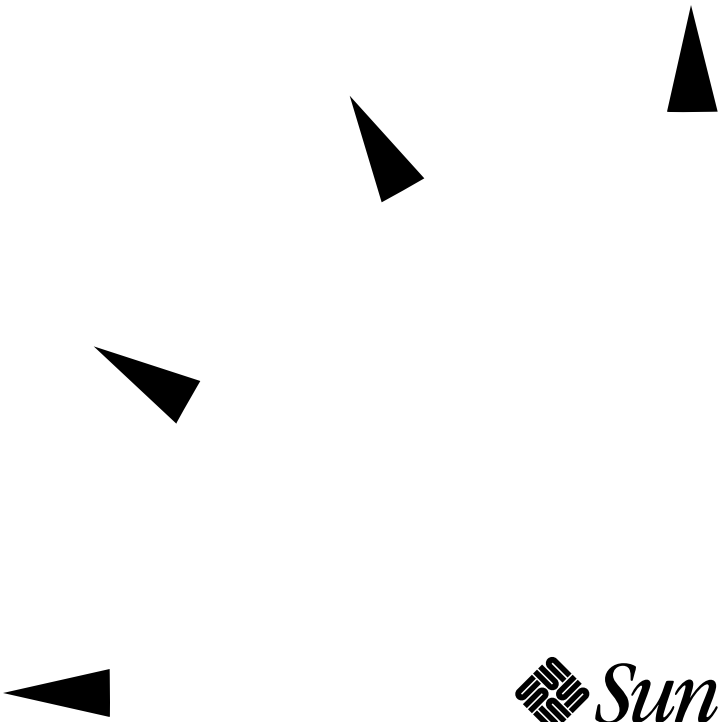
Trusted Solaris Installation and Configuration

Trusted Solaris 2.5



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

Part No: 805-8009-10
Revision A, July 1997

Sun microsystems

THE NETWORK IS THE COMPUTER™

Please
Recycle

Adobe PostScript

Contents

Figures

Tables

About This Book

Who is the Audience?

This book is for knowledgeable system administrators and security officers 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.

Read Your Site Security Policy

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, read Chapter 1, “The Big Picture” for an overview of what is required to install and configure a secure site.

Read This Book Strategically

If you are installing and configuring a network of workstations, you can choose from several installation methods after installing the first workstation. The installation methods you choose determine what parts of the book you should read. Trade-offs between the methods are discussed in “Finishing Up the Planning” on page 52.

If you are installing and configuring all workstations interactively, you should read the following chapters:

How This Book Is Organized

Note – This book does not include instructions for setting up system hardware or other peripherals. Setting up hardware and peripherals is described in your hardware guides.

Planning a Secure Installation

Chapter 1, “The Big Picture”	*page 1*
Chapter 2, “Planning”	*page 15*

Installing a Workstation

Chapter 3, “Installing a Workstation”	*page 55*

Configuring the NIS+ Root Master

Chapter 5, “Configuring the NIS+ Root Master”	*page 69*

Configuring a Non-networked Workstation

Chapter 4, “Configuring a Workstation without the NIS+ Name Service”	*page 61*

Configuring NIS+ Clients

Chapter 6, “Configuring a NIS+ Client: Interactive”	*page 105*

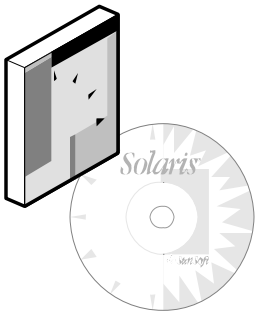
Installing NIS+ Clients Over the Network

Chapter 7, “Preparing to Install Trusted Solaris Over a Network”	*page 115*
Chapter 6, “Configuring a NIS+ Client: Interactive”	*page 105*

Installing and Configuring NIS+ Clients Using Custom JumpStart

Configuring and Booting Diskless Clients

Related Information



All sites should have the following books or information available when installing Trusted Solaris software:

From Sun Microsystems

- *Trusted Solaris 2.5 Release Notes*
  Describes any late-breaking news about installing Trusted Solaris software including known problems.
- *Solstice AdminSuite 2.1 User's Guide, 802-3339*
  Describes the basic applications that Trusted Solaris 2.5 uses to administer the network. Trusted Solaris 2.5 has added security features; the additions are described in *Trusted Solaris Administrator's Procedures*.
- *Solaris 1.x to 2.x Transition Guide, 802-6638*
  Describes transition issues including backing up 4.1.x files before installing Trusted Solaris software, and restoring files after Trusted Solaris software is installed.
- *NIS+ and DNS Setup and Configuration Guide, 802-1964*
  Describes how to set up a NIS+ domain at your site. Required for a network installation.
- *Trusted Solaris Label Administration*
  Describes labels and includes a copy of *Compartmented Mode Workstation Labeling: Encodings Format* issued by the U.S. government.
- *Trusted Solaris Audit Administration*
  Describes auditing one or more Trusted Solaris workstations.
- *Trusted Solaris Administrator's Procedures*
  Describes administration tasks in detail.
- *NFS Administration Guide, 802-1963*
  Describes how to administer a networked file system. Recommended for a network installation.

From Elsewhere

- *Your site security policy*
  Describes the security policy and security procedures at your site.
- *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

What Typographic Changes and Symbols Mean

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

Table P-1 Typographic Conventions

Typeface or Symbol	**Meaning**	**Example**
`Filename, command,` or `code example`	The names of commands, files, and directories; onscreen computer output	Edit your `.login` file. Use `ls -a` to list all files. machine_name% You have mail.
`User Type`	What you type, contrasted with on-screen computer output	`machine_name% su` `Password:`
Argument	Used in command line examples: replace with an appropriate name or value	To delete a file, type `rm` *filename.*
	Book titles, new words or terms, or words to be emphasized	Read Chapter 6 in *User’s Guide.* These are called *audit tokens.* You *must* be root to do this.

Which Trusted Solaris Prompts Indicate Particular Environments

Shell	Prompt
C shell prompt	*machine_name*%
Bourne shell and Korn shell prompt	$
Profile Shell prompt	$
root prompt	#
PROM mode prompt	>

The Big Picture 1

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. Experienced administrators familiar with Trusted Solaris 1.2 or Solaris 2.5 may find Appendix C, "Checklists for Configuring and Installing Trusted Solaris" to be a useful summary of steps.

Differences from Solaris 2.5.1 Installation and Configuration

If you are familiar with installing Solaris software, note that there are packaging and installation differences when installing Trusted Solaris.

1

Software Bundled with Trusted Solaris 2.5

Products that are unbundled in the Solaris environment are bundled into Trusted Solaris. Auditing, which is disabled by default in Solaris, is enabled by default.

Common Desktop Environment (CDE)

Trusted Solaris desktop environment. Trusted Solaris software no longer runs on the OpenWindows™ desktop. End users and administrators access Trusted Solaris software and third-party software from CDE.

Solstice™ AdminSuite™

Trusted Solaris administrative tools for central administration of a network. The Trusted Solaris installation program installs Solstice AdminSuite automatically and makes the individual tools selectively available to users who assume administrative roles. Adminstration of users, roles, execution profiles, and network host types is enabled by Solstice tools.

Installation Options for Trusted Solaris 2.5 Environment

Fewer options are available when installing Trusted Solaris software than are available when installing Solaris 2.5.1 software. Specifically,

- No factory JumpStart™. Custom JumpStart support with Trusted Solaris configuration options is provided.
- No remote filesystem mounting during installation. File systems can be mounted after installation.
- No upgrade option for Trusted Solaris 2.5. Upgrades from Trusted Solaris 2.5 will be possible in later releases.
- Volume Manager is not supported.
- No support for Solstice™ AutoClient™ or dataless clients
- NIS+ is the only supported Name Service..
- The software clusters Core and Entire + OEM are not supported. The three supported software clusters are End-user, Developer, and Entire.

The Trusted Solaris installation program adds a prompt for label configuration information as shown in Figure 1-1 on page 3.

