Sun Open Telecommunications Platform 1.1 Installation and Administration Guide

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

Part No: 820–1134
July 2007

070726@18135

Contents

Figures

Tables

Preface

The *Sun Open Telecommunications Platform 1.1 Installation and Administration Guide* describes the requirements for installing and configuring the Sun Open Telecommunications Platform (OTP) software on your OTP system.

Who Should Use This Book

This guide is intended for system administrators who are responsible for installing the Open Telecommunications Platform hardware and software. The system administrators must have extensive knowledge and experience in the following areas:

- The Solaris™ operating systems and the network administration tools provided by the Solaris operating system
- DNS, DHCP, IP addressing, subnetworks, VLANs, SNMP, TFTP, and NFS

How This Book Is Organized

- Chapter 1, "Sun Open Telecommunications Platform Introduction" provides an overview of the Open Telecommunications Platform and a summary of the installation process.
- Chapter 2, "Sun Open Telecommunications Platform Hardware and Software Requirements" provides the hardware and software requirements, and provides descriptions of the settings and worksheets for the settings needed for installation and configuration.
- Chapter 3, "Preparing Servers for Open Telecommunications Platform Installation" provides the procedures for installing and configuring the operating system on the external OTP installation server, and on the servers selected for the Open Telecommunications Platform system.
- Chapter 4, "Installing the Open Telecommunications Platform For the First Time Using the Command Line" provides the procedures for using the external OTP installation server and the command line interface to install the Open Telecommunications Platform on the servers selected for the Open Telecommunications Platform system.

- Chapter 5, "Installing the Open Telecommunications Platform For the First Time Using the Graphical User Interface" provides the procedures for using the external OTP installation server and the graphical user interface to install Open Telecommunications Platform on the servers selected for the Open Telecommunications Platform system.
- Chapter 6, "Installing the Open Telecommunications Platform Using the Provisioning Service On an Existing OTP System" provides the procedures for using an existing production OTP System provisioning service to install and configure OTP on a new standalone OTP host or a new clustered OTP system.
- Chapter 7, "Installing the Open Telecommunications Platform Using the System Management Service On an Existing OTP System" provides the procedures for using an existing production OTP System system management service to install and configure OTP on a new standalone OTP host or a new clustered OTP system.
- Chapter 8, "Backing Up and Restoring the OTP Provisioning Service and the OTP System Management Service" provides the procedures for backing up and restoring the OTP system management service and theOTP provisioning service database and configuration files.
- Chapter 9, "Open Telecommunications Platform Administration" provides the procedures for enabling and disabling the OTP system management service and application provisioning service. It also provides procedures for adding a host to the existing cluster, repairing a host in the cluster, converting a node from standalone configuration to multinode configuration.
- Appendix A, "Application Programming Interfaces and Protocols" lists the application programming interfaces (APIs) and protocols you can use for application development.
- Glossary provides definitions of Open Telecommunications Platform terms.

Product Documentation

This guide is part of a two-volume implementation reference set. Read the release notes and the installation guide before installing the Open Telecommunications Platform.

- *Sun Open Telecommunications Platform 1.1 Release Notes*
- Sun Open Telecommunications Platform 1.1 Installation and Administration Guide

Related Documentation

- Solaris 10 1/06 Release and Installation Documentation (`http://docs.sun.com/app/docs/coll/1236`)
- Sun Cluster 3.1 Update 4 Software Collection for Solaris OS, SPARC Platform Edition (`http://docs.sun.com/app/docs/coll/1124.4`)
- Sun N1 System Manager 1.3.2 (`http://docs.sun.com/app/docs/coll/1283.6`)
- Sun N1 Service Provisioning System 5.2.4 (`http://docs.sun.com/app/docs/coll/1119.6`)

- *Sun N1 Service Provisioning System User's Guide for OS Provisioning Plug-In 3.1*

Before You Read This Book

Before reading this book, you should read the *Sun Open Telecommunications Platform 1.0 Release Notes* and be familiar with the general design of OTP software.

Accessing Sun Resources Online

The docs.sun.com web site enables you to access Sun technical documentation online. You can browse the docs.sun.com archive or search for a specific book title or subject. Books are available as online files in PDF and HTML formats. Both formats are readable by assistive technologies for users with disabilities.

To access the following Sun resources, go to `http://www.sun.com`:

- Downloads of Sun products
- Services and solutions
- Support (including patches and updates)
- Training
- Research
- Communities (for example, Sun Developer Network)

Accessibility Features for People With Disabilities

To obtain accessibility features that have been released since the publishing of this media, consult Section 508 product assessments available from Sun upon request to determine which versions are best suited for deploying accessible solutions.

For information on Sun's commitment to accessibility, visit http://sun.com/access (`http://sun.com/access`).

Related Third-Party Web Site References

Third-party URLs are referenced in this document and provide additional, related information.

Note – Sun is not responsible for the availability of third-party web sites mentioned in this document. Sun does not endorse and is not responsible or liable for any content, advertising, products, or other materials that are available on or through such sites or resources. Sun will not be responsible or liable for any actual or alleged damage or loss caused or alleged to be caused by or in connection with use of or reliance on any such content, goods, or services that are available on or through such sites or resources.

Sun Welcomes Your Comments

Sun is interested in improving its documentation and welcomes your comments and suggestions. To share your comments, go to `http://docs.sun.com` and click Send Comments. In the online form, provide the full document title and part number. The part number is located on the book's title page and in the document's URL. For example, the name of this book is Sun Open Telecommunications Platform Installation and Administration Guide, and the part number of this book is 819–7370.

Documentation, Support, and Training

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

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

Typographic Conventions

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

TABLE P–1 Typographic Conventions

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

TABLE P–1 Typographic Conventions *(Continued)*

Typeface	Meaning	Example
aabbcc123	Placeholder: replace with a real name or value	The command to remove a file is `rm` *filename*.
AaBbCc123	Book titles, new terms, and terms to be emphasized	Read Chapter 6 in the *User's Guide*. A *cache* is a copy that is stored locally. Do *not* save the file. **Note:** Some emphasized items appear bold online.

Shell Prompts in Command Examples

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

TABLE P–2 Shell Prompts

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

◆ ◆ ◆ CHAPTER 1

Sun Open Telecommunications Platform Introduction

This chapter provides an overview of Open Telecommunications Platform (OTP) features and components, and a high-level summary of the steps required to install the Open Telecommunications Platform.

The following topics are discussed:

Open Telecommunications Platform Features

The Open Telecommunications Platform OTP provides integrated high availability services, system management services , and operating system and application provisioning services that enable you to develop, deploy, and host network equipment provider (NEP) applications. The Open Telecommunications Platform is comprised of the following software components:

OTP system management service	The OTP system management service is used to provision the OS to OTP hosts, and to manage the OTP hardware, the operating systems running on the OTP hardware, and the firmware necessary for hardware operation. The management software is comprised of operational elements and administrative elements.
OTP application provisioning service	The OTP application provisioning service is used to provision network equipment provider (NEP) applications. OTP application provisioning service can also be used to provision the OS to OTP hosts.
OTP high availability framework	The OTP high availability framework is used to manage OTP system membership, interconnects,

networking quorums and highly available OTP deployments.

The Open Telecommunications Platform enables you to perform the following tasks:

- Discover additional OTP hosts that are to be managed and provisioned by the Open Telecommunications Platform system. Once discovered, each new host is known as an *OTP host.*
- Provision operating systems to OTP hosts.
- Provision NEP applications and other applications to OTP hosts.
- Provision firmware and patches to OTP hosts.
- Monitor the health of OTP hosts.
- Simplify OTP host configuration and recovery.
- Maximize OTP host utilization
- Minimize user-visible hardware downtime.
- Log system and OTP host events.

Open Telecommunications Platform Hardware Components

The following figure provides a high-level overview of the hardware components of the Open Telecommunications Platform.

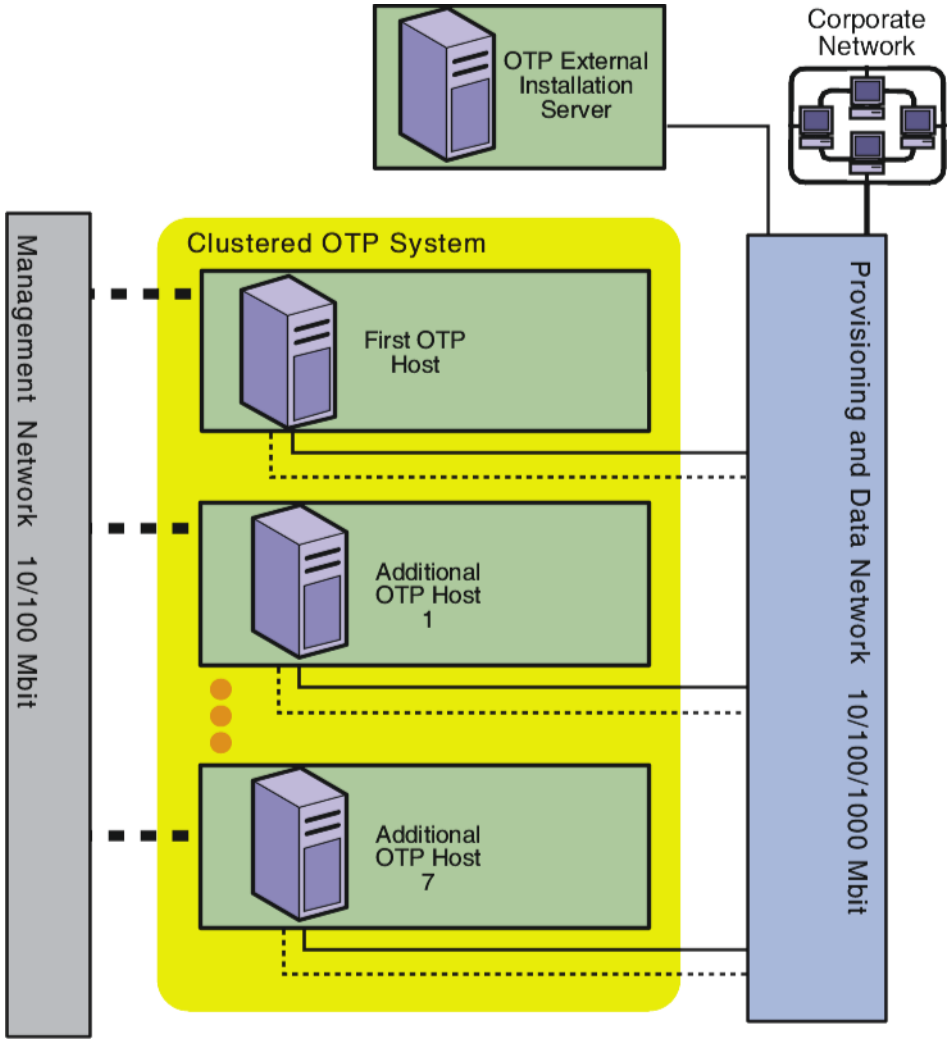

FIGURE 1–1 Open Telecommunications Platform Architecture

10/100 Mbit Ethernet minimum is required by the management network. 10/100/1000 Mbit Ethernet is required by the provisioning and the data networks.

The above diagram represents one of the possible clustered OTP system configurations. In a standalone OTP host configuration, only the first OTP host is present.

The following list describes each of the Open Telecommunications Platform components.

- External OTP installation server

  A non-clustered server that is used to install the Open Telecommunications Platform software for the first time to an OTP host.

- First OTP host

  The first host in a clustered OTP system on which the Open Telecommunications Platform is installed. A standalone OTP host is comprised only of the first OTP host.

- Additional OTP hosts

  One or more secondary hosts within a clustered OTP system that provide high availability. Additional OTP hosts are managed and monitored using the OTP high availability framework and the OTP system management service. Network Equipment Provider (NEP) applications can be provisioned to the OTP hosts using the OTP application provisioning service.

Open Telecommunications Platform Installation Summary

Installation of the Open Telecommunications Platform is comprised of the following major steps.

- **Site preparation**

  Ensure that your equipment meets the requirements listed in "OTP System Hardware and Firmware Requirements" on page 25.

- **Record your Open Telecommunications Platform Plan information**

  Use the worksheets provided in "Open Telecommunications Platform Plan Worksheets" on page 30 for each host to record the information that is applied by the Open Telecommunications Platform installation and configuration process. Plan information includes items such as management and provisioning interface ports, IP addresses for each OTP host, the clustered OTP system name, IPMP options, and more. Using the worksheets will assist you during installation and configuration, and reduce the chance for errors.

- **Install the operating system on each server**.

  Install and configure the Solaris 10 Update 2 operating system on external OTP installation server and on the servers selected for the Open Telecommunications Platform system as described in Chapter 3, "Preparing Servers for Open Telecommunications Platform Installation."

- Set up the external OTP installation server

  The external OTP installation server must be set up as described in "Setting Up the External OTP Installation Server" on page 44 before you can use the server to install the Open Telecommunications Platform for the first time.

- **Install the Open Telecommunications Platform to the OTP systems**. If you are installing the Open Telecommunications Platform for the first time, use either of the following two methods:
  - Install the Open Telecommunications Platform using the external OTP installation server and the command line as described in Chapter 4, "Installing the Open Telecommunications Platform For the First Time Using the Command Line."
  - Install the Open Telecommunications Platform using the external OTP installation server and the graphical user interface (GUI) installation as described in Chapter 5, "Installing the Open Telecommunications Platform For the First Time Using the Graphical User Interface."

  If you have already installed the Open Telecommunications Platform to a standalone OTP host or to a clustered OTP system, you can use a production OTP system to using install the Open Telecommunications Platform to a new OTP host as follows:
  - Install the Open Telecommunications Platform using the OTP provisioning service as described in Chapter 6, "Installing the Open Telecommunications Platform Using the Provisioning Service On an Existing OTP System."
  - Install the Open Telecommunications Platform using the OTP system management service as described in Chapter 7, "Installing the Open Telecommunications Platform Using the System Management Service On an Existing OTP System."

◆ ◆ ◆ CHAPTER 2

Sun Open Telecommunications Platform Hardware and Software Requirements

This chapter provides the Open Telecommunications Platform hardware and software requirements, and the Open Telecommunications Platform plan worksheets that can assist you during installation. The information in this section will help you determine what operating system, hardware, and storage resources must be allocated or acquired to implement the Open Telecommunications Platform system.

This chapter discusses the following topics:

OTP System Hardware and Firmware Requirements

The following table lists the hardware, OS, patch, and firmware requirements for OTP system servers, and for the optional external OTP installation server.

TABLE 2–1 OTP System Server Hardware, Operating System, Patch, and Firmware Requirements

Type	Management Port	OS	Patch	Firmware
Netra™ 240	ALOM	Solaris 10 Update 2, 64 bit	121683-04	OBP 4.22.23, POST 4.22.23, OBDIAG 4.22.23
Netra 440	ALOM	Solaris 10 Update 2, 64 bit	121685-02	OBP 4.22.19, POST 4.22.19, OBDIAG 4.22.19
Sun Fire™ V215	ALOM	Solaris 10 Update 2, 64 bit	121692-02	OBP 4.22.22, POST 4.22.22, OBDIAG 4.22.22

TABLE 2–1 OTP System Server Hardware, Operating System, Patch, and Firmware Requirements *(Continued)*

Type	Management Port	OS	Patch	Firmware
Sun FireV240	ALOM	Solaris 10 Update 2, 64 bit	121683-04	OBP 4.22.23, POST 4.22.23, OBDIAG 4.22.23
Sun Fire V245	ALOM	Solaris 10 Update 2, 64 bit	121692-02	OBP 4.22.22, POST 4.22.22, OBDIAG 4.22.22
Sun Fire V440	ALOM	Solaris 10 Update 2, 64 bit	121685-02	OBP 4.22.19, POST 4.22.19, OBDIAG 4.22.19
Sun Fire V445	ALOM	Solaris 10 Update 2, 64 bit	121690-03, 123485-01	OBP 4.22.24, POST 4.22.24, OBDIAG 4.22.24, 1.0.39
Sun Fire V490	RSC	Solaris 10 Update 2, 64 bit		
Sun Fire V890	RSC/ALOM	Solaris 10 Update 2, 64 bit	121688-01	OBP 4.22.19, POST 4.22.19, OBDIAG 4.22.19
Sun Fire T2000	ALOM	Solaris 10 Update 2, 64 bit	124750-03	Sun System Firmware 6.3.2

Note –

- The OTP Application Hosting Environment (AHE) components are supported only on these platforms for Network Equipment Providers' (NEP) application development or deployment, or for both.
- The Open Telecommunications Platform supports one to eight-host clusters. At least one shared disk is mandatory for installing the Open Telecommunications Platform on a two to eight-host cluster.

The following table lists the minimum OTP system server requirements. Ensure that the external OTP installation server meets the following partitioning requirements as well.

TABLE 2–2 OTP System Server RAM, Disk, and Connectivity Requirements

Category	Requirement
Minimum physical memory	4 GB

TABLE 2–2 OTP System Server RAM, Disk, and Connectivity Requirements *(Continued)*

Category	Requirement
Minimum disk space	External OTP installation server: 32 Gbytes OTP host: 72 GBytes
Ethernet connectivity for management interfaces	10/100 connection
Ethernet connectivity for provisioning and data interfaces	10/100/1000 connection

The following table lists the supported storage hardware and NIC devices by server type.

TABLE 2–3 OTP System Supported Storage Hardware and NIC Devices

Server	Storage	NIC
Netra 240 and 440	FC 3510	On-board GE
	FC 3511	X4445A QGE
	SCSI 3120 JBOD	X4150A-2 2 GE
	SCSI 3310 JBOD	X4150A GE
	SCSI 3320 JBOD	X4422A-2 combo
	SCSI 3310 RAID	
	SCSI 3320 RAID	
Sun Fire V215	FC 3310	On-board GE
	FC 3320	X4445A QGE
	FC 3510	
	FC 6130	
	SCSI 3320	
Sun Fire V245	FC 3510	On-board GE
	FC 3511	X4445A QGE
	FC 6130	
	SCSI 3120	
	SCSI 3310	
	SCSI 3320	

TABLE 2–3 OTP System Supported Storage Hardware and NIC Devices *(Continued)*

Server	Storage	NIC
Sun Fire V240, V440, and V890	FC 3510	On-board GE
	FC 3511	X4445A QGE
	FC 6130	X4150A-2 GE
	SCSI 3310 JBOD	X4150A GE
	SCSI 3120 JBOD	X4422A-2 combo
	SCSI 3320 JBOD	
	SCSI 3310 RAID	
	SCSI 3320 RAID	
Sun Fire V445	FC 3510	On-board GE
	FC 3511	X4445A QGE
	SCSI 3320	
Sun Fire V490	FC 6130	On board GE
	FC 3511	X4422A Combo
	FC 3510	
	SCSI 3320	
	SCSI 3120	
Sun Fire T2000	FC 3510	On-board GE (e1000g driver)
	FC 3511	X4150A-2 2 GE
	FC 6130	X4150A GE
	SCSI 3120 JBOD	
	SCSI 3310 JBOD	
	SCSI 3310 RAID	

The following table lists the storage device firmware requirements.

TABLE 2–4 OTP System Storage Device Firmware Requirements

Type	Patch	Requirement
FC StorEdge™ 3510	RAID 113723-15, JBOD 113662-01	Version 2.3 of the sccli CLI utility must be installed first.

TABLE 2–4 OTP System Storage Device Firmware Requirements *(Continued)*

Type	Patch	Requirement
FC StorEdge 3511	113724-09	Version 2.3 of the sccli CLI utility must be installed first.
SCSI StorEdge 3120	113728-02 Array Controller Firmware	Version 2.3 of the sccli CLI utility must be installed first.
SCSI StorEdge 3310	113722-15	Version 2.3 of the sccli CLI utility must be installed first.
SCSI StorEdge 3320	113730-01	Version 2.3 of the sccli CLI utility must be installed first.
FC StorEdge 6130	118185-15 6130 services Release, 117856-19 6130 Baseline Firmware Release	StorEDGE 6130 Array Firmware Upgrader patch 118185-15 must be installed first.

Note – The `sccli CLI utility` is included in the `SUNWsscs` package which can be downloaded from the Sun Download Center. The `sccli CLI utility` can also be installed from the optional Sun StorEdge Professional Storage Manager CD.

OTP System Server Considerations

Hard drive capacity and the number of OTP hosts to be managed are the primary considerations for your OTP system.

- Hard drive capacity is affected by three factors: the number of OS distributions that are to be provisioned, the management log files generated by Open Telecommunications Platform components, and the size of the applications to be provisioned.
  - If you are using the OTP system management service to provision OS distributions, the OS distributions are stored in the `/var/js` file hierarchy on the first OTP host
  - If you are using the OTP application provisioning service to provision OS distributions, the OS distributions are stored in the `/var/otp` file hierarchy on the first OTP host
- System processing is affected by three major factors: The number of additional OTP hosts being managed, the types of monitoring being performed on the additional OTP hosts, and the number of jobs running on the first OTP host.

Open Telecommunications Platform Plan Worksheets

This section provides a description of the Open Telecommunications Platform settings, and provides worksheets to assist you with recording the settings you need to provide when installing the Open Telecommunications Platform on one or more OTP hosts. The settings comprise an installation and configuration plan, which the Open Telecommunications Platform installation process applies to automate the setup and configuration of your OTP hosts.

The following topics are discussed:

OTP System Plan Settings Descriptions

The following list describes each of the OTP system plan settings that are used by the Open Telecommunications Platform graphical user interface installation and configuration process.

- **Media Directory**

  The fully-qualified path name to the Open Telecommunications Platform installation source directory. For example:

  – `/cdrom/otp_11_dvd/otp1.1` for physical media

  – The fully qualified path name of NFS-mounted OTP installation directory on the external OTP installation server, for example: `/net/otpsource.mycompany.com/otp1.1`.

- **Cluster Name**

  The name of the clustered OTP system that is assigned to the cluster during the Open Telecommunications Platform installation and configuration process.

- **h*n* Enable Auto Configuration of IPMP** Required:

  - GUI default value: `no`, checkbox does not contain the ✓ symbol
  - CLI default value: `yes`

  Valid values: `yes`, `no`, checkbox contains a symbol, checkbox does not contain a symbol

---

Note – You should configure all physical interfaces of a multipathing group with a test IP address. Test addresses are required to detect failures.

For more information about IPMP, see *System Administration Guide: IP Services* If you set `Enable Auto Configuration of IPMP=yes`, then you must also specify the following values:

- **h*n* Secondary interface for failover**

  The name of the network adapter failover (NAFO) network adapter to be added to an IP Network Multipathing group along with the primary network adapter. This interface is used as the failover interface if a fault is detected on the primary interface. Examples: `cd1, bge1, hme1, eri1`

- **h*n* Secondary IP**

  The IP address of the secondary interface secondary IP interface that is used for failover.

- **h*n* Test Address for IPMP**

  An unused IP address that is to be assigned as a routable, no-failover, and deprecated test IP address to the adapter. IP Network Multipathing uses test addresses to detect network path failures, switch port faults, and partial network equipment outages. For additional information on configuring test IP addresses, see *System Administration Guide: IP Services*

- **h*n* Sponsoring Node**

  The name of the first OTP host in a clustered OTP system. The first OTP host is the sponsoring note for additional OTP host *n*. Required when installing the Open Telecommunications Platform on a two or more host clustered OTP system.

- **h*n* Host Name**

  The name of the additional OTP host *n* in a two host or more cluster. Required when installing the Open Telecommunications Platform on a two or more host clustered OTP system.

- **h*n* Physical IP Adddress**

  The IP address of the additional OTP host *n* in a two host or more cluster. Required when installing the Open Telecommunications Platform on a two or more host clustered OTP system.

- **h*n* Private Interface 1**

  The first physical interface on additional OTP host *n*, for example `bge0` or `ce0`.

- **h*n* Private Interface 2**

  The second physical interface on additional OTP host *n*, for example `bge1` or `ce1`.

- **h*n* Transport Type Interface 1**

  Required value is `dlpi`, do not change.

  The transport type of the first private interconnect adapter on additional OTP host *n*

- **h*n* Transport Type Interface 2**

  Required value is `dlpi`, do not change.

The transport type of the second private interconnect adapter on additional OTP host *n*

- **h*n* Quorum Auto Configuration**

Note – Quorum automatic configuration applies only to two-host clusters.

Required, default value: `yes`, checkbox selected, and contains the ✓ symbol

Valid values: `yes`, `no`, checkbox contains a symbol, checkbox does not contain a symbol

Quorum autoconfiguration provides an option to enable or disable auto configuration of the quorum device in a two-host only clustered OTP system.

Note – If this value is set to `no`, a manual administrative procedure is required to configure the quorum disk in a two-host clustered OTP system. The cluster must be manually reset from install mode to normal mode. For details on how to configure quorum disks, refer to the `scconf` command documentation in `scconf`(1M)

- **Logical Host**

  A unique host name assigned to the OTP high availability framework
- **Logical IP Address**

  An unused IP address on the same subnet as the first OTP host, assigned to the logical host
- **Install All Patches**

  Required, default value: `yes`, checkbox selected, and contains the ✓ symbol. All patches are to be installed.

  Valid values: `yes`, `no`, checkbox contains a symbol, checkbox does not contain a symbol. Only mandatory patches are to be installed.

  To install all Open Telecommunications Platform patches, specify `yes`.

  To install mandatory patches only, specify `no`.
- **Management Interface**

  The name of the network interface used for OTP system management services. The name of the interface depends on the platform type. For example:

  `bge0`, `ce0`, `cd0`, `hme0`, or `eri0`.
- **Manager Host Name**

  The name of the first OTP host in the clustered OTP system, for example, cluster01manager.
- **Manager Physical IP Address**

  The IP address of the first OTP host in the clustered OTP system.
- **Manager Node Authentication**

Required value is `sys`, do not change.

- **Manager Private Interface 1**

  The first physical interface on the OTP host, for example `bge0` or `ce0`.

- **Manager Private Interface 2**

  The second physical interface on the OTP host, for example `bge1` or `ce1`.

- **Manager Transport Type Interface 1**

  Required value is `dlpi`, do not change.

- **Manager Transport Type Interface 2**

  Required value is `dlpi`, do not change.

- **Manager Autoconfig IPMP**

  Set `managerAutoConfigureIPMP=no` if you do not want to set up IPMP. To set up IPMP, set `managerAutoConfigureIPMP=yes`, and add the following three lines:

  - `managerSecondaryInterface=`*Ethernet interface 2*, for example `bge1`
  - `managerSecondaryIPMP=`*111.112.113.114* where *111.112.113.114* is the IP address of *Ethernet interface 2*.
  - `managerTestIPAddress=`*111.112.113.222* where *111.112.113.222* is the IP address used for IPMP configuration.

- **Node Authentication**

  Required value is `sys`, do not change.

  This option establishes the authentication policies for hosts that are to be added to a clustered OTP system configuration.

- **Private Interface 1**

  The network adapter connected to private interconnect.

- **Private Interface 2**

  The network adapter connected to private interconnect.

- **Provisioning Interface**

  The name of the network interface used for operating system and applications provisioning. The name of the interface depends on the platform type. For example, `bge0`, `ce0`, `cd0`, `hme0`, or `eri0`.

- **Target Host Physical Name**

  The name to be assigned to the OTP host

- **Target Host Physical IP**

  The IP address to be assigned to the standalone OTP host.

- **Transport Type 1**

  Required value is `dlpi`, do not change.

The transport type of the private interconnect adapters.

- **Transport Type 2**

  Required value is `dlpi`, do not change.

  The transport type of the private interconnect adapters.

Standalone OTP Host Plan Worksheet

The following table lists the plan settings that you need to provide during installation and configuration of the Open Telecommunications Platform on a standalone OTP host. Plan setting names used in the graphical user interface installation are listed in **bold text**.

Tip – Print the following table and then fill out the required information to use while installing and configuring the Open Telecommunications Platform on the standalone OTP host.

TABLE 2–5 Standalone OTP Host System Settings Worksheet

Setting Name	Example	Setting Value

Media Directory (GUI)
`mediaDirectory` (CLI)
	`/cdrom/otp_11_dvd/otp1.1`
	`/net/`*external OTP installation server*`/otp1.1`
	`/otp1.1`
		_____

Target Host Physical Name (GUI) `targetHostPhysicalName` (CLI)	OTPstandalone OTPhost01	_____
Target Host Physical IP (GUI) `targetHostPhysicalIP` (CLI)		_____
Cluster Name (GUI) `clusterName` (CLI)	*standalone-cluster-name*	_____
Enable Auto Configuration of IPMP (GUI) `autoConfigureIPMP` (CLI)		❒ `yes` ❒ `no`
Secondary Interface for failover (GUI) `secondaryInterface` (CLI)	`cd1`, `bge1`, `hme1`, `eri1`	_____
Secondary IP (GUI) `secondaryIP` (CLI)		_____
Test Address for IPMP (GUI) `testIPAddress` (CLI)		_____
Logical Host (GUI) `logicalHost` (CLI)	*host–01–logical*	_____
Logical IP Address (GUI) `logicalIPAddress` (CLI)		_____
Install All Patches (GUI) `allPatches` (CLI)		❒ `yes` ❒ `no`
Management Interface (GUI) `managementInterface` (CLI)	`bge0`, `ce0`, `cd0`, `hme0`, `eri0`	_____

TABLE 2–5 Standalone OTP Host System Settings Worksheet *(Continued)*

Setting Name	Example	Setting Value
Provisioning Interface (GUI) `provisioningInterface` (CLI)	`bge0`, `ce0`, `cd0`, `hme0`, `eri0`	_____

Clustered OTP Host Plan Worksheet

The following table lists the plan settings that you need to provide for each host during installation and configuration of the Open Telecommunications Platform on a clustered OTP system. Plan setting names used in the graphical user interface installation are listed in **bold text**.

Tip – Print a copy of the following table for each host and then fill out the required information to use when installing and configuring the Open Telecommunications Platform on a clustered OTP system.

TABLE 2–6 Clustered OTP System System Settings Worksheet

Setting Name	Example	Setting Value
Media Directory (GUI) `mediaDirectory` (CLI)	`/cdrom/otp_11_dvd/otp1.1` `/net/`*external OTP installation server*`/otp1.1`	_____
Cluster Name (GUI) `clusterName` (CLI)	*otp-cluster-name*	_____
Secondary Interface for failover (GUI) `secondaryInterface` (CLI)	`cd1`, `bge1`, `hme1`, `eri1`	_____
Secondary IP (GUI) `secondaryIP` (CLI)		_____
Test Address for IPMP (GUI) `testIPAddress` (CLI)		_____
Install All Patches (GUI) `allPatches` (CLI)		❒ `yes` ❒ `no`
Enable Auto Configuration of IPMP (GUI) h*n*`_autoConfigureIPMP` (CLI)		❒ `yes` ❒ `no`
Sponsoring Node (GUI) h*n*`_sponsorNode` (CLI) This is the name that is to be assigned to the first OTP host for additional OTP host *n*.	OTPfirsthost h1_sponsorNode=OTPfirsthost … h*n*_sponsorNode=OTPfirsthost	_____
Host Name (GUI) h*n*`_hostName` (CLI) This is the name that is to be assigned to additional OTP host *n*.	OTPhost1 h1_hostName=OTPhost1 … h*n*_hostName=OTPhost*n*	_____
Physical IP Address (GUI) h*n*`_physicalIPAddress` (CLI)	*10.20.30.10* h1_physicalIPAddress=10.20.30.10 … h*n*_physicalIPAddress=10.20.30.11	_____

TABLE 2–6 Clustered OTP System System Settings Worksheet *(Continued)*

Setting Name	Example	Setting Value
Private Interface 1 h*n*_privateInterface1 (CLI)	bge0, ce0, cd0, hme0, eri0 h1_privateInterface1=bge0 … h*n*_privateInterface1=bge0	_____
Private Interface 2 h*n*_privateInterface2 (CLI)	bge1, ce1, cd1, hme1, eri10 h1_privateInterface2=bge0 … h*n*_privateInterface2=bge0	_____
Transport Type Interface 1 (GUI) h*n*_transportTypeInterface1 (CLI)	dlpi	dlpi
Transport Type Interface 2 (GUI) h*n*_transportTypeInterface2 (CLI)	dlpi	dlpi
Quorum Auto Configuration (GUI) h*n*_quorumAutoConfiguration (CLI)		❒ Default:yes ❒ no **Note –** Quorum automatic configuration applies only to two-host clustered OTP systems. If you disable quorum automatic configuration on a two-host cluster by choosing no, you must manually configure the quorum for the two-host cluster and reset the cluster configuration as described in "Installing the Open Telecommunications Platform on a Clustered OTP System" on page 127.
Logical Host (GUI) logicalHost (CLI)	*host–01–logical*	_____
Logical IP Address (GUI) logicalIPAddress (CLI)		_____
Manager Host Name (GUI) managerHostName (CLI)	*cluster01manager*	_____

TABLE 2–6 Clustered OTP System System Settings Worksheet *(Continued)*

Setting Name	Example	Setting Value
Manager Physical IP Address (GUI) `managerPhysicalIPAddress` (CLI)		_____
Manager Node Authentication (GUI) `managerNodeAuthentication` (CLI)	sys	sys
Manager Private Interface 1 (GUI) `managerPrivateInterface1` (CLI)	`bge0`, `ce0`, `cd0`, `hme0`, `eri0`	_____
Manager Private Interface 2 (GUI) `managerPrivateInterface2` (CLI)	`bge1`, `ce1`, `cd1`, `hme1`, `eri1`	_____
Manager Transport Type Interface 1 (GUI) `managerTransportTypeInterface1` (CLI)	dlpi	dlpi
Manager Transport Type Interface 2 (GUI) `managerTransportTypeInterface2` (CLI)	dlpi	dlpi
Manager Management Interface (GUI) `managerManagementInterface` (CLI)	`bge0`, `ce0`, `cd0`, `hme0`, `eri0`	_____
Manager Provisioning Interface (GUI) `managerProvisioningInterface` (CLI)	`bge0`, `ce0`, `cd0`, `hme0`, `eri0`	_____
Number of Nodes (GUI) `noOfNodes` (CLI)		_____

◆ ◆ ◆ CHAPTER 3

Preparing Servers for Open Telecommunications Platform Installation

This chapter provides the procedures for downloading and uncompressing the combined Open Telecommunications Platform (OTP) and Solaris 10 Update 2 installation image, and the procedures for installing and configuring the Solaris OS on the external OTP installation server and on theOTP host or hosts you chose for the OTP system.

Solaris 10 Update 2 must be installed and configured on the external OTP installation server and on each OTP host before you can install the Open Telecommunications Platform.

The following topics are discussed:

Note – If you have purchased the OTP installation DVD-ROM, go to "To Install Solaris 10 Update 2 on the External OTP Installation Server" on page 44.

Downloading and Uncompressing the OTP and Solaris OS Software

This section provides the procedures for downloading the Open Telecommunications Platform installation zip files and creating the Solaris 10 Update 2 OS installation image and the Open Telecommunications Platform installation directory and files.

▼ To Download and Uncompress the OTP and Solaris OS Installation Zip Files

Before You Begin The server to which you download the Open Telecommunications Platform installation zip files must be network-accessible by the external OTP installation servers and by the OTP hosts, and have at least 6 Gbytes of available free disk space

1. **Log in as root (`su - root`) to a server that is network-accessible by your OTP system.**

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

   Downloads of large files using Web browsers can sometimes fail. For this reason, use the Sun Download Manager to download the Open Telecommunications Platform installation zip files. For instructions about how to download, install, and use the Sun Download Manager, go to `http://www.sun.com/download/sdm/index.xml`.

3. **Create a directory into which the installation zip files are to be saved.**

   For example:

   ```
   # mkdir /otp-download
   ```

4. **Open a web browser and go to the Tech/OEM Web site `https://sdlc2j.sun.com/eeAdmin/AdminActionServlet?LMLoadBalanced=`. Access is password protected. Your password for the Tech/OEM site is provided at the time of the order.**

   a. **Download the following five Solaris 10 Update 2zip files to the directory you created in Step 3:**

      - `sol-10-u2-ga-sparc-dvd-iso-a.zip`
      - `sol-10-u2-ga-sparc-dvd-iso-b.zip`
      - `sol-10-u2-ga-sparc-dvd-iso-c.zip`
      - `sol-10-u2-ga-sparc-dvd-iso-d.zip`
      - `sol-10-u2-ga-sparc-dvd-iso-e.zip`

   b. **Download the following four Open Telecommunications Platform installation zip files to the directory you created in Step 8:**

      - `otp1.1.zip-a`
      - `otp1.1.zip-b`
      - `otp1.1.zip-c`

5. **Change directory to the installation directory you created in Step 3.**

6 Create the single Solaris 10 Update 2 ISO image.

a. Unzip each of the ISO image zip files.

For example:

```
# unzip sol-10-u21-ga-sparc-dvd-iso-a.zip
# unzip sol-10-u21-ga-sparc-dvd-iso-b.zip
# unzip sol-10-u21-ga-sparc-dvd-iso-c.zip
# unzip sol-10-u21-ga-sparc-dvd-iso-d.zip
# unzip sol-10-u21-ga-sparc-dvd-iso-e.zip
```

b. Concatenate the unzipped ISO files to a single ISO image.

For example:

```
# cat sol-10-u2-ga-sparc-dvd-iso-a sol-10-u2-ga-sparc-dvd-iso-b \
    sol-10-u2-ga-sparc-dvd-iso-c sol-10-u2-ga-sparc-dvd-iso-d \
    sol-10-u2-ga-sparc-dvd-iso-e > sol10u2-ga-sparc-dvd.iso
```

7 Prepare the Solaris 10 Update 2 ISO image.

Use any of the three following three methods to prepare the Solaris 10 Update 2 ISO image for installation on the each server selected for the Open Telecommunications Platform system.

- **Burn the Solaris 10 Update 2 ISO image you created to a DVD-R.**
- **Set up a JumpStart server to install Solaris 10 Update 2.**
- **Create an empty NFS-mounted directory and then mount the Solaris 10 Update 2 to the NFS-mounted directory as follows:**
  - Create an empty directory that will be used as the Solaris 10 Update 2 ISO image mount-point directory. For example: **`mkdir /sol10u2`**
  - Add the mount-point directory name to the `/etc/dfs/dfstab` file.

    For example: **`echo 'share -F nfs -o ro,log=global -d "Sol10U2 ISO mount point" /sol10u2' >> /etc/dfs/dfstab`**
  - Type **`svcadm restart nfs/server`** to stop and then restart NFS.
  - Mount the Solaris 10 Update 2 ISO image to the mount-point directory. For example:

    `mount -F hsfs -o ro 'lofiadm -a /otp-download/sol10u2-ga-sparc-dvd.iso' /sol10u2`

8 Create the Open Telecommunications Platform installation directory and files.

a. Concatenate the zipped Open Telecommunications Platform files to a single zip file.

For example:

```
# cat otp1.1.zip-a otp1.1.zip-b otp1.1.zip-c> otp1.1.zip
```

b. Unzip the Open Telecommunications Platform zip file you created to create the installation directory and files.

For example:

```
# unzip otp1.1.zip
```

The Open Telecommunications Platform installation directory `otp1.1` is created.

9 Move the `otp1.1` directory to the root file system.

For example:

```
#  mv otp1.1 /
```

10 NFS-mount the `/otp1.1` directory.

a. Add the fully-qualified path name of the `/otp1.1` installation directory to the `/etc/dfs/dfstab` file.

For example:

```
echo ‘share -F nfs -o ro,log=global -d "OTP 1.1 Installation Directory" /otp1.1’ >> /etc/dfs/dfstab
```

b. Type `svcadm restart nfs/server` to stop and then restart NFS and NFS-mount the `/otp1.1` OTP installation directory.

NFS-mounting the `/otp1.1` simplifies setting up the external OTP installation server.

Next Steps Set up the external OTP installation server as described in the next section.

Setting Up the External OTP Installation Server

This section provides the procedures for installing Solaris 10 Update 2 on the external OTP installation server, creating the OTP installation directory, and for installing the OTP OS provisioning plug-in on the external OTP installation server.

The following topics are discussed:

▼ To Install Solaris 10 Update 2 on the External OTP Installation Server

This procedure provides the procedural summary for installation of Solaris 10 Update 2 on the external OTP installation server.

You can use a JumpStart server or the Solaris 10 Update 2 installation DVD-ROM to install the Solaris OS on the external OTP installation server.

Before You Begin

- Review the following Solaris 10 Update 2 installation guides: *Solaris 10 Installation Guide: Basic Installations*, and *Solaris 10 Installation Guide: Custom JumpStart and Advanced Installations*.
- If the hard drive contains partitions, delete the partitions before installing the Solaris OS.

1. **When prompted for the Type of Install, choose Custom Install.**
2. **When prompted to provide the Ethernet port selections, assign the IP addresses, netmask, and gateway values according to your network architecture.**
3. **When prompted for the Software Group, choose Entire Distribution Plus OEM.**

Caution – If you do not choose `Entire Distribution plus OEM`, Open Telecommunications Platform installation and configuration will fail.

4. **When prompted for disk selection, choose all available disks.**
5. **When prompted to lay out file systems, partition the system disk according to the requirements listed in Table 3–1.**

Next Steps

- Configure Solaris 10 Update 2 as described in "Configuring Solaris 10 Update 2" on page 94
- Create the OTP installation directory on the external OTP installation server as described in the next procedure.

▼ To Create the OTP Installation Directory on the External OTP Installation Server

Before You Begin

- The OTP 1.1 installation source must be available, either on DVD-ROM, or as an NFS-mounted directory on a server in your network as described in "Downloading and Uncompressing the OTP and Solaris OS Software" on page 41
- Solaris 10 Update 2 must be installed on the external OTP installation server

1. **Log in as root (`su - root`) to the external OTP installation server.**
2. **Create the OTP installation directory `/otp1.1`.**
3. **Copy the OTP installation source files to `/otp1.1`.**

- If you purchased the OTP Installation DVD-ROM, copy the contents of `/cdrom/otp_11_dvd/otp1.1` to the `/otp1.1` directory. For example:

  ```
  # cp -r /cdrom/otp_11_dvd/otp1.1/* /otp1.1
  ```

- If you downloaded the OTP installation source to an external download server as described in "Downloading and Uncompressing the OTP and Solaris OS Software" on page 41, copy the contents of the NFS-mounted `/otp1.1` directory on the download server to the `/otp1.1` on the external OTP installation server.

  For example, if the name of the download server is `downloads` and the domain is `mycompany`, you would then type:

  ```
  # cp -r /net/downloads.mycompany/otp1.1/* /otp1.1
  ```

4 NFS-mount the `/otp1.1` directory.

a. Add the fully-qualified path name of the `/otp1.1` installation directory to the `/etc/dfs/dfstab` file.

For example:

```
share -F nfs -o ro,log=global -d "OTP 1.1 Installation Directory" /otp1.1
```

This eliminates the need to type long directory path names during installation.

Note – The `/otp1.1` directory is referred to throughout this document as the *OTP installation directory*.

---

b. Type `svcadm restart nfs/server` to stop and then restart NFS and NFS-mount the `/otp1.1` OTP installation directory.

Next Steps Install the OTP services, agent, and plug-ins as described in the next procedure.

▼ To Install the OTP Services, Agent, and Plug-ins on the External OTP Installation Server

Before You Begin The OTP 1.1 installation source directory must created and NFS-mounted on the external OTP installation server as described in "To Create the OTP Installation Directory on the External OTP Installation Server" on page 45.

1 Log in as root (`su - root`) to the external OTP installation server.

2 Install the `SUNWotpcli` package.

Type **`# pkgadd -d /otp1.1/Products/packages -R / SUNWotpcli`**.

3 Set up the external installation server.

Type **`/opt/SUNWotp10/CLI/setupExternalInstallServer /otp1.1`**

The `setupExternalInstallServer` script performs the following tasks:

- Installs the master server and the OTP Application Provisioning Service remote agent
- Loads the OTP and OSP plug-ins
- Installs the OSP server and JET Boot/Install server.
- Changes the default DHCP lease time for Solaris OS provisioning from 5 to 15 minutes.

Wait for the installation process to complete. The installation process can take up to 35 minutes to complete.

4 Verify installation.

Go to URL http://*install server*:9090 where *install server* is either the IP address or the fully qualified name of the external OTP installation server.

If installation was successful, the service provisioning system log in page appears.

a. (Optional) Click `change password` and change the password on the next page.

Type the default user name and password `admin` in the `user name:` and `current password:` fields.

Type the new password in the `new password:` and `confirm new password:` fields, and then click `continue to change password`.

