



Trusted Solaris 7 Installation and Configuration on the Sun Enterprise 10000

Sun Microsystems, Inc.
901 San Antonio Road
Palo Alto, CA 94303-4900
U.S.A.

Part Number 805-8110
November 1999

Copyright 1999 Sun Microsystems, Inc. 901 San Antonio Road, Palo Alto, California 94303-4900 U.S.A. All rights reserved.

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

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

Sun, Sun Microsystems, the Sun logo, docs.sun.com, AnswerBook, AnswerBook2, Trusted Solaris, and Solaris are trademarks, registered trademarks, or service marks of Sun Microsystems, Inc. in the U.S. and other countries. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc.

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

Federal Acquisitions: Commercial Software – Government Users Subject to Standard License Terms and Conditions

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

Copyright 1999 Sun Microsystems, Inc. 901 San Antonio Road, Palo Alto, Californie 94303-4900 Etats-Unis. Tous droits réservés.

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

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

Sun, Sun Microsystems, le logo Sun, docs.sun.com, AnswerBook, AnswerBook2, Trusted Solaris, et Solaris sont des marques de fabrique ou des marques déposées, ou marques de service, de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pays. Toutes les marques SPARC sont utilisées sous licence et sont des marques de fabrique ou des marques déposées de SPARC International, Inc. aux Etats-Unis et dans d'autres pays. Les produits portant les marques SPARC sont basés sur une architecture développée par Sun Microsystems, Inc.

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

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



Preface

The *Trusted Solaris 7 Installation and Configuration on the Sun Enterprise 10000* describes how to install and configure Trusted Solaris 7 on the Sun Enterprise™ 10000.

Who Should Use This Book

Trusted Solaris 7 Installation and Configuration on the Sun Enterprise 10000 is intended for the system administrator whose duties include setting up and configuring operating system software, and for the security administrator whose duties include determining who is allowed to perform what tasks on the system. The system administrator should be familiar with installation and operation of the Sun Enterprise 10000 server, and of the Trusted Solaris 7 operating environment. The security administrator should be familiar with the site security policy.

How This Book Is Organized

This book is organized as follows:

Chapter 1 provides general information on using Trusted Solaris 7 on the Sun Enterprise 10000. It describes supported software configurations, differences between Solaris 7 and Trusted Solaris 7 features, and offers two illustrations of supported configurations.

Chapter 2 describes tasks to perform for installing and configuring the Trusted Solaris operating environment on a workstation that will become the Trusted Solaris

SSP. It includes how to retain a pre-existing Solaris SSP 3.1 and SSP 3.1.1 environment, configuring the SSP network, and installing an AnswerBook2 server for the SSP man pages. This chapter replaces the procedures in *Sun Enterprise 10000 SSP 3.1.1 Installation and Release Notes*, 805-7521-10.

Chapter 3 describes installing and configuring Trusted Solaris SSP 3.1.1 on an SSP running the Trusted Solaris operating environment. It includes how to restore an SSP 3.1 or SSP 3.1.1 environment, and how to follow Trusted Solaris procedures for a more secure administrative setup. This chapter replaces the procedures in *Sun Enterprise 10000 SSP 3.1.1 Installation and Release Notes*, 805-7521-10.

Chapter 4 describes installing and configuring the Trusted Solaris 7 operating environment on a Sun Enterprise 10000 domain. This chapter replaces the procedures in “Solaris 7 8/99 on the Sun Enterprise 10000 Server” in *Solaris 7 8/99 Sun Hardware Platform Guide*, 806-1117-10.

Chapter 5 describes installing Trusted Solaris Alternate Pathing 2.2 on the Sun Enterprise 10000. This chapter replaces the procedures in “Alternate Pathing 2.2 on the Sun Enterprise 10000 Server” in *Solaris 7 8/99 Sun Hardware Platform Guide*, 806-1117-10.

Related Documents

You should have the following documents on hand for reference and use when installing and configuring your Sun Enterprise 10000.

- *Sun Enterprise 10000 System Hardware Installation and De-Installation Guide*, 805-4651-11, Revision A, July 1998
- *Sun Enterprise 10000 SSP 3.1.1 User Guide*
- *Sun Enterprise 10000 SSP 3.1.1 Reference Manual*
- *Trusted Solaris Installation and Configuration Guide*
- *Trusted Solaris Administration Overview*
- *Trusted Solaris Administrator's Procedures*

Note - Postscript copies of the Solaris documentation on the SSP 3.1.1, AP 2.2, and Dynamic Reconfiguration are located in the `Docs` directory of the Trusted Solaris Supplemental CD.

Ordering Sun Documents

The Sun Software Shop stocks select manuals from Sun Microsystems, Inc. You can purchase individual printed manuals and AnswerBook2™ CDs.

For a list of documents and how to order them, visit the Software Shop at <http://www.sun.com/software/shop/>.

Accessing Sun Documentation Online

The docs.sun.comSM 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. The URL is <http://docs.sun.com>.

Typographic Conventions

TABLE P-1 Typographic Conventions

Typeface or Symbol	Meaning	Example
AaBbCc123	The names of commands, files, and directories; on-screen computer output	Edit your .login file. Use <code>ls -a</code> to list all files. <code>machine_name%</code> You have mail.
AaBbCc123	What you type, contrasted with on-screen computer output	<code>machine_name%</code> su <code>Password:</code>

TABLE P-1 Typographic Conventions *(continued)*

Typeface or Symbol	Meaning	Example
<i>AaBbCc123</i>	Command-line placeholder: replace with a real name or value	To delete a file, type <code>rm filename</code> .
<i>AaBbCc123</i>	Book titles, new words or terms, or words to be emphasized	Read Chapter 6 in <i>User's Guide</i> . These are called <i>class</i> options. You <i>must</i> be root to do this.

Trusted Solaris 7 on a Sun Enterprise 10000

This chapter provides general information on installing, configuring, and using the Trusted Solaris 7 operating environment on the Sun Enterprise™ 10000. It describes supported software configurations, differences between Solaris 7 and Trusted Solaris 7 features, and offers two illustrations of supported configurations.

Trusted Solaris SSP and Domain Software for the Sun Enterprise 10000

The recommended configuration for Trusted Solaris 7 on a Sun Enterprise 10000 is to run the Trusted Solaris 7 operating environment on the SSPs and on the domains. It is possible to run a heterogeneous environment, with both the Trusted Solaris environment and the Solaris environment on the SSPs and the domains.

The Trusted Solaris operating environment is based on the Solaris 7 8/99 release. As does the Solaris 7 8/99 release, Trusted Solaris 7 supports DR (Dynamic Reconfiguration), but does not support IDN (InterDomain Networking):

Trusted Solaris 7 Software for the Sun Enterprise 10000

The Trusted Solaris version of SSP 3.1.1 (referred to as Trusted Solaris SSP 3.1.1), is shipped on the Trusted Solaris 7 Supplemental CD, as is the Trusted Solaris version of AP 2.2 (referred to as Trusted Solaris AP 2.2). If an SSP is to run the Trusted

Solaris 7 operating environment, then Trusted Solaris SSP 3.1.1 and Trusted Solaris AP 2.2 should be installed. For a domain running the Trusted Solaris 7 operating environment, Trusted Solaris AP 2.2 should be used.

Solaris 7 Software Environment

If an SSP is to run Solaris 7 software, then the Solaris version of SSP 3.1.1 and AP 2.2 must be used for that SSP. If a domain is to run Solaris 7 software, then the Solaris version of AP 2.2 must be used for that domain.

Differences from Solaris 7 Installation and Configuration of the Sun Enterprise 10000

For administrators familiar with Trusted Solaris installation, installing a Trusted Solaris SSP and a Trusted Solaris domain are extensions of installing the Trusted 7 operating environment with trusted packages. Administrators familiar with installing Solaris software on a Sun Enterprise 10000 should be aware of the differences between the Solaris and Trusted Solaris environments.

Trusted Solaris Roles Replace Solaris Users

The Trusted Solaris environment does not have a superuser. Superuser tasks are divided among administrative roles. Trusted Solaris administrative roles run with a special shell, the profile shell (`pfsh(1M)`). Roles do not directly log in; they are “assumed” by a user who is assigned the role by the security administrator. A role can only log in remotely from the same role on another Trusted Solaris workstation. For more information on roles, see “Assuming a Role and Working in a Role Workspace” in *Trusted Solaris Administrator's Procedures*.

SSP User Versus SSP Role

The `ssp` user on Solaris SSP 3.1.1 has been replaced by the `ssp` role on Trusted Solaris SSP 3.1.1. Any commands that the `ssp` user runs in the Solaris environment are run by the `ssp` role in the Trusted Solaris environment. The `ssp` role runs with the profile shell (`pfsh`), and should not be changed to run with other shells.

The home directory (`/export/home/ssp`) for the `ssp` role is created at installation as a multilevel directory (MLD). The `ssp` role runs at label `admin_low`, and its files

are stored in an SLD (single-label directory) at the label `admin_low`. See *Trusted Solaris Administration Overview* for an explanation of the Trusted Solaris environment and concepts.

Superuser (root) Versus root Role

The Solaris superuser (root) has been replaced by the Trusted Solaris root role. For the Trusted Solaris SSP 3.1.1 and the Trusted Solaris AP 2.2, any commands that superuser runs in a Solaris environment are run by the root role in a Trusted Solaris environment. The root role runs with the profile shell (`pfsh`), and should not be changed to run with other shells.

SSP Local and Remote Access Using Trusted Solaris Software

Trusted Solaris access to the SSP console is different from Solaris access because of Trusted Solaris role constraints.

SSP Local Access

On a Solaris SSP console, the `ssp` user can directly log in. On a Trusted Solaris SSP console, an administrator first logs in as a user who can assume the `ssp` role, then assumes the role.

On a Solaris SSP console, the superuser can directly log in, or can use the `su(1M)` command to become superuser. On a Trusted Solaris SSP console, an administrator who can assume the root role first logs in as a user, then assumes the role.

SSP Remote Access

To access the `ssp` user remotely on a Solaris SSP, a user can `rlogin(1)` or `telnet(1)` to the SSP and then log in as the `ssp` user. A user can also CDE `rlogin` to the SSP, then CDE log in as the `ssp` user.

To access the `ssp` role remotely on a Trusted Solaris SSP:

- From another Trusted Solaris workstation, assume the `ssp` role. In the `ssp` role, `rlogin(1)` to the SSP. This method works only from another Trusted Solaris SSP because only a Trusted Solaris SSP has the `ssp` role.
- From another Trusted Solaris workstation, perform a CDE remote login to the SSP. The SSP becomes the remote host on your local Trusted Solaris workstation. Then perform a CDE login to the SSP as a user who can assume the `ssp` role, and assume the `ssp` role. This method does not require the local Trusted Solaris

workstation to have the ssp role. You can use this method to access remotely the Trusted Solaris SSP from any local Trusted Solaris workstation. These methods also work for accessing the root role on the Trusted Solaris SSP. See “Remote Administration Options” in *Trusted Solaris Administrator's Procedures* for a full discussion of remote administration.

Domain Access Using Trusted Solaris Software

Solaris and Trusted Solaris domains can be accessed from the SSP console or from other workstations.

From the SSP Console

A Solaris domain can be logged into from a `netcon(1M)` session. Trusted Solaris does not support command line login, so a Trusted Solaris domain can not be logged into from a `netcon` session. The `netcon` window still receives the domain's console messages and can be used for OBP (OpenBoot Prom) commands.

To log in to a Trusted Solaris domain from an SSP console:

- From a Solaris SSP console, you can `rlogin(1)` as a user to the Trusted Solaris domain. However, you cannot access the root role on a Trusted Solaris domain from a Solaris SSP console.
- From a user workspace on a Trusted Solaris SSP console, you can `rlogin` as a user to the Trusted Solaris domain. For performing administrative tasks, you assume an administrative role on the Trusted Solaris SSP console, and then `rlogin` to the domain as the same role.

From Other Workstations

You can `rlogin` to a Solaris domain from a Solaris workstation. You can `rlogin(1)` as a user to the Trusted Solaris domain from a Solaris workstation. You cannot perform administrative tasks in a Trusted Solaris domain from a Solaris workstation, because you do not have access to any administrative roles.

To log in to a Trusted Solaris domain from a Trusted Solaris workstation:

- From a user workspace on a Trusted Solaris workstation, you can `rlogin` as a user to the Trusted Solaris domain. From an administrative role on a Trusted Solaris workstation (example: root role), you can `rlogin` to the domain as the same role. This method enables access to a Trusted Solaris domain when the Trusted Solaris SSP is not available.

- From another Trusted Solaris workstation, you can also perform a remote CDE login to the Trusted Solaris domain. The Trusted Solaris domain becomes the remote host on your local Trusted Solaris workstation. You can CDE login as a user to the domain and then assume roles. This method is useful when there is a spare Trusted Solaris workstation available. It is generally not desirable to do this using the Trusted Solaris SSP because it prevents the SSP from being used for SSP tasks.

Installation Options are Reduced

Trusted Solaris 7 installation does not fully support the following options offered by Solaris 7 installation software:

- WebStart. Trusted Solaris SSP 3.1.1 is installed from a CDROM.
- Upgrade. You cannot upgrade from the Solaris operating environment to the Trusted Solaris 7 operating environment. You cannot upgrade to Trusted Solaris 3.1.1 or to Trusted Solaris AP 2.2 from their Solaris versions.
- SSP Backup. Like its Solaris version, Trusted Solaris 3.1.1 can use the `ssp_restore` command to restore the SSP environment from a backup file created by the `ssp_backup` command on a Solaris SSP 3.1 or 3.1.1.
- NIS. Trusted Solaris 7 supports the NIS+ name service, not NIS.

Trusted Solaris Installation

The Trusted Solaris 7 operating environment must be installed and configured on the SSP workstation before the Trusted Solaris SSP 3.1.1 software is installed on it.