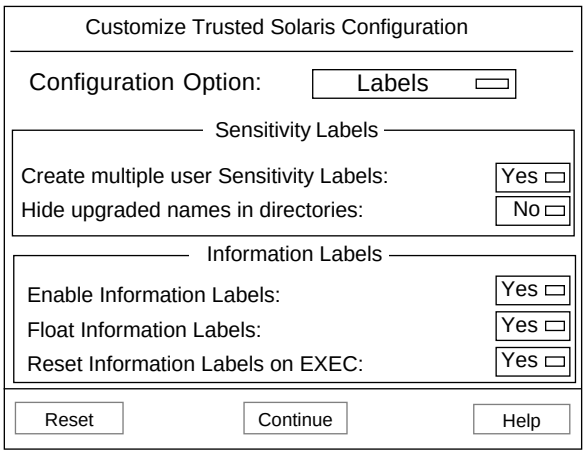


Figure 1-1 Trusted Solaris Label Configuration Options

Installation Results and Security

After installing Trusted Solaris software, the following security and system modules are in effect on your system. Auditing, CDE, and Solstice AdminSuite have been modified for Trusted Solaris; the others are unique to the Trusted Solaris environment.

- Auditing
  Auditing is one factor in maintaining a secure system. Trusted Solaris enables auditing by default. An administrator must perform an extra step to turn auditing off. The security administrator is responsible for establishing what is audited and its secure setup. The Trusted Solaris software ensures security during audit record generation, collection, and archiving.

- Labeling, based on label encodings file and label configuration
  The Trusted Solaris installation program establishes a default labeling scheme. The security administrator is responsible for installing and configuring labels appropriate to the site during configuration.
  Trusted Solaris software enforces the labeling of processes and files. It also enforces clearances and initial labels, which set the bounds on the labels that a user or workstation can access.

1

- Common Desktop Environment (CDE)
  A trusted windowing environment
- Solstice AdminSuite tools
  Tools to administer user, execution profile, and other system databases.
- Administrative CDE actions
  Actions that open or check local administrative files in a trusted editor.
- Three administrative roles - secadmin, admin, and root
  The three roles: secadmin (security administrator), admin (system administrator), and root (for adding software packages) divide the work of superuser. The security administrator is responsible for deciding if overriding this default is permissible.
- One non-administrative role - oper
  The oper role is provided for system backup, archiving, and restoration.
- Execution profiles
  Execution profiles are collections of commands, actions, and authorizations that define a role, or part of a role.

Two-Role Configuration

Trusted Solaris software installation and configuration is designed for two administrators acting in two distinct roles, `secadmin` and `admin`. Each role has configuration responsibilities that are enforced by the software once the roles are assigned to users. The install team assigns the roles to users during configuration. Figure 1-2 on page 5 gives an overview of the division of administrative responsibilities between the two roles.

