



Sun N1 System Manager 1.1 Administration Guide

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

Part No: 819-2666
September 2005

Copyright 2005 Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 U.S.A. All rights reserved.

This product or document is protected by copyright and distributed under licenses restricting its use, copying, distribution, and decompilation. No part of this product or document may be reproduced in any form by any means without prior written authorization of Sun and its licensors, if any. Third-party software, including font technology, is copyrighted and licensed from Sun suppliers.

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

Sun, Sun Microsystems, the Sun logo, docs.sun.com, AnswerBook, AnswerBook2, N1, Sun Fire, JDK, Netra, Sun Enterprise and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc. Netscape Navigator and Mozilla is a trademark or registered trademark of Netscape Communications Corporation in the United States and other countries.

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

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

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

Copyright 2005 Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 U.S.A. Tous droits réservés.

Ce produit ou document est protégé par un copyright et distribué avec des licences qui en restreignent l'utilisation, la copie, la distribution, et la décompilation. Aucune partie de ce produit ou document ne peut être reproduite sous aucune forme, par quelque moyen que ce soit, sans l'autorisation préalable et écrite de Sun et de ses bailleurs de licence, s'il y en a. Le logiciel détenu par des tiers, et qui comprend la technologie relative aux polices de caractères, est protégé par un copyright et licencié par des fournisseurs de Sun.

Des parties de ce produit pourront être dérivées du système Berkeley BSD licenciés par l'Université de Californie. UNIX est une marque déposée aux Etats-Unis et dans d'autres pays et licenciée exclusivement par X/Open Company, Ltd.

Sun, Sun Microsystems, le logo Sun, docs.sun.com, AnswerBook, AnswerBook2, N1, Sun Fire, JDK, Netra, Sun Enterprise et Solaris sont des marques de fabrique ou des marques déposées, de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pays. Toutes les marques SPARC sont utilisées sous licence et sont des marques de fabrique ou des marques déposées de SPARC International, Inc. aux Etats-Unis et dans d'autres pays. Les produits portant les marques SPARC sont basés sur une architecture développée par Sun Microsystems, Inc. Netscape Navigator et Mozilla sont des marques de Netscape Communications Corporation aux Etats-Unis et dans d'autres pays.

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

CETTE PUBLICATION EST FOURNIE "EN L'ETAT" ET AUCUNE GARANTIE, EXPRESSE OU IMPLICITE, N'EST ACCORDEE, Y COMPRIS DES GARANTIES CONCERNANT LA VALEUR MARCHANDE, L'APTITUDE DE LA PUBLICATION A REpondre A UNE UTILISATION PARTICULIERE, OU LE FAIT QU'ELLE NE SOIT PAS CONTREFAISANTE DE PRODUIT DE TIERS. CE DENI DE GARANTIE NE S'APPLIQUERAIT PAS, DANS LA MESURE OU IL SERAIT TENU JURIDIQUEMENT NUL ET NON AVENU.



050829@12762



Contents

Preface 17

1 Managing the N1 System Manager on the Management Server 23

Introduction to Accessing the N1 System Manager 23

Command Line Tips 24

- ▼ To Access the N1 System Manager Command Line 25
- ▼ To Access the N1 System Manager Browser Interface 26
- ▼ To Show Your Current Session Role 27
- ▼ To Switch Your Session Role 27
- ▼ To Exit the N1 System Manager Command Line 28
- ▼ To Run a Script of N1 System Manager Commands 28

Introduction to N1 System Manager User Security 29

Security Administrator Rules 33

Managing Users 34

- ▼ To Add an N1 System Manager User 35
- ▼ To Delete an N1 System Manager User 35
- ▼ To Set a User's Default Role 36
- ▼ To Show a User's Default Role 36
- ▼ To Add a Role to a User 37
- ▼ To Remove a Role From a User 37
- ▼ To List the Roles Added to a Specific User 37

Managing Roles 38

- ▼ To Create a Role 39
- ▼ To Delete a Role 39
- ▼ To Add a Privilege to a Role 40
- ▼ To Remove a Privilege From a Role 40

▼ To List the Available Roles	40
▼ To List Privileges Added to a Role	41
▼ To List the Roles Added to All Users	41
▼ To List the Available Privileges	41
Backing Up and Restoring N1 System Manager Database and Configuration Files	42
▼ To Back Up the N1 System Manager Database and Configuration Files	42
▼ To Restore the N1 System Manager Database and Configuration Files	43
2 Discovering, Grouping, and Replacing Servers in the Sun N1 System Manager	47
Discovering Servers	47
▼ To Discover New Servers	49
Creating and Maintaining Server Groups	53
Creating Groups and Adding Servers to Groups	54
▼ To Create a Server Group	54
▼ To Add a Server to a Group	55
Removing Servers From Groups	55
▼ To Remove a Server From a Group	55
Replacing Provisionable Servers	56
▼ To Replace a Server	56
3 Provisioning Operating Systems, OS Updates, and Firmware Updates	57
Introduction to OS Provisioning	57
Supported Operating Systems on Provisionable Servers	60
Provisioning the Solaris 10 Operating System	62
▼ To Provision the Solaris 10 OS	62
Managing OS Distributions	65
Copying OS Distributions and Flash Archives	66
▼ To Copy an OS Distribution From ISO Files	66
▼ To Copy an OS Distribution From CDs or a DVD	67
▼ To Copy a Flash Archive to the Management Server	69
▼ To Delete an OS Distribution	71
Managing OS Profiles	71
Creating, Listing, and Modifying OS Profiles	71
Default OS Profiles	72
▼ To List the Available OS Profiles	74
▼ To Create an OS Profile	74

▼ To Clone an Existing OS Profile	76
▼ To Modify an OS Profile	77
▼ To Delete an OS Profile	78
Installing OS Distributions by Deploying OS Profiles	79
Deploying OS Profiles	79
▼ To Load an OS Profile on a Server or a Server Group	81
Adding Base and OS Management Features	84
▼ To Add the Base Management Feature	84
▼ To Add the OS Monitoring Feature	85
▼ To Remove the OS Monitoring Feature	87
▼ To Modify the Agent IP for a Server	88
▼ To Manually Uninstall the Linux OS Monitoring Feature	88
▼ To Manually Uninstall the Solaris OS Monitoring Feature	89
Managing Packages, Patches, and RPMs	89
Introduction to Managing OS Updates	90
▼ To Copy an OS Update	91
▼ To Load an OS Update on a Server or a Server Group	93
▼ To List the Available OS Updates	95
▼ To List the OS Updates Installed on a Provisionable Server	96
▼ To Delete an OS Update	96
▼ To Uninstall an OS Update on a Provisionable Server	96
▼ To Uninstall an OS Update on a Server Group	97
Managing Firmware SP, BIOS, and ALOM Updates	98
Introduction to Managing Firmware Updates	99
▼ To Copy a Firmware Update	99
▼ To Load a Firmware Update on a Server or a Server Group	101
▼ To List the Available Firmware Updates	103
▼ To List the Firmware Updates Installed on a Provisionable Server	104
▼ To Modify Firmware Update Information	104
▼ To Delete a Firmware Update	104
4 Managing Servers and Server Groups	107
Introduction to Server and Group Management	107
Identifying Servers and Server States	110
Supported Server Actions	111
Listing and Viewing Servers and Server Groups	111
Listing Servers and Server Groups	111
▼ To List Servers and Server Groups	112

▼ To View Failed Servers	113
Viewing Server Details and Group Members	115
▼ To View Server Details and Server Group Members	115
Modifying Server and Server Group Information	116
Renaming a Server or a Server Group	117
▼ To Rename a Server or a Server Group	118
Adding a Server Note	118
▼ To Add a Server Note	119
Starting, Stopping, and Resetting Servers and Server Groups	120
Starting Servers and Server Groups	120
▼ To Power On and Boot a Server or a Server Group	122
Stopping Servers and Server Groups	122
▼ To Shut Down and Power Off a Server or a Server Group	124
Resetting Servers and Server Groups	125
▼ To Reboot a Server or a Server Group	126
Issuing Remote Commands on Servers and Server Groups	127
▼ To Issue Remote Commands on a Server or a Server Group	127
Connecting to the Serial Console for a Server	131
▼ To Open a Server's Serial Console	131
Refreshing and Finding Servers and Server Groups	134
Refreshing Server and Server Group Data	134
▼ To Refresh Data for a Server or a Server Group	135
Finding a Server in a Rack	135
▼ To Find a Server in a Rack	135
Deleting Servers and Server Groups	136
▼ To Delete a Server or a Server Group	136
 5 Monitoring Your Servers	 137
Introduction to Monitoring	138
Hardware Health Monitoring	139
OS Resource Utilization Monitoring	140
Network Reachability Monitoring	141
Enabling Monitoring	142
▼ To Monitor a Server	144
▼ To Monitor a Server Group	145
▼ To Disable Monitoring for a Server	145
▼ To Disable Monitoring for a Server Group	146
Monitoring Threshold Values	147

What Happens When a Threshold is Broken	147
▼ To Retrieve Threshold Values for a Server	148
Managing Default Threshold Values	148
▼ To Modify Default Threshold Values for a Server	151
Hardware Sensor Attributes	152
Setting Threshold Values	156
▼ To Set Threshold Values for a Server	156
▼ To Set Threshold Values for a Server Group	157
Setting Polling Intervals	158
Changing Polling Intervals With the Monitoring Configuration File	158
▼ To Retrieve Polling Interval Values for a Server	160
▼ To Modify the Default Polling Interval for a Server	160
Setting Polling Intervals	161
▼ To Set Polling Intervals for a Server	161
▼ To Set Polling Intervals for a Server Group	162
Monitoring MIBs	163
Managing Jobs	163
▼ To List Jobs	165
▼ To View a Specific Job	166
▼ To Stop a Job	167
▼ To Delete a Job	169
Managing Event Log Entries	172
Event Log Overview	172
▼ To View the Event Log	173
▼ To Filter the Event Log	174
▼ To View Event Details	174
Setting Up Notifications	175
Viewing and Modifying Notifications	175
▼ To View Notifications	176
▼ To View Notification Details	176
▼ To Modify a Notification	176
Creating, Testing, and Deleting Notifications	177
▼ To Create and Test a Notification	177
▼ To Delete a Notification	178
Starting and Stopping Notifications	179
▼ To Start a Notification	179
▼ To Stop a Notification	179

6 Troubleshooting	181
Security	181
▼ How to Regenerate Common Agent Container Security Keys	182
General Security Considerations	182
Troubleshooting OS Distributions	183
Distribution Copy Failures	183
Patching Solaris 9 Distributions	184
Using a Provisionable Server to Patch OS Distributions	184
▼ To Patch a Solaris 9 OS Distribution by Using a Solaris 9 OS on x86 Patch Server	185
▼ To Patch a Solaris 9 OS Distribution by Using a Solaris 9 OS on SPARC Patch Server	187
OS Profile Deployment Failures	190
▼ To Modify the Default Solaris OS Profile for a Sun Fire V40z or a SPARC v440 Server	191
▼ To Modify a Solaris 9 OS Profile for a Sun Fire V20z Server With a K2.0 Motherboard	192
Solaris Deployment Job Times Out or Stops	194
▼ To Modify the Network Interface Configuration	194
Solaris OS Profile Installation Fails	195
Invalid Management Server Netmask	195
Linux Deployment Stops	195
Restarting NFS to Resolve Boot Failed Errors	196
Resolving wget Command Failures Related to OS Monitoring	196
OS Update Problems	197
OS Update Creation Failures	197
OS Update Deployment Failures	198
Downloading V20z and V40z Server Firmware Updates	201
▼ To Download and Prepare Sun Fire V20z and V40z Server Firmware	201
Handling Threshold Breaches	203
Identifying Hardware and OS Threshold Breaches	203
Identifying Network Connectivity Failure	203
Identifying Monitoring Failure	204
 Index	 205

Tables

TABLE 1-1	System Default Roles	30
TABLE 1-2	N1 System Manager Privileges	31
TABLE 1-3	Managing Users Quick Reference	34
TABLE 1-4	Managing Roles Quick Reference	38
TABLE 3-1	Provisionable Server Hardware and Operating System Requirements	60
TABLE 3-2	Default OS Profile Parameter Settings	72
TABLE 3-3	OS Profile Installation Parameters	80
TABLE 5-1	Factory-Configured Default Threshold Values for OS Resource Utilization Attributes	149
TABLE 5-2	All OS Resource Utilization Attributes	149
TABLE 5-3	Factory-Configured Default Polling Intervals	159
TABLE 6-1	Task Map for Patching a Solaris 9 Distribution	184

Figures

FIGURE 4-1 Menus and Links in the Browser Interface 109

Examples

EXAMPLE 1-1	n1sh Custom Script File	28
EXAMPLE 1-2	Setting a User's Default Role	36
EXAMPLE 1-3	Showing a User's Default Role	37
EXAMPLE 1-4	Listing the Roles that are Added to a Specific User	38
EXAMPLE 1-5	Listing Privileges Added to a Role	41
EXAMPLE 2-1	Discovering Servers Through the Command Line	51
EXAMPLE 2-2	Adding the OS Management Feature	52
EXAMPLE 2-3	Creating a Group and Adding Servers in a Single Operation	54
EXAMPLE 3-1	Provisioning the Solaris 10 OS Through the Command Line	64
EXAMPLE 3-2	Creating an OS Distribution From a File	67
EXAMPLE 3-3	Deploying a Solaris 9 OS Flash Archive	70
EXAMPLE 3-4	Listing Available OS Profiles Through the Command Line	74
EXAMPLE 3-5	Creating a Solaris OS Profile Through the Command Line	75
EXAMPLE 3-6	Creating a Red Hat OS Profile Through the Command Line	75
EXAMPLE 3-7	Creating a SUSE OS Profile Through the Command Line	76
EXAMPLE 3-8	Modifying an OS Profile Through the Command Line	78
EXAMPLE 3-9	Loading a Solaris OS Profile on a Server Through the Command Line	82
EXAMPLE 3-10	Loading a Solaris OS Profile on a Server Group Through the Command Line	83
EXAMPLE 3-11	Loading a Linux OS Profile on a Server	83
EXAMPLE 3-12	Loading a Linux OS Profile on a Server Group	83
EXAMPLE 3-13	Scripting OS Monitoring Support	87
EXAMPLE 3-14	Creating an OS Update Through the Command Line	93
EXAMPLE 3-15	Loading an OS Update Through the Command Line	95
EXAMPLE 3-16	Loading an OS Update on a Server Group	95
EXAMPLE 3-17	Listing Available OS Updates Through the Command Line	95

EXAMPLE 3-18	Loading Firmware on a Server Through the Command Line	102
EXAMPLE 3-19	Loading Firmware on a Server Group Through the Command Line	103
EXAMPLE 3-20	Listing the Available Firmware Updates Through the Command Line	104
EXAMPLE 4-1	Listing Servers Through the Command Line	113
EXAMPLE 4-2	Listing Groups Through the Command Line	113
EXAMPLE 4-3	Viewing Failed Critical Servers Through the Command Line	115
EXAMPLE 4-4	Viewing Server Details Through the Command Line	116
EXAMPLE 4-5	Viewing Server Group Members Through the Command Line	116
EXAMPLE 4-6	Renaming a Server Through the Command Line	118
EXAMPLE 4-7	Renaming a Group Through the Command Line	118
EXAMPLE 4-8	Adding a Server Note Through the Command Line	119
EXAMPLE 4-9	Starting a Server From the Network	122
EXAMPLE 4-10	Starting a Server Group from the Network	122
EXAMPLE 4-11	Forcing Power Off of a Server	124
EXAMPLE 4-12	Forcing Power Off of a Server Group	124
EXAMPLE 4-13	Forcing Reset of a Server	126
EXAMPLE 4-14	Forcing Reset of a Server Group	126
EXAMPLE 4-15	Rebooting a Server From the Network	126
EXAMPLE 4-16	Rebooting a Server Group from the Network	126
EXAMPLE 4-17	Issuing a Remote Command on a Server	128
EXAMPLE 4-18	Issuing a Remote Command With a Timeout	129
EXAMPLE 4-19	Issuing a Remote Command on a Server Group	129
EXAMPLE 4-20	Connecting to the Serial Console Through the Command Line	134
EXAMPLE 5-1	Modifying the Default Threshold Value for File System Usage	152
EXAMPLE 5-2	Setting Multiple Threshold Values for CPU Usage on a Server	157
EXAMPLE 5-3	Setting Multiple Threshold Values for File System Usage On a Server	157
EXAMPLE 5-4	Deleting a Threshold Value for File System Usage on a Server	157
EXAMPLE 5-5	Setting Multiple Threshold Values for File System Usage on a Server Group	158
EXAMPLE 5-6	Modifying Default Values	161
EXAMPLE 5-7	Setting the Polling Interval for Hardware Health Monitoring of a Server	162
EXAMPLE 5-8	Setting the Polling Interval for Network Reachability Monitoring of a Server Group	162
EXAMPLE 5-9	Receiving SNMP Traps	163
EXAMPLE 5-10	Listing All Jobs	166
EXAMPLE 5-11	Viewing Job Details	166

EXAMPLE 5-12	Stopping a Remote Command Job	168
EXAMPLE 5-13	Deleting a Job	170
EXAMPLE 5-14	Deleting All Jobs	170
EXAMPLE 5-15	Viewing Event Details	174
EXAMPLE 5-16	Viewing Notification Details	176
EXAMPLE 5-17	Modifying a Notification Name	177
EXAMPLE 5-18	Creating an Email Notification	178
EXAMPLE 5-19	Creating an SNMP Notification	178
EXAMPLE 6-1	Adding a Script to a Solaris OS Profile	193

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, to perform OS installations and updates, and to provision, discover, monitor, and manage servers.

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

Who Should Use This Book

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

- Knowledge of the Solaris™ Operating System and 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 and Cisco
- Knowledge of network device interconnections and cabling

Before You Read This Book

Read the following documents:

- *Sun N1 System Manager 1.1 Introduction*
- *Sun N1 System Manager 1.1 Site Preparation Guide*
- *Sun N1 System Manager 1.1 Installation and Configuration Guide*

How This Book Is Organized

[Chapter 1](#) describes the following:

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

[Chapter 2](#) describes the discovery process, how to add managed servers to groups, and how to replace failed servers.

[Chapter 3](#) provides conceptual and procedural information about how to manage OS installations, OS updates, and firmware updates.

[Chapter 4](#) contains procedures on how to refresh, replace, rename, reboot, and remove managed servers and groups.

[Chapter 5](#) explains how to monitor servers and groups, and how to set and manage polling intervals and thresholds. This chapter also explains how to view and manage jobs and event logs, and how to create notifications.

[Chapter 6](#) describes possible troubleshooting scenarios and solutions for threshold breaches, OS distribution issues, OS deployment failures, and OS update issues.

Related Books

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

- *Sun N1 System Manager 1.1 Introduction*
- *Sun N1 System Manager 1.1 Site Preparation Guide*
- *Sun N1 System Manager 1.1 Installation and Configuration Guide*
- *Sun N1 System Manager 1.1 Command Line Reference Manual*
- *Sun N1 System Manager 1.1 Release Notes*

The monitoring agent that is deployed by the Sun N1 System Manager software is based on the Simple Network Management Protocol (SNMP) agent used by the SunTM Management Center software. See the *Sun Management Center 3.5 Service Availability Manager User's Guide* for more information about this SNMP agent.

Documentation, Support, and Training

Sun Function	URL	Description
Documentation	http://www.sun.com/documentation/	Download PDF and HTML documents, and order printed documents
Support and Training	http://www.sun.com/supporttraining/	Obtain technical support, download patches, and learn about Sun courses

Typographic Conventions

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

TABLE P-1 Typographic Conventions

Typeface or Symbol	Meaning	Example
AaBbCc123	The names of commands, files, and directories, and onscreen computer output	Edit your <code>.login</code> file. Use <code>ls -a</code> to list all files. <code>machine_name%</code> you have mail.
AaBbCc123	What you type, contrasted with onscreen computer output	<code>machine_name% su</code> Password:
<i>aabbcc123</i>	Placeholder: replace with a real name or value	The command to remove a file is <code>rm filename</code> .
<i>AaBbCc123</i>	Book titles, new terms, and terms to be emphasized	Read Chapter 6 in the <i>User's Guide</i> . Perform a <i>patch analysis</i> . Do <i>not</i> save the file. [Note that some emphasized items appear bold online.]

Shell Prompts in Command Examples

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

TABLE P-2 Shell Prompts

Shell	Prompt
C shell prompt	<code>machine_name%</code>
C shell superuser prompt	<code>machine_name#</code>
Bourne shell and Korn shell prompt	<code>\$</code>
Bourne shell and Korn shell superuser prompt	<code>#</code>

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 the standard command line. Precede N1 System Manager commands by the `n1sh` command in the standard command line in a UNIX shell.

Managing the N1 System Manager on the Management Server

This chapter provides information about the N1 System Manager user interfaces, security features, user management, and backup and restore procedures for the management server. For an overview of the Sun N1 System Manager features and components, see the *Sun N1 System Manager 1.1 Introduction*.

The main sections in this chapter are as follows:

- [“Introduction to Accessing the N1 System Manager” on page 23](#)
- [“Introduction to N1 System Manager User Security” on page 29](#)
- [“Managing Users” on page 34](#)
- [“Managing Roles” on page 38](#)
- [“Backing Up and Restoring N1 System Manager Database and Configuration Files” on page 42](#)

Introduction to Accessing the N1 System Manager

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

- **Command line** – The `n1sh` command. The default method is to use the `n1sh` shell, which uses an `N1-ok>` prompt. The shell mode provides a tab completion feature to navigate through all the command options. See the `n1sh` man page for details.
- **Browser interface** – A web-based user interface that provides a subset of the command line features. The browser interface also includes the `n1sh` shell in the Command Line pane. As you use the browser interface to perform management tasks, the corresponding commands are displayed in the Command Line pane. The Command Line pane provides the same features as the `n1sh` command in shell mode.

The `n1sh` command provides two other ways to issue management commands. The `n1sh -e` option, or UNIX® command mode, enables you to type management commands one at a time within a UNIX® shell. The `n1sh -f` option enables you to specify a custom script of management commands to run. See the `n1sh` man page for details.

Command Line Tips

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

id Keyword

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

Equal Sign

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

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

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

Script Comments

When creating a customized `n1sh` script, you can specify the comment character (#) at the beginning of the line to indicate that the rest of the line should be ignored. See [“To Run a Script of N1 System Manager Commands” on page 28](#) for details.

Multiple Attribute Values

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

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

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

Quotation Marks

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

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

Special Characters

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

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

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

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

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

▼ 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 35.

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

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

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

You are prompted for a password.

2. Type a password for the user account.

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

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

```
# /opt/sun/nlmc/bin/nlsh [-r role-name]
```

The superuser (`root`) user account typically does not have its login configured to automatically log in to the `nlsh` 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 1.1 Command Line Reference Manual* for details.

▼ To Access the N1 System Manager Browser Interface

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

Before You Begin

During management server configuration, the superuser (`root`) account is set up with all the system default roles added to it (`Admin`, `ReadOnly`, and `SecurityAdmin`). If you want to log in as a valid user other than the superuser account, see [“To Add an N1 System Manager User” on page 35](#).

The following browsers are supported:

- Netscape Navigator™ 7.1 or later (Linux or Microsoft Windows version)
- Mozilla™ 1.4 or later (Solaris, Linux, or Microsoft Windows version)
- Internet Explorer 6 or later (Microsoft Windows version)

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

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

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

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

`http://management-server`

where *management-server* is the host name or IP address of the management server.
The 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 1.1 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 1.1 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 38 for more details about roles.

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

See “To Access the N1 System Manager Command Line” on page 25 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 38 for more details about roles and privileges.

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

See [“To Access the N1 System Manager Command Line”](#) on page 25 for details.

2. Switch to a different session role.

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

See “set session” in *Sun N1 System Manager 1.1 Command Line Reference Manual* for details.

▼ To Exit the N1 System Manager Command Line

Step ● Exit the N1 System Manager command line.

```
N1-ok> exit
```

The `n1sh` shell is terminated.

▼ To Run a Script of N1 System Manager Commands

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

Steps 1. Log in to the N1 System Manager.

See [“To Access the N1 System Manager Command Line”](#) on page 25 for details.

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

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

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

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

Example 1–1 `n1sh` Custom Script File

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

```
# n1sh custom script

show group all

create group RACK1
create group RACK2
```

```
create group RACK3
create group RACK4
create group RACK5

add group RACK1 server SERVER1
add group RACK1 server SERVER2

add group RACK2 server SERVER3
add group RACK2 server SERVER4

add group RACK3 server SERVER5
add group RACK3 server SERVER6

add group RACK4 server SERVER7
add group RACK4 server SERVER8

add group RACK4 server SERVER9
add group RACK4 server SERVER10

add group RACK5 server SERVER11
add group RACK5 server SERVER12

show group all
```

Introduction to N1 System Manager User Security

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

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

- [“To Add an N1 System Manager User” on page 35](#)
- [“To Delete an N1 System Manager User” on page 35](#)
- [“To Set a User’s Default Role” on page 36](#)
- [“To Show a User’s Default Role” on page 36](#)
- [“To Add a Role to a User” on page 37](#)
- [“To Remove a Role From a User” on page 37](#)
- [“To List the Roles Added to a Specific User” on page 37](#)

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

- [“To Create a Role” on page 39](#)
- [“To Delete a Role” on page 39](#)
- [“To Add a Privilege to a Role” on page 40](#)

- “To Remove a Privilege From a Role” on page 40
- “To List the Available Roles” on page 40
- “To List Privileges Added to a Role” on page 41
- “To List the Roles Added to All Users” on page 41
- “To List the Available Privileges” on page 41

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

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

TABLE 1–1 System Default Roles

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

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

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

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

Note – Non-root users with only the `SecurityAdmin` role are not allowed to extend their own privilege set, either by adding new privileges to the `SecurityAdmin` role (which cannot be modified) or by adding new roles to their own user account. See [“Security Administrator Rules” on page 33](#) for more details.

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

TABLE 1–2 N1 System Manager Privileges

Privilege	Description	Commands
Discover	Discover servers	<code>discover</code>
FirmwareRead	List firmware updates	<code>show firmware</code>
FirmwareWrite	Manage firmware updates	<code>create firmware</code>
		<code>delete firmware</code>
		<code>set firmware</code>
GroupRead	List server groups	<code>show group</code>
GroupWrite	Manage server groups	<code>create group</code>
		<code>delete group</code>
		<code>add group</code>
		<code>remove group</code>
		<code>set group</code>
JobRead	List jobs	<code>show job</code>
JobWrite	Delete or stop jobs	<code>delete job</code>
		<code>stop job</code>
LogRead	List event log	<code>show log</code>
NotificationRuleRead	List notification rules	<code>show notification</code>
NotificationRuleTest	Test a notification rule	<code>set notification</code> <i>notification</i> <code>test</code>

TABLE 1–2 N1 System Manager Privileges (Continued)

Privilege	Description	Commands
NotificationRuleWrite	Manage notification rules	create notification delete notification set notification start notification stop notification
OSProfileRead	List OS profiles	show osprofile
OSProfileWrite	Manage OS profiles	add osprofile remove osprofile create osprofile delete osprofile set osprofile
OSRead	List OS distributions	show os
OSWrite	Manage OS distributions	create os delete os set os
PrivilegeRead	List privileges	show privilege
RoleRead	List roles	show role
RoleWrite	Manage roles	create role delete role add role remove role set role
ServerBoot	Reboot servers	reset group reset server
ServerConsole	Connect to server's serial console	connect server
ServerDeployFirmware	Install firmware on servers	load server <i>server</i> firmware load group <i>group</i> firmware
ServerDeployOS	Install OS on servers	load server <i>server</i> osprofile load group <i>group</i> osprofile

TABLE 1–2 N1 System Manager Privileges (Continued)

Privilege	Description	Commands
ServerDeployUpdate	Install or uninstall OS updates on servers	load server <i>server</i> update
		load group <i>group</i> update
		unload server <i>server</i> update
		unload group <i>group</i> update
ServerExecute	Execute command on servers	start server <i>server</i> command
		start group <i>group</i> command
ServerPower	Power off and power on servers	stop group
		stop server
		start group
		start server
ServerRead	List and refresh servers	show server
		set group <i>group</i> refresh
		set server <i>server</i> refresh
ServerWrite	Manage servers and management features	add server <i>server</i> feature
		delete server
UpdateRead	List OS updates	show update
UpdateWrite	Add and remove OS updates	create update
		delete update
UserRead	List users	show user
UserWrite	Manage users	create user
		delete user
		add user
		remove user
		set user

For more information about these commands, see the *Sun N1 System Manager 1.1 Command Line Reference Manual*.

Security Administrator Rules

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

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

Managing Users

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

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

TABLE 1-3 Managing Users Quick Reference

Task	Command Syntax
"To Add an N1 System Manager User" on page 35	# <code>useradd -s</code> # <code>n1sh create user <i>user</i> role <i>role</i></code>
"To Delete an N1 System Manager User" on page 35	# <code>n1sh delete user <i>user</i></code> # <code>userdel</code>
"To Set a User's Default Role" on page 36	<code>set user <i>user</i> defaultrole <i>defaultrole</i></code>
"To Show a User's Default Role" on page 36	<code>show user <i>user</i></code>
"To Add a Role to a User" on page 37	<code>add user <i>user</i> role <i>role</i></code>
"To Remove a Role From a User" on page 37	<code>remove user <i>user</i> role <i>role</i></code>
"To List the Roles Added to a Specific User" on page 37	<code>show user <i>user</i></code>

For more information about these commands, see the *Sun N1 System Manager 1.1 Command Line Reference Manual*.

▼ To Add an N1 System Manager User

Before You Begin

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

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

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

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

See [“To Access the N1 System Manager Command Line”](#) on page 25 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 1.1 Command Line Reference Manual* for details. You can also use the `add user` command to later add more roles.

▼ To Delete an N1 System Manager User

Before You Begin

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

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

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

See [“To Access the N1 System Manager Command Line”](#) on page 25 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 1.1 Command Line Reference Manual*.

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

▼ To Set a User’s Default Role

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

Steps 1. Log in to the N1 System Manager.

See “To Access the N1 System Manager Command Line” on page 25 for details.

2. Show which roles are added to the user.

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

See “show user” in *Sun N1 System Manager 1.1 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 1.1 Command Line Reference Manual* for details.

Example 1–2 Setting a User’s Default Role

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

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

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

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

▼ To Show a User’s Default Role

Steps 1. Log in to the N1 System Manager.

See “To Access the N1 System Manager Command Line” on page 25 for details.

2. Show a user's default role.

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

See “show user” in *Sun N1 System Manager 1.1 Command Line Reference Manual* for details.

Example 1–3 Showing a User's Default Role

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

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

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

▼ To Add a Role to a User

Steps 1. Log in to the N1 System Manager.

