Sun Open Telecommunications Platform 1.0 Installation and Administration Guide

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

Part No: 819–7370
December 2006

070208@16599

Contents

Tables

Figures

Preface

The *Sun Open Telecommunications Platform 1.0 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 provides an overview of the Open Telecommunications Platform and a summary of the installation process.
- Chapter 2 provides hardware and software requirements, and descriptions of the settings and worksheets for the settings needed for installation and configuration.
- Chapter 3 provides the procedures for installing and configuring the operating system on the servers selected for the Open Telecommunications Platform system, creating the cluster file system, and verifying system settings.
- Chapter 4 provides the procedures for using the command line interface to install the Open Telecommunications Platform on the servers selected for the Open Telecommunications Platform system.
- Chapter 5 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 provides the procedures for using an existing production OTP System to install and configure OTP on a new standalone OTP host or a new clustered OTP system.

- Chapter 7 provides the procedures for backing up the OTP system management service database and configuration files and restoring the database and configuration files to the fail-over host.
- Appendix A lists the application programming interfaces (APIs) and protocols you can use for application development.
- Glossary provides definitions of Open Telecommunications Platform terms.

Related Documentation

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

- *Sun Open Telecommunications Platform 1.0 Release Notes*
- *Sun Open Telecommunications Platform 1.0 Installation and Administration Guide*

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:`
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 and 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 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.

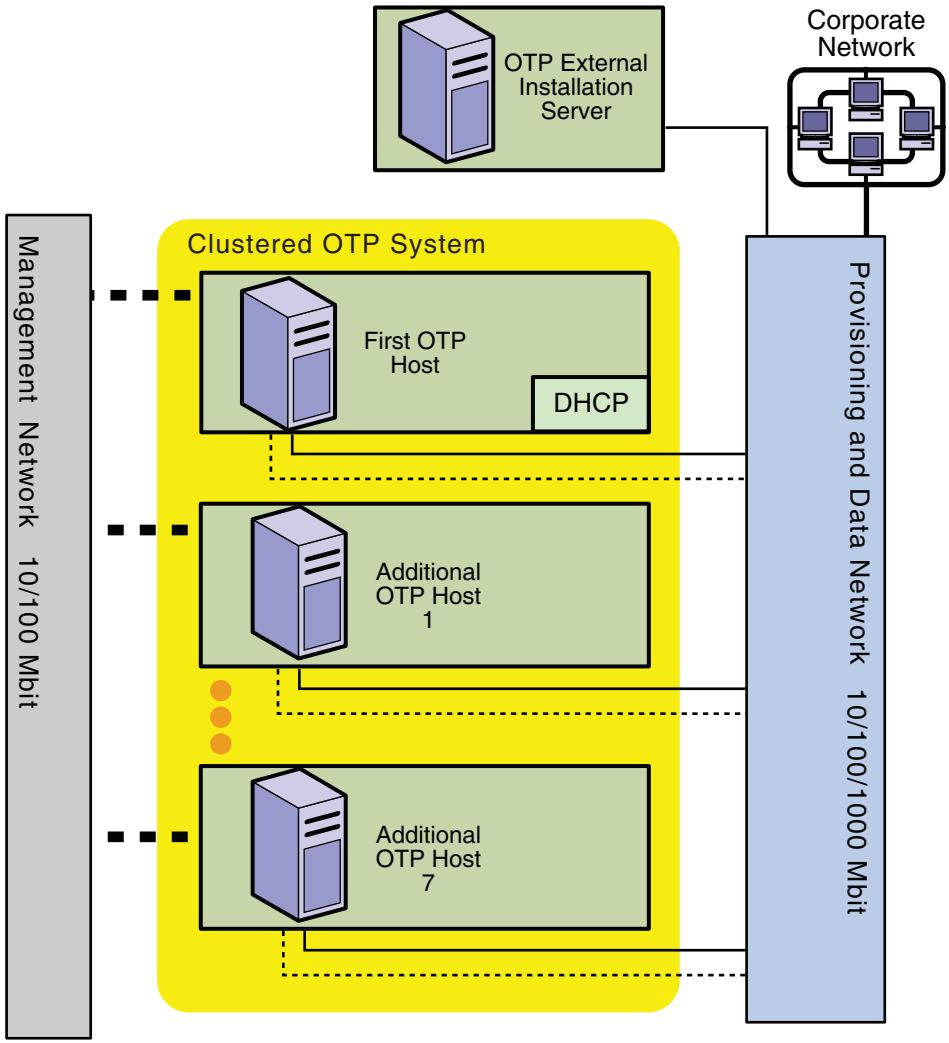

FIGURE 1–1 Open Telecommunications Platform Architecture

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 server that is used for a first-time installation of the Open Telecommunications Platform software to an OTP host using the OTP graphical user interface.

  Note – If you choose to install the Open Telecommunications Platform software manually using the command line, then the external OTP installation server is not required.

- 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.

  In a clustered OTP system, the first OTP host DHCP service allocates IP addresses to the OTP hosts for use by the provisioning network. The OTP system management service uses the provisioning network to load operating systems and updates to the additional OTP hosts.

  Caution – The Solaris OS DHCP service is the only DHCP service supported by Open Telecommunications Platform 1.0. ISC DHCP is not supported.

- 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 21.

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

  Use the worksheets provided in "Open Telecommunications Platform Plan Worksheets" on page 25 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 the servers selected for the Open Telecommunications Platform system as described in Chapter 3.

  Note – If you plan to install the Open Telecommunications Platform using an external OTP installation server, also install and configure the Solaris 10 Update 2 operating system on the external OTP installation server.

- **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 command line as described in Chapter 4. An external OTP installation server is not required using this method.

  – Install the Open Telecommunications Platform using the graphical user interface (GUI) installation as described in Chapter 5. An external OTP installation server is required for this method.

  Note – The external OTP installation server is a temporary server, and is needed only for the duration of the GUI-based installation and configuration process.

- If you have already installed the Open Telecommunications Platform using either of the above methods, you can install the Open Telecommunications Platform to a new standalone OTP host or new clustered OTP hosts using your existing OTP System as described in Chapter 6.

◆ ◆ ◆ 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 server	ALOM	Solaris 10 Update 2, 64 bit	121684-01	OBP 4.18.10, POST 4.18.10, OBDIAG 4.18.10
Netra 440 server	ALOM	Solaris 10 Update 2, 64 bit	121685-02	OBP 4.22.19, POST 4.22.19, OBDIAG 4.22.19
Sun Fire™ V240 server	ALOM	Solaris 10 Update 2, 64 bit	121684-01	OBP 4.18.10, POST 4.18.10, OBDIAG 4.18.10

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

Type	Management Port	OS	Patch	Firmware
Sun Fire V440 server	ALOM	Solaris 10 Update 2, 64 bit	121685-02	OBP 4.22.19, POST 4.22.19, OBDIAG 4.22.19
Sun Fire V890 server	RSC/ALOM	Solaris 10 Update 2, 64 bit	121688-01	OBP 4.22.19, POST 4.22.19, OBDIAG 4.22.19
Sun Fire E2900 server **Note –** The E2900 can only be used as an first OTP host.	SC/LOM	Solaris 10 Update 2, 64 bit	114527-03	ScApp:5.20.2, RTOS:45, SC POST:45
Sun Fire T2000 server	ALOM	Solaris 10 Update 2, 64 bit	123482-03	Sun System Firmware 6.2.6

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. Only the N-by-N cluster configuration is supported.

The following table lists the minimum OTP system server requirements. If you plan to install the Open Telecommunications Platform using an external OTP installation server, 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
Minimum disk space	72 GB
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 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 E2900	FC 3510	On-board GE
Note – The E2900 can only be used as an first OTP host.	SCSI 3120 JBOD	X4445A QGE
	SCSI 3310 JBOD	X4150A-2 2GE
	SCSI 3310 RAID	X4150A GE
	SCSI 3320 JBOD	X4422A-2 combo
	SCSI 3320 RAID	
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	

For the latest list of supported storage and NIC devices, see *(url to be determined)*.

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.
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. OS distributions are stored in the `/var/otp` file hierarchy on the first OTP host. Allocate 3 Gbytes for each OS distribution and each distribution's associated profiles and scripts.
- 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:

  - `/cddrom/otp1.0` for physical media
  - `/net/`*server name*`/otp1.0` where *server name* is the name of a server on which the Open Telecommunications Platform installation source directory `/otp1.0` has been NFS-mounted.

  Note – If you are using an external OTP installation server, this is the fully-qualified path and name of the NFS-mounted Open Telecommunications Platform installation directory on the external OTP installation server.

- **Cluster Name**

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

- **Enable Auto Configuration of IPMP**

  Default value: `yes`

  Valid values: `yes`, `no`

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:

- **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`

- **Secondary IP**

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

- **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*

- **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`

  Valid values: `yes`, `no`

  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`.

- **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`.

- **Node Authentication**

  Required, default value: `sys`

  Valid values: `sys`, `des`

  This option establishes the authentication policies for hosts that are to be added to a clustered OTP system configuration. If you specify `des` (Diffie-Hellman), first add entries to the `publickey(4)` database for each additional OTP host that is to be added to the cluster before running the plans. You can change authentication type at any time by using the `scconf` command from an active cluster host. For details on how to change the node authentication type, refer to the `scconf` command documentation in `scconf`(1M).

- **Private Interface 1**

  The network adapter connected to private interconnect.

- **Private Interface 2**

  The network adapter connected to private interconnect.

- **Transport Type 1**

  Required, default `dlpi`.

  The transport type of the private interconnect adapters.

- **Transport Type 2**

  Required, default `dlpi`.

  The transport type of the private interconnect adapters.

- **Sponsoring Node**

  The name of the first OTP host. Required when installing the Open Telecommunications Platform on a two-to-eight host clustered OTP system.

- **Quorum Auto Configuration**

  Required, default value: `yes`

  Valid values: `yes`, `no`

  Quorum autoconfiguration provides an option to enable or disable auto configuration of the quorum device in a two-host 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 and to reset the cluster from install mode to normal mode. For details on how to configure quorum disks, refer to the `scconf` command documentation in `scconf`(1M)

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/otp1.0`
	`/net/`*install_server*`/otp1.0`
	`/otp1.0`
		_____

Cluster Name (GUI) `clusterName` (CLI)	*otp-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`	_____
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/otp1.0` `/net/`*install_server*`/otp1.0`	_____
Cluster Name (GUI) `clusterName` (CLI)	*otp-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`	_____
Provisioning Interface (GUI) `provisioningInterface` (CLI)	`bge0`, `ce0`, `cd0`, `hme0`, `eri0`	_____
Node Authentication (GUI) `nodeAuthentication` (CLI)		❒ `sys` ❒ `des`
Private Interface 1 (GUI) `privateInterface1` (CLI)	`bge2`	_____
Private Interface 2 (GUI) `privateInterface2` (CLI)	`bge3`	_____

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

Setting Name	Example	Setting Value
Transport Type 1 (GUI) `transportTypeInterface1` (CLI)		`dlpi`
Transport Type 2 (GUI) `transportTypeInterface2` (CLI)		`dlpi`
Sponsoring Node (GUI) `sponsorNode` (CLI) This is the name of the first OTP host.	OTPhost1	
Quorum Auto Configuration (GUI) `quorumAutoConfiguration` (CLI)		❒ Default:`yes` ❒ `no` **Note –** 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 84.

◆ ◆ ◆ 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 clustered OTP systems.

The following topics are discussed:

Note – The installation procedures in this manual assume that the Open Telecommunications Platform installation source is located in the NFS-mounted directory `/opt1.0` on a server that is external to the OTP hosts. If you have purchased the OTP installation DVD-ROM, create the directory `/opt1.0` on an external a server that is external to the OTP hosts, and then copy the DVD-ROM contents to the `/opt1.0`

The directory contents should be as follows:

```
# ls -a /otp1.0
.otp.version  OTP-Readme.html   Products   copyright-otp1.0.txt
```

When you have verified the `/opt1.0` directory, NFS-mount the directory as described in Step 10 in the following procedure.

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 accessible by the standalone OTP host or the clustered OTP hosts, and have at least 6 Gbytes of available free disk space

---

Note – If you have chosen to install the Open Telecommunications Platform using the graphical user interface, you can set up the server as the external OTP installation server as described in "Preparing for Installation" on page 69.

---

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 three Open Telecommunications Platform installation zip files to the directory you created in Step 8:

- `otp1.0.zip-a`
- `otp1.0.zip-b`
- `otp1.0.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
```

- If you are installing the Open Telecommunications Platform for the first time, use either of the two following 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.

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.**

- 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: **share -F nfs -o ro,log=global -d "Sol10U2 ISO mount point" /sol10u2**
- 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 otp1.0.zip-a otp1.0.zip-b otp1.0.zip-c > otp1.0.zip
```

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

For example:

```
# unzip otp1.0.zip
```

The Open Telecommunications Platform installation directory otp1.0 is created.

9 Move the otp1.0 directory to the root file system.

For example:

```
#  mv otp1.0 /
```

The instructions and examples in this manual assume that the OTP installation directory is /otp1.0, and that the /otp1.0 directory has been NFS-mounted as described in the next step.

10 NFS-mount the Open Telecommunications Platform installation directory.

a. Add the fully-qualified path name of the Open Telecommunications Platform installation directory to the /etc/dfs/dfstab file.