Trusted Solaris SSP Installation

Installing the Trusted Solaris 7 operating environment on the SSP is the same as installing Trusted Solaris 7 on a NIS+ client workstation or a NIS+ master server. Please see *Trusted Solaris Installation and Configuration* for details.

After the Trusted Solaris operating environment is installed and configured on the SSP, the Trusted Solaris version of SSP 3.1.1 software can be installed. See Chapter 3 for details.

After Trusted Solaris SSP 3.1.1 is installed, the Trusted Solaris version of AP 2.2 software can be installed. See Chapter 5 for details.

Trusted Solaris Domain Installation

Installation of the Trusted Solaris operating environment on a domain can be done using the Trusted Solaris SSP as the net install server. See Chapter 4 for details.

After the Trusted Solaris operating environment is installed and configured on the domain, the Trusted Solaris version of AP 2.2 software can be installed. See Chapter 5 for details.

Creating a Sun Enterprise 10000 System Running Trusted Solaris 7

The following are examples of creating recommended Trusted Solaris 7 configurations on a Sun Enterprise 10000:

- “A New Sun Enterprise 10000 Server with No Domains” on page 12
- “An Existing Sun Enterprise 10000 Server with Domains” on page 12

Note - The examples are very high level. Each site should create a detailed plan that best fits the site and site security requirements.

A New Sun Enterprise 10000 Server with No Domains

1. On the SSPs, install the Trusted Solaris 7 operating environment and Trusted Solaris SSP 3.1.1. If alternate pathing is required, install Trusted Solaris AP 2.2.
2. Create each domain and install the Trusted Solaris 7 operating environment on each. If alternate pathing is required, install Trusted Solaris AP 2.2.

An Existing Sun Enterprise 10000 Server with Domains

1. Back up the current SSP environment.
2. On the spare SSP, install the Trusted Solaris 7 operating environment and Trusted Solaris SSP 3.1.1. If alternate pathing is required, install Trusted Solaris AP 2.2. Restore the SSP environment on the spare SSP so that the spare is synchronized with the main SSP.
3. Switch the SSPs so that the main SSP is now running Trusted Solaris 7, Trusted Solaris SSP 3.1.1, and Trusted Solaris AP 2.2.
4. On the spare SSP, install the Trusted Solaris 7 operating environment and Trusted Solaris SSP 3.1.1. If alternate pathing is required, install Trusted Solaris AP 2.2. Restore the spare SSP environment so it is synchronized with the main SSP.
5. To convert each domain from Solaris software to Trusted Solaris 7, install the Trusted Solaris 7 operating environment on each domain. If alternate pathing is required, install Trusted Solaris AP 2.2.

Installing and Configuring the Trusted Solaris 7 Environment on the SSP

This chapter covers installing and configuring the Trusted Solaris 7 operating environment on the Sun Enterprise 10000 SSP. These steps are prerequisites to installing the Trusted Solaris SSP 3.1.1 on the SSP.

- “Back Up the SSP” on page 14
- “Install Trusted Solaris 7 on the SSP” on page 15
- “Configure the SSP Network” on page 15
- “Install the AnswerBook2 Server” on page 26

The procedures in this guide use the conventions shown in the following table for command line prompts.

TABLE 2-1 Command Line Prompt Conventions

Prompt	User Indicated
ssp#	root role on the SSP
ssp%	ssp role on the SSP
#	root role or superuser on a system other than the SSP

Back Up the SSP

Backing up an existing SSP is required if you want to retain the current SSP environment. The backup file must be created with the `ssp_backup` command on a Solaris SSP 3.1 or SSP 3.1.1 system; a SSP 3.0 backup file can not be restored to Trusted Solaris SSP 3.1.1. If you have a new system or you do not wish to restore the SSP environment after Trusted Solaris installation, you do not need to create backup file.

To determine what version of the SSP software is currently running, see your current SSP documentation.

▼ To Back Up the SSP Environment

Note - The size of the SSP backup file can range from approximately 4Mbytes to well over 80Mbytes, depending upon the contents of the `adm`, `data`, `etc`, `ict`, and `.ssp_private` directories in the `/var/opt/SUNWssp/` directory). You can use the `du(1M)` command to determine the approximate amount of disk space required for the backup file. Delete any unnecessary message or log files from the `/var/opt/SUNWssp/adm` directory prior to invoking `ssp_backup`.

1. On the main Solaris SSP, log in as superuser to create a backup file.

2. Run the `ssp_backup` command:

```
ssp# /opt/SUNWssp/bin/ssp_backup target_directory
```

The directory specified by `target_directory` must exist. This is the directory where the backup file, named `ssp_backup.cpio`, will be created. After `ssp_backup` is run, do not make any changes to the Sun Enterprise 10000 environment, such as domain state or power status of boards, until you have completed the install procedure and restored the SSP environment.

3. Save the `/target_directory/ssp_backup.cpio` file to a safe location.

This file will be used during installation of Trusted Solaris SSP 3.1.1 to restore the SSP environment on a single SSP system, or to synchronize the SSP environment between the SSPs on a dual SSP system.

Note - It is suggested that you also back up the SSP with `ufsdump(1M)` before the install. You can back up all of the files on the SSP using `usfdump`, instead of just the SSP configuration information that is backed up by `ssp_backup`. This backup can be used to restore the SSP in the event of a disk failure.

Install Trusted Solaris 7 on the SSP

Installation of the Trusted Solaris 7 operating environment on the SSP is same as installing it on a workstation that will be a NIS+ client.

See *Trusted Solaris Installation and Configuration Guide* for details.

Configure the SSP Network

After installing the Trusted Solaris operating environment on the SSP, you need to configure its SSP network files before installing the Trusted Solaris SSP 3.1.1 software.

Note - Configuring the network is very important. Complete it before installing the SSP 3.1.1 software.

This section describes the following SSP network configurations:

- “Two Subnets” on page 15
- “Three Subnets” on page 17
- “Spare SSP” on page 18

Two Subnets

The following table and figure describe the two-subnet network configuration.

TABLE 2-2 Two-Subnet Network Configuration

Subnet	Name	Description
Primary	Domain Subnet or dom_subnet	SSP and the domains
Second	Control Board Subnet or cb0_subnet	SSP and the control board

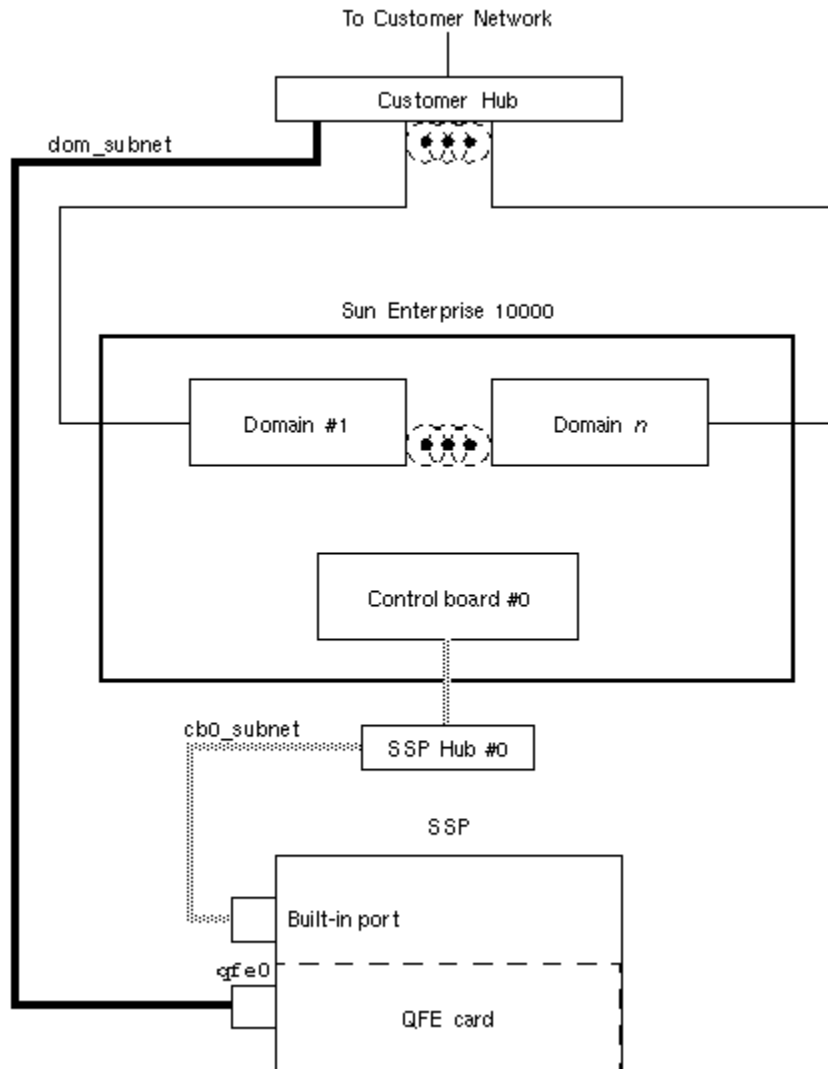


Figure 2-1 Two-Subnet Network Configuration

In Figure 2-1, the Built-in port is `le0` for a Sparcstation™ 5 and `hme0` for a Sun Ultra™ 5.

Three Subnets

The following table and figure describe the three-subnet network configuration.

TABLE 2-3 Three-Subnet Network Configuration

Subnet	Name	Description
Primary	Domain Subnet or <code>dom_subnet</code>	SSP and the domains
Second	Control Board Subnet 0 or <code>cb0_subnet</code>	SSP and the first control board
Third	Control Board Subnet 1 or <code>cb1_subnet</code>	SSP and the second control board

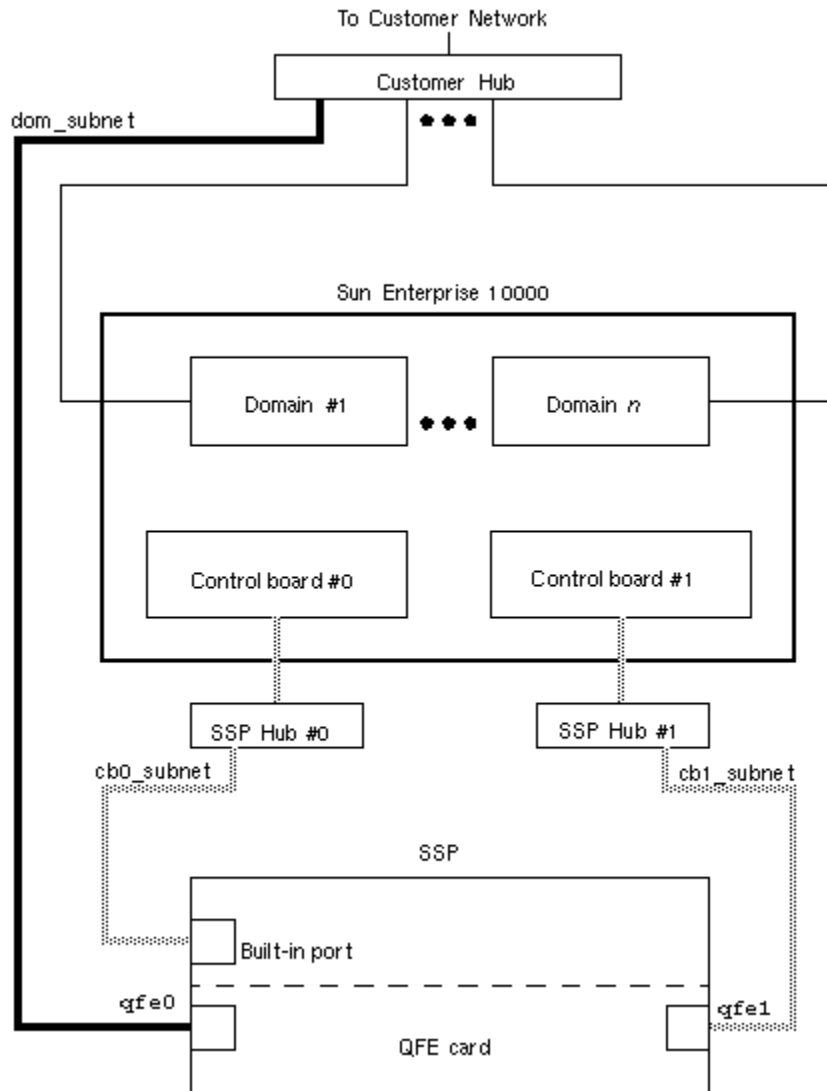


Figure 2-2 Three-Subnet Network Configuration

In Figure 2-2, the Built-in port is `le0` for a Sparcstation 5 and `hme0` for a Sun Ultra 5.

Spare SSP

The following table and figure describe the spare SSP network configuration.

