Trusted Solaris Installation and Configuration

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

Part Number 805-8114-10
December 2000

Contents

Tables

Figures

About This Book

This book is for knowledgeable system administrators and security administrators who are installing the Trusted Solaris™ operating environment at networked or non-networked sites. Level of trust required by site security policy and level of expertise will determine who can perform the tasks required to install Trusted Solaris software.

Implement Trusted Solaris in Accordance with Site Security

Successfully installing and configuring Trusted Solaris consistent with site security requires understanding the security features of Trusted Solaris and your site security policy. Before attempting to install Trusted Solaris 8, read Chapter 1 for how to ensure site security when installing and configuring the Trusted Solaris environment.

Use Solaris and Trusted Solaris Installation Books

Installing the Trusted Solaris operating environment requires Solaris installation books as well as Trusted Solaris ones. See Chapter 2 for which books cover which tasks. Because Trusted Solaris software modifies Solaris software for security, Trusted Solaris books often supplement Solaris ones. Administrators should have access to both.

For example, to install the first one or two workstations, Chapter 4 supplements the Solaris installation guides.

If you are installing and configuring a network of workstations, you can choose from several installation methods after installing the first workstation. *Solaris 8 Advanced Installation Guide*, 806-0957-10, contains background information for networked installation, and describes interactive installations: network, JumpStart, and custom JumpStart. Some of the instructions are modified in the Trusted Solaris environment. See "Trusted Solaris Modifications to Network Installation" on page 135 for a list of commands and procedures that the Trusted Solaris environment secures or enhances for network and JumpStart installations.

Note - Instructions for setting up hardware and peripherals is described in hardware guides, such as the *Solaris 8 Sun Hardware Platform Guide*.

How This Book is Organized

This section describes the chapters in this book.

Chapter 1 describes the security issues when installing the Trusted Solaris operating environment on one or more hosts.

Chapter 2 identifies where various installation tasks and methods are documented.

Chapter 3 describes procedures specific to the Trusted Solaris environment when installing and configuring Trusted Solaris software.

Chapter 4 provides instructions for shutting down a Trusted Solaris host and installing the Trusted Solaris 8 operating environment.

Chapter 5 provides step-by-step instructions for installing a host that will use files, not a naming service, for administration.

Chapter 6 provides step-by-step instructions for installing a server for the NIS+ naming service.

Chapter 7 provides step-by-step instructions for installing a server for the NIS naming service.

Chapter 8 provides step-by-step instructions for installing a client for the naming services.

Chapter 9 lists differences in Trusted Solaris network installation from Solaris network installation, including JumpStart and Custom JumpStart.

Appendix A addresses site security policy and places the Trusted Solaris operating environment in the context of wider organizational and site security.

Appendix B provides a checklist for the install team when installing and configuring Trusted Solaris.

Appendix C provides sample answers to Trusted Solaris installation program questions.

Glossary defines selected terms and phrases used in this book.

Related Books from Sun Microsystems

The following books contain information useful when installing Trusted Solaris software. The Solaris 8 AnswerBook CD and the Trusted Solaris 8 AnswerBook CD are shipped with the product. Solaris 8 books are available from the Solaris 8 AnswerBook CD.

Release Notes

Trusted Solaris 8 Release Notes — Describes late-breaking news about installing Trusted Solaris software, including known problems.

Solaris 8 (SPARC Platform Edition) Release Notes — Describes bugs, known problems, software being discontinued, and patches related to the Solaris release on the SPARC™ platform.

Solaris 8 (Intel Platform Edition) Release Notes — Describes bugs, known problems, software being discontinued, and patches related to the Solaris release on the Intel platform.

Hardware and Devices Guides

Solaris 8 Sun Hardware Platform Guide, 806-2221-10 — Describes hardware supported in the Solaris and Trusted Solaris environments.

Solaris 8 (Intel Platform Edition) Device Configuration Guide, 806-1053-10 — Describes Intel hardware configurations supported in the Solaris and Trusted Solaris environments.

Solaris 8 (Intel Platform Edition) Hardware Compatibility List, 806-1054-10 — Describes Intel hardware compatibility with the Solaris and Trusted Solaris environments.

Installation Guides

Trusted Solaris Label Administration — Describes labels and includes a copy of *Compartmented Mode Workstation Labeling: Encodings Format* issued by the U.S. government.

Solaris 8 (SPARC Platform Edition) Installation Guide, 806-0955-10 — Describes how to install the Solaris environment on a SPARC platform. See *Trusted Solaris Documentation Roadmap* for additional AnswerBook2 server setup required for the Trusted Solaris environment.

Solaris 8 (Intel Platform Edition) Installation Guide, 806-0956-10 — Describes how to install the Solaris environment on an Intel platform. See *Trusted Solaris Documentation Roadmap* for additional AnswerBook2 server setup required for the Trusted Solaris environment.

Solaris 8 Advanced Installation Guide, 806-0957-10 — Describes interactive installations: network, JumpStart, and custom JumpStart. Contains background information for networked installation. Forms the basis for Trusted Solaris interactive installation — see Chapter 9 for Trusted Solaris modifications to the Solaris procedures.

Configuration Guides

Trusted Solaris Audit Administration — Describes how to set up and administer auditing on one or more Trusted Solaris hosts.

Trusted Solaris Administrator's Procedures — Describes administration tasks in the Trusted Solaris environment in detail.

"Planning Your TCP/IP Network" in *System Administration Guide, Volume 3*, 805-7229-10 — Describes how to set up a network. Required for networked sites only.

Solaris Naming Administration Guide, 806-1391-10 — Describes how to administer naming services.

Solaris Naming Setup and Configuration Guide, 806-1386-10 — Describes how to set up and configure naming services.

Other Books

What's New in the Solaris 8 Operating Environment, 805-6332-10 — Describes new features in the Solaris environment.

System Administration Guide, Volume 1: Basic Administration, 806-7228-10 — Describes basic administrative tasks in Solaris 8, such as creating and mounting file systems.

System Administration Guide, Volume 2: Advanced Administration, 805-7229-10 — Describes more advanced administrative tasks in Solaris 8, such as print management.

Books from Elsewhere

Your site security policy document — Describes the security policy and security procedures at your site.

Solaris Common Desktop Environment: Advanced User's and System Administrator's Guide — Describes the Common Desktop Environment.

The administrator guide for your currently installed operating system. — Describes how to back up system files.

Automating Solaris® Installations: A Custom JumpStart™ Guide by Paul Anthony Kasper and Alan L. McClellan, published by Prentice Hall (SunSoft Press), 1995. — Describes how to set up "hands-off" network installations. ISBN .0-13-312505-X

Ordering Sun Documents

Fatbrain.com, the Internet's most comprehensive professional bookstore, stocks select product documentation from Sun Microsystems, Inc.

For a list of documents and how to order them, visit the Sun Documentation Center on Fatbrain.com at `http://www1.fatbrain.com/documentation/sun`.

Accessing Sun Documentation Online

The docs.sun.com℠ Web site enables you to access Sun technical documentation online. You can browse the docs.sun.com archive or search for a specific book title or subject. The URL is `http://docs.sun.com`.

What Typographic Conventions Mean

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

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 `ls –a` to list all files. `machine_name% you have mail.`
`AaBbCc123`	What you type, contrasted with on-screen computer output	`machine_name%` **`su`** `Password:`
AaBbCc123	Command-line placeholder: replace with a real name or value	To delete a file, type **`rm`** *filename.*
AaBbCc123	Book titles, new words, or terms, or words to be emphasized.	Read Chapter 6 in *User's Guide.* These are called *class* options. You must be *root* to do this.

Shell Prompts in Command Examples

The following table shows the default system prompts for administrative roles.

TABLE P–2 Shell Prompts

Shell	Prompt
administrative role prompt	$
root role prompt	#

CHAPTER 1

Security Overview

Trusted Solaris software implements a portion of your site's security policy. This chapter provides an overview of the security and administrative aspects of installation.

- "The Big Picture" on page 23 — For administrators of the Trusted Solaris operating environment.
- "Differences from Solaris 8 Installation and Configuration" on page 34 — For experienced Solaris administrators. Addresses specific differences from the Solaris operating environment.
- "Installation Results from an Administrator's Perspective" on page 34 — Describes the security features in effect after a host is installed.

See Appendix B for a checklist of Trusted Solaris 8 configuration tasks. Customers interested in localizing their site, see "For International Customers" on page 26. Customers interested in running an evaluated configuration, see "Understand Your Site's Security Policy" on page 24.

The Big Picture

This section outlines the planning required before installing and configuring the Trusted Solaris operating environment.

- "Understand the Trusted Solaris Environment" on page 24
- "Devise an Administration Strategy" on page 25
- "Devise a Label Strategy" on page 26
- "Plan User Security" on page 27

▼ Understand the Trusted Solaris Environment

Installation and configuration of the Trusted Solaris environment involves more than loading executable files, entering your site's data, and setting configuration variables. It requires considerable background. Trusted Solaris provides a unique environment based on the following concepts:

- Superuser has been eliminated. No one can log in as or `su` to root.
- Capabilities formerly assigned to superuser are available to discrete administrative roles to be assigned to a limited number of users.
- Users are limited to those applications necessary for performing their jobs.
- In addition to UNIX permissions, access to data is controlled by special security tags called sensitivity labels which are assigned to users and objects (such as data files and directories).
- The ability to override security policy can be assigned to specific users and applications.

To familiarize yourself with the Trusted Solaris environment, you should at a minimum read the *Trusted Solaris User's Guide* and *Trusted Solaris Administration Overview*. You should also be familiar with the rest of the documentation set, which is described in the *Trusted Solaris Documentation Roadmap*.

▼ Understand Your Site's Security Policy

Through its configurability, the Trusted Solaris environment effectively lets you integrate your site's security policy with the operating environment. Thus, you need to have a good feel for the scope of your policy and the ability of Trusted Solaris to accommodate it. A good configuration should provide a balance between consistency with your site security policy and convenience for those working in the environment.

The Trusted Solaris operating environment is configured by default to conform with the ITSEC evaluation certificate FB1 (and FC2 which is less stringent). To meet these evaluated levels, you must:

- Select NIS+ as the naming service.
- Select multiple-label environment operation for the FB1 level. The FC2 level permits single- or multiple-label operation.

Note that your configuration may no longer conform with the ITSEC security levels if you do any of the following:

- Change the kernel switch settings in the `/etc/system` file, other than those switches and their values documented in this manual.
- Provide security-relevant execution profiles to non-administrative users.
- Change the default entries in these configurable files:
  - `/usr/openwin/server/tsol/*`
  - `/usr/dt/app-defaults/C/Sel_Mgr`
  - `/usr/dt/bin/Xsession`
  - `/usr/dt/bin/Xtsolusersession`
  - `/usr/dt/config/sel_config`
  - `/usr/dt/app-defaults/C/Dtwm`
  - `/usr/dt/app-defaults/C/Dt`
  - `/usr/dt/config/C/sys.dtwmrc`

▼ Devise an Administration Strategy

The root role is mainly responsible for installing the Trusted Solaris 8 CD-ROM. After the initial Trusted Solaris installation, the root role is mostly not useful. In place of root or superuser, the Trusted Solaris environment suggests creating three or four administrative roles for managing the environment:

- The security administrator is responsible for security-related tasks, such as setting up and assigning sensitivity labels, configuring auditing, and setting password policy.
- The system administrator is responsible for the non-security aspects of setup, maintenance, and general administration.
- The primary administrator is responsible for creating rights profile for the security administrator, and for fixing things when the security and system administrators do not have the power.
- A less trusted role called “oper” for operator is responsible for backing up files.

As part of your administration strategy, you need to decide:

- Which users will be handling which administration responsibilities.
- Which non-administrative users will be allowed to run trusted applications, that is, will be permitted to override security policy when necessary.
- Which users will have access to which groups of data.

▼ Devise a Label Strategy

Planning labels requires setting up a hierarchy of sensitivity levels and a categorization of information in your environment. The “label encodings” file contains this type of information for your organization. You can use one of the label_encodings files supplied on the Trusted Solaris CD-ROM, modify one of the supplied files, or create a new label encodings file specific to your site. The file should include the SUN-specific local extensions (at least the COLOR NAMES section) when used in the Trusted Solaris environment.

Note - The default `label_encodings` file is useful for demos, but it is not a good choice for use by a customer site.

IMPORTANT: you must have the final version of the label encodings file ready prior to configuring the first workstation.

To learn more about the label encodings file, see *Trusted Solaris Label Administration*. You can also refer to *Compartmented Mode Workstation Labeling: Encodings Format*.

Planning labels also involves planning label configuration. After installation, you need to make the following decisions regarding the use of labels:

- Single- or multiple-label environment — If all of your non-administrative users can operate at the same security label, select a single-label system. Multiple-label environments are required for the FB1 level. If you want a no-label system, select single-label, and then hide the labels for all users.
- Hide or display upgraded names in directories — If you want to prevent a user (or intruder) from viewing the names of files or directories at higher levels than the current sensitivity label, choose this option.

After installation, you can make the following label configuration display changes using User Accounts:

- Display administrative label names — You can show the actual administrative label names, or show substitute names for the labels.
- Hide or display labels — You can hide or display labels on a per-user basis.

For International Customers

When localizing a `label_encodings` file, international customers should localize the label names *only*. The administrative label names, ADMIN_HIGH and ADMIN_LOW, must not be localized. All labeled workstations that you contact, from any vendor, must have label names that match the label names in the Trusted Solaris `label_encodings` file.

▼ Plan User Security

The software ships with reasonable security defaults for users, in two files listed in Table 1–1. Where two values are listed, the first value is the default. The security administrator can modify these defaults to reflect the site's security policy. After the security administrator has set the defaults, the system administrator can create all the users, who will inherit the established defaults. See the `label_encodings`(4) and `policy.conf`(4) man pages for a description of the keywords and values.

The system administrator can set up a standard user template that will set appropriate system defaults for users. For example, by default each user's initial shell is a Bourne shell. The system administrator can set up a template that gives each user a C shell by default. See the Solaris Management Console online help for User Accounts for more information.

TABLE 1–1 Trusted Solaris Security Defaults for User Accounts

File name	Keyword	Value
`/etc/security/policy.conf`	IDLECMD	**`lock`** | logout
	IDLETIME	**`30`**
	LABELVIEW	**`showsl`** | hidesl
	LOCK_AFTER_RETRIES	**`yes`** | no
	PASSWORD	**`manual`** | auto
	PROFS_GRANTED	**`Basic Solaris User`**
LOCAL DEFINITIONS section of `/etc/security/tsol/label_encodings`	Default User Clearance	**`c`**
	Default User Sensitivity Label	**`u`**
	Admin Low Name	**`ADMIN_LOW`**
	Admin HIgh Name	**`ADMIN_HIGH`**
	Default Label View	**`External`** | Internal

Note - Each site should replace the label encodings file provided on the Trusted Solaris CD with their own. Their file should have appropriate values for the label encodings keywords.

▼ Plan Workstation Hardware and Capacity

Workstation hardware includes the workstation itself and its attached devices (tape drives, microphones, CD drives, and disk packs). Its capacity includes its memory, its network interfaces, and its disk space.

Consult the *Solaris 8 Sun Hardware Platform Guide* for a list of hardware that supports the Trusted Solaris environment. Any exceptions are noted in *Trusted Solaris 8 Release Notes*.

Peripheral hardware and capacity required for initial installation on a SPARC include:

- 64 MB minimum memory — 256 MB memory recommended to handle Solaris Management Console requests
- Local CD-ROM drive

Memory over the minimum is required on Trusted Solaris workstations that:

- Are used as servers: name servers, file servers, audit servers, boot servers
- Run graphics or other large applications
- Run compilers
- Run number-crunching applications
- Run at more than one sensitivity label
- Are used by users who can assume an administrative role

Similarly, disk space requirements are greater for some workstations. See “Disk Space Planning” in *Solaris 8 Advanced Installation Guide* for a list of factors that affect disk space. Particular Trusted Solaris features that require more disk space include:

- Disks with files stored at more than one label
- Disks that are used by users who can assume an administrative role

For each Trusted Solaris workstation, you need to determine the following:

- Name and IP address
- Ethernet address (for network installations)
- Sun architecture (for network installations)
- Root password
- PROM security level: maintenance password only, or boot password

- PROM password (for Intel Architecture: BIOS protection)
- What devices may be attached to the workstation
- Which users may use the workstation
- Which printers at what labels are accessible from the workstation

▼ Plan Your Network

If you are installing a non-networked workstation, you can skip this step.

For help in planning network hardware, see "Planning Your TCP/IP Network" in *System Administration Guide, Volume 3*.

As in any client-server network, you need to identify hosts by their function (server or client) and configure the software appropriately. The following table lists servers you may need to create and their function. For more information, see *System Administration Guide: Basic Administration*.

TABLE 1–2 Possible Servers in a Trusted Solaris Environment

Create ...	**If You Plan to ...**
Audit data server	Enable auditing
Audit administration server	Analyze the audit trail
File server	Centrally locate files for general use
Install server	Install over the network or use Custom JumpStart scripts
DNS server	Resolve internet names and addresses outside your local network
Home directory server	Enable remote mounting of users' home directories. Required in a name service environment.
Mail server	Funnel mail to end user workstations from a central location
Network gateway	Operate an open network
Name Service Servers	Establish a NIS or NIS+ domain
Print server	Print hard copy

To plan the system administration aspects of servers, see the administration guides in the *Solaris 8 System Administrator Collection* including:

- *System Administration Guide, Volume 1*
- *System Administration Guide, Volume 2*

Trusted Solaris–specific administration is covered in *Trusted Solaris Administrator's Procedures*.

Additional Planning for Open Networks

If your network is open to other networks, you need to specify accessible domains and workstations, and identify which Trusted Solaris hosts will serve as gateways to access them. You need to identify the Trusted Solaris accreditation range for these gateways, and the sensitivity label at which data from other hosts may be viewed. Trusted Solaris software recognizes four labeled host types, including Trusted Solaris (`sun_tsol`), and provides eleven templates by default, as shown in Table 1–3. The unlabeled template names correspond to the label names in the demo `label_encodings`(4) file installed from the Trusted Solaris CD.

TABLE 1–3 Templates Provided with Trusted Solaris Network Software

Host Type	Template Name	Purpose
Unlabeled	`admin_low`	For initial boot, before the host is configured with Trusted Solaris software.
	`unclassified`	For hosts or networks that send unlabeled packets, for example, SUN workstations running Solaris software.
	`confidential`	
	`secret`	
	`top_secret`	
Labeled		
Trusted Solaris (`sun_tsol`)	`tsol`	For Trusted Solaris 2.5.1, 7, and 8 hosts or networks.
	`tsol_ripso`	For Trusted Solaris 2.5.1, 7, and 8 hosts or networks that label packets with the RIPSO security option.

TABLE 1–3 Templates Provided with Trusted Solaris Network Software *(continued)*

Host Type	Template Name	Purpose
	`tsol_cipso`	For Trusted Solaris 2.5.1, 7, and 8 hosts or networks that label packets with the CIPSO security option.
TSIX	`tsix`	For TSIX(RE1.1) hosts or networks.
CIPSO	`cipso`	For hosts or networks that send CIPSO packets.
RIPSO	`ripso_top_secret`	For hosts or networks that send RIPSO Top Secret packets.

The `tnrhtp`(4) man page gives complete descriptions of each host type with several examples.

▼ Plan Auditing

Auditing requires the storage and analysis of potentially a huge amount of data. Before you set up auditing, you need to:

- Decide which classes of activity you need to audit. It is good practice to keep these to a minimum.
- Plan how you are going to handle the storage and administration of the auditing data.

  Each host should have a disk dedicated to audit data collection with a primary partition and a second partition for overflow records.

  If you are auditing a network, you should dedicate at least one server to data collection and another server to data administration and analysis. Ideally, you should have your primary and secondary data collection areas on different hosts. In addition, it is recommended that you reserve a fallback area on the local hosts in case the network goes down.
- Read *Trusted Solaris Audit Administration* for step by step assistance.

▼ Devise an Installation and Configuration Strategy

The Trusted Solaris software is initially loaded by root. Since root cannot log into the Trusted Solaris environment, a local user named “install” has been provided for the first part of the configuration process. Subsequent configuration is a two-person process (by default) using the security administrator and the system administrator

roles. Once the roles have been assigned to users, and the workstation is rebooted, the software enforces task division by role.

If two-person installation is not a site security requirement, assigning the two administrative roles to one person enables that person to configure both security and system information.

In a name service environment, you should install and configure workstations in the order:

1. Name service master
2. Home directory server
3. Install server
4. Other name service servers
5. Other servers
6. End user workstations

▼ Collect Information

Each role needs to gather the information for the tasks particular to the role. Concrete examples are in Appendix B.

▼ Back Up the Workstation

If your workstation has any files on it that you want to save, make sure you perform a backup. The safest way to back up files is to do a level 0 dump. If you do not have a backup procedure in place, see the administrator's guide to your current operating system for instructions.

Note - If you are migrating from Trusted Solaris 2.5, Trusted Solaris 2.5.1, or Trusted Solaris 7 to the Trusted Solaris 8 release, and you want to retain some profile and user information, be sure to convert the `tsoluser` and `tsolprof` databases to their Trusted Solaris 8 formats *before* installing Trusted Solaris 8. See the `tsolconvert` man page on the Trusted Solaris web site, `http://www.sun.com/software/solaris/trustedsolaris/ts_tech_faq/`. Backup and conversion *must be completed* before Trusted Solaris 8 is installed.

▼ Install the Trusted Solaris Software

Installing Trusted Solaris can be done interactively using CD-ROMs, over the network, or with Custom JumpStart™ scripts. The first three workstations, the name service master (NIS or NIS+) , the home directory server, and the install server (if you wish to do network or Custom JumpStart installs), must be installed from the CD-ROM. Subsequent workstations can be installed using the server.

Installing over the network requires network setup. The installation program prompts the install team for needed information. Using Custom JumpStart requires some knowledge of Bourne shell scripting to automate installation. However, you can write scripts where no human interaction with the installation program is required.

For security reasons, the installation program does not offer some of the options that are available for Solaris 8 software. See “Differences from Solaris 8 Installation and Configuration” on page 34 for details.

▼ Configure the Software

After the installation image is installed, the install team logs in as the user “install” and assumes the root role to configure initial security, network, and administrative role information, as shown in the following figure.

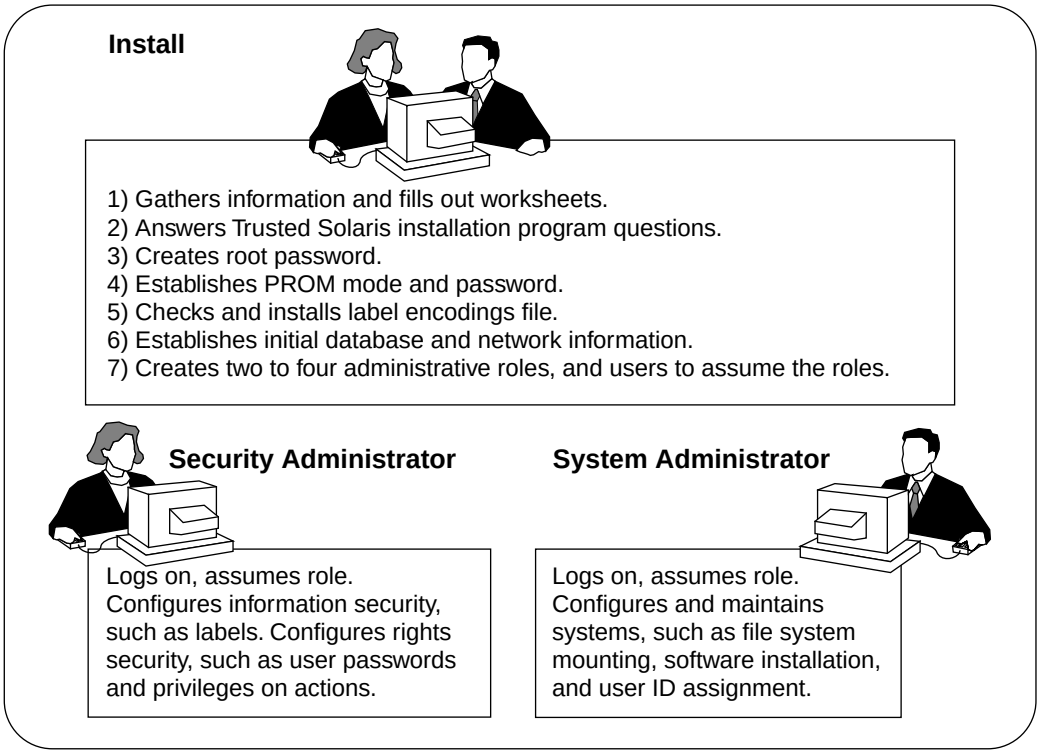


Figure 1–1 Two Roles Administering a Workstation

Once users who can assume the administrative roles are created, the install team reboots the workstation. Further configuration tasks are then partitioned by the software to a particular role.

The security administrator sets up auditing, protects file systems, sets device policy, determines which programs require privilege to run, and protects users, among other

tasks. The system administrator shares and mounts file systems, installs software packages, and creates users, among other tasks.

Differences from Solaris 8 Installation and Configuration

CDE is the only desktop supported and installed by Trusted Solaris software, and the Solaris Management Console™ GUIs manage local and network administrative databases.

Some options that are available when installing Solaris 8 software are not available when installing Trusted Solaris 8 software. Specifically,

- No remote file system mounting during installation. File systems are mounted after installation.
- Upgrade is not supported. However, there are manual steps to perform for keeping user and profile databases from earlier Trusted Solaris releases.
- Solaris™ Web Start install is not supported.

Note - Trusted Solaris 8 supports the Volume Manager and the name services that are supported by the Solaris 8 release, including the NIS name service.

Installation Results from an Administrator's Perspective

After installing Trusted Solaris software, the following security features are in place. Many features are configurable by the security administrator.

- Auditing is enabled.
- A SUN label_encodings file is configured and installed.
- CDE creates four labeled workspaces.
- Rights profiles for Trusted Solaris administrative roles are defined. It is the install team's job to create the roles.
- The Solaris Management Console enables administrative roles to administer user, execution profile and other system databases.
- A trusted editor enables administrators to modify local administrative files. It is implemented as a CDE action named Admin Editor.

- Trusted Solaris-defined CDE actions to view and edit local administrative files in a trusted editor are available to users in administrative roles.
- The Device Allocation Manager manages attached devices.
- Three Trusted Solaris-defined databases, `tnidb`, `tnrhtp`, and `tnrhdb`, handle trusted networking. They are administered using the Interface Manager and Security Families tools in the Solaris Management Console.