For example, if you moved the directory otp1.0 to the root file system, you would add the following line to the file /etc/dfs/dfstab:

```
share -F nfs -o ro,log=global -d "OTP 1.0 Installation Directory" /otp1.0
```

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

Note – The `/otp1.0` 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 Open Telecommunications Platform installation directory.

Next Steps

- Review the OTP System server disk partitioning requirements in the next section. If you have chosen to use JumpStart to install the Solaris OS to the server or servers selected for OTP, ensure that the JumpStart script partitions each server's hard drive as described in Table 3–1.
- If you have chosen to install the Open Telecommunications Platform using the graphical user interface, you can set up the server on which you downloaded the Open Telecommunications Platform as the external OTP installation server as described in "Preparing for Installation" on page 69.

Disk Drive Partitioning Requirements

The following table lists the partitioning requirements for the disk drive of each server within your OTP system.

TABLE 3–1 OTP System Server Disk 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.

Installing and Configuring Solaris 10 Update 2 Operating System

This section provides the procedures for installing Solaris 10 Update 2 on the server or servers you chose for the OTP system. Solaris 10 Update 2 must be installed and configured on each OTP system server before installing the Open Telecommunications Platform software on each server.

If you use an external OTP installation server to install the Open Telecommunications Platform software, you must also install and configure Solaris 10 Update 2 on the external server as well.

This section discusses the following topics:

▼ To Install Solaris 10 Update 2 on the Open Telecommunications Platform Servers

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 When Solaris 10 Update 2 installation has completed and the server has rebooted, perform each of the following procedures in sequence to configure the operating environment.

▼ 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, where *server_name.company.com*

```
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.

▼ (Optional) 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.

▼ (Optional) To Enable FTP

To manage clustered OTP systems, you must enable the FTP service as follows.

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

2 **Type 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
enabled   online         svc:/network/telnet:default
enabled   online         svc:/network/nfs/rquota:default
disabled  disabled       svc:/network/echo:dgram
disabled  disabled       svc:/network/time:stream
enabled   online         svc:/network/ftp:default
```

Next Steps

- Ensure that each OTP system server and storage device meets firmware versions requirements. 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 System Servers" on page 43.

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 "Installing and Configuring Solaris 10 Update 2 Operating System" on page 38
- 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 21

Refer to "OTP System Hardware and Firmware Requirements" on page 21 for the list of required patches and firmware versions for the T2000 server and storage devices, and to the hardware documentation for firmware validation and update procedures. All firmware must be at the required level on the T2000 and on the storage devices prior to installing the Open Telecommunications Platform.

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 `reboot -- -sx` to reboot the T2000 in single user mode.**
   Wait for the T2000 to finish rebooting.
7. **Type `/usr/sbin/e1000g_transition -e -f` to complete the transition to the e1000g driver.**
8. **Type `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 System Servers

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 during installation of the operating system, 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 Install the Open Telecommunications Platform on each of your OTP system servers using either of the following two methods:

- Install the Open Telecommunications Platform using the command line as described in Chapter 4. An external OTP installation server is not required using this method.
- Install the Open Telecommunications Platform using the graphical user interface (GUI) installation as described in Chapter 5. An external OTP installation server is required for this method.

Note – The external OTP installation server is a temporary server, and is needed only for the duration of the GUI-based installation and configuration process.

◆ ◆ ◆ CHAPTER 4

Installing the Open Telecommunications Platform Using the Command Line

This chapter provides the command-line procedures for installing and configuring the Open Telecommunications Platform 1.0.

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.

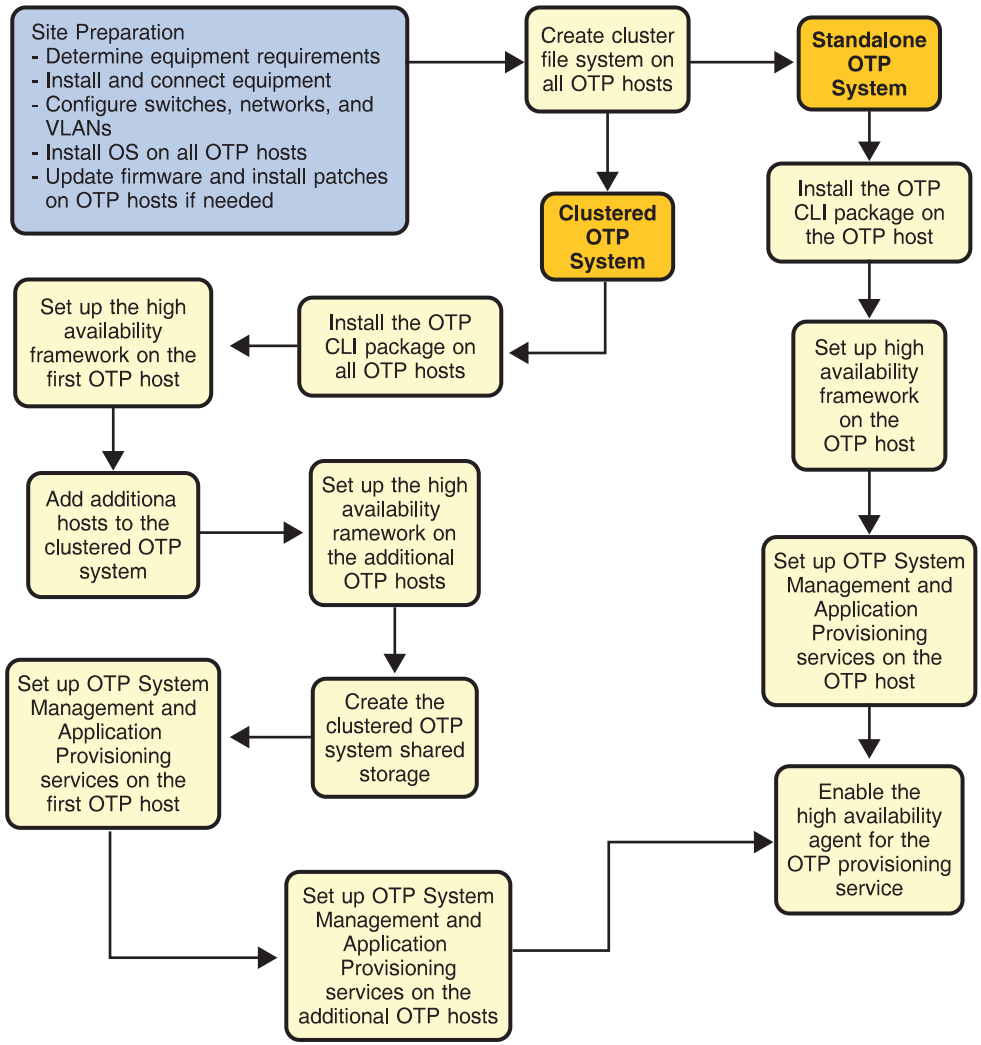

FIGURE 4–1 Open Telecommunications Platform Site Preparation Task Flow

Open Telecommunications Platform Prerequisites

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

- Solaris 10 Update 2 must be installed and configured on each OTP system server as described in "Installing and Configuring Solaris 10 Update 2 Operating System" on page 38.
- NIS setup must be completed on all OTP system server as described in "Installing and Configuring Solaris 10 Update 2 Operating System" on page 38s.
- 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 21.

Installing the Open Telecommunications Platform On A Standalone OTP Host

Manual command-line installation and setup of the Open Telecommunications Platform on a standalone OTP host is comprised of the following steps:

This section discusses the following topics:

Caution –

- Failure to perform the following procedures in sequence presented will result in Open Telecommunications Platform installation failure.
- Manual installation requires the creation of several OTP system state files which contain key names and values used by the installation and configuration process. Do not change the key names. The key names are case sensitive. For example, `mediaDirectory` is valid, whereas `MediaDirectory` is not valid and will cause installation to fail. Providing incorrect values for a key name will cause installation to fail, or cause the installed OTP system to become unstable.

  If installation fails, you must perform a complete reinstall of the Solaris 10 Update 2 OS, and then install the Open Telecommunications Platform again.

▼ To Set Up the OTP High Availability Framework

1 **Log in as root (`su - root`) to the standalone OTP host.**

2 **Install the OTP CLI package.**

Type **`pkgadd -d /net/`***OTP install directory***`/Products/packages -R / SUNWotpcli`** where *OTP install directory* is the installation source directory you created in Step 8 of the procedure "To Download and Uncompress the OTP and Solaris OS Installation Zip Files" on page 34.

For example, if the installation server name is `otpinstall`, and the NFS-mounted installation directory is `/otp1.0`, you would then type:

```
# pkgadd -d /net/otpinstall/otp1.0/Products/packages -R / SUNWotpcli
```

The directory `/opt/SUNWotp10/CLI` is created.

3 **Create the standalone OTP host availability state file.**

a. **Change directory to `/opt/SUNWotp10/CLI`.**

b. **Type `cp templates/setupAvailabilityServiceOnStandalone.dat /var/tmp/setupAvailabilityServiceOnStandalone.dat`**

4 **Edit the file `/var/tmp/setupAvailabilityServiceOnStandalone.dat` as follows.**

- `mediaDirectory=`*OTP_Installation_directory*: The fully qualified path name of the Open Telecommunications Platform installation directory, for example: `/net/otpinstall/otp1.0`
- `clusterName=`*cluster_name*: The name you have chosen for the clustered OTP system.
- `allPatches=yes` to install all patches.

  `allPatches=no` to install mandatory patches only.
- `autoConfigureIPMP`:

  `autoConfigureIPMP=no` if you do not want to set up IPMP.

  To set up IPMP, set `autoConfigureIPMP=yes`, and add the following three lines:
  - `secondaryInterface=`*Ethernet interface 2*
  - `secondaryIP=`*111.112.113.114* where *111.112.113.114* is the IP address of *Ethernet interface 2*.
  - `testIPAddress=`*111.112.113.222* where *111.112.113.222* is the IP address used for IPMP configuration.

Save and close the file.

The single-node availability state file should be similar to the following:

```
mediaDirectory=/net/otpinstall/otp1.0
clusterName=otp-standalone-host
allPatches=yes
autoConfigureIPMP=yes
secondaryInterface=bge1
secondaryIP=10.11.52.68
testIPAddress=10.11.52.74
```

5 Set up the availability service.

Type **`/opt/SUNWotp10/CLI/setupAvailabilityServiceOnStandalone /var/tmp/setupAvailabilityServiceOnStandalone.dat`**.

The `setupAvailabilityServiceOnStandalone` script performs the following tasks:

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

The `setupAvailabilityServiceOnStandalone` installation process logs to the file `/var/tmp/OTPInstaller.log`. You can use the `tail -f` command during installation to view the log file.

When the standalone OTP host has rebooted, log in as root again.

6 Run the `setupAvailabilityServiceOnStandalone` script again, specifying the same availability state file.

For example:

```
# /opt/SUNWotp10/CLI/setupAvailabilityServiceOnStandalone \
/var/tmp/setupAvailabilityServiceOnStandalone.dat
```

The `setupAvailabilityServiceOnStandalone` script verifies the OTP high availability framework installation and configuration.

Next Steps Set up the OTP system management and application provisioning services as described in the next procedure.

▼ To Set Up the OTP System Management and Application Provisioning Services

1 **Log in as root (`su - root`) to the standalone OTP host.**

2 **Create the standalone OTP host management and provisioning state file.**

   a. **Change directory to `/opt/SUNWotp10/CLI`.**

   b. **Type `cp templates/setupManagementServicesOnStandalone.dat /var/tmp/setupManagementServicesOnStandalone.dat`**

3 **Edit the file `/var/tmp/setupManagementServicesOnStandalone.dat` as follows.**

   - `mediaDirectory=`*OTP_Installation_directory*: The fully qualified path name of the Open Telecommunications Platform installation directory, for example: `/net/otpinstall/otp1.0`
   - `managementInterface=`*management interface name* where *management interface name* is `bge0` or `bge1` or `ce0` or `ce1` depending on the interface you have chosen for the management interface, and on the platform type.
   - `provisioningInterface=`*provisioning interface name* where *provisinoing interface name* is `bge0` or `bge1` or `ce0` or `ce1` depending on the interface you have chosen for the provisioning interface, and on the platform type.
   - `logicalHost=`*logical host name* where *logical host name* is an unused logical host name on the same subnet as the standalone OTP host. If a logical host name that exists on a different subnet is specified, installation fails.
   - `logicalIPAddress=`*logical host IP address* where *logical host IP address* is an unused IP address to be assigned to `logicalHost`

   Save and close the file.

   The single-node management and provisioning state file should be similar to the following:

```
mediaDirectory=/net/otpinstall/otp1.0
managementInterface=bge0
provisioningInterface=bge0
logicalHost=otpclient1-logicalhostname
logicalIPAddress=10.11.55.170
```

4 **Set up the management and provisioning services.**

   Type **`/opt/SUNWotp10/CLI/setupManagementServicesOnStandalone /var/tmp/setupManagementServicesOnStandalone.dat`**.

   The `setupManagementServicesOnStandalone` script performs the following tasks:

- Installs the Java Web console
- Installs the OTP system management service high availability agent
- Installs the OTP application provisioning service high availability agent
- Installs patches required by the Open Telecommunications Platform
- Installs and configures the OTP system management service
- Installs and configures the OTP application provisioning service

The `setupManagementServicesOnStandalone` installation process logs to the file `/var/tmp/OTPInstaller.log`. You can use the `tail -f` command during installation to view the log file.

