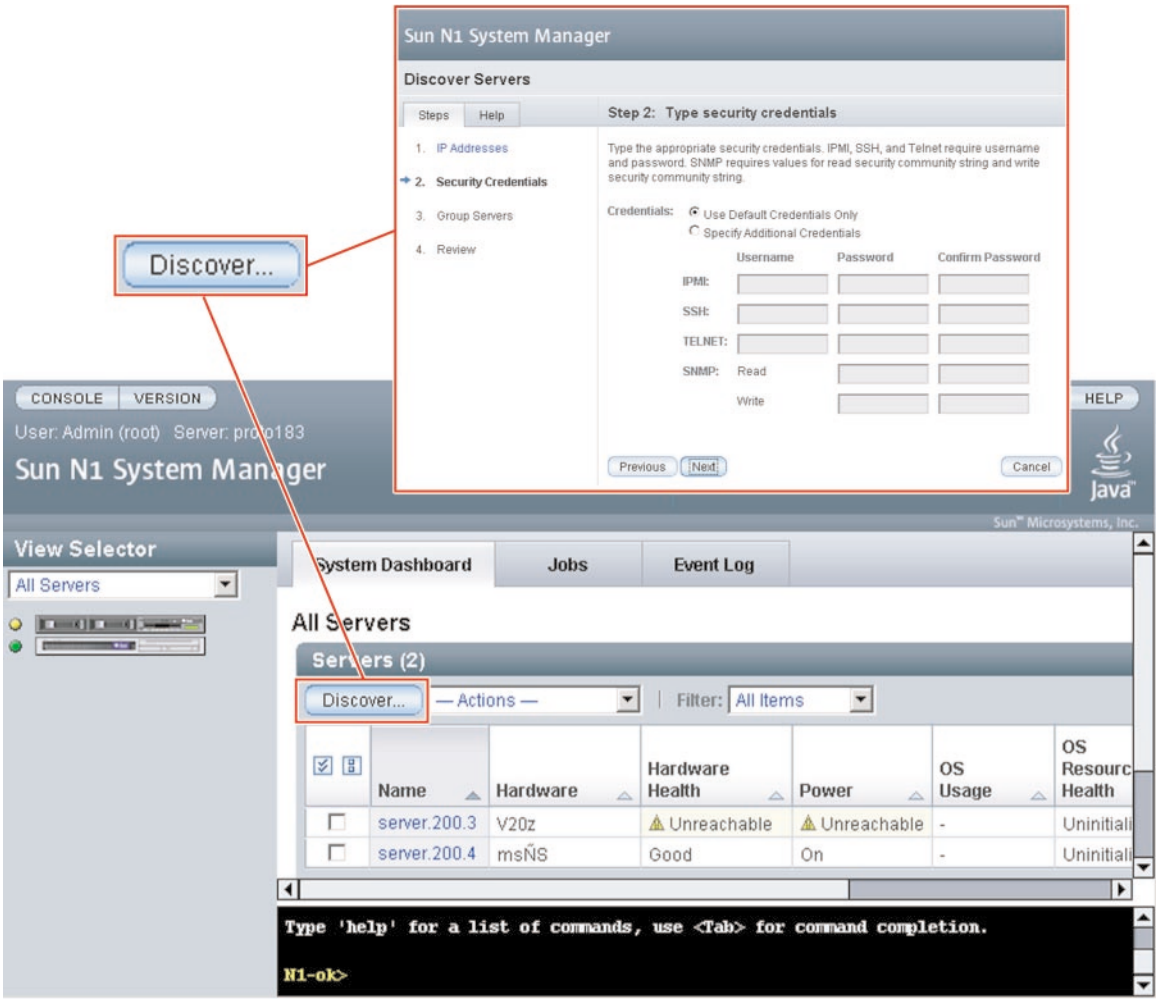
1. **Log in to the N1 System Manager.**

   See "To Access the N1 System Manager Browser Interface" on page 29 for details.

   The All Servers page appears.

2. **Click the Discover button in the Servers table.**

   The Discover Servers wizard appears.



3. **Use the wizard steps to guide you through the screens.**
4. **Click the Finish button to begin the discovery operation.**
   The wizard window closes and a job ID appears in the Command Line pane.
5. **To view the Discovery job, click the Jobs tab.**
   The Discovery job appears in the Jobs table.
6. **When the job completes successfully, do one of the following:**

- **Choose All Servers from the View Selector menu.**
  The discovered server appears in the list.
- **If you selected a group for the discovered servers, view the list of server groups as follows:**
  a. **Select the Servers By Group from the View Selector menu.**
     The Server Groups table appears.
  b. **Select the group name.**
     The list of discovered servers appears.

The server or servers are available for OS provisioning.

7. **If you installed an OS on a server before it was discovered, add the OS monitoring feature.**

Note – The SSH user account that is used in the following command must have root privileges on the remote machine.

```
N1-ok> add server server feature osmonitor agentip agentip agentssh username/password
```

See "add server" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.

Example 2–1 Discovering Servers Through the Command Line

IP addresses, IP address ranges, and IP subnets can be input as a comma-separated list. Overlapping IP address ranges are allowed. Security credentials for IPMI, Simple Network Management Protocol (SNMP), SSH, and Telnet are optional. However, for Sun Fire X4000 series servers, `username` is required by IPMI. If credentials are not specified, the manufacturer defaults are used. See *Sun N1 System Manager 1.2 Site Preparation Guide* for information about the default accounts.

```
N1-ok> discover IP,IP-IP,subnet/mask [group group]
[ipmi username/password]
[snmp credential/credential]
[ssh username/password]
[telnet username/password]
```

The following example of the `discover` command shows how to discover servers that have the following management network IP addresses: `192.168.1.1–192.168.1.3`, `192.168.1.5-192.168.1.95`, and `192.168.1.107`.

```
N1-ok> discover 192.168.1.1-192.168.1.3,192.168.1.5-192.168.1.95,192.168.1.107
 group dev ssh root/admin
Job 3 started.
```

The `group` subcommand adds the successfully discovered servers into a server group called `dev`. The `ssh` option specifies the user name and password configured for access on the management port. In this example, the SSH user name `root` and password `admin` are used to authenticate the hardware discovery.

The following example command shows how to view the Discovery job and the job status.

```
N1-ok> show job all
Job ID  Date                        Type                        Status        Owner
3       2005-06-28T06:53:53-0700    Discovery                   Completed     root
2       2005-06-28T06:01:20-0700    Create OS Distribution      Completed     root
1       2005-06-28T05:57:14-0700    Create OS Distribution      Completed     root
```

The following example command shows how to verify that the discovered servers were added to the server group.

```
N1-ok> show group all
Name          Status      Jobs  Servers  Spare
dev                           7
```

The following example command shows how to view the list of servers in the group and the power and hardware health status.

```
N1-ok> show group dev
Name             Hardware    Hardware Health   Power   OS Usage             OS Resource Health
192.168.1.1      V20z        Good              On      --                   Uninitialized
192.168.1.2      V20z        Good              On      --                   Uninitialized
192.168.1.5      V40z        Good              On      --                   Uninitialized
192.168.1.15     NETRA-240   Good              On      --                   Uninitialized
192.168.1.25     X4100       Good              On      --                   Uninitialized
192.168.1.95     X4200       Good              On      --                   Uninitialized
192.168.1.107    SF-V240     Good              On      --                   Uninitialized
```

The following example of the `discover` command shows how to discover any servers that have management network IP addresses assigned in the `192.168.1.0/8` netmask.

```
N1-ok> discover 192.168.1.0/8 ssh root/admin
Job 18 started.
```

The following example shows how to view the discovered servers.

```
N1-ok> show server all
Name             Hardware    Hardware Health   Power   OS Usage             OS Resource Health
192.168.1.1      V20z        Good              On      --                   Uninitialized
192.168.1.2      V20z        Good              On      --                   Uninitialized
192.168.1.5      V40z        Good              On      --                   Uninitialized
192.168.1.15     NETRA-240   Good              On      --                   Uninitialized
192.168.1.25     X4100       Good              On      --                   Uninitialized
192.168.1.95     X4200       Good              On      --                   Uninitialized
192.168.1.107    SF-V240     Good              On      --                   Uninitialized
192.168.1.200    V20z        Good              On      --                   Uninitialized
192.168.1.245    V40z        Good              On      --                   Uninitialized
192.168.1.255    NETRA-240   Good              On      --                   Uninitialized
```

Example 2–2 Adding the OS Monitoring Feature to Discovered Servers

The following example of the `add` command shows how to add the OS monitoring feature to a server that had an OS installed prior to being discovered by the N1 System Manager.

```
N1-ok> add server 192.168.1.1 feature osmonitor
agentip 192.168.10.10 agentssh admin/admin
```

The `agentip` parameter specifies the IP address of the provisionable server's data network interface to be monitored by the management server. The `ssh` user name `admin` and password `admin` are used for root access authentication. For more information, see "Adding and Upgrading Base Management and OS Monitoring Features" on page 157.

The following example of the `show` command shows how to verify that the OS monitoring feature was added successfully to a server that had an OS installed prior to being discovered.

```
N1-ok> show server 192.168.1.1
Name            Hardware    Hardware Health   Power   OS Usage        OS Resource Health
192.168.1.1     V20z        Good              On      Solaris         Good
```

Troubleshooting The `discover` command credential attributes are used for security. SSH, IPMI, and Telnet require a username and a password. SNMP requires that you input a valid value for the read security community string. If credentials are not specified, the discovery process uses the default credentials that were defined during installation. See "Discovering Servers" on page 51 for default credentials.

Discovery might fail due to stale SSH entries on the management server. If the `discover` command fails with an error message indicating that there are `invalid credentials` and no true security breach has occurred, remove the `known_hosts` file or the specific entry in the file that corresponds to the provisionable server. Then, retry the `discover` command.

If the management server is running Linux, the `known_hosts` file is at `/root/.ssh/known_hosts`. If the management server is running the Solaris OS, the `known_hosts` file is at `/.ssh/known_hosts`.

The OS does not belong to the server in question if the `add` command fails with the following error:

```
Internal error: No mac address match found
```

See Also *Sun N1 System Manager 1.2 Site Preparation Guide*

Next Steps

- "To Open a Server's Serial Console" on page 138

Creating and Maintaining Server Groups

This section describes the following tasks:

Creating Groups and Adding Servers to Groups

After successful completion of the Discovery job, a server is identified by its *management name*. The server's management name is initially set to the server's management IP address. You can rename discovered servers at any time.

You can create groups of discovered, or *provisionable*, servers according to the make and model for aggregate installation of firmware updates. Then, you can create functional groups for the aggregate installation of operating systems, or *OS profiles*, and OS updates. Provisionable servers can belong to more than one server group, so you can create new server groups for aggregate maintenance tasks, as needed.

To create server groups, you use the `create` command with the `group` keyword. To add servers to a group, you use the `add` command with the `group` keyword and the `server` subcommand.

To create a group and add servers in a single operation, you use the `create` command with the `group` keyword and the `server` subcommand. This task can also be performed during the discovery process. To do so, you can add an option to the `discover` command to create a new group and add the servers to the new group. See "To Discover New Servers" on page 53 for instructions.

For syntax and parameter details, type `help create group` or `help add group` at the `N1-ok` command line.

▼ To Create a Server Group

This task shows you how to create groups of discovered, or *provisionable*, servers. Provisionable servers can belong to more than one server group, so you can create new server groups for aggregate maintenance tasks, as needed.

Steps

1. **Log in to the N1 System Manager.**
   See "To Access the N1 System Manager Command Line" on page 28 for details.
2. **Type the following command:**

```
N1-ok> create group group
```

The new group is created. See "create group" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.

Example 2–3 Creating a Group and Adding Servers in a Single Operation

The following example shows how to create a group named `dev` and add servers named `server1` and `server2`. Then, the `show group` command output provides the list of servers in the `dev` group.

```
N1-ok> create group dev server server1,server2
N1-ok> show group dev
Name        Hardware    Power        Health        OS Usage
server1       V20z       On           Good           --
server2       V20z       On           Good         RH30
```

▼ To Add a Server to a Group

Note – Servers can belong to more than one group.

Steps

1. **Log in to the N1 System Manager.**
   See "To Access the N1 System Manager Command Line" on page 28 for details.
2. **Type the following command:**

   `N1-ok>` **`add group`** *group* **`server`** *server*

   The server is added to the group. See "add group" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.

Removing Servers From Groups

To remove a server from a group, use the `remove` command with the `group` keyword and the `server` subcommand. For syntax and parameter details, type `help remove group` at the `N1-ok` command line.

▼ To Remove a Server From a Group

Steps

1. **Log in to the N1 System Manager.**
   See "To Access the N1 System Manager Command Line" on page 28 for details.
2. **Type the following command:**

   `N1-ok>` **`remove group`** *group* **`server`** *server*

The server is removed from the group. See "remove group" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.

Replacing Provisionable Servers

This section describes how to replace a failed provisionable server in the N1 System Manager.

▼ To Replace a Server

Steps

1. **Log in to the N1 System Manager.**
   See "To Access the N1 System Manager Command Line" on page 28 for details.
2. **Type the following command:**

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

   The server is shut down and powered off. See "stop server" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.
3. **Disconnect the physical server from the rack.**
4. **Remove the server from the system.**

   ```
   N1-ok> delete server server
   ```

5. **Connect the new server.**
   Follow the instructions in *Sun N1 System Manager 1.2 Site Preparation Guide*.
6. **Discover the replacement server.**

   ```
   N1-ok> discover IP | IP-IP | subnet/mask [group group]
   [ipmi password] [snmp credential/credential] [ssh username/password]
   ```

   The replacement server is managed. See "discover" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details. You can now set up monitoring. See "Supporting Monitoring" on page 156 and "Enabling and Disabling Monitoring" on page 170 for details.

Troubleshooting The `discover` command credential attributes are used for security. SSH, IPMI, and Telnet require a username and a password. SNMP requires that you input a valid value for the read security community string. If credentials are not specified, the discovery process uses the default credentials that were defined during installation. See "Discovering Servers" on page 51 for default credentials.

Discovery might fail due to stale SSH entries on the management server. If the `discover` command fails with an error message indicating that there are `invalid credentials` and no true security breach has occurred, remove the `/root/.ssh/known_hosts` file or the specific entry in the file that corresponds to the provisionable server. Then, retry the `discover` command.

CHAPTER 3

Provisioning Operating Systems, OS Updates, and Firmware Updates

This chapter describes how to manage the aggregate installation of operating systems, OS updates, and firmware updates.

The N1 System Manager enables you to perform the management tasks in the following sections:

Introduction to OS Provisioning

This section provides an overview of the OS provisioning process and supported OS types. This section includes the following:

OS Provisioning Command Overview

The N1 System Manager enables you to provision hundreds of heterogeneous servers using one interface. The `N1-ok` shell provides a simple command set with which to provision and reprovision servers.

The OS provisioning process consists of the following high-level steps:

1. Copying an OS image to the management server.
2. (Optional) Creating a custom OS profile. *Default OS profiles* are created automatically when OS distributions are copied.
3. Installing an OS profile on a server or a server group.

To import an OS image, use the `create os` command with the `cdrom` or `file` attribute. For example:

```
N1-ok> create os os file files
```

The Create OS job uses the location of the OS media or files to import the image and save it on the management server. You can view the job results to track the process.

After successful completion of the Create OS job, an image or *distribution* is identified by its name. The same name is used for the default OS profile. To view the available OS profiles, use the `show osprofile` command and the `all` attribute. For example:

```
N1-ok> show osprofile all
```

Provision individual servers and groups of servers by using the `load server` command with the `group` attribute, and the `osprofile` parameter and the required values. For example:

```
N1-ok> load server server osprofile osprofile networktype networktype
```

Tip – The N1 System Manager browser interface provides an OS profile wizard and drag-and-drop installation of groups of servers to limit the complexity of OS provisioning. The wizard builds commands to help you learn the syntax and provides default settings to enable efficient configuration of common parameters. See "To Access the N1 System Manager Browser Interface" on page 29 for login instructions. Refer to the N1 System Manager online help for wizard instructions.

Reprovision servers and server groups with a new OS profile by running the `load` command on servers or server groups that have previously been provisioned.

The following graphic illustrates the OS provisioning process.

OS Provisioning Process

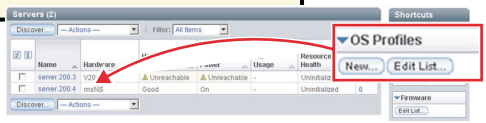
1. Assume a user role with appropriate privileges.

2. Copy an OS distribution to the management server by using the command line.

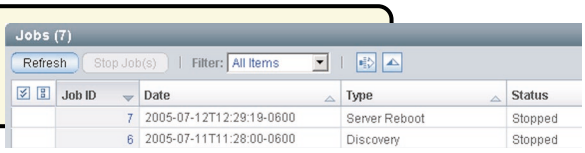
```
N1-ok> create os myos file /tmp/filename.iso
```

3. Edit the OS Profiles list to view the Shortcut.

4. Drag and drop the icon to launch the Load OS Profile wizard.



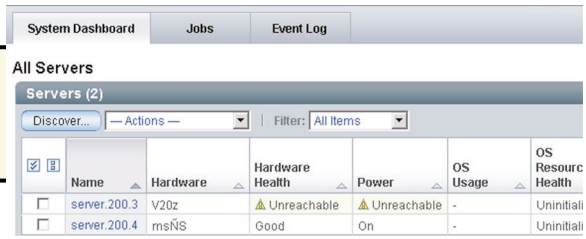
5. Track the Load OS job to completion by viewing the Jobs table. Click the job ID to view the job results.



6. Use the command line to add OS monitoring support.

```
N1-ok> add server myserver feature osmonitor
agentip myip agentssh myssh
```

7. Check the System Dashboard to validate that the provisioned OS is running and monitored.



The following list provides links to the tasks that are illustrated in the graphic.

- Assume a user role with appropriate privileges. See "Introduction to N1 System Manager User Security" on page 32 for procedural information.

- Copy an OS distribution to the management server by using the command line. See "To Copy an OS Distribution From CDs or a DVD" on page 76, "To Copy an OS Distribution From ISO Files" on page 75, and "Copying OS Distributions and Flash Archives" on page 74 for conceptual information.
- (Optional) Create a flash archive file and copy it to the management server. See "To Copy a Flash Archive to the Management Server" on page 78.
- Modify the default OS profile to customize the parameters that are used to install the distribution. See "To Modify an OS Profile" on page 86.
- Load the OS profile onto your provisionable servers by using the `load` command. Alternatively, use the browser interface's Shortcuts pane to drag-and-drop OS profiles onto listed servers. See "To Load an OS Profile on a Server or a Server Group" on page 90.
- Track the Kickstart or JumpStart or AutoYaST installation output and the Load OS job progress. See "Connecting to the Serial Console for a Server" on page 138 and "Managing Jobs" on page 183.
- After the Load OS job completes, monitor the installed OS. See "OS Health Monitoring" on page 153 and "To Add the OS Monitoring Feature" on page 158.

Supported Operating Systems on Provisionable Servers

The following tables provide the complete list of operating systems that can be installed and are supported on the provisionable servers with the N1 System Manager.

Note – Solaris 9 OS on x86 platform distributions require the application of two updates from a separate patch server if your management server is running Linux. See "To Patch a Solaris 9 OS Distribution by Using a Solaris 9 OS on x86 Patch Server" on page 206 for detailed instructions on how to create a valid Solaris 9 OS on x86 platform distribution. These patches are necessary for the N1 System Manager to be able to provision Solaris OS 9 update 7 and below. This procedure is not required for Solaris OS 9 update 8 and above.

Provisionable server hardware and operating software requirements for the N1 System Manager are listed in the following tables.

TABLE 3–1 SPARC-Based Provisionable Server Hardware and Operating System Requirements

Type	Management Port Type	Provisionable OS	Disk Space Requirements	RAM Requirements
Sun Netra 240 and 440	ALOM	Solaris 10 GA and later Solaris 9 Update 7 and Update 8	12 Gbytes minimum for all provisionable servers	512 Mbytes minimum, 1-Gbyte recommended for all provisionable servers
Sun Fire V210, V240, and V440	ALOM	Solaris 10 GA and later Solaris 9 Update 7 and Update 8		
Sun Fire T1000 and T2000	ALOM	Solaris 10 HW2 and later		

TABLE 3–2 x86–Based Provisionable Server Hardware and Operating System Requirements

Type	Management Port Type	Provisionable OS	Disk Space Requirements	RAM Requirements
Sun Fire X2100 with the 8081A IPMI 1.5 Remote Management Card: Part Number: 371-0743	SP	Solaris x86 Version 10 HW1 and later Red Hat Enterprise Linux 3.0 WS, ES, and AS Update 5, 32–bit and 64–bit Red Hat Enterprise Linux 4.0 WS, ES, and AS update 1, 32–bit and 64–bit SUSE Linux Professional 9.2, 64–bit only SUSE Linux Professional 9.3, 64–bit only	12 Gbytes minimum for all	512 Mbytes minimum, 1-Gbyte recommended
Sun Fire X4100 and X4200	ILOM	Solaris x86 Version 10 HW1 and later Red Hat Enterprise Linux 3.0 WS, ES, and AS Update 5, 32–bit and 64–bit Red Hat Enterprise Linux 4.0 WS, ES, and AS update 1, 64–bit only SUSE Linux Enterprise Server 9 SP1, 64–bit only		

TABLE 3–2 x86–Based Provisionable Server Hardware and Operating System Requirements *(Continued)*

Type	Management Port Type	Provisionable OS	Disk Space Requirements	RAM Requirements
Sun Fire V20z and V40z	SP	Solaris x86 Version 10 and later		
		Solaris x86 Version 9 update 7 and update 8		
		Red Hat Enterprise Linux 3.0 WS, ES, and AS, Updates 1 through 5 for 32–bit only		
		Red Hat Enterprise Linux 3.0 WS, ES, and AS, Updates 3 through 5, 64-bit only		
		Red Hat Enterprise Linux 4.0 WS, ES, and AS, 64-bit only		
		Red Hat Enterprise Linux 4.0 WS, ES, and AS update 1, 32–bit and 64-bit		
		SUSE Linux Enterprise Server 9, 32–bit and 64–bit		
		SUSE Linux Enterprise Server 9 SP1, 32–bit and 64–bit		
		SUSE Linux Professional 9.2 , 32–bit and 64–bit		
		SUSE Linux Professional 9.3, 32–bit and 64–bit		

Provisioning the Solaris 10 Operating System

This section provides instructions for provisioning the Solaris 10 OS by using the browser interface or the command line. See "To Provision the Solaris 10 OS" on page 70. This procedure familiarizes you with the provisioning process and the most reliable method for performing aggregate server installations at any skill level.

The example that follows the procedure provides the command-line equivalents for provisioning the Solaris 10 OS. The command-line interface is the most efficient method for performing aggregate installations for more experienced system administrators.

▼ To Provision the Solaris 10 OS

Before You Begin

- Read "Discovering Servers" on page 51.
- Download the Solaris 10 DVD ISO file to a directory that is accessible by the management server.
- Update the disk device path for the machine type on which you will be provisioning the Solaris OS.

Steps

1. **Copy the Solaris 10 OS ISO file to the management server.**

   ```
   N1-ok> create os os file file-location
   ```

   Note – This operation is CPU intensive and might take several minutes to complete.

   A default OS profile is created on the management server. To view the list of OS profiles, type **`show osprofile all`**.

   See "To Copy an OS Distribution From ISO Files" on page 75 or "To Copy an OS Distribution From CDs or a DVD" on page 76 for more information.

2. **(Optional) Set up a flash archive file on the management server.**

   See "To Copy a Flash Archive to the Management Server" on page 78.

3. **(Optional) Create a custom post-installation script to configure the `bge1` data network interface when the server boots. Save the file on the management server.**

   The following sample script configures the provisionable server's `bge1` data network interface at system boot using the data network DHCP server.

   ```
   cat << EOF > /etc/sysconfig/network-scripts/ifcfg-eth1DEVICE=bge1
   BOOTPROTO=dhcp
   ONBOOT=yesEOF
   ```

4. **(Optional) Customize the default OS profile so that it uses a flash archive and a post-installation script.**

   ```
   N1-ok> set osprofile osprofile flar flar
   ```

   The *flar* attribute value is the full path and flash archive file name, for example, `/jumpstart/Flash/archive1.flar`.

   ```
   N1-ok> add osprofile osprofile script script type type
   ```

The *script* attribute value is the full path and script file name, for example, `/etc/sysconfig/network-scripts/ifcfg-bge1`.

The *type* attribute specifies the time when the custom script will run during the installation. Valid values for the type attribute are:

- `pre` – Run the script before the installation (for example, drivers).
- `post` – Run the script after the installation.
- `postnochroot` – Run the script after the installation. The script does not have to be run as superuser (root).

The OS profile is modified to use the designated post-installation script and the flash archive file.

5. **Show the drag-and-drop OS profile icon on the Dashboard tab.**

   a. **Click the Edit List button beneath the OS Profiles list.**
      The list of available OS profiles appears.

   b. **Select the relevant check box and click OK.**
      The selected OS profile is added to the Shortcuts pane.

6. **(Optional) Connect to the serial console of the provisionable server.**

   a. **Choose All Servers from the View Selector menu.**
      The Servers table appears.

   b. **Select the server for which you want to launch a serial console.**
      The Server Details page appears.

   c. **Choose Open Serial Console from the Actions menu.**
      The serial emulator appears.

7. **Choose Servers By Group from the View Selector menu.**
   The Server Groups table appears.

8. **Drag and drop the OS profile icon from the Shortcuts pane to a server group.**
   The Load OS Profile wizard appears. Use the wizard steps to guide you through the screens.

9. **To begin loading the OS profile on the selected servers, click the Finish button in the final step of the wizard.**
   The wizard window closes and a job number appears in the Command Line pane.

10. **Track the OS profile installation by using any of the following methods:**

    - View the Serial Console window output from Step 5.
    - Click the Jobs tab to view the OS Load job, and click the Job ID for details.
    - Click the Event Log tab to view any events generated by the job.

Example 3–1 Provisioning the Solaris 10 OS Through the Command Line

For the following example, assume that you have created a Solaris 10 OS on x86 platform flash archive file named `archive1.flar` and that you have created a post-installation script called `ifcfg-bge1`. Your management server is also assumed to be running the Solaris 10 OS on x86 platform software.

The following example shows how to copy an OS distribution from the `/tmp/solarisdvd.iso` file.

```
N1-ok> create os solaris_ver10 file /tmp/solarisdvd.iso
Job "1" started.
```

The following example shows how to add a line to the `/etc/dfs/dfstab` file, below the last comment, which creates the `/jumpstart/Flash` directory.

```
# vi /etc/dfs/dfstab

# Put custom additions below (Do not change/remove this line)
share -F nfs -o ro,anon=0 -d "Flash Share" /jumpstart/Flash
```

The following example shows how to copy the flash archive to the `/jumpstart/Flash` directory.

```
# cp /tmp/archive1.flar /jumpstart/Flash/
```

The following example shows how to restart NFS.

```
# /etc/init.d/nfs.server stop
# /etc/init.d/nfs.server start
```

The following example shows how to create an OS profile that uses the flash archive.

```
N1-ok> create osprofile solaris_ver10 rootpassword admin flar /jumpstart/Flash/archive1.flar
description "solaris 10with flar" os solx86
Job "2" started.
```

The following example shows how to add a swap partition to the OS profile.

```
N1-ok> add osprofile solaris_ver10 partition swap sizeoption fixed size 2048
device c1t1d0s1 type swap
```

The following example shows how to add a root partition to the OS profile.

```
N1-ok> add osprofile solaris_ver10 partition / sizeoption free device
c1t1d0s0 type ufs
```

The following example shows how to add a post-installation script to the OS profile.

```
N1-ok> add osprofile solaris_ver10 script
/etc/sysconfig/network-scripts/ifcfg-bge1 type post
```

The following example shows how to load the OS profile on a server group with the name `devgroup`.

```
N1-ok> load group devgroup osprofile solaris_ver10
excludeserver=192.168.73.205,192.168.73.31,192.168.73.14
```

```
networktype=static ip=192.168.72.201-192.168.73.214
Job "3" started.
```

The `excludeserver` attribute shows how to exclude certain provisionable IP addresses from the load operation. The `networktype` attribute specifies the static IP range to assign to the provisioned servers.

The `networktype` attribute must be set to `static` for Solaris profile installations. See Table 3–4 and "load server" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.

The following example shows how to view the job status.

```
N1-ok> show job 3
Job ID:   3
Date:     2005-06-01T13:11:46-0600
Type:     OS Load
Status:   Completed (2005-06-01T13:11:59-0600)
Command:      load group devgroup osprofile solaris_ver10
excludeserver=192.168.73.205,192.168.73.31,192.168.73.14
networktype=static ip=192.168.72.201-192.168.73.214Owner:    root
Errors:   0
Warnings: 0
```

Troubleshooting

- "Troubleshooting OS Distributions" on page 204
- "OS Profile Deployment Failures" on page 211

See Also

- "To Copy a Flash Archive to the Management Server" on page 78
- "Connecting to the Serial Console for a Server" on page 138

Next Steps "To Add the OS Monitoring Feature" on page 158

Managing OS Distributions

This section describes the following tasks:

- "To Copy an OS Distribution From ISO Files" on page 75
- "To Copy a SUSE Linux Enterprise Server 9 SP1 OS Distribution from ISO Files" on page 76
- "To Copy an OS Distribution From CDs or a DVD" on page 76
- "To Copy a Flash Archive to the Management Server" on page 78
- "To Delete an OS Distribution" on page 80

Copying OS Distributions and Flash Archives

Before you can install an OS profile on a provisionable server, you must copy an OS image. This copied image is called an OS *distribution*. You can copy an OS image from files that are located on the management server or from a network mounted file system. OS distributions are copied to the directories on the management server as follows:

- Linux management server:
  - Linux OS distributions: `/var/opt/sun/scs/share/allstart/`
  - Solaris OS distributions: `/var/opt/sun/scs/share/allstart/jumpstart/`
- Solaris management server:
  - Linux OS distributions: `/var/opt/SUNWscs/share/allstart`
  - Solaris OS distributions: `/var/js`

Supported file types are:

- CD ISO files (Linux only)
- CD media (Linux only)
- DVD ISO files
- DVD media

Note – The N1 System Manager does not support the copying of Solaris OS CDs and CD ISO files. You must copy a Solaris DVD or DVD ISO file.

Refer to "Supported Operating Systems on Provisionable Servers" on page 66 for a detailed list of supported distributions for each provisionable server type.

To copy an OS distribution, use the `create os` command. Type `help create os` at the `N1-ok` command line for syntax and parameter details, or see "create os" in *Sun N1 System Manager 1.2 Command Line Reference Manual*. Refer to the following procedures for instructions about how to copy an OS distribution:

- "To Copy an OS Distribution From ISO Files" on page 75
- "To Copy a SUSE Linux Enterprise Server 9 SP1 OS Distribution from ISO Files" on page 76
- "To Copy an OS Distribution From CDs or a DVD" on page 76

After you have copied an OS distribution, you can copy a flash archive file to the management server for use with a customized OS profile. Copying flash archives involves several manual steps, but it provides the most efficient method for loading OS distributions with the N1 System Manager. See "To Copy a Flash Archive to the Management Server" on page 78.

▼ To Copy an OS Distribution From ISO Files

This procedure describes how to copy an OS distribution to the management server from a set of ISO files by using the command line.

Note – After a distribution is copied, an OS profile of the same name is created by default. This profile appears in the OS Profiles list in the Shortcuts pane of the browser interface or by typing `show osprofile all` at the `N1-ok>` prompt.

Before You Begin

- Download the set of ISO files to a directory that is accessible or that can be network-mounted by the management server.

  Note – The N1 System Manager does not support the copying of Solaris OS CDs and CD ISO files. You must copy a Solaris DVD or DVD ISO file.

- Move any file systems off of the `/mnt` mount point.

Steps

1. **Log in to the N1 System Manager.**

   See "To Access the N1 System Manager Command Line" on page 28 for details.

2. **Type the following command:**

   `N1-ok>` **`create os`** *os* **`file`** *file*`[,`*file*`...]`

   Refer to "create os" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.

3. **Verify that the OS distribution was copied.**

   ```
   N1-ok> show os all
   ```

   The OS distribution appears in the output.

Example 3–2 Creating an OS Distribution From a File

The following example shows how to create an OS distribution called `solaris_ver9` from a single Solaris DVD ISO file.

```
N1-ok> create os solaris_ver9 file /tmp/solaris_9_dvd.iso
Job "7" started.
```

See Also To find out how to load the OS distribution, see "To Load an OS Profile on a Server or a Server Group" on page 90.

▼ To Copy a SUSE Linux Enterprise Server 9 SP1 OS Distribution from ISO Files

The following procedure describes how to copy the SLES 9 SP1 OS distribution to the management server.

Before You Begin

Move any file systems off of the `/mnt` mount point.

Steps

1. **Copy the SLES 9 distribution:**

```
# n1sh create os sles9u1 file
  /directory/SLES-9-i386-RC5-CD1.iso,/directory/SLES-9-i386-RC5-CD2.iso,
  /directory/SLES-9-i386-RC5-CD3.iso,/directory/SLES-9-i386-RC5-CD4.iso,
  /directory/SLES-9-i386-RC5-CD5.iso,/directory/SLES-9-i386-RC5-CD6.iso
```

Note – Wait for the Create OS command to complete before going to the next step.

---

2. **Copy the SLES 9 Update 1 distribution:**

Note – The same OS profile name should be used when adding Update1.

```
# n1sh create os sles9u1 file
  /directory/SLES-9-SP-1-i386-RC5-CD1.iso,directory/SLES9/SLES-9-SP-1-i386-RC5-CD2.iso,
  /directory/SLES-9-SP-1-i386-RC5-CD3.iso
```

3. **Verify that the OS distribution was copied.**

```
N1-ok> show os all
```

The OS distribution appears in the output.

See Also

To find out how to load the OS distribution, see "To Load an OS Profile on a Server or a Server Group" on page 90.

▼ To Copy an OS Distribution From CDs or a DVD

This procedure describes how to copy an OS distribution to the management server from CDs or a DVD by using the command line.

Note – The N1 System Manager does not support the copying of Solaris OS CDs and CD ISO files. You must copy a Solaris DVD or DVD ISO file.

When copying an OS distribution from multiple installation CDs, you must run the `create os` command multiple times. For example, if you are copying an OS distribution that is provided on two CDs, you must insert the first CD, run the `create os` command, and wait for the job to complete. Once the first job completes, you must insert the second CD, run the `create os` command again, and wait for the job to complete. The OS distribution is successfully copied when the second job completes.