CHAPTER 2

Installation Task Maps

This chapter outlines the tasks for installing and configuring the Trusted Solaris operating environment, and where the procedures are documented.

Where Do I Go?

The following task maps direct you to the book, or the book and chapter of the task you want to do. Note that some tasks require that you use a Solaris book for the main steps of the task, and a Trusted Solaris book for security modifications. Modifications include assuming a role, operating at a label, and using a trusted program.

TABLE 2–1 Task Map: To Prepare for Installation

If you want to ...	Then, go to ...
Use data from Trusted Solaris 2.5, Trusted Solaris 2.5.1 or Trusted Solaris 7 tsoluser, tsolprof, tnidb, tnrhtp, or tnrhdb databases in Trusted Solaris 8.	"How to Save and Restore Trusted Solaris Databases" on page 81.
Back up a Trusted Solaris host.	*Trusted Solaris Administrator's Procedures*
Back up a Solaris host.	*System Administration Guide, Volume I*
Find out what hardware is supported in this release.	*Solaris 8 Sun Hardware Platform Guide*

TABLE 2–1 Task Map: To Prepare for Installation *(continued)*

If you want to ...	Then, go to ...
Shut down a Trusted Solaris host.	"Shut Down a Trusted Solaris system" on page 85.
Shut down and reboot a Solaris host.	*Solaris 8 (SPARC Platform Edition) Installation Guide* or *Solaris 8 (Intel Platform Edition) Installation Guide*

TABLE 2–2 Task Map: To Choose an Installation Method

If you want to ...	Then read ....
Find out what installation methods are available.	*Solaris Advanced Installation Guide* Note that the Solaris Web Start method is not supported.
See an example of a jumpstart install.	*Solaris Advanced Installation Guide*

TABLE 2–3 Task Map: To Use an Installation Method

If you want to ...	Then follow the instructions in ....
Install from a CD–ROM.	Chapter 4 and for greater detail — *Solaris 8 (SPARC Platform Edition) Installation Guide* or *Solaris 8 (Intel Platform Edition) Installation Guide*
Install over the network.	Chapter 9, for differences from Solaris procedures, and for Solaris procedures, read — *Solaris Advanced Installation Guide*

TABLE 2–4 Task Map: To Configure Your Machine after Installation

If you want to ...	Then follow the instructions in ....
Set up a host with no name service	Chapter 5
Set up a Trusted Solaris NIS+ network.	Chapter 6
Set up a Trusted Solaris NIS name service.	Chapter 7
Set up NIS or NIS+ clients.	Chapter 8
Install Trusted Solaris over the network.	*Solaris 8 Advanced Installation Guide*, with Trusted Solaris modifications from Chapter 9.
See a checklist of all tasks to be completed.	Appendix B
Complete other tasks.	*Trusted Solaris Administrator's Procedures*

CHAPTER 3

Basic Procedures

This chapter covers common administrative procedures when configuring a Trusted Solaris host. Later chapters point to the procedures in this chapter.

Note - Installation and configuration commands and actions are limited to particular roles and particular labels. Read each task for the administrative role that can perform it, and the label required. After doing the task, return to the installation and configuration chapter you were working from.

How to Log In

The predefined user `install` logs in immediately after installation to configure the workstation. At most sites, two or more administrators, an install team, are present when configuring the workstation. “You”, in the following procedure, refers to the install team.

▼ To Log In as the User Install

1. **Log in to the workstation as the user** `install`**.**
   a. **Enter** `install` **as the user name and press the** Return **key.**
      The Password dialog box is displayed.
   b. **Enter** `install` **for the password.**
      The Enable Logins dialog offers four choices, as shown in the following figure:

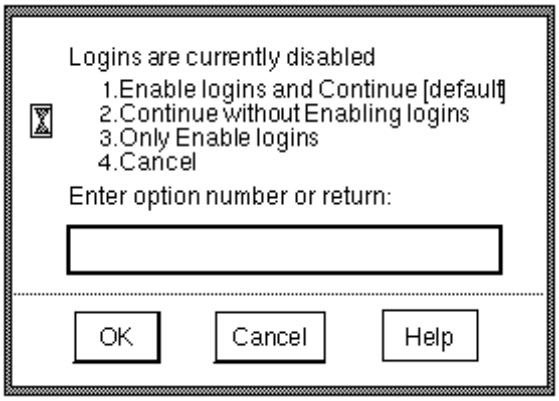


Figure 3–1 The Enable Logins Dialog

c. Depending on site security requirements, enter 1 or 2, then click OK.
The Message Of the Day dialog is displayed; the label is `ADMIN_LOW`.

d. Click OK to dismiss the dialog.
The Trusted Solaris screen appears briefly; then you are in a CDE workspace, as shown in Figure 3–2. The trusted stripe below the front panel shows the window sensitivity label.

2. Return to the procedure and chapter you are working from.

▼ To Log In as a Regular User

1. Log in to the workstation using your user account name.

2. Enter your password.

Note - Users must not disclose their passwords to another person, as that person may then have access to the data of the user and will not be uniquely identified or accountable. Note that disclosure can be direct, through the user deliberately disclosing his/her password to another person, or indirect, such as through writing it down, or choosing an insecure password. Trusted Solaris provides protection against insecure passwords, but cannot prevent a user disclosing his/her password or writing it down.

The Enable Logins dialog, shown in Figure 3–1, is displayed if you are authorized to enable logins.

If you see the error message:

```
Logins are currently disabled.
Please ask your system administrator to enable logins.
```

then your user was not assigned the Enable Login right (see Table 3–4). To fix, give the user the Enable Login right, or have someone else log in and enable logins.

3. **Choose a login option and dismiss the dialog.**

   The Message Of the Day dialog is displayed. In a multilevel session, the default is to log in at the lowest label in your label range. You can also restrict your session to a single label.

4. **Click OK to accept the default given to you by the security administrator.**

   Once the login process is complete, the Trusted Solaris screen appears briefly, and you are in a CDE session with four workspaces. If your user account is configured to display labels, the label of your session (a user account *cannot* be `ADMIN_LOW`) will show in the trusted stripe.

Note - The install team must log off or utilize the lockscreen functionality before leaving a workstation unattended. Otherwise a person may have access to the workstation without having to pass identification and authentication, and that person would not be uniquely identified or accountable.

---

5. **Return to the procedure and chapter you are working from.**

How to Assume a Role

An administrative role configures the workstation, however, a role cannot log in. Users log in, and assume one or more of their assigned roles. The role `root` has been pre-assigned to the user `install`.

▼ To Assume a Role

1. **Log in to the workstation as a user, such as `install`.**

2. **Right click on the middle of the Front Panel.**

3. **Assume a role from the roles displayed on the TP (Trusted Path) menu.**

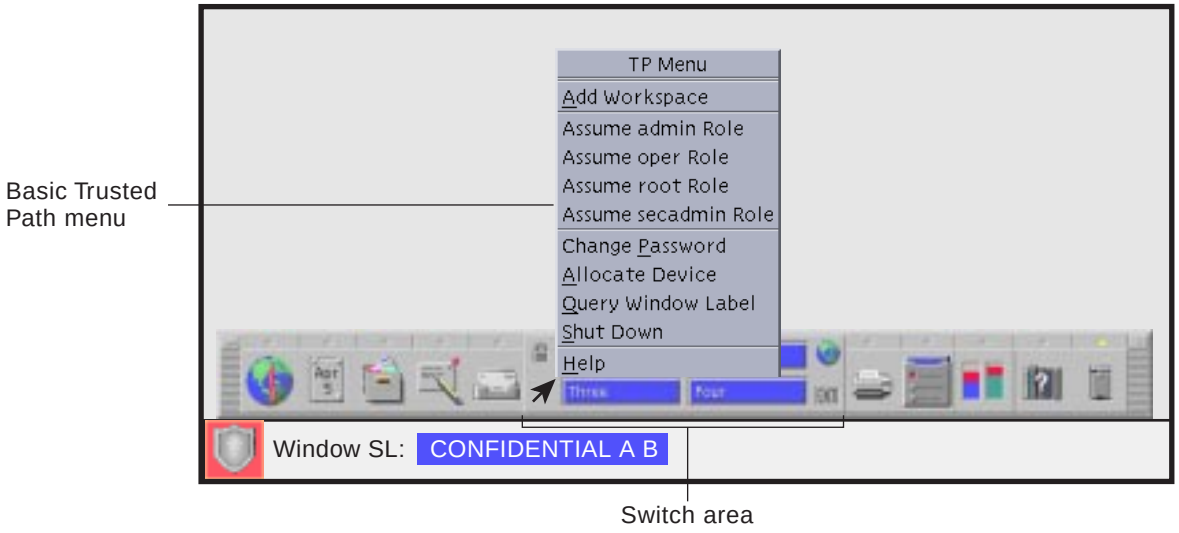


Figure 3–2 A Trusted Solaris User Workspace

After initial installation from a CD-ROM, only the root role will be displayed on the TP menu, since no other roles have been created.

   a. **Choose Assume *rolename* Role from the menu.**

   b. **At the password prompt, enter the password for the role.**

      The password for the root role is the password that the install team entered for root at the final stage of installation.

4. **Return to the procedure and chapter you are working from.**

How to Launch a Terminal

Use the background menu to launch a terminal. The terminal displays the default shell for the user or role who launches the terminal.

▼ To Launch a Terminal

1. **Right-click on the workstation background and select Tools > Terminal from the Workspace Menu.**

   Note - The Options menu enables you to customize the appearance of the terminal. Customizations for the user “install” are not saved.

2. **Return to the procedure and chapter you are working from.**

How to Create an Admin_High Workspace

Some administrative actions require a process at a higher label than the default. To get a higher-labeled process, create a workspace at that higher label, and launch actions and terminals from the new workspace.

Note - If you are not allowed to change the workspace label, the Change Workspace Label menu item is not displayed.

▼ To Create an Admin_High Workspace

1. **Click the right menu button on workspce label for the TP menu.**

2. **Choose Change Workspace Label from the menu, select the** `ADMIN_HIGH` **label and click OK.**

Actions, terminals, commands and windows originating from the newly labeled workspace run at the label of the workspace.

3. **Return to the procedure and chapter you are working from.**

How to Protect Machine Hardware

For security, access to the PROM should also be protected with a password.

▼ SPARC: To Set the PROM Mode and Password

- **As root, label** `ADMIN_LOW`**, in the profile shell, enter the PROM security mode.**
  - **Choose the value** `command` **or** `full` **(see the** `eeprom`**(1M) man page for more details).**
    You are prompted to enter and confirm the PROM password.

```
# eeprom security-mode=command

Changing PROM password:
 New password: password
 Retype new password: password
```

  - **If you are not prompted to enter a PROM password, the workstation already has a PROM password. To change it, run the command:**

```
# eeprom security-password=Return
Changing PROM password:
New password: password
Retype new password: password
```

The new PROM security mode and password are in effect immediately, but are most likely to be noticed at the next boot.

Caution - Do not forget this password. The hardware is unusable without it.

For more information on PROM values that you can set, see *OpenBoot 2.x Command Reference Manual* or *OpenBoot 3.x Command Reference Manual*.

▼ IA: To Protect the BIOS

On Intel architecture, the equivalent to protecting the PROM is to protect the BIOS.

- **Refer to your machine's manuals for how to protect the BIOS.**

How to Allocate and Deallocate a Device

Users and roles must allocate a device for exclusive use before using it. Allocatable devices include audio, floppy, CD-ROM, and tape devices. The Device Allocation action handles device allocation and administering device allocation.

▼ To Allocate a Device

1. **In a workspace at the target label, click the left mouse button on the triangle above the Style Manager icon on the Front Panel.**

Its Tools subpanel includes the Device Allocation icon.

2. **Click the Device Allocation icon once.**

3. **Double-click the device to be allocated from the list of available devices.**
   floppy_0 allocates a diskette.

4. **Click** `Yes` **to the mount question.**

A File Manager pops up showing the mount point. (If it does not pop up, open a File Manager from the Front Panel, navigate to /, and double-click `floppy`.)

5. **If you are in the admin role allocating a CD-ROM for network installation, see "Additional Steps to Set up Software Installation" on page 139 for additional steps. Otherwise, return to the procedure and chapter you are working from.**

▼ To Deallocate a Device

1. **Go to the workspace where the Device Allocation action is displayed.**

   If it is not displayed, click the Device Allocation icon

   on the Tools subpanel, at the same label and in the same role as the one who allocated the device.

2. **Double-click the device to be deallocated from the list of allocated devices.**

3. **Remove the device and click `OK` in the Deallocation dialog.**

4. **Return to the procedure and chapter you are working from.**

How to Copy to and from a Portable Medium

When copying to a portable medium, label the medium with the sensitivity label of the information.

Note - During installation, the role `root` copies administrative files to and from portable media. Most files are copied at label `ADMIN_LOW`. The two exceptions are the `label_encodings` and `vfstab_adjunct` files, that are labeled `ADMIN_HIGH`.

▼ To Copy to a Diskette

1. **First, in a workspace at the target label, allocate the floppy device at the correct label using the Device Allocation action, and insert a clean diskette.**

   For a fuller description, see “To Allocate a Device” on page 47.

2. **Open a second File Manager from the Front Panel and navigate to the folder that contains the files to be copied, such as** `/export/clientfiles`**.**

3. **Rename the** `label_encodings` **file that you are copying.**

   For example, name it `label_encodings.site` (for SPARC architecture), or `lblcdsit` (for Intel architecture). Audit system files such as `audit_event`, and routing files such as `nsswitch.conf`, and `resolv.conf` do not need to be renamed.

4. **Highlight the icon for the file and drag the file to the floppy disk folder.**

5. **Deallocate the device, as described in “To Deallocate a Device” on page 48.**

6. **On the floppy disk folder, choose Eject from the File menu.**

   Note - Remember to physically affix a label to the medium with the sensitivity label of the copied files.

   ---

7. **Return to the procedure and chapter you are working from.**

▼ To Copy from a Diskette

It is safe practice to rename the original Trusted Solaris file before copying in a file to replace it. During installation, the root role renames and copies administrative files at `ADMIN_LOW`

1. **Allocate the floppy device using the Device Allocation action and insert the diskette.**

   For a fuller description, see “To Allocate a Device” on page 47. The `label_encodings` file requires a diskette allocated at the label `ADMIN_HIGH`.

2. **If the workstation has a file of the same name, copy it to a new name and remove the original.**

Note - Exception: If the file you are copying is to replace the current `label_encodings` file, do not rename or remove the original file. See "How to Install a Label Encodings File" on page 59 for the full procedure.

3. **Open a second File Manager from the Front Panel and navigate to the desired destination directory, such as** `/etc/security/tsol`**.**
4. **Highlight the icon for the file and drag the file from the floppy disk folder to the destination directory.**
5. **Deallocate the device as described in "To Deallocate a Device" on page 48.**
6. **Click OK on the dialog when prompted to manually eject** `/dev/rdiskette`**, and eject the floppy.**
7. **Return to the procedure and chapter you are working from.**

How to Run Administrative Actions

The Application Manager contains a folder that holds administrative applications for the local machine, `System_Admin` and an action, `Solaris Management Console`, for administering local and distributed databases.

How To Use System_Admin Actions

The System_Admin folder contains CDE actions for administering the local workstation. See the following table for a list of actions used during installation and configuration. For a full list of System_Admin actions, read the CDE online help.

TABLE 3–1 Trusted Solaris Actions in the System_Admin Folder

Action Name	Action Behavior
Add Allocatable Device	Edit `/etc/security/device_maps`
Admin Editor	Create or edit any file
Audit Classes	Edit `/etc/security/audit_class`
Audit Control	Edit `/etc/security/audit_control`
Audit Events	Edit `/etc/security/audit_event`
Audit Startup	Edit `/etc/security/audit_startup`
Audit Users	Edit `/etc/security/audit_user`
Check Encodings	Check syntax (and install) a label encodings file
Check TN Files	Check local `tnrhdb` and `tnrhtp` files
Check TN NIS+ Tables	Check NIS+ `tnrhdb` and `tnrhtp` databases
Create NIS Client	Make this host a NIS client
Create NIS+ Client	Make this host a NIS+ client
Create NIS Server	Establish a NIS server with NIS maps
Create NIS+ Server	Establish a NIS+ domain
Configure Selection ...	Edit `/usr/dt/config/sel_config`
Edit Encodings	Edit a label encodings file
Name Service Switch	Edit `/etc/nsswitch.conf`
Populate NIS+ Tables	Populate NIS+ tables from a files directory
Set Default Routes	Edit `/etc/defaultrouter`
Set DNS Servers	Edit `/etc/resolv.conf`
Set Mount Attributes	Edit `/etc/security/tsol/vfstab_adjunct`

TABLE 3–1 Trusted Solaris Actions in the System_Admin Folder *(continued)*

Action Name	Action Behavior
Set Mount Points	Edit `/etc/vfstab`
Set TSOL Gateways	Edit `/etc/tsolgateways`
Share Filesystems	Edit `/etc/dfs/dfstab`

▼ To Run a System_Admin Action

1. **In an administrative role, open the Application Manager by right-clicking the background to bring up the Workspace menu. Choose Applications > Application Manager from the top of the menu.**
2. **Double-click the System_Admin folder icon —** 
3. **Double-click the appropriate action. For more details, see "To Create or Open a File from the Trusted Editor" on page 52, "To Open a File that has a Defined Action" on page 53 and "To Run a Script from the System_Admin Folder" on page 53.**

▼ To Create or Open a File from the Trusted Editor

1. **To create or open a file that does not have its own action, double-click the Admin Editor action.**

   A prompt appears for you to specify the file to be opened.

2. **Enter the name of the file to be opened.**

    If the file exists, it is opened. If the file does not exist, it is created. You can create an empty file (`touch`) by exiting the editor.

Note - You cannot save a file to a different name from the trusted editor.

---

3. **Return to the procedure and chapter you are working from.**

▼ To Open a File that has a Defined Action

1. **To open a file that has its own action, double-click its action in the System_Admin folder.**

    The file associated with the action appears in the trusted editor.

2. **Enter the required information, write the file, and exit the editor.**

3. **Return to the procedure and chapter you are working from.**

▼ To Run a Script from the System_Admin Folder

1. **To run a script that has its own action, double-click the action in the System_Admin folder.**

   When the script requires input, the prompts are displayed.

2. **Follow the instructions.**

    The script is finished when all prompt windows have been dismissed.

3. **Return to the procedure and chapter you are working from.**

How to Use the Solaris Management Console

The Solaris Management Console action in the Application Manager folder invokes a Java-based administrative GUI for configuring and maintaining a Trusted Solaris environment. The GUI lists toolboxes in a Navigation pane.

The following can be configured through the Solaris Management Console, using the Trusted Solaris Management Console > Trusted Solaris Configuration toolboxes in the Navigation pane:

User Accounts	Part of the Users tool, for administering users.
Administrative Roles	Part of the Users tool, for administering roles.

Rights	Part of the Users tool, for constructing rights profiles. A user account is not usable until the user's Rights have been assigned.
Mailing Lists	Part of the Users tool, for administering mail aliases.
Computers and Networks	For setting up networks.
Computers	Part of the Computers and Networks tool, for setting up hosts (the `hosts` database).
Security Families	Part of the Computers and Networks tool, for creating and assigning remote host templates (the `tnrhtp`(4) and `tnrhdb`(4) databases).
Interface Manager	For securing network interfaces (the `tnidb`(4) database). Accessible only when `Scope=Files`.

The following are configured through the Solaris Management Console, using Trusted Solaris Management Console toolboxes:

Mounts	Part of the Storage tool, for mounting file systems. Accessible only when `Scope=Files`.
Shares	Part of the Storage tool, for sharing file systems. Accessible only when `Scope=Files`.

▼ To Initialize the SMC Server

1. **In the root role, open the Application Manager by right-clicking the background to bring up the Workspace menu. Choose Applications > Application Manager from the top of the menu.**

2. **Double-click the Solaris Management Console action.**

Note - The Solaris Management Console action initiates the SMC server. The first time the server is launched, it performs several registration tasks, which can take from 5 to 10 minutes. The following message may appear briefly: "There is no Solaris Management Console server …". The message goes away, and can be ignored.

---

3. **If the Navigation Pane is not visible and no toolboxes are displayed, do the following:**
   a. **In the Open Toolbox dialog that is displayed, click Load next to where this machine's name is listed under Server.**
      If this machine does not have the recommended amount of memory and swap, it may take a few minutes for the toolboxes to display. See "Recommendations for the Trusted Solaris Environment" on page 84.
   b. **From the list of toolboxes, select Trusted Solaris Management Console, then click the Open button.**
   c. **Before continuing, save the current setting as described in "To Save the Current Toolbox" on page 55.**

4. **If the Navigation pane is visible, but the toolbox icons are stop signs, do the following:**
   a. **Select the Trusted Solaris Management Console toolbox.**
   b. **Click the Open Toolbox button.**
   c. **Click Load next to** `Server:` *this_machine_name***.**
   d. **From the list of toolboxes, select Trusted Solaris Management Console, then click the Open button.**
   e. **Before continuing, save the current setting as described in "To Save the Current Toolbox" on page 55.**

▼ To Save the Current Toolbox

Save the toolbox preference to provide the Trusted Solaris Management Console toolboxes by default. The preferences are saved per role, per host (SMC server).

1. **From the Console menu, choose Preferences.**
2. **Click the Use Current Toolbox button, then OK.**
3. **Return to the procedure and chapter you are working from.**

▼ To Select a Toolbox of the Appropriate Scope

Prerequisite: The Solaris Management Console (SMC) server has been initialized on this computer, the Trusted Solaris Management Console toolboxes have been saved as the current toolbox, and they are displayed in the Navigation pane.

- **Select the toolbox of the appropriate scope:**
  - OPTION 1: Select *this_host*: `Scope=Files, Policy=TSOL` if you plan to administer each machine locally, or are administering files that can only be administered locally, such as local users (like root or install), the `tnidb`(4) database, or the local `tnrhdb`(4) database before the name service has been established.
  - OPTION 2: Select *name_server*: `Scope=`*name_service*`, Policy=TSOL` if you are administering name service maps or tables, and have established the name service domain and have edited the toolbox with the name of the server and the domain on this client machine (see "To Edit Name Service Toolbox Definitions" on page 57).

▼ To Locate a Solaris Management Console Tool

`Scope=Files` and `Scope=`*name_service* contain different tools.

1. **To find aand use a tool in** *this_host*: `Scope=Files, Policy=TSOL` **in the Navigation pane:**
   - Click the System Status key to view the Processes and Log Viewer tools.
     - To manage and monitor system processes, double-click Processes.
     - To see the logs monitored by WBEM, double-click Log Viewer.
   - Click the Trusted Solaris Configuration key to view the Users, Computers and Networks, and Interface Manager tools.
     - To add or modify a user, a role, a right, a group, or a mailing list on this machine, double-click Users.
     - To add or modify a remote host definition for this machine, double-click Computers and Networks.
       - To add or modify a host, double-click Computers, select a computer, then choose an item from the Action menu.
       - To add or modify a remote host template, double-click Security Families, then choose an item from the Action menu.
       - To add or modify a remote host template assignment, double-click Security Families, double-click a template name, then choose Add Host(s) from the Action menu.

- To modify the security attributes of a network interface, double-click Interface Manager.
- Click the Services key to view the SMC Server and the Scheduled Jobs tools.
  - The SMC Server tool is not fully implemented.
  - To see this machine's scheduled jobs, double-click Scheduled Jobs.
- Click the Storage key to view the Mounts and Shares and Disks tools.
  - To mount a remote file system, double-click Mounts and Shares, then Mounts.
  - To share a file system, double-click Mounts and Shares, then Shares.
  - To view and format disks, double-click Disks.
- Click the Devices and Hardware key to view the Serial Ports tool. Double-click Serial Ports to configure and manage existing serial ports.

2. **To find and use a tool in the** *name_server*`: Scope=`*name_service*`, Policy=TSOL` **toolbox in the Navigation pane, click the Trusted Solaris Configuration key to view the Users and the Computers and Networks tools:**
   - To add or modify a user, a role, a right, a group, or a mailing list on the domain, double-click Users.
   - To add or modify a remote host definition on the domain, double-click Computers and Networks.
3. **When prompted, enter the role password in the Role Login prompt.**
4. **Read and follow the online help for assistance with each tool.**
5. **Return to the procedure and chapter you are working from.**

▼ To Edit Name Service Toolbox Definitions

If you are running a NIS or NIS+ name service, the `tsol_nis.tbx` or `tsol_nisplus.tbx` file must be edited on the name service master before it can be used on the domain.

If administrators plan to administer the name service's tables or maps from a client machine, this procedure must be done on the client.

Note - Administrators who want to administer a name service using SMC *must* do this procedure on every machine that will be used to administer the name service.

---

1. **In the root role at the label** `ADMIN_LOW`**, change to the toolboxes directory and list the toolboxes.**

```
# cd /var/sadm/smc/toolboxes
# ls tsol*/*tbx
tsol_files/tsol_files.tbx        tsol_nis/tsol_nis.tbx
tsol_smc/tsol_smc.tbx            tsol_nisplus/tsol_nisplus.tbx
```

- If you are running the NIS+ name service, your toolbox file is `tsol_nisplus/tsol_nisplus.tbx`
- If you are running the NIS name service, your toolbox file is `tsol_nis/tsol_nis.tbx`

2. **Invoke the Admin Editor, as described in "To Create or Open a File from the Trusted Editor" on page 52.**

3. **Copy and paste the full pathname to the toolbox into the dialog, as in:** `/var/sadm/smc/toolboxes/tsol_nisplus/tsol_nisplus.tbx`

4. **In the editor, replace each instance of** `<?server ?>` **with either the name of the master server or the name of the domain.**

   a. **In the line beginning with** `<Scope>`**, replace the first instance of** `<?server ?>` **with the name service master, and the second with the fully-qualified domain name, as in:**

```
<Scope>nisplus:/toucan/aviary.eco.org</Scope>
```

   b. **Replace every other instance of** `<?server?>` **or** `<?server ?>` **with the name service master, as in:**

```
<Name>  toucan: Scope=NIS+, Policy=TSOL</Name>
services and configuration of toucan.</Description>
and configuring toucan.</Description>
<ServerName>toucan</ServerName>
<ServerName>toucan</ServerName
```

5. **Write (**`:wq!`**) and quit the editor.**

6. **Return to the procedure and chapter you are working from.**

How to Install a Label Encodings File

Consult *Trusted Solaris Label Administration* for requirements, procedures, and suggestions for the label encodings file.