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

▼ To Enable High Availability for the OTP Provisioning Service

1. **Log in as root (`su - root`) to the standalone OTP host.**

2. **Create the standalone OTP host high availability state file.**

   a. **Change directory to `/opt/SUNWotp10/CLI`.**

   b. **Type `cp templates/enableManagementServicesHA.dat /var/tmp/templates/enableManagementServicesHA.dat`**

3. **Edit the file `/var/tmp/templates/enableManagementServicesHA.dat` as follows.**

   - `mediaDirectory=`*OTP_Installation_directory*: The fully qualified path name of the Open Telecommunications Platform installation directory, for example: `/net/otpinstall/otp1.0`
   - `logicalHost=`*logical host name* where *logical host name* is an unused logical host name on the same subnet as the standalone OTP host. If a logical host name that exists on a different subnet is specified, cluster installation fails.

   Save and close the file.

   The single-node high availability state file should be similar to the following:

   ```
   mediaDirectory=/net/otpinstall/otp1.0
   logicalHost=otpclient1-logicalhostname
   ```

4. **Enable high availability for the OTP provisioning service.**

   Type **`/opt/SUNWotp10/CLI/enableManagementServicesHAOnStandalone /var/tmp/enableManagementServicesHA.dat`**

The `enableManagementServicesHAOnStandalone` script installs and enables the OTP application provisioning service high availability agent, and logs to the file `/var/tmp/OTPInstaller.log`.

This completes the Open Telecommunications Platform manual installation process for a standalone OTP host.

5 **Log in as root on 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 first OTP host will not work properly.

Installing the Open Telecommunications Platform On Clustered OTP Hosts

Manual command-line installation and setup of the Open Telecommunications Platform on clustered OTP hosts is comprised of the following steps:

This section discusses the following topics:

Caution –

- Failure to perform the following procedures in sequence will result in Open Telecommunications Platform installation failure.
- Manual installation requires the creation of several OTP system state files containing key names and values used by the installation and configuration process. Do not change the key names. The key names are case sensitive. For example, `mediaDirectory` is valid, whereas `MediaDirectory` is not valid and will cause cluster installation to fail.

▼ To Install the OTP CLI Package to the Clustered OTP System Hosts

The OTP CLI package must be installed to all hosts in the clustered OTP system before you start OTP installation.

1. **Log in as root (`su - root`) to the first OTP host of the clustered OTP system.**

2. **Install the OTP CLI package.**

   Type **`pkgadd -d /net/`***OTP install directory*`/Products/packages -R / SUNWotpcli`** where *OTP install directory* is the installation source directory you created in Step 8 of the procedure "To Download and Uncompress the OTP and Solaris OS Installation Zip Files" on page 34.

   For example, if the installation server name is `otpinstall`, and the NFS-mounted installation directory is `/otpinstall/otp1.0`, you would then type:

   ```
   # pkgadd -d /net/otpinstall/otp1.0/Products/packages -R / SUNWotpcli
   ```

   The directory `/opt/SUNWotp10/CLI` is created.

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

When you have completed installing the OTP CLI package on all clustered OTP system hosts, set up the OTP high availability framework on the first OTP host as described in the next section.

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

Before You Begin The OTP CLI package must be installed on the host as described in "To Install the OTP CLI Package to the Clustered OTP System Hosts" on page 53.

1. **Log in as root (`su - root`) to the first OTP host of the clustered OTP system.**

2. **Create the first OTP host high availability state file.**

   a. **Create the first OTP host high availability state file.**

   b. **Type `cp templates/setupAvailabilityServiceOnFirstHost.dat /var/tmp/setupAvailabilityServiceOnFirstHost.dat`**

3. **Edit the file `setupAvailabilityServiceOnFirstHost.dat` as follows.**

- `mediaDirectory=`*OTP_Installation_directory*: The fully qualified path name of the Open Telecommunications Platform installation directory, for example: `/net/otpinstall/otp1.0`.
- `clusterName=`*cluster_name*: The name you have chosen for the clustered OTP system.
- `nodeAuthentication=sys`: Default value `sys`, valid values are `sys` and `des`. This option establishes the authentication policies for OTP hosts. For further information see *Node Authentication* in "Clustered OTP Host Plan Worksheet" on page 30.
- `privateInterface1=`*Ethernet interface 2* where *Ethernet interface 2* is `bge2` or `ce2` depending on platform type.
- `privateInterface2=`*Ethernet interface 3* where *Ethernet interface 3* is `bge3` or `ce3` depending on platform type.
- `transportTypeInterface1=dlpi`
- `transportTypeInterface2=dlpi`
- `autoConfigureIPMP`:

  `autoConfigureIPMP=no` if you do not want to set up IPMP.

  To set up IPMP, set `autoConfigureIPMP=yes`, and add the following three lines:

  – `secondaryInterface=`*Ethernet interface 2*
  – `secondaryIP=`*111.112.113.114* where *111.112.113.114* is the IP address of *Ethernet interface 2*.
  – `testIPAddress=`*111.112.113.222* where *111.112.113.222* is the IP address used for IPMP configuration.
- `allPatches=yes` to install all patches.

  `allPatches=no` to install mandatory patches only.

Save and close the file.

The multiple-node availability state file should be similar to the following:

```
mediaDirectory=/net/otpinstall/otp1.0
clusterName=otp-cluster1
nodeAuthentication=sys
privateInterface1=bge2
privateInterface2=bge3
transportTypeInterface1=dlpi
transportTypeInterface2=dlpi
autoConfigureIPMP=yes
secondaryInterface=bge1
secondaryIP=10.11.53.174
testIPAddress=10.11.53.175
allPatches=yes
```

4 **Set up the availability service.**

Type **`/opt/SUNWotp10/CLI/setupAvailabilityServiceOnFirstHost /var/tmp/setupAvailabilityServiceOnFirstHost.dat`**

The `setupAvailabilityServiceOnFirstHost` script performs the following tasks:

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

The `setupAvailabilityServiceOnFirstHost` installation process logs to the file `/var/tmp/OTPInstaller.log`. You can use the `tail -f` command during installation to view the log file.

When the first OTP host has rebooted, log in as root again.

5 **Run the `setupAvailabilityServiceOnFirstHost` script again.**

Type **`/opt/SUNWotp10/CLI/setupAvailabilityServiceOnFirstHost /var/tmp/setupAvailabilityServiceOnFirstHost.dat`**

The `setupAvailabilityServiceOnFirstHost` script verifies the OTP high availability framework installation and configuration.

Next Steps Add the additional OTP hosts to the Clustered OTP Systemas described in the next procedure.

▼ To Add Additional OTP Hosts to the Clustered OTP System

Caution – The host name of each additional OTP host in your clustered OTP system must be added to the first OTP host. Failure to do so will result in OTP high availability framework configuration failure.

Tip – Log in to each additional host and type the command **`uname -n`** to display the host name.

Before You Begin

- The OTP CLI package must be installed on the host as described in "To Install the OTP CLI Package to the Clustered OTP System Hosts" on page 53.
- The OTP high availability framework must be set up and configured on the first OTP host as described in "To Set Up the OTP High Availability Framework on the First OTP Host" on page 53

1 **Log in as root (`su - root`) on the first OTP host. Thefirst OTP host must be connected to shared storage.**

2 Add each additional OTP host to the first OTP host.

For each additional OTP host, type `/opt/SUNWotp10/CLI/addNewHost` *OTP host name* where *OTP host name* is the name of the additional OTP host.

For example:

```
# /opt/SUNWotp10/CLI/addNewHost otpclient2 \
/opt/SUNWotp10/CLI/addNewHost otpclient3 \
/opt/SUNWotp10/CLI/addNewHost otpclient4 \
/opt/SUNWotp10/CLI/addNewHost otpclient5 \
/opt/SUNWotp10/CLI/addNewHost otpclient6 \
/opt/SUNWotp10/CLI/addNewHost otpclient7 \
/opt/SUNWotp10/CLI/addNewHost otpclient8
```

Next Steps Set up the OTP high availability framework on each of the additional OTP hosts as described in the next procedure.

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

The following steps must be performed on each additional OTP host in your clustered OTP system.

Before You Begin

- The OTP high availability framework must be set up and configured on the first OTP host as described in "To Set Up the OTP High Availability Framework on the First OTP Host" on page 53
- The additional OTP host must be added to the clustered OTP system as described in "To Add Additional OTP Hosts to the Clustered OTP System" on page 55

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

2 Create the additional OTP host high availability state file.

a. Change directory to `/opt/SUNWootp10/CLI`.

b. Type `cp templates/setupAvailabilityServiceOnOtherHosts /var/tmp/setupAvailabilityServiceOnOtherHosts.dat`

3 Edit the `/var/tmp/setupAvailabilityServiceOnOtherHosts.dat` as follows.

- `mediaDirectory=`*OTP_Installation_directory*: The fully qualified path name of the Open Telecommunications Platform installation directory, for example: `/net/otpinstall/otp1.0`.
- `sponsorNode=`*first OTP host*: The name of the first OTP host.

- `privateInterface1`=*Ethernet interface 2* where *Ethernet interface 2* is `bge2` or `ce2` depending on platform type.
- `privateInterface2`=*Ethernet interface 3* where *Ethernet interface 3* is `bge3` or `ce3` depending on platform type.
- `transportTypeInterface1=dlpi`
- `transportTypeInterface2=dlpi`
- `quorumAutoConfiguration=yes`: Required by the OTP high availability framework
- `autoConfigureIPMP`:

  `autoConfigureIPMP=no` if you do not want to set up IPMP.

  To set up IPMP, set `autoConfigureIPMP=yes`, and add the following three lines:

  – `secondaryInterface`=*Ethernet interface 2*
  – `secondaryIP`=*111.112.113.114* where *111.112.113.114* is the IP address of *Ethernet interface 2*.
  – `testIPAddress`=*111.112.113.222* where *111.112.113.222* is the IP address used for IPMP configuration.
- `allPatches=yes` to install all patches.

  `allPatches=no` to install mandatory patches only.

Save and close the file.

The setup additional OTP hosts high availability state file should be similar to the following:

```
mediaDirectory=/net/otpinstall/otp1.0
sponsorNode=otpclient1
privateInterface1=bge2
privateInterface2=bge3
transportTypeInterface1=dlpi
transportTypeInterface2=dlpi
quorumAutoConfiguration=yes
autoConfigureIPMP=yes
secondaryInterface=bge1
secondaryIP=10.11.55.174
testIPAddress=10.11.55.175
allPatches=yes
```

4 Set up the OTP high availability framework.

Type **`/opt/SUNWotp10/CLI/setupAvailabilityServiceOnOtherHosts /var/tmp/setupAvailabilityServiceOnOtherHosts.dat`**

The `setupAvailabilityServiceOnOtherHosts` script performs the following tasks:

- Installs required Solaris OS patches
- Installs and configures the OTP high availability framework

- Reboots the OTP host

The `setupAvailabilityServiceOnOtherHosts` installation process logs to the file `/var/tmp/OTPInstaller.log`. You can use the `tail -f` command during installation to view the log file.

When the first OTP host has rebooted, log in as root again.

5 Run the `setupAvailabilityServiceOnOtherHosts` script again.

Type **`/opt/SUNWotp10/CLI/setupAvailabilityServiceOnOtherHosts /var/tmp/setupAvailabilityServiceOnOtherHosts.dat`**

The `setupAvailabilityServiceOnOtherHosts` script verifies the OTP high availability framework installation and configuration.

6 If you set `quorumAutoConfiguration=no` on a two-host cluster, you must manually select and configure the quorum disk after cluster configuration is complete as follows.

Note – The following sub-steps apply only to a two-host cluster. If you are setting up the OTP high availability framework on a three-host or more clustered OTP system, this step is optional.

---

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

b. 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.

c. 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
```

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

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

▼ To Create Clustered OTP System Shared Storage

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.

Before You Begin

- The OTP CLI package must be installed on the host as described in "To Install the OTP CLI Package to the Clustered OTP System Hosts" on page 53.
- The OTP high availability framework must be set up and configured on the first OTP host as described in "To Set Up the OTP High Availability Framework on the First OTP Host" on page 53
- The additional OTP hosts must be added to the clustered OTP system as described in "To Add Additional OTP Hosts to the Clustered OTP System" on page 55
- The OTP high availability framework must be set up and configured on the additional OTP host as described in "To Set Up the OTP High Availability Framework on the Additional OTP Hosts" on page 56

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 systemand choose one to be the shared disk to the metaset.

In the following example d4, d5, d6, and d7 are shared disks.

```
# /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
```

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 strings for the `sps-dg` disk group.

Type `metaset -s sps–dg -a -m` *otpclient1 otpclientn* `where` *otpclient1 otpclientn* is the list of OTP hosts separated by a space. For example:

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

h. Type `metaset` to verify the mediator host setup.

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

```
# metaset
Set name = sps–dg, Set number = 1
Host                Owner
  otpclient1         Yes
  otpclient2
Mediator Host(s)    Aliases
  otpclient1
  otpclient2
Driv Dbase
d4   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 Set up OTPsystem management and application provisioning services on the first OTP host as described in the next procedure.