The log in page appears. Log in to the service provisioning system. The Common Tasks page appears.

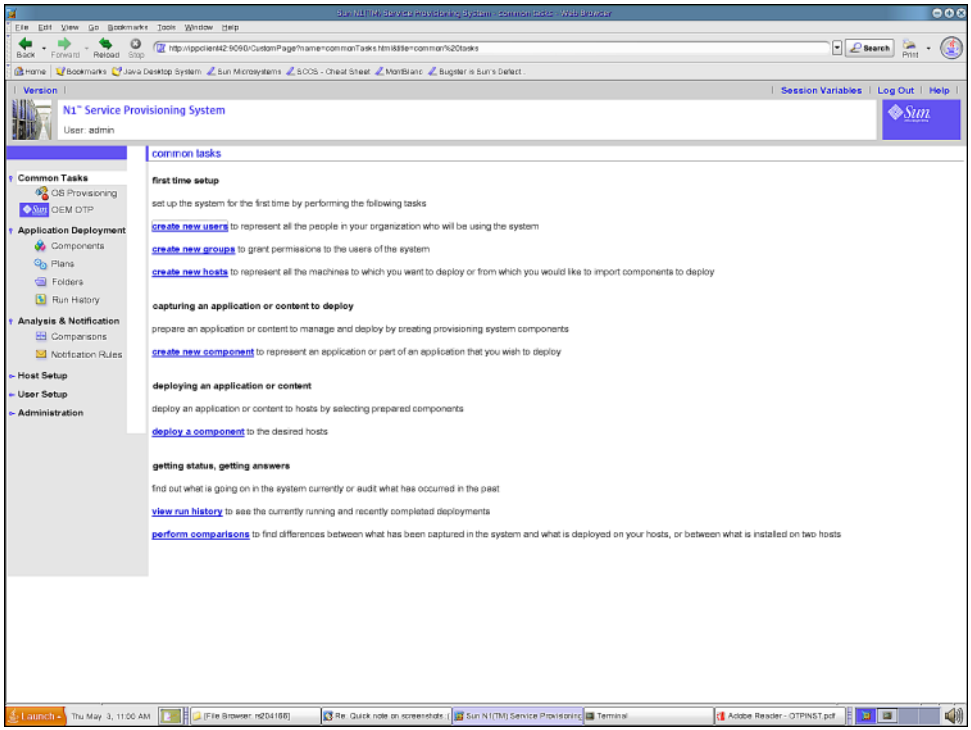

FIGURE 3–1 Common Tasks Page

b. Click OEM OTP under Common Tasks in the left menu to display the Open Telecommunications Platform home page.

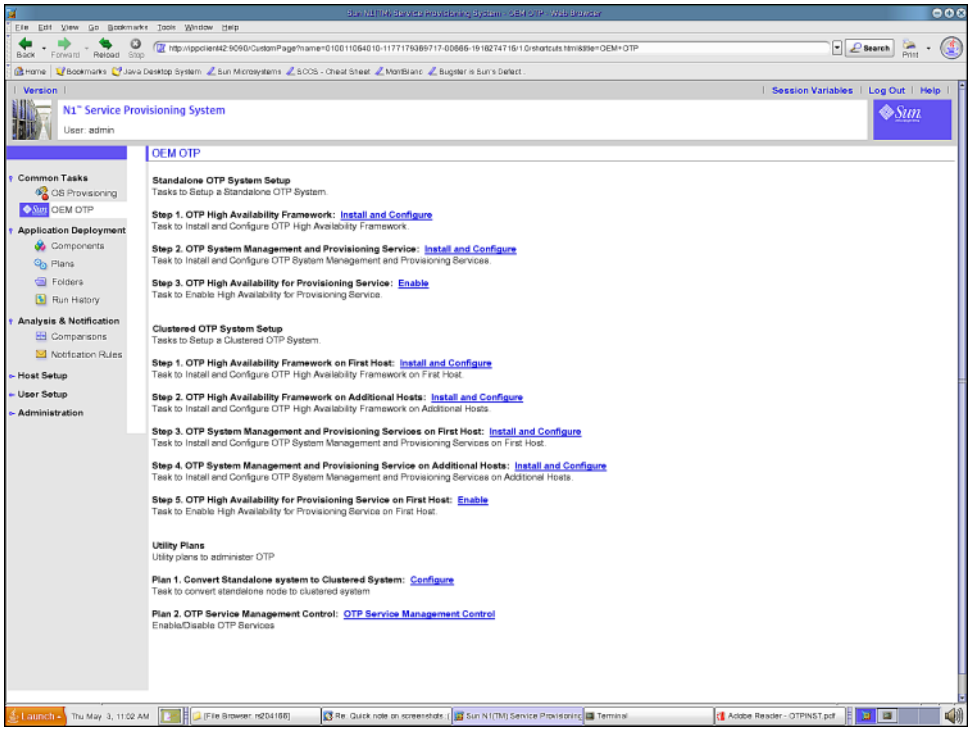

FIGURE 3–2 Open Telecommunications Platform Tasks Page

c. Click Plans under Application Deployment to display the plans screen.

If you do not see the plans screen, click change folder and navigate to `/com/sun/OTP`.

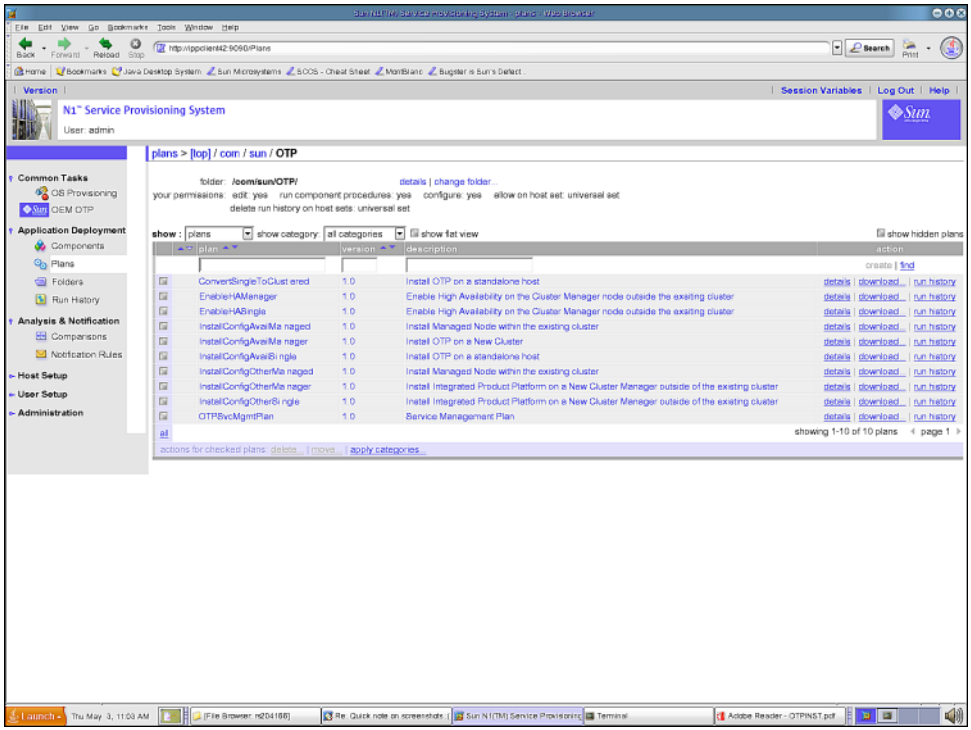

FIGURE 3–3 Plans Screen

Successful display of the screens verifies installation of the service provisioning system and the Open Telecommunications Platform plug-in.

Next Steps Install Solaris 10 Update 2 on the OTP hosts as described in the next section.

Installing Solaris 10 Update 2 and the Remote Agent on the OTP Hosts

This section provides the procedures for installing Solaris 10 Update 2 on the OTP host or hosts you chose for the OTP system. You must install and configure Solaris 10 Update 2 on each OTP host before you can install the Open Telecommunications Platform.

The following topics are discussed:

- "Manually Installing the Solaris OS and the Remote Agent on a New OTP Host" on page 52
- "Installing the Solaris OS and Remote Agent on a New OTP Host Using the External Installation Server OSP Plug-in Graphical User Interface" on page 53

Note – Before you install Solaris 10 Update 2, review the OTP host disk drive partitioning requirements listed in the following table.

If you have chosen to use JumpStart to install the Solaris OS to the OTP host or hosts selected for OTP, also ensure that the JumpStart scripts remove all existing partitions from earch server's hard drive, and that the JumpStart scripts allocate the new partitions on each server's hard drive as described in the following table.

TABLE 3–1 OTP Host Disk Drive Partition Requirements

Slice	Partition	Size
0	`/` (root)	All remaining free space on the disk after allocating space for slices 2 through 7.
1	`swap`	Two to three times total system ram, or 4 Gbytes, whichever is greater.
2	overlap	The entire system disk.
3	`/globaldevices`	512 Mbytes minimum. The OTP high availability framework later assigns this slice a different mount point and mounts the slice as a cluster file system. **Note –** `/globaldevices` can reside on any unused slice on any disk on the server. Failure to allocate `/globaldevices` on an OTP systemwill cause Open Telecommunications Platform to fail.
4 through 6	unused	Not used.
7	Solaris Volume Manager	20 Mbytes Used by Solaris Volume Manager software for the state database replica.

Manually Installing the Solaris OS and the Remote Agent on a New OTP Host

The following procedure provides the steps for manually installing the Solaris OS and service provisioning remote agent on a new OTP host.

▼ To Manually Install the Solaris OS and the Remote Agent on a New OTP Host

1. **Install the Solaris OS on the OTP host as described in described in "To Install Solaris 10 Update 2 on the External OTP Installation Server" on page 44.**

   The requirements and procedures for installing the Solaris OS on a new OTP hostare identical to those for the external OTP installation server.

   Note – Ensure that you specify Entire Distribution Plus OEM and that you partition the OTP host disk drive as described in Table 3–1.

   ---

2. **Log in as root (`su - root`) to the new OTP host.**

3. **Configure the Solaris OS on the OTP host as described in "Configuring Solaris 10 Update 2" on page 94.**

4. **If you did not create the `/globaldevices` file system on the OTP host, create the file system as described in "Creating the `/globaldevices` File System on the OTP Hosts" on page 100.**

5. **Install the `SUNWotpcli` package on the OTP host.**

   Type the command:

   `pkgadd -d /net/`*OTP_install_server.domain_name*`/`*media_path*`/Products/packages -R / SUNWotpcli`

   where *OTP_install_server* is the name of the external OTP installation server, *domain_name* is your company's domain name, and *media_path* is the fully qualified path of the OTP installation directory on the external OTP installation server.

   For example, if the name of the external OTP installation server is `otpsource`, your company domain name is `mycompany.com`, and the OTP installation source directory is `otp1.1`, you would then type:

   ```
   # pkgadd -d /net/otpsource.mycompany.com/otp1.1/Products/packages -R / SUNWotpcli
   ```

6. **Install the service provisioning remote agent on the OTP host.**

   Type the command

   `/opt/SUNWotp10/CLI/setupRemoteAgent` *OTP_installation_directory*

where *OTP_installation_directory* is the fully qualified path to the NFS-mounted OTP installation source directory you created on the external OTP installation server as described in "To Create the OTP Installation Directory on the External OTP Installation Server" on page 45.

For example, if your external OTP installation server is named `otpsource`, the domain name is `mycompany.com`, and the NFS-mounted OTP installation directory on `otpsource` is /otp1.1, you would then type:

```
# /opt/SUNWotp10/CLI/setupRemoteAgent  /net/otpsource.mycompany.com/otp1.1
```

The `setupRemoteAgent` script creates the service provisioning user account and installs the remote agent.

Next Steps When you have completed installing and configuring Solaris 10 Update 2 and the remote agent on each OTP host, install the Open Telecommunications Platform on the OTP host.

- To install OTP on one or more OTP hosts using the command line, see Chapter 4, "Installing the Open Telecommunications Platform For the First Time Using the Command Line"
- To install OTP on one or more OTP hosts using the graphical user interface, see Chapter 5, "Installing the Open Telecommunications Platform For the First Time Using the Graphical User Interface"
- To install OTP on one or more OTP hosts using a production standalone or a clustered OTP host, see Chapter 6, "Installing the Open Telecommunications Platform Using the Provisioning Service On an Existing OTP System"

Installing the Solaris OS and Remote Agent on a New OTP Host Using the External Installation Server OSP Plug-in Graphical User Interface

This section provides the procedures for using the OSP plug-in graphical user interface on the external OTP installation server to install the Solaris OS and the service provisioning remote agent on a new OTP host.

The following topics are discussed:

Note – The external OTP installation server must already be set up and configured as described in "Setting Up the External OTP Installation Server" on page 44.

▼ To Create and Register the Subnet

1 **Open a Web browser and go to URL http://*external OTP installation server*:9090 where *external OTP installation server* is either the IP address or the fully qualified name of the external OTP installation server.**

The OTP provisioning service log in screen appears. Log in to the service provisioning system.

2 **Click OS Provisioning.**

The OS Provisioning screen appears.

3 **Scroll down and locate OSP Subnets.**

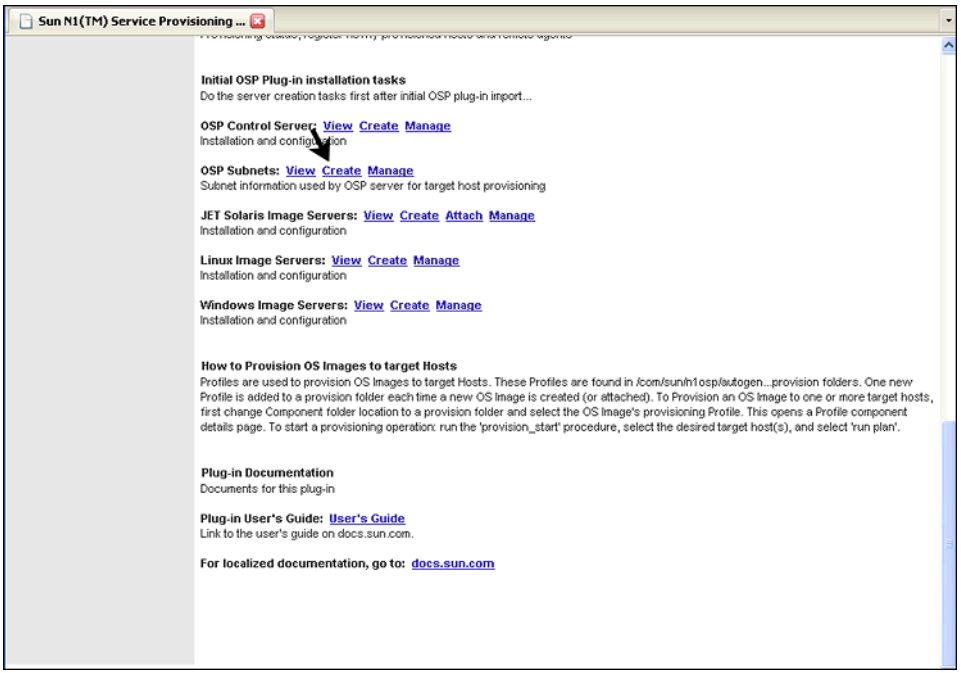

FIGURE 3–4 OS Provisioning Screen: Selecting OSP Subnets Create

Click Create. The Subnet-create screen appears.

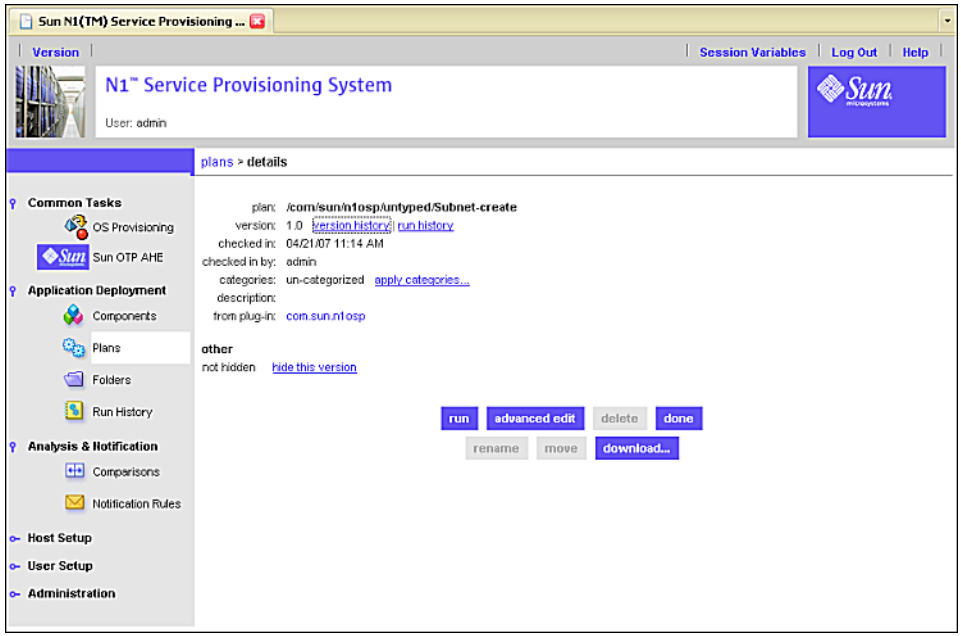

FIGURE 3–5 Create Subnet Plan Screen

4 Click run.

The Create Subnet Plan Run screen appears.

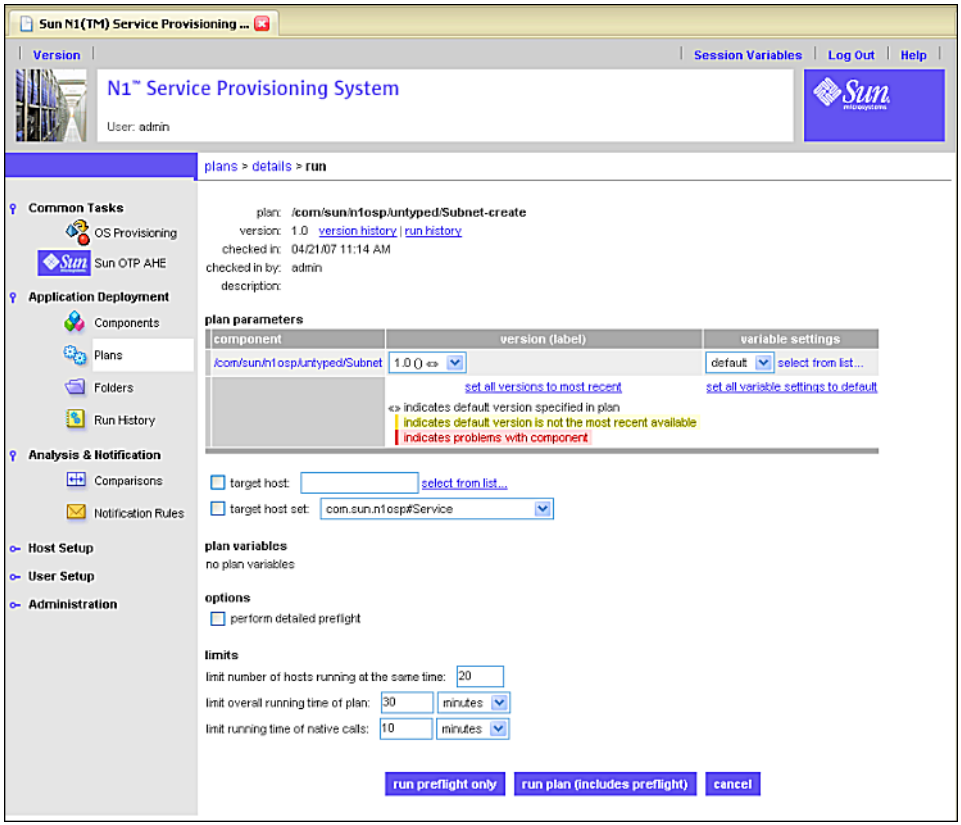

FIGURE 3–6 Create Subnet Plan Run Screen

5 Click select from list... beneath variable settings.

The select variable setting from list... screen appears.

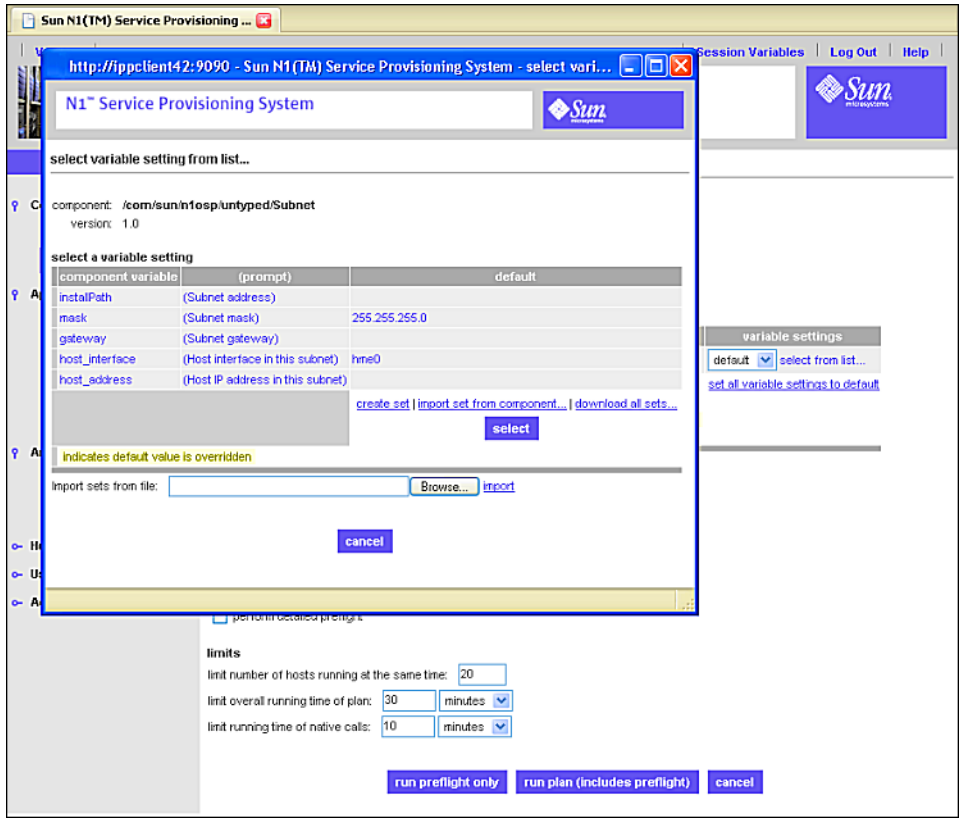

FIGURE 3–7 Create Subnet Plan: Select Variable Setting From List Screen

6 Click `create set` in the Variable Setting From List screen as shown by the following figure.

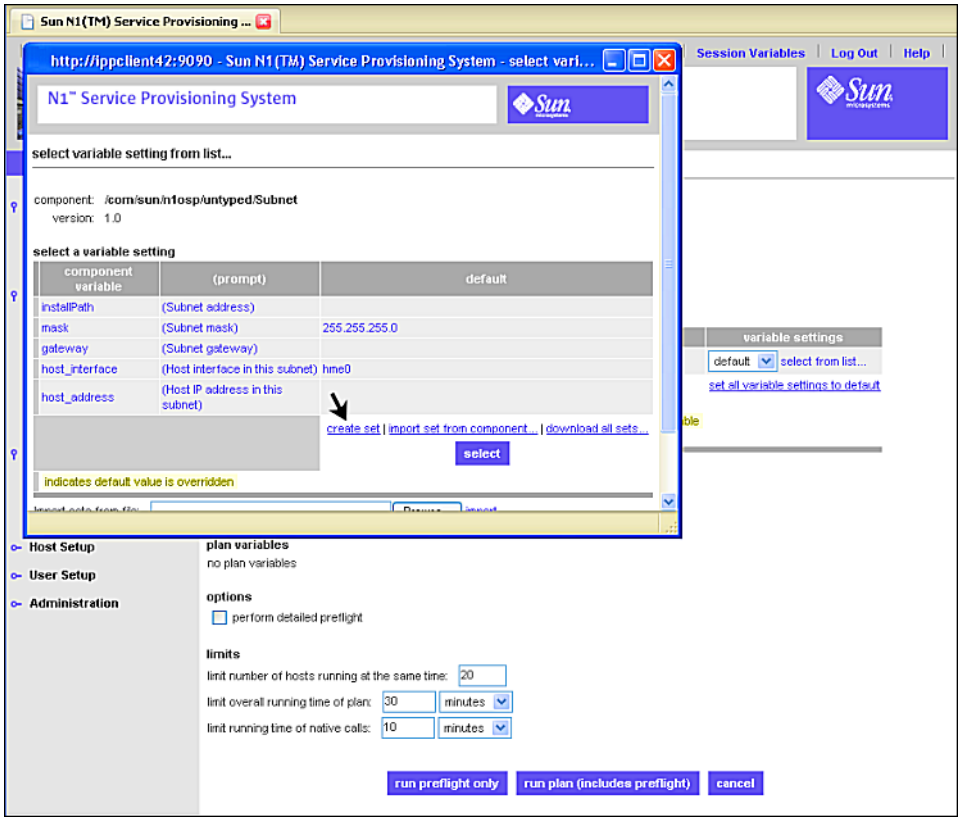

FIGURE 3–8 Create Subnet Plan: Create Set Screen

When you click `create set`, the subnet variables screen appears:

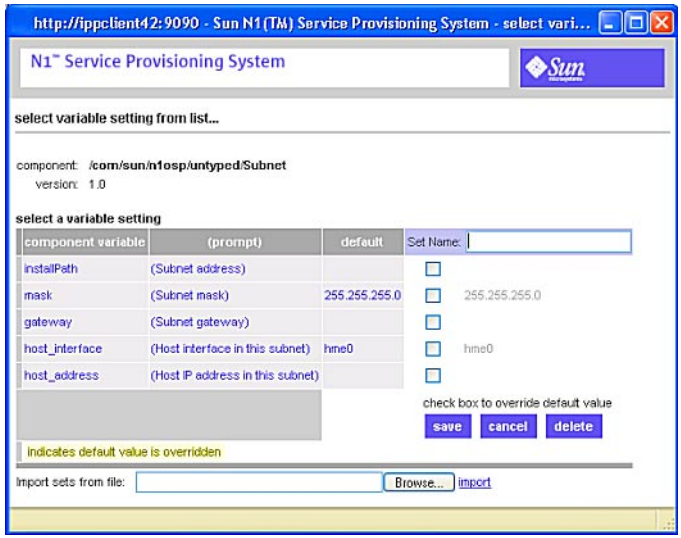

FIGURE 3–9 Create Subnet Plan: Create Set Variables Screen

7 Enter the values on the Create Set Variables Screen as follows:

a. Type a name for the subnet set in the Set Name field.

For example, *subnet53*

b. Click the installPath check box.

A text field appears to the right of the check box. Type the base IP address of the subnet.

c. Click the mask check box.

A text field appears to the right of the check box populated with the default subnet mask 255.255.255.0. If needed, type in a different subnet mask in the text field. .

d. Click the gateway check box.

Type the gateway IP address in the text field that appeared.

e. Click the host_interface check box.

Type the name of the external OTP installation server's provisioning interface, for example, `bge0`. Do not specify the logical interface.

f. Click the host_address check box.

Type the IP address of the provisioning interface..

The Create Set Variables screen should be similar to the following:

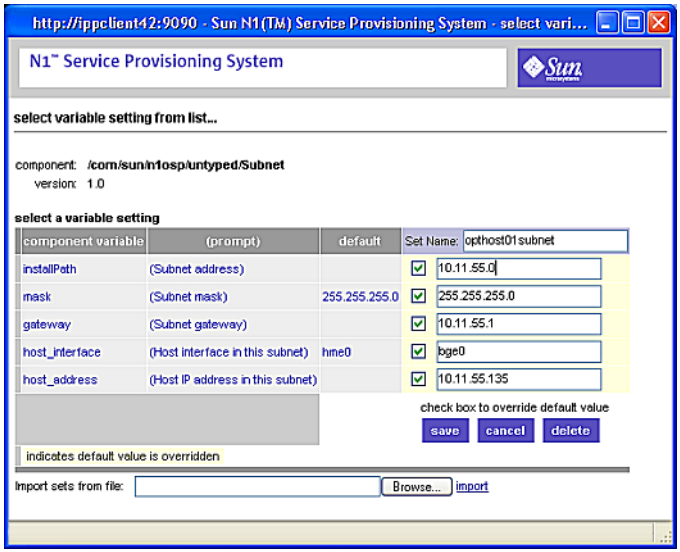

FIGURE 3–10 Create Subnet Plan: Example of Completed Create Set Variables Screen

g. Click save.

The Create Set Variables Screen refreshes and displays your entries:

FIGURE 3–11 Create Subnet Plan: Example of Saved Create Set Variables Screen

h. Click the right-most select button.

The Create Set Variables screen closes. and the Subnet Plan Run Screen is updated.

If the variable settings field does not display the plan set you created, click select from list... and click the name of the set you created.

8 Click on the target host field `select from list...` link on the Subnet Plan Run screen as shown by the following figure.

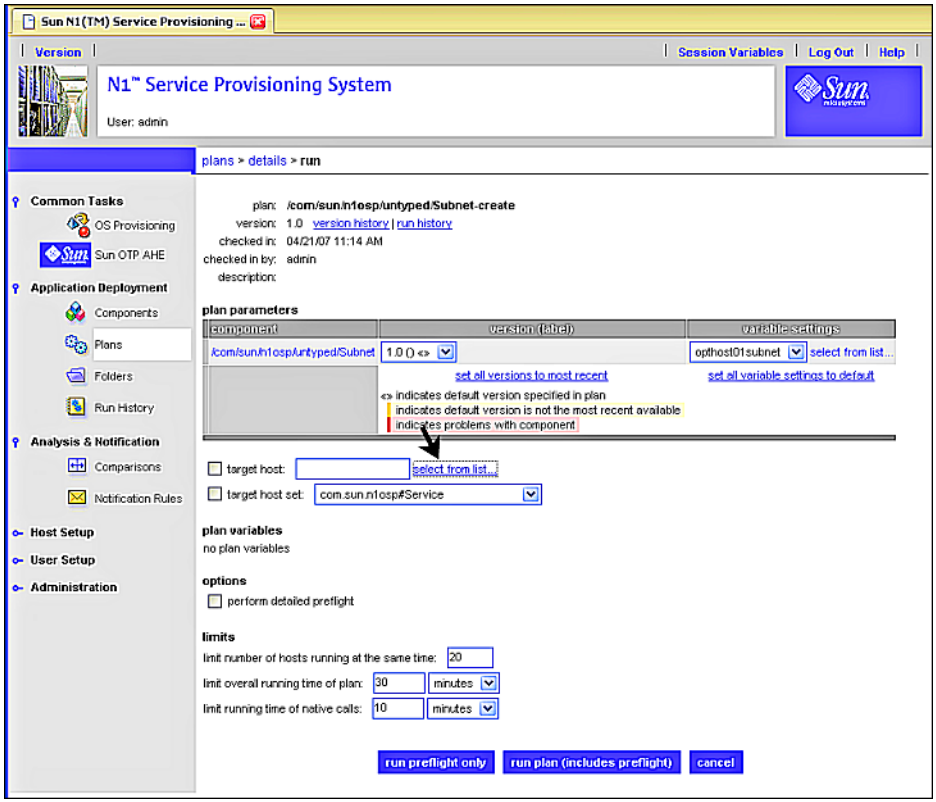

FIGURE 3–12 Create Subnet Plan: Selecting Target Host Select From List

When you click the target host `select from list...` link, the target host select from list screen appears:

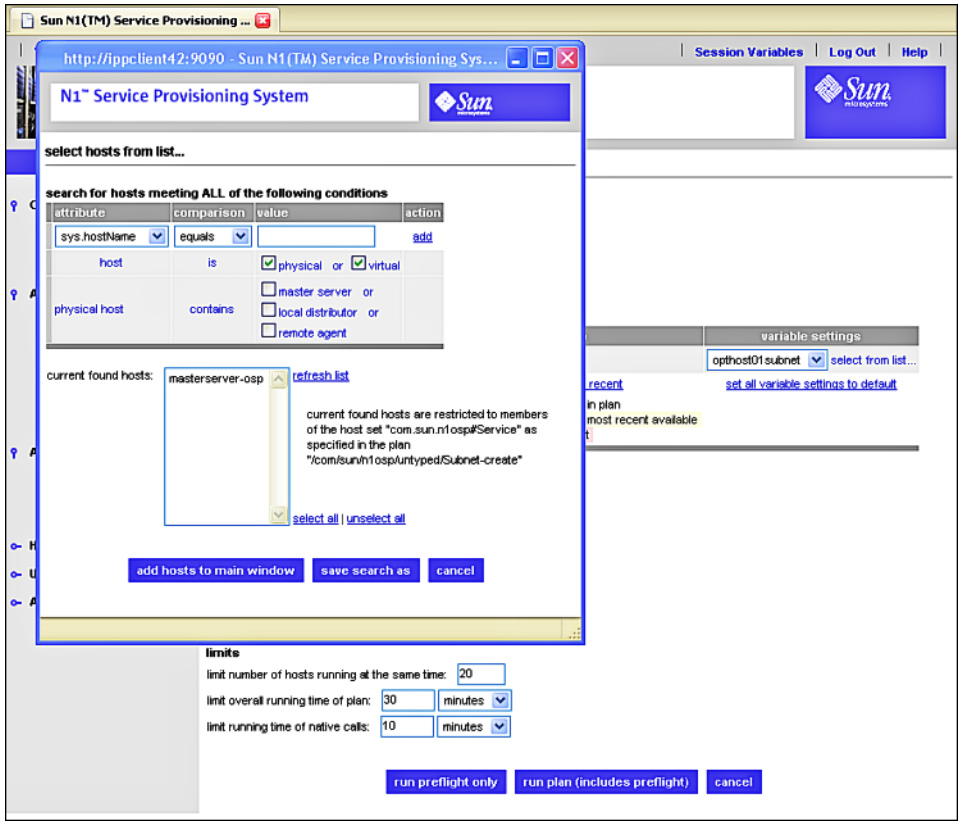

FIGURE 3–13 Create Subnet Plan: Target Host Select From List Screen

9 **Click `masterserver-osp`, then click add hosts to main window.**

The Target Host Select From List screen closes, and the target host field on the Subnet Plan Run screen is populated with masterserver-osp.

10 **Click `run plan (includes preflight)`.**

Several screens are displayed as the plan runs. When the plan completes, the deployment results screen appears. Your screen should be similar to the following example.

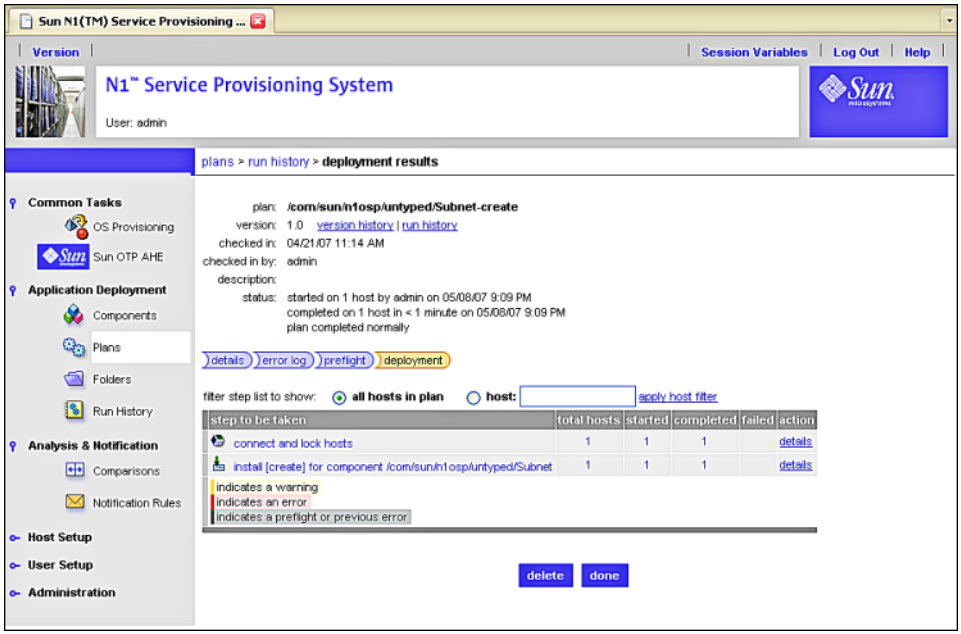

FIGURE 3–14 Create Subnet Plan: Example Deployment Results

11 **Click done.**

Next Steps Create the Solaris 10 Update 2 image as described in the next procedure.

▼ To Create the Solaris 10 Update 2 Image

1 **Open a Web browser and go to URL http://*external OTP installation server*:9090 where *external OTP installation server* is either the IP address or the fully qualified name of the external OTP installation server.**

The OTP provisioning service log in screen appears. Log in to the service provisioning system.

2 **Click OS Provisioning.**

The OS Provisioning screen appears:

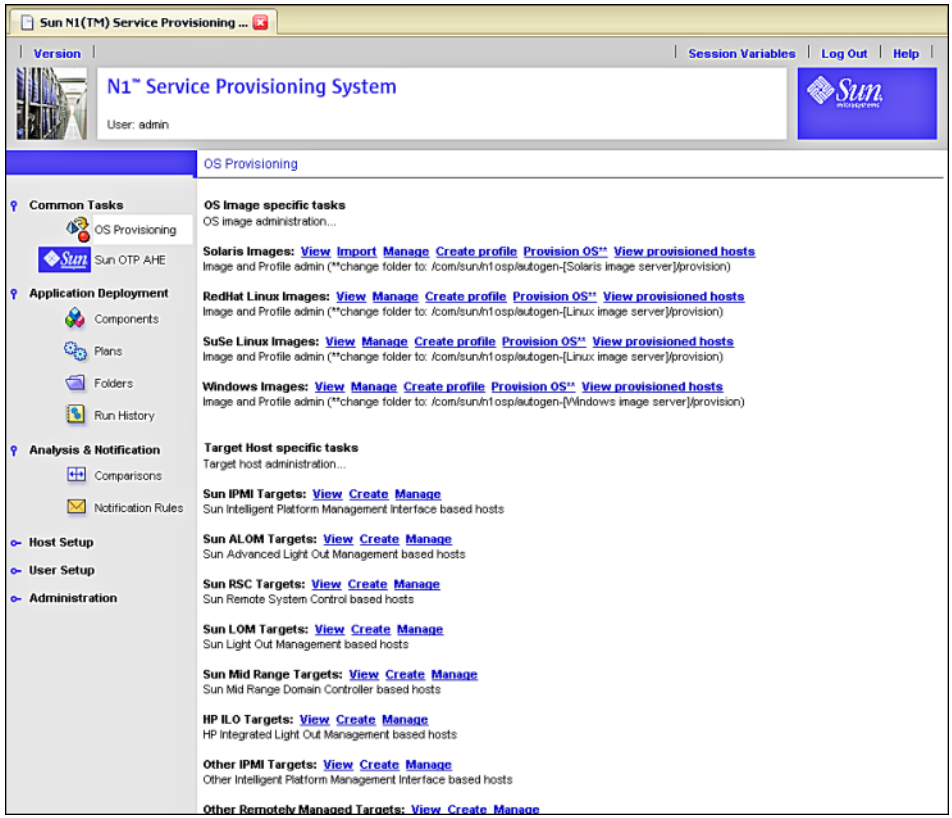

FIGURE 3–15 OS Provisioning Screen: Selecting Solaris Images Import

3 Click the Solaris Images `Import` link.

The Solaris Image Import plans screen appears.

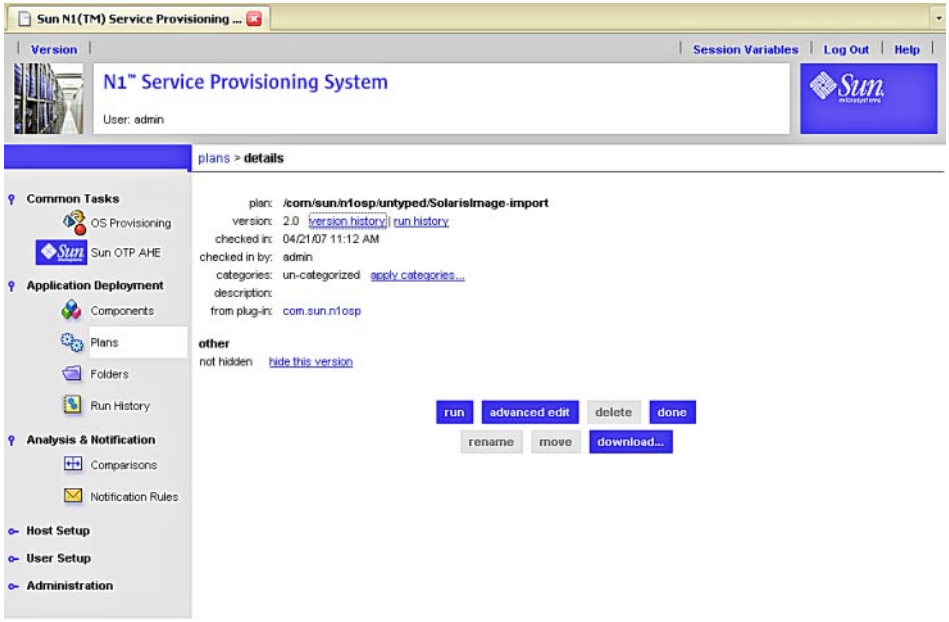

FIGURE 3–16 Solaris Images Import Plan Screen

4 Click run.

The Solaris Image Plan Variables screen appears.

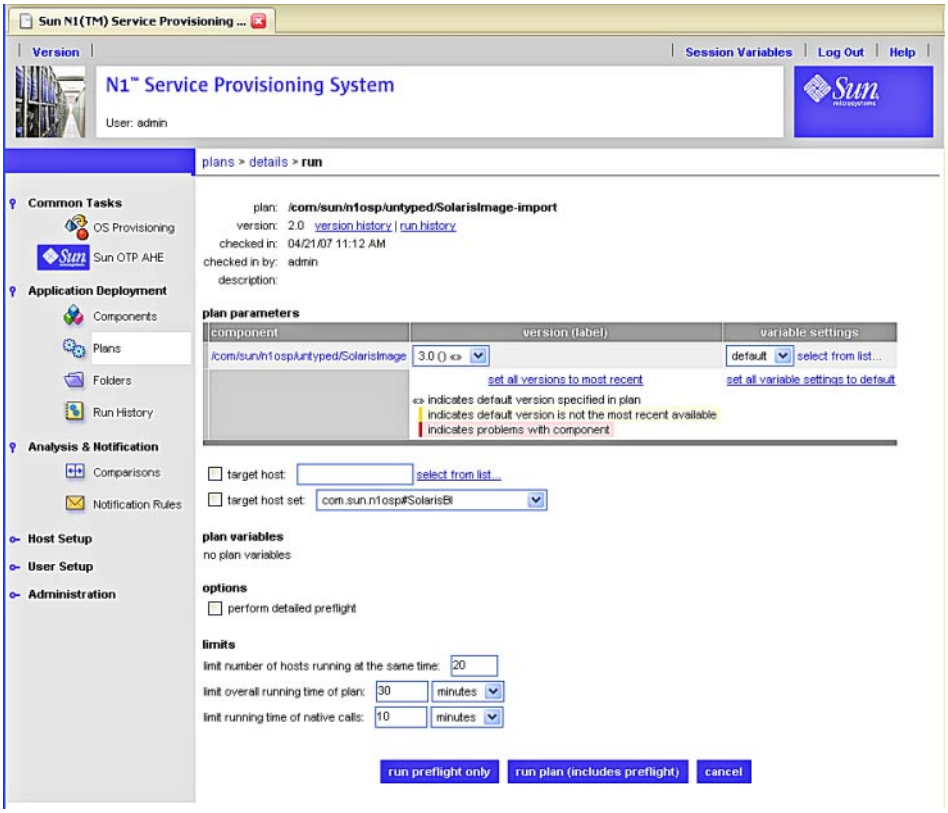

FIGURE 3–17 Solaris Images Import Plan Variables Screen

5 Click `select from list...` beneath variable settings.

The select variable setting from list... screen appears.