You can edit the placeholder `label_encodings`(4) file that the Trusted Solaris installation program installed, or install your own. The security administrator is responsible for editing, checking, and maintaining the `label_encodings` file.

Note - The `label_encodings` file is protected at the label `ADMIN_HIGH`. For security, copy, edit, check and install your label encodings file at `ADMIN_HIGH`.

▼ To Install a Site-Specific Label Encodings File

1. **In the root role (before other roles are created), or in the secadmin role (after roles have been created and verified), create an `ADMIN_HIGH` workspace.**

   See "How to Create an Admin_High Workspace" on page 45 if you are unfamiliar with operating at the label `ADMIN_HIGH`.

2. **Copy your site's label encodings file from an `ADMIN_HIGH` diskette to a writable location, such as `/export/clientfiles/label_encodings.site` using the File Manager.**

   If you are unsure of the steps, see "To Copy from a Diskette" on page 49.

   If you plan to tweak the file, make sure that the file itself is writable.

3. **Check the syntax of the new label encodings file.**

   a. **Double-click the Check Encodings action in the System_Admin folder in the Application Manager.**

      For more information on running a script from the System_Admin action, see "To Run a Script from the System_Admin Folder" on page 53. You can ignore any Trash Can Error dialog error messages.

   b. **In the dialog box, enter the full path name of the file:**
      `/export/clientfiles/label_encodings.site`

4. **Read the contents of the Check Encodings dialog box that is displayed.**

   The `chk_encodings`(1M) command checks the syntax of the file. If the file passes the check, the action asks whether you want to overwrite the currently-installed `label_encodings` file. If the answer is `yes`, the action

creates a backup copy (naming it `label_encodings.orig`), installs the checked version, then restarts the label daemon.

CONTINUE Only if it reports no errors can you continue installing.

RESOLVE ERRORS If it reports errors, they *must* be resolved before continuing with installation.

For detailed procedures and explanation, consult "Creating or Editing the Encodings File" in *Trusted Solaris Label Administration*.

Caution - Your label encodings file *must* pass the Check Encodings test before you continue.

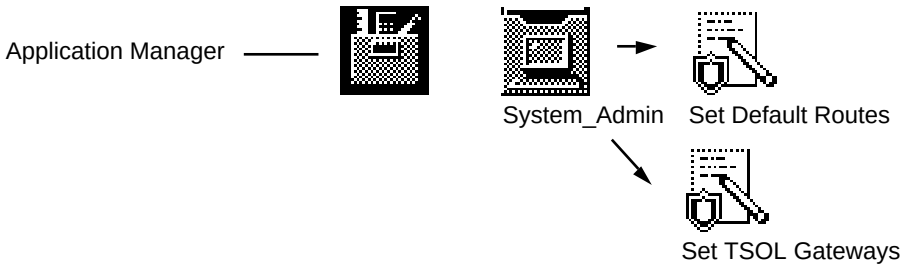
How to Set Up Static Routing

Routing is required only if the security administrator has planned for an open network. There are three routing methods available: dynamic routing (the default), and static routing (using a `defaultrouter` or `tsolgateways` file).

For small networks, an `/etc/defaultrouter` file provides a simple routing method. If your workstation or site accesses a complex network of gateways, the `/etc/tsolgateways` file offers more control over static routing. See "Administering Trusted Networking" in *Trusted Solaris Administration Overview* and the `tsolgateways`(4) man page for more information.

▼ To Set Up Simple Static Routing

Note - For static routing, do either this procedure, *or* "To Set Up Complex Static Routing" on page 61.



1. **Double-click the Set Default Routes action in the System_Admin folder.**

   See “To Open a File that has a Defined Action” on page 53 if you are unfamiliar with using trusted actions.

   An empty `/etc/defaultrouter` file appears in the trusted editor.

2. **Enter the name or the IP address of the defaultrouter. If there is more than one, enter them all, one per line, and then save the file.**

   For example, if the workstations `trustworthy` and `forwardho` are routers, enter them, one per line:

```
trustworthy
forwardho
```

3. **Return to the procedure and chapter you are working from.**

▼ To Set Up Complex Static Routing

1. **Double-click the Set TSOL Gateways action in the System_Admin folder.**

   See “To Open a File that has a Defined Action” on page 53 if you are unfamiliar with using trusted actions.

   An empty `/etc/tsolgateways` file appears in the trusted editor. See the `tsolgateways`(4) man page for examples of how to format the file.

2. **Enter the IP address of the net, the name of the gateway and its metric. Repeat for every gateway and save the file.**

   For example, if the workstations `trustworthy` and `forwardho` are gateways:

```
129.150.150.0 trustworthy 1
129.150.8.0 forwardho 2
```

Note - If the workstation has an `/etc/defaultrouter` file and an `/etc/tsolgateways` file, only the `/etc/tsolgateways` file is used for routing decisions.

---

3. **Return to the procedure and chapter you are working from.**

How to Add Hosts

The install team enters every host that the local machine should contact upon booting into the local hosts database. If the local machine is a name service client, it will find its file servers, home directory server, and other servers from the name service master.

▼ To Add Hosts to Local Machine's Known Network

1. **At the label `ADMIN_LOW`, in an administrative role, initially the root role, invoke the Solaris Management Console from the Application Manager.**

   If you are unfamiliar with accessing the Solaris Management Console, see "To Initialize the SMC Server" on page 54. Note that the SMC must be initialized before use.

2. **Click** *this_host*`: Scope=Files, Policy=TSOL` **under Trusted Solaris Management Console in the Navigation pane.**

3. **Click Trusted Solaris Configuration, then Computers and Networks, then double-click Computers.**

Note - If toolbox icons display as red stop signs, the toolboxes will not load. To load them, do Step 4 on page 55.

The known hosts are displayed in the View pane. This workstation should already be in the database. You should add the following hosts:

1. Name service master, if any.
2. Static routers, if any.
3. Audit servers for this workstation.
4. If this workstation does not use a name service, add all computers that this machine can contact.

4. Choose Add Computer from the Action menu.

5. Click Apply to add a computer, and click OK when the entries are complete.

6. If the network `0.0.0.0` is defined under Computers and Networks, remove it. It is a security risk. See "Modifying the Boot-time Trusted Network Databases" in *Trusted Solaris Administrator's Procedures*

a. Double-click Computers and Networks.

b. Click `0.0.0.0` in the View pane.

c. Choose Delete from the Edit menu, and confirm the deletion when prompted.

7. Return to the procedure and chapter you are working from.

How to Add a Remote Host Template

The `tnrhtp`(4) file installed by the Trusted Solaris installation CDs contains examples of templates that match the `label_encodings`(4) file installed by the Trusted Solaris installation CDs. Sites who install a site-specific `label_encodings` file must create templates that match the labels that they recognize, as described the following procedure.

▼ To Add a Remote Host Template

1. **At the label** `ADMIN_LOW`**, in an administrative role, initially the root role, invoke the Solaris Management Console from the Application Manager.**

   If you are unfamiliar with accessing the Solaris Management Console, see "To Initialize the SMC Server" on page 54. Note that the SMC must be initialized before use.

2. **Click** *this_host*`: Scope=Files, Policy=TSOL` **under Trusted Solaris Management Console in the Navigation pane.**

   Note - If toolbox icons display as red stop signs, the toolboxes will not load. To load them, do Step 4 on page 55.

   ---

3. **Click Trusted Solaris Configuration, then Computers and Networks, then double-click Security Families.**

   The existing templates are displayed in the View pane.

   Note - If you installed a site-specific label_encodings file, it is highly likely that the existing templates will not work with your file. The `tnrhtp` must contain templates that reflect the labels of machines and networks your site can contact.

   You should have templates for:

   1. The Trusted Solaris hosts that this machine can contact.
   2. Any unlabeled hosts/networks that this machine can contact..

4. **Choose Add Template from the Action menu.**

5. **In the Basic Information tab, create a template named** `unlab`***_userlabel*****, of host type Unlabeled, with an** `ADMIN_HIGH` **clearance and a process label of *low_user_label*.**

   The default clearance must dominate the default label. The label `ADMIN_HIGH` dominates all labels.

6. **Click OK when the template is complete.**

7. **Return to the procedure and chapter you are working from.**

How to Assign a Remote Host Template

The trusted network remote host database, `tnrhdb`(4), enables this host to communicate with remote hosts. The man page describes the format of the `tnrhdb`, and suggests how to minimize the number of entries required.

▼ To Assign a Template to a Host

1. **At the label `ADMIN_LOW`, in an administrative role, initially the root role, invoke the Solaris Management Console from the Application Manager.**

   If you are unfamiliar with accessing the Solaris Management Console, see "To Initialize the SMC Server" on page 54. Note that the SMC must be initialized before use.

2. **Click *this_host*`: Scope=Files, Policy=TSOL` under Trusted Solaris Management Console in the Navigation pane.**

   Note - If toolbox icons display as red stop signs, the toolboxes will not load. To load them, do Step 4 on page 55.

   ---

3. **Click Trusted Solaris Configuration, then Computers and Networks, then double-click Security Families.**

   The remote host templates display in the View pane.

4. **Double-click the `tsol` security family.**

5. **Choose Add Host(s) from the Action menu.**

6. **In the Add Host(s) dialog, click Add Wildcard to assign this template to all hosts on your Trusted Solaris 8 subnet.**

   a. **Enter the subnet IP address and choose the template name.**

      For example, enter `129.150.110.0` and `tsol`. The final zero signifies a subnet address; all hosts on that subnet are recognized as `tsol` hosts.

      Note - Note that the zero (`0`) is the wildcard. Do not use a star (`*`).

      ---

   b. **Click OK.**

7. **Choose Add Host(s) from the Action menu and click Add Host in the Add Host(s) dialog to enter any exceptions to the subnet template assigment. Click OK to end the entry.**

   For example, enter `129.150.110.3` and `unlab_`*user_label*. This host on the subnet is an unlabeled host, an exception to the `tsol` wildcard entry.

8. **Choose Add Host(s) from the Action menu and click Add Host to enter the IP address of every host in your `/etc/defaultrouter` or `/etc/tsolgateways` file, and assign to each an appropriate template name. Click OK to end each entry.**

9. **Enter the details of other subnets and hosts.**

   a. **Enter the wildcard designation of each subnet and choose its appropriate template by choosing Add Host(s) — Choose Wildcard.**

   b. **Individually assign a different template to any host that is an exception to its subnet's assigned template by choosing Add Host(s) — Choose Host.**

      Use the details provided by your system administrator, then choose the appropriate template name from the menu. See Table 1–3 for host types and their associated templates provided by Trusted Solaris software.

10. **Open a terminal and reload and verify the updated `tnrhdb` database.**

```
# tnctl –H /etc/security/tsol/tnrhdb
# tninfo –h
```

11. **Return to the procedure and chapter you are working from.**

How to Share a File System

The install team performs this procedure on the home directory or on a file server. If the directory is being shared before the `admin` role is created, the install team performs the procedure in the `root` role.

Caution - Do not use proprietary names for shared file systems. The names of shared file systems are visible to every user.

▼ To Share File Systems

See the *NIS+ and FNS Administration Guide* for ways to restrict home directory access to particular groups.

1. **In the admin role, (or root if the admin role does not exist), at label** `ADMIN_LOW`**, under Trusted Solaris Management Console, click** *this_host*: `Scope=Files, Policy=TSOL`**.**

   Note - If toolbox icons display as red stop signs, the toolboxes will not load. To load them, do Step 4 on page 55.

2. **Click Storage, then double-click Mounts and Shares, then double-click Shares.**

3. **Choose Add Shared Directory from the Action menu.**

4. **Follow the online help to share the** `/export/home` **directory.**
   The tool shares the directory and starts the NFS daemons,

5. **Verify that the directories are shared.**

```
$ showmount –e
export list for homedir_server:
/export/home
```

6. **Return to the procedure and chapter you are working from.**

How to Mount a File System

In the Trusted Solaris environment, unlabeled and labeled hosts can be mounted on a Trusted Solaris labeled host.

Caution - Do not use proprietary names for mounted file systems. The names of mounted file systems are visible to every user.

▼ To Mount a File System

1. **In the admin role, (or root if the admin role does not exist), at label** `ADMIN_LOW`**, under Trusted Solaris Management Console, click** *this_host*`: Scope=Files, Policy=TSOL`**.**

   Note - If toolbox icons display as red stop signs, the toolboxes will not load. To load them, do Step 4 on page 55.

2. **Click Storage, then double-click Mounts and Shares, then double-click Mounts.**

3. **Choose Add NFS Mount from the Action menu.**

4. **Follow and answer the prompts to mount the file system.**

   You are prompted to allow creation of the mount point if it does not exist. The tool adds an entry in the `/etc/vfstab` file, creates the mount point, and mounts the file system

5. **Return to the procedure and chapter you are working from.**

How to Create Administrative Roles

The install team creates the administrative roles (other than root) to be used at the site. The team assigns each role its rights profiles. Initial rights profiles are provided on the installation CD-ROM.

Prerequisite: If you are using a name service, the name service and home directory must be set up before you create the administrative roles secadmin, admin, and oper.

▼ To Create a Role

Note - In previous releases, roles were local. In Trusted Solaris 8, roles (other than root) can be distributed, and are created by the install team. Profiles are hierarchical, so each role can be assigned a profile that includes other profiles.

---

1. **In the root role, at label `ADMIN_LOW`, invoke the Solaris Management Console action from the Application Manager.**

   See "To Initialize the SMC Server" on page 54 if you are unsure of how to start the SMC server.

2. **Select the appropriate toolbox.**

   See "To Select a Toolbox of the Appropriate Scope" on page 56 for assistance.

3. **Click Trusted Solaris Configuration, then double-click Users.**

4. **Enter the role password at the prompt.**

5. **Double-click Administrativ... (Administrative Roles).**

   Note - If toolbox icons display as red stop signs, the toolboxes will not load. To load them, do Step 4 on page 55.

   ---

6. **Choose Add Administrative Role from the Action menu.**

   The Add Administrative Role wizard enables you to enter all values that are required for a role to work well. Values that you are not prompted to enter will get the default. If you want to view or modify all fields of a role, double-click the role after creating it.

7. **Create the secadmin role to be the security administrator. Use the following table when creating the role.**

   The secadmin password, and all passwords, should be one that is not easy to guess, thus reducing the chance of an attacker gaining unauthorized access by attempting to guess passwords.

   Note - For all administrative roles make the account Always Available, and do not set password expiration dates.

TABLE 3–2 secadmin Values in Add Role Dialog

Tab	Role Field	(Recommended) Value
Role Name	Role name	secadmin
	Full Name	Security Administrator
	Description	No proprietary info here.
	Role ID Number	≥100
	Role shell	Administrator's Bourne (profile shell)
	Create a role mailing list	checked
Password	Password and confirm	Assign a password of at least 6 alphanumeric characters.
Rights	Available and Granted	Information Security Rights Security
Home Directory	Server	*home directory server*
	Path	/*mount_path*
Assign Users	Add and Delete	This will be automatically filled in when you assign a role to a user.

8. After creating the role, select it and double-click it to modify it using information from the following table as a guide.

TABLE 3–3 secadmin Values in Properties / Modify Dialog

Tab	Role Field	(Recommended) Value
Password	Set password by Type in or Choose from list	(Set in Table 3–2.)
	Update password by Choose from list or Type in	
Group	Available Groups	
Trusted Solaris Attributes	Minimum Label: Edit	Default value is correct.
	Clearance: Edit	Default value is correct.
	View: External or Internal	The default value is External.
	Label: Show or Hide	If your site is a no-label site, choose Hide.
	Lock account …	Default value, No, is correct.
Audit	Excluded and Included	Set flags per site security policy

9. Using the preceding tables as a guide, create the following roles with unique IDs:

Role Name	Granted Rights
admin	System Administrator
primaryadmin	Primary Administrator
oper	Operator

Caution - You must create the administrative roles before you create the users, since you will assign a role to each user.

10. Return to the procedure and chapter you are working from.

How to Create Users to Assume Roles

The install team in the root role creates users to assume the roles secadmin, admin, and primaryadmin. Where site security policy permits, the team can choose to create one user who can assume more than one administrative role.

Prerequisite: Administrative roles must be created before creating users who will assume those roles.

▼ To Create a User

1. **In the root role, at label `ADMIN_LOW`, invoke the Solaris Management Console action from the Application Manager.**

   See "To Initialize the SMC Server" on page 54 if you are unsure of how to start the SMC server.

2. **Select the appropriate toolbox.**

   See "To Select a Toolbox of the Appropriate Scope" on page 56 for assistance.

3. **Click Trusted Solaris Configuration, then double-click Users.**

4. **Enter the role password at the prompt.**

5. **Double-click User Accounts.**

   Note - If toolbox icons display as red stop signs, the toolboxes will not load. To load them, do Step 4 on page 55.

   ---

6. **Choose Add User > Use Wizard from the Action menu.**

Caution - Role and user IDs come from the same pool of IDs. Do not use existing names or IDs for the users you add.

---

7. **Begin to create a user who can assume the secadmin role and use Table 3–4 to fill out the fields.**

   The Add User > Use Wizard dialog boxes create most aspects of a user.

8. **After creating the user, double-click the created user to modify some user properties.**

Use Table 3–5 as a guide.

9. **Read the (Recommended) Values columns for guidance.**

   Parentheses enclose suggestions. Requirements or defaults are not enclosed in parentheses.

Note - When the install team chooses a password, the team must select one that is not easy to guess, thus reducing the chance of an attacker gaining unauthorized access by attempting to guess passwords.

TABLE 3–4 User Values in Add User Dialog

Tab	User Field	(Recommended) Value
User Name	User name	
	Full name	
	Description	No proprietary info here.
	User ID number	(1001 or higher)
Password	Set password by Type in or Choose from list	Assign a password of at least 6 alphanumeric characters.
	Confirm	
Group	Primary group	Staff
Home directory	Server	*home directory server*
	Path	
Mail	Server	
	Path	

For the user who can assume the secadmin role, select the Always Available for Account Availability under General, below. Choose an appropriate account availability for other users.

TABLE 3–5 User Values in Properties/Modify Dialog

Tab	User Field	(Recommended) Value
General	Shell	
	Account Availability	Always Available
Password	Set password by Type in or Choose from list	(Set in Table 3–4.)
	Update password by Choose from list or Type in	
Group	Additional Groups	
Roles	Available Roles and Assigned Roles	secadmin
Trusted Solaris Attributes	Minimum Label: Edit	Default value is correct.
	Clearance: Edit	Default value is correct.
	View: External or Internal	
	Label: Show or Hide	If your site is a no-label site, choose Hide.
Account Usage	Idle time	
	Idle action	
	Lock account …	No — for user who will assume a role
Rights	Available and Granted	Enable Login … See Note below.
Audit	Excluded and Included	Set flags per site security policy

Note - Although Basic Solaris User does not appear in the Granted column, this right is assigned automatically to a user that is created using the Add User wizard. Do not assign the right explicitly.

10. Create and modify another user, one who can assume the admin role.

11. **Create and modify third and fourth users to assume the primaryadmin and oper roles, and provide them with unique IDs, and appropriate Rights.**

Note - If site security permits, users can assume more than one role.

These first users should each have at least the Enable Login right — user can enable logins after a workstation reboot.

After checking your site security policy, you may want to add the Convenient Authorizations right — user can allocate devices, enable logins, print PostScript files, print without labels, remotely log in, and shut down the workstation.

12. **Return to the procedure and chapter you are working from.**

Note - Setting up users is a two-role, trusted procedure. See Table 1–1 for the security defaults that the security administrator can set. Once the security defaults are set, the system administrator can set up user accounts.

In a multilabel environment, users are set up with a useful file, .link_files. See "Managing Initialization Files" in *Trusted Solaris Administrator's Procedures* for further discussion.

See "Using the SMC User Manager to Manage User and Role Accounts and Profiles" in *Trusted Solaris Administrator's Procedures* for details on setting up users and user files.

How to Verify that Users and Roles Work

Being able to modify a user's details in User Accounts confirms that the administrative roles secadmin and admin are working correctly.

▼ To Verify that the Roles secadmin and admin Work

1. **For each role, log in as a user who can assume the role and assume it.**

2. **In the role workspace, open the Solaris Management Console, select the Trusted Solaris Management Console with the appropriate scope for your site, and navigate to User Accounts.**

Note - If toolbox icons display as red stop signs, the toolboxes will not load. To load them, do Step 4 on page 55.

---

3. **Click a user.**
   - The admin role should be able to modify fields under the tabs General, Home Directory, and Group.
   - The secadmin role should be able to modify fields under all tabs.

▼ To Verify that the Role primaryadmin Works

1. **Log in as a user who can assume the primaryadmin role and assume it.**
2. **In the role workspace, open the Solaris Management Console, select the Trusted Solaris Management Console with the appropriate scope for your site, and navigate to Rights.**

Note - If toolbox icons display as red stop signs, the toolboxes will not load. To load them, do Step 4 on page 55.

---

3. **Create a new right by choosing Add Right from the Action menu.**
4. **Save the new right, then delete it before continuing.**
5. **Return to the procedure and chapter you are working from.**

How to Delete a Local User

When a user is deleted from the system, the administrator must ensure that the user's home directory and any objects owned by that user are also deleted. As an alternative to deleting objects owned by the user, the administrator may change the ownership of these objects to another user who is defined on the system.

The administrator must also ensure that all batch jobs still to run that are associated with the deleted user are also deleted. The administrator must ensure that there are no objects or processes belonging to a deleted user that remain on the system.

Note - The `tsolconvert` utility requires the root role to be available. Do not delete the install user until you have completed all the steps required on a Trusted Solaris 8 system. See "How to Save and Restore Trusted Solaris Databases" on page 81 for more information on converting Trusted Solaris 7 to Trusted Solaris 8 databases.

▼ To Delete the install User

1. **In the admin role, label `ADMIN_LOW`, in the Solaris Management Console, choose the *this_host*`: Scope=Files, Policy=TSOL`, and then select User Accounts.**

   The user "install" is defined locally.

   Note - If toolbox icons display as red stop signs, the toolboxes will not load. To load them, do Step 4 on page 55.

   ---

2. **Click the user to be deleted and click the Delete button.**

   For the user install, you do not have mail files to delete. Other local users may have home directories and mail files to delete.

How to Modify a Role's Rights

When setting up a network or custom JumpStart install, some required commands may not be available to the role because they are in a path that is not assigned to the role. To add commands, programs, or scripts to the role's rights, the security administrator must modify the role's rights.

▼ To Add a Command to a Role's Rights

1. **Log in as a user who can assume the role secadmin and assume it.**

2. **In the secadmin role, at label `ADMIN_LOW`, invoke the Solaris Management Console from the Application Manager.**

3. **Click the appropriate toolbox under Trusted Solaris Management Console.**
   - Choose *this_host*: `Scope=Files, Policy=TSOL` if you are adding a command for a locally-defined role, or are not using a name service.
   - Choose *name_server*: `Scope=`*name_service*`, Policy=TSOL` if you are adding a command for a role defined on the network, such as for the admin role when setting up network install.

4. **In the Navigation pane, click Trusted Solaris Configuration, then Users, then double-click Rights. Enter the role password when prompted.**

Note - If toolbox icons display as red stop signs, the toolboxes will not load. To load them, do Step 4 on page 55.

---

5. **In the View pane, scroll to the Custom *Rolename* Role and double-click.**

6. **Follow the online help for assistance in setting up the Custom *Rolename* Role right.**

   For a network installation example, use the Commands tab to add the `add_install_client` command from a non-standard directory, such as `/export/ultra_install/sparc/tsol_policy/Trusted_Solaris_8/Tools` to the Custom Admin Role right. The command should have all privileges.

7. **Make sure that the Custom *Rolename* Role right is assigned to *Rolename*. If it is not, assign it to *Rolename*.**
   a. **Navigate to Administrative Roles.**
   b. **Double-click the *Rolename* role.**
   c. **Click the Rights tab.**
   d. **Open the rights displayed in the Granted Rights column.**
      If the Custom *Rolename* Role right is not granted, continue. If it has already been granted, click the Cancel button.
   e. **Add Custom *Rolename* Role to the role's Granted Rights.**
   f. **Click OK to save your work.**

8. **Return to the procedure and chapter you are working from.**

▼ To Verify That a Command is Available to a Role

1. **Log in as a user who can assume the role whose profile has been updated.**

2. **Assume the role and launch a terminal from the role's workspace.**

3. **Verify that the new profile is in effect in the new terminal by using the** `profiles`**(1) command.**

   For example, to verify that the command in the network installation example is included in the admin role's rights profile with all privileges, as admin enter the following:

```
$ profiles –l | grep setup_install_server
/export/ultra_install/sparc/tsol_policy/Trusted_Solaris_8/Tools/setup_install_server: all
```

4. **Return to the procedure and chapter you are working from.**

▼ To Remove a Command from a Role's Rights

1. **As secadmin, at label** `ADMIN_LOW`**, in the Solaris Management Console use the same toolbox that you used to add the command to the rights profile, and navigate to Rights.**

2. **In the View pane, select the Custom *Rolename* Profile.**

3. **Follow the online help for how to remove the command from the profile.**

4. **Return to the procedure and chapter you are working from.**

How to End a Session

Users can lock their screen or log out at the end of a session. Users authorized to shut down the workstation can halt it and reboot.

Note - Users must log off or utilize the lockscreen functionality before leaving a workstation unattended. Otherwise a person may have access to the data of a user without having to pass identification and authentication, and that person would not be uniquely identified or accountable.

▼ To Lock the Screen

- **Left-click the padlock at the left of the middle section of the Front Panel.**

▼ To Log Out

1. **Right-click the workspace background and select Log out... from the Workspace Menu, or left-click the EXIT icon on the Front Panel.**
2. **When prompted, confirm that you want to log out.**

▼ To Reboot the Workstation

1. **Right click the CDE front panel and select Shut Down from the TP (Trusted Path) menu.**

   The menu appears when the user or role is authorized to shut down the workstation.

2. **Confirm the shutdown.**
3. **Enter `boot` at the** ok **prompt or `b` at the** > **prompt**:

```
Type help for more information
<#2> ok boot
```

```
Type b (boot), c (continue), or n (new command mode)
> b
```

4. **Return to the procedure and chapter you are working from.**

How to Save and Restore Trusted Solaris Databases

The Trusted Solaris 8 user and profile databases are in new formats with new names. To retain the usable data from their previous versions requires an administrator, before installing Trusted Solaris 8, to run the `tsolconvert` utility on a Trusted Solaris 7 system, to save the output directory to a safe storage area, and then to restore the files and run a shell script on the Trusted Solaris 8 machine.