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

Before You Begin

- The OTP CLI package must be installed on the host as described in "To Install the OTP CLI Package to the Clustered OTP System Hosts" on page 53.
- The OTP high availability framework must be set up and configured on the first OTP host as described in "To Set Up the OTP High Availability Framework on the First OTP Host" on page 53
- The additional OTP hosts must be added to the clustered OTP system as described in "To Add Additional OTP Hosts to the Clustered OTP System" on page 55
- The OTP high availability framework must be set up and configured on the additional OTP host as described in "To Set Up the OTP High Availability Framework on the Additional OTP Hosts" on page 56
- Shared storage must be set up on the clustered OTP systems as described in "To Create Clustered OTP System Shared Storage" on page 59

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

2. **Create the OTP system management and application provisioning manager state file.**

   a. **Change directory to `/opt/SUNWotp10/CLI`.**

   b. **Type `cp templates/setupManagementServicesOnFirstHost.dat /var/tmp/setupManagementServicesOnFirstHost.dat`**

3. **Edit the file `/var/tmp/setupManagementServicesOnFirstHost.dat` as follows.**

   - `mediaDirectory=`*OTP_Installation_directory*: The fully qualified path name of the Open Telecommunications Platform installation directory, for example: `/net/otpinstall/otp1.0`.
   - `managementInterface=`*management interface name*: The name of the first OTP host management port, for example `bge1`.
   - `provisioningInterface=`*provisioning interface name*: The name of the first OTP host provisioning port, for example `bge0`
   - `logicalHost=`*logical host name*: An unused logical host name on the same subnet as the first OTP host. If a logical host name that exists on a different subnet is specified, cluster installation fails.

- `logicalIPAddress=`*logical host name IP address:* An unused IP address on the same subnet as the first OTP host.

Save and close the file.

```
mediaDirectory=/net/otpinstall/otp1.0
managementInterface=bge0
provisioningInterface=bge0
logicalHost=otpclient1-logicalhostname
logicalIPAddress=10.11.55.172
```

4 Set up the system management and application provisioning services.

Type **`/opt/SUNWotp10/CLI/setupManagementServicesOnFirstHost /var/tmp/setupManagementServicesOnFirstHost.dat`**.

The `setupManagementServicesOnFirstHost` script performs the following tasks:

- Installs the Java Web console
- Installs Open Telecommunications Platform patches
- Installs the OTP high availability framework agent
- Installs the OTP system management services
- Installs the OTP application provisioning services on shared storage
- Installs J2SE patches

  The `setupManagementServicesOnFirstHost` installation process logs to the file `/var/tmp/OTPInstaller.log`. You can use the `tail -f` command during installation to view the log file.

Next Steps Set up system management and application provisioning services on theadditional OTP hosts as described in the next procedure.

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

OTP system management and application provisioning services must be set up on each additional OTP host. Perform the following procedure on each additional OTP host.

Before You Begin

- The OTP CLI package must be installed on the host as described in "To Install the OTP CLI Package to the Clustered OTP System Hosts" on page 53.
- The OTP high availability framework must be set up and configured on the first OTP host as described in "To Set Up the OTP High Availability Framework on the First OTP Host" on page 53

- The additional OTP hosts must be added to the clustered OTP system as described in "To Add Additional OTP Hosts to the Clustered OTP System" on page 55
- The OTP high availability framework must be set up and configured on the additional OTP host as described in "To Set Up the OTP High Availability Framework on the Additional OTP Hosts" on page 56
- Shared storage must be set up on the clustered OTP systems as described in "To Create Clustered OTP System Shared Storage" on page 59
- System management and application provisioning services must be set up on the on the first OTP host as described in "To Set Up OTP System Management and Application Provisioning Services on the First OTP Host" on page 62

1 Log in as root (`su - root`) to the additional OTP host.

2 Create the additional OTP host system management and application provisioning state file.

a. Change directory to `/opt/SUNWotp10/CLI`.

b. Type `templates/setupManagementServicesOnOtherHosts /var/tmp/setupManagementServicesOnOtherHosts.dat`.

3 Edit the file `/var/tmp/setupManagementServicesOnOtherHosts.dat` as follows.

- `mediaDirectory=`*OTP_Installation_directory*: The fully qualified path name of the Open Telecommunications Platform installation directory, for example: `/net/otpinstall/otp1.0`.
- `logicalHost=`*logical host name*: An unused logical host name on the same subnet as the first OTP host. If a logical host name that exists on a different subnet is specified, cluster installation fails.
- `logicalIPAddress=`*logical host name IP address:* An unused IP address assigned to the host logical name that is on the same subnet as the first OTP host.

Save and close the file.

The system management and application provisioning manager state file should be similar to the following:

```
mediaDirectory=/net/otpinstall/otp1.0
logicalHost=otpclient2-logicalhostname
logicalIPAddress=10.11.55.182
```

4 Set up the OTP system management and application provisioning services.

Type **`/opt/SUNWotp10/CLI/setupManagementServicesOnOtherHosts /var/tmp/setupManagementServicesOnOtherHosts.dat`**.

The `setupManagementServicesOnOtherHosts` script performs the following tasks:

- Installs the Java Web console
- Installs Open Telecommunications Platform patches
- Installs the OTP high availability framework agent
- Installs the OTP system management services
- Installs the OTP application provisioning services on shared storage
- Installs J2SE patches

The `setupManagementServicesOnOtherHosts` installation process logs to the file `/var/tmp/OTPInstaller.log`. You can use the `tail -f` command during installation to view the log file.

Next Steps Enable the high availability agent as described in the next procedure.

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

The high availability agents must be enabled on the first OTP host.

Before You Begin

- The OTP CLI package must be installed on the host as described in "To Install the OTP CLI Package to the Clustered OTP System Hosts" on page 53.
- The OTP high availability framework must be set up and configured on the first OTP host as described in "To Set Up the OTP High Availability Framework on the First OTP Host" on page 53
- The additional OTP hosts must be added to the clustered OTP system as described in "To Add Additional OTP Hosts to the Clustered OTP System" on page 55
- The OTP high availability framework must be set up and configured on the additional OTP hosts as described in "To Set Up the OTP High Availability Framework on the Additional OTP Hosts" on page 56
- Shared storage must be set up on the clustered OTP systems as described in "To Create Clustered OTP System Shared Storage" on page 59
- System management and application provisioning services must be set up on the on the first OTP host as described in "To Set Up OTP System Management and Application Provisioning Services on the First OTP Host" on page 62
- System management and application provisioning services must be set up on the on the additional OTP hosts as described in "To Set Up System Management and Application Provisioning Services on the Additional OTP Hosts" on page 63

The following steps must be performed on the first OTP host.

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

2 **Create the enable high availability state file.**

a. **Change directory to** `/opt/SUNWotp10/CLI`**.**

b. **Type** `cp templates/enableManagementServicesHA.dat /var/tmp/templates/enableManagementServicesHA.dat`

3 **Edit the state file** `/var/tmp/templates/enableManagementServicesHA.dat` **as follows.**

- `mediaDirectory=`*OTP_Installation_directory*: The fully qualified path name of the Open Telecommunications Platform installation directory, for example: `/net/otpinstall/otp1.0`.
- `logicalHost=`*logical host name*: An unused logical host name on the same subnet as the first OTP host. If a logical host name that exists on a different subnet is specified, cluster installation fails.
- `logicalIPAddress=`*logical host name IP address:* An unused IP address on the same subnet as the first OTP host.

Save and close the file.

The system management and application provisioning manager state file should be similar to the following:

```
mediaDirectory=/net/otpinstall/otp1.0
logicalHost=otpclient1-logicalhostname
logicalIPAddress=10.11.55.182
```

4 **Enable high availability on the clustered OTP system.**

Type **`/opt/SUNWotp10/CLI/enableManagementServicesHAOnFirstHost.dat /var/tmp/enableManagementServicesHA.dat`**

The `enableManagementServicesHA` script installs and enables the OTP application provisioning services high availability agent.

The `enableManagementServicesHA` installation process logs to the file `/var/tmp/OTPInstaller.log`. You can use the `tail -f` command during installation to view the log file.

5 **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.

◆ ◆ ◆ CHAPTER 5

Installing the Open Telecommunications Platform Using the Graphical User Interface

This chapter provides the procedures for using the OTP provisioning service graphical user interface on an 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.

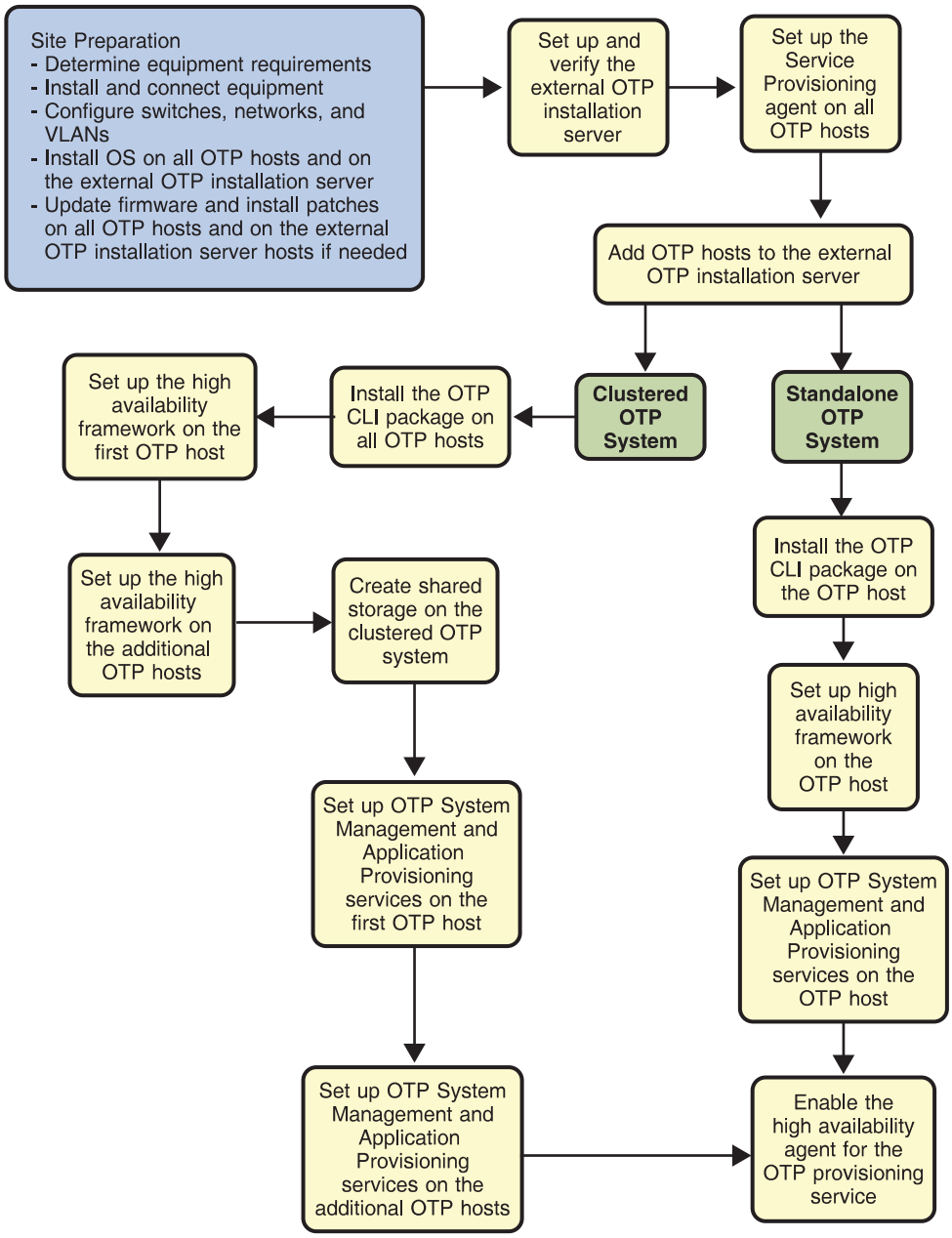

FIGURE 5–1 GUI-Based Open Telecommunications Platform Installation Task Flow

Summaries of each of the above graphical user interface install tasks are provided in the following list.

- Site Preparation

  This task involves the following actions:

  – Inventory the equipment you want to use with the Open Telecommunications Platform, and compare the inventory to the system requirements in as described in "OTP System Hardware and Firmware Requirements" on page 21.

Open Telecommunications Platform Prerequisites

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

- Solaris 10 Update 2 must be installed and configured on each clustered OTP system server as described in "Installing and Configuring Solaris 10 Update 2 Operating System" on page 38.
- NIS setup must be completed on all clustered OTP system servers.
- All clustered OTP system serverss and storage devices must meet the minimum patch and firmware requirements as described in "OTP System Plan Settings Descriptions" on page 25.
- The Solaris 10 Update 2 operating system must be installed and configured on the external OTP installation server as described in "Installing and Configuring Solaris 10 Update 2 Operating System" on page 38.

Preparing for Installation

This section provides the procedures for preparing the external OTP installation server and the clustered OTP hosts for Open Telecommunications Platform installation.

The preparation process is comprised of the following procedures, which must be performed in sequence.