TABLE 2-4 Spare SSP Network Configuration

Subnet	Name	Description
Primary	Domain Subnet or <code>dom_subnet</code>	Both SSPs and the domains
Second	Control Board Subnet 0 or <code>cb0_subnet</code>	Both SSPs and the first control board
Third	Control Board Subnet 1 or <code>cb1_subnet</code>	Both SSPs and the second control board

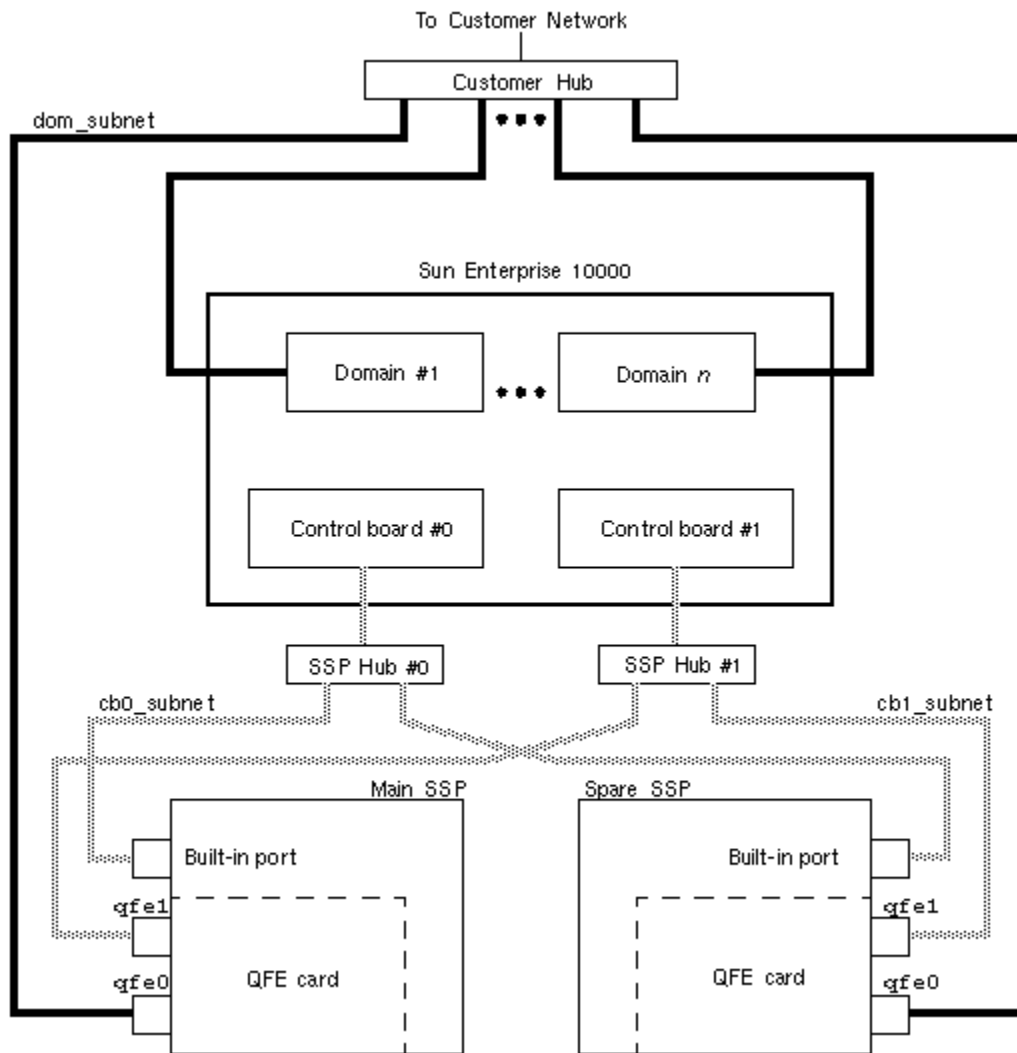


Figure 2-3 Spare SSP Network Configuration

In Figure 2-3, the Built-in port on the main SSP and the spare SSP is `le0` for a Sparcstation 5 and `hme0` for a Sun Ultra 5.

▼ To Configure Your SSP Network

This procedure provides instructions for configuring your SSP network in one of the three configurations discussed earlier in this chapter.

1. Log in to the SSP and assume the root role.

Do the following steps as root at the label `admin_low`.

2. Create the `/etc/hostname.*` configuration files.

If you need to view your network controllers, use `ifconfig -a`.

For example, if you are using a QuadFastEthernet™ (QFE) card, model 1049A, in the two-subnet, three-subnet, or spare SSP network configuration on a Sun Ultra 5, you need the following files:

- `/etc/hostname.qfe0` — contains the current SSP host name; it configures the primary subnet, `dom_subnet`.
- `/etc/hostname.hme0` — contains `ssp_hostname-hme0`; it configures the second subnet, `cb0_subnet`.

The following file is also needed if you are using either the three-subnet or spare SSP configuration:

- `/etc/hostname.qfe1` — contains `ssp_hostname-qfe1`; it configures the third subnet, `cb1_subnet`.

EXAMPLE 2-1 SSP with hostname `xf4-ssp`

File Name	File Contents
<code>/etc/hostname.qfe0</code>	<code>xf4-ssp</code>
<code>/etc/hostname.hme0</code>	<code>xf4-ssp-hme0</code>
<code>/etc/hostname.qfe1</code>	<code>xf4-ssp-qfe1</code>

3. Set the contents of the `defaultrouter` file to the IP address of the primary network interface:

```
ssp# echo primary_network_IP_address > /etc/defaultrouter
```

4. Manually update your name service `hosts` registry to include the host names and IP addresses of your control board(s) and other hosts, such as domains and the SSP.

This can involve updating the Network Information Service (NIS+), or the `/etc/hosts` file, or the Domain Name Service (DNS).

The following example shows the typical modifications for an `/etc/hosts` file:

```
# Internet host table
127.0.0.1  localhost
0.0.0.0    tsol_default
# Entries for dom_subnet.
www.xxx.yyy.zzz domain1_hostname
www.xxx.yyy.zzz domain2_hostname
```

```

...
www.xxx.yyy.zzz domainn_hostname(n is the number of domains)
#
# Entries on both ssp's.
# NOTE : On the spare SSP, make sure ``loghost``
# belongs to the spare.
#
www.xxx.yyy.zzz main_ssp_hostname loghost
www.xxx.yyy.zzz spare_ssp_hostname
#
# The next three entries need to be on cb0_subnet.
#
www.xxx.yyy.zzz main_ssp_hostname-hme0
www.xxx.yyy.zzz spare_ssp_hostname-hme0
www.xxx.yyy.zzz cb0_hostname
#
# The next three entries need to be on cb1_subnet.
#
www.xxx.yyy.zzz main_ssp_hostname-qfel
www.xxx.yyy.zzz spare_ssp_hostname-qfel
www.xxx.yyy.zzz cb1_hostname

```

Here is an example of a main SSP's `/etc/hosts` file. In this example, the SSP is configured as follows:

- `xf4` and `xf4-b3` are host domains.
- `xf4-ssp` is the main SSP and `xf4-ssp1` is the spare SSP.
- `xf4-cb0` and `xf4-cb1` are the host names for the two control boards.

```

#/etc/hosts
#
127.0.0.1 localhost
0.0.0.0 tsol_default
#dom_subnet (www.xxx.49.zzz). The 49 subnet
#
129.153.49.8 xf4
129.153.49.9 xf4-b3
129.153.49.113 xf4-ssp loghost
129.153.49.114 xf4-ssp1
#
#cb0_subnet (www.xxx.151.zzz). The 151 subnet
#
129.153.151.113 xf4-ssp-hme0
129.153.151.114 xf4-ssp1-hme0
129.153.151.123 xf4-cb0
#
#cb1_subnet (www.xxx.152.zzz). The 152 subnet
#
129.153.152.113 xf4-ssp-qfel
129.153.152.114 xf4-ssp1-qfel
129.153.152.127 xf4-cb1

```

The `/etc/hosts` file is a link to the `/etc/inet/hosts` file.

Note - The SSP and the host domains must be on the same subnet so you can boot domains from the network.

5. Manually update your name service `ethers` registry to include the Ethernet addresses for the domain(s), SSP(s), and control board(s).

You need to update NIS+, or the `/etc/ethers` file. For example:

```
08:00:20:ac:5b:ba      xf4-ssp
08:00:20:b0:64:78      xf4-ssp1
00:00:be:a6:55:88      xf4
00:00:be:a6:6f:89      xf4-b3
00.00.be.01.00.1e      xf4-cb0
00.00.be.01.00.57      xf4-cb1
```

Note - The Ethernet address of the control board(s) is located on the front of each control board.

6. Update the `tnrhdb(4)` file to indicate the template for the SSP(s), domain(s), control board(s) and interface(s).

You need to update the NIS+ `tnrhdb` table, or the `/etc/security/tsol/tnrhdb` file. For example, if the E10000 is configured as follows:

EXAMPLE 2-2 Tnrhdb Information for SSP xf4-ssp (129.153.49.113)

Main SSP	xf4-ssp (129.153.49.113)	
	Is running the Trusted Solaris 7 operating environment.	
Interfaces	xf4-ssp-hme0 (129.153.151.113)	
	xf4-ssp-qfe1 (129.153.152.113)	
Spare SSP	xf4-ssp1 (129.153.49.114)	
	Is running the Trusted Solaris 7 operating environment.	
Interfaces	xf4-ssp1-hme0 (129.153.151.114)	
	xf4-ssp1-qfe1 (129.153.152.114)	

Domain1	xf4 (129.153.49.8)
	Is running the Trusted Solaris 7 operating environment.
Domain2	xf4-b3 (129.153.49.9)
	Is running the Solaris 7 operating environment.
Control boards	xf4-cb0 (129.153.151.123)
	xf4-cb1 (129.153.152.127)

1. Its `tnrhdb` file or NIS+ table has the following entries:

```
# /etc/security/tsol/tnrhdb
#
# Assume that template unlab and tsol is defined in the tnrtpt database.
#
127.0.0.1:tsol
0.0.0.0:unlab
129.153.49.113:tsol
129.153.151.113:tsol
129.153.152.113:tsol
129.153.49.114:tsol
129.153.151.114:tsol
129.153.152.114:tsol
129.153.49.8:tsol
129.153.49.9:unlab
129.153.151.123:unlab
129.153.152.127:unlab
```

2. If there are other Solaris or Trusted Solaris machines that the SSP needs to communicate with, they also need to be viewed by the SSP using the correct template. This would require additional entries in this `/etc/security/tsol/tnhdb` file.
3. Depending on the site's configuration, you might also need to update `tnrhdb` files on other Trusted Solaris machines so that they can communicate with the freshly installed SSP using the correct template.

7. Update the `/etc/inet/netmasks` file.

If the `netmasks` file does not contain the netmask for all the network numbers used in the `/etc/inet` file.

For example, if the `/etc/hosts` file defines the control boards to be:

```
10.100.100.100  ctrl_brd_0
10.100.101.100  ctrl_brd_1
```


The `/etc/inet/netmasks` file would need to have an entry:

```
10.100.0.0      255.255.255.0
```

8. Update the `/etc/default/login` file to allow remote login to the root role from any workstation.

Comment out the `CONSOLE=/dev/console` line in the `/etc/default/login` file, as in:

```
#CONSOLE=/dev/console
```

Requirements for remote login are discussed in greater detail in “Remote Administration Options” in *Trusted Solaris Administrator's Procedures*.

9. Edit the `/etc/nsswitch.conf` file on the main SSP and the spare SSP.

If you are using local configuration files, the lines in the `/etc/nsswitch.conf` files are similar to the following example:

```
hosts:      files
ethers:     files
netmasks:  files
bootparams: files
netmasks:  files
tnrhttp:   files
tnrhdb:    files
tsoluser:  files
tsolprof:  files
```

For NIS+, the lines in the file are similar to the following example:

```
hosts:      files nisplus
ethers:     files nisplus
netmasks:  files nisplus
bootparams: files nisplus
tnrhttp:   nisplus files
tnrhdb:    nisplus files
tsoluser:  nisplus files
tsolprof:  files nisplus
```

Note - The name server information (NIS+) is dependent on your network configuration.

Install the AnswerBook2 Server

You will need the server to be able to view books in the SSP 3.1.1 AnswerBook2™ collection.

If you have not installed the AnswerBook2 server, or are not sure if you have, at a minimum, version 3.0, you can check the version of the AnswerBook2 server as described in the following procedure.

▼ To Check the AnswerBook2 Server Version

1. On a Trusted Solaris SSP, assume the root role.

2. Type:

```
ssp# pkginfo -l SUNWab2r
```

If your version of the AnswerBook2 server is earlier than version 3.0, you must re-install it.

Note - It is suggested that you install the AnswerBook2 server on a system other than the SSP.

If you have installed the AnswerBook2 server on another system, you can install the SSP 3.1.1 AnswerBook2 package on the SSP and add the SSP 3.1.1 AnswerBook2 to the AnswerBook2 index by using the `ab2admin(1M)` command.

If you do not have the AnswerBook2 server installed on any system, or if you have a version earlier than 3.0, you can install the AnswerBook2 server from the Solaris Documentation CD or from the Web. To install the AnswerBook2 server from the Solaris Documentation CD, refer to the *Installation Library* for your version of the Solaris operating environment. To install the AnswerBook2 server from the Web, follow the steps in the procedure below.

▼ To Install the AnswerBook2 Server From the Web

1. **On a Trusted Solaris SSP, assume the root role.**
2. **Point your browser to `http://www.sun.com/software/ab2`.**
3. **Click Download Versions.**
4. **Click Download Version 1.4.**
5. **Read the License Agreement and click on the Accept button.**
You cannot download the software if you do not accept the License Agreement.
6. **Read the Export Agreement and click on the Accept button.**
You cannot download the software if you do not accept the Export Agreement.
7. **Choose the version of the AnswerBook2 server that is appropriate for the operating environment on your system.**
 - If your system is running the Trusted Solaris 7 operating environment, or the Solaris 2.6 or 7 operating environment, click `Solaris 2.6` or `Solaris 7 Operating Environment`.
8. **Follow the instructions on the web page to download the software and install the AnswerBook2 server.**

Installing and Configuring the Trusted Solaris SSP 3.1.1

After the Trusted Solaris 7 operating environment is installed and configured on the SSP and the SSP network is configured, the Trusted Solaris version of SSP 3.1.1 software can be installed. The procedures in this chapter require that you have completed the steps in Chapter 2. This chapter describes the following topics:

- “Installing from a CDROM” on page 29
- “Installing a Dual SSP Configuration” on page 32
- “Installing a Single SSP Configuration” on page 38
- “Entering System Information in the Trusted Solaris 3.1.1 Environment” on page 41
- “Configuring Trusted Solaris SSP 3.1.1” on page 43

Installing from a CDROM

To install the Trusted Solaris version of SSP 3.1.1 shipped on the Trusted Solaris Supplemental CD, you need to set up the CDROM. The following set of procedures properly allocates and mounts the CDROM for installing the Trusted Solaris SSP 3.1.1 software.

