Sun N1 System Manager 1.3 Discovery and Administration Guide

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

Part No: 819–5136
April 2006

060421@14774

Contents

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, manage groups of servers, set up monitoring, and set up notification rules.

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 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 1.3 Introduction*
- *Sun N1 System Manager 1.3 Site Preparation Guide*
- *Sun N1 System Manager 1.3 Installation and Configuration Guide*

How This Book Is Organized

Chapter 1 describes the following:

- How to access the N1 System Manager by using the command-line interface and the browser interface
- Showing and switching session roles

Chapter 2 describes the following:

- Adding and deleting users
- Creating and managing roles
- Privileges required for commands
- Security administrator rules

Chapter 3 describes how to backup and recover database and configuration files

Chapter 4 describes the following:

- How to choose a method of discovering servers
- How to discover servers through their service processors
- How to discover server through the IP of the operating system installed on the server
- How to discover servers manually
- How to troubleshoot server discovery

Chapter 5 describes the following:

- How to create groups of servers and how to manage servers and groups
- How to replace servers
- How to rename servers and groups
- How to start, stop and reset servers and groups
- How to remove servers and groups
- How to connect to a serial console for a server
- How to issue remote commands on a server

Chapter 6 describes the following:

- How monitoring works
- How to support monitoring by ensuring key features are installed
- How to enable or disable 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

Related Books

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

- *Sun N1 System Manager 1.3 Introduction*
- *Sun N1 System Manager 1.3 Site Preparation Guide*
- *Sun N1 System Manager 1.3 Installation and Configuration Guide*
- *Sun N1 System Manager 1.3 Operating System Provisioning Guide*
- *Sun N1 System Manager 1.3 Troubleshooting Guide*
- *Sun N1 System Manager 1.3 Command Line Reference Manual*
- *Sun N1 System Manager 1.3 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*.

TABLE P–1 Typographic Conventions *(Continued)*

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

Shell Prompts in Command Examples

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

TABLE P–2 Shell Prompts

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

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

Accessing the N1 System Manager

There are two ways to manage a rack of managed servers using the N1 System Manager:

- Through the command line. The default method is to use the `n1sh` shell, which uses an `N1–ok>` prompt.
- Through the browser interface. A web-based user interface is provided, that provides a subset of the command line features. The browser interface also includes the `n1sh` shell in the command line pane.

This chapter contains the following sections:

Accessing the N1 System Manager Through the Command Line

You can access the N1 System Manager using 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.

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.

For information about command line syntax, keywords, special characters, and general syntax, see "Command Line Interface Tips" in *Sun N1 System Manager 1.3 Command Line Reference Manual*.

▼ 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 20.

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 1.3 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 21 for more details about roles.

1 Log in to the N1 System Manager.

See "To Access the N1 System Manager Command Line" on page 14 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 21 for more details about roles and privileges.

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

   See "To Access the N1 System Manager Command Line" on page 14 for details.

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

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

   See "set session" in *Sun N1 System Manager 1.3 Command Line Reference Manual* for details.

To Exit the N1 System Manager Command Line

1. **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.

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

   See "To Access the N1 System Manager Command Line" on page 14 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
```

Accessing the N1 System Manager Through the Browser Interface

The N1 System Manager provides a web-based user interface that provides a subset of the command line features. This browser interface also includes the `n1sh` shell in a 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.

▼ 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 20.

The following browsers are supported:

- Mozilla™ 1.5 or later (for Solaris, Linux, or Microsoft Windows)
- Internet Explorer 6 or later (for Microsoft Windows)
- Mozilla Firefox 1.5 or later (for Linux or Microsoft Windows)
- Netscape Navigator 7.1 or later (for Linux or Microsoft Windows)

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.

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 1.3 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 1.3 Command Line Reference Manual* for details.

◆ ◆ ◆ CHAPTER 2

Managing Users and Roles

This chapter provides information about user and role management on the N1 System Manager.

This chapter contains the following sections:

Introduction to User Security

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

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 five system default roles, but customized roles can be created depending on your needs.

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. The `Admin` role is the account's default role. See Table 2–3 for details.

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

TABLE 2–1 Managing Users Quick Reference

Task	Command Syntax
"To Add an N1 System Manager User" on page 20	`# useradd -s n1sh user` `# n1sh create user` *user* `role` *role*
"To Delete an N1 System Manager User" on page 21	`# n1sh delete user` *user* `# userdel`
"To Set a User's Default Role (Normal Configuration)" on page 31	`set user` *user* `defaultrole` *defaultrole*
"To Show a User's Default Role" on page 33	`show user` *user*
"To Add a Role to a User" on page 34	`add user` *user* `role` *role*
"To Remove a Role From a User" on page 34	`remove user` *user* `role` *role*
"To List the Roles Added to a Specific User" on page 34	`show user` *user*

For more information about these commands, see *Sun N1 System Manager 1.3 Command Line Reference Manual*.

The N1 System Manager allows LDAP authentication using the Pluggable Authentication Module (PAM) subsystem. You can also use the LDAP PAM module on the management server if the management server is running either the Solaris OS or Linux.

▼ 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.

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 14 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 1.3 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.

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 14 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 1.3 Command Line Reference Manual.*

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

Managing Roles

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

TABLE 2–2 Managing Roles Quick Reference

Task	Command Syntax
"To Create a Role" on page 29	`create role` *role* `privilege` *privilege*
"To Delete a Role" on page 29	`delete role` *role*
"To Add a Privilege to a Role" on page 30	`add role` *role* `privilege` *privilege*
"To Remove a Privilege From a Role" on page 30	`remove role` *role* `privilege` *privilege*
"To List the Available Roles" on page 30	`show role all`
"To List Privileges Added to a Role" on page 31	`show role` *role*
"To List the Roles Added to All Users" on page 31	`show user all`
"To List the Available Privileges" on page 31	`show privilege all`

For more information about these commands, see *Sun N1 System Manager 1.3 Command Line Reference Manual*.

Table 2–3 lists the system default roles that are automatically provided by the N1 System Manager. These system default roles cannot be modified.

TABLE 2–3 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.

The following table lists the restricted mode roles that are automatically provided by the N1 System Manager. Unlike system default roles, these restricted mode roles *can* be modified, so that you can

create customized roles for your users to fit your organizational and business needs. For more information, see "Restricted Mode Capabilities" on page 47.

TABLE 2–4 Restricted Mode Roles

Role	Privileges	Description
`ProvAdmin`	`RoleRead`, `RoleWrite`, `UserRead`, `UserWrite`, `PrivilegeRead`	The N1 System Manager is configured so that it only has access to the provisioning network. See "Restricted Mode Capabilities" on page 47 for details.
`MgmtAdmin`	`RoleRead`, `RoleWrite`, `UserRead`, `UserWrite`, `PrivilegeRead`	The N1 System Manager is configured so that it only has access to the management network. See "Restricted Mode Capabilities" on page 47 for details.

The security administrator is responsible for assigning restricted mode roles to users if the N1 System Manager is configured such that it operates in restricted mode. For information about restricted mode of operation, see "Restricted Mode Capabilities" on page 47.

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

Users with the `SecurityAdmin` system default role (security administrators) are allowed to create new custom roles as needed in their organization, and can add 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 managed 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`. Then, the security administrator would add that role to those specific users. If `OSUpdateAdmin` is the only role added to the users, the users cannot access any part of the N1 System Manager other than the OS update management feature.

- If the N1 System Manager is configured so that it only has access to the provisioning network, the administrator should assign only the `ProvAdmin` restricted mode role to non-root users. See Table 2–4 for details about privileges for this role.
- If the N1 System Manager is configured so that it only has access to the management network, the administrator should assign only the `MgmtAdmin` restricted mode role to non-root users. See Table 2–4 for details about privileges for this role.

See "Restricted Mode Capabilities" on page 47 for details about the operation of the N1 System Manager in restricted mode.

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 or by adding new roles to their own user account. See "Security Administrator Rules" on page 28 for more details.

The following tables list 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 2–5 N1 System Manager Privileges for `add`, `connect`, and `create` Commands

Command	Privileges Required
`add group`	`GroupRead`
`add osprofile`	`OSProfileWrite`
	`OSProfileRead`
	`UpdateRead`
`add role`	`RoleWrite`
`add server`	`ServerRead`
	`ServerExecute`
	`JobRead`
`connect server`	`ServerConsole`
	`ServerRead`
	`UpdateRead`
`create firmware`	`FirmwareWrite`
`create group`	`GroupRead`
	`GroupWrite`
`create notification`	`NotificationRuleWrite`
`create os`	`OSWrite`
	`JobRead`
	`UpdateRead`
	`UpdateWrite`
`create osprofile`	`OSProfileWrite`
	`OSProfileRead`
	`UpdateRead`

TABLE 2–5 N1 System Manager Privileges for `add`, `connect`, and `create` Commands *(Continued)*

Command	Privileges Required
`create role`	`RoleWrite`
`create update`	`UpdateRead`
	`UpdateWrite`
`create user`	`UserWrite`

TABLE 2–6 N1 System Manager Privileges for `delete`, `discover` and `load` Commands

Command	Privileges Required
`delete firmware`	`FirmwareRead`
	`FirmwareWrite`
`delete group`	`GroupRead`
	`GroupWrite`
`delete job`	`JobWrite`
	`JobRead`
`delete notification`	`NotificationRuleWrite`
`delete os`	`OSWrite`
`delete osprofile`	`OSProfileWrite`
`delete role`	`RoleWrite`
`delete server`	`ServerWrite`
	`JobRead`
`delete update`	`UpdateRead`
	`UpdateWrite`
`discover`	`Discover`
	`JobRead`

TABLE 2–6 N1 System Manager Privileges for `delete`, `discover` and `load` Commands *(Continued)*

Command	Privileges Required
`load group`	`GroupRead`
	`FirmwareRead`
	`FirmwareWrite`
	`ServerDeployFirmware`
	`ServerDeployOS`
	`ServerDeployUpdate`
	`UpdateRead`
	`JobRead`
`unload group`	`GroupRead`
	`ServerDeployUpdate`
	`UpdateRead`
	`JobRead`
`load server`	`FirmwareRead`
	`FirmwareWrite`
	`ServerDeployFirmware`
	`ServerDeployOS`
	`ServerDeployUpdate`
	`JobRead`
`unload server`	`ServerDeployUpdate`
	`UpdateRead`
	`JobRead`

TABLE 2–7 N1 System Manager Privileges for `remove`, `set`, and `reset` Commands

Command	Privileges Required
`remove group`	`GroupWrite`
`remove osprofile`	`OSProfileWrite`
`remove role`	`RoleWrite`
`set firmware`	`FirmwareRead`
	`FirmwareWrite`

TABLE 2–7 N1 System Manager Privileges for `remove`, `set`, and `reset` Commands *(Continued)*

Command	Privileges Required
`set group`	`GroupRead`
	`GroupWrite`
`set group` *group* `refresh`	`ServerWrite`
	`JobRead`
`set notification`	`NotificationRuleRead`
	`NotificationRuleTest`
	`NotificationRuleWrite`
`set os`	`OSWrite`
`set osprofile`	`OSProfileWrite`
	`OSProfileRead`
	`UpdateRead`
`set role`	`RoleWrite`
`set server`	`ServerExecute`
	`ServerRead`
	`UpdateRead`
	`JobRead`
`set server` *server* `refresh`	`ServerWrite`
	`JobRead`
`reset server`	`ServerWrite`
	`JobRead`
`reset group`	`ServerWrite`
	`JobRead`

TABLE 2–8 N1 System Manager Privileges for `show`, `start` and `stop` Commands

Command	Privileges Required
`show firmware`	`FirmwareRead`
`show group`	`GroupRead`
`show job`	`JobRead`

TABLE 2–8 N1 System Manager Privileges for `show`, `start` and `stop` Commands *(Continued)*

Command	Privileges Required
`show log`	`LogRead`
`show notification`	`NotificationRuleRead`
`show privilege`	`None`
`show role`	`RoleRead`
`show os`	`OSRead`
`show osprofile`	`OSProfileRead`
	`UpdateRead`
`show server`	`ServerRead`
`show update`	`UpdateRead`
`show user`	`UserRead`
`start group`	`ServerWrite`
	`JobRead`
`start notification`	`NotificationRuleWrite`
`start server`	`ServerWrite`
	`JobRead`
`stop group`	`ServerWrite`
	`JobRead`
`stop job`	`JobWrite`
	`JobRead`
`stop server`	`ServerWrite`
	`JobRead`

For more information about these commands, see *Sun N1 System Manager 1.3 Command Line Reference Manual*.

Security Administrator Rules

Important rules for N1 System Manager security administrators are:

- 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 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.

▼ To Create a Role

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

1 Log in to the N1 System Manager.

See "To Access the N1 System Manager Command Line" on page 14 for details.

2 Create a new role with one or more privileges.

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

See "create role" in *Sun N1 System Manager 1.3 Command Line Reference Manual* for details. You can also use the `add role` command to add privileges to the role later.

▼ 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.

1 Log in to the N1 System Manager.

See "To Access the N1 System Manager Command Line" on page 14 for details.

2 Delete a role.

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

See "delete role" in *Sun N1 System Manager 1.3 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.

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

   See "To Access the N1 System Manager Command Line" on page 14 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 1.3 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 unrequired 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.

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

   See "To Access the N1 System Manager Command Line" on page 14 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 1.3 Command Line Reference Manual* for details.

▼ To List the Available Roles

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

   See "To Access the N1 System Manager Command Line" on page 14 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.

1. **Log in to the N1 System Manager.**
   See "To Access the N1 System Manager Command Line" on page 14 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 1.3 Command Line Reference Manual* for details.

Example 2–1 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

1. **Log in to the N1 System Manager.**
   See "To Access the N1 System Manager Command Line" on page 14 for details.

2. **List the roles that are added to all users.**
   ```
   N1-ok> show user all
   ```

▼ To List the Available Privileges

1. **Log in to the N1 System Manager.**
   See "To Access the N1 System Manager Command Line" on page 14 for details.

2. **List the available privileges.**
   ```
   N1-ok> show privilege all
   ```

▼ To Set a User's Default Role (Normal Configuration)

This task is based on the normal configuration of the N1 System Manager, where the management server has access to both the provisioning and management networks.

Users are automatically logged in to the N1 System Manager with their assigned user default role. The user default role can be a custom role that has been assigned as a default role to the user, and does not have to be a system default role. System default roles are shown in Table 2–3.

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. You can still set the `root` user's default role to a different role, but the assignment is not permanent.

---

1 Log in to the N1 System Manager.

See "To Access the N1 System Manager Command Line" on page 14 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 1.3 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 1.3 Command Line Reference Manual* for details.

If the N1 System Manager is running in normal configuration with access to both the provisioning and management networks, you can assign the `Admin` role as the default role for all users. Alternatively, you can create a custom role with the same privileges.

If the N1 System Manager is running in normal configuration with access to both the provisioning and management networks, any custom role you create for users must have the privileges necessary for full functionality of the N1 System Manager.

Example 2–2 Setting a User's Default Role

The following example shows how to set 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 Set a User's Role (Restricted Mode)

This task is based on the restricted mode configuration of the N1 System Manager, where the management server has access only to either the provisioning network or to the management network, but not to both networks.

Users are automatically logged in to the N1 System Manager with their assigned user default role. The user default role can be a custom role that has been assigned as a default role to the user, and does not have to be a system default role. System default roles are shown in Table 2–3.

1 Log in to the N1 System Manager.

See "To Access the N1 System Manager Command Line" on page 14 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 1.3 Command Line Reference Manual* for details.

3 Set a user's restricted mode role.

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

See "set user" in *Sun N1 System Manager 1.3 Command Line Reference Manual* for details.

- **For the restricted mode in which the N1 System Manager has access only to the management network, use the following command:**

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

- **For the restricted mode in which the N1 System Manager has access only to the provisioning network, use the following command:**

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

See Table 2–4 for details about privileges associated with these roles.

It is possible to delete or modify the `ProvAdmin` and `MgmtAdmin` restricted mode roles, but care should be taken that custom roles contain the correct privilege set for N1 System Manager to operate in restricted mode, for system stability. See "Restricted Mode Capabilities" on page 47 for details.

▼ To Show a User's Default Role

1 Log in to the N1 System Manager.

See "To Access the N1 System Manager Command Line" on page 14 for details.

2 Show a user's default role.

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

See "show user" in *Sun N1 System Manager 1.3 Command Line Reference Manual* for details.

Example 2–3 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

1 Log in to the N1 System Manager.

See "To Access the N1 System Manager Command Line" on page 14 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 1.3 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

1 Log in to the N1 System Manager.

See "To Access the N1 System Manager Command Line" on page 14 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 1.3 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

1 Log in to the N1 System Manager.

See "To Access the N1 System Manager Command Line" on page 14 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 1.3 Command Line Reference Manual* for details.

Example 2–4 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, and that the user has the `Admin` default role.