When copying the SUSE Linux Enterprise Server 9 SP1 distribution, you must run the create os command multiple times. First, copy the SLES 9 base distribution. When that job finishes, you can then copy the SLES 9 Update 1 distribution. A default OS profile is automatically created for each newly created OS distribution, with the same name as the OS distribution. The default profile is provided as an example. Most of the time, you will have to update the default profile to match your hardware or it may be easier to just create a new profile. Use the `show osprofile` *osprofile* command to see the configuration of an OS profile. The same OS profile name should be used when adding the Update 1 distribution.

Note – After a distribution is copied, an OS profile of the same name is created by default. This profile appears in the OS Profiles list in the Shortcuts pane of the browser interface or by typing `show osprofile all` at the `N1-ok>` prompt.

Before You Begin

Move any file systems off of the `/mnt` mount point.

Steps

1. **Insert Disk 1 and type the following command:**

   ```
   N1-ok> create os os cdrom cdrom
   ```

   A Create OS Distribution job is started. Note the job ID. When the job completes, insert the next disk. See "create os" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.

   Note – You are not prompted to insert the next disk, so you must track the Create OS Distribution job completion and the disk number for your OS. When the job completes, an event is generated.

2. **Insert Disk 2 and type the following command:**

   ```
   N1-ok> create os os cdrom cdrom
   ```

3. **Continue with additional disks if needed.**

4. **When the final Create OS Distribution job completes, type the following command:**

   ```
   N1-ok> show os os
   ```

   The new OS distribution appears in the output.

Troubleshooting "Troubleshooting OS Distributions" on page 204

Next Steps To find out how to load the OS distribution by using an profile, see "To Load an OS Profile on a Server or a Server Group" on page 90.

▼ To Copy a Flash Archive to the Management Server

This procedure describes how to set up and deploy a flash archive on a server or a server group by using the command line.

Before You Begin

- Copy an OS distribution to the management server.

  See "To Copy an OS Distribution From ISO Files" on page 75 or "To Copy an OS Distribution From CDs or a DVD" on page 76.

- Create a flash archive file.

  Flash archives for complete Solaris installations might be too large to provision successfully if the management server is running Linux. Consider compressing the file or using a smaller flash archive with less content. See *Solaris 10 Installation Guide: Solaris Flash Archives (Creation and Installation)* for instructions on creating a flash archive.

Steps

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

   See "To Access the N1 System Manager Command Line" on page 28 for details.

2. **Perform one of the following actions:**

   - **If your management server is running the Solaris Operating System, modify the `/etc/dfs/dfstab` file to add `share -F nfs -o ro,anon=0 -d "Flash Share" /jumpstart/Flash` below the last comment in the file.**

     For example:

     ```
     # Put custom additions below (Do not change/remove this line)
     share -F nfs -o ro,anon=0 -d "Flash Share" /jumpstart/Flash
     ```

- **If your management server is running Linux, modify the `/etc/exports` file to add `/jumpstart/Flash *(ro,no_root_squash)` below the last comment in the file.**

  For example:

  ```
  # Put custom additions below (Do not change/remove this line)
  /jumpstart/Flash      *(ro,no_root_squash)
  ```

3. **Copy the flash archive file to the `/jumpstart/Flash` directory.**

4. **Perform one of the following actions to restart NFS:**

   - **If your management server is running the Solaris Operating System, type the following commands:**

     ```
     # /etc/init.d/nfs.server stop
     # /etc/init.d/nfs.server start
     ```

   - **If your management server is running Linux, type the following commands:**

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

     OR

     ```
     # /etc/rc3.d/S60nfs restart
     ```

5. **Create an OS profile that specifies the location of the flash archive file that you copied in Step 3.**

   N1-ok> **create osprofile** *osprofile* **os** *os* **rootpassword** *rootpassword* **flar** *flar* **description** *description* **language** *language* **timezone** *timezone*

   The *flar* attribute value is the path and flash archive file name, for example, `/jumpstart/Flash/archive1.flar`.

   The OS profile is created.

6. **To verify the OS profile settings, type the following command:**

   N1-ok> **show osprofile** *osprofile*

   The OS profile details appear. Check that the partition settings are appropriate for your business needs. See "To Create an OS Profile" on page 83 for partition settings and examples.

7. **Load the OS profile on a server or a server group.**

   See "To Load an OS Profile on a Server or a Server Group" on page 90.

Example 3–3 Deploying a Solaris 9 OS Flash Archive

The following example shows how to create an OS profile that uses a flash archive file.

```
N1-ok> create osprofile solaris9_flar rootpassword admin description "solaris
9 with flar" os solx86 flar /jumpstart/Flash/S9-u7-req-v20z.archive
```

The following examples show how to add root and swap partitions to the OS profile.

```
N1-ok> add osprofile solaris9_flar partition / sizeoption free device
c1t1d0s0 type ufs

N1-ok> add osprofile solaris9_flar partition swap sizeoption fixed size 128
device c1t1d0s1 type swap
```

The following example shows how to deploy the modified OS profile to a server.

```
N1-ok> load server 192.168.73.2 osprofile
solaris9_flar networktype=static ip=192.168.73.244
```

The `networktype` attribute specifies that the installed host is assigned the `192.168.73.244` IP address.

▼ To Delete an OS Distribution

Note – An OS distribution cannot be deleted if it is associated with a deployed OS profile. A *deployed* OS profile is a profile that is currently being installed on a provisionable server.

Before You Begin

Delete all of the OS profiles that are associated with the OS distribution. This process includes deleting the default OS profile that was created when the OS distribution was copied. An OS profile cannot be deleted while it is being deployed. You may remove it after the deployment is completed. See "To Delete an OS Profile" on page 87 for instructions.

Steps

1. **Log in to the N1 System Manager.**

   See "To Access the N1 System Manager Command Line" on page 28 for details.

2. **Type the following command:**

   ```
   N1-ok> delete os os
   ```

   The distribution is deleted. See "delete os" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.

3. **View the available OS distributions.**

   ```
   N1-ok> show os all
   ```

   The deleted OS distribution should not appear in the output.

Managing OS Profiles

This section describes the following tasks:

Creating, Listing, and Modifying OS Profiles

OS profiles specify the following information:

- OS distribution to install
- Default language and time zone for the installed host
- Flash archive file to use
- Additional packages to install with the distribution
- Configuration information for partitions
- Custom installation scripts to run

After you have copied an OS distribution, the N1 System Manager automatically creates an OS profile of the same name on the management server. This OS profile is also called a *default OS profile*. See "Default OS Profiles" on page 81 for parameter settings and best practices for customizing OS profiles.

To view details of a default OS profile, use the `show` command with the `osprofile` keyword.

To create a new OS profile, use the `create osprofile`, `add osprofile`, and `set osprofile` commands. See Example 3–5 and Example 3–6 for command-line examples.

Default OS Profiles

When you copy an OS distribution, a default OS profile is automatically created for the OS distribution. The default profile is created for a typical Sun Fire V20z server, and it is mainly provided as an example. Settings for the default OS profiles are described in the following table.

TABLE 3–3 Default OS Profile Parameter Settings

Parameters	Solaris OS	Red Hat OS	SUSE OS
Root password	`admin`	`admin`	`admin`
Language	U.S. English	U.S. English	U.S. English
Time zone	Greenwich Mean Time (GMT)	Greenwich Mean Time (GMT)	Greenwich Mean Time (GMT)
Partitions	■ Root mount point `ufs` with a free file system size option on the `c1t1d0s0` slice ■ `swap` mount point 2048-Mbyte `swap` on the `c1t1d0s1` slice	■ Root mount point `ext3` with a free file system size option on the `sda` slice ■ `swap` mount point 2048-Mbyte `swap` on the `sda` slice	■ Root mount point `reiser` with a free file system size option on the `/dev/sda` slice ■ `swap` mount point 2048-Mbyte `swap` on the `/dev/sda` slice
Distribution group	`Entire Distribution plus OEM support`	`Everything`	`Default Installation`
Network Interfaces	Provisioning interface configured	Provisioning interface configured	Provisioning interface configured
	Data interface not configured	Data interface not configured	Data interface not configured

Best Practices for Modifying Default OS Profiles

To provision servers other than Sun Fire V20z servers, you need to modify the default profile, create a new OS profile, or clone an existing OS profile and customize the parameter settings. Each server at your site with different hardware and provisioning requirements requires the creation of a customized OS profile.

The browser interface provides a wizard for creating new OS profiles to limit the complexity of this operation. See "To Create an OS Profile" on page 83 for instructions.

Some best practices for modifying default OS profiles are:

- To increase the speed of OS configuration, modify OS profiles to use flash archives. See Example 3–8 for examples of how to modify a default profile and "To Copy a Flash Archive to the Management Server" on page 78 for instructions.
- To automatically configure the data network interface after OS profile installation, use the `add osprofile` command to add a script. See Step 4 in "To Provision the Solaris 10 OS" on page 70.

- Modify the default OS profile for a server other than a V20z server, remember to remove the existing partitions and add new partition information that is appropriate for the server model. See "To Modify the Default Solaris OS Profile for a Sun Fire V40z or a SPARC v440 Server" on page 212 for instructions.

▼ To List the Available OS Profiles

This procedure describes how to list the available OS profiles by using the browser interface. The example that follows the procedure provides the command-line equivalent.

Steps

1. **Log in to the N1 System Manager.**
   See "To Access the N1 System Manager Command Line" on page 28 for details.
2. **Click the System Dashboard tab.**
   The Shortcuts pane appears on the right side of the page.
3. **Click the Edit List button beneath the OS Profiles list.**
   The list of available OS profiles appears.

Example 3–4 Listing Available OS Profiles Through the Command Line

The following example shows how to view all of the OS profiles in the system.

```
N1-ok> show osprofile all
```

All available OS profiles appear in the output. See "show osprofile" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.

▼ To Create an OS Profile

This procedure describes how to use the browser interface's OS Profile wizard. The examples that follow the procedure provide command-line equivalents for creating and customizing OS profiles for the Solaris, Red Hat, and SUSE platforms.

Before You Begin

You must copy an OS distribution before you can create an OS profile. See "To Copy an OS Distribution From CDs or a DVD" on page 76 or "To Copy an OS Distribution From ISO Files" on page 75.

Steps

1. **Log in to the N1 System Manager.**
   See "To Access the N1 System Manager Command Line" on page 28 for details.
2. **Click the System Dashboard tab.**
   The Shortcuts pane appears on the right side of the page.

3. **Click the New button beneath the OS Profiles list.**
   The Create New Operating System Profile wizard appears.
4. **Use the wizard steps to guide you through the screens.**

Note – Click the Help tab in the left pane of the wizard for detailed information about the entry fields.

---

5. **To complete the creation of the OS profile, click the Finish button in the wizard.**
   The wizard window closes.
6. **Click the Edit List button in the OS Profile Shortcuts.**
   A dialog box appears.
7. **Select the check box for the OS profile and click the OK button.**
   The drag-and-drop icon appears in the OS profiles Shortcuts list.

Example 3–5 Creating a Solaris OS Profile Through the Command Line

The following example illustrates the commands that are used to create an OS profile for a Solaris OS distribution. The first command creates a Solaris 10 profile that is named `S10profile` and sets the root password to `admin`.

```
N1-ok> create osprofile S10profile rootpassword admin
description "S10 for host123" os solaris10
```

The following example command shows how to configure a `swap` partition with a size of 2048 Mbytes.

```
N1-ok> add osprofile s10profile partition swap size 2048 device c1t1d0s1
type swap
```

The following example command shows how to configure a free `ufs` partition.

```
N1-ok> add osprofile s10profile partition / sizeoption free device c1t1ds0
type ufs
```

The following example command shows how to add the default Solaris distribution group.

```
N1-ok> add osprofile s10profile distributiongroup "Entire Distribution
plus OEM support"
```

OS profiles that install only the Core System Support distribution group cannot be monitored by using the OS monitoring feature.

Example 3–6 Creating a Red Hat OS Profile Through the Command Line

The following example illustrates the commands that are used to create an OS profile for a Red Hat distribution.

```
N1-ok> create osprofile RH30profile rootpassword admin
os RedHat30
```

The following example command shows how to configure a `root` partition.

```
N1-ok> add osprofile RH30profile partition / device sda type ext3
sizeoption free
```

The following example command shows how to configure a `swap` partition.

```
N1-ok> add osprofile RH30profile partition swap device sda type swap
size 2048 sizeoption fixed
```

The following example command shows how to specify the distribution group.

```
N1-ok> add osprofile RH30profile distributiongroup "Everything"
```

Example 3–7 Creating a SUSE OS Profile Through the Command Line

The following example illustrates the commands that are used to create an OS profile for a SUSE distribution.

```
N1-ok> create osprofile default os suse rootpassword admin
```

The following example command shows how to configure a `root` partition.

```
N1-ok> add osprofile default partition / device /dev/sda type reiser
sizeoption free
```

The following example command shows how to configure a `swap` partition.

```
N1-ok> add osprofile default partition swap device /dev/sda type swap
size 2048 sizeoption fixed
```

The following example command shows how to specify the distribution group.

```
N1-ok> add osprofile default distributiongroup "Default Installation"
```

Troubleshooting

- "To Modify the Default Solaris OS Profile for a Sun Fire V40z or a SPARC v440 Server" on page 212
- "To Modify a Solaris 9 OS Profile for a Sun Fire V20z Server With a K2.0 Motherboard" on page 213

See Also To find out how to load the OS profile, see "To Load an OS Profile on a Server or a Server Group" on page 90.

▼ To Clone an Existing OS Profile

The following procedure describes how to *clone* or copy an existing OS profile. You might want to clone an existing OS profile if you need to modify it, but cannot do so because it is deployed. A *deployed* OS profile is a profile that is currently being installed on a provisionable server.

Steps

1. **Log in to the N1 System Manager.**
   See "To Access the N1 System Manager Command Line" on page 28 for details.
2. **Type the following command:**

   ```
   N1-ok> create osprofile osprofile clone oldprofile
   ```

   The new OS profile is created. See "create osprofile" in *Sun N1 System Manager 1.2 Command Line Reference Manual*
3. **Type the following command:**

   ```
   N1-ok> show osprofile osprofile
   ```

   The new OS profile appears in the output.

See Also To find out how to load the OS profile, see "To Load an OS Profile on a Server or a Server Group" on page 90.

▼ To Modify an OS Profile

This procedure describes how to modify the scripts, partitions, updates, and distribution groups that are configured for an OS profile.

Note – An OS profile that is currently being deployed cannot be modified.

Steps

1. **Log in to the N1 System Manager.**
   See "To Access the N1 System Manager Command Line" on page 28 for details.
2. **Modify an OS profile by performing one of the following actions:**
   - **Add new OS profile attributes.**

     ```
     N1-ok> add osprofile osprofile [configuration-attributes]
     ```

     See "add osprofile" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.
   - **Remove existing OS profile attributes.**

     ```
     N1-ok> remove osprofile osprofile [configuration-attributes]
     ```

     See "remove osprofile" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.
   - **Change existing OS profile parameters.**

     ```
     N1-ok> set osprofile osprofile [configuration-attributes]
     ```

See "set osprofile" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.

3. **View the new OS profile details.**

   ```
   N1-ok> show osprofile osprofile
   ```

   The modified OS profile information appears in the output.

Example 3–8 Modifying an OS Profile Through the Command Line

This example shows how to use a flash archive and a post-installation script by modifying the `solaris_ver10` OS profile.

For this example, assume that you have created the following script in a directory named `/scripts` on the management serverdirectory.

This sample script name is `add_host.sh` and the script adds a host to the `/etc/hosts` file on a provisionable server.

```
echo "129.10.12.101 myhost" >>/a/etc/hosts
```

Note that the root file system on the provisioned server is `/a` during the post installation time.

This example also assumes that you have created a flash archive file called `archive1.flar` and that you have completed the steps in "To Copy a Flash Archive to the Management Server" on page 78.

The following example shows how to add the script to the OS profile.

```
N1-ok> add osprofile solaris_ver10 script
/scripts/add_host.sh type post
```

The following example shows how to set up the OS profile to use the flash archive.

```
N1-ok> set osprofile solaris_ver10 flar /jumpstart/Flash/archive1.flar
```

See Also To find out how to load the modified OS profile, see "To Load an OS Profile on a Server or a Server Group" on page 90.

▼ To Delete an OS Profile

An OS profile cannot be deleted if it is deployed. A profile is *deployed* if it is currently being installed on a provisionable server.

Steps

1. **Log in to the N1 System Manager.**

   See "To Access the N1 System Manager Command Line" on page 28 for details.

2. **Type the following command:**

   ```
   N1-ok> delete osprofile osprofile
   ```

   The OS profile is deleted from the management server.

3. **Type the following command:**

   ```
   N1-ok> show osprofile all
   ```

   The deleted OS profile should not appear in the output.

Installing OS Distributions by Deploying OS Profiles

This section describes the following tasks:

Deploying OS Profiles

OS profile installations can be customized to fit your provisioning and network needs.

To deploy default or custom OS profiles, use the `load` command with the `server` or `group` keyword and the `osprofile` subcommand.

To add the base management and OS monitoring features that support updating and patching, use the `feature` attribute with the `osmonitor` value when you issue the `load` command. The `feature` attribute of the `load` command enables you to automatically configure monitoring when you load the OS profile.

For syntax and parameter details, type `help load server`, `help load group`, and `help add server` at the `N1-ok` command line.

Servers boot from their default network boot interface automatically as the final step of a load operation.

The following table provides a quick reference of all the parameters that are available for the `load group` and `load server` commands.

Note – Before you attempt any Solaris OS on x86 platform deployments by using the N1 System Manager, you must ensure that the `nameserver` and `search` values are correctly configured at the operating system level on your management server. Otherwise, the installations will fail.

For more details, see the `resolv.conf`(5) man page. You need `root` user access on your management server to modify these settings.

TABLE 3–4 OS Profile Installation Parameters

Parameters	Red Hat or SUSE OS	Solaris OS	Multiple Servers	Single Server	Notes
bootip	✓ (R)		✓	✓	Also known as provisionable IP.
ip	✓	✓ (R)	✓	✓	Required if *networktype* is set to `static`.
networktype	✓ (R)	✓ (R)	✓	✓	Must be set to `static` for Solaris installation.
bootgateway	✓		✓	✓	
boothostname	✓			✓	
bootnameserver	✓		✓	✓	
bootnetmask	✓		✓	✓	Default is set to the provisioning network interface that is specified using the `n1smconfig` utility.
bootnetworkdevice	✓	✓	✓	✓	
bootpath		✓		✓	
console	✓	✓		✓	
consolebaud	✓	✓		✓	
kernelparameter	✓		✓	✓	
domainname		✓	✓	✓	If `domainname` is not specified, a default will be configured
gateway	✓	✓	✓	✓	
hostname	✓	✓		✓	
nameserver	✓	✓	✓	✓	
netmask	✓	✓	✓	✓	Default is set to the provisioning network interface that is specified using the `n1smconfig` utility.

TABLE 3–4 OS Profile Installation Parameters *(Continued)*

Parameters	Red Hat or SUSE OS	Solaris OS	Multiple Servers	Single Server	Notes
networkdevice	✓		✓	✓	The Linux default is `eth0`. The Primary network interface is the default for Solaris installations.

(R) = Required

✓ = Configurable

▼ To Load an OS Profile on a Server or a Server Group

The following procedure describes how to load an OS profile on a server or a server group by using the browser interface. The examples that follow the procedure provide command-line equivalents.

Caution – Uninstallation of an OS profile is not supported. However, you can reprovision a server by loading another OS profile on a server that is already provisioned.

Before You Begin

- Create an OS profile. See "To Create an OS Profile" on page 83.
- Disable monitoring for the servers that will be loaded with an OS profile. See "To Disable Monitoring for a Server or a Server Group" on page 173 for details. Disabling monitoring prevents the fault notifications that are generated if the server reboots after installation.
- Ensure that you have enough disk space available to load an OS profile.
- If you are loading a Red Hat 4 OS profile on a Sun Fire X2100 server or group of Sun Fire X2100 servers, see Example 3–13 for the required `bootnetworkdevice` and `networkdevice` attribute values.
- Optionally create and copy a flash archive file. See "To Copy a Flash Archive to the Management Server" on page 78.
- Optionally create and copy a post-installation script to the management server. See Step 4.

Steps

1. **Log in to the N1 System Manager.**

   See "To Access the N1 System Manager Browser Interface" on page 29 for details.

2. **(Optional) Modify the OS profile to use a flash archive and a post-installation script.**

   ```
   N1-ok> set osprofile osprofile flar flar
   ```

The *flar* attribute value is the full path and flash archive file name, for example, `/jumpstart/Flash/archive1.flar`.

```
N1-ok> add osprofile osprofile script script type type
```

The *script* attribute value is the full path and script file name, for example, `/etc/sysconfig/network-scripts/ifcfg-eth1`.

The *type* attribute specifies the time when the custom script will run during the installation. Valid values for the `type` attribute are:

- `pre` – Run the script before the installation (for example, drivers).
- `post` – Run the script after the installation.
- `postnochroot` – Run the script after the installation. The script does not have to be run as superuser (root).

The OS profile is modified to use the designated post-installation script and the flash archive file.

3. **Navigate to the table that contains the server or the server group by performing one of the following actions:**

   - **Choose All Servers from the View Selector menu.**
     The Servers table appears.
   - **Choose Servers By Group from the View Selector menu.**
     The Server Groups table appears.

4. **Drag and drop the OS profile icon from the Shortcuts pane to the server or the server group.**
   The Load OS Profile wizard appears.

5. **Use the wizard steps to guide you through the screens.**

Note – Click the Help tab in the left pane of the wizard for detailed information about the entry fields.

---

6. **To begin loading the OS profile on the selected servers, click the Finish button in the wizard.**
   The wizard window closes and a job ID appears in the Command Line pane.

7. **Click the Jobs tab.**
   The Jobs table appears with information about your Load OS job.

Note – The Load OS job will not complete until a final reboot occurs.

---

8. **Save the options that you used to load the OS profile as a note in case you need to restore the server sometime in the future.**

   See "Modifying Server and Server Group Information" on page 123 for details.

Example 3–9 Loading a Solaris OS Profile on a Server Through the Command Line

The following example shows you how to install a Solaris OS profile on a server by using the `load` command. The feature parameter specifies that the OS monitoring feature is installed. See "Adding and Upgrading Base Management and OS Monitoring Features" on page 157 for details.

```
N1-ok> load server 192.168.8.9 osprofile S10profile
networktype static ip 192.168.18.19 feature osmonitor agentssh root/rootpassword
```

The `networktype` attribute must be set to `static` for Solaris profile installations. See Table 3–4 and "load server" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.

Use the `show job` command to view the results.

```
N1-ok> show job target=192.168.8.9
```

Example 3–10 Loading a Solaris OS Profile on a Server Group Through the Command Line

The following example shows you how to install a Solaris OS profile on a server group by using the `load` command.

```
N1-ok> load group devgroup osprofile S10profile
excludeserver=server1 networktype static ip 192.186.8.8-192.186.8.9
Job "14" started.
```

The `networktype` attribute must be set to `static` for Solaris profile installations. See Table 3–4 and "load server" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.

The following command shows you how to view the job results.

```
N1-ok> show job 14
```

Example 3–11 Loading a Linux OS Profile on a Server

The following example shows you how to install a Linux OS profile on a server by using the `load` command.

```
N1-ok> load server 192.168.8.9 osprofile RH3profile
bootip 192.168.8.9 networktype dhcp
```

The `bootip` attribute is only used for Linux profile installations.

The following command shows you how to view the job results.

```
N1-ok> show job target=192.168.8.9
```

Setting the `networktype` attribute to DHCP means that the server uses DHCP to get its provisioning network IP address. If the system reboots, any added management features will break. In this case, use the `set server agentip` command to modify the server's agent IP address. See "To Modify the Agent IP for a Server" on page 162 for more information.

Example 3–12 Loading a Linux OS Profile on a Server Group

The following example shows you how to install a Linux OS profile on a server group by using the `load` command.

```
N1-ok> load group devgroup osprofile RH3profile
bootip 192.186.8.8-192.186.8.9 networktype dhcp
Job "15" started
```

The following command shows you how to view the job results.

```
N1-ok> show job 15
```

Setting the `networktype` attribute to DHCP means that the server uses DHCP to get its provisioning network IP address. If the system reboots, any added management features will break. In this case, use the `set server agentip` command to modify the server's agent IP address. See "To Modify the Agent IP for a Server" on page 162 for more information.

Example 3–13 Loading a Red Hat Enterprise Linux 4 OS Profile on a Sun Fire X2100 Server

This example shows you how to load a Red Hat Enterprise Linux 4 OS profile onto a Sun Fire X2100 server using static IP network configuration.

```
N1-ok> load server server1 osprofile RHEL4profile bootip 192.168.8.8
networktype static ip 192.168.8.8 bootnetworkdevice eth1 networkdevice eth1
```

This example shows you how to load a Red Hat Enterprise Linux 4 OS profile onto a Sun Fire X2100 server using DHCP network configuration.

```
N1-ok> load server server34 osprofile rh4u1es-64-min bootip=10.0.101.34
networktype=dhcp bootnetworkdevice=eth1 networkdevice=eth1
```

The values `bootnetworkdevice` and `networkdevice` are only required for Red Hat Linux 4 on Sun Fire X2100 servers.

Example 3–14 Loading a Solaris 10 x86 OS Profile on a Sun Fire X2100 Server

When loading Solaris 10 x86 to a Sun Fire X2100 server , you need to first add a script to the profile. This script will disable the loading of the `bge` driver in `/etc/system`.

If your management server is running Linux, use the following command to add the script to the profile:

```
N1-ok> add osprofile profile_name script
/opt/sun/scs/data/allstart/scripts/solaris_bge_disable.sh type=post
```

If your management server is running the Solaris OS, use the following command to add the script to the profile:

```
N1-ok> add osprofile profile_name script
/opt/SUNWscs/data/allstart/scripts/solaris_bge_disable.sh type=post
```

The service processor will become inaccessible while the machine is being provisioned.

Troubleshooting If a value is not specified for the `bootnetmask` or `netmask` parameters during the load operation, the netmask will default to the provisioning network interface that is specified in the `n1smconfig` utility. See "To Configure the N1 System Manager System" in *Sun N1 System Manager 1.2 Installation and Configuration Guide*.

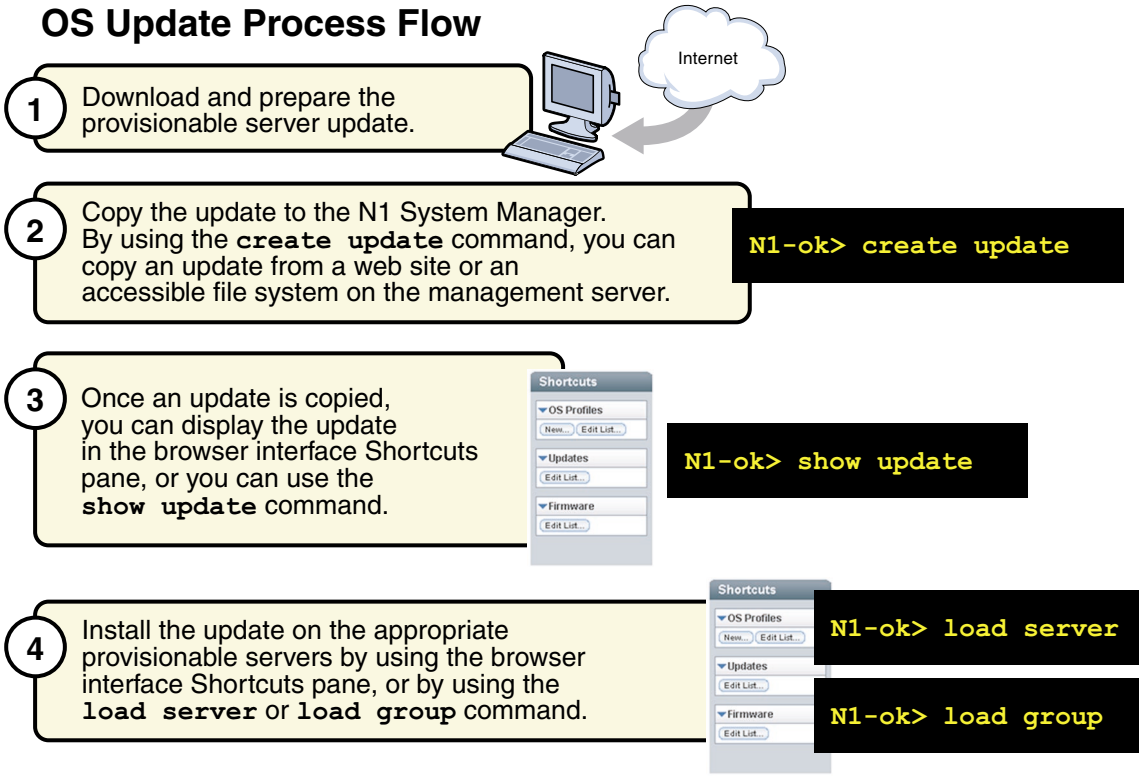
If the deployment fails, see the topics in "OS Profile Deployment Failures" on page 211 for possible solutions.

Next Steps To enable remote connectivity, OS resource monitoring, package deployment, and inventory management, you must add the OS monitoring feature on each server. See "To Add the OS Monitoring Feature" on page 158.

Managing Packages, Patches, and RPMs

The N1 System Manager enables you to perform following OS update management tasks:

The following graphic describes the order in which these tasks should be completed.



Introduction to Managing OS Updates

After you have installed an OS on a provisionable server, the N1 System Manager enables you to install OS updates. These OS updates consist of Solaris packages and patches and Linux RPMs.

For Solaris packages or patches, you can issue an optional parameter to install the updates by using a script. This parameter is useful for installation of a set of packages or patches that have dependencies. Use the `create update` command with the `installscriptfile` parameter to specify the script. See Example 3–16 for an example script and sample command syntax.

Installing OS updates on servers for the first time involves the following four-step process when you use the N1 System Manager:

1. Downloading the OS update.
2. Copying the OS update to the N1 System Manager

   The N1 System Manager must have system access to the OS update before the update can be installed on the provisionable servers.

By using the `create update` command, you can import an OS update from a web site or an accessible file system on the management server. After an OS update is imported, you can display the update in the browser interface's Shortcuts pane, or you can use the `show update` command.

3. Verifying that the OS update was copied by displaying the Shortcut in the browser interface or by using the `show update` command.
4. Installing the OS update on the appropriate provisionable servers by using the browser interface or the `load server` or `load group` commands. The provisionable servers must have the base management feature supported.

OS update installations behave differently for every operating system because the native package installation mechanisms are used. For example, if a Solaris package is already installed on the target server, the installation might succeed without reporting an error. However, this same scenario for a Linux RPM results in an error message indicating that the package is already installed.

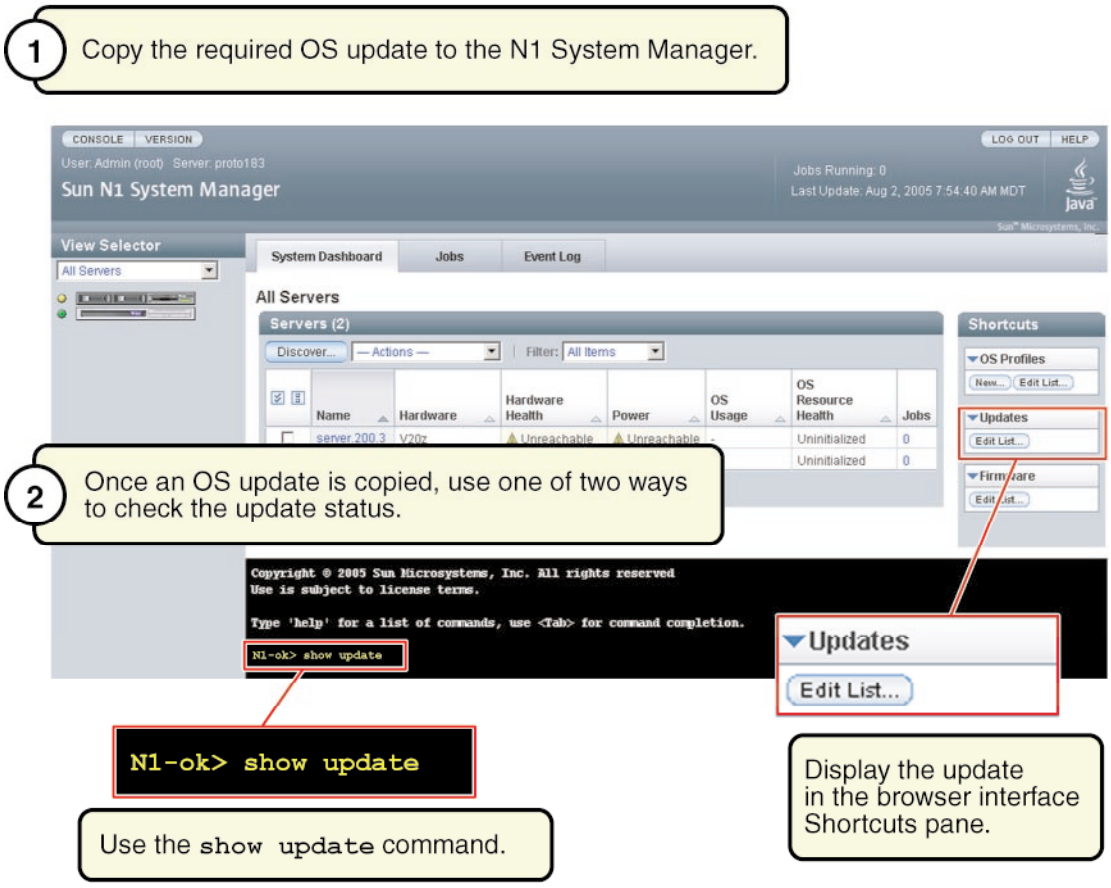
See "OS Update Problems" on page 219 for troubleshooting information.

▼ To Copy an OS Update

This procedure describes how to copy an OS update to the N1 System Manager. Once an OS update is copied, you can use the command line or the browser interface to install the OS update on a provisionable server.

The following graphic illustrates the use of the browser user interface for confirming that an OS update has been successful.

Update Process Flow



Before You Begin

Ensure that the OS update is available to the management server on the local file system, a network accessible file, or a web site. You can copy OS updates in the following formats:

- `*.rpm` – Linux RPM
- `*.pkg` or `*.tar` – Solaris package
- `*.zip` – Solaris patch.