- “Prepare the CDROM Device” on page 30
- “Add the `/cdrom/root/Tools/ssp_install` Command to the Custom Root Role Profile” on page 31
- “Check the `tsolprof` Setting in the `nsswitch.conf` File” on page 32
- “Assume the root Role with the New Profile” on page 32

▼ Prepare the CDROM Device

1. Log in as a user on the SSP that can assume the root and secadmin roles. Assume the root role.
2. In the root role, at label `admin_low`, use the Device Allocation Manager to allocate the CDROM drive, but do not mount it.
Do not try to use the Volume Manager; it is disabled in the Trusted Solaris environment.
 - a. Click the triangle above the Style Manager on the Front Panel to display the Trusted Desktop subpanel. Click Device Allocation.
 - b. Double-click the CDROM device to move it to the Allocated Devices list.
 - c. Write down the device name for the CDROM drive as indicated in the "Insert disk into..." message in the Device Allocation window.
For example, if the message reads:

```
Insert disk into /dev/dsk/c0t2d0s0.  
Make sure disk is labeled ADMIN_LOW [ADMIN_LOW].  
Press RETURN when cdrom_0 is ready, or ^C to cancel.
```


then write down the device name, `/dev/dsk/c0t2d0s0`, before continuing.
 - d. Insert the Trusted Solaris Supplemental CD into the CDROM drive and press the Return key.
 - e. Answer **n** to the Do you want `cdrom_0` mounted: (y/n)? **n** question.

Note - This differs from the instructions in *Trusted Solaris Installation and Configuration*. Follow these instructions: do not mount the CDROM.

3. In the root role, at label `admin_low`, make sure that `/cdrom/root` exists.
If it does not, create it:

```
ssp# mkdir -p /cdrom/root
```

4. Mount the CDROM with all allowed and forced privileges.

```
ssp# mount -F hsfs -o ro -S "allowed=all;forced=all" cdrom_device /cdrom/root
```

For example, for the CDROM on device `/dev/dsk/c0t2d0s0`, type:

```
ssp# mount -F hsfs -o ro -S "allowed=all;forced=all" \  
/dev/dsk/c0t2d0s0 /cdrom/root
```

5. Check that the mount succeeded with the `df(1M)` command:

```
ssp# df -k grep | cdrom  
/dev/dsk/c0t2d0s0 544100 544100 0 100% /cdrom/root
```

▼ Add the `/cdrom/root/Tools/ssp_install` Command to the Custom Root Role Profile

This procedure requires that the CDROM has been mounted as described in “Prepare the CDROM Device” on page 30.

1. Assume the `secadmin` role. At label `admin_low`, open the Profile Manager application.
2. In the Profile Manager: Load window, select `none` for Name Service then click the OK button.
3. In the Profile Manager: Open window select Custom Root Role then click the Modify button.
4. In the Profile Manager main window, select View from the menu bar then select Commands from the submenu.
5. Enter `/cdrom/root/Tools` in the Pathname: box, then click the Add button next to it.
You should see `/cdrom/root/Tools` added to the Exclude list.
6. Click on `/cdrom/root/Tools` in the Exclude list.
It expands to display all the commands available in the `/cdrom/root/Tools` directory.
7. Select command `ssp_install` and add it to the Include list.
8. Click on the Privileges... button and select ALL privileges for the `ssp_install` command.

9. **Select Profiles from the Profile Manager main window menu bar then select Save Profile from the submenu to save the Custom Root Role profile.**

For more details on adding commands to role's profile, see "To Add a Command to a Role's Profile" section in *Trusted Solaris Installation and Configuration*.

▼ Check the tsolprof Setting in the nsswitch.conf File

1. **Assume the root role. In the root role, make sure that the tsolprof entry in the /etc/nsswitch.conf file has files as its first value:**

```
tsolprof: files nisplus
```

▼ Assume the root Role with the New Profile

1. **Go to the workspace of the user who can assume the root role.**
2. **Delete the root role workspace.**
3. **Assume the root role again.**
This action re-reads the root role's profiles. The Custom Root Role profile with your changes is now in effect.
4. **In the root role, at label admin_low, issue the clist(1M) command to verify that the command /cdrom/root/Tools/ssp_install is available.**

```
ssp# clist -p | grep /cdrom/root/Tools/ssp_install  
/cdrom/root/Tools/ssp_install: all
```

The list should indicate all, which means all privileges.

Installing a Dual SSP Configuration

The following table shows the supported combinations of SSP software for dual SSP configurations:

TABLE 3-1 Supported Dual SSP Configurations

SSP version on the Main SSP	SSP Version on the Spare SSP
3.1	3.1 or 3.1.1
3.1.1	3.1 or 3.1.1

▼ To Install Trusted Solaris SSP 3.1.1 on the Spare SSP

1. On the spare SSP (referred to here as SSP2), log in as a user who can assume the root and secadmin roles. Assume the root role.
2. As root at label `admin_low`, perform “Installing from a CDROM” on page 29 if you have not done so.

3. Change directory to the `Tools` directory:

```
ssp# cd /cdrom/root/Tools
```

4. Install the Trusted Solaris SSP 3.1.1 software on SSP2 by typing:

```
ssp# ./ssp_install pathname
```

Where *pathname* specifies the path to the `Product` directory, `/cdrom/root/Product`.

5. When you are asked if you want to install the SSP 3.1.1 AnswerBook (the `SUNWuessp` package), type `y` to install it; otherwise, type `n`.

If you install the SSP 3.1.1 Answerbook, you must respond to the following prompts:

- a. When you are requested to select an installation option, type 2 (heavy installation): `Select an installation option: 2`
- b. When requested to specify the parent path for the AnswerBook2 Collection, type the path to the directory in which you want to put the SSP 3.1.1 AnswerBook.

It is suggested that you install it in /opt.
Specify the parent path of this AnswerBook2 Collection directory:
/opt

c. Type y at this prompt:

This package contains scripts which will be executed with superuser permission during the process of installing this package.

Do you want to continue with the installation of <SUNWuessp> [y,n,?] **y**

6. When you are asked if you want to install the SUNWsspfp package, type y to the prompts.

Do you want to install the SUNWsspfp package? (y/n) **y**
This package contains scripts which will be executed with superuser permission during the process of installing this package.

Do you want to continue with the installation of <SUNWsspfp> [y,n,?] **y**

- 7. Remove the /cdrom/root/Tools/ssp_install command from the Custom Root Role profile.**
 - a. Assume the secadmin role. At label admin_low, open the Profile Manager application.**
 - b. In the Profile Manager: Load window, select none for the Name Service then click the OK button.**
 - c. In the Profile Manager: Open window select Custom Root Role, then click the Modify button.**
 - d. In the Profile Manager main window, select View from the menu bar, then select Commands from the submenu.**
 - e. Select the /cdrom/root/Tools/ssp_install command from the Include list and move it to the Exclude list.**
 - f. Select Profiles from the Profile Manager main window menu bar then select Save Profile from the submenu to save the profile.**

For more details on removing commands from a role's profile, see "To Remove a Command from a Role's Profile" section in *Trusted Solaris Installation and Configuration*.

8. Assume the root role, at label `admin_low` to unmount `/cdrom/root` using the following command:

```
ssp# umount /cdrom/root
```

9. In the root role, at label `admin_low`, use the Device Allocation Manager to deallocate the CDROM drive. Remove the CDROM.
Do not use the Volume Manager, it is disabled in the Trusted Solaris environment.

10. If you have a backup file from the main SSP, restore it on SSP2.

- a. In the root role, at label `admin_low`, copy the `ssp_backup.cpio` file to a backup directory on SSP2.

- b. Type:

```
ssp# /opt/SUNWssp/bin/ssp_restore \  
backup_directory/ssp_backup.cpio
```

Where *backup_directory* is the directory to which you copied the `ssp_backup.cpio` file in Step 10 on page 35. This restores the SSP environment on the spare SSP.

11. Configure the main SSP (referred to here as SSP1) to be a spare SSP using `ssp_config(1M)`.

- a. On SSP1, log in as superuser if SSP1 is running Solaris software. If SSP1 is running Trusted Solaris software, log in as a user who can assume the root role, and assume it.

- b. Type:

```
ssp# /opt/SUNWssp/bin/ssp_config  
Beginning setup of this workstation to act as a MAIN or SPARE SSP.  
Are you currently configuring the MAIN SSP? (y/n)n  
SPARE SSP configuration completed.
```

- c. If SSP1 is currently running SSP 3.1, kill the `rarpd` process:

```
ssp# ps -ef | grep rarpd
ssp# kill -9 rarpd_pid
```

Where *rarpd_pid* is the process ID shown by the `ps` command for `rarpd`. Killing the `rarpd` process prevents the SSP from responding to control board boot requests.

12. Change SSP2 to be the main SSP.

- a. On SSP2, log in as a user who can assume the root role, and assume it.
- b. Type:

```
ssp# /opt/SUNWssp/bin/ssp_config
Beginning setup of this workstation to act as a MAIN or SPARE SSP.
Are you currently configuring the MAIN SSP? (y/n)y
MAIN SSP configuration completed.
```

If you did not restore the SSP environment during the install procedure, you will be prompted for system information. See “To Name the Platform and Control Board” on page 41 for details.

13. Reboot SSP2.

14. Log in as the user `install` who can assume the role `ssp` on SSP2. The password for `install` is `install`.

The installation of Trusted Solaris SSP 3.1.1 created the `ssp` role, and assigned the `ssp` role to the `install` user.

15. Assume the role `ssp`. The password for the `ssp` role is `ssp`.

16. In the `ssp` role, open a terminal window and check the log message:

```
ssp% tail -f $SSPLOGGER/messages
```

Wait for the “Startup of SSP programs complete” message.

17. On each domain, perform the following steps as root.

If the domain is running Trusted Solaris software, the following steps need to be run from the root role. See Step 1 on page 70 for how to access a Trusted Solaris domain from the root role.

If the domain is running Solaris software, you can get to the domain's root user via `netcon(1M)` then logging in as root.

- a. **Edit the `/etc/ssphostname` file to replace the host name of SSP1 with the host name of SSP2.**

- b. **Switch console communication from SSP1 to SSP2.**

If the domain is running Trusted Solaris 7 or Solaris 7 5/99 release or later, issue the following:

```
# /etc/init.d/cvc stop
# /etc/init.d/cvc start
```

If the domain is running Solaris 2.5, 2.6 or the Solaris 7 3/99 release or earlier, issue the following:

```
# ps -ef | grep cvcd
# kill -9 cvcd_pid
# cvcd_path/cvcd
```

where *cvcd_path* is `/sbin` under the Solaris 2.5 and 2.6 operating environments, and *cvcd_path* is `/platform/SUNW,Ultra-Enterprise-10000/lib/cvcd` under the Solaris 7 operating environment.

18. On the SSP2, perform the steps in “Configuring Trusted Solaris SSP 3.1.1” on page 43.

19. If alternate pathing is desired on install the Trusted Solaris AP 2.2 as described in Chapter 5.

20. After SSP2 is installed and configured, you can install SSP1.

- a. **Install Trusted Solaris 7, Trusted Solaris SSP 3.1.1, and Trusted Solaris AP 2.2 on SSP1.**
- b. **If you have made changes to the SSP environment or SSP2, synchronize the two SSPs using new backup files.**
 - i. **In the root role at label `admin_low`, create a backup file on SSP2.**

```
ssp# /opt/SUNWssp/bin/ssp_backup target_directory
```

- ii. In the root role at label `admin_low`, restore the backup file on SSP1.

```
ssp# /opt/SUNWssp/bin/ssp_restore \
    backup_directory/ssp_backup.cpio
```

Installing a Single SSP Configuration

▼ To Install Trusted Solaris SSP 3.1.1 on the Main SSP

1. Log in as a user who can assume the root and secadmin roles. Assume the root role.
2. As root at label `admin_low`, perform “Installing from a CDROM” on page 29 if you have not done so.
3. Change directory to the `Tools` directory:

```
ssp# cd /cdrom/root/Tools
```

4. Install the Trusted Solaris SSP 3.1.1. software by typing:

```
ssp# ./ssp_install pathname
```

Where *pathname* is the path to the `Product` directory, `/cdrom/root/Product`.

5. When you are asked if you want to install the SSP 3.1.1 AnswerBook (the `SUNWuessp` package), type `y` to install it; otherwise, type `n`.
If you install the SSP 3.1.1 Answerbook, you must respond to the following prompts:

- a. **When you are requested to select an installation option, type 2 (heavy installation):** Select an installation option: 2
- b. **When requested to specify the parent path for the AnswerBook2 Collection, type the path to the directory in which you want to put the SSP 3.1.1 AnswerBook.**
It is suggested that you install it in /opt.

Specify the parent path of this AnswerBook2 Collection directory: /opt

- c. **Type y at this prompt:**

This package contains scripts which will be executed with superuser permission during the process of installing this package.

Do you want to continue with the installation of <SUNWuessp> [y,n,?] y

6. **When you are asked if you want to install the SUNWsspfp package, type y to the prompts.**

Do you want to install the SUNWsspfp package? (y/n) y

This package contains scripts which will be executed with superuser permissions during the process of installing this package.