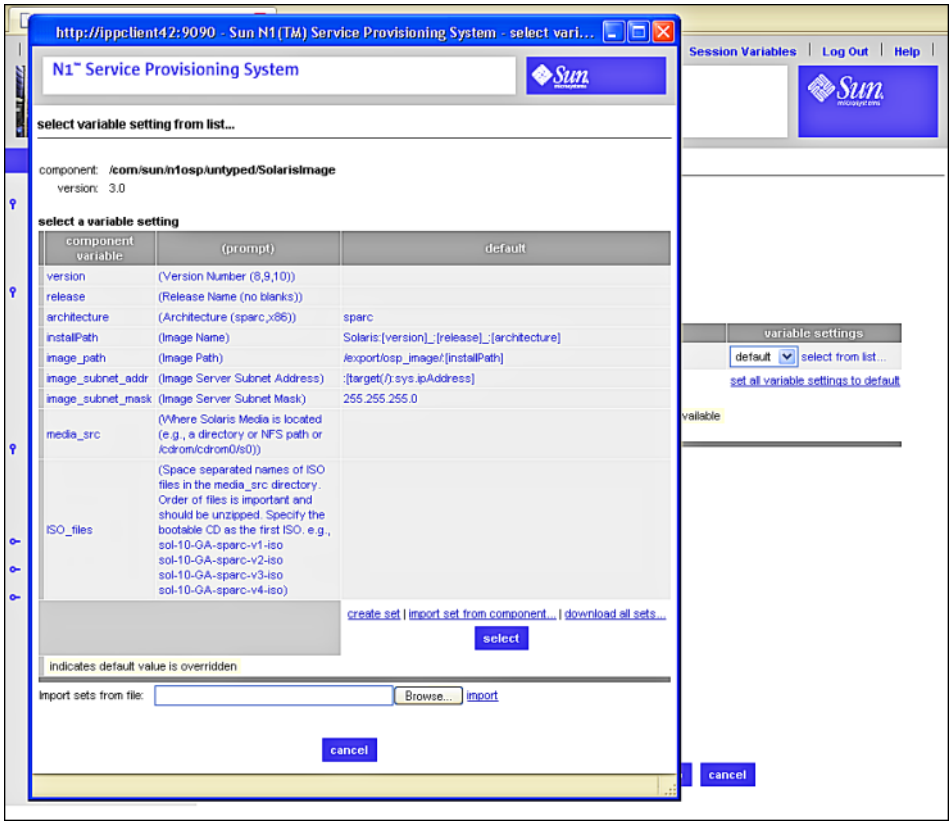

FIGURE 3–18 Solaris Images Select Variable Setting From List Screen

6 **Click `create set` in the Select Variable Setting From List screen.**

The Solaris Images Create Set variables screen appears:

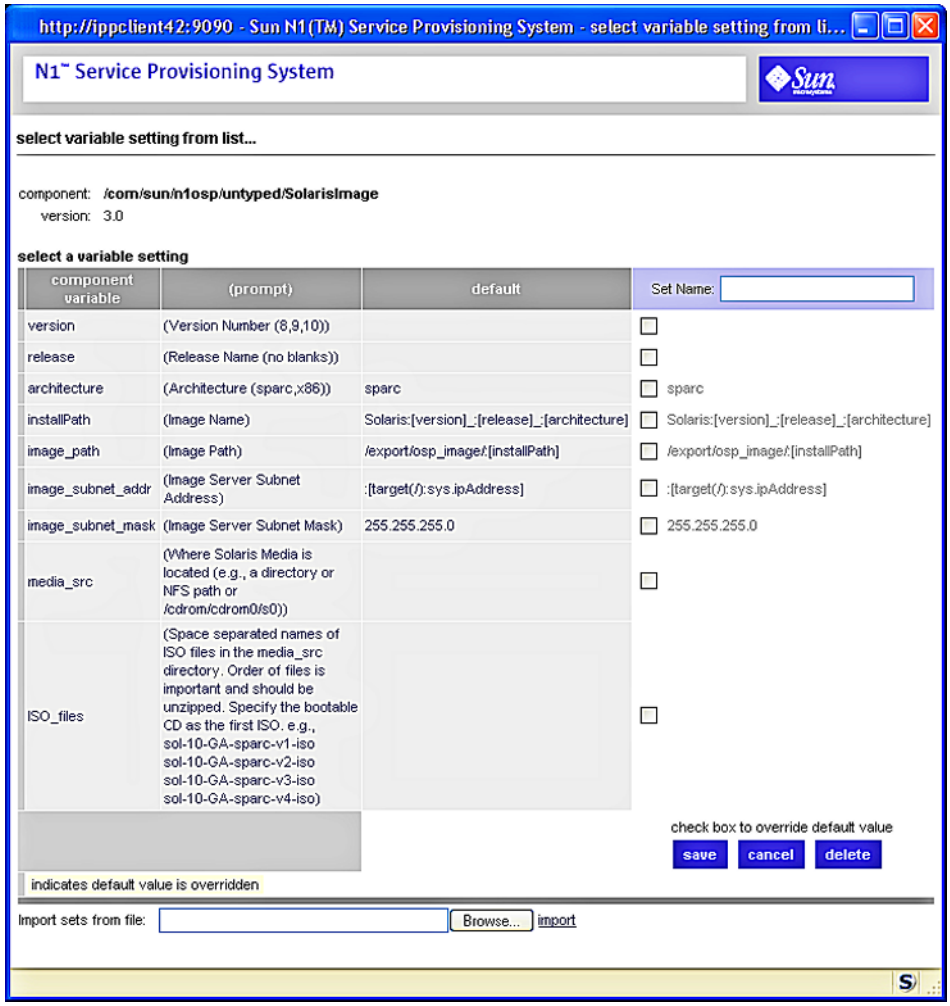

FIGURE 3–19 Solaris Images Create Set Variables Screen

7 Enter the values on the Solaris Images Create Set Variables Screen as follows:

a. Type a name for the Solaris OS image in the Set Name field.

For example, *sol10u2*. The name must start with an alphabetic character.

b. Click the version check box.

A text field appears to the right of the check box. Type the Solaris OS version number, for example, 10.

c. Click the release check box.

A text field appears to the right of the check box. Type the Solaris release version, for example u2.

d. Click the architecture check box.

The text field is populated with the default value sparc.

e. Click the installPath check box.

Type the name of the Solaris OS image, for example sol-10–u2–ga-sparc

f. Click the image_path check box.

Type the full path to which to the Solaris OS ISO image will be copied. This can be a shared file system on the external OTP installation server or an shared file system on a clustered OTP host.

g. Click the image_subnet_addr check box.

Type the IP address of the server on which the OS image is to be copied.

h. Click the image_subnet_mask check box.

A text field appears to the right of the check box populated with the default subnet mask 255.255.255.0. If needed, type in a different subnet mask in the text field. .

i. Click the media_src check box.

Type the full path to the source Solaris OS image. This can be an NFS-mounted ISO image as described in "To Download and Uncompress the OTP and Solaris OS Installation Zip Files" on page 42.

j. Click the ISO_files check box.

Type the names of the Solaris OS ISO files as directed.

The Solaris Images Create Set Variables Screen should be similar to the following example:

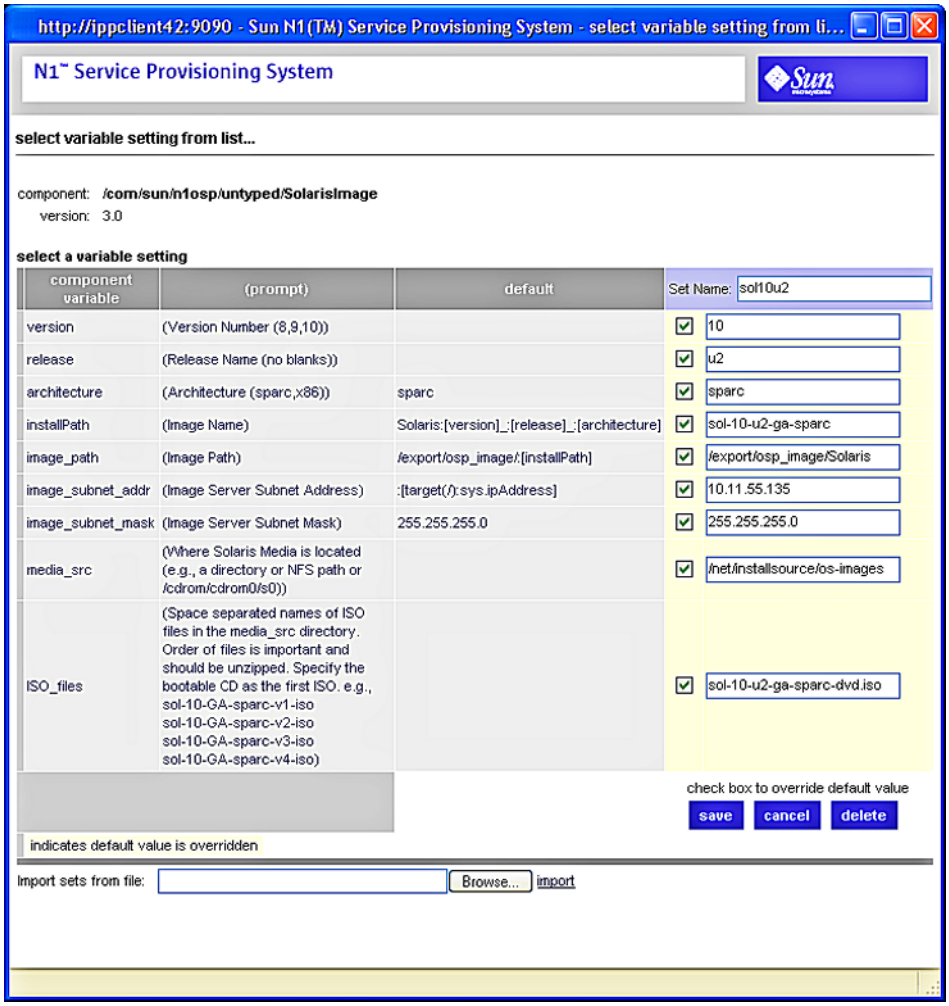

FIGURE 3–20 Solaris Images: Example Create Set Variables Screen

k. Click save.

The Create Set Variables Screen refreshes and displays your entries

l. Click the right-most select button.

The Create Set Variables screen closes. and the Solaris Images Plan Run Screen is updated.

If the variable settings field does not display the plan set you created, click select from list... and click the name of the set you created.

8 **Click on the target host field `select from list...` link on the Solaris Images Plan Run screen.**

The target host select from list screen appears:

FIGURE 3–21 Solaris Images Target Host Select From List Screen

9 **Click `masterserver-jet`, then click `add hosts to main window`.**

The Target Host Select From List screen closes, and the target host field on the Solaris Images Plan Run screen is populated with `masterserver-jet`.

10 **Change `limit overall running time of plan` to two hours.**

11 **Change `limit running time of native calls` to two hours.**

12 **Click `run plan (includes preflight)`.**

The Solaris Images plan will take about an hour to complete. When the plan completes, the deployment results screen appears.

13 **Click done.**

Next Steps Create the Solaris OS provisioning profile as described in the next procedure.

▼ To Create the Solaris OS Provisioning Profile

1. **Log in as root (`su - root`) to the external OTP installation server.**

2. **Type the following command to populate the custom packages with the appropriate JET path:**

   `/opt/SUNWjet/bin/copy_custom_packages` */OTP_media_path*`/Products/packages sparc SUNWotpra SUNWotpcli SUNWotputil`

   where */OTP_media_path* is the fully-qualifed path to the OTP installation directory you created in "To Create the OTP Installation Directory on the External OTP Installation Server" on page 45. For example:

   ```
   # /opt/SUNWjet/bin/copy_custom_packages \
   /otp1.1/Products/packages sparc SUNWotpra SUNWotpcli SUNWotputil
   ```

   The media is copied to the directory `/export/install/pkgs/custom/sparc` by default. To change the default directory, modify the setting in `/opt/SUNWjet/etc/jumpstart.conf`.

   For further information, see Chapter 5, "Provisioning the Solaris Operating System," in *Sun N1 Service Provisioning System User's Guide for OS Provisioning Plug-In 3.1*.

3. **Open a Web browser and go to URL http://***external OTP installation server***:9090 where** *external OTP installation server* **is either the IP address or the fully qualified name of the external OTP installation server.**

   The OTP provisioning service log in screen appears. Log in to the service provisioning system.

4. **Click OS Provisioning.**

   The OS Provisioning screen appears.

5. **Click the Solaris Images `Create Profile` link.**

   The Create Profile run screen appears.

6. **Click run.**

   The Create Profile variable settings run screen appears.

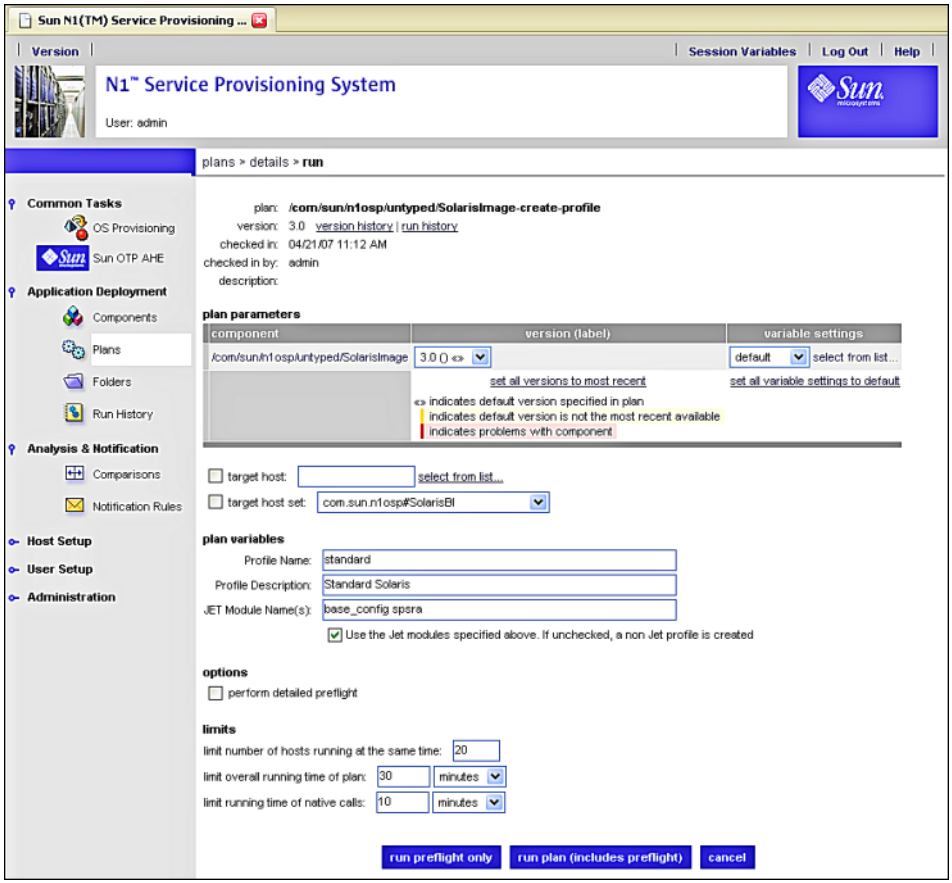

FIGURE 3–22 Create OS Profile Plan Variable Settings Run Screen

7 **Click the drop-down list beneath `variable settings`, and choose the OS image you created in the previous procedure.**

For example, sol10u2.

8 **Click on the target host field `select from list...` link on the Solaris Images Plan Run screen.**

The target host `select from list` screen appears.

9 **Click `masterserver-jet`, then click `add hosts to main window`.**

The Target Host Select From List screen closes, and the target host field on the Solaris Images Plan Run screen is populated with `masterserver-jet`.

10 **Add `custom` to the text in the JET Module Name(s) field.**

Ensure that the check box beneath the JET Module Name(s) field is checked.

The custom module ensures that the service provisioning remote agent is installed to the new OTP host after OS installation has completed.

The Create OS Profile Plan run screen should be similar to the following example:

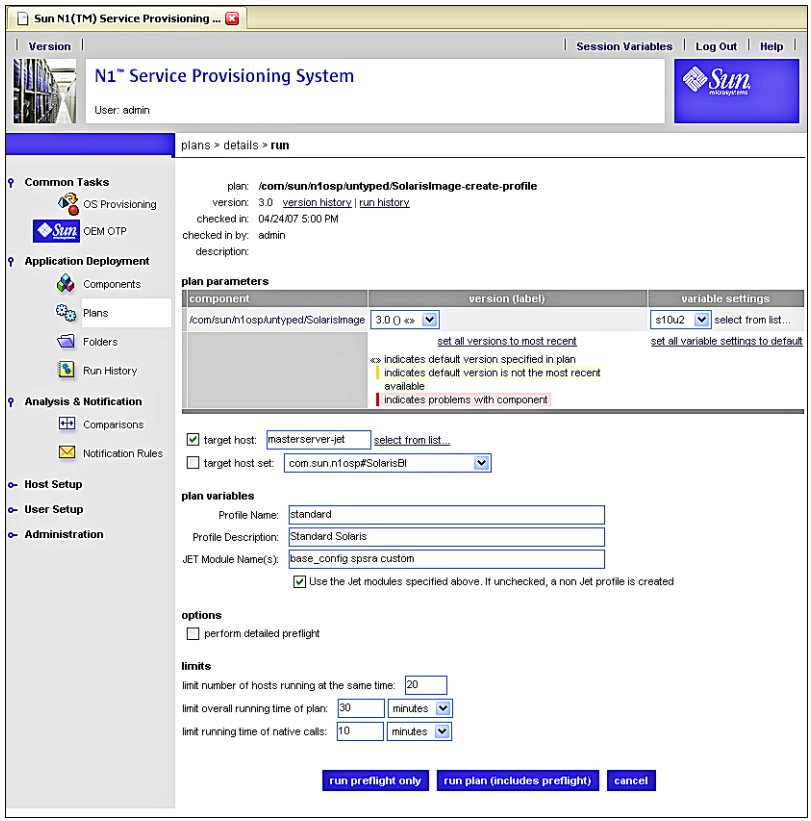

FIGURE 3–23 Create OS Profile Plan Variable Settings Run Screen Example

11 **Click** `run plan (includes preflight).`

The Create OS Profile plan will take a few minutes to complete. When the plan completes, the deployment results screen appears.

12 **Click done.**

Next Steps Create the ALOM target host as described in the next procedure.

▼ To Create the ALOM Target Host

1 **Open a Web browser and go to URL http://*external OTP installation server*:9090 where *external OTP installation server* is either the IP address or the fully qualified name of the external OTP installation server.**

The OTP provisioning service log in screen appears. Log in to the service provisioning system.

2 **Click OS Provisioning.**

The OS Provisioning screen appears.

3 **Click the Sun ALOM Target `Create` link.**

The Create ALOM Targets run screen appears.

4 **Click run.**

The Create ALOM Targets variable settings run screen appears.

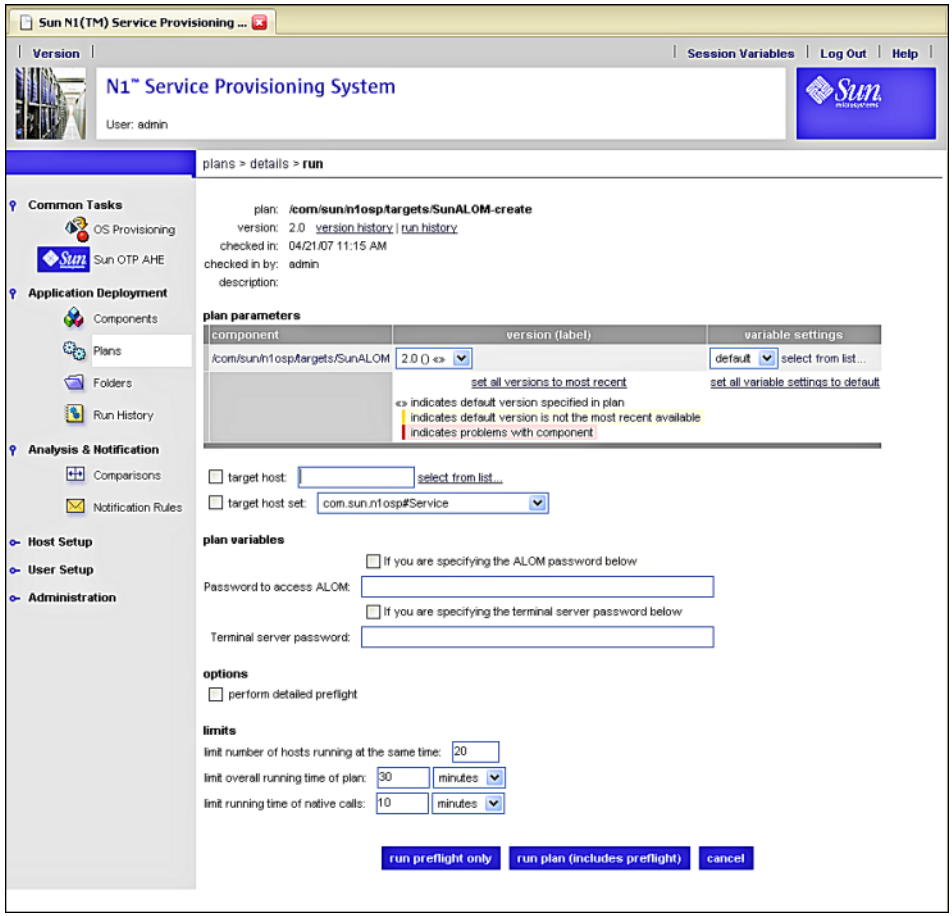

FIGURE 3–24 Create ALOM Target Variable Settings Run Screen

5 **Click `select from list...` beneath variable settings.**

The select variable setting from list... screen appears.

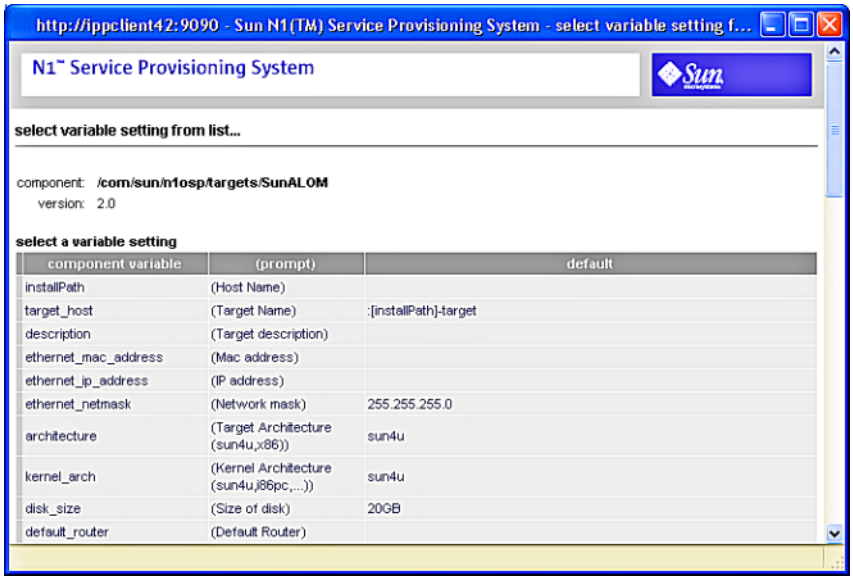

FIGURE 3–25 Create ALOM Target Select Variable Settings Screen

6 **Scroll to the bottom of the select variable settings screen and click `create set`.**

The Create ALOM Target Create Set variables screen appears:

FIGURE 3–26 Create ALOM Target Create Set Variables Screen

7 Enter the values on the Create ALOM Target Create Set Variables Screen as follows.

Scroll as needed, and click check boxes to activate text entry fields.

The following list describes only the required fields. All other fields are optional.

Set Name — Type a name for the ALOM target in the Set Name field.

For example, *otphost01*. The name must start with an alphabetic character.

installPath	The name to be assigned to the new OTP host.
ethernet_mac_address	The MAC address of the new OTP host.
ethernet_ip_address	The IP address of the primary Ethernet port of the new OTP host.
disk_size	(Optional) The size of the new OTP host hard drive in Gbytes.
default_router	(Optional) The IP address of the default router for the subnet to which the new OTP host is assigned.
alom_ip_address	The IP address assigned to the service processor of the new OTP host.
alom_access_userid	The ALOM user account name.

alom_access_password	The encrypted ALOM user account password.
	
	Create the encrypted password as described in "Password Encryption" in *Sun N1 Service Provisioning System User's Guide for OS Provisioning Plug-In 3.1*. For example:
	
	`# /opt/SUNWn1osp/sbin/n1osp_encrypter admin`
	`Encrypted Text: Clz6pK2b6qw=`

8 Click save.

The ALOM Target Create Set Variables screen refreshes and displays the values you entered.

9 Click the right-most select button.

The Create Set Variables screen closes. and the Create ALOM Target Variable Settings Plan Run Screen is updated.

If the variable settings field does not display the plan set you created, click `select from list...` and click the name of the set you created.

10 Click on the target host field `select from list...` link on the Settings Plan Run screen.

The target host select from list screen appears.

11 Click `masterserver-osp`, and then click `add hosts to main window`.

The Target Host Select From List screen closes, and the target host field on the Solaris Images Plan Run screen is populated with `masterserver-osp`.

12 Under plan variables, click the check box `If you are specifying the ALOM password below`.

Type the ALOM password in the Password to access ALOM: field.

13 **Click** `run plan (includes preflight).`

The Create ALOM Target plan will take about a minute to complete. When the plan completes, the deployment results screen appears.

14 **Click done.**

Next Steps Install the Solaris OS on the new OTP host as described in the next procedure.

▼ To Install the Solaris OS on a New OTP Host

1 **Open a Web browser and go to URL http://*external OTP installation server*:9090 where *external OTP installation server* is either the IP address or the fully qualified name of the external OTP installation server.**

The OTP provisioning service log in screen appears. Log in to the service provisioning system.

2 **Click OS Provisioning.**

The OS Provisioning screen appears.

3 **Click the Solaris Images** `Provision OS**` **link.**

The components screen appears.

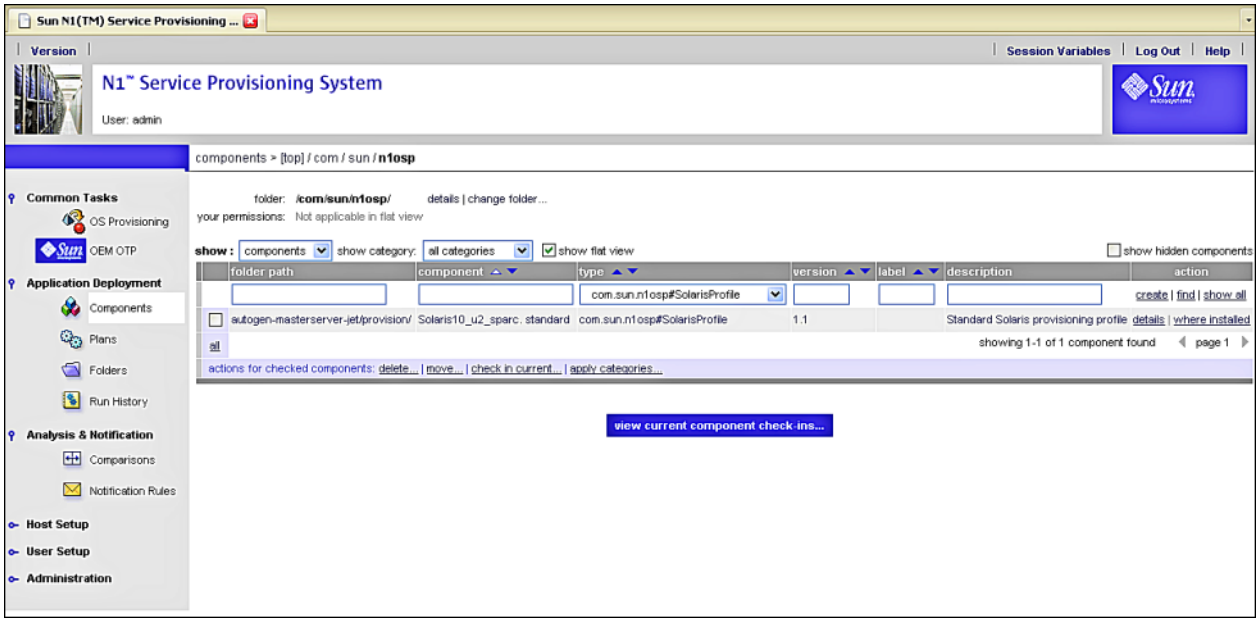

FIGURE 3–27 OS Provisioning Components Screen

4 **Click `Solaris10_u2_sparc. standard` or `Standard Solaris provisioning profile`.**

The Components Details screen appears.

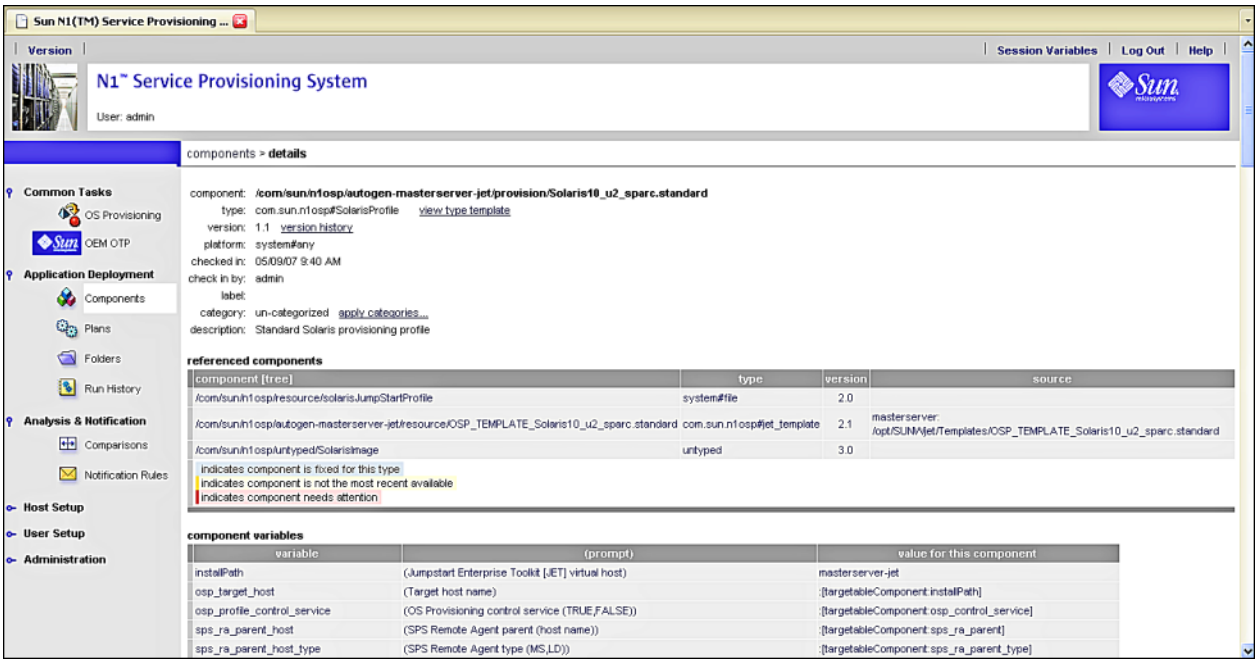

FIGURE 3–28 OS Provisioning Component Details Screen

5 **Scroll to the bottom and click run as shown by the following figure.**

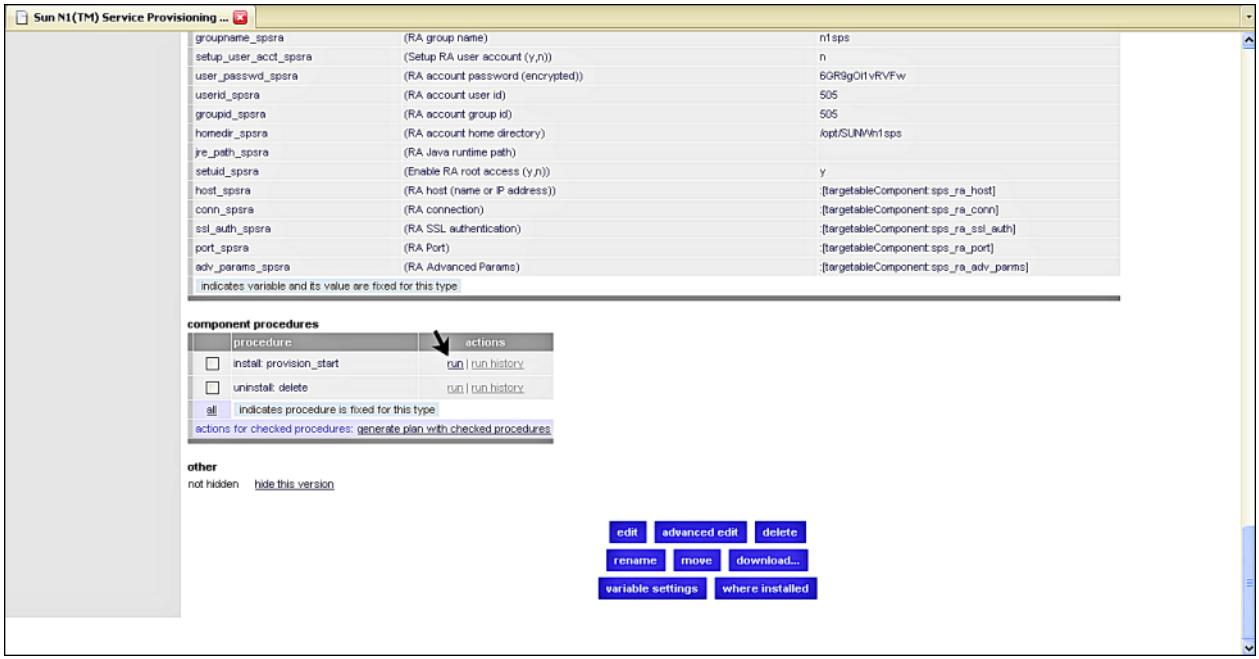

FIGURE 3–29 OS Provisioning Component Details Screen, Selecting Run

The Plans Details Run screen appears.

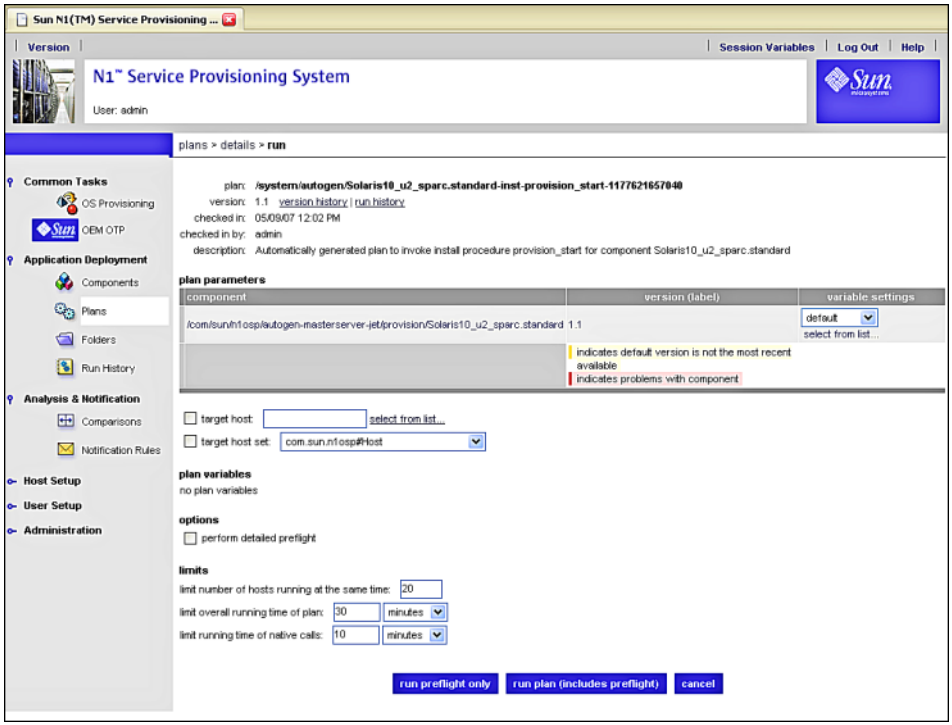

FIGURE 3–30 OS Provisioning Plans Details Run Screen

6 **Click select from list... beneath variable settings.**

The select variable setting from list... screen appears.

7 **Scroll to the bottom of the select variable setting from list screen and click** `create set`**.**

The create set variables screen appears.

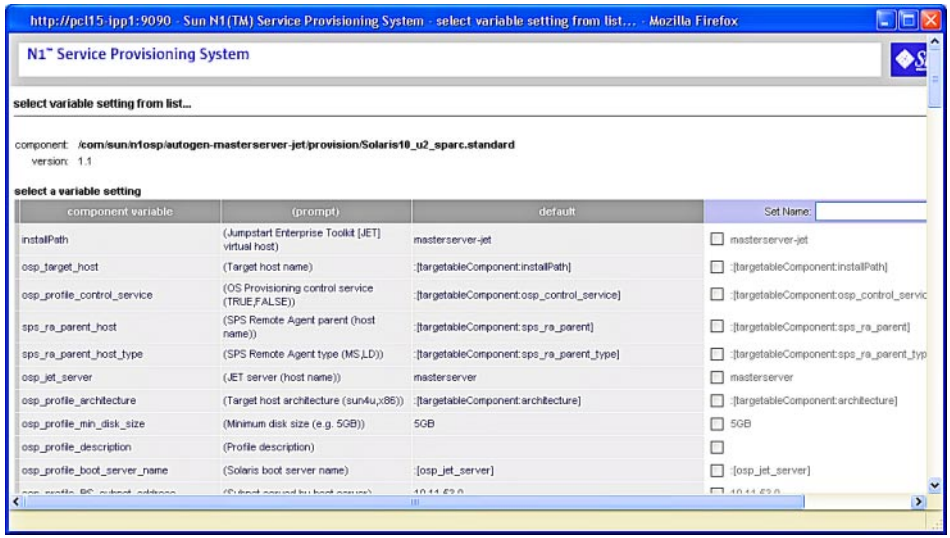

FIGURE 3–31 OS Provisioning Create Set Variables Screen

8 Enter the values on the Create OS Provisioning Set Variables Screen as follows:

The following list describes only the required fields. All other fields are optional.

a. Type a name for the OS Provisioning variables set in the Set Name field.

For example, *otpclient35–set*. The name must start with an alphabetic character.

b. Click the `profile_cluster_base_config` check box.

Type **`SUNWCXall`** in the field to install Entire Distribution plus OEM.

c. Make certain that the `profile_del_cluster_base_config` check box is unchecked.

d. Click the `profile_swap_base_config` check box.

Type **`4096`** in the field.

e. Click the `profile_s3_mtpt_base_config` check box.

Type **`/globaldevices`** in the field.

f. Click the `profile_s3_size_base_config` check box.

Type **`512`** in the field.

g. Click the `profile_s5_mtpt_base_config` check box.

Clear the field.

h. Click the `profile_s6_mtpt_base_config` check box.

Clear the field.

i. Click the `profile_s7_mtpt_base_config` check box.

Clear the field.

j. Click the `profile_s7_size_base_config` check box.

Type **128** in the field.

k. Click the `sysidcfg_root_password_base_config` check box.

Copy and paste the encrypted root password from the file `/etc/shadow` in to the field.

For further information about generating and entering encrypted passwords, see "Password Encryption" in *Sun N1 Service Provisioning System User's Guide for OS Provisioning Plug-In 3.1*.

l. Click the `install_spsra` and `setuid_spsra` check boxes.

Type **n** in both fields to prevent installation of the service provisioning remote agent. The remote agent is installed at a later point.

m. Click the `packages_m_custom` check box.

Note – This key is displayed only if the JET server custom modules were included in the OS Profile.

Type **`SUNWotpra SUNWotpcli SUNWotputil`** to install the required OTP packages.

The `SUNWotpra` package is required in order to install the remote agent after the Solaris OS installation completes.

9 Click save.

10 Click the right-most select button.

The create set screen closes, and the variable set name you created is displayed in the OS Provisioning Plans Details Run screen variable settings field.

11 Click on the target host field `select from list...` link on the Settings Plan Run screen.

The select hosts from list screen appears.

12 Click the names of the hosts you want to jumpstart.

13 **Click add hosts to main window.**

The select hosts from list screen closes, and the hosts you selected are added to the Plans Details Run screen.

14 **Click** `run plan (includes preflight).`

The OS provisioning plan will take a few minutes to complete. OS provisioning takes about a hour to complete.

To check the OS provisioning status:

a. **In the Common Tasks section of the N1 SPS browser interface, select OS Provisioning.**

b. **On the OS Provisioning Common Tasks page, click Status in the OS Provisioning Administration Tasks section.**

c. **On the Plans Details page, click Run.**

d. **On the Plan Details Run page, select the OTP host on which you provisioned the OS.**

e. **Click run plan (includes preflight).**

f. **Follow the Details links to view the status.**

When the plan completes, the results screen appears. Click Done.

Note – The OSP plug-in also installs the `SUNWotpra`, `SUNWotpcli`, and `SUNWotputil` packages. You do not need to add the `SUNWotpcli` package or setup the remote agent on the target host as these steps are done as part of the post OS installation processing by the OSP plug-in.

Next Steps

- Configure the Solaris OS on the OTP host as described in "Configuring Solaris 10 Update 2" on page 94.
- If you did not create the `/globaldevices` file system on the OTP host, create the file system as described in "Creating the `/globaldevices` File System on the OTP Hosts" on page 100.
- If the OTP host is a Sun Fire T2000, install the OTP patches on the OTP host as described in "Installing the Open Telecommunications Platform Patches On Sun Fire T2000 Servers" on page 99.

When you have completed configuring Solaris 10 Update 2 on each new OTP host, install the Open Telecommunications Platform on the OTP host.

- To install OTP on one or more OTP hosts using the command line, see Chapter 4, "Installing the Open Telecommunications Platform For the First Time Using the Command Line"
- To install OTP on one or more OTP hosts using the graphical user interface, see Chapter 5, "Installing the Open Telecommunications Platform For the First Time Using the Graphical User Interface"
- To install OTP on one or more OTP hosts using a production standalone or clustered OTP system, see Chapter 6, "Installing the Open Telecommunications Platform Using the Provisioning Service On an Existing OTP System"

Installing the Solaris OS and Remote Agent on a New OTP Host Using the External Installation Server OSP Plug-in Command Line Interface

This section provides the procedures for using the OSP plug-in command line interface on the external OTP installation server to install the Solaris OS and the service provisioning remote agent on a new OTP host.

The following topics are discussed:

Tip – Add `/var/otp/spsotp/N1_Service_Provisioning_System_5.2/cli/bin` to the root account PATH statement before performing the following procedures. Type **`rehash`** after you have set the path.

The following procedures assume you have added `/var/otp/spsotp/N1_Service_Provisioning_System_5.2/cli/bin` to the root account PATH statement in the root account initialization script.

▼ To Create and Register the Subnet

For detailed instructions, "Creating and Registering the Subnet" in *Sun N1 Service Provisioning System User's Guide for OS Provisioning Plug-In 3.1*.

1. **Log in as root (`su - root`) to the external OTP installation server.**

2. **Create the subnet variable list.**

   Type the command

   `cr_cli -cmd cdb.vs.add -comp NM:/com/sun/n1osp/untyped/Subnet -name "`*subnet_name*`" -u admin -p admin -vars "installPath=`*install path IP adddress*`;mask=`*subnet mask IP address*`;gateway=`*gateway IP address*`;host_interface=`*interface name*`;host_address=`*host IP address*`"`

   where:

   - *subnet_name* is the name of the subnet , for example *subnet53*
   - *install path IP adddress* is the base IP address of the subnet, for example *10.11.53.0*.
   - *subnet mask IP address*is the subnet mask, for example *255.255.255.0*.
   - *gateway IP address* is the subnet gateway IP address, for example *10.11.53.1*.
   - *interface name* is the name of the provisioning interface of the external OTP installation server, for example *bge0*. Do not specify the logical interface.
   - *host IP address* is the IP address of the provisioning interface, for example *10.11.53.200*.

3. **Initialize the subnet.**

   Type the command

   `cr_cli -cmd pe.p.run -u admin -p admin -PID NM:/com/sun/n1osp/untyped/Subnet-create -tar H:NM:masterserver-osp -comp - -vs `*subnet_name*` -pto 30 -nto 10`

   where *subnet_name* is the name of the subnet , for example *subnet53*.

Next Steps Create the Solaris 10 Update 2 image as described in the next procedure.