The following table shows the name or content difference between earlier releases and the Trusted Solaris 8 release.

Trusted Solaris Databases	Trusted Solaris 8 Database Description
`/etc/security/tsol/tsoluser`	`user_attr`(4)
`/etc/security/tsol/tsolprof`	`exec_attr`(4) and `prof_attr`(4)
`/etc/security/tsol/tnidb`	Format is extended for IPv6. No conversion required.
`/etc/security/tsol/tnrhtp`	Format is extended for IPv6. New templates with `doi` and `ip_label` changes. See the `tnrhtp`(4) man page.
`/etc/security/tsol/tnrhdb`	Format is extended for IPv6. No conversion required.

▼ To Save Profile and User Attribute Information

- **See the** `README` **file and** `tsolconvert`**(1M) man page on the Trusted Solaris web site,** `http://www.sun.com/software/solaris/trustedsolaris/ts_tech_faq/` **for instructions.**

  Backup and conversion *must be completed* on the Trusted Solaris 2.5.1 or Trusted Solaris 7 NIS+ master before Trusted Solaris 8 is installed.

CHAPTER 4

Installing a Workstation

This chapter describes Trusted Solaris exceptions to Solaris installation procedures and recommendations. It also describes Trusted Solaris requirements that are optional in the Solaris environment. For example, an evaluated configuration must collect auditing records. The partitions for those audit records are created during installation.

Note - If you are planning to use data from Trusted Solaris 7 or Trusted Solaris 2.5.1 databases on your new Trusted Solaris 8 system, do *not* start installing. First, on a Trusted Solaris 7 or Trusted Solaris 2.5.1 system, create the Trusted Solaris 8 versions of `tsolprof` (`exec_attr` and `prof_attr`) and `tsoluser` (`user-attr`). Read and follow the procedures in the FAQ on the Trusted Solaris website, `http://www.sun.com/software/solaris/trustedsolaris/ts_tech_faq`.

Install Team Responsibilities

Trusted Solaris software is designed to be installed and configured by two people with distinct responsibilities. However, the installation program does not enforce two-role task division. Task division is enforced by users who can assume Trusted Solaris roles. Since roles and users are not created until after installation, we recommend that an install team of at least two persons be present during the installation of a workstation.

During Trusted Solaris 8 installation, the team should:

- Partition the disks with security in mind: name the partitions thoughtfully, so as not to disclose security information, and provide space for audit records.
- A root password is *required*. Enter a root password when prompted.

Trusted Solaris Differences from the Solaris 8 Installation Program

In the Trusted Solaris environment, upgrade is not supported nor is patch analysis. Trusted Solaris software supports fewer locales than does Solaris 8 software.

Recommendations for the Trusted Solaris Environment

On *all systems,* for audit records...

— Create at least one audit partition named `/etc/security/audit/`*workstation_name.*

On a system that will run the Solaris Management Console to administer the site...

— Provide at least 256 MB of memory. Provide swap space.

On *all systems,* for users who can assume a role...

— Create sufficient swap space. Swap space that is double the size of the workstation's memory is a good rule of thumb.

On a system that will be the *home directory server*...

— Create an `/export/home` partition large enough for the users' home directories.

On a system that will *not be* a home directory server...

— Create a small `/export` partition to hold some temporary configuration files. It also serves as a mount point.

Shutting Down the System to be Installed

For basic information on installation, see the *Solaris 8 Start Here* booklet and the platform-specific books described in “Installation Guides” on page 20.

▼ Shut Down a Trusted Solaris system

Trusted Solaris systems are shut down differently from Solaris systems.

1. **Shut Down the workstation from the TP menu.**

2. **If the screen displays the** > **prompt, enter** `n` **and press** Return **to display the** ok **prompt.**

   On a SPARC, if the PROM is protected, enter **`login`** and when prompted, the root password.

Installing a Trusted Solaris System from CD

See your hardware manual, such as the *Solaris 8 Sun Hardware Platform Guide* for full instructions. The following are examples.

▼ Boot from CD-ROM

Installing the first two systems requires using the 2 Trusted Solaris 8 installation CDs. The following are examples of booting from a CD on a SPARC and on an Intel machine.

1. **Insert the first of two (2) Trusted Solaris 8 Installation CDs and type the boot command.**

   For example, on a SPARC system:

```
boot cdrom
```

See the following example for the Intel Architecture boot procedure.

EXAMPLE 4–1 IA: Typical boot procedure

1. Do one of the following:
   - OPTION 1: Enable the system to boot from a CD by using the system's BIOS setup tool.
   - OPTION 2: Insert the provided floppy, then insert the first CD.
2. Follow the directions in the platform-specific book described in "Installation Guides" on page 20, keeping in mind that Solaris Web Start ard upgrade are not supported, and that you are using Trusted Solaris CDs, not Solaris CDs.

▼ Read Booting Messages

After you type the boot command, the workstation goes through a booting phase where hardware and system components are checked. The following screen provides an example of what you see.

```
Type b (boot), c (continue), or n (new command mode)
>n
Type help for more information
ok boot cdrom Rebooting with command: boot cdrom
Boot device: /sbus/espdma@e, 8400000/esp@e, 8800000/sd@6, 0:f
File and args:
NOTICE: 64-bit OS installed, but the 32-bit OS is the default
        for the processor(s) on the system.
        See boot(1M) for more information.
Booting the 32-bit OS ...
SunOS Release 5.8 Version Trusted_Solaris_8 32-bit
Copyright 1983-2000, Sun Microsystems, Inc. All rights reserved.
Configuring /dev and /devices
Using RPC Bootparams for network configuration information.
Configured interface le0
Starting OpenWindows…
```

The booting phase will last for a few minutes. Then a Welcome to Trusted Solaris screen briefly appears, then the screen turns blue-gray and a Solaris Install Console is displayed in the upper left corner. Messages display in the Install Console during installation.

The Trusted Solaris installation program is running.

▼ Answer Installation Questions

If you are installing from CD-ROM, the program guides you step by step through installing Trusted Solaris software. Online help is also available.

- **Use "Root NIS+ Master Installation Program Example" on page 167 for guidance in answering the questions the first time that you install. In particular, note the following:**
  - When asked whether to use DHCP (Dynamic Host Configuration Protocol), choose `No`.
  - When installing the name service master, choose `None` when asked for the name service. The name service domain is configured after installing the first workstation.

  For screenshots of the installation program questions, see "Using the Solaris 8 Interactive Installation Program" in *Solaris 8 Advanced Installation Guide*.

▼ Enter a root Password

Users must not disclose their passwords to another person, as that person may then have access to the data of the user and will not be uniquely identified or accountable. Note that disclosure can be direct, through the user deliberately disclosing her/his password to another person, or indirect, for example, through writing it down, or choosing an insecure password. Trusted Solaris provides protection against insecure passwords, but cannot prevent a user disclosing her/his password or writing it down.

Caution - A Trusted Solaris system *must* have a root password in order for the root role to work. The root role is required for successful configuration.

1. If you manually reboot your system, type:

```
# halt
ok  boot disk
```

2. Choose a root password by answering the password prompts.

```
Root password: rootpassword
Re-enter your root password: rootpassword
```

Caution - Do not forget the root password. The software cannot be configured without it.

▼ Insert the Second Trusted Solaris 8 CD

The second CD installs packages only; it does not contain installation questions.

Note - The prompts are misleading. The installation program asks for Solaris 8 CD-ROM #2. You should insert Trusted Solaris 8 CD-ROM #2.

1. **Insert the second Trusted Solaris 8 installation CD.**

   Upon insertion, the CD prints out that it is a Solaris 8 CD-ROM. If you inserted a CD-ROM with the Trusted Solaris 8 Installation CD label, you inserted the correct CD.

   Note - The screen may display overwriting for the second CD. However, the packages are installing.

2. **Answer yes to installing the software.**

   Package installation is displayed in 25% increments:
   `|-1%---25%---50%---75%---100%`

3. **Enter 1 or 2 when prompted.**

4. **Remove the CD and press** Return**.**

▼ Read the Log

Before reboot, the install log is in the file `/tmp/install_log`. After reboot, the install log is in the file `/var/sadm/system/logs/install_log`.

- **Look for successful installation of packages.**

▼ Configure the Trusted Solaris System

Finish system setup by configuring the system. A Trusted Solaris system must be configured correctly after installation.

- **To configure the system, follow the instructions in the appropriate chapter, as shown in the task map in Table 2–4.**

Troubleshooting

Errors you encounter during installation are described and debugged in the Troubleshooting section of the *Solaris 8 Installation Collection* (see `http://docs.sun.com/ab2/coll.241.7`).

Installing Over the Network

The admin role is in charge of installing over a network. The secadmin role is called upon to modify or set up files or profiles to enable the admin role to complete software installation.

▼ Boot over the Network or with Custom Files

Prerequisite: The network and/or custom files are correctly set up. See the *Solaris 8 Advanced Installation Guide*, 806-0957-10, which describes network installations. The same procedures apply to Trusted Solaris network installations, with the Trusted Solaris security protections described in Chapter 9.

1. **Boot using the appropriate boot command on the system being installed.**

EXAMPLE 4–2 SPARC: Boot command for a

custom JumpStart installation

```
boot net
```

EXAMPLE 4–3 SPARC: Boot command for a custom JumpStart installation

```
boot net - install
```

A space is required between the minus sign and `install`**.**

2. **Answer any prompts that appear.**

   If you have correctly set up a network installation, you will be prompted for information after system identification is completed.

   If you have correctly set up a custom JumpStart installation, you are not prompted for information. If you are using a name service, you must set up the clients after JumpStart has completed.

▼ Complete Network and JumpStart Installations

For pointers to administration books, see “Configuration Guides” on page 20 and “Other Books” on page 20.

- **Check that all Trusted Solaris configuration tasks are complete.**

  For an overview of individual workstation configuration tasks, see Chapter 8.

CHAPTER 5

Configuring a Workstation with No Name Service

This chapter covers how to configure a workstation without a name service. Administration is through local files.

Note - Installation and configuration commands and actions are limited to particular roles and particular labels. Read each task for the administrative role that can perform it, and the label required.

Who Does What

Trusted Solaris software is designed to be installed and configured by an install team. Once the team has created users who can assume Trusted Solaris roles, and has rebooted the workstation, the software enforces task division by role. If two-person installation is not a site security requirement, you can assign the administrative roles to one person.

Local Files Configuration Tasks

A host that is administered using local files instead of a name service is configured much like a NIS+ root master, except that `/etc` files are used for administration rather than NIS+ tables.

Other setup tasks, such as protecting file systems, handling mail, and setting up printing are covered in *Trusted Solaris Administrator's Procedures.*

If you are configuring the workstation to satisfy criteria for an evaluated configuration, please read "Understand Your Site's Security Policy" on page 24

Depending on how you set up the workstation, some procedures can be omitted.

▼ Log In and Launch a Terminal

1. **Log on to the workstation as the user install.**

   See "How to Log In" on page 41 if you have not logged in before.

2. **Assume the root role.**

   See "How to Assume a Role" on page 43 if you have not assumed a role before.

   You are in a new workspace named `root`, designed for the root role. The session label is still `ADMIN_LOW`, but the root role has more powers than the user `install`.

3. **Launch a terminal.**

   See "How to Launch a Terminal" on page 45 if you are unfamiliar with launching a terminal in the Solaris or Trusted Solaris environment. The terminal contains a profile shell that is specific to the root role.

▼ Protect the Workstation

- **Protect the PROM or the BIOS.**

See “How to Protect Machine Hardware” on page 46 if you are unfamiliar with the steps.

▼ Check and Install the label_encodings File

The Trusted Solaris `label_encodings`(4) file has been checked and is installed. Note that it must be compatible with any Trusted Solaris host with which you are communicating.

Note - The default `label_encodings` file is useful for demos, but it is not a good choice for use by a customer site. However, if you plan to use it, you can skip this step.

If you are familiar with label encodings files, you can use the following procedure. However, if you are not familiar with label encodings files, read the requirements and follow the procedures in *Trusted Solaris Label Administration*.

- **Follow the procedure in “How to Install a Label Encodings File” on page 59.**

Caution - You *must* successfully complete this step before continuing or the installation will fail.

▼ Initialize the Solaris Management Console

- **Follow the procedure “To Initialize the SMC Server” on page 54.**

▼ Set Up Network Files

Perform these tasks only if the security administrator has planned for an open network, you do not plan to use dynamic routing (the default), and you plan to access other workstations without using a name service.

Set up Static Routing

- **To set up static routing, complete one of the following procedures: “To Set Up Simple Static Routing” on page 60 or “To Set Up Complex Static Routing” on page 61.**

Set up DNS

- **If your workstation is going to use DNS, click the Set DNS Servers action in the System_Admin folder and enter the nameservers.**

  For a detailed list of steps, see “Set Up DNS” on page 105, except do not edit the `nsswitch.conf` file.

Add Hosts

- **If your workstation is going to contact other hosts, enter them in the `/etc/hosts` file.**

  Follow the procedure “How to Add Hosts” on page 62.

Assign Templates to Remote Hosts

1. **If this host is going to contact unlabeled hosts, the `tnrhtp` must have an appropriate unlabeled template for those unlabeled hosts. See “How to Add a Remote Host Template” on page 63 for the explanation and procedure.**

2. **Follow the procedure “How to Assign a Remote Host Template” on page 65.**

   Assign a remote host template to every host or network that this machine may contact. Include every host in the `/etc/hosts` file.

▼ Create Administrative Roles

The administrative roles must be created before the users are created.

1. **Log in as the user install and assume the root role.**

2. **Follow the steps in “How to Create Administrative Roles” on page 68.**

▼ Create Users to Assume Roles

The install team in the root role creates at least two users, to assume the roles secadmin and admin. It is also useful to create one or two users to assume the primaryadmin and oper roles. Where site security permits, a user can be assigned more than one administrative role.

Note - *Prerequisite*: The secadmin and admin administrative roles have been created.

- **Still in the root role, follow the steps in "To Create a User" on page 72, and select the** *this_host*`: Scope=Files, Policy=TSOL` **toolbox.**

▼ Reboot the Workstation

Note - This step is required only if you have set up static routing or DNS.

- **Shut down the workstation from the TP (Trusted Path) menu, as described in "To Reboot the Workstation" on page 80.**

▼ Verify That Users and Roles Work

- **Log in as a user, assume an administrative role, and test the role for effectiveness.**

  Using the *this_host*`: Scope=Files, Policy=TSOL` toolbox, follow the procedures in "How to Verify that Users and Roles Work" on page 75 to ensure that every role is working.

▼ Mount File Systems

Perform this task only if the security administrator has planned for an open network, and you plan to access a file server without using a name service.

- **Use the SMC Mounts tool to mount the file system, as described in "How to Mount a File System" on page 68.**

▼ Share File Systems

Perform this task only if others are permitted to access directories on this workstation.

- **To share file systems that other workstations may access, use the SMC Shares tool as described in "How to Share a File System" on page 66.**

▼ Delete the User install

The user `install` is useful for installing and initially configuring a workstation. Where site security requires, remove the user.

- **See “How to Delete a Local User” on page 76 if you have not deleted a local user in the Trusted Solaris system before.**

CHAPTER 6

Configuring the NIS+ Domain

This chapter covers how to configure the NIS+ root master and the home directory server, the first workstations you install at a networked site.

Note - Installation and configuration commands and actions are limited to particular roles and particular labels. Read each task for the administrative role that can perform it, and the label required.

Who Does What

Trusted Solaris software is designed to be installed and configured by an install team. Once the team has created users who can assume Trusted Solaris roles, and has rebooted the workstation, the software enforces task division by role. If two-person installation is not a site security requirement, you can assign the administrative roles to one person.

NIS+ Root Master Configuration Tasks

The first workstation installed on a network has special status. It must be installed interactively from the CDROM, and it must be configured as the NIS+ root master.

Configuring a NIS+ root master involves entering security information, some of which is copied to the clients, and entering details local to the workstation itself.

Other administrative tasks, such as protecting file systems, handling mail, and setting up printing are covered in *Trusted Solaris Administrator's Procedures*.

If you are configuring a site that satisfies criteria for an evaluated configuration, please read "Understand Your Site's Security Policy" on page 24.

The procedures are not numbered. Depending on your site configuration, some procedures can be omitted.

▼ Log In and Launch a Terminal

1. **Log on to the workstation as the user install.**
   See "How to Log In" on page 41 if you have not logged in before.

2. **Assume the root role.**
   See "How to Assume a Role" on page 43 if you have not assumed a role before.

You are in a new workspace named `root`, designed for the root role. The session label is still `ADMIN_LOW`, but the root role has more powers than the user `install`.

3. **Launch a terminal.**

   See "How to Launch a Terminal" on page 45 if you are unfamiliar with launching a terminal in the Solaris or Trusted Solaris environment. The terminal contains a profile shell that is specific to the root role.

▼ Protect the Workstation

- **Protect the PROM or the BIOS.**

  See "How to Protect Machine Hardware" on page 46 if you are unfamiliar with the steps.

▼ Check and Install the label_encodings File

The label_encodings file should be the same on every host in your domain. The security administrator is responsible for preparing, checking, and maintaining the `label_encodings` file.

Note - The default `label_encodings` file is useful for demos, but it is not a good choice for use by a customer site. However, if you plan to use it, you can skip this step.

You will use a copy of the `label_encodings` file on the NIS+ clients.

If you are familiar with label encodings files, you can use the following procedure. However, if you are not familiar with label encodings files, read the requirements and follow the procedures in *Trusted Solaris Label Administration*.

1. **Follow the procedure in "How to Install a Label Encodings File" on page 59.**

Caution - You *must* successfully complete this step before continuing or the installation will fail.

---

2. **Set up a copy of the `label_encodings` file for the NIS+ clients in "Copy Configuration Files for Distribution to Clients" on page 109.**

▼ Initialize the Solaris Management Console

- **Follow the procedure "To Initialize the SMC Server" on page 54.**

▼ Set Up Static Routing (Optional)

Note - If you plan to use dynamic routing, skip this procedure.

- **To set up static routing, complete one of the following procedures: "To Set Up Simple Static Routing" on page 60 or "To Set Up Complex Static Routing" on page 61.**

▼ Add Remote Hosts

- **Follow the procedure "How to Add Hosts" on page 62.**

▼ Add and Assign Remote Host Templates

Note - If your site is using a site-specific label encodings file, you must ensure that the templates in the `tnrhtp`(4) accurately reflect the `label_encodings` file.

If you plan to mount file systems from unlabeled hosts at a label available to users, or enable communications using services such as `ftp`, or route through an unlabeled host, you must have a template to assign those unlabeled hosts. If you are using the `label_encodings` file provided on the Trusted Solaris installation CD, the `tnrhtp` shipped on the installation CD contains possible templates.

The `tnrhdb` should include the host type and IP addresses of the workstations on your network and the host type and IP addresses of any other subnets and hosts with which your Trusted Solaris 8 network can communicate. The system administrator collects the IP addresses. The security administrator determines what networks can contact the Trusted Solaris 8 network; for a list of host types, see Table 1–3.

Add an Unlabeled Remote Host Template to the tnrhtp

This procedure adds a new template, `unlab_`*userlabel*, to the `tnrhtp`(4) database. Creating a template for an unlabeled host type is a prerequisite to mounting an unlabeled host at a user label, such as Confidential.

Note - You can skip this step if your site is using two files that are provided Trusted Solaris installation CD: the `label_encodings` file and the `tnrhtp` file. If you have installed your own label encodings file, you *must* ensure that the templates in the `tnrhtp` file accurately describe the hosts, labeled and unlabeled, that communicate with your site.

♦ **Follow the procedure "How to Add a Remote Host Template" on page 63.**

Assign Templates to Remote Hosts

The following procedure is required to set up a working Trusted Solaris network.

♦ **Follow the procedure "How to Assign a Remote Host Template" on page 65.**

Summary

The `tnrhdb` database must have an IP address and template name for every host or subnet that the computers in the Trusted Solaris 8 domain can communicate with:

1. The NIS master server (that is, this host)
2. Every NIS client that will be in the Trusted Solaris 8 domain, or its subnet wildcard mechanism ***nnn.nnn.nnn.*0**
3. Every static router (open network only)
4. Every other workstation with which the domain can communicate, or a wildcard address for its subnet (open network only)

▼ Set Up the NIS+ Domain

Setting up the NIS+ root master sets up the NIS+ domain for the Trusted Solaris NIS+ clients. Several NIS+ tables have been created or modified to hold Trusted Solaris data about label configuration, users, roles, execution profiles, and remote hosts.

To Set the Stage

1. **As root, create a staging area for files you plan to use to populate the NIS+ databases.**

You can place the staging area wherever you have enough space. Usually a few megabytes is more than enough room to store some files temporarily.

```
# mkdir –p /setup/files
```

2. Copy the sample `/etc` files into the staging area.

Most of the files you need already exist on the installed system and have enough data in them to get you started. The following files in the `/etc` directory are usually not found on a newly installed system: `bootparams`, `ethers`, `netgroup`, `netmasks`, and `timezone`. You can create these with an editor, load them from a backup diskette, or merely create empty versions of these files, so that the NIS+ tables are created all at once. If you choose not to create these files, you can create them later, but the `nispopulate`(1M) command may print out a few warning messages.

```
# cd /etc
# touch bootparams ethers netgroup netmasks timezone

# cp bootparams ethers netgroup netmasks timezone \
aliases auto_home auto_master group hosts networks \
protocols publickey rpc services /setup/files

# cd security
# cp  auth_attr prof_attr exec_attr /setup/files/
# #
# cd /etc/security/tsol
# cp tnrhdb tnrhtp /setup/files
# #
# cd /etc/inet
# cp ipnodes /setup/files
```

3. Create empty files in the staging area of files whose contents should not be distributed.

```
# cd /setup/files
# touch audit_user passwd shadow user_attr
```

All entries in the `passwd`, `shadow`, and `user_attr` files on a newly-installed system are local users who should be restricted to local access. The name service will create empty databases from the empty files, and will not print spurious warning messages.

4. **Check that all the files are now in your staging area; there are 25.**

```
# ls | wc -l
     25
```

5. **Edit the `hosts` file in your staging area.**

   a. **Open the Admin Editor and enter `/setup/files/hosts` for editing.**

   For more detailed instructions, see "To Create or Open a File from the Trusted Editor" on page 52.

   The file already contains the NIS+ root master (that is, this host's address) and the static routers, if any.

   b. **Add every workstation that will be in the Trusted Solaris 8 domain.**

   There is no wildcard mechanism here. The IP address of every workstation to be contacted *must* be in this file.

Caution - Failure to include a workstation will cause client authentication to fail; the NIS+ client will have no credentials.

   c. **Add every other workstation with which the domain can communicate.**

   d. **Use the `:wq!` command to write the file and exit the editor.**

There is enough information in your staging area to convert your host to a NIS+ master.

Caution - If you have edited any files, you must be very careful to provide all of the information necessary in the correct formats before populating the NIS+ tables. Failure to do so can result in the inability to further administer or use the system.

To Set Up NIS+ with Databases from the Staging Area

For fuller descriptions of NIS+ setup and administration, see

- *Solaris Naming Setup and Configuration Guide* and
- *Solaris Naming Administration Guide*

1. **Double-click the Create NIS+ server action in the System_Admin folder.**

   See "To Run a Script from the System_Admin Folder" on page 53 if you are unfamiliar with using trusted actions.

2. **Enter your NIS+ domain name.**

   This workstation will be the root master. For example,

```
Domain Name: aviary.eco.org.
```

   There is a period at the end of the domain name.

3. **Answer the prompts (y, y, *rootpassword*).**

   You can ignore diagnostics printing out that the file `/etc/defaultdomain` cannot be located. The file will be created.

4. **In the `/setup/files` directory, make sure that you have added all NIS+ clients to the hosts file.**

```
# cd /setup/files
# more hosts
```

5. **Populate the standard NIS+ databases from the `/setup/files` directory by running the Populate NIS+ Tables action in the System_Admin folder.**

6. **Enter your staging area when prompted.**

```
Populate from which directory? /setup/files
```

7. **Answer the prompts (y, y).**

```
…
Is this information correct? y
…
Do you want to continue? y
```

8. **Load any additional NIS+ tables you may have backed up, such as** `auto_home`**.**

   Procedures vary depending on the format of the backup and on what types of NIS+ tables they are. Refer to the *Solaris Naming Setup and Configuration Guide* for details of how to load your tables.

9. **Do not reboot your system yet.**

▼ Set Up the NIS+ SMC Toolbox

The `tsol_nisplus.tbx` file on the NIS+ master must be edited before it can be used to administer the domain.

♦ **Follow the procedure "To Edit Name Service Toolbox Definitions" on page 57.**

▼ Set Up DNS

Note - Skip this procedure if the security administrator has planned a closed network.

If you are using DNS to contact hosts outside of your domain, you must set it up. For detailed information about DNS, see the *Solaris Naming Setup and Configuration Guide.*

1. **Create a** `resolv.conf` **file with the appropriate name servers using the Set DNS Servers action.**

   a. **Enter the string** `nameserver` **followed by the IP address of one of your name servers, and repeat for all name servers.**

      The file looks something like:

```
nameserver nnn.nnn.nnn.nnn
nameserver nnn.nnn.nnn.nnn
```

b. Write the file and exit the editor.

2. **Using the Name Service Switch action, change the `hosts` entry in the `/etc/nsswitch.conf` file to use DNS.**

```
~
#hosts:      nisplus [NOTFOUND=return] files
#Uncomment the following line, and comment out the above,
#to use both DNS and NIS+.  You must also set up the
#/etc/resolv.conf file for DNS name server lookup.
#See resolv.conf(4).
hosts:     files nisplus dns
~
```

▼ Reboot the Workstation

- **Shut down the workstation from the TP (Trusted Path) menu, as described in "To Reboot the Workstation" on page 80.**

▼ Install and Configure the Home Directory Server

Install and configure the home directory server and mount the home directories before adding roles and users.

1. **Install the host that will become the home directory server.**

   Follow the procedure described in "Installing a Trusted Solaris System from CD" on page 85, then return here.

2. **Configure the home directory server as described in "Client Configuration Tasks" on page 125 through the procedure, "Share Home Directories" on page 133.**

3. **Then, create the administrative roles on the NIS+ master as described in "Create Roles on the NIS+ Master" on page 107.**

Note - The administrative roles are created as network-visible accounts, not as local accounts. Their home directories are mounted from the home directory server.