Do you want to continue with the installation of <SUNWsspfp> [y,n,?] y

7. **Remove the /cdrom/root/Tools/ssp_install command from the Custom Root Role profile.**
 - a. **Assume the secadmin role. At label admin_low, open the Profile Manager application.**
 - b. **In the Profile Manager: Load window, select none for Name Service then click the OK button.**

- c. In the Profile Manager: Open window select Custom Root Role, then click the Modify button.
 - d. In the Profile Manager main window, select View from the menu bar, then select Commands from the submenu.
 - e. Select the `/cdrom/root/Tools/ssp_install` command from the Include list and move it to the Exclude list.
 - f. Select Profiles from the Profile Manager main window menu bar then select Save Profile from the submenu to save the profile.
8. Assume the root role, at label `admin_low` to unmount `/cdrom/root` using the following command:

```
ssp# umount /cdrom/root
```

9. In the root role, at label `admin_low`, use the Device Allocation Manager to deallocate the CDROM drive. Remove the CDROM.
Do not use the Volume Manager, it is disabled in the Trusted Solaris environment.
10. If you have a backup file of the SSP environment, restore it.
- a. In the root role, at label `admin_low`, copy the `ssp_backup.cpio` file to a backup directory on SSP1.
 - b. Type:

```
ssp# /opt/SUNWssp/bin/ssp_restore backup_directory/ssp_backup.cpio
```

Where *backup_directory* is the directory to which you copied the `ssp_backup.cpio` file in Step 10 on page 40.
This restores the SSP environment on SSP1.

11. Type:

```
ssp# /opt/SUNWssp/bin/ssp_config
Beginning setup of this workstation to act as a MAIN or SPARE SSP.
Are you currently configuring the MAIN SSP? (y/n) y
```

(continued)

MAIN SSP configuration completed.

If you did not perform a restore in Step 10 on page 40, you will need to provide system information. See “To Name the Platform and Control Board” on page 41 for more information.

12. Reboot the SSP.

13. To configure Trusted Solaris SSP 3.1.1 on the SSP, perform the steps in “Configuring Trusted Solaris SSP 3.1.1” on page 43.

14. If alternate pathing is desired on the SSP, install the Trusted Solaris AP 2.2 as described in Chapter 5.

Entering System Information in the Trusted Solaris 3.1.1 Environment

▼ To Name the Platform and Control Board

If you did not restore the SSP environment during the install procedure, you will be prompted for system information when running the `/opt/SUNWssp/bin/ssp_config` command for the main SSP, or during the reboot of the SSP.



Caution - If you are rebooting, you *must* be at the SSP workstation console to see the messages described in this section. You cannot see these messages or perform these steps from a remote login session.

1. Specify the processor speed by typing in the corresponding number:

- 1 for 250 MHz processors
- 2 for 336 MHz processors
- 3 for 400 MHz processors
- 4 for 500 MHz processors
- 5 for Unlisted (manually enter clock values)

If you have a mixture of processors, select the number corresponding to the lowest processor speed. You are prompted to confirm your selection.

2. Enter the name of the platform this SSP will service.

The platform name is simply a name by which the SSP software refers to the entire Sun Enterprise 10000 host. The platform name is *not* the host name of a domain. A domain name can be the same as the platform name, but it is not recommended.

Note - The term *starfire* is reserved and cannot be used as the platform name.

Note - If you make a mistake during this configuration session, continue to the end of the prompts where you will be given an opportunity to correct any errors.

3. Define the host control boards.

For each control board slot, indicate whether there is a control board present and the host name for the respective control board (host names are in the `/etc/hosts` file). If the IP address for a control board is not found, you will be prompted for this information. If two control boards are present, you will be asked which control board is the primary (active) control board.

Here is a representative session:

```
Do you have a control board 0? (y/n)y
Please enter the host name of the control board 0 [allxf4cb0]: xf4-cb0
Do you have a control board 1? (y/n)y
Please enter the host name of the control board 1 [allxf4cb1]: xf4-cb1

Please identify the primary control board.

Is Control Board 0 [xf4-cb0] the primary? (y/n)y

Platform name      = allxf4
Control board 0 = xf4-cb0 => 129.153.151.123
Control board 1 = xf4-cb1 => 129.153.152.123
Primary Control Board = 0

Is this correct? (y/n)y
```

You are prompted to indicate whether this is a main SSP or spare SSP:

```
Are you currently configuring the MAIN SSP? (y/n) y
```

When the upgrade is complete, the following message is displayed:

```
MAIN SSP configuration completed.
```

Configuring Trusted Solaris SSP 3.1.1

After you have completed installing Trusted Solaris SSP 3.1.1, you need to check the version of the flash PROM and upgrade if necessary. For SSP 3.1.1, you must upgrade your flash PROM if the version is earlier than 3.46. See “Checking and Upgrading the Control Board Flash PROM” on page 43 below.

You may also need to:

- Edit some of the initialization files in the `/export/home/ssp` directory. If you made changes to the files, did not restore the environment during the install, and want to retain your changes, see “Editing Initialization Files” on page 44.
- Configure the Network Time Protocol Daemon. See “Configuring the Network Time Protocol Daemon” on page 45.
- Create a user on the SSP who can assume the `ssp`, `root`, `admin`, and `secadmin` roles. See “Creating a User for the SSP Administrator” on page 46.

Checking and Upgrading the Control Board Flash PROM

You need to have the correct version of the flash PROM boot firmware installed on the control boards; the boot firmware is required to download the control board executive (CBE). You must upgrade if the version is earlier than 3.46.

▼ To Check the Flash PROM Version

1. Log in as a user and assume the `ssp` role on the main SSP.
2. Check the version of the flash PROM on your control boards by typing:

```
ssp% cb_prom -r -h control_board_name
```

```
Checking PROM revision...3.44
```

where *control_board_name* is the name of the control board as specified in the `/etc/hosts` configuration file.

If the version displayed is earlier than 3.46, you must update the flash PROM. To do this, you must upgrade the PROM as described in the following procedure.

▼ To Upgrade the PROM

1. Type:

```
ssp% cb_prom -p /opt/SUNWssp/cbobjs/flash_boot.ima -h \
control_board_name
Programming PROM...complete.
```

2. To have the PROM change take effect, type:

```
ssp% cb_reset

Resetting host xf4-cb0...
Resetting host xf4-cb1...
xf4-cb1 is ready...
xf4-cb0 is ready...
```

where `xf4-cb1` and `xf4-cb0` are replaced with the names of the control boards for your system.

3. Verify the PROM version by typing:

```
ssp% cb_prom -r -h control_board_name
Checking PROM revision...3.46
```

where *control_board_name* is the name of the control board as specified in the `/etc/hosts` configuration file. The version shown should be 3.46.

Editing Initialization Files

When you run the `ssp_restore` command, the following files are copied and saved with a `.__upgrade` suffix. If you have made changes to these files, you can incorporate these changes into the new versions of the files when you have completed the install procedure.

The default `blacklist(4)` file found in `/var/opt/SUNWssp/etc` is backed up by `ssp_backup` and restored by `ssp_restore`. However, if you have created a `.postrc` file that changes the location of the `blacklist` file, the relocated `blacklist` file is not backed up by `ssp_backup`.

The following files are copied and saved when you run `ssp_restore`.

- `/export/home/ssp/.Xdefaults`
- `/export/home/ssp/.openwin-menu`
- `/export/home/ssp/.xinitrc`
- `/export/home/ssp/.drtclrc`
- `/export/home/ssp/.openwin-init`
- `/export/home/ssp/.openwin-menu-ssp`
- `/export/home/ssp/.redxrc`
- `/export/home/ssp/.cshrc`
- `/export/home/ssp/.login`
- `/export/home/ssp/.postrc`
- `/var/opt/SUNWssp/.ssp_private/ssp_resource`
- `/var/opt/SUNWssp/adm/.logger`
- `/export/home/ssp/.ssp_env`
- `/export/home/ssp/.dtprofile`
- `/export/home/ssp/.dt/dtwmrc`
- `/export/home/ssp/.dt/user.dtwmrc`
- `/export/home/ssp/.Xdefaults-ssp-hostname`
- `/export/home/ssp/.profile`

If you made changes to the `Ultra-Enterprise-10000.snmpd.cnf` file that is in the `/etc/opt/SUNWssp/snmp/agt` directory, you will have to incorporate your changes into the file installed on the restored system.

Note - No copy is made if a file does not exist.

Configuring the Network Time Protocol Daemon

The NTP daemon, `ntpd(1M)`, provides a mechanism for keeping the time settings synchronized between the SSP and the domains. OBP obtains the time from the SSP when the domain is booted, and NTP keeps the time synchronized from that point on.

The configuration is based on information provided by the system administrator. If you are not currently running in an NTP subnet, and you do not have access to the Internet, and you are not going to use a radio clock, you can set up the Sun Enterprise 10000 system to use its own internal time-of-day clock as the reference clock. Usually, however, the SSP uses its internal time-of-day clock for the Sun Enterprise 10000 system.

The NTP packages are compiled with support for a local reference clock. This means that your system can poll itself for the time instead of polling another system or network clock. The poll is done through the network loopback interface. The first three numbers in the IP address are 127.127.1. The last numbers in the IP address are the NTP stratum to use for the clock.

When setting up a Sun Enterprise 10000 system and its SSP, set the SSP to stratum 4. Set up the Sun Enterprise 10000 system as a peer to the SSP and set the local clock two strata higher.

If the `ntp.conf` file does not exist, create it as described in the following procedure.

▼ To Create the `ntp.conf` File

1. On the SSP, log in as a user who can assume the root role and assume it.
2. Create the `/etc/inet/ntp.conf` file in a text editor.

You must have an `ntp.conf` file on both the SSP and the platform. The following is an example of server/peer lines in the `/etc/inet/ntp.conf` file on the SSP.

```
server 127.127.1.4
```

You can add lines similar to the following to the `/etc/inet/ntp.conf` file on the platform:

```
server ssp_name
server 127.127.1.13
fudge 127.127.1.13 stratum 13
```

For more information on the NTP daemon, refer to the *Network Time Protocol User's Guide* and the *NTP Reference*.

Creating a User for the SSP Administrator

The installation of Trusted Solaris SSP 3.1.1 enabled the user `install` to assume the `ssp` role. This was done to make it easier to do the rest of the SSP 3.1.1 installation and configuration procedures. However, the user `install` is not a normal user and should not be used as such. It is highly recommended that a normal user be created for the SSP administrator's login. This user should be able to assume the `ssp`, `root`, `admin` and `secadmin` roles. For more information on creating a user, see "Using the User Manager to Configure Accounts" in *Trusted Solaris Administrator's Procedures*.

Trusted Solaris 7 on a Sun Enterprise 10000 Domain

This chapter describes the installation and configuration of Trusted Solaris 7 software on a Sun Enterprise 10000 domain. The procedures given in this chapter assume that the main SSP is running Trusted Solaris 7 and Trusted Solaris SSP 3.1.1.

Note - Please read the entire chapter carefully and make sure you understand the steps before you start the installation.

What You Need to Start

You need to be very familiar with your site configuration and with the configuration of the server before you start an install. Some of the information is in the server configuration files; however, site configuration information must be gotten from the site administrator. The following list contains references to information that you must have to complete the installation:

- IP address for the new domain
- IP address and host name of the main SSP
- Logical name of the boot device in the form cxtxdxx

Creating a Domain

This section contains instructions on how to create a new domain. The entire procedure includes the following tasks:

- Creating the `eeeprom.image` file for the new domain
- Creating the new domain on the SSP

Once a domain is created, you can install Trusted Solaris by performing the procedures in “Installing Trusted Solaris 7 on a Domain” on page 52.

You must have the system identification key and the host ID *before* you perform the following instructions. You can obtain the key and ID from your service provider. This key is used to generate an `eeeprom.image` file.

▼ To Create the `eeeprom.image` File

1. Log in as a user to the SSP and assume the `ssp` role.
2. If prompted for the `SUNW_HOSTNAME` variable, use either the platform name or the name of any existing domain.
If not prompted for the `SUNW_HOSTNAME` variable, it will default to the platform name.
3. Use the `sys_id(1M)` command to create the `eeeprom.image` file.

```
ssp% sys_id -h hostid -k key \  
-f $SSPVAR/.ssp_private/eeeprom_save/eeeprom.image.domain_name
```

Where *hostid* is the number provided with the key in the form of `0x80A66xxx`, *key* is the EEPROM key number, and *domain_name* is the hostname of the new domain.

Note - All *key* and *hostid* numbers are case-sensitive and must be entered exactly as they are received.

4. Execute the following `sys_id(1M)` command to check the results.

```
ssp% sys_id -d -f \  
$SSPVAR/.ssp_private/eeeprom_save/eeeprom.image.domain_name
```

In the following example, 49933C54C64C858CD4CF is the *key* and 0x80a66e05 is the *hostid*:

```
ssp% sys_id -h 0x80a66e05 49933C54C64C858CD4CF \  
-f $SSPVAR/.ssp_private/eeeprom_save/eeeprom.image.domain_name  
ssp% sys_id -d -f $SSPVAR/.ssp_private/eeeprom_save/ \  
eeeprom.image.domain_name
```

IDPROM in eeeprom.image.domain_name

```
Format = 0x01  
Machine Type = 0x80  
Ethernet Address = 0:0:be:a6:6e:5  
Manufacturing Date = Wed Dec 31 16:00:00 1997  
Serial number (machine ID) = 0xa66e05  
Checksum = 0x3f
```

5. **Back up the SSP eeeprom.image files to tape or disk where they can be accessed in case of an SSP boot-disk failure.**

You are done creating the eeeprom.image file for the domain. You can now create the new domain on the SSP, as described in the following section.

▼ To Create a New Domain on the SSP

1. **Log in as a user to the SSP and assume the ssp role.**
2. **If prompted for the SUNW_HOSTNAME variable, specify the name of the domain that you wish to create.**

If not prompted for the SUNW_HOSTNAME variable, it will default to the platform name. Use the domain_switch(1M) command to change SUNW_HOSTNAME to the name of the domain that you wish to create:

```
ssp% domain_switch domain-name
```

Ensure that the domain name corresponds with the hostname of the domain in which the operating system is to be installed. Domain names cannot be longer than 14 characters.