▼ To Create the Solaris 10 Update 2 Image

For detailed instructions, see "Creating Solaris Images and Profiles" in *Sun N1 Service Provisioning System User's Guide for OS Provisioning Plug-In 3.1*.

1. **Log in as root (`su - root`) to the external OTP installation server.**

2. **Create the Solaris OS image import variable list.**

   Type the command

   `cr_cli -cmd cdb.vs.add -comp NM:/com/sun/n1osp/untyped/SolarisImage -name "`*image name*`" -u admin -p admin -vars "version=`*OS version*`;release=`*OS*

release;architecture=*architecture*;image_subnet_addr=*image subnet adress*;image_subnet_mask=*subnet mask*;media_src=*media_source*;ISO_files=*OS ISO file name*"

where:

- *image name* is the name assigned to the imported Solaris OS image, for example *s10u2*.
- *OS version* is the Solaris OS version number, for example *10*.
- *OS release* is the Solaris OS release, for example *u2*.
- *architecture* is the platform architecture for the Solaris OS, for example *sparc*
- *image subnet adress* is the IP address of the server on which the OS image is to be copied, for example *10.11.53.200*.
- *subnet mask* is the subnet mask IP address, for example *255.255.255.0*.
- *media_source* is the full path to the source Solaris OS image. This can be an NFS-mounted ISO image as described in "To Download and Uncompress the OTP and Solaris OS Installation Zip Files" on page 42
- *OS ISO file name* is the name of Solaris OS ISO image, for example *sol-10-u2-ga-sparc-dvd.iso*

3 Import the Solaris OS image.

Type `cr_cli -cmd pe.p.run -u admin -p admin -PID NM:/com/sun/n1osp/untyped/SolarisImage-import -tar H:NM:masterserver-jet -comp + -vs` *s10u2* `-pto 300 -nto 100` where *s10u2* is the name you assigned to the import image in the previous step.

Next Steps Create the Solaris OS provisioning profile as described in the next step.

▼ To Create the Solaris OS Provisioning Profile

1 Log in as root (`su - root`) to the external OTP installation server.

2 Type the following command to populate the custom packages with the appropriate JET path:

`/opt/SUNWjet/bin/copy_custom_packages` */OTP_media_path*`/Products/packages sparc SUNWotpra SUNWotpcli SUNWotputil`

where */OTP_media_path* is the fully-qualifed path to the OTP installation directory you created in "To Create the OTP Installation Directory on the External OTP Installation Server" on page 45. For example:

```
# /opt/SUNWjet/bin/copy_custom_packages \
/otp1.1/Products/packages sparc SUNWotpra SUNWotpcli SUNWotputil
```

The media is copied to the directory `/export/install/pkgs/custom/sparc` by default. To change the default directory, modify the setting in `/opt/SUNWjet/etc/jumpstart.conf`.

For further information, see Chapter 5, "Provisioning the Solaris Operating System," in *Sun N1 Service Provisioning System User's Guide for OS Provisioning Plug-In 3.1*.

3 Create the file `/tmp/solaris-profile` with the following text.

```
standard
Standard Solaris
base_config spsra custom
true
```

Save and close the file.

4 Type the following command to create the OS profile.

```
# cr_cli -cmd pe.p.run -u admin -p admin \
-PID NM:/com/sun/n1osp/untyped/SolarisImage-create-profile \
-tar H:NM:masterserver-jet -comp + -vs s10u2  -pto 300 -nto 300 \
-f /tmp/solaris-profile
```

For further information, see "Creating Solaris Images and Profiles" in *Sun N1 Service Provisioning System User's Guide for OS Provisioning Plug-In 3.1*.

Note – Ensure that the provisioning profiles specify Entire Distribution Plus OEM and that the profiles partition the OTP host disk drive as described in Table 3–1.

Next Steps Create the ALOM target host as described in the next procedure.

▼ To Create the ALOM Target Host

1 Log in as root (`su - root`) to the external OTP installation server.

2 Create the encrypted password for the ALOM account.

Create the encrypted password as described in "Password Encryption" in *Sun N1 Service Provisioning System User's Guide for OS Provisioning Plug-In 3.1*. For example, if the ALOM account password is admin, you would type:

```
# /opt/SUNWn1osp/sbin/n1osp_encrypter admin
    Encrypted Text: Clz6pK2b6qw=
```

You will need the encrypted password in the next step.

3 Type the following command to create the ALOM target host variable set.

`cr_cli -cmd cdb.vs.add -comp NM:/com/sun/n1osp/targets/SunALOM -name "`*new OTP host name*`" -u admin -p admin -vars "installPath=`*new OTP host name*`;ethernet_mac_address=`*MAC address*`1;ethernet_ip_address=`*IP address*`; alom_ip_address=`*ALOM IP address*`;alom_access_userid=admin;alom_access_password=`*encrypted password*`"` where:

- *new OTP host name* is the name of the new OTP host
- *MAC address* is the new OTP host MAC address
- *IP address* is the new OTP host provisioning interface IP address
- *ALOM IP address* is the ALOM interface IP address
- *encrypted password* is the encrypted password you generated in the previous step

For example

```
# cr_cli -cmd cdb.vs.add -comp NM:/com/sun/n1osp/targets/SunALOM \
-name "pcl1-ipp1" -u admin -p admin \
-vars "installPath=pcl1-ipp1;ethernet_mac_address=0:3:ba:9:6a:51;\
ethernet_ip_address=10.11.52.61;\alom_ip_address=10.11.52.51;\
alom_access_userid=admin;alom_access_password=Clz6pK2b6qw="
```

4 Create the file `/tmp/`*OTP hostname*.

For example, `/tmp/pcl1-ipp1`

Add the following four lines to the file.

```
true
admin
false
admin
```

The second line is the password for the new OTP host ALOM. The fourth line is the password for the external OTP installation server.

Save and close the file.

5 Type the following command to create the ALOM target.

```
#  cr_cli -cmd pe.p.run -u admin -p admin \
-PID NM:/com/sun/n1osp/targets/SunALOM-create \
-tar H:NM:masterserver-osp -comp + -vs pcl1-ipp1 -pto 300 \
-nto 100 -f /tmp/OTP hostname
```

where *OTP hostname* is the name of the file you created in the previous step.

For detailed information, see "Example Tasks for Defining Target Hosts" in *Sun N1 Service Provisioning System User's Guide for OS Provisioning Plug-In 3.1* and "Sun ALOM Target Host Variables" in *Sun N1 Service Provisioning System User's Guide for OS Provisioning Plug-In 3.1*.

Next Steps Install the Solaris OS on the new OTP host as described in the next procedure.

▼ To Install the Solaris OS on a New OTP Host

1 Log in as root (`su - root`) to the external OTP installation server.

2 Type the following command to create the OS provisioning variables set.

```
# cr_cli -cmd cdb.vs.add \
-comp NM:/com/sun/n1osp/autogen-masterserver-jet/provision/Solaris10_u2_sparc.standard \
-name "variables set name" -u admin -p admin \
-vars "sysidcfg_default_route_base_config=default router IP address;\
sysidcfg_root_password_base_config=encryped OTP host password;\
profile_cluster_base_config=SUNWCXall;profile_del_clusters_base_config=;\
profile_swap_base_config=4096;profile_s3_mtpt_base_config=/globaldevices;\
profile_s3_size_base_config=512;profile_s5_mtpt_base_config=;\
profile_s6_mtpt_base_config=;profile_s7_mtpt_base_config=;\
profile_s7_size_base_config=128;install_spsra=n;setuid_spsra=n;\
packages_m_custom=SUNWotpra SUNWotpcli SUNWotputil
```

where

- *variables set name* is the name to be assigned to the variables set, for example sfv240–target.
- *default router IP address* is the IP address of the default router, for example 10.11.12.0.
- *encryped OTP host password* is the encrypted password, which can be copied from the file `/etc/shadow`.

3 Type the following command to provision the OS to the new OTP host.

```
# cr_cli -cmd pe.p.run -u admin -p admin -PID \
NM:/com/sun/n1osp/autogen-masterserver-jet/provision/SolarisProfile-provision-start-Solaris10_u2_sparc.standard \
-tar H:NM:variables set name -comp + -vs new OTP host host name -pto 600 -nto 600
```

where *variables set name* is the name you assigned to the variables set in the previous step, and *new OTP host host name* is the name of the new OTP host to which the OS is to be provisioned.

Repeat this step for each new OTP host.

For detailed instructions, see "Installing the Solaris OS on the Target Host" in *Sun N1 Service Provisioning System User's Guide for OS Provisioning Plug-In 3.1* and Appendix B, "Solaris Profile Component Variables," in *Sun N1 Service Provisioning System User's Guide for OS Provisioning Plug-In 3.1*

Note – The OSP plug-in also installs the `SUNWotpra`, `SUNWotpcli`, and `SUNWotputil` packages. You do not need to add the `SUNWotpcli` package or setup the remote agent on the target host as these steps are done as part of the post OS installation processing by the OSP plug-in.

Next Steps

- Configure the Solaris OS on the OTP host as described in "Configuring Solaris 10 Update 2" on page 94.
- If you did not create the `/globaldevices` file system on the OTP host, create the file system as described in "Creating the `/globaldevices` File System on the OTP Hosts" on page 100.
- If the OTP host is a Sun Fire T2000, install the OTP patches on the OTP host as described in "Installing the Open Telecommunications Platform Patches On Sun Fire T2000 Servers" on page 99.

When you have completed installing and configuring Solaris 10 Update 2 on each OTP host, install the Open Telecommunications Platform on the OTP host.

- To install OTP on one or more OTP hosts using the command line, see Chapter 4, "Installing the Open Telecommunications Platform For the First Time Using the Command Line"
- To install OTP on one or more OTP hosts using the graphical user interface, see Chapter 5, "Installing the Open Telecommunications Platform For the First Time Using the Graphical User Interface"
- To install OTP on one or more OTP hosts using a production standalone or clustered OTP system, see Chapter 6, "Installing the Open Telecommunications Platform Using the Provisioning Service On an Existing OTP System"

Configuring Solaris 10 Update 2

After completing installation of Solaris 10 Update 2 on the external OTP installation server or on an OTP host, you must configure Solaris 10 Update 2 as described in the following procedures before you can install the Open Telecommunications Platform on the OTP host.

▼ To Update the `/etc/default/nfs` file

The Open Telecommunications Platform supports only NFS version 3. To ensure system integrity and availability, update the `/etc/default/nfs` file as follows:

1 log in as root (`su - root`) to the server.

2. **Add the following line to the file `/etc/default/nfs`:**

   ```
   NFS_SERVER_VERSMAX=3
   ```

3. **Save and close the `/etc/default/nfs` file.**

Next Steps Update the `/etc/hosts` file as described in the next procedure.

▼ To Update the `/etc/hosts` file

The IP address and the name of the server must be added to the `/etc/hosts` on that server. Failure to add the IP address and name will cause Open Telecommunications Platform installation to fail.

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

2. **Verify that the `/etc/hosts` file has entries for loopback and the server primary and secondary Ethernet interfaces.**

   a. **Make certain that either of the following loopback entries is in the `/etc/hosts` file.**

      ```
      127.0.0.1    localhost
      ```

      or

      ```
      127.0.0.1    localhost.localdomain    localhost
      ```

   b. **Make certain that an entry exists for the server primary and secondary Ethernet IP address.**

      For example:

      111.11.111.11 server_name_interface1.domain_name
      111.11.111.22 server_name_interface2.domain_name

      where:

      - *111.11.111.11* is the IP address of the primary Ethernet interface
      - *server_name_interface1* is the primary name of the server being configured such as the external OTP installation server, the first OTP host, or the additional OTP host
      - *111.11.111.22* is the IP address of the secondary Ethernet interface
      - *server_name_interface2* is the secondary name of the server being configured
      - *domain_name* is your corporate domain name

The `/etc/hosts` should be similar to the following example.

```
127.0.0.1    localhost.localdomain    localhost
10.11.123.15  management-server.company.com
10.11.123.16  management-server-port2.company.com
```

c. Save and close the `/etc/hosts` file.

3 Reboot the server.

Next Steps Ensure port 162 is not in use as described in the next procedure.

▼ To Determine Whether Port 162 is in use

The OTP system management service requires exclusive use of port 162 for SNMP trap notifications. To determine if port 162 is assigned to any process, proceed as follows:

1 log in as root (`su - root`) to the server.

2 Type `grep 162 /etc/services` to determine whether port 162 has been assigned to a process.

- If only the command prompt is returned, then port 162 has not been assigned to a process. No further action is required.
- If port 162 is assigned to a process on the server, then results similar to the following are displayed:

```
# grep 162 /etc/services
snmpd     162/udp    daemon name     #daemon description
```

You must disable the daemon or the application that is using port 162. To disable a daemon, refer to the operating system documentation. To disable an application that is using the port, refer to the application documentation.

Next Steps Enable FTP on the server as described in the next procedure.

▼ To Enable FTP

To manage clustered OTP systems using the OTP system management service, you must enable the FTP service.

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

2 **Enable the FTP service by typing the command** `svcadm -v enable network/ftp`**.**

The FTP service is enabled, and starts when the server is rebooted. After the system is rebooted, you can verify whether the FTP service has start using the `inetadm` command:

```
# inetadm | grep network/ftp
enabled   online         svc:/network/ftp:default
```

Next Steps Label all the disks available in the new OTP host.

▼ To Label All the Disks Available in the New OTP Host

The Open Telecommunications Platform requires all the available disks to be labeled prior to the Sun OTP deployment. The boot disk is already labeled and should be excluded from the procedure. For all the remaining disks, perform the following steps.

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

2 **Start the** `format` **utility. The output similar to the following will be displayed:**

```
# format
Searching for disks...done


AVAILABLE DISK SELECTIONS:
       0. c1t0d0 <SUN72G cyl 14087 alt 2 hd 24 sec 424>
          /pci@1f,700000/pci@0/pci@2/pci@0/pci@8/LSILogic,sas@1/sd@0,0
       1. c1t1d0 <SUN72G cyl 14087 alt 2 hd 24 sec 424>
          /pci@1f,700000/pci@0/pci@2/pci@0/pci@8/LSILogic,sas@1/sd@1,0
       2. c2t8d0 <SUN72G cyl 14087 alt 2 hd 24 sec 424>
          /pci@1f,700000/pci@0/pci@2/pci@0/pci@8/scsi@2/sd@8,0
       3. c2t9d0 <SUN72G cyl 14087 alt 2 hd 24 sec 424>
          /pci@1f,700000/pci@0/pci@2/pci@0/pci@8/scsi@2/sd@9,0
       4. c2t10d0 <SUN72G cyl 14087 alt 2 hd 24 sec 424>
          /pci@1f,700000/pci@0/pci@2/pci@0/pci@8/scsi@2/sd@a,0
       5. c2t11d0 <SUN72G cyl 14087 alt 2 hd 24 sec 424>
          /pci@1f,700000/pci@0/pci@2/pci@0/pci@8/scsi@2/sd@b,0
Specify disk (enter its number):
```

3 **Select the disk that needs to be labeled by entering its number:**

```
Specify disk (enter its number): 3
selecting c2t9d0
[disk formatted]
Disk not labeled.  Label it now?
```

4 **Enter `y`.**

Note – If there is no “Disk not labeled. Label it now?” prompt, it means that the disk was previously labeled and no further action is required for it. Go to step 5

```
Disk not labeled.  Label it now? y


FORMAT MENU:
        disk       - select a disk
        type       - select (define) a disk type
        partition  - select (define) a partition table
        current    - describe the current disk
        format     - format and analyze the disk
        repair     - repair a defective sector
        label      - write label to the disk
        analyze    - surface analysis
        defect     - defect list management
        backup     - search for backup labels
        verify     - read and display labels
        save       - save new disk/partition definitions
        inquiry    - show vendor, product and revision
        volname    - set 8-character volume name
        !<cmd>    - execute <cmd>, then return
        quit
format>
```

5 To label another disk enter `disk` and repeat steps 3 and 4. If all disks are already labeled then type `quit` to close the format utility.

```
format> disk

AVAILABLE DISK SELECTIONS:
       0. c1t0d0 <SUN72G cyl 14087 alt 2 hd 24 sec 424>
          /pci@1f,700000/pci@0/pci@2/pci@0/pci@8/LSILogic,sas@1/sd@0,0
       1. c1t1d0 <SUN72G cyl 14087 alt 2 hd 24 sec 424>
          /pci@1f,700000/pci@0/pci@2/pci@0/pci@8/LSILogic,sas@1/sd@1,0
       2. c2t8d0 <SUN72G cyl 14087 alt 2 hd 24 sec 424>
          /pci@1f,700000/pci@0/pci@2/pci@0/pci@8/scsi@2/sd@8,0
       3. c2t9d0 <SUN72G cyl 14087 alt 2 hd 24 sec 424>
          /pci@1f,700000/pci@0/pci@2/pci@0/pci@8/scsi@2/sd@9,0
       4. c2t10d0 <SUN72G cyl 14087 alt 2 hd 24 sec 424>
          /pci@1f,700000/pci@0/pci@2/pci@0/pci@8/scsi@2/sd@a,0
       5. c2t11d0 <SUN72G cyl 14087 alt 2 hd 24 sec 424>
          /pci@1f,700000/pci@0/pci@2/pci@0/pci@8/scsi@2/sd@b,0
Specify disk (enter its number)[3]:
```

Next Steps

- Ensure that each OTP system server and storage device meets the firmware versions requirements listed in "OTP System Hardware and Firmware Requirements" on page 25. If necessary, update the server and storage firmware as directed by the hardware documentation.
- If one or more of your OTP system servers is a Sun Fire T2000 server, you must install the `e1000g` transition patches 118833-24 and 123334-04 on each Sun Fire T2000 as described in the next section before installing the Open Telecommunications Platform.

  If your clustered OTP systems do not include any Sun Fire T2000 servers, go to "Creating the `/globaldevices` File System on the OTP Hosts" on page 100.

Installing the Open Telecommunications Platform Patches On Sun Fire T2000 Servers

▼ To Install Required Patches On Sun Fire T2000 Servers

Before You Begin

- The Solaris 10 Update 2 OS must be installed on each T2000 as described in "Setting Up the External OTP Installation Server" on page 44
- The T2000 and storage device firmware versions must be at the required version levels as described in "OTP System Hardware and Firmware Requirements" on page 25

1. **Log in as root (`su - root`) to the Sun Fire T2000.**
2. **Open a web browser and download the following two patches from `http://sunsolve2.central.sun.com/pub-cgi/show.pl?target=patches/patch-access`.**
   - 118833-24
   - 123334-04
3. **Change directory to the directory in which you downloaded the T2000 patches.**
4. **Type `patchadd 118833-24` to install the first patch.**

   Wait for patch installation to complete.
5. **Type `patchadd 123334-04` to install the second patch.**

   Wait for patch installation to complete.
6. **Type `init s` to enter single user mode.**

7 **Type `/usr/sbin/e1000g_transition -e -f` to complete the transition to the e1000g driver.**

You are asked whether you want to reboot.

8 **Type y to reboot.**

Next Steps Ensure that the `/globaldevices` file system has been created on each clustered OTP system as described in the next section.

Creating the `/globaldevices` File System on the OTP Hosts

If you have not partitioned each clustered OTP system server's hard drive to include the `/globaldevices` file system as described in Table 3–1 when installing Solaris 10 Update 2, then you must create and configure the `/globaldevices` file system on each server in order to enable management of global devices.

The OTP high availability framework requires the `/globaldevices` file system on one of the local disks on each clustered OTP system server's hard drive. The `/globaldevices` file system is later mounted as the OTP cluster file system.

For further information about global devices, see the *Sun Cluster Concepts Guide for Solaris OS*. For information on planning for the global devices file system, see *Sun Cluster Software Installation Guide for Solaris OS*.

Skip the following procedure If you have already created a `/globaldevices` file system containing at least 512 Mbytes on the hard drive of each of the clustered OTP systems.

▼ To Create the `/globaldevices` File System on the OTP SystemServers

If you have not allocated the `/globaldevices` file system on one of the local disks on each clustered OTP system server, then you must perform the following procedure on each server in the clustered OTP system.

1 **Log on to the server as root (`su - root`)**

2 **Type `newfs /dev/dsk/c0t0d0s3` to create the cluster file system**

Note – In this step and the following steps, the file system is mounted on disk slice 3. You can create and mount the file system on any available slice.

If the server has more than one disk, the `/globaldevices` file system can be created on a disk other than the disk containing the root file system.

3. **Add the following line to the file `/etc/vfstab`.**

```
/dev/dsk/c0t0d0s3 /dev/rdsk/c0t0d0s3   /globaldevices   ufs   2   no   global,logging
```

4. **Type `mkdir /globaldevices` to create the cluster global devices directory.**

5. **Type `mount /globaldevices` to mount the `/globaldevices` file system**

Next Steps When you have completed installing and configuring Solaris 10 Update 2 on each OTP host, install the Open Telecommunications Platform on the OTP host.

- To install OTP on one or more OTP hosts using the command line, see Chapter 4, "Installing the Open Telecommunications Platform For the First Time Using the Command Line"
- To install OTP on one or more OTP hosts using the graphical user interface, see Chapter 5, "Installing the Open Telecommunications Platform For the First Time Using the Graphical User Interface"
- To install OTP on one or more OTP hosts using a production standalone or clustered OTP system, see Chapter 6, "Installing the Open Telecommunications Platform Using the Provisioning Service On an Existing OTP System"

◆ ◆ ◆ CHAPTER 4

Installing the Open Telecommunications Platform For the First Time Using the Command Line

This chapter provides the command-line procedures for installing and configuring the Open Telecommunications Platform 1.1.

The following topics are discussed:

This section discusses the following topics:

Command-line Installation and Configuration Overview

This section provides summaries of the high-level tasks that you will perform as part of the Open Telecommunications Platform site preparation, installation, configuration, and run time processes.

The following diagram illustrates the sequence of the high-level tasks for site planning, installation and configuration of the Open Telecommunications Platform software.

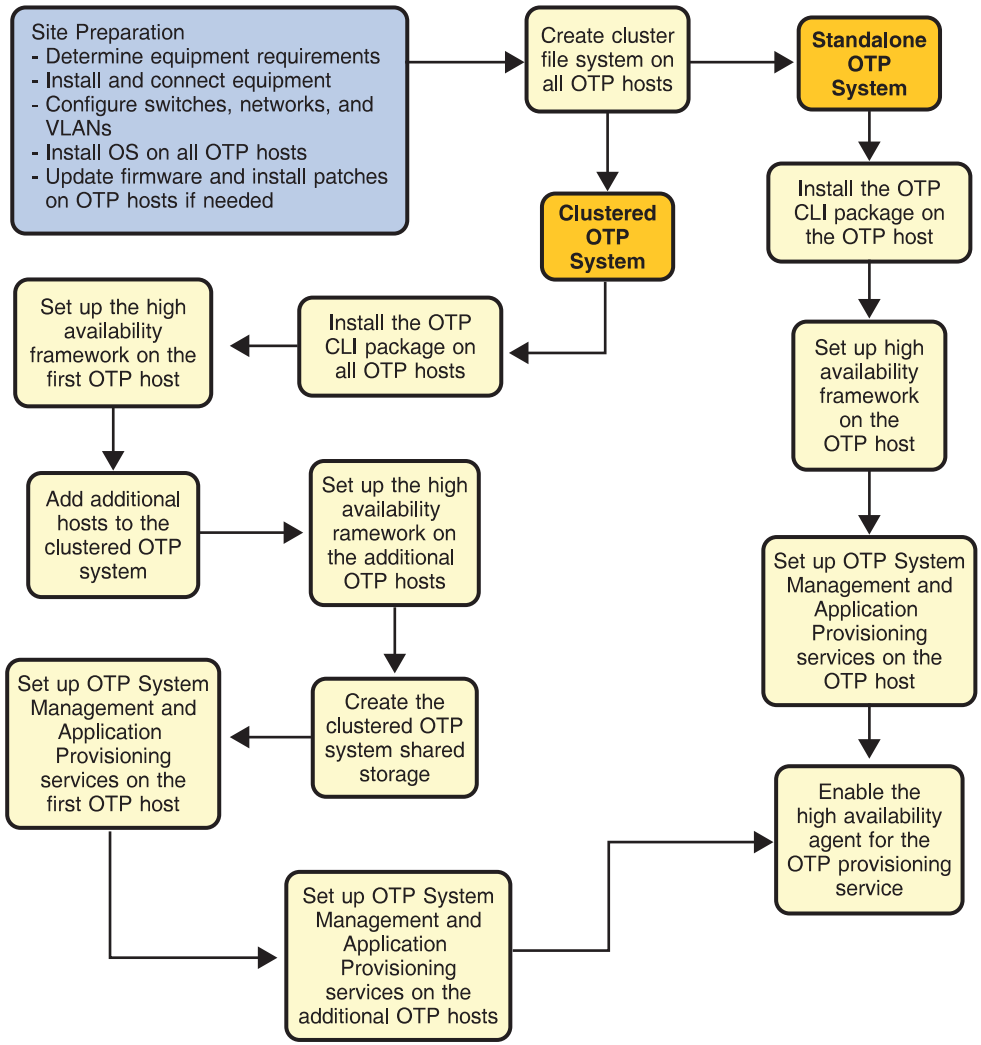

FIGURE 4–1 Open Telecommunications Platform Site Preparation Task Flow

Open Telecommunications Platform Installation Prerequisites

The following prerequisites must be met before you can install the Open Telecommunications Platform using the command line.

- The external OTP installation server must be set up and configured as described in "Setting Up the External OTP Installation Server" on page 44.
- Solaris 10 Update 2 must be installed and configured on each OTP system server as described in "Installing Solaris 10 Update 2 and the Remote Agent on the OTP Hosts" on page 50.
- A naming service such as NIS, NIS+, or `/etc/hosts` must be set up and all host names and IP addresses must be set up on that naming service.
- All OTP system servers and storage devices must meet the minimum patch and firmware requirements as described in "OTP System Hardware and Firmware Requirements" on page 25.

Installing the Open Telecommunications Platform on a Standalone OTP Host

This section provides the procedures for using the command line to install the Open Telecommunications Platform on a standalone OTP host.

▼ To Install the Open Telecommunications Platform on a Standalone OTP Host

Before You Begin Before you begin, review the OTP Plan settings described in "Open Telecommunications Platform Plan Worksheets" on page 30 and then print out the "Standalone OTP Host Plan Worksheet" on page 34 and fill in the values based on the standalone OTP host to which you will install OTP

1. **Log in as root (`su - root`) on the external OTP installation server.**

2. **Copy the `inputOTPSingleNode.dat` file to `/var/tmp`.**

   Type the command **`cp /opt/SUNWotp10/CLI/templates/inputOTPSingleNode.dat /var/tmp`**

3. **Edit the `/var/tmp/inputOTPSingleNode.dat` file.**

   Specify the values for each keyword as described by "Open Telecommunications Platform Plan Worksheets" on page 30 and the standalone OTP host Plan worksheet.

4 **Run the `deployOTPSingleNode` script on the external OTP installation server to install OTP on the standalone OTP host.**

```
# /opt/SUNWotp10/CLI/deployOTPSingleNode /var/tmp/inputOTPSingleNode.dat
```

The `deployOTPSingleNode` script does the following tasks:

- Sets up the OTP High Availability Framework
- Sets up the OTP System Management and Application Provisioning Services
- Enables High Availability for the OTP Provisioning Service

Note – The installation log files and input files generated for the plans are stored on the external OTP installation server in the directory `/var/tmp/OTP_INSTALL`.

---

5 **Log in as root to the standalone OTP host and restart the remote agent.**

Type **`/etc/init.d/n1spsagent restart`** to restart the remote agent. If the remote agent is not restarted, then the service provisioning service on the standalone OTP host will not work properly.

This completes installation of the Open Telecommunications Platform on the standalone OTP host.

Installing and Setting Up the Open Telecommunications Platform on a Clustered OTP System

This section provides the procedures for using the command line to install the Open Telecommunications Platform on the OTP hosts in a clustered OTP system.

Installing and configuring OTP on a clustered OTP system is comprised of the following tasks:

- Installing the Open Telecommunications Platform On a Clustered OTP System
- Configuring the Quorum Disk on a Two-Host Cluster
- Creating Clustered OTP System Shared Storage
- Completing and Validating Open Telecommunications Platform Installation

▼ To Install the Open Telecommunications Platform on a Clustered OTP System

Before You Begin Before you begin, review the OTP Plan settings described in "Open Telecommunications Platform Plan Worksheets" on page 30 and then print out the "Clustered OTP Host Plan Worksheet" on page 36 and fill in the values based on the clustered OTP system to which you will install OTP

1 **Log in as root (`su - root`) on the external OTP installation server.**

2 **Copy the `inputOTPMultiNode.dat` file to `/var/tmp`.**

Type the command `cp /opt/SUNWotp10/CLI/templates/inputOTPMultiNode.dat /var/tmp`

3 **Edit the `/var/tmp/inputOTPMultiNode.dat`.**

Specify the values for each keyword as described by "Open Telecommunications Platform Plan Worksheets" on page 30 and the clustered OTP host Plan worksheet.

4 **Run the `deployOTPMultiNode` script on the external OTP installation server to install OTP on the OTP hosts in the clustered OTP system.**

```
# /opt/SUNWotp10/CLI/deployOTPMultiNode /var/tmp/inputOTPMultiNode.dat
```

The `deployOTPMultiNode` script does the following tasks:

- Sets up the OTP High Availability Framework on the first OTP host
- Adds additional OTP hosts to the clustered OTP system
- Sets up the OTP High Availability Framework on the additional OTP hosts

---

Note – The installation log files for this procedure and subsequent procedures, and the input files generated for the plans by the procedures are stored on the external OTP installation server in the directory `/var/tmp/OTP_INSTALL`.

Next Steps

- If you chose `no` for `Quorum Auto Configuration` on a two-host cluster, you must manually select and configure the quorum disk as described in the following procedure.
- If you are setting up a three-host or more clustered OTP system, quorum disk configuration is optional. Go to "To Configure the Quorum Disk on a Two-Host Cluster" on page 107.

▼ To Configure the Quorum Disk on a Two-Host Cluster

If you chose `no` for `Quorum Auto Configuration` on a two-host cluster, you must manually select and configure the quorum disk as described in this procedure.

Note – The following sub-steps apply only to a two-host cluster. If you are setting up a three-host or more clustered OTP system, this procedure iis optional.

---

1 **Open a separate terminal window and log in as root to the first OTP host.**

2 **Type `/usr/cluster/bin/scdidadm -L` to display the cluster disk information. For example:**

```
# /usr/cluster/bin/scdidadm -L
                1        otpclient1:/dev/rdsk/c0t8d0     /dev/did/rdsk/d1
                1        otpclient2:/dev/rdsk/c0t8d0     /dev/did/rdsk/d1
                2        otpclient1:/dev/rdsk/c0t9d0     /dev/did/rdsk/d2
```

```
2       otpclient2:/dev/rdsk/c0t9d0     /dev/did/rdsk/d2
3       otpclient1:/dev/rdsk/c1t0d0     /dev/did/rdsk/d3
4       otpclient1:/dev/rdsk/c1t1d0     /dev/did/rdsk/d4
5       otpclient2:/dev/rdsk/c1t0d0     /dev/did/rdsk/d5
6       otpclient2:/dev/rdsk/c1t1d0     /dev/did/rdsk/d6
```

In the above example, disks `d1` and `d2` are shared by both hosts of the two-host cluster. The quorum disk must be a shared disk.

3 Configure a quorum disk.

Type `/usr/cluster/bin/scconf -a -q globaldev=`*shared disk ID* `where` *shared disk ID* is a shared disk ID. For example:

```
# /usr/cluster/bin/scconf -a -q globaldev=d1
```

4 Type `/usr/cluster/bin/scconf -c -q reset` to reset the two-host cluster to normal mode.

Next Steps Create the system shared storage as described in the next procedure.

▼ To Create Shared Storage on the Clustered OTP System

Caution – Set the hard drive variables according to your cluster settings. Failure to do so will result in OTP high availability framework installation failure. The following steps must be performed on each host in your clustered OTP system, including the first OTP host.

1 Create the shared storage meta database on all hosts in the clustered OTP system.

The following steps must be performed for each host in the clustered OTP system.

a. Log in to the as root (`su - root`) on the clustered OTP host.

b. Determine the drive on which root is mounted and the available free space.

Type `prtvtoc 'mount | awk '/^\/ / { print $3 }''` to list the hard drive slices and available space.

For example:

```
# prtvtoc 'mount | awk '/^\/ / { print $3 }''
* /dev/rdsk/c0t0d0s0 partition map
*
* Dimensions:
*     512 bytes/sector
*     424 sectors/track
*      24 tracks/cylinder
*   10176 sectors/cylinder
```

```
*   14089 cylinders
*   14087 accessible cylinders
*
* Flags:
*   1: unmountable
*  10: read-only
*
* Unallocated space:
*       First     Sector    Last
*       Sector     Count    Sector
*    63620352  79728960 143349311
*
*                          First     Sector    Last
* Partition  Tag  Flags    Sector     Count    Sector  Mount Directory
       0      2    00    8201856  51205632  59407487   /
       1      3    01          0   8201856   8201855
       2      5    00          0 143349312 143349311
       3      0    00   59407488   2106432  61513919   /globaldevices
       7      0    00   61513920   2106432  63620351
```

c. Create the database.

Type `metadb -a -f -c 6` *disk slice* where *disk slice* is an available file system.

For example, based on the example in the previous step:

```
# metadb -a -f -c 6 c0t0d0s7
```

2 Create the shared storage files on the first OTP host only.

The first OTP host must be connected to the shared storage.

a. Log in to the first OTP host as root (`su - root`).

b. Type `scdidadm` to determine which disks are seen on all nodes of the clustered OTP system and choose one to be the shared disk to the metaset.

In the following example d4, d5, d6, and d7 are shared disks. They are displayed as connected to more than one node in the listing.

```
# /usr/cluster/bin/scdidadm -L
1   otpclient1:/dev/rdsk/c1t0d0    /dev/did/rdsk/d1
2   otpclient1:/dev/rdsk/c2t0d0    /dev/did/rdsk/d2
3   otpclient1:/dev/rdsk/c2t1d0    /dev/did/rdsk/d3
4   otpclient1:/dev/rdsk/c3t600C0FF000000000092C187A9755BE14d0 /dev/did/rdsk/d4
4   otpclient2:/dev/rdsk/c3t600C0FF000000000092C187A9755BE14d0 /dev/did/rdsk/d4
5   otpclient1:/dev/rdsk/c3t600C0FF000000000092C187A9755BE13d0 /dev/did/rdsk/d5
5   otpclient2:/dev/rdsk/c3t600C0FF000000000092C187A9755BE13d0 /dev/did/rdsk/d5
6   otpclient1:/dev/rdsk/c3t600C0FF000000000092C187A9755BE12d0 /dev/did/rdsk/d6
6   otpclient2:/dev/rdsk/c3t600C0FF000000000092C187A9755BE12d0 /dev/did/rdsk/d6
7   otpclient1:/dev/rdsk/c3t600C0FF000000000092C187A9755BE11d0 /dev/did/rdsk/d7
```

```
7   otpclient2:/dev/rdsk/c3t600C0FF000000000092C187A9755BE11d0 /dev/did/rdsk/d7
8   otpclient2:/dev/rdsk/c1t0d0    /dev/did/rdsk/d8
9   otpclient2:/dev/rdsk/c2t0d0    /dev/did/rdsk/d9
10  otpclient2:/dev/rdsk/c2t1d0    /dev/did/rdsk/d10
```

c. Add the additional OTP hosts.

Type `metaset -s sps–dg -a -h` *otpclient-1 otpclient-n* `where` *otpclient-1 otpclient-n* is the list of OTP hosts separated by a space. For example:

```
# metaset -s sps–dg -a -h otpclient1 otpclient2 otpclient3 \
  otpclient4 otpclient5 otpclient6 otpclient7 otpclient8
```

Caution – Only the nodes connected to the shared storage (displayed as such in the `scdidadm -L` output) should be added to the metaset.

d. Type `metaset -s sps–dg -a` *shared-disk* to add the shared disk to the metaset.

In the following example, the `d7` disk is assigned as the shared disk:

```
# metaset -s sps–dg -a /dev/did/rdsk/d7
```

e. Type `metainit -s sps-dg d0 1 1 /dev/did/rdsk/d7s0`

f. Type `newfs /dev/md/sps–dg/rdsk/d0`

g. On a two-host cluster only, set up the mediator hosts for the `sps-dg` disk group.

Type `metaset -s sps–dg -a -m` *otpclient1 otpclient2* where *otpclient1 otpclient2* are the OTP hosts separated by a space.

Caution – Only the nodes connected to the shared storage (displayed as such in the scdidadm -L output) should be added to the metaset.

h. Type `metaset -s sps-dg` to verify the mediator host setup.

The following example shows hosts `otpclient1` and `otpclient2` set up as mediator hosts.

The following example shows hosts otpclient1 and otpclient2 in a setup for 2 node OTP system or pair + N topology cluster:

```
# metaset
Set name = sps–dg
Host                Owner
  otpclient1         Yes
  otpclient2
Mediator Host(s)    Aliases
  otpclient1
  otpclient2
d7   Yes
```

3 **Update the `/etc/vfstab` file on all OTP hosts.**

The following steps must be performed on each clustered OTP host.

a. **Log in to theOTP host as root (`su - root`).**

b. **Update the `/etc/vfstab` file.**

Type **`echo /dev/md/sps-dg/dsk/d0 /dev/md/sps-dg/rdsk/d0 /var/otp ufs 2 no global,logging >>/etc/vfstab`**

c. **Type `mkdir -p /var/otp`**

Next Steps

- If you are performing a command line installation, complete and validate the Open Telecommunications Platform installation as described in the next procedure.
- If you are performing a graphical user interface installation, set up the system management and provisioning services as described in "To Set Up OTP System Management and Provisioning Services on the First OTP Host" on page 133

▼ To Complete and Validate Open Telecommunications Platform Installation

1 **Log in as root (`su - root`) on the external OTP installation server.**

2 **Rerun the `deployOTPMultiNode` script with the `-cont` option.**

```
# /opt/SUNWotp10/CLI/deployOTPMultiNode -cont /var/tmp/inputOTPMultiNode.dat
```

The `deployOTPMultiNode` script does the following tasks:

- verifies the OTP high availability framework installation and configuration
- Sets up OTP System Management and Application Provisioning Services on the first OTP host
- Sets up System Management and Application Provisioning Services on the additional OTP hosts
- Enables High Availability for the OTP Provisioning Service on the first OTP host

3 **Log in as root on the first OTP host and restart the remote agent.**

Type **`/etc/init.d/n1spsagent restart`** to restart the remote agent. If the remote agent is not restarted, then the service provisioning service on the first OTP host will not work properly.

4 **Configure and enable fail-over.**

a. **Type `/usr/cluster/bin/scrgadm -c -g otp-system-rg -y RG_system=false` to set the `system` property for the `otp-system-rg` resource group to false.**

b. **Type `/usr/cluster/bin/scswitch -F -g otp-system-rg` to take the remote group offline.**

c. **Type the following commands in the sequence shown to disable cluster resources.**

```
/usr/cluster/bin/scswitch -n -j otp-spsms-rs

/usr/cluster/bin/scswitch -n -j otp-spsra-rs

/usr/cluster/bin/scswitch -n -j otp-sps-hastorage-plus

/usr/cluster/bin/scswitch -n -j otp-lhn
```

d. **Type `/usr/cluster/bin/scswitch -u -g otp-system-rg` to put the remote group into the unmanaged state.**

e. **Type `/usr/cluster/bin/scrgadm -c -j otp-spsra-rs -x Stop_signal="15"` to change the `Stop_signal` property of the remote agent resource to 15.**

f. **Type `/usr/cluster/bin/scrgadm -c -j otp-spsms-rs -x Stop_signal="15"` to change the `Stop_signal` property of the management service resource to 15.**

g. **Type `/usr/cluster/bin/scswitch -o -g otp-system-rg` to put the remote group into the managed state.**

h. **Type `/usr/cluster/bin/scswitch -Z -g otp-system-rg` to bring the remote group back online.**

i. **Type `/usr/cluster/bin/scrgadm -c -g otp-system-rg -y RG_system=true` to set the system property for the `otp-system-rg` resource group to true.**

This completes the command line installation of the Open Telecommunications Platform on a clustered OTP system.

◆ ◆ ◆ CHAPTER 5

Installing the Open Telecommunications Platform For the First Time Using the Graphical User Interface

This chapter provides the procedures for using the OTP provisioning service graphical user interface on the external OTP installation server to install and configure Open Telecommunications Platform to your clustered OTP systems.

The following topics are discussed:

Graphical User Interface Installation and Configuration Overview

The following figure provides a summary of the high-level tasks that you will perform as part of the GUI-based Open Telecommunications Platform installation and configuration processes.

The following diagram illustrates the sequence of the high-level tasks for site planning, installation and configuration of the Open Telecommunications Platform.

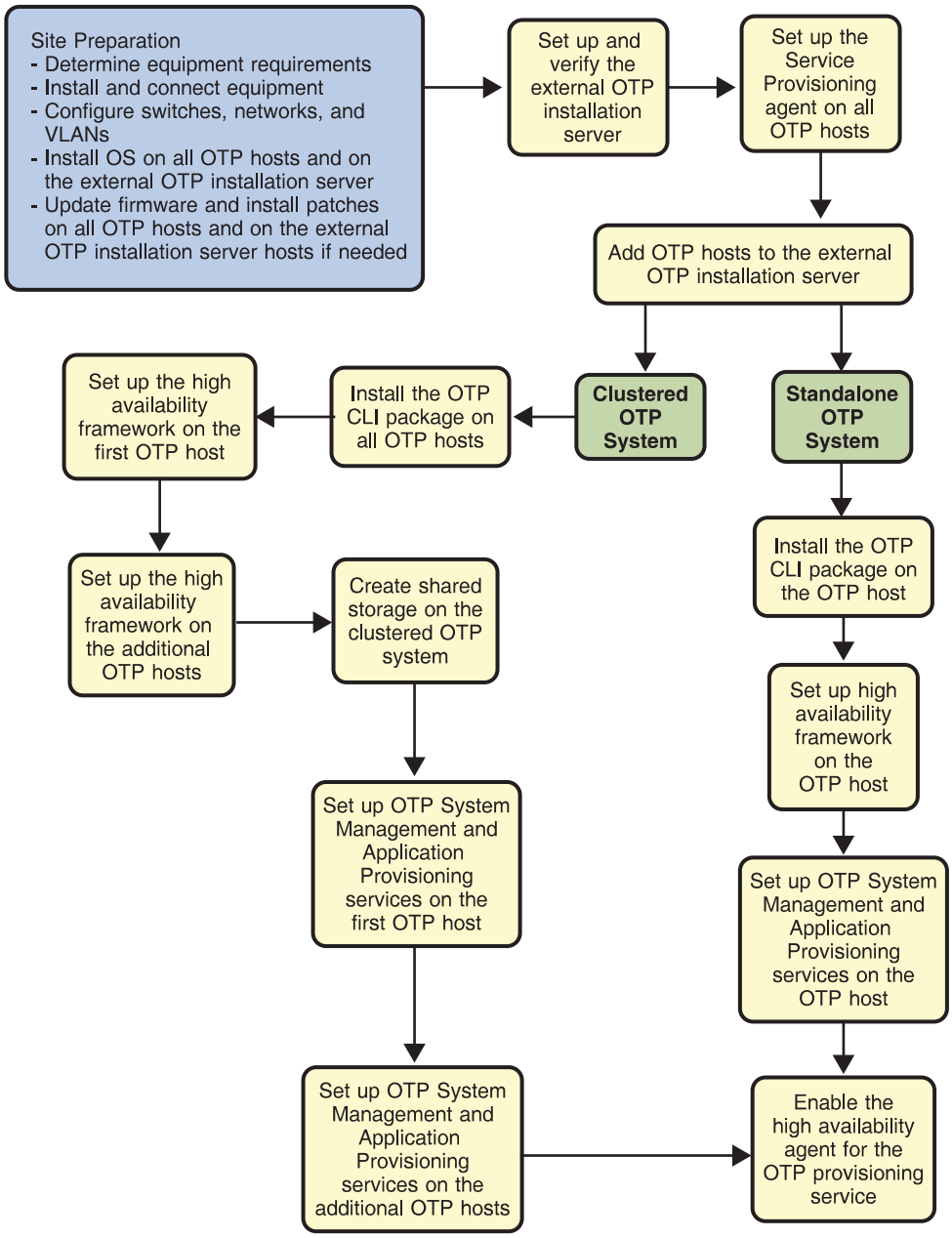

FIGURE 5–1 GUI-Based Open Telecommunications Platform Installation Task Flow

Open Telecommunications Platform Installation Prerequisites

The following prerequisites must be met before you can install the Open Telecommunications Platform using the external OTP installation server graphical user interface.