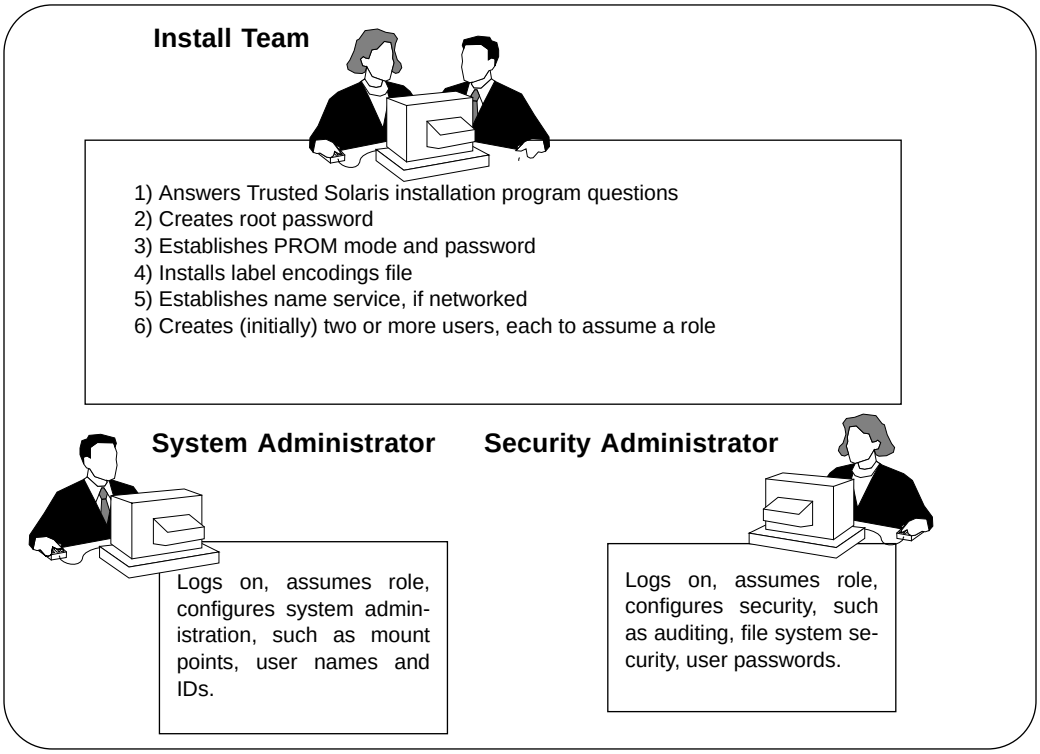


Figure 1-2 Two Roles Administering a Workstation

1

Overview of Installation and Configuration

Installing Trusted Solaris can be done interactively, over the network, or with scripts customized for particular workstations. Figure 1-3 shows the installation options.

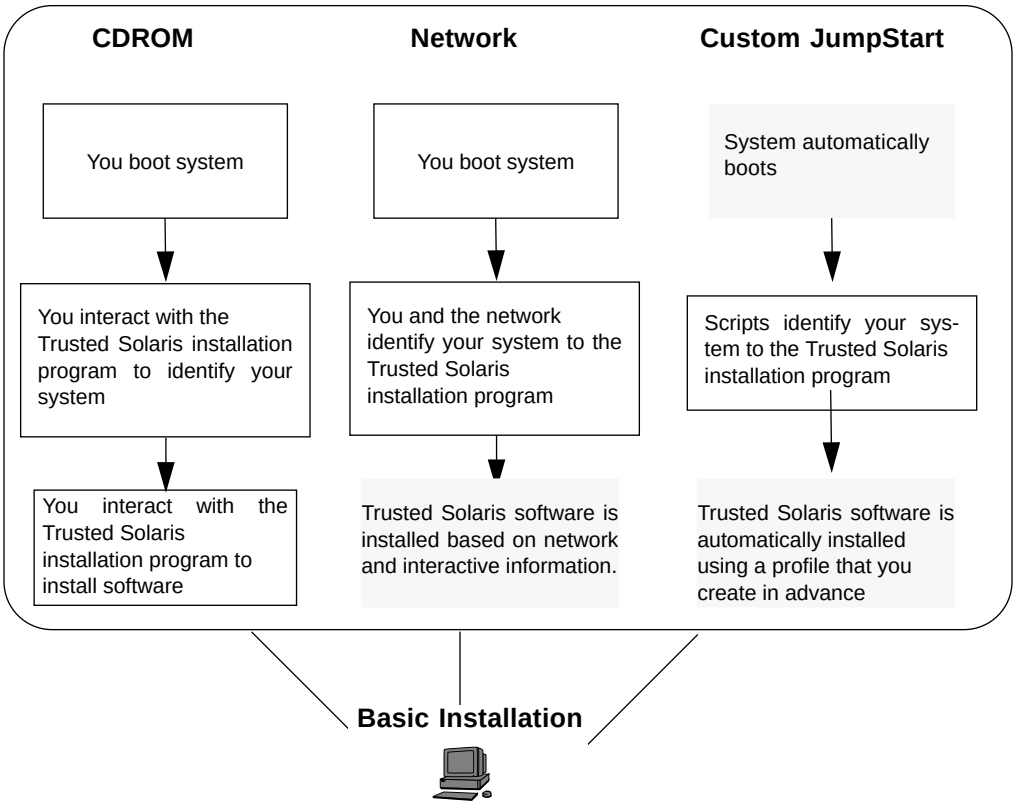


Figure 1-3 Installing a Workstation

The Trusted Solaris installation program asks basic workstation information questions, including the Trusted Solaris label configuration options, the name of the software cluster, and how to partition the disks.

After installation, you configure the workstation to operate with or without a name service. Figure 1-4 shows the configuration options.