```
N1-ok> show user root

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

◆ ◆ ◆ CHAPTER 3

Backing Up and Restoring

This chapter provides information about backup and restore procedures for the management server's database and configuration files.

This chapter contains the following sections:

Backing Up Database and Configuration Files

This section describes how to back up the N1 System Manager database and configuration files. Successful completion of the procedure in this section enables you to swap management server and management server-related hardware without losing the N1 System Manager database and configuration files.

Note – Using the back up script provided in the N1 System Manager software as described in this section does not back up OS profiles.

▼ To Back Up 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 managed servers during the period between executing the backup and restore procedures.

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

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

See "To Access the N1 System Manager Command Line" on page 14 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 Database and Configuration Files" on page 39

Restoring N1 System Manager Database and Configuration Files

This section describes how to restore the N1 System Manager database and configuration files. Successful completion of the procedure in this section enables you to replicate the database and configuration files from one N1 System Manager installation to another installation.

▼ To Restore Database and Configuration Files

This procedure describes how to restore the N1 System Manager 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 should be 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

- To backup the database and configuration files, follow the instructions in "To Back Up Database and Configuration Files" on page 37.
- 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 1.3 Site Preparation Guide*, and the *Sun N1 System Manager 1.3 Installation and Configuration Guide* for details.

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

See "To Access the N1 System Manager Command Line" on page 14 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. 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 14 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" in *Sun N1 System Manager 1.3 Operating System Provisioning Guide* and "To Create an OS Profile" in *Sun N1 System Manager 1.3 Operating System Provisioning Guide*. For OS distributions and profiles based on the Microsoft Windows operating system, see Chapter 3, "Provisioning Windows Operating Systems," in *Sun N1 System Manager 1.3 Operating System Provisioning Guide*.

Alternatively, restore your previous OS distributions as described in "To Backup and Restore OS Distributions" on page 41.

▼ To Backup and Restore OS Distributions

1. **Using any file level backup and restore program, back up the following directories.**

   For Linux, back up the `/var/opt/sun/scs/share/allstart` directory.

   For the Solaris OS, back up the `/var/opt/SUNWscs/share/allstart` directory.

2. **Back up the `/tftpboot` directory for both Linux and the Solaris OS.**

3. **Restore the N1 System Manager as described in "To Restore Database and Configuration Files" on page 39.**

4. **Restore the directories described in steps 1 and 2.**

◆ ◆ ◆ CHAPTER 4

Discovering Manageable Servers

This chapter describes the ways to discover a manageable server using the N1 System Manager, how to choose which method of discovery use, and what level of service to expect from the N1 System Manager for a managed server, based on how the server was discovered.

To manage servers with the N1 System Manager, you must first allow the N1 System Manager to discover the manageable servers. Before the N1 System Manager discovers a server, the server is referred to as a manageable server. After it has been discovered, the server becomes a managed server.

This chapter contains the following sections:

Choosing a Method of Discovery

This section describes how to choose which method of discovery is best for your installation. The method you choose is related to how you have cabled and configured the N1 System Manager environment. For details on the configuration of the management network, see "Sun N1 System Manager Connection Information" in *Sun N1 System Manager 1.3 Site Preparation Guide*.

Note – If your installation provides only a management network, or only a provisioning network, the N1 System Manager must operate in restricted mode. See "Restricted Mode Capabilities" on page 47 for details.

The types of discovery available in this version of the N1 System Manager are as follows:

SP-Based Discovery — Discovery of a manageable server through its Service Processor (SP). Choose this method of discovery if you want the N1 System Manager to be

able to completely manage and monitor servers. Also, choose this method of discovery if your data center configuration allows the N1 System Manager to connect to both the provisioning and management networks.

See "SP-Based Discovery" on page 51 for details about this method of discovery.

OS-Based Discovery

Discovery of a manageable server using its operating system (OS). Choose this method of discovery for servers that are already running a supported OS.

If you require full manageability of servers, do not choose this method of discovery, because the N1 System Manager must run in *restricted mode* as described in "Restricted Mode Capabilities" on page 47. Consider configuring your data center's N1 System Manager installation so that the management server is connected to both the provisioning and management networks, which allows SP-based discovery to be used.

See "OS-Based Discovery" on page 59 for details about this method of discovery.

Manual Discovery

Discovery of a manageable server manually, using its MAC address and model name. Choose this method if you want to discover servers that satisfy the following conditions:

- The server does not have an installed OS.
- You cannot access the server's service processor and are therefore unable to use SP-based discovery.
- The server hardware appears in the supported hardware list. See "Manageable Server Requirements" in *Sun N1 System Manager 1.3 Site Preparation Guide*.

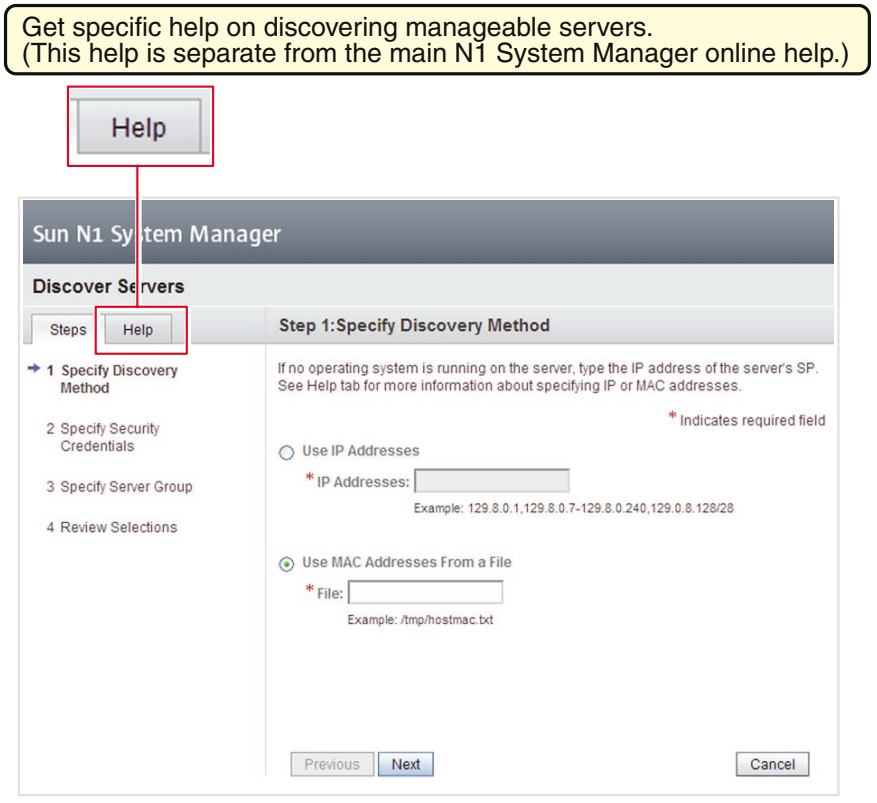
This method of discovery is useful if your data center configuration does not allow the N1 System Manager to connect to the management network. If you require full manageability of servers, do not choose this method of discovery, because the N1 System Manager must run in restricted mode as described in "Restricted Mode Capabilities" on page 47.

See "Manual Discovery" on page 66 for details about this method of discovery.

Note – Once you have used the N1 System Manager to discover manageable servers, rehosting of the management server is not supported.

For details on rehosting, see "Management Server Rehosting" in *Sun N1 System Manager 1.3 Installation and Configuration Guide*.

The procedures in this chapter focus on discovery of manageable servers using the command line. You can also use browser interface, or a special Discovery wizard. For information about how to use the browser interface, see the Sun N1 System Manager 1.3 Online Help. The wizard help is separate from the main online help, as shown in the following figure.



Capability of Managed Servers Based on Discovery

Depending on how a server was discovered, some features are not be available. The following table shows the features of the N1 System Manager that are available for a managed server once it is discovered.

TABLE 4–1 Capabilities of a Managed Server Based on Discovery Method

Feature	Discovered by Service Processor	Discovered by OS	Discovered Manually
Power control	Yes	No	No

TABLE 4–1 Capabilities of a Managed Server Based on Discovery Method *(Continued)*

Feature	Discovered by Service Processor	Discovered by OS	Discovered Manually
Serial console[1]	Yes	No	No
Firmware update[1]	Yes	No	No
Hardware sensor monitoring	Yes	No	No
OS provisioning	Yes	No	No
OS provisioning with netboot option	Yes	Yes	Yes
Package/patch/rpm deployment	Yes	Yes	Yes
Display Model	Yes	Yes for Sun Fire™ X4000 series servers running supported versions of Linux of Solaris 10 update 1 or above, and if recorded correctly in BIOS. Otherwise, no.	Yes
Display Manufacturer	Yes	Yes	No
Support for base management and OS monitoring	Yes	Yes	Yes
Launch web console (Sun Fire X4000 series servers only)	Yes	No	No
Enable/Disable Locator	Yes	No	No
Enable/Disable Monitoring	Yes	Yes	Yes
Show server output [2]	Yes	No	No

[1] Availability of these capabilities also depends on your choice of hardware. Serial Console access and firmware updates are not supported for Sun Fire V490, V890 and X2100 servers, regardless of the method of discovery.

[2] show server output includes locator, power status, hardware health, hardware type, processor, memory, serial number

TABLE 4–1 Capabilities of a Managed Server Based on Discovery Method *(Continued)*

Feature	Discovered by Service Processor	Discovered by OS	Discovered Manually
Show server serial number	Yes	Yes for Sun Fire X4000 series servers running a supported Linux or Solaris 10 update 1, if the BIOS has the serial number. Otherwise no.	No
Show server management IP	Yes	Yes (provisioning IP address used for discovery)	No
Initial server name	IP address used to discover the server	IP address used to discover the server	Name is supplied in file

The features that are available for a managed server are displayed in the managed server's Capabilities table. The Capabilities table is available in the Server Details page in the browser interface or by using the `show server` command.

Restricted Mode Capabilities

If your data center configuration does not allow the N1 System Manager to connect to both the management network and the provisioning network, the N1 System Manager operates in *restricted mode*.

The restricted mode is related to the privileges associated with the role of N1 System Manager users. Depending on how the N1 System Manager is configured, the administrator should assign the appropriate restricted mode role to users.

- If the N1 System Manager is configured so that it only has access to the provisioning network, the administrator should assign only the `ProvAdmin` restricted mode role to non-root users.
- If the N1 System Manager is configured so that it only has access to the management network, the administrator should assign only the `MgmtAdmin` restricted mode role to non-root users.

When the N1 System Manager is operating in restricted mode, users should be assigned only those privileges associated with the `ProvAdmin` or `MgmtAdmin` restricted mode roles, depending on the configuration. The `ProvAdmin` and `MgmtAdmin` restricted mode roles have been created specifically for the N1 System Manager's restricted mode of operation. It is possible to delete or modify the `ProvAdmin` and `MgmtAdmin` roles. Any custom roles you create should conform to the privilege set included in the `ProvAdmin` and `MgmtAdmin` roles, for stable performance of the product in restricted mode.

For information about roles, see "Introduction to User Security" on page 19.

Some N1 System Manager functions are not available based on whether your restricted mode installation has access to a management network only, or a provisioning network only. The following table lists all the commands that are valid for each restricted installation mode. If your installation provides only a management network, then only those items marked X in the management network column are available in the restricted mode. If you have only a provisioning network, then only those items marked X in the provisioning network column are available in the restricted installation mode.

TABLE 4–2 Restricted Mode Command Map

Command	Management Network	Provisioning Network
`add group`	X	X
`add osprofile`	-	X
`add server feature`	-	X
`add role`	X	X
`add user`	X	X
`connect`	X	-
`create firmware`	X	-
`create group`	X	X
`create notification`	X	X
`create os`	-	X
`create osprofile`	-	X
`create update`	-	X
`create role`	X	X
`delete firmware`	X	-
`delete group`	X	X
`delete job`	X	X
`delete notification`	X	X
`delete os`	-	X
`delete osprofile`	-	X
`delete server`	X	X
`delete update`	-	X
`discover`	X	X
`exit`	X	X

TABLE 4–2 Restricted Mode Command Map *(Continued)*

Command	Management Network	Provisioning Network
`help`	X	X
`load server firmware`	X	-
`load group firmware`	X	-
`load server osprofile`	-	X
`load group osprofile`	-	X
`load server update`	-	X
`load group update`	-	X
`remove group`	X	X
`remove osprofile`	-	X
`remove server`	X	X
`reset`	X	X
`set firmware`	X	-
`set group`	X	X
`set notification`	X	X
`set os`	-	X
`set osprofile`	-	X
`set role`	X	X
`set server agent SSH`	-	X
`set server SSH`	X	-
`set server filesystem threshold`	-	X
`set server IP`	X	-
`set server IPMI`	X	-
`set server locator`	X	-
`set server monitored`	X	X
`set server`	X	X
`set server name`	X	X
`set server note`	X	X

TABLE 4–2 Restricted Mode Command Map *(Continued)*

Command	Management Network	Provisioning Network
`set server refresh`	X	X
`set session`	X	X
`set user`	X	X
`show firmware`	X	X
`show os`	-	X
`show osprofile`	-	X
`show update`	-	X
`show group`	X	X
`show job`	X	X
`show log`	X	X
`show privilege`	X	X
`show notification`	X	X
`show role`	X	X
`show server`	X	X
`show session`	X	X
`show user`	X	X
`start group command`	-	X
`start server command`	-	X
`start group`	X	-
`start server`	X	-
`stop job`	X	X
`stop notification`	X	X
`unload server`	-	X
`unload group`	-	X

SP-Based Discovery

This section describes how to use the N1 System Manager to discover a server through the service processor (SP).

The *SP-based* discovery of manageable servers is possible if your data center configuration allows the N1 System Manager to connect to both the provisioning and management networks. For details on the configuration of provisioning and management networks, see "Sun N1 System Manager Connection Information" in *Sun N1 System Manager 1.3 Site Preparation Guide*. In addition, servers discovered by their service processors must be fully supported by the N1 System Manager. For a list of supported hardware and software, see "Sun N1 System Manager Hardware and OS Requirements" in *Sun N1 System Manager 1.3 Site Preparation Guide*.

Using SP-based discovery, you can discover a manageable server through its management network interface (management IP address). After the server is discovered, you can change the management IP address using the `set server` command with the `ip` configuration attribute.

The IP address of the server's system controller or service processor must be assigned as a prerequisite for SP-based discovery. Initiate SP-based discovery of multiple servers by specifying a range of IP addresses to search for servers.

Hardware Requirements for SP-Based Discovery

For SP-based discovery to work, manageable servers must comply with the revisions of firmware listed in "Manageable Server Firmware Requirements" in *Sun N1 System Manager 1.3 Site Preparation Guide*. See "Managing Firmware Updates (Tasks)" in *Sun N1 System Manager 1.3 Operating System Provisioning Guide* for instructions, or refer to Sun System Handbook documentation for your server.

SP-based discovery uses a Service Access Point (SAP) to access server capabilities. A *SAP* is generically defined as an IP address, protocol, and security credentials. Each hardware platform requires a minimum set of credentials to be discovered. If you do not specify the correct credentials such as Secure Shell (SSH) and Intelligent Platform Management Interface (IPMI) accounts and passwords, the discovery process assumes that the default credentials are configured on the manageable servers. For details about default credentials for each hardware type, see "Setting Up Manageable Servers" in *Sun N1 System Manager 1.3 Site Preparation Guide*.

Note – Automatic configuration of credentials is supported for Sun Fire V20z and V40z servers and X4000 series servers, if they are in the factory default state. See "Setting Up Manageable Servers" in *Sun N1 System Manager 1.3 Site Preparation Guide*.

If you do specify the login accounts and passwords, the SP-based discovery process configures the credentials you specify. If only one credential is specified, the missing credentials are configured with one of the defaults specified in "Setting Up Manageable Servers" in *Sun N1 System Manager 1.3 Site Preparation Guide*.