- "To Set Up and Verify the External OTP Installation Server" on page 69
- "To Set Up the Service Provisioning Remote Agent on the Clustered OTP Systems" on page 73
- "To Add Hosts to the External OTP Installation Server" on page 74

▼ To Set Up and Verify the External OTP Installation Server

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

- If the external OTP installation server is the same server to which you downloaded the Open Telecommunications Platform software, go to Step 2.
- If the external OTP installation server is not the same server to which you downloaded the Open Telecommunications Platform software, perform the following steps.

a. Copy the entire Open Telecommunications Platform installation directory from the download server or from the OTP Installation DVD-ROMto the external OTP installation server.

The download server is the server to which you downloaded the Open Telecommunications Platform product in "To Download and Uncompress the OTP and Solaris OS Installation Zip Files" on page 34. :

For example:

- If your download server name is `downloads`
- You have moved the unzipped OTP install directory to `/otp1.0`
- You have NFS-mounted the `/otp1.0` directory on the download server

You would then type:

```
# cp -r /net/downloads/otp1.0 /otp1.0
```

b. Add the following line to the `/etc/dfs/dfstab` file.

```
share -F nfs -o ro,log=global -d "OTP 1.0 Installation Directory" /otp1.0
```

Note – The `/otp1.0` directory is referred to throughout this document as the OTP installation directory.

---

c. Type `svcadm restart nfs/server` to stop and then restart NFS and NFS-mount the installation directory.

2 Install the OTP CLI package.

Type **`pkgadd -d /otp1.0/Products/packages -R / SUNWotpcli`**

The directory `/opt/SUNWotp10/CLI` is created.

3 Set up the external OTP installation server.

Type **`/opt/SUNWotp10/CLI/setupExternalInstallServer /otp1.0`**

The installation process installs the OTP application provisioning service and the Open Telecommunications Platform plug-in.

Wait for the installation process to complete. The installation process may take up to 10 minutes to complete.

4 Open a Web browser.

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.

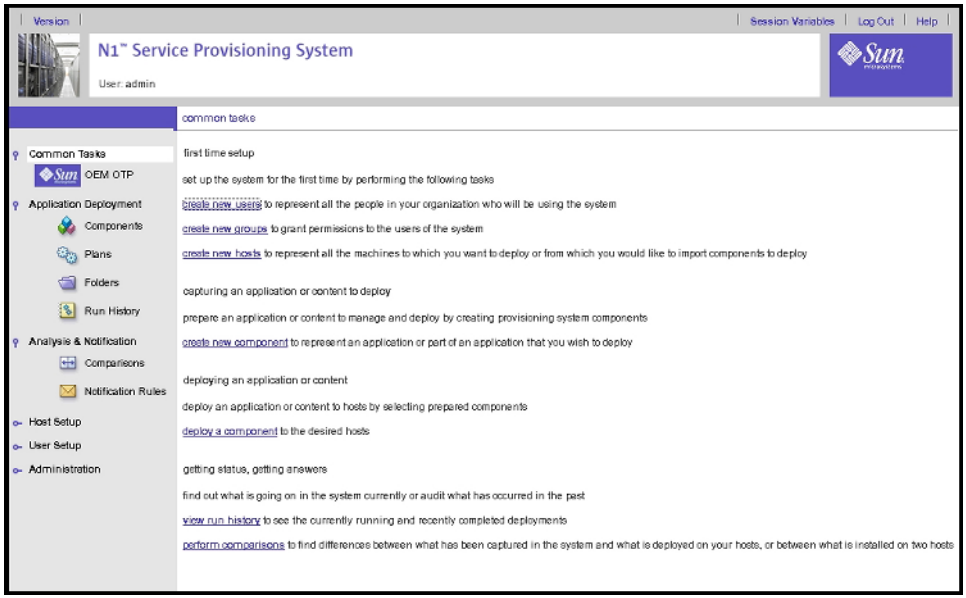

FIGURE 5–2 Common Tasks Page

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

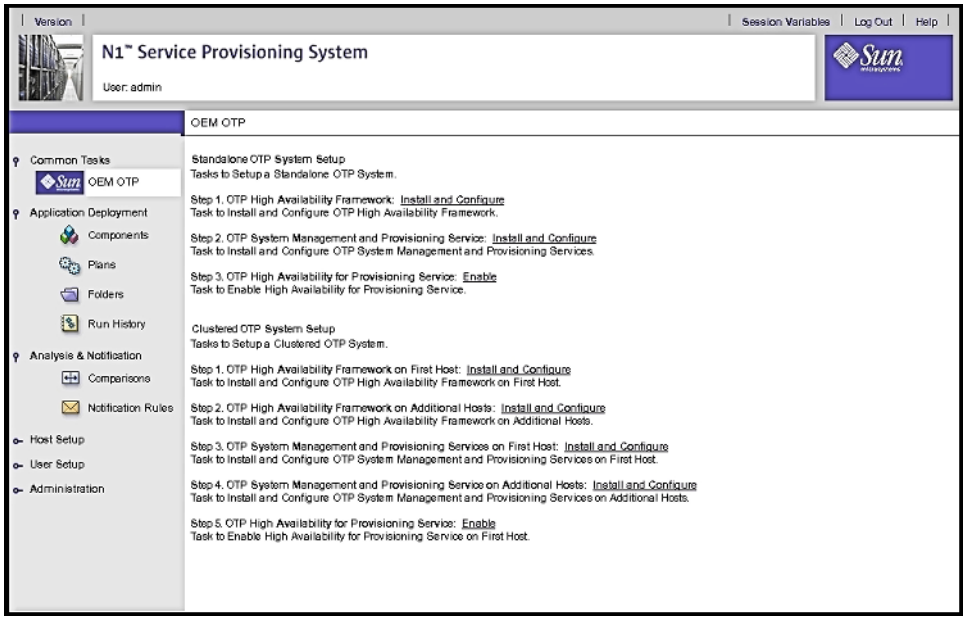

FIGURE 5–3 Open Telecommunications Platform Tasks Page

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

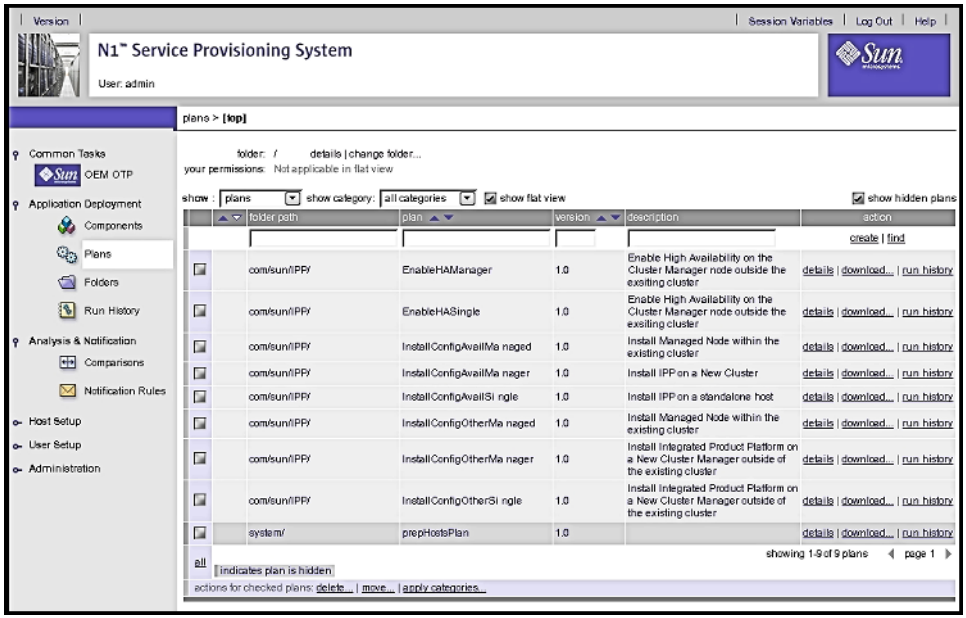

FIGURE 5–4 Plans Screen

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

Next Steps Set up the service provisioning remote agent on the clustered OTP systems as described in the next procedure.

▼ To Set Up the Service Provisioning Remote Agent on the Clustered OTP Systems

The service provisioning remote agent must be installed on the standalone OTP host for a standalone OTP system, and on each clustered OTP host for a clustered OTP system. The remote agent must be installed on each OTP host for Open Telecommunications Platform installation to succeed..

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 "Preparing for Installation" on page 69.

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

2 Install the OTP CLI package.

Type `pkgadd -d /net/`*external OTP installation server*`/otp1.0/Products/packages -R / SUNWotpcli` where *external OTP installation server* is the name of the external OTP installation server.

For example, if the installation server name is `otpinstall`, you would then type:

```
# pkgadd -d /net/otpinstall/otp1.0/Products/packages -R / SUNWotpcli
```

The directory `/opt/SUNWotp10/CLI` is created.

3 Install the service provisioning remote agent.

Type `/opt/SUNWotp10/CLI/setupRemoteAgent` *install directory* where *install directory* is the Open Telecommunications Platform installation source directory. For example:

```
# /opt/SUNWotp10/CLI/setupRemoteAgent  /net/otpinstall/otp1.0-install
```

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

Next Steps Add each new OTP host to the external OTP installation server as described in the next section.

▼ 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 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 "Preparing for Installation" on page 69.
- The service provisioning remote agent must be installed on all of the clustered OTP system hosts as described in "To Set Up the Service Provisioning Remote Agent on the Clustered OTP Systems" on page 73

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:

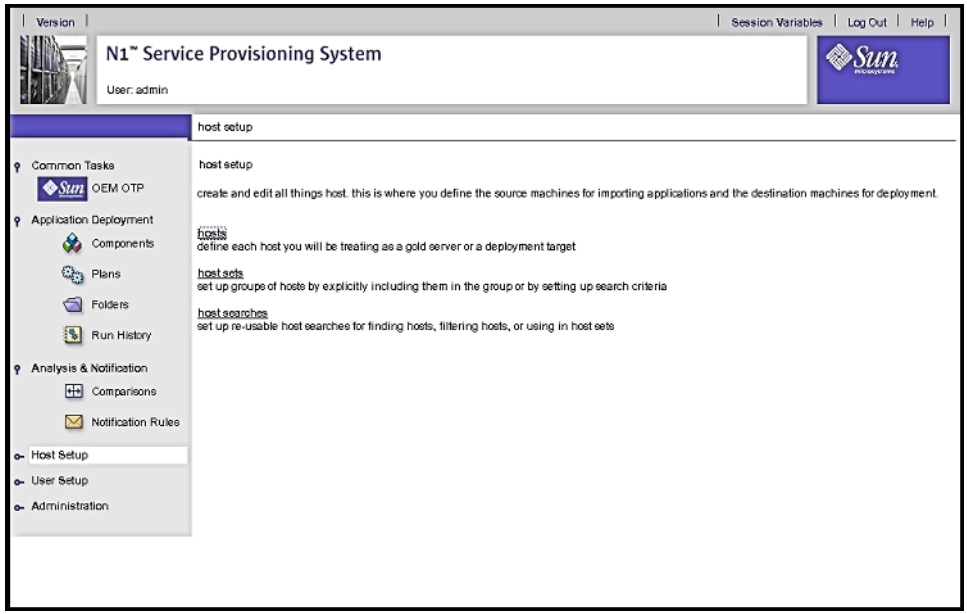

FIGURE 5–5 Host Setup page

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

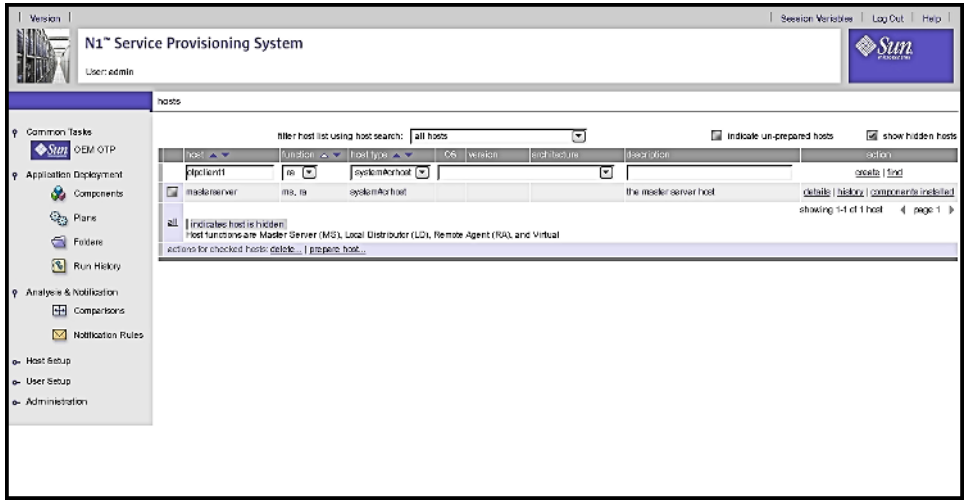

FIGURE 5–6 Hosts Page

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:

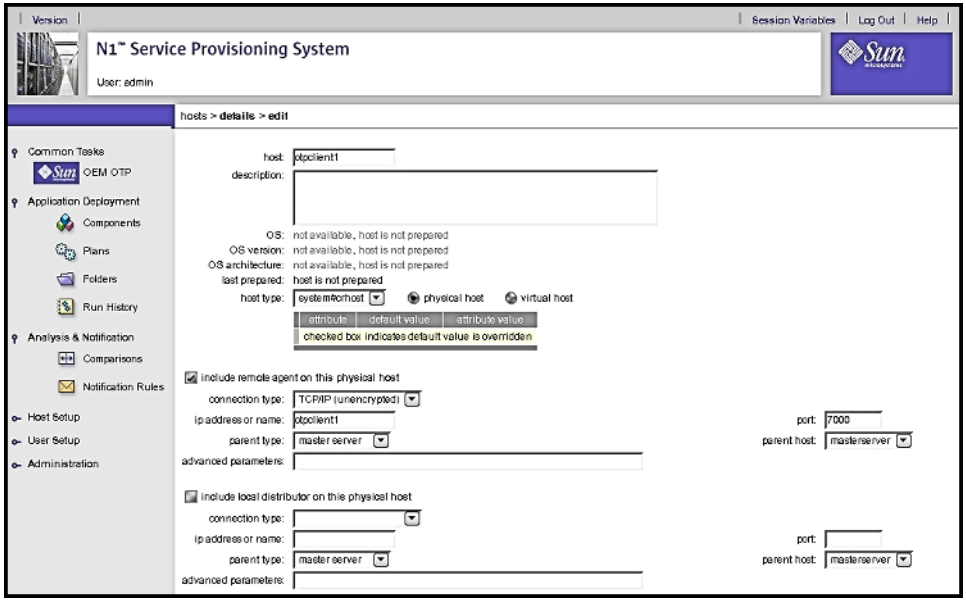

FIGURE 5–7 Host Edit Details Page

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. **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 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 77.
- 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 84.