Note – The `*.tar` file must match the top-level directory name after the tar expansion. For example, if the tar file is `SUNWstade.tar`, the top-level directory of the tar expansion must be `SUNWstade`.

Steps

1. **Log in to the N1 System Manager.**

   See "To Access the N1 System Manager Command Line" on page 28 for details.

2. **Copy the OS update to the N1 System Manager.**

   ```
   N1-ok> create update update file file ostype ostype [adminfile adminfile]
   [responsefile responsefile] [installscriptfile installscriptfile]
   ```

   Valid `ostype` values are in the following list:

   - `redhat-es3` – Red Hat Enterprise Linux ES 3.0
   - `redhat-ws3` – Red Hat Enterprise Linux WS 3.0
   - `redhat-as3` – Red Hat Enterprise Linux, AS 3.0
   - `redhat-as4` – Red Hat Enterprise Linux, AS 4.0
   - `redhat-es4` – Red Hat Enterprise Linux, ES 4.0
   - `redhat-ws4` – Red Hat Enterprise Linux, WS 4.0
   - `redhat-es3-64` – Red Hat Enterprise Linux ES 3.0, 64-bit
   - `redhat-ws3-64` – Red Hat Enterprise Linux WS 3.0, 64-bit
   - `redhat-as3-64` – Red Hat Enterprise Linux, AS 3.0, 64-bit
   - `redhat-as4-64` – Red Hat Enterprise Linux, AS 4.0, 64-bit
   - `redhat-es4-64` – Red Hat Enterprise Linux, ES 4.0, 64-bit
   - `redhat-ws4-64` – Red Hat Enterprise Linux, WS 4.0, 64-bit
   - `solaris9x86` – Solaris x86 Version 9 Update 7
   - `solaris10x86` – Solaris x86 Version 10
   - `solaris9sparc` – Solaris SPARC Version 9 Update 7
   - `solaris10sparc` – Solaris SPARC Version 10
   - `suse-es9` – SUSE LINUX Enterprise Server 9
   - `suse-es9-64` –SUSE LINUX Enterprise Server 9, 64-bit
   - `suse-pro92` – SUSE Professional Edition 9.2
   - `suse-pro92-64` – SUSE Professional Edition 9.2, 64-bit
   - `suse-pro93` – SUSE Professional Edition 9.3
   - `suse-pro93-64` – SUSE Professional Edition 9.3, 64-bit

   See "create update" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.

Example 3–15 Creating an OS Update Through the Command Line

The following example command shows how to create an OS update named `RH3_update` where the `ostype` is Red Hat Enterprise Linux, AS 3.0 and the location of the update file is `/tmp/test-i386.rpm`.

```
N1-ok> create update RH3_update file /tmp/test-i386.rpm ostype=redhat-as3
```

Example 3–16 Copying an OS Update With a Package Install Script Through the Command Line

This example shows an executable Bourne (`/bin/sh`) shell package installation script.

```
#!/bin/sh
echo "This is from the install script:"
```

```
echo "pkgadd -n -a /tmp/combo-pkgs.pkg.admin -d /tmp/combo-pkgs.pkg SUNWtest1 SUNWtest2"
pkgadd -n -a /tmp/combo-pkgs.pkg.admin -d /tmp/combo-pkgs.pkg SUNWtest1 SUNWtest2
exit $?
```

The following sample command shows how to associate the package installation script with the OS update files. This example assumes that you have copied the script to the management server's `/tmp` directory with the name `install.sh`.

```
N1-ok> create update combo file /tmp/combo-pkgs.pkg ostype solaris10x86 adminfile
/tmp/combo-pkgs.pkg.admin installscriptfile /tmp/install.sh
```

In this example, `/tmp/combo-pkgs.pkg` contains two Solaris packages in the datastream format.

The script and the source files for the OS update are copied to the target server when the `create os` command is issued. The script file is executed by using the Bourne shell with the full path to the package file as the sole argument. If the `adminfile` subcommand is not specified, the default `admin` file is also copied to the target server and is renamed with `.admin` appended to the source file name.

Example 3–17 Copying an OS Update With a Patch Install Script Through the Command Line

This example shows an executable Bourne (`/bin/sh`) shell patch installation script.

As a best practice, any installation script that you use should create a new subdirectory, for example, in the `/tmp` directory. The script should then move or extract the OS update `.tar` file into that subdirectory. After the update is complete, the script should remove this subdirectory.

By default, the script executes in the invoker's `home` directory. In this case, this is the `root` directory. In addition, the installation script should refer to the full path to the package source files to avoid conflicts.

```
#!/bin/sh
mkdir /tmp/layer
cd /tmp/layer
echo "untar the source:"
tar -xvf /tmp/mypatches.tar
echo "let's install mypatches:"
patchadd -M /tmp/layer 117448-01 117466-01
exit $?
```

The following sample command shows how to associate the patch installation script with the OS update files. This example assumes that you have copied the script to the management server's `/tmp` directory with the name `install.sh`.

```
N1-ok> create update mypatches file /tmp/mypatches.tar ostype solaris10x86 installscriptfile
/tmp/install.sh
```

In this example, `/tmp/mypatches.tar` contains the Solaris patches 117448–01 and 117466–01 in the datastream format.

The script and the source files for the OS update are copied to the target server when the `create os` command is issued. The script file is executed by using the Bourne shell with the full path to the package file as the sole argument.

Troubleshooting If you use the `installscriptfile` parameter when creating an OS update, consider loading the OS update on a single server to test whether the script is working correctly before loading on a large server group.

Refer to "OS Update Creation Failures" on page 220 for solutions to common errors.

See Also To find out how to load an OS update, see "To Load an OS Update on a Server or a Server Group" on page 100

▼ To Load an OS Update on a Server or a Server Group

This procedure describes how to load an OS update by using the browser interface. The example that follows the procedure provides a command-line equivalent.

The following default `admin` file is used to install Solaris packages:

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

The `admin` file is located in the `/opt/sun/n1gc/etc` directory on the management server.

Before You Begin

- Copy the OS update to the N1 System Manager. See "To Copy an OS Update" on page 96 for details.
- Disable monitoring for the provisionable server. This action is required only if you want to avoid the fault notifications if the server reboots after an OS update installation. See "To Disable Monitoring for a Server or a Server Group" on page 173 for details.
- Ensure that the base management feature is added to the provisionable server. This action provides the necessary support to install OS updates. You can automatically add base management support by adding the OS monitoring feature. See "To Add the OS Monitoring Feature" on page 158 for details.

- Ensure that the package file name matches the name of the package. If the file name does not match that of the package and an `adminfile` is used to install the OS update, uninstallation will fail.

Steps

1. **Log in to the N1 System Manager.**
   See "To Access the N1 System Manager Browser Interface" on page 29 for details.
2. **Navigate to the table that contains the server or the server group by performing one of the following actions:**
   - **Choose All Servers from the View Selector menu.**
     The Servers table appears.
   - **Choose Servers By Group from the View Selector menu.**
     The Server Groups table appears.
3. **Drag and drop the OS update icon from the Shortcuts pane to the server or the server group.**
   The Load OS Update confirmation dialog box appears.
4. **To begin loading the OS update on the selected servers, click the OK button.**
   The dialog box closes.
5. **Click the Jobs tab.**
   The Jobs table appears with information about your Load OS Update job.
6. **Verify that the installation was successful.**

   ```
   N1-ok> show server server
   ```

Example 3–18 Loading an OS Update Through the Command Line

The following command shows you how to install an OS update on two servers by using the load command.

```
N1-ok> load server server1,server2 update SUNWn1gcsolsparcag
```

See "load server" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.

Example 3–19 Loading an OS Update on a Server Group Through the Command Line

The following command shows you how to install an OS update on a server group by using the load command.

```
N1-ok> load group devgroup update SUNWupdate1,SUNWupdate2
```

See "load group" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.

Troubleshooting "Solaris OS Update Deployment Failures" on page 221

▼ To List the Available OS Updates

This procedure describes how to list the available OS updates that have been copied to the N1 System Manager. These OS updates can be installed on a provisionable server.

The example that follows the procedure provides a command-line equivalent.

Steps

1. **Log in to the N1 System Manager.**
   See "To Access the N1 System Manager Browser Interface" on page 29 for details.
2. **Click the System Dashboard tab.**
   The Shortcuts pane appears.
3. **Click the Expand/Collapse icon on the Update title bar.**
   The Update list expands.
4. **Click the Edit List button.**
   The Edit List dialog box appears with the list of available updates.

Example 3–20 Listing Available OS Updates Through the Command Line

The following command shows you how to list all of the OS updates in the system.

```
N1-ok> show update all
```

▼ To List the OS Updates Installed on a Provisionable Server

Tip – You can also use the browser interface Server Details page to view all of the OS updates that are installed on a server.

Steps

1. **Log in to the N1 System Manager.**
   See "To Access the N1 System Manager Command Line" on page 28 for details.
2. **List the OS updates that are installed on a provisionable server.**

   ```
   N1-ok> show server server
   ```

   See "show server" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details

▼ To Delete an OS Update

This procedure describes how to delete an OS update from the N1 System Manager. This procedure does not delete an OS update from a provisionable server. See "To Uninstall an OS Update From a Provisionable Server" on page 103 for details on that specific task.

Steps

1. **Log in to the N1 System Manager.**

   See "To Access the N1 System Manager Command Line" on page 28 for details.

2. **Delete an OS update from the N1 System Manager.**

   ```
   N1-ok> delete update update
   ```

   See "delete update" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.

▼ To Uninstall an OS Update From a Provisionable Server

Before You Begin

- Disable monitoring for the provisionable server. Disabling monitoring prevents the fault notifications if the server reboots after an OS update uninstallation. See "To Disable Monitoring for a Server or a Server Group" on page 173 for details.
- Ensure that the OS monitoring feature is supported on the provisionable server. This action provides the necessary support to uninstall OS updates. See "To Add the OS Monitoring Feature" on page 158 for details.

Steps

1. **Log in to the N1 System Manager.**

   See "To Access the N1 System Manager Command Line" on page 28 for details.

2. **Uninstall an OS update from a provisionable server.**

   ```
   N1-ok> unload server server[,server...] update update
   ```

Caution – If the user-specified update name is not found, the command tries to uninstall an OS update with a matching file name. The `show update` command enables you to list an OS update's corresponding file name.

See "unload server" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.

Troubleshooting If you cannot uninstall an OS update that was installed with an `admin` file, check that the package file name matches the name of the package. If the name is not the same, rename the `admin` file in the provisionable server's `/tmp` directory to match the name of the package and try the `unload` command again. If the package still exists, remove it from the provisionable server by using `pkgrm`.

See Also "OS Update Uninstallation Failures" on page 225

▼ To Uninstall an OS Update on a Server Group

Before You Begin

- Disable monitoring for the provisionable servers. This action is required only if you want to avoid the fault notifications if the servers reboot after an OS update uninstallation. See "To Disable Monitoring for a Server or a Server Group" on page 173 for details.
- Ensure that the OS monitoring feature is supported on the provisionable servers. This action provides the necessary support to uninstall OS updates. See "To Add the OS Monitoring Feature" on page 158 for details.

Steps

1. **Log in to the N1 System Manager.**

   See "To Access the N1 System Manager Command Line" on page 28 for details.

2. **Uninstall an OS update on the provisionable servers in a server group.**

   ```
   N1-ok> unload group group update update
   ```

Caution – If the user-specified update name is not found, the command tries to uninstall an OS update with a matching file name. Use the `show update` command to list an OS update's corresponding file name.

See "unload group" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.

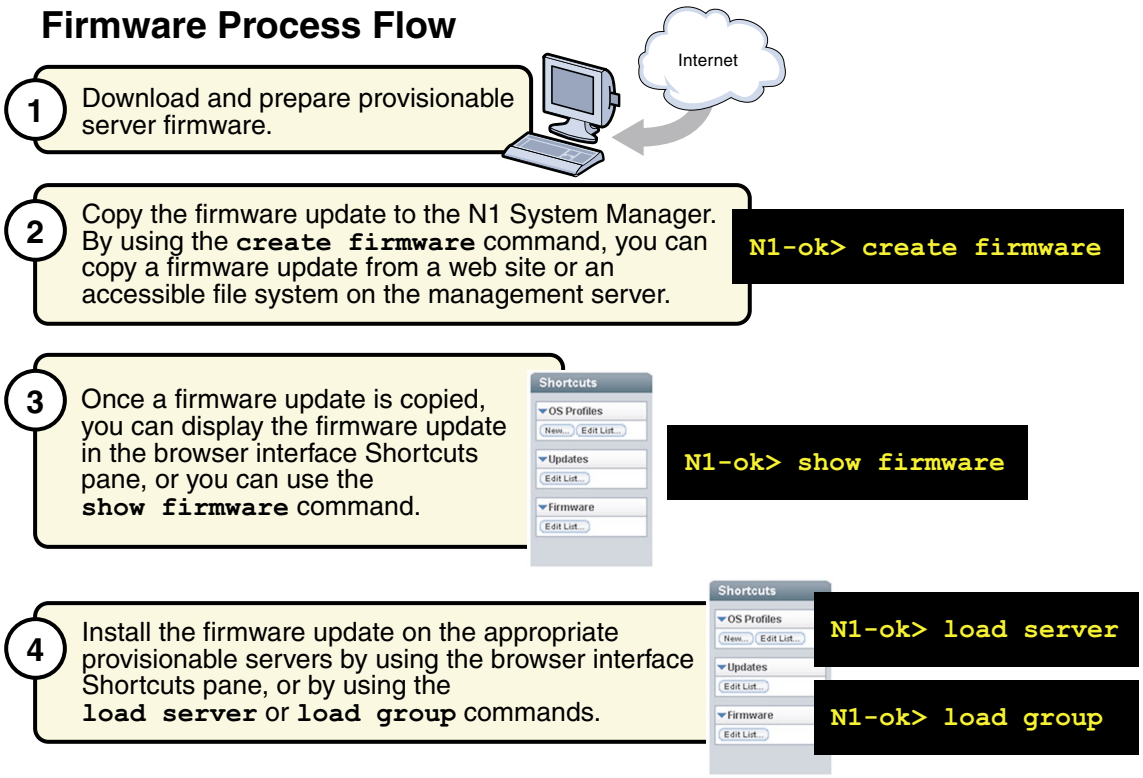
Managing Firmware SP, BIOS, and ALOM Updates

The N1 System Manager enables you to perform the following firmware management tasks:

- "To Copy a Firmware Update" on page 106

Note – Firmware updates to Sun Fire X2100 servers are not supported. Refer to Sun System Handbook documentation for the Sun Fire X2100 server for information about how to update firmware to the versions that are required for management by the Sun N1 System Manager. See "Discovering Servers" on page 51 for the firmware versions required to discover a Sun Fire X2100 server.

The following graphic describes the order in which firmware management tasks must be performed.



Introduction to Managing Firmware Updates

Updating the firmware on the provisionable servers is a primary administrative task. Installing a firmware update on a provisionable server for the first time involves the following four-step process when you use the N1 System Manager:

1. Downloading and preparing the firmware update. Ensure that the firmware version matches those set out in "Discovering Servers" on page 51.
2. Copying the firmware update to the N1 System Manager. The N1 System Manager must have system access to the firmware update before the firmware update can be installed on the provisionable servers.

   By using the `create firmware` command, you can copy a firmware update from a web site or an accessible file system on the management server. Once a firmware update is copied, you can display the firmware update in the browser interface Shortcuts pane, or you can use the `show firmware` command.
3. Verifying that the firmware update was copied successfully by displaying the firmware Shortcut in the browser interface or by using the `show firmware` command.
4. Installing the firmware update on the appropriate provisionable servers by using the browser interface, or by using the `load server` or `load group` command.

When importing firmware updates, you must specify the following metadata:

- Vendor – The name of the firmware update vendor
- Model – The model name of a valid hardware system for the firmware update
- Type – The type of firmware update, required only for Sun Fire V20z and V40z servers:
  - SP – Service Processor
  - BIOS – Server Platform BIOS
  - PIC – Service Processor Operator Panel
- Version – (Optional) The version number of the firmware update

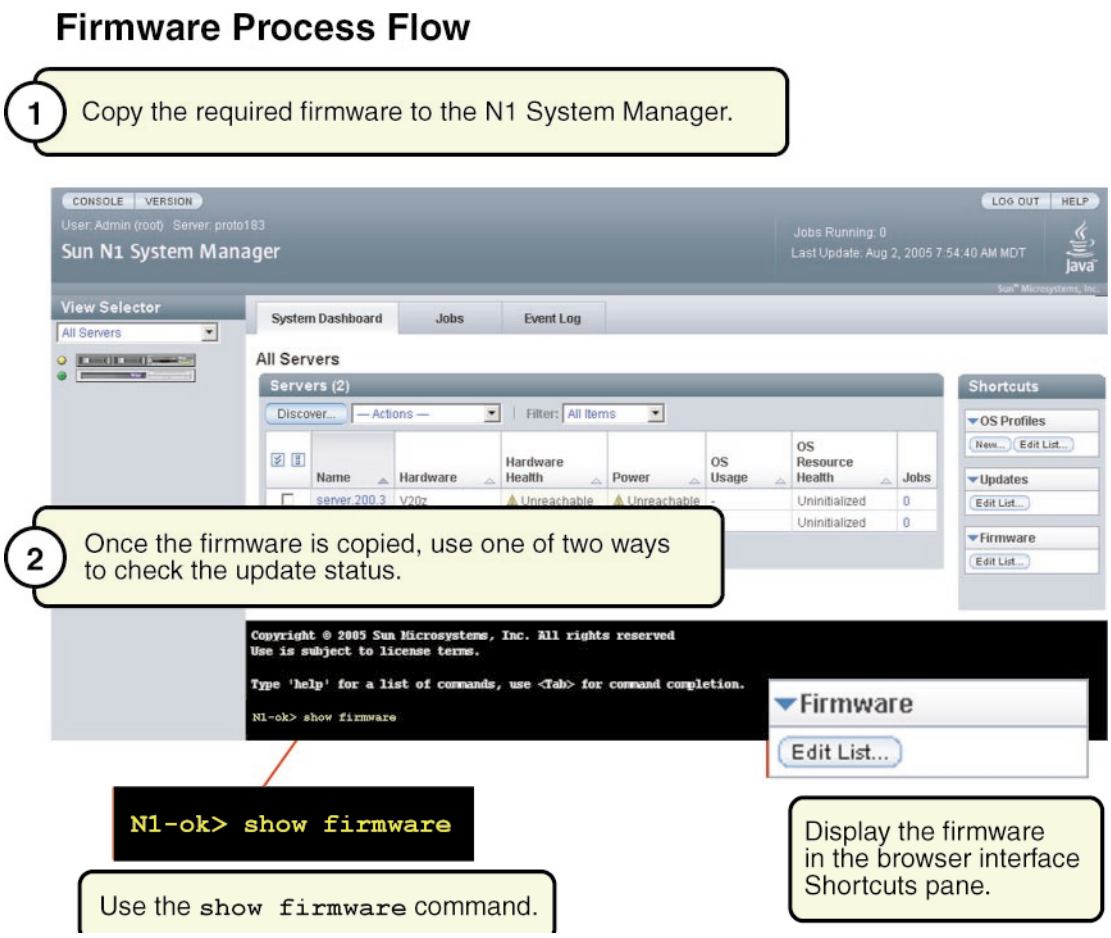
---

Note – Firmware version 2.2 and above for the Sun Fire V20z servers do not support the PIC firmware upgrade. The upgrade of PIC firmware will fail, and the job step will show an error message similar to the following: "This operation is not supported on *server*. Refer to the log file for more information."

▼ To Copy a Firmware Update

This procedure describes how to copy a new firmware update to the N1 System Manager. Once a firmware update is copied, you can use the command line or the browser interface to install the firmware update on a provisionable server.

The following graphic illustrates the use of the browser interface to verify a firmware update.



Before You Begin

Ensure that the firmware update is available to the management server from the local file system, a network accessible file, or a web site.

Steps

1. **Log in to the N1 System Manager.**

   See "To Access the N1 System Manager Command Line" on page 28 for details.

2. **Copy the firmware update.**

   ```
   N1-ok> create firmware firmware url=url vendor=vendor model=model[,model...] [type type]
     [description description] [version version]
   ```

The `type` attribute is required for Sun Fire V20z and V40z servers. Valid values for the `type` are `BIOS` and `SP`. All values are case-sensitive.

See "create firmware" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.

3. **Verify that the firmware update was copied.**

```
N1-ok> show firmware firmware
```

See "show firmware" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.

Example 3–21 To Copy an ALOM 1.5 Firmware Through the Command Line

The following example shows how to copy the ALOM 1.5 firmware images. There are two separate firmware images, but both can be associated with the ALOM `type` attribute value.

```
N1-ok> create firmware alom-boot type ALOM model SF-V240 vendor
SUN url file:///var/tmp/alombootfw
N1-ok> create firmware alom-main type ALOM model SF-V240 vendor SUN
url file:///var/tmp/alommainfw
N1-ok> show firmware
Name                        Type   Vendor      Version     Compatible Model
alom-boot                   ALOM   SUN                     SF-V240
alom-main                   ALOM   SUN                     SF-V240
```

See Also

- "To Load a Firmware Update on a Server or a Server Group" on page 108

▼ To Load a Firmware Update on a Server or a Server Group

This procedure describes how to load a firmware update by using the browser interface. The examples that follow the procedure provide command-line equivalents.

Before You Begin

- Consult your hardware documentation for instructions and information on upgrading your server firmware. See the Sun System Handbook documentation or the documentation that came with your server.
- The firmware update must be copied to the N1 System Manager. See "To Copy a Firmware Update" on page 106 for details.
- Power off the provisionable server by using the browser interface or the command line before loading a firmware update on it. Sun Fire V20z, Sun Fire V40z, or ALOM(1.5)–based servers can remain powered on during firmware SP updates. The `stop server` command performs a graceful shutdown of the OS on the server, followed by a power off. The base management and OS monitoring features must be added to the server to perform this step. See "Adding and Upgrading Base Management and OS Monitoring Features" on page 157. Otherwise, you can force

a power off using the `stop server` *server* `force` command or the `stop group` *group* `force` command.

- Disable monitoring for the provisionable server. This action is required only if you want to avoid the fault notifications as you shut down the OS on the server to complete the firmware installation. See "To Disable Monitoring for a Server or a Server Group" on page 173 for details.

Note – Firmware version 2.2 and above for the Sun Fire V20z servers do not support the PIC firmware upgrade. The upgrade of PIC firmware will fail, and the job step will show an error message similar to the following: "This operation is not supported on *server*. Refer to the log file for more information."

Steps

1. **Log in to the N1 System Manager.**
   See "To Access the N1 System Manager Browser Interface" on page 29 for details.
2. **Choose All Servers from the View Selector menu.**
   The Servers table appears.
3. **Select the server or servers that you want to update.**
   A check mark appears.
4. **Choose Load Firmware from the Actions menu.**
   The Load Firmware dialog box appears
5. **Select the appropriate firmware from the Firmware menu.**
6. **To apply the firmware update to the listed target servers, click OK.**
   The dialog box closes.
7. **Click the Jobs tab.**
   A Load Firmware job appears in the Jobs table.
8. **Click the job ID.**
   The Job Details page appears. Job steps indicate progress and results. Review the information in the Results section of the Job Details page to determine which servers were successfully updated.

   Note – After successful completion, the firmware version number is updated with the actual version number that is reported by the hardware. If the reported version number does not match the original version number, a warning is logged.

   ---

9. **Verify that the installation was successful.**

```
N1-ok> show server server
```

Example 3–22 Loading Firmware on a Server Through the Command Line

The following example command shows you how to stop a server in preparation for installing a firmware update.

```
N1-ok> stop server server
```

The following example command shows you how to install a firmware update on a server by using the `load` command.

```
N1-ok> load server server1,server2 firmware v20z-bios.sp force true
```

See "load server" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.

By default, the firmware update's model and vendor settings must match every provisionable server that you select for installation; otherwise, the update fails. You can specify the `force` option to bypass this check. However, installing a noncompatible firmware update on a server might render the server unusable.

Example 3–23 Loading Firmware on a Server Group Through the Command Line

The following example command shows you how to stop a server group in preparation for installing a firmware update.

```
N1-ok> stop group group
```

The following example command shows you how to install a firmware update on a server group by using the `load` command.

```
N1-ok> load group devgroup firmware bios.sp
```

See "load group" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.

▼ To List the Available Firmware Updates

This procedure describes how to list the available firmware updates by using the browser interface. The example that follow the procedure provides the command-line equivalent.

Steps

1. **Log in to the N1 System Manager.**
   See "To Access the N1 System Manager Browser Interface" on page 29 for details.
2. **Click the System Dashboard tab.**
   The Shortcuts pane appears.
3. **Click the Expand/Collapse icon on the Firmware title bar.**
   The Firmware list expands.

4. **Click the Edit List button.**
   The Edit List dialog box appears with the available firmware list.

Example 3–24 Listing the Available Firmware Updates Through the Command Line

```
N1-ok> show firmware all
```

▼ To List the Firmware Updates Installed on a Provisionable Server

---

Tip – You can also use the browser interface Server Details page to view all of the firmware updates that are installed on a server.

Steps

1. **Log in to the N1 System Manager.**
   See "To Access the N1 System Manager Command Line" on page 28 for details.
2. **List the firmware updates that are installed on a provisionable server.**

   ```
   N1-ok> show server server
   ```

   See "show server" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.

Example 3–25 Listing the Firmware for an ALOM Server

The following example shows how to view all of the firmware for an ALOM enabled server. You must log into the service processor before running this command.

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

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

SC Build Release: 02
SC firmware checksum: 6FFB200D

SC firmware built Jan  6 2005, 17:05:12
SC firmware flashupdate MAY 25 2005, 01:33:55

SC System Memory Size: 8 MB
```

```
SC NVRAM Version = b

SC hardware type: 0
```

▼ To Modify Firmware Update Information

This procedure describes how to modify the information about a firmware update.

Steps

1. **Log in to the N1 System Manager.**

   See "To Access the N1 System Manager Command Line" on page 28 for details.

2. **Modify the name or description of a firmware update.**

   N1-ok> **set firmware** *firmware* [**description** *description*]
   [**name** *name*] [**model=***model*]
   [**vendor=***vendor*] [**version=***version*]

   See "set firmware" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.

▼ To Delete a Firmware Update

This procedure describes how to delete a firmware update from the N1 System Manager. This procedure does not delete a firmware update from a provisionable server.

Note – After you install a firmware update on a provisionable server, you cannot uninstall it.

Steps

1. **Log in to the N1 System Manager.**

   See "To Access the N1 System Manager Command Line" on page 28 for details.

2. **Delete a firmware update from the N1 System Manager.**

   N1-ok> **delete firmware** *firmware*

   See "delete firmware" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.

CHAPTER 4

Managing Servers and Server Groups

This chapter provides conceptual and procedural information about N1 System Manager server management and server group management.

The N1 System Manager enables you to perform the server maintenance tasks described in the following sections:

Introduction to Server and Group Management

The N1 System Manager enables you to manage hundreds of heterogeneous servers by using one interface. The `N1-ok` shell provides a simple command set with which to identify, manage, provision, and reprovision servers.

You can use the `discover` command to initiate the management of provisionable servers. The server discovery process creates a Discovery job in the N1 System Manager. The Discovery job uses the management IP address and default security credentials to identify each physical server. You can view the job results to track the discovery process.

After successful completion of the Discovery job, a server is identified by its *management name*. The server's management name is initially set to the server's management IP address. You can rename discovered servers at any time.

You can create groups of discovered, or *provisionable*, servers according to the make and model for aggregate installation of firmware updates. Then, you can create functional groups for the aggregate installation of operating systems, or *OS profiles*, and OS updates. Provisionable servers can belong to more than one server group, so you can create new server groups for aggregate maintenance tasks.

The sections in this chapter describe the prerequisites and instructions for performing server and server group maintenance tasks. You will use the View Selector menu, the Actions menu, and server name links to perform the operations that are described in these sections.

The following graphic shows the View Selector menu, the Actions menu, and the server name links.

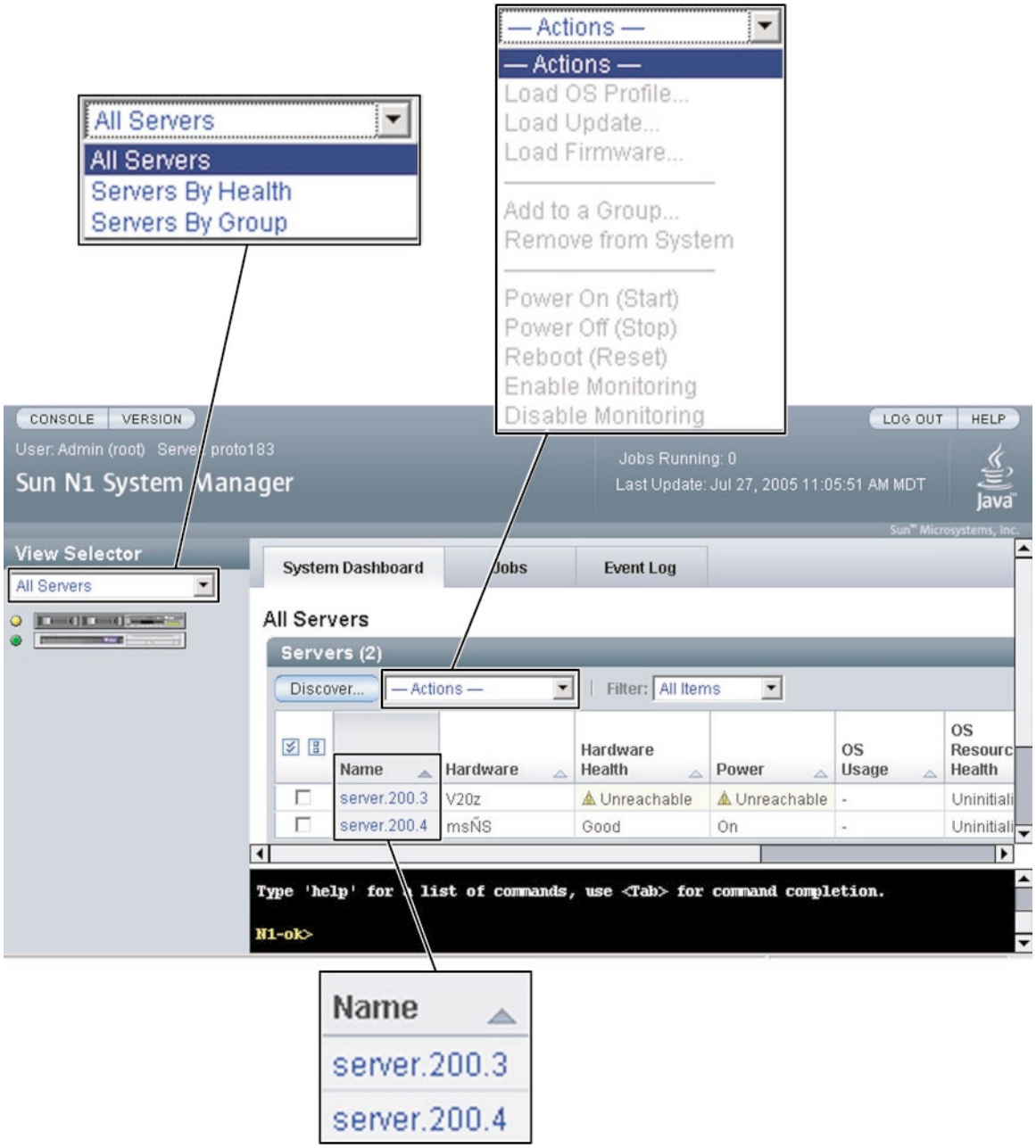


FIGURE 4–1 Menus and Links in the Browser Interface

Identifying Servers and Server States

This section describes the information that the N1 System Manager reports for each server when you issue the `show server` command with the `all` keyword, or the `show group` command.

- **Name** – The server or server group name. Server name is initially set to the management IP address. For instructions on how to change this name, see "Modifying Server and Server Group Information" on page 123.
- **Hardware** – Describes the type of managed server. See the Sun System Handbook documentation for your provisionable server.
- **Hardware Health** – The status for attributes such as memory, processor information, and Network Interface Card (NIC) information.
- **Power** – Power status for the physical server.
- **OS Usage** – If an OS profile is loaded, the OS name appears here.
- **OS Resource Health** – If an OS profile is loaded, the OS state appears here if monitoring is enabled.
- **Jobs** – If a job is in progress or has completed on the server, the job ID appears here.

Server Power States

Server power is indicated by the following states:

- **On** – The server is powered on and running.
- **Standby** – The server is powered off but still responsive to commands, for example, `start`.
- **Unknown** – The server is not returning any power status information.
- **Unreachable** – The server cannot be contacted for power status information.

Hardware Health States

Server hardware health is indicated by the following states:

- **Good** – The server hardware is working properly.
- **Unreachable** – The server cannot be contacted for information about the status of hardware health. This state is most often caused by a network problem.
- **Warning Failure** – A potential or impending fault condition has been detected on the server. Take action to prevent the problem from becoming more serious. See "Monitoring Threshold Values" on page 174 for information about viewing and tuning hardware sensor threshold values.
- **Critical Failure** – A fault condition has occurred on the server. Corrective action is required.

- **Nonrecoverable Failure** – The server has completely failed. Recovery is not possible.
- **Unknown** – The server is not returning any hardware health status.
- **Offline** – The server is not managed.

Supported Server Actions

The following aggregate server actions are supported:

- Starting, stopping, and resetting server power.
- Listing and refreshing server data.
- Loading servers with OS profiles, updates, and firmware. See Chapter 3.
- Enabling and disabling server monitoring. See Chapter 5.
- Adding servers to server groups. See"Creating and Maintaining Server Groups" on page 58.
- Removing servers from the N1 System Manager.

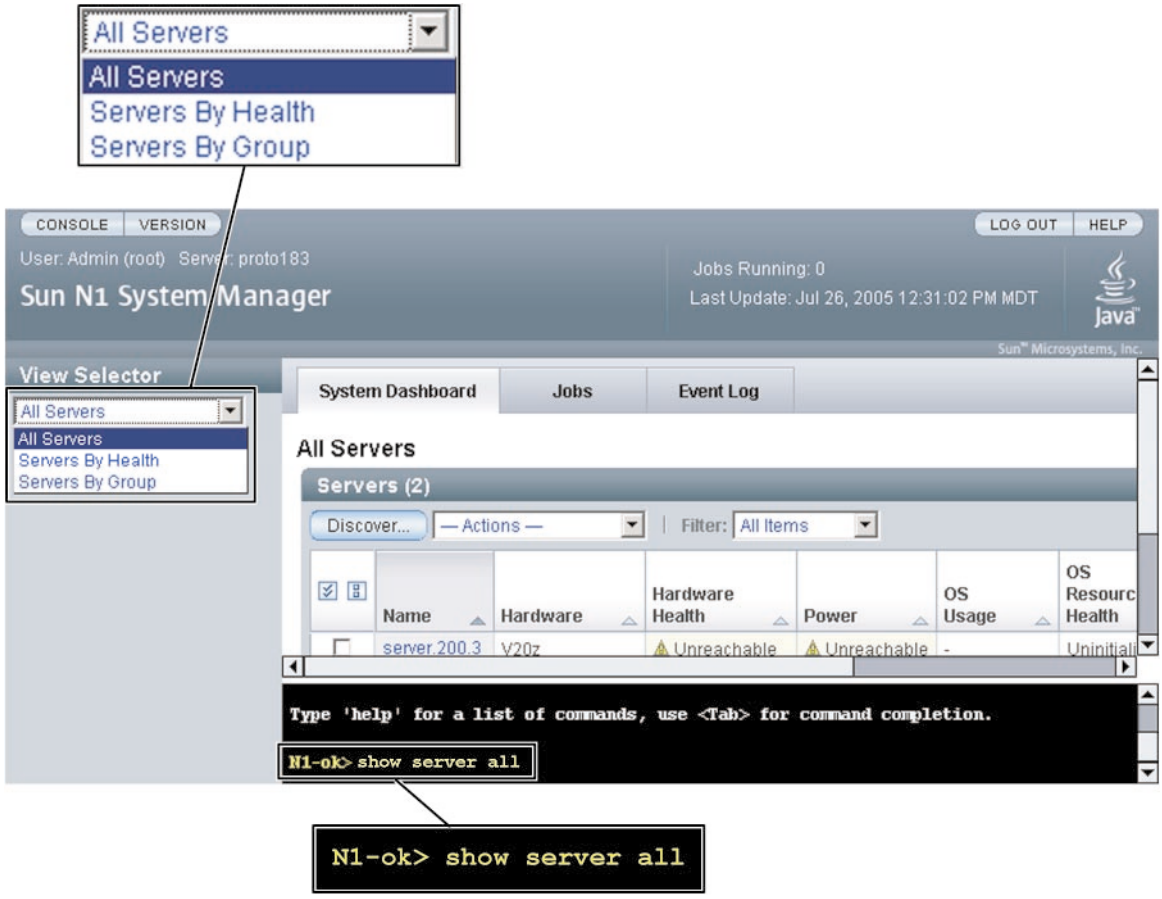
Listing and Viewing Servers and Server Groups

This section describes the following tasks:

Listing Servers and Server Groups

To list servers, use the View Selector menu. Alternatively, use the `show` command with the `server` keyword and the `all` subcommand to list all servers in the N1 System Manager.

As the following graphic shows, you can use the View Selector menu or the `show server` command to list servers.



▼ To List Servers and Server Groups

This procedure describes how to list servers and server groups by using the browser interface. The example that follows the procedure provides a command-line equivalent.

Steps

1. **Log in to the N1 System Manager.**
   See "To Access the N1 System Manager Browser Interface" on page 29 for details.

2. **Navigate to the table that contains the server or the server group by performing one of the following actions:**

   - **Choose All Servers from the View Selector menu.**
     The Servers table appears.

- **Choose Servers By Group from the View Selector menu.**
  The Server Groups table appears.

Example 4–1 Listing Servers Through the Command Line

The following example shows how to view all servers in the system by using the `show` command.