▼ Create Roles on the NIS+ Master

The roles admin, secadmin, primaryadmin and oper must be created in the new NIS+ domain using the Administrative Roles tool in the Solaris Management Console.

Prerequisite: The home directory server has been created and the home directories are automounting.

1. **Log in to the NIS+ master as the user install and assume the root role.**

2. **Follow the steps in "How to Create Administrative Roles" on page 68.**

Note - If, after reboot, SMC complains that the server is not running, re-check your edits from "To Edit Name Service Toolbox Definitions" on page 57. Look for misplaced periods, extra characters, and leftover < or > brackets.

▼ Add Roles to the NIS+ Admin Group

The first `admin` argument is the name of a NIS+ table. The last two arguments are the names of Trusted Solaris administrative roles, admin, secadmin, and primaryadmin.

♦ **Add the admin, secadmin, and primaryadmin roles to the NIS+ admin group.**

```
# nisgrpadm –a admin admin secadmin primaryadmin
```

▼ Create Users to Assume Roles

The install team in the root role creates at least two users, to assume the roles secadmin and admin. It is also useful to create a user who can assume the primaryadmin role. Where site security permits, a user can be assigned more than one administrative role.

Note - *Prerequisite*: The secadmin and admin administrative roles have been created.

- **Still in the root role, follow the steps in "To Create a User" on page 72, and select the** *name_server*`: Scope=NIS+, Policy=TSOL` **toolbox.**

▼ Log Out

- **Log out by clicking the EXIT button on the Front Panel.**

▼ Verify that Users and Roles Work

- **Log in as a user, assume an administrative role, and test the role for effectiveness.**

  Using the *name_server*`: Scope=NIS+, Policy=TSOL` toolbox, follow the procedures in "How to Verify that Users and Roles Work" on page 75 to ensure that every role is working.

▼ Set Up Auditing

The security administrator is responsible for auditing decisions.

1. **If site security does not require auditing, disable it.**

   To disable auditing in the Trusted Solaris environment, follow the procedures described in *Trusted Solaris Audit Administration*.

2. **After disabling auditing, go to the next task you plan to do.**

To Configure Auditing

- **Follow the procedures in *Trusted Solaris Audit Administration* to configure auditing at your site.**

  Who is audited and for what events should be the same on every workstation. Copy any modified audit configuration files from the NIS+ root master to every NIS+ client using the procedure in "Copy Configuration Files for Distribution to Clients" on page 109. Note that the `/etc/security/audit_user` file is governed by the NIS+ name service, so does not need to be copied.

▼ Mount File Systems

- **Use the SMC Mounts tool to mount the file system, as described in "How to Mount a File System" on page 68.**

▼ Share File Systems

- **To share file systems that other workstations may access, use the SMC Shares tool as described in "How to Share a File System" on page 66.**

▼ Copy Configuration Files for Distribution to Clients

1. **As root at label** `ADMIN_LOW`**, create a directory that cannot be deleted between reboots.**

```
# mkdir /export/clientfiles
```

2. **As root at label** `ADMIN_HIGH`**, use the File Manager to copy your modified** `label_encodings` **file to the** `/export/clientfiles` **directory.**

   See "How to Copy to and from a Portable Medium" on page 48 if you are unsure of the procedure.

3. **If you modified other files, copy them to the** `/export/clientfiles` **directory. You must be root at label** `ADMIN_LOW`**.**

   For example, most sites will want to copy the `/var/sadm/smc/toolboxes/tsol_`*nameservice*`/tsol_`*nameservice*`.tbx` file to the client machines. A site that is using a modified `tnrhtp` file, DNS, and auditing might copy the files `/etc/security/audit_control`, `/etc/security/audit_startup`, `/etc/security/tsol/tnrhtp`, `/etc/resolv.conf`, and `/etc/nsswitch.conf`.

4. **Transfer the** `label_encodings` **file to a diskette labeled** `ADMIN_HIGH`**.**

   If you are unsure of the steps, see "To Copy to a Diskette" on page 49.

5. **Transfer the other files to a diskette labeled** `ADMIN_LOW`**.**

▼ Delete the User install

The user `install` is useful for installing and initially configuring a workstation. Where site security demands, the admin role at label `ADMIN_LOW` removes the user.

Caution - Do not remove the user install until you are satisfied that the client workstations can communicate with the NIS+ master.

- **See "How to Delete a Local User" on page 76 if you have not deleted a local user in the Trusted Solaris system before.**

CHAPTER 7

Configuring a NIS Network

This chapter covers how to configure NIS machines.

Note - Installation and configuration commands and actions are limited to particular roles and particular labels. Read each task for the administrative role that can perform it, and the label required.

Who Does What

Trusted Solaris software is designed to be installed and configured by an install team. Once the team has created users who can assume Trusted Solaris roles, and has rebooted the workstation, the software enforces task division by role. If two-person installation is not a site security requirement, you can assign the administrative roles to one person.

NIS Configuration Tasks

The first workstation installed on a network has special status. It must be installed interactively from the CD-ROM, and is configured as the NIS master server. Subsequent machines are installed as NIS clients.

Configuring a NIS master involves entering security information, some of which is copied to the clients, and entering details local to the workstation itself.

Other administrative tasks, such as protecting file systems, handling mail, and setting up printing are covered in *Trusted Solaris Administrator's Procedures*.

If you are configuring a site that satisfies criteria for an evaluated configuration, use NIS+, not NIS.

The procedures are not numbered. Depending on your site configuration, some procedures can be omitted.

▼ Log In and Launch a Terminal

1. **Log on to the workstation as the user install.**

   See "How to Log In" on page 41 if you have not logged in before.

2. **Assume the root role.**

   See "How to Assume a Role" on page 43 if you have not assumed a role before.

   You are in a new workspace named `root`, designed for the root role. The session label is still `ADMIN_LOW`, but the root role has more powers than the user `install`.

3. **Launch a terminal.**

   See "How to Launch a Terminal" on page 45 if you are unfamiliar with launching a terminal in the Solaris or Trusted Solaris environment. The terminal contains a profile shell that is specific to the root role.

▼ Protect the Workstation

- **Protect the PROM or the BIOS.**

  See "How to Protect Machine Hardware" on page 46 if you are unfamiliar with the steps.

▼ Check and Install the label_encodings File

The label_encodings file should be the same on every host in your domain. The security administrator is responsible for preparing, checking, and maintaining the `label_encodings` file.

You will use a copy of the `label_encodings` file on the NIS clients.

If you are familiar with label encodings files, you can use the following procedure. However, if you are not familiar with label encodings files, read the requirements and follow the procedures in *Trusted Solaris Label Administration*.

1. **Follow the procedure in "How to Install a Label Encodings File" on page 59.**

Caution - You *must* successfully complete this step before continuing or the installation will fail.

2. **Set up a copy of the `label_encodings` file for the NIS clients in "Copy Configuration Files for Distribution to Clients" on page 123.**

▼ Initialize the Solaris Management Console

- **Follow the procedure "To Initialize the SMC Server" on page 54.**

▼ Set Up Static Routing (Optional)

Note - If you plan to use dynamic routing, skip this procedure.

- **To set up static routing, complete one of the following procedures: "To Set Up Simple Static Routing" on page 60 or "To Set Up Complex Static Routing" on page 61.**

▼ Add Remote Hosts

- **Follow the procedure "How to Add Hosts" on page 62.**

▼ Add and Assign Remote Host Templates

Note - If your site is using a site-specific label encodings file, you must ensure that the templates in the `tnrhtp`(4) accurately reflect the `label_encodings` file.

If you plan to mount file systems from unlabeled hosts at a label available to users, or enable communications using services such as `ftp`, or route through an unlabeled host, you must have a template to assign those unlabeled hosts. If you are using the `label_encodings` file provided on the Trusted Solaris installation CD, the `tnrhtp` shipped on the installation CD contains possible templates.

The `tnrhdb` should include the host type and IP addresses of the workstations on your network and the host type and IP addresses of any other subnets and hosts with which your Trusted Solaris 8 network can communicate. The system administrator collects the IP addresses. The security administrator determines what networks can contact the Trusted Solaris 8 network; for a list of host types, see Table 1–3.

1. **Follow the procedure for editing the `tnrhtp` described in "How to Add a Remote Host Template" on page 63.**

   Note - You can skip this step if your site is using two files that are provided Trusted Solaris installation CD: the `label_encodings` file and the `tnrhtp` file. If you have installed your own label encodings file, you *must* ensure that the templates in the `tnrhtp` file accurately describe the hosts, labeled and unlabeled, that communicate with your site.

2. **Follow the procedure for assigning templates to remote hosts described in "How to Assign a Remote Host Template" on page 65.**

   This step is required to set up a working Trusted Solaris network.

Summary

The `tnrhdb` database must have an IP address and template name for every host or subnet that the computers in the Trusted Solaris 8 domain can communicate with:

1. The NIS master server (that is, this host)
2. Every NIS client that will be in the Trusted Solaris 8 domain, or its subnet wildcard mechanism ***nnn.nnn.nnn.*0**
3. Every static router (open network only)
4. Every other workstation with which the domain can communicate, or a wildcard address for its subnet (open network only)

▼ Set Up the NIS Domain on the Master Server

Setting up the NIS domain on the NIS master server starts the processes that enable the Trusted Solaris NIS clients to reach the server. Several NIS files have been created or modified to hold Trusted Solaris data about label configuration, users, roles, execution profiles, and remote hosts.

For fuller descriptions of NIS setup and administration, see

- *Solaris Naming Setup and Configuration Guide* and
- *Solaris Naming Administration Guide*

Set Up the Staging Area

1. **As root, create a staging area for files you plan to use to populate the NIS files.**

   You can place the staging area wherever you have enough space. Usually a few megabytes is more than enough room to store some files temporarily.

```
# mkdir –p /setup/files/security/tsol
```

2. **Copy the sample `/etc` files into the `/setup/files` directory of the staging area.**

   Most of the files you need already exist on the installed system and have enough data in them to get you started. The following files in the `/etc` directory are usually not found on a newly installed system: `bootparams`, `ethers`,

netgroup, netmasks, and timezone. You can create these with an editor, load them from a backup diskette, or merely create empty versions of these files, so that the NIS databases are created all at once. If you choose not to create these files, you can create them later, but the ypinit(1M) command may print out a few warning messages.

```
# cd /etc
# touch bootparams ethers netgroup netmasks timezone

# cp bootparams ethers netgroup netmasks timezone \
aliases auto_home auto_master group hosts networks \
protocols publickey rpc services /setup/files

# cd /etc/inet
# cp ipnodes /setup/files
```

3. **Create empty files in the** /setup/files **directory of the staging area for files whose contents should not be distributed.**

```
# cd /setup/files
# touch passwd shadow user_attr
```

All entries in the passwd, shadow, and user_attr files on a newly-installed system are users who should be restricted to local access. The name service will create empty databases from the empty files, and will not print spurious warning messages.

4. **Copy the** *attr **files from the** /etc/security **directory into the** /setup/files/security **directory of the staging area.**

```
# cd /setup/files/security
# cp /etc/security/*attr /setup/files/security
```

5. **Add an empty** audit_user **file to the** /setup/files/security **directory and count the files in the directory.**

```
# pwd
/setup/files/security
# touch audit_user
# ls –F /setup/files | grep –v "/" | wc –l
4
```

6. **Copy the** `tnrhdb` **and** `tnrhtp` **files from the** `/etc/security/tsol` **directory into the** `/setup/files/security/tsol` **directory of the staging area. List and count the files.**

```
# cd /setup/files/security/tsol
# cp /etc/security/tsol/tnrh* .
# ls ; ls | wc –l
tnrhdb tnrhtp
       2
```

7. **Check that a total of 25 files are now in your staging area.**

   There are 4 in the `security` directory, 2 in the `tsol` directory, and 19 in the `files` directory.

```
# cd /setup/files
# ls –F /setup/files | grep –v "/" | wc –l
      19
```

8. **Edit the** `hosts` **file in your staging area.**

   a. **Open the Admin Editor and enter** `/setup/files/hosts` **for editing.**

      The file already contains the NIS master server (that is, this host's address) and the static routers, if any.

   b. **Add every workstation that will be in the Trusted Solaris 8 domain.**

      There is no wildcard mechanism here. The IP address of every workstation to be contacted *must* be in this file.

Caution - Failure to include a workstation will cause client connection to fail.

   c. **Add every other workstation with which the domain can communicate.**

   d. **Use the** `:wq!` **command to write the file and exit the editor.**

There is enough information in your staging area to convert your host to a NIS master.

Caution - If you have edited any files, you must be very careful to provide all of the information necessary in the correct formats before populating the NIS maps. Failure to do so can result in the inability to further administer or use the system.

Modify the /yp/Makefile

The `/var/yp/Makefile` file must be modified to point to the staging area and its subdirectories.

1. **Edit the `/var/yp/Makefile` in the Admin Editor.**

2. **Change three variables: PWDIR, DIR, and INETDIR to point to `/setup/files`.**

3. **Change the RBACDIR variable to point to the `$(DIR)/security` directory.**

4. **Change all four instances of `$(DIR)/tnrhtp` in the `tnrhtp.time:` target to `$(DIR)/security/tsol/tnrhtp`, as shown in the following lines:**

```
tnrhtp.time:  $(DIR)/security/tsol/tnrhtp
      -@if [ -f $(DIR)/security/tsol/tnrhtp ]; then \
              sed -e "/^#/d" -e s/#.*$$// $(DIR)/security/tsol/tnrhtp \
              ...
              echo "couldn't find $(DIR)/security/tsol/tnrhtp"; \
```

Note - Do not do a global replace. There are lines at the end of the Makefile that should not be changed.

5. **Change all four instances of `$(DIR)/tnrhdb` in the `tnrhdb.time:` target to `$(DIR)/security/tsol/tnrhdb`, as shown in the following lines:**

```
tnrhdb.time:  $(DIR)/security/tsol/tnrhdb
     -@if [ -f $(DIR)/security/tsol/tnrhdb ]; then \
             sed -e "/^#/d" -e s/#.*$$// $(DIR)/security/tsol/tnrhdb \
             ...
             echo "couldn't find $(DIR)/security/tsol/tnrhdb"; \
```

Note - Do not do a global replace. There are lines at the end of the Makefile that should not be changed.

Create NIS Maps from the Staging Area

1. **Double-click the Create NIS Server action in the System_Admin folder.**

   See "To Run a Script from the System_Admin Folder" on page 53 if you are unfamiliar with using trusted actions.

2. **Enter your NIS domain name.**

   For example,

```
Domain Name: aviary.eco.org
```

   This action creates the domain name, establishes this workstation as the NIS master server, and copies the `/etc/nsswitch.nis` file over `/etc/nsswitch.conf`.

3. **When prompted for other NIS servers, enter their host names one by one.**

   For example,

```
Host: tern
```

4. **Follow the instructions for ending the prompts.**

   The action creates NIS maps from the `/setup/files` directory. It uses your modified `/var/yp/Makefile` to create the `/var/yp/`*NIS_maps*.

5. **Do not reboot your system yet.**

▼ Set Up the NIS SMC Toolbox

The `tsol_nis.tbx` file on the NIS master server must be edited before it can be used to administer the domain.

♦ **Follow the procedure "To Edit Name Service Toolbox Definitions" on page 57.**

▼ Set Up DNS

Note - Skip this procedure if the security administrator has planned a closed network.

If you are using DNS to contact hosts outside of your domain, you must set it up. For detailed information about DNS, see the *Federated Naming Service Guide*.

1. **Create a `resolv.conf` file with the appropriate name servers using the Set DNS Servers action.**
   a. **Enter the string `nameserver` followed by the IP address of one of your name servers, and repeat for all name servers.**
      The file looks something like:

```
nameserver nnn.nnn.nnn.nnn
nameserver nnn.nnn.nnn.nnn
```

   b. **Write the file and exit the editor.**

2. **Using the Name Service Switch action, change the `hosts` entry in the `/etc/nsswitch.conf` file to use DNS.**

```
~
#hosts:     nis [NOTFOUND=return] files
hosts:   nis files dns
~
```

▼ Reboot the Workstation

- **Shut down the workstation from the TP (Trusted Path) menu, as described in "To Reboot the Workstation" on page 80.**

▼ Install and Configure the Home Directory Server

Install and configure the home directory server, reboot it, and share the home directories before adding roles and users.

1. **Install the host that will become the home directory server.**

   Follow the procedure described in “Installing a Trusted Solaris System from CD” on page 85, then return here.

2. **Configure the home directory server as described in “Client Configuration Tasks” on page 125 through the procedure, “Share Home Directories” on page 133.**

3. **Then, create the administrative roles on the NIS master server, as described in “Create Roles on the NIS Master Server” on page 121.**

Note - The administrative roles are created as network-visible accounts, not as local accounts.Their home directories are mounted from the home directory server.

▼ Create Roles on the NIS Master Server

The roles admin, secadmin, and oper must be created in the new NIS domain using Administrative Roles in the Solaris Management Console.

Prerequisite: The home directory server has been created and the home directories are automounting.

1. **Log in to the NIS master server as the user install and assume the root role.**

2. **Follow the steps in “How to Create Administrative Roles” on page 68.**

Note - If, after reboot, SMC complains that the server is not running, re-check your edits from “To Edit Name Service Toolbox Definitions” on page 57. Look for misplaced periods, extra characters, and leftover < or > brackets.

▼ Create Users to Assume Roles

The install team in the root role creates at least two users, to assume the roles secadmin and admin. It is also useful to create a user who can assume the

primaryadmin role. Where site security permits, a user can be assigned more than one administrative role.

Note - *Prerequisite*: The secadmin and admin administrative roles have been created.

- **Still in the root role, follow the steps in "To Create a User" on page 72, and select the** *name_server*`: Scope=NIS, Policy=TSOL` **toolbox.**

▼ Log Out

- **Log out by clicking the EXIT button on the Front Panel.**

▼ Verify that Users and Roles Work

- **Log in as a user, assume an administrative role, and test the role for effectiveness.**

  Using the *name_server*`: Scope=NIS, Policy=TSOL` toolbox, follow the procedures in "How to Verify that Users and Roles Work" on page 75 to ensure that every role is working.

▼ Set Up Auditing

The security administrator is responsible for auditing decisions.

1. **If site security does not require auditing, disable it.**

   To disable auditing in the Trusted Solaris environment, follow the procedures described in *Trusted Solaris Audit Administration*.

2. **After disabling auditing, go to the next task you plan to do.**

To Configure Auditing

- **Follow the procedures in *Trusted Solaris Audit Administration* to configure auditing at your site.**

  Who is audited and for what events should be the same on every workstation. Copy any modified audit configuration files from the NIS master to every NIS client using the procedure in "Copy Configuration Files for Distribution to Clients" on page 123. Note that the `/etc/security/audit_user` file is governed by the NIS name service, so does not need to be copied.

▼ Mount File Systems

- **Use the SMC Mounts tool to mount the file system, as described in "How to Mount a File System" on page 68.**

▼ Share File Systems

- **To share file systems that other workstations may access, use the SMC Shares tool as described in "How to Share a File System" on page 66.**

▼ Copy Configuration Files for Distribution to Clients

1. **As root at label** `ADMIN_LOW`**, create a directory that cannot be deleted between reboots.**

```
# mkdir /export/clientfiles
```

2. **As root at label** `ADMIN_HIGH`**, use the File Manager to copy your modified** `label_encodings` **file to the** `/export/clientfiles` **directory.**

   See "How to Copy to and from a Portable Medium" on page 48 if you are unsure of the procedure.

3. **If you modified other files, copy them to the** `/export/clientfiles` **directory. You must be root at label** `ADMIN_LOW`**.**

   For example, most sites will want to copy the `/var/sadm/smc/toolboxes/tsol_`*nameservice*`/tsol_`*nameservice*`.tbx` file to the client machines. A site that is using a modified `tnrhtp` file, DNS, and auditing might copy the files `/etc/security/audit_control`, `/etc/security/audit_startup`, `/etc/security/tsol/tnrhtp`, `/etc/resolv.conf`, and `/etc/nsswitch.conf`.

4. **Transfer the** `label_encodings` **file to a diskette labeled** `ADMIN_HIGH`**.**

   If you are unsure of the steps, see "To Copy to a Diskette" on page 49.

5. **Transfer the other files to a diskette labeled** `ADMIN_LOW`**.**

▼ Delete the User install

The user `install` is useful for installing and initially configuring a workstation. Where site security demands, the admin role at label `ADMIN_LOW` removes the user.

Caution - Do not remove the user install until you are satisfied that the client workstations can communicate with the NIS master server.

- **See "How to Delete a Local User" on page 76 if you have not deleted a local user in the Trusted Solaris system before.**

CHAPTER 8

Configuring a NIS or NIS+ Client

This chapter provides procedures to configure the name service clients at your site interactively, after you have configured the NIS+ master.

Who Does What

Trusted Solaris software is designed to be installed and configured by an install team. Once the team has created users who can assume Trusted Solaris roles, and has rebooted the workstation, the software enforces task division by role. If two-person installation is not a site security requirement, you can assign the administrative roles to one person.

Client Configuration Tasks

Configuring a name service client is similar to configuring its master, except that configuration details the client receives from the master do not have to be repeated.

Depending on your site configuration and installation method, some procedures can be omitted.

▼ Log In and Protect the Workstation

1. **Log in as a user who can assume the root role and assume it.**

   See "How to Log In" on page 41 if you are unsure of the steps.

2. **Protect the workstation.**

   See "How to Protect Machine Hardware" on page 46 if you are unsure of the steps.

▼ Copy Configuration Files from the Master

For the NIS+ name service, you made a diskette for the client in "Copy Configuration Files for Distribution to Clients" on page 109. For the NIS name service, you made a diskette for the client in "Copy Configuration Files for Distribution to Clients" on page 123.

To Copy Master Files from Diskette

1. **As root, at label** `ADMIN_LOW`**, make a temporary directory and go to it.**

```
# mkdir /export/clientfiles
# cd /export/clientfiles
```

2. **Copy the files from the diskette.**

   See “To Copy from a Diskette” on page 49 if you are unsure of the steps.

▼ Copy the Name Service Master’s label_encodings File

The `label_encodings` file on the client machine must be identical to the one on the name service master. If you are *sure* it is identical, you may skip this step.

1. **As root, at label `ADMIN_HIGH`, copy the name service master’s `label_encodings` file to the `/etc/security/tsol` directory.**

   Follow the procedure in “To Copy from a Diskette” on page 49.

2. **Continue with “How to Install a Label Encodings File” on page 59 to install and read the label encodings file into the environment.**

▼ Initialize the Solaris Management Console

1. **Follow the procedure “To Initialize the SMC Server” on page 54.**

2. **Use two File Managers to copy the name service master’s toolbox file from `/export/clientfiles` to `/var/sadm/smc/toolboxes/tsol_`*name_service*`/tsol_`*name_service*`.tbx`.**

▼ Set Up Static Routing

If you set up static routing on the name service master, set it up on the clients.

1. **Determine the appropriate static routing for the client.**

TABLE 8–1 Client Static Routing Entry

	Client on same subnet	Client on different subnet
Name service master has 1 network interface	Use same entry as master's	Static routing will be slightly different for the subnet
Name service master has >1 network interface	Enter master's other network interface(s) in static routing file	

2. **To set up static routing, complete one of the following procedures: "To Set Up Simple Static Routing" on page 60 or "To Set Up Complex Static Routing" on page 61**

▼ Add Remote Hosts

The install team enters every host that the local machine should contact upon booting into the local hosts database. If the local machine is a name service client, it will find its file servers, home directory server, and other servers from the name service master.

- **Follow the procedure "How to Add Hosts" on page 62.**

▼ Copy the Name Service Master's Tnrhtp Database

You can skip this step if your site is using the `label_encodings` file and the `tnrhtp` file that were installed from the Trusted Solaris 8 Installation CD.

Note - The `tnrhtp`(4) template definition and name for the name service master must be identical on the client and master when you create the client.

- **As root, at label `ADMIN_LOW`, use two File Managers to copy the `tnrhtp` file from the `/export/clientfiles` directory to `/etc/security/tsol/tnrhtp`.**

▼ Assign Templates to Remote Hosts

The clients get most of their template assignments from the name service. The local `tnrhdb` database must contain servers that are contacted during boot, such as the name service master (or its subnet), static routers, and any audit servers.

1. **At the label `ADMIN_LOW`, in an administrative role, initially the root role, invoke the Solaris Management Console from the Application Manager.**

2. **Click *this_host*`: Scope=Files, Policy=TSOL` under Trusted Solaris Management Console in the Navigation pane.**

3. **Click Trusted Solaris Configuration, then Computers and Networks, then double-click Security Families.**

   The remote host templates display in the View pane.

4. **Double-click the `tsol` remote host template.**

5. **Choose Add Host(s) from the Action menu.**

6. **Click Add Host, then enter the IP address and template name (`tsol`) of the Trusted Solaris name service master**

   See "How to Assign a Remote Host Template" on page 65 if you are unsure of the steps.

7. **If the client's audit records are stored on an audit server, add the audit server by choosing Action > Add Host(s), Add Host, and entering the audit servers's IP address and `tsol` host type.**

8. **Choose Add Host(s) from the Action menu, click Add Host, and enter the IP address and host type of the static router(s).**

   A client with one defaultrouter and no audit server would have three entries in its `tnrhdb`:

   1. The client and its host type (`tsol`),
   2. The name service master and its host type (`tsol`) (or its subnet fallback IP address and `tsol`)
   3. The defaultrouter and its host type.

9. **Open a terminal to reload and verify the updated `tnrhdb` database.**

```
# tnctl –H /etc/security/tsol/tnrhdb
# tninfo –h
```

▼ Verify Communication with the Name Service Master

Note - Skip this procedure if the client specified the name service, NIS or NIS+, during network install.

1. **As root, at label** `ADMIN_LOW`**, check to see that you can** `ping` **the name service master.**

```
# ping name-service-master
```

2. **Check to see that you can** `rup` **the name service master.**

```
# rup name-service-master
```

If the `rup`(1) command succeeds, you may proceed. If it fails, debug your network setup until the `rup` command succeeds.

Note - If you have added a client that was not initially on the master, you must add it to the master and assign it a template. On the master, the `ping` and `rup` commands must work to contact the new client.