See “To Access the N1 System Manager Command Line” on page 25 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 1.1 Command Line Reference Manual* for details. You can use the show role all command to list all of the valid roles.

▼ To Remove a Role From a User

Steps 1. Log in to the N1 System Manager.

See “To Access the N1 System Manager Command Line” on page 25 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 1.1 Command Line Reference Manual* for details. You can use the show user user command to list all the roles currently added to the user.

▼ To List the Roles Added to a Specific User

Steps 1. Log in to the N1 System Manager.

See “To Access the N1 System Manager Command Line” on page 25 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 1.1 Command Line Reference Manual* for details.

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

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

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

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

Managing Roles

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

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

TABLE 1–4 Managing Roles Quick Reference

Task	Command Syntax
“To Create a Role” on page 39	<code>create role <i>role</i> privilege <i>privilege</i></code>
“To Delete a Role” on page 39	<code>delete role <i>role</i></code>
“To Add a Privilege to a Role” on page 40	<code>add role <i>role</i> privilege <i>privilege</i></code>
“To Remove a Privilege From a Role” on page 40	<code>remove role <i>role</i> privilege <i>privilege</i></code>
“To List the Available Roles” on page 40	<code>show role all</code>
“To List Privileges Added to a Role” on page 41	<code>show role <i>role</i></code>

TABLE 1-4 Managing Roles Quick Reference (Continued)

Task	Command Syntax
“To List the Roles Added to All Users” on page 41	<code>show user all</code>
“To List the Available Privileges” on page 41	<code>show privilege all</code>

For more information about these commands, see the *Sun N1 System Manager 1.1 Command Line Reference Manual*.

▼ To Create a Role

Steps 1. Log in to the N1 System Manager.

See [“To Access the N1 System Manager Command Line” on page 25](#) for details.

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

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

Use the `show privileges all` command to list all of the valid privileges or see [Table 1-2](#).

See “create role” in *Sun N1 System Manager 1.1 Command Line Reference Manual* for details. You can also use the `add role` command to later add privileges to the role.

▼ To Delete a Role

Before You Begin

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

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

Steps 1. Log in to the N1 System Manager.

See [“To Access the N1 System Manager Command Line” on page 25](#) for details.

2. Delete a role.

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

See “delete role” in *Sun N1 System Manager 1.1 Command Line Reference Manual* for details.

▼ To Add a Privilege to a Role

Before You Begin Use the `show privilege all` command to list all of the valid privileges or see [Table 1-2](#).

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

See [“To Access the N1 System Manager Command Line”](#) on page 25 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 1.1 Command Line Reference Manual* for details.

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

▼ To Remove a Privilege From a Role

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

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

See [“To Access the N1 System Manager Command Line”](#) on page 25 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 1.1 Command Line Reference Manual* for details.

▼ To List the Available Roles

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

See [“To Access the N1 System Manager Command Line”](#) on page 25 for details.

2. **List the available roles.**

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


▼ To List Privileges Added to a Role

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

- Steps**
1. **Log in to the N1 System Manager.**
See [“To Access the N1 System Manager Command Line”](#) on page 25 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 1.1 Command Line Reference Manual* for details.

Example 1–5 Listing Privileges Added to a Role

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

```
N1-ok> show role SecurityAdmin

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

▼ To List the Roles Added to All Users

- Steps**
1. **Log in to the N1 System Manager.**
See [“To Access the N1 System Manager Command Line”](#) on page 25 for details.
 2. **List the roles that are added to all users.**

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

▼ To List the Available Privileges

- Steps**
1. **Log in to the N1 System Manager.**
See [“To Access the N1 System Manager Command Line”](#) on page 25 for details.
 2. **List the available privileges.**

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

Backing Up and Restoring N1 System Manager Database and Configuration Files

This section provides the following procedures:

- [“To Back Up the N1 System Manager Database and Configuration Files” on page 42](#)
- [“To Restore the N1 System Manager Database and Configuration Files” on page 43](#)

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

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

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

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

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

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

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

- Steps**
1. **Log in to the management server as superuser (root).**
See [“To Access the N1 System Manager Command Line” on page 25](#) for details.
 2. **Run the `n1smbbackup.sh` script.**

For example:

```
# /opt/sun/nlmc/bin/nlsmbackup.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/nlsmbackup/nlsmbackup.tgz.

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

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

Next Steps [“To Restore the N1 System Manager Database and Configuration Files” on page 43](#)

▼ To Restore the N1 System Manager Database and Configuration Files

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

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

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

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

- Before You Begin**
- Follow the instructions in [“To Back Up the N1 System Manager Database and Configuration Files”](#) on page 42 to backup the database and configuration files.
 - Identify a server with similar hardware and network configurations as that of the original management server.

- Steps**
1. **Log in to the management server as superuser (root).**
See [“To Access the N1 System Manager Command Line”](#) on page 25 for details.
 2. **Run the `n1smconfig` utility.**

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

The current system configuration appears, and lists the network interfaces. You are then asked to enter the interface for the provisioning network.
 3. **Specify the port for the provisioning network interface.**
The available interfaces are listed in the prompt. Type the interface name that is to be used for the provisioning interface, for example `eth0`, `hme0`, `bge0` and so on depending on the machine architecture and installed OS.
 4. **Answer the remaining questions in the `n1smconfig` utility.**
Note that the remaining answers given in `n1smconfig` will be overwritten by the following steps in this procedure. But, it is important to provide the answers and to apply the new settings in order to complete the restore process.
 5. **Create the `/var/tmp/n1smbbackup` directory on the management server.**

```
# mkdir /var/tmp/n1smbbackup
```
 6. **Copy the `n1smbbackup.tgz` backup file to the `/var/tmp/n1smbbackup` directory.**
 7. **Restore the N1 System Manager database and configuration files:**

```
# /opt/sun/n1gc/bin/n1smrestore.sh -f /var/tmp/n1smbbackup/n1smbbackup.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 25 for details.

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

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

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

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

Next Steps You will need to copy new OS distributions and create new OS profiles. See [“Copying OS Distributions and Flash Archives”](#) on page 66 and [“To Create an OS Profile”](#) on page 74.

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

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

- [“Discovering Servers” on page 47](#)
- [“Creating and Maintaining Server Groups” on page 53](#)
- [“Replacing Provisionable Servers” on page 56](#)

Discovering Servers

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

Note – Before you can perform any of the management activities in this section, physical servers must be cabled and prepared according to the instructions in Chapter 2, “Sun N1 System Manager System and Network Preparation,” in *Sun N1 System Manager 1.1 Site Preparation Guide*.

Servers must also comply with the following revisions of firmware to be discovered. See [“Downloading V20z and V40z Server Firmware Updates” on page 201](#) for instructions or refer to Sun System Handbook documentation for your provisionable server.

	Minimum Requirement	Best Practice
Sun Fire V20z and V40z Service Processor (SP)	2.1.0.5	2.3.0.11
Sun Fire V20z Server Platform BIOS	N/A	1.33.5.2
Sun Fire V40z Server Platform BIOS	N/A	2.33.5.2
Sun Fire X4100 and X4200 with Integrated Lights Out Manager (ILOM)	1.0	1.0
Sun SPARC servers with Advanced Lights Out Manager (ALOM)	1.4	1.5.3

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

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

- Sun Fire X4100 and X4200 servers
 - SSH user = root
 - SSH password = changeme
 - IMPI user = root
 - IMPI password = changeme
- Sun Fire V20z and V40z servers
 - SSH user = admin
 - SSH password = admin
 - IMPI user = Null
 - IMPI password = admin
 - SNMP read community string = public
- Sun Fire V210, V240, V440 servers
 - Telnet login = admin
 - Telnet password = admin

Note – Automatic configuration of credentials is supported for Sun Fire V20z and V40z servers if they are in the factory default state. See “Setting Up Provisionable Servers” in *Sun N1 System Manager 1.1 Site Preparation Guide*.

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

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

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

The N1 System Manager must be restarted for the disabling of autoconfiguration to take effect. Note that after autoconfiguration is disabled, any servers in the factory default state cannot be discovered until their SSH and IPMI accounts are configured. For further information, see *Sun N1 System Manager 1.1 Site Preparation Guide*.



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

▼ To Discover New Servers

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

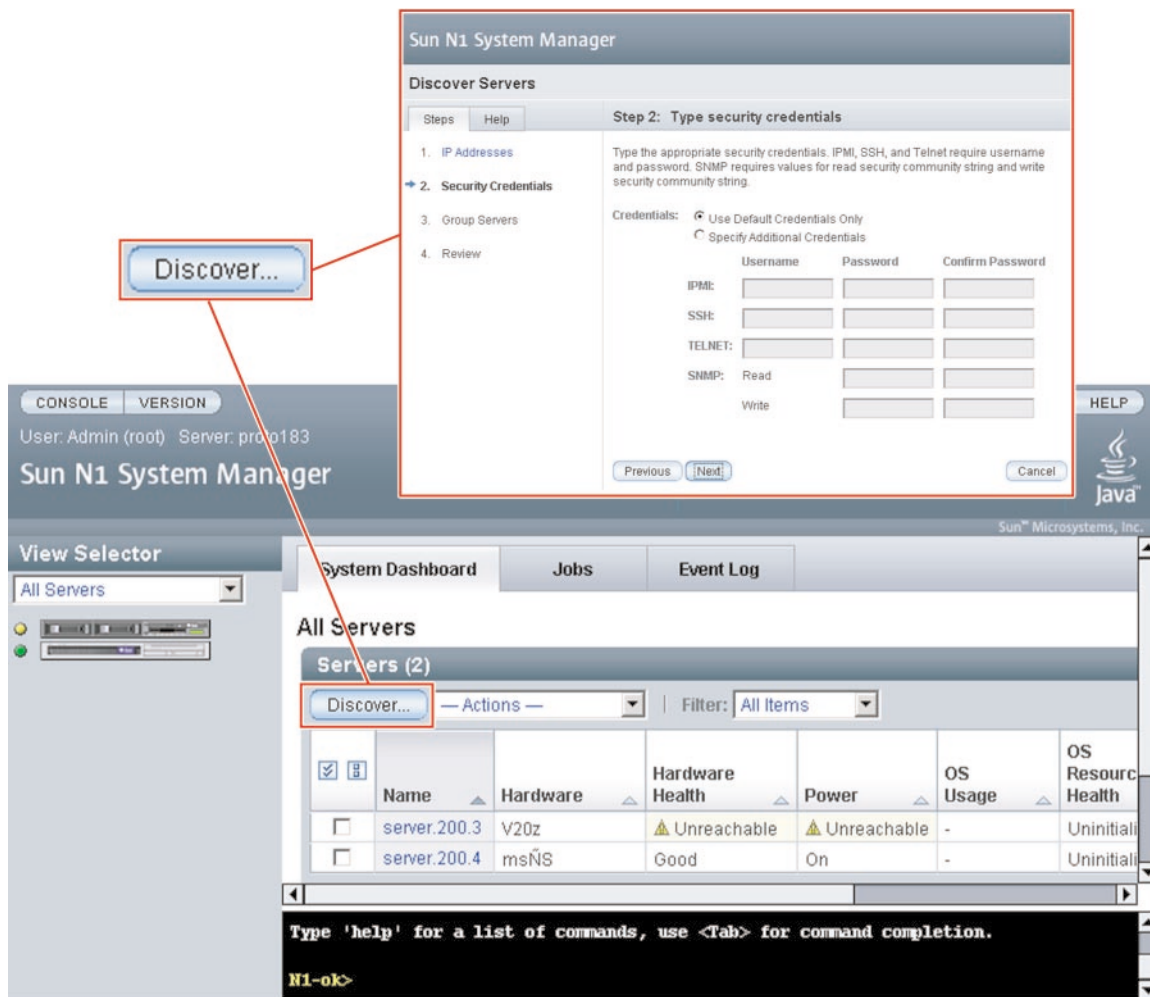
Note – Discovered servers are automatically monitored for hardware health.

Before You Begin

- Before you discover a new hardware component, read Chapter 2, “Sun N1 System Manager System and Network Preparation,” in *Sun N1 System Manager 1.1 Site Preparation Guide*.

Steps

1. **Log in to the N1 System Manager.**
See “[To Access the N1 System Manager Browser Interface](#)” on page 26 for details.
The All Servers page appears.
2. **Click the Discover button in the Servers table.**
The Discover Servers wizard appears.



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

- If you selected a group for the discovered servers, view the list of server groups as follows:
 - a. Select the Servers By Group from the View Selector menu.
The Server Groups table appears.
 - b. Select the group name.
The list of discovered servers appears.
The server or servers are available for OS provisioning.
- 7. If you installed an OS on a server before it was discovered, add the OS monitoring feature.

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

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

See “add server” in *Sun N1 System Manager 1.1 Command Line Reference Manual* for details.

Example 2–1 Discovering Servers Through the Command Line

IP addresses, IP address ranges, and IP subnets can be input as a comma-separated list. Overlapping IP address ranges are allowed. Security credentials for IPMI, Simple Network Management Protocol (SNMP), SSH, and Telnet are optional. However, for Sun Fire X4000 series servers, username is required by IPMI. If credentials are not specified, the manufacturer defaults are used. See *Sun N1 System Manager 1.1 Site Preparation Guide* for information about the default accounts.

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

The following example of the discover command shows how to discover servers that have the following management network IP addresses:

```
192.168.1.1-192.168.1.3 , 192.168.1.5-192.168.1.95, and
192.168.1.107.
```

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

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

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

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

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

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

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

Name	Status	Jobs	Servers	Spare
dev			7	

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

```
N1-ok> show group dev
```

Name	Hardware	Hardware Health	Power	OS Usage	OS Resource Health
192.168.1.1	V20z	Good	On	--	Uninitialized
192.168.1.2	V20z	Good	On	--	Uninitialized
192.168.1.5	V40z	Good	On	--	Uninitialized
192.168.1.15	NETRA-240	Good	On	--	Uninitialized
192.168.1.25	X4100	Good	On	--	Uninitialized
192.168.1.95	X4200	Good	On	--	Uninitialized
192.168.1.107	SF-V240	Good	On	--	Uninitialized

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

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

The following example shows how to view the discovered servers.

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

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

Example 2-2 Adding the OS Management Feature

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

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

The `agentip` parameter sets the IP address of the provisionable server's data network interface to be monitored by the management server. The `ssh` user name `admin` and password `admin` are used for root access authentication.

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

```
N1-ok> show server 192.168.1.1
```

Name	Hardware	Hardware Health	Power	OS Usage	OS Resource Health
192.168.1.1	V20z	Good	On	Solaris	Good

Troubleshooting The `discover` command credential attributes are used for security. SSH, IPMI, and Telnet require a username and a password. SNMP requires that you input a valid value for the read security community string. If credentials are not specified, the discovery process uses the default credentials that were defined during installation. See [“Discovering Servers” on page 47](#) for default credentials.

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

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

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

See Also *Sun N1 System Manager 1.1 Site Preparation Guide*

Next Steps ■ [“To Open a Server’s Serial Console” on page 131](#)

Creating and Maintaining Server Groups

This section describes the following tasks:

- [“To Create a Server Group” on page 54](#)
- [“To Add a Server to a Group” on page 55](#)
- [“To Remove a Server From a Group” on page 55](#)

Creating Groups and Adding Servers to Groups

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

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

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

To create a group and add servers in a single operation, you use the `create` command with the `group` keyword and the `server` subcommand. This task can also be performed during the discovery process. To do so, you can add an option to the `discover` command to create a new group and add the servers to the new group. See [“To Discover New Servers” on page 49](#) for instructions.

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

▼ To Create a Server Group

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

Steps 1. Log in to the N1 System Manager.

See [“To Access the N1 System Manager Command Line” on page 25](#) for details.

2. Type the following command:

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

The new group is created. See “create group” in *Sun N1 System Manager 1.1 Command Line Reference Manual* for details.

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

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

```
N1-ok> create group dev server server1,server2
N1-ok> show group dev
```

Name	Hardware	Power	Health	OS Usage
server1	V20z	On	Good	--
server2	V20z	On	Good	RH30

▼ To Add a Server to a Group

Note – Servers can belong to more than one group.

Steps 1. Log in to the N1 System Manager.

See [“To Access the N1 System Manager Command Line”](#) on page 25 for details.

2. Type the following command:

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

The server is added to the group. See “add group” in *Sun N1 System Manager 1.1 Command Line Reference Manual* for details.

Removing Servers From Groups

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

▼ To Remove a Server From a Group

Steps 1. Log in to the N1 System Manager.

See [“To Access the N1 System Manager Command Line”](#) on page 25 for details.

2. Type the following command:

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

The server is removed from the group. See “remove group” in *Sun N1 System Manager 1.1 Command Line Reference Manual* for details.

Replacing Provisionable Servers

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

▼ To Replace a Server

- Steps**
1. **Log in to the N1 System Manager.**
See [“To Access the N1 System Manager Command Line” on page 25](#) for details.
 2. **Type the following command:**

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

The server is shut down and powered off. See “stop server” in *Sun N1 System Manager 1.1 Command Line Reference Manual* for details.
 3. **Disconnect the physical server from the rack.**
 4. **Remove the server from the system.**

```
N1-ok> delete server server
```
 5. **Connect the new server.**
Follow the instructions in *Sun N1 System Manager 1.1 Site Preparation Guide*.
 6. **Discover the replacement server.**

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

The replacement server is managed and monitored. See “discover” in *Sun N1 System Manager 1.1 Command Line Reference Manual* for details. You can set the monitoring threshold values for OS resource utilization. See [“Setting Threshold Values” on page 156](#) for details.

Provisioning Operating Systems, OS Updates, and Firmware Updates

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

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

- [“Introduction to OS Provisioning” on page 57](#)
- [“Provisioning the Solaris 10 Operating System” on page 62](#)
- [“Managing OS Distributions” on page 65](#)
- [“Managing OS Profiles” on page 71](#)
- [“Installing OS Distributions by Deploying OS Profiles” on page 79](#)
- [“Managing Packages, Patches, and RPMs” on page 89](#)
- [“Managing Firmware SP, BIOS, and ALOM Updates” on page 98](#)

Introduction to OS Provisioning

This section provides an overview of OS image management, supported OS types, and Solaris 10 provisioning. This section includes the following:

- [“To Provision the Solaris 10 OS” on page 62](#)
- [“Supported Operating Systems on Provisionable Servers” on page 60](#)

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

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

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

3. Installing an OS profile on a server or a server group.

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

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

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

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

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

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

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

Tip – The N1 System Manager browser interface provides an OS profile wizard and drag-and-drop installation of groups of servers to limit the complexity of OS provisioning. The wizard builds commands to help you learn the syntax and provides default settings to enable efficient configuration of common parameters. See [“To Access the N1 System Manager Browser Interface” on page 26](#) for login instructions. Refer to the N1 System Manager online help for wizard instructions.

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

The following graphic illustrates the OS provisioning process.

OS Provisioning Process



- 1 Assume a user role with appropriate privileges.

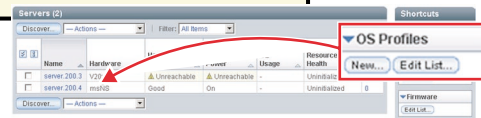
- 2 Copy an OS distribution to the management server by using the command line.

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

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



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



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

Jobs (7)				
Refresh		Stop Job(s)		Filter: All Items
<input checked="" type="checkbox"/>	Job ID	Date	Type	Status
<input type="checkbox"/>	7	2005-07-12T12:29:19-0600	Server Reboot	Stopped
<input type="checkbox"/>	6	2005-07-11T11:28:00-0600	Discovery	Stopped

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

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

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

System Dashboard

Jobs

Event Log

All Servers

Servers (2)

Discover... Actions Filter: All Items

<input checked="" type="checkbox"/>	Name	Hardware	Hardware Health	Power	OS Usage	OS Resource Health
<input type="checkbox"/>	server.200.3	V20z	▲ Unreachable	▲ Unreachable	-	Uninitial
<input type="checkbox"/>	server.200.4	msNS	Good	On	-	Uninitial

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

- Assume a user role with appropriate privileges. See [“Introduction to N1 System Manager User Security”](#) on page 29 for procedural information.

- Copy an OS distribution to the management server by using the command line. See [“To Copy an OS Distribution From CDs or a DVD” on page 67](#), [“To Copy an OS Distribution From ISO Files” on page 66](#), and [“Copying OS Distributions and Flash Archives” on page 66](#) for conceptual information.
- (Optional) Create a flash archive file and copy it to the management server. See [“To Copy a Flash Archive to the Management Server” on page 69](#).
- Modify the default OS profile to customize the parameters that are used to install the distribution. See [“To Modify an OS Profile” on page 77](#).
- Load the OS profile onto your provisionable servers by using the `load` command. Alternatively, use the browser interface’s Shortcuts pane to drag-and-drop OS profiles onto listed servers. See [“To Load an OS Profile on a Server or a Server Group” on page 81](#).
- Track the Kickstart or JumpStart installation output and the Load OS job progress. See [“Connecting to the Serial Console for a Server” on page 131](#) and [“Managing Jobs” on page 163](#).
- After the Load OS job completes, monitor the installed OS. See [“OS Resource Utilization Monitoring” on page 140](#) and [“To Add the OS Monitoring Feature” on page 85](#).

Supported Operating Systems on Provisionable Servers

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

Note – Solaris 9 OS on x86 platform distributions require the application of two updates from a separate patch server if your management server is running Linux. See [“To Patch a Solaris 9 OS Distribution by Using a Solaris 9 OS on x86 Patch Server” on page 185](#) for detailed instructions on how to create a valid Solaris 9 OS on x86 platform distribution.

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

TABLE 3–1 Provisionable Server Hardware and Operating System Requirements

Server Type	Provisionable OS	Disk Space Requirements	RAM Requirements
SPARC			

TABLE 3–1 Provisionable Server Hardware and Operating System Requirements *(Continued)*

Server Type	Provisionable OS	Disk Space Requirements	RAM Requirements
x86	Sun Netra 240 and 440	Solaris 10	512 Mbytes minimum, 1 Gbyte recommended
		Solaris 9 7/05	
	Sun Fire V210, V240, and V440	Solaris 10	512 Mbytes minimum, 1 Gbyte recommended
		Solaris 9 7/05	
	Sun Fire X4100 and X4200	Solaris 10 HW1	512 Mbytes minimum, 1 Gbyte recommended
		Red Hat Enterprise Linux AS 4.0 Update 1, 64 bit only	
		Red Hat Enterprise Linux ES 4.0 Update 1, 64 bit only	
		Red Hat Enterprise Linux AS 3.0, Update 5, 32 bit and 64 bit	
		Red Hat Enterprise Linux ES 3.0, Update 5, 32 bit and 64 bit	
		SUSE Linux Enterprise Server 9 SP1, 64 bit only	
Sun Fire V20z and V40z	Solaris 10	12 Gbytes minimum	512 Mbytes minimum, 1 Gbyte recommended
	Solaris 9 7/05		
	Red Hat Enterprise Linux AS 4.0, 32 bit and 64 bit		
	Red Hat Enterprise Linux ES 4.0, 32 bit and 64 bit		
	Red Hat Enterprise Linux AS 3.0, Updates 1 through 5, 32 and 64 bit		
	Red Hat Enterprise Linux ES 3.0, Updates 1 through 5, 32 and 64 bit		
	SUSE Linux Enterprise Server 9 and SP1, 32 and 64 bit		

Provisioning the Solaris 10 Operating System

This section provides instructions for provisioning the Solaris 10 OS by using the browser interface or the command line. This procedure will familiarize you with the provisioning process and the most reliable method for performing aggregate server installations at any skill level.

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

▼ To Provision the Solaris 10 OS

Before You Begin

- Read [“Discovering Servers” on page 47](#).
- Download the Solaris 10 DVD ISO file to a directory that is accessible by the management server.

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

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

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

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

See [“To Copy an OS Distribution From ISO Files” on page 66](#) or [“To Copy an OS Distribution From CDs or a DVD” on page 67](#) for more information.

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

See [“To Copy a Flash Archive to the Management Server” on page 69](#).

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

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

```
DEVICE=bge1  
BOOTPROTO=dhcp
```

ONBOOT=yes

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

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

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

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

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

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

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

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

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

a. Click the Edit List button beneath the OS Profiles list.

The list of available OS profiles appears.

b. Select the relevant check box and click OK.

The selected OS profile is added to the Shortcuts pane.

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

a. Choose All Servers from the View Selector menu.

The Servers table appears.

b. Select the server for which you want to launch a serial console.

The Server Details page appears.

c. Choose Open Serial Console from the Actions menu.

The serial emulator appears.

7. Choose Servers By Group from the View Selector menu.

The Server Groups table appears.

8. Drag and drop the OS profile icon from the Shortcuts pane to a server group.

The Load OS Profile wizard appears. Use the wizard steps to guide you through the screens.

9. To begin loading the OS profile on the selected servers, click the Finish button in the final step of the wizard.

The wizard window closes and a job number appears in the Command Line pane.

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

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

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

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

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

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

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

```
# vi /etc/dfs/dfstab

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

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

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

The following example shows how to restart NFS.

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

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

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

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

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

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


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

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

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

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

```
N1-ok> load group devgroup osprofile solaris_ver10  
excludeserver=192.168.73.205,192.168.73.31,192.168.73.14  
networktype=static ip=192.168.72.201-192.168.73.214  
Job "3" started.
```

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

The following example shows how to view the job status.

```
N1-ok> show job 3  
Job ID: 3  
Date: 2005-06-01T13:11:46-0600  
Type: OS Load  
Status: Completed (2005-06-01T13:11:59-0600)  
Owner: root  
Errors: 0  
Warnings: 0
```

Troubleshooting ■ [“Troubleshooting OS Distributions” on page 183](#)
■ [“OS Profile Deployment Failures” on page 190](#)

See Also ■ [“To Copy a Flash Archive to the Management Server” on page 69](#)
■ [“Connecting to the Serial Console for a Server” on page 131](#)

Next Steps [“To Add the OS Monitoring Feature” on page 85](#)

Managing OS Distributions

This section describes the following tasks:

- [“To Copy an OS Distribution From ISO Files” on page 66](#)
- [“To Copy an OS Distribution From CDs or a DVD” on page 67](#)
- [“To Copy a Flash Archive to the Management Server” on page 69](#)
- [“To Delete an OS Distribution” on page 71](#)

Copying OS Distributions and Flash Archives

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

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

Supported file types are in the following list:

- CD ISO files
- CD media
- DVD ISO files
- DVD media

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

Refer to [“Supported Operating Systems on Provisionable Servers” on page 60](#) for a detailed list of supported distributions for each provisionable server type.

To copy an OS distribution, use the `create` command with the `os` keyword. Type `help create os` at the `N1-ok` command line for syntax and parameter details, or see “create os” in *Sun N1 System Manager 1.1 Command Line Reference Manual*.

After you have copied an OS distribution, you can copy a flash archive file to the management server for use with a customized OS profile. Copying flash archives involves several manual steps, but it provides the most efficient method for loading OS distributions with the N1 System Manager. See [“To Copy a Flash Archive to the Management Server” on page 69](#).

▼ To Copy an OS Distribution From ISO Files

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

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

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

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

- Steps**
1. **Log in to the N1 System Manager.**
See [“To Access the N1 System Manager Command Line”](#) on page 25 for details.
 2. **Type the following command:**

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


Refer to the “create os” in *Sun N1 System Manager 1.1 Command Line Reference Manual* for details.
 3. **Verify that the OS distribution was copied.**

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


The OS distribution appears in the output.

Example 3–2 Creating an OS Distribution From a File

The following example shows how to create an OS distribution called `solaris_ver9`.

```
N1-ok> create os solaris_ver9 file /tmp/solaris_9.iso1,/tmp/solaris_9.iso2  
Job "7" started.
```

See Also To find out how to load the OS distribution, see [“To Load an OS Profile on a Server or a Server Group”](#) on page 81.

▼ To Copy an OS Distribution From CDs or a DVD

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

Note – The N1 System Manager does not support the copying of Solaris OS CDs. You must copy a Solaris DVD.

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

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

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

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

A Create OS Distribution job is started. Note the job ID. When the job completes, insert the next disk. See “create os” in *Sun N1 System Manager 1.1 Command Line Reference Manual* for details.

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

2. Insert Disk 2 and type the following command:

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

3. Continue with additional disks if needed.

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

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

The new OS distribution appears in the output.

Troubleshooting [“Troubleshooting OS Distributions” on page 183](#)

Next Steps To find out how to load the OS distribution by using an profile, see [“To Load an OS Profile on a Server or a Server Group” on page 81.](#)

▼ To Copy a Flash Archive to the Management Server

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

Before You Begin

- Copy an OS distribution to the management server.

See [“To Copy an OS Distribution From ISO Files” on page 66](#) or [“To Copy an OS Distribution From CDs or a DVD” on page 67](#).

- Create a flash archive file.

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

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

See [“To Access the N1 System Manager Command Line” on page 25](#) for details.

2. Perform one of the following actions:

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

For example:

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

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

For example:

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

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

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

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

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

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

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

OR

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

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

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

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

The OS profile is created.

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

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

The OS profile details appear. Check that the partition settings are appropriate for your business needs. See [“To Create an OS Profile” on page 74](#) for partition settings and examples.

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

See [“To Load an OS Profile on a Server or a Server Group” on page 81](#).

Example 3–3 Deploying a Solaris 9 OS Flash Archive

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

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

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

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

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

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

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

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

▼ To Delete an OS Distribution

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

Before You Begin Delete all of the OS profiles that are associated with the OS distribution. This includes deleting the default OS profile that was created when the OS distribution was copied. An OS profile cannot be deleted while it is being deployed; it may be removed after the deployment is completed. See [“To Delete an OS Profile” on page 78](#) for instructions.

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

See [“To Access the N1 System Manager Command Line” on page 25](#) for details.

2. **Type the following command:**

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

The distribution is deleted. See “delete os” in *Sun N1 System Manager 1.1 Command Line Reference Manual* for details.

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

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

The deleted OS distribution should not appear in the output.

Managing OS Profiles

This section describes the following tasks:

- [“To List the Available OS Profiles” on page 74](#)
- [“To Create an OS Profile” on page 74](#)
- [“To Clone an Existing OS Profile” on page 76](#)
- [“To Modify an OS Profile” on page 77](#)
- [“To Delete an OS Profile” on page 78](#)

Creating, Listing, and Modifying OS Profiles

OS profiles specify the following information:

- OS distribution to install

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

After you have copied an OS distribution, the N1 System Manager automatically creates an OS profile of the same name on the management server. This OS profile is also called a *default OS profile* in documentation. See [“Default OS Profiles” on page 72](#) for parameter settings and best practices for customizing OS profiles.