```
N1-ok> show server all
```

A list of all servers in the system appears. See "show server" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.

Example 4–2 Filtering Servers Through the Command Line Based on IP Address

The following example shows how to filter a list of provisionable servers in the system based on the server's management network IP address by using the `show` command:

```
N1-ok> show server ip 192.168.200.4
```

The following example shows how to filter a list of provisionable servers in the system based on a range of management network IP addresses:

```
N1-ok> show server ip 192.168.200.4-192.168.200.60
```

The following example shows how to filter a list of provisionable servers in the system based on subnet and mask length. In this case the subnet is `10.0.8` and the mask length is `24`:

```
N1-ok> show server ip 10.0.8/24
```

Example 4–3 Filtering Servers Through the Command Line Based on Job Count

The following example shows how to filter a list of provisionable servers in the system based on job count. In this case the job count is `0`:

```
N1-ok> show server jobcount 0
```

Example 4–4 Filtering Servers Through the Command Line Based on Model

The following example shows how to filter a list of provisionable servers in the system based on the server model. In this case the server model is Sun Fire v240 machines:

```
N1-ok> show server model SF-V240
```

Example 4–5 Filtering Servers Through the Command Line Based on Name

The following example shows how to filter a list of provisionable servers in the system based on the server name. In this case the server name is `server3`:

```
N1-ok> show server name server3
```

The following example shows how to filter a list of provisionable servers in the system based on the server name. In this case the server name is `s 3`:

```
N1-ok> show server name "s 3"
```

Example 4–6 Filtering Servers Through the Command Line Based on Running OS

The following example shows how to filter a list of provisionable servers in the system based on the OS that is running on the server. In this case an implicit, case-sensitive wildcard is used for SUSE Linux:

```
N1-ok> show server runningos SLES
```

Example 4–7 Filtering Servers Through the Command Line Based on OS Health

The following example shows how to filter a list of provisionable servers in the system based on the health of the OS that is running on the server. In this case, all servers that have OS health monitored are listed:

```
N1-ok> show server oshealth monitored
```

The following example shows how to filter a list of provisionable servers in the system based on the health of the OS that is running on the server. In this case, all servers that do not have OS health monitored are listed:

```
N1-ok> show server oshealth unmonitored
```

The following example shows how to filter a list of provisionable servers in the system based on the health of the OS that is running on the server. In this case, all servers that are sending no OS health information because the OS monitoring feature has not been added, are listed:

```
N1-ok> show server oshealth uninitialized
```

For information on adding the OS monitoring feature, see "Supporting Monitoring" on page 156.

Example 4–8 Listing Groups Through the Command Line

```
N1-ok> show group all
```

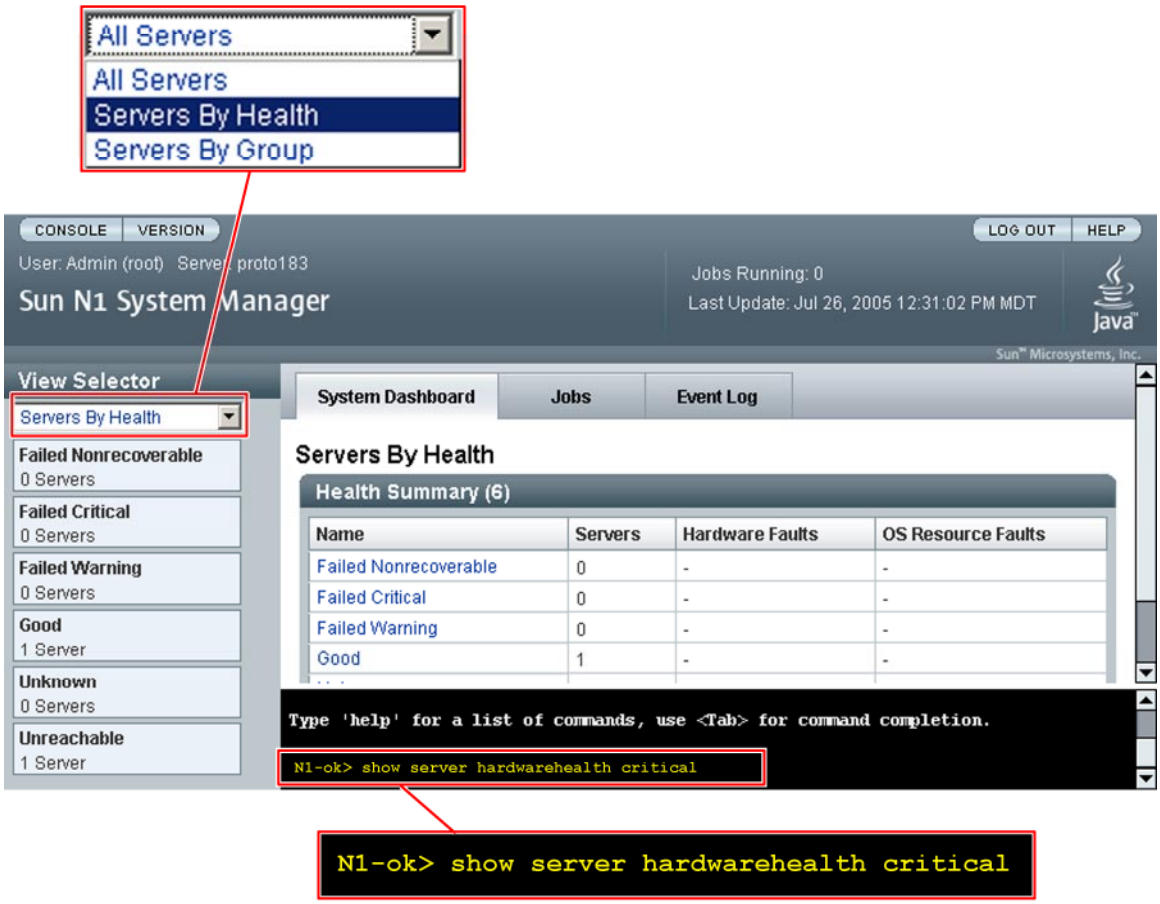
A list of all server groups in the system appears. See "show group" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.

▼ To View Failed Servers

This procedure describes how to view failed servers using the browser interface. The example following the procedure provides a command-line equivalent.

The following graphic shows how to use the View Selector menu to list servers by heath state. Alternatively, use the `hardwarehealth` or `oshealth` subcommands and an appropriate health state to filter the list of servers by health state. For example:

```
N1-ok> show server hardwarehealth nonrecoverable
```



Steps

1. **Log in to the N1 System Manager.**
   See "To Access the N1 System Manager Browser Interface" on page 29 for details.

2. **Choose Servers By Health from the View Selector menu.**
   The Health Summary table appears.

   Note – You cannot perform any actions on servers from the Health Summary table.

   ---

3. **Select the fault state that you want to view.**
   The available fault states are:

   - Failed Nonrecoverable

- Failed Critical
- Failed Warning
- Unreachable
- Unknown

The list of servers in the selected state appears. See "Hardware Health States" on page 116 for a description of fault states.

Example 4–9 Viewing Failed Critical Servers Through the Command Line

The following example shows how to view servers that have a health status of `critical`.

```
N1-ok> show server hardwarehealth critical
Name            Hardware    Hardware Health   Power   OS Usage            OS Resource Health
10.0.0.26       V20z        Failed Critical   On      Solaris             Unknown
```

See Also For descriptions of the icons and various failure levels that are shown on the Servers By Health page, see "Hardware Health States" on page 116. For descriptions of monitoring thresholds, see "Monitoring Threshold Values" on page 174.

Viewing Server Details and Group Members

To view detailed server information and group members, use the `show` command with the `server` or `group` keyword. For syntax and parameter details, type `help show server` or `help show group` at the `N1-ok` command line. Server information is also provided on the Server Details page in the browser interface.

▼ To View Server Details and Server Group Members

This procedure describes how to view server details and server group members by using the browser interface. The example that follows the procedure provides a command-line equivalent.

Steps

1. **Log in to the N1 System Manager.**
   See "To Access the N1 System Manager Browser Interface" on page 29 for details.
2. **Navigate to the table that contains the server or the server group by performing one of the following actions:**
   - **Choose All Servers from the View Selector menu.**
     The Servers table appears.
   - **Choose Servers By Group from the View Selector menu.**
     The Server Groups table appears.

3. **Select the server or the server group that you want to view.**

   The Server Details page or the Servers By Group page appears.

Example 4–10 Viewing Server Details Through the Command Line

The following example shows how to view the server details by using the `show` command.

```
N1-ok> show server server1
```

Detailed server information appears. See "show server" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.

Example 4–11 Viewing Server Group Members Through the Command Line

The following example shows how to view the list of servers in a server group by using the `show` command.

```
N1-ok> show group devgroup
```

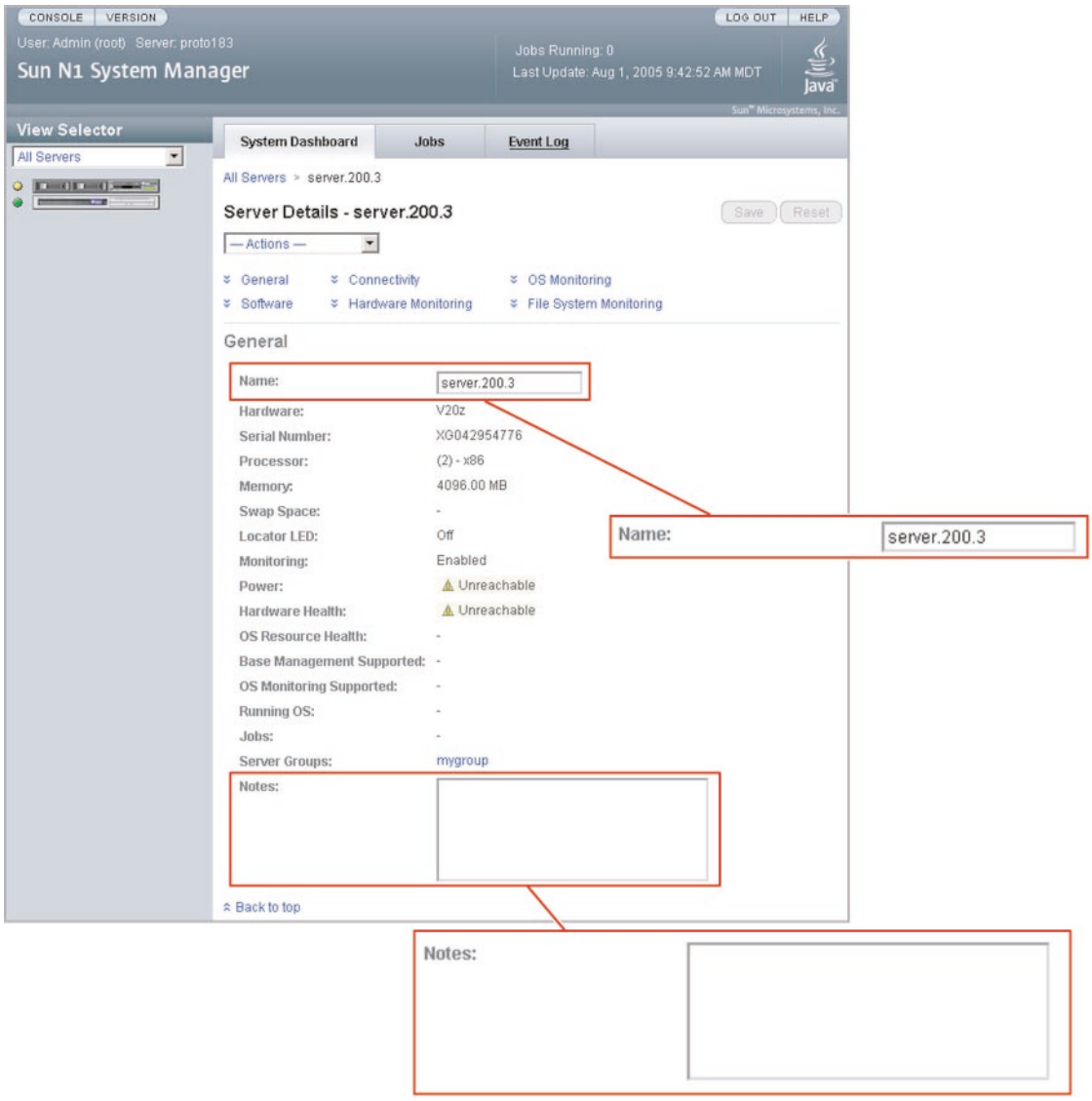
The list of servers in the group appears. See "show group" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.

Modifying Server and Server Group Information

This section describes the following tasks:

- "To Rename a Server or a Server Group" on page 125
- "To Add a Server Note" on page 126

The following graphic illustrates how to rename servers and server groups by using the Server Details page. Alternatively, use the `set` command with the `server` or `group` keyword and the `name` subcommand. For syntax and parameter details, type `help set server` or `help set group` at the `N1-ok` command line.



Renaming a Server or a Server Group

Servers are identified by the management IP address that is specified during discovery. This name is also referred to as the *management name* in documentation. You might want to rename a server with the DNS host name or track the host name by adding it to the server notes. Server and server group names must be unique and may include letters A through Z, digits 0 through 9, hyphens, and underscore characters.

▼ To Rename a Server or a Server Group

This procedure describes how to rename a server or a server group by using the browser interface. The example that follows the procedure provides a command-line equivalent.

Steps

1. **Log in to the N1 System Manager.**
   See "To Access the N1 System Manager Browser Interface" on page 29 for details.
2. **Choose All Servers from the View Selector menu.**
   The Servers table appears.
3. **Select the server name that you want to change.**
   The Server Details page appears.
4. **Type the new name into the Name entry field.**
   Server names must be unique and may include letters A through Z, digits 0 through 9, hyphens, and underscores.

   The Save button on the right side of the page is enabled.
5. **Click the Save button to apply the new name.**
   The Servers table appears with the renamed server.

Example 4–12 Renaming a Server Through the Command Line

The following example shows how to change a server name by using the `set` command.

```
N1-ok> set server 192.168.12.1 name=svr4rck7
```

The server name is changed to `svr4rck7`. See "set server" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.

Example 4–13 Renaming a Group Through the Command Line

The following example shows how to change a server group name by using the `set` command.

```
N1-ok> set group devgroup name=labgroup
```

The group name is changed to `labgroup`. See "set group" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.

Adding a Server Note

Consider saving the following types of data as a server note:

- Physical location such as rack, slot, building, and geographic region

- DNS host name
- Provisioning parameters and the network configuration information that is set for the OS profile installation
- Internal asset tracking identifiers

To add server notes, use the `set` command with the `server` keyword and the `note` subcommand. For syntax and parameter details, type `help set server` at the `N1-ok` command line or refer to "set server" in *Sun N1 System Manager 1.2 Command Line Reference Manual*.

▼ To Add a Server Note

This procedure describes how to add a server note by using the browser interface. The example that follows the procedure provides a command-line equivalent.

Steps

1. **Log in to the N1 System Manager.**
   See "To Access the N1 System Manager Browser Interface" on page 29 for details.
2. **Choose All Servers from the View Selector menu.**
   The Servers table appears.
3. **Select the name of the server.**
   The Server Details page appears.
4. **Scroll down to the Notes entry field.**
   The Notes entry field appears at the bottom of the General section.
5. **Type new data into the Notes field.**
   The Save button is enabled.
6. **To apply your changes, click the Save button.**
   The new data is saved.

Example 4–14 Adding a Server Note Through the Command Line

The following example shows how to view any existing notes by using the `show` command.

```
N1-ok> show server server1
```

The output shows any existing notes.

The following example shows how to add a server note by using the `set` command.

```
N1-ok> set server server1 note="loaded with S10"
```

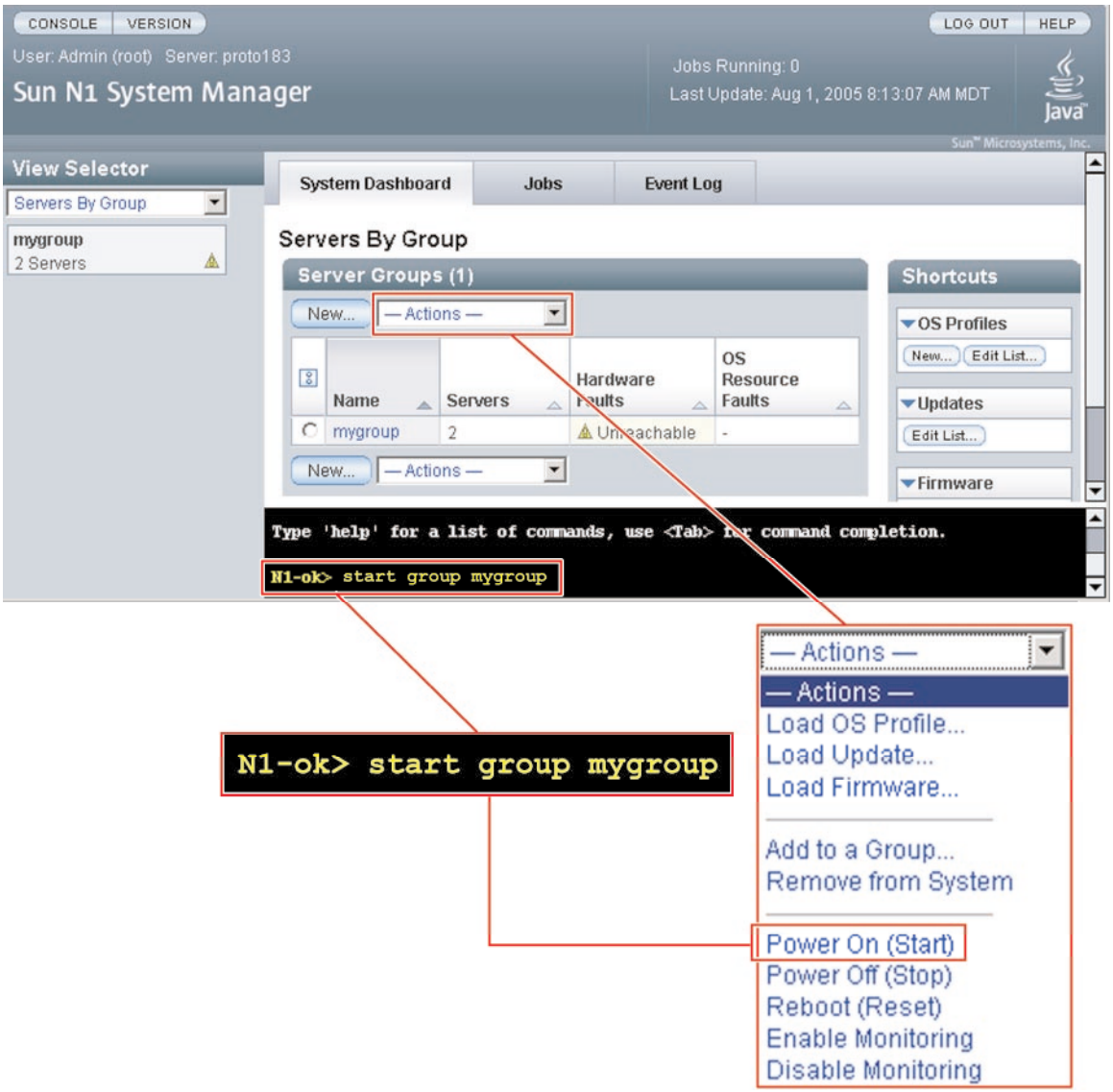
The note is added to the server information. See "set server" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.

Starting, Stopping, and Resetting Servers and Server Groups

This section describes the following activities:

Starting Servers and Server Groups

Use the `start` command with the `server` or `group` keyword to power on a server or a server group. If boot PROMS are configured, the servers boot. You may also use the Actions menu on the Servers By Group page to initiate the start operation. The Actions menu is shown in the following graphic.



For syntax and parameter details, type `help start server` or `help start group` at the `N1-ok` command line.

▼ To Power On and Boot a Server or a Server Group

Steps

1. **Log in to the N1 System Manager.**
   See "To Access the N1 System Manager Command Line" on page 28 for details.
2. **Type one of the following commands:**

   ```
   N1-ok> start server server
   ```

   The server is powered on and, if boot PROMs are configured, the server boots. See "start server" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for syntax details.

   ```
   N1-ok> start group group
   ```

   The server group is powered on and, if boot PROMs are configured, the servers in the group boot. Job completion takes longer for large server groups. See "start group" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for syntax details.

Example 4–15 Starting a Server From the Network

The following command-line example shows how to boot a server from the network.

```
N1-ok> start server 10.5.7.2 netboot=true
```

Example 4–16 Starting a Server Group From the Network

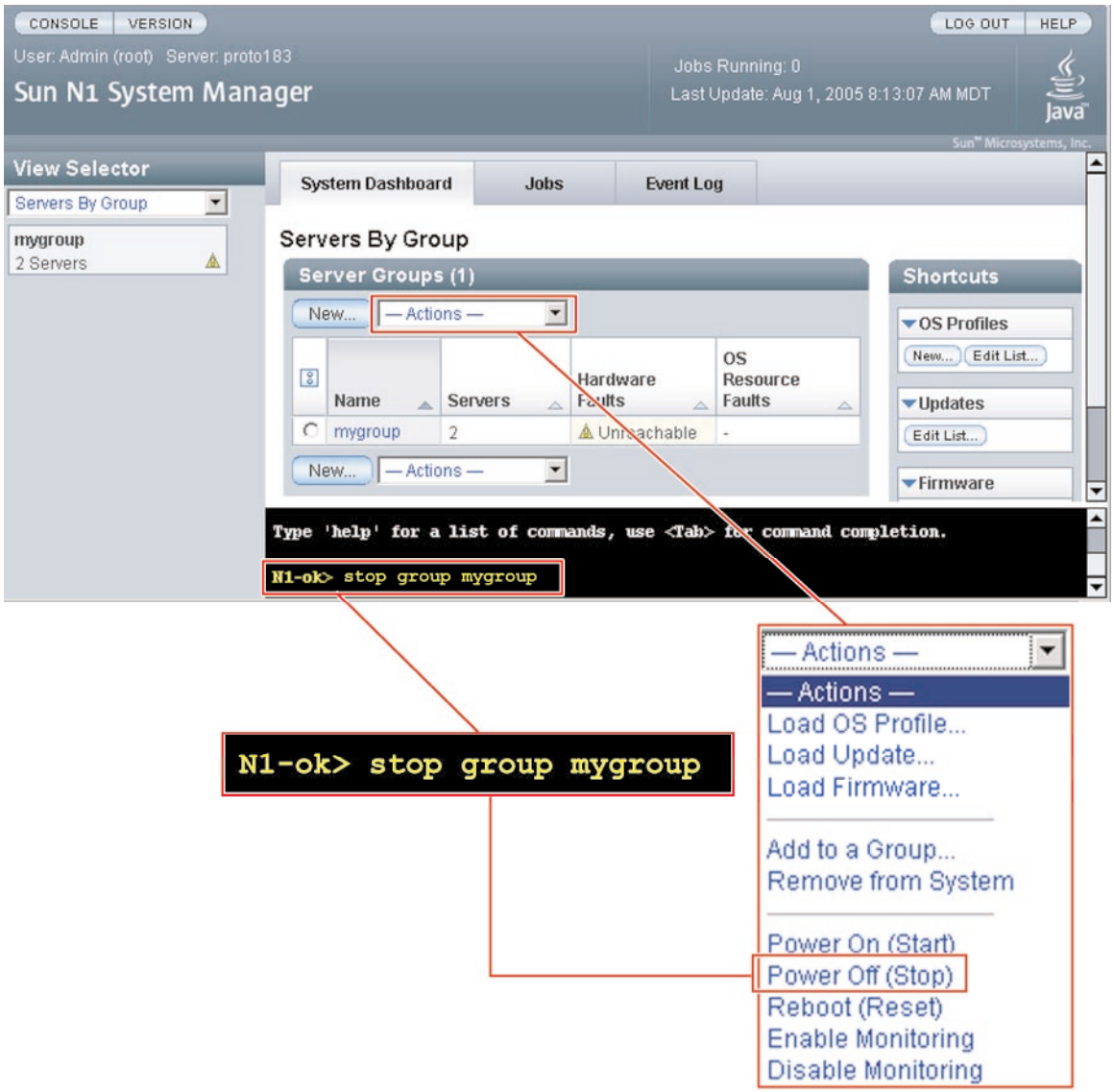
The following command-line example shows how to boot a server group from the network.

```
N1-ok> start group dev netboot=true
```

Stopping Servers and Server Groups

To shut down and power off a server or group, use the `stop` command with the `server` or `group` keyword. Stopping a server or server group will initiate graceful shutdown of the operating systems and subsequent power off of the physical servers. If servers do not have an OS installed or do not shutdown, you can use the `force` subcommand to power off the server group.

The following graphic shows how to stop a group by using the Actions menu on the Servers By Group page, or by issuing the `stop group` command.



For syntax and parameter details, type `help stop server` or `help stop group` at the `N1-ok` command line.

▼ To Shut Down and Power Off a Server or a Server Group

Steps

1. **Log in to the N1 System Manager.**

   See "To Access the N1 System Manager Command Line" on page 28 for details.

2. **Type one of the following commands:**

   ```
   N1-ok> stop server server
   ```

   The server is stopped. See "stop server" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for syntax details.

   ```
   N1-ok> stop group group
   ```

   The server group is stopped. See "stop group" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for syntax details.

Example 4–17 Forcing Power Off of a Server

The following command-line example shows how to force shutdown of the OS.

```
N1-ok> stop server 10.0.7.2
This operation is not supported. Please use the force option.
N1-ok> stop server 10.0.7.2 force=true
Server 10.0.7.2 powered off.
```

Example 4–18 Forcing Power Off of a Server Group

The following command-line example shows how to force shutdown of the OS for a server group.

```
N1-ok> stop group dev
This operation is not supported. Please use the force option.
N1-ok> stop group dev force=true
Group dev powered off.
```

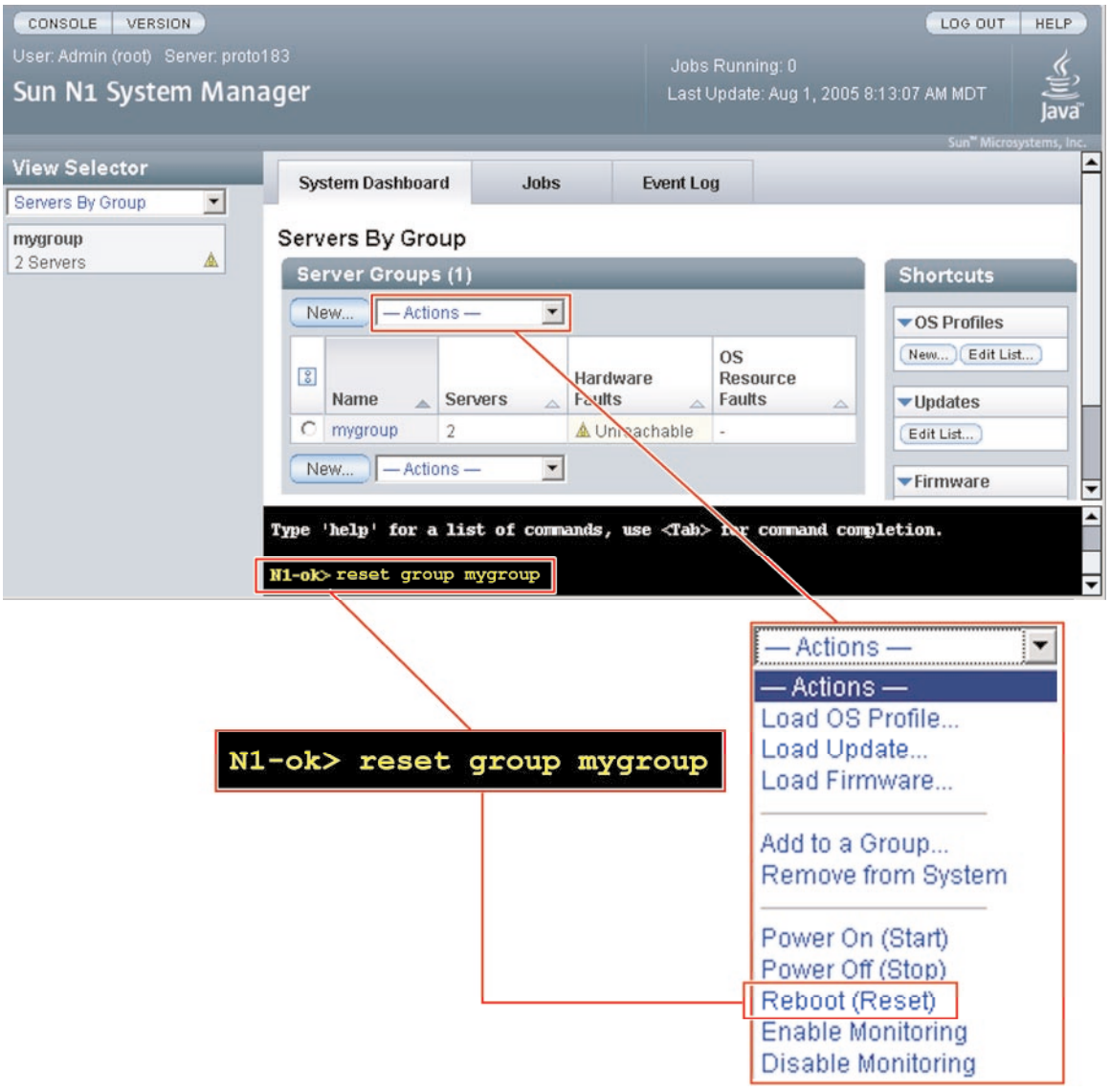
Troubleshooting If you use the `force` option, run one of the following file system check commands on the client via the console that you access from the service processor, when the server reboots.

- For the Solaris OS, run `fsck`
- For Linux, run `reiserfsck` or `e2fsck`

To find out how to run the `fsck` command on a provisioned server, see "Issuing Remote Commands on Servers and Server Groups" on page 134.

Resetting Servers and Server Groups

To initiate graceful shutdown of the operating system followed by power off of the physical server or server group, use the `reset` command with the `server` or `group` keyword. Then, the servers are powered on and, if boot PROMs are configured, the servers reboot. If servers do not have an OS installed or do not shutdown, you can use the `force` subcommand to reboot the server or server group.



For syntax and parameter details, type `help reset server` or `help reset group` at the `N1-ok` command line.

▼ To Reboot a Server or a Server Group

Steps

1. **Log in to the N1 System Manager.**
   See "To Access the N1 System Manager Command Line" on page 28 for details.
2. **Type one of the following commands:**

   ```
   N1-ok> reset server server [force=true]
   ```

   The server is rebooted. See "reset server" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.

   ```
   N1-ok> reset group group [force=true]
   ```

   The servers in the group reboot. See "reset group" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.

Example 4–19 Forcing Reset of a Server

The following command-line example shows how to force reset of the OS.

```
N1-ok> reset server 10.5.7.2 force=true
```

Example 4–20 Forcing Reset of a Server Group

If the OS does not gracefully shut down, use the following command-line example to force reset of the operating systems for the servers in the group.