- The Solaris 10 Update 2 operating system and OSP plug-in must be installed and configured on the external OTP installation server as described in "Setting Up the External OTP Installation Server" on page 44.

Note – External OTP installation server installation and configuration includes creating the OTP installation directory and installing the OTP services, OSP plug-in, and agents on the external OTP installation server,

---

- All OTP hosts and storage devices must meet the minimum patch and firmware requirements as described in "OTP System Hardware and Firmware Requirements" on page 25.
- Solaris 10 Update 2 must be installed and configured on each new OTP host as described in "Installing Solaris 10 Update 2 and the Remote Agent on the OTP Hosts" on page 50.

Note – OTP host post-operating system configuration procedures include installation of the service provisioning remote agent.

- A naming service such as NIS, NIS+, or `/etc/hosts` must be set up and all host names and IP addresses must be set up on that naming service.

Preparing To Install OTP To New OTP Hosts

Before you can install OTP to new OTP hosts using the external OTP installation server, you must add each new OTP host to the external OTP installation server as described in the following procedure.

▼ To Add Hosts to the External OTP Installation Server

Before you can install the Open Telecommunications Platform to the standalone OTP host or to the clustered OTP hosts, you must add each new OTP host to the host list on the external OTP installation server. Perform the following steps for each new OTP host.

Before You Begin

- The external OTP installation server must be set up and verified as described in "Setting Up the External OTP Installation Server" on page 44.

- The Solaris OS and the remote agent must be installed on all of the clustered OTP system hosts as described in "Installing Solaris 10 Update 2 and the Remote Agent on the OTP Hosts" on page 50.

1 Open a Web browser and log in to the external OTP installation server service provisioning service.

Go to URL http://*install server*:9090 where *install server* is either the IP address or the fully qualified name of the external OTP installation server.

2 Click Host Setup in the left menu to display the Host Setup page:

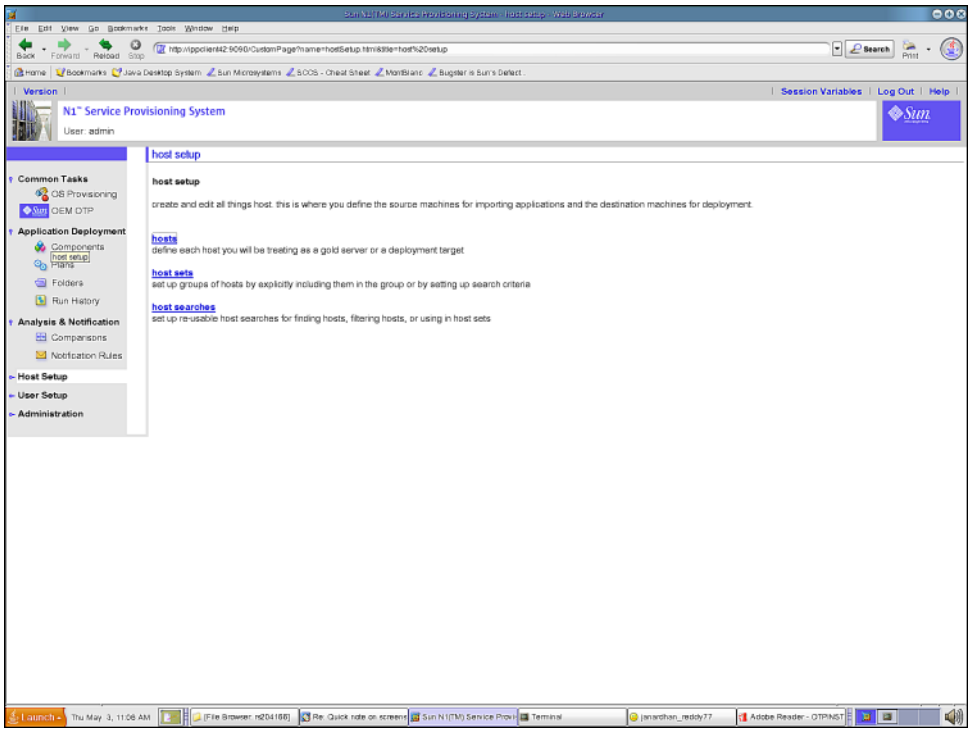

FIGURE 5–2 Host Setup page

3 Click hosts in the central menu to display the hosts page:

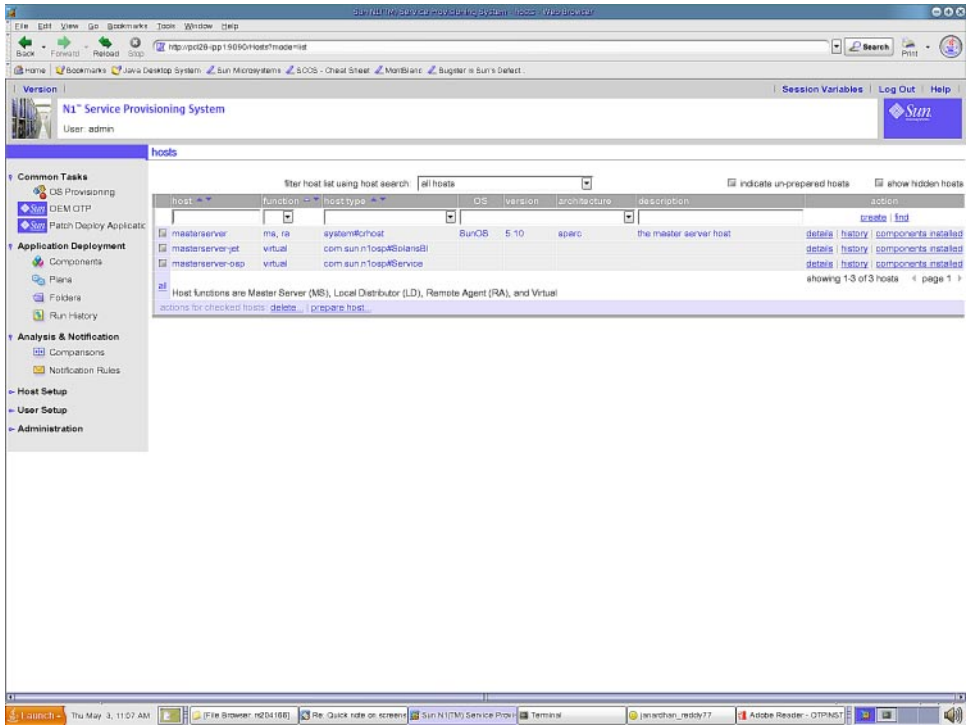

FIGURE 5–3 Hosts Page

a. **In the** `host field`**, type the name of the new OTP host.**

b. **(Optional) In the** `description field`**, type a description of the new OTP host.**

c. **Click** `create`**.**

The host details edit page is displayed as shown in the next step.

4 **Specify the host values on the details edit page:**

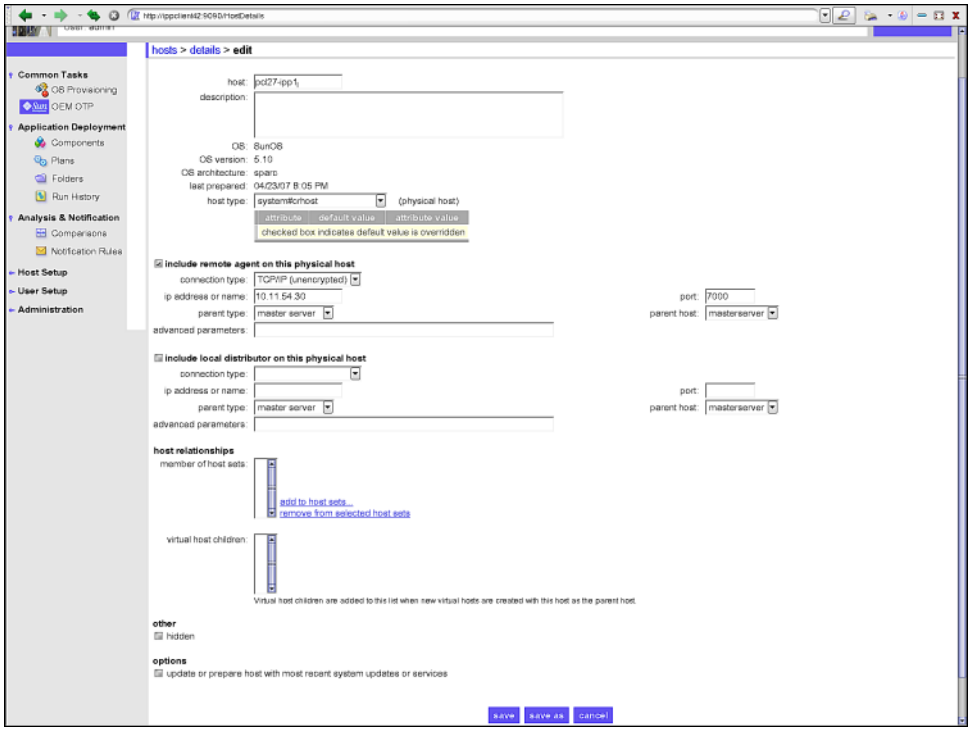

FIGURE 5–4 Host Edit Details Page

Note – The above example of the host edit details page shows only the required fields at the top of the page.

---

a. **Click** `include remote agent` **on this physical host**

b. **Click the arrow to the right of the** `connection type` **field to display the drop-down list.**
   Choose TCP/IP (unencrypted).

c. **In the** `ip address or name` **field, type either the IP address of the host or the host name.**

d. **In the** `port field`**, type 7000.**

e. **Scroll to the bottom of the page and click save.**
   The host is added to the hosts list on the external OTP installation server. The hosts list page is displayed.

f. **Click Host Setup.**

g. **Click the name of the host you are setting up.**

h. **Click Update remote agent.**

i. **Check the box to the left of the host name, and then click** `prepare host...`
The host is prepared for provisioning.

Troubleshooting Before adding a node to an existing cluster, ensure that the sponsoring node (first OTP host of the cluster) is added to the host list in the service provisioning service using this procedure.

Next Steps Repeat this procedure for every host to which the Open Telecommunications Platform is to be installed. When you have finished adding all hosts to the external OTP installation server hosts list:

- If you are installing the Open Telecommunications Platform to a standalone OTP host, install the Open Telecommunications Platform as described in "Installing the Open Telecommunications Platform on a Standalone OTP Host" on page 119.
- If you are installing Open Telecommunications Platform to a clustered OTP system, install the Open Telecommunications Platform as described in "Installing the Open Telecommunications Platform on a Clustered OTP System" on page 127.

Installing the Open Telecommunications Platform on a Standalone OTP Host

Graphical user interface installation and setup of the Open Telecommunications Platform on a standalone OTP host is comprised of the following procedures:

- "To Set Up the OTP High Availability Framework" on page 119
- "To Set Up OTP System Management and Provisioning Services" on page 123
- "To Enable High Availability For the OTP Provisioning Service" on page 125

Refer to the "OTP System Plan Settings Descriptions" on page 30 and the "Standalone OTP Host Plan Worksheet" on page 34 for information needed during installation.

Note – A standalone OTP host can be converted clustered OTP host as described in "Converting a Standalone OTP Host to a Clustered OTP Host" on page 206.

▼ To Set Up the OTP High Availability Framework

The OTP high availability framework must be set up on the standalone OTP host.

Before You Begin

- The external OTP installation server must be set up and verified as described in "To Install the OTP Services, Agent, and Plug-ins on the External OTP Installation Server" on page 46.
- The Solaris OS and the remote agent must be installed on all of the clustered OTP system hosts as described in "Installing Solaris 10 Update 2 and the Remote Agent on the OTP Hosts" on page 50.
- The standalone OTP host must be added to the external OTP installation server as described in "To Add Hosts to the External OTP Installation Server" on page 115.

1 Open a Web browser and log in to the external OTP installation server service provisioning service.

Go to URL http://*install server*:9090 where *install server* is either the IP address or the fully qualified name of the external OTP installation server.

2 Click OEM OTP to display the Open Telecommunications Platform home page.

3 Click `Step 1. OTP High Availability Framework: Install and Configure`

The edit availability plan page appears.

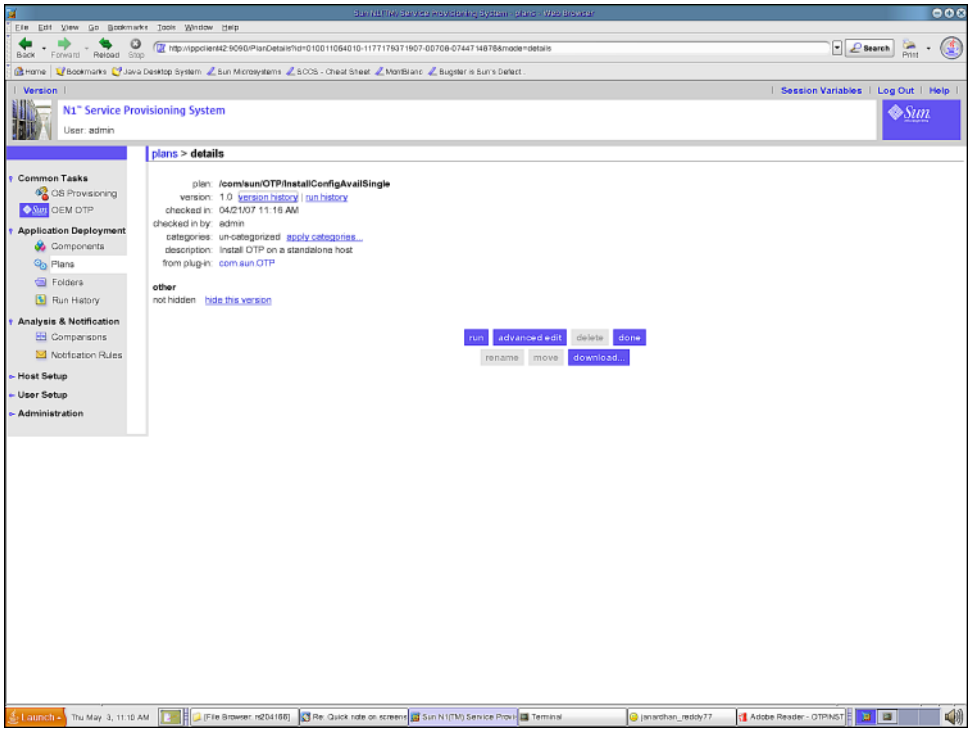

FIGURE 5–5 Edit Availability Plan Page

4 Click run.

The Availability Plan Variables page appears.

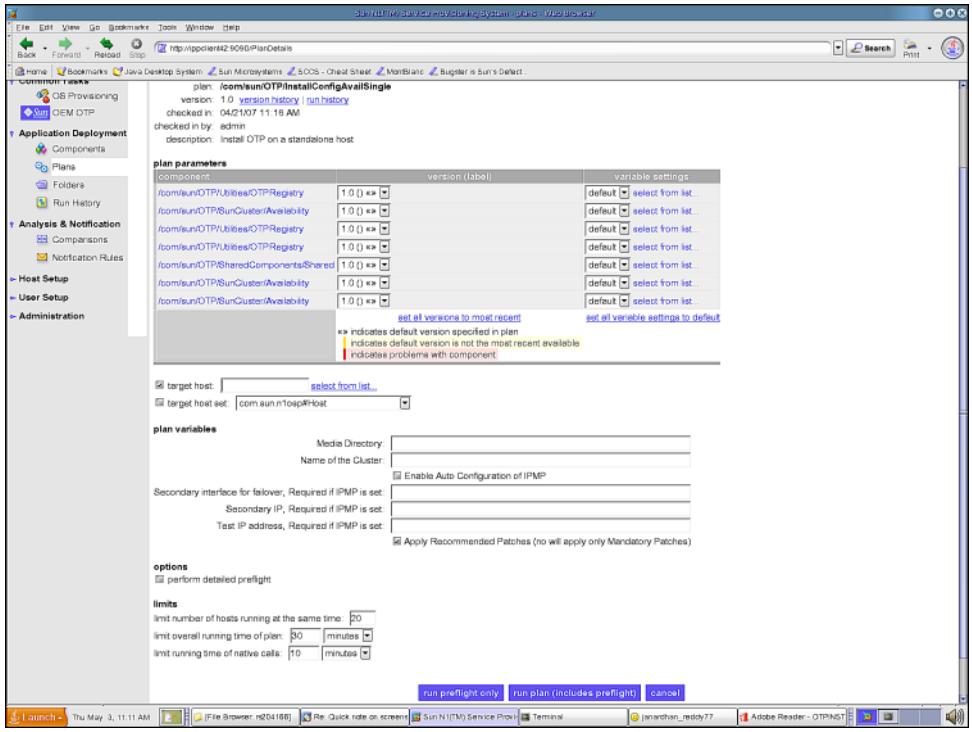

FIGURE 5–6 Availability Plan Variables Page

Scroll the page down to view the variables:

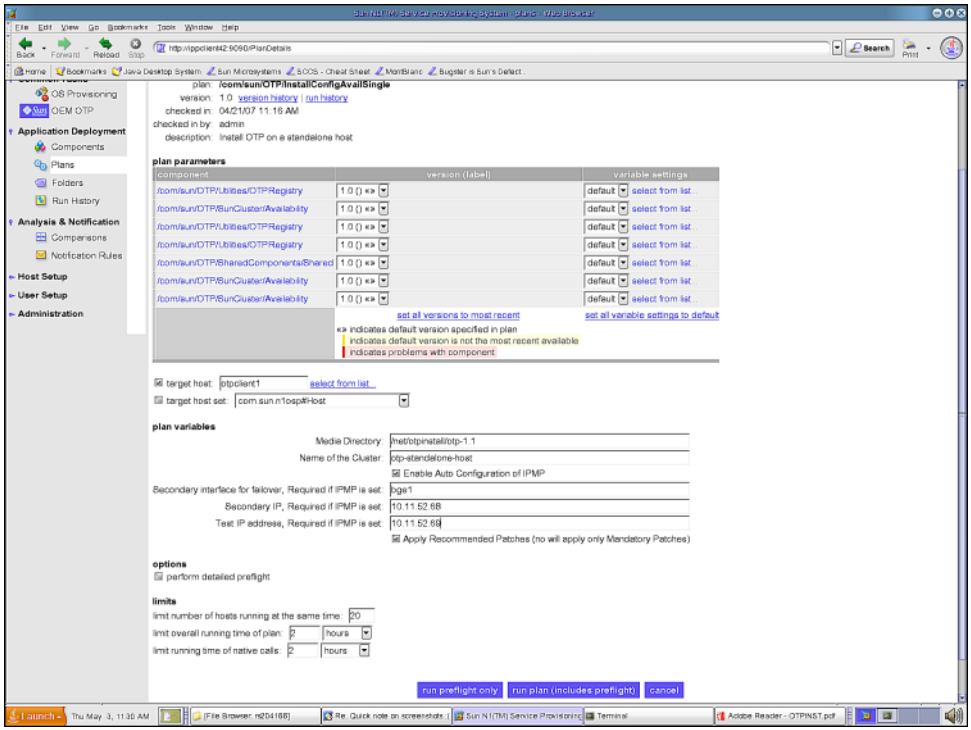

FIGURE 5–7 Availability Plan Variables Page: Variables

Type the host name on which you want to install Sun OTP in the target host field. Do not modify the target host set.

Type the information in the plan variables fields according to your "Standalone OTP Host Plan Worksheet" on page 34. Refer to the "OTP System Plan Settings Descriptions" on page 30 for information about each variable.

Caution – Set limit overall running time of plan and limit running time of native calls to 2 hours each.

5 Click run plan (includes preflight).

The page refreshes, and a progress bar is displayed during the provisioning process.

The provisioning process:

- Installs required Solaris OS patches
- Installs the OTP high availability framework
- Configures the standalone OTP host
- Reboots the standalone OTP host

- Verifies the OTP high availability framework configuration

Next Steps Set up the system management and provisioning services on the standalone OTP host as described in the following procedure.

▼ To Set Up OTP System Management and Provisioning Services

Before You Begin The OTP high availability framework must be set up on the standalone OTP host as described in the previous procedure.

1. **Open a Web browser and log in to the external OTP installation server service provisioning service.**

   Go to URL http://*install server*:9090 where *install server* is either the IP address or the fully qualified name of the external OTP installation server.

2. **Click OEM OTP to display the Open Telecommunications Platform home page.**

3. **Click** `Step 2. OTP System Management and Provisioning Service: Install and Configure`**.**

   The edit System Management and Application Provisioning plan page appears.

4. **Click run.**

   The Availability Plan Variables page appears. Scroll the page down to display the variables

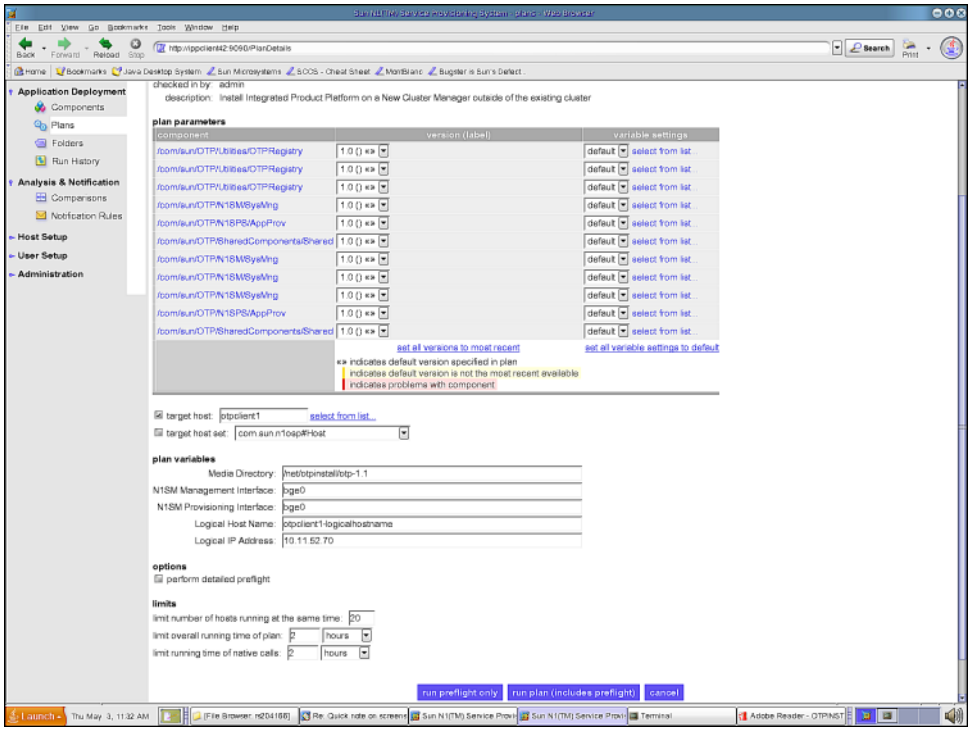

FIGURE 5–8 System Management and Application Provisioning Plan Variables Page

Type the host name on which you want to install Sun OTP in the target host field. Do not modify the target host set.

Type the information in the plan variables fields according to your "Standalone OTP Host Plan Worksheet" on page 34. Refer to the "OTP System Plan Settings Descriptions" on page 30 for information about each variable.

Caution – Set limit overall running time of plan and limit running time of native calls to 2 hours each.

5 **Click run plan (includes preflight).**

The page refreshes, and a progress bar is displayed during the provisioning process.

The provisioning process:

- Installs the Web console
- Applies patches required by the Open Telecommunications Platform
- Installs the system management service
- Installs the service provisioning service

- Installs Java patches

When the provisioning process completes, click done.

Next Steps Enable high availability on the standalone OTP host as described in the following procedure.

▼ To Enable High Availability For the OTP Provisioning Service

Before You Begin OTP System management and provisioning services must be set up on the standalone OTP host as described in the previous procedure.

1. **Open a Web browser and log in to the external OTP installation server service provisioning service.**

   Go to URL http://*install server*:9090 where *install server* is either the IP address or the fully qualified name of the external OTP installation server.

2. **Click OEM OTP to display the Open Telecommunications Platform home page.**

3. **Click** `Step 3. OTP High Availability for Provisioning Service: Enable .`

   The edit High Availability plan page appears.

4. **Click run.**

   The High Availability Plan Variables page appears.

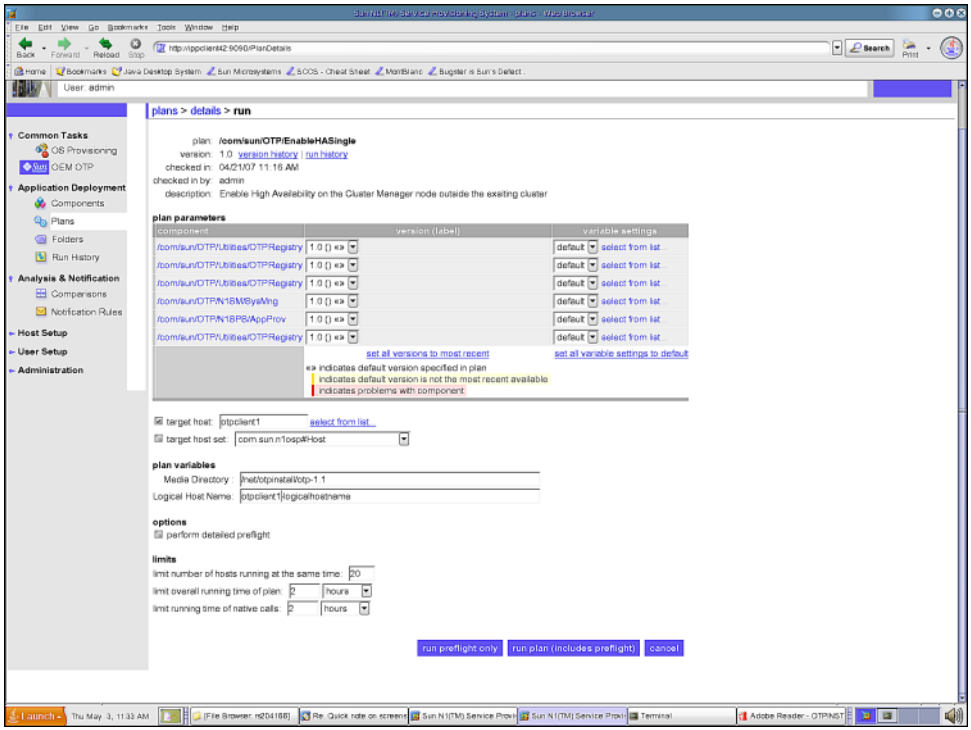

FIGURE 5–9 High Availability Plan Variables Page

Type the host name on which you want to install OTP in the target host field. Do not modify the target host set.

Type the information in the plan variables fields according to your "Standalone OTP Host Plan Worksheet" on page 34. Refer to the "OTP System Plan Settings Descriptions" on page 30 for information about each variable.

Caution – Set limit overall running time of plan and limit running time of native calls to 2 hours each.

5 Click run plan (includes preflight).

The page refreshes, and a progress bar is displayed during the provisioning process.

The provisioning process installs and enables the application provisioning service high availability agent.

When the provisioning process completes, click done.

6 **Log in as root to the standalone OTP host and restart the remote agent.**

Type **`/etc/init.d/n1spsagent restart`** to restart the remote agent. If the remote agent is not restarted, then the service provisioning service on the standalone OTP host will not work properly.

This completes installation of the Open Telecommunications Platform on a standalone OTP host.

Installing the Open Telecommunications Platform on a Clustered OTP System

Graphical user interface installation and setup of the Open Telecommunications Platform on a clustered OTP system is comprised of the following steps:

- "To Set Up the OTP High Availability Framework on the First OTP Host" on page 127
- "To Set Up the OTP High Availability Framework on the Additional OTP Hosts" on page 130
- "To Set Up OTP System Management and Provisioning Services on the First OTP Host" on page 133
- "To Set Up OTP System Management and Provisioning Services on the Additional OTP Hosts" on page 135
- "To Enable High Availability for the OTP Provisioning Service on the First OTP Host" on page 137

Note – Refer to the "OTP System Plan Settings Descriptions" on page 30 and the "Clustered OTP Host Plan Worksheet" on page 36 for information needed during installation.

▼ To Set Up the OTP High Availability Framework on the First OTP Host

Availability services must first be set up on the first OTP host in your clustered OTP system.

Before You Begin

- The first OTP host must be connected to shared storage
- The external OTP installation server must be set up and verified as described in "To Install the OTP Services, Agent, and Plug-ins on the External OTP Installation Server" on page 46
- The Solaris OS and the remote agent must be installed on all of thenew OTP hosts as described in "Installing Solaris 10 Update 2 and the Remote Agent on the OTP Hosts" on page 50
- All hosts in the clustered OTP system must be added to the external OTP installation server hosts list as described in "To Add Hosts to the External OTP Installation Server" on page 115

1 **Open a Web browser and log in to the external OTP installation server service provisioning service.**

Go to URL http://*install server*:9090 where *install server* is either the IP address or the fully qualified name of the external OTP installation server.

2 **Click OEM OTP to display the Open Telecommunications Platform home page.**

3 **Click** `Step 1. OTP High Availability Framework on First Host: Install and Configure`**.**

The edit availability plan page appears.

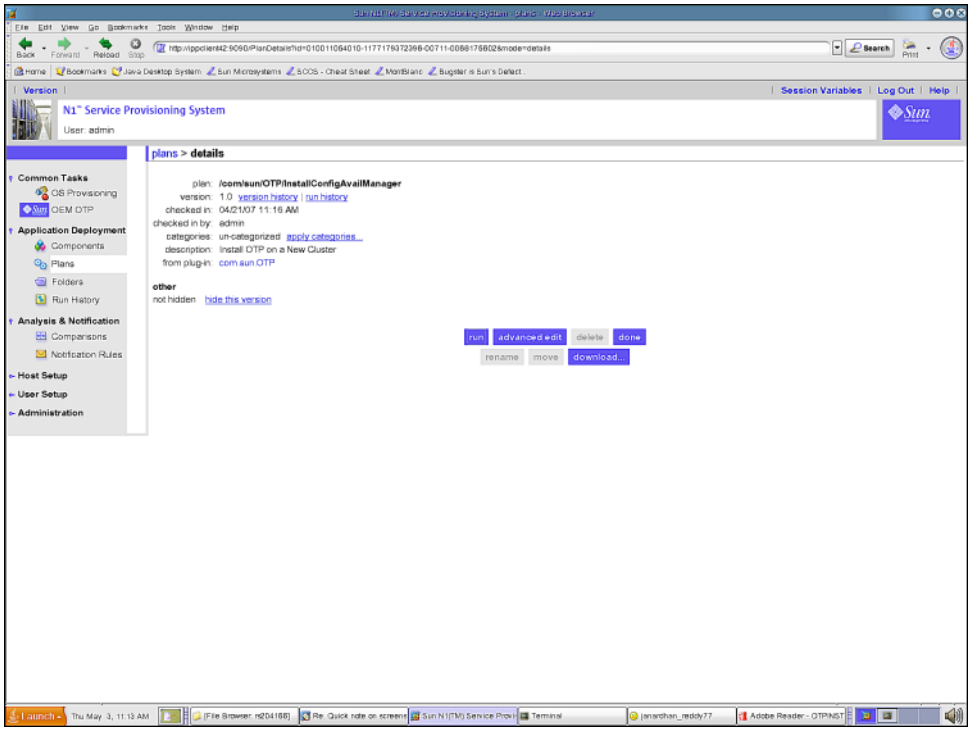

FIGURE 5–10 Clustered OTP Host Edit Availability Plan Page: System Management Server

4 **Click run.**

The Availability Plan Variables page appears. Scroll the page down to view the variables:

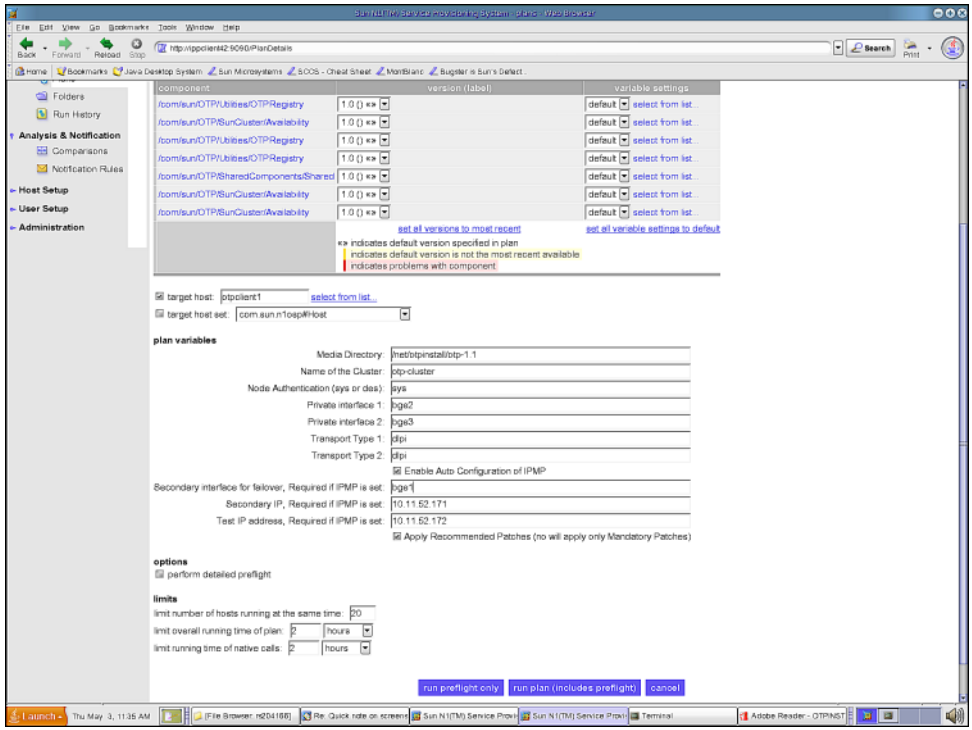

FIGURE 5–11 Clustered OTP Host Availability Plan Variables Page: System Management Server Variables

Type the host name on which you want to install Sun OTP in the target host field. Do not modify the target host set.

Type the information in the plan variables fields according to your "Clustered OTP Host Plan Worksheet" on page 36. Refer to the "OTP System Plan Settings Descriptions" on page 30 for information about each variable.

Caution – Set limit overall running time of plan and limit running time of native calls to 2 hours each.

5 Click run plan (includes preflight).

The page refreshes, and a progress bar is displayed during the provisioning process.

The provisioning process:

- Installs required Solaris OS patches
- Installs the OTP high availability framework
- Configures the first OTP host
- Reboots the first OTP host

- Verifies the first OTP host configuration

Next Steps Set up availability services on the additional OTP hosts as described in the next procedure.

▼ To Set Up the OTP High Availability Framework on the Additional OTP Hosts

The OTP high availability framework must be set up on each host in your clustered OTP system. Perform the following steps on each host.

Before You Begin The OTP high availability framework must be set up on the First OTP Host as described in the previous procedure.

1. **Open a Web browser and log in to the external OTP installation server service provisioning service.**

   Go to URL http://*install server*:9090 where *install server* is either the IP address or the fully-qualifed name of the external OTP installation server.

2. **Click OEM OTP to display the Open Telecommunications Platform home page.**

3. **Click** `Step 2. OTP High Availability Framework on Additional Hosts: Install and Configure`**.**

   The edit availability plan page appears.

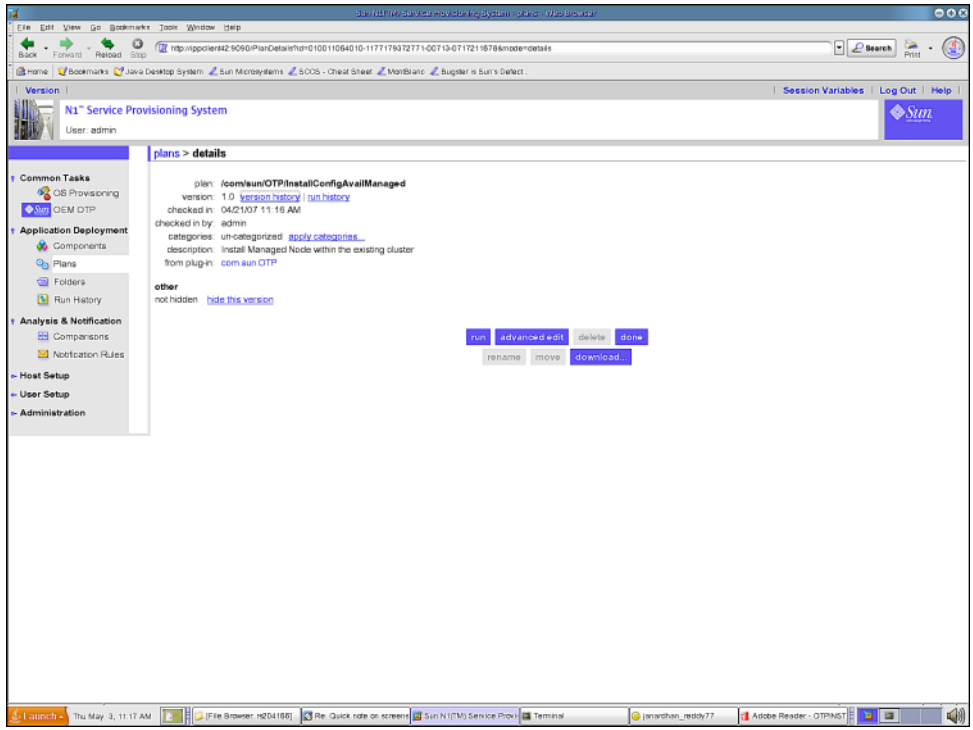

FIGURE 5–12 Clustered OTP Hosts Edit Availability Plan Page

4 Click run.

The Availability Plan Variables page appears. Scroll the page down to view the variables:

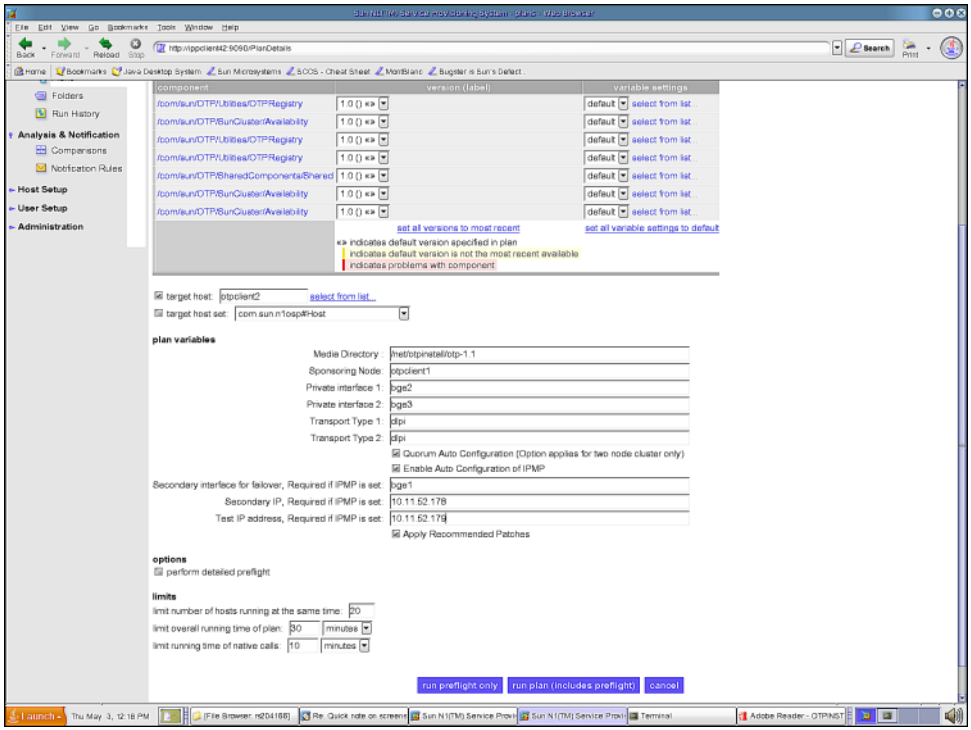

FIGURE 5–13 Clustered OTP Hosts Availability Plan Variables Page

Type the host name on which you want to install Sun OTP in the target host field. Do not modify the target host set.

Type the information in the plan variables fields according to your "Clustered OTP Host Plan Worksheet" on page 36. Refer to the "OTP System Plan Settings Descriptions" on page 30 for information about each variable.

Caution – Set limit overall running time of plan and limit running time of native calls to 2 hours each.

5 Click run plan (includes preflight).

The page refreshes, and a progress bar is displayed during the provisioning process.

The provisioning process:

- Installs required Solaris OS patches
- Installs the OTP high availability framework
- Configures the clustered OTP host
- Reboots the clustered OTP host

- Verifies the clustered OTP host configuration

6 **If you chose `no` for `Quorum Auto Configuration` on a two-host cluster, you must manually select and configure the quorum disk as described in "To Configure the Quorum Disk on a Two-Host Cluster" on page 107.**

Next Steps

- Create the shared storage on the clustered OTP system as described in "To Create Shared Storage on the Clustered OTP System" on page 108.
- When you have completed setting up shared storage, set up the system management and provisioning services as described in the next procedure.

▼ To Set Up OTP System Management and Provisioning Services on the First OTP Host

Before You Begin Shared storage must be set up on the first OTP host as described in the previous procedure.

1 **Open a Web browser and log in to the external OTP installation server service provisioning service.**

Go to URL http://*install server*:9090 where *install server* is either the IP address or the fully qualified name of the external OTP installation server.

2 **Click OEM OTP to display the Open Telecommunications Platform home page.**

3 **Click `Step 3. OTP System Management and Provisioning Services on First Host: Install and Configure`.**

The edit System Management and Application Provisioning plan page appears.

4 **Click run.**

The System Management and Application Provisioning Plan Variables page appears. Scroll the page down to display the variables

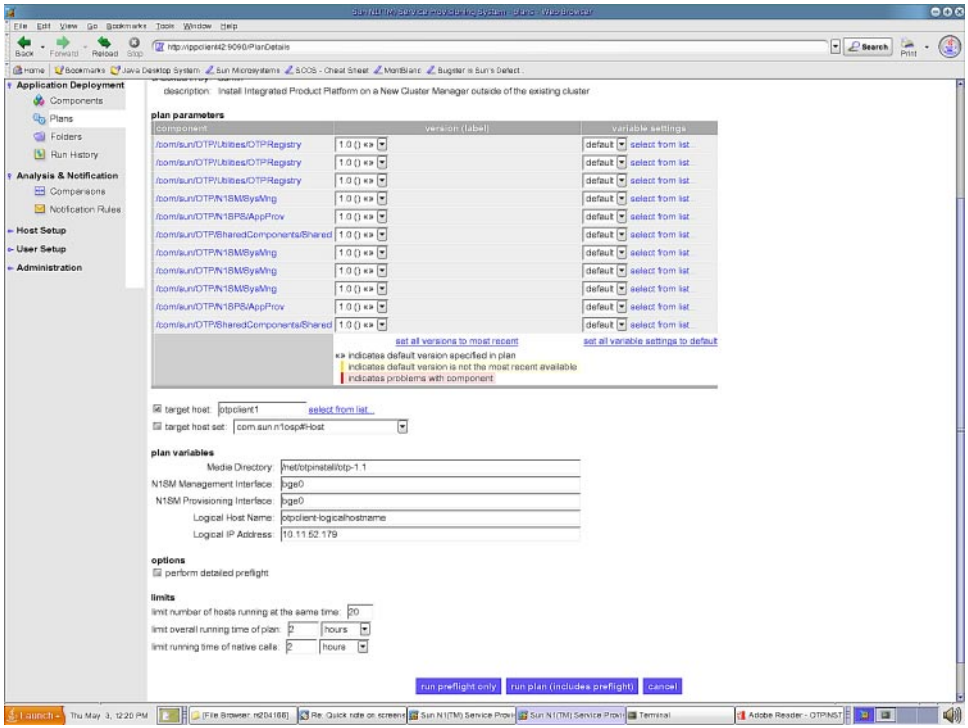

FIGURE 5–14 Clustered OTP Host System Management and Application Provisioning Plan Variables Page: First OTP Host

Type the host name on which you want to install Sun OTP in the target host field. Do not modify the target host set.