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

To create a new OS profile, use the `create` command with the `osprofile` keyword and the `os` subcommand. OS profiles must specify a distribution group, partition configuration information, and a root password. To add required distribution groups to the OS profile, use the `add` command with the `osprofile` keyword and the `distributiongroup` subcommand. To add partitions to an OS profile, use the `add` command with the `osprofile` keyword and the `partition` subcommand. For example:

```
N1-ok> create osprofile osprofile os os
```

```
N1-ok> add osprofile osprofile partition partition
```

```
N1-ok> add osprofile osprofile distributiongroup distributiongroup
```

To modify existing OS profile attributes, use the `set` command with the `osprofile` keyword and an appropriate subcommand.

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

See [Example 3-5](#) and [Example 3-6](#) for command-line examples.

Default OS Profiles

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

TABLE 3-2 Default OS Profile Parameter Settings

Parameters	Solaris OS	Red Hat OS	SUSE OS
Root password	admin	admin	admin

TABLE 3-2 Default OS Profile Parameter Settings *(Continued)*

Parameters	Solaris OS	Red Hat OS	SUSE OS
Language	U.S. English	U.S. English	U.S. English
Time zone	Greenwich Mean Time (GMT)	Greenwich Mean Time (GMT)	Greenwich Mean Time (GMT)
Partitions	<ul style="list-style-type: none"> ■ Root mount point ufs with a free file system size option on the c1t1d0s0 slice ■ swap mount point 2048-Mbyte swap on the c1t1d0s1 slice 	<ul style="list-style-type: none"> ■ Root mount point ext3 with a free file system size option on the sda slice ■ swap mount point 2048-Mbyte swap on the sda slice 	<ul style="list-style-type: none"> ■ Root mount point reiser with a free file system size option on the /dev/sda slice ■ swap mount point 2048-Mbyte swap on the /dev/sda slice
Distribution group	Entire Distribution plus OEM support	Everything	Default Installation
Network Interfaces	Provisioning interface configured Data interface not configured	Provisioning interface configured Data interface not configured	Provisioning interface configured Data interface not configured

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

The browser interface provides a wizard for creating new OS profiles to limit the complexity of this operation. See [“To Create an OS Profile” on page 74](#) for instructions.

The following is a list of best practices for modifying default OS profiles:

- To increase the speed of OS configuration, modify OS profiles to use flash archives. See [Example 3-8](#) for examples of how to modify a default profile and [“To Copy a Flash Archive to the Management Server” on page 69](#) for instructions.
- To automatically configure the data network interface after OS profile installation, use the `add osprofile` command to add a script. See [Step 4](#).
- Modify the default OS profile for a server other than a V20z server, remember to remove the existing partitions and add new partition information that is appropriate for the server model. See [“To Modify the Default Solaris OS Profile for a Sun Fire V40z or a SPARC v440 Server” on page 191](#) for instructions.

▼ To List the Available OS Profiles

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

- Steps**
1. **Log in to the N1 System Manager.**
See [“To Access the N1 System Manager Command Line”](#) on page 25 for details.
 2. **Click the System Dashboard tab.**
The Shortcuts pane appears on the right side of the page.
 3. **Click the Edit List button beneath the OS Profiles list.**
The list of available OS profiles appears.

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

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

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

All available OS profiles appear in the output. See [“show osprofile”](#) in *Sun N1 System Manager 1.1 Command Line Reference Manual* for details.

▼ To Create an OS Profile

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

Before You Begin You must copy an OS distribution before you can create an OS profile. See [“To Copy an OS Distribution From CDs or a DVD”](#) on page 67 or [“To Copy an OS Distribution From ISO Files”](#) on page 66.

- Steps**
1. **Log in to the N1 System Manager.**
See [“To Access the N1 System Manager Command Line”](#) on page 25 for details.
 2. **Click the System Dashboard tab.**
The Shortcuts pane appears on the right side of the page.
 3. **Click the New button beneath the OS Profiles list.**
The Create New Operating System Profile wizard appears.
 4. **Use the wizard steps to guide you through the screens.**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- Troubleshooting** ■ [“To Modify the Default Solaris OS Profile for a Sun Fire V40z or a SPARC v440 Server” on page 191](#)
- [“To Modify a Solaris 9 OS Profile for a Sun Fire V20z Server With a K2.0 Motherboard” on page 192](#)

See Also To find out how to load the OS profile, see [“To Load an OS Profile on a Server or a Server Group” on page 81](#).

▼ To Clone an Existing OS Profile

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

Before You Begin Move any file systems off the /mnt mount point.

Steps 1. Log in to the N1 System Manager.

See [“To Access the N1 System Manager Command Line”](#) on page 25 for details.

2. Type the following command:

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

The new OS profile is created. See “create osprofile” in *Sun N1 System Manager 1.1 Command Line Reference Manual*

3. Type the following command:

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

The new OS profile appears in the output.

See Also To find out how to load the OS profile, see [“To Load an OS Profile on a Server or a Server Group”](#) on page 81.

▼ To Modify an OS Profile

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

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

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

See [“To Access the N1 System Manager Command Line”](#) on page 25 for details.

2. Modify an OS profile by performing one of the following actions:

■ **Add new OS profile attributes.**

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

See “add osprofile” in *Sun N1 System Manager 1.1 Command Line Reference Manual* for details.

■ **Remove existing OS profile attributes.**

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

See “remove osprofile” in *Sun N1 System Manager 1.1 Command Line Reference Manual* for details.

■ **Change existing OS profile parameters.**

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

See “set osprofile” in *Sun N1 System Manager 1.1 Command Line Reference Manual* for details.

3. View the new OS profile details.

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

The modified OS profile information appears in the output.

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

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

For this example, assume that you have created and made available to the management server's `/etc/sysconfig/network-scripts` directory, the following script to configure the provisionable server's `bge1` data network interface. This sample script will configure the `bge1` port at system boot time by using the data network DHCP server.

```
DEVICE=bge1
BOOTPROTO=dhcp
ONBOOT=yes
```

This example also assumes that you have created a flash archive file called `archive1.flar` and that you have completed the steps in [“To Copy a Flash Archive to the Management Server”](#) on page 69.

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

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

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

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

See Also To find out how to load the modified OS profile, see [“To Load an OS Profile on a Server or a Server Group”](#) on page 81.

▼ To Delete an OS Profile

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

Steps 1. Log in to the N1 System Manager.

See [“To Access the N1 System Manager Command Line”](#) on page 25 for details.

2. Type the following command:

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

The OS profile is deleted from the management server.

3. Type the following command:

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

The deleted OS profile should not appear in the output.

Installing OS Distributions by Deploying OS Profiles

This section describes the following tasks:

- [“Deploying OS Profiles” on page 79](#)
- [“To Load an OS Profile on a Server or a Server Group” on page 81](#)

Deploying OS Profiles

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

To deploy default or custom OS profiles, use the `load` command with the `server` or `group` keyword and the `osprofile` subcommand. To add the base and OS management features that support updating and patching, use the `add` command with the `server` keyword and the `basemanagement` or `osmonitor` subcommand.

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

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

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

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

TABLE 3-3 OS Profile Installation Parameters

Parameters	Red Hat or SUSE OS	Solaris OS	Multiple Servers	Single Server	Notes
<i>bootip</i>	✓ (R)		✓	✓	Also known as provisionable IP.
<i>ip</i>	✓	✓ (R)	✓	✓	Required if <i>networktype</i> is set to <i>static</i> .
<i>networktype</i>	✓ (R)	✓ (R)	✓	✓	Must be set to <i>static</i> for Solaris installation.
<i>bootgateway</i>	✓		✓	✓	
<i>boothostname</i>	✓			✓	
<i>bootnameserver</i>	✓		✓	✓	
<i>bootnetmask</i>	✓		✓	✓	Default is set to the provisioning network interface that is specified using the <i>n1smconfig</i> utility.
<i>bootnetworkdevice</i>	✓	✓		✓	
<i>bootpath</i>		✓		✓	
<i>console</i>	✓	✓		✓	
<i>consolebaud</i>	✓	✓		✓	
<i>kernelparameter</i>	✓		✓	✓	
<i>domainname</i>		✓	✓	✓	If <i>domainname</i> is not specified, a default will be configured
<i>gateway</i>	✓	✓	✓	✓	
<i>hostname</i>	✓	✓		✓	
<i>nameserver</i>	✓	✓	✓	✓	
<i>netmask</i>	✓	✓	✓	✓	Default is set to the provisioning network interface that is specified using the <i>n1smconfig</i> utility.
<i>networkdevice</i>	✓			✓	The Linux default is <i>eth0</i> . The Primary network interface is the default for Solaris installations.
(R) = Required					
✓ = Configurable					

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

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



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

Before You Begin

- Create an OS profile. See [“To Create an OS Profile” on page 74](#).
- Disable monitoring for the servers that will be loaded with an OS profile. See [“To Disable Monitoring for a Server” on page 145](#) for details. Disabling monitoring prevents the fault notifications that are generated as the server reboots after installation.
- Ensure that you have enough disk space available to load an OS profile.
- Optionally create and copy a flash archive file. See [“To Copy a Flash Archive to the Management Server” on page 69](#).
- Optionally create and copy a post-installation script to the management server. See [Step 4](#).

Steps 1. Log in to the N1 System Manager.

See [“To Access the N1 System Manager Browser Interface” on page 26](#) for details.

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

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

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

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

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

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

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

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

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

- **Choose All Servers from the View Selector menu.**

The Servers table appears.

- **Choose Servers By Group from the View Selector menu.**

The Server Groups table appears.

4. **Drag and drop the OS profile icon from the Shortcuts pane to the server or the server group.**

The Load OS Profile wizard appears.

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

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

6. **To begin loading the OS profile on the selected servers, click the Finish button in the wizard.**

The wizard window closes and a job ID appears in the Command Line pane.

7. **Click the Jobs tab.**

The Jobs table appears with information about your Load OS job.

Note – The Load OS job must complete before the server is available for login. After the Load OS job completes, a final reboot occurs.

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

See [“Modifying Server and Server Group Information”](#) on page 116 for details.

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

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

```
N1-ok> load server 192.168.8.9 osprofile S10profile
networktype static ip 192.168.18.19
```

The `networktype` attribute must be set to `static` for Solaris profile installations. See [Table 3–3](#) and “load server” in *Sun N1 System Manager 1.1 Command Line Reference Manual* for details.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Troubleshooting If a value is not specified for the `bootnetmask` or `netmask` parameters during the load operation, the netmask will default to the provisioning network interface that is specified in the `n1smconfig` utility. See “To Configure the Sun N1 System Manager System” in *Sun N1 System Manager 1.1 Installation and Configuration Guide*.

If the deployment fails, see the topics in “OS Profile Deployment Failures” on page 190 for possible solutions.

Next Steps To enable remote connectivity, OS resource monitoring, package deployment, and inventory management, you must add the OS management feature on each server. See [“To Add the OS Monitoring Feature” on page 85](#).

Adding Base and OS Management Features

Base and OS management features enable you to monitor and patch the installed OS profiles. This section describes how to add the features, modify supported attributes, and remove feature support. For more information about OS monitoring provided by the OS monitoring feature, see [Chapter 5](#).

This section describes the following tasks:

- [“To Add the Base Management Feature” on page 84](#)
- [“To Add the OS Monitoring Feature” on page 85](#)
- [“To Modify the Agent IP for a Server” on page 88](#)
- [“To Remove the OS Monitoring Feature” on page 87](#)
- [“To Manually Uninstall the Linux OS Monitoring Feature” on page 88](#)
- [“To Manually Uninstall the Solaris OS Monitoring Feature” on page 89](#)

▼ To Add the Base Management Feature

This procedure describes how to enable the base management feature on a server with a newly deployed OS. The base management feature is used to enable remote command execution and package deployment.

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

The agent IP used in this procedure is the IP address of the provisionable server’s data network interface to be monitored by the management server. The interface can be eth1/bge1 or eth0/bge0, but usually is eth0/bge0.

Before You Begin

- Discover servers. See [Chapter 2](#)
- Load an OS if an OS is not already installed. See [“To Load an OS Profile on a Server or a Server Group” on page 81](#) and “load server” in *Sun N1 System Manager 1.1 Command Line Reference Manual*.

Steps 1. Log in to the N1 System Manager.

See [“To Access the N1 System Manager Command Line”](#) on page 25 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 1.1 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 85

▼ To Add the OS Monitoring Feature

This procedure describes how to add the OS monitoring feature on a server. You can add the OS monitoring feature to a server that already has the base management feature added. Alternatively, you can add the OS monitoring feature to a server with a newly loaded OS and the base management feature is added automatically. The OS monitoring feature is used for OS resource monitoring and inventory management. See [Chapter 5](#) for details.

The `add server feature osmonitor` command creates an Add OS Monitoring Support job. You can submit multiple, overlapping `add server feature osmonitor` commands and have them run in parallel. However, you should limit the number of overlapping Add OS Monitoring Support jobs to a maximum of 15.

If you submit `add server feature` commands by using a script, see [Example 3-13](#) for an example.

Before You Begin

- Discover servers. See [Chapter 2](#)
- Load an OS if one is not already installed, see [“To Load an OS Profile on a Server or a Server Group”](#) on page 81 and [“load server”](#) in *Sun N1 System Manager 1.1 Command Line Reference Manual*.

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

See “To Access the N1 System Manager Command Line” on page 25 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 1.1 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. In addition, the show server command output will appear with the OS Monitoring Supported value as OK.

4. Verify that the OS monitoring feature is supported by issuing one of the following sets of commands on the provisionable server.

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

```
# pkginfo |grep nlgc
system          SUNWnlgcso1x86ag          Nlgc Solaris x86 Agent
# ps -ef |grep -i esd
root 23817      1  0 19:57:59 ?          0:01 esd - init agent -dir
/var/opt/SUNWsymon -q
```

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

```
# rpm -qa | grep -i sun-symon-esagt
sun-symon-esagt-3.6-1.0
# ps -ef | grep -i esd
root 1940 1 0 Jan28 ? 00:00:14 esd - init agent -dir
```

```
/var/opt/SUNWsymon -q
```

Example 3-13 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 admin/admin &
n1sh add server 10.0.0.11 feature=osmonitor agentip 10.0.0.111 agentssh admin/admin &
n1sh add server 10.0.0.12 feature=osmonitor agentip 10.0.0.112 agentssh admin/admin &
```

Troubleshooting You must manually install the `wget` information if the `add server` feature `osmonitor agentip` command fails with the following error: Internal error: `wget` command failed: `/usr/bin/wget -O /tmp/hostinstall.pl http://xx.xx.xx.xx/pub/hostinstall.pl`, where `xx.xx.xx.xx` is the IP address of the machine in question. To correct this error, perform the following actions:

- For the Solaris Operating System, install the `SUNWwgetu` and `SUNWwgetr` packages in `/usr/sfw/bin/wget`.
- For Linux OS, install all RPMs that begin with `wget-` in `/usr/bin/wget`.

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 `/root/.ssh/known_hosts` file or the specific entry in the file that corresponds to the provisionable server. Then, retry the `add server` feature `osmonitor agentip` command.

Adding the OS monitoring feature might also 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

Steps 1. Log in to the N1 System Manager.

See [“To Access the N1 System Manager Command Line”](#) on page 25 for details.

2. Remove the OS monitoring feature.

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

The necessary packages and scripts are removed. See *“remove server”* in *Sun N1 System Manager 1.1 Command Line Reference Manual* for details about command syntax.

▼ To Modify the Agent IP for a Server

This procedure describes how to modify the agent IP for a server. The agent IP is the IP address of the provisionable server's data network interface to be monitored by the management server.

Note – If you change the provisionable server's IP address and credentials or manually remove some services outside the N1 System Manager, the enabling of the services will not succeed. Arbitrary changes to the OS outside of the N1 System Manager requires a rediscovery and subsequent addition of the base and OS management features.

- Steps**
1. **Log in to the N1 System Manager.**
See [“To Access the N1 System Manager Command Line”](#) on page 25 for details.
 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 agentsnmp public-community-string
```

The agent IP is modified. See *“add server”* in *Sun N1 System Manager 1.1 Command Line Reference Manual* for details about command syntax.

▼ To Manually Uninstall the Linux OS Monitoring Feature

After successful completion of this procedure, the OS monitoring feature will be unsupported for the provisionable server:

- Steps**
1. **Log in to the provisionable server as root.**
 2. **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 sunmc-linux-agent
```

The feature is removed.

5. Remove directories related to the feature.

```
# rm -rf /var/opt/SUNWsymon
```

The directories are removed.

▼ To Manually Uninstall the Solaris OS Monitoring Feature

After successful completion of this procedure, the OS monitoring feature will be unsupported for the provisionable server.

Steps 1. Log in to the provisionable server as root.

2. Stop the agent.

```
# /etc/rc3.d/S81es_agent stop
```

3. Run the uninstaller.

```
# /var/tmp/solx86-agent-installer/disk1/x86/sbin/es-uninst -X
```

4. Remove the packages.

```
# pkgrm SUNWnlgcsolx86ag
```

5. Remove associated directories.

```
# /bin/rm -rf /opt/SUNWsymon
# /bin/rm -rf /var/opt/SUNWsymon
```

The directories are removed.

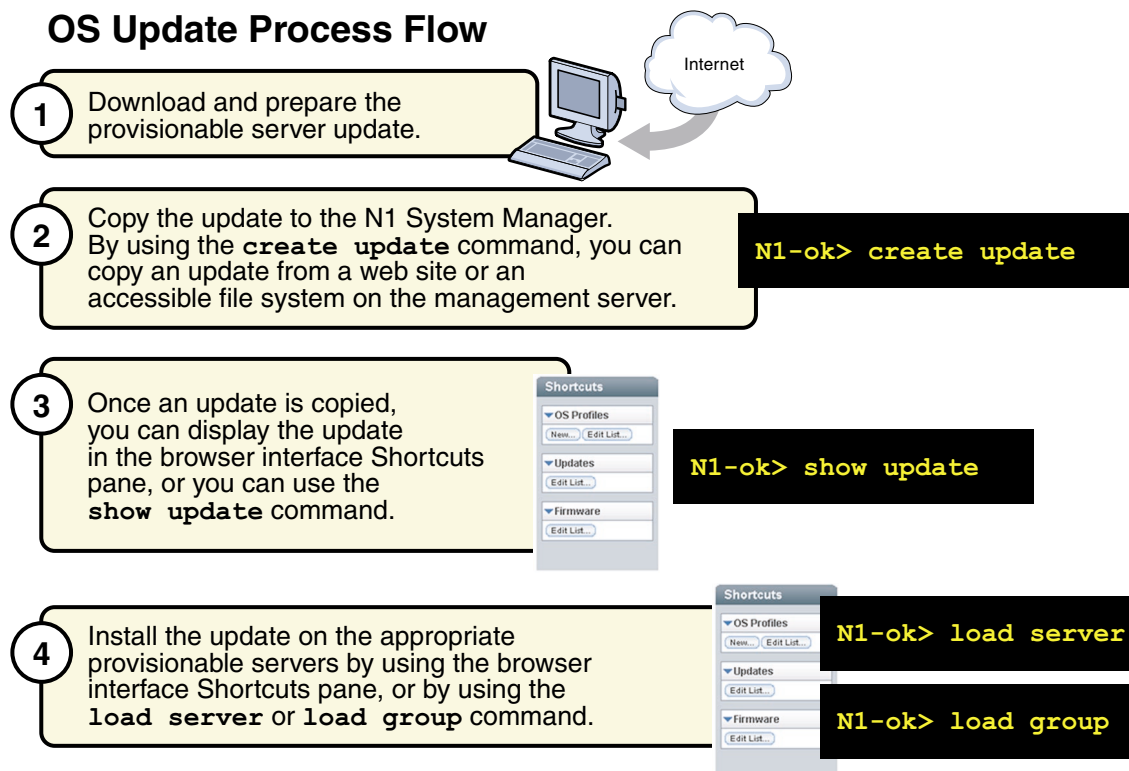
Managing Packages, Patches, and RPMs

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

- [“To Copy an OS Update” on page 91](#)
- [“To Load an OS Update on a Server or a Server Group” on page 93](#)
- [“To List the Available OS Updates” on page 95](#)

- “To List the OS Updates Installed on a Provisionable Server” on page 96
- “To Delete an OS Update” on page 96
- “To Uninstall an OS Update on a Provisionable Server” on page 96
- “To Uninstall an OS Update on a Server Group” on page 97

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



Introduction to Managing OS Updates

After you have installed an OS on a provisionable server, the N1 System Manager enables you to install OS updates. These OS updates consist of Solaris packages and patches and Linux RPMs. Installing OS updates on servers for the first time involves the following four-step process when you use the N1 System Manager:

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

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

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

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

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

See [“OS Update Problems” on page 197](#) for troubleshooting information.

▼ To Copy an OS Update

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

The following graphic illustrates the process for copying a new OS update.

Update Process Flow

- 1 Copy the required OS update to the N1 System Manager.

The screenshot displays the Sun N1 System Manager web interface. At the top, it shows 'User: Admin (root) - Server: proto183' and 'Sun N1 System Manager'. The 'View Selector' on the left shows 'All Servers'. The main area is titled 'All Servers' and contains a table with columns: Name, Hardware, Hardware Health, Power, OS Usage, OS Resource Health, and Jobs. A table with two rows is visible, showing 'server 200.3' and 'V20z' with 'Unreachable' status. On the right, the 'Shortcuts' pane is expanded to show 'Updates' and 'Firmware', each with an 'Edit List...' button. A terminal window at the bottom shows the command 'N1-ok> show update' entered. Callouts with numbered circles 1 and 2 point to the 'Edit List...' button in the Shortcuts pane and the terminal command respectively.

2 Once an OS update is copied, use one of two ways to check the update status.

N1-ok> show update

Use the `show update` command.

Display the update in the browser interface Shortcuts pane.

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

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

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

Steps 1. Log in to the N1 System Manager.

See [“To Access the N1 System Manager Command Line”](#) on page 25 for details.

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

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

Valid ostype values are in the following list:

- redhat-es3 – Red Hat Enterprise Linux ES 3.0
- redhat-as3 – Red Hat Enterprise Linux, AS 3.0
- redhat-as4 – Red Hat Enterprise Linux, AS 4.0
- redhat-es3-64 – Red Hat Enterprise Linux ES 3.0, 64 bit
- redhat-as3-64 – Red Hat Enterprise Linux, AS 3.0, 64 bit
- redhat-as4-64 – Red Hat Enterprise Linux, AS 4.0, 64 bit
- solaris9x86 – Solaris OS on x86 platform Version 9 7/05
- solaris10x86 – Solaris OS on x86 platform Version 10
- solaris9sparc – Solaris OS on SPARC platform Version 9 7/05
- solaris10sparc – Solaris OS on SPARC platform Version 10
- suse-es9 – SUSE LINUX Enterprise Server 9
- suse-es9-64 –SUSE LINUX Enterprise Server 9, 64 bit

See “create update” in *Sun N1 System Manager 1.1 Command Line Reference Manual* for details.

Example 3–14 Creating an OS Update Through the Command Line

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

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

Troubleshooting [“OS Update Creation Failures”](#) on page 197

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

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

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

```
mail=root
instance=unique
partial=nocheck
runlevel=nocheck
idepend=nocheck
rdepend=nocheck
```

```
space=quit
setuid=nocheck
conflict=nocheck
action=nocheck
basedir=default
authentication=nocheck
```

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

Before You Begin

- The OS update must be copied to the N1 System Manager. See [“To Copy an OS Update” on page 91](#) for details.
- Disable monitoring for the provisionable server. This action is required only if you want to avoid the fault notifications as the server reboots after an OS update installation. See [“To Disable Monitoring for a Server Group” on page 146](#) for details.
- Ensure that the base management feature is added to the provisionable server. This action provides the necessary support to install OS updates. You can automatically add base management support by adding the OS monitoring feature. See [“To Add the OS Monitoring Feature” on page 85](#) for details.

Steps

1. **Log in to the N1 System Manager.**
See [“To Access the N1 System Manager Browser Interface” on page 26](#) for details.
2. **Navigate to the table that contains the server or the server group by performing one of the following actions:**
 - **Choose All Servers from the View Selector menu.**
The Servers table appears.
 - **Choose Servers By Group from the View Selector menu.**
The Server Groups table appears.
3. **Drag and drop the OS update icon from the Shortcuts pane to the server or the server group.**
The Load OS Update confirmation dialog box appears.
4. **To begin loading the OS update on the selected servers, click the OK button.**
The dialog box closes.
5. **Click the Jobs tab.**
The Jobs table appears with information about your Load OS Update job.
6. **Verify that the installation was successful.**

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

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

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

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

See “load server” in *Sun N1 System Manager 1.1 Command Line Reference Manual* for details.

Example 3–16 Loading an OS Update on a Server Group

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

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

See “load group” in *Sun N1 System Manager 1.1 Command Line Reference Manual* for details.

Troubleshooting [“OS Update Deployment Failures” on page 198](#)

▼ To List the Available OS Updates

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

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

- Steps**
1. **Log in to the N1 System Manager.**
See [“To Access the N1 System Manager Browser Interface” on page 26](#) for details.
 2. **Click the System Dashboard tab.**
The Shortcuts pane appears.
 3. **Click the Expand/Collapse icon on the Update title bar.**
The Update list expands.
 4. **Click the Edit List button.**
The Edit List dialog box appears with the list of available updates.

Example 3–17 Listing Available OS Updates Through the Command Line

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

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

▼ To List the OS Updates Installed on a Provisionable Server

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

- Steps**
1. **Log in to the N1 System Manager.**
See [“To Access the N1 System Manager Command Line” on page 25](#) for details.
 2. **List the OS updates that are installed on a provisionable server.**

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


See *“show server” in Sun N1 System Manager 1.1 Command Line Reference Manual* for details

▼ To Delete an OS Update

This procedure describes how to delete an OS update from the N1 System Manager. This procedure does not delete an OS update from a provisionable server. See [“To Uninstall an OS Update on a Provisionable Server” on page 96](#) for details on that specific task.

- Steps**
1. **Log in to the N1 System Manager.**
See [“To Access the N1 System Manager Command Line” on page 25](#) for details.
 2. **Delete an OS update from the N1 System Manager.**

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


See *“delete update” in Sun N1 System Manager 1.1 Command Line Reference Manual* for details.

▼ To Uninstall an OS Update on a Provisionable Server

- Before You Begin**
- Disable monitoring for the provisionable server. Disabling monitoring prevents the fault notifications as the server reboots after an OS update uninstallation. See [“To Disable Monitoring for a Server Group” on page 146](#) for details.
 - Ensure that the OS monitoring feature is supported on the provisionable server. This action provides the necessary support to uninstall OS updates. See [“To Add the OS Monitoring Feature” on page 85](#) for details.

Steps 1. Log in to the N1 System Manager.

See [“To Access the N1 System Manager Command Line”](#) on page 25 for details.

2. Uninstall an OS update from a provisionable server.

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



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

See “unload server” in *Sun N1 System Manager 1.1 Command Line Reference Manual* for details.

▼ To Uninstall an OS Update on a Server Group

Before You Begin

- Disable monitoring for the provisionable servers. This action is required only if you want to avoid the fault notifications as the servers reboot after an OS update uninstallation. See [“To Disable Monitoring for a Server Group”](#) on page 146 for details.
- Ensure that the OS monitoring feature is supported on the provisionable servers. This action provides the necessary support to uninstall OS updates. See [“To Add the OS Monitoring Feature”](#) on page 85 for details.

Steps 1. Log in to the N1 System Manager.

See [“To Access the N1 System Manager Command Line”](#) on page 25 for details.

2. Uninstall an OS update on the provisionable servers in a server group.

```
N1-ok> unload group group update update
```



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

See “unload group” in *Sun N1 System Manager 1.1 Command Line Reference Manual* for details.

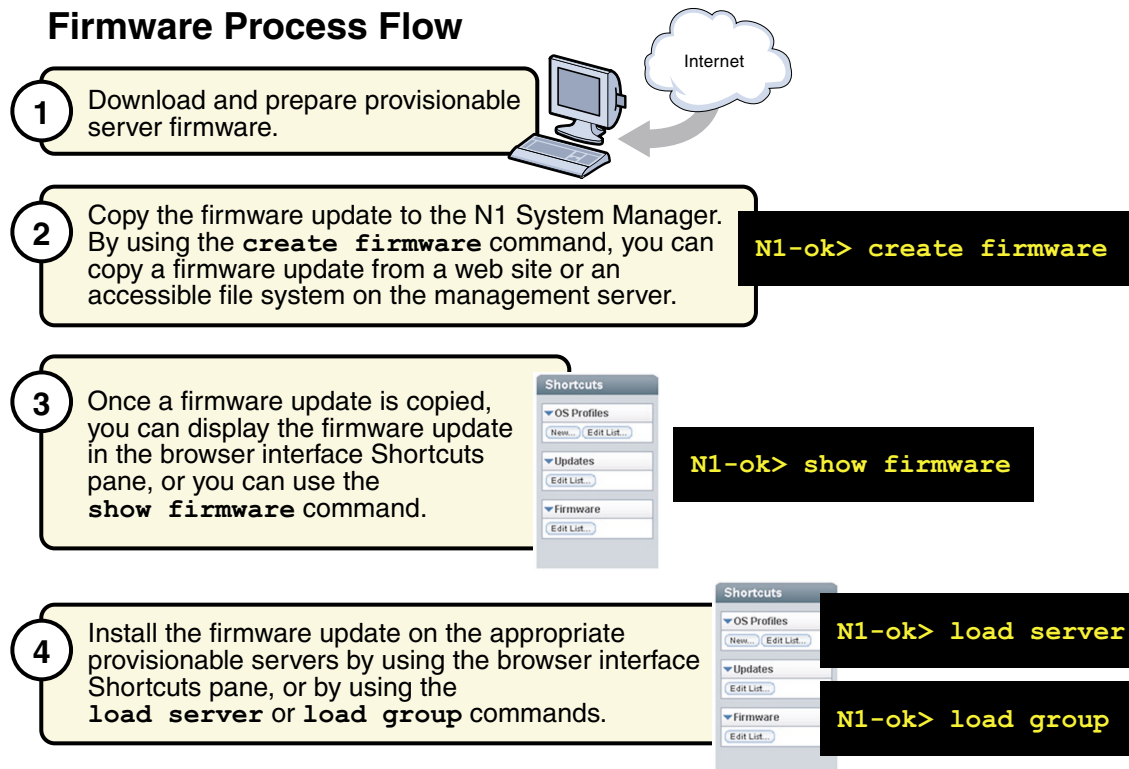
Managing Firmware SP, BIOS, and ALOM Updates

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

- “To Copy a Firmware Update” on page 99
- “To Load a Firmware Update on a Server or a Server Group” on page 101
- “To List the Available Firmware Updates” on page 103
- “To List the Firmware Updates Installed on a Provisionable Server” on page 104
- “To Modify Firmware Update Information” on page 104
- “To Delete a Firmware Update” on page 104

The following graphic describes the order in which firmware management tasks must be performed.

Firmware Process Flow



Introduction to Managing Firmware Updates

Updating the firmware on the provisionable servers is a primary administrative task. Installing a firmware update on a provisionable server for the first time involves the following four-step process when you use the N1 System Manager:

1. Download and prepare the firmware update.
2. Copying the firmware update to the N1 System Manager. The N1 System Manager must have system access to the firmware update before the firmware update can be installed on the provisionable servers.

By using the `create firmware` command, you can copy a firmware update from a web site or an accessible file system on the management server. Once a firmware update is copied, you can display the firmware update in the browser interface Shortcuts pane, or you can use the `show firmware` command.

3. Verify that the firmware update was copied successfully by displaying the firmware Shortcut in the browser interface or by using the `show firmware` command.
4. Installing the firmware update on the appropriate provisionable servers by using the browser interface, or by using the `load server` or `load group` command.

When importing firmware updates, you must specify the following metadata:

- Vendor – The name of the firmware update vendor
- Model – The model name of a valid hardware system for the firmware update
- Type – The type of firmware update, required only for Sun Fire V20z and V40z servers:
 - SP – Service Processor
 - BIOS – Server Platform BIOS
 - PIC – Service Processor Operator Panel
- Version – (Optional) The version number of the firmware update

Note – Firmware version 2.2 and above for the Sun Fire V20z servers do not support the PIC firmware upgrade. The upgrade of PIC firmware will fail, and the job step will show an error message similar to the following: “This operation is not supported on *server*. Refer to the log file for more information.”

▼ To Copy a Firmware Update

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

The following graphic illustrates the steps to copy a firmware update.

Firmware Process Flow

- 1 Copy the required firmware to the N1 System Manager.

The screenshot shows the Sun N1 System Manager web interface. At the top, it says 'Sun N1 System Manager' with a 'LOG OUT' and 'HELP' link. Below the header, there's a 'View Selector' on the left and a 'System Dashboard' with tabs for 'System Dashboard', 'Jobs', and 'Event Log'. The main area displays 'All Servers' with a table of servers. The table has columns: Name, Hardware, Hardware Health, Power, OS Usage, OS Resource Health, and Jobs. One server is listed: 'server 200.3' with hardware 'V20z', hardware health 'Unreachable', power 'Unreachable', OS usage '-', OS resource health 'Uninitialized', and jobs '0'. On the right, there's a 'Shortcuts' pane with sections for 'OS Profiles', 'Updates', and 'Firmware'. The 'Firmware' section has an 'Edit List...' button. A terminal window is overlaid on the interface, showing the command 'N1-ok> show firmware'.

2 Once the firmware is copied, use one of two ways to check the update status.

N1-ok> show firmware

Use the `show firmware` command.

Display the firmware in the browser interface Shortcuts pane.

Before You Begin Ensure that the firmware update is available to the management server from the local file system, a network accessible file, or a web site.

Steps 1. Log in to the N1 System Manager.

See [“To Access the N1 System Manager Command Line”](#) on page 25 for details.

2. Copy the firmware update.