```
N1-ok> reset group dev force=true
```

Example 4–21 Rebooting a Server From the Network

The following command-line example shows how to reboot a server from the network.

```
N1-ok> reset server 10.5.7.2 netboot=true
```

Example 4–22 Rebooting a Server Group from the Network

The following command-line example shows how to reboot a server group from the network.

```
N1-ok> reset group dev netboot=true
```

Troubleshooting If you use one of the above `force` commands, run one of the following file system check commands on the service processor when the server reboots.

- For the Solaris OS, run `fsck`
- For Linux, run `reiserfsck` or `e2fsck`

To find out how to run the `fsck` command on provisioned servers, see "Issuing Remote Commands on Servers and Server Groups" on page 134 for instructions.

Issuing Remote Commands on Servers and Server Groups

This section describes how to issue remote commands on servers and server groups.

To issue a remote command on a server or server group, use the `start` command with the `server` or `group` keyword and the `command` subcommand. For syntax and parameter details, type `help start server` or `help start group` at the `N1-ok` command line.

▼ To Issue Remote Commands on a Server or a Server Group

This procedure describes how to issue a remote command. A *remote command* is a UNIX command that is sent to a provisioned server to be run on that provisioned server.

Before You Begin

You must add the base management feature before you can issue remote commands on servers or server groups. See "Adding and Upgrading Base Management and OS Monitoring Features" on page 157.

Steps

1. **Log in to the N1 System Manager.**

   See "To Access the N1 System Manager Command Line" on page 28 for details.

2. **Type one of the following commands:**

   ```
   N1-ok> start server server command "command"
   ```

   The remote command is issued on the server. See "start server" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.

   ```
   N1-ok> start group group command "command"
   ```

   The remote command is issued on the group. See "start group" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.

3. **View the Remote Command job.**

```
N1-ok> show job job
```

The Remote Command output appears in the Results section.

Example 4–23 Issuing a Remote Command on a Server

The following command-line example shows how to issue a remote command on a server by using the `start` command.

```
N1-ok> start server hdco25 command "/bin/ls -l /"

Job "23" started.
```

The following command-line example shows how to view the results of the remote command by using the `show` command.

```
N1-ok> show job 23

Job ID:   23
Date:     2005-02-15T08:31:20-0700
Type:     Remote Command
Status:   Completed
Command:  start server hdco25 command "/bin/ls -l /"
Owner:    root
Errors:   0
Warnings: 0

Step 1:
Type:        103
Description: native procedure /bin/sh /opt/sun/n1gc/bin/remotecmd.sh
:[RCMD_KEY]
Start:       2005-02-15T08:31:22-0700
Completion:  2005-02-15T08:31:26-0700
Result:      Complete
Exception:   No Data Available

.
.
.

Result :
Server:          hdco25
Status:          0
Message:         Command executed successfully. Command: /bin/ls -l /
Standard Output: total 321
lrwxrwxrwx   1 root     root           9 Feb 11 13:21 bin -> ./usr/bin
drwxr-xr-x   4 root     sys          512 Feb 11 13:25 boot
drwxr-xr-x   3 root     sys          512 Feb 11 14:27 cr
drwxr-xr-x  15 root     sys         4096 Feb 11 14:09 dev
drwxr-xr-x   5 root     sys          512 Feb 11 14:06 devices
drwxr-xr-x  58 root     root        4096 Feb 14 12:36 etc
drwxr-xr-x   2 root     sys          512 Feb 11 13:46 export
dr-xr-xr-x   1 root     root           1 Feb 11 14:11 home
```

```
drwxr-xr-x  12 root     sys          512 Feb 11 13:25 kernel
lrwxrwxrwx   1 root     root           9 Feb 11 13:21 lib -> ./usr/lib
```

Example 4–24 Issuing a Remote Command With a Timeout

Timeouts are measured in seconds. The default timeout is two hours. If you want to turn the timeout off, type a value of zero into the command. The following example shows how to issue a remote command with a timeout that is set to 20 seconds.

```
N1-ok> start server hdco25 command "/root/sleep.sh 60" timeout 20

Job "10" started.
```

The following command-line example shows how to view the results of the remote command by using the `show` command.

```
N1-ok> show job 10

Job ID:   10
Date:     2005-02-15T16:46:45-0700
Type:     Remote Command
Status:   Completed
Command:  start server hdco25 command "/root/sleep.sh 60" timeout 20
Owner:    root
Errors:   0
Warnings: 0

Step 1:
Type:        103
Description: native procedure /bin/sh /opt/sun/n1gc/bin/remotecmd.sh
:[RCMD_KEY]
Start:       2005-02-15T16:46:48-0700
Completion:  2005-02-15T16:47:10-0700
Result:      Complete
Exception:   No Data Available
.
.
.
Result:
Server:          hdco25
Status:          -2
Message:         Command running on hdco25 did not finish within the
specified time limit of 20 seconds. Command: /root/sleep.sh 60
Standard Output: Sleeping for 60 seconds...
```

Example 4–25 Issuing a Remote Command on a Server Group

The following command-line example shows how to issue a remote command on a server group by using the `start` command.

```
N1-ok> start group g1 command "/bin/ls -l /"

Job "24" started.
```

The following command-line example shows how view the results of the remote command by using the `show` command.

```
N1-ok> show job 24

Job ID:   24
Date:     2005-02-15T08:31:20-0700
Type:     Remote Command
Status:   Completed
Command:     start group g1 command "/bin/ls -l /"
Owner:    root
Errors:   0
Warnings: 0

Step 1:
Type:        103
Description: native procedure /bin/sh /opt/sun/n1gc/bin/remotecmd.sh
:[RCMD_KEY]
Start:       2005-02-15T08:31:22-0700
Completion:  2005-02-15T08:31:26-0700
Result:      Complete
Exception:   No Data Available

.
.
.

Result :
Server:          server1
Status:          0
Message:         Command executed successfully. Command: /bin/ls -l /
Standard Output: total 321
lrwxrwxrwx   1 root     root           9 Feb 11 13:21 bin -> ./usr/bin
drwxr-xr-x   4 root     sys          512 Feb 11 13:25 boot
drwxr-xr-x   3 root     sys          512 Feb 11 14:27 cr
drwxr-xr-x  15 root     sys         4096 Feb 11 14:09 dev
drwxr-xr-x   5 root     sys          512 Feb 11 14:06 devices
drwxr-xr-x  58 root     root        4096 Feb 14 12:36 etc
drwxr-xr-x   2 root     sys          512 Feb 11 13:46 export
dr-xr-xr-x   1 root     root           1 Feb 11 14:11 home
drwxr-xr-x  12 root     sys          512 Feb 11 13:25 kernel
lrwxrwxrwx   1 root     root           9 Feb 11 13:21 lib -> ./usr/lib
Server:          server2
Status:          0
Message:         Command executed successfully. Command: /bin/ls -l /
Standard Output: total 321
lrwxrwxrwx   1 root     root           9 Feb 11 13:21 bin -> ./usr/bin
drwxr-xr-x   4 root     sys          512 Feb 11 13:25 boot
drwxr-xr-x   3 root     sys          512 Feb 11 14:27 cr
drwxr-xr-x  15 root     sys         4096 Feb 11 14:09 dev
drwxr-xr-x   5 root     sys          512 Feb 11 14:06 devices
drwxr-xr-x  58 root     root        4096 Feb 14 12:36 etc
drwxr-xr-x   2 root     sys          512 Feb 11 13:46 export
dr-xr-xr-x   1 root     root           1 Feb 11 14:11 home
drwxr-xr-x  12 root     sys          512 Feb 11 13:25 kernel
lrwxrwxrwx   1 root     root           9 Feb 11 13:21 lib -> ./usr/lib
```

See Also Example 5–11

Connecting to the Serial Console for a Server

This section describes how to open the serial console for a server.

To remotely access the serial console for a server, use the `connect` command with the `server` keyword.

Note – The Command Line pane in the browser interface does not support this operation. You must use the `n1sh` shell to access the `connect` command.

You can also perform this operation from the browser interface's Server Details page.

▼ To Open a Server's Serial Console

This procedure describes how to remotely access the serial console of provisionable servers. This feature is particularly useful for performing diagnosis before and during the OS installation and during the server power cycle.

Caution – 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.

For most hardware platforms, the first user to log in is given read-and-write privileges on the serial console. Subsequent user sessions are in read-only mode. Sun Fire X4100 and X4200 servers do not support read-only mode, so subsequent user session requests fail.

Note – Use of the serial console is not supported for Sun Fire X2100 servers.

When the escape sequence is issued, the connection closes and a `disconnect from server-name` message appears in the output. If another user has the console and you are in read-only mode, you are logged in to the console when the other user disconnects. When you click the Close button on the Serial Console window, the connection is closed.

The following list shows the supported serial console escape sequences:

- ALOM – `#.`
- Sun Enterprise X4100, X4200 – `ESC (`
- Sun Fire V20z and V40z – `^Ec.`

For HTTP connections, standard 128–bit SSL encryption is used for transport, authentication is password based, and a security session is used for each subsequent operation.

Note – If another user is logged in to the serial console for the server, you are logged in with read-only privileges. If another user has logged in to the physical serial console on a SPARC server, you are logged in with read-only privileges. The *physical* serial console is separate from the one that is available from the ALOM port.

Before You Begin

To use the Serial Console feature from the browser interface, the Sun Java Plugin 1.4.2 or later must be installed on the system where you are running the browser.

Steps

1. **Choose All Servers from the View Selector menu.**
   The Servers table appears.
2. **Select the server for which you want to open a serial console.**
   The Server Details page appears.
3. **Choose Open Serial Console from the Actions menu.**

The management server redirects output of the provisionable server's serial console to the terminal emulator applet that is running in the browser interface.

The serial emulator appears and takes you either to the root prompt or a read-only prompt.

Note – If a server is powered off, the console still connects, but no output appears until the server is powered on.

Example 4–26 Connecting to the Serial Console Through the Command Line

When in serial console mode, the `n1sh` shell sends all user input to the remote serial console. The N1 System Manager neither blocks nor supplements the platform-specific exit-control sequence. Note that the `connect` command is not implemented in the browser interface's Command Line pane. The `connect` command may only be run from the `n1sh` shell.

This example shows how to connect to the serial console as a `root` user. However, any user role with the `ServerConsole` privilege may issue the `connect` command.

```
% ssh -l root server1.central:6789
password:

Copyright (c) 2005 Sun Microsystems, Inc. All rights reserved
Use is subject to license terms.

N1-ok> connect server server1
```

Troubleshooting If the Open Serial Console menu item does not appear, SSHv1 is not enabled. To enable SSHv1, use the `n1smconfig` utility. See "To Configure the N1 System Manager System" in *Sun N1 System Manager 1.2 Installation and Configuration Guide*.

See Also After you have opened the serial console, you can view the detailed output during an OS deployment or a power cycle. For instructions, see "Deploying OS Profiles" on page 88 and "To Reboot a Server or a Server Group" on page 133.

Refreshing and Finding Servers and Server Groups

This section describes the following tasks:

Refreshing Server and Server Group Data

To update server and server group data, use the `set` command with the `server` or `group` keyword and the `refresh` subcommand. This command updates the following data:

- Hardware health information including power status, memory, processor information and NIC information
- Firmware information
- OS resource usage, such as CPU and filesystem usage, if an OS is loaded and if OS monitoring is supported and enabled.
- OS update information if an OS update is loaded and if OS monitoring is supported and enabled.

▼ To Refresh Data for a Server or a Server Group

Steps

1. **Log in to the N1 System Manager.**
   See "To Access the N1 System Manager Command Line" on page 28 for details.
2. **Type one of the following commands:**

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

   The server data is updated. See "set server" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.

   ```
   N1-ok> set group group refresh
   ```

   The server group data is updated. See "set group" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.

Note – Refresh job completion will be longer for server groups.

Finding a Server in a Rack

To illuminate the server's LED locator light, use the `set` command with the `server` keyword and the `locator` subcommand. For syntax and parameter details, type `help set server` at the `N1-ok` command line.

▼ To Find a Server in a Rack

This procedure describes how to illuminate the LED locator light on a physical server.

Steps

1. **Log in to the N1 System Manager.**
   See "To Access the N1 System Manager Command Line" on page 28 for details.
2. **Type the following command:**

   ```
   N1-ok> set server server locator=true
   ```

   The LED locator light on the physical server illuminates. See "set server" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.

Deleting Servers and Server Groups

To remove a server or group from the N1 System Manager, use the `delete` command with the `server` or `group` keyword.

For syntax and parameter details, type `help delete server` or `help delete group` at the `N1-ok` command line.

▼ To Delete a Server or a Server Group

Steps

1. **Log in to the N1 System Manager.**
   See "To Access the N1 System Manager Command Line" on page 28 for details.
2. **Type one of the following commands:**

   ```
   N1-ok> delete server server
   ```

   The server is deleted from the N1 System Manager. See "delete server" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.

   ```
   N1-ok> delete group group
   ```

   The group is deleted from the N1 System Manager. This command will **not** remove servers from the N1 System Manager. See "delete group" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.

CHAPTER 5

Monitoring Your Servers

The first section of this chapter provides an explanation of what monitoring is, in the context of the N1 System Manager, and describes how to monitor servers that are part of the N1 System Manager. This chapter provides procedures for enabling and disabling monitoring, and for managing monitoring thresholds using the command line.

This chapter also contains information about managing jobs, event log entries, and about setting up notifications.

This chapter contains the following sections:

Some procedures are also possible using the browser interface. These procedures are provided in the Sun N1 System Manager browser interface help.

Introduction to Monitoring

Monitoring in the Sun N1 System Manager software enables you to track changes to specific *attributes* in specific managed objects. Managed objects include server hardware elements, operating systems, file systems, and networks. Attributes are the

monitored elements, about which data is obtained and delivered by the N1 System Manager software. Examples of attributes are the average number of queued processes and the percentage of used memory. A list of attributes is provided in "Hardware Sensor Attributes" on page 148 and in Table 5–2.

Attributes are associated with three main areas:

- Hardware health attributes. For information about hardware health monitoring, see "Hardware Health Monitoring" on page 147.
- OS resource attributes. For information about OS health monitoring, see "OS Health Monitoring" on page 153.
- Network connectivity, or *reachability*. For information about network reachability monitoring, see "Network Reachability Monitoring" on page 154.

For a server or a group of servers, hardware health and operating system health and network connectivity are all monitored by the management server. All comparisons and verifications for monitoring are performed by the N1 System Manager. Provisionable servers are used only to access data about their health or network reachability.

Monitoring is connected with the broadcasting of the *events* for each monitored server or group of servers. Events are generated when certain conditions related to attributes occur. For information about events and when they occur, see "Managing Event Log Entries" on page 191. Monitoring data is stored as events in the N1 System Manager database instead of log files.

If monitoring is enabled for a server, each event causes a notification to be emitted from the N1 System Manager for that event. If monitoring is disabled for a server, monitoring events are not generated for that server. Lifecycle events continue to be generated, even with monitoring disabled. *Lifecycle events* include server discovery, server change or deletion, or server group creation. If you have requested notification of this type of event, you can still receive notifications for that event, even with monitoring disabled.

An SNMP agent that is used for data retrieval is provided in the N1 System Manager software. If the management server is running the N1 System Manager on the Solaris OS, this agent is based on the Sun Management Center 3.5 software SNMP agent. If the management server is running the N1 System Manager on Linux, this agent is based on the Sun Management Center 3.6 Linux SNMP agent. The agent is deployed when operating systems are deployed on servers that are managed by the N1 System Manager software. The N1 System Manager passively listens for the traps generated by the SNMP agent whenever there is a threshold breach. In case the traps generated by the SNMP agent are lost, the N1 System Manager also performs to types of polling-based monitoring as a backup: accessibility monitoring and status monitoring. Accessibility monitoring makes sure that the N1 System Manager can access the OS agent. Status monitoring periodically retrieves the current status from the SNMP agent and reports if the status is not OK.

Note – The default SNMP port for the agent for the monitoring feature is port 161. Changing the port number from the default is not supported in this release.

Hardware Health Monitoring

The hardware health of discovered servers is monitored. Sensors provided in the hardware are used to monitor temperature, voltage, and fan speed. For more information about associated hardware, see the "Sun N1 System Manager Connection Information" in *Sun N1 System Manager 1.2 Site Preparation Guide*.

Sensor data is retrieved from the service processor for SPARC devices through the Advanced Lights Out Manager (ALOM) interface. Sensor data is retrieved from IPMI for x64 servers.

Note – Servers that use ALOM do not send data to the management server by use of traps. Instead, they send management data by email. To ensure that the management server collects data from these servers, configure the management server server as an email server. This process is explained in "To Configure the ALOM Email Alert Settings" in *Sun N1 System Manager 1.2 Installation and Configuration Guide*.

The following characteristics of server hardware can be monitored:

- CPU temperature
- Ambient temperature
- Fan speed in revolutions per minute
- Voltages
- LEDs (for Sun Fire X4100 and Sun Fire X4200 only)

A detailed list of these sensors is provided in "Hardware Sensor Attributes" on page 148.

You can view filtered hardware health monitoring information for all servers by using the `show server` command:

```
N1-ok> show server hardwarehealth hardwarehealth
```

See "show server" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details of possible values of the *hardwarehealth* filters. For more information and a graphic explaining filtering servers by health state, see "To View Failed Servers" on page 120.

Hardware Sensor Attributes

For x86 servers, the management server software obtains the list of hardware sensor attributes to monitor through IPMI from the service processor of the server. For servers running the SPARC architecture, the ALOM interface is used. The list of hardware sensor attributes can vary from server to server, and between firmware versions. A sample listing for some servers and firmware versions is provided in this section. The attributes depend on the server type and on the number of CPUs that the server has.

Note – Hardware disk failure and memory failure are not monitored in this version of the N1 System Manager.

The following example lists sensor names and descriptions for a Sun Fire V40z server with firmware version 2.1.0.16.

```
ambienttemp     Ambient air temp
bulk.v12-0-s0   Bulk 12V S0 voltage at CPU 0
bulk.v12-2-s0   Bulk 12V S0 voltage at CPU 2
bulk.v12-3-s0   Bulk 12V S0 voltage at CPU 3
bulk.v1_8-s0    Bulk 1.8V S0 voltage
bulk.v1_8-s5    Bulk 1.8V S5 voltage
bulk.v2_5-s0    Bulk 2.5V S0 voltage
bulk.v2_5-s0-dc Bulk 2.5V S0 voltage at DC
bulk.v2_5-s5    Bulk 2.5V S5 voltage
bulk.v3_3-s0    Bulk 3.3V S0 voltage
bulk.v3_3-s0-dc Bulk 3.3V S0 voltage at DC
bulk.v3_3-s3    Bulk 3.3V S3 voltage
bulk.v3_3-s5    Bulk 3.3V S5 voltage
bulk.v3_3-s5-dc Aux 3.3V S5 voltage at DC
bulk.v5-s0      Bulk 5V S0 voltage
bulk.v5-s0-dc   Bulk 5V S0 voltage at DC
bulk.v5-s5      Bulk 5V S5 voltage
bulk.v5-s5-dc   Bulk 5V S5 voltage at DC
cpu0.dietemp    CPU 0 Die temperature
cpu0.heartbeat  CPU 0 Heartbeat
cpu0.inlettemp  CPU 0 Inlet temperature
cpu0.memtemp    CPU 0 Memory temperature
cpu0.v2_5-s0    CPU 0 VDDA (2.5V) S0 voltage
cpu0.v2_5-s3    CPU 0 VDD (2.5V) S3 voltage
cpu0.vcore-s0   CPU 0 VCore S0 voltage
cpu0.vid        CPU 0 VID Selection
cpu0.vldt0      CPU 0 LDT0 voltage
cpu0.vtt-s3     CPU 0 DDR VTT S3 voltage
cpu1.dietemp    CPU 1 Die temperature
cpu1.heartbeat  CPU 1 Heartbeat
cpu1.inlettemp  CPU 1 Inlet temperature
cpu1.memtemp    CPU 1 Memory temperature
cpu1.v2_5-s0    CPU 1 VDDA (2.5V) S0 voltage
cpu1.v2_5-s3    CPU 1 VDD (2.5V) S3 voltage
cpu1.vcore-s0   CPU 1 VCore S0 voltage
```

```
cpu1.vid        CPU 1 VID Selection
cpu1.vldt1      CPU 1 LDT1 voltage
cpu1.vldt2      CPU 1 LDT2 voltage
cpu1.vtt-s3     CPU 1 DDR VTT S3 voltage
cpu2.dietemp    CPU 2 Die temperature
cpu2.heartbeat  CPU 2 Heartbeat
cpu2.inlettemp  CPU 2 inlet temperature
cpu2.temp       CPU 2 downwind temperature
cpu2.v2_5-s0    CPU 2 VDDA (2.5V) S0 voltage
cpu2.v2_5-s3    CPU 2 VDD (2.5V) S3 voltage
cpu2.vcore-s0   CPU 2 VCore S0 voltage
cpu2.vid        CPU-2 VID Selection
cpu2.vtt-s3     CPU 2 DDR VTT voltage
cpu3.dietemp    CPU 3 Die temperature
cpu3.heartbeat  CPU 3 Heartbeat
cpu3.inlettemp  CPU 3 inlet temperature
cpu3.temp       CPU 3 downwind temperature
cpu3.v2_5-s0    CPU 3 VDDA (2.5V) S0 voltage
cpu3.v2_5-s3    CPU 3 VDD (2.5V) S3 voltage
cpu3.vcore-s0   CPU 3 VCore S0 voltage
cpu3.vid        CPU-3 VID Selection
cpu3.vtt-s3     CPU 3 DDR VTT voltage
fan1.tach       Fan 1 measured speed
fan10.tach      Fan 10 measured speed
fan11.tach      Fan 11 measured speed
fan12.tach      Fan 12 measured speed
fan2.tach       Fan 2 measured speed
fan3.tach       Fan 3 measured speed
fan4.tach       Fan 4 measured speed
fan5.tach       Fan 5 measured speed
fan6.tach       Fan 6 measured speed
fan7.tach       Fan 7 measured speed
fan8.tach       Fan 8 measured speed
fan9.tach       Fan 9 measured speed
faultswitch     System Fault Indication
g0.vldt1        AMD-8131 PCI-X Tunnel 0 LDT1 voltage
g1.vldt1        AMD-8131 PCI-X Tunnel 1 LDT1 voltage
gbeth.temp      Gigabit ethernet local temperature
golem-v1_8-s0   AMD-8131 PCI-X Tunnel 1.8V S0 voltage
identifyswitch  Identify switch
scsibp.temp     SCSI Disk backplane temperature
scsifault       SCSI Disk Fault Switch
sp.temp         SP local temperature
vldt-reg1-dc    LDT Regulator 1 Voltage
vldt-reg2-dc    LDT Regulator 2 Voltage
```

The following example lists sensor names and descriptions for a Sun Fire V20z server with firmware version 2.1.0.16.

```
ambienttemp    Ambient air temp
bulk.v12-0-s0  Bulk 12v supply voltage (cpu0)
bulk.v12-1-s0  Bulk 12v supply voltage (cpu1)
bulk.v1_8-s0   Bulk 1.8v S0 voltage
bulk.v1_8-s5   Bulk 1.8v S5 voltage
bulk.v2_5-s0   Bulk 2.5v S0 voltage
```

```
bulk.v2_5-s5   Bulk 2.5v S5 voltage
bulk.v3_3-s0   Bulk 3.3v supply
bulk.v3_3-s3   Bulk 3.3v S3 voltage
bulk.v3_3-s5   Bulk 3.3v S5 voltage
bulk.v5-s0     Bulk 5v supply voltage
bulk.v5-s5     Bulk 5v S5 voltage
cpu0.dietemp   CPU 0 die temp
cpu0.heartbeat CPU 0 heartbeat
cpu0.memtemp   CPU 0 memory temp
cpu0.temp      CPU 0 low side temp
cpu0.v2_5-s0   CPU VDDA voltage
cpu0.v2_5-s3   CPU 0 VDDIO voltage
cpu0.vcore-s0  CPU 0 core voltage
cpu0.vid       CPU-0 VID output
cpu0.vldt1     CPU0 HT 1 voltage
cpu0.vldt2     CPU 0 HT 2 voltage
cpu0.vtt-s3    CPU 0 VTT voltage
cpu1.dietemp   CPU 1 die temp
cpu1.heartbeat CPU 1 heartbeat
cpu1.memtemp   CPU 1 memory temp
cpu1.temp      CPU 1 low side temp
cpu1.v2_5-s3   CPU 1 VDDIO voltage
cpu1.vcore-s0  CPU 1 core voltage
cpu1.vid       CPU-1 VID output
cpu1.vtt-s3    CPU 1 VTT voltage
fan1.tach      Fan 1 measured speed
fan2.tach      Fan 2 measured speed
fan3.tach      Fan 3 measured speed
fan4.tach      Fan 4 measured speed
fan5.tach      Fan 5 measured speed
fan6.tach      Fan 6 measured speed
faultswitch    Fault switch (source for eval)
g.vldt1        AMD-8131 PCI-X Tunnel HT 1 voltage
gbeth.temp     Gigabit ethernet temp
golem.temp     PCIX bridge temp
hddbp.temp     Disk drive backplane temp
identifyswitch Identify switch
ps.fanfail     Power Supply fan failure sensor
ps.tempalert   Power Supply too hot sensor
sp.temp        SP temp
thor.temp      AMD-8111 I/O Hub temp
```

Monitoring data is retrieved by the N1 System Manager from most these sensors.

For Sun Fire X4100 and Sun Fire X4200 servers, the following sensors are monitored:

```
Chassis Sensors:
sys.id              Indicates chassis type
sys.intsw           State of the Chassis Intrusion switch. When the chassis cover to
                    the CPU area is opened this sensor logs an event
sys.psfail          LED indicator shows state of PS Fail / Rear LED
                    on the front panel
sys.tempfail        LED indicator shows state of Over Temperature LED
                    on the front panel
sys.fanfail         LED indicator shows state of Over Temperature LED
```

```
                    on the front panel

Back Panel Sensors
bp.power            LED indicator shows state of the Power LED on the back panel
bp.locate           LED indicator shows state of the Locate LED on the back panel
bp.locate.btn       Monitors the state of the back panel locate button
bp.alert            LED indicator shows state of Alert LED on the back panel

Front Panel Sensors
fp.prsnt            Monitors the presence of the front panel board
fp.ledbd.prsnt      Monitors the presence of the front panel LED board
fp.usbfail          Monitors the front panel USB over current sensor
fp.power            LED indicator shows state of Power LED on the front panel
fp.locate           LED indicator shows state of Locate LED on the front panel
fp.locate.btn       Monitors the state of the front panel locate button
fp.alert            LED indicator shows state of Alert LED on the front panel

I/O Sensors
io.id0.prsnt        Monitors the 2-disk I/O board presence signal
io.id1.prsnt        Monitors the 4-disk I/O board presence signal
io.f0.prsnt         Monitors the physical presence of the rear blower
                    (Sun Fire X4200 chassis only)
io.f0.speed         Monitors the speed of the rear blower
                    (Sun Fire X4200 chassis only)
io.f0.fail          LED indicator shows state of the I/O fan assembly
io.hdd0.fail        LED indicator shows state of the Hard Disk Drive 0 fault LED
io.hdd1.fail        LED indicator shows state of the Hard Disk Drive 1 fault LED
                    (Unused on the 2-disk Sun Fire X4100)
io.hdd2.fail        LED indicator shows state of the Hard Disk Drive 2 fault LED
                    (Unused on the 2-disk Sun Fire X4100)
io.hdd3.fail        LED indicator shows state of the Hard Disk Drive 3 fault LED
                    (Unused on the 2-disk Sun Fire X4100)

CPU 0 Sensors
p0.fail             LED indicator shows state of the CPU 0 fault LED
                    Illuminated for CPU voltage and temperature events
p0.d0.fail          LED indicator shows state of the CPU 0 DIMM 0 fault LED
                    Illuminated in response to ECC errors
                    PAIR 0 includes this and p0.d1.fail, both LEDs in the same pair
                    will be illuminated at the same time when one indicates a fault
p0.d1.fail          LED indicator shows state of the CPU 0 DIMM 1 fault LED
                    Illuminated in response to ECC errors
                    PAIR 0 includes this and p0.d0.fail, both LEDs in the same pair
                    will be illuminated at the same time when one indicates a fault
p0.d2.fail          LED indicator shows state of the CPU 0 DIMM 2 fault LED
                    Illuminated in response to ECC errors
                    PAIR 1 includes this and p0.d3.fail, both LEDs in the same pair
                    will be illuminated at the same time when one indicates a fault
p0.d3.fail          LED indicator shows state of the CPU 0 DIMM 3 fault LED
                    Illuminated in response to ECC errors
                    PAIR 1 includes this and p0.d2.fail, both LEDs in the same pair
                    will be illuminated at the same time when one indicates a fault

CPU 1 Sensors
p1.fail             Same as p0.fail, but for CPU 1
```

```
p1.d0.fail           Same as p0.d0.fail, but for CPU 1
p1.d1.fail           Same as p0.d1.fail, but for CPU 1
p1.d2.fail           Same as p0.d2.fail, but for CPU 1
p1.d3.fail           Same as p0.d3.fail, but for CPU 1

Power Supply Sensors
ps0.prsnt            Indicates whether Power Supply 0 is present
ps0.vinok            Indicates whether Power Supply 0 is connected to AC power
ps0.pwrok            Indicates whether Power Supply 0 is turned on and powering the system
ps1.prsnt            Indicates whether Power Supply 1 is present
ps1.vinok            Indicates whether Power Supply 1 is turned on and powering the system
ps1.pwrok            Indicates whether Power Supply 1 is turned on and powering the system

Fan Control Temperature Sensors
fp.t_amb             Monitors front panel ambient temperature
p0.t_core            Monitors CPU 0 core temperature
p1.t_core            Monitors CPU 1 core temperature

Other Temperature Sensors
mb.t_amb             Monitors ambient temperature from the internal temperature
                     sensor in the chip on the mainboard
pdb.t_amb            Monitors the ambient temperature of the power distibution board
io.t_amb             Monitors the ambient temperature from near the I/O area in the chassis

Mainboard Voltage Sensors
mb.v_bat             Monitors the 3V RTC battery on the mainboard
mb.v_+3v3stby        Monitors the 3.3V standby input that powers
                     the service processor and other standby devices
mb.v_+3v3            Monitors the 3.3V main input that is active when the power is on
mb.v_+5v             Monitors the 5V main input that is active when the power is on
mb.v_+12v            Monitors the 12V main input that is active when the power is on
mb.v_-12v            Monitors the -12V main input that is active when the power is on
mb.+2v5core          Monitors the 2.5V core input that is active when the power is on
mb.+1v8core          Monitors the 1.8V core input that is active when the power is on
mb.+1v2core          Monitors the 1.2V core input that is active when the power is on

CPU 0 Voltage Sensors
p0.v_+1v5            Monitors the CPU 0 1.5V input
p0.v_+2v5core        Monitors the CPU 0 2.5V core input
p0.v_+1v2core        Monitors the CPU 0 1.2V core input

CPU 1 Voltage Sensors
p1.v_+1v5            Monitors the CPU 1 1.5V input
p1.v_+2v5core        Monitors the CPU 1 2.5V core input
p1.v_+1v2core        Monitors the CPU 1 1.2V core input

Fan Presence Sensors (Sun Fire X4200 chassis only)
ft0.fm0.prsnt        Indicates the presence of Fan Tray 0, Fan Module 0
ft0.fm1.prsnt        Indicates the presence of Fan Tray 0, Fan Module 1
ft0.fm2.prsnt        Indicates the presence of Fan Tray 0, Fan Module 2
ft1.fm0.prsnt        Indicates the presence of Fan Tray 1, Fan Module 0
ft1.fm1.prsnt        Indicates the presence of Fan Tray 1, Fan Module 1
ft1.fm2.prsnt        Indicates the presence of Fan Tray 1, Fan Module 2

Fan Speed Sensors
```

```
ft0.fm0.f0.speed     Monitors speed of fan at Fan Tray 0, Fan Module 0, Fan 0
ft0.fm0.f1.speed     Monitors speed of fan at Fan Tray 0, Fan Module 0, Fan 1
                     (Sun Fire X4100 only)
ft0.fm1.f0.speed     Monitors speed of fan at Fan Tray 0, Fan Module 1, Fan 0
ft0.fm1.f1.speed     Monitors speed of fan at Fan Tray 0, Fan Module 1, Fan 1
                     (Sun Fire X4100 only)
ft0.fm2.f0.speed     Monitors speed of fan at Fan Tray 0, Fan Module 2, Fan 0
ft0.fm2.f1.speed     Monitors speed of fan at Fan Tray 0, Fan Module 2, Fan 1
                     (Sun Fire X4100 only)
ft1.fm0.f0.speed     Monitors speed of fan at Fan Tray 1, Fan Module 0, Fan 0
ft1.fm0.f1.speed     Monitors speed of fan at Fan Tray 1, Fan Module 0, Fan 1
                     (Sun Fire X4100 only)
ft1.fm1.f0.speed     Monitors speed of fan at Fan Tray 1, Fan Module 1, Fan 0
ft1.fm1.f1.speed     Monitors speed of fan at Fan Tray 1, Fan Module 1, Fan 1
                     (Sun Fire X4100 only)
ft1.fm2.f0.speed     Monitors speed of fan at Fan Tray 1, Fan Module 2, Fan 0
ft1.fm2.f1.speed     Monitors speed of fan at Fan Tray 1, Fan Module 2, Fan 1
                     (Sun Fire X4100 only)
```

For Sun Fire X2100 servers, only sensors describing fan speed, voltage, and temperature are used to retrieve data: Here is a list of sensors we monitored:

```
DDR 2.6V
CPU core Voltage
VCC 3.3V
VCC 5V
VCC 12V
Battery Volt
CPU TEMP
SYS TEMP
CPU FAN
SYSTEM FAN3
SYSTEM FAN1
SYSTEM FAN2
```

OS Health Monitoring

OS health can be monitored by the N1 System Manager. As part of the `add server feature` command, with the `agentip` keyword, you provide credentials to access the monitored server's operating system through `ssh` with the `agentssh` keyword. See "To Add the OS Monitoring Feature" on page 158 for additional details. This procedure is important for OS health monitoring but not for monitoring hardware health or network reachability.

Adding the OS monitoring feature provides support for OS monitoring and enables monitoring by default. After that, monitoring can be disabled and enabled by use of the `set server` command. See "Enabling and Disabling Monitoring" on page 170 for more information.

Platform OS interface data is obtained through `ssh` and SNMP. All attribute data is retrieved from the server's operating system by using `ssh` and SNMP. Statistics related to the central processor unit (CPU) are provided, as is data related to memory, swap usage, and file systems. For the purposes of monitoring, system load data, memory usage, and swap usage data can be categorized as follows:

- System usage, including system idle times
- System load, expressed as the average number of queued processes over 1, 5, and 15 minutes
- Memory usage and memory free statistics, in megabytes and as percentages
- Physical load statistics
- Swap space used and space available, in megabytes and as percentages
- File system used and space available, as percentages

A list of these attributes is provided in "Hardware Sensor Attributes" on page 148.

You can filter OS health monitoring information for all servers by using the `show server` command:

```
N1-ok> show server oshealth oshealth
```

See "show server" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details of possible values of the *oshealth* filters. For more information and a graphic explaining filtering servers by health state, see "To View Failed Servers" on page 120.

The health of an OS resource can be shown as `unknown` if the server is reachable but the agent for the monitoring feature cannot be contacted on SNMP port 161. The health of an OS resource can be shown as `unreachable` if the server is unreachable due to, for example, being in standby mode. See also "Understanding the Differences Between `Unreachable` and `Unknown` States for Provisionable Servers" on page 155.

The monitoring of OS health allows you to set specific thresholds for individual monitored servers, or for groups of monitored servers, at the command line by using the `set` command. See "Setting Threshold Values" on page 180 for details.

If you are not interested in the values of some attributes, you can disable the threshold severity for monitoring of those attributes. This action prevents annoyance alarms. Example 5–6 shows you how to accomplish this disabling action.

Network Reachability Monitoring

All management interfaces of provisionable servers and all platform interfaces are monitored by default by the N1 System Manager. Platform interfaces include the service processor's management interface, such as `eth0`, and data network interfaces, such as `eth1` or `eth2`.

Reachability is verified for Linux servers and servers running the Solaris OS by using an ICMP `ping` to the interface IP address. For further information, see "Discovery of Servers in the Factory Default State" in *Sun N1 System Manager 1.2 Installation and Configuration Guide*.

The reachability of all network interfaces is verified at regular intervals. The monitoring of network reachability is based on the IP address. If any monitored IP address is unreachable, an event is generated.

You can filter information for all servers by using the `show server` command with the appropriate parameters to view monitoring information. See "show server" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.

Understanding the Differences Between `Unreachable` and `Unknown` States for Provisionable Servers

Distinguishing between the unreachable and unknown states for provisionable servers is important.