3. Use the `domain_create(1M)` command to create the domain.

```
ssp% domain_create -d domain_name -b board_numbers -o \
OS_version -p platform_name
```

Where *domain_name* is the name of the domain specified in Step 2 on page 51, *board_numbers* is a list of the system boards, delimited by spaces, to be included in the domain, *OS_version* is the version of the domain's operating system (for Trusted Solaris 7, use 5.7), and *platform_name* is the name of the platform as defined during the SSP package configuration.

4. Check the power to the domain.

```
ssp% power
```

The output of the `power` command depends greatly on the configuration of the server. If you are unfamiliar with the output, refer to the `power(1M)` man page for an explanation, or contact your service provider for an explanation of the output.

5. If you have determined that elements of the domain are powered off, power on those elements.

```
ssp% power -on
```

You are done creating the domain. You can now install the Trusted Solaris 7 operating environment on the domain, as described in the following section.

Installing Trusted Solaris 7 on a Domain

This section describes how to install the Trusted Solaris operating environment on a domain. The installation includes the following tasks:

- Configuring the domain network information on the SSP
- Setting up the SSP as the net install server

- Bringing up the domain
- Configuring the OBP environment
- Installing the Trusted Solaris operating environment
- Configuring the Trusted Solaris operating environment
- Configuring the OBP variables
- Bringing up the domain
- Configuring the Network Time Protocol (NTP) packages
- Finishing the domain installation

▼ To Configure the Domain Network Information on the SSP

1. **Log in to the main SSP as a user who can assume the root role and assume the role.**
2. **Manually edit the `/etc/hosts` file to include the IP address of the new domain.**

You need to get the IP address from your network administrator.

The correct entries would look similar to the following `/etc/hosts` sample.

Note that the new entry is borabora:

```
# /etc/inet/hosts
#
# Internet host table
#
127.0.0.1      localhost
0.0.0.0 tsol-default
#
# domain subnet
#
129.153.107.101 bermuda loghost
129.150.107.100 jamaica
129.150.107.102 cuba
129.150.107.103 borabora
129.150.107.104 bali
129.150.107.105 fiji
#
# cb0 subnet
#
10.100.100.200 jamaica-qfe0
10.100.100.201 bermuda-qfe0
10.100.100.100 ctrl_brd_0
#
# cb1 subnet
#
10.100.101.200 jamaica-qfel
10.100.101.201 bermuda-qfel
```

```

10.100.101.100  ctrl_brd_1
#
# misc
#
129.150.103.178  wolf359      nis-master

```

The `/etc/hosts` file is actually a link to `./inet/hosts`.

3. Manually edit the `/etc/ethers` file to include the Ethernet address of the new domain.

The correct entries would look similar to the following `/etc/ethers` sample. Note that `borabora` represents the name of the new domain in this example:

```

08:00:20:ac:5c:b9      jamaica
08:00:20:b0:65:77      bermuda
00:00:be:01:0f:42      ctrl_brd_0
00:00:be:01:0f:6c      ctrl_brd_1
00:00:be:a6:56:78      cuba
00:00:be:a6:60:d1      borabora
00:00:be:a6:60:d2      bali
00:00:be:a6:60:d3      fiji

```

4. Update the `/etc/security/tsol/tnrhdb` file to indicate the template for the new domain.

The correct entries would look similar to the following example. Note that the new domain is `borabora` with IP address `129.150.107.103`.

```

# /etc/security/tsol/tnrhdb
#
# Assume that template unlab and tsol is defined in the tnrhtp database.
#
127.0.0.1:tsol
0.0.0.0:unlab
129.150.107.101:tsol
129.150.107.103:tsol
129.150.103.0:tsol
129.150.107.0:tsol
10.100.100.201:tsol
10.100.101.201:tsol

```

5. Make the changes in `/etc/security/tsol/tnrhdb` file active with the `tnctl(1M)` command:

```

ssp# tnctl -H /etc/security/tsol/tnrhdb

```

6. Check for the template of the new domain with the `tninfo(1M)` command:

```
ssp# tninfo -h borabora
=====
Remote Host Table Entries:
IP address= 129.150.107.103, port= 0
template = tsol
```

7. If the NIS+ master is running Trusted Solaris 7, its `hosts`, `ethers` and `tnrhdb(4)` files need to be updated with the information for the new domain. Update the NIS+ master files.

You are done configuring the domain network information. You can now set up the Trusted Solaris SSP as a net install server, as described in the next section.

▼ To Set Up the Trusted Solaris SSP as the Net Install Server

1. Log in as a user on the main SSP that can assume the root and secadmin roles. Assume the root role.

2. In the root role, at label `admin_low`, use the Device Allocation Manager to allocate the CDROM drive, but do not mount it.

Do not try to use the Volume Manager; it is disabled in the Trusted Solaris environment.

- a. Click the triangle above the Style Manager on the Front Panel to display the Trusted Desktop subpanel. Click Device Allocation.

- b. Double-click the CDROM device to move it to the Allocated Devices list.

- c. Write down the device name for the CDROM drive as indicated in the "Insert disk into" message in the Device Allocation window.

For example, if the message reads:

```
Insert disk into /dev/dsk/c0t2d0s0.
Make sure disk is labeled ADMIN_LOW [ADMIN_LOW].
Press RETURN when cdrom_0 is ready, or ^C to cancel.
```

then write down the device name, `/dev/dsk/c0t2d0s0`, before continuing.

- d. Insert the Trusted Solaris Supplemental CD into the CDROM drive and press the Return key.
- e. Answer `n` to the Do you want `cdrom_0` mounted: (y/n)? `n` question.

Note - This differs from the instructions in the *Trusted Solaris Installation and Configuration* manual. Follow these instructions; do not mount the CDROM.

3. In the root role, at label `admin_low`, make sure that `/cdrom/root` exists. If it does not, create it.

```
ssp# mkdir -p /cdrom/root
```

4. Mount the CDROM with all allowed and forced privileges.

```
ssp# mount -F hsfs -o ro -S "allowed=all;forced=all" cdrom_device /cdrom/root
```

For example, for the CDROM on device `/dev/dsk/c0t2d0s0`, type:

```
ssp# mount -F hsfs -o ro -S "allowed=all;forced=all" \  
/dev/dsk/c0t2d0s0 /cdrom/root
```

5. Check that the mount succeeded with the `df(1M)` command:

```
ssp# df -k grep | cdrom  
/dev/dsk/c0t2d0s0      544100  544100      0   100%    /cdrom/root
```

6. Add the `/cdrom/root/Trusted_Solaris_7/Tools/add_install_client` and `/cdrom/root/Trusted_Solaris_7/Tools/rm_install_client` commands to the Custom Root Role profile with all privileges.
 - a. Assume the `secadmin` role. At label `admin_low`, open the Profile Manager application.
 - b. In the Profile Manager: Load window, select `none` for Name Service then click the OK button.

- c. **In the Profile Manager: Open window select Custom Root Role then click the Modify button.**
 - d. **In the Profile Manager main window, select View from the menu bar then select Commands from the submenu.**
 - e. **Enter `/cdrom/root/Trusted_Solaris_7/Tools` in the Pathname: box and press the Return key.**
You should see `/cdrom/root/Trusted_Solaris_7/Tools` added to the Exclude list.
 - f. **Click on `/cdrom/root/Trusted_Solaris_7/Tools` in the Exclude list.**
It expands to display all the commands available in the `/cdrom/root/Trusted_Solaris_7/Tools` directory.
 - g. **Select command `add_install_client(1M)` and add it to the Include list.**
 - h. **Click on the Privileges... button and select ALL privileges for the `add_install_client` command.**
 - i. **Select command `rm_install_client(1M)` and add it to the Include list.**
 - j. **Click on the Privileges... button and select ALL privileges for the `rm_install_client` command.**
 - k. **Select Profiles from the Profile Manager main window menu bar then select Save Profile from the submenu to save the Custom Root Role profile.**
7. **In the root role, make sure the `/etc/nsswitch.conf` file is set up with files as the first value for `tsolprof`:**
- ```
tsolprof: files nisplus
```
8. **Go to the user's workspace. Delete the root role workspace then assume the root role again.**  
This action re-reads the root role's profiles. The Custom Root Role with your changes is now in effect.
9. **In the root role, at label `admin_low`, open a terminal and issue the `clist(1M)` command to verify that the command `/cdrom/root/Trusted_Solaris_7/Tools/add_install_client` and `/cdrom/root/Trusted_Solaris_7/Tools/add_install_client` are available.**

```
ssp# clist -p | grep /cdrom/root/Trusted_Solaris_7/Tools/add_install_client
/cdrom/root/Trusted_Solaris_7/Tools/add_install_client: all
ssp# clist -p | grep /cdrom/root/Trusted_Solaris_7/Tools/rm_install_client
/cdrom/root/Trusted_Solaris_7/Tools/rm_install_client: all
```

The commands should indicate `all` which means all privileges.

#### 10. Change to the `/Tools` directory on the CD.

```
ssp# cd /cdrom/root/Trusted_Solaris_7/Tools
```

#### 11. Set up the host domain as an install client.

```
ssp# ./add_install_client domain_name sun4u
```

The `add_install_client` command should share the CD across the net. If you receive the following warning, perform the `share(1M)` in the SSP window, as shown in the following example:

```
prom_panic: Could not mount filesystem
```

```
ssp# share -F nfs -o ro,anon=0 /cdrom/root
```

Confirm that the filesystem is shared:

```
ssp# showmount -e
export list for bermuda:
/cdrom/root (everyone)
```

If the command did not return `/cdrom/root (everyone)`, type the `share` command again, and re-confirm it with the `showmount(1M)` command.

If the `/etc/nsswitch.conf` file contains a DNS entry in its host list, you may receive the following warning:

```
Error: domain_name does not exist in the NIS+ ethers map.
```

If you receive this message, you need to remove the DNS entry in the `/etc/nsswitch.conf` file, to add the *domain\_name* to the ethers map if the name is not already in the map, and to re-run the `add_install_client` command.

#### 12. Leave the root role and assume the `ssp` role.

13. Use the `domain_status(1M)` command to ensure that the OS version is set to the proper value for the domain you are installing.

For Trusted Solaris 7, the OS version should be 5.7. If the OS version is correct, proceed to step Step 14 on page 59. If not, perform the following steps.

- a. Remove the existing domain.

```
ssp% domain_remove -d domain_name
```

The `domain_remove(1M)` command prompts you to save the domain directories, as in the following example:

```
domain_remove: The following subdirectories contain domain specific
 information such as messages files, configuration files,
 and hpost dump files. You may choose to keep these
 directories if you still need this information. This
 domain may be created with or without this information
 being saved.
```

```
/var/opt/SUNWssp/adm/xf4-b3
/var/opt/SUNWssp/etc/allxf4/xf4-b3
```

```
Keep directories (y/n)? y
Domain : xf4-b3 is removed !
```

Be sure to answer yes, **y**, to the prompt so that the domain information is saved. If you answer no, you will have to supply the board numbers and the platform name for the new domain.

- b. Create the new domain with the new OS version number.

```
ssp% domain_create -d domain_name -o 5.7
```

If you saved the domain information, you do not need to include the `-b` and `-p` arguments. The `domain_create(1M)` command uses the domain information that was saved and the information you provide with the command to create the new domain.

14. Use the `domain_switch(1M)` command to ensure that `SUNW_HOSTNAME` is set to the name of the domain you are installing.

```
ssp% domain_switch domain_name
```

---

**Note** - The `domain_switch(1M)` command must be executed from a `pfsh(1M)` shell. By default, the `ssp` role uses a `pfsh` shell.

---

## 15. Check for blacklisted components.

If SBus boards have been added to a system board, confirm that the processors on those system boards are not blacklisted. Processors are blacklisted at the factory when a system board does not have SBus cards installed.

During the bring-up process, observe the list of blacklisted components. Alternatively, for instructions on how to retrieve the blacklist file, refer to the `blacklist(4)` man page.

To remove a processor from the blacklist, edit the blacklist file and remove the number of the board from the `pc` line in the file. By default, the blacklist file resides at `$SSPVAR/etc/platform_name/blacklist`; however, the location of the blacklist file can be reconfigured so that the location of the blacklist file on your server may be different from the default location.

You are done setting up the SSP as a network install server. You can now bring up the domain, as described in the next section.

## ▼ To Bring Up the Domain

1. In the ssp role on the main SSP, with `SUNW_HOSTNAME` set to the domain being installed, bring up the domain.

```
ssp% bringup -A off
```

If this is the first domain to be brought up, you will be prompted to configure the centerplane. Type `y` to continue if you are sure that no other domains are running. Responding yes resets the entire platform; therefore, you must ensure that no other domains are running.

This bringup will configure the Centerplane. Please confirm (y/n)? `y`

After a few minutes the SSP prompt is displayed. Review the output of the `bringup(1M)` command. If errors occurred, you must correct those errors before you proceed. If no errors occurred, continue to the next step.

2. In the SSP window, open a `netcon(1M)` session.

```
ssp% netcon -g
```

The `ok` prompt is displayed after a few minutes. The duration depends directly on the size of the domain.

You are done bringing up the domain. You can now set up the OpenBoot PROM, as described in the next section.

## ▼ To Set Up the OpenBoot Prom Environment

1. On the domain's netcon, use the `devalias` command to check for duplicate devalias entries in OBP.

The `suninstall` utility may not work properly if you have defined duplicate devalias entries in OBP. Use the `devalias` command to check the aliases. The output may resemble the following example:

```
ok devalias
net /sbus@41,0/qec@0,20000/qe@1,0
ttya /ssp-serial
ssa_b_example /sbus@40,0/SUNW,soc@0,0/SUNW,pln@b0000000,XXXXXX/SUNW,ssd@0,0:a
ssa_a_example /sbus@40,0/SUNW,soc@0,0/SUNW,pln@a0000000,XXXXXX/SUNW,ssd@0,0:a
isp_example /sbus@40,0/QLGC,isp@0,10000/sd@0,0
net_example /sbus@40,0/qec@0,20000/qe@0,0
net /sbus@41,0/qec@0,20000/qe@0,0
ok
```

---

**Note** - If any devalias entries are defined twice (`net` is defined twice in the above example), you should remove the extra devalias entries.