Installing the Open Telecommunications Platform On A Standalone OTP Host

In a standalone OTP host, the single host is the first OTP host server for the cluster.

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 77
- "To Set Up OTP System Management and Provisioning Services" on page 80
- "To Enable High Availability For the OTP Provisioning Service " on page 82

Note – Refer to the "OTP System Plan Settings Descriptions" on page 25 and the "Standalone OTP Host Plan Worksheet" on page 28 for information needed during installation.

▼ 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 Set Up and Verify the External OTP Installation Server" on page 69
- The Service Provisioning remote agent must be set up on the standalone OTP host as described in "To Set Up the Service Provisioning Remote Agent on the Clustered OTP Systems" on page 73

- The standalone OTP host must be added to the external install server as described in "To Add Hosts to the External OTP Installation Server" on page 74

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.

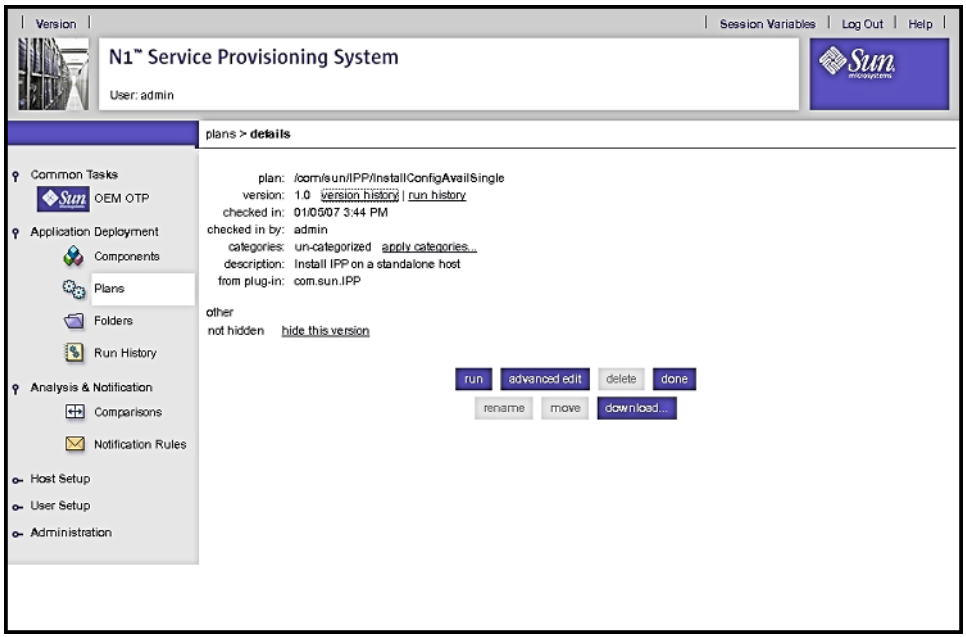

FIGURE 5–8 Edit Availability Plan Page

4 **Click run.**

The Availability Plan Variables page appears.

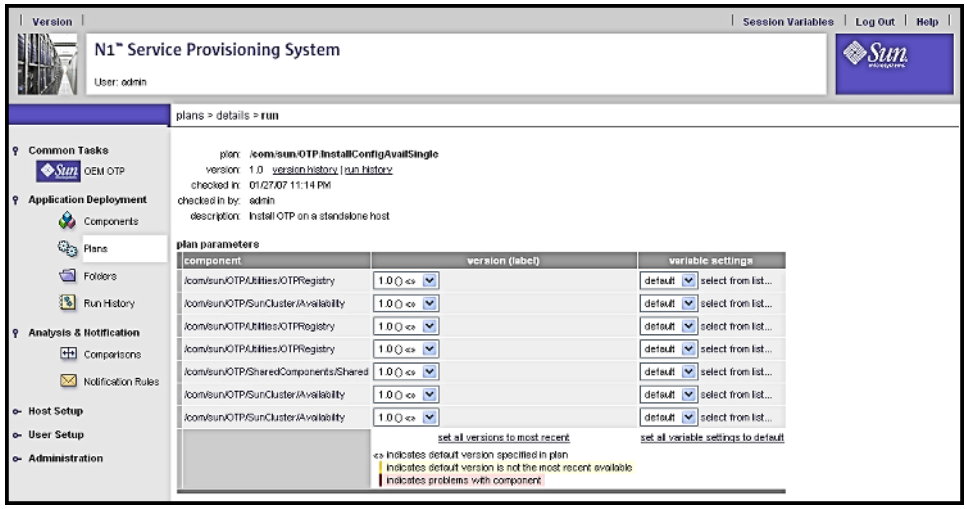

FIGURE 5–9 Availability Plan Variables Page

Scroll the page down to view the variables:

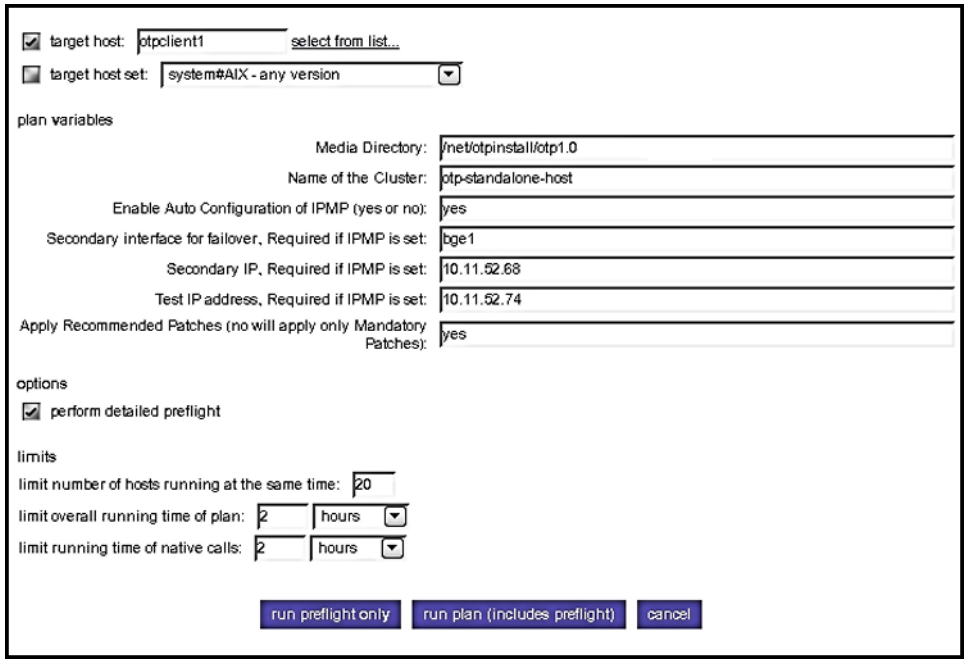

FIGURE 5–10 Availability Plan Variables Page: Variables

Type the information in the plan variables fields according to your "Standalone OTP Host Plan Worksheet" on page 28. Refer to the "OTP System Plan Settings Descriptions" on page 25 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

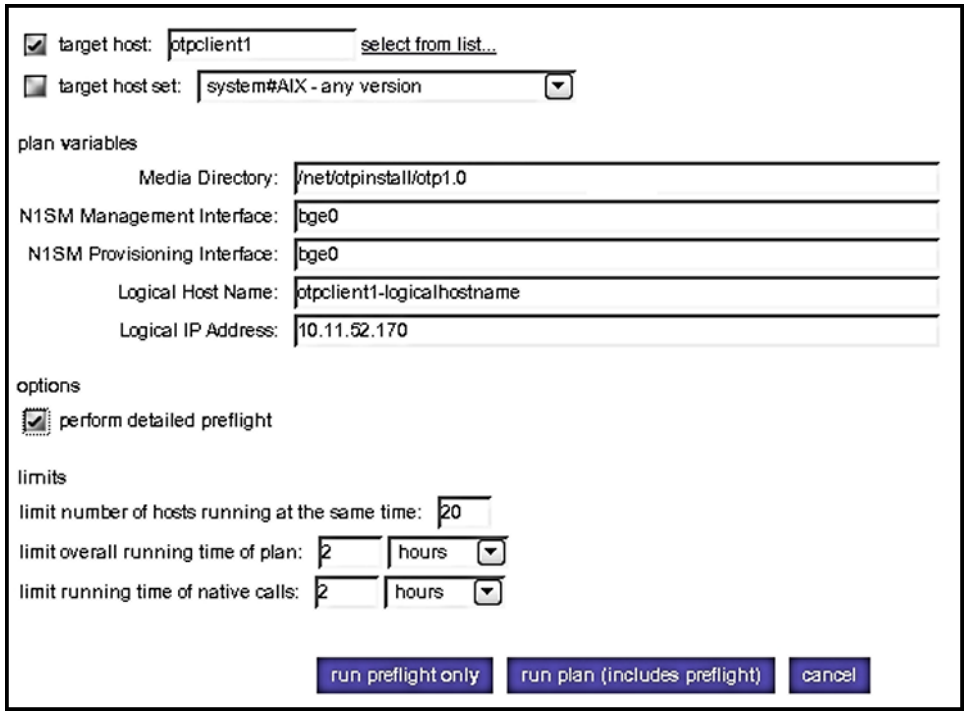

FIGURE 5–11 System Management and Application Provisioning Plan Variables Page

Type the information in the plan variables fields according to your "Standalone OTP Host Plan Worksheet" on page 28. Refer to the "OTP System Plan Settings Descriptions" on page 25 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. Scroll the page down to display the variables

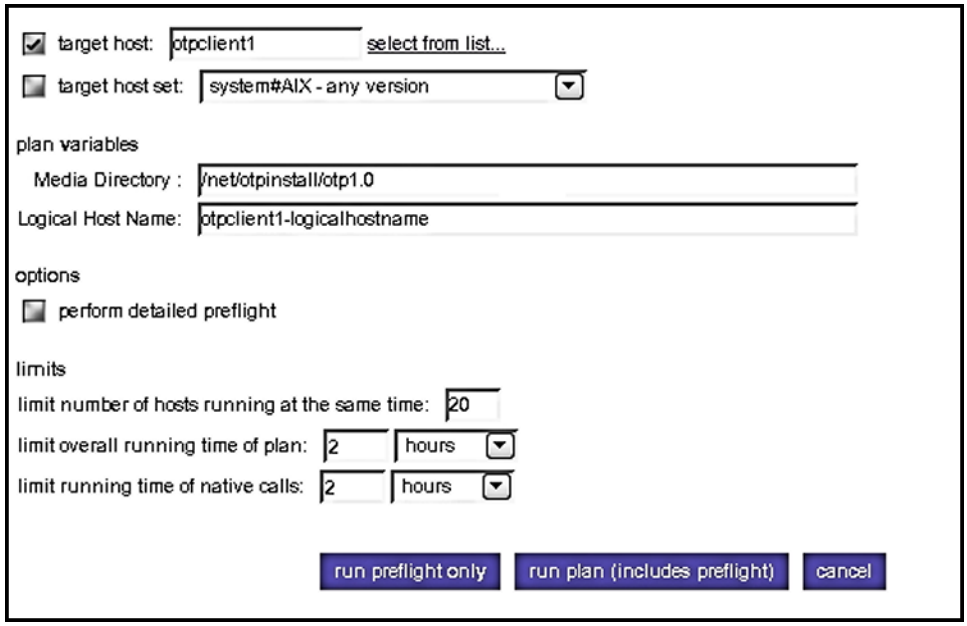

FIGURE 5–12 High Availability Plan Variables Page

Type the information in the plan variables fields according to your "Standalone OTP Host Plan Worksheet" on page 28. Refer to the "OTP System Plan Settings Descriptions" on page 25 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:

Note – Refer to the "OTP System Plan Settings Descriptions" on page 25 and the "Clustered OTP Host Plan Worksheet" on page 30 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 Set Up and Verify the External OTP Installation Server" on page 69
- The Service Provisioning remote agent must be set up on all hosts in the clustered OTP system as described in "To Set Up the Service Provisioning Remote Agent on the Clustered OTP Systems" on page 73
- 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 74

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.