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

```
initialize=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 using SP-based discovery until their SSH and IPMI accounts are configured. For further information, see *Sun N1 System Manager 1.3 Site Preparation Guide*.

How to Discover Manageable Servers Using SP-Based Discovery

The "To Discover Manageable Servers Using SP-Based Discovery Using the Command Line" on page 53 procedure shows how to use the command line to execute this task. You can also use the browser interface to execute this task. Use the discover button in the Servers table to call the Discover Servers wizard. See the Sun N1 System Manager 1.3 Online Help for details.

As shown by Table 2–6, you cannot execute the `discover` command without having the `JobRead` privilege.

▼ To Discover Manageable Servers Using SP-Based Discovery Using the Command Line

Note – Servers discovered through their SP 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 1.3 Site Preparation Guide* for details on setting up a server for discovery.

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, or any other system management applications including the N1 System Manager.

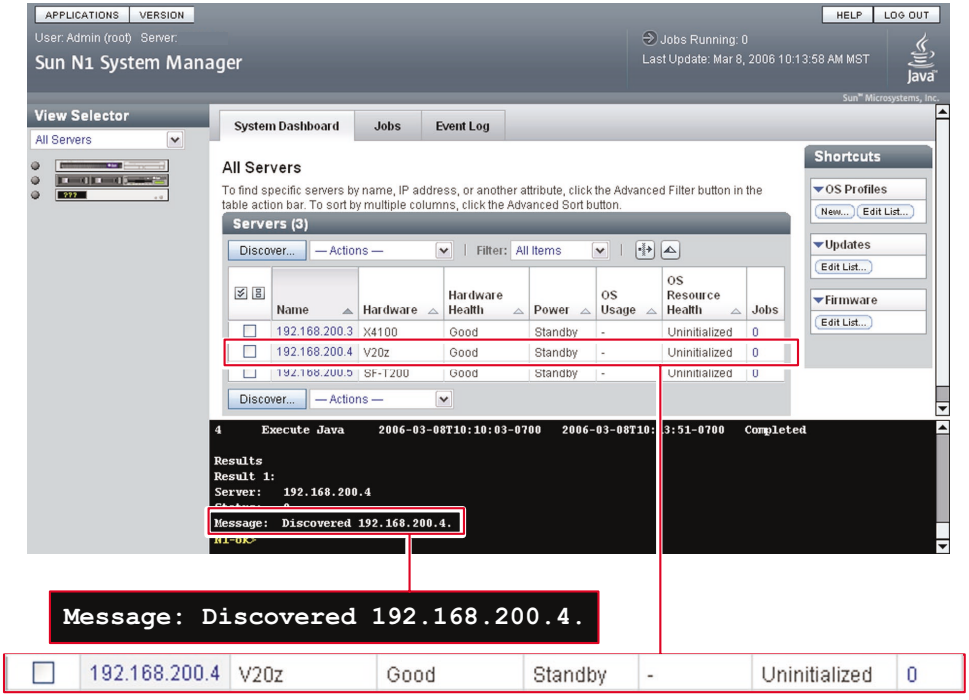
- **Use the `discover` command to discover a server through its SP.**

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

  IP addresses, IP address ranges, and IP subnets can be input as a comma-separated list. Overlapping IP address ranges are allowed.

  Note – When you specify the range of IP addresses for discovery, ensure that the IP address range does not include the IP addresses of the N1 System Manager management server.

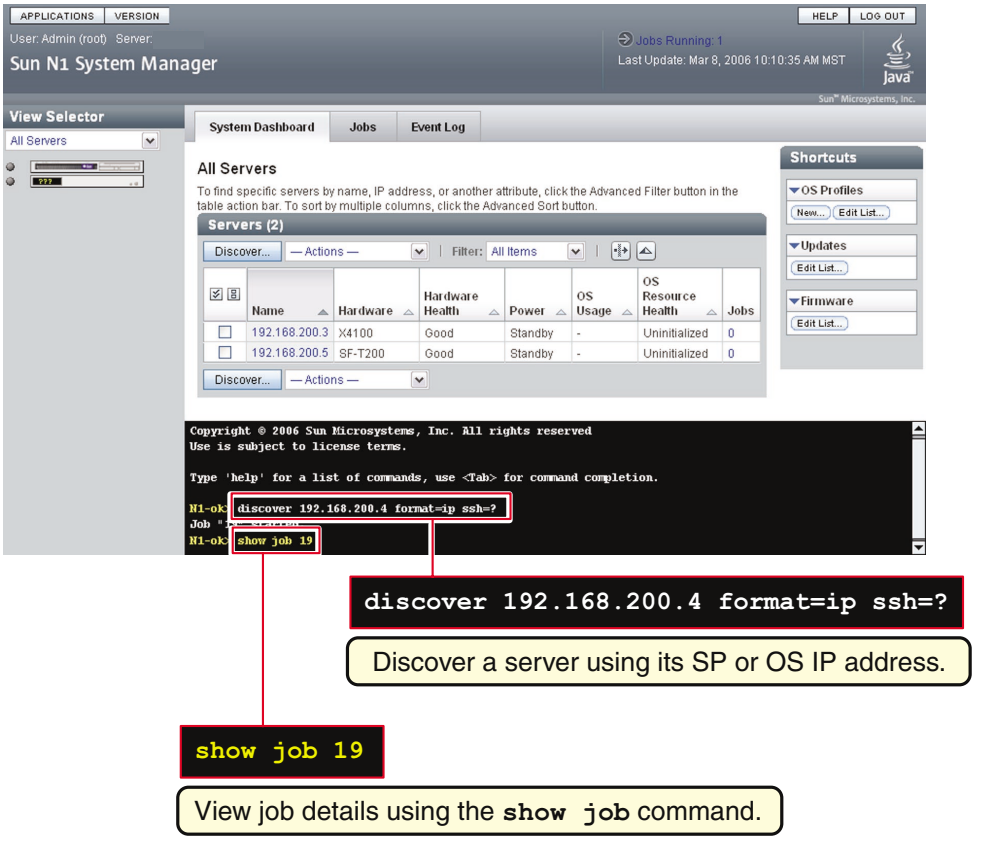
  Security credentials for IPMI, Simple Network Management Protocol (SNMP), SSH and Telnet are optional. If credentials are not specified, the manufacturer defaults are used. See *Sun N1 System Manager 1.3 Site Preparation Guide* for information about the default accounts.



Once discovered, the managed server appears in the list of managed servers on the System Dashboard.

See “discover” in *Sun N1 System Manager 1.3 Command Line Reference Manual* for more details about the syntax used in the `discover` command.

After successful completion of the Discovery job, a managed server is identified by its *management name*. If the server was discovered using SP-based discovery, its management name is initially set to the server’s management IP address. You can rename discovered servers at any time.



Example 4–1 Using SP-based Discovery With Management Network IP Addresses

The following example of the `discover` command shows how to discover servers through their service processor. The servers 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
 format ip 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    us      Jobs  Servers  Spare
dev                            7
```

The following example command shows how to view the list of managed 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
```

Example 4–2 Using SP-Based Discovery With Netmask

The following example of the `discover` command shows how to discover any servers through their SP, using the netmask. The servers 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
```

Troubleshooting

The `discover` command credential attributes are used for security. If used, 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.

Sun Fire X4000 series servers only initialize custom accounts once. For Sun Fire X4000 series servers discovered using a username and password combination:

- If `user` is root and the password supplied is not the default, and the SP root password is the default: the SP root password is changed by the N1 System Manager to the `password`.
- If `user` is not root and if `user` does not exist, and the SP root password is the default: the N1 System Manager creates the new user with a password of `password`. The N1 System Manager also changes the root password to the `password`.

For information about default credentials, see "Setting Up Manageable Servers" in *Sun N1 System Manager 1.3 Site Preparation Guide*.

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` or `SSH key changed: Cannot connect to host` and no true security breach has occurred, remove the `known_hosts` file or the specific entry in the file that corresponds to the managed server. Then, retry the `discover` command. See "To Update the ssh_known_hosts File" in *Sun N1 System Manager 1.3 Troubleshooting Guide* for details.

The problem of stale SSH entries on the management server can be avoided if, during the `n1smconfig` configuration process, you modify SSH policies by accepting changed or unknown host keys. Accepting changed or unknown host keys carries a security risk but avoids the problem of stale SSH entries on the management server. For more information, see "To Configure the N1 System Manager" in *Sun N1 System Manager 1.3 Installation and Configuration Guide*.

Discovery might fail due to a firmware version problem with drivers. See "Cannot Discover a Manageable Server" in *Sun N1 System Manager 1.3 Troubleshooting Guide* for details.

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
```

Discovery can fail with the following error message:

```
Check the Standard Output field for possible reasons for this failure
```

To see the Standard Output field, check the job details in the browser interface or by using the `show job` command with the job number of the discovery job that failed.

See Also

Sun N1 System Manager 1.3 Site Preparation Guide and "Troubleshooting Discovery" on page 71.

Next Steps

Open the server's serial console. To view information about accessing a server's serial console, in the Sun N1 System Manager online help, find the topic 'To Open the Serial Console for a Server'.

OS-Based Discovery

This section describes how to use the N1 System Manager to discover servers through their OS. The N1 System Manager provides a limited level of support for managed servers that are discovered using OS-based discovery. For more information, see "Capability of Managed Servers Based on Discovery" on page 45.

Use OS-based discovery to allow the N1 System Manager to find and manage servers that have an operating system already installed, even if the manageable servers are running on a configuration where access to their service processors is not possible. For details on the configuration of provisioning and management networks, see "Sun N1 System Manager Connection Information" in *Sun N1 System Manager 1.3 Site Preparation Guide*.

To enable OS-based discovery, use the `n1smconfig` script. See "Configuring the N1 System Manager" in *Sun N1 System Manager 1.3 Installation and Configuration Guide* for details about running the `n1smconfig` script.

Note – By default, the OS-based discovery feature is turned off.

To avoid discovering the same server more than once, do not issue the `discover` commands within the OS IP address space once OS-based discovery has been enabled. Only issue these commands, for example, if you have a platform itself whose service processor is not supported by the N1 System Manager, or have networking constraints that prohibit the use of a management network. For details about discovering duplicate servers, see "Discovering and Identifying Duplicate Servers" on page 71.

Using OS-based discovery, you can discover a manageable server through its provisioning network interface (its provisioning IP address, referred to as its OS IP address). After the server is discovered, you can change the OS IP address using the `set server` command with the `ip` configuration attribute.

Software Requirements for OS-Based Discovery

For OS-based discovery of a server, the server's OS must be supported by the N1 System Manager. All of the operating systems listed in "Manageable Server Requirements" in *Sun N1 System Manager 1.3 Site Preparation Guide* are supported for OS-based discovery by the N1 System Manager, with the exception of Microsoft Windows.

Note – OS-based discovery of managed servers that run the Microsoft Windows operating system is not possible in this release.

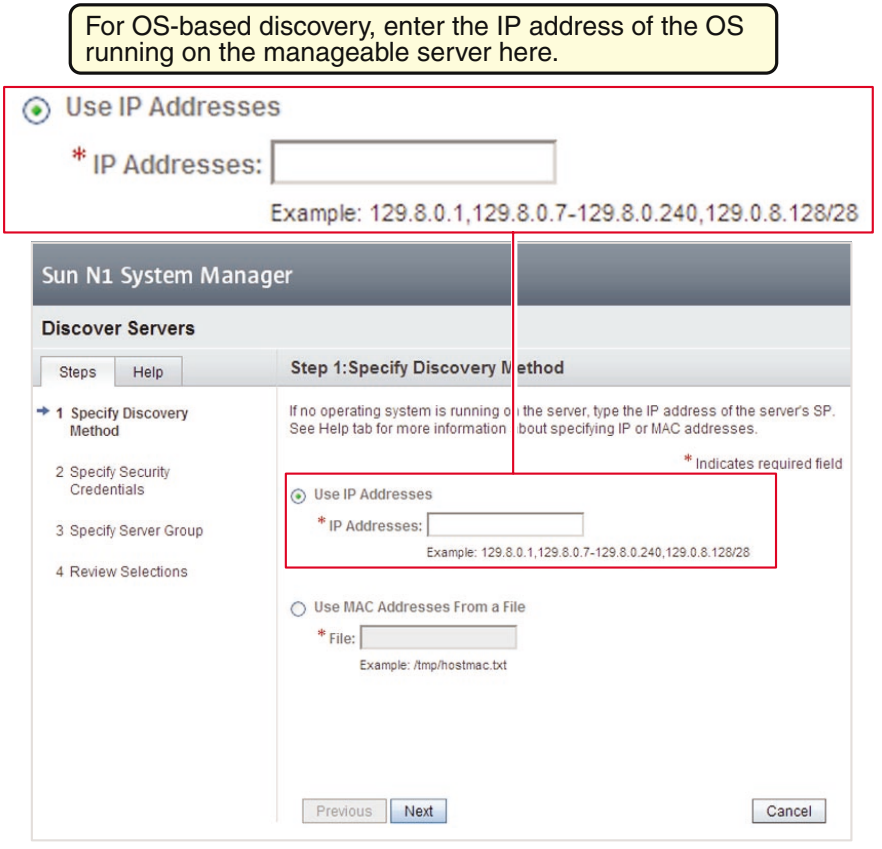
Hardware Requirements for OS-Based Discovery

OS-based discovery for each supported operating system has been officially qualified on supported hardware models for that operating system. The hardware supported by the N1 System Manager for each OS is described in "Sun N1 System Manager Hardware and OS Requirements" in *Sun N1 System Manager 1.3 Site Preparation Guide*.

The N1 System Manager can provision an OS on a managed server that was discovered by OS-based discovery, only if that managed server and target OS combination is supported by the N1 System Manager.

How to Discover Manageable Servers Using OS-Based Discovery

The "To Discover Manageable Servers Using OS-Based Discovery Using the Command Line" on page 61 procedure shows how to use the command line to execute the task. You can also use the browser interface to execute this procedure. Use the discover button in the Servers table to call the Discover Servers wizard. See the Sun N1 System Manager 1.3 Online Help for details.



As shown by Table 2–6, you cannot execute the `discover` command without having the `JobRead` privilege.

▼ To Discover Manageable Servers Using OS-Based Discovery Using the Command Line

Note – Servers discovered through their OS are not monitored for hardware health, as indicated in Table 4–1.

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 1.3 Site Preparation Guide* for details on setting up a server for discovery.

This procedure focuses on using the command line of the N1 System Manager.

The manageable server must be powered on and have a running OS before being discovered. The OS must be supported by the N1 System Manager. See "Software Requirements for OS-Based Discovery" on page 59 for details.

Before attempting to discover a manageable server using OS-based discovery, the OS-based discovery feature must be enabled. To enable OS discovery, use the `n1smconfig` script. See "Configuring the N1 System Manager" in *Sun N1 System Manager 1.3 Installation and Configuration Guide* for details about running the `n1smconfig` script.

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.

◗ **Use the `discover` command to discover a server through its OS.**

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

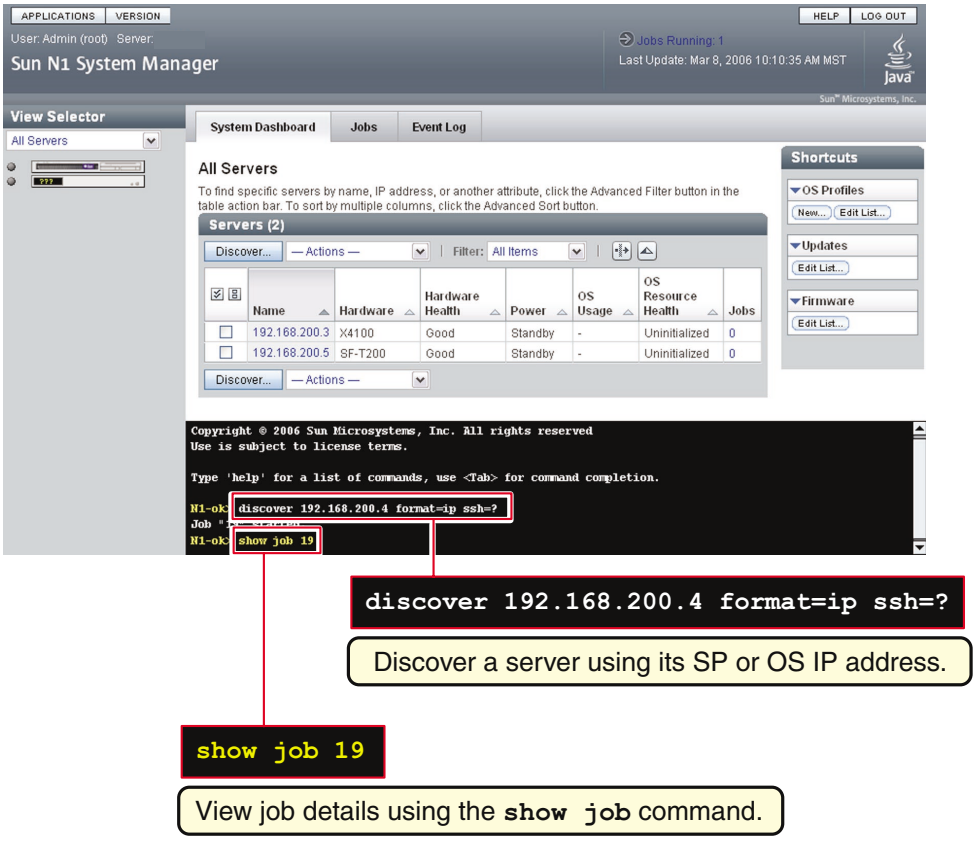
IP addresses, IP address ranges, and IP subnets can be input as a comma-separated list. Overlapping IP address ranges are allowed. See *Sun N1 System Manager 1.3 Site Preparation Guide* for information about the default accounts.

For OS-based discovery, SSH credentials should be provided. If not specified, default SSH credentials of `root/admin` are read.

Note – When you specify the range of IP addresses for discovery, ensure that the IP address range does not include the IP addresses of the N1 System Manager management server.

See "discover" in *Sun N1 System Manager 1.3 Command Line Reference Manual* for more details about the syntax used in the `discover` command.

After successful completion of the Discovery job, a managed server is identified by its *management name*. If the server was discovered using OS-based discovery, its management name is initially set to the server's provisioning (or OS) IP address. You can rename discovered servers at any time.



Example 4–3 OS-based Discovery Using OS IP Addresses

The following example of the `discover` command shows how to discover manageable servers through their OS. The servers have the following OS (or provisioning 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 OS-based 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
```