```
N1-ok> create firmware firmware url=url vendor=vendor model=model[,model...] [type type]
[description description] [version version]
```

Note – The valid value for `vendor` is `Sun`. The valid values for `model` are the following: `V20z`, `SF-V210`, `SF-V240`, `SF-V440`, `NETRA-440`, `NETRA-240`, `SF-V250`, `X4100`, `X4200`, and `V40z`. The `type` attribute value is only required for `V20z` and `V40z` servers. Valid values for the `type` are `BIOS` or `SP`. All values are case-sensitive.

See “create firmware” in *Sun N1 System Manager 1.1 Command Line Reference Manual* for details.

3. Verify that the firmware update was copied.

`N1-ok> show firmware firmware`

See “show firmware” in *Sun N1 System Manager 1.1 Command Line Reference Manual* for details.

See Also ■ [“To Load a Firmware Update on a Server or a Server Group” on page 101](#)

▼ To Load a Firmware Update on a Server or a Server Group

This procedure describes how to load a firmware update by using the browser interface. The examples that follow the procedure provide command-line equivalents.

Before You Begin

- Consult your hardware documentation for instructions and information on upgrading your server firmware. See the Sun System Handbook documentation for your server.
- The firmware update must be copied to the N1 System Manager. See [“To Copy a Firmware Update” on page 99](#) for details.
- Power off the provisionable server by using the browser interface or the command line before loading a firmware update on it (except for a firmware SP update on a Sun Fire V20z, Sun Fire V40z, or ALOM(1.5)-based server, which can remain powered on). The `stop server` command performs a graceful shutdown of the OS on the server, followed by a power off. The base management and OS monitoring features must be added to the server to perform this step. Otherwise, you must perform the shutdown and power off actions outside of the N1 System Manager.
- Disable monitoring for the provisionable server. This action is required only if you want to avoid the fault notifications as you shut down the OS on the server to complete the firmware installation. See [“To Disable Monitoring for a Server Group” on page 146](#) for details.

Note – Firmware version 2.2 and above for the Sun Fire V20z servers do not support the PIC firmware upgrade. The upgrade of PIC firmware will fail, and the job step will show an error message similar to the following: “This operation is not supported on *server*. Refer to the log file for more information.”

- Steps**
1. **Log in to the N1 System Manager.**
See “[To Access the N1 System Manager Browser Interface](#)” on page 26 for details.
 2. **Choose All Servers from the View Selector menu.**
The Servers table appears.
 3. **Select the server or servers that you want to update.**
A check mark appears.
 4. **Choose Load Firmware from the Actions menu.**
The Load Firmware dialog box appears
 5. **Select the appropriate firmware from the Firmware menu.**
 6. **To apply the firmware update to the listed target servers, click OK.**
The dialog box closes.
 7. **Click the Jobs tab.**
A Load Firmware job appears in the Jobs table.
 8. **Click the job ID.**
The Job Details page appears. Job steps indicate progress and results. Review the information in the Results section of the Job Details page to determine which servers were successfully updated.

Note – After successful completion, the firmware version number is updated with the actual version number that is reported by the hardware. If the reported version number does not match the original version number, a warning is logged.

9. **Verify that the installation was successful.**

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

Example 3–18 Loading Firmware on a Server Through the Command Line

The following example command shows you how to stop a server in preparation for installing a firmware update.

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

The following example command shows you how to install a firmware update on a server by using the `load` command.

```
N1-ok> load server server1,server2 firmware v20z-bios.sp force
```

See “load server” in *Sun N1 System Manager 1.1 Command Line Reference Manual* for details.

By default, the firmware update’s model and vendor settings must match every provisionable server that you select for installation; otherwise, the update fails. You can specify the `force` option to bypass this check. However, installing a noncompatible firmware update on a server might render the server unusable.

Example 3–19 Loading Firmware on a Server Group Through the Command Line

The following example command shows you how to stop a server group in preparation for installing a firmware update.

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

The following example command shows you how to install a firmware update on a server group by using the `load` command.

```
N1-ok> load group devgroup firmware bios.sp
```

See “load group” in *Sun N1 System Manager 1.1 Command Line Reference Manual* for details.

▼ To List the Available Firmware Updates

This procedure describes how to list the available firmware updates by using the browser interface. The example that follow the procedure provides the command-line equivalent.

- Steps**
1. **Log in to the N1 System Manager.**
See “To Access the N1 System Manager Browser Interface” on page 26 for details.
 2. **Click the System Dashboard tab.**
The Shortcuts pane appears.
 3. **Click the Expand/Collapse icon on the Firmware title bar.**
The Firmware list expands.
 4. **Click the Edit List button.**
The Edit List dialog box appears with the available firmware list.

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

```
N1-ok> show firmware all
```

▼ To List the Firmware Updates Installed on a Provisionable Server

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

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

See “To Access the N1 System Manager Command Line” on page 25 for details.

2. **List the firmware updates that are installed on a provisionable server.**

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

See “show server” in *Sun N1 System Manager 1.1 Command Line Reference Manual* for details.

▼ To Modify Firmware Update Information

This procedure describes how to modify the information about a firmware update.

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

See “To Access the N1 System Manager Command Line” on page 25 for details.

2. **Modify the name or description of a firmware update.**

```
N1-ok> set firmware firmware [description description]
[name name] [model=model]
[vendor=vendor] [version=version]
```

See “set firmware” in *Sun N1 System Manager 1.1 Command Line Reference Manual* for details.

▼ To Delete a Firmware Update

This procedure describes how to delete a firmware update from the N1 System Manager. This procedure does not delete a firmware update from a provisionable server. After you install a firmware update on a provisionable server, you cannot uninstall it.

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

See [“To Access the N1 System Manager Command Line”](#) on page 25 for details.

2. **Delete a firmware update from the N1 System Manager.**

```
N1-ok> delete firmware firmware
```

See “delete firmware” in *Sun N1 System Manager 1.1 Command Line Reference Manual* for details.

Managing Servers and Server Groups

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

The N1 System Manager enables you to perform the server maintenance tasks described in the following sections:

- [“Introduction to Server and Group Management” on page 107](#)
- [“Listing and Viewing Servers and Server Groups” on page 111](#)
- [“Modifying Server and Server Group Information” on page 116](#)
- [“Starting, Stopping, and Resetting Servers and Server Groups” on page 120](#)
- [“Issuing Remote Commands on Servers and Server Groups” on page 127](#)
- [“Connecting to the Serial Console for a Server” on page 131](#)
- [“Refreshing and Finding Servers and Server Groups” on page 134](#)
- [“Deleting Servers and Server Groups” on page 136](#)

Introduction to Server and Group Management

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

You can use the `discover` command to initiate the management of provisionable servers. The server discovery process creates a Discovery job in the N1 System Manager. The Discovery job uses the management IP address and default security credentials to identify each physical server. You can view the job results to track the discovery process.

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

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

The sections in this chapter describe the prerequisites and instructions for performing server and server group maintenance tasks. You will use the View Selector menu, the Actions menu, and server name links to perform the operations that are described in these sections.

The following graphic shows the View Selector menu, the Actions menu, and the server name links.

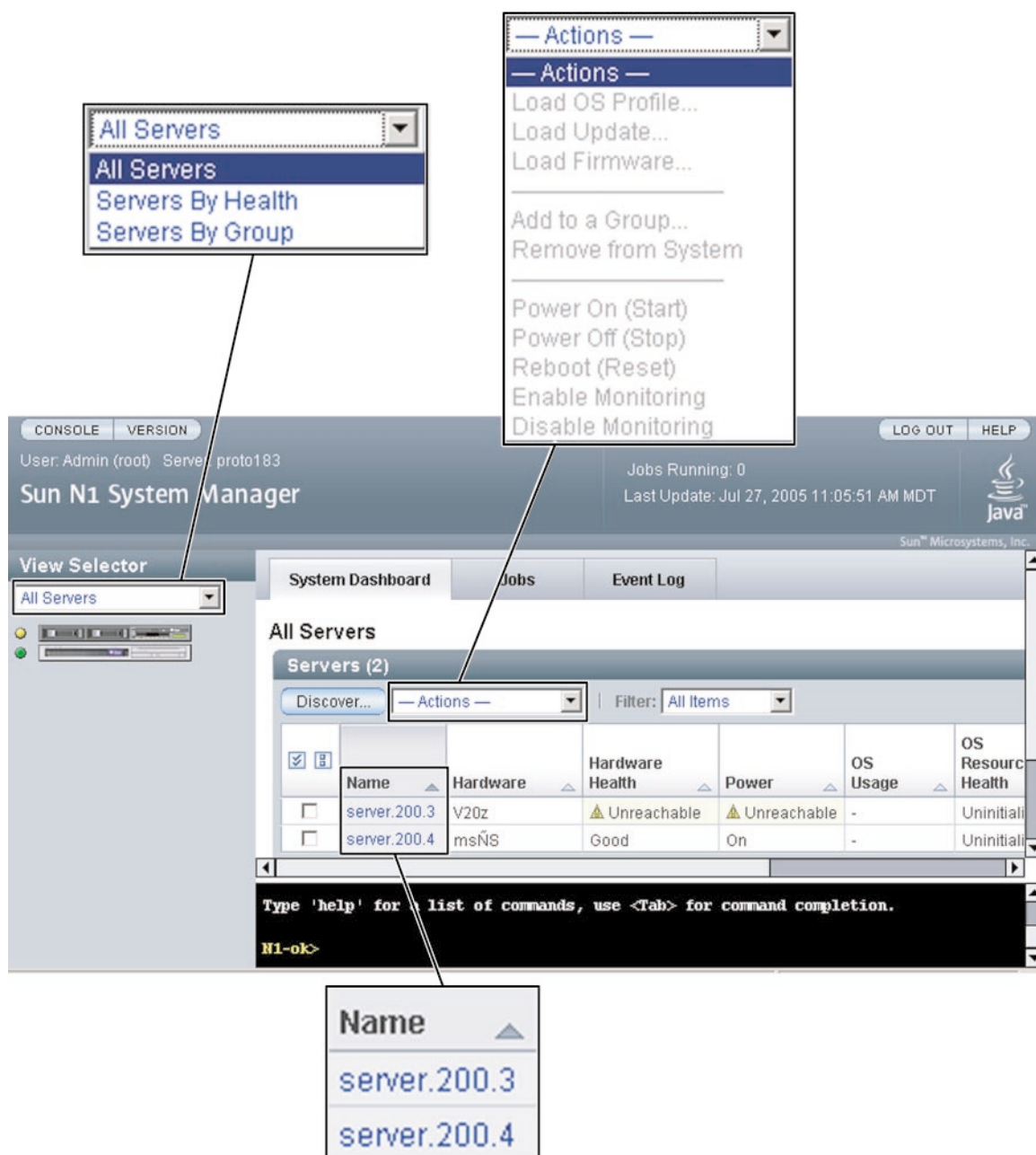


FIGURE 4-1 Menus and Links in the Browser Interface

Identifying Servers and Server States

This section describes the information that the N1 System Manager reports for each server when you issue the `show server all` and `show group` commands.

- **Name** – The server or server group name. Server name is initially set to the management IP address. For instructions on how to change this name, see [“Modifying Server and Server Group Information” on page 116](#).
- **Hardware** – Describes the type of managed server. See the Sun System Handbook documentation for your provisionable server.
- **Hardware Health** – The status for attributes such as memory, processor information, and Network Interface Card (NIC) information.
- **Power** – Power status for the physical server.
- **OS Usage** – If an OS profile is loaded, the OS name appears here.
- **OS Resource Health** – If an OS profile is loaded, the OS state appears here.
- **Jobs** – If a job is in progress or has completed on the server, the job ID appears here.

Server Power States

Server power is indicated by the following states:

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

Hardware Health States

Server hardware health is indicated by the following states:

- **Good** – The server hardware is working properly.
- **Unreachable** – The server cannot be contacted for information about the status of hardware health. This state is most often caused by a network problem.
- **Warning Failure** – A potential or impending fault condition has been detected on the server. Take action to prevent the problem from becoming more serious. See [“Monitoring Threshold Values” on page 147](#) for information about viewing and tuning hardware sensor threshold values.
- **Critical Failure** – A fault condition has occurred on the server. Corrective action is required.
- **Nonrecoverable Failure** – The server has completely failed. Recovery is not possible.

- **Unknown** – The server is not returning any hardware health status.
- **Offline** – The server is not managed.

Supported Server Actions

The following aggregate server actions are supported:

- Starting, stopping, and resetting server power
- Listing and refreshing server data
- Loading servers with OS profiles, updates, and firmware. See [Chapter 3](#)
- Enabling and disabling server monitoring. See [Chapter 5](#)
- Adding servers to server groups. See [“Creating and Maintaining Server Groups” on page 53](#).
- Removing servers from the N1 System Manager

Listing and Viewing Servers and Server Groups

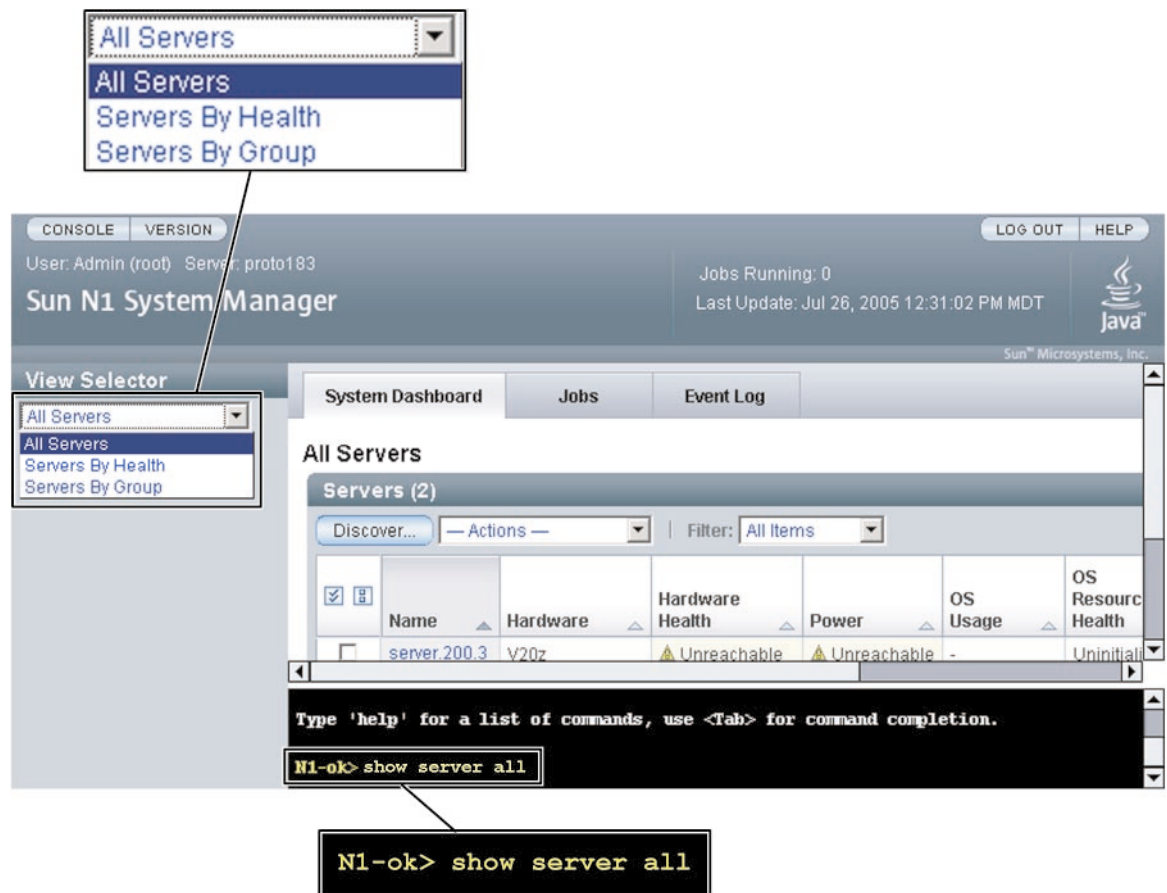
This section describes the following tasks:

- [“To List Servers and Server Groups” on page 112](#)
- [“To View Failed Servers” on page 113](#)
- [“To View Server Details and Server Group Members” on page 115](#)

Listing Servers and Server Groups

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

As the following graphic shows, you can use the View Selector menu or the `show server` command to list servers.



▼ To List Servers and Server Groups

This procedure describes how to list servers and server groups by using the browser interface. The example that follows the procedure provides a command-line equivalent.

- Steps**
1. **Log in to the N1 System Manager.**
See [“To Access the N1 System Manager Browser Interface”](#) on page 26 for details.
 2. **Navigate to the table that contains the server or the server group by performing one of the following actions:**
 - **Choose All Servers from the View Selector menu.**
The Servers table appears.

- **Choose Servers By Group from the View Selector menu.**

The Server Groups table appears.

Example 4–1 Listing Servers Through the Command Line

The following example shows how to view all servers in the system by using the `show` command.

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

A list of all servers in the system appears. See “show server” in *Sun N1 System Manager 1.1 Command Line Reference Manual* for details.

Example 4–2 Listing Groups Through the Command Line

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

A list of all server groups in the system appears. See “show group” in *Sun N1 System Manager 1.1 Command Line Reference Manual* for details.

▼ To View Failed Servers

This procedure describes how to view failed servers using the browser interface. The example following the procedure provides a command-line equivalent.

The following graphic shows how to use the View Selector menu to list servers by health state. Alternatively, use the `health` subcommand and an appropriate health state to filter the list of servers by health state. For example:

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

The screenshot shows the Sun N1 System Manager web interface. At the top, there's a header with 'CONSOLE' and 'VERSION' tabs, user information 'User: Admin (root) Server: proto183', and system status 'Jobs Running: 0' and 'Last Update: Jul 26, 2005 12:31:02 PM MDT'. The main content area is titled 'Sun N1 System Manager' and includes a 'View Selector' on the left. The 'View Selector' has a dropdown menu with 'All Servers', 'Servers By Health' (selected), and 'Servers By Group'. Below the dropdown, there are buttons for 'Failed Nonrecoverable' (0 Servers), 'Failed Critical' (0 Servers), 'Failed Warning' (0 Servers), 'Good' (1 Server), 'Unknown' (0 Servers), and 'Unreachable' (1 Server). The main panel displays 'Servers By Health' with a 'Health Summary (6)' table. The table has columns: Name, Servers, Hardware Faults, and OS Resource Faults. The rows are: Failed Nonrecoverable (0), Failed Critical (0), Failed Warning (0), and Good (1). Below the table, there's a console area with the prompt 'N1-ok> show server health critical'.

View Selector

- All Servers
- Servers By Health
- Servers By Group

Failed Nonrecoverable
0 Servers

Failed Critical
0 Servers

Failed Warning
0 Servers

Good
1 Server

Unknown
0 Servers

Unreachable
1 Server

Health Summary (6)

Name	Servers	Hardware Faults	OS Resource Faults
Failed Nonrecoverable	0	-	-
Failed Critical	0	-	-
Failed Warning	0	-	-
Good	1	-	-

Type 'help' for a list of commands, use <Tab> for command completion.

N1-ok> show server health critical

- Steps**
1. Log in to the N1 System Manager.
See "To Access the N1 System Manager Browser Interface" on page 26 for details.
 2. Choose Servers By Health from the View Selector menu.
The Health Summary table appears.

Note – You cannot perform any actions on servers from the Health Summary table.

3. Select the fault state that you want to view.
The available fault states are:
 - Failed Nonrecoverable
 - Failed Critical

- Failed Warning
- Unreachable
- Unknown

The list of servers in the selected state appears. See [“Hardware Health States” on page 110](#) for a description of fault states.

Example 4–3 Viewing Failed Critical Servers Through the Command Line

The following example shows how to view servers that have a health status of critical.

```
N1-ok> show server health critical
Name           Hardware  Hardware Health  Power  OS Usage  OS Resource Health
10.0.0.26      V20z     Failed Critical   On     Solaris   Unknown
```

See Also For descriptions of the icons and various failure levels that are shown on the Servers By Health page, see [“Hardware Health States” on page 110](#). For descriptions of monitoring thresholds, see [“Hardware Sensor Attributes” on page 152](#).

Viewing Server Details and Group Members

To view detailed server information and group members, use the show command with the server or group keyword. For syntax and parameter details, type help show server or help show group at the N1-ok command line. Server information is also provided on the Server Details page in the browser interface.

▼ To View Server Details and Server Group Members

This procedure describes how to view server details and server group members by using the browser interface. The example that follows the procedure provides a command-line equivalent.

- Steps**
1. **Log in to the N1 System Manager.**
See [“To Access the N1 System Manager Browser Interface” on page 26](#) for details.
 2. **Navigate to the table that contains the server or the server group by performing one of the following actions:**
 - **Choose All Servers from the View Selector menu.**
The Servers table appears.
 - **Choose Servers By Group from the View Selector menu.**
The Server Groups table appears.

3. **Select the server or the server group that you want to view.**

The Server Details page or the Servers By Group page appears.

Example 4–4 Viewing Server Details Through the Command Line

The following example shows how to view the server details by using the `show` command.

```
N1-ok> show server server1
```

Detailed server information appears. See “show server” in *Sun N1 System Manager 1.1 Command Line Reference Manual* for details.

Example 4–5 Viewing Server Group Members Through the Command Line

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

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

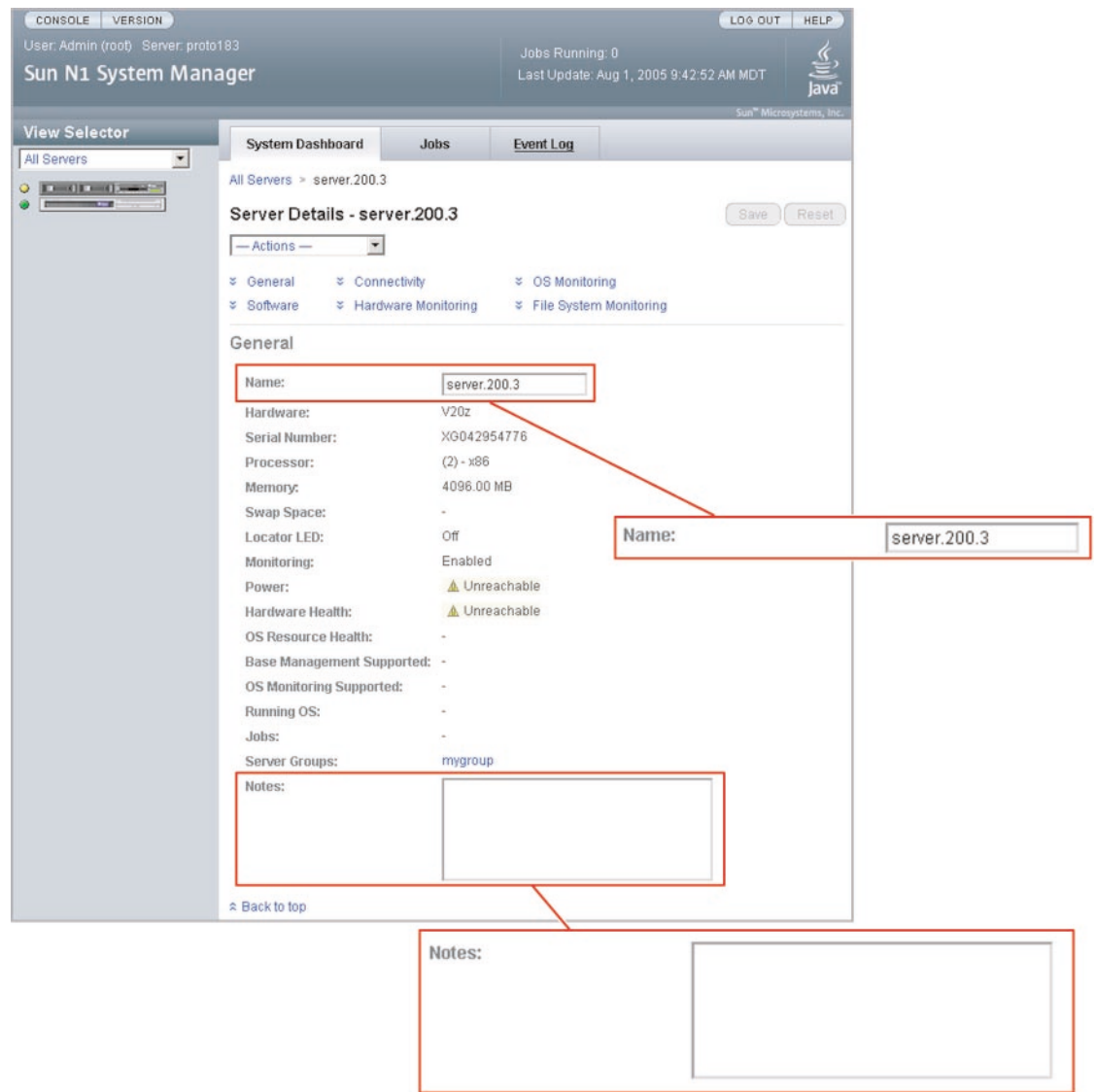
The list of servers in the group appears. See “show group” in *Sun N1 System Manager 1.1 Command Line Reference Manual* for details.

Modifying Server and Server Group Information

This section describes the following tasks:

- [“To Rename a Server or a Server Group” on page 118](#)
- [“To Add a Server Note” on page 119](#)

The following graphic illustrates how to rename servers and server groups by using the Server Details page. Alternatively, use the `set` command with the `server` or `group` keyword and the `name` subcommand. For syntax and parameter details, type `help set server` or `help set group` at the `N1-ok` command line.



Renaming a Server or a Server Group

Servers are identified by the management IP address that is specified during discovery. This name is also referred to as the *management name* in documentation. You might want to rename a server with the DNS host name or track the host name by adding it to the server notes. Server and server group names must be unique and may include letters A through Z, digits 0 through 9, hyphens, and underscore characters.

▼ To Rename a Server or a Server Group

This procedure describes how to rename a server or a server group by using the browser interface. The example that follows the procedure provides a command-line equivalent.

- Steps**
1. **Log in to the N1 System Manager.**
See [“To Access the N1 System Manager Browser Interface” on page 26](#) for details.
 2. **Choose All Servers from the View Selector menu.**
The Servers table appears.
 3. **Select the server name that you want to change.**
The Server Details page appears.
 4. **Type the new name into the Name entry field.**
Server names must be unique and may include letters A through Z, digits 0 through 9, hyphens, and underscores.
The Save button on the right side of the page is enabled.
 5. **Click the Save button to apply the new name.**
The Servers table appears with the renamed server.

Example 4–6 Renaming a Server Through the Command Line

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

```
N1-ok> set server 192.168.12.1 name=svr4rck7
```

The server name is changed to `svr4rck7`. See “set server” in *Sun N1 System Manager 1.1 Command Line Reference Manual* for details.

Example 4–7 Renaming a Group Through the Command Line

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

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

The group name is changed to `labgroup`. See “set group” in *Sun N1 System Manager 1.1 Command Line Reference Manual* for details.

Adding a Server Note

Consider saving the following types of data as a server note:

- Physical location such as rack, slot, building, and geographic region

- DNS host name
- Provisioning parameters and the network configuration information that is set for the OS profile installation
- Internal asset tracking identifiers

To add server notes, use the `set` command with the `server` keyword and the `note` subcommand. For syntax and parameter details, type `help set server` at the `N1-ok` command line or refer to “set server” in *Sun N1 System Manager 1.1 Command Line Reference Manual*.

▼ To Add a Server Note

This procedure describes how to add a server note by using the browser interface. The example that follows the procedure provides a command-line equivalent.

- Steps**
1. **Log in to the N1 System Manager.**
See [“To Access the N1 System Manager Browser Interface”](#) on page 26 for details.
 2. **Choose All Servers from the View Selector menu.**
The Servers table appears.
 3. **Select the name of the server.**
The Server Details page appears.
 4. **Scroll down to the Notes entry field.**
The Notes entry field appears at the bottom of the General section.
 5. **Type new data into the Notes field.**
The Save button is enabled.
 6. **To apply your changes, click the Save button.**
The new data is saved.

Example 4–8 Adding a Server Note Through the Command Line

The following example shows how to view any existing notes by using the `show` command.