```
N1-ok> show server oshealth unreachable
```

This command lists all provisionable servers that are unreachable. Any provisionable server returned in the output of this command is unreachable due to a network problem: the server cannot be contacted about its hardware health status. The `ping` command to the server is unsuccessful. This behavior does not necessarily mean that the server is not transmitting hardware health status information. The server could be in standby mode.

```
N1-ok> show server oshealth unknown
```

This command lists all provisionable servers that are not returning any information about hardware health status. The `ping` command might be successful but servers returned in the output of this command are not returning any hardware health information. The agent for the monitoring feature could not be contacted on port 161.

```
N1-ok> show server power unreachable
```

This command lists all provisionable servers that are unreachable. Any server returned in the output of this command is unreachable due to a network problem: the server cannot be contacted about its power status. The `ping` command to the server is unsuccessful. This behavior does not necessarily mean that the server is not transmitting power status information. The server could be in standby mode.

```
N1-ok> show server power unknown
```

This command lists all provisionable servers that are not returning any information about power status. The `ping` command might be successful but servers returned in the output of this command are not returning any power status information. The agent for the monitoring feature could not be contacted on port 161.

```
N1-ok> show server oshealth unreachable
```

This command lists all provisionable servers that are unreachable. Any server returned in the output of this command is unreachable due to a network problem: the server cannot be contacted about its OS health. The `ping` command to the server is unsuccessful. This behavior does not necessarily mean that the server is not transmitting OS health information. The server could be in standby mode.

```
N1-ok> show server oshealth unknown
```

This command lists all provisionable servers that are not returning any information about OS health. The `ping` command might be successful but servers returned in the output of this command are not returning any OS health information. The agent for the monitoring feature could not be contacted on port 161.

Supporting Monitoring

Before full monitoring of a provisionable server can be enabled, monitoring must be supported for that server. Monitoring is supported for a server when the base management and OS monitoring features are installed on the server.

The base management and OS monitoring features are installed when a provisionable server's OS is installed or updated by use of the `load group` or `load server` commands. See "load group" in *Sun N1 System Manager 1.2 Command Line Reference Manual* and "load server" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.

Note – If the `load server` or `load group` command is used to install software on the provisionable server, and the provisionable server's `networktype` attribute is to `dhcp`, the `feature` attribute cannot be used. Therefore if you want to load the base management and OS monitoring features when loading an OS with the `load server` or `load group` commands, set the `networktype` attribute to `static`. In addition, if you the `networktype` attribute to `dhcp`, every time the server reboots you have to change the agent IP address as explained in "To Modify the Agent IP for a Server" on page 162.

The base management and OS monitoring features can also be installed or updated when the `add server` command is used, as explained in "Adding and Upgrading Base Management and OS Monitoring Features" on page 157.

If the OS monitoring feature is not installed and you use the `set server monitored` command to enable monitoring, only hardware health monitoring is enabled. OS monitoring is not enabled if this command is executed without the OS monitoring feature first being installed. See "Enabling and Disabling Monitoring" on page 170 for more information.

Adding and Upgrading Base Management and OS Monitoring Features

The base management and OS monitoring features provide support for monitoring and patching the installed OS profiles, and for executing remote commands. This section describes how to add the base management and OS monitoring features, modify supported attributes, remove feature support, and upgrade the base management and OS monitoring features to the latest versions.

Adding the OS monitoring features provides support for monitoring and enables monitoring by default. You can subsequently enable and disable monitoring by using the `set server` command as explained in "Enabling and Disabling Monitoring" on page 170.

This section describes the following tasks:

▼ To Add the Base Management Feature

This procedure describes how to add the base management feature on a server with a newly deployed OS. The base management feature is used to enable remote command execution and package deployment.

Note – Uninstallation of the base management feature is not supported.

The agent IP used in this procedure is the IP address of the provisionable server's data network interface to be monitored by the management server. The interface can be `eth1/bge1` or `eth0/bge0`, but usually is `eth0/bge0`. For more information on the server's agent IP address, see "To Modify the Agent IP for a Server" on page 162.

Note – You can add the base management feature automatically as part of the `load server` or `load group` commands. See "load server" in *Sun N1 System Manager 1.2 Command Line Reference Manual* or "load group" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.

Before You Begin

- Discover servers. See Chapter 2
- Load an OS if an OS is not already installed. See "To Load an OS Profile on a Server or a Server Group" on page 90 and "load server" in *Sun N1 System Manager 1.2 Command Line Reference Manual*.

Steps

1. **Log in to the N1 System Manager.**

   See "To Access the N1 System Manager Command Line" on page 28 for details.

2. **Type the following command:**

   Note – The SSH user account that is used in the following command must have root privileges on the remote machine:

   ```
   N1-ok> add server server feature basemanagement agentip agentip agentssh username/password
   ```

   An Add Base Management Support job is started.

   The necessary packages and scripts are added. See "add server" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.

3. **After successful completion of the Add Base Management Support job, type the following command:**

   ```
   N1-ok> show server server
   ```

   The Base Management Supported field should appear with OK as the value.

Next Steps "To Add the OS Monitoring Feature" on page 158

▼ To Add the OS Monitoring Feature

This procedure describes how to add the OS monitoring feature on a server. You can add the OS monitoring feature to a server that already has the base management feature added. Alternatively, you can add the OS monitoring feature to a server with a newly loaded OS and the base management feature is added automatically. The OS monitoring feature is used for OS health monitoring and inventory management. See Chapter 5 for details.

The `add server feature osmonitor` command creates an Add OS Monitoring Support job. You can submit multiple, overlapping `add server feature osmonitor` commands and have them run in parallel. However, you should limit the number of overlapping Add OS Monitoring Support jobs to a maximum of 15.

If you submit `add server feature` commands by using a script, see Example 5–1 for an example.

Note – You can add the OS monitoring feature automatically as part of the `load server` or `load group` commands. See "load server" in *Sun N1 System Manager 1.2 Command Line Reference Manual* or "load group" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.

Before You Begin

- Discover servers. See Chapter 2
- Load an OS if one is not already installed, see "To Load an OS Profile on a Server or a Server Group" on page 90 and "load server" in *Sun N1 System Manager 1.2 Command Line Reference Manual*.

Steps

1. **Log in to the N1 System Manager.**
   See "To Access the N1 System Manager Command Line" on page 28 for details.
2. **To add the OS monitoring feature, perform one of the following actions:**

   - **If you have not added the base management feature, type the following command:**

     Note – The SSH user account that is used in the following command must have root privileges on the remote machine.

     ```
     N1-ok> add server server feature osmonitor agentip agentip agentssh username/password
     ```

   - **If you have already added the base management feature, type the following command:**

     Note – You cannot specify the agent IP or SSH credentials when adding OS monitoring support to a server that has base management support.

     ```
     N1-ok> add server server feature osmonitor
     ```

   An Add OS Monitoring Support job starts.

   See "add server" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details about command syntax.

3. **Track the Add OS Monitoring Support job to completion.**

   After the job completes successfully, the Servers table on the System Dashboard tab appears with values for OS Usage and OS Resource Health.

   Verify that the OS monitoring feature is supported by issuing the `show server` command. Output for the server appears with the OS Monitoring Supported value as OK one of the following sets of commands on the provisionable server.

Note – It can take 5-7 minutes before all OS monitoring data is fully initialized. You may see that CPU idle is at `0.0%`, which causes a Failed Critical status with OS usage. This should clear up within 5-7 minutes after adding or upgrading the OS monitoring feature.

   If no monitoring data is available for the server, see "Resolving Command Failures Related to OS Monitoring" on page 218.

   If the provisionable server's IP address changes, use the `set server` command again before enabling or disabling monitoring

Example 5–1 Scripting OS Monitoring Support

The following example script issues multiple `add server feature` commands on servers that do not have the base management feature support:

```
n1sh add server 10.0.0.10 feature=osmonitor agentip 10.0.0.110 agentssh root/admin &
n1sh add server 10.0.0.11 feature=osmonitor agentip 10.0.0.111 agentssh root/admin &
n1sh add server 10.0.0.12 feature=osmonitor agentip 10.0.0.112 agentssh root/admin &
```

Troubleshooting Adding the OS monitoring feature might fail due to stale SSH entries on the management server. If the `add server feature osmonitor agentip` command fails and no true security breach has occurred, remove the `known_hosts` file or the specific entry in the file that corresponds to the provisionable server. Then, retry the `add server feature osmonitor agentip` command. If the management server is running Linux, the `known_hosts` file is at `/root/.ssh/known_hosts`. If the management server is running the Solaris OS, the `known_hosts` file is at `/.ssh/known_hosts`.

Adding the OS monitoring feature will fail if you specify the agent IP or the SSH credentials in the `add server feature osmonitor` command when running it on servers that already have the base management feature support. To solve this problem, issue the `add server feature osmonitor` command without specifying values for the agent IP or for the SSH credentials.

▼ To Remove the OS Monitoring Feature

There are two levels of removing the OS monitoring feature with this command. If you don't specify the `uninstall` keyword, the OS monitoring feature remains installed on the provisionable server, but the feature is no longer supported and the server's OS can no longer be monitored with the N1 System Manager. If you specify the `uninstall` keyword, the OS monitoring feature is completely uninstalled from the provisionable server and consequently the OS monitoring feature is no longer supported.

Once removed in either case, the OS resource health state for the server becomes `uninitialized`.

After you remove a feature, provided you used the recommended procedure, you can always use the `add server` command to add it back again. The `Base Management Supported` and `OS Monitoring Supported` fields in the `show server` output provide the current status on a server's features.

Note – Do not manually remove the OS monitoring feature by attempting to delete the agent. Doing so will make it impossible to reinstall or reutilize the OS monitoring feature. Instead, to remove the OS monitoring feature, use the `remove server feature` procedure as described.

Steps

1. **Log in to the N1 System Manager.**

   See "To Access the N1 System Manager Command Line" on page 28 for details.

2. **Remove the OS monitoring feature.**

   ```
   N1-ok> remove server server feature osmonitor [uninstall]
   ```

   The necessary packages and scripts are removed. See "remove server" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details about command syntax.

▼ To Remove the Base Management Feature

The OS monitoring feature must be removed before the base management feature can be removed. See "To Remove the OS Monitoring Feature" on page 161 for details.

When you remove the base management feature, the feature is uninstalled from the provisionable server and it is no longer supported.

After you remove a feature, provided you used the recommended procedure, you can always use the `add server` command to add it back again. The `Base Management Supported` and `OS Monitoring Supported` fields in the `show server` output provide the current status on a server's features.

Note – Do not manually remove the base management feature by attempting to delete the agent. Doing so will make it impossible to reinstall or reutilize the base management feature. Instead, to remove the base management feature, use the `remove server feature` procedure as described.

Steps

1. **Log in to the N1 System Manager.**

   See "To Access the N1 System Manager Command Line" on page 28 for details.

2. **Remove the OS monitoring feature.**

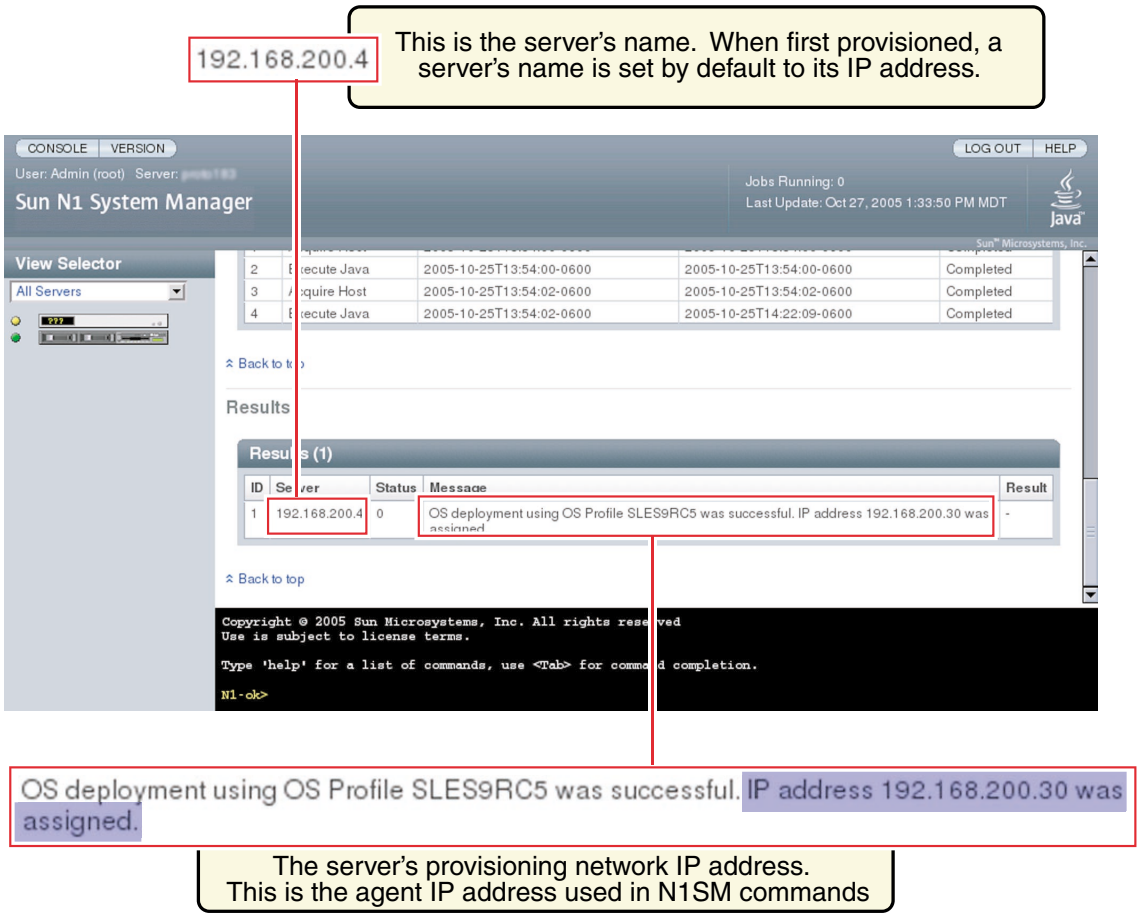
   ```
   N1-ok> remove server server feature basemanagement
   ```

   The necessary packages and scripts are removed. See "remove server" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details about command syntax.

▼ To Modify the Agent IP for a Server

This procedure describes how to modify the agent IP for a server. The agent IP is the IP address of the provisionable server's data network interface to be monitored by the management server. The agent IP is not the same as the server's management network IP address.

The following graphic shows the agent IP address for a server from the results table of a job, displayed in the Jobs tab. The graphic distinguishes the agent IP address for the server from the server's IP address.



Note – If you change the provisionable server's IP address and credentials or manually remove some services outside the N1 System Manager, the enabling of the services will not succeed. Arbitrary changes to the OS outside of the N1 System Manager require a rediscovery and subsequent addition of the base and OS management features.

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

- The OS Monitoring content of the `show server` command. (No OS monitoring)

- The `load server` *server* `update` and `load group` *group* `update` commands
- The `start server` *server* `command` command
- The `set server` *server* `threshold` command
- The `set server` *server* `refresh` command

In this case, use the `set server` *server* `agentip` command to correct the server's agent IP address as shown in this procedure.

Steps

1. **Log in to the N1 System Manager.**

   See "To Access the N1 System Manager Command Line" on page 28 for details.

2. **Run the following command:**

   ```
   N1-ok> set server server agentip IP
   ```

   The agent IP is modified. See "set server" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details about command syntax. This operation touches the provisionable server.

▼ To Modify the Secure Shell Credentials for the Management Features of a Server

This procedure describes how to modify the Secure Shell (SSH) credentials for the base management and OS monitoring features for a provisionable server. These management SSH credentials are required by or used in many N1 System Manager commands including `add server`, `set server`, `load server`, `start server`, `load group`, and `start group`. These credentials, specifically for the base management and OS monitoring features for a provisionable server and referred to by the examples in this chapter as `agentssh` credentials, are not the same as the SSH credentials required for the server's management network IP address.

Steps

1. **Log in to the N1 System Manager.**

   See "To Access the N1 System Manager Command Line" on page 28 for details. You need to have an SSH login and password for this step. Default SSH login/password pairs are provided in "Discovering Servers" on page 51.

2. **Run the following command:**

   Note – The SSH user account that is used in the following command must have root privileges on the remote machine.

   ```
   N1-ok> set server server agentip IP agentssh username/password
   ```

   The `agentssh` user name and password are modified. See "set server" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details about command syntax.

▼ To Modify the SNMP Credentials for the Management Features of a Server

This procedure describes how to modify the management feature SNMP credentials for a server. The management feature SNMP credentials allow the N1 System Manager to communicate with the Sun Management Center SNMP agent and are specifically for the base management and OS monitoring features for a provisionable server. These credentials, specifically for the base management and OS monitoring features for a provisionable server and referred to by the examples in this chapter as `agentsnmp` credentials, are not the same as the SNMP credentials required for the server's management network IP address.

See "Introduction to Monitoring" on page 145 for more information about the SNMP agents for OS monitoring in the N1 System Manager.

Steps

1. **Log in to the N1 System Manager.**

   See "To Access the N1 System Manager Command Line" on page 28 for details.

2. **Run the following command to specify the SNMP credentials on a server:**

   ```
   N1-ok> set server server agentsnmp agentsnmp
   ```

   The SNMP credentials are modified. See "set server" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details about command syntax.

   This `set server` operation does not actually touch the provisionable server. It just synchronizes the data on the management server itself.

▼ To Modify the SNMPv3 Credentials for the Management Features of a Server

This procedure describes how to modify the management feature SNMPv3 credentials for a server. The management feature SNMPv3 credentials allow the N1 System Manager to communicate with the Sun Management Center SNMP agent and are specifically for the base management and OS monitoring features for a provisionable server. These credentials, specifically for the base management and OS monitoring features for a provisionable server and referred to by the examples in this chapter as `agentsnmpv3` credentials, are not the same as the SNMP credentials required for the server's management network IP address.

See "Introduction to Monitoring" on page 145 for more information about the SNMP agents for OS monitoring in the N1 System Manager.

Steps

1. **Log in to the N1 System Manager.**

   See "To Access the N1 System Manager Command Line" on page 28 for details.

2. **Run the following command to specify the SNMP credentials on a server:**

   ```
   N1-ok> set server server agentsnmpv3 agentsnmpv3
   ```

   The SNMP credentials are modified. See "set server" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details about command syntax.

   This `set server` operation does not actually touch the provisionable server. It just synchronizes the data on the management server itself.

▼ To Manually Uninstall the Linux OS Monitoring Feature

After successful completion of this procedure, the OS monitoring feature is unsupported for the provisionable server:

Steps

1. **Log in to the provisionable server as root.**
2. **Type the following command:**

   ```
   # /etc/rc.d/rc3.d/S99es_agent stop
   ```

3. **Issue the following command and follow the prompts.**

   ```
   # /opt/SUNWsymon/sbin/es-uninst
   ```

   The agent is uninstalled.

4. **Manually remove the feature.**

   ```
   # rpm -e n1sm-linux-agent
   ```

   The feature is removed.

5. **Remove directories related to the feature.**

   ```
   # rm -rf /var/opt/SUNWsymon
   ```

   The directories are removed.

▼ To Manually Uninstall the Solaris OS Monitoring Feature

After successful completion of this procedure, the OS monitoring feature will be unsupported for the provisionable server.

Steps

1. **Log in to the provisionable server as root.**
2. **Stop the agent.**

   ```
   # /etc/rc3.d/S81es_agent stop
   ```

3. **Run the uninstaller.**

   ```
   # /var/tmp/solx86-agent-installer/disk1/x86/sbin/es-uninst -X
   ```

4. **Remove the packages.**

   For the Solaris OS running on the SPARC architecture:

   ```
   # pkgrm SUNWn1smsparcag-1-2
   ```

   For the Solaris OS running on the x86 architecture:

   ```
   # pkgrm SUNWn1smx86ag-1-2
   ```

5. **Remove associated directories.**

   ```
   # /bin/rm -rf /opt/SUNWsymon
   # /bin/rm -rf /var/opt/SUNWsymon
   ```

   The directories are removed.

▼ To Upgrade the Base Management Feature on a Server

This procedure describes how to upgrade the base management feature on a server. This procedure is necessary after upgrading the N1 System Manager from a previous release, for provisionable servers on which the previous version of the base management feature is still installed. This procedure is for individual servers. You can upgrade the base management feature on multiple servers at once. See Chapter 2, "Upgrading the Sun N1 System Manager Software and Provisionable Server Management Agents," in *Sun N1 System Manager 1.2 Installation and Configuration Guide* for details.

Note – If the server was freshly installed using the `load server` or `load group` commands from the latest version of the N1 System Manager, and the `feature` subcommand was used, this procedure is not necessary.

Use the `add server feature basemanagement` command with the `upgrade` keyword to upgrade a provisionable server to a new version from the existing base management feature.

If you submit `add server feature` commands by using a script, see Example 5–1 for an example.

Before You Begin

- Discover servers. See Chapter 2.
- This base management feature upgrade procedure applies to provisionable servers on which the base management feature is already installed by a previous version of the N1 System Manager.

Steps

1. **Log in to the N1 System Manager.**

   See "To Access the N1 System Manager Command Line" on page 28 for details.

2. **To upgrade the base management feature, type the following command:**

   ```
   N1-ok> add server server feature basemanagement upgrade
   ```

An Add Base Management Support job starts.

See "add server" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details about command syntax.

3. **Track the Add Base Management Support job to completion.**

   After the job completes successfully, the `show server` command output for the server appears with the OS Monitoring Supported value as OK. In addition, the Base Management Supported column on the Server Details page is marked as Yes. See "Enabling and Disabling Monitoring" on page 170 for a graphic that shows this.

Troubleshooting Adding the base management feature might fail due to stale SSH entries on the management server. If the `add server feature osmonitor agentip` command fails and no true security breach has occurred, remove the `known_hosts` file or the specific entry in the file that corresponds to the provisionable server. Then, retry the `add server feature osmonitor agentip` command. If the management server is running Linux, the `known_hosts` file is at `/root/.ssh/known_hosts`. If the management server is running the Solaris OS, the `known_hosts` file is at `/.ssh/known_hosts`.

▼ To Upgrade the OS Monitoring Feature on a Server

This procedure describes how to upgrade the OS monitoring feature on a server. This procedure is necessary after upgrading the N1 System Manager from a previous release, for provisionable servers on which the previous version of the OS monitoring feature is still installed. This procedure is for individual servers. You can upgrade the OS monitoring feature on multiple servers at once. See Chapter 2, "Upgrading the Sun N1 System Manager Software and Provisionable Server Management Agents," in *Sun N1 System Manager 1.2 Installation and Configuration Guide* for details.

Note – If the server was freshly installed using the `load server` or `load group` commands from the latest version of the N1 System Manager, and the `feature` subcommand was used, this procedure is not necessary.

Use the `add server feature osmonitor` command with the `upgrade` keyword to upgrade a provisionable server to a new version from the existing base management feature and OS monitoring feature.

If you submit `add server feature` commands by using a script, see Example 5–1 for an example.

Before You Begin

- Discover servers. See Chapter 2
- This OS monitor feature upgrade procedure applies to provisionable servers on which the OS is already installed by a previous version of the N1 System Manager.

Steps

1. **Log in to the N1 System Manager.**

   See "To Access the N1 System Manager Command Line" on page 28 for details.

2. **To upgrade the OS monitoring feature, type the following command:**

   ```
   N1-ok> add server server feature osmonitor upgrade
   ```

   An Modify OS Monitoring Support job starts. Note that this command also upgrades the base management feature.

   See "add server" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details about command syntax.

3. **Track the Add OS Monitoring Support job to completion.**

   After the job completes successfully, the Servers table on the System Dashboard tab appears with values for OS Usage and OS Resource Health.

   Verify that the OS monitoring feature is supported by issuing the `show server` command. Output for the server appears with the OS Monitoring Supported value as OK one of the following sets of commands on the provisionable server.

Note – It can take 5-7 minutes before all OS monitoring data is fully initialized. You may see that CPU idle is at `0.0`%, which causes a Failed Critical status with OS usage. This should clear up within 5-7 minutes after adding or upgrading the OS monitoring feature.

Troubleshooting Upgrading the OS monitoring feature might fail due to stale SSH entries on the management server. If the `add server feature osmonitor agentip` command fails and no true security breach has occurred, remove the `known_hosts` file or the specific entry in the file that corresponds to the provisionable server. Then, retry the `add server feature osmonitor agentip` command. If the management server is running Linux, the `known_hosts` file is at `/root/.ssh/known_hosts`. If the management server is running the Solaris OS, the `known_hosts` file is at `/.ssh/known_hosts`.

Upgrading the OS monitoring feature will fail if you specify the agent IP or the SSH credentials in the `add server feature osmonitor upgrade` command when running it on servers that already have the base management feature support. To solve this problem, issue the `add server feature osmonitor` command without specifying values for the agent IP or for the SSH credentials.

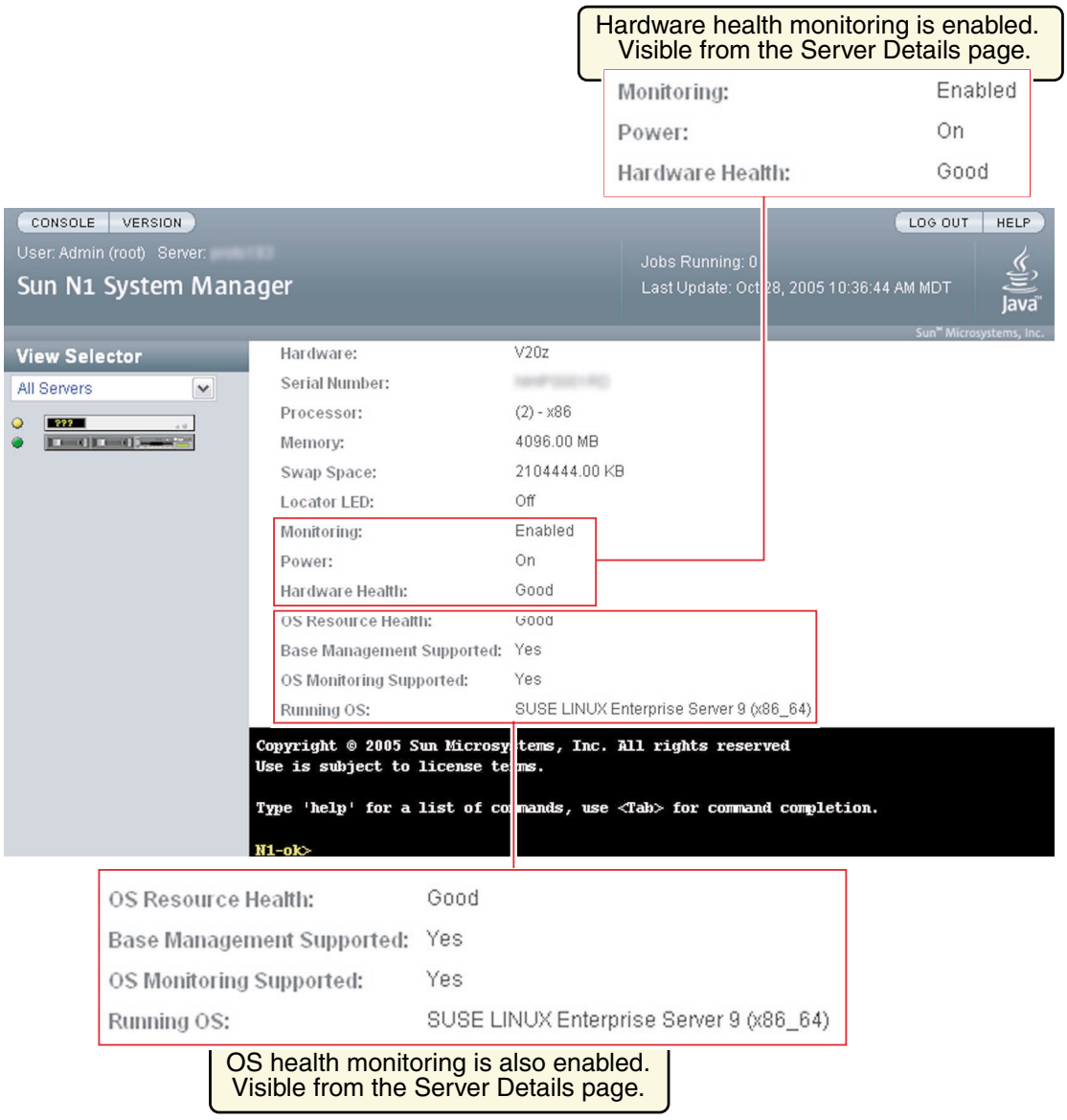
Enabling and Disabling Monitoring

Monitored file system and OS health data for a provisionable server is *not* available unless an operating system is deployed on the provisionable server, and the OS monitoring feature has been installed.

Once the OS monitoring feature is installed on a server, monitoring is enabled by default. For information on installing the OS monitoring feature on a server, see "Supporting Monitoring" on page 156.

Use the `set server monitored` command to enable or disable monitoring. See "Enabling and Disabling Monitoring" on page 170. If the OS monitoring feature is not installed on a server or on every server in a group, using the `set server monitored` command enables only *hardware monitoring* for the server or group of servers.

The following graphic shows a section of the Server Details page. The server is powered on, an OS has been installed and the base management and OS monitoring features are supported. Monitoring is enabled for the server.



Disabling monitoring by use of the `set server monitored` command does not remove the monitoring support provided by the OS monitoring feature, which remains installed on the server. However, disabling monitoring by the `set server monitored` command disables both hardware health and OS health monitoring.

▼ To Monitor a Server or a Server Group

The following procedure describes how to use the command line to enable the monitoring of hardware health and operating system health of a server or a server group. Hardware health and OS health monitoring are both enabled with this command, provided that the OS monitoring feature has been installed on the server or the server group. If the OS monitoring feature has not been installed on the server or server group, then only hardware health monitoring is enabled.

Before You Begin

To enable the management agent IP and security credentials on a server named *server*, add the management features on the server as explained in "Supporting Monitoring" on page 156.

Steps

1. **Log in to the N1 System Manager.**

   See "To Access the N1 System Manager Command Line" on page 28 for details.

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

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

   In this procedure, *server* is the name of the provisionable server that you want to monitor.

   - **For a server group, set the `monitored` attribute to `true` by using the `set group` command.**

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

     This command is executed for the group of servers that you have already named. See "set group" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details. In this procedure, *group* is the name of the group of provisionable servers that you want to monitor.

3. **View the server details.**

   ```
   N1-ok> show server server
   ```

   - **For a server group, view the server group details to determine if monitoring is enabled for each server in the group.**

     ```
     N1-ok> show group group
     ```

   Detailed monitoring information appears in the output. Information is displayed about hardware health, OS health and network reachability. OS health monitoring threshold values are also displayed.Monitoring threshold values are explained in "Monitoring Threshold Values" on page 174.

▼ To Disable Monitoring for a Server or a Server Group

The following procedure describes how to use the command line to disable the monitoring of hardware health and operating system health of a server or a server group. Hardware health and OS health monitoring are both disabled with this command, provided that the OS monitoring feature has been added.

You might want to disable monitoring of a hardware component to perform maintenance tasks without generating events.

Steps

1. **Log in to the N1 System Manager.**
   See "To Access the N1 System Manager Command Line" on page 28 for details.

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

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

   In this example, *server* is the name of the provisionable server that you want to stop monitoring. Executing this command disables monitoring of the server. With monitoring of a server disabled, the violation of threshold values by attributes related to that server does not generate events.

   - **For a server group, set the `monitored` attribute to `false` by using the `set group` command.**

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

     This command is executed for the group of servers that you have already named. See "set group" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details. In this procedure, *group* is the name of the group of provisionable servers for which you want to disable monitoring.

3. **View the server details.**

   ```
   N1-ok> show server server
   ```

   The output shows that monitoring is disabled.

   If you are not interested in the values of some OS health attributes, you can disable the threshold severity for the monitoring of those attributes, while continuing to monitor other OS health attributes. This action prevents annoyance alarms. Example 5–6 shows how to accomplish this task. For general information about threshold values, see "Monitoring Threshold Values" on page 174. You can also remove the OS health monitoring feature. See "To Remove the OS Monitoring Feature" on page 161.

   - **For a server group, view the server group details to determine if monitoring is disabled for each server in the group.**

     ```
     N1-ok> show group group
     ```

Default States of Monitoring

The default status of monitoring in the Sun N1 System Manager for discovered servers and initialized operating systems is as follows:

Default status of hardware monitoring
: When a server or other hardware is discovered, monitoring of the server or other hardware is enabled by default. Before a server can be monitored, however, it must be discovered and correctly registered with the N1 System Manager. This process is described in "Discovering Servers" on page 51. The monitoring of hardware sensors is enabled by default for all managed servers. If a server is deleted and then rediscovered, all states related to that server for the purposes of monitoring are lost, regardless of whether monitoring was enabled or disabled for that server when the server was deleted. When the server is rediscovered, monitoring is set to `true` by default. For more information about discovering servers, see "To Discover New Servers" on page 53.

Default status of OS health monitoring
: Disabled by default. When an OS has been successfully provisioned on a provisionable server and the N1 System Manager management features are supported by using the `add server feature` command with the `agentip` specified, OS health monitoring is enabled. The OS provisioning can be performed either through the N1 System Manager or by an external OS installation.

  If you are not interested in the values of some OS health attributes, you can disable the threshold severity for the monitoring of those attributes, while continuing to monitor other OS health attributes. This action prevents annoyance alarms. Example 5–6 shows how to accomplish this task. For general information about threshold values, see "Monitoring Threshold Values" on page 174.

Default status of network reachability monitoring
: When the management interface of the provisionable server is discovered, monitoring of the interface is enabled by default. When the management features are added, monitoring of other interfaces is enabled by default.

Monitoring Threshold Values

The value of any given monitored OS health attribute is compared to a threshold value. Low and high threshold values are defined and can be configured.

Attribute data is compared against thresholds at regular intervals.

When a monitored attribute's value is beyond the default or user-defined threshold safe range, an event is generated and a status is issued. If the value of the attribute is lower than the low threshold or higher than the high threshold, then depending on the severity of the threshold, an event is generated to show a status of `nonrecoverable`, `critical`, or `warning`. Otherwise, the status of the OS health monitored attribute is `OK`, provided that a value can be obtained.

If no value can be obtained, an event is generated to show that the status of the monitored attribute is `unknown`. The health of an OS resource can be shown as `unknown` if the server is reachable but the agent for the monitoring feature cannot be contacted on SNMP port 161. For more information, see "Understanding the Differences Between `Unreachable` and `Unknown` States for Provisionable Servers" on page 155.

The values `nonrecoverable, critical`, and `warning` are discussed in "show server" in *Sun N1 System Manager 1.2 Command Line Reference Manual*.

What Happens When a Threshold Is Broken

If the value of an OS health monitored attribute rises above the `warninghigh` threshold, a status of `warninghigh` is issued. If the value continues to rise and passes the `criticalhigh` threshold, a status of `Failed Critical` is issued. If the value continues to rise above the `nonrecoverablehigh` threshold, a status of `nonrecoverablehigh` is issued.

If the value then falls back to the safe range, no further events are generated until the value falls below the `Failed Warning` threshold, at which point an event is generated to show a status of `normal`.

If the value of a monitored attribute falls below the `warninglow` threshold, a status of `Failed Warning` is issued. If the value continues to fall, and passes the `criticallow` threshold, a status of `Failed Critical` is issued. If the value continues to fall below the `nonrecoverablelow` threshold, a status of `nonrecoverablelow` is issued.

If the value then rises back to the safe range, no further events are generated until the value rises above the `warninglow` threshold, at which point an event is generated to show a status of `normal`.

Threshold values for OS health attributes can be configured at the command line. This process is explained in "Setting Threshold Values" on page 180. For threshold values measuring percentages, the valid range is from `0` to `100`%. If you try to set a threshold value outside of this range, an error is generated. For attributes that do not measure percentages, these values depend on the number of processors in your system and on the usage characteristics of your installation.

Tuning Threshold Values for Your Installation

After a period of usage, you can develop an awareness of what levels to set for OS health attribute values. You can adjust thresholds once you determine more closely what value indicates a genuine justification for an event to be generated and for an event notification to be sent to your pager or email address. For example, you might want to receive event notifications every time a certain attribute reaches a `warninghigh` severity threshold level. For more information, see "Setting Up Event Notifications" on page 195.

For important or crucial attributes at your installation, you can set the `warninghigh` threshold level to a low percentage value so that you are notified about a rising value as early as possible.

▼ To Retrieve Threshold Values for a Server

Before You Begin

To enable the management agent IP and security credentials on a server named *server*, add the management features on the server as explained in "Adding and Upgrading Base Management and OS Monitoring Features" on page 157.

Steps

1. **Log in to the N1 System Manager.**

   See "To Access the N1 System Manager Command Line" on page 28 for details.

2. **Type the `show server` command:**

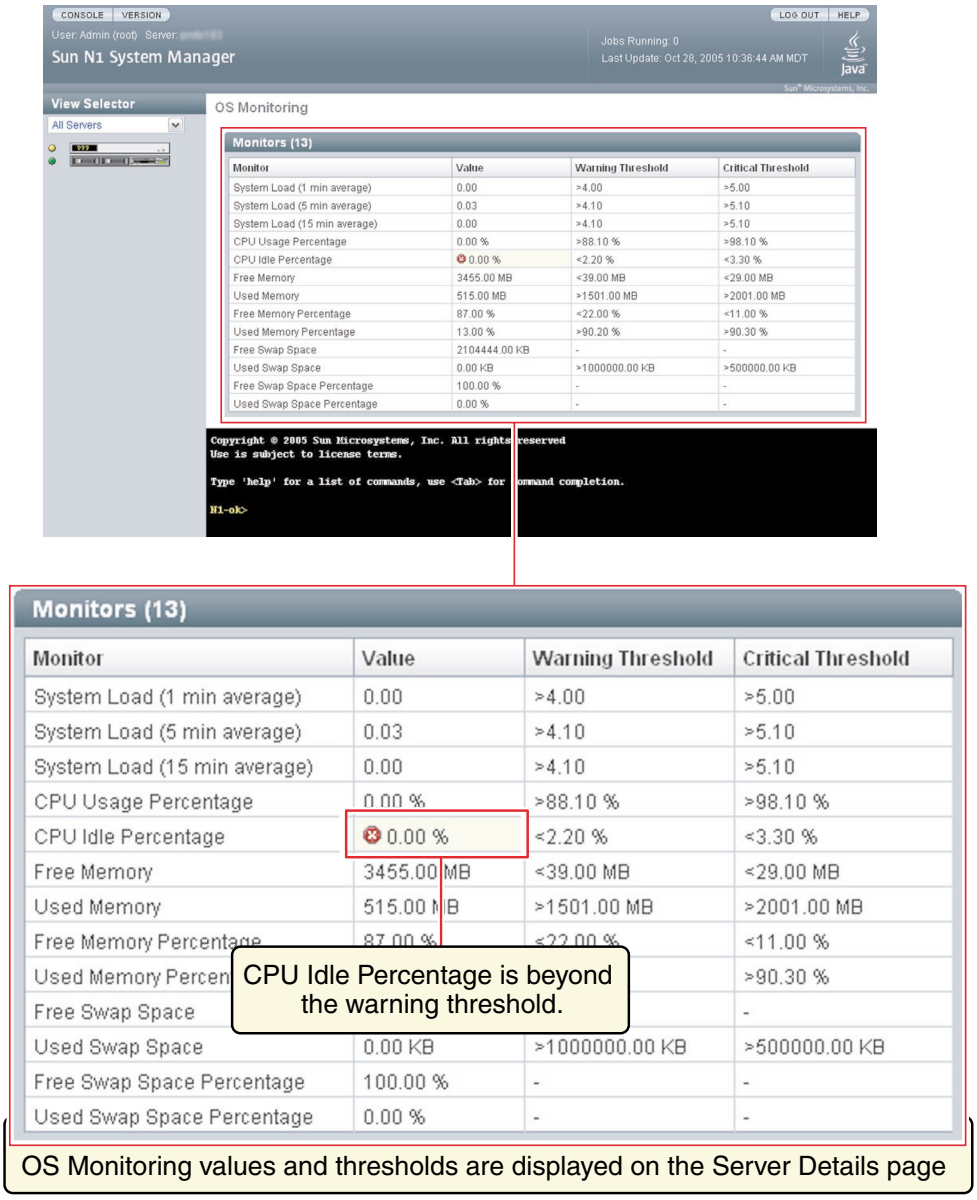
   ```
   N1-ok> show server server
   ```

   In this procedure, *server* is the name of the provisionable server for which you want to retrieve threshold values.

   Detailed monitoring threshold values appear in the output, including threshold information for the server's hardware health, OS health, and network reachability. Default values are shown if no specific values have been set.

   See "show server" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.

   - **Threshold information is also available from the Server Details page in the browser interface. This is shown in the following graphic.**



Managing Default Threshold Values

Factory-configured default threshold values are provided in the N1 System Manager software for some OS health thresholds. These values are stated as percentages. Table 5–1 lists default values for these OS health attributes for a Sun Fire V20z server.

Note – Setting or modifying threshold values for hardware health attributes is *not* supported in this version of the Sun N1 System Manager.

TABLE 5–1 Sun Fire V20zFactory-Configured Default Threshold Values for OS Health Attributes

Attribute Name	Description	Default Threshold	Default Threshold
`cpustats.loadavg1min`	System load expressed as average number of queued processes over 1 minute	`warninghigh` >4.00	`criticalhigh` >5.00
`cpustats.loadavg5min`	System load expressed as average number of queued processes over 5 minutes	`warninghigh` >4.10	`criticalhigh` >5.10
`cpustats.loadavg15min`	System load expressed as average number of queued processes over 15 minutes	`warninghigh` >4.10	`criticalhigh` >5.10
`cpustats.pctusage`	Percentage of overall CPU usage	`warninghigh` >80%	`criticalhigh` >90.1%
`cpustats.pctidle`	Percentage of CPU idle	`warninglow` <20%	`criticallow` <10%
`memusage.mbmemfree`	Memory free in MB	`warninghigh` <39%	`criticalhigh` <29%
`memusage.mbmemused`	Memory used in MB	`warninghigh` >1501	`criticalhigh` >2001
`memusage.pctmemused`	Percentage of memory in use	`warninghigh` >80%	`criticalhigh` >90%
`memusage.pctmemfree`	Percentage of memory free	`warninglow` <20%	`criticallow` <10%
`memusage.kbswapused`	Swap space in use in Kb	`warninghigh` >500000	`criticalhigh` >1000000
`fsusage.kbspacefree`	File system free space in Kb	`warninglow` <94.0Kb	`criticallow` <89.0Kb

Specific threshold values can be set at the command line by following the procedures described in "Setting Threshold Values" on page 180.

Table 5–2 provides the complete list of OS health attributes.

TABLE 5–2 All OS Health Attributes

Attribute Name	Description	Supported Threshold	Supported Threshold
`cpustats.loadavg1min`	System load expressed as average number of queued processes over 1 minute	`warninghigh`	`criticalhigh`
`cpustats.loadavg5min`	System load expressed as average number of queued processes over 5 minutes	`warninghigh`	`criticalhigh`
`cpustats.loadavg15min`	System load expressed as average number of queued processes over 15 minutes	`warninghigh`	`criticalhigh`
`cpustats.pctusage`	Percentage of overall CPU usage	`warninghigh`	`criticalhigh`
`cpustats.pctidle`	Percentage of CPU idle	`warninglow`	`criticallow`
`memusage.pctmemused`	Percentage of memory in use	`warninghigh`	`criticalhigh`
`memusage.pctmemfree`	Percentage of memory free	`warninglow`	`criticallow`
`memusage.mbmemused`	Memory in use in MB	`warninghigh`	`criticalhigh`
`memusage.mbmemfree`	Memory free in MB	`warninglow`	`criticallow`
`memusage.kbswapused`	Swap space in use in Kb	`warninghigh`	`criticalhigh`
`memusage.mbswapfree`	Free swap space in MB	`warninglow`	`criticallow`
`memusage.pctswapfree`	Percentage of free swap space	`warninglow`	`criticallow`
`fsusage.pctused`	Percentage of file system space in use	`warninghigh`	`criticalhigh`
`fsusage.kbspacefree`	File system free space in Kb	`warninghigh`	`criticalhigh`

Setting Threshold Values

Threshold values for OS health attributes can be set on specific servers. If you set specific threshold values at the command line for OS health attributes, that any factory-configured threshold values for the attributes.

▼ To Set Threshold Values for a Server

Before You Begin

To enable the management agent IP and security credentials on a server named *server*, add the management features on the server as explained in "Adding and Upgrading Base Management and OS Monitoring Features" on page 157.

Steps

1. **Log in to the N1 System Manager.**

   See "To Access the N1 System Manager Command Line" on page 28 for details.

2. **Use the `set server` command with the `threshold` attribute.**

   The syntax requires the `threshold` keyword to be followed by the *attribute* for which you are setting a threshold. The *attribute* is an OS health attribute. OS health attributes are described in "OS Health Monitoring" on page 153 and listed in Table 5–2.

   The *threshold* is either `criticallow`, `warninglow`, `warninghigh`, or `criticalhigh`. The value is a numeric figure and usually represents a percentage.

   This `set server` operation does not actually touch the provisionable server. It just synchronizes the data on the management server itself.

   - **To set one threshold value, type the following:**

     `N1-ok>` **`set server`** *server* **`threshold`** *attribute threshold value*

   - **To set multiple threshold values for the server, type the following:**

     `N1-ok>` **`set server`** *server* **`threshold`** *attribute threshold value threshold value*

   - **For a server group, use the `set group` command with the `threshold` attribute. To modify one threshold for the server group:**

     `N1-ok>` **`set group`** *group* **`threshold`** *attribute threshold value*

   - **To modify multiple thresholds for the server group:**

     `N1-ok>` **`set group`** *group* **`threshold`** *attribute threshold value threshold value*

Example 5–2 Setting Multiple Threshold Values for CPU Percentage Usage on a Server

This example shows how to set the CPU usage `warninghigh` severity threshold on a provisionable server named `serv1` to 53 percent. This example also shows how to set the `criticalhigh` severity threshold value to 75 percent.