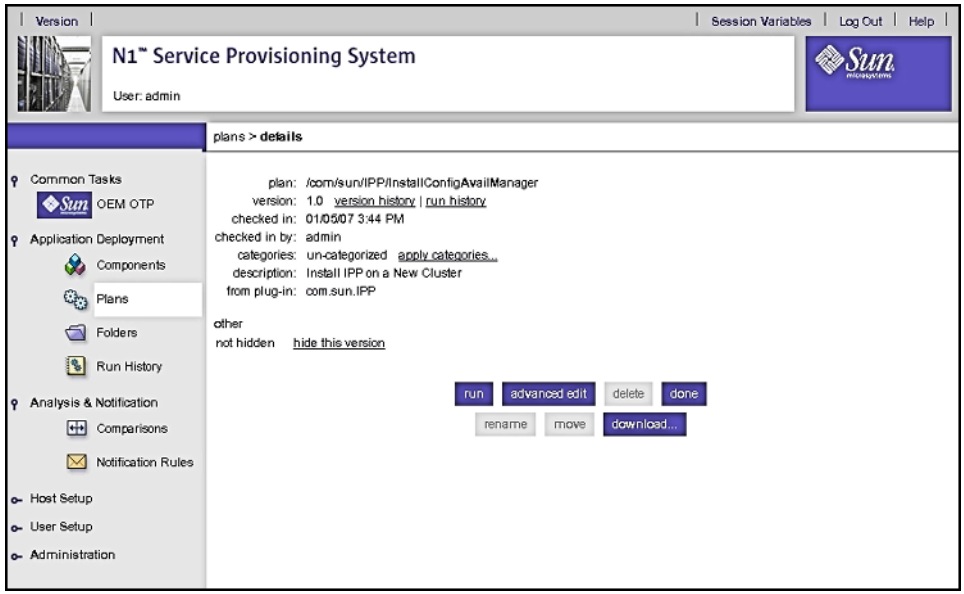

FIGURE 5–13 Clustered OTP Host Edit Availability Plan Page: System Management Server

4 **Click run.**

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

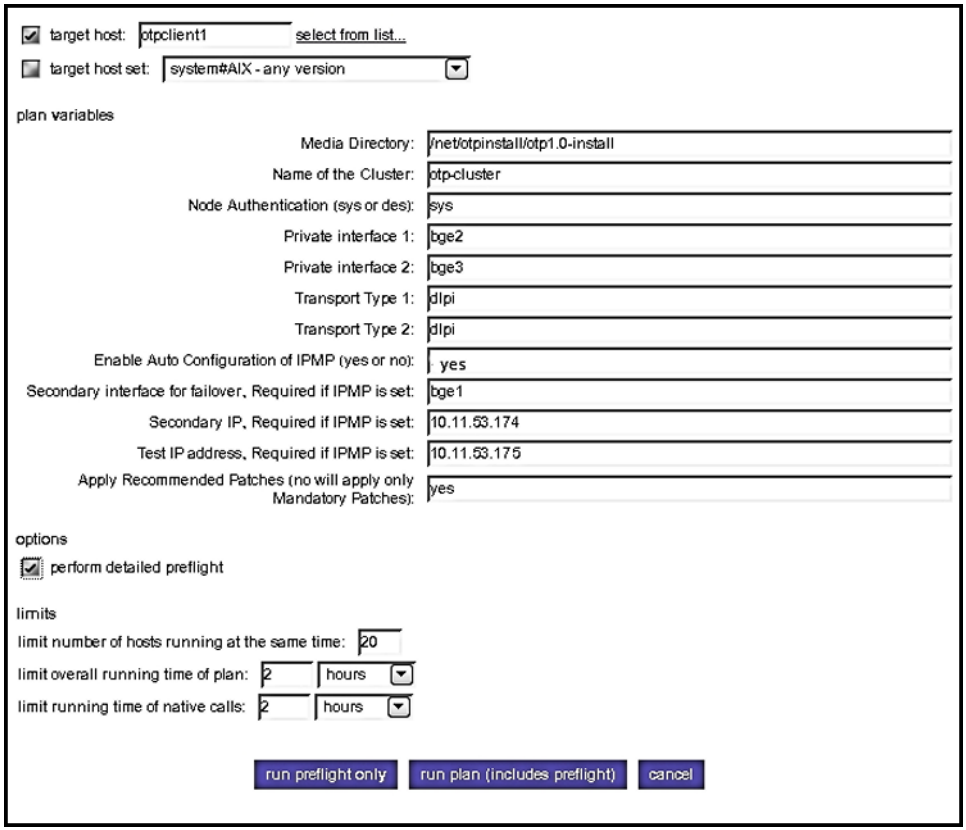

FIGURE 5–14 Clustered OTP Host Availability Plan Variables Page: System Management Server Variables

Type the information in the plan variables fields according to your "Clustered OTP Host Plan Worksheet" on page 30. Refer to the "OTP System Plan Settings Descriptions" on page 25 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.

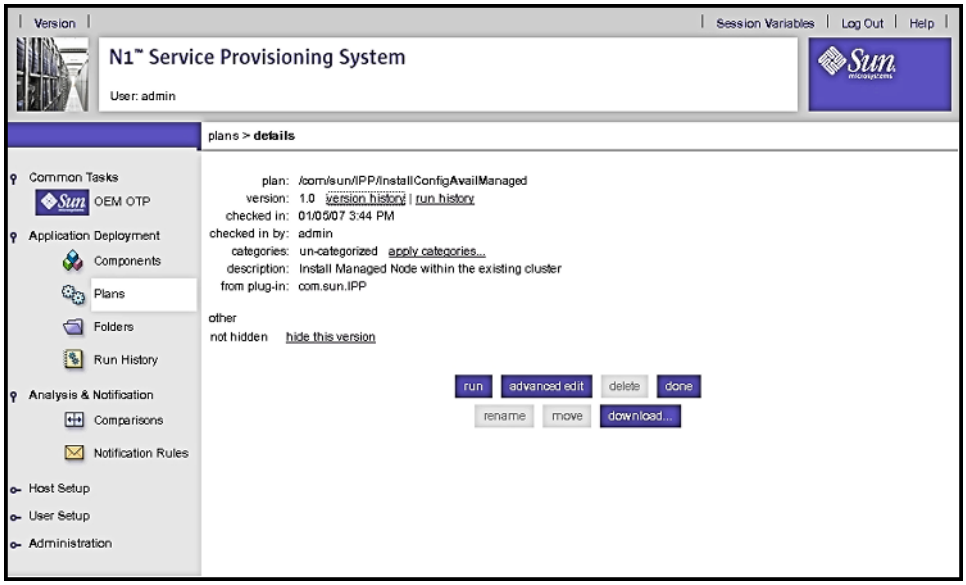

FIGURE 5–15 Clustered OTP Hosts Edit Availability Plan Page

4 Click run.

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

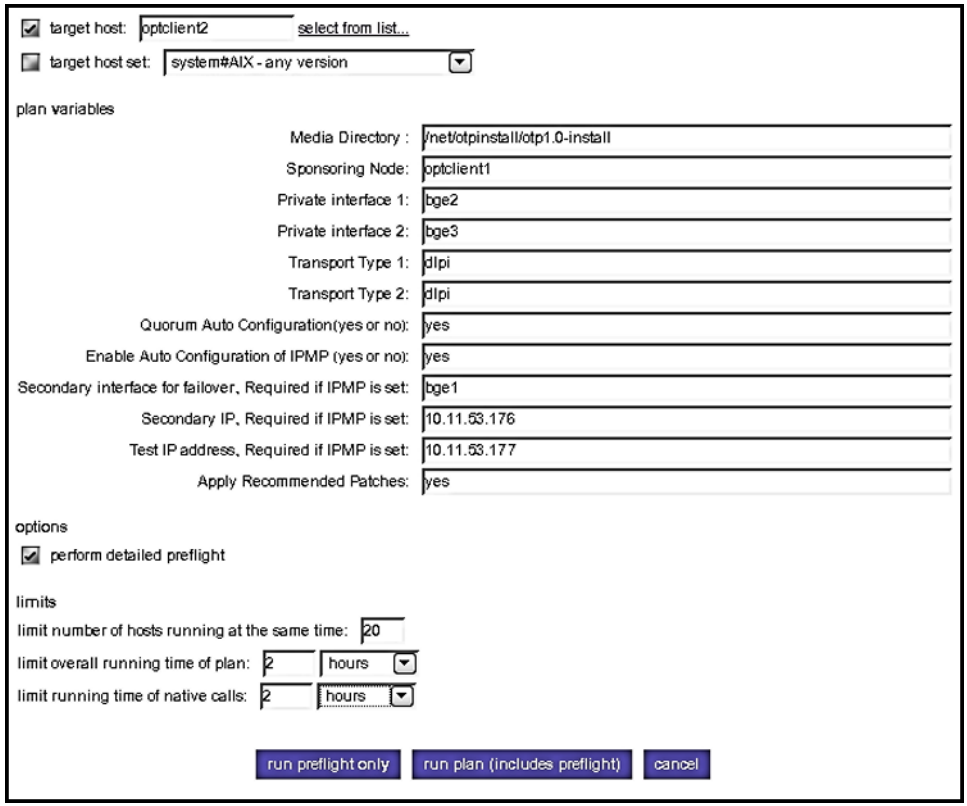

FIGURE 5–16 Clustered OTP Hosts Availability Plan Variables Page

Type the information in the plan variables fields according to your "Clustered OTP Host Plan Worksheet" on page 30. Refer to the "OTP System Plan Settings Descriptions" on page 25 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 follows.**

Note – The following sub-steps apply only to a two-host cluster. If you are setting up the OTP high availability framework on a three-host or more clustered OTP system, this step is optional.

---

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

b. 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.

c. 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
```

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

▼ 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.

Before You Begin The OTP high availability framework must be set up on all OTP hosts in the clustered OTP system.

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

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

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

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 only on the first OTP host.

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 the `scdidadm` command to determine which disks are seen on all nodes of cluster and choose one to be the shared disk to metaset.

In the following example d4, d5, d6, and d7 are shared disks.

```
# /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` *otpclient1 otpclientn* `where` *otpclient1 otpclientn* is the list of OTP hosts separated by a space. For example, assuming that `otpclient1` is the First OTP host

```
# metaset -s sps–dg -a -h  otpclient2 otpclient3 otpclient4 otpclient5 \
ontclient6 otpclient7 otpclient8
```

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

In the following example, the d7 shared disk is added:

```
# 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 strings for the `sps-dg` disk group.

Type `metaset -s sps–dg -a -m` *otpclient1 otpclientn* `where` *otpclient1 otpclientn* is the list of OTP hosts separated by a space. For example:

```
# metaset -s sps–dg -a -m otpclient1 otpclient2 otpclient3 otpclient4 otpclient5 \
ontclient6 otpclient7 otpclient8
```

h. Type `metaset` to verify the mediator host setup.

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