```
N1-ok> show server server1
```

The output shows any existing notes.

The following example shows how to add a server note by using the `set` command.

```
N1-ok> set server server1 note="loaded with S10"
```

The note is added to the server information. See “set server” in *Sun N1 System Manager 1.1 Command Line Reference Manual* for details.

Starting, Stopping, and Resetting Servers and Server Groups

This section describes the following activities:

- [“To Power On and Boot a Server or a Server Group” on page 122](#)
- [“To Shut Down and Power Off a Server or a Server Group” on page 124](#)
- [“To Reboot a Server or a Server Group” on page 126](#)

Starting Servers and Server Groups

Use the `start` command with the `server` or `group` keyword to power on a server or a server group. If boot PROMS are configured, the servers boot. You may also use the Actions menu on the Servers By Group page to initiate the start operation. The Actions menu is shown in the following graphic.

CONSOLE VERSION LOG OUT HELP

User: Admin (root) Server: proto183

Sun N1 System Manager

Jobs Running: 0
Last Update: Aug 1, 2005 8:13:07 AM MDT

Sun Microsystems, Inc.

View Selector

Servers By Group

mygroup
2 Servers

System Dashboard Jobs Event Log

Servers By Group

Server Groups (1)

New... — Actions —

Name	Servers	Hardware Faults	OS Resource Faults
mygroup	2	Unreachable	-

New... — Actions —

Type 'help' for a list of commands, use <Tab> for command completion.

N1-ok> start group mygroup

Shortcuts

OS Profiles

New... Edit List...

Updates

Edit List...

Firmware

— Actions —

— Actions —

Load OS Profile...

Load Update...

Load Firmware...

Add to a Group...

Remove from System

Power On (Start)

Power Off (Stop)

Reboot (Reset)

Enable Monitoring

Disable Monitoring

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

▼ To Power On and Boot a Server or a Server Group

Steps 1. Log in to the N1 System Manager.

See “To Access the N1 System Manager Command Line” on page 25 for details.

2. Type one of the following commands:

```
N1-ok> start server server
```

The server is powered on and, if boot PROMs are configured, the server boots. See “start server” in *Sun N1 System Manager 1.1 Command Line Reference Manual* for syntax details.

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

The server group is powered on and, if boot PROMs are configured, the servers in the group boot. Job completion takes longer for large server groups. See “start group” in *Sun N1 System Manager 1.1 Command Line Reference Manual* for syntax details.

Example 4–9 Starting a Server From the Network

The following command-line example shows how to boot a server from the network.

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

Example 4–10 Starting a Server Group from the Network

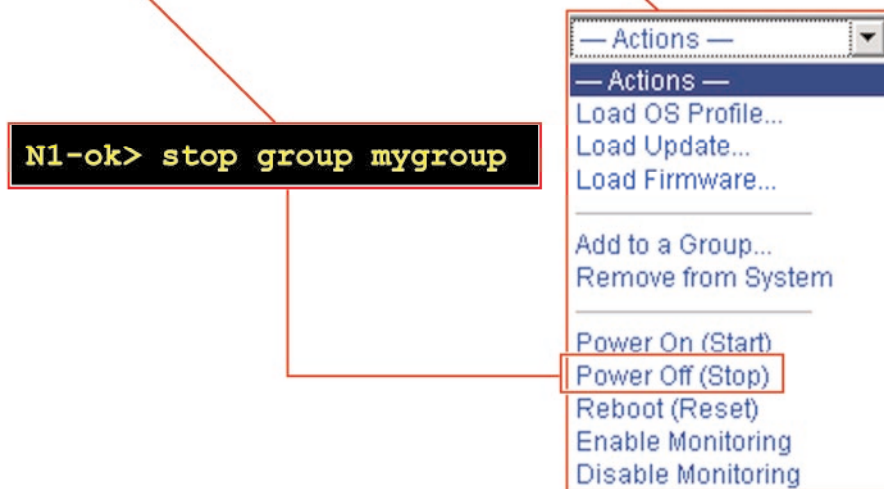
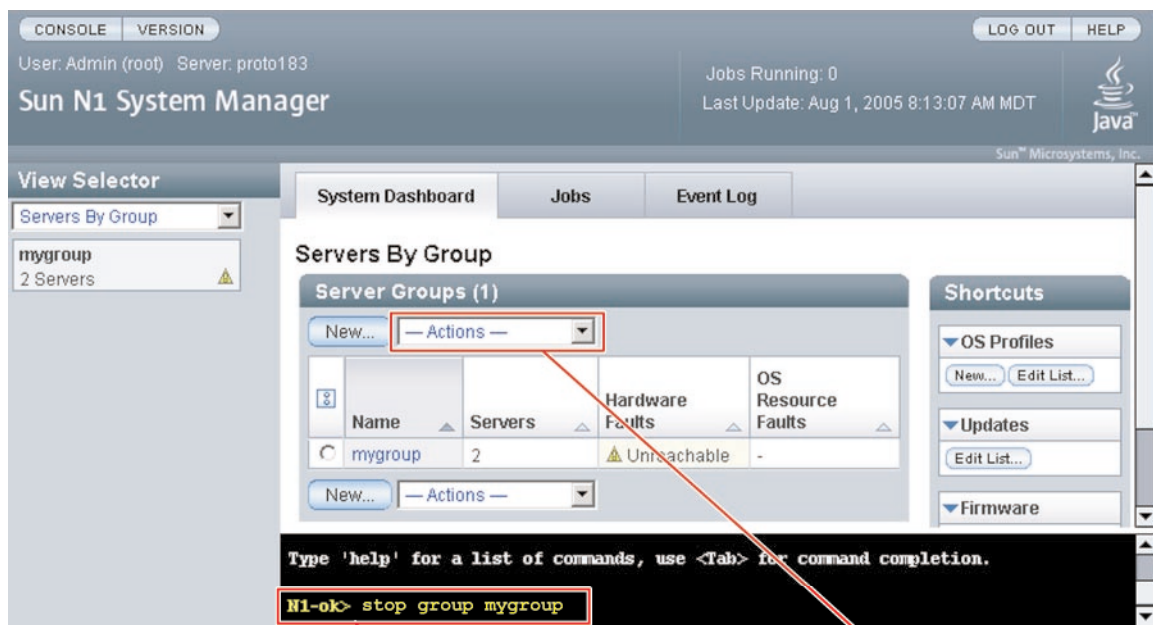
The following command-line example shows how to boot a server group from the network.

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

Stopping Servers and Server Groups

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

The following graphic shows how to stop a group by using the Actions menu on the Servers By Group page, or by issuing the `stop group` command.



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

▼ To Shut Down and Power Off a Server or a Server Group

- Steps**
1. **Log in to the N1 System Manager.**
See [“To Access the N1 System Manager Command Line”](#) on page 25 for details.
 2. **Type one of the following commands:**


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

The server is stopped. See “stop server” in *Sun N1 System Manager 1.1 Command Line Reference Manual* for syntax details.


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

The server group is stopped. See “stop group” in *Sun N1 System Manager 1.1 Command Line Reference Manual* for syntax details.

Example 4–11 Forcing Power Off of a Server

The following command-line example shows how to force shutdown of the OS.

```
N1-ok> stop server 10.0.7.2
Could not stop server "10.0.7.2".
N1-ok> stop server 10.0.7.2 force=true
Server 10.0.7.2 powered off.
```

Example 4–12 Forcing Power Off of a Server Group

The following command-line example shows how to force shutdown of the OS for a server group.

```
N1-ok> stop group dev
Could not stop group "dev".
N1-ok> stop group dev force=true
Group dev powered off.
```

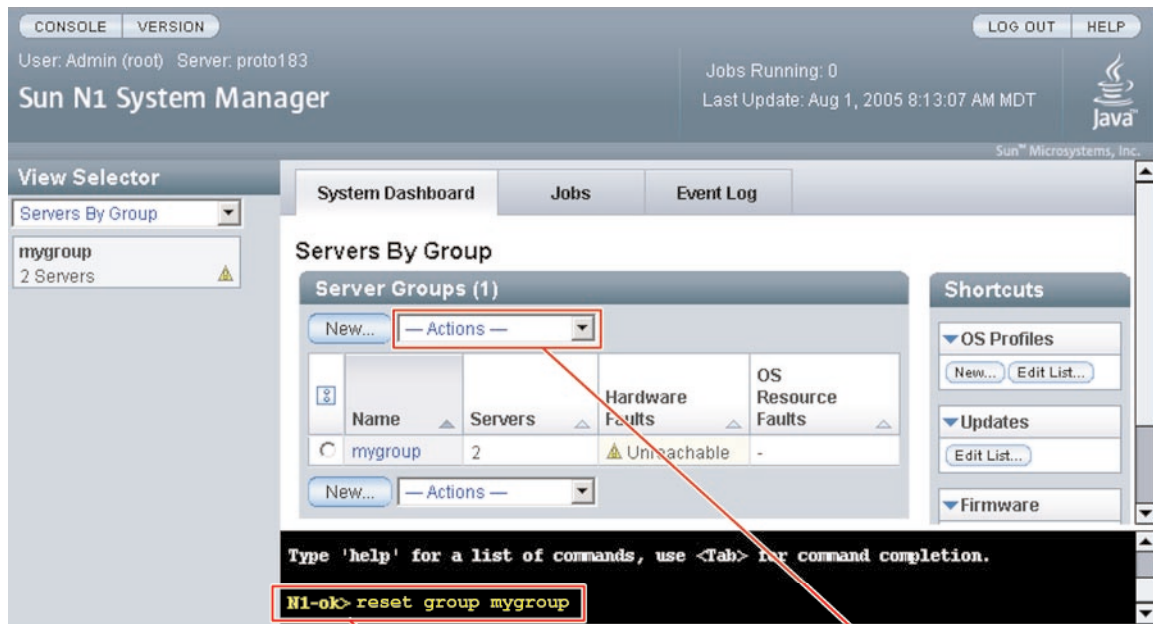
Troubleshooting If you use the `force` option, run one of the following file system check commands on the service processor when the server reboots.

- Run `fsck` for UNIX®
- Run `reiserfsck` or `e2fsck` for Linux

To find out how to run the `fsck` command on a provisioned server, see [“Issuing Remote Commands on Servers and Server Groups”](#) on page 127.

Resetting Servers and Server Groups

To initiate graceful shutdown of the operating system followed by power off of the physical server or server group, use the `reset` command with the `server` or `group` keyword. Then, the servers are powered on and, if boot PROMs are configured, the servers reboot. If servers do not have an OS installed or do not shutdown, you can use the `force` subcommand to reboot the server or server group.



N1-ok> reset group mygroup

- Actions —
- Actions —
- Load OS Profile...
- Load Update...
- Load Firmware...
- Add to a Group...
- Remove from System
- Power On (Start)
- Power Off (Stop)
- Reboot (Reset)**
- Enable Monitoring
- Disable Monitoring

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

▼ To Reboot a Server or a Server Group

- Steps**
1. **Log in to the N1 System Manager.**
See [“To Access the N1 System Manager Command Line”](#) on page 25 for details.
 2. **Type one of the following commands:**

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

The server is rebooted. See “reset server” in *Sun N1 System Manager 1.1 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 1.1 Command Line Reference Manual* for details.

Example 4-13 Forcing Reset of a Server

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

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

Example 4-14 Forcing Reset of a Server Group

If the OS does not gracefully shut down, use the following command-line example to force reset of the operating systems for the servers in the group.

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

Example 4-15 Rebooting a Server From the Network

The following command-line example shows how to reboot a server from the network.

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

Example 4-16 Rebooting a Server Group from the Network

The following command-line example shows how to reboot a server group from the network.

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

Troubleshooting If you use one of the above `force` commands, run one of the following file system check commands on the service processor when the server reboots.

- Run `fsck` for UNIX®
- Run `reiserfsck` or `e2fsck` for Linux

To find out how to run the `fsck` command on provisioned servers, see [“Issuing Remote Commands on Servers and Server Groups”](#) on page 127 for instructions.

Issuing Remote Commands on Servers and Server Groups

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

To issue a remote command on a server or server group, use the `start` command with the `server` or `group` keyword and the command subcommand. For syntax and parameter details, type `help start server` or `help start group` at the `N1-ok` command line.

▼ To Issue Remote Commands on a Server or a Server Group

This procedure describes how to issue a remote command. A *remote command* is a UNIX® command that is sent to a provisioned server to be run on that provisioned server.

Before You Begin You must add the OS monitoring feature before you can issue remote commands on servers or server groups. See [“To Add the OS Monitoring Feature”](#) on page 85.

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

See [“To Access the N1 System Manager Command Line”](#) on page 25 for details.

2. **Type one of the following commands:**

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

The remote command is issued on the server. See “start server” in *Sun N1 System Manager 1.1 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 1.1 Command Line Reference Manual* for details.

3. **View the Remote Command job.**

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

The Remote Command output appears in the Results section.

Example 4–17 Issuing a Remote Command on a Server

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

```
N1-ok> start server hdco25 command "/bin/ls -l /"
```

```
Job "23" started.
```

The following command-line example shows how 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
Owner:     root
Errors:    0
Warnings:  0
```

```
Step 1:
Type:      103
Description: native procedure /bin/sh /opt/sun/nlgc/bin/remotecmd.sh
: [RCMD_KEY]
Start:      2005-02-15T08:31:22-0700
Completion: 2005-02-15T08:31:26-0700
Result:     Complete
Exception:  No Data Available
```

```
.
.
.
```

```
Result :
Server:      hdco25
Status:      0
Message:     Command executed successfully. Command: /bin/ls -l /
Standard Output: total 321
lrwxrwxrwx   1 root    root          9 Feb 11 13:21 bin -> ./usr/bin
drwxr-xr-x   4 root    sys          512 Feb 11 13:25 boot
drwxr-xr-x   3 root    sys          512 Feb 11 14:27 cr
drwxr-xr-x  15 root    sys         4096 Feb 11 14:09 dev
drwxr-xr-x   5 root    sys          512 Feb 11 14:06 devices
drwxr-xr-x  58 root    root         4096 Feb 14 12:36 etc
drwxr-xr-x   2 root    sys          512 Feb 11 13:46 export
dr-xr-xr-x   1 root    root          1 Feb 11 14:11 home
drwxr-xr-x  12 root    sys          512 Feb 11 13:25 kernel
lrwxrwxrwx   1 root    root          9 Feb 11 13:21 lib -> ./usr/lib
```


Example 4-18 Issuing a Remote Command With a Timeout

Timeouts are measured in seconds. The default timeout is two hours. If you want to turn the timeout off, type a value of zero into the command. The following example shows how to issue a remote command with a timeout that is set to 20 seconds.

```
N1-ok> start server hdco25 command "/root/sleep.sh 60" timeout 20
```

```
Job "10" started.
```

The following command-line example shows how 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
Owner:     root
Errors:    0
Warnings:  0
```

```
Step 1:
```

```
Type:      103
Description: native procedure /bin/sh /opt/sun/nlgc/bin/remotecmd.sh
: [RCMD_KEY]
Start:      2005-02-15T16:46:48-0700
Completion: 2005-02-15T16:47:10-0700
Result:     Complete
Exception:  No Data Available
```

```
.
.
.
```

```
Result :
```

```
Server:      hdco25
Status:      -2
Message:      Command running on hdco25 did not finish within the
specified time limit of 20 seconds. Command: /root/sleep.sh 60
Standard Output: Sleeping for 60 seconds...
```

Example 4-19 Issuing a Remote Command on a Server Group

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

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

```
Job "24" started.
```

The following command-line example shows how view the results of the remote command by using the show command.

N1-ok> **show job 24**

Job ID: 24
Date: 2005-02-15T08:31:20-0700
Type: Remote Command
Status: Completed
Owner: root
Errors: 0
Warnings: 0

Step 1:
Type: 103
Description: native procedure /bin/sh /opt/sun/nlgc/bin/remotecmd.sh
: [RCMD_KEY]
Start: 2005-02-15T08:31:22-0700
Completion: 2005-02-15T08:31:26-0700
Result: Complete
Exception: No Data Available

.
.
.

Result :
Server: server1
Status: 0
Message: Command executed successfully. Command: /bin/ls -l /
Standard Output: total 321
lrwxrwxrwx 1 root root 9 Feb 11 13:21 bin -> ./usr/bin
drwxr-xr-x 4 root sys 512 Feb 11 13:25 boot
drwxr-xr-x 3 root sys 512 Feb 11 14:27 cr
drwxr-xr-x 15 root sys 4096 Feb 11 14:09 dev
drwxr-xr-x 5 root sys 512 Feb 11 14:06 devices
drwxr-xr-x 58 root root 4096 Feb 14 12:36 etc
drwxr-xr-x 2 root sys 512 Feb 11 13:46 export
dr-xr-xr-x 1 root root 1 Feb 11 14:11 home
drwxr-xr-x 12 root sys 512 Feb 11 13:25 kernel
lrwxrwxrwx 1 root root 9 Feb 11 13:21 lib -> ./usr/lib
Server: server2
Status: 0
Message: Command executed successfully. Command: /bin/ls -l /
Standard Output: total 321
lrwxrwxrwx 1 root root 9 Feb 11 13:21 bin -> ./usr/bin
drwxr-xr-x 4 root sys 512 Feb 11 13:25 boot
drwxr-xr-x 3 root sys 512 Feb 11 14:27 cr
drwxr-xr-x 15 root sys 4096 Feb 11 14:09 dev
drwxr-xr-x 5 root sys 512 Feb 11 14:06 devices
drwxr-xr-x 58 root root 4096 Feb 14 12:36 etc
drwxr-xr-x 2 root sys 512 Feb 11 13:46 export
dr-xr-xr-x 1 root root 1 Feb 11 14:11 home
drwxr-xr-x 12 root sys 512 Feb 11 13:25 kernel
lrwxrwxrwx 1 root root 9 Feb 11 13:21 lib -> ./usr/lib

See Also [Example 5-12](#)

Connecting to the Serial Console for a Server

This section describes how to open the serial console for a server.

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

Note – The Command Line pane in the browser interface does not support this operation. You must use `n1sh` shell to access the `connect` command.

You can also perform this operation from the browser interface's Server Details page.

▼ To Open a Server's Serial Console

This procedure describes how to remotely access the serial console of provisionable servers. This feature is particularly useful for performing diagnosis before and during the OS installation and during the server power cycle.



Caution – The terminal emulator applet that is used by the browser interface for the serial console feature does not provide a certificate-based authentication of the applet. The applet also requires that you enable SSHv1 for the management server. For certificate-based authentication or to avoid enabling SSHv1, use the serial console feature by running the `connect` command from the `n1sh` shell.

For most hardware platforms, the first user to log in is given read-and-write privileges on the serial console. Subsequent user sessions are in read-only mode. Sun Fire X4100 and X4200 servers do not support read-only mode, so subsequent user session requests fail.

When the escape sequence is issued, the connection closes and a `disconnect from server-name` message appears in the output. If another user has the console and you are in read-only mode, you are logged in to the console when the other user disconnects. When you click the Close button on the Serial Console window, the connection is closed.

The following list shows the supported serial console escape sequences:

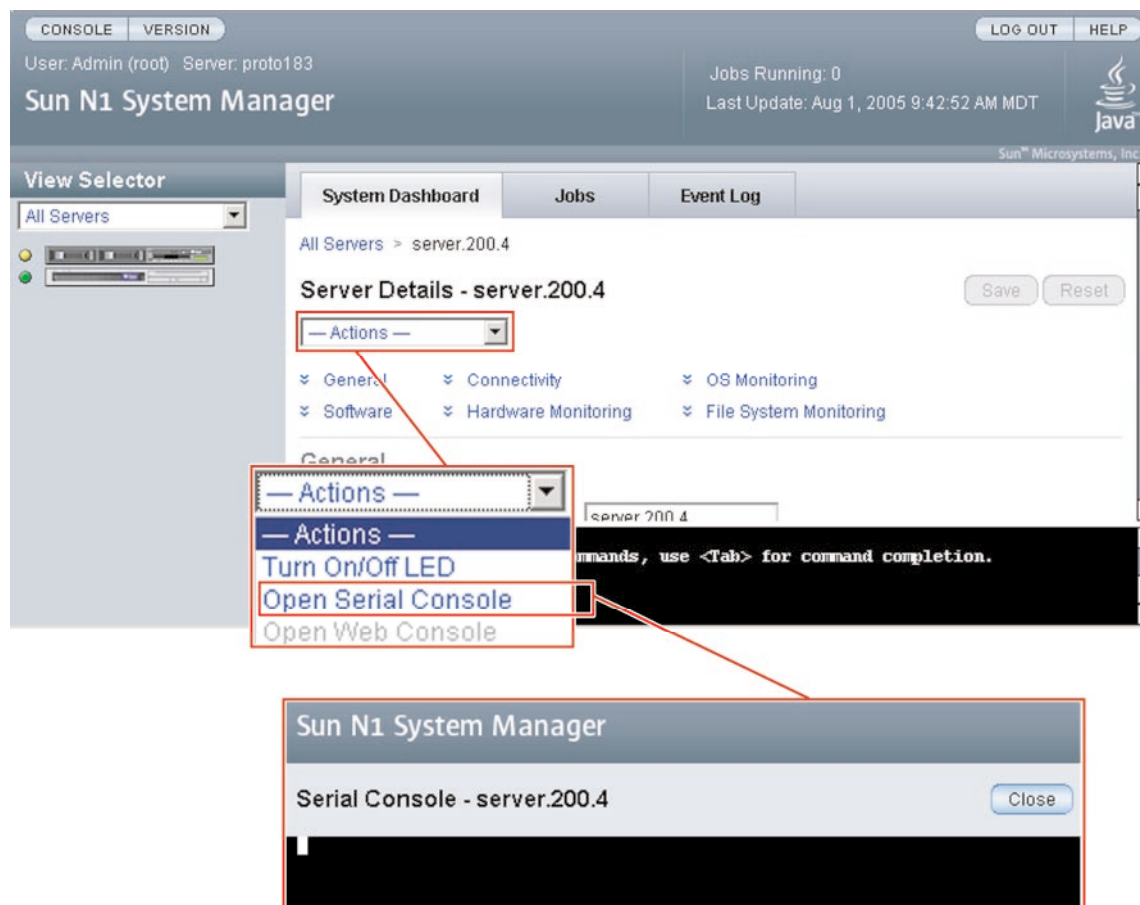
- `ALOM – #.`

- Sun Enterprise X4100, X4200 – ESC (
- Sun Fire V20z and V40z – ^Ec .

For HTTP connections, standard 128-bit SSL encryption is used for transport, authentication is password based, and a security session is used for each subsequent operation.

Note – If another user is logged in to the serial console for the server, you are logged in with read-only privileges. If another user has logged in to the physical serial console on a SPARC server, you are logged in with read-only privileges. The *physical* serial console is separate from the one that is available from the ALOM port.

- Steps**
1. **Choose All Servers from the View Selector menu.**
The Servers table appears.
 2. **Select the server for which you want to open a serial console.**
The Server Details page appears.
 3. **Choose Open Serial Console from the Actions menu.**



The management server redirects output of the provisionable server's serial console to the terminal emulator applet that is running in the browser interface. The serial emulator appears and takes you either to the root prompt or a read-only prompt.

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

Example 4-20 Connecting to the Serial Console Through the Command Line

When in serial console mode, the `n1sh` shell sends all user input to the remote serial console. The N1 System Manager neither blocks nor supplements the platform-specific exit-control sequence. Note that the `connect` command is not implemented in the browser interface's Command Line pane. The `connect` command may only be run from the `n1sh` shell.

This example shows how to connect to the serial console as a root user. However, any user role with the `ServerConsole` privilege may issue the `connect` command.

```
% ssh -l root server1.central:6789
password:
```

```
Copyright (c) 2005 Sun Microsystems, Inc. All rights reserved
Use is subject to license terms.
```

```
N1-ok> connect server server1
```

Troubleshooting If the Open Serial Console menu item does not appear, SSHv1 is not enabled. To enable SSHv1, use the `n1smconfig` utility. See “To Configure the Sun N1 System Manager System” in *Sun N1 System Manager 1.1 Installation and Configuration Guide*.

See Also After you have opened the serial console, you can view the detailed output during an OS deployment or a power cycle. For instructions, see [“Deploying OS Profiles” on page 79](#) and [“To Reboot a Server or a Server Group” on page 126](#).

Refreshing and Finding Servers and Server Groups

This section describes the following tasks:

- [“To Refresh Data for a Server or a Server Group” on page 135](#)
- [“To Find a Server in a Rack” on page 135](#)

Refreshing Server and Server Group Data

To update server and server group data, use the `set` command with the `server` or `group` keyword and the `refresh` subcommand. This command updates the following data:

- Hardware health information including power status, memory, processor information and NIC information

- Firmware information
- OS resource usage, such as CPU and filesystem usage, if an OS is loaded
- OS update information if an OS update is loaded

▼ To Refresh Data for a Server or a Server Group

- Steps**
1. **Log in to the N1 System Manager.**
See [“To Access the N1 System Manager Command Line”](#) on page 25 for details.

2. **Type one of the following commands:**

N1-ok> **set server** *server* **refresh**

The server data is updated. See “set server” in *Sun N1 System Manager 1.1 Command Line Reference Manual* for details.

N1-ok> **set group** *group* **refresh**

The server group data is updated. See “set group” in *Sun N1 System Manager 1.1 Command Line Reference Manual* for details.

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

Finding a Server in a Rack

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

▼ To Find a Server in a Rack

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

- Steps**
1. **Log in to the N1 System Manager.**
See [“To Access the N1 System Manager Command Line”](#) on page 25 for details.

2. **Type the following command:**

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

The LED locator light on the physical server illuminates. See “set server” in *Sun N1 System Manager 1.1 Command Line Reference Manual* for details.

Deleting Servers and Server Groups

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

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

▼ To Delete a Server or a Server Group

Steps 1. Log in to the N1 System Manager.

See [“To Access the N1 System Manager Command Line”](#) on page 25 for details.

2. Type one of the following commands:

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

The server is deleted from the N1 System Manager. See “delete server” in *Sun N1 System Manager 1.1 Command Line Reference Manual* for details.

```
N1-ok> delete group group
```

The group is deleted from the N1 System Manager. This command will **not** remove servers from the N1 System Manager. See “delete group” in *Sun N1 System Manager 1.1 Command Line Reference Manual* for details.

Monitoring Your Servers

The first section of this chapter provides an explanation of what monitoring is, in the context of the N1 System Manager, and describes how to monitor servers that are part of the N1 System Manager. This chapter provides procedures for enabling and disabling monitoring, and for managing monitoring thresholds and polling intervals, 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:

- [“Introduction to Monitoring” on page 138](#)
- [“Enabling Monitoring” on page 142](#)
- [“Monitoring Threshold Values” on page 147](#)
- [“Setting Polling Intervals” on page 158](#)
- [“Monitoring MIBs” on page 163](#)
- [“Managing Jobs” on page 163](#)
- [“Managing Event Log Entries” on page 172](#)
- [“Setting Up Notifications” on page 175](#)

Some procedures are also possible using the browser interface. These procedures are provided in the Sun N1 System Manager browser interface help.

This chapter contains descriptions of the following tasks:

- [“To Monitor a Server” on page 144](#)
- [“To Monitor a Server Group” on page 145](#)
- [“To Disable Monitoring for a Server” on page 145](#)
- [“To Disable Monitoring for a Server Group” on page 146](#)
- [“To Retrieve Threshold Values for a Server” on page 148](#)
- [“To Modify Default Threshold Values for a Server” on page 151](#)
- [“To Set Threshold Values for a Server” on page 156](#)
- [“To Set Threshold Values for a Server Group” on page 157](#)
- [“To Retrieve Polling Interval Values for a Server” on page 160](#)
- [“To Modify the Default Polling Interval for a Server” on page 160](#)

- [“To Set Polling Intervals for a Server” on page 161](#)
- [“To Set Polling Intervals for a Server Group” on page 162](#)
- [“To List Jobs” on page 165](#)
- [“To View a Specific Job” on page 166](#)
- [“To Stop a Job” on page 167](#)
- [“To Delete a Job” on page 169](#)
- [Example 5–14](#)
- [“To View the Event Log” on page 173](#)
- [“To Filter the Event Log” on page 174](#)
- [“To View Event Details” on page 174](#)
- [“To View Notifications” on page 176](#)
- [“To View Notification Details” on page 176](#)
- [“To Modify a Notification” on page 176](#)
- [“To Create and Test a Notification” on page 177](#)
- [“To Delete a Notification” on page 178](#)
- [“To Start a Notification” on page 179](#)
- [“To Stop a Notification” on page 179](#)

Introduction to Monitoring

Monitoring in the Sun N1 System Manager software enables you to track changes to specific *attributes* in specific managed objects. Managed objects include server hardware elements, operating systems, file systems, and networks. Attributes are the monitored elements, about which data is obtained and delivered by the N1 System Manager software. Examples of attributes are the average number of queued processes and the percentage of used memory. A list of attributes is provided in [“Hardware Sensor Attributes” on page 152](#) and in [Table 5–2](#).

Attributes are associated with one of three main areas:

- **Hardware health attributes.** For information about hardware health monitoring, see [“Hardware Health Monitoring” on page 139](#).
- **OS resource utilization attributes.** For information about OS resource utilization monitoring, see [“OS Resource Utilization Monitoring” on page 140](#).
- **Network connectivity, or *reachability*.** For information about network reachability monitoring, see [“Network Reachability Monitoring” on page 141](#).

For a server or a group of servers, hardware health and operating system utilization and network connectivity are all monitored by the management server. All comparisons and verifications for monitoring are performed by the N1 System Manager. Provisionable servers are used only to access data.

An SNMP agent that is used for data retrieval is provided in the N1 System Manager software. If the management server is running the N1 System Manager on the Solaris OS, this agent is based on the Sun Management Center 3.5 software SNMP agent. If

the management server is running the N1 System Manager on Linux, this agent is based on the Sun Management Center 3.6 Linux SNMP agent. The agent is deployed when operating systems are deployed on servers that are managed by the N1 System Manager software.

Note – On Linux platforms, the N1 System Manager software only monitors `ext3` file systems. Other types of file systems are not monitored for Linux platforms.

Monitoring is connected with the broadcasting of the *events* for each monitored server or group of servers. Events are generated when certain conditions related to attributes occur. For information about events and when they occur, see [“Managing Event Log Entries” on page 172](#). There are no log files related to monitoring. Instead of log files, monitoring data is stored as events in the N1 System Manager database.

If monitoring is enabled for a server, each event causes a notification to be emitted from the N1 System Manager for that event. If monitoring is disabled for a server, monitoring events are not generated for that server. Lifecycle events continue to be generated, even with monitoring disabled. *Lifecycle events* include server discovery, server change or deletion, or server group creation. If you have requested notification of this type of event, you can still receive notifications even with monitoring disabled.

Hardware Health Monitoring

The hardware health of discovered servers is monitored. Sensors provided in the hardware are used to monitor temperature, voltage, and fan speed. For more information about associated hardware, see the “Sun N1 System Manager Connection Information” in *Sun N1 System Manager 1.1 Site Preparation Guide*.

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

General management interface data for Sun Fire V20z and Sun Fire V40z machines is obtained through the command line. General management interface data for Sun Fire x4100 and Sun Fire x4200 servers is obtained through IPMI. Data can be retrieved dynamically from the command line.

The following characteristics of server hardware can be monitored:

- CPU temperature
- Ambient temperature
- Fan speed in revolutions per minute
- Voltages
- LEDs

A detailed list of these sensors is provided in [“Hardware Sensor Attributes” on page 152](#).

You can view filtered hardware health monitoring information for all servers by using the `show server` command:

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

See “show server” in *Sun N1 System Manager 1.1 Command Line Reference Manual* for details of possible values of the *health* filters.

OS Resource Utilization Monitoring

OS resource utilization is monitored by the N1 System Manager. As part of the `add server feature` command, with the `agentip` keyword, you provide credentials to access the monitored server’s operating system through `ssh` with the `agentssh` keyword. See [“To Add the OS Monitoring Feature” on page 85](#) for additional details. This procedure is important for OS resource utilization monitoring but not for monitoring hardware health or network reachability.

Access to the operating system by this mechanism is required primarily for the Remote Command Execution feature. Access to the operating system by this mechanism is how the management features are used to retrieve data for OS resource utilization monitoring. Platform OS interface data is obtained through `ssh` and `SNMP`; all attribute data is retrieved from the server’s operating system by using `ssh` and `SNMP`. Statistics related to the central processor unit (CPU) are provided, as is data related to memory, swap usage, and file systems. For the purposes of monitoring, system load data, memory usage, and swap usage data can be broken down as follows:

- System usage, including system idle times
- System load, expressed as the average number of queued processes over 1, 5, and 15 minutes
- Memory usage and memory free statistics, in megabytes and as percentages
- Physical load statistics
- Swap space used and space available, in megabytes and as percentages
- File system used and space available, as percentages

A list of these attributes is provided in [“Hardware Sensor Attributes” on page 152](#).

You can filter OS resource utilization monitoring information for all servers by using the `show server` command:

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

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

The health of an OS resource can be shown as `unknown` if the server is reachable but the monitoring agent 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 “show server” in *Sun N1 System Manager 1.1 Command Line Reference Manual* for details.

The monitoring of OS resource utilization attributes enables you to modify the default threshold values for all servers being managed by the N1 System Manager, through the creation and editing of a configuration file. See [“Changing Threshold Values With the Monitoring Configuration File” on page 150](#) for details.

The monitoring of OS resource utilization attributes also enables 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 156](#) for details.

If you are not interested in the values of some attributes, you can disable the threshold severity for monitoring of those attributes. This action prevents annoyance alarms. [Example 5–4](#) shows you how to accomplish this disabling action.

Network Reachability Monitoring

All management interfaces of provisionable servers and all platform interfaces are monitored by default by the N1 System Manager. Platform interfaces include the service processor’s management interface, such as `eth0`, and data network interfaces, such as `eth1` or `eth2`.

Reachability is verified for Linux servers and servers running the Solaris OS by using an ICMP ping to the interface IP address. For further information, see “Discovery of Servers in the Factory Default State” in *Sun N1 System Manager 1.1 Installation and Configuration Guide*.

The reachability of all network interfaces is verified at regular intervals. These polling intervals are configurable. For information about configuring polling intervals, see [“Setting Polling Intervals” on page 158](#). 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 1.1 Command Line Reference Manual* for details.

It is important to distinguish between the unreachable and unknown states for provisionable servers.

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

This command lists all provisionable servers that are unreachable. Any provisionable server returned in the output of this command is unreachable due to a network problem: the server cannot be contacted about its hardware health status. The ping command to the server is unsuccessful. This 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 health unknown
```

This command lists all provisionable servers that are not returning any information about hardware health status. The `ping` command may be successful but servers returned in the output of this command are not returning any hardware health information. The monitoring agent could not be contacted on port 161.