- *Without a name service*: Workstation uses only its local files (in the `/etc` directory) for administration.
- *NIS+ name service*: Workstation consults tables on a Trusted Solaris NIS+ master for administration, in addition to consulting local files not handled by the NIS+ name service.

Note – All Trusted Solaris NIS+ clients must be administered by a Trusted Solaris NIS+ master.

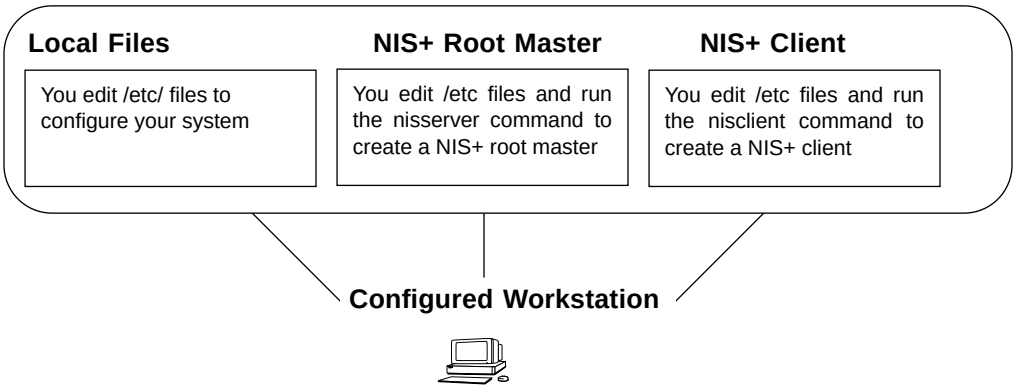


Figure 1-4 Configuring a Workstation

After configuring, you can further set up workstations to be servers that handle network booting and installation. Figure 1-5 shows some of the servers.

- *Boot server*: Contains boot information required by diskless clients and by workstations being installed over a network.
- *Install server*: Handles network installation.
- *Trusted Solaris configuration server*: HoldsTrusted Solaris configuration values.
- *OS server*: Provides disk space, file systems, and services to diskless clients.
- *JumpStart server*: Contains custom JumpStart installation scripts.