```
N1-ok> set server serv1 threshold cpustats.pctusage warninghigh 53 criticalhigh 75
```

Example 5–3 Setting Multiple Threshold Values for File System Percentage Usage On a Server

This example sets the file system percentage usage `warninghigh` threshold on a provisionable server named `serv1` to 75 percent. This example also sets the `criticalhigh` threshold value to 87 percent. This example sets the threshold for *every file system* on the server.

```
N1-ok> set server serv1 threshold fsusage.pctused warninghigh 75 criticalhigh 87
```

You can also *specify* the file system for which you want to set multiple threshold values. To set the `warninghigh` threshold to 75 percent and the `criticalhigh` threshold value to 87 percent, for the `/usr` file system on the same server, use the `filesystem` attribute:

```
N1-ok> set server serv1 filesystem /usr threshold fsusage.pctused
warninghigh 75 criticalhigh 87
```

Example 5–4 Setting a Threshold Value for File System Free Space On a Server

This example sets the `warninghigh` threshold for file system free space for the `/var` file system on a provisionable server named `serv1` to 150 Kbytes of free space.

```
N1-ok> set server serv1 filesystem /var threshold fsusage.kbspacefree warninghigh 150
```

Example 5–5 Setting a Threshold Value for Percentage of Free Memory On a Server

This example sets the `criticalhigh` threshold for the percentage of free memory on a provisionable server named `serv1` to 5%.

```
N1-ok> set server serv1 threshold memusage.pctmemused criticalhigh 5
```

Example 5–6 Deleting a Threshold Value for File System Percentage Usage on a Server

This example shows how to delete a value that was set for the `warninghigh` threshold on a provisionable server named `serv1`.

```
N1-ok> set server serv1 threshold fsusage warninghigh none
```

In this case, any previously set value for this threshold at this severity is deleted. In effect, monitoring is disabled for the `warninghigh` threshold for file system usage for this server.

Example 5–7 Setting Multiple Threshold Values for File System Usage on a Server Group

This example shows how to set the file system usage `warninghigh` threshold to 75 percent on a group of provisionable servers with a group name of `grp3`. This example also shows how to set the `criticalhigh` threshold severity value to 87 percent.

```
N1-ok> set group grp3 threshold fsusage.pctused warninghigh 75 criticalhigh 87
```

Monitoring MIBs

Two MIBS are provided with the N1 System Manager. These MIBs provide the data structure that third-party monitoring tools can use to retrieve the data from the N1 System Manager using SNMP, and provide the data structure that third party monitoring tools can use to parse the SNMP notifications generated by the N1 System Manager. The MIBs can be found at `/opt/sun/n1gc/etc/`. These MIBs therefore enable you to use any SNMP client to query the N1 System Manager, and to listen for events using SNMP. The following MIBs are provided:

SUN-N1SM-INFO-MIB	This MIB describes the information that you can retrieve from the N1 System Manager by querying it using an SNMP client.
SUN-N1SM-TRAP-MIB	This MIB describes all of the events related to the N1 System Manager about which you can receive SNMP traps.

These MIBs are read-only. Using them requires a detailed knowledge of SNMP, although detailed descriptions of each object are provided in the MIBs. How you configure your monitoring system to start receiving traps depends on the nature of your monitoring system.

The MIBs are hardware independent.

EXAMPLE 5–8 Receiving SNMP Traps

This example shows you how to use the simple UNIX trap listener, the `snmptrapd` command, to start receiving N1 System Manager traps.

```
# snmptrapd -m all -M /opt/sun/n1gc/etc:/usr/share/snmp/mibs -P
```

This example uses the `snmptrapd` command to start monitoring on default port 162 for SNMP traps. It also instructs the command to use the MIBs stored at `/opt/sun/n1gc/etc` and `/usr/share/snmp/mibs` to parse the contents of SNMP traps.

Managing Jobs

This section describes jobs and their integral role in of server monitoring.

Each major action you take in the N1 System Manager starts a job. Use the job log to track the status on a currently running action or to verify that a job has finished. Monitoring jobs is useful particularly because some N1 System Manager actions can take a long time to finish. An example of such an action is installing an OS distribution on one or more provisionable servers.

You can track jobs through the Jobs tab in the browser interface or the `show job` command. The `show job` command provides information about most of the following characteristics:

Job ID Generated unique identifier.

Date Date on which the job was started.

Job Type Type of job. See "show job" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details. When using the `show job` command with the `type` parameter, jobs can be any of the following types:

- `addbase` – Add base management support.
- `addosmonitor` – Add OS monitoring support.
- `createos` – Create OS distribution from CD/DVD media or ISO files.
- `deletejob` – Delete job.
- `discover` – Server discovery.
- `loadfirmware` – Load firmware update.
- `loados` – Load OS.
- `loadupdate` – Load OS update.
- `refresh` – Server refresh.
- `reset` – Server reboot.
- `removeosmonitor` – Remove OS monitoring support.
- `setagentip` – Modify management feature configuration. Related to the base management and OS monitoring features.
- `start` – Server power on.
- `startcommand` – Remote command execution.
- `stop` – Server power off.
- `unloadupdate` – Unload OS update.

State State of the current job step. Job steps indicate the progress of a job and update results. Each job step has a type, a start time and, when the job completes, a completion time. For the purposes of filtering, job progress is indicated with the following states:

`notstarted` Jobs in a `notstarted` state cannot be stopped.

`preflight`	When you select a job by ID and view the details of that job, each step of that job can appear twice:the preflight check and the execution of the step itself.
`running`	The job is currently running. Jobs that are currently running cannot be deleted using the `delete job` command. Jobs that are currently running must finish running or be stopped using the `stop job` command.

Job completion is indicated with the following results:

`completed`	Indicates that the job step completed successfully.
`warning`	Indicates a warning during the job execution. A warning can be an issue reported that might be severe enough to terminate the job step, and the job, with errors.
`stopped`	Indicates that the job step stopped before it completed.
`pendingstop`	Indicates that the job is still running but that the job step cannot complete successfully.
`error`	Indicates a general error in that job step.
`timed_out`	Indicates that the job timed out before all of the job steps could complete successfully, or that the next step of the job started before the current step completed successfully.

`Complete - Warning` is issued in the output for an overall job status, if the job successfully completed all of its steps one or more `WARNING` states were issued for steps during the job execution and these warnings were not severe enough to terminate the job with errors.

You can filter jobs depending on their state. See "show job" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.

Command The command that was used to start the job.

Owner The user who started the job. Also called the job *creator*.

Job Results Provides details about the results of a completed job. You can review the standard output of remote command operations and completion statuses for all other job types.

▼ To List Jobs

Steps

1. **Log in to the N1 System Manager.**

   See "To Access the N1 System Manager Command Line" on page 28 for details.

2. **View the list of jobs.**

   ```
   N1-ok> show job all
   ```

   A list of all jobs for the N1 System Manager is returned.

   See "show job" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.

Example 5–9 Listing All Jobs

This example shows that using the `show job` command with the `all` option returns a list of jobs by Job ID, together with the date and time at which the job was started. The job type and status are also returned, along with the identity of the user who created the job.

```
N1-ok> show job all
Job ID          Date                        Type                Status        Owner
7               2005-09-16T10:51:07-0700    Discovery           Completed      root
6               2005-09-14T14:42:52-0700    Server Reboot       Error          root
5               2005-09-14T14:38:25-0700    Server Power On     Completed      root
4               2005-09-14T14:29:20-0700    Server Power Off    Completed      root
3               2005-09-09T13:01:35-0700    Discovery           Completed      root
2               2005-09-09T12:38:16-0700    Discovery           Completed      root
1               2005-09-09T10:32:40-0700    Discovery           Completed      root
```

▼ To View a Specific Job

Steps

1. **Log in to the N1 System Manager.**

   See "To Access the N1 System Manager Command Line" on page 28 for details.

2. **View a specific job.**

   ```
   N1-ok> show job job
   ```

   Detailed information about the job appears in the output.

   See "show job" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.

Example 5–10 Viewing Job Details

This example shows that using the `show job` command with the Job ID returns the date and time at which the job was started, the job type and status, and the identity of the user who created the job. The job in this example is to load an OS profile on a server named `192.168.200.4` using the `load server` command. Further details are provided for each *step* of that job, including the time at which the step started and completed and whether the step was successful.

```
N1-ok> show job 21
Job ID:   21
Date:     2005-10-27T10:09:18-0600
Type:     Load OS
Status:   Completed (2005-10-27T10:37:23-0600)
Command:  load server 192.168.200.4 osprofile SLES9RC5
bootip=192.168.200.30 networktype=static ip=192.168.200.31
Owner:    root
Errors:   0
Warnings: 0

Steps
ID     Type             Start                      Completion                 Result
1      Acquire Host     2005-10-27T10:09:19-0600   2005-10-27T10:09:19-0600   Completed
2      Execute Java     2005-10-27T10:09:19-0600   2005-10-27T10:09:19-0600   Completed
3      Acquire Host     2005-10-27T10:09:21-0600   2005-10-27T10:09:21-0600   Completed
4      Execute Java     2005-10-27T10:09:21-0600   2005-10-27T10:37:22-0600   Completed

Results
Result 1:
Server:   192.168.200.4
Status:   0
Message:  OS deployment using OS Profile SLES9RC5 was successful.
IP address 192.168.200.30 was assigned.
```

▼ To Stop a Job

Steps

1. **Log in to the N1 System Manager.**
   See "To Access the N1 System Manager Command Line" on page 28 for details.

2. **Stop a specific job.**

   ```
   N1-ok> stop job job
   ```

   The job is stopped.

   See "stop job" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.

3. **View the job details.**

   ```
   N1-ok> show job job
   ```

   The Result section of the output shows that the job was stopped.

   Any job can be stopped. In practice, however, only a job that is not in its last step can be stopped. Some jobs only have one step and so can never be stopped. Jobs in a `notstarted` state cannot be stopped. Operations that are performed on large groups of servers can take longer and might include a large number of steps.

   See "show job" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.

Example 5–11 Stopping a Job

This example shows that using the `stop job` command with the Job ID returns a message confirmed that the request has been received.

```
N1-ok> stop job 32

Stop Job "32" request received.
```

This example also shows that the `show job` command can be used with the Job ID of the job that was stopped to gain more data about the job that was stopped. The command returns the confirmation, in `Status`, that the job was stopped, and the command that was used to create the job. Further details are provided for each *step* of that job, including the time at which the step started and completed and whether the step was successful. The `Result` section shows that the job was stopped.

```
N1-ok> show job 32
Job ID:   32
Date:     2005-11-02T08:08:37-0700
Type:     Server Refresh
Status:   Stopped (2005-11-02T08:08:48-0700)
Command:  set server 192.168.200.2 refresh
Owner:    root
Errors:   0
Warnings: 0

Steps
ID   Type           Start                      Completion                 Result
1    Acquire Host   2005-11-02T08:08:38-0700   2005-11-02T08:08:38-0700   Completed
2    Run Command    2005-11-02T08:08:38-0700   2005-11-02T08:08:38-0700   Completed
3    Acquire Host   2005-11-02T08:08:40-0700   2005-11-02T08:08:40-0700   Completed
4    Run Command    2005-11-02T08:08:40-0700   2005-11-02T08:08:47-0700   Stopped
```

See Also "To Issue Remote Commands on a Server or a Server Group" on page 134

▼ To Delete a Job

Steps

1. **Log in to the N1 System Manager.**

   See "To Access the N1 System Manager Command Line" on page 28 for details.

2. **Determine the job you want to delete.**

   ```
   N1-ok> show job all
   ```

   All jobs and job IDs appear in the output.

   See "show job" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.

3. **Delete the desired job.**

   ```
   N1-ok> delete job job
   ```

   The job is deleted.

   See "delete job" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.

4. **Verify that the job was deleted.**

   ```
   N1-ok> show job all
   ```

   The deleted job should not appear in the output.

   See "show job" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.

Example 5–12 Deleting a Job

This example shows how to delete a job.

First, the `show job` command is used with the `all` option, which lists all jobs in descending order.

```
N1-ok> show job all
Job ID     Date                       Type               Status        Creator
7          2005-02-16T10:51:07-0700   Discovery          Completed     root
6          2005-02-14T14:42:52-0700   Server Reboot      Error         root
5          2005-02-14T14:38:25-0700   Server Power On    Completed     root
4          2005-02-14T14:29:20-0700   Server Power Off   Completed     root
3          2005-02-09T13:01:35-0700   Discovery          Completed     root
2          2005-02-09T12:38:16-0700   Discovery          Completed     root
1          2005-02-09T10:32:40-0700   Discovery          Completed     root
```

Job ID 6 has an error and can be deleted. The `delete job` command is now used with the Job ID of the job to be deleted.

```
N1-ok> delete job 6
```

The `show job` command is used again with the `all` option, which lists all jobs in descending order. The deleted job no longer appears on the list.

```
N1-ok> show job all
Job ID     Date                        Type               Status        Creator
7          2005-02-16T10:51:07-0700    Discovery          Completed     root
5          2005-02-14T14:38:25-0700    Server Power On    Completed     root
4          2005-02-14T14:29:20-0700    Server Power Off   Completed     root
3          2005-02-09T13:01:35-0700    Discovery          Completed     root
2          2005-02-09T12:38:16-0700    Discovery          Completed     root
1          2005-02-09T10:32:40-0700    Discovery          Completed     root
```

Example 5–13 Deleting All Jobs

This example shows how to delete all jobs.

First, the `show job` command is used with the `all` option, which lists all jobs in descending order.

```
N1-ok> show job all
Job ID     Date                        Type               Status        Creator
7          2005-09-16T10:51:07-0700    Discovery          Completed     root
6          2005-09-14T14:42:52-0700    Server Reboot      Error         root
5          2005-09-14T14:38:25-0700    Server Power On    Completed     root
4          2005-09-14T14:29:20-0700    Server Power Off   Completed     root
3          2005-09-09T13:01:35-0700    Discovery          Running       root
2          2005-09-09T12:38:16-0700    Discovery          Completed     root
1          2005-09-09T10:32:40-0700    Discovery          Completed     root
```

The `delete job` command is now used with the `all` option, to delete all jobs.

```
N1-ok> delete job all

Unable to delete job "3"
```

The `show job` command is used with the `all` option, to confirm whether all jobs were successfully deleted.

```
N1-ok> show job all
Job ID     Date                        Type             Status     Creator
3          2005-09-09T13:01:35-0700    Discovery        Running    root
```

Job ID 3 is still running. This is because jobs that were in a `running` state when the `delete job` command was issued must finish running, or must be stopped, before they can be deleted.

To stop the job and then delete it, first the `stop job` command is used with the ID of the job to be stopped.

```
N1-ok> stop job 3

Stop Job "3" request received.
```

The `show job` command is used to confirm that the job has been stopped.

```
N1-ok> show job all
Job ID     Date                        Type             Status        Creator
3          2005-09-09T13:02:35-0700    Discovery        Aborted       root
```

The job has been stopped while running and is in the `aborted` state. The `delete job` command is now used with the `all` option, to delete all jobs.

```
N1-ok> delete job all
```

The `show job` command is used to confirm that all jobs have now been deleted.

```
N1-ok> show job all
Job ID     Date                       Type             Status        Creator
```

Job Queueing

Each type of job in the N1 System Manager has a weight associated with it. The weight is a reflection of the load created by the job on the system resources. There is also a global limit on how much total load can be placed on the system. The following table provides a listing of the weight for each type of (user level) job. The maximum load permitted is 5000.

TABLE 5–3 Job Weight Values

Task	Weight
OS Deployment	500
Package Deployment	500
Package Uninstall	500
Discovery	200
Firmware Deployment	500
Remote Command Execution	200
Job Deletion	400
Create OS	1000
Reset Server	200
Server Power Off	200
Server Power On	200
Server Refresh	200
Set Server Feature	200

TABLE 5–3 Job Weight Values *(Continued)*

Task	Weight
Remove Server	100
Add Server	100

The total load is the sum of the loads of all the current running jobs. The system will compare the current total load with the maximum permitted load at the following points in time:

- After enqueueing a new job
- After completion or stopping a running job

If the difference between the current total load and the maximum permitted load is great enough to accommodate the job at the head of the job queue, then that job is promoted to a running state. Otherwise, it is left in the queued state. The current total load governs the permissible concurrent running job mix within the system.

For example, only two OS Deployment jobs can be running at one time:

```
500 + 500 = 1000
```

Or only one OS Deployment job and two Server Power Off jobs can be running at one time:

```
500 + 200 + 200 < 1000
```

Managing Event Log Entries

This section describes events and their integral role in to monitoring your servers.

`Events` are generated when certain conditions related to attributes occur. Each event has an associated topic. For example, when a server is discovered by the management server, an event is generated with the topic `Action.Physical.Discovered`. For a complete list of event topics, see "create notification" in *Sun N1 System Manager 1.2 Command Line Reference Manual*.

Events can be monitored. Monitoring is connected with the broadcasting of events for each monitored server or group of servers. When a monitored attribute's value is beyond the default or user-defined threshold safe range, an event is generated and a status is issued.

- If monitoring is enabled for a server, provided a notification rule has been added for the event, the event causes a *notification* to be emitted from the management server for that event.

- If monitoring is disabled for a server, monitoring events are not generated for that server. You might want to disable monitoring of a hardware component to perform maintenance tasks without generating events.

See "Introduction to Monitoring" on page 145 for more information about monitoring.

See "Setting Up Event Notifications" on page 195 for more information about event notifications.

Lifecycle events continue to be generated even with monitoring disabled. *Lifecycle events* include server discovery, server change or deletion, or server group creation. If you have requested notification of this type of event, you can still receive notifications even with monitoring disabled.

Event logs are created when events occur. For example, if any monitored IP address is unreachable, an event is generated. This event creates an event log record, which is visible from the browser interface.

Note – Machines based on the Advanced Lights Out Manager (ALOM) standard use email to send event notifications to the management server. This must be configured as shown in "Configuring the Management Server Mail Service and Account" in *Sun N1 System Manager 1.2 Site Preparation Guide*. Troubleshooting information is provided in "Fixing Notifications From ALOM-based Servers" on page 231.

Event Log Overview

During the installation and configuration of the N1 System Manager, you can configure which events to log and you can also interactively configure severity levels for event topics. See "Configuring the N1 System Manager System" in *Sun N1 System Manager 1.2 Installation and Configuration Guide*.

Even if a log is not saved, it can still generate an event notification.

Use the `show log` command to view the following information about events:

- **Date** – The date and time of the event.
- **Subject** – The server on which the event occurred.
- **Topic** – The topic of the event, which can be useful for setting up event notifications. Refer to "Setting Up Event Notifications" on page 195 for information.
- **Severity** – Relative severity of the event.
- **Level** – Relative level of the event.
- **Source** – The name of the component that generated the event. For events that are generated during the execution of a job, the `source` is the job number.

- **Role** – Role or user name of the user who initiated the event.
- **Message** – Complete text of the event log message.

The `n1smconfig` script can be used to change the number of days for which event logs are kept. Reducing the number of days for which event logs are stored reduces the average size of the event log files. This task ensures that the event log file size does not impair performance. The `n1smconfig` script is stored at `/usr/bin` for both the Linux and Solaris OS platforms. This script can be used to set the number of days for which event logs are held. To configure event logging, specify an event category and a resource category. The following event categories are defined:

- `Action`
- `Ereport`
- `Lifecycle`
- `List`
- `Problem`
- `Statistic`
- `all`

Use the `all` event category to indicate that all events are to be logged. To understand how other event categories relate to actual events, see the event notification topics at "create notification" in *Sun N1 System Manager 1.2 Command Line Reference Manual*. General log files are saved to the `syslog` file at `/var/adm/messages` or `/var/log/messages`

▼ To View the Event Log

Steps

1. **Log in to the N1 System Manager.**

   See "To Access the N1 System Manager Command Line" on page 28 for details.

2. **Type the following command:**

   ```
   N1-ok> show log [count count]
   ```

   The Events log appears with events listed most recent first. The value for the `count` attribute is the number of events to show in the output. The default value for `count` is 500. See "show log" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.

See Also "Event Log Overview" on page 192

▼ To Filter the Event Log

Steps

1. **Log in to the N1 System Manager.**

   See "To Access the N1 System Manager Command Line" on page 28 for details.

2. **Type the following command:**

```
N1-ok> show log [after after] [before before] [count count] [severity severity]
```

The output shows only the events that match the specified criteria. The *before* or *after* variable values must be formatted appropriately, for example, `2005-07-20T11:53:04`. The possible values for severity are as follows:

- `unknown`
- `other`
- `information`
- `warning`
- `minor`
- `major`
- `critical`
- `fatal`

See "show log" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.

▼ To View Event Details

Steps

1. **Log in to the N1 System Manager.**

See "To Access the N1 System Manager Command Line" on page 28 for details.

2. **Type the following command:**

```
N1-ok> show log log
```

The details of the event appear in the output. The *log* variable is the log ID. See "show log" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.

Example 5–14 Viewing Event Details

```
N1-ok> show log 72
ID:       72
Date:     2005-03-15T13:35:59-0700
Subject:  RemoteCmdPlan
Topic:    Action.Logical.JobStarted
Severity: Information
Level:    FINE
Source:   Job Service
Role:     root
Message:  RemoteCmdPlan job initiated by root: job ID = 15.
```

Setting Up Event Notifications

The N1 System Manager provides the ability to set up email or SNMP event notifications when events occur, either within the N1 System Manager itself or when specific events occur on provisionable servers. You can set up customized event notification rules for as many different scenarios as you need. Setting up default notifications for events can be done using the `n1smconfig` utility at install time. See "Configuring the N1 System Manager System" in *Sun N1 System Manager 1.2 Installation and Configuration Guide* for more information about installing and configuring the N1 System Manager.

You can create additional event notifications at the command line. Use the `create notification` command to create event *notification rules* based on events that occur or might occur about which you are interested. Use a topic to create an event notification.

For setting up event notifications using SNMP traps, use the SNMP MIB located at `/opt/sun/n1gc/etc/SUN-N1SM-TRAP-MIB.mib`. For more information about SNMP MIBs, see "Monitoring MIBs" on page 182.

A notification rule can be used to send a notification of each type of event to a selected destination, using either email or SNMP as the communication medium. For example, you can create a notification rule so that each time a new provisionable server is discovered by the management server, you receive a message on your pager to indicate that the event has happened:

`create notification` *notification* **`destination`** *destination* **`topic`** *topic*
`type` *type* `[description` *description*`]`

See "create notification" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details of the terms used in this command syntax.

You can configure your SMTP server to use event notification, during the installation and configuration of the N1 System Manager. See "Configuring the N1 System Manager System" in *Sun N1 System Manager 1.2 Installation and Configuration Guide*.

Viewing and Modifying Event Notifications

Use the `show notification` and `set notification` commands to view and modify event notification details. Type `help show notification` or `help set notification` at the `N1-ok` command line for syntax and parameter details.

▼ To View Event Notifications

Steps

1. **Log in to the N1 System Manager.**

   See "To Access the N1 System Manager Command Line" on page 28 for details.

2. **Type the following command:**

   ```
   N1-ok> show notification all
   ```

   The event notifications for which you have read privileges appear in the output. See "show notification" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.

▼ To View Event Notification Details

Steps

1. **Log in to the N1 System Manager.**

   See "To Access the N1 System Manager Command Line" on page 28 for details.

2. **Type the following command:**

   ```
   N1-ok> show notification notification
   ```

   The specified event notification details appear in the output. See "show notification" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.

Example 5–15 Viewing Event Notification Details

This example shows how to use the `show notification` command to display the details about a notification.