Type the information in the plan variables fields according to your "Clustered OTP Host Plan Worksheet" on page 36. Refer to the "OTP System Plan Settings Descriptions" on page 30 for information about each variable.

Caution – Set limit overall running time of plan and limit running time of native calls to 2 hours each.

5 Click run plan (includes preflight).

The page refreshes, and a progress bar is displayed during the provisioning process.

The provisioning process:

- Installs the Web console
- Applies patches required by the Open Telecommunications Platform
- Installs the system management agent
- Installs the system management service

- Installs the service provisioning service
- Installs Java patches

When the provisioning process completes, click done.

▼ To Set Up OTP System Management and Provisioning Services on the Additional OTP Hosts

Before You Begin System management and provisioning services must be set up on the first OTP host as described in the previous procedure.

1. **Open a Web browser and log in to the external OTP installation server service provisioning service.**

   Go to URL http://*install server*:9090 where *install server* is either the IP address or the fully qualified name of the external OTP installation server.

2. **Click OEM OTP to display the Open Telecommunications Platform home page.**

3. **Click** `Step 4. OTP System Management and Provisioning Service on Additional Hosts: Install and Configure`**.**

   The edit System Management and Application Provisioning plan page appears.

4. **Click run.**

   The System Management and Application Provisioning Plan Variables page appears. Scroll the page down to display the variables

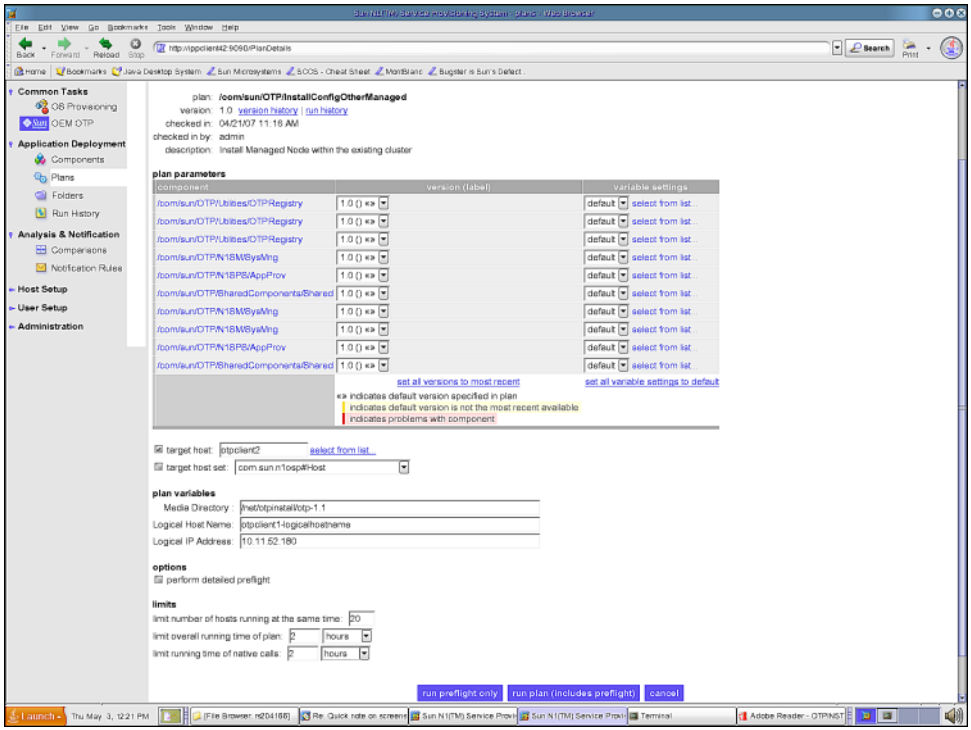

FIGURE 5–15 Clustered OTP Host System Management and Application Provisioning Plan Variables Page: Additional OTP Host

Type the host name on which you want to install Sun OTP in the target host field. Do not modify the target host set.

Type the information in the plan variables fields according to your "Clustered OTP Host Plan Worksheet" on page 36 for this OTP host. Refer to the "OTP System Plan Settings Descriptions" on page 30 for information about each variable.

Caution – Set limit overall running time of plan and limit running time of native calls to 2 hours each.

5 Click run plan (includes preflight).

The page refreshes, and a progress bar is displayed during the provisioning process.

The provisioning process:

- Installs the Web console
- Applies patches required by the Open Telecommunications Platform
- Installs the system management agent
- Installs the system management service

- Installs the service provisioning service
- Installs Java patches

When the provisioning process completes, click done.

Next Steps Repeat this procedure for the next OTP host in your clustered OTP system.

When you have finished setting up system management and provisioning services on all OTP hosts, enable high availability on the first OTP host as described in the next procedure.

▼ To Enable High Availability for the OTP Provisioning Service on the First OTP Host

Before You Begin System management and provisioning services must be set up on the additional OTP hosts as described in the previous procedure.

1 **Open a Web browser and log in to the external OTP installation server service provisioning service.**

Go to URL http://*install server*:9090 where *install server* is either the IP address or the fully-qualifed name of the external OTP installation server.

2 **Click OEM OTP to display the Open Telecommunications Platform home page.**

3 **Click** `Step 5. OTP High Availability for Provisioning Service on First Host: Enable` **beneath Multi Cluster Setup in the central menu.**

The edit High Availability plan page appears.

4 **Click run.**

The High Availability Plan Variables page appears. Scroll the page down to display the variables

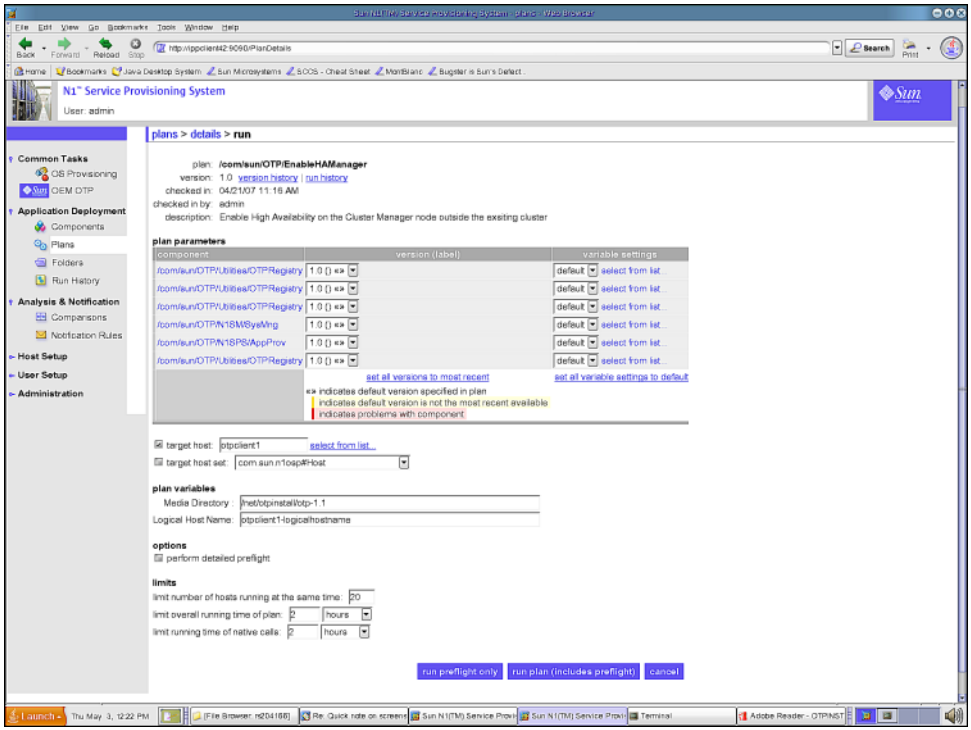

FIGURE 5–16 Clustered OTP Host High Availability Plan Variables Page: First OTP Host

Type the host name on which you want to install Sun OTP in the target host field. Do not modify the target host set.

Type the information in the plan variables fields according to your "Clustered OTP Host Plan Worksheet" on page 36. Refer to the "OTP System Plan Settings Descriptions" on page 30 for information about each variable.

Caution – Set limit overall running time of plan and limit running time of native calls to 2 hours each.

5 Click run plan (includes preflight).

The page refreshes, and a progress bar is displayed during the provisioning process.

The provisioning process installs and enables the application provisioning service high availability agent.

When the provisioning process completes, click done.

6. **Log in as root on the first OTP host and restart the remote agent.**

   Type **`/etc/init.d/n1spsagent restart`** to restart the remote agent. If the remote agent is not restarted, then the service provisioning service on the first OTP host will not work properly.

7. **Configure and enable fail-over.**

   a. **Type `/usr/cluster/bin/scrgadm -c -g otp-system-rg -y RG_system=false` to set the `system` property for the `otp-system-rg` resource group to false.**

   b. **Type `/usr/cluster/bin/scswitch -F -g otp-system-rg` to take the remote group offline.**

   c. **Type the following commands in the sequence shown to disable cluster resources.**

      ```
      /usr/cluster/bin/scswitch -n -j otp-spsms-rs
      /usr/cluster/bin/scswitch -n -j otp-spsra-rs
      /usr/cluster/bin/scswitch -n -j otp-sps-hastorage-plus
      /usr/cluster/bin/scswitch -n -j otp-lhn
      ```

   d. **Type `/usr/cluster/bin/scswitch -u -g otp-system-rg` to put the remote group into the unmanaged state.**

   e. **Type `/usr/cluster/bin/scrgadm -c -j otp-spsra-rs -x Stop_signal="15"` to change the `Stop_signal` property of the remote agent resource to 15.**

   f. **Type `/usr/cluster/bin/scrgadm -c -j otp-spsms-rs -x Stop_signal="15"` to change the `Stop_signal` property of the management service resource to 15.**

   g. **Type `/usr/cluster/bin/scswitch -o -g otp-system-rg` to put the remote group into the managed state.**

   h. **Type `/usr/cluster/bin/scswitch -Z -g otp-system-rg` to bring the remote group back online.**

   i. **Type `/usr/cluster/bin/scrgadm -c -g otp-system-rg -y RG_system=true` to set the system property for the `otp-system-rg` resource group to true.**

   This completes the Open Telecommunications Platform graphical user interface installation process for a clustered OTP system.

◆ ◆ ◆ CHAPTER 6

Installing the Open Telecommunications Platform Using the Provisioning Service On an Existing OTP System

This chapter provides the procedures for using the OTP provisioning service on an existing production standalone OTP host or on the first OTP host in a clustered OTP system to install and configure the Open Telecommunications Platform software to a new OTP host or hosts.

Note – In the following sections and procedures, the production OTP host used as the OTP installation source is called the *OTP master server*. The new standalone OTP host and each new clustered OTP host is called a *new OTP host*.

Before you begin, review the OTP Plan settings described in "OTP System Plan Settings Descriptions" on page 30, and then print out the worksheet and fill in the values based on the host or hosts to which you will install OTP:

Preparing the OTP Master Server Using GUI

This section provides the procedures for preparing an existing production OTP master server for use as an OS, OTP, and NEP application provisioning host using the GUI interface.

The following topics are discussed:

▼ To Identify the OTP Master Server in a Clustered OTP System

Skip this procedure if you are using a standalone OTP host to install the OS, OTP, and applications to a new OTP host.

In a clustered OTP system, the OTP master server is the clustered OTP host on which the resource group is active.

1. **Log in as root (`su - root`)to an OTP host in the cluster.**

2. **Type `/usr/cluster/bin/scstat -g` to determine which host in the cluster is online.**

   The host on which the resource group `otp-system-rg` is online is the OTP master server.

   For example:

```
# /usr/cluster/bin/scstat -g | grep Online
    Group: otp-system-rg       otp-node17          Online
 Resource: otp-lhn             otp-node17          Online    Online - LogicalHostname online
 Resource: otp-sps-hastorage-plus otp-node17          Online    Online
 Resource: otp-spsms-rs        otp-node17          Online    Online
 Resource: otp-spsra-rs        otp-node17          Online    Online
```

   In the above example, the resource group `otp-system-rg` is running on the clustered OTP host otp-node17, and otp-node17 is therefore the OTP master server.

Next Steps Update the OTP master server remote agent as described in the next procedure.

▼ To Update the Service Provisioning Remote Agent

1. **Open a Web browser and go to URL http://*OTP master server*:9090 where *install server* is either the IP address or the fully qualified name of the OTP master server or of the standalone OTP host.**

   The OTP provisioning service log in screen appears.

2. **Log in to the OTP provisioning service.**

   The Service Provisioning System screen appears.

3. **Click Host Setup in the left panel.**

   The host setup screen appears.

4. **Click hosts in the central panel.**

   The hosts screen appears.

5. **Click masterserver.**

   The hosts > details screen appears.

6. **Click update remote agent.**

   The update hosts progress window appears. When the update remote agent task completes, click close.

7. **Click Host Setup in the left panel of the hosts > details screen.**

8. **Click hosts.**

9. **Click the check box to the left of masterserver. Make sure the box contains a check.**

10. **Click prepare host.**

    The prepare hosts progress window appears. When the prepare hosts task completes, click close.

Next Steps Create the OS provisioning server on the OTP master server as described in the next procedure.

▼ To Create the OS Provisioning Server

1. **Open a Web browser and go to URL http://***OTP master server***:9090 where** *install server* **is either the IP address or the fully qualified name of the OTP master server or of the standalone OTP host.**

   The OTP provisioning service log in screen appears.

2. **Log in to the OTP provisioning service.**

   The default user name is `admin` and the default password is `admin`.

   The Service Provisioning System screen appears.

3. **Click OS Provisioning.**

   The OS Provisioning task list page appears.

   Scroll down to OSP Control Server.

4. **Click the OSP Control Server `Create` link.**

   The plans > details screen appears.

5. **Click run.**

   The plans > details > run screen appears.

6. **Click select from list... beneath variable settings.**
   The select variable from list... pop-up screen appears.
7. **Scroll to the bottom of the pop-up screen and click create set.**
   The select variable screen refreshes and enables the check boxes and data fields.
8. **Type a name for the new variable set in the Set Name field., for example, otp.**
9. **Click the sps_cli check box.**
   The sps_cli data field is enabled.
10. **Type** `/var/otp/spsotp/N1_Service_Provisioning_System_5.2/cli/bin/cr_cli` **in the sps_cli data field.**
    The screen refreshes and the check boxes and data fields are disabled.
11. **Click Save.**
12. **Click the right-most select button.**
    The select variables screen closes, and the plans > details > run screen is updated.
13. **Click on the target host field** `select from list...` **link.**
    The select hosts from list screen appears.
14. **Click masterserver, and then click add hosts to main window.**
    The select hosts from list screen closes, and the plans > details> run screen is updated.
15. **Click run plan (includes preflight)**
    The Create Provisioning Server plan will take a few minutes to complete. When the plan completes, the results screen appears.
16. **Click done.**

Next Steps Create the JET boot/install server as described in the next procedure.

▼ To Create the JET Boot/Install Server

1. **Open a Web browser and go to URL http://*OTP master server*:9090 where *install server* is either the IP address or the fully qualified name of the OTP master server or of the standalone OTP host.**
   The OTP provisioning service log in screen appears.

2. **Log in to the OTP provisioning service.**
   The Service Provisioning System screen appears.

3. **Click OS Provisioning.**
   The OS Provisioning task list page appears.
   Scroll down to JET Solaris Image Servers.

4. **Click the JET Solaris Image Servers `Create` link.**
   The plans > details screen appears.

5. **Click run.**
   The plans > details > run screen appears.

6. **Click select from list... beneath variable settings.**
   The select variable from list... pop-up screen appears.

7. **Scroll to the bottom of the pop-up screen and click create set.**
   The select variable screen refreshes and enables the check boxes and data fields.

8. **Type a name for the new variable set in the Set Name field., for example, otp.**

9. **Click the sps_cli check box.**
   The sps_cli data field is enabled.

10. **Type `/var/otp/spsotp/N1_Service_Provisioning_System_5.2/cli/bin/cr_cli` in the sps_cli data field.**
    The screen refreshes and the check boxes and data fields are disabled.

11. **Click Save.**

12. **Click the right-most select button.**
    The select variables screen closes, and the plans > details > run screen is updated.

13. **Click on the target host field `select from list...` link.**
    The select hosts from list screen appears.

14. **Click masterserver, and then click add hosts to main window.**
    The select hosts from list screen closes, and the plans > details> run screen is updated.

15 **Click run plan (includes preflight)**

The Create JET Server plan will take a few minutes to complete. When the plan completes, the results screen appears.

16 **Click done.**

This completes preparation of the OTP master server.

Next Steps Prepare the new OTP hosts for OTP installation as described in the next section.

Preparing the OTP Master Server Using CLI

This section provides the procedures for preparing an existing production OTP master server for use as an OS, OTP, and NEP application provisioning host using the CLI interface.

The following topics are discussed:

Tip – Add `/var/otp/spsotp/N1_Service_Provisioning_System_5.2/cli/bin` to the root account PATH statement before performing the following procedures. Type **`rehash`** after you have set the path.

The following procedures assume you have added `/var/otp/spsotp/N1_Service_Provisioning_System_5.2/cli/bin` to the root account PATH statement in the root account initialization script.

▼ To Identify the OTP Master Server in a Clustered OTP System

- **See "To Identify the OTP Master Server in a Clustered OTP System" on page 142.**

Next Steps Update the OTP master server remote agent as described in the next procedure.

▼ To Update the Service Provisioning Remote Agent

1. **Log in as root (`su - root`)to the OTP master server.**
2. **Run the following command to update the Service Provisioning Remote Agent.**

   ```
   cr_cli -cmd node.au.run -u admin -p admin -all true
   ```

3. **Run the following command to prepare the Service Provisioning Remote Agent.**

   ```
   cr_cli -cmd pe.h.prep -u admin -p admin -tar NM:masterserver
   ```

Next Steps Create the OS provisioning server on the OTP master server as described in the next procedure.

▼ To Create the OS Provisioning Server

1. **Log in as root (`su - root`)to the OTP master server.**
2. **Run the following command to create the variable set for OS Provisioning Server creation.**

   ```
   cr_cli -cmd cdb.vs.add -comp NM:/com/sun/n1osp/untyped/Service -name "otp" -u
   admin -p admin -vars
   "sps_cli=/var/otp/spsotp/N1_Service_Provisioning_System_5.2/cli/bin/cr_cli"
   ```

3. **Run the following command to create the OS Provisioning Server.**

   ```
   cr_cli -cmd pe.p.run -u admin -p admin -PID
   NM:/com/sun/n1osp/untyped/Service-create -tar H:NM:masterserver -comp - -vs otp
   -pto 300 -nto 100
   ```

Next Steps Create the JET boot/install server as described in the next procedure.

▼ To Create the JET Boot/Install Server

1. **Log in as root (`su - root`)to the OTP master server.**
2. **Run the following command to create the variable set for JET Boot/Install Server creation.**

   ```
   cr_cli -cmd cdb.vs.add -comp NM:/com/sun/n1osp/untyped/Jet -name "otp" -u admin
   -p admin -vars
   "sps_cli=/var/otp/spsotp/N1_Service_Provisioning_System_5.2/cli/bin/cr_cli"
   ```

3 **Run the following command to create the JET Boot/Install Server.**

```
cr_cli -cmd pe.p.run -u admin -p admin -PID NM:/com/sun/n1osp/untyped/Jet-create
-tar H:NM:masterserver -comp + -vs otp -pto 300 -nto 100
```

This completes preparation of the OTP master server.

Next Steps Prepare the new OTP hosts for OTP installation as described in the next section.

Preparing the New OTP Hosts for OTP Installation

Before you can install OTP to the new OTP host or hosts, you must install the Solaris OS and the remote agent on each new OTP host as described in "Installing Solaris 10 Update 2 and the Remote Agent on the OTP Hosts" on page 50, and configure the Solaris OS on each host as described in "Configuring Solaris 10 Update 2" on page 94.

▼ To Add New OTP Hosts to the OTP Master Server

1 **Open a Web browser and log in to the OTP master server service provisioning service.**

Go to URL http://*OTP master server*:9090 where *OTP master server* is either the IP address or the fully qualified name of the OTP master server.

2 **Click Host Setup in the left menu to display the Host Setup page.**

3 **Click hosts in the central menu to display the hosts page.**

a. **In the** `host field`**, type the name of the new OTP host.**

b. **(Optional) In the** `description field`**, type a description of the host.**

c. **Click** `create`**.**

The host details edit page is displayed.

4 **Specify the new OTP host values on the details edit page.**

a. **Click** `include remote agent on this physical host`**.**

b. **Click the arrow to the right of the** `connection type` **field to display the drop-down list.**

Choose TCP/IP (unencrypted).

c. **In the** `ip address or name` **field, type either the IP address of the host or the host name.**

d. **In the `port field`, type 7000.**

e. **Scroll to the bottom of the page and click save.**

The host is added to the hosts list on the production OTP host. The hosts list page is displayed.

f. **Click Host Setup.**

g. **Click the name of the host you are setting up.**

h. **Click Update remote agent.**

i. **Check the box to the left of the host name, and then click `prepare host...`**

The host is prepared for provisioning.

Next Steps Repeat this procedure for every new OTP host. When you have finished adding all hosts to theOTP master server hosts list:

- If you are installing the Open Telecommunications Platform to a standalone OTP host, install the Open Telecommunications Platform as described in "Installing the Open Telecommunications Platform on a Standalone OTP Host" on page 119.
- If you are installing Open Telecommunications Platform to a clustered OTP system, install the Open Telecommunications Platform as described in "Installing the Open Telecommunications Platform on a Clustered OTP System" on page 127.

Installing OTP on a New OTP Host Using the OTP Master Server

With the exception that you use the OTP Master Server instead of an external OTP installation server to install OTP to a new standalone OTP host or to new clustered OTP hosts, the procedures are otherwise identical.

Caution – Make certain that you use the OTP master server when performing the following tasks. When directed to log in to the OTP provisioning service, use URL https://*OTP master server logical host name*:9090 in each procedure where *production OTP host logical host name* is the name of the of the OTP master server.

The following topics are discussed:

▼ To Install OTP on a Standalone OTP Host

Make certain that you use the OTP master server as noted above when performing the following tasks. When directed to log in to the OTP provisioning service, use URL https://*OTP master server logical host name*:9090 in each procedure.

Before You Begin The new standalone OTP host must be prepared for Open Telecommunications Platform as described in "Preparing the New OTP Hosts for OTP Installation" on page 148.

1. **Set up the OTP high availability framework as described in "To Set Up the OTP High Availability Framework" on page 119.**
2. **Set up the OTP System Management and Provisioning Services as described in"To Set Up OTP System Management and Provisioning Services" on page 123.**
3. **Enable the OTP high availability framework as described in"To Enable High Availability For the OTP Provisioning Service" on page 125**

▼ To Install OTP on a Clustered OTP System

Make certain that you use the OTP master server as noted above when performing the following tasks. When directed to log in to the OTP provisioning service, use URL https://*OTP master server logical host name*:9090 in each procedure.

Before You Begin Each new OTP host must be prepared for Open Telecommunications Platform as described in "Preparing the New OTP Hosts for OTP Installation" on page 148.

1. **Set up the OTP high availability framework on the first OTP host as described in "To Set Up the OTP High Availability Framework on the First OTP Host" on page 127**
2. **Set up the OTP high availability framework on the additional OTP hosts as described in "To Set Up the OTP High Availability Framework on the Additional OTP Hosts" on page 130**
3. **Create the shared storage on the clustered OTP system as described in "To Create Shared Storage on the Clustered OTP System" on page 108.**
4. **Set up the OTP system management and application provisioning services on the first OTP host as described in "To Set Up OTP System Management and Provisioning Services on the First OTP Host" on page 133.**
5. **Set up the OTP system management and application provisioning services on the additional OTP hosts as described in "To Set Up OTP System Management and Provisioning Services on the Additional OTP Hosts" on page 135.**

6 **Enable the OTP high availability framework on the first OTP host as described in "To Enable High Availability for the OTP Provisioning Service on the First OTP Host" on page 137**

◆ ◆ ◆ CHAPTER 7

Installing the Open Telecommunications Platform Using the System Management Service On an Existing OTP System

This chapter provides the procedures for using the OTP system management service on an existing production standalone OTP host or on the first OTP host in a clustered OTP system to install and configure the Open Telecommunications Platform software to a new OTP System.

The following topics are discussed:

Note – In the following sections and procedures, the production OTP host used as the OTP installation source is called the *OTP master server*. The new standalone OTP host and each new clustered OTP host is called a *new OTP host*.

Before you begin, review the OTP Plan settings described in "OTP System Plan Settings Descriptions" on page 30, and then print out the worksheet and fill in the values based on the host or hosts to which you will install OTP:

Preparing the OTP System Management Service to Provision the Solaris OS

This section provides the procedures for preparing the OTP system management service to provision the Solaris 10 Update 2 OS to a new standalone OTP host or to clustered OTP hosts.

Before you can use an existing OTP system to install the Open Telecommunications Platform to one or more OTP hosts, you must first perform the following tasks:

- Create the OS image on the source OTP master server as described in "To Create the OS Image" on page 154.
- If you are going to provision the OS to bare metal OTP hosts, in other words, hosts on which an OS has not been installed, create the XML discovery file which the OTP discovery process requires to discover and manage the bare metal new OTP hosts as described in "Provisioning Bare Metal Systems Using Manual Discovery" on page 155.
- If you are going to install OTP to new OTP hosts on a different subnet using the OTP system management service, create a DHCP relay as described in "To Create the DHCP Relay for Deploying to New OTP Hosts On Different Subnets" on page 156

▼ To Create the OS Image

1 Log in as root to the OTP master server.

2 Type `/opt/sun/n1gc/bin/n1sh` to open the OTP command shell. For example:

```
# /opt/sun/n1gc/bin/n1sh
N1-ok>
```

3 Create the Solaris 10 Update 2 OS image.

In the OTP command shell, type `create os` *os name* `file` *path to iso image* where *os name* is the name of the image to create, and *path to iso image* is the path to the Solaris 10 Update 2 ISO image you created and NFS-mounted in "To Download and Uncompress the OTP and Solaris OS Installation Zip Files" on page 42.

For example, if:

- The name of the OS image to be created is to be `sol10u2`
- The name of the server on which you created the ISO image is `otpsource`
- The ISO image `sol10u2-ga-sp-dvd.iso` was created in the NFS-mounted directory `/otp-download`

you would then type:

```
N1-ok> create os sol10u2 file /net/otpsource/otp-download/sol10u2-ga-sp-dvd.iso
```

Note – A job is submitted to create the OS image, and a job ID is displayed. The `create os` command can take up to 60 minutes to complete.

To check for job completion, type **`show job`** *job ID*. When the job has completed, type **`show os`** to list the OS images.

Next Steps Create the XML discovery file as described in the next section.

▼ Provisioning Bare Metal Systems Using Manual Discovery

To discover, manage, and provision an OS to a bare metal (no operating system installed) OTP host or hosts, you must create an XML discovery file that lists the host name, model number, and MAC address for each new OTP host.

1 Log in as root to the OTP master server.

2 Create the XML discovery file.

For example, `vi /tmp/discovery-mac-addresses`.

3 Add the system name, model number, Ethernet port address, and MAC address for each host to be discovered.

The file format is:

```
<!xml version='1.0' encoding='utf-8'?>
<servers>
    <server name="otpclient1" model="model name">
        <ethernetPort name="GB_0" mac="mac address"/>
    </server>
    <server name="otpclient2" model="model name">
        <ethernetPort name="GB_0" mac="mac address"/>
    </server>
</servers>
```

Where *otpclient1* is the name to be assigned to the host, *model name* is the model name listed in the following table, and *mac address* is the MAC address of the host.

Host Type	Model Type for Bare Metal Discovery
Sun Netra 240	NETRA-240
Sun Netra 440	NETRA-250

Host Type	Model Type for Bare Metal Discovery
Sun Fire V240	SF-V240
Sun Fire V440	SF-V440
Sun Fire V890	SF-V890
Sun Fire T2000	SF-T2000

For example:

```
<!xml version='1.0' encoding='utf-8'?>
<servers>
    <server name="otpclient1" model="NETRA-240">
        <ethernetPort name="GB_0" mac="0:3:ba:19:c5:b"/>
    </server>
    <server name="otpclient2" model="SF-V20">
        <ethernetPort name="GB_0" mac="0:7:3c:12:b6:a"/>
    </server>
    <server name="otpclient3" model="SF-T2000">
        <ethernetPort name="GB_0" mac="0:14:4f:25:5e:78"/>
    </server></servers>
```

4 Save and close the file.

Next Steps

- If you are deploying the OS to new OTP hosts in the same subnet, prepare and deploy the OS as described in "Preparing and Deploying the Solaris OS to the New OTP Hosts" on page 158.
- If you are deploying the OS to new OTP hosts in a different subnet using the OTP system management service, create the DHCP relay as described in the next procedure.

▼ To Create the DHCP Relay for Deploying to New OTP Hosts On Different Subnets

If you are going to deploy the Solaris 10 Update 2 to new OTP hosts on a different subnet using the OTP system management service, you must set up a DHCP relay on each subnet as described in this procedure before you can discover and subsequently deploy the OS to the hosts.

The examples in the following procedure assume:

- The production OTP host that is to be used to provision the OS is on subnet 10.1.15
- The new OTP host or hosts are on subnet 10.1.30

1. **Log in as root to a Solaris OS SPARC server on the 10.1.30 subnet.**

   The server must not be a standalone OTP host or a clustered OTP host.

2. **Type the `ps -ef | grep dhcp` to verify that the DHCP service has started.**

   ```
   # ps -ef | grep dhcp
   oot 24992     1   0 18:20:53 ?           0:00 /usr/lib/inet/in.dhcpd
   ```

3. **Type `dhcpconfig -R` *production OTP hostIP address*, *otpclient1 IP address ..., otpclientn IP address*.**

   For example:

   ```
   # dhcpconfig -R 10.1.15.1,10.1.30.5, 10.1.30.6,10.1.30.7,10.1.30.8,\
   10.1.30.9,10.1.30.10,10.1.30.11,10.1.30.12
   ```

4. **Log in as root to the OTP master server.**

5. **Type `/opt/sun/n1gc/bin/n1sh` to open the OTP command shell.**

   ```
   # /opt/sun/n1gc/bin/n1sh
   N1-OK>
   ```

6. **Set up the OTP DHCP service.**

   In the OTP command shell, type `create dhcpconfig` *DHCP configuration name* `network` *IP address of base network* `netmask` *netmask value* `defaultgw` *gateway IP address* `domain` *domain name* where:

   - *DHCP configuration name* is the name you assign to the OTP DHCP configuration
   - *IP address of base network* is the base address of the target subnet
   - *netmask value* is the netmask value of the target subnet
   - *gateway IP address* is the IP address of the target subnet gateway
   - *domain name* is your corporate domain name

   For example:

   ```
   N1-ok> create dhcpconfig test network 10.11.55.0 netmask 255.255.255.0
   defaultgw 10.11.55.1 domain mycompany.com
   ```

   Note – The above example was split into two lines to fit on the page. When typing the `create dhcpconfig` command, type the full command as a single line.

Next Steps Prepare and deploy the OS as described in the next section.

Preparing and Deploying the Solaris OS to the New OTP Hosts

This section provides the procedures for using either the graphical user interface or the command line to create an OS profile, discover the new OTP hosts, and deploy the OS to the new OTP hosts.

The following topics are discussed:

Tip – If you are unfamiliar with the OTP system, use the graphical user interface to prepare and deploy the OS to the new OTP hosts. The graphical user interface provides setup wizards to help you create the OS profile.

Preparing and Deploying the OS to the New OTP Hosts Using the Graphical User Interface

This section provides the graphical user interface procedures for creating the OS profile, discovering the new OTP hosts, and deploying the OS to the new OTP hosts.

▼ To Create the OS Profile

1 **Open a Web browser and log in to the OTP master server system management service.**

Go to URL https://*OTP master server*:6789 where OTP master server is either the IP address or the fully qualified name of the OTP master server.

The Java Web console log in page is appears. Type your OTP account name and password to log in.

The system management page appears.

2 **Click Sun N1 System manager.**

The System Manager page appears.

3 **Click New... beneath OS Profiles in the Task Shortcuts panel on the right side of the page.**

The Create Operating System Profile wizard appears. Step 1, Specify Initial OS Profile Information is displayed.

Tip – Click Help on this panel and subsequent panels for a description of each panel.

4 **Specify the initial OS profile information.**

   a. **Type a name for the OS profile in the Name field.**

   b. **(Optional) Type a description of the OS profile in the Description field.**

   c. **Choose the OS distribution from the drop-down list in the Distribution field.**

   d. **Type the root password to be used for the new OS distribution in the Root Password field.**

   e. **Type the root password again in the Confirm Password field.**

   Click Next. Step 2, Specify Preferences is displayed.

5 **Specify the language and time zone preferences.**

   a. **Choose the language locale from the Language drop down list.**

   b. **Choose the time zone from the Time Zone drop down list.**

   Click Next. Step 2.1, Specify Solaris Flash archive is displayed.

6 **(Optional) Type the full path to the Solaris flash archive.**

   - If you have not created a Solaris flash archive, click Next.
   - If you have created a Solaris flash archive, type the full path to the location of the flash archive, and then click Next.

   Step 3, Add Distribution Groups is displayed.

7 **Choose Entire Distribution plus OEM.**

   Click Entire Distribution plus OEM in the Available column and then click Add to add it to the Selected column.

   Note – If your browser displays only a portion of the distributions, choose the second `Entire Distribution` in the list.

   Click Next. Step 4, Define Partitions is displayed.

8 **Define the partitions.**

   Refer to Table 3–1 for disk drive partitioning requirements when allocating the root `/`, `swap`, and `/globaldevices` partitions.

For each partition:

- **Type the partition name in the Mount Point field.**
- **Type the file system type in the File System field.**
- **Type the partition size in Mbytes in the Size (MB) field.**
- **Click add.**

The partition is added beneath the entry fields.

Caution – When specifying the disk partitions, ensure that you allocate the `/globaldevices` directory with at least 512 Mbytes of free space.

The Partitions panel should be similar to the following:

Partitions (3)

Mount Point	File System	Size (MB)	Device	Action
	ufs			Add
/globaldevices	ufs	512	c0t0d0s4	Remove
swap	swap	4000	c0t0d0s1	Remove
/	ufs	free	c0t0d0s0	Remove

When you have completed defining the partitions, click Next. Step 4, Specify NIS and LDAP Preferences is displayed.

9 (Optional) Specify NIS and LDAP Preferences.

- If you do not want to specify NIS and LDAP preferences, click Next.

  Step 6, Review Selections is displayed.
- To specify NIS and LDAP preferences, check the items you want to specify and then click Next.

  Additional sub-steps labeled 5.1 up to 5.4 are displayed for each item you have checked. Click the Help tab within each step to display information about that step.

  When you have completed specifying the information for all of your selections, click Next. Step 6, Review Selections is displayed.

Check the items that you want to specify and then click next. Depending on your choices

10 Review your selections.

Caution – Make certain that Entire Distribution plus OEM has been selected.

If the selections are correct, click Finish. Otherwise, click the appropriate Step to correct the selections.

When you click Finish, a job ID is displayed in the Command Pane. To view the job status, click the Jobs tab or type **`show job`** *job ID* in the Command Pane. When the job completes, the OS profile name is listed beneath OS Profiles in the Task Shortcuts panel.

Next Steps Discover the new OTP hosts as described in the next procedure.

▼ To Discover the New OTP Host

1. **Open a Web browser and log in to the OTP master server system management service.**

   Go to URL https://*OTP master server*:6789 where OTP master server is either the IP address or the fully qualified name of the OTP master server.

   The Java Web console log in page is appears. Type your OTP account name and password to log in.

   The system management page appears.

2. **Click Discover.**

   The Discovery wizard appears. Step 1, Specify Discovery Method is displayed.

   Tip – Click Help on this panel and subsequent panels for a description of each panel.

3. **Specify the discovery method.**

   Select Use MAC address From a File and type the name of the file you created in "Provisioning Bare Metal Systems Using Manual Discovery" on page 155. For example, `/tmp/discovery-mac-addresses`

   Step 2, Specify Security Credentials is displayed.

4. **Specify the security credentials.**

   - If you have not changed the ALOM settings, select Use Default Credentials and then click next.
   - If you have changed the settings, type the user name and password in the fields provided, and then click next.

     Refer to the server hardware documentation for information about ALOM credentials.

   Step 3, Specify the Server Group is displayed.

5 **Specify the server group into which the discovered new OTP host or hosts are to be placed and then click next.**

Tip – Place all of the new OTP hosts of a clustered OTP system in a single server group.

Step 4, Review Selections is displayed.

---

6 **Review your selections.**

If the selections are correct, click Finish. Otherwise, click the appropriate step to correct the selections.

When you click Finish, a job ID is displayed in the Command Pane. To view the job status, click the Jobs tab or type **`show job`** *job ID* in the Command Pane. Wait for discovery to complete. When the new OTP host or hosts are discovered, discovered hosts are listed on the System Dashboard tab.

Next Steps Deploy the OS to the clustered OTP hosts as described in the next procedure.

▼ To Deploy the OS to the New OTP Hosts

1 **If you have closed the Web browser, open a Web browser and log in to the OTP master server system management service as described in the previous procedure.**

When you have logged on, click Sun N1 System manager to display the System Manager page.

2 **If the OS profile you created is not displayed beneath OS Profiles in the Task Shortcuts panel, click Edit List to display the list of available OS profiles.**

In the OS profile list, click the checkbox to the left of the OS profile you created, and then click OK.

The OS profile list closes, and the OS profile name is displayed beneath OS Profiles in the Task Shortcuts panel.

3 **Click and drag OS profile over the name of the new OTP host that is to be provisioned, and release the mouse button.**

The Load OS wizard appears. Step 1, Specify OS Profile Loading Options is displayed.

4 **Specify OS profile loading operations.**

Note – If the OS profile name you chose in the previous step is not displayed in the OS Profile field, choose the OS profile from the drop-down menu.

---

a. **Select Static IP, and then enter the IP address that is to be assigned to the new OTP host when OS provisioning is completed.**

b. Clear the Use Default Settings checkbox.

Click Next. Step 1.1, Specify Boot Parameters appears.

5 Specify the boot parameters.

Select Enable Manual Net Boot.

Note – Do not specify any other values for this section. For more information, click the Help tab.

Click Next. Step 1.2, Specify Boot Parameters appears.

6 (Optional) Specify the boot parameters.

a. Type `ttya` in the Console field.

b. Type the baud rate in the Console Baud field. The default is 9600 baud.

Click Next. Step 1.3, Specify Network Configuration is displayed.

7 (Optional) Specify the network configuration.

a. Type the gateway IP address in the Gateway field.

b. Type the IP address of the DNS server in the Name Server field.

c. Type the domain name in the Domain Name field.

Click Next. Step 1.4, Specify Hostname is displayed.

8 Specify the host name.

Type the host name in the Hostname field and then click Next. Step 2, Select OS Management Features is displayed.

9 Select OS management features.

Choose the OS management feature from the Features drop-down list.

- If you choose Base management, only the SSH credentials are required, and the remaining fields are disabled.
- If you choose Base management and OS monitoring, all credentials are required.

Type the required credentials in each field. Click the Help tab for information about each field.

Click Next when you have completed typing the required information.

10 Review your selections.

Caution – Make certain that Entire Distribution plus OEM has been selected. If Entire Distribution plus OEM is not listed, you must create a new OS Profile in which Entire Distribution plus OEM has been specified as described in "To Create the OS Profile" on page 158.

If the selections are correct, click Finish. Otherwise, click the appropriate Step to correct the selections.

When you click Finish, the Load OS wizard closes, and a job is submitted to load the OS profile to the new OTP host. A job ID is displayed in the Command Line pane.

11 **Click the Jobs tab to view the job status, or type `show job` *job ID* in the Command Pane, where *job ID* is the ID that was displayed when you clicked Finish.**

Note – The new OTP host status on the System Dashboard tab will not update until the host has rebooted and the Load OS job has completed.

Next Steps Repeat the above steps for each new OTP host that is to be provisioned.

When you have completed provisioning the OS to all new OTP hosts, install OTP to the hosts as described in "Installing OTP on a New OTP Host Using the OTP Master Server" on page 149

Preparing and Deploying the OS to the New OTP Hosts Using the Command Line

This section provides the command-line procedures for creating the OS profile, discovering the new OTP hosts, and deploying the OS to the new OTP hosts.

▼ To Create the OS Profile

1 **Log in as root to the OTP master server.**

2 **Type `/opt/sun/n1gc/bin/n1sh` to open the OTP N1™ command shell. For example:**

```
# /opt/sun/n1gc/bin/n1sh
N1-ok>
```

3 **In the OTP command shell, type `create osprofile` *os profile name* `os` *OS image name* `rootpassword` *root password* where:**

- *os profile name* is the name of the OS profile to be created
- *OS image name* is the name of the OS image you created in "To Create the OS Image" on page 154

- *root password* is the root password of the production OTP host

For example:

```
N1-ok> create osprofile s10u2-profile os sol10u2 rootpassword otpadmin
```

4 Set the OS profile language and time zone.

Type `set osprofile` *os profile name* `language` *locale* `timezone` *time zone* where:

- *os profile name* is the name of the OS profile you created in the previous step
- *language* is your locale code
- *time zone* is your time zone

For example:

```
N1-ok> set osprofile s10u2-profile language en_US.ISO8859-15 timezone GMT
```

5 Set the OS installation type in the OS profile.

Type `add osprofile` *os profile name* `distributiongroup "Entire Distribution plus OEM support"` where *os profile name* is the name of the OS profile you created .

For example:

```
N1-ok> add osprofile s10u2-profile distributiongroup "Entire Distribution plus OEM support"
```

6 Set the root partition allocation in the OS profile.

Type `add osprofile` *os profile name* `partition / device` *disk slice* `type ufs sizeoption free`.

For example:

```
N1-ok> add osprofile s10u2-profile partition / c0t0d0s0 type ufs sizeoption free
```

7 Set the swap space allocation in the OS profile.

Type `add osprofile` *os profile name* `partition swap device` *disk slice* `type swap sizeoption fixed size` *size in Mbytes*.

For example:

```
N1-ok> add osprofile s10u2-profile partition swap device c0t0d0s1 type swap sizeoption fixed size 4000
```

8 Set the `/globaldevices` file system allocation in the OS profile.

Type `add osprofile` *os profile name* `partition /globaldevices device` *disk slice* `type ufs sizeoption fixed size` *size in Mbytes*.

For example:

```
N1-ok> add osprofile s10u2-profile partition /globaldevices device c0t0d0s3
 type ufs sizeoption fixed size 4000
```

Note – The above example was split into two lines to fit on the page. When typing the `add osprofile` command, type the full command as a single line.

Next Steps Run discovery to identify the new OTP hosts to which the Solaris 10 Update 2 OS is to be deployed as described in the next procedure.

▼ To Discover the New OTP Hosts

1. **Log in as root to the OTP master server.**

2. **Type `/opt/sun/n1gc/bin/n1sh` to open the OTP N1 command shell. For example:**

```
# /opt/sun/n1gc/bin/n1sh
N1-ok>
```

3. **Discover the new OTP host or hosts.**

   Type the command `discover` *XML discovery file name* `format=file` where *XML discovery file name* is the name of the XML discovery file you created in "Provisioning Bare Metal Systems Using Manual Discovery" on page 155.

   An OTP job is submitted to discover the servers, and a job ID is displayed.

   Type **`show job`** to display the job status. When the job has completed, type **`show servers all`** to display a list of the new OTP hosts that have been discovered. To view details about a specific server, type `show server` *server id* where *server id* is a server ID listed by the `show servers all`.

Next Steps Repeat the above steps for each new OTP host. When you have completed discovering the hosts, deploy the OS to the discovered hosts as described in the next procedure.

▼ To Deploy the OS to the New OTP Host

1. **Log in as root to the OTP master server.**

2. **Type `/opt/sun/n1gc/bin/n1sh` to open the OTP command shell.**

3. **Deploy the OS to the new OTP hosts**

   In the OTP command shell, type `load server` *ALOM IP address* `osprofile` *OS profile name* `networktype static IP` *Provisioning IP address* `hostname` *hostname* `manualnetboot=true` where:

   - *ALOM IP address* is the IP address of the new OTP host's ALOM management port
   - *OS profile name* is the name of the OS profile
   - *Provisioning IP address* is the IP address of the new OTP host's provisioning interface

- *hostname* is the name that will be assigned to the new OTP host

For example:

```
N1-ok> load server 10.1.15.1 osprofile sol10u2-profile networktype
static IP 10.1.15.5 otpclient1 manualnetboot=true
```

Note – The above example has been split into two lines to fit on the page. When typing the `load server` command, type the entire command as one continuous line.