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

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

The following example command shows how to view the list of managed 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 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 4–4 OS-based Discovery Using Netmask

The following example of the `discover` command shows how to discover any manageable servers through their OS, using the netmask. The servers have OS 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.
```

Troubleshooting

The `discover` command credential attributes are used for security. SSH credentials are required for OS-based discovery. If not specified, SSH credentials or root/admin are used by the N1 System Manager.

For information about default credentials, see "Setting Up Manageable Servers" in *Sun N1 System Manager 1.3 Site Preparation Guide*.

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` or `SSH key changed: Cannot connect to host` and no true security breach has occurred, remove the `known_hosts` file or the specific entry in the file that corresponds to the managed server. Then, retry the `discover` command. See "To Update the ssh_known_hosts File" in *Sun N1 System Manager 1.3 Troubleshooting Guide* for details.

The problem of stale SSH entries on the management server can be avoided if, during the `n1smconfig` configuration process, you modify SSH policies by accepting changed or unknown host keys. Accepting changed or unknown host keys carries a security risk but avoids the problem of stale SSH entries on the management server. For more information, see "To Configure the N1 System Manager" in *Sun N1 System Manager 1.3 Installation and Configuration Guide*.

Some commands are not supported for managed servers that were discovered through OS-based discovery. See "Capability of Managed Servers Based on Discovery" on page 45 for details about which features are not available for managed servers that were discovered through OS-based discovery. Unsupported commands generate the following error:

```
Unsupported operation
```

This error is displayed either in the job status or immediately in the command line interface.

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
```

Discovery can fail with the following error message:

```
Check the Standard Output field for possible reasons for this failure
```

To see the Standard Output field, check the job details in the browser interface or by using the `show job` command with the job number of the discovery job that failed.

Discovery might fail due to a firmware version problem with drivers. See "Cannot Discover a Manageable Server" in *Sun N1 System Manager 1.3 Troubleshooting Guide* for details.

See Also

Sun N1 System Manager 1.3 Site Preparation Guide and "Troubleshooting Discovery" on page 71.

Next Steps

Open the server's serial console. To view information about accessing a server's serial console, in the Sun N1 System Manager Online Help, find the topic 'To Open the Serial Console for a Server'.

Manual Discovery

Read "Choosing a Method of Discovery" on page 43 to see if you should use this method of discovering servers.

You can manually discover servers that have no operating system installed, even if you have no access to the service processor. Servers with no OS installed are called *bare metal* servers.

Note – When using the N1 System Manager to load an OS on managed servers that were discovered using manual discovery, the `manualnetboot` feature must be turned on. For more information, see *Sun N1 System Manager 1.3 Operating System Provisioning Guide*.

To avoid discovering the same server more than once, do not use manual discovery unless absolutely necessary. For example, unless you have a platform whose service processor is not supported by the N1 System Manager, or have networking constraints that prohibit the use of a provisioning network. For details about discovering duplicate servers, see "Discovering and Identifying Duplicate Servers" on page 71.

The N1 System Manager provides only a restricted level of support for managed servers that were discovered manually. For more information, see "Capability of Managed Servers Based on Discovery" on page 45. Consider configuring your data center's N1 System Manager installation so that the management server is connected to both the provisioning and management networks, which allows SP-based discovery to be used. For details on the configuration of provisioning and management networks, see "Sun N1 System Manager Connection Information" in *Sun N1 System Manager 1.3 Site Preparation Guide*. For details on the restricted mode of operation of the N1 System Manager, see "Restricted Mode Capabilities" on page 47.

For manual discovery, use an XML file containing MAC addresses of the server that you want to discover. The file format should be similar to the following example:

```
<?xml version='1.0' encoding='utf-8'?>
<servers>
<server name="stinger1" model="V20z" guid="01234567-89ab-cdef-0123-456789abcdef">
<ethernetPort name="GB_0" mac="00:11:22:33:44:55"/>
<ethernetPort name="GB_1" mac="00:11:22:33:44:56"/>
</server>
</servers>
```

The `guid` attribute is optional.

In the example, the model number used is `V20z`, which represents a Sun Fire V20z server. See Table 4–3 for a list of recognized model numbers to be used in the file for manual discovery.

Discovering and Identifying Servers by Their Model Numbers

In the manual discovery XML file, use the appropriate model number for manageable servers that you want to discover manually. For details about this file, see "Manual Discovery" on page 66.

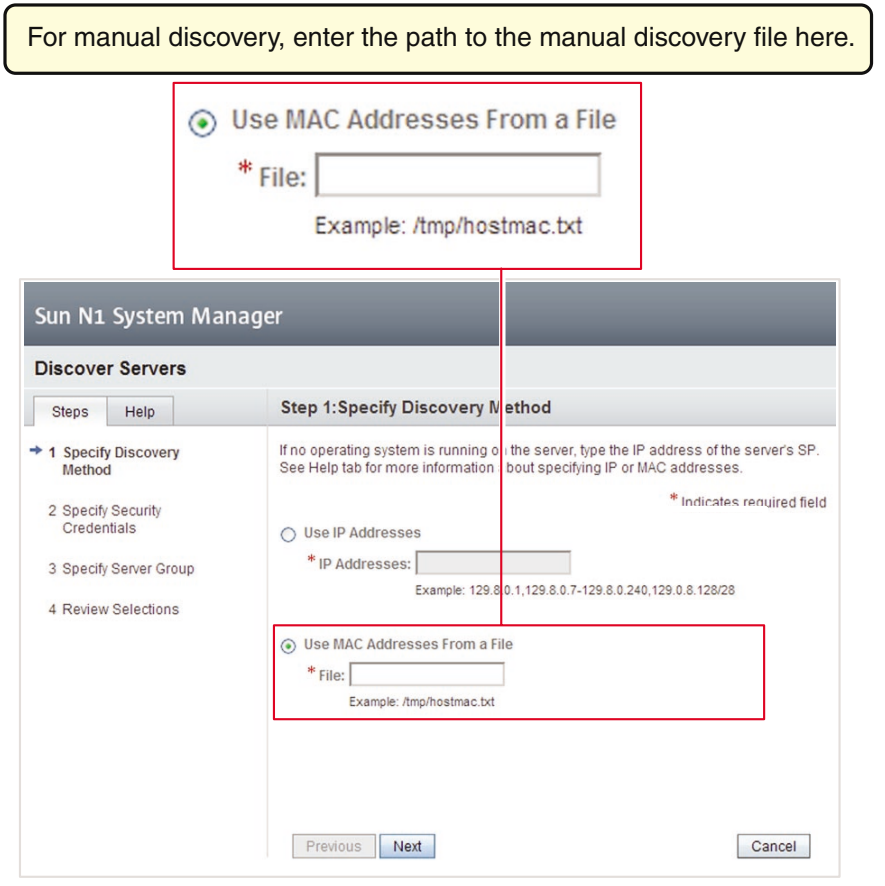
The following table shows the model numbers recognized by the N1 System Manager for manual discovery.

TABLE 4–3 Model Numbers for Discovering Managed Servers

Server Type	Model Type for Manual Discovery
Sun Netra 240	NETRA-240
Sun Netra 440	NETRA-250
Sun Fire V210	SF-V210
Sun Fire V240	SF-V240
Sun Fire V250	SF-V250
Sun Fire V440	SF-V440
Sun Fire V490	SF-490
Sun Fire V890	SF-890
Sun Fire V20z	V20z
Sun Fire V40z	V40z
Sun Fire X2100	X2100
Sun Fire X4100	X4100
Sun Fire X4200	X4200
Sun Fire T1000	SF-T1000
Sun Fire T2000	SF-T2000

How to Discover a Manageable Server Using Manual Discovery

The "To Discover a Manageable Server Using Manual Discovery Using the Command Line" on page 68 procedure shows how to use the command line to execute the task. You can also use the browser interface to execute this procedure. Use the discover button in the Servers table to call the Discover Servers wizard. See the Sun N1 System Manager 1.3 Online Help for details.



As shown by Table 2–6, you cannot execute the `discover` command without having the `JobRead` privilege.

▼ To Discover a Manageable Server Using Manual Discovery Using the Command Line

Note – Servers discovered manually are not automatically monitored for hardware health, as indicated in Table 4–1.

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 1.3 Site Preparation Guide* for details on setting up a managed server for discovery.

The N1 System Manager can provision an OS on a managed server that was discovered by OS-based discovery, only if that managed server and target OS combination is supported by the N1 System Manager.

Note – Manual discovery of diskless clients is not supported.

The manageable server must be powered on before being discovered.

Note – When using the N1 System Manager to load an OS on managed servers that were discovered manually, the `manualnetboot` feature must be turned on. For more information, see *Sun N1 System Manager 1.3 Operating System Provisioning Guide*.

◗ **Use the `discover` command to discover a server manually.**

```
N1-ok> discover file format file [group group]
```

The *file* must be a fully qualified path to an XML file, containing the manageable server's MAC address. To manually discover a group of manageable servers with one command, their MAC addresses must be specified in the same XML file.

This command makes the servers part of the same group.

See "discover" in *Sun N1 System Manager 1.3 Command Line Reference Manual* for more details about the syntax used in the `discover` command.

After successful completion of the Discovery job, a managed server is identified by its *management name*. This name is the name you provided in the XML file. You can rename discovered servers at any time.

Example 4–5 Discovering Manageable Servers Manually

The following example of the `discover` command shows how to discover manageable servers manually. The servers have the following MAC addresses: `00:11:22:33:44:55` and `00:11:22:33:44:77`.

```
N1-ok> discover /net/machine1.brasil/XMLfiles/manual_disco.xml format file group group1
Job 1 started.
```

The XML file contains the machine names and MAC addresses for manual discovery.

```
<?xml version='1.0' encoding='utf-8'?>
<servers>
<server name="galaxy1" model="X4100" guid="01234567-89ab-cdef-0123-456789abcdff">
```

```
<ethernetPort name="GB_0" mac="00:11:22:33:44:55"/>
<ethernetPort name="GB_1" mac="00:11:22:33:44:56"/>
</server>
<server name="galaxy2" model="X4100" guid="01234567-89ab-cdef-0123-456789abcdee">
<ethernetPort name="GB_0" mac="00:11:22:33:44:77"/>
<ethernetPort name="GB_1" mac="00:11:22:33:44:76"/>
</server>
</servers>
```

The `guid` attribute is optional.

The `group` subcommand adds the successfully discovered servers into a server group called `group1`.

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
```

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

```
N1-ok> show group all
Name    us      Jobs  Servers  Spare
group1                          2
```

Troubleshooting

Some commands are not supported for managed servers that were discovered manually. See "Capability of Managed Servers Based on Discovery" on page 45 for details about which features are not available for managed servers that were discovered manually. Unsupported commands generate the following error:

```
Unsupported operation
```

This error is displayed either in the job status or immediately in the command line interface.

Discovery can fail with the following error message:

```
Check the Standard Output field for possible reasons for this failure
```

To see the Standard Output field, check the job details in the browser interface or by using the `show job` command with the job number of the discovery job that failed.

Discovery might fail due to a firmware version problem with drivers. See "Cannot Discover a Manageable Server" in *Sun N1 System Manager 1.3 Troubleshooting Guide* for details.

See Also

Sun N1 System Manager 1.3 Site Preparation Guide and "Troubleshooting Discovery" on page 71

Next Steps

Open the server's serial console. To view information about accessing a server's serial console, in the Sun N1 System Manager Online Help, find the topic 'To Open the Serial Console for a Server'.

Software Requirements for Manual Discovery

To manually discover a manageable server, the server does not need to have an OS installed before being discovered.

Hardware Requirements for Manual Discovery

All of the hardware listed at "Sun N1 System Manager Hardware and OS Requirements" in *Sun N1 System Manager 1.3 Site Preparation Guide* is supported for manual discovery.

Troubleshooting Discovery

This section describes potential problems with server discovery and explains how to deal with these problems.

Discovery and Routers

Discovery of manageable servers using N1 System Manager works across routers if the network services used by the discovery process are not blocked by a firewall. Network services used by the discovery process can include SSH and SNMP.

RSC Server Discovery Problems

Manageable servers based on the Remote System Control (RSC) technology, such as Sun Fire V800 series servers, must be powered off before they can be discovered by the N1 System Manager. See "Discovery of RSC Servers" in *Sun N1 System Manager 1.3 Troubleshooting Guide* for details.

Discovering and Identifying Duplicate Servers

For managed servers that were discovered manually or by OS-based discovery, the N1 System Manager could discover the same server more than once. This duplication can happen in the following conditions:

- You discover a server manually. You then use SP-based discovery to discover another server but one of the platform MAC addresses of the second server matches a MAC address in the manual discovery file. A duplicate server has been discovered.
- You discover a server using OS-based discovery but its service processor is on a different subnet from its OS. You then use SP-based discovery to discover another server, but due to the conflict with subnets, the SP-based discovery command discovers the same server. A duplicate server has been discovered.

- Both of the above cases happen. Two duplicate servers have been discovered, and the same server appears three times.

Discovery of duplicate servers can lead to confusion and is not recommended. In addition, there is a risk that multiple attempts to provision an OS on the same managed server might occur simultaneously, or simultaneous attempts might be made to provision an OS on a server and power off the server.

If you use OS-based discovery or manual discovery to discover servers, use the `detectduplicates` utility to identify duplicate servers:

```
N1-ok> /opt/sun/n1gc/bin/detectduplicates
Name           Hardware       Discovered At  Network
manual1        V20z           -              File
manual2        V20z           -              File
192.168.79.2   V20z           192.168.79.2   Management