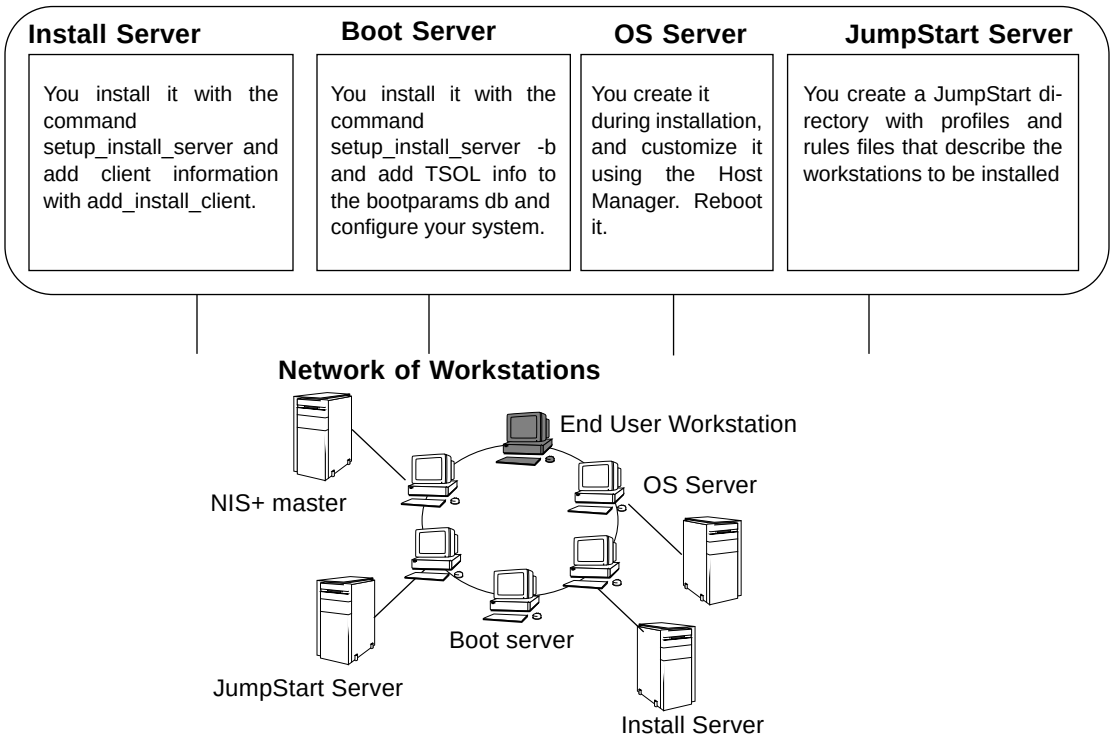


Figure 1-5 Establishing Network Servers

Task Map: Interactive CDROM Installations

Activity	Description	Read	
Gather information	**Plan**	Chapter 2, “Planning”	page 15
	Use worksheets to gather answers to questions asked by the Trusted Solaris installation program.	Appendix B, “Worksheets for Configuring and Installing Trusted Solaris”	page 221
Back up your files	**Save important data**	***Your current workstation backup procedures***	
Install Trusted Solaris software	**Install from local CD-ROM** Boot and install Trusted Solaris software.	Chapter 3, “Installing a Workstation”	page 55
	Do one of:		
Configure Trusted Solaris software	**Configure NIS+ master** Configure and create a NIS+ master.	Chapter 5, “Configuring the NIS+ Root Master”	page 69
	Configure non-networked workstation Configure Trusted Solaris local administrative files.	Chapter 4, “Configuring a Workstation without the NIS+ Name Service”	page 61
	Configure NIS+ client Configure and create a NIS+ client.	Chapter 6, “Configuring a NIS+ Client: Interactive”	page 105

Figure 1-6 Task Map for CDROM Installations

1

Task Map: Network Installations

Activity	Description	Read	
Gather information	**Plan**	Chapter 2, “Planning”	page 15
	Use worksheets to plan server configurations.	Appendix B, “Worksheets for Configuring and Installing Trusted Solaris”	page 221
Use a NIS+ client …	**Start with a configured NIS+ client (See “Task Map: Interactive CDROM Installations”)**	Chapter 6, “Configuring a NIS+ Client: Interactive”	page 105
… as network server	**Set up install server and boot server on the client** Set up servers for network installations.	Chapter 7, “Preparing to Install Trusted Solaris Over a Network”	page 115
Install Trusted Solaris software over the net	**From another system on the network** Type `boot net`	Chapter 3, “Installing a Workstation”	page 55
	Do one of:		
Configure Trusted Solaris software	**Configure NIS+ client** Configure and create a NIS+ client.	Chapter 6, “Configuring a NIS+ Client: Interactive”	page 105
	Configure non-networked workstation Configure Trusted Solaris local administrative files.	Chapter 4, “Configuring a Workstation without the NIS+ Name Service”	page 61

Figure 1-7 Task Map for Network Installations

Task Map: Network Custom JumpStart Installations

Activity	Description	Read	
Gather information	**Plan**	Chapter 2, “Planning”	page 15
	Use worksheets to plan workstation configurations.	Appendix B, “Worksheets for Configuring and Installing Trusted Solaris”	page 221
Back up files	**Save important data**	***Your current workstation backup procedures***	
Set up network servers	**Set up already configured NIS+ clients as network installation servers**	Chapter 7, “Preparing to Install Trusted Solaris Over a Network”	page 115
Set up custom JumpStart	**Perform the following tasks:** • Create a JumpStart directory • Enable clients to access the JumpStart directory • Create profiles • Create a `rules` file • Use check to validate the `rules` file • Add JumpStart information to network servers	Chapter 8, “Preparing Custom JumpStart Installations”	page 139
Install Trusted Solaris software	**From another system on the network** Type `boot net - install`	Chapter 10, “Booting and Installing Trusted Solaris: Custom JumpStart”	page 197
Configure Trusted Solaris Software	**Configure each custom JumpStart client** Finish configuring a NIS+ client.	Chapter 6, “Configuring a NIS+ Client: Interactive”	page 105