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

This command lists all provisionable servers that are unreachable. Any server returned in the output of this command is unreachable due to a network problem: the server cannot be contacted about its power status. The `ping` command to the server is unsuccessful. This does not necessarily mean that the server is not transmitting power status information. The server could be in standby mode.

```
N1-ok> show server power unknown
```

This command lists all provisionable servers that are not returning any information about power status. The `ping` command may be successful but servers returned in the output of this command are not returning any power status information. The monitoring agent could not be contacted on port 161.

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

This command lists all provisionable servers that are unreachable. Any server returned in the output of this command is unreachable due to a network problem: the server cannot be contacted about its OS resource utilization. The `ping` command to the server is unsuccessful. This does not necessarily mean that the server is not transmitting OS resource utilization information. The server could be in standby mode.

```
N1-ok> show server utilization unknown
```

This command lists all provisionable servers that are not returning any information about OS resource utilization. The `ping` command may be successful but servers returned in the output of this command are not returning any OS resource utilization information. The monitoring agent could not be contacted on port 161.

Enabling Monitoring

For all provisionable servers, that is to say for all physical servers that have been discovered by the Sun N1 System Manager software, management features are supported when the `add server` command is used to create monitorable objects. The management features are used to periodically retrieve CPU statistics, filesystem, and memory data, for monitoring purposes.

Monitored file system data for a provisionable server is not available unless an operating system is deployed on the provisionable server, and the management features have been added by using the `add server` feature command with the `agentip` keyword:

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

The `agentip` is the IP address of the provisioning network interface of the provisionable server that you want to monitor. See “add server” in *Sun N1 System Manager 1.1 Command Line Reference Manual* for details. See also “[To Add the Base Management Feature](#)” on page 84 and “[To Add the OS Monitoring Feature](#)” on page 85 for additional details on the syntax used in these commands.

When you specify or change features, you must use the `add server` command. The `set server` command cannot be used to specify a feature.

The `add server` command is useful for enabling OS resource utilization monitoring and network reachability monitoring, but not for monitoring hardware health. Hardware health is already monitored by default as soon as the Sun N1 System Manager software discovers a physical server.

Note – The polling of network reachability is not possible if OS resource utilization monitoring is not enabled.

For more information about the `agentip` subcommand, see “[To Add the OS Monitoring Feature](#)” on page 85.

The `add server` command needs to be issued only once for a server and not each time you want to enable or disable monitoring.

Note – If the provisionable server’s IP address changes, use the `set server` command again before enabling or disabling monitoring.

The default status of monitoring in the Sun N1 System Manager for discovered servers and initialized operating systems is as follows:

Default status of hardware monitoring

When a server or other hardware is discovered, monitoring of the server or other hardware is enabled by default. Before a server can be monitored, however, it must be discovered and correctly registered with the N1 System Manager. This process is described in “[Discovering Servers](#)” on page 47. The monitoring of hardware sensors is enabled by default for all managed servers. If a server is deleted and then rediscovered, all states related to that server for the purposes of monitoring are lost. This is the case regardless of whether monitoring was enabled or disabled for that

server when the server was deleted. When the server is rediscovered, monitoring is set to `true` by default. For more information about discovering servers, see [“To Discover New Servers” on page 49](#).

Default status of OS resource utilization monitoring

Disabled by default. When an OS has been successfully provisioned on a provisionable server and the N1 System Manager management features are supported by using the `add server feature` command with the `agentip` specified, OS resource utilization 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 resource utilization attributes, you can disable the threshold severity for the monitoring of those attributes, while continuing to monitor other OS resource utilization attributes. This action prevents annoyance alarms. [Example 5-4](#) shows how to accomplish this task. For general information about threshold values, see [“Monitoring Threshold Values” on page 147](#).

Default status of network reachability monitoring

When the management interface of the provisionable server is discovered, monitoring of the interface is enabled by default. When the management features are added, monitoring of other interfaces is enabled by default.

▼ To Monitor a Server

The following procedure describes how to use the command line to enable the monitoring of hardware health, operating system utilization, and network reachability of 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 Base and OS Management Features” on page 84](#).

Steps 1. Log in to the N1 System Manager.

See [“To Access the N1 System Manager Command Line” on page 25](#) for details.

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

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

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

3. View the server details.

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


▼ To Monitor a Server Group

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 Base and OS Management Features” on page 84](#). This procedure is important for OS resource utilization monitoring but not for monitoring hardware health.

Steps

1. Log in to the N1 System Manager.

See [“To Access the N1 System Manager Command Line” on page 25](#) for details.

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

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

This command is executed for the group of servers that you have already named. See “set group” in *Sun N1 System Manager 1.1 Command Line Reference Manual* for details. In this procedure, *group* is the name of the group of provisionable servers that you want to monitor.

3. View the server group details to determine if monitoring is enabled for each server in the group.

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

4. View the specific monitoring details for individual servers in the group.

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

Detailed monitoring information appears in the output. Information is displayed about polling intervals and threshold values for the monitoring of hardware health, OS resource utilization and network reachability. Polling intervals are explained in [“Setting Polling Intervals” on page 158](#). Monitoring threshold values are explained in [“Monitoring Threshold Values” on page 147](#).

▼ To Disable Monitoring for a Server

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

Steps

1. Log in to the N1 System Manager.

See [“To Access the N1 System Manager Command Line” on page 25](#) for details.

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

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

In this example, *server* is the name of the provisionable server that you want to stop monitoring. Executing this command disables monitoring of the server. With monitoring of a server disabled, the violation of threshold values by attributes

related to that server does not generate events.

3. View the server details.

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

The output shows that monitoring is disabled.

If you are not interested in the values of some OS resource utilization attributes, you can disable the threshold severity for the monitoring of those attributes, while continuing to monitor other OS resource utilization attributes. This action prevents annoyance alarms. [Example 5-4](#) shows how to accomplish this task. For general information about threshold values, see “[Monitoring Threshold Values](#)” on page 147. You can also completely remove the OS resource utilization monitoring feature. See “[To Remove the OS Monitoring Feature](#)” on page 87.

▼ To Disable Monitoring for a Server Group

This procedure describes how to disable monitoring for a server group. You might want to disable monitoring of hardware components to perform maintenance tasks without generating events.

Note – When you disable monitoring for a server, hardware health monitoring, OS monitoring, and network reachability monitoring are all disabled for that server.

Steps 1. Log in to the N1 System Manager.

See “[To Access the N1 System Manager Command Line](#)” on page 25 for details.

2. Set the monitored attribute to false by using the set group command.

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

This command is executed for the group of servers that you have already named. See “set group” in *Sun N1 System Manager 1.1 Command Line Reference Manual* for details. In this procedure, *group* is the name of the group of provisionable servers that you want to stop monitoring. Executing this command disables monitoring for all servers in the group. With monitoring of a server group disabled, the violation of threshold values by attributes related to servers in that group does not generate events.

3. View the server group details to determine if monitoring is disabled for all servers in the group.

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

Monitoring Threshold Values

The value of any given monitored 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. These polling intervals are configurable. For further information about polling intervals, see [“Setting Polling Intervals” on page 158](#).

When a monitored attribute is polled and the value of the attribute 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 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 monitoring agent cannot be contacted on SNMP port 161.

The values `nonrecoverable`, `critical`, and `warning` are discussed in “show server” in *Sun N1 System Manager 1.1 Command Line Reference Manual*.

What Happens When a Threshold is Broken

If the value of a 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 `criticalhigh` 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 `warninghigh` 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 `warninglow` is issued. If the value continues to fall, and passes the `criticallow` threshold, a status of `criticallow` is issued. If the value continues to fall below the `nonrecoverablelow` threshold, a status of `nonrecoverablelow` is issued.

If the value then rises back to the safe range, no further events are generated until the value rises above the `warninglow` threshold, at which point an event is generated to show a status of `normal`.

Threshold values for OS resource utilization attributes can be configured at the command line. This process is explained in [“Setting Threshold Values” on page 156](#). For threshold values measuring percentages, the valid range is from 0 to 100%. If you try to set a threshold value outside of this range, an error is generated. For attributes that do not measure percentages, these values depend on the number of processors in your system and on the usage characteristics of your installation.

Tuning Threshold Values for Your Installation

After a period of usage, you can develop an awareness of what levels to set for OS resource utilization 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 a notification to be sent to your pager or email address. For example, you might want to receive notifications every time a certain attribute reaches a warninghigh severity threshold level.

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 Base and OS Management Features” on page 84](#).

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

See [“To Access the N1 System Manager Command Line” on page 25](#) for details.

2. **Type the `show server` command:**

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

In this procedure, *server* is the name of the provisionable server for which you want to retrieve threshold values.

Detailed monitoring threshold values appear in the output, including threshold information for the server’s hardware health, OS resource utilization, and network reachability. Default values are shown if no specific values have been set.

See “show server” in *Sun N1 System Manager 1.1 Command Line Reference Manual* for details.

Managing Default Threshold Values

Factory-configured default threshold values are provided in the N1 System Manager software for some OS resource utilization thresholds. These values are stated as percentages. [Table 5–1](#) lists default values for these OS resource utilization attributes.

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

TABLE 5-1 Factory-Configured Default Threshold Values for OS Resource Utilization Attributes

Attribute Name	Description	Default Threshold	Default Threshold
cpustats.pctusage	Percentage of overall CPU usage	warninghigh 80%	criticalhigh 90%
cpustats.pctidle	Percentage of CPU idle	warninglow 20%	criticalallow 10%
memusage.pctmemused	Percentage of memory in use	warninghigh 80%	criticalhigh 90%
memusage.pctmemfree	Percentage of memory free	warninglow 20%	criticalallow 10%
memusage.pctswapped	Percentage of swap space in use	warninghigh 80%	criticalhigh 90%
fsusage.pctused	Percentage of file system space in use	warninghigh 80%	criticalhigh 90%

Table 5-2 provides the complete list of OS resource utilization attributes and their default values. Where factory-configured default values exist for attributes, these are shown in parentheses.

TABLE 5-2 All OS Resource Utilization Attributes

Attribute Name	Description	Supported Threshold (Default)	Supported Threshold (Default)
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

TABLE 5–2 All OS Resource Utilization Attributes *(Continued)*

Attribute Name	Description	Supported Threshold (Default)	Supported Threshold (Default)
<code>cpustats.pctusage</code>	Percentage of overall CPU usage	warninghigh (80%)	criticalhigh (90%)
<code>cpustats.pctidle</code>	Percentage of CPU idle	warninglow (20%)	criticallow (10%)
<code>memusage.pctmemused</code>	Percentage of memory in use	warninghigh (80%)	criticalhigh (90%)
<code>memusage.pctmemfree</code>	Percentage of memory free	warninglow (20%)	criticallow (10%)
<code>memusage.mbmempused</code>	Memory in use in MB	warninghigh	criticalhigh
<code>memusage.mbmempfree</code>	Memory free in MB	warninglow	criticallow
<code>memusage.pctswapused</code>	Percentage of swap space in use	warninghigh (80%)	criticalhigh (90%)
<code>memusage.mbswapfree</code>	Free swap space in MB	warninglow	criticallow
<code>fsusage.pctused</code>	Percentage of file system space in use	warninghigh (80%)	criticalhigh (90%)

Changing Threshold Values With the Monitoring Configuration File

You can modify default values for thresholds by editing the `monitoring.properties` configuration file.

If the `monitoring.properties` configuration file is not present, create and save it in `/etc/opt/sun/nlgc/`. The `monitoring.properties` configuration file is not created by default at installation.

Any entries that you make in the `monitoring.properties` configuration file for the threshold values of the attributes listed in [Table 5–1](#) overwrite the factory-configured defaults for the corresponding threshold values.

The `monitoring.properties` configuration file should be stored only on the management server and not on provisionable servers.

Modifying or adding new entries to the `monitoring.properties` configuration file affects all the provisionable servers managed by the N1 System Manager.

Specific threshold values can be set at the command line by following the procedures described in [“Setting Threshold Values” on page 156](#).

Once a default value for a monitored item has been modified by manually adding it in the `monitoring.properties` configuration file, that modified default value applies to all provisionable servers except those servers for which specific values for the monitored attribute have been set at the command line.

Note – You do not need to reboot the management server or the monitored provisionable server for changes to the `monitoring.properties` file to take effect.

Monitored attributes for hardware health that are declared as percentages cannot be changed either at the command line or in the `monitoring.properties` file.

▼ To Modify Default Threshold Values for a Server

To modify default threshold values, edit the `/etc/opt/sun/nlgc/monitoring.properties` file. Only those default threshold values that relate to OS resource utilization attributes can be modified. Hardware health attribute default threshold values cannot be modified for servers.

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 Base and OS Management Features” on page 84](#).

- Steps**
1. **Open the `/etc/opt/sun/nlgc/monitoring.properties` file.**
If the file does not exist, create it.
 2. **Modify or add lines in the `monitoring.properties` file that describe default threshold values.**
`threshold.attribute.threshold value`
The syntax requires the `threshold` keyword to be followed by the *attribute* for which you are setting a threshold. The *attribute* is an OS resource utilization attribute. OS resource utilization attributes are described in [“OS Resource Utilization Monitoring” on page 140](#).
The *threshold* is either `criticallow`, `warninglow`, `warninghigh`, or `criticalhigh`.
The value is a numeric figure and usually represents a percentage value.
 3. **Save the file.**
You do not need to reboot the management server or the provisionable server for the changes to take effect. The modified default threshold values now apply to all servers managed by the N1 System Manager.

Example 5–1 Modifying the Default Threshold Value for File System Usage

This example shows how to modify the default `criticalhigh` threshold value for file system usage to 75 percent of maximum file system usage capacity. The following line is added to or amended in the

`/etc/opt/sun/nlgc/monitoring.properties` file:

```
threshold.fsusage.pctused.criticalhigh=75
```

This value applies to all provisionable servers, unless you have set specific values for the threshold value at the command line, by using the `set` command as described in “Setting Threshold Values” on page 156.

Threshold values can be disabled. This process is shown in [Example 5–4](#).

Hardware Sensor Attributes

For x86 servers, the management server software obtains the list of hardware sensor attributes to monitor through IPMI from the service processor of the server. For servers running the SPARC architecture, the ALOM interface is used. The list of hardware sensor attributes can vary from server to server, and between firmware versions. A sample listing for some servers and firmware versions is provided in this section. It depends on the server type and on the number of CPUs that the server has.

Note – Hardware disk failure and memory failure are not monitored in this version of the N1 System Manager.

The following list contains sensor names and descriptions for a Sun Fire V40z server with firmware version 2.1.0.16:

<code>ambienttemp</code>	Ambient air temp
<code>bulk.v12-0-s0</code>	Bulk 12V S0 voltage at CPU 0
<code>bulk.v12-2-s0</code>	Bulk 12V S0 voltage at CPU 2
<code>bulk.v12-3-s0</code>	Bulk 12V S0 voltage at CPU 3
<code>bulk.v1_8-s0</code>	Bulk 1.8V S0 voltage
<code>bulk.v1_8-s5</code>	Bulk 1.8V S5 voltage
<code>bulk.v2_5-s0</code>	Bulk 2.5V S0 voltage
<code>bulk.v2_5-s0-dc</code>	Bulk 2.5V S0 voltage at DC
<code>bulk.v2_5-s5</code>	Bulk 2.5V S5 voltage
<code>bulk.v3_3-s0</code>	Bulk 3.3V S0 voltage
<code>bulk.v3_3-s0-dc</code>	Bulk 3.3V S0 voltage at DC
<code>bulk.v3_3-s3</code>	Bulk 3.3V S3 voltage
<code>bulk.v3_3-s5</code>	Bulk 3.3V S5 voltage
<code>bulk.v3_3-s5-dc</code>	Aux 3.3V S5 voltage at DC
<code>bulk.v5-s0</code>	Bulk 5V S0 voltage
<code>bulk.v5-s0-dc</code>	Bulk 5V S0 voltage at DC
<code>bulk.v5-s5</code>	Bulk 5V S5 voltage
<code>bulk.v5-s5-dc</code>	Bulk 5V S5 voltage at DC

cd.lp	CDROM Light path location LED
cpu0.dietemp	CPU 0 Die temperature
cpu0.heartbeat	CPU 0 Heartbeat
cpu0.inlettemp	CPU 0 Inlet temperature
cpu0.lp	CPU 0 Light path location LED
cpu0.mem0.lp	CPU 0 Dimm 0 Light path location LED
cpu0.mem1.lp	CPU 0 Dimm 1 Light path location LED
cpu0.mem2.lp	CPU 0 Dimm 2 Light path location LED
cpu0.mem3.lp	CPU 0 Dimm 3 Light path location LED
cpu0.memtemp	CPU 0 Memory temperature
cpu0.memvrm.lp	CPU 0 Memory VRM Light path location LED
cpu0.v2_5-s0	CPU 0 VDDA (2.5V) S0 voltage
cpu0.v2_5-s3	CPU 0 VDD (2.5V) S3 voltage
cpu0.vcore-s0	CPU 0 VCore S0 voltage
cpu0.vid	CPU 0 VID Selection
cpu0.vldt0	CPU 0 LDT0 voltage
cpu0.vrm.lp	CPU 0 VRM Light path location LED
cpu0.vtt-s3	CPU 0 DDR VTT S3 voltage
cpu1.dietemp	CPU 1 Die temperature
cpu1.heartbeat	CPU 1 Heartbeat
cpu1.inlettemp	CPU 1 Inlet temperature
cpu1.lp	CPU 1 Light path location LED
cpu1.mem0.lp	CPU 1 Dimm 0 Light path location LED
cpu1.mem1.lp	CPU 1 Dimm 1 Light path location LED
cpu1.mem2.lp	CPU 1 Dimm 2 Light path location LED
cpu1.mem3.lp	CPU 1 Dimm 3 Light path location LED
cpu1.memtemp	CPU 1 Memory temperature
cpu1.memvrm.lp	CPU 1 Memory VRM Light path location LED
cpu1.v2_5-s0	CPU 1 VDDA (2.5V) S0 voltage
cpu1.v2_5-s3	CPU 1 VDD (2.5V) S3 voltage
cpu1.vcore-s0	CPU 1 VCore S0 voltage
cpu1.vid	CPU 1 VID Selection
cpu1.vldt1	CPU 1 LDT1 voltage
cpu1.vldt2	CPU 1 LDT2 voltage
cpu1.vrm.lp	CPU 1 VRM Light path location LED
cpu1.vtt-s3	CPU 1 DDR VTT S3 voltage
cpu2.dietemp	CPU 2 Die temperature
cpu2.heartbeat	CPU 2 Heartbeat
cpu2.inlettemp	CPU 2 inlet temperature
cpu2.lp	CPU 2 Light path location LED
cpu2.mem0.lp	CPU 2 Dimm 0 Light path location LED
cpu2.mem1.lp	CPU 2 Dimm 1 Light path location LED
cpu2.mem2.lp	CPU 2 Dimm 2 Light path location LED
cpu2.mem3.lp	CPU 2 Dimm 3 Light path location LED
cpu2.memvrm.lp	CPU 2 Memory VRM Light path location LED
cpu2.temp	CPU 2 downwind temperature
cpu2.v2_5-s0	CPU 2 VDDA (2.5V) S0 voltage
cpu2.v2_5-s3	CPU 2 VDD (2.5V) S3 voltage
cpu2.vcore-s0	CPU 2 VCore S0 voltage
cpu2.vid	CPU-2 VID Selection
cpu2.vrm.lp	CPU 2 VRM Light path location LED
cpu2.vtt-s3	CPU 2 DDR VTT voltage
cpu3.dietemp	CPU 3 Die temperature
cpu3.heartbeat	CPU 3 Heartbeat
cpu3.inlettemp	CPU 3 inlet temperature

cpu3.lp	CPU 3 Light path location LED
cpu3.mem0.lp	CPU 3 Dimm 0 Light path location LED
cpu3.mem1.lp	CPU 3 Dimm 1 Light path location LED
cpu3.mem2.lp	CPU 3 Dimm 2 Light path location LED
cpu3.mem3.lp	CPU 3 Dimm 3 Light path location LED
cpu3.memvrm.lp	CPU 3 Memory VRM Light path location LED
cpu3.temp	CPU 3 downwind temperature
cpu3.v2_5-s0	CPU 3 VDDA (2.5V) S0 voltage
cpu3.v2_5-s3	CPU 3 VDD (2.5V) S3 voltage
cpu3.vcore-s0	CPU 3 VCore S0 voltage
cpu3.vid	CPU-3 VID Selection
cpu3.vrm.lp	CPU 3 VRM Light path location LED
cpu3.vtt-s3	CPU 3 DDR VTT voltage
cpuplanar.lp	Daughtercard Light path location LED
fan1.tach	Fan 1 measured speed
fan10.tach	Fan 10 measured speed
fan11.tach	Fan 11 measured speed
fan12.tach	Fan 12 measured speed
fan2.tach	Fan 2 measured speed
fan3.tach	Fan 3 measured speed
fan4.tach	Fan 4 measured speed
fan5.tach	Fan 5 measured speed
fan6.tach	Fan 6 measured speed
fan7.tach	Fan 7 measured speed
fan8.tach	Fan 8 measured speed
fan9.tach	Fan 9 measured speed
faultswitch	System Fault Indication
floppy.lp	Floppy Light path location LED
frontpanel.lp	LCD Light path location LED
g0.vldt1	AMD-8131 PCI-X Tunnel 0 LDT1 voltage
g1.vldt1	AMD-8131 PCI-X Tunnel 1 LDT1 voltage
gbeth.temp	Gigabit ethernet local temperature
golem-v1_8-s0	AMD-8131 PCI-X Tunnel 1.8V S0 voltage
identifyswitch	Identify switch
pci1.lp	PCI Slot 1 Light path location LED
pci2.lp	PCI Slot 2 Light path location LED
pci3.lp	PCI Slot 3 Light path location LED
pci4.lp	PCI Slot 4 Light path location LED
pci5.lp	PCI Slot 5 Light path location LED
pci6.lp	PCI Slot 6 Light path location LED
pci7.lp	PCI Slot 7 Light path location LED
pcifan.lp	Fan Board Light path location LED
planar.lp	Motherboard Light path location LED
scsibp.lp	SCSI Backplane Light path location LED
scsibp.temp	SCSI Disk backplane temperature
scsifault	SCSI Disk Fault Switch
sp.temp	SP local temperature
vldt-reg1-dc	LDT Regulator 1 Voltage
vldt-reg2-dc	LDT Regulator 2 Voltage

The following list contains sensor names and descriptions for a Sun Fire V20z server with firmware version 2.1.0.16:

ambienttemp	Ambient air temp
bulk.v12-0-s0	Bulk 12v supply voltage (cpu0)

bulk.v12-1-s0	Bulk 12v supply voltage (cpu1)
bulk.v1_8-s0	Bulk 1.8v S0 voltage
bulk.v1_8-s5	Bulk 1.8v S5 voltage
bulk.v2_5-s0	Bulk 2.5v S0 voltage
bulk.v2_5-s5	Bulk 2.5v S5 voltage
bulk.v3_3-s0	Bulk 3.3v supply
bulk.v3_3-s3	Bulk 3.3v S3 voltage
bulk.v3_3-s5	Bulk 3.3v S5 voltage
bulk.v5-s0	Bulk 5v supply voltage
bulk.v5-s5	Bulk 5v S5 voltage
cd.lp	CD-ROM Light path location led
cpu0.dietemp	CPU 0 die temp
cpu0.heartbeat	CPU 0 heartbeat
cpu0.lp	CPU 0 Light path location led
cpu0.mem0.lp	CPU 0 Dimm 0 Light path location led
cpu0.mem1.lp	CPU 0 Dimm 1 Light path location led
cpu0.mem2.lp	CPU 0 Dimm 2 Light path location led
cpu0.mem3.lp	CPU 0 Dimm 3 Light path location led
cpu0.memtemp	CPU 0 memory temp
cpu0.memvrm.lp	CPU 0 Memory VRM Light path location led
cpu0.temp	CPU 0 low side temp
cpu0.v2_5-s0	CPU VDDA voltage
cpu0.v2_5-s3	CPU 0 VDDIO voltage
cpu0.vcore-s0	CPU 0 core voltage
cpu0.vid	CPU-0 VID output
cpu0.vldt1	CPU0 HT 1 voltage
cpu0.vldt2	CPU 0 HT 2 voltage
cpu0.vrm.lp	CPU 0 VRM Light path location led
cpu0.vtt-s3	CPU 0 VTT voltage
cpu1.dietemp	CPU 1 die temp
cpu1.heartbeat	CPU 1 heartbeat
cpu1.lp	CPU 1 Light path location led
cpu1.mem0.lp	CPU 1 Dimm 0 Light path location led
cpu1.mem1.lp	CPU 1 Dimm 1 Light path location led
cpu1.mem2.lp	CPU 1 Dimm 2 Light path location led
cpu1.mem3.lp	CPU 1 Dimm 3 Light path location led
cpu1.memtemp	CPU 1 memory temp
cpu1.memvrm.lp	CPU 1 Memory VRM Light path location led
cpu1.temp	CPU 1 low side temp
cpu1.v2_5-s3	CPU 1 VDDIO voltage
cpu1.vcore-s0	CPU 1 core voltage
cpu1.vid	CPU-1 VID output
cpu1.vrm.lp	CPU 1 VRM Light path location led
cpu1.vtt-s3	CPU 1 VTT voltage
fan1.tach	Fan 1 measured speed
fan2.tach	Fan 2 measured speed
fan3.tach	Fan 3 measured speed
fan4.tach	Fan 4 measured speed
fan5.tach	Fan 5 measured speed
fan6.tach	Fan 6 measured speed
faultswitch	Fault switch (source for eval)
floppy.lp	Floppy Disk Drive Light path location led
frontpanel.lp	LCD Light path location led
g.vldt1	AMD-8131 PCI-X Tunnel HT 1 voltage
gbeth.temp	Gigabit ethernet temp

golem.temp	PCIX bridge temp
hdd1.lp	Hard Disk Drive 1 Light path location led
hdd2.lp	Hard Disk Drive 2 Light path location led
hddbp.lp	Hard Disk Drive Backplane Light path location led
hddbp.temp	Disk drive backplane temp
identifyswitch	Identify switch
pci1.lp	PCI Slot 1 Light path location led
pci2.lp	PCI Slot 2 Light path location led
planar.lp	Motherboard Light path location led
ps.fanfail	Power Supply fan failure sensor
ps.lp	Powersupply Light path location led
ps.tempalert	Power Supply too hot sensor
sp.temp	SP temp
thor.temp	AMD-8111 I/O Hub temp

Monitoring data is retrieved by the N1 System Manager from many of these sensors. For Sun Fire x4100 and x4200 servers, sensors other than analog sensors are not used to retrieve data. Only sensors describing fan speed, voltage and temperature are used to retrieve data. For descriptions of sensors in the Sun Fire x4100 and x4200 servers, refer to the IPMI reference information in the Sun Fire x4100 and x4200 server product documentation.