192.168.79.67  SF-T2000       192.168.79.67  Management
 manual3        T2000          -              File
```

In the output of the `detectduplicates` utility, duplicates are organized into groups, separated by a blank line. In this example, the `detectduplicates` utility has detected two groups of duplicates.

The output of the `detectduplicates` utility displays the following information:

- Name – The name of the server, as reported by the `show server` command.
- Hardware – The model of the server as reported by the `show server` command.
- Discovered At – The IP address that was used to discover the server. The IP address is reported as '-' for manually discovered servers.
- Network – The network that was used to discover the server. Possible values are:
  - Management – The management (service processor) network
  - Data – The provisioning network
  - File – Manually asserted

Server Details Information Is Missing

The N1 System Manager provides a limited set of features for managed server that were discovered manually or using OS-based discovery. Some server details might not be displayed in the Server details page for the server, or using the `show server` command. See "Capability of Managed Servers Based on Discovery" on page 45 for more information about what capabilities are provided for servers depending on how they were discovered.

Identifying How a Managed Server Was Discovered

You can identify whether a managed server was discovered by OS-based discovery if in the server details section of the N1 System Manager browser interface or by using the `show server` command, the following states should be true:

- The connection section does not show a `mgmtEth` interface
- The management IP address is identical to the IP address used in the `discover` command when the server was discovered
- Power control capability is listed as `unavailable`

Some functionality might be absent, based on how the server was discovered. Table 4–1 lists supported and unsupported operations for managed servers based on how they were discovered. For managed servers discovered manually or by OS-based discovery, attempts to execute operations that are unsupported because of how the server was discovered are flagged by `unsupported operation` error messages.

Some servers support Remote System Control (RSC). For some models of RSC servers, the model number displayed by the N1 System Manager can depend on how the server was discovered.

- For Sun Fire V490 servers discovered manually or through OS-based discovery, the model name returned is `SF-V490`. If the Sun Fire V490 server was discovered through its service processor, the model name is returned as `SF-RSC`.
- For Sun Fire V890 servers discovered manually or through OS-based discovery, the model name returned is `SF-V890`. If the server was discovered automatically through its service processor, the model name is returned as `SF-RSC`.

See "Discovering and Identifying Servers by Their Model Numbers" on page 67 for details.

Reprovisioning Servers That Were Discovered Manually or Using OS-based Discovery

There are several issues to be aware of when attempting to reprovision managed servers that were discovered manually or using OS-based discovery. Using the `load server` command, reset the SSH and management IP address if they have changed. For more information, see *Sun N1 System Manager 1.3 Operating System Provisioning Guide*.

Note – When using the N1 System Manager to load an OS on managed servers that were discovered manually or using OS-based discovery, the `manualnetboot` feature must be turned on. For more information, see *Sun N1 System Manager 1.3 Operating System Provisioning Guide*.

◆ ◆ ◆ CHAPTER 5

Managing Servers and Server Groups

This chapter provides conceptual and procedural information about N1 System Manager server management and server group management.

This chapter contains 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 and manage servers, as well as to provision or update operating systems and firmware and to redeploy manageable servers.

Use the `discover` command to initiate the management of manageable servers. See Chapter 4 for details.

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

For aggregate installation of firmware updates, you can create groups of discovered servers, or managed servers, according to make and model. Create functional groups for the aggregate

installation of operating systems, or *OS profiles*, and OS updates. Managed nodes 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 using the command line. You can also use the View Selector menu, the Actions menu, and server name links in the browser interface to perform the operations that are described in these sections.

For information about the management of diskless clients, see "Managing Diskless Clients" in *Sun N1 System Manager 1.3 Operating System Provisioning Guide*.

Identifying Managed Servers and Server States

This section describes the information that the N1 System Manager reports for each managed server when you issue the `show server` command with the `all` keyword, or the `show group` command.

- **Name** – The managed server or group name. The managed server name is initially set to the management IP address. For instructions on how to change the managed server name, see "Modifying Managed Server and Group Information" on page 84.
- **Hardware** – Describes the type of managed server. See the Sun System Handbook documentation for your managed server.
- **Hardware Health** – The status for attributes such as memory, processor information, and Network Interface Card (NIC) information.
- **Power** – Power status for the managed 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 managed server, the job ID appears here.

Managed Server Power States

Server power is indicated by the following states:

- **On** – The managed server is powered on and running.
- **Standby** – The managed server is powered off but still responsive to commands, for example, `start`.
- **Unknown** – The managed server is not returning any power status information.
- **Unreachable** – The managed server cannot be contacted for power status information.

Hardware Health States

The hardware health of managed servers is indicated by the following states:

- **Good** – The managed server hardware is working properly.

- **Unreachable** – The managed 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 managed server. Take action to prevent the problem from becoming more serious. See "Monitoring Threshold Values" on page 130 for information about hardware sensor threshold values.
- **Critical Failure** – A fault condition has occurred on the managed server. Corrective action is required.
- **Nonrecoverable Failure** – The managed server has completely failed. Recovery is not possible.
- **Unknown** – The managed server is not returning any hardware health status.
- **Offline** – The server is not managed.

Supported Actions on Managed Servers

The following aggregate server actions are supported:

- Starting, stopping, and resetting power.
- Listing and refreshing server data.
- Loading managed servers with OS profiles, updates, and firmware. See *Sun N1 System Manager 1.3 Operating System Provisioning Guide*.
- Enabling and disabling managed server monitoring. See Chapter 6.
- Adding managed server to groups. See"Creating and Maintaining Groups of Managed Servers" on page 77.
- Removing managed servers from the N1 System Manager.

Creating and Maintaining Groups of Managed Servers

This section describes the following tasks:

Creating Groups and Adding Managed Servers to Groups

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

For aggregate installation of firmware updates, you can create groups of managed servers, according to the make and model. Then, you can create functional groups for the aggregate installation of operating systems, or *OS profiles*, and OS updates. For details about provisioning operating systems, see *Sun N1 System Manager 1.3 Operating System Provisioning Guide*. Managed servers can belong to more than one group, so you can create new groups for aggregate maintenance tasks as needed.

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

To create a group and add managed servers in a single operation, use the `create group` command and the `server` subcommand. This task can also be performed during the service processor discovery process. Add an option to the `discover` command to create a new group and add the servers to the new group. See "To Discover Manageable Servers Using SP-Based Discovery Using the Command Line" on page 53 or "To Discover Manageable Servers Using OS-Based Discovery Using the Command Line" on page 61 for instructions.

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

▼ To Create a Group of Managed Servers

This task shows you how to create groups of managed servers. Managed nodes can belong to more than one server group, so you can create new groups for aggregate maintenance tasks as needed.

1 Log in to the N1 System Manager.

2 Use the following command:

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

The new group is created. See "create group" in *Sun N1 System Manager 1.3 Command Line Reference Manual* for details.

Example 5–1 Creating a Group and Adding Servers in a Single Operation

The following example shows how to create a group named `dev` and add managed 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 Managed Server to a Group

Note – Managed Servers can belong to more than one group.

1. **Log in to the N1 System Manager.**
2. **Use the following command:**

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

   The managed server is added to the group. See "add group" in *Sun N1 System Manager 1.3 Command Line Reference Manual* for details.

Removing A Managed Server From A Group

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

▼ To Remove a Managed Server From a Group

1. **Log in to the N1 System Manager.**
2. **Use 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 1.3 Command Line Reference Manual* for details.

Replacing Managed Servers

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

▼ To Replace a Server

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

   See "To Access the N1 System Manager Command Line" on page 14 for details.

2. **Type the following command:**

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

The managed server is shut down and powered off. See "stop server" in *Sun N1 System Manager 1.3 Command Line Reference Manual* for details.

3 Disconnect the manageable server from the rack.

4 Remove the manageable server from the system.

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

5 Connect the new manageable server.

Follow the instructions in *Sun N1 System Manager 1.3 Site Preparation Guide*.

6 Discover the replacement manageable server using your chosen method of discovery.

Follow the instructions in Chapter 4.

The replacement server is managed. See "discover" in *Sun N1 System Manager 1.3 Command Line Reference Manual* for details. You can now set up monitoring. See "Supporting OS Monitoring" on page 111 and "Enabling and Disabling Monitoring" on page 125 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. For default credentials, see "Setting Up Manageable Servers" in *Sun N1 System Manager 1.3 Site Preparation Guide*.

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` or `SSH key changed: Cannot connect to host` and no true security breach has occurred, remove the `known_hosts` file or the specific entry in the file that corresponds to the managed server. Then, retry the `discover` command. See "To Update the ssh_known_hosts File" in *Sun N1 System Manager 1.3 Troubleshooting Guide* for details.

The problem of stale SSH entries on the management server can be avoided if, during the `n1smconfig` configuration process, you modify SSH policies by accepting changed or unknown host keys. Accepting changed or unknown host keys carries a security risk but avoids the problem of stale SSH entries on the management server. For more information, see "To Configure the N1 System Manager" in *Sun N1 System Manager 1.3 Installation and Configuration Guide*.

Listing and Viewing Managed Servers and Groups

This section describes the following tasks:

Listing Managed Server and Groups

To list servers, use the View Selector menu. Alternatively, use the `show server` command with `all` subcommand to list all servers in the N1 System Manager.

▼ To List Managed Server and Groups

This procedure uses the N1 System Manager command line. You also can use the browser interface for this procedure, by choosing All Servers from the View Selector menu. See the Sun N1 System Manager 1.3 Online Help for details.

1 Log in to the N1 System Manager.

See "To Access the N1 System Manager Browser Interface" on page 16 for details.

2 Type the `show server` command with the `all` keyword to view all managed servers in the system.

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

A list of all managed servers in the system appears. See "show server" in *Sun N1 System Manager 1.3 Command Line Reference Manual* for details.

Example 5–2 Filtering Managed Servers Based on IP Address

The following example shows how to filter a list of managed 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 managed 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 managed 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 5–3 Filtering Managed Servers Based on Job Count

The following example shows how to filter a list of managed servers in the system based on job count. In this case the job count is `0`:

```
N1-ok> show server jobcount 0
```

Example 5–4 Filtering Managed Servers Based on Model

The following example shows how to filter a list of managed 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 5–5 Filtering Managed Servers Based on Name

The following example shows how to filter a list of managed servers in the system based on the managed server's name. In this case the name is `server3`:

```
N1-ok> show server name server3
```

Example 5–6 FilteringManaged Servers Based on Running OS

The following example shows how to filter a list of managed 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 5–7 Filtering Managed Servers Based on OS Health

The following example shows how to filter a list of managed servers in the system based on the health of the OS that is running on the server. In this case, all managed servers that have OS health monitored are listed:

```
N1-ok> show server oshealth monitored
```

The following example shows how to filter a list of managed servers in the system based on the health of the OS that is running on the managed 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 managed servers in the system based on the health of the OS that is running on the managed 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 OS Monitoring" on page 111.

Example 5–8 Listing Groups

```
N1-ok> show group all
```

A list of all groups in the system appears. See "show group" in *Sun N1 System Manager 1.3 Command Line Reference Manual* for details.

▼ To View Failed Managed Servers

This procedure describes how to view failed managed servers using the N1 System Manager command line. You can also use the browser interface by choosing Servers By Health from the View Selector menu. See the Sun N1 System Manager 1.3 Online Help for details.

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

2. **Use the `show server` command with the `hardwarehealth` keyword and the fault state that you want to view.**

   ```
   N1-ok> show server hardwarehealth nonrecoverable

   N1-ok> show server hardwarehealth warning

   N1-ok> show server hardwarehealth critical

   N1-ok> show server hardwarehealth unreachable

   N1-ok> show server hardwarehealth unknown
   ```

   See "Hardware Health States" on page 76 for a description of fault states.

Example 5–9 Viewing Failed Critical Servers

The following example shows how to view Managed 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 failure levels of managed servers, see "Hardware Health States" on page 76. For descriptions of monitoring thresholds, see "Monitoring Threshold Values" on page 130.

Viewing Managed Server Details and Group Members

To view detailed server information and group members, use the `show server` command or `show group` commands. For syntax and parameter details, type `help show server` or `help show group` at the `N1–ok` command line. Information about managed servers is also provided on the Server Details page in the browser interface.

▼ To View Managed Server Details and Server Group Members

This procedure describes how to view managed server details and server group members by using the command line. You can also use the browser interface by choosing All Servers from the View Selector menu. See the Sun N1 System Manager 1.3 Online Help for details.

1 Log in to the N1 System Manager.

2 Use the show server command with the server's name.

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

Detailed server information appears. See "show server" in *Sun N1 System Manager 1.3 Command Line Reference Manual* for details.

Example 5–10 Viewing Server Group Members

The following example shows how to view the list of managed servers in a server group named `devgroup`, by using the `show server` command.

```
N1-ok> show group devgroup
```

The list of servers in the group appears. See "show group" in *Sun N1 System Manager 1.3 Command Line Reference Manual* for details.

Modifying Managed Server and Group Information

This section describes the following tasks:

- "To Rename a Managed Server or a Group" on page 85
- "To Add a Server Note" on page 85

Use the `set server` command with the `name` subcommand. For syntax and parameter details, type `help set server` or `help set group` at the `N1–ok` command line.

Renaming a Managed Server or a Group

Managed servers are identified by the management IP address that is specified during discovery. This name is also referred to as the *management name*. You might want to rename a server with the DNS host name or track the host name by adding it to the server notes.

Managed server and group names must be unique and may include numbers, letters, and some special symbols. The following special symbols are prohibited: comma, asterisk, single quote, double quote, parenthesis, question mark, equal sign, and newline.

▼ To Rename a Managed Server or a Group

This procedure describes how to rename a managed server or a group by using the command line. You also can use the browser interface for this procedure, by choosing All Servers from the View Selector menu. See the Sun N1 System Manager 1.3 Online Help for details.

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

2. **Use the** `set server` **command to change the name of the managed server.**

   ```
   N1-ok> set server server name=newname
   ```

   Server names must be unique and may include letters A through Z, digits 0 through 9, hyphens, and underscores.

   See "set server" in *Sun N1 System Manager 1.3 Command Line Reference Manual* for details.

Example 5–11 Renaming a Group

The following example shows how to change a server group name by using the `set group` command.

```
N1-ok> set group devgroup name=labgroup
```

The group name is changed from `devgroup` to `labgroup`. See "set group" in *Sun N1 System Manager 1.3 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 server` command with 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 1.3 Command Line Reference Manual.*

▼ To Add a Server Note

This procedure describes how to add a server note by using the command line. You also can use the browser interface for this procedure, by choosing All Servers from the View Selector menu. See the Sun N1 System Manager 1.3 Online Help for details.

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

2. **Use the `set server` command to show any existing notes for the managed server.**

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

   The output shows any existing notes.

3. **Use the `set server` command with the `note` keyword to add a note for the managed server.**

   ```
   N1-ok> set server server note="your note"
   ```

   The note is added to the server information. See "set server" in *Sun N1 System Manager 1.3 Command Line Reference Manual* for details.

Starting, Stopping, and Resetting Managed Servers and Groups

This section describes the following activities:

- "To Power On and Boot a Managed Server or a Group" on page 86
- "To Shut Down and Power Off a Managed Server or a Group" on page 87
- "To Reboot a Managed Server or a Group" on page 89

Starting Managed Servers and Groups

Use the `start server` or `start group` commands to power on a server or a server group. If boot PROMS are configured, the servers boot. You can also use the Actions menu on the Servers By Group page in the browser interface to initiate the start operation. See the Sun N1 System Manager 1.3 Online Help for details.

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 Managed Server or a Group

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

2. **Use the `start server` or `start group` 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 1.3 Command Line Reference Manual* for syntax details.

   ```
   N1-ok> start group group
   ```

The group is powered on and, if boot PROMs are configured, the manageable servers in the group boot. Job completion takes longer for large groups. See "start group" in *Sun N1 System Manager 1.3 Command Line Reference Manual* for syntax details.

Note – RSC servers can take several minutes to start. The job status for the RSC server can indicate that the server has already started or rebooted before the startup or reboot process has actually completed with the server's OS running. Any subsequent jobs started on the RSC server before the startup or reboot process has completed and before the server's OS is running will fail.

For details about setting up RSC servers, see "Preparing RSC-based Manageable Servers" in *Sun N1 System Manager 1.3 Site Preparation Guide*. See also "Discovery of RSC Servers" in *Sun N1 System Manager 1.3 Troubleshooting Guide*.

Example 5–12 Starting a Managed Server From the Network

The following example shows how to boot a managed server from the network.

```
N1-ok> start server 10.5.7.2 netboot=true
```

Example 5–13 Starting a Group From the Network

The following example shows how to boot a group of managed servers from the network.

```
N1-ok> start group dev netboot=true
```

Stopping Managed Servers and Groups

To shut down and power off a managed server or a group, use the `stop server` or `stop group` commands. Stopping a server or server group initiates graceful shutdown of the operating systems and subsequent power off the managed servers. If managed servers do not have an OS installed or do not shutdown, you can use the `force` subcommand to power off the server group.

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 Managed Server or a Group

1. **Log in to the N1 System Manager.**
2. **Type one of the following commands:**

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

The managed server is stopped. See "stop server" in *Sun N1 System Manager 1.3 Command Line Reference Manual* for syntax details.