Summary

These client files must be compatible with the name service master files:

- `/etc/security/tsol/label_encodings`
- `/etc/security/tsol/tnrhtp`

The client's local `tnrhdb`(4) file must have the IP address and host type of the NIS+ master (or the IP address and host type of the subnet), the client's static routers, and the client.

In addition, the client's address and name, the NIS+ master's name and address, and the static routers' names and addresses must be in the local `hosts` database.

Add the Client to the Name Service Domain

Note - Skip this procedure if the client specified a name service during network install. After JumpStart installation, you must do the procedure to add the client to the domain.

▼ Add Client to the NIS+ Domain

Prerequisite: The `rup` command must succeed in both directions: from client to master, and master to client.

1. **As root, at label `ADMIN_LOW`, add the workstation as a NIS+ client using the Create NIS+ Client action in the System_Admin folder.**

   See "To Run a Script from the System_Admin Folder" on page 53 if you are unfamiliar with using trusted actions.

2. **Enter the NIS+ domain name and hostname of the root master. There is a period at the end of the domain name.**

   For example,

   ```
   Domain Name: aviary.eco.org.
   Hostname of NIS+ Master: toucan
   ```

3. **Answer the prompts (`y`, (*your-master's-ip-address*), `nisplus`, *rootpassword*).**

   You can ignore diagnostics printing out that certain files and directories cannot be located. The files and directories will be created.

4. **Do not reboot when the `nisclient`(1M) script prints out:**

   ```
   Once initialization is done, you will need to reboot your machine.
   ```

   You will reboot after setting up DNS.

▼ Add Client to the NIS Domain

1. **As root, at label `ADMIN_LOW`, add the workstation as a NIS client using the Create NIS Client action in the System_Admin folder.**

   Note - If this is a NIS slave server, make sure you enter this host name and the name of the master server at the prompts.

See “To Run a Script from the System_Admin Folder” on page 53 if you are unfamiliar with using trusted actions.

The action copies the `nsswitch.nis` file to the `nsswitch.conf` file.

2. **Do not reboot until after you have set up DNS.**

▼ Set Up DNS and the Name Service Switch

If you are using DNS to contact hosts outside of your domain, or if you have altered the `resolv.conf` and `nsswitch.conf` files on the name service master, set up DNS before rebooting.

- **As root, at label `ADMIN_LOW`, set up the DNS nameservers and the name service switch by copying the files `resolv.conf` and `nsswitch.conf` from the `/export/clientfiles` diskette to the `/etc` directory.**

  Make a copy of the original file and use the File Manager, as described in “To Copy from a Diskette” on page 49.

▼ Reboot the Workstation

Note - Skip this procedure if the client was installed over the network.

---

1. **Shut down the workstation from the TP (Trusted Path) menu.**

2. **If this is a NIS slave server, do the following steps**:

   a. **Log in as install and assume the root role.**

   b. **Open a terminal and run the following command**

```
# /usr/sbin/ypinit –s master_server
```

   c. **Reboot again to enable the slave server to serve clients.**

▼ Share Home Directories

1. **If this client is the home directory server, share home directories by following the steps in “How to Share a File System” on page 66.**

2. **Return to the procedure and chapter you are working from.**

▼ Finish Configuring the Workstation

If you are configuring a site that satisfies criteria for an evaluated configuration, read “Understand Your Site’s Security Policy” on page 24.

Security Administrator Responsibilities

The `secadmin` role handles auditing and security attributes on file systems.

- To configure or to disable auditing, see *Trusted Solaris Audit Administration*.

Note - To ensure that every workstation and user is audited identically, in the root role at label `ADMIN_LOW`, copy the name service master’s `/etc/security/audit*` configuration files to each workstation (see “Copy Configuration Files from the Master” on page 126) . Modify the `dir:` entries as described in *Trusted Solaris Audit Administration*.

- To set security attributes on an unlabeled file system, enter the file system in the `vfstab_adjunct`(4) file.

System Administrator Responsibilities

The `admin` role handles file system management, and user account creation and deletion.

- To share a file system, see “How to Share a File System” on page 66.
- To mount a file system, see “How to Mount a File System” on page 68.
- To delete the install user, see “How to Delete a Local User” on page 76 if you have not deleted a local user in the Trusted Solaris environment before.

Trusted Solaris Administrator’s Procedures provides examples; *Trusted Solaris Administration Overview* provides background.

CHAPTER 9

Installing Trusted Solaris Over a Network

When installing Trusted Solaris software over a network, the system administrator uses the *Solaris 8 Advanced Installation Guide* in conjunction with the Trusted Solaris exceptions and additions described in this chapter.

Due to the security features in the Trusted Solaris environment, Trusted Solaris software modifies some of the procedures used for network installation, JumpStart installation, and Custom JumpStart installation. Also, the Trusted Solaris security and system administrators must enable access to commands on the installation CD-ROM or its image.

Trusted Solaris Modifications to Network Installation

Trusted Solaris software modifies network installation commands and procedures that require greater security. For example, the Volume Manager adds a mounting–user directory when mounting devices in the Trusted Solaris environment.

TABLE 9–1 Solaris and Trusted Solaris Installation and Configuration Differences

Solaris Software	Trusted Solaris Software
You can log in as root.	There is no superuser. You log in as a user who can assume the root role, or as a user who can assume the admin or secadmin role, depending on the task. Then, assume the role to perform the task.
Processes and files do not have a label.	All processes and files are labeled. Commands and actions are run at a particular label. Most administrative tasks are run at the label `ADMIN_LOW`.
Administrators can often use a command line interface, even if a corresponding GUI equivalent exists.	Many administrative commands are run from a GUI, which calls checking and synchronizing functions.
Administrators can run an administrative command from a CD-ROM or diskette.	Commands that are on a diskette or CD–ROM, or are accessible from an NFS mount, may need to be added to the admin role's profile before they can be run.
Allows you to use a CD–ROM or diskette without allocating it.	Requires you to allocate a peripheral device at a particular label before its use. Before removing the medium, you must deallocate it.

Modifications to Network Installation Commands

The following commands and actions are used when installing Solaris software or Trusted Solaris software over a network, and their use is modified in the Trusted Solaris environment. The following listing describes the additional procedures or security requirements. Commands that do not require a change in procedure are not listed. See the "Preparing to Install Solaris Software Over the Network" in *Solaris 8 Advanced Installation Guide* for the installation procedures themselves.

TABLE 9–2 Modified Network Commands

Network Command or GUI	Trusted Solaris Modification in its Use
`setup_install_server`(1M)	You must be in the admin role, at label `ADMIN_LOW`, in a terminal where the command is in a profile assigned to the admin role. If the admin role does not have this */pathname/* command in its assigned profiles, the secadmin role, at label `ADMIN_LOW`, must add it to the Custom Admin Role profile. For the procedure, see "How to Modify a Role's Rights" on page 77.
`add_install_client`(1M)	The requirements for this command to succeed are the same as the requirements for those for `setup_install_server`.
`add_to_install_server`(1M)	The requirements for this command to succeed are the same as those for `setup_install_server`.
`rm_install_client`(1M)	The requirements for this command to succeed are the same as those for `setup_install_server`.
`mount`(1M)	The admin role, at label `ADMIN_LOW`, runs this command. If you are mounting a CD-ROM or diskette on an installed workstation, the admin role must allocate the device at a particular label, usually `ADMIN_LOW`. When the medium is removed, the device must be deallocated.
Host Manager	A graphical user interface that is available from the Solaris Management Console action. You can use Host Manager to specify client information for network installation. This GUI is not available in the Solaris release.

Modifications to Network Installation Procedures

The following procedures are slightly different in the Trusted Solaris environment. The admin role installs software at the label `ADMIN_LOW`; the secadmin role modifies files connected with security.

TABLE 9–3 Modified Network Installation Procedures

Installation Procedure	Trusted Solaris Modification
Create an install server	Users who can assume the roles admin and secadmin should be present.
Give mounted media all allowed privileges.	The secadmin role modifies the `rmmount.conf` file. See "Give Mounted Media All Allowed Privileges" on page 139 for the procedure.
Allocate CD-ROM	The admin role allocates the CD-ROM drive. See "To Allocate a Device" on page 47 if you are unsure of the steps. See "Modify Permissions of Mount Point Parent" on page 140 for additional steps for network install preparation.
Deallocate CD-ROM	The admin role deallocates the drive and removes the CD-ROM. See "To Deallocate a Device" on page 48 if you are unsure of the steps.
Add a command to a role's profile	The secadmin role adds a command to a profile when, for example, the command is not located in the expected directory. See "How to Modify a Role's Rights" on page 77 for this procedure.
Verify that a command is available to a role	The role that needs the command, at the appropriate label (usually `ADMIN_LOW`), verifies that a command that the security administrator has added to the role's profile is available to the role. For the full procedure, see "To Verify That a Command is Available to a Role" on page 79. See Example 9–1 at the end of this table for a sample verification command.
Remove a command from a role's profile	The secadmin role removes the command from the role's profile. This is a security measure, so that the command will not be used at an inappropriate time. For the procedure, see "To Remove a Command from a Role's Rights" on page 79.
Add client information with the add_install_client command	The admin role, on the install server launches the Name Service Switch action. Ensure that the value of `ethers` and `bootparams` is `files nisplus`, as in: ethers: files nisplus dns netmasks: files nisplus dns bootparams: files nisplus dns

TABLE 9–3 Modified Network Installation Procedures *(continued)*

Installation Procedure	Trusted Solaris Modification
Remove client information with the rm_install_client command	The admin role, on the install server, executes the `rm_install_client` command.
Reboot the install server	If you are unfamiliar with rebooting a Trusted Solaris workstation, see "To Reboot the Workstation" on page 80.

EXAMPLE 9–1 Admin Role Verifying that a Command is Available

If the commands `add_install_client` and `rm_install_client` are in the admin role's profile, the `profiles`(1) command should display something like the following for a disk image:

```
$ profiles –l | grep install_client
/export/install/ts8_sparc/add_install_client: 4,5,6,10,11,12,17,30,32,33,35,36,39,52,55,57,61,68,69
/export/install/ts8_sparc/rm_install_client:  4,5,6,10,11,12,17,30,32,33,35,36,39,52,55,57,61,68,69
```

Additional Steps to Set up Software Installation

To install from a CD-ROM, users who can assume administrative roles must be present. The secadmin role gives all allowed privileges to the CD-ROM device and modifies profiles where necessary. The admin role allocates the device, changes the permissions on the parent of the mount point, and installs the software.

▼ Give Mounted Media All Allowed Privileges

1. **Log in as a user who can assume the secadmin role and assume it.**
2. **Open the Admin Editor from the System_Admin folder.**
3. **Assign all allowed privileges to mounted removable media in the `/etc/rmmount.conf` file, as in:**

```
mount * hsfs udfs ufs -o nosuid allowed=all
```

4. **Write the file with `:wq!` and exit the editor.**

▼ Modify Permissions of Mount Point Parent

In the admin role, after allocating the CD-ROM, a File Manager will pop up showing the mount point of the CD-ROM. If it does not appear, bring up a File Manager from the Front Panel.

For Trusted Solaris software, the mount point should be `/cdrom/admin-cdrom_0/trusted_sol_8_sparc` or `/cdrom/admin-cdrom_0/trusted_sol_8_ia`.

1. **In the File Manager, highlight `/cdrom/admin-cdrom_0`, the parent of the mount point.**

2. **From the Selected menu, choose Properties.**

   Note that the directory, named CD-ROM_FOLDER, has mode 700, so it is not searchable. The following steps will fix that.

3. **Click the Show Access Control List button, then Add ...**

4. **Highlight the Mask entry and click Change.**

5. **Change the Mask to Read and Execute, and click Change.**

6. **Click Add..., and enter root in the User field, giving it Read and Execute.**

7. **Click Add, then click OK to exit the dialog.**

8. **Leave the File Manager up, available for the installation setup commands.**

▼ Load Trusted Solaris Images from CDs

1. **In the File Manager, open the Tools folder, one of `/cdrom/admin-cdrom_0/trusted_sol_8_sparc/Trusted_Solaris_8/Tools` or `/cdrom/admin-cdrom_0/trusted_sol_8_ia/Trusted_Solaris_8/Tools`.**

2. **From the File menu select Open Terminal.**

3. **Still in the admin role, transfer the files from the first CD to the install server by typing**

```
$ ./setup_install_server /export/install/ts8_{sparc,ia}
```

Note - Do not double-click on this tool because the command must be started in a profile shell, not the shell defined in the File Manager.

By default, the Software Installation profile contains the exact pathname for this command, assuming that the role name is called "admin". This profile must be modified if a different mount point is used. To modify a profile, see “How to Modify a Role’s Rights” on page 77.

4. **When the pound sign (#) prompt displays, deallocate the CD.**

5. **Insert the second CD and allocate it.**

6. **For the second CD, still in the admin role, repeat Step 1 on page 140 through Step 8 on page 140.**

7. **In the File Manager, open the Tools folder on the second CD, one of** `/cdrom/admin-cdrom_0/trusted_sol_8_sparc/Solaris_8/Tools` **or** `/cdrom/admin-cdrom_0/trusted_sol_8_ia/Solaris_8/Tools`**.**

8. **From the File menu select Open Terminal.**

9. **Transfer the files from the second CD to the install server by typing**

```
$ ./add_to_install_server /export/install/ts8_{sparc,ia}
```

Note - Do not double-click on this tool because the command must be started in a profile shell, not the shell defined in the File Manager.

▼ Set up the Network Install Server for Installation Clients

To complete client installation, editing files and executing commands must be done in the admin role. Follow the instructions for Solaris network installation setup, using the following procedures when needed.

1. **To share the server's network install directories so that they are available to the clients, in the admin role at label** `ADMIN_LOW`**, do the following:**

   a. **Run the Share Filesystems action from the System_Admin folder in the Application Manager.**

      The Share Filesystems action opens the `/etc/dfs/dfstab` file.

   b. **Enter the network install directory, and any relevant options.**

      For example,

      ```
      share –F nfs –o ro,anon=0 –d "netinstall dir" /export/ts8_sparc_install
      ```

   c. **Write the file and quit the editor.**

   d. **Open a terminal to run the** `share`**(1M) command to share the file systems.**

      For example,

```
$ share /export/ts8_sparc_install
$ share /jumpstart
```

   e. **Verify that the directories are shared by running the** `showmount` **command:**

```
$ showmount –e
export list for install_server:
/export/ts8_sparc_install
/jumpstart
```

   f. **If it returns the following error:** `showmount: server: RPC: Program not registered`**, start the nfs.server daemon, and verify the directories are shared.**

```
$ /etc/init.d/nfs.server stop
$ /etc/init.d/nfs.server start
$ showmount –e
export list for install_server:
/export/ts8_sparc_install
/jumpstart
```

2. **To modify or create files in the `/etc` directory, use the Admin Editor from the System_Admin folder in the Application Manager in order to give the file the correct security attributes.**

   See "To Create or Open a File from the Trusted Editor" on page 52 for how to create or modify a file using the Admin Editor. For example, to create an empty `ethers` file, do the following:

   a. **In the admin role in an `ADMIN_LOW` workspace, invoke the Admin Editor.**

   b. **Enter the full path to the file, `/etc/ethers`.**

   c. **Once the editor is open, type `:wq` to save the empty file.**

3. **Run the Name Service Switch action from the System_Admin folder.**

4. **Run the Admin Editor action, and enter `/etc/nsswitch.conf` as the file to edit.**

5. **Change the `ethers`, `netmasks`, and `bootparams` entries in the file to read as follows:**

```
ethers: files nisplus dns
netmasks: files nisplus dns
bootparams: files nisplus dns
```

Note - After adding clients to the network install server, reboot the server before attempting to install the clients over the network.

Trusted Solaris Modifications to Custom JumpStart

In the Trusted Solaris environment, Custom JumpStart procedures are handled by administrative roles. For an explanation of Custom JumpStart, see "Preparing Custom JumpStart Installations" in *Solaris 8 Advanced Installation Guide*. Prepare to modify Custom JumpStart procedures with Trusted Solaris security requirements, such as device allocation and task allocation by role.

Note - Factory-installed JumpStart may not be supported by Trusted Solaris software.

Modifications to Custom JumpStart Procedures

The following procedures are slightly different in the Trusted Solaris environment.

Note - The Trusted Solaris environment does not support mounting remote file systems during installation.

TABLE 9–4 Modified Custom JumpStart Procedures Setup

Custom JumpStart Procedure	Trusted Solaris Modification
Create a Custom JumpStart diskette	Users who can assume the roles admin and secadmin should be present.
Allocate diskette drive	As admin, at label `ADMIN_LOW`, allocate the floppy drive. See “To Allocate a Device” on page 47 if you are unsure of the steps.
Deallocate diskette drive	As admin, at label `ADMIN_LOW`, deallocate the drive and remove the diskette. See “To Deallocate a Device” on page 48 if you are unsure of the steps.
Format a diskette	As admin, at label `ADMIN_LOW`, run the `fdformat` command.
Create a filesystem on a diskette	As admin, at label `ADMIN_LOW`, run the `newfs` command.
Create a mount point on a diskette	As admin, at label `ADMIN_LOW`, run the `mkdir` command.
Mount the directory	As admin, at label `ADMIN_LOW`, run the `mount` command. See Example 9–2 at the end of this table for a sample `mount` command.
Populate the directory	As admin, at label `ADMIN_LOW`, run the `cp` command to copy the JumpStart sample directory to the diskette.
Create a JumpStart directory on a server	As admin, at label `ADMIN_LOW`, run the `mkdir` command.

TABLE 9–4 Modified Custom JumpStart Procedures Setup *(continued)*

Custom JumpStart Procedure	Trusted Solaris Modification
Share the directory	For details of the procedure, see “How to Share a File System” on page 66.
Share the file system	For details of the procedure, see “How to Share a File System” on page 66.
Enable access to JumpStart directory	As admin, at label `ADMIN_LOW`, use the `–c` option to the `add_install_client` command to add JumpStart details to the local `bootparams` database.
Check access to JumpStart directory	On the install server, as role admin at label `ADMIN_LOW`, view the `bootparams` database. For details, see “To Locate a Solaris Management Console Tool” on page 56.

EXAMPLE 9–2 Mount a UFS Filesystem on a Diskette

To create a UFS file system on a diskette to be used for Custom JumpStart, as admin at `ADMIN_LOW`:

```
$ mkdir /ts8_jumpstart
$ mount –F ufs /dev/diskette /ts8_jumpstart
```

Modifications to Custom JumpStart Profiles

Use the Trusted Solaris information in the following table to modify the procedures in “Creating a Profile” in *Solaris 8 Advanced Installation Guide*.

TABLE 9–5 Modified JumpStart Profile Procedures

Solaris Procedure	Trusted Solaris Modification
Edit a profile file.	As admin role at label `ADMIN_LOW`, use the Admin Editor action. For how to use the Admin Editor, see “To Create or Open a File from the Trusted Editor” on page 52. The upgrade keyword is not supported in Trusted Solaris 8.

Use the Trusted Solaris information that follows to modify the procedures in "Testing a Profile" in *Solaris 8 Advanced Installation Guide* and "pfinstall" in *Solaris 8 Advanced Installation Guide.*

In the Trusted Solaris environment, testing profiles is handled by the admin role.

▼ How to Use pfinstall to Test a Profile

1. **On an installed and configured Trusted Solaris host, log in as a user who can assume the admin role.**

2. **As admin at label** `ADMIN_LOW`**, launch a terminal and see that the** `pfinstall`**(1M) command is available in the role's profile shell.**

```
$ profiles –l | grep pfinstall
```

Note - The name profile shell refers to a shell that recognizes Trusted Solaris execution profiles. It does not refer to the machine profiles being tested here.

---

3. **If the command is not in the profile, the secadmin role must add it to the admin role's rights, and then the admin role launches a new terminal in which to run the command.**

   See "How to Modify a Role's Rights" on page 77 for how to add the `pfinstall` command to the admin role's rights profile.

Modifications to Custom JumpStart Rules

Use the Trusted Solaris information in the following table to modify the procedures in "Creating the rules File" in *Solaris 8 Advanced Installation Guide.*

TABLE 9–6 Modified JumpStart Rule Procedures

Solaris Procedure	Trusted Solaris Modification
Edit a rules file	As role admin at label `ADMIN_LOW`, use the Admin Editor action. For how to use the Admin Editor, see "To Create or Open a File from the Trusted Editor" on page 52.
Use a Trusted Solaris–specific value for a keyword	For the `installed` option, the *version* keyword. *version* - A version name, such as `Trusted_Solaris_8`, or the special word `any`. If `any` is used, any Trusted Solaris or SunOS release is matched. For the `osname` option, the *version* keyword. *version* — A version of Trusted Solaris the Trusted Solaris environment installed on the workstation: for example, Trusted Solaris 7.
Validate a rules file	Run the `check` script as role admin at label `ADMIN_LOW`.
Copy a rules file	As admin at label `ADMIN_LOW`, copy the file.

Modifications to Optional Custom JumpStart

Use the Trusted Solaris information that follows to modify the procedures in "Using Optional Custom JumpStart Features" in *Solaris 8 Advanced Installation Guide*.

Modifications to Begin and Finish Scripts

Use the Trusted Solaris information in the following table to modify the procedures in "Creating Begin Scripts" in *Solaris 8 Advanced Installation Guide* and "Creating Finish Scripts" in *Solaris 8 Advanced Installation Guide*.

TABLE 9–7 Modified JumpStart Script Procedures

Solaris Procedure	Trusted Solaris Modification
Create a begin or finish script	Scripts are handled by the admin role at label `ADMIN_LOW` using the Admin Editor action. The scripts must be profile shell scripts, such as `pfsh` or `pfksh`. See the `pfexec`(1) man page.

Trusted Solaris Script Examples

Begin and finish scripts in the Trusted Solaris environment are edited by an administrative role, and run in a profile shell. See the `pfexec`(1) man page for information on profile shells.

▼ Reboot the Workstation with a Finish Script

♦ **Add the last line in the example finish script to every finish script you create.**

```
#!/bin/pfsh
/usr/sbin/reboot
```

▼ Add label_encodings File with a Finish Script

Note - Use the Trusted Solaris information that follows to modify the procedure in "To Add Files With a Finish Script" in *Solaris 8 Advanced Installation Guide*.

♦ **For example, if you are using a custom JumpStart diskette to install Trusted Solaris software, place a copy of the site's `label_encodings` file into the JumpStart directory on the diskette.**

The following finish script copies the file from the JumpStart directory into a workstation's `/etc/security/tsol` directory during a custom JumpStart installation:

```
#!/bin/pfsh
cp ${SI_CONFIG_DIR}/ label_encodings  /a/etc/security/tsol
```

▼ Set the Root Password With a Finish Script

Note - Use the Trusted Solaris information that follows to modify the procedures in "Setting the System's Root Password With a Finish Script" in *Solaris 8 Advanced Installation Guide.*

♦ **As admin at label** `ADMIN_LOW`**, set the variable PASSWD to an encrypted root password obtained from an existing entry in a workstation's** `/etc/shadow` **file.**

Caution - If you set your root password by using a finish script, be sure to safeguard against those who will try to discover the root password from the encrypted password in the finish script.

Modifications to Creating a Disk Configuration File

In the Trusted Solaris environment, configuration files are handled by the admin role. Use the following information to modify the procedures in "Creating Disk Configuration Files" in *Solaris 8 Advanced Installation Guide.*The Intel architecture procedure also modifies "fdisk" in *Solaris 8 Advanced Installation Guide.*

▼ SPARC: To Create a SPARC Disk Configuration File

1. **Log on as a user who can assume the admin role.**

2. **As admin at label** ADMIN_LOW**, launch a terminal and determine the device name for the workstation's disk.**

3. **Redirect the output of** prtvtoc **to create the disk configuration file:**

```
$ prtvtoc /dev/rdsk/device_name > disk_config
```

▼ IA: To Create an Intel Disk Configuration File

1. **As admin at label** ADMIN_LOW**, redirect the output of the following** prtvtoc **command to a file.**

```
$ prtvtoc /dev/rdsk/device_name > file1
```

2. **Save the output of the following** fdisk **command to a file.**

```
$ fdisk –R –d –n /dev/rdsk/device_name 2>file2
```

3. **Concatenate the two files to create a disk configuration file.**

```
$ cat file1 file2 > disk_config
```

4. **Copy the disk configuration file to the JumpStart directory: :**

```
$ cp disk_config     jumpstart_dir_path
```

Trusted Solaris Differences for a JumpStart Example

Note - Use the Trusted Solaris information that follows to modify the example in "Example of Setting Up and Installing Solaris Software With Custom JumpStart" in *Solaris 8 Advanced Installation Guide.*

In the Trusted Solaris environment, the Solaris JumpStart marketing and engineering example requires a user to assume the admin role.

- The site uses NIS+. The Ethernet addresses, IP addresses, and host names are in NIS+ tables.
- JumpStart information must use "None" for the naming service. Hosts installed by JumpStart are cliented after JumpStart finishes.
- All commands are done by a particular role at a particular label, usually `ADMIN_LOW`. To execute a command, the role must have the command at that label in its Rights Profile.
- All directories are created by the admin role at the label `ADMIN_LOW`, as in:

```
$ cp –r /export/install/jumpstart_sample /jumpstart
```

- To create a shared directory, in the admin role at label `ADMIN_LOW` follow the procedure in "How to Share a File System" on page 66 to create a `vfstab` entry, as in:

```
share –F nfs –o ro,anon=0 /jumpstart
```

- To create a profile, the security administrator in the admin role at label `ADMIN_LOW` uses the Admin Editor action.
- To edit the rules file, the admin role at the label `ADMIN_LOW` uses the Admin Editor action.
- To execute the check script, the admin role at the label `ADMIN_LOW` runs the `check`(1M) script, as in:

```
$ cd /jumpstart
$ ./check
```

▼ Set up the engineering systems for installation

On the install server, the admin role at the label ADMIN_LOW uses the add_install_client(1M) command:

```
$ cd /export/install
$ ./add_install_client –c server_1:/jumpstart host_eng1 sun4u
$ ./add_install_client –c server_1:/jumpstart host_eng2 sun4u
  .
```

▼ Set up the marketing systems for installation

An administrator in the admin role at label ADMIN_LOW then uses the setup_install_server(1M) command that copies the boot software from the CD to the marketing server.

```
$ cd /cdrom/cdrom0/s0/Trusted_Solaris_8/Tools
$ ./setup_install_server –b /marketing/boot-dir sun4c
```

At label ADMIN_LOW, the admin role uses the add_install_client command on the marketing group's boot server.

```
$ cd /marketing/boot-dir
$ ./add_install_client –s server_1:/export/install \
–c server_1:/jumpstart host_mkt1 sun4c
$ ./add_install_client –s server_1:/export/install \
–c server_1:/jumpstart host_mkt2 sun4c
  …
```

APPENDIX **A**

Site Security Policy

Each Trusted Solaris site is unique and must determine its own security policy. Perform the following tasks when creating and managing a security policy.