Next Steps Repeat the above steps for each new OTP host that is to be provisioned.

When you have completed provisioning the OS to all new OTP hosts, prepare each new OTP host as described in the next section.

- To install the Open Telecommunications Platform on a standalone OTP host, see "To Install OTP on a Standalone OTP Host" on page 150.
- To install the Open Telecommunications Platform on a clustered OTP system, see "To Install OTP on a Clustered OTP System" on page 150.

Preparing the New OTP Hosts for OTP Installation

This section provides the procedure for preparing the new OTP host or hosts for Open Telecommunications Platform and for installing the Open Telecommunications Platform.

▼ To Prepare the New OTP Hosts for OTP Installation

1. **Configure the Solaris OS on each new OTP host as described in "Configuring Solaris 10 Update 2" on page 94.**
2. **Install the service provisioning remote agent on each new OTP host as described in "To Manually Install the Solaris OS and the Remote Agent on a New OTP Host" on page 52.**
3. **Add each new OTP host to the OTP master server as described in "To Add New OTP Hosts to the OTP Master Server" on page 148.**

Next Steps Install the Open Telecommunications Platform as follows:

- To install the Open Telecommunications Platform on a standalone OTP host, see "To Install OTP on a Standalone OTP Host" on page 150.
- To install the Open Telecommunications Platform on clustered OTP hosts, see "To Install OTP on a Clustered OTP System" on page 150.

◆ ◆ ◆ CHAPTER 8

Backing Up and Restoring the OTP Provisioning Service and the OTP System Management Service

This chapter provides the procedures for backing up the provisioning service and system management and database and configuration files, restoring the files to a new OTP host, and for enabling the services on a new OTP host.

The following topics are discussed:

Backing Up and Restoring the OTP Provisioning Service Database and Configuration Files

This section provides the procedure for backing up and restoring the provisioning service database and configuration files. Backup of the provisioning service database and configuration files should be performed on a regular basis. Situations that could warrant provisioning service restoration of the service after applying system patches or performing a JumpStart installation.

The following topics are discussed:

Backing Up and Restoring the OTP Provisioning Service on the External OTP Installation Server

This section provides the procedures for backing up and restoring the OTP provisioning service on the external OTP installation server

The following topics are discussed:

▼ To Back Up the Provisioning Service on the External OTP Installation Server

1 Log in to the external OTP installation server as root.

2 Type the following command to back up the provisioning service.

Tip – copy and paste the following command to the terminal window.

```
su - spsotp \
/var/otp/spsotp/N1_Service_Provisioning_System_5.2/server/bin/cr_backup.sh \
-b /var/otp/spsotp/N1_Service_Provisioning_System_5.2 \
-l /var/tmp/backup.log \
-o /var/tmp -nors -noconfig -nokeystore  -z -shutdown yes
```

The compressed backup tar file and the backup log file are created in the directory `/var/tmp/`. For example, `/var/tmp/backup_log.`*070411145059* and `/var/tmp/`*070411145059*`.tar.Z` where *070411145059* is the system date and time stamp.

▼ To Restore the Provisioning Service on the External OTP Installation Server

Before You Begin The provisioning service on the external OTP installation server must be backed up as described in "To Back Up the Provisioning Service on the External OTP Installation Server" on page 170

1 Log in to the external OTP installation server as root.

2 Type the following command to back up the provisioning service.

```
su - spsotp \
/var/otp/spsotp/N1_Service_Provisioning_System_5.2/server/bin/cr_restore.sh \
-b /var/otp/spsotp/N1_Service_Provisioning_System_5.2 \
```

```
-f /var/tmp/backup tar file name \
-l /var/tmp/log_file_name \
-t /var/tmp -shutdown yes -nors -noconfig -nokeystore -overwrite yes
```

where *backup tar file name* is the name of the backup tar file created in "To Back Up the Provisioning Service on the External OTP Installation Server" on page 170, and *log file name* is the name you specify for the log file. The system date and time stamp is automatically appended to the log file name you specify. For example, `/var/tmp/restore_log.`*070411145059*

Backing Up the OTP Provisioning Service on an External OTP Installation Server and Restoring to a Clustered OTP Host

This section provides the procedures for backing up the provisioning service on an external OTP installation server and restoring the provisioning service to a clustered OTP host.

Backing up the provisioning service on an external OTP installation server and restoring it to an OTP host is comprised of the following tasks:

- Removing the Remote Agent from the External OTP Installation Server
- Removing the Remote Agent from the Restore Target OTP Host
- Backing Up the Provisioning Service on the External OTP Installation Server
- Restoring the Provisioning Service Backup to the Target OTP Host
- Adding the Remote Agent to the External OTP Installation Server
- Adding the Remote Agent to the Target OTP Host

▼ To Remove the Remote Agent from the External OTP Installation Server

1. **Open a Web browser and go to URL https://*install server*:9090 where *install server* is either the IP address or the fully qualified name of the external OTP installation server.**

   The OTP provisioning service log in screen appears.

2. **Log in to the OTP provisioning service.**

   The Service Provisioning System screen appears.

3. **Click Host Setup in the left panel.**

   The host setup screen appears.

4. **Click hosts in the central panel.**

   The hosts screen appears.

5. **Click master server.**
   The hosts > details screen appears.
6. **Scroll to the bottom of the screen and click edit.**
   The hosts > details > edit screen appears.
7. **If the checkbox labeled `include remote agent on this physical host` has a check mark in it, click the check box to remove the check mark.**
8. **Scroll to the bottom of the screen and click save.**

Next Steps Remove the remote agent from the restore target OTP host as described in the next procedure.

▼ To Remove the Remote Agent from the Restore Target OTP Host

Before You Begin The remote agent must be removed from the external OTP installation server as described in "To Remove the Remote Agent from the External OTP Installation Server" on page 171

1. **Open a Web browser and go to URL https://*OTP host*:9090 where *OTP host* is either the IP address or the fully qualified name of the OTP host to which the provisioning service is to be restored.**
   The OTP provisioning service log in screen appears.
2. **Log in to the OTP provisioning service.**
   The Service Provisioning System screen appears.
3. **Click Host Setup in the left panel.**
   The host setup screen appears.
4. **Click hosts in the central panel.**
   The hosts screen appears.
5. **Click master server.**
   The hosts > details screen appears.
6. **Scroll to the bottom of the screen and click edit.**
   The hosts > details > edit screen appears.
7. **If the checkbox labeled `include remote agent on this physical host` has a check mark in it, click the check box to remove the check mark.**
8. **Scroll to the bottom of the screen and click save.**

Next Steps Back up the provisioning service on the external OTP installation server as described in the next procedure.

▼ To Back Up the Provisioning Service on the External OTP Installation Server

Before You Begin

- The remote agent must be removed from the external OTP installation server as described in "To Remove the Remote Agent from the External OTP Installation Server" on page 171
- The remote agent must be removed from the restore target OTP host as described in "To Remove the Remote Agent from the Restore Target OTP Host" on page 172

1 Log in as root to the external OTP installation server.

2 Type the following command to back up the provisioning service.

Tip – Copy and paste the following command to your root terminal window.

```
su - spsotp \
/var/otp/spsotp/N1_Service_Provisioning_System_5.2/server/bin/cr_backup.sh \
-b /var/otp/spsotp/N1_Service_Provisioning_System_5.2 \
-o /var/tmp -nors -noconfig -nokeystore  -z -shutdown yes
```

The backup tar file is created as `/var/tmp/`*timestamp*`.tar.Z`. For example:

The compressed backup tar file and the backup log file are created in the directory `/var/tmp/`. For example, `/var/tmp/backup_log.`*070411145059* and `/var/tmp/`*070411145059*`.tar.Z` where *070411145059* is the system date and time stamp.

Next Steps Restore the backup from the external OTP installation server to the target OTP host as described in the next procedure.

▼ To Restore the Provisioning Service Backup to the Target OTP Host

Before You Begin

- The remote agent must be removed from the external OTP installation server as described in "To Remove the Remote Agent from the External OTP Installation Server" on page 171
- The remote agent must be removed from the restore target OTP host as described in "To Remove the Remote Agent from the Restore Target OTP Host" on page 172
- The provisioning service on the external OTP installation server must be backed up as described in "To Back Up the Provisioning Service on the External OTP Installation Server" on page 173

1. **Log in as root to an OTP host in the cluster.**

2. **Type `/usr/cluster/bin/scstat -g` to determine which host in the cluster is online.**

   Make note of the host on which the resource group `otp-system-rg` is online.

   For example:

```
# /usr/cluster/bin/scstat -g | grep Online
    Group: otp-system-rg       otp-node17          Online
 Resource: otp-lhn             otp-node17          Online    Online - LogicalHostname online
 Resource: otp-sps-hastorage-plus otp-node17          Online    Online
 Resource: otp-spsms-rs        otp-node17          Online    Online
 Resource: otp-spsra-rs        otp-node17          Online    Online
```

   In the above example, the resource group `otp-system-rg` is running on online host otp-node17.

3. **Log in as root on the OTP host on which the resource group is online.**

4. **Disable the Provisioning service resource in the resource group.**

   Type the following commands:

```
/usr/cluster/bin/scrgadm -c -g otp-system-rg -y RG_system=FALSE

/usr/cluster/bin/scswitch -n -j otp-spsms-rs
```

5. **Restore the Provisioning service database to the OTP host.**

   Type the following command:

```
su - spsotp \
/var/otp/spsotp/N1_Service_Provisioning_System_5.2/server/bin/cr_restore.sh \
-b /var/otp/spsotp/N1_Service_Provisioning_System_5.2 \
-f /var/tmp/backup tar file name \
-l /var/tmp/log file name \
-t /var/tmp -shutdown yes -nors -noconfig -nokeystore -overwrite yes
```

   where *backup tar file name* is the name of the backup tar file created in "To Back Up the Provisioning Service on the External OTP Installation Server" on page 173, and *log file name* is the name you specify for the log file. The system date and time stamp is automatically appended to the log file name you specify. For example, `/var/tmp/restore_log.070411145059`

6. **Drop the tables used by the cluster to poll the resource group.**

   Type the following commands. Wait for each command to complete before typing the next command.

```
su - spsotp \
/var/otp/spsotp/N1_Service_Provisioning_System_5.2/server/bin/cr_server start
su - spsotp \
/var/otp/spsotp/N1_Service_Provisioning_System_5.2/server/bin/roxdbcmd psql rox
drop user sc_test;
```

The semicolon at the end of the `drop user sc_test;` is required.

7 **Press Cntrl-d to terminate the SQL session.**

8 **Recreate the tables used by the cluster to poll the resource group.**

Type the following commands. Wait for each command to complete before typing the next command.

```
su - spsotp \
/opt/SUNWscsps/master/util/db_prep_postgres \
 /var/otp/spsotp/N1_Service_Provisioning_System_5.2/

su - spsotp \
/var/otp/spsotp/N1_Service_Provisioning_System_5.2/server/bin/cr_server stop
```

9 **Enable the provisioning service resource in the resource group.**

Type the following commands.

```
/usr/cluster/bin/scswitch -e -j otp-spsms-rs

/usr/cluster/bin/scrgadm -c -g otp-system-rg -y RG_system=TRUE
```

Next Steps Add the remote agent to the external OTP installation server as described in the next procedure.

▼ To Add the Remote Agent to the External OTP Installation Server

Before You Begin

- The remote agent must be removed from the external OTP installation server as described in "To Remove the Remote Agent from the External OTP Installation Server" on page 171
- The remote agent must be removed from the restore target OTP host as described in "To Remove the Remote Agent from the Restore Target OTP Host" on page 172
- The provisioning service on the external OTP installation server must be backed up as described in "To Back Up the Provisioning Service on the External OTP Installation Server" on page 173
- The provisioning service backup must be restored to the target OTP host as described in "To Restore the Provisioning Service Backup to the Target OTP Host" on page 173

1 **Open a Web browser and go to URL http://*install server*:9090 where *install server* is either the IP address or the fully qualified name of the external OTP installation server.**

The OTP provisioning service log in screen appears.

2 **Log in to the OTP provisioning service.**

The Service Provisioning System screen appears.

3. **Click Host Setup in the left panel.**
   The host setup screen appears.
4. **Click hosts in the central panel.**
   The hosts screen appears.
5. **Click master server.**
   The hosts > details screen appears.
6. **Scroll to the bottom of the screen and click edit.**
   The hosts > details > edit screen appears.
7. **If the checkbox labeled `include remote agent on this physical host` does not have a check mark in it, click the check box to add the check mark.**
8. **In connection type, choose TCP/IP (unencrypted).**
9. **Type the external OTP installation server IP address in the ip address or name field.**
10. **Type 7010 in the port field.**
11. **Click Save.**
12. **Click master server.**
13. **Scroll to the bottom of the screen and click update remote agent.**
14. **Click prepare remote agent.**

Next Steps Add the remote agent to the target OTP host as described in the next procedure.

▼ To Add the Remote Agent to the Target OTP Host

Before You Begin

- The remote agent must be removed from the external OTP installation server as described in "To Remove the Remote Agent from the External OTP Installation Server" on page 171
- The remote agent must be removed from the restore target OTP host as described in "To Remove the Remote Agent from the Restore Target OTP Host" on page 172
- The provisioning service on the external OTP installation server must be backed up as described in "To Back Up the Provisioning Service on the External OTP Installation Server" on page 173
- The provisioning service backup must be restored to the target OTP host as described in "To Restore the Provisioning Service Backup to the Target OTP Host" on page 173

- The remote agent must be added to the external OTP installation server as described in "To Add the Remote Agent to the External OTP Installation Server" on page 175

1. **Open a Web browser and go to URL http://*OTP host*:9090 where *OTP host* is either the IP address or the fully qualified name of the target OTP host.**

   The OTP provisioning service log in screen appears.

2. **Log in to the OTP provisioning service.**

   The Service Provisioning System screen appears.

3. **Click Host Setup in the left panel.**

   The host setup screen appears.

4. **Click hosts in the central panel.**

   The hosts screen appears.

5. **Click master server.**

   The hosts > details screen appears.

6. **Scroll to the bottom of the screen and click edit.**

   The hosts > details > edit screen appears.

7. **If the checkbox labeled `include remote agent on this physical host` does not have a check mark in it, click the check box to add the check mark.**

8. **In connection type, choose TCP/IP (unencrypted).**

9. **Type the target OTP host IP address in the ip address or name field.**

10. **Type 7010 in the port field.**

11. **Scroll to the bottom of the screen and click save.**

12. **Click master server.**

    Scroll to the bottom of the screen.

13. **Click update remote agent.**

14. **Click prepare remote agent.**

Backing Up the OTP Provisioning Service on one Clustered OTP Host and Restoring to Another Clustered OTP Host

This section provides the procedures for backing up and restoring the OTP provisioning service from one clustered OTP host and restoring the provisioning service to a different clustered OTP host.

Backing up the provisioning service on one OTP host and restoring it to an OTP host is comprised of the following tasks:

- Removing the Remote Agent from the Backup Source OTP Host
- Removing the Remote Agent from the Restore Target OTP Host
- Backing up the Provisioning Service On the Source OTP Host
- Restoring the Provisioning Service Backup To The Restore Target OTP Host
- Adding the Remote Agent To The Backup Source OTP Host
- Adding the Remote Agent To The Restore Target OTP Host

▼ To Remove the Remote Agent from the Backup Source OTP Host

1. **Log in as root to an OTP host in the cluster.**

2. **Type `/usr/cluster/bin/scstat -g` to determine which host in the cluster is online.**

   Make note of the host on which the resource group `otp-system-rg` is active.

   For example:

```
# /usr/cluster/bin/scstat -g | grep Online
    Group: otp-system-rg       otp-node17          Online
 Resource: otp-lhn             otp-node17          Online    Online - LogicalHostname online.
 Resource: otp-sps-hastorage-plus otp-node17          Online    Online
 Resource: otp-spsms-rs        otp-node17          Online    Online
 Resource: otp-spsra-rs        otp-node17          Online    Online
```

   In the above example, the resource group online host is otp-node17.

3. **Open a Web browser and go to URL http://*backup source OTP host*:9090 where *backup source OTP host* is either the IP address or the fully qualified name of the OTP host on which the resource group is active.**

   The OTP provisioning service log in screen appears.

4. **Log in to the OTP provisioning service.**

   The Service Provisioning System screen appears.

5 **Click Host Setup in the left panel.**
The host setup screen appears.

6 **Click hosts in the central panel.**
The hosts screen appears.

7 **Click master server.**
The hosts > details screen appears.

8 **Scroll to the bottom of the screen and click edit.**
The hosts > details > edit screen appears.

9 **If the checkbox labeled `include remote agent on this physical host` has a check mark in it, click the check box to remove the check mark.**

10 **Scroll to the bottom of the screen and click save.**

Next Steps Remove the remote agent from the restore target OTP host as described in the next procedure.

▼ To Remove the Remote Agent from the Restore Target OTP Host

Before You Begin The remote agent must be removed from the backup source OTP host as described in "To Remove the Remote Agent from the Backup Source OTP Host" on page 178

1 **Log in as root to an OTP host in the restore target cluster.**

2 **Type `/usr/cluster/bin/scstat -g` to determine which host in the cluster is active.**
Make note of the host on which the resource group `otp-system-rg` is active.

3 **Open a Web browser and go to URL http://*target OTP host*:9090 where *target OTP host* is either the IP address or the fully qualified name of the OTP host on which the resource group is active.**
The OTP provisioning service log in screen appears.

4 **Log in to the OTP provisioning service.**
The Service Provisioning System screen appears.

5 **Click Host Setup in the left panel.**
The host setup screen appears.

6 **Click hosts in the central panel.**
The hosts screen appears.

7 **Click master server.**

The hosts > details screen appears.

8 **Scroll to the bottom of the screen and click edit.**

The hosts > details > edit screen appears.

9 **If the checkbox labeled `include remote agent on this physical host` has a check mark in it, click the check box to remove the check mark.**

10 **Scroll to the bottom of the screen and click save.**

Next Steps Back up the provisioning service on the source OTP host as described in the next procedure.

▼ To Back Up the Provisioning Service on the Source OTP Host

Before You Begin

- The remote agent must be removed from the backup source OTP host as described in "To Remove the Remote Agent from the Backup Source OTP Host" on page 178
- The remote agent must be removed from the restore target OTP host as described in "To Remove the Remote Agent from the Restore Target OTP Host" on page 179

1 **Log in as root on the backup source OTP host you identified in "To Remove the Remote Agent from the Backup Source OTP Host" on page 178.**

2 **Disable the provisioning service resource in the resource group**

Type the following commands:

```
/usr/cluster/bin/scrgadm -c -g otp-system-rg -y RG_system=FALSE

/usr/cluster/bin/scswitch -n -j otp-spsms-rs
```

3 **Backup the provisioning service database**

Type the following command:

```
su - spsotp \
/var/otp/spsotp/N1_Service_Provisioning_System_5.2/server/bin/cr_backup.sh \
-b /var/otp/spsotp/N1_Service_Provisioning_System_5.2 \
-o /var/tmp -nors -noconfig -nokeystore  -z -shutdown yes
```

The compressed backup tar file is created as `/var/tmp/`*timestamp*`.tar.Z` where *timestamp* is the system date and time stamp. For example, `/var/tmp/`*070411145059*`.tar.Z`

4 **Enable the Provisioning service resource in the resource group.**

Type the following commands:

```
/usr/cluster/bin/scswitch -e -j otp-spsms-rs
```

```
/usr/cluster/bin/scrgadm -c -g otp-system-rg -y RG_system=TRUE
```

Next Steps Restore the provisioning service to the restore target OTP host as described in the next procedure.

▼ To Restore the Provisioning Service Backup To The Restore Target OTP Host

Before You Begin

- The remote agent must be removed from the backup source OTP host as described in "To Remove the Remote Agent from the Backup Source OTP Host" on page 178
- The remote agent must be removed from the restore target OTP host as described in "To Remove the Remote Agent from the Restore Target OTP Host" on page 179
- The backup source OTP host provisioning service must be backed up as described in "To Back Up the Provisioning Service on the Source OTP Host" on page 180.

1 Log in as root to the restore target OTP host.

This is the OTP host from which you removed the remote agent as described in "To Remove the Remote Agent from the Restore Target OTP Host" on page 179.

2 Disable the provisioning service resource in the resource group.

Type the following commands:

```
/usr/cluster/bin/scrgadm -c -g otp-system-rg -y RG_system=FALSE

/usr/cluster/bin/scswitch -n -j otp-spsms-rs
```

3 Restore the Provisioning service database.

Type the following command

```
su - spsotp \
/var/otp/spsotp/N1_Service_Provisioning_System_5.2/server/bin/cr_restore.sh \
-b /var/otp/spsotp/N1_Service_Provisioning_System_5.2 \
-f /var/tmp/backup tar file name \
-l /var/tmp/log file name \
-t /var/tmp -shutdown yes -nors -noconfig -nokeystore -overwrite yes
```

Where *backup tar file name* is the name of the backup file you created in "To Back Up the Provisioning Service on the Source OTP Host" on page 180, and *log file name* is the name you specify for the log file.

4 Drop and recreate the tables used by the cluster to poll the resource group.

Type the following commands:

```
su - spsotp \
/var/otp/spsotp/N1_Service_Provisioning_System_5.2/server/bin/cr_server start
```

```
cd /var/otp/spsotp/N1_Service_Provisioning_System_5.2/server/bin/

su - spsotp \
/var/otp/spsotp/N1_Service_Provisioning_System_5.2/server/bin/roxdbcmd psql rox

drop user sc_test;

drop table sc_test;
```

The semicolon at the end of the `drop user sc_test;` and `drop table sc_test;` is required.

5 **Type Ctrl-d to terminate the SQL session.**

6 **Recreate the tables used by the cluster to poll the resource group.**

```
su - spsotp \
/opt/SUNWscsps/master/util/db_prep_postgres \
/var/otp/spsotp/N1_Service_Provisioning_System_5.2/

su - spsotp \
/var/otp/spsotp/N1_Service_Provisioning_System_5.2/server/bin/cr_server stop
```

7 **Enable the provisioning service resource in the resource group.**

```
/usr/cluster/bin/scswitch -e -j otp-spsms-rs

/usr/cluster/bin/scrgadm -c -g otp-system-rg -y RG_system=TRUE
```

Next Steps Add the remote agent to the backup source OTP host as described in the next procedure.

▼ To Add the Remote Agent To The Backup Source OTP Host

Before You Begin

- The remote agent must be removed from the backup source OTP host as described in "To Remove the Remote Agent from the Backup Source OTP Host" on page 178
- The remote agent must be removed from the restore target OTP host as described in "To Remove the Remote Agent from the Restore Target OTP Host" on page 179
- The backup source OTP host provisioning service must be backed up as described in "To Back Up the Provisioning Service on the Source OTP Host" on page 180.
- The provisioning service backup must be restored to the restore target OTP host as described in "To Restore the Provisioning Service Backup To The Restore Target OTP Host" on page 181

1 **Open a Web browser and go to URL http://*backup source OTP host*:9090 where *backup source OTP host* is either the IP address or the fully qualified name of the OTP host you identified in "To Remove the Remote Agent from the Backup Source OTP Host" on page 178.**

The OTP provisioning service log in screen appears.

2. **Log in to the OTP provisioning service.**
   The Service Provisioning System screen appears.
3. **Click Host Setup in the left panel.**
   The host setup screen appears.
4. **Click hosts in the central panel.**
   The hosts screen appears.
5. **Click master server.**
   The hosts > details screen appears.
6. **Scroll to the bottom of the screen and click edit.**
   The hosts > details > edit screen appears.
7. **If the checkbox labeled `include remote agent on this physical host` does not have a check mark in it, click the check box to add the check mark.**
8. **In connection type, choose TCP/IP (unencrypted).**
9. **Type the backup source OTP host IP address in the ip address or name field.**
10. **Type 7010 in the port field.**
11. **Scroll to the bottom of the screen and click save.**
12. **Click master server.**
13. **Click update remote agent.**
14. **Click prepare remote agent.**

Next Steps Add the remote agent to the restore target OTP host as described in the next procedure.

▼ To Add the Remote Agent To The Restore Target OTP Host

Before You Begin

- The remote agent must be removed from the backup source OTP host as described in "To Remove the Remote Agent from the Backup Source OTP Host" on page 178
- The remote agent must be removed from the restore target OTP host as described in "To Remove the Remote Agent from the Restore Target OTP Host" on page 179
- The backup source OTP host provisioning service must be backed up as described in "To Back Up the Provisioning Service on the Source OTP Host" on page 180.

- The provisioning service backup must be restored to the restore target OTP host as described in "To Restore the Provisioning Service Backup To The Restore Target OTP Host" on page 181
- The remote agent must be added to the backup source OTP host as described in "To Add the Remote Agent To The Backup Source OTP Host" on page 182

1. **Open a Web browser and go to URL http://*restore target OTP host*:9090 where *restore targetOTP host* is either the IP address or the fully qualified name of the target OTP host to which you restored the provisioning service in "To Restore the Provisioning Service Backup To The Restore Target OTP Host" on page 181.**

   The OTP provisioning service log in screen appears.

2. **Log in to the OTP provisioning service.**

   The Service Provisioning System screen appears.

3. **Click Host Setup in the left panel.**

   The host setup screen appears.

4. **Click hosts in the central panel.**

   The hosts screen appears.

5. **Click master server.**

   The hosts > details screen appears.

6. **Scroll to the bottom of the screen and click edit.**

   The hosts > details > edit screen appears.

7. **If the checkbox labeled `include remote agent on this physical host` does not have a check mark in it, click the check box to add the check mark.**

8. **In connection type, choose TCP/IP (unencrypted).**

9. **Type the restore target OTP host IP address in the ip address or name field.**

10. **Type 7010 in the port field.**

11. **Scroll to the bottom of the screen and click save.**

12. **Click master server.**

13. **Click update remote agent.**

14 Click prepare remote agent.

Backing Up the OTP Provisioning Service on a Clustered OTP Host and Restoring to the External OTP Installation Server

This section provides the procedures for backing up and restoring the OTP provisioning service from one clustered OTP host and restoring the provisioning service to the external OTP installation server.

Backing up the provisioning service on an OTP host and restoring it to the external OTP installation server is comprised of the following tasks:

- Removing the Remote Agent from the Backup Source OTP Host
- Removing the Remote Agent from the External OTP installation server
- Backing Up the Provisioning Service On The Source OTP Host
- Restoring the Provisioning Service Backup To The External OTP Installation Server
- Adding the Remote Agent To The Backup Source OTP Host
- Adding the Remote Agent To External OTP Installation Server

▼ To Remove the Remote Agent from the Backup Source OTP Host

1 Log in as root to an OTP host in the cluster.

2 Type `/usr/cluster/bin/scstat -g | grep Online` to determine which host in the cluster is active.

Make note of the host on which the resource group `otp-system-rg` is active.

3 Open a Web browser and go to URL http://*backup source OTP host*:9090 where *backup source OTP host* is either the IP address or the fully qualified name of the OTP host on which the resource group is active.

The OTP provisioning service log in screen appears.

4 Log in to the OTP provisioning service.

The Service Provisioning System screen appears.

5 Click Host Setup in the left panel.

The host setup screen appears.

6 **Click hosts in the central panel.**

The hosts screen appears.

7 **Click master server.**

The hosts > details screen appears.

8 **Scroll to the bottom of the screen and click edit.**

The hosts > details > edit screen appears.

9 **If the checkbox labeled** `include remote agent on this physical host` **has a check mark in it, click the check box to remove the check mark.**

10 **Scroll to the bottom of the screen and click save.**

Next Steps Remove the remote agent from the External OTP Installation Server as described in the next procedure.

▼ To Remove the Remote Agent from the External OTP installation server

Before You Begin The remote agent must be removed from the backup source OTP host as described in "To Remove the Remote Agent from the Backup Source OTP Host" on page 185

1 **Open a Web browser and go to URL http://***external OTP installation server***:9090 where** *external OTP installation server* **is either the IP address or the fully qualified name of the external OTP installation server.**

The OTP provisioning service log in screen appears.

2 **Log in to the OTP provisioning service.**

The Service Provisioning System screen appears.

3 **Click Host Setup in the left panel.**

The host setup screen appears.

4 **Click hosts in the central panel.**

The hosts screen appears.

5 **Click master server.**

The hosts > details screen appears.

6 **Scroll to the bottom of the screen and click edit.**

The hosts > details > edit screen appears.

7 **If the checkbox labeled `include remote agent on this physical host` has a check mark in it, click the check box to remove the check mark.**

8 **Scroll to the bottom of the screen and click save.**

Next Steps Back up the provisioning service on the source OTP host as described in the next procedure.

▼ To Back Up the Provisioning Service on the Source OTP Host

Before You Begin

- The remote agent must be removed from the backup source OTP host as described in "To Remove the Remote Agent from the Backup Source OTP Host" on page 185
- The remote agent must be removed from the external OTP installation server as described in "To Remove the Remote Agent from the External OTP installation server" on page 186

1 **Log in as root on the backup source OTP host you identified in "To Remove the Remote Agent from the Backup Source OTP Host" on page 185.**

2 **Disable the provisioning service resource in the resource group**

Type the following commands:

```
/usr/cluster/bin/scrgadm -c -g otp-system-rg -y RG_system=FALSE

/usr/cluster/bin/scswitch -n -j otp-spsms-rs
```

3 **Backup the provisioning service database**

Type the following command:

```
su - spsotp \
/var/otp/spsotp/N1_Service_Provisioning_System_5.2/server/bin/cr_backup.sh \
-b /var/otp/spsotp/N1_Service_Provisioning_System_5.2 \
-o /var/tmp -nors -noconfig -nokeystore  -z -shutdown yes
```

The compressed backup tar file is created as `/var/tmp/`*timestamp*`.tar.Z` where *timestamp* is the system date and time stamp. For example, `/var/tmp/`*070411145059*`.tar.Z`

4 **Enable the Provisioning service resource in the resource group.**

Type the following commands:

```
/usr/cluster/bin/scswitch -e -j otp-spsms-rs

/usr/cluster/bin/scrgadm -c -g otp-system-rg -y RG_system=TRUE
```

Next Steps Restore the provisioning service to the external OTP installation server as described in the next procedure.

To Restore the Provisioning Service Backup To The External OTP Installation Server

Before You Begin

- The remote agent must be removed from the backup source OTP host as described in "To Remove the Remote Agent from the Backup Source OTP Host" on page 185
- The remote agent must be removed from the external OTP installation server as described in "To Remove the Remote Agent from the External OTP installation server" on page 186
- The backup source OTP host provisioning service must be backed up as described in "To Back Up the Provisioning Service on the Source OTP Host" on page 187.

1 **Log in as root to the external OTP installation server.**

2 **Restore the provisioning service database.**

Type the following command

```
su - spsotp \
/var/otp/spsotp/N1_Service_Provisioning_System_5.2/server/bin/cr_restore.sh \
-b /var/otp/spsotp/N1_Service_Provisioning_System_5.2 \
-f /var/tmp/backup tar file name \
-l /var/tmp/log file name \
-t /var/tmp -shutdown yes -nors -noconfig -nokeystore -overwrite yes
```

Where *backup tar file name* is the name of the backup file you created in "To Back Up the Provisioning Service on the Source OTP Host" on page 187, and *log file name* is the name you specify for the log file.

Next Steps Add the remote agent to the backup source OTP host as described in the next procedure.

To Add the Remote Agent To The Backup Source OTP Host

Before You Begin

- The remote agent must be removed from the backup source OTP host as described in "To Remove the Remote Agent from the Backup Source OTP Host" on page 185
- The remote agent must be removed from the external OTP installation server as described in "To Remove the Remote Agent from the External OTP installation server" on page 186
- The backup source OTP host provisioning service must be backed up as described in "To Back Up the Provisioning Service on the Source OTP Host" on page 187.
- The provisioning service backup must be restored to the external OTP installation server as described in "To Restore the Provisioning Service Backup To The External OTP Installation Server" on page 188

1 **Open a Web browser and go to URL http://***backup source OTP host***:9090 where** *backup source OTP host* **is either the IP address or the fully qualified name of the OTP host you identified in "To Remove the Remote Agent from the Backup Source OTP Host" on page 185.**

The OTP provisioning service log in screen appears.

2. **Log in to the OTP provisioning service.**
   The Service Provisioning System screen appears.
3. **Click Host Setup in the left panel.**
   The host setup screen appears.
4. **Click hosts in the central panel.**
   The hosts screen appears.
5. **Click master server.**
   The hosts > details screen appears.
6. **Scroll to the bottom of the screen and click edit.**
   The hosts > details > edit screen appears.
7. **If the checkbox labeled `include remote agent on this physical host` does not have a check mark in it, click the check box to add the check mark.**
8. **In connection type, choose TCP/IP (unencrypted).**
9. **Type the backup source OTP host IP address in the ip address or name field.**
10. **Type 7010 in the port field.**
11. **Scroll to the bottom of the screen and click save.**
12. **Click master server.**
13. **Click update remote agent.**
14. **Click prepare remote agent.**

Next Steps Add the remote agent to the restore external OTP installation server as described in the next procedure.

▼ To Add the Remote Agent To External OTP Installation Server

Before You Begin

- The remote agent must be removed from the backup source OTP host as described in "To Remove the Remote Agent from the Backup Source OTP Host" on page 185
- The remote agent must be removed from the external OTP installation server as described in "To Remove the Remote Agent from the External OTP installation server" on page 186

- The backup source OTP host provisioning service must be backed up as described in "To Back Up the Provisioning Service on the Source OTP Host" on page 187.
- The provisioning service backup must be restored to the external OTP installation server as described in "To Restore the Provisioning Service Backup To The External OTP Installation Server" on page 188
- The remote agent must be added to the backup source OTP host as described in "To Add the Remote Agent To The Backup Source OTP Host" on page 188

1. **Open a Web browser and go to URL http://*external OTP installation server*:9090 where *external OTP installation server* is either the IP address or the fully qualified name of the external OTP installation server.**

   The OTP provisioning service log in screen appears.

2. **Log in to the OTP provisioning service.**

   The Service Provisioning System screen appears.

3. **Click Host Setup in the left panel.**

   The host setup screen appears.

4. **Click hosts in the central panel.**

   The hosts screen appears.

5. **Click master server.**

   The hosts > details screen appears.

6. **Scroll to the bottom of the screen and click edit.**

   The hosts > details > edit screen appears.

7. **If the checkbox labeled `include remote agent on this physical host` does not have a check mark in it, click the check box to add the check mark.**

8. **In connection type, choose TCP/IP (unencrypted).**

9. **Type the external OTP installation server IP address in the ip address or name field.**

10. **Type 7010 in the port field.**

11. **Scroll to the bottom of the screen and click save.**

12. **Click master server.**

13. **Click update remote agent.**

14 **Click prepare remote agent.**

Backing Up and Restoring the OTP System Management Service

This section provides the procedure for backing up and restoring the system management database and configuration files. Backup of the system management database and configuration files should be performed on a regular basis.

If the OTP host on which the OTP system management service is installed fails, you can restore the management services to any other standalone OTP host or clustered OTP host as described in this section.

Note – Because the backup process does not back up the Solaris 10 Update 2 OS image and OS profile to conserve space in the backup file, you must either recreate the OS image and OS profile on the new OTP host, or manually backup and restore the OS image and OS profiles as described in the"Backing Up and Restoring OS Images and OS Profiles" on page 198

The following topics are discussed:

Backing Up The OTP System Management Service Database and Configuration Files

This section provides the procedure for backing up the system management database and configuration files.

▼ To Back Up the OTP System Management Service Database and Configuration Files

This procedure describes how to back up the system management database and configuration files. The system management is restarted several times during this process. Therefore, perform these steps only when the system management service is not currently running jobs.

Do not change the configuration or OS usage of the standalone OTP host or of the clustered OTP hosts during the period between executing the backup and restore procedures.

Before You Begin Choose a server that is external to the standalone OTP host or the clustered OTP hosts on which to save the backup files.

1 **Log in as root (`su - root`) to the OTP host on which the system management service is installed.**

2 **Type `/opt/sun/n1gc/bin/n1smbackup.sh` to start the backup process.**

For example:

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

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

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

Verify that N1SM does not have outstanding jobs before proceeding.

The backup process will take about 8 minutes.

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

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

The backup file is `/var/tmp/n1smbackup/n1smbackup.tgz`.

3 **Copy the file `/var/tmp/n1smbackup/n1smbackup.tgz` a server external to the OTP system.**

Restoring the OTP System Management Service Database and Configuration Files to Another OTP Host

This section provides the procedures for restoring and enabling the system management service on another OTP host. Restoring and enabling the system management service on another OTP host is comprised of the following two tasks:

- Configuring the OTP system management service to run on the OTP host as described in "To Configure the OTP System Management Service on Another OTP Host" on page 193.

To ensure that the system management service runs correctly on the OTP host, you must configure the system management to use the provisioning and management network interfaces of the OTP host.

- Restoring the OTP system management service database and configuration files to the OTP host as described in "To Restore the OTP System Management Service to Another OTP Host" on page 196.

  The restoration process restores the system management database and configuration files, which contain information about the clustered OTP hosts, DNS servers, SMTP settings, logging options, and more.

▼ To Configure the OTP System Management Service on Another OTP Host

This procedure describes how to configure the OTP system management service on another OTP host within the clustered OTP system.

Before You Begin

- A backup of the OTP System Management Service database and configuration files must exist on a server external to the clustered OTP system. See "To Back Up the OTP System Management Service Database and Configuration Files" on page 191 for further information.

1 Log in as root to the OTP host you have chosen for OTP system management service database and configuration file restoration.

2 Type `n1smconfig` to configure the system management service.

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

The current system configuration appears, and lists the network interfaces. You are then asked to specify the DHCP server.

For example:

```
# /usr/bin/n1smconfig

- - - - - - CURRENT CONFIGURATION - - - - - - -

   Provisioning Interface = ce0 : 10.11.52.79
   DHCP IP range: none
   Management Interface = ce0 : 10.11.52.79

  Logging values:
      job.plan-timeout = 1440
      job.step-timeout = 120
      filter.topic = all
      filter.severity = 0
      Days before deleting log entries = 365
```

```
    DNS settings = none.

   Web console auto login enabled = no
   Serial console with SSHv1 enabled = no

Current SSH policy:
accept CHANGED host keys for Management IP address = yes
accept CHANGED host keys for Platform IP address = yes
accept UNKNOWN host keys for Management IP address = yes
accept UNKNOWN host keys for Platform IP address = yes

ALOM email server = internal server

DHCP server = Solaris

Discover servers by the OS IP addresses = no

CURRENT RIS Servers:


- - - - - - - - - - - - - - - - - - - - - - - - -
This program configures the N1SM Management Server.
Only options that can be changed will be displayed.
Would you like to continue? ([n]/y) y
```

3 Choose the Solaris DHCP server.

Type **s** to choose the Solaris DHCP server. The Open Telecommunications Platform does not support ISC DHCP.

A description of the tasks you can perform at this point appears. You are then asked whether you want to modify the interface that is to be used by the provisioning network.

4 Type y to specify the provisioning network interface.

Note – Even if the provisioning interface shown matches the current provisioning interface, type **y** to rebind the provisioning interface IP addresst of the new system management host.

The available interfaces are listed. You are asked to specify the provisioning network interface port.

5 Type the interface name that is to be used for the provisioning interface.

Type the interface name that is to be used for the provisioning interface, for example `ce0`, `eth0`, `hme0`, `bge0` and so on depending on the host architecture and installed OS.

You are asked if you want the DHCP server to use a specific IP address range.

6 **Type n to disable DHCP IP address range use.**

You are asked if you want to modify the interface that is to be used by the management network.

7 **Type y to specify for the management network interface.**

Note – Even if the provisioning interface shown matches the current provisioning interface, type **y** to rebind the management interface IP addresst of the new system management host.

A description of the management network appears, followed by a list of the network interfaces that have been detected. You are then prompted to specify the interface that is to be used by the management network.

8 **Type the interface name that is to be used for the management interface.**

Type the interface name that is to be used for the management interface, for example `ce0`, `eth0`, `hme0`, `bge0` and so on depending on the host architecture and installed OS.

You are asked whether you want to configure the DNS name servers and search list entry.

9 **Type n.**

The OTP system management restore process will restore the OTP DNS and search list configuration data.

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

10 **Type n.**

The restore process will restore the SMTP configuration data.

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

11 **Type n.**

The restore process will restore the logging configuration data.

You are asked whether you want to enable auto-login for the ILOM Web GUI.

12 **Type n.**

The restore process will restore the auto—login configuration data.

You are asked whether you want to enable SSHv1 protocol.

13 **Type n.**

The restore process will restore the SSHv1 configuration data.

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

14 Type n.

The restore process will restore the SSH configuration data.

The current status of the ALOM email server is displayed. You are asked whether you want to modify the ALOM email server.

15 Type n.

The restore process will restore the ALOM email configuration data.

You are asked whether you want to add, delete, or modify the Windows™ RIS server.

16 Type n.

This release of the Open Telecommunications Platform does not support Windows.

A description of OS Discovery appears. You are asked whether you want to enable OS discovery.

17 Type n.

The Open Telecommunications Platform requires IP address-based discovery.

You are asked whether you want to modify the default password on the execution server.

18 Type n.

The restore process will restore the execution server password.

The configuration process then displays the settings you have specified, and asks whether you want to apply the settings.

19 Review the proposed settings.

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

  The settings are applied, and the OTP system management service is restarted.
- Type **n** if the settings are not correct.

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

Next Steps Restore the system management database and files to the OTP host as described in the next procedure.

▼ To Restore the OTP System Management Service to Another OTP Host

This procedure describes how to restore the OTP system management service on another OTP host within the clustered OTP system.

Before You Begin

- A backup of the OTP System Management Service database and configuration files must exist on a server external to the clustered OTP system. See "To Back Up the OTP System Management Service Database and Configuration Files" on page 191 for further information.
- The OTP system management service on the target OTP host must be configured as described in "To Configure the OTP System Management Service on Another OTP Host" on page 193.

1. **Log in as root on the target OTP host.**

2. **Type** `mkdir -p /var/tmp/n1smbackup`**.**

3. **Copy the** `n1smbackup.tgz` **backup file you created in "To Back Up the OTP System Management Service Database and Configuration Files" on page 191 to the** `/var/tmp/n1smbackup` **directory.**

4. **Type** `/opt/sun/n1gc/bin/n1smrestore.sh -f /var/tmp/n1smbackup/n1smbackup.tgz` **to restore the system management database and files.**

   For example:

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

This program will restore Sun N1SM from backup files.

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

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

The restore process will take about 8 minutes.

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

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

5. **Type** `n1smconfig` **to reconfigure the system management services.**

   The current configuration is displayed, and you are asked whether you want to continue.

   Type **y** to continue. Reconfigure the system management as described in "To Configure the OTP System Management Service on Another OTP Host" on page 193.

6 Verify that the OTP System Management Service is working properly.

a. Open a web browser and log in to the system management service on the OTP host.

Go to URL https://*OTP host*:6789 where *OTP host* is either the IP address or the fully qualified name of the OTP host.

The Java Web console log in page is appears. Type your system management user name and password to log in.

The system management page appears.

b. Type `/opt/sun/n1gc/bin/n1sh` to open the OTP command shell. For example:

```
# /opt/sun/n1gc/bin/n1sh
N1-ok>
```

Successful display of the system management web page and of the `N1–ok>` prompt signifies successful configuration and restoration of the system management service to the OTP host.

If the system management Web page or the `N1–ok>` prompt fail to appear, log in as root to the OTP host and type the command `svcadm disable n1sm`. Wait for the services to stop, and then type the command `svcadm enable n1sm`. Wait for the services to complete startup, and then retry verification.