```
N1-ok> stop group group
```

The group is stopped. See "stop group" in *Sun N1 System Manager 1.3 Command Line Reference Manual* for syntax details.

Example 5–14 Forcing a Managed Server to Power Off

The following example shows how to force the 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 5–15 Forcing a Group of Servers to Power Off

The following 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 managed servers, see "Issuing Remote Commands on Servers and Server Groups" on page 90.

Resetting Managed Servers and Groups

To initiate graceful shutdown of the operating system followed by power off for managed server or group, use the `reset server` or `reset group` commands. The managed 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 group.

For syntax and parameter details, type `help reset server` or `help reset group` at the `N1–ok` command line.

▼ To Reboot a Managed Server or a Group

1 Log in to the N1 System Manager.

2 Use one of the following commands:

```
N1-ok> reset server server [force=true]
```

The managed server is rebooted. See "reset server" in *Sun N1 System Manager 1.3 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 1.3 Command Line Reference Manual* for details.

Example 5–16 Forcing Reset of a Managed Server

The following example shows how to force reset of the OS.

```
N1-ok> reset server 10.5.7.2 force=true
```

Example 5–17 Forcing Reset of a Group

If the OS does not gracefully shut down, the following example shows the forced reset of the operating systems for servers in the group.

```
N1-ok> reset group dev force=true
```

Example 5–18 Rebooting a Managed Server From the Network

The following example shows how to reboot a managed server from the network.

```
N1-ok> reset server 10.5.7.2 netboot=true
```

Example 5–19 Rebooting a Group from the Network

The following 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 managed servers, see "Issuing Remote Commands on Servers and Server Groups" on page 90 for instructions.

Issuing Remote Commands on Servers and Server Groups

This section describes how to issue remote commands on managed server and groups.

To issue a remote command on a managed server or group, use the `start server` or `start group` command with 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 Managed Server or a Group

This procedure describes how to issue a remote command. A *remote command* is a UNIX command that is sent to a managed server to be run on that managed 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 112 for details.

1 Log in to the N1 System Manager.

2 Use one of the following commands:

```
N1-ok> start server server command "command"
```

The remote command is issued on the managed server. See "start server" in *Sun N1 System Manager 1.3 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 1.3 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 5–20 Issuing a Remote Command on a Managed Server

The following 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 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 5–21 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, use a value of zero seconds. 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 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 5–22 Issuing a Remote Command on a Group

The following example shows how to issue a remote command on a server group by using the `start group` command.

```
N1-ok> start group g1 command "/bin/ls -l /"

Job "24" started.
```

The following example shows how view the results of the remote command by using the `show job` 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
```

Connecting to the Serial Console for a Managed Server

To remotely access the serial console for a managed server, use the `connect server` command.

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.

This feature is particularly useful for performing diagnosis before and during the OS deployment and during the server power cycle. For example, the best way to monitor an OS provisioning job is to use the serial console of the system being deployed, as this displays the console output of an OS deployment.

You can perform this operation from the browser interface's Server Details page, as shown in the illustration. To view information about using the browser interface to access the serial console for a server, in the Sun N1 System Manager 1.3 Online Help, find the topic 'To Open the Serial Console for a Server.'

The management server redirects output of the managed server's serial console to the terminal emulator applet that is running in the browser interface.

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.

The serial emulator appears and takes you either to the root prompt or a read-only prompt.

Note – If a managed server is powered off, the console still connects, but no output appears until the managed server is powered on.

To use the Serial Console feature from the Server Details page in the browser interface, the Sun Java Plugin 1.4.2 or later must be installed on the system where you are running the browser. Not all of the supported browsers for the N1 System Manager have the Sun Java Plugin 1.4.2 installed, so you might have to install the plugin.

Note – Use of the serial console is not supported for Sun Fire X2100 servers.

This procedure describes how to remotely access the serial console of managed servers.

EXAMPLE 5–23 Connecting to the Serial Console

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
```

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" in *Sun N1 System Manager 1.3 Operating System Provisioning Guide* and "To Reboot a Managed Server or a Group" on page 89.

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" in *Sun N1 System Manager 1.3 Installation and Configuration Guide*.

Connecting to the Sun ILOM Web GUI for a Managed Server

To remotely access the Sun ILOM Web GUI for a Sun Fire X4000 Series server, use the `connect server` command.

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.

This feature is supported only for Sun Fire X4000 Series servers. Use the `n1smconfig` script to enable auto-log to the ILOM Web GUI. For further information on enabling auto-log to the ILOM Web GUI, and on subsequently disabling it, see "Configuring the N1 System Manager" in *Sun N1 System Manager 1.3 Installation and Configuration Guide*.

This feature is particularly useful for ILOM managed servers, for performing diagnosis before and during the OS installation and during the server power cycle.

You can perform this operation from the browser interface. To view information about using the browser interface to access the Sun ILOM Web GUI for a server, in the Sun N1 System Manager 1.3 Online Help, find the topic 'To Open the Sun ILOM Web GUI for a Sun Fire X4000 Series Server.'

The management server redirects output of the managed server's console to the terminal emulator applet that is running in the browser interface.

The terminal emulator applet that is used by the browser interface for the ILOM Web GUI feature does not provide a certificate-based authentication of the applet. The applet also requires that you enable SSHv1 for the management server.

The 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.

To use the Sun ILOM Web GUI feature from the Server Details page in the browser interface, the Sun Java Plugin 1.4.2 or later must be installed on the managed server where you are running the browser. Not all of the supported browsers for the N1 System Manager have the Sun Java Plugin 1.4.2 installed, so you might have to install the plugin.

This procedure describes how to remotely access the Sun ILOM Web GUI for managed servers of the Sun Fire X4000 series.

Note – Use of the Sun ILOM Web GUI is only supported for Sun Fire X4000 series servers.

EXAMPLE 5–24 Connecting to the Sun ILOM Web GUI

The only way to connect to the Sun ILOM Web GUI is through the simple option in the browser interface. See the Sun N1 System Manager 1.3 Online Help for details.

If the Open ILOM Web GUI menu item does not appear, SSHv1 is not enabled. To enable SSHv1, use the `n1smconfig` utility. See "To Configure the N1 System Manager" in *Sun N1 System Manager 1.3 Installation and Configuration Guide*.

The Sun ILOM Web GUI autlogin feature for Sun Fire X4100 and Sun Fire X4200 servers exposes the server's service processor credentials. See "Security Considerations" in *Sun N1 System Manager 1.3 Installation and Configuration Guide* for details.

After you have opened the Sun ILOM Web GUI, you can view the detailed output during an OS deployment or a power cycle. For instructions, see "Deploying OS Profiles" in *Sun N1 System Manager 1.3 Operating System Provisioning Guide* and "To Reboot a Managed Server or a Group" on page 89.

Refreshing and Finding Managed Servers and Groups

This section describes the following tasks:

Refreshing Managed Server and Group Data

To update managed server and group data, use the `set server` command with 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 Managed Server or a Group

1 Log in to the N1 System Manager.

2 Use one of the following commands:

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

The managed server data is updated. See "set server" in *Sun N1 System Manager 1.3 Command Line Reference Manual* for details.

```
N1-ok> set group group refresh
```

The group data is updated. See "set group" in *Sun N1 System Manager 1.3 Command Line Reference Manual* for details.

Note – Refresh job completion will be longer for server groups.

Finding a Managed Server in a Rack

To illuminate the server's LED locator light, use the `set server` command with the `locator` subcommand. For syntax and parameter details, type `help set server` at the `N1–ok` command line.

▼ To Find a Managed Server in a Rack

This procedure describes how to illuminate the LED locator light on a managed server.

1 Log in to the N1 System Manager.

2 Use the following command:

```
N1-ok> set server server locator=true
```

The LED locator light on the managed server illuminates. See "set server" in *Sun N1 System Manager 1.3 Command Line Reference Manual* for details.

Deleting Managed Servers and Groups

To remove a server or group from the N1 System Manager, use the `delete server` or `delete group` command.

For syntax and parameter details, type `help delete server` or `help delete group` at the `N1–ok` command line.

▼ To Delete a Managed Server or a Group

1 Log in to the N1 System Manager.

2 Use one of the following commands:

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

The managed server is deleted from the N1 System Manager. See "delete server" in *Sun N1 System Manager 1.3 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 managed servers from the N1 System Manager. See "delete group" in *Sun N1 System Manager 1.3 Command Line Reference Manual* for details.

◆ ◆ ◆ CHAPTER 6

Monitoring Servers and Server Groups

The 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. Attributes are associated with three main areas:

- Hardware health attributes. For information about hardware health monitoring, see "Hardware Health Monitoring" on page 103.
- OS resource attributes. For information about OS health monitoring, see "OS Health Monitoring" on page 106.
- Network connectivity, or *reachability*. For information about network reachability monitoring, see "Network Reachability Monitoring" on page 109.

For a managed server or server group, 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. Managed nodes are used only to access data about their health or network reachability.

Introduction to Events and Notifications

Monitoring is connected with the broadcasting of the *events* for each managed server or server group. 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 145. Monitoring data is stored as events in the N1 System Manager database instead of log files.

If monitoring is enabled for a managed servers, each event causes a *notification* to be emitted from the N1 System Manager for that event. Notification rules can be created to notify staff about events that happen with managed servers. See "Setting Up Event Notifications" on page 148 for details.

Monitoring Using SNMP

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, the SNMP agent that is used for data retrieval is based on the Sun Management Center 3.5 software SNMP agent.
- If the management server is running the N1 System Manager on Linux, the SNMP agent that is used for data retrieval is based on the Sun Management Center 3.6 Linux SNMP agent.

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.

The SNMP agent is deployed when operating systems are provisioned on to servers that are managed by the N1 System Manager. 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 two types of polling-based monitoring as a backup:

- 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.

Hardware Health Monitoring

The hardware health of managed servers is monitored by the N1 System Manager. Sensors provided in the hardware of managed servers are used by the N1 System Manager to monitor temperature, voltage, and fan speed. For information about supported hardware, see "Manageable Server Requirements" in *Sun N1 System Manager 1.3 Site Preparation Guide*. For a managed server's hardware health to be monitored by the N1 System Manager, the managed server must have a service processor.

Sensor data is retrieved from the service processor for SPARC devices through the Advanced Lights Out Manager (ALOM) interface. Sensor data is retrieved through the Intelligent Platform Management Interface (IPMI) for x64 servers.

Note – Managed servers that use ALOM do not send data to the management server by use of traps. Instead, managed servers that use ALOM send management data by email. To ensure that the management server collects data from these servers, the management server has its own port 25 email server.

The following characteristics of a managed server's 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)
- Hard disks and memory. Monitoring of hard disks and memory is only possible for some hardware types. See Table 6–1 for more information

---

Note – The N1 System Manager does not monitor RAID controller states.

All details for a managed server's hardware health, where available, are displayed in the hardware monitoring table on the Server Details page of the browser interface, and in the Event Log.

TABLE 6–1 Hard Disk and Memory Failure Monitoring

Type	Disk Monitoring	Memory Failure Monitoring
ALOM servers: Netra 240 and Netra 440	None	None
ALOM servers: Sun Fire V210, V240 and V440	None	None
ALOM servers: Sun Fire T1000 and T2000	None	None

TABLE 6–1 Hard Disk and Memory Failure Monitoring *(Continued)*

Type	Disk Monitoring	Memory Failure Monitoring
IPMI server: Sun Fire X2100	None	None
ILOM servers: X4100 and X4200	Yes	Yes
IPMI servers: Sun Fire V20z and V40z	None	Yes

A detailed list of hardware health sensors is provided in the documentation that accompanies your hardware.

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 1.3 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 Managed Servers" on page 83.

The locator lights for Sun Fire X2100, X4100 and X4200 servers can be switched on or off using the N1 System Manager. You can switch on or off a managed server's locator light by using the `set server` command:

```
N1-ok> set server server locator locator-state
```

The *locator-state* value can be either *on* or *off*. For a group of servers, use the `set group` command with the group's name.

Hardware Memory Problems on Sun Fire V20z and V40z Managed Servers

Memory problems on the Sun Fire V20z and V40z managed servers are handled differently by the N1 System Manager. Sun Fire V20z and V40z memory problems, if they occur, are detected by polling through the managed server's service processor.

A memory error has occurred on a Sun Fire V20z or V40z server if all of the following are true:

- The Sun Fire V20z or V40z managed server's status in the Server Details of the browser interface shows a warning or critical state
- No sensors for the managed server are in the warning or critical state
- No detail about the event is provided in the event log, but there is a memory event error shown by the server's service processor.

If a memory error has occurred, see the example on how to correct it. To avoid false warning statuses in the future, the service processor's event log must be cleared after the defective memory has been replaced or repaired.

EXAMPLE 6–1 Examining Memory Errors on Sun Fire V20z or V40z Managed Servers

If a memory error has occurred on a Sun Fire V20z or V40z managed server, log into the server's service processor.

```
# ssh -l admin 10.0.3.2
```

Enter the password and check the managed server's status.

```
# sp get status
```

Check the service processor's event log.

```
# sp get events
ID Last Update      Component Severity      Message
1  01/01/1970 00:02 SP        informational SP localhost.localdomain IP is now set to 0.0.0.0
2  01/01/1970 18:47 SP        informational SP localhost.localdomain IP is now set to 0.0.0.0
3  01/01/1970 18:47 SP        informational SP localhost.localdomain IP is now set to 10.0.3.2
```

Clear the service processor's event log.

```
# sp delete event -a
```

Hardware Sensor Attributes

For x64 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.

To receive notifications for events from discrete sensors, create a notification rule and subscribe to the `Ereport.Physical.ThresholdExceeded` topic, as described in "Setting Up Event Notifications" on page 148.

For Sun Fire X4100 and Sun Fire X4200 servers, refer to the hardware documentation for to see the monitored hardware sensors.

For Sun Fire X2100 servers, only sensors describing fan speed, voltage, and temperature are used to retrieve data. Here is a list of sensors that are monitored for SP firmware version 4.11:

```
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
```

For X2100 servers with SP firmware versions previous to version 4.11, `CPU Core Voltage` was called `CPU Voltage`.

OS Health Monitoring

OS health can be monitored by the N1 System Manager.

Two distinct levels of OS Monitoring are possible with the N1 System Manager. These are as follows:

Base management	This feature provides support for basic OS monitoring. The base management feature also provides support for OS updates and remote command execution. For more information, see "Base Management (Basic OS Monitoring)" on page 107.
Full OS Monitoring	This feature provides support for basic OS monitoring, and provides support for threshold monitoring. For more information, see "Full OS Monitoring (With Thresholds)" on page 108.

Supported Operating Systems for OS Monitoring

All of the operating systems listed in "Manageable Server Requirements" in *Sun N1 System Manager 1.3 Site Preparation Guide* can be monitored by the N1 System Manager, with the exception of Microsoft Windows.

Note – OS monitoring of managed servers running Microsoft Windows is not possible in this release.

For supported versions of the Solaris operating system:

When choosing which distribution groups to install, note that `Entire Distribution plus OEM support` must be chosen. All other distribution groups do not contain the necessary packages to support OS monitoring using the N1 System Manager.

For supported versions of the Red Hat Linux operating system:

When choosing which distribution groups to install, note that `Everything` must be chosen. All other distribution groups do not contain the necessary packages to support OS monitoring using the N1 System Manager.

For supported versions of the SUSE operating system:

When choosing which distribution groups to install, note that `Default Installation` must be chosen. All other distribution groups do not contain the necessary packages to support OS monitoring using the N1 System Manager.

Base Management (Basic OS Monitoring)

As part of the `add server feature` command, with the `basemanagement` and `agentip` keywords, you provide support for base management and you provide credentials to access the monitored server's operating system through `ssh` with the `agentssh` keyword. See "To Add the Base Management Feature" on page 113 for additional details. This procedure is important for basic OS health monitoring but not for monitoring hardware health or network reachability.

Adding the base management feature using the `add server feature` command, with the `basemanagement` keyword provides support for base management, 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 125 for more information.

The base management feature provides basic OS monitoring, but does not provide support for monitoring of thresholds. For the monitoring of thresholds, the full OS monitoring feature must be added. See "Full OS Monitoring (With Thresholds)" on page 108 for details.

With the base management feature, 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. (Individual swap partitions cannot be monitored)
- File system used and space available, as percentages

For more information about these monitored attributes, see Table 6–2.

The base management feature also provides support for remote command execution. See "Issuing Remote Commands on Servers and Server Groups" on page 90 for details. In addition, the base management feature provides support for OS updates. see Chapter 5, "Managing Packages, Patches, and RPMs," in *Sun N1 System Manager 1.3 Operating System Provisioning Guide* for information about OS updates.

Full OS Monitoring (With Thresholds)

As part of the `add server feature` command, with the `osmonitor` and `agentip` keywords, 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 114 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 using the `add server feature` command, with the `osmonitor` keywords provides support for *both* OS monitoring and base management, 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 125 for more information.

The OS monitoring feature provides all the basic monitoring data that comes with the base management feature. See "Base Management (Basic OS Monitoring)" on page 107 for details about the base management feature. In addition, the OS monitoring feature provides support for *threshold monitoring*. The OS monitoring feature 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 134 for details. For information about thresholds, see "Monitoring Threshold Values" on page 130.

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.

A complete list of OS health attributes is provided in Table 6–2. Associated supported thresholds are also provided.

TABLE 6–2 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`

TABLE 6–2 All OS Health Attributes *(Continued)*

Attribute Name	Description	Supported Threshold	Supported Threshold
`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`

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 1.3 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 Managed Servers" on page 83.

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 Managed Servers" on page 110.

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 6–9 shows you how to accomplish this disabling action.

Network Reachability Monitoring

All management interfaces of managed 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.

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 1.3 Command Line Reference Manual* for details.

Understanding the Differences Between `Unreachable` and `Unknown` States for Managed Servers

Distinguishing between the unreachable and unknown states for managed servers is important.