- Establish a security team. The security team should have representation from toplevel management, personnel management, computer system management and administrators, and facilities management. The team should review Trusted Solaris administrators' policies and procedures, and recommend general security policies that apply to all system users.
- Educate management and administration personnel about the site security policy All personnel involved in the management and administration of the site should be educated about the security policy. Security policies should not be made available to ordinary users since this policy information has direct bearing on the security of the computer systems.
- Educate users about Trusted Solaris and the policy. All users must be familiar with the Trusted Solaris User's Guide. Because the users are usually the first to know when a system is not functioning normally, the user should become acquainted with the system and report any problems to a system administrator. A secure environment needs the users to notify the system administrators immediately if they notice:
  - A discrepancy in the last login time that is reported at the beginning of each session
  - An unusual change to file data
  - A lost or stolen human-readable printout
  - The inability to operate a user function
- Enforce the security policy. If the security policy is not followed and enforced, the data contained in Trusted Solaris will not be secure. Procedures should be established to record any problems and the measures that were taken to resolve the incidents.

- Review the security policy. The security team should perform a periodic review of the security policy and all incidents that occurred since the last review. Adjustments to the policy can then lead to increased security.

Site Security Policy and the Distributed System

The security administrator should design the distributed system based on the site's security policy. The security policy dictates configuration decisions regarding such things as:

- How much auditing will be done for all users in the system and for which classes of events
- How much auditing will be done for users in roles and for which classes of events
- How audit data will be managed, archived, and reviewed
- Which labels will be used in the system and whether the ADMIN_LOW and ADMIN_HIGH labels will viewable by ordinary users
- Which user clearances will be assigned to individuals
- Which devices (if any) will be allocatable by which normal users
- Which label ranges are defined for machines, printers, and other devices
- Whether the Trusted Solaris system will be used in an evaluated configuration or in an extended configuration.

Computer Security Recommendations

The following list of guidelines provides some things to consider when developing a security policy for your site.

- The maximum label of the Trusted Solaris distributed system (the highest label in the user accreditation range) should not be greater than the maximum security level of work being done at the site.
- System reboots, power failures, and shutdowns should all be recorded manually in a site log.
- File-system damage should be documented and all affected files should be analyzed for potential security-policy violations.
- Operating manuals and administrator documentation should be restricted to individuals with a valid need for access to that information.

- Unusual or unexpected behavior of any Trusted Solaris software should be reported and documented, and the cause should be determined.
- If possible, at least two individuals should administer Trusted Solaris. One should be assigned security administrator authorization for security-related decisions, and the other should be assigned the system administrator authorization for computer management tasks.
- A regular backup routine should be established.
- Authorizations should be assigned only to users who need them and who can be trusted to use them properly.
- Privileges should be assigned to programs only when the program needs the privileges to do its work, and only when the programs have been scrutinized and proven to be trustworthy in their use of privilege. Review the privileges on existing Trusted Solaris programs for a guide to setting privileges on new programs.
- Audit information should be reviewed and analyzed regularly. Any irregular events should be noted and investigated to determine the cause of the event.
- The number of administration IDs should be minimized. The install user account should be disabled after an authorized security administrator user is established.
- The number of set user ID and set group ID programs should be minimized. Setuid/setgid programs should be employed only in protected subsystems.
- An administrator should regularly verify that normal users have a valid login shell.
- An administrator should regularly verify that normal users have valid user ID values and not system administration ID values.
- Consider TEMPEST shielded equipment and fiber-optic network cables to reduce electronic radiation emitted from computer equipment.
- Only certified technicians should open and close TEMPEST equipment to ensure its ability to shield electromagnetic radiation.

Physical Security Recommendations

- Restrict access to the Trusted Solaris system. The most secure locations are generally interior rooms that are not on the ground floor.
- Monitor and document access to Trusted Solaris.
- Secure computer equipment to large objects such as tables and desks to prevent theft. When equipment is secured to a wooden item, increase the strength of the item by adding metal plates.

- Consider removable storage media for sensitive information. Lock up all removable media when not in use.
- Store system backups and archives in a secure location separate from the location of the Trusted Solaris system.
- Restrict physical access to the backup and archival media in the same manner as access to the Trusted Solaris system.
- Install a high-temperature alarm in the computer facility to indicate when the temperature is outside of the range of the manufacturer's specifications. A suggested range is 10°C to 32°C (50°F to 90°F).
- Install a water alarm in the computer facility to indicate water on the floor, in the subfloor cavity, and in the ceiling.
- Install a smoke alarm to indicate fire.
- Install a fire-suppression system.
- Install a humidity alarm to indicate too much or too little humidity.
- Consider TEMPEST shielding if machines do not have it. TEMPEST shielding may be appropriate for facility walls, floors, and ceilings.
- Check for physical gaps that allow entrance to the facility or the rooms containing computer equipment. Look for openings under raised floors, in suspended ceilings, in roof ventilation equipment, and in adjoining walls between original and secondary additions.
- Prohibit eating, drinking, and smoking in computer facilities or near computer equipment. Establish areas where these activities can occur without threat to the computer equipment.
- Protect architectural drawings and diagrams of the computer facility.
- Restrict the use of building diagrams, floor maps, and photographs of the computer facility.

Personnel Security Recommendations

- Inspect packages, documents, and storage media entering and leaving a secure site.
- Require identification badges on all personnel and visitors at all times.
- Use identification badges that are difficult to copy or counterfeit.
- Establish areas that are prohibited for visitors and clearly mark the areas.
- Escort visitors at all times.

Common Security Violations

Because no computer is 100% secure, a computer facility is only as secure as the people who use it. The limitations of an administrator are directly related to the actions of all individuals involved with the use of computer equipment and its facilities. Although most actions that violate security are easily resolved by careful users or additional equipment, the following list gives examples of problems that can occur:

- Users give passwords to other individuals who should not have access to the computer system.
- Users write down passwords and lose or leave the passwords in nonsecure locations.
- Users set their passwords to easily guessed words or names.
- Users learn passwords by watching other users when they enter a password.
- Unauthorized users remove, replace, or physically tamper with hardware.
- Users leave their workstations or terminals unattended without locking the screen.
- Users change the permissions on a file to allow other users to read the file.
- Users change the labels on a file to allow other users to read the file.
- Users discard sensitive hardcopy documents without shredding them or leave sensitive hardcopy documents in insecure locations.
- Users leave access doors unlocked.
- Users lose their keys.
- Users do not lock up removable storage media.
- Computer screens are visible through exterior windows.
- Network cables are tapped.
- Electronic eavesdropping captures signals emitted from computer equipment.
- Power outages, surges, and spikes destroy data.
- Earthquakes, floods, tornadoes, hurricanes, and lightning destroy data.
- External electromagnetic radiation interference such as sun-spot activity scrambles files.

Additional Security References

As a trusted administrator, you should become familiar with the standards established by various government agencies. Government publications describe in

detail the standards, policies, methods, and terminology associated with computer security.

Other publications listed here are guides for system administrators of UNIX systems and are useful in gaining a thorough understanding of UNIX security problems and solutions. Some publications listed here describe successful attempts to penetrate computer systems around the world and illustrate real threats to computer security. These publications emphasize the importance of computer systems managed by knowledgeable and capable administrators.

U.S. Government Publications

Computer Security Requirements, Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments, DoD, CSC-STD-003-85, 1985.

Department of Defense Password Management Guideline, DoD, CSC-STD-002-85, 1985.

Department of Defense Trusted Computer System Evaluation Criteria (TCSEC) National Computer Security Center, DoD 520.28-STD, 1985.

Graubart, Richard D., J.L. Berger, and John P.L. Woodward, *Compartmented Mode Workstations Evaluation Criteria, Version 1*, DIA DDS-2600-6243-91, Mitre, Bedford, Massachusetts, March 1991.

Personal Computer Security Considerations, National Computer Security Center, NCSC-WA-002-85, 1985.

Technical Rationale behind CSC-STD-003-85 Computer Security Requirements, Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments, DoD, CSC-STD-004-85, 1985.

Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria, National Computer Security Center, NCSC-TG-005 Version 1, 1987.

Woodward, John P.L., *Security Requirements for System High and Compartmented Mode Workstations*, DIA DDS-2600-5502-87, Mitre, Bedford, Massachusetts, November 1987.

UNIX Security Publications

Farrow, Rik, *UNIX System Security*, Addison-Wesley, Reading, MA, 1991.

Garfinkel, Simson, and Gene Spafford, *Practical UNIX Security*, O'Reilly & Associates, Inc., Sebastopol, CA, 1991.

Gregory, Peter, *Solaris Security*, Sun Microsystems Press, September 1999.

Hayes, Frank, "Is Your System Safe?" *UNIXWORLD*, June 1990.

Wood, Patrick H., and Stephen Kochan, *UNIX System Security*, Hayden Books, Indianapolis, IN, 1986.

General Computer Security Publications

Denning, Peter J., *Computers under Attack: Intruders, Worms and Viruses*, ACM Press, Addison-Wesley, Reading, MA, 1990.

Farrow, Rik, "Inside the Internet Worm," *UNIXWORLD*, June 1990.

Hafner, Katie, and John Markroff, *Cyberpunk: Outlaws and Hackers on the Computer Frontier*, Simon & Schuster, New York, NY, 1991.

Levy, Steven, *Hackers: Heroes of the Computer Revolution*, Dell Books, New York, NY, 1984.

McAffe, John, and C. Haynes, *Computer Viruses, Worms, Data Diddlers, Killer Programs, and Other Threats to Your System*, St. Martin's Press, New York, NY, 1989.

Page, Bob, "A Report on the Internet Worm," University of Lowell, Computer Science Department, November 1988.

Russell, Deborah, and G.T. Gangemi, Sr., *Computer Security Basics*, O'Reilly & Associates, Inc., Sebastopol, CA, 1990.

"Special Report: Computer Security and the Internet", *Scientific American*, October 1998. pp 95–117. Contains articles on hackers, firewalls, encryption, digital signatures, and Java, with extensive bibliographies.

Seeley, Donn, "A Tour of the Worm," University of Utah Department of Computer Science, Technical Report, November 1988.

Spafford, Eugene H., "The Internet Worm: Crisis and Aftermath," *Communications of the ACM*, June 1989.

Stoll, Cliff, *The Cuckoo's Egg*, Doubleday, Garden City, NY, 1989.

Thompson, Ken, "Reflections on Trusting Trust," 1983 ACM Turing Award Lecture, *Communications of the ACM*, August 1984.

General UNIX Publications

Bach, Maurice J., *The Design of the UNIX Operating System*, Prentice Hall, Englewood Cliffs, NJ, 1986.

Kobert, Jeannie Johnstone, *Guide To High Availability: Configuring boot/root/swap*, Sun Microsystems Press, September 1999.

Nemeth, Evi, Garth Snyder, and Scott Seebas, *UNIX System Administration Handbook*, Prentice Hall, Englewood Cliffs, NJ, 1989.

Winsor, Janice, *Solaris 7 Reference*, Sun Microsystems Press, September 1999.

APPENDIX **B**

Checklists for Configuring and Installing Trusted Solaris

The checklists are for planning and for reference. They provide an overall view of what to remember when installing and configuring the workstations at your site, and a record of doing so.

Site Summary Checklist

The following checklists summarize what you have done at your site. Where indicated, there are separate worksheets to plan particular site features, such as servers and labels.

Background Checklist

- Read *Trusted Solaris Administration Overview*.
- Understand site security requirements.
- Read Appendix A.

Checklist Summaries

Labels	See *Trusted Solaris Label Administration*. For highlights, see "Planning Labels" on page 162.

Network	See “Planning the Network” on page 163.
Auditing	See *Trusted Solaris Audit Administration*. For highlights, see “Planning Auditing” on page 164.
Workstations and Servers	See “Planning Workstations” on page 165.
First Users	See “Plan User Security” on page 27 and Table 3–4.
Administrative Roles	See “To Create a Role” on page 69 for password and account locking considerations.
Users, Roles and Rights Profiles	See *Trusted Solaris Administrator’s Procedures.*
Printers	See *Trusted Solaris Administrator’s Procedures* and “Planning Workstations” on page 165.

Planning Labels

Planning labels requires extensive knowledge. *Trusted Solaris Label Administration* describes in detail the modifications required to the `label_encodings` file you choose.

Label visibility exceptions are implemented per user when creating users.

Label visibility exceptions per workstation can be done but are not recommended. See *Trusted Solaris Label Administration* for why and how.

Note - When localizing a label_encodings file, localize the label names only. However, the names ADMIN_HIGH and ADMIN_LOW *must not* be localized. All labeled workstations that you contact must have label names that match the label names in the Trusted Solaris label_encodings file.

Label Decisions

Choose a label_encodings file

1. GFI
2. Site-specific
3. Modified Trusted Solaris single-label
4. Modified Trusted Solaris multilabel

Decide Trusted Solaris configuration	■ Create multiple user Sensitivity Labels — Yes, default ■ Hide upgraded names in directories — No, default
Decide label visibility	Visible to each user, default

Planning the Network

The first decision to make is whether to have an open network or a closed network.

Open Network Security Information

If the network is open:

- Identify accessible domains
- Identify accessible workstations
- Identify Trusted Solaris workstations that can access to unlabeled workstations or domains

Name Service Domain Information

For the NIS or NIS+ domain:

1. Identify the NIS or NIS+ master
2. Identify the NIS or NIS+ slaves/replicas
3. Identify the NIS+ subdomain masters
4. Identify the file servers
5. Identify the audit servers
6. Identify the print servers
7. Identify the mail servers
8. Identify network routers/gateways
9. Identify end user workstations
10. Identify other workstations on the network

Labels of Communicating Machines

Identify the labels at which machines can communicate.

- Determine the label range of each workstation's network interfaces
- Determine the label(s) applied to incoming data from unlabeled workstations

Planning Auditing

Planning auditing can require extensive knowledge. *Trusted Solaris Audit Administration* describes in detail how to set up auditing.

Auditing Security Information

Auditing security decisions include:

- Classes of events to audit for success
- Classes of events to audit for failure
- Classes of events to audit for both
- Users/roles with what additional auditing
- Who has access to the audit administration server
- Who has access to the audit servers
- Who has the rights profile for audit file backup
- Who has the rights profile for audit file review

Auditing System Information

Auditing system decisions include:

- Primary and secondary audit partitions for each workstation
- Size of audit partitions

Planning Workstations

System Information for Each Machine

List the system information for each workstation/server in the Trusted Solaris network:

- name
- kernel architecture
- IP address

Security Information for Each Machine

Determine the security information for each workstation/server in the Trusted Solaris network:

- root password
- PROM/BIOS security level
- PROM/BIOS password
- Attached peripherals permitted?
- Access to printers
- Access to unlabeled domains

APPENDIX **C**

Example Worksheets

The worksheet examples provide you with samples for your workstations, devices, and network.

How to Use the Examples

These are examples only. Do *not* use the IP addresses, names, and other details as they are written here.

Root NIS+ Master Installation Program Example

Dialog Box Title	Answer	Comment
Select a language	0	English
Select a locale	0	English
Networked?	Yes	
Host name	toucan	
IP address	129.159.110.1	
DHCP	No	You should choose DHCP only if this system does not have a permanent IP address and instead gets one from a DHCP server that you have already set up.

Dialog Box Title	Answer	Comment
Primary network interface	le0	You are not prompted for this unless the workstation has more than one network card.
Name service	None	You will turn the machine into the name service master later.
Subnet?	Yes	If your LAN is part of a larger network, say yes.
Subnet mask	255.255.255.0	Check that the default is the appropriate mask for your site.
Time zone	Geographical, US Pacific	A time zone map is provided on the `WWW`.
Date and Time		The default provided is usually the correct clock time.
The answers to the above questions are System ID Information (sysidinfo). When installing over a network, system information is automatically given to the installation program, reducing the installer's interaction with the program.		
Select Geographic Region	North America	Select the regions for which support should be installed.
Install	Install	Upgrade is not supported for this release.
System type	Standalone	
Select Software	Entire software group	For a server, choose Developer or larger.
	Solaris 64-bit support	Choose to enable 64–bit support or not. If you chose IPv6, above, you must choose 64.
Customize?	Yes | No	Customizing a software group often results in software dependencies; system administration knowledge is required to fix dependencies.
Select Disks	c0t0d0, c0t1d0, c0t3d0, c0t5d0	See "Root NIS+ Master Disk Partitioning Example" on page 170 for the details of the example.
Preserve Data?	Preserve | Continue	Probably Continue.
Auto Layout	Continue	Auto Layout displays the minimum disk amounts required per file system.

Dialog Box Title	Answer	Comment
File systems to auto-layout	`/, /usr, /var`	See “Root NIS+ Master Disk Partitioning Example” on page 170
Customize File System and Disk Layout	Customize	Customizing requires advanced system administration skills.
Customize Disks	OK | Continue	See “Root NIS+ Master Disk Partitioning Example” on page 170
Mount remote file systems	No	Mounting in Trusted Solaris is secure. Remote file systems are mounted after their security attributes are known to this machine.
Begin installation	Begin	Read the disk layout and confirm its accuracy.
Auto Reboot	Auto | Manual	
The following prompts are on a plain screen, not in dialog boxes.		
Root password	*List it elsewhere*	Workstation security requires a root password.
Automatic power-saving shutdown	y | n | ?	To recover from power shutdown, press the power key at keyboard upper right.
Confirm	Yes | No	
The Web Launcher starts in Command Line Mode.		
Continue install: [1] Media | [2] Network | [3] Skip.	1	The CD drawer opens. Remove the CD.
Insert the CD for Solaris Software 2.	Insert the second CD and press the `Return` key.	
The screen may be overwritten with messages. Package installation is displayed in 25% increments: `|-1%---25%---50%---75%---100%`		
Enter 1 to review the log, or 2 to end.	2	Press the `Return` key.
The CD drawer opens. Remove the CD. Press the `Return` key to reboot the system.		

Root NIS+ Master Disk Partitioning Example

Workstation Name: toucan

Disk	Slice	Mount point	Size	Disk	Slice	Mount point	Size
c0t0d0	s0	/	80	c0t1d0	s0	/export/Answerbooks	600
	s1	swap	180		s1		
	s2	entire disk	1034		s2	entire disk	1570
	s3	/var	224		s3		
	s4				s4		
	s5				s5		
	s6	/usr	520		s6		410
	s7	/export	10		s7	/export/tools	1380

Disk	Slice	Mount point	Size	Disk	Slice	Mount point	Size
c0t3d0	s0			c0t5d0	s0		
	s1				s1		
	s2	entire disk	2028		s2	entire disk	1980
	s3	/etc/security/audit/toucan	1014		s3	/swapfile	600
	s4				s4		
	s5				s5		
	s6				s6		
	s7	/etc/security/audit/toucan.1	1014		s7	/opt	1380

Services Provided by Servers Example

Use	Name	IP address	Shared File Systems	Security Information
NIS+ servers				
Root NIS+ master	toucan	129.159.110.1	/etc/security/audit/toucan	
NIS+ replica	willet	129.159.110.3	/etc/security/audit/willet	nosuid, nodev, [high]
			/etc/security/audit/willet.1	nosuid, nodev, [high]
Network routers	willet-118 le1	129.159.118.25		
	stilt-223 ie1	129.159.223.20		
	heron-119 le1	129.159.119.26		
File Servers (Share file systems for mounting by end user workstations)				
for home directories	nest	129.159.118.2	/export/home	
for AnswerBooks	worker	129.159.118.7	/usr/all/books	
for CodeMgr	ada	129.159.110.5	/opt/utils/cmgr	
for Man Pages	ada	129.159.110.5	/opt/utils/man	
for Utilities	ada	129.159.118.5	/opt/utils/	
for Applications	worker	129.159.118.7	/usr/all/apps	
Audit Servers (Share all audit file systems for mounting by audit administration server and user workstations)				
	willet		/etc/security/audit/willet.1	nosuid, nodev, [high]
	egret		.../egret.1,2,3,4	nosuid, nodev, [high]
	stilt		.../stilt.1,2,3	nosuid, nodev, [high]
	tern		.../tern.1,2,3,4	nosuid, nodev, [high]
Audit Administration Server (Shares no file systems; mounts all audit file systems)				

Use	Name	IP address	Shared File Systems	Security Information
	audacious	129.159.110.7	None	nosuid, nodev, [high]
Install Server (Shares file system that contains Trusted Solaris image)				
	penguin			
Boot Server (One per NIS+ subdomain)				
	penguin			
Mail Server (Share /var/mail file system)				
	willet			
Print Servers				
	cirrus			
	cumulus			

Audit Server Installation Program Example

Note - You will not be prompted for information that you have provided in NIS+ or in the *boot_server*:`/etc/bootparams` file (during a Custom JumpStart install).

Dialog Box Title	Answer	Comment
Select a language	0	English
Select a locale	0	English
Networked?	Yes	
Host name	willett	
IP address	129.159.110.3	
DHCP	No	You should choose DHCP only if this system does not have a permanent IP address and instead gets one from a DHCP server that you have already set up.

Dialog Box Title	Answer	Comment
Primary network interface	le0	You are not prompted for this unless the workstation has more than one network card.
Name service	NIS+ | NIS | None	Choose the name service if the master is up and running.
Subnet?	Yes	If your LAN is part of a larger network, say yes.
Subnet mask	255.255.255.0	Check that the default is the appropriate mask for your site.
Time zone	Geographical, US Pacific	A time zone map is provided on the WWW.
Date and Time		The default provided is usually the correct clock time.
The answers to the above questions are System ID Information (sysidinfo). When installing over a network, system information is automatically given to the installation program, reducing the installer's interaction with the program.		
Select Geographic Region	North America	Select the regions for which support should be installed.
Install	Install	Upgrade is not supported for this release.
System type	Standalone	
Select Software	Entire software group	For a server, choose Developer or larger.
	Solaris 64-bit support	Choose to enable 64–bit support or not. If you chose IPv6, above, you must choose 64.
Customize?	Yes | No	Customizing a software group often results in software dependencies; system administration knowledge is required to fix dependencies.
Select Disks	c0t0d0, c0t1d0, c0t3d0, c0t5d0	See "Audit Server Disk Partitioning Example" on page 175 for the details of the example.
Preserve Data?	Preserve | Continue	Probably Continue.
Auto Layout	Continue	Auto Layout displays the minimum disk amounts required per file system.

Dialog Box Title	Answer	Comment
File systems to auto-layout	`/, /usr, /var`	See "Root NIS+ Master Disk Partitioning Example" on page 170
Customize File System and Disk Layout	Customize	Customizing requires advanced system administration skills.
Customize Disks	OK | Continue	See "Audit Server Disk Partitioning Example" on page 175 for the details of the example.
Mount remote file systems	No	Mounting in Trusted Solaris is secure. Remote file systems are mounted after their security attributes are known to this machine.
Begin installation	Begin	Read the disk layout and confirm its accuracy.
Auto Reboot	Auto | Manual	
The following prompts are on a plain screen, not in dialog boxes.		
Root password	*List it elsewhere*	Workstation security requires a root password.
Automatic power-saving shutdown	y | n | ?	To recover from power shutdown, press the power key at keyboard upper right.
Confirm	Yes | No	
The Web Launcher starts in Command Line Mode.		
Continue install: [1] Media | [2] Network | [3] Skip.	1	The CD drawer opens. Remove the CD.
Insert the CD for Solaris Software 2.	Insert the second CD and press the `Return` key.	
The screen may be overwritten with messages. Package installation is displayed in 25% increments: `|-1%---25%---50%---75%---100%`		
Enter 1 to review the log, or 2 to end.	2	Press the `Return` key.
The CD drawer opens. Remove the CD. Press the `Return` key to reboot the system.		

Audit Server Disk Partitioning Example

Note - This workstation will be configured as a NIS+ client of the NIS+ root master.

Workstation Name: willet

Disk	Slice	Mount point	Size	Disk	Slice	Mount point	Size
c0t0d0	s0	/	75	c0t1d0	s0		
	s1	swap	160		s1		
	s2	entire disk	1034		s2	entire disk	1980
	s3				s3	/etc/security/audit/willet.1	990
	s4	/var	200		s4		
	s5				s5		
	s6	/usr	350		s6		
	s7	/export/home	250		s7	/etc/security/audit/willet.2	990

Disk	Slice	Mount point	Size	Disk	Slice	Mount point	Size
c0t3d0	s0			c0t5d0	s0		
	s1				s1		
	s2	entire disk	1980		s2	entire disk	1980
	s3	/etc/security/audit/willet.3	990		s3	/etc/security/audit/willet	990
	s4				s4		
	s5				s5		
	s6				s6		
	s7	/etc/security/audit/willet.4	990		s7	/etc/security/audit/willet.5	990

Audit Server Configuration Worksheet

System Administrator Information		Security Officer Information	
Name	willet	root password	
IP address	129.159.110.3	PROM mode	full
Ethernet address	8:0:20:4c:7e:2f	PROM password	
Sun architecture	sun4m		
Network interfaces	le0		
Network router	willet-118 le1 (129.159.118.25)		
Mount Points (For local file systems)		Security Attributes	
	/		
	/usr		
	/var		
	/export/home		nosuid
for NIS+ utils	/opt/nis/		
Mount Points (For remote file systems)			
for Sol AnswerBks	/usr/AB/Sol8.1/		
for TS AnswerBks	/usr/AB/TS8/		
for ManPages	/usr/share/man		
for CodeMgr	/opt/prog/Code		
for Utilities	/opt/dist/Util		
for Applications	/opt/dist/App		
Audit Mount Points			
Primary	/etc/security/audit/tern.1		nosuid, nodev, [high]

System Administrator Information		Security Officer Information
Secondary	/etc/security/audit/egret.1	nosuid, nodev, [high]
Local	/etc/security/audit/willet	nosuid, nodev, [high]
Audit File Systems		
Primary	tern:/etc/security/audit/tern.1/files	
Secondary	egret:/etc/security/audit/egret.1/files	
Local	/etc/security/audit/willet/files	
Mail Server	toucan	
Attached Devices	CDROM (sd6) tape drive (st4)	only usable by those whose profile includes the `device_allocate` command and the `solaris.device.allocate` authorization
Remote Printers	cirrus	
	cumulus	Administrator printer [admin_high] only

Glossary

access control list One type of discretionary access control based on a list of entries that the owner can specify for a file or directory. An access control list (ACL) can restrict or permit access to any number of individuals and groups, allowing finer-grained control than provided by the standard UNIX permission bits.

accreditation range A set of sensitivity labels that are approved for a class of users or resources. See also workstation accreditation range and user accreditation range.