```
N1-ok> show notification notif33
Name:          notif33
Event Topic:   EReport.Physical.ThresholdExceeded
Notifier Type: Email
Destination:   nobody@sun.com
State:         enabled
```

▼ To Modify an Event Notification

This procedure describes how to change the name, description, or destination of an event notification.

Steps

1. **Log in to the N1 System Manager.**

   See "To Access the N1 System Manager Command Line" on page 28 for details.

2. **Type the following command:**

```
N1-ok> set notification notification name name description description
 destination destination
```

The specified event notification attributes are set to the new values specified. See "set notification" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.

Example 5–16 Modifying an Event Notification Name

This example shows how to use the `set notification` command with the `name` option to change a notification name from `notif22` to `notif23`.

```
N1-ok> set notification notif22 name notif23
```

Creating, Testing, and Deleting Event Notifications

Use the `create notification` or `delete notification` commands to create and delete event notifications.

Use the `start notification` command with the `test` keyword to test an even notification.

Type `help create notification` or `help delete notification` at the `N1-ok` command line for syntax and parameter details.

▼ To Create and Test an Event Notification

Steps

1. **Log in to the N1 System Manager.**

See "To Access the N1 System Manager Command Line" on page 28 for details.

2. **Type the following command:**

```
N1-ok> create notification notification topic topic
type type destination destination
```

The event notification is created and enabled. See "create notification" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details and valid topics.

3. **Type the following command:**

```
N1-ok> start notification notification test
```

A test notification message is sent. See "start notification" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.

Example 5–17 Creating an Email Notification

This example shows how to create an event notification to be sent by email if a server group is created. Note that an SMTP email server must first be configured using the `n1smconfig` utility as described in "Configuring the N1 System Manager System" in *Sun N1 System Manager 1.2 Installation and Configuration Guide*.

The event notification is called `notif2`. The recipient's email address is `nobody@sun.com`

```
N1-ok> create notification notif2 destination nobody@sun.com
Lifecycle.Logical.CreateGroup type email
```

The `show notification` command can be used to verify that the event notification has been created.

```
N1-ok> show notification
Name    Event Topic                          Destination       State
notif2  EReport.Physical.ThresholdExceeded   nobody@sun.com    enabled
```

The event can be invoked by creating a false group, as a test.

```
N1-ok> create group test
```

An email should be sent if the notification was created successfully. Otherwsie, the following error message is displayed:

```
Notification test failed.
```

Verify if the SMTP server is configured correctly and is reachable, and if the email address used in the notification rule is valid.

Example 5–18 Creating an SNMP Notification

This example shows how to create an event notification to be sent by SNMP if a physical threshold value is exceeded. The event notification is called `notif3`. The recipient SNMP address is `sun.com`

```
N1-ok> create notification notif3 destination sun.com
topic EReport.Physical.ThresholdExceeded type snmp
```

The `show notification` command can be used to verify that the event notification has been created.

```
N1-ok> show notification
Name    Event Topic                          Destination  State
notif3  EReport.Physical.ThresholdExceeded   sun.com      enabled
```

You can specify the event notification you want to see by using `show notification`command with the notification attribute value.

```
N1-ok> show notification notif3
Name    Event Topic                          Destination  State
notif3  EReport.Physical.ThresholdExceeded   sun.com      enabled
```

▼ To Delete an Event Notification

Steps

1. **Log in to the N1 System Manager.**
   See "To Access the N1 System Manager Command Line" on page 28 for details.
2. **Type the following command:**

   ```
   N1-ok> delete notification notification
   ```

   The event notification is deleted.

Starting and Stopping Event Notifications

Event notifications are enabled, or *started*, by default at creation. Use the `start notification` command to enable an event notification that has been disabled. Type `help start notification` at the `N1-ok` command line for syntax and parameter details.

▼ To Start an Event Notification

Steps

1. **Log in to the N1 System Manager.**
   See "To Access the N1 System Manager Command Line" on page 28 for details.
2. **Type the following command:**

   ```
   N1-ok> start notification notification
   ```

   The event notification is enabled. See "start notification" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.

▼ To Stop an Event Notification

Steps

1. **Log in to the N1 System Manager.**
   See "To Access the N1 System Manager Command Line" on page 28 for details.
2. **Type the following command:**

   ```
   N1-ok> stop notification notification
   ```

   The event notification is disabled. See "stop notification" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for details.

CHAPTER 6

Troubleshooting

This chapter provides troubleshooting information on the following topics:

Discovery Problems

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

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

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

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

   ```
   sp get snmp-destinations
   ```

The SNMP destinations appear in the output.

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

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

Security Problems

This section provides security-based troubleshooting information.

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

The keys used by the N1 System Manager are stored under the `/etc/opt/sun/cacao/security` directory on each server where the servers are running Linux. For servers running the Solaris OS, these keys are stored under the `/etc/opt/SUNWcacao/security` directory.

Why Regenerate Security Keys?

The security keys used by the N1 System Manager must be identical across all servers. Under normal operation, the security keys used by the keys can be left in their default configuration. You might have to regenerate security keys from time to time:

- If there is a risk that the root password of the management server has been exposed or compromised, regenerate the security keys.
- If the system date on the management server has been changed using the `date` command, regenerate the security keys. If the system date on the management server has been changed using the `date` command, there is a risk that the next time the N1 System Manager management daemon, `n1sminit`, is restarted, no services are subsequently provided by the management server. In this case, keys

must be regenerated, and the N1 System Manager management daemon restarted, as explained in "How to Regenerate Common Agent Container Security Keys" on page 203.

▼ How to Regenerate Common Agent Container Security Keys

Steps

1. **On the management server as root, stop the N1 System Manager management daemon.**

   ```
   # /etc/init.d/n1sminit stop
   ```

2. **Regenerate security keys using the `create-keys` subcommand.**

   If the management server is running Linux:

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

   If the management server is running the Solaris OS:

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

3. **As root on the management server, restart the N1 System Manager management daemon.**

   ```
   # /etc/init.d/n1sminit start
   ```

General Security Considerations

The following list provides general 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 provisionable servers are automatically acknowledged by the N1 System Manager software. This automation might make the provisionable 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 System" in *Sun N1 System Manager 1.2 Installation and Configuration Guide* for details.

Troubleshooting OS Distributions

This section describes scenarios that cause OS deployment to fail and explains how to correct failures.

Distribution Copy Failures

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

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

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

Errors
Error 1:
Description: INFO   : Mounting /images/rhel-3-U4-i386-es-disc1.iso at
/mnt/loop23308
INFO   : Version is 3ES, disc is 1
INFO   : Version is 3ES, disc is 1
INFO   : type redhat ver: 3ES
cp: /var/opt/SUNWscs/data/allstart/image/3ES-bootdisk.img: Bad address
INFO   : Could not copy PXE file bootdisk.img
INFO   : umount_exit: mnt is: /mnt/loop23308
```

```
INFO   : ERROR: Could not add floppy to the Distro

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

In the above case, try copying a different set of distribution files to the management server. See "To Copy an OS Distribution From CDs or a DVD" on page 76 or "To Copy an OS Distribution From ISO Files" on page 75.

Mount Point Issues

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

Patching Solaris 9 Distributions

The inability to deploy Solaris 9 OS distributions to servers from a Linux management server is usually due to a problem with NFS mounts. To solve this problem, you need to apply a patch to the mini-root of the Solaris 9 OS distribution. This section provides instructions for applying the required patches. The instructions differ according to the management and patch server configuration scenarios in the following table.

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

Management Server	Patch Server	Task
Red Hat 3.0 u2	Solaris 9 OS on x86 platform	"To Patch a Solaris 9 OS Distribution by Using a Solaris 9 OS on x86 Patch Server" on page 206
Red Hat 3.0 u2	Solaris 9 OS on SPARC platform	"To Patch a Solaris 9 OS Distribution by Using a Solaris 9 OS on SPARC Patch Server" on page 208

Using a Provisionable Server to Patch OS Distributions

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

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

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

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

Before You Begin

- Create a Solaris 9 OS distribution on the management server. See "To Copy an OS Distribution From CDs or a DVD" on page 76 or "To Copy an OS Distribution From ISO Files" on page 75. Type `show os os-name` at the command line to view the ID of the OS distribution. This number is used in place of *DISTRO_ID* in the instructions.
- Install the Solaris 9 OS on x86 platform software on a machine that is not the management server.
- Create a `/patch` directory on the Solaris 9 x86 patch server.
- For a Solaris OS on x86 distribution, download and unzip the following patches into the `/patch` directory on the Solaris 9 OS on x86 patch server: 117172-17 and 117468-02. You can access these patches from `http://sunsolve.sun.com`.
- For a Solaris OS on SPARC distribution, download and unzip the following patches into the `/patch` directory on the Solaris 9 OS on x86 patch server: 117171-17, 117175-02, and 113318-20. You can also access these patches from `http://sunsolve.sun.com`.

Steps

1. **Patch the Solaris 9 OS on x86 patch server.**

   a. **Log in as root.**

   ```
   % su
   password:password
   ```

   The root prompt appears.

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

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

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

   ```
   # cd /patch
   ```

   d. **Install the patches.**

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

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

2. **Prepare to patch the distribution on the management server.**

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

   ```
   % su
   password:password
   ```

   The root prompt appears.

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

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

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

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

   e. **Restart NFS.**

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

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

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

   ```
   % su
   password:password
   ```

   The root prompt appears.

   b. **Mount the management server.**

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

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

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

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

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

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

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

d. **Unmount the management server.**

```
# unmount /mnt
```

4. **Restart NFS on the management server.**

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

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

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

   c. **Restart NFS.**

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

   NFS is restarted.

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

5. **Fix the Solaris 9 OS on x86 distribution.**

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

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

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

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

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

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

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

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

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

Before You Begin

- Create a Solaris 9 OS distribution on the management server. See "To Copy an OS Distribution From CDs or a DVD" on page 76 or "To Copy an OS Distribution From ISO Files" on page 75. Type `show os os-name` at the command line to view the ID of the OS distribution. This number is used in place of *DISTRO_ID* in the instructions.
- Install the Solaris 9 OS on SPARC software on a machine that is not the management server. See "To Load an OS Profile on a Server or a Server Group" on page 90.
- Create a `/patch` directory on the Solaris 9 SPARC patch server.
- For a Solaris OS on x86 distribution, download and unzip the following patches into the `/patch` directory on the Solaris 9 OS on x86 patch server: 117172-17 and 117468-02. You can access these patches from `http://sunsolve.sun.com`.
- For a Solaris OS on SPARC distribution, download and unzip the following patches into the `/patch` directory on the Solaris 9 OS on x86 patch server: 117171-17, 117175-02, and 113318-20. You can access these patches from `http://sunsolve.sun.com`.

Steps

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

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

```
% su
password:password
```

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

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

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

```
# cd /patch
```

d. Install the patches.

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

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

---

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

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

```
% su
password:password
```

b. Mount the management server.

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

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

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

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

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

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

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

---

d. **Unmount the management server.**

```
# unmount /mnt
```

3. **Restart NFS on the management server.**

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

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

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

c. **Restart NFS.**

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

NFS is restarted.

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

4. **Fix the Solaris 9 OS on x86 distribution.**

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

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

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

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

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

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

OS Profile Deployment Failures

Chapter 2, "Sun N1 System Manager System and Network Preparation," in *Sun N1 System Manager 1.2 Site Preparation Guide* recommends that the OS provisioning network be isolated. This is mainly due to the use of DHCP on the network and due to the high bandwidth consumed by provisioning operations.

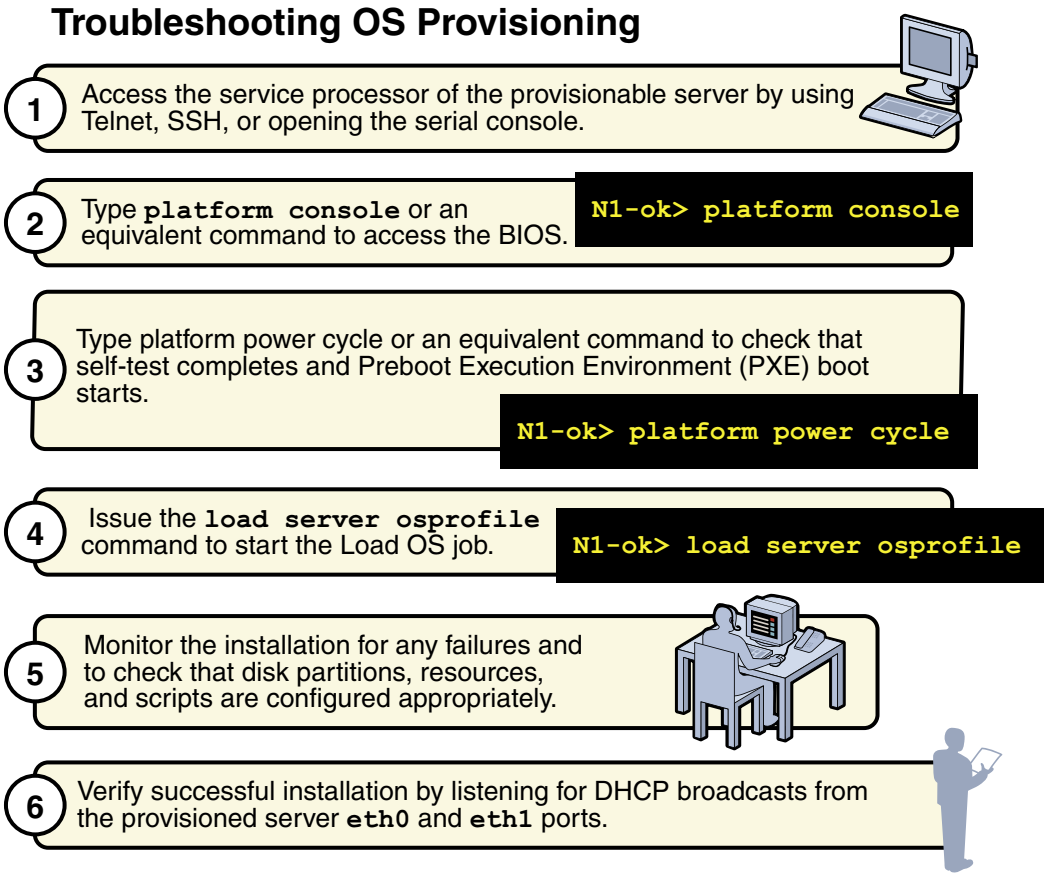
Since DHCP is a broadcast protocol it can cause conflicts on a network between DHCP servers. OS monitoring is also performed on the provisioning network. OS monitoring can consume significant network bandwidth in larger configurations.

It is also recommended that the management network hosts the hardware monitoring and management capabilities. However, if your business needs require that the networks be unified and you can configure your network to deal with the DHCP and bandwidth considerations outlined above, your site might not need to isolate the networks.

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

- Partitions are not modified to suit a Sun Fire V40z or SPARC V440 server. See "To Modify the Default Solaris OS Profile for a Sun Fire V40z or a SPARC v440 Server" on page 212.
- Scripts are not modified to install the driver needed to recognize the Ethernet interface on a Sun Fire V20z server. See "To Modify a Solaris 9 OS Profile for a Sun Fire V20z Server With a K2.0 Motherboard" on page 213.
- DHCP is not correctly configured. See "Solaris Deployment Job Times Out or Stops" on page 215.
- OS profile installs only the Solaris Core System Support distribution group. See "Solaris OS Profile Installation Fails" on page 216.
- The target server cannot access DHCP information or mount distribution directories. See "Invalid Management Server Netmask" on page 216.
- The management server cannot access files during a Load OS operation. See "Restarting NFS to Resolve `Boot Failed` Errors" on page 218.
- The Linux deployment stops. See "Linux Deployment Stops" on page 216.
- The Red Hat deployment fails. See "Red Hat OS Profile Deployment Failures" on page 217.

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



▼ To Modify the Default Solaris OS Profile for a Sun Fire V40z or a SPARC v440 Server

This procedure describes how to modify the Solaris OS profile that is created by default. The following modification is required for successful installation of the default Solaris OS profile on a Sun Fire V40z or a SPARC v440 server.

Steps **1. Log in to the N1 System Manager.**

See "To Access the N1 System Manager Command Line" on page 28 for details.

2. **Clone the default profile.**

```
N1-ok> create osprofile sol10v40z clone sol10
```

3. **Remove the root partition.**

```
N1-ok> remove osprofile sol10v40z partition /
```

4. **Remove the swap partition.**

```
N1-ok> remove osprofile sol10v40z partition swap
```

5. **Add new root parameters.**

```
N1-ok> add osprofile sol10v40z partition / device c1t0d0s0 sizeoption free
 type ufs
```

6. **Add new swap parameters.**

```
N1-ok> add osprofile sol10v40z partition swap device c1t0d0s1 size 2000
 type swap sizeoption fixed
```

See Also To find out how to load the modified OS profile, see "To Load an OS Profile on a Server or a Server Group" on page 90.

▼ To Modify a Solaris 9 OS Profile for a Sun Fire V20z Server With a K2.0 Motherboard

This procedure describes how to create and add a script to your Solaris OS profile. This script installs the Broadcom 5704 NIC driver needed for Solaris 9 x86 to recognize the NIC Ethernet interface on a Sun Fire V20z server with a K2.0 motherboard. Earlier versions of the Sun Fire V20z server use the K1.0 motherboard. Newer versions use the K2.0 motherboard.

Note – This patch is needed for K2.0 motherboards but can also be used on K1.0 motherboards without negative consequences.

Steps

1. **Log in to the N1 System Manager.**
   See "To Access the N1 System Manager Command Line" on page 28 for details.

2. **Type the following command:**

```
% /opt/sun/n1gc/bin/n1sh show os
```

   The list of available OS distributions appears.

3. **Note down the `ID` for the Solaris 9 distribution.**
   You use this ID, which is in fact the `DISTRO_ID` of the OS, in the next step.

4. **Type the following command:**

   ```
   # mkdir /js/DISTRO_ID/patch
   ```

   Here, `distro_id` is the ID you noted previously. A patch directory is created for the Solaris 9 distribution.

5. **Download the 116666-04 patch from `http://sunsolve.sun.com` to the `/js/`*DISTRO_ID*`/patch` directory.**

6. **Change to the `/js/`*DISTRO_ID*`/patch` directory.**

   ```
   # cd /js/DISTRO_ID/patch
   ```

7. **Unzip the patch file.**

   ```
   # unzip 116666-04.zip
   ```

8. **Type the following command:**

   ```
   # mkdir /js/scripts
   ```

9. **In the `/js/scripts` directory, create a script called `patch_sol9_k2.sh` that includes the following three lines:**

   ```
   #!/bin/sh
   echo "Adding patch for bge devices."
   patchadd -R /a -M /cdrom/patch 116666-04
   ```

   Note – Ensure the script is executable. You can use the `chmod 775 patch_sol9_k2.sh` command.

   ---

10. **Add the script to the Solaris 9 OS profile.**

    ```
    N1-ok> add osprofile osprofile script /js/scripts/patch_sol9_k2.sh type post
    ```

Example 6–1 Adding a Script to a Solaris OS Profile

This example shows how to add a script to an OS profile. The `type` attribute specifies that the script is to be run after the installation.

```
N1-ok> add osprofile sol9K2 script /js/scripts/patch_sol9_k2.sh
type post
```

Next Steps To load the modified Solaris OS profile, see "To Load an OS Profile on a Server or a Server Group" on page 90.

Solaris Deployment Job Times Out or Stops

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

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

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

Note – The best diagnostic tool is to open a console window on the target machine and then run the deployment. See "To Open a Server's Serial Console" on page 138.

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

▼ To Modify the Network Interface Configuration

Steps

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

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

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

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

   The `n1smconfig` utility appears.

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

   See "Configuring the N1 System Manager System" in *Sun N1 System Manager 1.2 Installation and Configuration Guide* for detailed instructions.

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

Solaris OS Profile Installation Fails

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

Invalid Management Server Netmask

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

```
Booting kernel/unix...
  krtld: Unused kernel arguments: 'install'.
  SunOS? Release 5.10 Version Generic 32-bit
  Copyright 1983-2005 Sun Microsystems, Inc.  All rights reserved.
  Use is subject to license terms.
  Unsupported Tavor FW version: expected: 0003.0001.0000, actual: 0002.0000.0000
  NOTICE: tavor0: driver attached (for maintenance mode only)
  Configuring devices.
  Using DHCP for network configuration information.
  Beginning system identification...
  Searching for configuration file(s)...
  Using sysid configuration file /sysidcfg
  Search complete.
  Discovering additional network configuration...
  Completing system identification...
  Starting remote procedure call (RPC) services: done.
  System identification complete.
  Starting Solaris installation program...
  Searching for JumpStart directory...
  /sbin/dhcpinfo: primary interface requested but no primary interface is set
  not found
  Warning: Could not find matching rule in rules.ok
  Press the return key for an interactive Solaris install program...
```

To fix the problem, set the management server netmask value to `255.255.255.0`. See "To Configure the N1 System Manager System" in *Sun N1 System Manager 1.2 Installation and Configuration Guide*.

Linux Deployment Stops

If you are deploying a Linux OS and the deployment stops, check the console of the target server to see if the installer is in interactive mode. If the installer is in interactive mode, the deployment timed out because of a delay in the transmission of data from

the management server to the target server. This delay usually occurs because the switch or switches connecting the two machines has `spanning tree` enabled. Either turn off `spanning tree` on the switch or disable `spanning tree` for the ports that are connected to the management server and the target server.

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

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

Red Hat OS Profile Deployment Failures

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

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

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

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

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

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

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

Restarting NFS to Resolve `Boot Failed` Errors

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

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

On a Solaris system, type the following:

```
# /etc/init.d/nfs.server stop
# /etc/init.d/nfs.server start
```

On a Linux system, type the following:

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

Resolving Command Failures Related to OS Monitoring

Adding the feature might fail due to stale SSH entries on the management server. If the `add server server-name feature osmonitor agentip` command fails and no true security breach has occurred, remove the `/root/.ssh/known_hosts` file or the specific entry in the file that corresponds to the provisionable server. Then, retry the `add` command.

Additionally, adding the OS monitoring feature to a server that has the base management feature might fail. The following job output shows the error:

```
Repeat attempts for this operation are not allowed.
```

This error indicates that SSH credentials have previously been supplied and cannot be altered. To avoid this error, issue the `add server feature osmonitor` command without `agentssh` credentials. See "To Add the OS Monitoring Feature" on page 158 for instructions.

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

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

```
2 Run Command 2005-08-16T16:14:28-0400 2005-08-16T16:14:28-0400 Completed
3 Acquire Host 2005-08-16T16:14:29-0400 2005-08-16T16:14:30-0400 Completed
4 Run Command 2005-08-16T16:14:30-0400 2005-08-16T16:14:36-0400 Error

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

Checking for OS Monitoring Agents

If you tried to install the OS monitoring agents as described in "To Add the OS Monitoring Feature" on page 158 and OS monitoring data did not appear, verify that the OS monitoring feature was installed, as follows:

- It can take 5-7 minutes before all OS monitoring data is fully initialized. You may see that CPU idle is at `0.0`%, which causes a Failed Critical status with OS usage. This should clear up within 5-7 minutes after adding or upgrading the OS monitoring feature. At that point, OS monitoring data should be available for the provisionable server by using the `show server` *server* command.
- Use the `grep` command and try to see if indeed the agents themselves were successfully installed.

  To verify the Solaris feature, type the following commands:

  ```
  # pkginfo |grep n1sm

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

  To verify the Linux feature, type the following commands:

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

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

OS Update Problems

This section describes possible solutions for the following troubleshooting scenarios:

- "OS Update Creation Failures" on page 220
- "Solaris OS Update Deployment Failures" on page 221

■ "OS Update Uninstallation Failures" on page 225

OS Update Creation Failures

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

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

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

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

If you use an `adminfile` to install an OS update, ensure that the package file name matches the name of the package. If the file name does not match that of the package, and an `adminfile` is used to install the OS update, uninstallation will fail. See "OS Update Uninstallation Failures" on page 225.

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

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

For Solaris packages, a response file might also be needed. For instructions on how to specify an `admin` file and a `response` file when you create an OS update, see "To Copy an OS Update" on page 96.

Solaris OS Update Deployment Failures

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

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

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

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

Always check the package is targeted to the correct architecture.

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

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

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

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

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

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

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

The following are possible causes for Load Update job failures:

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

`error: Failed dependencies:`

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

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

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

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

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

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

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

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

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

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

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

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

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

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

`Job step failure without error details`

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

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

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

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

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

To manually install a patch, type the following command:

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

Then, run the `unload` command again.

`Job hangs`

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

To manually kill the job, type the following command:

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

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

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

Then run the `unload` command again.

Linux OS Update Deployment Failures

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

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

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

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

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

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

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

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

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

The following are possible causes for Load Update job failures:

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

`error: Failed dependencies:`

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

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

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

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

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

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

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

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

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

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

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

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

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

To manually install an RPM, type the following command:

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

Then, run the `unload` command again.

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

To manually kill the job, type the following command:

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

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

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

Then run the `unload` command again.

OS Update Uninstallation Failures

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

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

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

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

Downloading V20z and V40z Server Firmware Updates

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

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

Steps

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

   The `N1-ok` prompt appears.

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

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

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

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

   The Sun Fire V20z/V40z Server downloads page appears.

4. **Click Current Release.**

   The Sun Fire V20z/V40z NSV Bundles 2.3.0.11 page appears.

5. **Click Download.**

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

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

The Download page appears. Several downloadable files are displayed.

6. **To download the V20z firmware zip file, click V20z BIOS and SP Firmware, English (nsv-v20z-bios-fw_V2_3_0_11.zip).**

   Save the 10.21–Mbyte file to the directory that you created for the V20z firmware in Step 2.

7. **To download the V40z firmware zip file, click V40z BIOS and SP Firmware, English (nsv-v40z-bios-fw_V2_3_0_11.zip).**

   Save the 10.22–Mbyte file to the directory you created for the V40z firmware in Step 2.

8. **Change to the directory where you downloaded the V20z firmware file.**

   a. **Type `unzip` to unpack the file.**

      Type **`y`** to continue.

      The `sw_images` directory is extracted.

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

      - Service Processor:

        `sw_images/sp/spbase/V2.3.0.11/install.image`

      - BIOS

        `sw_images/platform/firmware/bios/ V2.33.5.2/bios.sp`

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

   a. **Type `unzip nsv-v40z-bios-fw_V2_3_0_11.zip` to unpack the zip file.**

      The `sw_images` directory is extracted.

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

      - Service Processor:

        `sw_images/sp/spbase/V2.3.0.11/install.image`

      - BIOS:

        `sw_images/platform/firmware/bios/V2.33.5.2/bios.sp`

Next Steps

- Copy the firmware updates to the N1 System Manager as described in "To Copy a Firmware Update" on page 106.
- Update the firmware on a single server or server group provisionable server as described in "To Load a Firmware Update on a Server or a Server Group" on page 108.

Downloading ALOM 1.5 Firmware Updates

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

▼ To Download and Prepare ALOM 1.5 Firmware

Steps

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

   The `N1-ok` prompt appears.

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

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

   ```
   # mkdir ALOM-firmware
   ```

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

   The downloads page appears.

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

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

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

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

   The files are extracted.

Next Steps

- Copy the firmware updates to the N1 System Manager as described in "To Copy a Firmware Update" on page 106.
- Update the firmware on a single server or server group provisionable server as described in "To Load a Firmware Update on a Server or a Server Group" on page 108.

Handling Threshold Breaches

If a threshold value is breached for a monitored attribute, an event is generated. You can create notification rules to warn you about this type of event. Notification of threshold breaches or warnings is done through the event log. This log is most easily viewed through the browser interface.

Notifications can be created using the `create notification` command and the resulting notification sent by email or to a pager. See "create notification" in *Sun N1 System Manager 1.2 Command Line Reference Manual* for syntax details.

Identifying Hardware and OS Threshold Breaches

If the value of a monitored hardware health attribute, or OS resource utilization attribute breaches a threshold value, an event log is immediately created, which indicates that the threshold has been breached. The event log is available from the browser interface. A symbol appears among the monitored data table in the browser interface to indicate that a threshold has been breached, as shows in the graphic at "To Retrieve Threshold Values for a Server" on page 176

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

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

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

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

Identifying Monitoring Failure

If monitoring is enabled, as described in "Enabling and Disabling Monitoring" on page 170, and the status in the output of the `show server` or `show group` commands is `unknown` or `unreachable`, then the server or server group is not being reached successfully for monitoring. If the status remains `unknown` or `unreachable`

for less than `30` minutes, it is possible that a transient network problem is occurring. However if the status remains `unknown` or `unreachable` for more than `10` minutes, it is possible that monitoring has failed. This could be the result of a failure in the monitoring feature. For more information, see "Resolving Command Failures Related to OS Monitoring" on page 218.

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

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

Problems After Rebooting or Restarting Services

If you reboot the management server, and the N1 System Manager services do not restart, you must regenerate security keys as explained in "Why Regenerate Security Keys?" on page 202.

If you stop the N1 System Manager services using the `n1sminit stop` command, and the services do not restart after using the `n1sminit start` command, you must regenerate security keys as explained in "Why Regenerate Security Keys?" on page 202.

Management Features Unavailable on Provisionable Servers After Rebooting

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

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

In this case, use the `set server` *server* `agentip` command to correct the server's agent IP address as shown in this procedure. See "To Modify the Agent IP for a Server" on page 162 for details.

Fixing Notifications From ALOM-based Servers

The ports of some models of provisionable servers use the Advanced Lights Out Manager (ALOM) standard. These servers, detailed in "Provisionable Server Requirements" in *Sun N1 System Manager 1.2 Site Preparation Guide*, use email instead of SNMP traps to send notifications about hardware events to the management server. For information about other events, see "Managing Event Log Entries" on page 191 and "Setting Up Event Notifications" on page 195.

To ensure that the management server receives event notifications from these servers, configure the management server, or another designated server that can be accessed by the N1 System Manager, as a mail server to receive notifications about hardware events from provisionable servers that use ALOM. This is explained in "Configuring the Management Server Mail Service and Account" in *Sun N1 System Manager 1.2 Site Preparation Guide* and "Configuring the N1 System Manager System" in *Sun N1 System Manager 1.2 Installation and Configuration Guide*.

If there are no notifications about hardware events from provisionable servers that use ALOM, it could mean that all managed servers are all healthy. However, it is also possible that the management server, or other designated server that can be accessed by the N1 System Manager, has not been configured correctly as an email server, or that email configuration has been invalidated due to other issues such as network error or domain name change.

If an email server has been configured, the problem might be that mail accounts have to be reset. The email accounts for provisionable servers may have been deleted or corrupted, or changes could have been made to the email server that impact its configuration, such as a change in the domain name or in a management network IP address.

To reset or change email addresses used by the management server, use the following procedure.

▼ To Reset Email Accounts for ALOM-based Provisionable Servers

The following procedure describes how to reset email accounts for provisionable servers. Following this procedure enables you to replace previous email addresses used by the management server with new addresses.

The email addresses you reset should be reserved for use only by the N1 System Manager.

Before You Begin

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

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

See "Discovering Servers" on page 51 for information about default `telnet` login and passwords for servers.

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

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

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

Steps

1. **Log in to the N1 System Manager.**

   See "To Access the N1 System Manager Command Line" on page 28 for details.

2. **Switch off monitoring for ALOM-based provisionable servers.**

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

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

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

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

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

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

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

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

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

---

4. **Switch on monitoring for the ALOM-based provisionable server.**

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

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

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

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

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

Index

E

F

G

H

I

J

L

P

R

S

T

U

V

W