```
N1-ok> show server oshealth unreachable
```

This command lists all managed servers that are unreachable. Any managed 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 managed 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 managed 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 managed 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 managed 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 managed 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 OS Monitoring

Before full monitoring of a managed server can be enabled, OS monitoring must be supported for that server. OS 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 managed 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 1.3 Command Line Reference Manual* and "load server" in *Sun N1 System Manager 1.3 Command Line Reference Manual* for details.

Note – If the `load server` or `load group` command is used to install software on the managed server, and the managed 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`.

If you set 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 118.

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 112.

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 the `set server monitored` command is executed without the OS monitoring feature first being installed. See "Enabling and Disabling Monitoring" on page 125 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 OS profiles installed on managed servers, 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 OS 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 125.

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 full OS health monitoring and inventory management. For more information, see "Full OS Monitoring (With Thresholds)" on page 108.

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. For more information about jobs, see "Managing Jobs" on page 136.

This section describes the following tasks:

Note – Many of the tasks in this section require credentials to be entered at the command line. The credentials are those of the manageable server and not those of the service processor.

▼ 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, and provides basic OS monitoring. For more information about base management, see "Base Management (Basic OS Monitoring)" on page 107.

Note – Uninstallation of the base management feature is not supported.

The agent IP used in this procedure is the IP address of the managed 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 118.

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 1.3 Command Line Reference Manual* or "load group" in *Sun N1 System Manager 1.3 Command Line Reference Manual* for details.

Before You Begin

- Discover servers. See Chapter 4.
- Load an OS if an OS is not already installed. See "To Load an OS Profile on a Server or a Server Group" in *Sun N1 System Manager 1.3 Operating System Provisioning Guide* and "load server" in *Sun N1 System Manager 1.3 Command Line Reference Manual*.

1 Log in to the N1 System Manager.

See "To Access the N1 System Manager Command Line" on page 14 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 1.3 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 114

▼ To Add the OS Monitoring Feature

This procedure describes how to add the OS monitoring feature on a server.

If you submit `add server feature` commands by using a script, see Example 6–4 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 1.3 Command Line Reference Manual* or "load group" in *Sun N1 System Manager 1.3 Command Line Reference Manual* for details.

Before You Begin

- Discover servers. See Chapter 4.
- Load an OS if one is not already installed, see "To Load an OS Profile on a Server or a Server Group" in *Sun N1 System Manager 1.3 Operating System Provisioning Guide* and "load server" in *Sun N1 System Manager 1.3 Command Line Reference Manual*.

1 Log in to the N1 System Manager.

See "To Access the N1 System Manager Command Line" on page 14 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 1.3 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.

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 Failed Critical status clears 5-7 minutes after adding or upgrading the OS monitoring feature.

If no monitoring data is available for the server, see "Monitoring Problems" in *Sun N1 System Manager 1.3 Troubleshooting Guide*.

If the managed server's IP address changes, use the `set server` command again before enabling or disabling monitoring

Example 6–2 Adding the OS Monitoring Feature to Managed Servers Discovered by SP-Based Discovery

The following example shows how to add the OS monitoring feature to a server that had an OS installed prior to being discovered through SP-Based discovery.

```
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 managed 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.

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 through its SP.

```
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
```

See "SP-Based Discovery" on page 51 for details about this method of discovering servers.

Example 6–3 Adding the OS Monitoring Feature to Servers Discovered by OS-Based Discovery

The following example shows how to add the OS monitoring feature to a server that had an OS installed before being discovered by OS-based discovery.

```
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 managed 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.

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 by OS-based discovery.

```
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
```

See "OS-Based Discovery" on page 59 for details about this method of discovering servers.

Example 6–4 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 managed server. Then, retry the `add server feature osmonitor agentip` command. See "To Update the ssh_known_hosts File" in *Sun N1 System Manager 1.3 Troubleshooting Guide* for details.

The problem of stale SSH entries on the management server can be avoided if, during the `n1smconfig` configuration process, you modify SSH policies by accepting changed or unknown host keys. Accepting changed or unknown host keys carries a security risk but avoids the problem of stale SSH entries on the management server. For more information, see "To Configure the N1 System Manager" in *Sun N1 System Manager 1.3 Installation and Configuration Guide*.

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 managed 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 managed 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.

---

1 Log in to the N1 System Manager.

See "To Access the N1 System Manager Command Line" on page 14 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 1.3 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 116 for details.

When you remove the base management feature, the feature is uninstalled from the managed 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.

---

1 Log in to the N1 System Manager.

See "To Access the N1 System Manager Command Line" on page 14 for details.

2 Remove the OS monitoring feature.

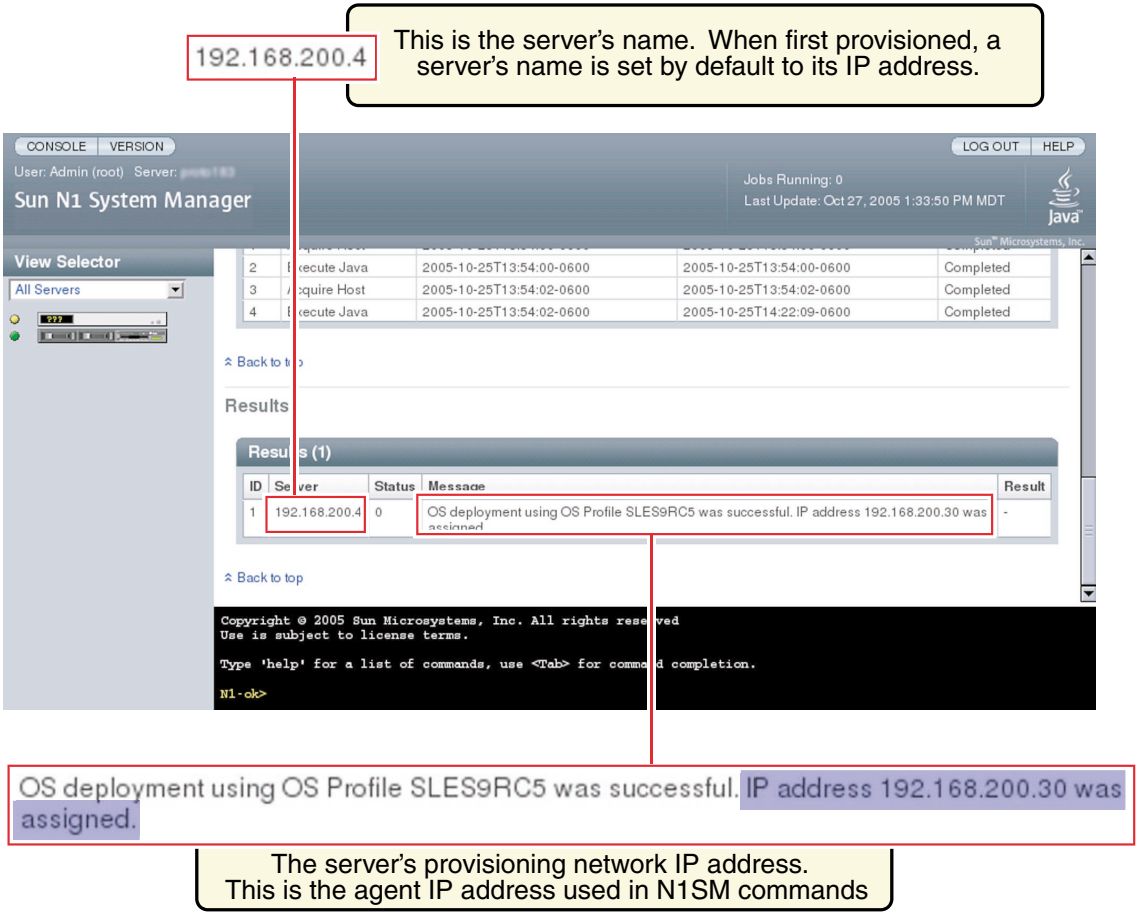
```
N1-ok> remove server server feature basemanagement
```

The necessary packages and scripts are removed. See "remove server" in *Sun N1 System Manager 1.3 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 managed server's network interface, which is to be monitored by the management server. This interface is usually the server's *provisioning network interface*. 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 managed 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 managed server, the managed server's `networktype` attribute could be set to `dhcp`. This setting means that the server uses DHCP to get its provisioning network IP address. If the system reboots and obtains a different IP address than the one that was used for the `agentip` parameter during the `load` command or `add server` 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.

1 Log in to the N1 System Manager.

See "To Access the N1 System Manager Command Line" on page 14 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 1.3 Command Line Reference Manual* for details about command syntax. This operation touches the managed 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 managed 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 managed 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.

1 Log in to the N1 System Manager.

See "To Access the N1 System Manager Command Line" on page 14 for details. You need to have an SSH login and password for this step. Default SSH login/password pairs are provided in "SP-Based Discovery" 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 1.3 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 managed server. These credentials, specifically for the base management and OS monitoring features for a managed 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 101 for more information about the SNMP agents for OS monitoring in the N1 System Manager.

1 Log in to the N1 System Manager.

See "To Access the N1 System Manager Command Line" on page 14 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 1.3 Command Line Reference Manual* for details about command syntax.

This `set server` operation does not actually touch the managed 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 managed server. These credentials, specifically for the base management and OS monitoring features for a managed 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 101 for more information about the SNMP agents for OS monitoring in the N1 System Manager.

1 Log in to the N1 System Manager.

See "To Access the N1 System Manager Command Line" on page 14 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 1.3 Command Line Reference Manual* for details about command syntax.

   This `set server` operation does not actually touch the managed 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 managed server:

1. **Log in to the managed 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 managed server.

1. **Log in to the managed 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 only necessary after upgrading the N1 System Manager from a previous release, for managed servers that still run the earlier version of the base management feature included N1 System Manager 1.1 or Sun Management Center 3.5.1. This procedure is for individual servers. You can upgrade the base management feature on multiple servers at once. See Chapter 3, "Upgrading the Sun N1 System Manager Software," in *Sun N1 System Manager 1.3 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 with the `update` keyword, this procedure is not necessary.

Use the `add server feature basemanagement` command with the `upgrade` keyword to upgrade a managed server to a new version from the existing base management feature.

If you submit `add server feature` commands by using a script, see Example 6–4 for an example.

Before You Begin

- Discover servers. See Chapter 4.
- This base management feature upgrade procedure applies to managed servers on which the base management feature is already installed by a previous version of the N1 System Manager.

1 Log in to the N1 System Manager.

See "To Access the N1 System Manager Command Line" on page 14 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 1.3 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 125 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 managed server. Then, retry the `add server feature osmonitor agentip` command. See "To Update the ssh_known_hosts File" in *Sun N1 System Manager 1.3 Troubleshooting Guide* for details.

The problem of stale SSH entries on the management server can be avoided if, during the `n1smconfig` configuration process, you modify SSH policies by accepting changed or unknown host keys. Accepting changed or unknown host keys carries a security risk but avoids the problem of stale SSH entries on the management server. For more information, see "To Configure the N1 System Manager" in *Sun N1 System Manager 1.3 Installation and Configuration Guide*.

▼ 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 only necessary after upgrading the N1 System Manager from a previous release, for managed servers that still run the earlier version of the OS monitoring feature included N1 System Manager 1.1 or Sun Management Center 3.5.1. This procedure is for individual servers. You can upgrade the OS monitoring feature on multiple servers at once. See Chapter 3, "Upgrading the Sun N1 System Manager Software," in *Sun N1 System Manager 1.3 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 with the `update` keyword, this procedure is not necessary.

Use the `add server feature osmonitor` command with the `upgrade` keyword to upgrade a managed 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 6–4 for an example.

Before You Begin

- Discover servers. See Chapter 4.
- This OS monitor feature upgrade procedure applies to managed servers on which the OS is already installed by a previous version of the N1 System Manager.

1 Log in to the N1 System Manager.

See "To Access the N1 System Manager Command Line" on page 14 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 1.3 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 managed 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 managed server. Then, retry the `add server feature osmonitor agentip` command. See "To Update the ssh_known_hosts File" in *Sun N1 System Manager 1.3 Troubleshooting Guide* for details.

The problem of stale SSH entries on the management server can be avoided if, during the `n1smconfig` configuration process, you modify SSH policies by accepting changed or unknown host keys. Accepting changed or unknown host keys carries a security risk but avoids the problem of stale SSH entries on the management server. For more information, see "To Configure the N1 System Manager" in *Sun N1 System Manager 1.3 Installation and Configuration Guide*.

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.

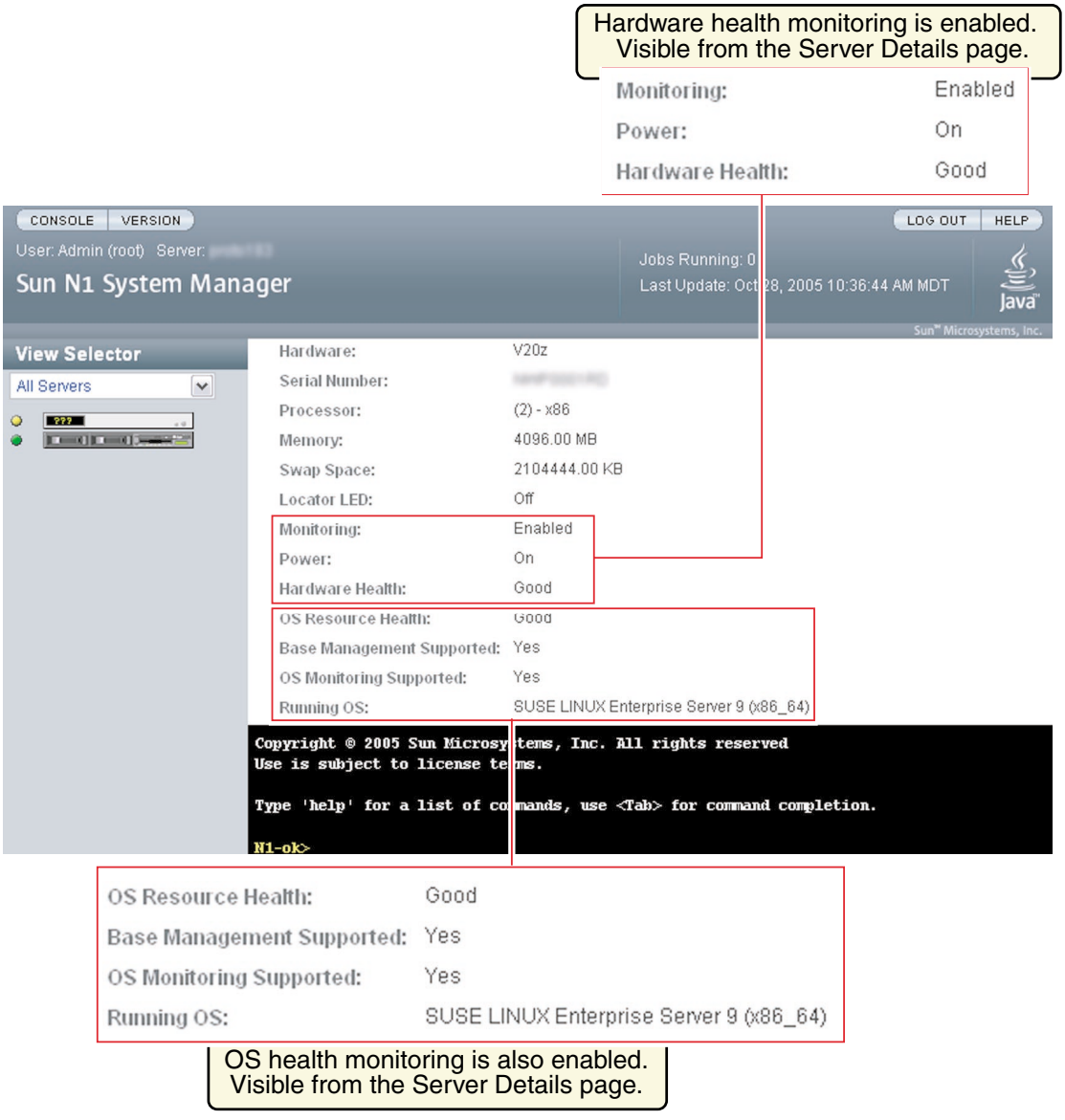
Enabling and Disabling Monitoring

Monitored file system and OS health data for a managed server is *not* available unless an operating system is deployed on the managed 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 OS Monitoring" on page 111.

Use the `set server monitored` command to enable or disable monitoring. See "Enabling and Disabling Monitoring" on page 125. 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 Managed Server or a Managed 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 managed server or a group of managed servers 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 managed server or a group of managed servers, then only hardware health monitoring is enabled.

Note – It can take up to one minute for monitoring to be enabled after running the command in this procedure.

Before You Begin To enable the management agent IP and security credentials on a managed server named *server*, add the management features on themanaged server or a group of managed servers as explained in "Supporting OS Monitoring" on page 111.

1 Log in to the N1 System Manager.

See "To Access the N1 System Manager Command Line" on page 14 for details.

2 Set the `monitored` attribute to `true`.

- **Use the `set server` command.**

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

  In this procedure, *server* is the name of the managed server that you want to monitor.

- **For a group of managed servers, 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 managed servers that you have already named. See "set group" in *Sun N1 System Manager 1.3 Command Line Reference Manual* for details. In this procedure, *group* is the name of the group of managed servers that you want to monitor.

3 View the details to determine if monitoring is enabled.

- **View the managed server details.**

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

- **For a server group, view the managed server group details to determine if monitoring is enabled for each managed 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 130.

▼ To Disable Monitoring for a Managed Server or a Managed 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 managed server or a group of managed servers. Hardware health and OS health monitoring are both disabled with this command, provided that the OS monitoring feature has been added.

Note – It can take up to one minute for monitoring to be disabled after running the command in this procedure.

You might want to disable monitoring of a hardware component to perform maintenance tasks without generating events.

1 Log in to the N1 System Manager.

See "To Access the N1 System Manager Command Line" on page 14 for details.

2 Set the `monitored` attribute to `false`.

- **Use the `set server` command.**

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

  In this example, *server* is the name of the managed server that you want to stop monitoring. Executing this command disables monitoring of the server. With monitoring of a managed server disabled, the violation of threshold values by attributes related to that managed 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 managed servers that you have already named. See "set group" in *Sun N1 System Manager 1.3 Command Line Reference Manual* for details. In this procedure, *group* is the name of the group of managed servers for which you want to disable monitoring.

3 View the details to determine that monitoring is disabled.

- **View the managed server details.**

  The output shows that monitoring is disabled.

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

  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 6–9 shows how to accomplish this task. For general information about threshold values, see "Monitoring Threshold Values" on page 130. You can also remove the OS health monitoring feature. See "To Remove the OS Monitoring Feature" on page 116.

- **For a group of managed servers, view the managed server group details to determine if monitoring is disabled for each managed 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 managed server or other hardware is discovered, monitoring of the managed server or other hardware is enabled by default. Before a manageable server can be monitored, however, it must be discovered and correctly registered with the N1 System Manager. This process is described in Chapter 4. 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 managed 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 managed server is rediscovered, monitoring is set to `true` by default. This is true only for servers that were discovered by SP-based discovery.

Default status of OS health monitoring
: Disabled by default. When an OS has been successfully provisioned on a managed 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 6–9 shows how to accomplish this task. For general information about threshold values, see "Monitoring Threshold Values" on page 130.

Default status of network reachability monitoring
: When the management interface of the managed 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 Managed Servers" on page 110.

The `nonrecoverable`, `critical`, `warning`, and `unknown` statuses are represented by alarms displayed in the browser interface.

The values `nonrecoverable`, `critical`, and `warning` are discussed in "show server" in *Sun N1 System Manager 1.3 Command Line Reference Manual*.

Threshold values for OS health attributes can be configured at the command line. This process is explained in "Setting Threshold Values" on page 134. 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.

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`.

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 148.

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 112.

1 Log in to the N1 System Manager.

See "To Access the N1 System Manager Command Line" on page 14 for details.

2 Type the `show server` command:

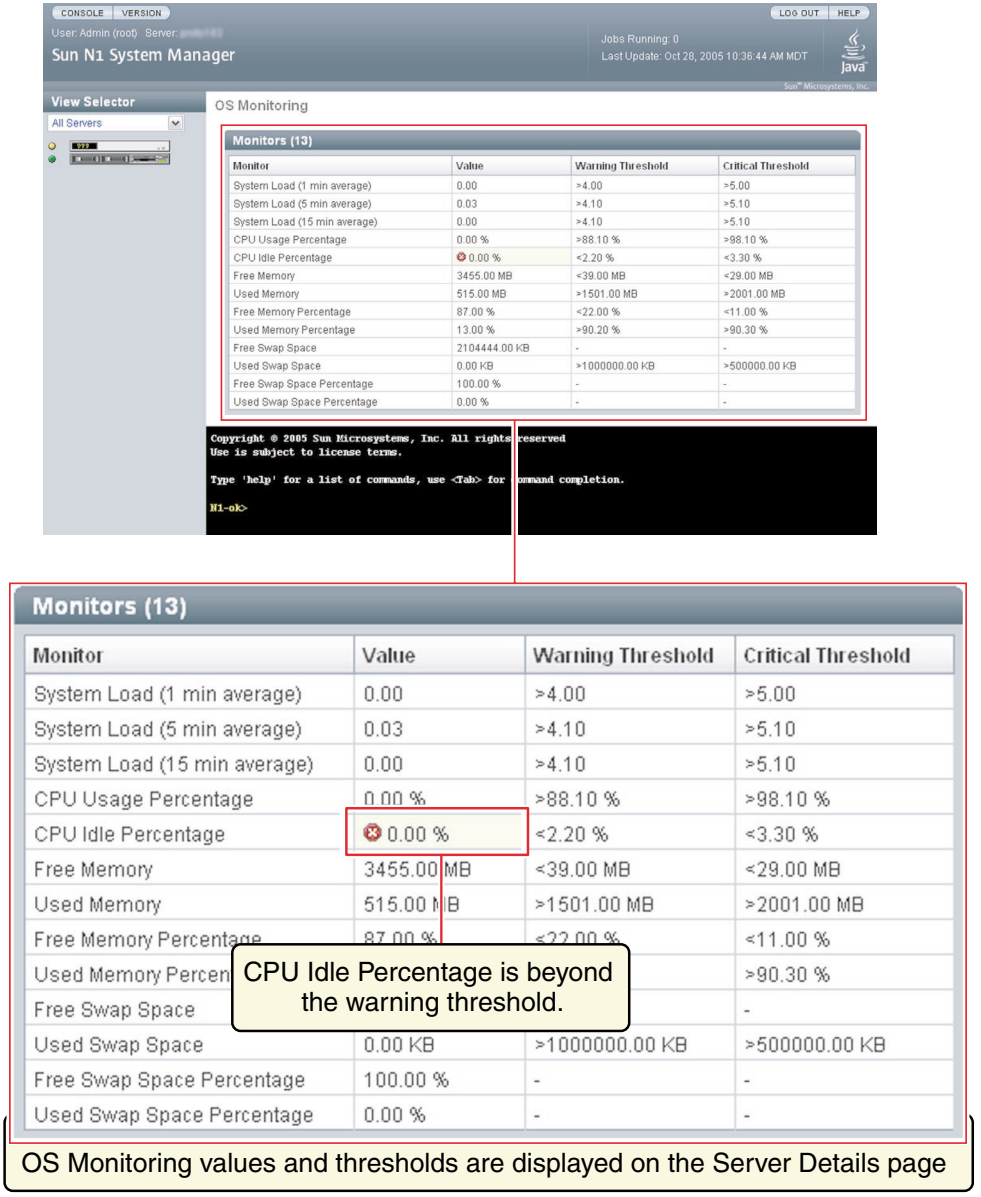
```
N1-ok> show server server
```

In this procedure, *server* is the name of the managed 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 1.3 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.**



OS Monitoring values and thresholds are displayed on the Server Details page

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 6–3 lists default values for these OS health attributes.

Note – Setting or modifying threshold values for hardware health attributes is *not* supported in this version of the Sun N1 System Manager.

TABLE 6–3 Factory-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 134.

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 overwrites 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 112.

1 Log in to the N1 System Manager.

See "To Access the N1 System Manager Command Line" on page 14 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 106 and listed in Table 6–2.

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 managed 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 6–5 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 managed 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 6–6 Setting Multiple Threshold Values for File System Percentage Usage On a Server

This example sets the file system percentage usage `warninghigh` threshold on a managed 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 6–7 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 managed server named `serv1` to 150 Kbytes of free space.