---

2. If any duplicate entries exist in the `devalias` list, remove them.

The following example removes the last-created `net` devalias. You may have to issue a second `nvunalias` command if the second `net` alias is the incorrect one. Then issue an `nvalias` command to create the correct `net` device alias.

```
ok nvunalias net
```

3. If a `net` alias does not exist for the network interface that is on the same subnet as the SSP, create one by typing a command similar to the following example:

```
ok nvalias net /sbus@41,0/SUNW,hme@0,8c00000
```

Where `/sbus@41,0` refers to system board 0 and SBus 1. The `/SUNW,hme@0` portion of the device name defines a 100BASE-T network interface installed in Slot 0. This information is site-specific; thus, your configuration may vary.

The following table contains the SBus numbers used in the `devalias` file.

TABLE 4-1 SBus Numbers in the devalias File

| system<br>board | sysio 0  | sysio 1  | system<br>board | sysio 0  | sysio 1  |
|-----------------|----------|----------|-----------------|----------|----------|
| 0               | /sbus@40 | /sbus@41 | 8               | /sbus@60 | /sbus@61 |
| 1               | /sbus@44 | /sbus@45 | 9               | /sbus@64 | /sbus@65 |
| 2               | /sbus@48 | /sbus@49 | 10              | /sbus@68 | /sbus@69 |
| 3               | /sbus@4c | /sbus@4d | 11              | /sbus@6c | /sbus@6d |
| 4               | /sbus@50 | /sbus@51 | 12              | /sbus@70 | /sbus@71 |
| 5               | /sbus@54 | /sbus@55 | 13              | /sbus@74 | /sbus@75 |
| 6               | /sbus@58 | /sbus@59 | 14              | /sbus@78 | /sbus@79 |
| 7               | /sbus@5c | /sbus@5d | 15              | /sbus@7c | /sbus@7d |

The `watch-net-all` command (no spaces) displays the functioning network interfaces.

You are done setting up the OBP environment. You can now install the Trusted Solaris operating environment, as described in the following section.

## ▼ To Install the Trusted Solaris 7 Operating Environment

You can use these instructions to install the Trusted Solaris operating environment without saving any previous files.

During the installation, you will use the `suninstall` utility, which has its own instructions. The following instructions are specific to the Sun Enterprise 10000. For more information about the `suninstall` utility, refer to the Solaris installation instructions in your Solaris media kit.



**Caution** - The next step starts the `suninstall` utility. During the installation, you will be asked to specify the device name of the boot disk. Do not begin the installation until you know the device name.

1. In the `netcon` window, boot the system from the network.

```
ok boot net
```

---

**Note** - You should have an alias (usually `net`) in OBP for the proper network interface. Use that alias with the `boot` command, as shown in the example above. Otherwise, you must type in the complete OBP device path. If you specify an alias (or path) that does not describe the proper network interface, the `boot` command will fail, and you will have to bring up the domain again.

---

If you install the operating system on a drive other than the one designated as the boot drive, the `suninstall` utility displays a warning message similar to the following:

```
Warning
You have an invalid disk configuration because of the condition(s)
displayed in the window below. Errors should be fixed to ensure a
successful installation. Warnings can be ignored without causing
the installation to fail.
```

```
> To go back and fix errors or warnings, select Cancel.
> To accept the error conditions or warnings and continue with
> the installation, select Continue.
```

```
WARNING: The boot disk is not selected or does not have
a '/' mount point (c0t3d0)
```

You can safely ignore this warning and press F2 to continue.

The `boot net` command starts the `suninstall` utility. This utility prompts you to provide site and platform-specific information. Refer to the following table for the platform-specific information you may need to supply.

**TABLE 4-2** Platform-Specific Information for the `suninstall` Utility

| If you are asked to                                                                 | Do this                                                                                                                                                                                                                                                     |
|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Please enter the hostname of the SSP for <i>domain_name</i> [ <i>default_name</i> ] | Enter the hostname for your SSP. Note that the default value is to append <code>-ssp</code> to the domain name.                                                                                                                                             |
| Set the network information                                                         | Select the appropriate level of information you want to provide. If you select any option other than <code>None</code> , the <code>suninstall</code> utility displays a series of dialogs that request configuration information. Provide that information. |

**TABLE 4-2** Platform-Specific Information for the `suninstall` Utility (continued)

| If you are asked to               | Do this                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Solaris Interactive Installation  | Select <code>Initial</code> for fresh install.                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Select 64 bit                     | Click “Select To Include Solaris 64-bit Support” to install the 64-bit kernel. Refer to the <i>Solaris 7 8/99 Release Notes Supplement</i> for instructions on how to check the operating mode, to set the default mode, and to switch the operating mode.                                                                                                                                                                                                                                  |
| Select Software                   | Select <code>Entire Distribution</code> plus <code>OEM Support</code> .                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Select Disk(s)                    | Select the disk(s) on which the software is to be installed. If you choose a drive other than the one designated as the boot drive, a warning message appears later in the installation process. At that point, you can choose whether to continue, or not.                                                                                                                                                                                                                                 |
| Automatically Layout File Systems | Select <code>Manual Layout</code> . The <code>suninstall</code> utility enables you to customize the root disk by specifying disk partitions. Refer to <i>System Administration Guide, Volume 1</i> as a guide.                                                                                                                                                                                                                                                                             |
| Mount Remote File System          | Press <code>F4</code> if file systems are to be mounted from a remote file server. Press <code>F2</code> if they are not.                                                                                                                                                                                                                                                                                                                                                                   |
| Manual Reboot after installation  | Select <code>manual reboot</code> and press <code>F2</code> to begin the installation. This step, which installs the software from the Trusted Solaris CD, can take approximately 40 minutes to complete. When the install ends successfully, the superuser prompt is displayed in the domain's <code>netcon</code> console window. You can now configure the Trusted Solaris 7 operating environment, as described in “To Configure the Trusted Solaris Operating Environment” on page 65. |

---

**Note** - Make sure that you select `Manual Reboot` and not `Automatic Reboot`.

---

When you perform a full install of the Trusted Solaris 7 operating environment on a domain, the `suninstall` utility allows you to manually enter the disk partition sizes for your file systems. Do not use disk partitions that are less than the minimum sizes in Table 4-3.

If two disks are used, `root (/)` and `/usr` must be on the device specified in the OBP boot alias.



TABLE 4-3 Minimum Partition Sizes

| Partition |         | Minimum Sizes | Notes                                                                                                                                                                                          |
|-----------|---------|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 0         | /       | 256 Mbyte     | Bare minimum size                                                                                                                                                                              |
| 1         | swap    | 1024 Mbyte    | Bare minimum size                                                                                                                                                                              |
| 2         | overlap |               | Actual total disk size                                                                                                                                                                         |
| 3         | /var    | 512 Mbyte     |                                                                                                                                                                                                |
| 4         |         | 3 Mbyte       | This slice must be reserved for the Alternate Pathing and Solstice DiskSuite <sup>™</sup> products. Otherwise, subsequent Alternate Pathing installations will overwrite the operating system. |
| 5         | /opt    | 512 Mbyte     | This may be larger depending upon remaining space.                                                                                                                                             |
| 6         | /usr    | 1 Gbyte       | Asian-language users may need more space here.                                                                                                                                                 |

Use the Tab key to move the cursor, and use the keyboard to type the size for each partition. Press F2 when you are done.

Return to Table 4-2 to continue the `suninstall` installation.

## ▼ To Configure the Trusted Solaris Operating Environment

1. After the operating system is loaded and the superuser prompt is displayed, list the `devices` entry for your boot disk.

```
domain_name# ls -l /dev/dsk/root_partition_device
```

where `root_partition_device` is in the form `cxtxdxsx`.

2. Copy the part of the string that begins with either `/sbus` or `/pci`.

Example:

```
/sbus@65,0/SUNW,fas@1,8800000/sd@3,0:a.
```

Record your device string here:

```
/
```

3. To enable keyboard abort and allow the domain's netcon key sequence ~# to drop to the ok prompt, change the value of abort\_enable to 1 in the /a/etc/system file.

```
set abort_enable = 1
```

4. Update the /a/etc/default/login file to allow the root role to log in remotely from any workstation.

Comment out the `CONSOLE=/dev/console` line.

```
CONSOLE=/dev/console
```

5. Update the /a/etc/inet/hosts file to include IP addresses and names of the main and spare SSP.

In the following example, the domain is borabora, the main and spare SSPs are jamaica and bermuda.

```
/etc/inet/hosts
#
Internet host table
#
127.0.0.1 localhost
0.0.0.0 tsol-default
129.150.107.103 borabora loghost
129.150.107.101 bermuda
129.150.107.100 jamaica
```

6. Update the /a/etc/security/tsol/tnrhdb file to include templates for the main and spare SSP and any other workstations the domain communicates with.

In the following example, the domain has IP address 129.150.107.103 and the SSPs have IP addresses 129.150.107.100 and 129.150.107.101.

```
/etc/security/tsol/tnrhdb
#
Assume that template tsol is defined in the tnrhtp database.
#
127.0.0.1:tsol
0.0.0.0:unlab
129.150.107.103:tsol
```

```
129.150.107.0:tsol
129.150.103.0:tsol
129.150.107.100:unlab
129.150.107.101:tsol
129.150.107.102:unlab
```

7. **Perform any site-specific configuration tasks on the newly installed environment by editing the configuration files in the `/a` directory.**

The number and extent of any site-specific configuration task, such as configuring the default router, are highly dependent on the local configuration of the server and the network on which it resides. If you are unsure about what tasks you should perform, contact your service provider, or refer to the *System Administration Guide, Volume 1* and the *Trusted Solaris Administrator's Procedures*.

8. **Shut down the domain from the `netcon` window.**

```
domain_name# init 0
```

You are done configuring the Trusted Solaris operating environment. You can now configure the OpenBoot PROM variables, as described in the following section.

## ▼ To Configure the OBP Variables

1. **In the `netcon` window, assign the device string to an alias (refer to Step 2 on page 65 in “To Configure the Trusted Solaris Operating Environment” on page 65 for the *device\_string*).**

```
ok nvalias bootdisk_alias device_string
```

As in this example, the `nvalias` command should be entered on a single line.

2. **Use the `setenv` command to set the default boot-device alias to the correct device.**

```
ok setenv boot-device bootdisk_alias
```

Where *bootdisk\_alias* corresponds to the user-defined alias you established in Step 1 on page 67.

You are done configuring the OBP variables. You can now bring up the domain, as described in the following section.

## ▼ To Bring Up the Domain

1. On the main SSP, assume the root role.
2. Change to the `/Tools` directory.

```
ssp# cd /cdrom/root/Trusted_Solaris_7/Tools
```

3. Remove the host domain as an install client.

```
ssp# ./rm_install_client domain_name
```

4. Remove the

`/cdrom/root/Trusted_Solaris_7/Tools/add_install_client` and  
`/cdrom/root/Trusted_Solaris_7/Tools/rm_install_client`  
commands from the Custom Root Role profile.

- a. Assume the secadmin role. At label `admin_low`, open the Profile Manager application.
- b. In the Profile Manager: Load window, select none for Name Service then click the OK button.
- c. In the Profile Manager: Open window select Custom Root Role, then click the Modify button.
- d. In the Profile Manager main window, select View from the menu bar, then select Commands from the submenu.
- e. Select the  
`/cdrom/root/Trusted_Solaris_7/Tools/add_install_client`  
command from the Include list and move it to the Exclude list.
- f. Select the  
`/cdrom/root/Trusted_Solaris_7/Tools/rm_install_client`  
command from the Include list and move it to the Exclude list.
- g. Select Profiles from the Profile Manager main window menu bar then select Save Profile from the submenu to save the profile.

5. On the SSP, assume the root role. At label `admin_low`, unshare then unmount the `/cdrom/root` filesystem:

```
ssp# cd /
ssp# unshare /cdrom/root
ssp# umount /cdrom/root
```

6. In the root role, at label `admin_low`, use the Device Allocation Manager to deallocate the CDROM drive. Remove the CDROM.  
Do not use the Volume Manager, it is disabled in the Trusted Solaris environment.
7. On the SSP, assume the `ssp` role.
8. Switch to the domain and bring it up.

```
ssp% domain_switch domain-name
ssp% bringup -A on
```

If this is the first domain to be brought up, you will be prompted to configure the centerplane. Type `y` to confirm if you are sure that no other domains are running. Responding yes resets the entire platform; therefore, you must ensure that no other domains are running.

```
This bringup will configure the Centerplane. Please confirm (y/n)? y
```

9. After the domain boots, type the root password then re-enter the password when prompted in the `netcon(1M)` window.

```
Root password: password
Please re-enter your root password: password
```

Your entry will become the new root role password for the domain.  
You are done bringing up the domain.

## ▼ To Access the Domain's root Role

On the `netcon`, when the Trusted Solaris domain has finished rebooting, you will not get the "console login:" prompt, because command line login is disabled in the Trusted Solaris environment for security reasons. For now, to finish configuring the

Trusted Solaris domain, you can access the domain's root role by logging in remotely from the Trusted Solaris SSP.

When accessing a Trusted Solaris domain, a user who can assume the root role must remotely log in to the domain. For a discussion of remote administration options, see "Remote Administration Options" in *Trusted Solaris Administrator's Procedures*.

1. **On the Trusted Solaris SSP, assume the root role.**
  - a. **In the role root on the SSP, rlogin to the domain.**  
You are now in the domain's root role.
  - b. **To verify that you are in the domain's root role:**

```
ssp# uname -a
ssp# id -a
```

For a broader view of what is and is not allowed in a Trusted Solaris environment on a Sun Enterprise 10000, see "Differences from Solaris 7 Installation and Configuration of the Sun Enterprise 10000" on page 8.