Setting Threshold Values

Threshold values for monitored objects can be set on specific servers. Setting specific threshold values at the command line for attributes of a monitored object overrides for that object any factory-configured threshold values concerning the attribute. Any entries in the `monitoring.properties` configuration file concerning the attribute are also overridden.

▼ 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 Base and OS Management Features” on page 84](#).

Steps 1. Log in to the N1 System Manager.

See [“To Access the N1 System Manager Command Line” on page 25](#) 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 resource utilization attribute. OS resource utilization attributes are described in [“OS Resource Utilization Monitoring” on page 140](#) and listed in [Table 5-2](#).

The *threshold* is either `criticallow`, `warninglow`, `warninghigh`, or `criticalhigh`. The value is a numeric figure and usually represents a percentage.

- 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
```

Example 5–2 Setting Multiple Threshold Values for CPU Usage on a Server

This example shows how to set the CPU usage warninghigh severity threshold on a provisionable server named `serv1` to 53 percent. This example also shows how to set the criticalhigh severity threshold value to 75 percent.

```
N1-ok> set server serv1 threshold cpustats.pctusage warninghigh 53 criticalhigh 75
```

These values override the default values stored in the `monitoring.properties` configuration file on the management server for the server named `serv1`.

Example 5–3 Setting Multiple Threshold Values for File System Usage On a Server

This example sets the file system usage warninghigh threshold on a provisionable server named `serv1` to 75 percent. This example also shows how to set the criticalhigh threshold value to 87 percent.

```
N1-ok> set server serv1 threshold fsusage.pctused warninghigh 75 criticalhigh 87
```

Example 5–4 Deleting a Threshold Value for File System Usage on a Server

This example shows how to delete a value that was set for the warninghigh threshold on a provisionable server named `serv1`.

```
N1-ok> set server serv1 threshold fsusage warninghigh none
```

In this case, any previously set value for this threshold at this severity is deleted. The threshold severity value does not revert back to the default threshold value, which is stored in the `monitoring.properties` configuration file, or to the factory-configured default, if this default existed for the attribute. In effect, monitoring is disabled for the warninghigh threshold for file system usage for this server.

▼ To Set Threshold Values for a Server Group

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 Base and OS Management Features”](#) on page 84.

Steps 1. Log in to the N1 System Manager.

See “To Access the N1 System Manager Command Line” on page 25 for details.

2. Use the **set group** 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 resource utilization attribute. OS resource utilization attributes are described in “OS Resource Utilization Monitoring” on page 140 and listed in Table 5-2.

The *threshold* is either **criticallow**, **warninglow**, **warninghigh**, or **criticalhigh**. The value is a numeric figure, and usually represents a percentage.

■ To modify one threshold for the server group:

```
N1-ok> set group group threshold attribute threshold value
```

■ To modify multiple thresholds for the server group:

```
N1-ok> set group group threshold attribute threshold value threshold value
```

Example 5-5 Setting Multiple Threshold Values for File System Usage on a Server Group

This example shows how to set the file system usage **warninghigh** threshold to 75 percent on a group of provisionable servers with a group name of **grp3**. This example also shows how to set the **criticalhigh** threshold severity value to 87 percent.

```
N1-ok> set group grp3 threshold fsusage.pctused warninghigh 75 criticalhigh 87
```

Setting Polling Intervals

The monitoring of an object consists of regular checks, or polls, of the monitored object. The frequency of these polls is controlled by setting the *polling interval*. The appropriate interval length between polls of the monitored object is related to the object being monitored and its environment, and the performance conditions to which the monitored object is being subjected. Default polling intervals are provided for some monitored objects, including server hardware objects such as fans. Default polling intervals apply for those servers or groups of servers for which specific interval values have not been set by using the **set** command.

Changing Polling Intervals With the Monitoring Configuration File

You can modify default values for polling intervals for hardware health, OS resource utilization, and network reachability by editing the **monitoring.properties** configuration file.

Note – The polling of network reachability is not possible if OS monitoring is not enabled.

If the `monitoring.properties` configuration file is not present, create it and save it in `/etc/opt/sun/nlgc/monitoring.properties`. The `monitoring.properties` is not created by default at installation.

Factory-configured default polling intervals are provided in the N1 System Manager software. These values are stated in seconds. The factory-configured defaults are provided in [Table 5-3](#).

TABLE 5-3 Factory-Configured Default Polling Intervals

Type of Monitoring	Default Polling Interval
Hardware health	120 seconds
OS resources	120 seconds
Network reachability	60 seconds

Any entries you make in the `monitoring.properties` configuration file overwrite these factory-configured defaults.

Note – The minimum default polling interval that you can set is 60 seconds

The `monitoring.properties` configuration file exists only on the management server and not on provisionable servers. Modifying the default polling intervals stored in the `monitoring.properties` configuration file affects all the provisionable servers managed by the N1 System Manager.

You do not need to reboot the management server or the monitored provisionable server for changes to the `monitoring.properties` file to take effect.

Default polling intervals stored in the `monitoring.properties` configuration file apply to all servers unless specific values have been set at the command line for a specific server or group of servers. Set specific polling interval values by using the `set` command, as described in [“Setting Polling Intervals” on page 161](#).

Tuning Polling Intervals for Your Installation

After a period of usage after installation and deployment, you can develop an awareness of how frequently you should be polling hardware health attributes and OS resource utilization attributes, and how often you need to poll your network

reachability. Your configuration of the N1 System Manager depends on what your priorities are, in terms of crucial events. When setting polling intervals, or when changing default polling intervals, consider the number of servers you are managing with your N1 System Manager software. Consider also the application loads or application expected loads of your provisionable servers, and the capabilities of your network. Your expected responsiveness to events is also relevant. If you are able to react quickly to events as they occur, polling more frequently is appropriate.

For further information about tuning polling intervals for your installation, see “To Increase the N1 System Manager Performance” in *Sun N1 System Manager 1.1 Installation and Configuration Guide*.

▼ To Retrieve Polling Interval Values for a Server

Steps 1. Log in to the N1 System Manager.

See “To Access the N1 System Manager Command Line” on page 25 for details.

2. Type the `show server` command:

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

In this procedure, *server* is the name of the provisionable server for which you want to retrieve polling intervals.

Detailed monitoring polling intervals appear in the output, including polling interval information for the server’s hardware health, OS resource utilization, and network reachability.

See “show server” in *Sun N1 System Manager 1.1 Command Line Reference Manual* for details.

▼ To Modify the Default Polling Interval 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 Base and OS Management Features” on page 84.

Steps 1. Open the `/etc/opt/sun/nlmc/monitoring.properties` file.

If the file does not exist, create it.

2. Modify or add lines in the `monitoring.properties` file that describe default polling intervals.

```
pollinginterval.monitor=value
```

The syntax requires the `pollinginterval` keyword.

monitor is either `hardwarehealth`, `osresources` or `network`. The polling of network reachability is not possible unless OS resource monitoring has been

enabled, as described in “Enabling Monitoring” on page 142.

The *value* is in seconds, and the minimum value is 60.

3. Save the file.

You do not need to reboot the management server or the provisionable server for the changes to take effect. The modified default polling intervals values now apply to all servers managed by the N1 System Manager.

Example 5–6 Modifying Default Values

This example shows how to set the hardware health monitoring polling interval to 180 seconds, the OS resource utilization monitoring polling interval to 175 seconds, and the network reachability monitoring polling interval to 160 seconds. The following entries are made in the `monitoring.properties` configuration file.

```
pollinginterval.hardwarehealth=180
pollinginterval.osresources=175
pollinginterval.network=160
```

Setting Polling Intervals

This section contains procedures that describe how to set the polling intervals for a server or a server group.

▼ To Set Polling Intervals for a Server

This procedure shows you how to set a polling interval for a server at the command line. Any value set this way overwrites the factory-configured default value or the value in the `monitoring.properties` configuration file, if the file exists.

Steps 1. Log in to the N1 System Manager.

See “To Access the N1 System Manager Command Line” on page 25 for details.

2. Type the `set server` command with the `monitor` attribute.

```
set server server monitor monitor interval value
```

This command is executed for a server that you have already named. In this procedure, this name appears as *server*. See “set server” in *Sun N1 System Manager 1.1 Command Line Reference Manual* for details.

The *monitor* is either `hardwarehealth`, `osresources`, or `network`.

The *value* is in seconds.

Note – The minimum polling interval that you can set is 60 seconds.

Example 5–7 Setting the Polling Interval for Hardware Health Monitoring of a Server

This example shows how to set a polling interval of 280 seconds for hardware health monitoring of a provisionable server named `serv1`.

```
N1-ok> set server serv1 monitor hardwarehealth interval 280
```

▼ **To Set Polling Intervals for a Server Group**

Any value set this way overwrites the factory-configured default value or the value in the `monitoring.properties` configuration file, if the file exists.

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

See [“To Access the N1 System Manager Command Line”](#) on page 25 for details.

2. **Type the `set group` command with the `monitor` attribute.**

```
set group group monitor monitor interval value
```

This command is executed for a group of servers that you have already named. In this procedure, this name appears as *group*. See “*set group*” in *Sun N1 System Manager 1.1 Command Line Reference Manual* for details.

The *monitor* is either `hardwarehealth`, `osresources`, or `network`.

The *value* is in seconds.

Note – The minimum polling interval that you can set is 60 seconds.

Example 5–8 Setting the Polling Interval for Network Reachability Monitoring of a Server Group

This example shows how to set a polling interval of 250 seconds for network reachability monitoring of a group of provisionable servers named `grp5`.

```
N1-ok> set group grp5 monitor network interval 250
```

Monitoring MIBs

Two MIBs are provided with the N1 System Manager. These MIBs provide the data structure that third-party monitoring tools can use to retrieve the data from the N1 System Manager using SNMP, and provide the data structure that third party monitoring tools can use to parse the SNMP notifications generated by the N1 System Manager. The MIBs can be found at `/opt/sun/nlgc/etc/`. These MIBs therefore enable you to use any SNMP client to query the N1 System Manager, and to listen for events using SNMP. The following MIBs are provided:

SUN-N1SM-INFO-MIB	This MIB describes the information that you can retrieve from the N1 System Manager by querying it using an SNMP client.
SUN-N1SM-TRAP-MIB	This MIB describes all of the events related to the N1 System Manager about which you can receive SNMP traps.

These MIBs are read-only. Using them requires a detailed knowledge of SNMP, although detailed descriptions of each object are provided in the MIBs. How you configure your monitoring system to start receiving traps depends on the nature of your monitoring system.

The MIBs are hardware independent.

EXAMPLE 5-9 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.

```
N1-ok> snmptrapd -m all -M /opt/sun/nlgc/etc:/usr/share/snmp/mibs -P 1010
```

This example uses the `snmptrapd` command to start monitoring port 1010 for SNMP traps. It also instructs the command to use the MIBs stored at `/opt/sun/nlgc/etc` and `/usr/share/snmp/mibs` to parse the contents of SNMP traps.

How you configure your monitoring system to start receiving traps depends on the nature of your monitoring system.

Managing Jobs

This section describes jobs and how they are an integral part of server monitoring.

Each major action you take in the N1 System Manager starts a job. Use the job log to track the status on a currently running action or to verify that a job has finished. Monitoring jobs is useful particularly because some N1 System Manager actions can take a long time to finish. An example of such an action is installing an OS distribution on one or more provisionable servers.

You can track jobs through the Jobs tab in the browser interface or the `show job` command. The `show job` command provides information about most of the following characteristics:

Job ID	Generated unique identifier.
Date	Date on which the job was started.
Job Type	Type of job. See “show job” in <i>Sun N1 System Manager 1.1 Command Line Reference Manual</i> for details. When using the <code>show job</code> command with the <code>type</code> parameter, jobs can be any of the following types: <ul style="list-style-type: none"> ■ <code>addbase</code> – Add base management support. ■ <code>addbasemonitor</code> – Add OS monitoring support. ■ <code>createos</code> – Create OS distribution from CD/DVD media or ISO files. ■ <code>deletejob</code> – Delete job. ■ <code>discover</code> – Server discovery. ■ <code>loadfirmware</code> – Load firmware update. ■ <code>loados</code> – Load OS. ■ <code>loadupdate</code> – Load OS update. ■ <code>refresh</code> – Server refresh. ■ <code>removeosmonitor</code> – Remove OS monitoring support. ■ <code>setagentip</code> – Modify OS monitoring support. ■ <code>start</code> – Server power on. ■ <code>stop</code> – Server power off. ■ <code>unloadupdate</code> – 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: <ul style="list-style-type: none"> <code>notstarted</code> Jobs in a <code>notstarted</code> state cannot be stopped. <code>preflight</code> When you select a job by ID and view the details of that job, each step of that job appears twice – the preflight check and the execution of the step itself. <code>running</code> The job is currently running. Jobs that are currently running cannot be deleted using the <code>delete job</code> command. Jobs that are currently running must finish running or be stopped using the <code>stop job</code> 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 or might not necessarily be severe enough to terminate the job step, and the job, with errors.
abort	Indicates that the job step stopped before it completed.
abort_pending	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 but there were one or more WARNING states 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 1.1 Command Line Reference Manual* for details.

Owner The user who started the job. Also called the job *creator*.

Job Results Provides details about the results of a completed job. You can review the standard output of remote command operations and completion statuses for all other job types.

▼ To List Jobs

Steps 1. Log in to the N1 System Manager.

See “[To Access the N1 System Manager Command Line](#)” on page 25 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 1.1 Command Line Reference Manual* for details.

Example 5–10 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	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	Completed	root
2	2005-09-09T12:38:16-0700	Discovery	Completed	root
1	2005-09-09T10:32:40-0700	Discovery	Completed	root

▼ To View a Specific Job

Steps 1. Log in to the N1 System Manager.

See “To Access the N1 System Manager Command Line” on page 25 for details.

2. View a specific job.

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

Detailed information about the job appears in the output.

See “show job” in *Sun N1 System Manager 1.1 Command Line Reference Manual* for details.

Example 5–11 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. 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 5
```

Job ID:	5
Date:	2005-02-14T14:38:25-0700
Type:	Server Power On
Status:	Completed
Creator:	root

```

Errors:      0
Warnings:    0
Step 1:
Type:        103
Description: native procedure /bin/sh /opt/sun/nlgc/bin/serverPowerOn.sh :[SERVER_NAME] :[JOBID_KEY]
Start:       2005-02-14T14:38:25-0700
Completion:  2005-02-14T14:38:25-0700
Result:      Complete
Exception:   No Data Available
Step 2:
Type:        103
Description: native procedure /bin/sh /opt/sun/nlgc/bin/serverPowerOn.sh :[SERVER_NAME] :[JOBID_KEY]
Start:       2005-02-14T14:38:28-0700
Completion:  2005-02-14T14:38:35-0700
Result:      Complete
Exception:   No Data Available
Step 3:
Type:        135
Description: connect and lock hosts
Start:       2005-02-14T14:38:25-0700
Completion:  2005-02-14T14:38:25-0700
Result:      Complete
Exception:   No Data Available
Step 4:
Type:        135
Description: connect and lock hosts
Start:       2005-02-14T14:38:27-0700
Completion:  2005-02-14T14:38:28-0700
Result:      Complete
Exception:   No Data Available
Result 1:
Server:      192.168.200.3
Status:      0
Message:     The server operation was successful.
N1-ok>

```

Each step appears twice in the output. The first appearance of the step in the list is the preflight check, and the second appearance of the step in the list is the actual execution of the step.

▼ To Stop a Job

Steps 1. Log in to the N1 System Manager.

See [“To Access the N1 System Manager Command Line”](#) on page 25 for details.

2. Stop a specific job.

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

The job is stopped.

See “stop job” in *Sun N1 System Manager 1.1 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 1.1 Command Line Reference Manual* for details.

Example 5–12 Stopping a Remote Command 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 9
```

```
Stop Job "9" 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. This returns the confirmation, in Status, that the job was stopped, and that the job was a remote command 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 canceled.

```
N1-ok> show job 9
```

```
Job ID:    9
Date:      2005-02-15T16:43:58-0700
Type:      Remote Command
Status:     Stopped
Owner:     root
Errors:    0
Warnings:  0
```

```
Step 1:
Type:      135
Description: connect and lock hosts
Start:      2005-02-15T16:43:58-0700
Completion: 2005-02-15T16:43:58-0700
Result:     Complete
Exception:  No Data Available
```

```
Step 2:
Type:      103
Description: native procedure /bin/sh /opt/sun/nlgc/bin/remotecmd.sh
```



```

: [RCMD_KEY]
Start:      2005-02-15T16:43:58-0700
Completion: 2005-02-15T16:43:58-0700
Result:     Complete
Exception:  No Data Available

Step 3:
Type:       135
Description: connect and lock hosts
Start:      2005-02-15T16:44:00-0700
Completion: 2005-02-15T16:44:00-0700
Result:     Complete
Exception:  No Data Available

Step 4:
Type:       103
Description: native procedure /bin/sh /opt/sun/nlgc/bin/remotecmd.sh
: [RCMD_KEY]
Start:      2005-02-15T16:44:00-0700
Completion: 2005-02-15T16:44:49-0700
Result:     Incomplete - Aborted
Exception:  No Data Available

Result :
Server:   server1
Status:   -1
Message:  Command running on server1 was canceled. Command:
/root/sleep.sh 60
Standard Output: Sleeping for 60 seconds...

```

Each step appears twice in the output. The first appearance of the step in the list is the preflight check, and the second appearance of the step in the list is the actual execution of the step.

See Also [“To Issue Remote Commands on a Server or a Server Group” on page 127](#)

▼ To Delete a Job

Steps 1. Log in to the N1 System Manager.

See [“To Access the N1 System Manager Command Line” on page 25](#) 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 1.1 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 1.1 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 1.1 Command Line Reference Manual* for details.

Example 5-13 Deleting a Job

This example shows how to delete a job.

First, the `show job` command is used with the `all` option, which lists all jobs in descending order.

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

Job ID	Date	Type	Status	Creator
7	2005-02-16T10:51:07-0700	Discovery	Completed	root
6	2005-02-14T14:42:52-0700	Server Reboot	Error	root
5	2005-02-14T14:38:25-0700	Server Power On	Completed	root
4	2005-02-14T14:29:20-0700	Server Power Off	Completed	root
3	2005-02-09T13:01:35-0700	Discovery	Completed	root
2	2005-02-09T12:38:16-0700	Discovery	Completed	root
1	2005-02-09T10:32:40-0700	Discovery	Completed	root

Job ID 6 has an error and can be deleted. The `delete job` command is now used with the Job ID of the job to be deleted.

```
N1-ok> delete job 6
```

The `show job` command is used again with the `all` option, which lists all jobs in descending order. The deleted job no longer appears on the list.

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

Job ID	Date	Type	Status	Creator
7	2005-02-16T10:51:07-0700	Discovery	Completed	root
5	2005-02-14T14:38:25-0700	Server Power On	Completed	root
4	2005-02-14T14:29:20-0700	Server Power Off	Completed	root
3	2005-02-09T13:01:35-0700	Discovery	Completed	root
2	2005-02-09T12:38:16-0700	Discovery	Completed	root
1	2005-02-09T10:32:40-0700	Discovery	Completed	root

Example 5-14 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
--------	------	------	--------	---------

Managing Event Log Entries

This section describes events and how they are integral 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 1.1 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 is polled and the value of the attribute 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 138 for more information about monitoring.

See “[Setting Up Notifications](#)” on page 175 for more information about 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.

Logs are created when events occur. For example, if any monitored IP address is unreachable, an event is generated. This event creates a log record, which is visible from the browser interface.

Event Log Overview

During the installation and configuration of the N1 System Manager, you can configure which events to log and you can also interactively configure severity levels for event topics. See “Configuring the N1 System Manager System” in *Sun N1 System Manager 1.1 Installation and Configuration Guide*.

Even if a log is not saved, it can still generate a notification.

Use the `show` command with the `log` keyword 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 notifications. Refer to [“Setting Up Notifications” on page 175](#) 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 logs are kept. Reducing the number of days for which logs are stored reduces the average size of the log files. This task ensures that the log file size does not impair performance. The `n1smconfig` script is stored at `/opt/sun/n1gc/bin`. This script can be used to set the number of days for which logs are held. To configure logging, you must 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 notification topics at “create notification” in *Sun N1 System Manager 1.1 Command Line Reference Manual*.

▼ To View the Event Log

Steps 1. Log in to the N1 System Manager.

See [“To Access the N1 System Manager Command Line” on page 25](#) 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 1.1 Command Line Reference Manual* for details.

See Also [“Event Log Overview” on page 172](#)

▼ To Filter the Event Log

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

See [“To Access the N1 System Manager Command Line” on page 25](#) for details.

2. **Type the following command:**

```
N1-ok> show log [severity severity] [before date] [after date]
```

The output shows only the events that match the specified criteria. The *date* variable values must be formatted appropriately, for example, 2005-07-20T11:53:04. The possible values for severity are critical, fatal, information, major, minor, other, unknown, and warning. See “show log” in *Sun N1 System Manager 1.1 Command Line Reference Manual* for details.

▼ To View Event Details

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

See [“To Access the N1 System Manager Command Line” on page 25](#) 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 1.1 Command Line Reference Manual* for details.

Example 5–15 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 Notifications

The N1 System Manager provides the ability to set up email or SNMP notifications when events occur, either within the N1 System Manager itself or when specific events occur on provisionable servers. You can set up customized notification rules for as many different scenarios as you need. Setting up notifications can be done only through the command line.

Use the `create notification` command to create *notification rules* based on events that occur or might occur about which you are interested. Use a topic to create a notification.

For setting up 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 163](#).

A notification rule can be used to send a notification of each type of event to a selected destination, using either email or SNMP as the communication medium. For example, you can create a notification rule so that each time a new provisionable server is discovered by the management server, you receive a message on your pager to indicate that the event has happened:

```
create notification notification destination destination topic topic  
type type [description description]
```

See “`create notification`” in *Sun N1 System Manager 1.1 Command Line Reference Manual* for details of the terms used in this command syntax.

You can configure your SMTP server to use event notification, during the installation and configuration of the N1 System Manager. See “Configuring the N1 System Manager System” in *Sun N1 System Manager 1.1 Installation and Configuration Guide*.

Viewing and Modifying Notifications

Use the `show` and `set` commands with the `notification` option to view and modify notification details. Type `help show notification` or `help set notification` at the N1-ok command line for syntax and parameter details.

▼ To View Notifications

- Steps**
1. **Log in to the N1 System Manager.**
See [“To Access the N1 System Manager Command Line”](#) on page 25 for details.
 2. **Type the following command:**

```
N1-ok> show notification all
```

The notifications for which you have read privileges appear in the output. See *“show notification”* in *Sun N1 System Manager 1.1 Command Line Reference Manual* for details.

▼ To View Notification Details

- Steps**
1. **Log in to the N1 System Manager.**
See [“To Access the N1 System Manager Command Line”](#) on page 25 for details.
 2. **Type the following command:**

```
N1-ok> show notification notification
```

The specified notification details appear in the output. See *“show notification”* in *Sun N1 System Manager 1.1 Command Line Reference Manual* for details.

Example 5–16 Viewing Notification Details

```
N1-ok> show notification test2
Name:          test2
Event Topic:   EReport.Physical.ThresholdExceeded
Notifier Type: Email
Destination:   nobody@sun.com
State:         enabled
```

▼ To Modify a Notification

This procedure describes how to change the name, description, or destination of a notification.

- Steps**
1. **Log in to the N1 System Manager.**
See [“To Access the N1 System Manager Command Line”](#) on page 25 for details.

2. Type the following command:

```
N1-ok> set notification notification name name description description
destination destination
```

The specified notification attributes are set to the new values specified. See “set notification” in *Sun N1 System Manager 1.1 Command Line Reference Manual* for details.

Example 5–17 Modifying a Notification Name

This example shows how to use the set notification command with the name option to change a notification name from test2 to test3.

```
N1-ok> set notification test2 name test3
```

Creating, Testing, and Deleting Notifications

Use the create or delete command with the notification option to create and delete notifications.

Use the create command with the notification option and the test subcommand to test a notification.

Type help create notification or help delete notification at the N1-ok command line for syntax and parameter details.

▼ To Create and Test a Notification

Steps 1. Log in to the N1 System Manager.

See “[To Access the N1 System Manager Command Line](#)” on page 25 for details.

2. Type the following command:

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

The notification is created and enabled. See “create notification” in *Sun N1 System Manager 1.1 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 1.1 Command Line Reference Manual* for details.

Example 5–18 Creating an Email Notification

This example shows how to create a notification to be sent by email if a physical threshold value is exceeded. The notification is called `test2`. The recipient's email address is `nobody@sun.com`

```
N1-ok> create notification test2 destination nobody@sun.com
topic EReport.Physical.ThresholdExceeded type email
```

The `show notification` command can be used to verify that the notification has been created.

```
N1-ok> show notification
Name      Event Topic                               Destination      State
test2     EReport.Physical.ThresholdExceeded  nobody@sun.com   enabled
```

Example 5–19 Creating an SNMP Notification

This example shows how to create a notification to be sent by SNMP if a physical threshold value is exceeded. The notification is called `test23`. The recipient SNMP address is `sun.com`

```
N1-ok> create notification test23 destination sun.com
topic EReport.Physical.ThresholdExceeded type snmp
```

The `show notification` command can be used to verify that the notification has been created.

```
N1-ok> show notification
Name      Event Topic                               Destination      State
test23    EReport.Physical.ThresholdExceeded  sun.com          enabled
```

▼ To Delete a Notification

Steps 1. Log in to the N1 System Manager.

See [“To Access the N1 System Manager Command Line”](#) on page 25 for details.

2. Type the following command:

```
N1-ok> delete notification notification
```

The notification is deleted.

Starting and Stopping Notifications

Notifications are enabled, or *started*, by default at creation. Use the `start` command with the `notification` option to enable a notification that has been disabled. Type `help start notification` at the `N1-ok` command line for syntax and parameter details.

▼ To Start a Notification

- Steps**
1. **Log in to the N1 System Manager.**
See [“To Access the N1 System Manager Command Line”](#) on page 25 for details.
 2. **Type the following command:**

```
N1-ok> start notification notification
```

The notification is enabled. See “start notification” in *Sun N1 System Manager 1.1 Command Line Reference Manual* for details.

▼ To Stop a Notification

- Steps**
1. **Log in to the N1 System Manager.**
See [“To Access the N1 System Manager Command Line”](#) on page 25 for details.
 2. **Type the following command:**

```
N1-ok> stop notification notification
```

The notification is disabled. See “stop notification” in *Sun N1 System Manager 1.1 Command Line Reference Manual* for details.

Troubleshooting

This chapter provides troubleshooting information on the following topics:

- “Security” on page 181
- “Troubleshooting OS Distributions” on page 183
- “OS Profile Deployment Failures” on page 190
- “OS Update Problems” on page 197
- “To Download and Prepare Sun Fire V20z and V40z Server Firmware” on page 201
- “Handling Threshold Breaches” on page 203

Security

This section provides security-based troubleshooting information.

The Sun N1 System Manager Server uses strong encryption techniques to ensure secure communication between the management server and each managed server.

The keys used by the Sun N1 System Manager are stored under the `/etc/opt/sun/cacao/security` directory on each server where the servers are running Linux. These keys should be identical across all servers. For servers running the Solaris OS, these keys are stored under the `/etc/opt/SUNWcacao/security` directory.

Under normal operation, these keys can be left in their default configuration. You might have to regenerate security keys. For example, if there is a risk that the root password of the management server has been exposed or compromised, regenerate the security keys.

▼ How to Regenerate Common Agent Container Security Keys

- Steps** 1. **On the management server as root, stop the common agent container management daemon.**

If the management server is running Linux:

```
# /opt/sun/cacao/bin/cacoadm stop
```

If the management server is running the Solaris OS:

```
# /opt/SUNWcacao/bin/cacoadm stop
```

2. **Regenerate security keys using the `create-keys` subcommand.**

If the management server is running Linux:

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

If the management server is running the Solaris OS:

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

3. **As root on the management server, restart the common agent container management daemon.**

If the management server is running Linux:

```
# /opt/sun/cacao/bin/cacoadm start
```

If the management server is running the Solaris OS:

```
# /opt/SUNWcacao/bin/cacoadm start
```

General Security Considerations

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

- The Java™ Web Console that is used to launch the N1 System Manager's browser interface uses self-signed certificates. These certificates should be treated with the appropriate level of trust by clients and users.
- The terminal emulator applet that is used by the browser interface for the serial console feature does not provide a certificate-based authentication of the applet. The applet also requires that you enable SSHv1 for the management server. For certificate-based authentication or to avoid enabling SSHv1, use the serial console feature by running the `connect` command from the `n1sh` shell.
- SSH fingerprints that are used to connect from the management server to the provisioning network interfaces on the provisionable servers are automatically acknowledged by the N1 System Manager software. This automation might make the provisionable servers vulnerable to "man-in-the middle" attacks.

- The Web Console (Sun ILOM Web GUI) autologin feature for Sun Fire X4100 and Sun Fire X4200 servers exposes the server's service processor credentials to users who can view the web page source for the Login page. To avoid this security issue, disable the autologin feature by running the `n1smconfig` utility. See "Configuring the N1 System Manager System" in *Sun N1 System Manager 1.1 Installation and Configuration Guide* for details.

Troubleshooting OS Distributions

This section describes scenarios that cause OS deployment to fail and explains how to correct failures.

Distribution Copy Failures

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

```
bash-3.00# /opt/sun/nlgc/bin/nlsh show job 25
Job ID:    25
Date:      2005-07-20T14:28:43-0600
Type:      Create OS Distribution
Status:    Error (2005-07-20T14:29:08-0600)
Owner:     root
Errors:    1
Warnings:  0
```

Steps

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

Errors

Error 1:

```
Description: INFO : Mounting /images/rhel-3-U4-i386-es-disc1.iso at
/mnt/loop23308
INFO : Version is 3ES, disc is 1
INFO : Version is 3ES, disc is 1
INFO : type redhat ver: 3ES
```

```

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

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

```

Patching Solaris 9 Distributions

The inability to deploy Solaris 9 OS distributions to servers from a Linux management server is usually due to a problem with NFS mounts. To solve this problem, you need to apply a patch to the mini-root of the Solaris 9 OS distribution. This section provides instructions for applying the required patches. The instructions differ according to the management and patch server configuration scenarios in the following table.