```
N1-ok> set server serv1 filesystem /var threshold fsusage.kbspacefree warninghigh 150
```

Example 6–8 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 managed server named `serv1` to 5%.

```
N1-ok> set server serv1 threshold memusage.pctmemused criticalhigh 5
```

Example 6–9 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 managed 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 6–10 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 managed 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 Management Information Bases (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 6–11 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 managed 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 1.3 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.
- `removeserver` – Server deletion.
- `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 1.3 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

1 Log in to the N1 System Manager.

See "To Access the N1 System Manager Command Line" on page 14 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 1.3 Command Line Reference Manual* for details.

Example 6–12 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

1 Log in to the N1 System Manager.

See "To Access the N1 System Manager Command Line" on page 14 for details.

2 View a specific job.

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

Detailed information about the job appears in the output.

- **You can also filter jobs based on their Job Type.**

  ```
  N1-ok> show job type
  ```

  See "show job" in *Sun N1 System Manager 1.3 Command Line Reference Manual* for details.

Example 6–13 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.
```

Example 6–14 Viewing all OS Monitoring Jobs

This example shows how to use the `show job` command with the `addosmonitor` Job Type to filter all jobs that add OS monitoring support.

```
N1-ok> show job type addosmonitor
```

▼ To Stop a Job

1 Log in to the N1 System Manager.

See "To Access the N1 System Manager Command Line" on page 14 for details.

2 Stop a specific job.

```
N1-ok> stop job job
```

The job is stopped.

See "stop job" in *Sun N1 System Manager 1.3 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 1.3 Command Line Reference Manual* for details.

Example 6–15 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 Managed Server or a Group" on page 90

▼ To Delete a Job

1 Log in to the N1 System Manager.

See "To Access the N1 System Manager Command Line" on page 14 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 1.3 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 1.3 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 1.3 Command Line Reference Manual* for details.

Example 6–16 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 6–17 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. A global limit governs 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 1000.

TABLE 6–4 Job Weight Values

Job	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

TABLE 6–4 Job Weight Values *(Continued)*

Job	Weight
Server Power Off	200
Server Power On	200
Server Refresh	200
Set Server Feature	200
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 1.3 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 101 for more information about monitoring.

See "Setting Up Event Notifications" on page 148 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 – Servers that use ALOM do not send event notifications to the management server by use of traps. Instead, they send event notifications by email. To ensure that the management server collects data from these servers, the N1 System Manager management server has its own port 25 email server.

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" in *Sun N1 System Manager 1.3 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 148 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 1.3 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

1 Log in to the N1 System Manager.

See "To Access the N1 System Manager Command Line" on page 14 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 1.3 Command Line Reference Manual* for details.

See Also "Event Log Overview" on page 146

▼ To Filter the Event Log

1 Log in to the N1 System Manager.

See "To Access the N1 System Manager Command Line" on page 14 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 1.3 Command Line Reference Manual* for details.

▼ To View Event Details

1 Log in to the N1 System Manager.

See "To Access the N1 System Manager Command Line" on page 14 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 1.3 Command Line Reference Manual* for details.

Example 6–18 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 managed 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" in *Sun N1 System Manager 1.3 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 that might occur, about

which you are interested. Subscribe to a *topic* to create an event notification. For example, to receive notifications for discrete sensor events, subscribe to the `Ereport.Physical.ThresholdExceeded` topic. This topic covers events for both discrete sensors and bi-state sensors. For a list of topics, and to see the mapping of event categories to actual events, see "create notification" in *Sun N1 System Manager 1.3 Command Line Reference Manual*.

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 136.

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 managed 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 1.3 Command Line Reference Manual* for more details of the terms used in this command syntax.

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

1 Log in to the N1 System Manager.

See "To Access the N1 System Manager Command Line" on page 14 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 1.3 Command Line Reference Manual* for details.

▼ To View Event Notification Details

1 Log in to the N1 System Manager.

See "To Access the N1 System Manager Command Line" on page 14 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 1.3 Command Line Reference Manual* for details.

Example 6–19 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.

1 Log in to the N1 System Manager.

See "To Access the N1 System Manager Command Line" on page 14 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 1.3 Command Line Reference Manual* for details.

Example 6–20 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

1 Log in to the N1 System Manager.

See "To Access the N1 System Manager Command Line" on page 14 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 1.3 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 1.3 Command Line Reference Manual* for details.

You can also create a notification that is triggered by a script. See "To Create a Notification That is Triggered by a Script" on page 153 for details.

Example 6–21 Creating an Email Notification for Server Groups Being Created

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" in *Sun N1 System Manager 1.3 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  Lifecycle.Logical.CreateGroup       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. Otherwise, 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 6–22 Creating an SNMP Notification for Hardware Health Thresholds Being Exceeded

This example shows how to create an event notification to be sent by SNMP if a hardware health threshold 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 topic, which is the type of event to trigger the notification, is Ereport.Physical.ThresholdExceeded

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
```

Example 6–23 Creating an Email Notification for Hardware State Changes

This example shows how to create an event notification to be sent by email if a server's hardware state changes. Hardware state changes include power state changes, such as a power supply failure. Note that an SMTP email server must first be configured using the `n1smconfig` utility as described in "Configuring the N1 System Manager" in *Sun N1 System Manager 1.3 Installation and Configuration Guide*.

The event notification is called `notif44`. The recipient's email address is `nobody@sun.com`

```
N1-ok> create notification notif44 destination nobody@sun.com
EReport.Physical.ThresholdExceeded 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
notif44 EReport.Physical.ThresholdExceeded  nobody@sun.com    enabled
```

Verify if the SMTP server is configured correctly and is reachable, and if the email address used in the notification rule is valid.

▼ To Create a Notification That is Triggered by a Script

You can create a notification rule for an event that triggers the execution of a Borne shell script on the management server. The Borne shell script must be executable by the root user.

The script should be written to direct its output (`stdout`/`stderr`) to a log file.

The fields of the event are passed into the script as environment variables:

- `N1SM_SCRIPT_DESCRIPTION`
- `N1SM_SCRIPT_TOPIC`
- `N1SM_SCRIPT_USER`
- `N1SM_SCRIPT_TIME`
- `N1SM_SCRIPT_SUBJECT`
- `N1SM_SCRIPT_SOURCE`
- `N1SM_SCRIPT_SEVERITY`

1 Log in to the N1 System Manager.

See "To Access the N1 System Manager Command Line" on page 14 for details.

2 Type the following command:

```
N1-ok> create notification notification destination destination topic topic
type script
```

The event notification is created and enabled. The *destination* must be a fully qualified path to a custom Bourne shell script used to manage the notification. The script must be executable by the root user. See "create notification" in *Sun N1 System Manager 1.3 Command Line Reference Manual* for details and valid topics.

If the script is executed as a result of an event triggered internally by the N1 System Manager, the script is executed as root.

If the script is executed as a result of an event triggered by a user, the script is executed by the user that triggered the event.

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 1.3 Command Line Reference Manual* for details.

▼ To Delete an Event Notification

1 Log in to the N1 System Manager.

See "To Access the N1 System Manager Command Line" on page 14 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

1 Log in to the N1 System Manager.

See "To Access the N1 System Manager Command Line" on page 14 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 1.3 Command Line Reference Manual* for details.

▼ To Stop an Event Notification

1 Log in to the N1 System Manager.

See "To Access the N1 System Manager Command Line" on page 14 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 1.3 Command Line Reference Manual* for details.

Index

O

P

R

S

T

U

V

W