## ▼ To Make the Domain a NIS+ Client

1. **If the domain is to be a NIS+ client, assume the domain's root role to update the hosts entry in the /etc/nsswitch.conf file after running the nisclient command.**

```
hosts: files nisplus
```

Failure to do this will result in the domain communicating in JTAG instead of network mode after a reboot.

## ▼ To Configure the NTP Packages

Perform the following steps to configure the `ntp.conf` file, which resides at `/etc/inet/ntp.conf`.

1. **Assume the root role on the Trusted Solaris SSP and rlogin to the domain.**  
You should now be in the root role on the domain. To confirm:

```
uname -a
id -a
```

**2. Create the `ntp.conf` file in your text editor.**

**3. Edit the file so that it resembles the following example.**

```
example Starfire domain /etc/inet/ntp.conf
configuration file ntp.conf
for Trusted Solaris 7 5/
substitute actual ssp name for <ssp-name>

server <ssp-name> prefer
we can always fall back to the local clock.
server 127.127.1.0
fudge 127.127.1.0 stratum 9

Other ntp files.
driftfile /etc/inet/ntp.drift

Encryption:
disable auth
controlkey 1
requestkey 1
authdelay 0.000793

precision declaration
precision -18 # clock reading precision (1 usec)
```

Each domain should use the SSP as its source for time, and the SSP should use at least two other sources, besides its internal clock, to avoid a single point of failure in case the SSP's clock fails.

You are done configuring the NTP packages. You can now finish the domain installation, as described in the following section.

## ▼ To Finish the Domain Installation

**1. As root role on the domain, check the operating mode.**

```
domain_name# isainfo -k
```

If you are running in 64-bit mode, you should get the following output.

```
sparcv9
```

**2. Reboot the domain with the proper operating mode.**

For the Trusted Solaris 7 operating environment, you can use either the 32-bit mode or the 64-bit mode. The 64-bit mode is the default for all `sun4u` platforms.

**a. For 32-bit mode, type the following command.**

```
domain_name# reboot boot_alias kernel/unix
```

**b. For 64-bit mode, type one of the following commands.**

If you are not already in 32-bit mode, use the following command.

```
domain_name# reboot boot_alias
```

If you are switching from the 32-bit mode, use the following command.

```
domain_name# reboot boot_alias kernel/sparcv9/unix
```

**3. If you want to install Trusted Solaris AP 2.2, see Chapter 5.**

Otherwise, you are done with the install unless you need to license your software, as described in the following section.

## Licensing Your Software

The Sun Enterprise 10000 domain feature requires different approaches to software licensing when compared to systems that cannot be logically partitioned.

### FLEXlm-Based Licensing

License management (the license server) is normally tied to a machine host ID. On a Sun Enterprise 10000 system, the license server is tied to the domain host ID. Each domain receives its own domain host ID.

Therefore, if licensing is installed on a Sun Enterprise 10000 system, it must be installed in a domain that will not be removed. Adding or removing processors from the domain will not affect licensing, as long as the domain always has at least one active processor.

If licensing ever needs to be moved from one domain to another, the licenses will need to be regenerated using the new domain host ID. This is identical to the



situation when moving the license server from one machine to another. This process is called a *server move*; contact the Sun License Center to request a *server move*.

For more licensing information, use the following Sun License Center URL:

- <http://www.sun.com/licensing>

To obtain the Sun Enterprise 10000 system domain host ID, type `hostid` in a shell window.

## Other Software Licensing

Other software vendors may have unique software licensing policies on the Sun Enterprise 10000 system. All major independent service providers have been notified and should have software policies in place. For additional information, contact your service provider.



## Trusted Solaris Alternate Pathing 2.2 on the Sun Enterprise 10000 Server

---

This chapter contains install instructions for Trusted Solaris Alternate Pathing (AP) 2.2 on the Sun Enterprise 10000 server.

The Trusted Solaris version of AP 2.2 shipped on the Trusted Solaris 7 supplemental CD requires a Trusted Solaris 7 operating environment. The procedures given in this chapter assume that the SSP and the domains are running Trusted Solaris 7.

---

### Installing Trusted Solaris AP

The Trusted Solaris AP 2.2 release includes one package that must be installed on the Trusted Solaris SSP and a set of core packages that must be installed on the Sun Enterprise 10000 domain running Trusted Solaris software.

The Trusted Solaris AP packages require approximately 2.7 megabytes of disk space on the domain and 37 kilobytes on the SSP. The following table lists the total size of the AP software by file system:

**TABLE 5-1** AP Disk Space Requirements by File System

| File System | Size      |
|-------------|-----------|
| SSP:        |           |
| /opt        | 31 Kbytes |

**TABLE 5-1** AP Disk Space Requirements by File System *(continued)*

| File System | Size        |
|-------------|-------------|
| Host:       |             |
| /usr        | 317 Kbytes  |
| /           | 1.3 Mbytes  |
| /etc        | 13 Kbytes   |
| /kernel     | 1528 Kbytes |
| /sbin       | 1481 Kbytes |

## ▼ To Install Trusted Solaris AP 2.2

The Trusted Solaris AP software must be installed on a Trusted Solaris 7 system.

- 1. On the main SSP, log in as a user who can assume the root role , and assume it.**
- 2. In the root role, at label admin\_low, use the Device Allocation Manager to allocate the CDROM drive, but do not mount it.**

Do not try to use the Volume Manager; it is disabled in the Trusted Solaris environment.

- a. Click the triangle above the Style Manager on the Front Panel to display the Trusted Desktop subpanel. Click Device Allocation.**
- b. Double-click the CDROM device to move it to the Allocated Devices list.**
- c. Write down the device name for the CDROM drive as indicated in the "Insert disk into" message in the Device Allocation window.**

For example, if the message reads:

```
Insert disk into /dev/dsk/c0t2d0s0.
Make sure disk is labeled ADMIN_LOW [ADMIN_LOW].
Press RETURN when cdrom_0 is ready, or ^C to cancel.
```

then write down the device name, /dev/dsk/c0t2d0s0, before continuing.

- d. Insert the Trusted Solaris Supplemental CD into the CDROM drive and press the Return key.
- e. Answer “n” to the question: Do you want cdrom\_0 mounted: (y/n)? **n**

---

**Note** - This differs from the instructions in *Trusted Solaris Installation and Configuration*. Follow the instructions here; do not mount the CDROM.

---

3. In the root role, at label `admin_low`, make sure that `/cdrom/root` exists. If not, create it.

```
ssp# mkdir -p /cdrom/root
```

4. Mount the CDROM with all allowed and forced privileges.

```
ssp# mount -F hsfs -o ro -S "allowed=all;forced=all" \
cdrom_device /cdrom/root
```

For example, for the CDROM on device `/dev/dsk/c0t2d0s0`, type:

```
ssp# mount -F hsfs -o ro -S "allowed=all;forced=all" \
/dev/dsk/c0t2d0s0 /cdrom/root
```

5. Check that the mount succeeded with the `df(1M)` command:

```
ssp# df -k grep | cdrom
/dev/dsk/c0t2d0s0 544100 544100 0 100% /cdrom/root
```

6. Share /cdrom/root by issuing the `share(1M)` command:

```
ssp# share -F nfs -o ro,anon=0 /cdrom/root
```

7. Use the `showmount(1M)` command to confirm that the /cdrom/root filesystem is being shared:

```
ssp# showmount -e
export list for bermuda:
/cdrom/root (everyone)
```

8. Install the Trusted Solaris AP packages on the SSP (and spare SSP, if applicable)

- a. Change to the AP 2.2 product directory and execute the `pkgadd(1M)` command to add the `SUNWapssp` package onto the SSP.

```
ssp# cd /cdrom/root/Product
ssp# pkgadd -d . SUNWapssp
```

- b. Start the `ap_ssp_daemon`.

```
ssp# init q
```

- c. If you have a spare SSP, perform the above steps on the spare SSP.

9. Install Trusted Solaris AP on the domain.

- a. From the Trusted Solaris SSP's root role, `rlogin(1)` to the domain.  
You are now logged in to the domain in the root role.
- b. Create and mount the /cdrom directory.

```
mkdir /cdrom
mount ssp_hostname:/cdrom/root /cdrom
```

- c. Install the AP 2.2 host packages on the domain.

```
pkgadd -d /cdrom/Product SUNWapdoc \
SUNWapu SUNWapr SUNWapdv
```

## 10. Unmount and remove the CDROM.

- a. Unmount the CDROM on the domain.

```
cd /
umount /cdrom
```

- b. On the SSP, assume the root role. At label `admin_low`, unshare then `umount /cdrom/root`:

```
ssp# cd /
ssp# unshare /cdrom/root
ssp# umount /cdrom/root
```

- c. In the root role, at label `admin_low`, use the Device Allocation Manager to deallocate the CDROM drive and remove the Trusted Solaris Supplemental CD.

Do not use the Volume Manager; it is disabled in the Trusted Solaris environment.

## 11. Configure Trusted Solaris AP.

For an example of the steps you need to follow, see “To Configure a Trusted Solaris AP” on page 80. Also see the *Sun Enterprise Server Alternate Pathing User's Guide*.

## ▼ To Configure a Trusted Solaris AP

All procedures are performed on the domain, in the role root at the label `admin_low`.

### 1. Create three to five AP databases.

```
ssp# apdb -c raw_disk_slice -f
```

### 2. Create AP metadisks.

You must know the configuration of the domain's hardware so that you know which two ports are connected to the same disk array. The following examples use `pln` ports. Your ports may vary, depending on the configuration of the domain.

#### a. Display all of the ports and their disk device nodes.

```
apinst
pln0
/dev/dsk/c1t0d0
/dev/dsk/c1t1d0
/dev/dsk/c1t2d0
/dev/dsk/c1t3d0
/dev/dsk/c1t4d0
/dev/dsk/c1t5d0
pln1
/dev/dsk/c2t0d0
/dev/dsk/c2t1d0
/dev/dsk/c2t2d0
/dev/dsk/c2t3d0
/dev/dsk/c2t4d0
/dev/dsk/c2t5d0
```

#### b. Create an uncommitted disk pathgroup.

```
ssp# apdisk -c -p pln0 -a pln1
ssp# apconfig -S -u
```

where:

`-c` causes the pathgroup to be created

`-p` designates the primary path

`-a` designates the alternate path.

You can verify the results by using the `apconfig` command as shown above.

#### c. Commit the database entries.

```
apdb -C
```



You can verify the results of the above command by using `apconfig -S`.

**d. Rebuild the devices directories.**

```
ssp# drvconfig -i ap_dmd
ssp# ls -l /devices/pseudo/ap_dmd*
...
```

As shown above, you can verify the results of the `drvconfig(1M)` command by listing the contents of `/devices/pseudo/ap_dmd*`.

**e. Create symbolic links from the devices directory `/devices/pseudo` to the special metadisk files in `/dev/ap/dsk` and `/dev/ap/rdisk`.**

```
ssp# apconfig -R
ssp# ls -l /dev/ap/dsk
...
```

As shown above, you can verify the results of the `apconfig` command by listing the contents of `/dev/ap/dsk` to view the symbolic links.

**f. If you are placing the boot disk under AP control, use `apboot` to define the new AP boot device.**

```
apboot metadisk_name
```

The `apboot` command modifies the `/etc/vfstab` file and the `/etc/system` file. The *metadisk\_name* must be in the form: `mcxtxdx`.

**g. Modify any references that use a physical device node (that is, a path that begins with `/dev/dsk` or `/dev/rdsk`) to use the corresponding metadisk device node (that is, a path that begins with `/dev/ap/dsk` or `/dev/ap/rdsk`).**

If a partition is mounted under a physical path, unmount and remount it under the metadisk path.

Examine `/etc/vfstab` for any physical devices that should be changed to AP metadevices. If necessary, edit `/etc/vfstab` to make the necessary modifications.



---

**Caution** - You must be a knowledgeable system administrator to edit `/etc/vfstab`. If you do not configure your file systems properly in `/etc/vfstab`, it is possible that you will lose data the next time you boot the domain.

---

**3. Create AP metanetworks (for non-primary networks).**

---

**Note** - The following steps should be applied to all networks that you want to alternately path *except* the primary network.

---

**a. Create the network pathgroup.**

```
ssp# apnet -c -p network_interface -a network_interface
ssp# apconfig -N -u
...
```

As shown above, you can verify the results of the `apnet` command by using `apconfig`.

**b. Commit the network pathgroup entries in the database.**

```
apdb -C
```

You can verify the results of the `apdb` command by using the `apconfig` command with the `-N` option.

**c. Remove all direct usage of both members of the network pathgroups.**

If the physical interface is currently plumbed, and it is not the interface that you will be using as you run commands to configure the metanetwork, you can unplumb the physical interface by using the `ifconfig(1M)` command.

**d. Create an `/etc/hostname.mnetwork_interface_name` file for any metanetworks that you want to configure when the domain is rebooted.**

**4. Create the AP metanetwork for the primary network.**

**a. View the contents of the `/etc/nodename` and `/etc/hostname.interface_name` files to verify that the interface name is the same.**

**b. Create the primary network pathgroup.**

```
ssp# apnet -c -p network_interface -a network_interface
```

In this example, `-c` creates the new primary network pathgroup, `-p` designates the primary network path, and `-a` designates the alternate path.

**c. Commit the network pathgroup entry in the database.**

```
ssp# apdb -C
ssp# apconfig -N
```

As shown above, you can verify the results of the `apdb` command by using `apconfig`.

- d. **Create the new `/etc/hostname.minterface_name` file to configure the network when you reboot the domain.**

For example, `/etc/hostname.minterface_name` might contain `hmb`.

- e. **Remove the configuration files that correspond to the metanetwork interface.**

```
ssp# rm -f /etc/hostname.primary_interface_name \
/etc/hostname.alternate_interface_name
```

5. **Reboot the domain.**