TABLE 6-1 Task Map for Patching a Solaris 9 Distribution

Management Server	Patch Server	Task
Red Hat 3.0 u2	Solaris 9 OS on x86 platform	“To Patch a Solaris 9 OS Distribution by Using a Solaris 9 OS on x86 Patch Server” on page 185
Red Hat 3.0 u2	Solaris 9 OS on SPARC platform	“To Patch a Solaris 9 OS Distribution by Using a Solaris 9 OS on SPARC Patch Server” on page 187

Using a Provisionable Server to Patch OS Distributions

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

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

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

Before You Begin

- Create a Solaris 9 OS distribution on the management server. See [“To Copy an OS Distribution From CDs or a DVD” on page 67](#) or [“To Copy an OS Distribution From ISO Files” on page 66](#). Type `show os os-name` at the command line to view the ID of the OS distribution. This number is used in place of `DISTRO_ID` in the instructions.
- Install the Solaris 9 OS on x86 platform software on a machine that is not the management server.
- Create a `/patch` directory on the Solaris 9 x86 patch server.
- For a Solaris OS on x86 distribution, download and unzip the following patches into the `/patch` directory on the Solaris 9 OS on x86 patch server: 117172-17 and 117468-02. You can access these patches from <http://sunsolve.sun.com>.
- For a Solaris OS on SPARC distribution, download and unzip the following patches into the `/patch` directory on the Solaris 9 OS on x86 patch server: 117171-17, 117175-02, and 113318-20. You can also access these patches from <http://sunsolve.sun.com>.

Steps 1. Patch the Solaris 9 OS on x86 patch server.

a. Log in as root.

```
% su
password:password
The root prompt appears.
```

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

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

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

```
# cd /patch
```

d. Install the patches.

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

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

2. Prepare to patch the distribution on the management server.

a. Log in to the management server as root.

```
% su
password:password
The root prompt appears.
```

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

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

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

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

e. Restart NFS.

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

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

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

```
% su
password:password
The root prompt appears.
```

b. Mount the management server.

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

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

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

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

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

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

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

- d. Unmount the management server.

```
# umount /mnt
```

- 4. Restart NFS on the management server.

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

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

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

- c. Restart NFS.

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

NFS is restarted.

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

- 5. Fix the Solaris 9 OS on x86 distribution.

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

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

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

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

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

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

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

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

Before You Begin

- Create a Solaris 9 OS distribution on the management server. See [“To Copy an OS Distribution From CDs or a DVD” on page 67](#) or [“To Copy an OS Distribution From ISO Files” on page 66](#). Type `show os os-name` at the command line to view the ID of the OS distribution. This number is used in place of `DISTRO_ID` in the

instructions.

- Install the Solaris 9 OS on SPARC software on a machine that is not the management server. See [“To Load an OS Profile on a Server or a Server Group” on page 81.](#)
- Create a /patch directory on the Solaris 9 SPARC patch server.
- For a Solaris OS on x86 distribution, download and unzip the following patches into the /patch directory on the Solaris 9 OS on x86 patch server: 117172-17 and 117468-02. You can access these patches from <http://sunsolve.sun.com>.
- For a Solaris OS on SPARC distribution, download and unzip the following patches into the /patch directory on the Solaris 9 OS on x86 patch server: 117171-17, 117175-02, and 113318-20. You can access these patches from <http://sunsolve.sun.com>.

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

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

```
% su
password:password
```

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

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

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

```
# cd /patch
```

d. Install the patches.

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

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

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

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

```
% su
password:password
```

b. Mount the management server.

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

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

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

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

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

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

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

- d. Unmount the management server.

```
# umount /mnt
```

3. Restart NFS on the management server.

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

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

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

- c. Restart NFS.

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

NFS is restarted.

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

4. Fix the Solaris 9 OS on x86 distribution.

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

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

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

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

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

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


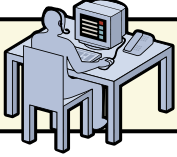

OS Profile Deployment Failures

OS profile deployments might fail if any of the following conditions occur:

- Partitions are not modified to suit a Sun Fire V40z or SPARC V440 server. See [“To Modify the Default Solaris OS Profile for a Sun Fire V40z or a SPARC v440 Server” on page 191.](#)
- Scripts are not modified to install the driver needed to recognize the Ethernet interface on a Sun Fire V20z server. See [“To Modify a Solaris 9 OS Profile for a Sun Fire V20z Server With a K2.0 Motherboard” on page 192.](#)
- DHCP is not correctly configured. See [“Solaris Deployment Job Times Out or Stops” on page 194.](#)
- OS profile installs only the Solaris Core System Support distribution group. See [“Solaris OS Profile Installation Fails” on page 195.](#)
- The target server cannot access DHCP information or mount distribution directories. See [“Invalid Management Server Netmask” on page 195.](#)
- The management server cannot access files during a Load OS operation. See [“Restarting NFS to Resolve Boot Failed Errors” on page 196.](#)
- The Linux deployment stops. See [“Linux Deployment Stops” on page 195.](#)

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

Troubleshooting OS Provisioning

- 1 Access the service processor of the provisionable server by using Telnet, SSH, or opening the serial console. 
- 2 Type `platform console` or an equivalent command to access the BIOS. `N1-ok> platform console`
- 3 Type `platform power cycle` or an equivalent command to check that self-test completes and Preboot Execution Environment (PXE) boot starts. `N1-ok> platform power cycle`
- 4 Issue the `load server osprofile` command to start the Load OS job. `N1-ok> load server osprofile`
- 5 Monitor the installation for any failures and to check that disk partitions, resources, and scripts are configured appropriately. 
- 6 Verify successful installation by listening for DHCP broadcasts from the provisioned server `eth0` and `eth1` ports. 

▼ To Modify the Default Solaris OS Profile for a Sun Fire V40z or a SPARC v440 Server

This procedure describes how to modify the Solaris OS profile that is created by default. The following modification is required for successful installation of the default Solaris OS profile on a Sun Fire V40z or a SPARC v440 server.

Steps 1. Log in to the N1 System Manager.

See [“To Access the N1 System Manager Command Line”](#) on page 25 for details.

2. Clone the default profile.

```
N1-ok> create osprofile sol10v40z clone sol10
```

3. Remove the root partition.

```
N1-ok> remove osprofile sol10v40z partition /
```

4. Remove the swap partition.

```
N1-ok> remove osprofile sol10v40z partition swap
```

5. Add new root parameters.

```
N1-ok> add osprofile sol10v40z partition / device c1t0d0s0 sizeoption free  
type ufs
```

6. Add new swap parameters.

```
N1-ok> add osprofile sol10v40z partition swap device c1t0d0s1 size 2000  
type swap sizeoption fixed
```

See Also To find out how to load the modified OS profile, see [“To Load an OS Profile on a Server or a Server Group” on page 81.](#)

▼ To Modify a Solaris 9 OS Profile for a Sun Fire V20z Server With a K2.0 Motherboard

This procedure describes how to create and add a script to your Solaris OS profile. This script installs the Broadcom 5704 NIC driver needed for Solaris 9 x86 to recognize the NIC Ethernet interface on a Sun Fire V20z server with a K2.0 motherboard. Earlier versions of the Sun Fire V20z server use the K1.0 motherboard. Newer versions use the K2.0 motherboard.

Note – This patch is needed for K2.0 motherboards but can also be used on K1.0 motherboards without negative consequences.

Steps 1. Log in to the N1 System Manager.

See [“To Access the N1 System Manager Command Line” on page 25](#) for details.

2. Type the following command:

```
% /opt/sun/nlgc/bin/nlsh show os
```

The list of available OS distributions appears. Note the name of the Solaris 9 distribution.

3. Run the `as_distro.pl` script, and view the output.

```
# /scs/sbin/as_distro.pl -l
```

4. Note down the `DISTRO_ID` for the Solaris 9 distribution.

You use this ID in the next step.

5. Type the following command:

```
# mkdir /js/DISTRO_ID/patch
```

A patch directory is created for the Solaris 9 distribution.

6. Download the 116666-04 patch from <http://sunsolve.sun.com> to the /js/DISTRO_ID/patch directory.

7. Change to the /js/DISTRO_ID/patch directory.

```
# cd /js/DISTRO_ID/patch
```

8. Unzip the patch file.

```
# unzip 116666-04.zip
```

9. Type the following command:

```
# mkdir /js/scripts
```

10. In the /js/scripts directory, create a script called patch_sol9_k2.sh that includes the following three lines:

```
#!/bin/sh
echo "Adding patch for bge devices."
patchadd -R /a -M /cdrom/patch 116666-04
```

Note – Ensure the script is executable. You can use the `chmod 775 patch_sol9_k2.sh` command.

11. Add the script to the Solaris 9 OS profile.

```
N1-ok> add osprofile osprofile script /js/scripts/patch_sol9_k2.sh type post
```

Example 6–1 Adding a Script to a Solaris OS Profile

This example shows how to add a script to an OS profile. The `type` attribute specifies that the script is to be run after the installation.

```
N1-ok> add osprofile sol9K2 script /js/scripts/patch_sol9_k2.sh
type post
```

Next Steps To load the modified Solaris OS profile, see [“To Load an OS Profile on a Server or a Server Group” on page 81](#).

Solaris Deployment Job Times Out or Stops

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

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

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

Note – The best diagnostic tool is to open a console window on the target machine and then run the deployment. See [“To Open a Server’s Serial Console” on page 131](#).

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

▼ To Modify the Network Interface Configuration

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

2. Inspect the `dhcpd.conf` file for errors.

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

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

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

The `n1smconfig` utility appears.

4. Modify the provisioning network interface configuration.

See “Configuring the N1 System Manager System” in *Sun N1 System Manager 1.1 Installation and Configuration Guide* for detailed instructions.

5. Load the OS profile on the target server.

Solaris OS Profile Installation Fails

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

Invalid Management Server Netmask

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

```
Booting kernel/unix...
krtld: Unused kernel arguments: 'install'.
SunOS? Release 5.10 Version Generic 32-bit
Copyright 1983-2005 Sun Microsystems, Inc. All rights reserved.
Use is subject to license terms.
Unsupported Tavor FW version: expected: 0003.0001.0000, actual: 0002.0000.0000
NOTICE: tavor0: driver attached (for maintenance mode only)
Configuring devices.
Using DHCP for network configuration information.
Beginning system identification...
Searching for configuration file(s)...
Using sysid configuration file /sysidcfg
Search complete.
Discovering additional network configuration...
Completing system identification...
Starting remote procedure call (RPC) services: done.
System identification complete.
Starting Solaris installation program...
Searching for JumpStart directory...
/sbin/dhccpinfo: primary interface requested but no primary interface is set
not found
Warning: Could not find matching rule in rules.ok
Press the return key for an interactive Solaris install program...
```

To fix the problem, set the management server netmask value to 255.255.255.0. See “To Configure the Sun N1 System Manager System” in *Sun N1 System Manager 1.1 Installation and Configuration Guide*.

Linux Deployment Stops

If you are deploying a Linux OS and the deployment stops, check the console of the target server to see if the installer is in interactive mode. If the installer is in interactive mode, the deployment timed out because of a delay in the transmission of data from

the management server to the target server. This delay usually occurs because the switch or switches connecting the two machines has spanning tree enabled. Either turn off spanning tree on the switch or disable spanning tree for the ports that are connected to the management server and the target server.

If spanning tree is already disabled and OS deployment stops, you may have a problem with your network.

Restarting NFS to Resolve Boot Failed Errors

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

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

On a Solaris system, type the following:

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

On a Linux system, type the following:

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

Resolving wget Command Failures Related to OS Monitoring

You must manually install the wget information if the add server feature osmonitor agentip command fails with the following error: Internal error: wget command failed: /usr/bin/wget -O /tmp/hostinstall.pl http://xx.xx.xx.xx/pub/hostinstall.pl, where xx.xx.xx.xx is the IP address of the machine in question.

- For a Solaris system, install the SUNWwgetu and SUNWwgetr packages in /usr/sfw/bin/wget.
- For a Linux system, install all RPMs that begin with wget- in /usr/bin/wget.

Adding the feature might also fail due to stale SSH entries on the management server. If the add server server-name feature osmonitor agentip command fails and no true security breach has occurred, remove the /root/.ssh/known_hosts file or the specific entry in the file that corresponds to the provisionable server. Then, retry the add command.

Additionally, adding the OS monitoring feature to a server that has the base management feature might fail. The following job output shows the error: Repeat attempts for this operation are not allowed. This error indicates that SSH

credentials have previously been supplied and cannot be altered. To avoid this error, issue the `add server feature osmonitor` command without `agentssh` credentials. See [“To Add the OS Monitoring Feature” on page 85](#) for instructions.

```
N1-ok> show job 61
Job ID: 61
Date: 2005-08-16T16:14:27-0400
Type: Modify OS Monitoring Support
Status: Error (2005-08-16T16:14:38-0400)
Owner: root
Errors: 1
Warnings: 0

Steps
ID Type Start Completion Result
1 Acquire Host 2005-08-16T16:14:27-0400 2005-08-16T16:14:28-0400 Completed
2 Run Command 2005-08-16T16:14:28-0400 2005-08-16T16:14:28-0400 Completed
3 Acquire Host 2005-08-16T16:14:29-0400 2005-08-16T16:14:30-0400 Completed
4 Run Command 2005-08-16T16:14:30-0400 2005-08-16T16:14:36-0400 Error

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

OS Update Problems

This section describes possible solutions for the following troubleshooting scenarios:

- [“OS Update Creation Failures” on page 197](#)
- [“OS Update Deployment Failures” on page 198](#)

OS Update Creation Failures

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

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

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

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

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

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

For Solaris packages, a response file might also be needed. For instructions on how to specify an admin file and a response file when you create an OS update, see [“To Copy an OS Update” on page 91](#).

OS Update Deployment Failures

This section describes troubleshooting scenarios and possible solutions for the following categories of failures:

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

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

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

Always check the package is targeted to the correct architecture. The N1 System Manager does not distinguish 32-bit from 64-bit for the Solaris (x86 or SPARC) OS, so the package or patch might not install successfully if it is installed on an incompatible OS. If the package or patch does install successfully, but performance decreases, check that the architecture of the patch matches the architecture of the OS.

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

Target server is not initialized

Solution: Check that the add server feature `osmonitor` command was issued and that it succeeded.

Another running job on the target server

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

Update is incompatible with operating system on target server

Solution: Check that the OS type of the target server matches one of the update OS types. Type `show update update-name` at the `N1-ok>` prompt to view the OS type for the update.

Target server is not in a good state or is powered off

Solution: Check that the target server is up and running. Type `show server server-name` at the `N1-ok>` prompt to view the server status. Type `reset server server-name force` to force a reboot.

The following are possible causes for Load Update job failures:

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

error: Failed dependencies:

A prerequisite package and should be installed.

Solution: Use an RPM tool to address and resolve Linux RPM dependencies. For a Solaris system, configure the `idepend=` parameter in the `admin` file.

Preinstall or postinstall scripts failure: Non-zero status

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

Solution: Check the pre-installation or post installation scripts for possible errors to resolve this error.

Interactive request script supplied by package

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

patch-name was installed without backing up the original files

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

Insufficient disk space

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

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

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

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

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

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

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

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

Removal of <SUNWssmu> was suspended (interaction required)

Solution: This message indicates a failed dependency for uninstalling a Solaris package. Check the admin file setting and provide an appropriate response file.

Job step failure without error details

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

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

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

To manually install an RPM, type the following command:

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

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

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

To manually install a patch, type the following command:

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

Then, run the `unload` command again.

Job hangs

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

To manually kill the job, type the following command:

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

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


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

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

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

Then run the `unload` command again.

Downloading V20z and V40z Server Firmware Updates

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

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

- Steps**
- 1. Log in as root to the N1 System Manager management server.**
The `N1-ok` prompt appears.
 - 2. Create directories into which the V20z and V40z firmware update zip files are to be saved.**
Create separate directories for each server type firmware download. For example:

```
# mkdir V20z-firmware V40z-firmware
```
 - 3. In a web browser, go to <http://www.sun.com/servers/entry/v20z/downloads.html>.**
The Sun Fire V20z/V40z Server downloads page appears.
 - 4. Click Current Release.**
The Sun Fire V20z/V40z NSV Bundles 2.3.0.11 page appears.
 - 5. Click Download.**
The download Welcome page appears. Type your username and password, and then click Login.
The Terms of Use page appears. Read the license agreement carefully. You must accept the terms of the license to continue and download the firmware. Click Accept and then click Continue.

The Download page appears. Several downloadable files are displayed.

6. **To download the V20z firmware zip file, click V20z BIOS and SP Firmware, English (nsv-v20z-bios-fw_V2_3_0_11.zip).**

Save the 10.21-Mbyte file to the directory that you created for the V20z firmware in Step 2.

7. **To download the V40z firmware zip file, click V40z BIOS and SP Firmware, English (nsv-v40z-bios-fw_V2_3_0_11.zip).**

Save the 10.22-Mbyte file to the directory you created for the V40z firmware in Step 2.

8. **Change to the directory where you downloaded the V20z firmware file.**

- a. **Type `unzip` to unpack the file.**

Type **y** to continue.

The `sw_images` directory is extracted.

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

- Service Processor:
`sw_images/sp/spbase/V2.3.0.11/install1.image`
- BIOS
`sw_images/platform/firmware/bios/V2.33.5.2/bios.sp`

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

- a. **Type `unzip nsv-v40z-bios-fw_V2_3_0_11.zip` to unpack the zip file.**

The `sw_images` directory is extracted.

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

- Service Processor:
`sw_images/sp/spbase/V2.3.0.11/install1.image`
- BIOS:
`sw_images/platform/firmware/bios/V2.33.5.2/bios.sp`

- Next Steps**
- Copy the firmware updates to the N1 System Manager as described in [“To Copy a Firmware Update” on page 99](#).
 - Update the firmware on a single server or server group provisionable server as described in [“To Load a Firmware Update on a Server or a Server Group” on page 101](#).

Handling Threshold Breaches

If a threshold value is breached for a monitored attribute, an event is generated. You can create notification rules to warn you about this type of event. Notification of threshold breaches or warnings is done through the event log. This log is most easily viewed through the browser interface.

Notifications can be created using the `create notification` command and the resulting notification sent by email or to a pager. See “create notification” in *Sun N1 System Manager 1.1 Command Line Reference Manual* for syntax details.

Identifying Hardware and OS Threshold Breaches

If the value of a monitored hardware health attribute, or OS resource utilization attribute breaches a threshold value, an event log indicates that the threshold has been breached. The event log becomes available from the browser interface. The length of time it takes for the event log to be available from the browser interface depends on the polling interval for the attribute:

$t + \text{polling interval}$

The time at which the breach occurs is indicated by t . The polling interval is in seconds, and is the amount of time between successive polls of the monitored attribute. See “[Setting Polling Intervals](#)” on page 158 for more information. Use the `show log` command to verify that the event log has been generated:

```
N1-ok> show log
Id          Date          Severity    Subject      Message
.
.
10          2004-11-22T01:45:02-0800  WARNING    Sun_V20z_XG041105786
A critical high threshold was violated for server Sun_V20z_XG041105786: Attribute cpu0.vtt-s3 Value 1.32

13          2004-11-22T01:50:08-0800  WARNING    Sun_V20z_XG041105786
A normal low threshold was violated for server Sun_V20z_XG041105786: Attribute cpu0.vtt-s3 Value 1.2
```

Identifying Network Connectivity Failure

If the IP addresses of the management server, monitoring agent or the data network are unavailable, an event indicates that there is a network connectivity problem. This is part of network reachability monitoring. See “[Network Reachability Monitoring](#)” on page 141 for more information. The event log becomes available from the browser interface. The length of time it takes for the event log to be available from the browser interface depends on the polling interval for the attribute:

$t + \text{polling interval}$

The time at which the breach occurs is indicated by t . The polling interval is in seconds, and is the amount of time between successive polls of the monitored attribute. See [“Setting Polling Intervals” on page 158](#) for more information. Use the `show log` command to verify that the event log has been generated:

```
N1-ok> show log
.
.
13      2004-11-19T10:24:33-0800    INFORMATION    Sun_V20z_XGserial_number
Ip Address /<ip_address> on server Sun_V20z_XGserial_number is unreachable.

14      2004-11-19T10:24:38-0800    INFORMATION    Sun_V20z_XGserial_number
Ip Address /<ip_address> on server Sun_V20z_XGserial_number is unreachable.
```

Identifying Monitoring Failure

If monitoring is enabled, as described in [“Enabling Monitoring” on page 142](#), and the status in the output of the `show server` or `show group` commands is `unknown` or `unreachable`, then the server or server group is not being reached successfully for monitoring. If the status remains `unknown` or `unreachable` over the duration of less than five polling intervals, it is possible that a transient network problem is occurring. However if the status remains `unknown` or `unreachable` over the duration of more than five polling intervals, it is possible that monitoring has failed. This could be the result of a failure in the monitoring agent.

A time stamp is provided in the monitoring data output. The relationship between this time stamp and the value of the polling interval can also be used to judge if there is an error with the monitoring agent. If the monitored output for a provisionable server continues to show the same timestamp, even after several polling intervals have passed, this indicates that the provisionable server has not been successfully polled, and is no longer being monitored. This could be the result of a failure in the monitoring agent.

Index

A

- accessing
 - browser interface features, 26-27
 - N1 System Manager interfaces
 - browser interface, 26-27
 - command line, 25-26
 - overview, 23-29
- actions menu, supported server actions, 111
- adding
 - OS management features, 85-87
 - privileges to roles, 40
 - roles to users, 37
 - scripts to OS profiles, 192-193
 - server notes, 118-119
 - servers to groups, 55
 - users, 35

B

- base management feature, enabling, 84-85
- booting, servers, 120-121
- browser interface, accessibility features, 26-27

C

- cabling servers, 47
- changing, roles, 27-28
- cloning, OS profiles, 76-77
- command line
 - exiting, 28

command line (Continued)

- servers
 - showing failed power state, 115
- commands, `show job`, 164
- configuring, security policies, 33-34
- connectivity, troubleshooting, 203-204
- copying
 - firmware updates, 99-101
 - flash archive files, 69-70
 - OS distributions
 - CD or DVD, 67-68
 - ISO, 66-67
 - OS updates, 91-93
- creating
 - notifications, 177
 - overview, 175-179
 - OS profiles, 74-76
 - roles, 39
 - server groups, 54
- critical threshold values, 147
- customizing, script files, 28-29

D

- default credentials
 - V20z and V40z server, 48
 - V210, V240, and V440 server, 48
 - X4100 and X4200 server, 48
- deleting
 - firmware updates, 104-105
 - groups, 136
 - jobs, 169-172

- deleting (Continued)
 - notifications, 178
 - OS distributions, 71
 - OS updates, 96
 - roles, 39
 - servers, 136
 - users, 35-36
- deleting privileges, See removing, 40
- deleting roles, See removing, 37
- disabling monitoring, 145
- discovering, servers, 49-53

E

- enabling, base management feature, 84-85
- enabling monitoring, 142-146
- event logs, viewing, 173-174
- events, 139, 147
 - filtering, 174
 - managing, 172-175
 - viewing details, 174-175
- exiting
 - N1 System Manager
 - command line, 28

F

- filtering, events, 174
- finding, servers, 135
- firmware management overview, 98-105
- firmware updates
 - copying, 99-101
 - deleting, 104-105
 - installing, 101-103
 - listing, 103-104
 - modifying, 104
- flash archive files, copying, 69-70
- flash archives, managing, 66

G

- groups
 - deleting, 136
 - viewing members, 115

H

- hardware, 110
- hardware health state definitions, 110

I

- installing
 - OS updates, 93-95
 - See loading, 81-84

J

- jobs
 - deleting, 169-172
 - listing, 165-166
 - management overview, 163-172
 - stopping, 167-169
 - viewing details, 166-167

L

- listing
 - firmware updates, 103-104
 - jobs, 165-166
 - OS profiles, 74
 - OS updates, 95
 - privileges, 41
 - roles, 40, 41
 - roles for users, 37-38
 - server groups, 111-112
 - servers, 111-112
- loading, OS profiles, 81-84
- locator LED, 135

M

- management server, 60
 - operating system, 60
 - requirements, 60
- managing
 - events, 172-175
 - flash archives, 66
 - jobs
 - overview, 163-172

- managing (Continued)
 - roles
 - quick reference, 38-41
 - user security, 29-34
 - users
 - quick reference, 34-38
- MIB, 163
- modifying
 - firmware updates, 104
 - notifications, 176-177
 - OS profiles, 77-78
 - for K2 motherboards, 192-193
 - V40z partitions, 191-192
- monitored attributes, 138
- monitoring
 - disabling, 145
 - enabling, 142-146
 - handling threshold breaches, 203-204
 - hardware health, 139-140
 - introduction, 138-142
 - network reachability, 141-142
 - OS resource utilization, 140-141
 - troubleshooting network
 - connectivity, 203-204

N

- N1 System Manager
 - accessing interfaces, 23-29
 - server requirements, 60
- n1sh shell
 - accessing, 23-29
 - exiting, 28
- network booting, 122
- network connectivity, troubleshooting, 203-204
- nonrecoverable threshold values, 147
- notifications
 - creating, 177
 - deleting, 178
 - modifying, 176-177
 - overview, 175-179
 - starting, 179
 - stopping, 179
 - using topics, 175
 - viewing details, 176
 - viewing list, 175

O

- operating systems
 - installation introduction, 57-61
 - managing distributions, 66
 - requirements, 60
- OS distributions
 - copying
 - CD or DVD, 67-68
 - ISO, 66-67
 - deleting, 71
 - overview, 66
 - updating
 - Solaris 9 x86, 185-187, 187-190
- OS installation management overview, 79-84
- OS management features, adding, 85-87
- OS profile management overview, 71-79
- OS profiles
 - adding scripts for driver
 - installation, 192-193
 - cloning, 76-77
 - creating, 74-76
 - installation parameters, 80
 - listing, 74
 - loading, 81-84
 - modifying, 77-78
 - V40z partitions, 191-192
 - modifying for K2 motherboard, 192-193
 - using default settings, 72-73
- OS update management overview, 89-97
- OS updates
 - copying, 91-93
 - deleting, 96
 - listing, 95
- OS usage state definitions, 110

P

- patching
 - See updating, 185-187, 187-190
- polling intervals, 158-162
 - factory configured defaults, 159
 - modifying defaults, 160-161
 - setting, 161
- power state definitions, 110
- privileges, 31-33
 - listing, 41

- provisionable server
 - operating systems, 60
 - requirements, 60

R

- Red Hat, requirements, 60
- refreshing
 - server groups, 134-135
 - servers, 134-135
- regenerating, common agent container security strings, 181-183
- remote commands
 - servers, 127-130
 - stopping, 168-169
- removing
 - privileges from roles, 40
 - roles from users, 37
 - See deleting, 96
 - servers, 55
- renaming
 - server groups, 117
 - servers, 117
- replacing, servers, 56
- requirements
 - management server, 60
 - operating systems, 60
 - provisionable server, 60
- resetting
 - server groups, 125-126
 - servers, 125-126
- resetting servers, 126
- roles
 - adding privileges, 40
 - adding to users, 37
 - changing, 27-28
 - creating, 39
 - default settings, 30
 - deleting, 39
 - listing, 40, 41
 - listing for users, 37-38
 - removing from users, 37
 - removing privileges, 40
 - SecurityAdmin description, 30
 - setting defaults, 36
 - viewing, 27
 - viewing defaults, 36-37

- running, command line scripts, 28-29

S

- screen reader support, 26-27
- script files, customizing, 28-29
- scripting, commands, 28-29
- scripts, adding to OS profiles for driver installation, 192-193
- security
 - configuration policies, 33-34
 - privileges, 31-33
- security overview, 29-34
- security strings, regenerating for common agent container, 181-183
- SecurityAdmin, role description, 30
- server administration overview, 107-111
- server groups
 - creating, 54
 - installing OS profiles, 81-84
 - listing, 111-112
 - rebooting from network, 126
 - refreshing, 134-135
 - renaming, 117
 - resetting, 125-126
 - stopping, 122-123
 - uninstalling OS management features, 96-97
 - uninstalling OS monitoring, 88-89, 89
 - uninstalling OS updates, 97
- server name, 110
- servers
 - adding notes, 118-119
 - adding to groups, 54, 55
 - booting, 120-121
 - cabling, 47
 - deleting, 136
 - discovering, 49-53
 - finding in a rack, 135
 - health state definitions, 110
 - illuminating locator LED, 135
 - installing firmware updates, 101-103
 - installing OS profiles, 81-84
 - installing OS updates, 93-95
 - listing, 111-112
 - listing firmware updates, 104
 - listing installed OS updates, 96

- servers (Continued)
 - management server
 - requirements, 60
 - power state definitions, 110
 - provisionable server
 - requirements, 60
 - rebooting from network, 126
 - refreshing, 134-135
 - removing from groups, 55
 - renaming, 117
 - replacing, 56
 - requirements, 60
 - resetting, 125-126
 - running remote commands, 127-130
 - starting, 120-121
 - stopping, 122-123
 - supported actions, 111
 - supported operating systems, 58
 - uninstalling OS monitoring, 88-89, 89
 - uninstalling OS updates, 96-97
 - viewing details, 115
 - viewing failed, 113-115
- setting, default roles, 36
- show job, command description, 164
- showing, See viewing, 36-37
- SNMP, 138, 163, 175
- Solaris, requirements, 60
- starting
 - notifications, 179
 - servers, 120-121
- stopping
 - jobs, 167-169
 - notifications, 179
 - remote commands, 168-169
 - server groups, 122-123
 - servers, 122-123
- stopping servers
 - force, 124
- SUSE, requirements, 60
- switching, See changing, 27-28

T

- threshold values, 147-158
 - managing defaults, 148-152
 - retrieving for a server, 148
 - setting, 156-158

- thresholds, handling breaches, 203-204
- troubleshooting, 181-204
 - threshold breaches, 203-204
 - V20z or V40z server, default credentials, 48
 - V210, V240, or V440 server, default credentials, 48
 - X4100 or X4200 server, default credentials, 48

U

- UNIX commands, 127-130
- unloading, 96-97
- updating
 - Solaris 9 x86 OS distributions, 185-187, 187-190
- user role descriptions, 30
- user roles
 - adding privileges, 40
 - creating, 39
 - deleting, 39
 - listing, 37-38, 40, 41
 - listing privileges, 41
 - removing privileges, 40
- users
 - adding, 35
 - deleting, 35-36
 - managing, 29-34
- using, default roles, 30

V

- V20z and V40z server, default credentials, 48
- V210, V240, and V440 server, default credentials, 48
- viewing
 - default roles, 36-37
 - event details, 174-175
 - event logs, 173-174
 - failed servers, 113-115
 - group members, 115
 - job details, 166-167
 - jobs, 165-166
 - notification details, 176
 - notifications, 175
 - roles, 27

viewing (Continued)
server details, 115

W

warning threshold values, 147

X

X4100 and X4200 server, default credentials, 48