```
# metaset
Set name = sps–dg, Set number = 1
```

```
Host                Owner
  otpclient1         Yes
  otpclient2
Mediator Host(s)    Aliases
  otpclient1
  otpclient2
Driv Dbase
d4   Yes
```

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

The following steps must be performed for each host.

a. **Log in to the clustered OTP 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 Set up the system management and provisioning services on the first OTP host 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

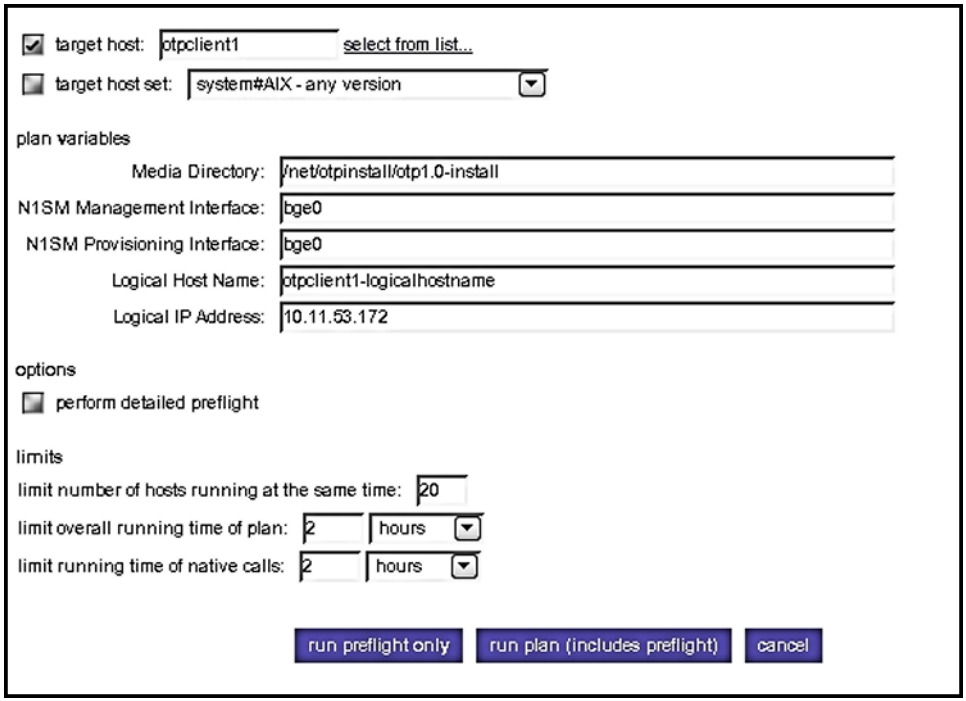

FIGURE 5–17 Clustered OTP Host System Management and Application Provisioning Plan Variables Page: First OTP Host

Type the information in the plan variables fields according to your "Clustered OTP Host Plan Worksheet" on page 30. Refer to the "OTP System Plan Settings Descriptions" on page 25 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

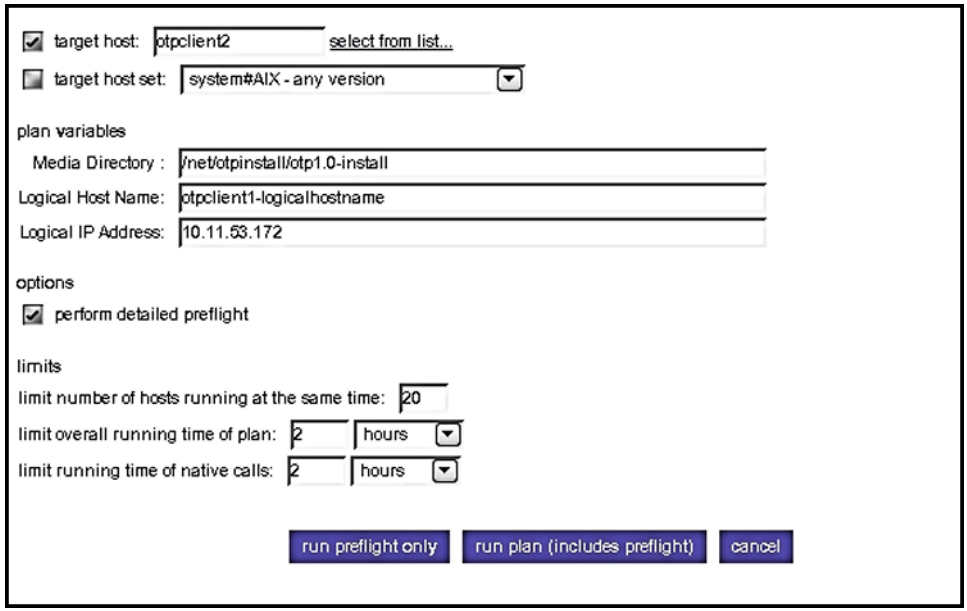

FIGURE 5–18 Clustered OTP Host System Management and Application Provisioning Plan Variables Page: Additional OTP Host

Type the information in the plan variables fields according to your "Clustered OTP Host Plan Worksheet" on page 30 for this OTP host. Refer to the "OTP System Plan Settings Descriptions" on page 25 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

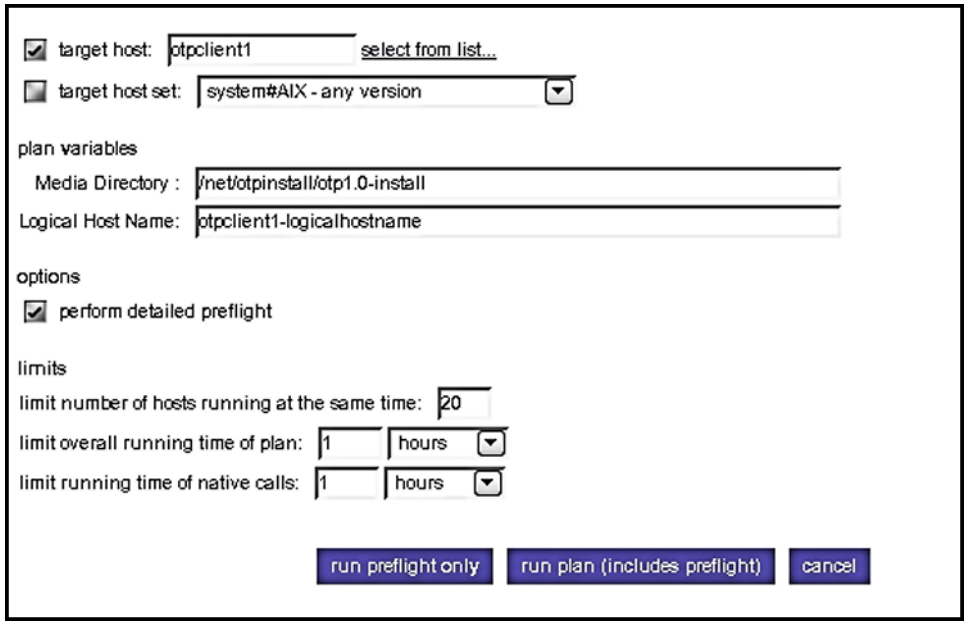

FIGURE 5–19 Clustered OTP Host High Availability Plan Variables Page: First OTP Host

Type the information in the plan variables fields according to your "Clustered OTP Host Plan Worksheet" on page 30. Refer to the "OTP System Plan Settings Descriptions" on page 25 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 thefirst 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/scswitch -F -g otp-system-rg` to take the remote group offline.

b. 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
```

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

d. 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.

e. 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.

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

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

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

◆ ◆ ◆ CHAPTER 6

Installing the Open Telecommunications Platform Using an Existing OTP System

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

In the following sections and procedures, the OTP host used as the 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*.

The following topics are discussed:

Tip – Before you begin, review the OTP Plan settings described in "OTP System Plan Settings Descriptions" on page 25, 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 OS

This section provides the procedures for preparing the OTP system management service to provision the Solaris 10 Update 2 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 100
- 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 uses to discover and manage the bare metal new OTP hosts as described in "To Create the XML Discovery File" on page 101
- If you are going to install OTP to new OTP hosts on a different subnet, create a DHCP relay as described in "To Create the DHCP Relay for Deploying to New OTP Hosts on Different Subnets" on page 102

▼ To Create the OS Image

1 Log in as root to the production OTP host.

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 34.

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.

▼ To Create the XML Discovery File

To discover, manage, and provision an OS to bare metal (no operating system installed) OTP hosts, you must create an XML discovery file that lists the server name, model number, and MAC address of each OTP host.

1. **Log in as root to the production OTP host.**

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
Sun Fire V240	SF-V240

Host Type	Model Type for Bare Metal Discovery
Sun Fire V440	SF-V440
Sun Fire V890	SF-V890
Sun Fire E2900	SF-E2900
Sun Fire T1000	SF-T1000

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-T1000">
        <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 OS to the New OTP Hosts" on page 104.
- If you are deploying the OS to new OTP hosts in a different subnet, 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, 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 substeps 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 production OTP host.**

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 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 production OTP host system management service.**

Go to URL https://*production OTP host*:6789 where *production OTP host* is either the IP address or the fully qualified name of the production OTP host.

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 "Disk Drive Partitioning Requirements" on page 38 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 substeps 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 production OTP host system management service.**

Go to URL https://*production OTP host*:6789 where *production OTP host* is either the IP address or the fully qualified name of the production OTP host.

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 "To Create the XML Discovery File" on page 101. 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, 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 104.

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.

12 **When the new OTP host has rebooted, set up NIS on the host according to your network requirements.**

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 New OTP Hosts Using the Production OTP Host" on page 115

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 production OTP host.**

2 **Type `/opt/sun/n1gc/bin/n1sh` to open the OTP 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 100
- *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 "To Create the XML Discovery File" on page 101.

   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 production OTP host.**

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, install OTP to the hosts as described in "Installing OTP on New OTP Hosts Using the Production OTP Host" on page 115

Preparing the New OTP Hosts for OTP Installation

Before you can install OTP to the new OTP hosts, you must set up the OTP provisioning service remote agent on each host, and then add the host to the production OTP host as described in the following procedures.

The following topics are discussed:

▼ To Install the Service Provisioning Remote Agent on a New OTP Host

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

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

2 **Install the OTP CLI package.**

Type `pkgadd -d /net/`*OTP install directory*`/Products/packages -R / SUNWotpcli` where *OTP install directory* is the installation source directory you created in Step 8 of the procedure "To Download and Uncompress the OTP and Solaris OS Installation Zip Files" on page 34.

For example, if the installation server name is `otpinstall`, and the NFS-mounted installation directory is `/otpinstall/otp1.0`, you would then type:

```
# pkgadd -d /net/otpinstall/otp1.0/Products/packages -R / SUNWotpcli
```

The directory `/opt/SUNWotp10/CLI` is created.

3 **Install the service provisioning remote agent.**

Type`/opt/SUNWotp10/CLI/setupRemoteAgent` *install directory* where *install directory* is the Open Telecommunications Platform installation source directory. For example:

```
# /opt/SUNWotp10/CLI/setupRemoteAgent  /net/otpinstall/otp1.0
```

The `setupRemoteAgent` script creates the service provisioning account, installs the patches needed by the remote agent, and installs the remote agent.

Next Steps Add each new OTP host to the production OTP host as described in the following procedure.

▼ To Add New OTP Hosts to the Production OTP Host

1 **Open a Web browser and log in to the production OTP host service provisioning service.**

Go to URL http://*production OTP host*:9090 where *production OTP host* is either the IP address or the fully qualified name of the production OTP host.

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 host edit details page and click `save`.**

f. **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.

g. **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 the production OTP host 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 77.
- 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 84.

Installing OTP on New OTP Hosts Using the Production OTP Host

With the exception that you use the production OTP host 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 production OTP host when performing the following tasks. When directed to log in to the OTP provisioning service, use URL http://*production OTP host logical host name*:9090 in each procedure where *production OTP host logical host name* of the production OTP host. Refer to the worksheet you prepared for the production OTP host logical host name.

The following topics are discussed:

▼ To Install OTP on a Standalone OTP Host

Make certain that you use the production OTP host as noted above when performing the following tasks. When directed to log in to the OTP provisioning service, use URL http://*production OTP host logical host name*:9090 in each procedure.

Before You Begin

- The service provisioning remote agent must be installed on the standalone OTP host as described in "To Install the Service Provisioning Remote Agent on a New OTP Host" on page 113.
- The standalone OTP host must be added to the OTP master server as described in "To Add New OTP Hosts to the Production OTP Host" on page 114.

1. **Set up the OTP high availability framework as described in "To Set Up the OTP High Availability Framework" on page 77.**
2. **Set up the OTP System Management and Provisioning Services as described in"To Set Up OTP System Management and Provisioning Services" on page 80.**
3. **Enable the OTP high availability framework as described in"To Enable High Availability For the OTP Provisioning Service " on page 82**

▼ To Install OTP on a Clustered OTP System

Make certain that you use the production OTP host as noted above when performing the following tasks. When directed to log in to the OTP provisioning service, use URL http://*production OTP host logical host name*:9090 in each procedure.

Before You Begin

- The service provisioning remote agent must be installed on all hosts in the new clustered OTP system as described in "To Install the Service Provisioning Remote Agent on a New OTP Host" on page 113.
- Each new clustered OTP host must be added to the OTP master server as described in "To Add New OTP Hosts to the Production OTP Host" on page 114.

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 84**
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 87**
3. **Set up the OTP shared storage as described in "To Create Shared Storage on the Clustered OTP System" on page 90**

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 93.**

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 95.**

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 96**

◆ ◆ ◆ CHAPTER 7

Backing Up and Restoring the OTP System Management Service

If the OTP host on which the OTP system management service is installed fails, you can restore the management services to any other clustered OTP host as described in this chapter.

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 127

This chapter provides the procedures for backing up the system management database and configuration files, restoring the files to a new OTP host, and for enabling the system management service on the new OTP host.

The following topics are discussed:

Backing Up OTP System Management Service Database and Configuration Files

This section provides the procedure for backing up the system management database and configuration files. Backup of the system management database and configuration files should be performed on a regular basis.

▼ To Back Up the OTP Master Server 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

Enabling the OTP 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 121.

  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 on the OTP Host" on page 125.

  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.

This section describes how to configure the system management on the OTP host and then restore the system management database and configuration files to the OTP host.

▼ 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 Master Server Database and Configuration Files" on page 120 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 Open Telecommunications Platform requires IP address-based discovery.

You are asked whether you want to modify the default password on the execution server.

19 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.

20 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 on the OTP Host

1. **Log in as root on the OTP host.**
2. **Type** `mkdir -p /var/tmp/n1smbackup`**.**
3. **Copy the** `n1smbackup.tgz` **backup file you created in** **"To Back Up the OTP Master Server Database and Configuration Files" on page 120** **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 121.

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

▼ To Backup and Restore OS Distributions 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 OTP host.**

◆ ◆ ◆ 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 1.0 APIs

Interface	Component	Category	Documentation
POSIX.1 (IEEE Std 1003.1)	Solaris™ 10 OS	Standard	man pages:`POSIX.1`(5)

TABLE A–1 OTP 1.0 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 1.0 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 1.0 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. Software components such as operating system or applications, also known as logical elements. An entity that supports well-defined capabilities of use to other element.

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