ACL

See access control list

accreditation range A set of valid labels. See accreditation range and user accreditation range for more about the two types of accreditation ranges in the Trusted Solaris environment.

administrative role A role that in the Trusted Solaris environment gives required authorizations, privileged commands, and the Trusted Path security attribute to allow the role to perform part of Solaris superuser's capabilities, such as backup or auditing.

advisory label See information label.

allocation A device to which access is controlled in the Trusted Solaris environment by making the device allocatable to a single user at a time. Allocatable devices include tape drives, floppy drives, audio devices, and CDROM devices. See device allocation.

allowed privilege set The allowed set of privileges limits which privileges a process can use. A process that runs a program that has a forced privilege set

limits that program to the forced privileges that are also in the process' allowed privilege set.

authorization — A right granted to a user or role to perform an action that would otherwise not be allowed by the Trusted Solaris security policy. Authorizations are granted in execution profiles. Certain commands require the user to have certain authorizations to succeed. Similar to the use of privilege on programs.

application search path — In CDE the search path used by the system to find applications and certain configuration information. The application search path is controlled by a trusted role.

AutoClient system — A system type that caches all of its needed system software from an OS server. Because it contains no permanent data, an AutoClient is a field replaceable unit (FRU). It requires a small local disk for swapping and for caching its individual root (`/`) and `/usr` file systems from an OS server. Trusted Solaris does not support autoclients.

begin script — A user-defined Bourne shell script, specified within the rules file, that performs tasks before the Trusted Solaris software is installed on the system. Begin scripts can be used only with custom JumpStart installations.

bootparams file — A file that is consulted when a workstation boots. In Trusted Solaris, the bootparams file contains a keyword=value entry that points the boot server to the Trusted Solaris label configuration for the workstation. A workstation can have a local bootparams file (`/etc/bootparams`), or it can use the bootparams NIS+ table. See bootparams(4).

boot server — A server that provides boot services to workstations on the same subnet. A boot server is required if you plan to push Trusted Solaris information from a central location to every workstation in the system. If the install server is on a different subnet than the workstations that need to install the Trusted Solaris software, you must create a boot server for that subnet.

CDE — See Common Desktop Environment.

clearance — The upper bound of the set of labels at which a user may work, whose lower bound is the minimum label assigned by the security administrator. There are two types of clearance, the session clearance and the user clearance.

client A workstation connected to a network.

closed network A *closed network* is a network of Trusted Solaris workstations that is cut off from any non-Trusted Solaris workstation. The cutoff can be physical, where there is no wire that extends past the Trusted Solaris network. The cutoff can be in the software, where the Trusted Solarisworkstations recognize only Trusted Solarisworkstations. Data entry from outside the network is restricted to peripherals attached to Trusted Solarisworkstations.

cluster A logical grouping of software packages. The Trusted Solaris software is divided into four main software groups, which are each composed of clusters and packages.

CMW label Consists of an `ADMIN_LOW` information label followed by a sensitivity label in brackets, in the form: ADMIN_LOW [SENSITIVITY LABEL].

Common Desktop Environment The required windowing environment for administering the Trusted Solaris software.

.copy_files An optional setup file in a multilabel environment. The file contains the names of startup files, such as `.cshrc` or `.netscape`, that the user environment or user applications require in order for the environment or application to behave well. The files referenced in `.copy_files` are then *copied* to the user's home directory at other labels, when those directories are created. See also .link_files.

core A software group that contains the minimum software required to boot and run the Solaris operating environment on a system. It includes some networking software and the drivers required to run the OpenWindows environment; it does not include the windowing software. Trusted Solaris does not offer a core software group, since the Common Desktop Environment is the required administration environment.

core file A file that contains a picture of the state of a system when it crashed. Also called a core dump.

custom JumpStart installation A type of installation in which the Trusted Solaris software is automatically installed on a system based on a customized profile. You can customize profiles for different types of users.

DAC See discretionary access control.

derived profile A profile that is dynamically created by a begin script during a custom JumpStart installation.

device Devices include printers, workstations, tape drives, floppy drives, audio devices, and internal pseudo terminal devices. Devices are subject to the read equal write equal MAC policy.

device allocation A mechanism for protecting the information on an allocatable device from access by anybody except the user who allocates the device. Until a device is deallocated, no one but the user who allocated a device can access any information associated with the device. For a user to allocate a device, that user must have been granted the device allocation authorization by the security administrator.

developer system support A software group that contains the End User System Support software group plus the libraries, include files, man pages, and programming tools for developing software.

discretionary access control The type of access granted or denied by the owner of a file or directory at the discretion of the owner. The Trusted Solaris environment provides two kinds of discretionary access controls (DAC): permission bits and access control list.

disk configuration file A file that represents a structure of a disk (for example, bytes/sector, flags, slices). Disk configuration files enable you to use `pfinstall` from a single system to test profiles on different sized disks.

domain A part of the Internet naming hierarchy. It represents a group of systems on a local network that share administrative files.

domain address IP address whose last number is 0.

domain name The identification of a group of systems on a local network. A domain name consists of a sequence of component names separated by periods (for example: `tundra.mpk.ca.us`). As you read a domain name from left to right, the component names identify more general (and usually remote) areas of administrative authority.

end user system support A software group that contains the core software group plus the recommended software for an end user, including OpenWindows and DeskSet software.

entire distribution A software group that contains the entire Trusted Solaris release.

entire distribution plus OEM support

A software group contains the entire Trusted Solaris release, plus additional hardware support for OEMs. This software group is recommended when installing Trusted Solaris software on servers.

EISA

Extended Industry Standard Architecture. A type of bus on x86 systems. EISA bus standards are “smarter” that ISA bus systems, and attached devices can be automatically detected when they have been configured via the “EISA configurator” program supplied with the system. See ISA.

/etc

A directory that contains critical system configuration files and maintenance commands.

evaluated configuration

One or more Trusted Solaris workstations which are running in a configuration that has been certified as meeting specific criteria by a certification authority. In the United States, those criteria are the TCSEC and the evaluating and certifying body is the NSA. Trusted Solaris 8 will be certified to the Common Criteria v2.1 [August 1999], an ISO standard, to Evaluation Assurance Level (EAL) 4, and against a number of protection profiles which provide functionality similar to the TCSEC C2 and B1 levels, with some additional functionality.

One or more Trusted Solaris workstations which are running in a configuration that has been certified as meeting specific criteria by a certification authority. Trusted Solaris 8 will be certified to the Common Criteria v2.1 [published in August 1999], an ISO standard, to Evaluation Assurance Level (EAL) 4, and against a number of protection profiles. The Common Criteria v2 (CCv2) and protection profiles make the earlier TCSEC U.S. standard obsolete through level B1+. A mutual recognition agreement for CCv2 has been signed by the United States, the United Kingdom, Canada, the Netherlands, Germany, and France.

The Trusted Solaris 8 configuration target provides functionality similar to the TCSEC C2 and B1 levels, with some additional functionality.

execution profile

Renamed rights profiles in the Solaris 8 release. A bundling mechanism for commands and CDE actions and for the security attributes assigned to the commands and CDE actions. Rights profiles allow Trusted Solaris administrators to control who can execute which commands and to control the attributes these commands have when they are executed. When a user logs in, all rights assigned to that user are in effect, and the user has access to all the commands, CDE actions, and authorizations assigned in all of that user’s rights profiles.

/export A file system on an OS server that is shared with other systems on a network. For example, the `/export` file system can contain the home directories for users on the network.

fdisk partition A logical partition of a disk drive dedicated to a particular operating system on x86 systems. During the Solaris installation program, you must set up at least one Solaris fdisk partition on an x86 system. x86 systems are designed to support up to four different operating systems on each drive; each operating system must reside on a unique fdisk partition.

file server A server that provides the software and file storage for systems on a network.

file privilege set These sets are the allowed and forced privileges specified for use by executable files (programs). The allowed set limits which privileges a process can use, whether the privileges are forced on the executable file or inherited (see inheritable privileges). Any privileges in the forced privilege set are available to any process that invokes the program, as long as they are also in the allowed set.

file system A collection of files and directories that, when set into a logical hierarchy, make up an organized, structured set of information. File systems can be mounted from your local system or a remote system.

finish script A user-defined Bourne shell script, specified within the rules file, that performs tasks after the Trusted Solaris software is installed on the system, but before the system reboots. Finish scripts can be used only with JumpStart installations.

forced privilege set The forced set of privileges are those placed on a file by the security administrator. Any privileges in the forced privilege set are available to any process that invokes the program, as long as they are also in the allowed privilege set.

GFI Government Furnished Information. In this manual, it refers to a U.S. government-provided label_encodings file. In order to use a GFI with Trusted Solaris software, you must add the Sun-specific LOCAL DEFINITIONS section to the end of the GFI. Trusted Solaris Label Administration explains the procedure in detail.

host name The name by which a system is known to other systems on a network. This name must be unique among all the systems within a given domain (usually, this means within any single organization).

A host name can be any combination of letters, numbers, and minus sign (–), but it cannot begin or end with a minus sign.

IA Intel Architecture.

information label A label that signifies the actual security level of the information contained in a file or directory, and which may be used in deciding whether to downgrade the sensitivity label of the file or directory, how to physically label information stored on backup media, and how to handle printed output or mail. Also known as an *advisory label*. Trusted Solaris 7 and later releases no longer support information labels.

inheritable privilege The privileges that a process can pass to a program across an `execve( )` without their being affected by the new program's forced or allowed privilege sets. When a new program is executed by a process, the inheritable set of the process is set to be equal to the inheritable set of the old program. The inheritable set is not affected by the forced or allowed privileges on the currently executing program, which allows privileges to be passed from programs that cannot use them to programs that can.

initial label The minimum label assigned to a user or role, and the label of the user's initial workspace. It is the lowest label at which the user or role can work.

initial installation option An option presented during the Trusted Solaris installation program that overwrites the disk(s) with the new version of Trusted Solaris. The initial installation option is the only installation option supported in the Trusted Solaris release.

install server A server that provides the Trusted Solaris installation image for other systems on a network to boot and install from (also known as a *media server*). The Trusted Solaris installation image can reside on the install server's CDROM drive or hard disk.

install team A team of at least two people who together oversee the installation of a Trusted Solaris workstation. One team member is responsible for security decisions, and the other for system administration decisions.

interactive installation A type of installation where you have full hands-on interaction with the Trusted Solaris installation program to install the Trusted Solaris software on a system.

IP address Internet protocol address. A unique number that identifies a networked system so it can communicate via Internet protocols. It consists of four numbers separated by periods. Most often, each part of the IP address is a number between 0 and 225; however, the first number must be less than 224 and the last number cannot be 0.

IP addresses are logically divided into two parts: the network (similar to a telephone area code), and the system on the network (similar to a phone number).

ISA Industry Standard Architecture. A type of bus found in x86 systems. ISA bus systems are "dumb" and provide no mechanism the system can use to detect and configure devices automatically. See EISA.

JumpStart directory When using a diskette for custom JumpStart installations, the JumpStart directory is the root directory on the diskette that contains all the essential custom JumpStart files. When using a server for custom JumpStart installations, the JumpStart directory is a directory on the server that contains all the essential custom JumpStart files.

JumpStart installation A type of installation in which the Solaris software is automatically installed on a system by using factory-installed JumpStart software. The Trusted Solaris release does not offer this option; all JumpStart installations in Trusted Solaris are custom JumpStart installations.

kernel architecture See platform group.

label A security identifier assigned to a file or directory based on the level at which the information being stored in that file or directory should be protected. Depending on how the security administrator has configured the user, a user may see the complete CMW label, only the sensitivity label portion, only the information label portion, or no labels at all. See label_encodings file.

label configuration A Trusted Solaris installation choice of: single- or multilabel sensitivity labels; if multilabel, hide or show upgraded file names. Unless circumstances are unusual, label configuration should be identical on all workstations in the Trusted Solaris domain.

labeled workstation A labeled workstation sends labeled network packets, such as RIPSO, CIPSO, TSIX(RE1.1), and MSIX packets. All Trusted Solaris workstations are labeled workstations.

label_encodings file The file where the complete CMW label is defined, as are label view, admin_low and admin_high strings, default label visibility, and all other aspects of labels.

label range A set of sensitivity labels assigned to commands, file systems, and allocatable devices, specified by designating a maximum label and a minimum label. For commands, the minimum and maximum labels limit the sensitivity labels at which the command may be executed. For file systems, the minimum and maximum labels limit the sensitivity labels at which information may be stored on each file system. Trusted Solaris environments have multilabel file systems configured with a label range from the lowest sensitivity label to the highest sensitivity label. Remote hosts that do not recognize labels are assigned a single sensitivity label, along with any other hosts that the security administrator wishes to restrict to a single label; labels limit the sensitivity labels at which devices may be allocated and restrict thesensitivity labels at which information can be stored or processed using the device.

label view flags Label view flags control the translation and display of the internal `ADMIN_LOW` and `ADMIN_HIGH` labels. A value of External specifies that the actual label `ADMIN_LOW` displays as the lowest label name in the user accreditation range specified in the label_encodings file, and that the actual label `ADMIN_HIGH` displays as the highest label name in the user accreditation range. A value of Internal specifies that the `ADMIN_LOW` and `ADMIN_HIGH` labels are translated to the Admin Low Name and Admin High Name strings specified in the label_encodings file.

.link_files An optional setup file in a multilabel environment. The file contains the names of startup files, such as `.cshrc` or `.netscape`, that the user environment or user applications require in order for the environment or application to behave well. The files referenced in `.link_files` are then *linked* to the user's home directory at other labels, when those directories are created. See also .copy_files.

locale A specific language associated with a region or territory.

MAC See mandatory access control.

mandatory access control Access control based on comparing the sensitivity label of a file, directory, or device to the sensitivity label of the process that is trying to access it. The MAC rule — write up, read down (WURD) — applies when a process at one sensitivity label attempts to read or write to a file at another sensitivity label. The MAC rule — write equal, read down — applies when a process at one sensitivity label attempts to write to a directory at another sensitivity label. The MAC rule — read equal, write equal — applies when a process at one sensitivity label attempts to write to a device at another sensitivity label

MCA Micro Channel Architecture. A type of bus on IA systems. The MCA bus provides fast data transfer within the computer, and attached devices can be automatically detected when they have been configured using the reference disk provided by the manufacturer. The MCA bus is not compatible with devices for other buses.

media server See install server.

minimum label The lower bound of a user's sensitivity labels and the lower bound of all users' sensitivity labels. The minimum label set by the security administrator when specifying a user's security attributes is the sensitivity label of the first workspace that comes up after the user's first login. The sensitivity label specified in the minimum label field by the security administrator in the `label_encodings` file sets the lower bound for all users.

MLD See multilevel directory.

mount The process of making a remote or local file system accessible by executing the `mount` command. To mount a file system, you need a mount point on the local system and the name of the file system to be mounted (for example, `/usr`).

mount point A directory on a system where you can mount a file system that exists on the local or a remote system.

multilevel directory A directory in which information at differing sensitivity label is maintained in separate subdirectories called single-level directories (SLDs), while appearing to most interfaces to be a single directory under a single name. In the Trusted Solaris environment, directories that are used by multiple standard applications to store files at varying labels, such as the `/tmp` directory, `/var/spool/mail`, and users' `$HOME` directories, are set up to be MLDs. A user working in an MLD sees only files at the sensitivity label of the user's process.

name server A server that provides a name service to systems on a network.

name service A distributed network database that contains key system information about all the systems on a network, so the systems can communicate with each other. With a name service, the system information can be maintained, managed, and accessed on a network-wide basis. Sun supports the following name services: NIS (formerly YP) and NIS+. Without a name service, each system has to maintain its own copy of the system information (in the local `/etc` files).

network installation A way to install software over the network—from a system with a CDROM drive to a system without a CDROM drive. Network installations require a name server and an install server.

networked systems A group of workstations (called hosts) connected through hardware and software, so they can communicate and share information; referred to as a local area network (LAN). One or more servers are usually needed when systems are networked.

NIS+ Network Information Service, Plus. The name service for a Trusted Solaris network. NIS+ provides automatic information updating and adds security features such as authorization and authentication.

NIS+ master See NIS+ root master.

NIS+ root master The workstation that contains the master tables for a NIS+ network. Also called a root master or a NIS+ master.

non-networked systems Workstations that are not connected to a network or do not rely on other workstations.

open network An *open network* is a network of Trusted Solaris workstations that is connected physically to other networks and that uses Trusted Solaris software to communicate with non-Trusted Solaris workstations. Contrast with closed network.

/opt A file system that contains the mount points for third-party and unbundled software.

OS server A system that provides services to systems on a network.

outside the evaluated configuration When software that has been proved to be able satisfy the criteria for an evaluated configuration, is configured with settings that do not satisfy security criteria, it is described as being *outside the evaluated configuration*.

package A functional grouping of files and directories that form a software application. The Trusted Solaris software is divided into four main software groups, which are each composed of clusters and *packages*.

partition A disk partition is a slice of the disk.

permission bits A type of discretionary access control in which the owner specifies a set of bits to signify who can read, write, or execute a file or directory. Three different sets of permissions are assigned to each file

or directory: one set for the owner; one set for all members of the group specified for the file or directory; and one set for all others.

platform group — The output of the `uname -m` command. A vendor-defined grouping of hardware platforms for the purpose of distributing specific software. Examples of valid platform names are i86pc, sun4c. Often called kernel architecture.

platform name — The output of the `uname -i` command. For example, the platform name for the SPARCstation IPX is `SUNW,Sun_4_50`.

primary administrator — The person entrusted to create new rights profiles for the organization, and to fix machine difficulties that are beyond the power of the security administrator and system administrator combined. This role should be assumed rarely. After initial security configuration, more secure sites can choose not to create this role, and not to assign any role the Primary Administrator profile.

privilege — A right granted to a process executing a command that allows the command or one or more of its options to bypass some aspect of security policy. A privilege is only granted by a site's security administrator after the command itself or the person using it has been judged to be able to use that privilege in a trustworthy manner.

process — An action that executes a command on behalf of the user who invokes the command. A process receives a number of security attributes from the user, including the user ID (UID), the group ID (GID), the supplementary group list, and the user's audit ID (AUID). Security attributes received by a process include any privileges available to the command being executed, the process clearance (which is set to be the same as the session clearance), the sensitivity label of the current workspace, and an information label. If the label configuration option RESET IL ON EXEC is selected, the information label is set to be the lowest viewable label in the system when a new process is started. The information label floats if any information at a higher information label is accessed by the process.

profile — A text file used as a template by the custom JumpStart installation software. It defines how to install the Trusted Solaris software on a system (for example, initial installation option, system type, disk partitioning, software group), and it is named in the rules file.

profile shell — A special shell that recognizes privileges. A profile shell typically limits users to fewer commands, but can allow these commands to

run with privilege. The profile shell is the default shell of a trusted role.

remote host — A workstation that is not part of the Trusted Solaris NIS+ domain. A remote host can be an unlabeled workstation or a labeled workstation.

rights profile — Renamed from execution profiles in the Solaris 8 release.

role — A role is like a user, except that a role cannot log in. Roles are limited to a particular set of commands and CDE actions. See administrative role.

/ (root) — The file system at the top of the hierarchical file tree on a system. The root directory contains the directories and files critical for system operation, such as the kernel, device drivers, and the programs used to start (boot) a system.

root master — See NIS+ root master.

rule — A series of values that assigns one or more system attributes to a profile.

rules file — A text file used to create the rules.ok file. The `rules` file is a look-up table consisting of one or more rules that define matches between system attributes and profiles.

rules.ok file — A generated version of the rules file. It is required by the custom JumpStart installation software to match a system to a profile. You use the `check` script to create the `rules.ok` file.

security administrator — In an organization where sensitive information must be protected, the person or persons who define and enforce the site's security policy and who are cleared to access all information being processed at the site. In the Trusted Solaris software environment, an administrative role that is assigned to one or more individuals who have the proper clearance and whose task is to configure the security attributes of all users and workstations so that the software enforces the site's security policy. In contrast, see system administrator.

security attribute — An attribute used in enforcing the Trusted Solaris security policy. Various sets of security attributes, both in the base Solaris and the Trusted Solaris environments, are assigned to processes, users, files, directories, hosts on the trusted network, allocatable devices, and other entities.

security policy — In the Trusted Solaris environment, the set of DAC, MAC, and information labeling rules that define how information may be accessed. At a customer site, the set of rules that define the sensitivity of the information being processed at that site and the measures that are used to protect the information from unauthorized access.

sensitivity label — A security label assigned to a file or directory or process, which is used to limit access based on the security level of the data contained.

single-level directory — A directory within an MLD containing files at only a single sensitivity label. When a user working at a particular sensitivity label changes into an MLD, the user's working directory actually changes to a single-label directory within the MLD, whose sensitivity label is the same as the sensitivity label at which the user is working.

SLD — See single-level directory.

slice — An area on a disk composed of a single range of contiguous blocks. A slice is a physical subset of a disk (except for slice 2, which by convention represents the entire disk). A disk can be divided into eight slices. Before you can create a file system on a disk, you must format it into slices.

software group — A logical grouping of the Solaris software (clusters and packages). During a Solaris installation, you can install one of the following software groups: core, end user system software, developer system support, or entire distribution. In the Trusted Solaris environment, core and end user software are identical.

Solaris Management Console — A Java-based administrative action for Solaris and Trusted Solaris systems. Located in the Application Manager, it contains toolboxes of administrative programs. Most system, network, and user administration is done using the Console toolboxes.

standalone system — A system that has its own / (root) file system, swap space, and /usr file system, which reside on its local disk(s); it does not require boot or software services from an OS server. A standalone system can be connected to a network, but it does not have to be.

subnet — A working scheme that divides a single logical network into smaller physical networks to simplify routing.

subnet mask A bit mask, which is 32 bits long, used to determine important network or system information from an IP address.

swap space Disk space used for virtual memory storage when the system does not have enough system memory to handle current processes. Also known as the `/swap` or `swap` file system.

system Generic name for a workstation. After installation, a system is often called a host.

system accreditation range The set of all valid (well-formed) labels created according to the rules defined by each site's security administrator in the label_encodings file, plus the two administrative labels that are used in every Trusted Solaris environment, `ADMIN_LOW` and `ADMIN_HIGH`.

system administrator In the Trusted Solaris environment, the trusted role assigned to the user or users responsible for performing standard system management tasks such as setting up the non-security-relevant portions of user accounts. In contrast, see security administrator.

system type One of several different ways a workstation can be set up to run the Trusted Solaris software. Valid system types are: standalone system and OS server.

time zone Any of the 24 longitudinal divisions of the earth's surface for which a standard time is kept.

tnrhdb database The Trusted Network Remote Host DataBase, accessible either as a file in `/etc/security/tsol/tnrhdb` or as a NIS+ table.

tnrhtp database The Trusted Network Remote Host TemPlate, accessible either as a file in `/etc/security/tsol/tnrhtp` or as a NIS+ table.

toolbox A collection of programs in the Solaris Management Console. In the Trusted Solaris environment, administrators are presented with a selection of toolboxes, one for every name service (Files, NIS+, and NIS). Each toolbox has programs usable in the scope of the toolbox. For example, the Interface Manager, which handles the machine's `tnidb` database, exists only in the Files toolbox, since its scope is always local. The User Accounts program exists in all toolboxes, since an administrator can choose to create a local user (Files), as well as one that can log in to any machine in the name service (NIS+ or NIS toolboxes).

Trusted Network databases — tnrhtp, the Trusted Network Remote Host TemPlate and tnrhdb, the Trusted Network Remote Host DataBase together define the remote hosts that a Trusted Solaris domain can communicate with.

trusted role — See administrative role.

Trusted Solaris installation program — (1) A menu-driven, interactive program that enables you to set up a system and install the Trusted Solaris software on it. (2) Any part of the software that is used to install the Trusted Solaris software on a system.

trusted stripe — A region that cannot be spoofed along the bottom of the screen, which by default provides the following as visual feedback about the state of the window system: a trusted path indicator and window sensitivity label. When sensitivity labels are configured to not be viewable for a user, the trusted stripe is reduced to an icon that displays only the trusted path indicator.

prof_attr and exec_attr databases — The profiles attributes database, accessible either as files in `/etc/security/prof_attr` and `/etc/security/exec_attr`, or as NIS+ tables. After configuration, it contains execution profiles provided by the Trusted Solaris software.

user_attr database — The User Attributes database, accessible either as a file in `/etc/security/user_attr` or as a NIS+ table. After configuration, it contains roles provided by the Trusted Solaris software.

upgrade option — An option presented during the Solaris installation program. The upgrade procedure merges the new version of Solaris with existing files on your disk(s), and it saves as many local modifications as possible since the last time Solaris was installed. The upgrade option is not available with the Trusted Solaris 7 release.

unlabeled workstation — A workstation that sends unlabeled network packets, such as one running the Solaris 8 operating environment.

user accreditation range — The set of all possible labels at which any normal user may work on the system, as defined by each site's security administrator. The rules for well-formed labels that define the system accreditation range are additionally restricted by the values specified in the ACCREDITATION RANGE section of the site's `label_encodings`(4) file: the upper bound, the lower bound, the combination constraints and other restrictions.

user clearance — The clearance assigned by the security administrator that sets the upper bound of the set of labels at which one particular user may work at any time. The user may decide to accept or further restrict that clearance during any particular login session, when setting the session clearance after log in.

/usr — A file system on a standalone system or server that contains many of the standard UNIX programs. Sharing a large file system with a server rather than maintaining a local copy minimizes the overall disk space required to install and run the Trusted Solaris software on a system.

/var — A file system or directory (on standalone systems) containing system files that are likely to change or grow over the life of the system. These include system logs, `vi` files, mail files, and uucp files.

Volume Management — A program that provides a mechanism to administer and obtain access to the data on CDROMs and diskettes.

workstation accreditation range — The set of all valid (well-formed) labels created according to the rules defined by each site's security administrator in the label_encodings file, plus the two administrative labels that are used in every Trusted Solaris environment, `ADMIN_LOW` and `ADMIN_HIGH`. Also called the system accreditation range.

Index

D

E

F

H

I

J

L

M

N

O

P

R

S

T

U

V

W