7 (Optional) Remove any OS distributions or OS profiles that exist on the OTP host 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.
```

Backing Up and Restoring OS Images and OS Profiles

This section provides the procedure for backing up and restoring OS images and profiles.

▼ To Backup and Restore OS Images and OS Profiles

1. **Using any file level backup and restore program, back up the following directories to a server that is not a member of the clustered OTP system.**
   - `/var/opt/sun/scs/share/allstart`
   - `/tftpboot`
2. **Restore the directories to the target OTP host.**

◆ ◆ ◆ CHAPTER 9

Open Telecommunications Platform Administration

This chapter provides the procedures for administering the Open Telecommunications Platform 1.1.

The following topics are discussed:

OTP Topologies

This section provides an overview of the N*N and Pair+N clustered OTP system topologies supported by OTP. A topology is the connection scheme that connects the clustered OTP hosts to the storage platforms used in the cluster.

N*N

The N*N topology allows every shared storage device in the cluster to connect to every OTP host in the cluster. This topology allows highly available applications to failover from one node to another without service degradation. When failover occurs, the new node can access the storage device using a local path instead of the private interconnect.

The following figure illustrates an N*N configuration where all four OTP hosts connect to shared storage.

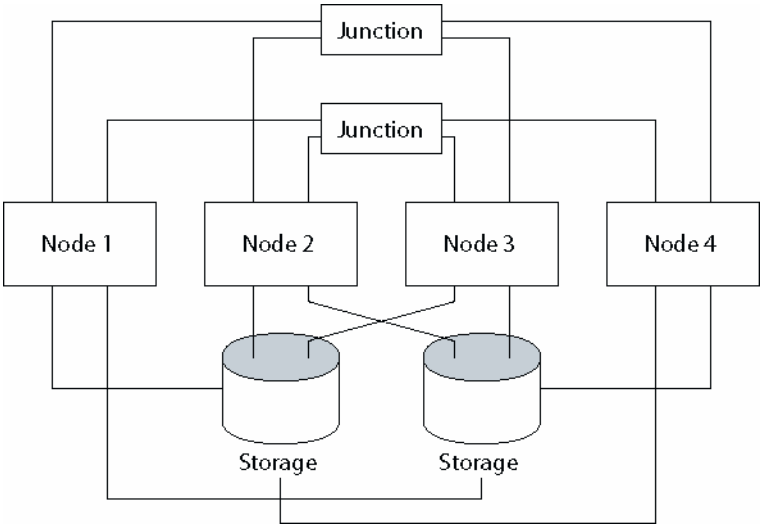

FIGURE 9–1 N*N Topology

The following procedures are supported in N*N topology.

- "Adding a Host to the Existing Cluster" on page 209
- "Repairing a Host in the Cluster" on page 211

Pair+N

The pair+N topology includes a pair of OTP hosts directly connected to shared storage and an additional set of OTP hosts that use the cluster interconnect to access shared storage. The additional OTP hosts have no direct connection to the shared storage.

The following figure illustrates a pair+N topology where two of the four OTP hosts (Node 3 and Node 4) use the cluster interconnect to access the storage. This configuration can be expanded to include additional OTP hosts that do not have direct access to the shared storage.

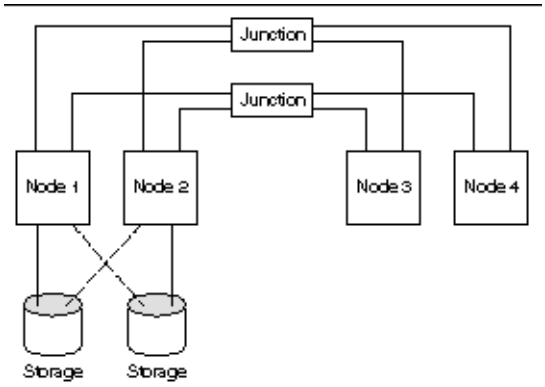

FIGURE 9–2 Pair+N Topology

The following procedures are supported in pair+N topology.

- "To Add an OTP Host That Is Not Connected to Shared Storage" on page 216
- "To Repair an OTP Host That Is Not Connected to Shared Storage" on page 217
- "To Repair an OTP Host That Is Connected to Shared Storage" on page 218

For further information about clustered OTP system topology, see *Sun Cluster Concepts Guide for Solaris OS*.

Enabling and Disabling the OTP System Management Service and Provisioning Service

This section provides the procedures for enabling and disabling the system management service and the provisioning service on a single OTP host.

▼ To Enable and Disable the OTP System Management Service Using the Command Line

The following steps enable and disable the OTP System Management Service only on the target host and not on the entire cluster.

1 **Log in as root (`su - root`) to the OTP host.**

2 **Use the `serviceManagement` script with the `n1sm` option to enable and disable the OTP System Management Service.**

- **To enable the service, use the `start` option.**

  `# /opt/SUNWotp10/CLI/serviceManagement n1sm start`

- **To disable the service, use the `stop` option.**

  `# /opt/SUNWotp10/CLI/serviceManagement n1sm stop`

▼ To Enable and Disable the OTP Application Provisioning Service Using the Command Line

Note –

- If the OTP application provisioning service is running in the high availability mode, the provisioning service is enabled or disabled on all hosts in the cluster.
- If the OTP Application Provisioning Service is not running in the High Availability mode, the OTP Application Provisioning Service is enabled or disabled only on the target host.

1 **Log in as root (`su - root`) to the OTP host.**

2 **Use the `serviceManagement` script with the `n1sps` option to enable and disable the OTP Application Provisioning Service.**

- **To enable the service, use the `start` option.**

  `# /opt/SUNWotp10/CLI/serviceManagement n1sps start`

- **To disable the service, use the `stop` option.**

  `# /opt/SUNWotp10/CLI/serviceManagement n1sps stop`

▼ To Enable and Disable the OTP System Management and Provisioning Services Using the Graphical User Interface

- The following steps enable and disable the OTP System Management Service only on the target host and not on the entire cluster.

- The graphical user interface cannot be used to disable the provisioning service on the host on which it is running. In other words, if the service is running on otpclient01, you cannot use the graphical user interface on otpclient01 to disable the provisioning service. Instead, use the command line interface to disable the provisioning service.

1 **Open a Web browser and go to URL https://*OTP host*:9090 where *OTP host* is either the IP address or the fully qualified name of the OTP host on which the resource group is active.**

The OTP provisioning service log in screen appears.

2 **Click OEM OTP.**

3 **Click Utility Plans.**

4 **Click OTP Service Management Control.**

5 **Click on OTP Service Management.**

The OTP Service Management Plan page appears:

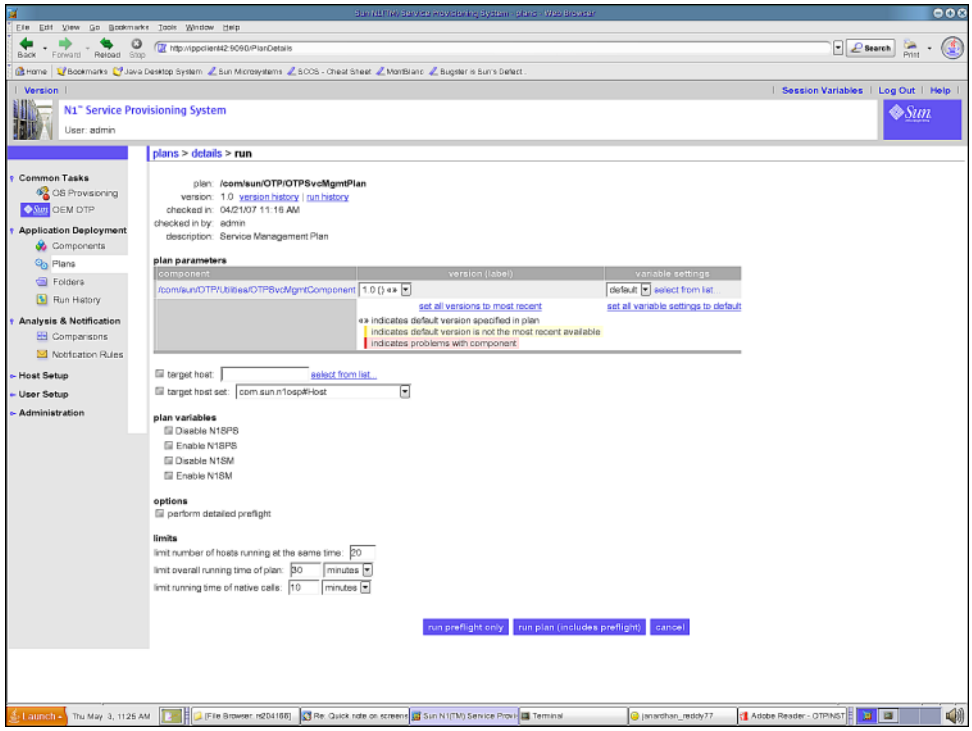

FIGURE 9–3 Service Management Plan Page

6. **Type the host name on which you want to enable or disable the services in the target host field. Do not modify the target host set.**
7. **Choose the services you want to enable and disable.**
8. **Click the perform detailed preflight checkbox.**
9. **Click run plan (includes preflight)**

Converting a Standalone OTP Host to a Clustered OTP Host

This section provides the procedure to convert a standalone OTP host to a clustered OTP host.

▼ To Convert a Standalone OTP Host to a Clustered OTP Host

1. **Log in as root (`su - root`) to the external OTP installation server.**
2. **Copy** `/opt/SUNWotp10/CLI/templates/inputOTPSingleNode.dat /var/tmp/inputOTPSingleNode.dat`**.**
3. **Edit the** `/var/tmp/inputOTPSingleNode.dat` **file.**

   Specify the values for each keyword as described by "Open Telecommunications Platform Plan Worksheets" on page 30 and the standalone OTP host Plan worksheet.
4. **Convert the standalone OTP host to aclustered OTP host.**

   - **Using the command line, type:**

     ```
     /opt/SUNWotp10/CLI/deployOTPSingleNode -convertToManager
     /var/tmp/inputOTPSingleNode.dat
     ```

   - **Using the graphical user interface:**

     a. **Open a Web browser and go to URL https://*OTP host*:9090 where *OTP host* is either the IP address or the fully qualified name of the OTP host on which the resource group is active.**

        The OTP provisioning service log in screen appears.

     b. **Click OEM OTP.**

     c. **Click Utility Plans.**

d. Click Convert Standalone system to Clustered System.

e. Click Configure.

The Convert Single to Clustered page appears:

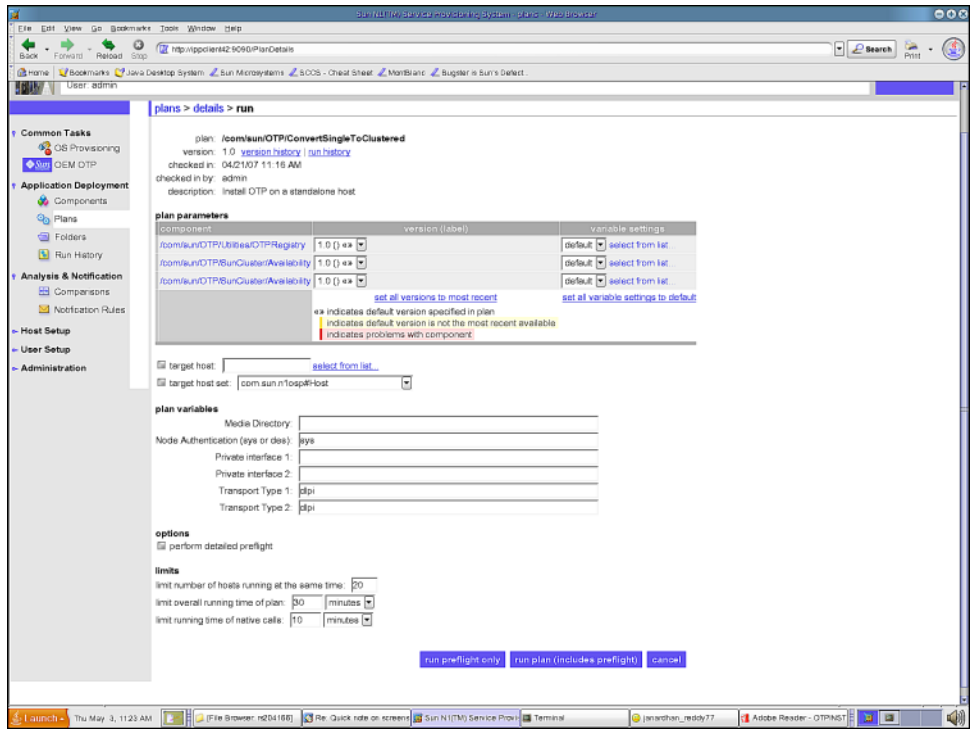

FIGURE 9–4 Convert Standalone OTP Host to Clustered OTP Host Page

f. Type the name of the standalone OTP host that you want to convert to a clustered OTP host in the target host field. Do not modify the target host set.

g. In the Media Directory field, type the fully-qualified name of the NFS-mounted OTP installation directory.

For example: `/net/otpsource.mycompany.com/otp1.1`

h. In the Private interface 1 field, type the name of the private interface.

For example, `ce0`.

i. In the Private interface 2 field, type the name of the private interface.

For example, `ce1`.

j. **Click the perform detailed preflight checkbox.**

k. **Click run plan (includes preflight)**

5 **Create the system shared storage as described in "To Create Shared Storage on the Clustered OTP System" on page 108.**

6 **Create a temporary mount point.**

```
mkdir -p /var/tmp_otp
```

7 **Mount the shared volume onto the temporary mount point.**

```
mount /dev/md/sps-dg/dsk/d0 /var/tmp_otp
```

8 **Bring the resource group offline.**

```
scrgadm -c -g otp-system-rg -y RG_system=false
scswitch -F -g otp-system-rg
```

9 **Move the OTP contents from the local disk to the shared volume.**

```
mv /var/otp/* /var/tmp_otp
umount /var/tmp_otp
```

10 **Disable the resources in the following order.**

```
scswitch -nj otp-spsms-rs
scswitch -nj otp-spsra-rs
scswitch -nj otp-sps-hastorage-plus
```

11 **Modify the `HAStoragePlus` resource properties.**

```
scrgadm -c -j otp-sps-hastorage-plus -x FilesystemMountPoints="/var/otp"
scrgadm -c -j otp-sps-hastorage-plus -x GlobalDevicePaths=/dev/md/sps-dg/dsk/d0
```

12 **Enable the resources in the following order.**

```
scswitch -ej otp-sps-hastorage-plus
scswitch -ej otp-spsra-rs
scswitch -ej otp-spsms-rs
```

13 **Bring the resource group online.**

```
scswitch -z -g otp-system-rg -h host name
```

14 **Set the `system` property for the `otp-system-rg` resource group to true.**

```
scrgadm -c -g otp-system-rg -y RG_system=true
```

N*N Topology Administration

This section provides the procedures for adding new OTP host to an N*N clustered OTP system, and for repairing an OTP host within an N*N clustered OTP system.

The following topics are discussed:

Adding a Host to the Existing Cluster

This section provides the procedure for adding a host to an existing clustered OTP system.

▼ To Add a Host to the Existing Cluster

Before You Begin Ensure that the sponsoring host (the first OTP host of the cluster) is added to the host list in the service provisioning service. See "To Add Hosts to the External OTP Installation Server" on page 115.

1 **Install the Solaris OS on the new OTP host as described in "Installing Solaris 10 Update 2 and the Remote Agent on the OTP Hosts" on page 50.**

2 **Configure the Solaris OS on the new OTP host as described in "Configuring Solaris 10 Update 2" on page 94**

3 **Create a mount point `/var/otp` on the new OTP host.**

```
# mkdir -p /var/otp
```

4 **Add the following entry to the `/etc/vfstab` file.**

```
/dev/md/sps-dg/dsk/d0 /dev/md/sps-dg/rdsk/d0 /var/otp ufs 2 no global,logging
```

5 **Provision OTP on the new OTP host using either the graphical user interface or the command line interface.**

a. **Perform the following steps to provision OTP using the graphical user interface.**

- Set up high availability as described in Set Up the OTP High Availability Framework on the Additional OTP Hosts

- Create the shared storage on the clustered OTP system as described in "To Create Shared Storage on the Clustered OTP System" on page 108.
- Set up the OTP services on the host as described in Set Up OTP System Management and Provisioning Services on the Additional OTP Hosts

b. Perform the following steps to provision OTP through the command line interface.

- Run the `deployOTPMultiNode` script with the `-addNode` option.

  Type the command

  `/opt/SUNWotp10/CLI/deployOTPMultiNode -addNode /`*local-path*`/inputOTPMultiNode.dat`

  where *local-path* is the path to the file `inputOTPMultiNode.dat`.
- Create `metadb` on the host and add the host to `metaset` as described in "To Create Shared Storage on the Clustered OTP System" on page 108.
- Run the `deployOTPMultiNode` script with the `-addNodeCont` option.

  Type the command

  `/opt/SUNWotp10/CLI/deployOTPMultiNode -addNodeCont /`*local-path*`/inputOTPMultiNode.dat`

  where *local-path* is the path to the file `inputOTPMultiNode.dat`.

Note – Quorum automatic configuration applies only to two-host clustered OTP systems. If you disable quorum automatic configuration on a two-host cluster by choosing `no`, you must manually configure the quorum for the two-host cluster and reset the cluster configuration as described in "Installing the Open Telecommunications Platform on a Clustered OTP System" on page 127.

For further information, see "Quorum and Quorum Devices" in *Sun Cluster Concepts Guide for Solaris OS* to understand the requirements for Quorum. Reconfigure the quorum as described in "Administering Quorum" in *Sun Cluster System Administration Guide for Solaris OS*.

You can use the `scsetup(1M)` utility to add a node to the node list of an existing quorum device. To modify a quorum device's node list, you must remove the quorum device, modify the physical connections of nodes to the quorum device you removed, then add the quorum device to the cluster configuration again. When a quorum device is added, `scconf(1M)` automatically configures the node-to-disk paths for all nodes attached to the disk.

---

6 Set the `system` property for the `otp-system-rg` resource group to false.

Type the command `scrgadm -c -g otp-system-rg -h RG_system=false`

7 **Determine the current IPMP groups.**

Type `scrgadm -pvv | grep otp-lhn:NetIfList | grep value` to list the current IPMP groups. For example:

```
# scrgadm -pvv | grep otp-lhn:NetIfList | grep value
    (otp-system-rg:otp-lhn:NetIfList) Res property value: sc_ipmp0@1
```

8 **Determine the node ID value as follows:**

```
# scconf -pvv | grep pcl3-ipp2 | grep ID
(pcl3-ipp2) Node ID: 2
```

The IPMP group for the new node in this example would be `sc_ipmp0@2`

9 **Add the IPMP group for the newly added host to the Logical Host Name resource.**

Type the command

`scrgadm -c -j otp-lhn -x NetIfList=`*list of IPMP groups*

where *list of IPMP groups* is the current list of IPMP groups. For example:

```
# scrgadm -c -j otp-lhn -x NetIfList=sc_ipmp0@1,sc_ipmp0@2
```

10 **Determine the current node list.**

Type the command `scrgadm -pvv | grep otp-system-rg | grep Nodelist`. For example:

```
# scrgadm -pvv | grep otp-system-rg | grep Nodelist
(otp-system-rg) Res Group Nodelist: pc13-ipp1
```

11 **Add the host to the resource group.**

`# scrgadm -c -g` *resource-group* `-y` *nodelist*

For example, add the host to the `otp-system-rg` resource group.

```
# scrgadm -c -g otp-system-rg -y nodelist=pcl3-ipp1,pcl3-ipp2
```

12 **Set the `system` property for the `otp-system-rg` resource group to true.**

```
scrgadm -c -g otp-system-rg -y RG_system=true
```

Repairing a Host in the Cluster

This section provides the procedure for repairing a failed host in a clustered OTP system. If a host fails in a multi-host cluster setup, the host has to be repaired. The host repair process involves the following two steps:

- Remove the failed host from the cluster.
- Add a host to the cluster as described in "Adding a Host to the Existing Cluster" on page 209.

To Remove a Failed Host From the Cluster

In this procedure, the host `pcl17-ipp2` is removed from a two-host cluster configuration. The hosts are `pcl17-ipp1` and `pcl17-ipp2`. Substitute your own cluster and host information.

Note – If the host that is being removed is the first host in the cluster, back up the system management database as described in "Backing Up The OTP System Management Service Database and Configuration Files" on page 191 so that the database can be restored to one of the remaining cluster hosts as described in "Restoring the OTP System Management Service Database and Configuration Files to Another OTP Host" on page 192.

---

1. **Log in as root (`su - root`) to the active host in the cluster.**

   If the cluster has more than two hosts:

   a. **Log in as root to an OTP host in the cluster.**

   b. **Type `/usr/cluster/bin/scstat -g | grep Online` to determine which host in the cluster is active.**

      Make note of the host on which the resource group `otp-system-rg` is online.

      For example:

```
# /usr/cluster/bin/scstat -g | grep Online
    Group: otp-system-rg          pcl17-ipp2   Online
 Resource: otp-lhn                pcl17-ipp2   Online  Online - LogicalHostname online.
 Resource: otp-sps-hastorage-plus pcl17-ipp2   Online  Online
 Resource: otp-spsms-rs           pcl17-ipp2   Online  Online
 Resource: otp-spsra-rs           pcl17-ipp2   Online  Online
```

      In the above example, the active host is `pcl17-ipp2`.

   c. **Log in as root on the OTP host on which the resource group is active.**

2. **Add the cluster binaries path to your $PATH.**

   # **`PATH=$PATH:/usr/cluster/bin`**

3. **Move all the resource groups and disk device groups to `pcl17-ipp1`.**

   # **`scswitch -z -g otp-system-rg -h pcl17-ipp1`**

4. **Remove the host from all resource groups.**

   # **`scrgadm -c -g otp-system-rg -y RG_system=false`**

   # **`scrgadm -c -g otp-system-rg -y Nodelist=pcl17-ipp1`**

Note – `Nodelist` must contain all the node names except the node to be removed.

5 If the node was set up as a mediator host, remove it from the set.

```
# metaset -s sps-dg -d -m pcl17-ipp2
```

6 Remove the node from `metaset`.

```
# metaset -s sps-dg -d -h -f pcl17-ipp2
```

7 Remove all the disks connected to the node except the quorum disk.

a. Check the disks connected to the node by typing the following command:

```
scconf -pvv |grep pcl17-ipp2|grep Dev
```

```
# scconf -pvv |grep pcl17-ipp2|grep Dev
(dsk/d12) Device group node list:                pcl17-ipp2
(dsk/d11) Device group node list:                pcl17-ipp2
(dsk/d10) Device group node list:                pcl17-ipp2
(dsk/d9) Device group node list:                 pcl17-ipp2
(dsk/d8) Device group node list:                 pcl17-ipp2
(dsk/d7) Device group node list:                 pcl17-ipp1, pcl17-ipp2
(dsk/d6) Device group node list:                 pcl17-ipp1, pcl17-ipp2
(dsk/d5) Device group node list:                 pcl17-ipp1, pcl17-ipp2
(dsk/d1) Device group node list:                 pcl17-ipp1, pcl17-ipp2
```

b. Remove the local disks.

```
# scconf -c -D name=dsk/d8,localonly=false
# scconf -c -D name=dsk/d9,localonly=false
# scconf -c -D name=dsk/d10,localonly=false
# scconf -c -D name=dsk/d11,localonly=false
# scconf -c -D name=dsk/d12,localonly=false
# scconf -r -D name=dsk/d8
# scconf -r -D name=dsk/d9
# scconf -r -D name=dsk/d10
# scconf -r -D name=dsk/d11
# scconf -r -D name=dsk/d12
```

c. Determine which disk is the quorum disk.

To determine which disk is the quorum disk, type the command `scstat -q | grep "Device votes"`. For example:

```
# scstat -q | grep "Device votes"
Device votes: /dev/did/rdsk/d1s2 1 1 Online
```

In this example, the quorum disk is dsk/d1

d. Remove the shared disks except for the quorum disk.

```
# scconf -r -D name=dsk/d5,nodelist=pcl17-ipp2
# scconf -r -D name=dsk/d6,nodelist=pcl17-ipp2
# scconf -r -D name=dsk/d7,nodelist=pcl17-ipp2
```

e. Check that only the quorum disk is in the list.

```
# scconf -pvv |grep pcl17-ipp2|grep Dev
(dsk/d1) Device group node list:                pcl17-ipp1, pcl17-ipp2
```

8 Shut down the failed node.

```
shutdown -y -g 0 -i 0
```

9 Place the failed node in maintenance state.

```
# scconf -c -q node=pcl17-ipp2,maintstate
```

10 Remove the private interconnect interfaces.

a. Check the private interconnect interfaces using the following command:

```
# scconf -pvv | grep pcl17-ipp2 | grep Transport
Transport cable:   pcl17-ipp2:ce0@0   switch1@2          Enabled
Transport cable:   pcl17-ipp2:ce2@0   switch2@2          Enabled
```

b. Disable and remove the private interconnect interfaces.

```
# scconf -c -m endpoint=pcl17-ipp2:ce0,state=disabled
# scconf -c -m endpoint=pcl17-ipp2:ce2,state=disabled
# scconf -r -m endpoint=pcl17-ipp2:ce0
# scconf -r -m endpoint=pcl17-ipp2:ce2
```

c. Remove the private interfaces of the failed node.

```
# scconf -r -A name=ce0,node=pcl17-ipp2
# scconf -r -A name=ce2,node=pcl17-ipp2
```

11 Remove the quorum disk from the failed node.

- **For a two-node cluster, type the following commands:**

  # **scconf -r -D name=dsk/d1,nodelist=pcl17-ipp2**

  # **scconf -c -q installmode**

  # **scconf -r -q globaldev=d1**

  # **scconf -c -q installmodeoff**

- **For a three-host or more cluster, type the following commands:**

  # **scconf -r -D name=dsk/d1,nodelist=pcl17-ipp2**

  # **scconf -r -q globaldev=d1**

12 Add the quorum devices only to the nodes that will remain in the cluster.

scconf -a -q globaldev=d[*n***],node=***node1***,node=***node2*

Where *n* is the disk DID number.

13 Remove the failed node from the node authentication list.

scconf -r -T node=pcl17-ipp2

14 Remove the failed node from the cluster node list.

scconf -r -h node=pcl17-ipp2

Perform this step from installmode (`scconf -c -q installmode`). Otherwise, you will get a warning about possible quorum compromise.

15 Use the following commands to verify whether the failed node is still in the cluster configuration.

scconf -pvv |grep pcl17-ipp2

scrgadm -pvv|grep pcl17-ipp2

If the failed node was successfully removed, both of the above commands return to the system prompt.

- If the `scconf` command failed, command out will be similar to the following:

```
# scconf -pvv | grep pcl17-ipp2
Cluster nodes: pcl17-ipp1 pcl17-ipp2
Cluster node name: pcl17-ipp2
(ipp-node70) Node ID: 1
(ipp-node70) Node enabled: yes
(ipp-node70) Node private hostname: clusternode1-priv
(ipp-node70) Node quorum vote count: 0
```

```
(ipp-node70) Node reservation key: 0x462DC27400000001
(ipp-node70) Node transport adapters:
```

If the `scrgadm` command output is similar to the following, then Step 4 was not executed.

```
# scrgadm -pvv|grep pcl17-ipp2
(otp-system-rg) Res Group Nodelist: pc117-ipp1 pc117-ipp2
```

16 **Change the `RG_system` property to true.**

Type **`scrgadm -c -g otp-system-rg -y RG_system=true`**

Next Steps Add the host to the cluster as described in "Adding a Host to the Existing Cluster" on page 209.

Pair+N Topology Administration

This section provides the procedures for adding a new OTP host to a Pair+N clustered OTP system, and for repairing an OTP host within a Pair+N clustered OTP system.

The following topics are discussed:

▼ To Add an OTP Host That Is Not Connected to Shared Storage

1 **Reinstall the Solaris 10 Update 2 operating system on the OTP host as described in "Installing Solaris 10 Update 2 and the Remote Agent on the OTP Hosts" on page 50.**

2 **Add the OTP host back into the cluster configuration as described in "To Add a Host to the Existing Cluster" on page 209**

Note – As the OTP host will not be part of the resource group, steps to add the OTP host to the resource group need not be performed.

---

3 **Install OTP on the OTP host.**

- To install OTP on the OTP hosts using the command line, see Chapter 4, "Installing the Open Telecommunications Platform For the First Time Using the Command Line"

- To install OTP on the OTP hosts using the graphical user interface, see Chapter 5, "Installing the Open Telecommunications Platform For the First Time Using the Graphical User Interface"
- To install OTP on the OTP hosts using a production standalone or clustered OTP system, see Chapter 6, "Installing the Open Telecommunications Platform Using the Provisioning Service On an Existing OTP System"

▼ To Repair an OTP Host That Is Not Connected to Shared Storage

In this procedure, `pcl8-ipp2` is the OTP host that is being repaired. Substitute your own host information.

1 Check the disks connected to the OTP host that needs to be repaired.

```
# scconf -pvv | grep pcl8-ipp2 | grep Dev
(dsk/d10) Device group node list:                pcl8-ipp2
(dsk/d9) Device group node list:                 pcl8-ipp2
```

2 Remove the disks connected to the OTP host.

```
# scconf -c -D name=dsk/d10,localonly=false
# scconf -c -D name=dsk/d9,localonly=false
# scconf -r -D name=dsk/d10
# scconf -r -D name=dsk/d9
```

3 Place the OTP host to be repaired in maintenance state.

```
# scconf -c -q node=pcl8-ipp2,maintstate
```

4 Remove the transport information of the OTP host from cluster configuration.

a. Check the transport information.

```
# scconf -pvv | grep pcl8-ipp2 | grep Transport
Transport cable:   pcl8-ipp2:bge1@0    switch1@3          Enabled
Transport cable:   pcl8-ipp2:ce1@0     switch2@3          Enabled
```

b. Remove the related transport.

```
# scconf -c -m endpoint=pcl8-ipp2:bge1,state=disabled
# scconf -c -m endpoint=pcl8-ipp2:ce1,state=disabled
# scconf -r -m endpoint=pcl8-ipp2:bge1
# scconf -r -m endpoint=pcl8-ipp2:ce1
```

```
# scconf -r -A name=bge1,node=pcl8-ipp2
# scconf -r -A name=ce1,node=pcl8-ipp2
```

5 **Remove the OTP host from authentication list.**

```
# scconf -r -T node=pcl8-ipp2
```

6 **Remove the OTP host from the host list.**

```
# scconf -r -h node=pcl8-ipp2
```

7 **Make sure that the OTP host is completely removed from the cluster configuration.**

If you see any output for the following command, revisit the above steps to make sure all the steps are executed properly.

```
# scconf -pvv | grep pcl8-ipp2
```

8 **Add the OTP host back into the cluster configuration as described in "To Add an OTP Host That Is Not Connected to Shared Storage" on page 216 for more information.**

Note – As the OTP host will not be part of the resource group, steps to add the OTP host to the resource group need not be performed.

▼ To Repair an OTP Host That Is Connected to Shared Storage

In this procedure, `pcl8-ipp3` is the OTP host that is being repaired. Substitute your own host information.

1 **Move all the resource groups to another OTP host in the resource group list.**

```
# scswitch -z -g otp-system-rg -h otherotphost
```

2 **Remove the disks connected to the OTP host.**

a. **Check the disks connected to the OTP host.**

```
# scconf -pvv | grep pcl8-ipp3 | grep Dev
(dsk/d8) Device group node list:                pcl8-ipp3
(dsk/d7) Device group node list:                pcl8-ipp3
(dsk/d6) Device group node list:                pcl8-ipp1, pcl8-ipp3
(dsk/d5) Device group node list:                pcl8-ipp1, pcl8-ipp3
(dsk/d4) Device group node list:                pcl8-ipp1, pcl8-ipp3
(dsk/d3) Device group node list:                pcl8-ipp1, pcl8-ipp3
```

b. Remove the local disks.

```
# scconf -c -D name=dsk/d8,localonly=false
# scconf -c -D name=dsk/d7,localonly=false
# scconf -r -D name=dsk/d8
# scconf -r -D name=dsk/d7
```

c. Remove the shared disks.

```
# scconf -r -D name=dsk/d5,nodelist=pcl8-ipp3
# scconf -r -D name=dsk/d6,nodelist=pcl8-ipp3
# scconf -r -D name=dsk/d4,nodelist=pcl8-ipp3
```

3 Shut down the OTP host.

```
# shutdown -y -g 0 -i 0
```

4 Place the OTP host in maintenance mode.

```
# scconf -c -q node=pcl8-ipp3,maintstate
```

5 Remove the transport information.

a. Check the transport information.

```
# scconf -pvv | grep pcl8-ipp3 | grep Transport
Transport cable:   pcl8-ipp3:bge1@0    switch1@2          Enabled
Transport cable:   pcl8-ipp3:ce1@0     switch2@2          Enabled
```

b. Remove the transport information.

```
# scconf -c -m endpoint=pcl8-ipp3:bge1,state=disabled
# scconf -c -m endpoint=pcl8-ipp3:ce1,state=disabled
# scconf -r -m endpoint=pcl8-ipp3:bge1
# scconf -r -m endpoint=pcl8-ipp3:ce1
# scconf -r -A name=bge1,node=pcl8-ipp3
# scconf -r -A name=ce1,node=pcl8-ipp3
```

6 Remove the quorum disk.

```
# scconf -r -D name=dsk/d3,nodelist=pcl8-ipp3
# scconf -r -q globaldev=d3
```

Note – If you perform this procedure on a three-host cluster, you will need to establish quorum before running the above procedure. Otherwise, you will get the following error:

```
# scconf -r -h node=pcl8-ipp3

scconf:  Failed to remove node (pcl8-ipp3) - quorum could be compromised.
scconf:    All two-node clusters must have at least one shared quorum device.
```

7 **Remove the host from the authentication list.**

```
# scconf -r -T node=pcl8-ipp3
```

8 **Remove the host from the host list.**

```
# scconf -r -h node=pcl8-ipp3
```

9 **Make sure that the OTP host is completely removed from the cluster configuration.**

If you see any output for the following command, revisit the above steps to make sure all the steps are executed properly.

```
# scconf -pvv | grep pcl8-ipp3
```

10 **Add the OTP host back into the cluster configuration as described in "To Add a Host to the Existing Cluster" on page 209 for more information.**

Changes to OTP High Availability Framework for Enterprise Installation Services Compliance

The main objective of the EIS installation standards is to produce a consistent, high-quality installation in an efficient way.

To make the OTP High Availability framework EIS compliant, the following steps must be performed. All these steps are not mandatory but they are recommended. The first five steps can be performed before setting up OTP. The last step can be performed after the OTP installation.

- `scsi-initiator-id` must be defined in the Open Boot Prom (OBP).
- Add all the cluster nodes and the logical hosts to the `/etc/inet/hosts` and `/etc/inet/ipnodes` files.
- Do not configure cluster nodes as routers. Create the `/etc/defaultrouter` file manually before installing the OTP high availability framework.
- If you use shared SCSI storage, add the following entries to the `/etc/system` file.

  ```
  set sd:sd_io_time=30

  set sd:sd_retry_count=3
  ```

```
set scsi_reset_delay=500
```

- If you use the `glm` driver, add the following entry to the `/kernel/drv/glm.conf` file.

  ```
  scsi-selection-timeout=64
  ```

- If you do not install the `SUNWescom` package, disable the `scsymon` service.

  ```
  # svcadm -v disable /system/cluster/scsymon-srv
  ```

◆ ◆ ◆ APPENDIX A

Application Programming Interfaces and Protocols

This appendix lists the application programming interfaces (APIs) and protocols you can use for application development. The Open Telecommunications Platform release supports both industry standard interfaces, such as POSIX, CORBA, and SNMP, as well as Sun proprietary interfaces such as PAM (Pluggable Authentication Modules), RMAPI (Resource Management API) and others that are not yet part of any standards body.

OTP Application Programming Interfaces

The following table lists the APIs included in the Open Telecommunications Platform release.

Interfaces are categorized according to the following definitions:

- **Standard.** These interfaces are defined by various standards bodies and their implementation is provided by one or more of the OTP components. These interfaces are guaranteed to be supported for the life of the OTP product or the life of the standards, whichever ends first.
- **Committed.** These interfaces are provided by OTP components, but do not have a standard definition by a standards body. These interfaces are guaranteed to be supported for the life of the OTP product.

Use the links in the last column in the table that follows to find information about these APIs.

TABLE A–1 OTP 1.1 APIs

Interface	Component	Category	Documentation
POSIX.1 (IEEE Std 1003.1)	Solaris™ 10 OS	Standard	man pages:`POSIX.1`(5)

TABLE A–1 OTP 1.1 APIs *(Continued)*

Interface	Component	Category	Documentation
POSIX.2 (IEEE Std 1003.2)	Solaris 10 OS	Standard	man pages:`POSIX.2`(5) (http://docs.sun.com/doc/819–5175)
PAM (Pluggable Authentication Modules)	Solaris 10 OS	Committed	Chapter 3, "Writing PAM Applications and Services," in *Solaris Security for Developers Guide* (http://docs.sun.com/doc/816–4863) man pages:`libpam`(3LIB) (http://docs.sun.com/doc/816–5173)
RMAPI version 7	Sun Cluster 3.1 8/05	Committed	*Sun Cluster Data Services Developer's Guide for Solaris OS* (http://docs.sun.com/doc/819–0581)
DSDL (Data Service Development Library), API Version 7	Sun Cluster 3.1 8/05	Committed	*Sun Cluster Data Services Developer's Guide for Solaris OS* (http://docs.sun.com/doc/819–0581)
Java SE 1.4.2 Java interfaces	Java™ 2 SDK SE 1.4.2	Standard	`(http://java.sun.com/j2se/1.4.2/docs/)`
Java SE 5.0 Java interfaces	Java SE 5.0 platform	Standard	`(http://java.sun.com/j2se/1.5.0/docs/)`
CORBA	Java 2 SDK SE 1.4.2 and Java SE 5.0 platform	Standard	`(http://java.sun.com/j2se/1.5.0/docs/guide/idl/)`

OTP Protocols

The following table lists the protocols supported by OTP, and are categorized within the table according to the following definitions:

- **Standard.** These protocols are defined by various standards bodies and their implementation is provided by one or more of the OTP components. These protocols are guaranteed to be supported for the life of the OTP product or the life of the standards, whichever ends first.
- **Committed.** These protocols are provided by OTP components, but do not have a standard definition by a standards body. These protocols are guaranteed to be supported for the life of the OTP product.

TABLE A–2 OTP 1.1 Protocols

Interface	Component	Category	Documentation
TCP/IP	Solaris 10 OS	Standard	man pages: `tcp`(7P) `ip`(7P) (http://docs.sun.com/doc/816–5177)
SNMP (Net-snmp SNMP V3)	Solaris 10 OS	Standard (For support level, see the *Sun Open Telecommunications Platform 1.0 Release Notes*.)	*Solaris System Management Agent Developer's Guide* and its appendix: "API Functions" in *Solaris System Management Agent Developer's Guide* (http://docs.sun.com/doc/817–3155) man pages:`netsnmp`(5) `sma_snmp`(5) (http://docs.sun.com/doc/819–5175)
SSH/SSL	Solaris 10 OS	Standard	man pages:`ssh`(1) (http://docs.sun.com/doc/81816–5165) `openssl`(5) (http://docs.sun.com/doc/819–5175)
RMI	Java 2 SDK SE 1.4.2 and Java SE 5.0 platform	Standard	`(http://java.sun.com/j2se/1.4.2/docs/guide/rmi/)` `(http://java.sun.com/j2se/1.5.0/docs/guide/rmi/)`
IIOP (RMI-IIOP)	Java 2 SDK SE 1.4.2 and Java SE 5.0 platform	Standard	`(http://java.sun.com/j2se/1.4.2/docs/guide/rmi-iiop/)` `(http://java.sun.com/j2se/1.5.0/docs/guide/rmi-iiop/)`
DNS	Solaris 10 OS	Standard	*System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)* (http://docs.sun.com/doc/816–4556)
iSCSI	Solaris 10 OS	Standard, except for a cluster node with iSCSI storage attached is not supported.	*System Administration Guide: Devices and File Systems* (http://docs.sun.com/doc/817–5093)
FC (FCP) ANSI X3.269-1996	Solaris 10 OS	Standard	Solaris Fibre Channel Storage Configuration and Multipathing Administration Guide overview and appendix

TABLE A–2 OTP 1.1 Protocols *(Continued)*

Interface	Component	Category	Documentation
LDAP	Solaris 10 OS	Standard	Part IV, "LDAP Naming Services Setup and Administration," in *System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)* (http://docs.sun.com/doc/816–4556) man pages: `ldap`(3LDAP) (http://docs.sun.com/doc/816–5170)

Glossary

AHE application hosting environment. See OTP application hosting environment

bare metal computer system A physical or virtualized computer system on which no operating system has been installed. Application deployment onto a bare metal computer system is not possible until an operating system has been installed or deployed onto the system. physical domain and virtual domains are also bare metal computer systems.

capability The ability and operational capacity to perform a particular function; a behavioral contract. Capability can be intrinsic, such as a specific OS version or processor architecture; or capability can be behavioral such as system failover or accounting.

cluster

- A computer system composed of two or more computer system that operate together as a functional whole to provide higher levels of application performance, resources, and reliability, availability, and service ability (RAS) characteristics than those provided by individual component computer systems. A cluster requires control software such as a cluster controller, which functionally complements the operating system installed on its constituent computer systems, and implements cluster-wide resource management functionality and policies.
- A virtualized application hosting environment that enables the highest possible levels of application availability.

clustered OTP system An OTP system which is cluster of two more OTP Systems.

compute element See computer system

computer system

- An element that is comprised of a collection of interoperating physical element, logical element, and software element that provide compute capabilities based on an operating system. See also bare metal computer system.

device A logical element that provides access to, or control of, the capabilities of one or more physical element.

domain A virtual bare metal computer system. See also logical domain and physical domain.

element Hardware components such as processors, disk drives, or devices; also known as physical element.

Softwa

grid

- A computer system composed of two or more computer systems that operate together as a functional whole to provide higher levels of application performance, resource and reliability, availability, and service ability (RAS) characteristics than those provided by individual component computer systems. A grid requires control software such as a grid controller, which functionally complements the operating system installed on its constituent computer systems, and implements grid-wide resource management functionality and policies.

host

- A computer system on which an operating system has been installed or deployed. The (potential) target of an Application Deployment.
- A computer system on which an application can be deployed.

hypervisor

Control software that supports the management of a virtual bare metal computer system. Synonymous with a Virtual Machine Monitor (VMM).

logical domain

A bare metal computer system composed entirely of virtual compute element, network element, and storage element that map to an equivalent or lesser set of element in a physical computer system. A logical domain can host a distinct operating system instance. Logical domains require the presence of underlying control software such as hypervisor.

logical element

An element not associated directly with a physical element. A logical element that provides access to capabilities of a particular physical element is a device. Logical Elements can also expose capabilities and functions that are not intrinsically mappable to a physical element, for example, services.

network element

A device capable of transmitting network packets across network endpoints.

network equipment provider (NEP) application hosting

The act of deploying and managing the life cycle and availability of applications developed by a network equipment provider (NEP) in the OTP application hosting environment

operating system

Control software that can be deployed to a bare metal computer system. An operating system manages access to the capabilities of its hosting computer system and may expose underlying logical element. Application deployment depends on the presence of an active operating system.

OTP

The Open Telecommunications Platform, which provides high availability, system management and application provisioning services that are integrated to create a base computing platform suitable for hosting, developing, and deploying telephone company applications.

OTP application hosting environment

The software element used for development and hosting of network equipment provider (NEP) applications, comprised of other software elements including platform management software, an application management framework, availability management framework, and the application runtime environment.

OTP application hosting environment software component

One of the software element comprising the OTP application hosting environment (AHE) software element.

OTP application run time environment	A set of programmatic interfaces exposed by the OTP application hosting environment software element for the purpose of development and runtime operation of hosted network equipment provider (NEP) applications.
OTP platform	A bare metal computer system designated for development and hosting of network equipment provider (NEP) applications An OTP platform can be a physical or virtual system.
OTP system	A computer system capable of hosting network equipment provider applications, comprised of an OTP platform, a deployed operating system instance and OTP application hosting environment software component.
physical domain	A bare metal computer system composed of compute element, network element, and storage element that map to a subset of the element in a particular physical computer system. A physical domain can host a distinct operating system instance. Physical domains require the presence of underlying control software such as hypervisor.
physical element	An element with a distinct physical existence that can be seen or touched. Physical elements occupy space and may consume power and generate heat.
software element	A piece of software that can be deployed onto a computer system. Examples include operating system, firmware, patches and application packages and images.
Solaris container	A virtualized host that isolates applications from one another by providing a virtualized operating system to each application. A Solaris container requires the presence of control software such as Global Zone to implements management functionality and policies.
storage element	A device capable of persistent storage of data. For example, disk drives and disk volumes such as network-attached storage (NAS) and storage area networks (SAN) devices.
virtual computer system	A computer system that is composed of partitioned or virtualized (mapped) element. See also logical domain and physical domain.
virtualized operating platform	See cluster, grid, Solaris container, and zone.
zone	See Solaris container.

Index

G

H

I

P

R

S

T

V

W

X

Z