Figure 1-8 Task Map for Network Custom JumpStart Installations

1

Task Map: CDROM + Diskette Custom JumpStart Installations

Activity	Description	Read	
Gather information	**Plan**	Chapter 2, “Planning”	page 15
	Use worksheets to gather answers to questions asked by the Trusted Solaris installation program.	Appendix B, “Worksheets for Configuring and Installing Trusted Solaris”	page 221
Back up	**Save important data**	***Your current workstation backup procedures***	
Set up custom JumpStart	**Perform the following tasks:** • Create a JumpStart directory on a diskette • Create profiles • Create a `rules` file • Use check to validate the `rules` file • Add JumpStart information to diskette	Chapter 8, “Preparing Custom JumpStart Installations”	page 139
Install Trusted Solaris software	**Install from local CDROM and JumpStart diskette** Type `boot cdrom - install`	Chapter 10, “Booting and Installing Trusted Solaris: Custom JumpStart”	page 197
Cofigure Trusted Solaris software	**Configure non-networked workstation** Configure Trusted Solaris local administrative files.	Chapter 4, “Configuring a Workstation without the NIS+ Name Service”	page 61

Figure 1-9 Task Map for CDROM Custom JumpStart Installations

Task Map: Diskless Booting

Activity	Description	Read	
Gather information	**Plan**	Chapter 2, “Planning”	page 15
	Use worksheets to plan server configurations.	Appendix B, “Worksheets for Configuring and Installing Trusted Solaris”	page 221
Set up network servers	**Configure NIS+ diskfull clients**	Chapter 6, “Configuring a NIS+ Client: Interactive”	page 105
	Set up NIS+ clients as network and install servers	Chapter 7, “Preparing to Install Trusted Solaris Over a Network”	page 115
	Set up NIS+ diskfull clients as OS servers Set up OS servers for network booting.	Chapter 11, “Configuring Diskless Clients”	page 201
Boot Trusted Solaris software over the net	**From diskless client on the network** Type `boot net`	Chapter 11, “Configuring Diskless Clients”	page 201

Figure 1-10 Task Map for Diskless Clients

1

Planning 2

This chapter prepares you to install and configure Trusted Solaris software on multiple workstations. It includes pointers to references and worksheets to guide you in making system and security decisions. If you are installing a workstation that will not connect to other workstations, you can skip the section “Planning the Network”.

Overview of Planning

Planning users, roles, execution profiles (to limit access to software), printing, and other configuration tasks are covered in *Trusted Solaris Administrator’s Procedures*.

2

Ensuring a Smooth Installation

Successfully installing and configuring the Trusted Solaris environment requires preparation:

- Reading and understanding security
- Reading and understanding Trusted Solaris security features
- Organizing the planning process

Reading and Understanding Security

Before installing the first workstation, the security administrator should be familiar with:

- Your site's security policy and procedure manual – Explains the security policy and procedures at your site.
- Appendix A, "Site Security Policy" – Explains where Trusted Solaris software fits in with security policy and procedures, and provides a more theoretical perspective on security. Includes a bibliography.

Reading and Understanding Trusted Solaris Security Features

The administrator's document set explains Trusted Solaris security features:

- *Trusted Solaris Administration Overview* – Introduces Trusted Solaris concepts, the user interface, and administration tasks.
- *Trusted Solaris Label Administration* – Introduces labels, and gives extensive examples of how to set them up, check them, and centrally administer them.
- *Trusted Solaris Audit Administration* – Introduces auditing, and describes the procedures for enabling auditing on one workstation or on a network of workstations, preselecting what to audit, collecting the auditing records, filtering the records, and analyzing them from a central location.

Organizing the Planning Process

The system administrator and the security administrator

- divide the planning (and installation and configuration) tasks, and
- gather the information required for installation and configuration of multiple workstations.

Dividing the Administrative Tasks

The process of installing and configuring the system is a security issue. Before the software enforces task division between two roles, security administrator and system administrator, it is the task of the site security administrator to supervise and enforce the division if site security policy requires it.

The security administrator is responsible for overseeing correct implementation of security policy in all aspects of Trusted Solaris installation and configuration, including:

- Planning Labels and Clearances on page 18
- Planning Auditing on page 23
- Planning Workstation Security on page 44
- Planning Network Security on page 27
- Planning the First Two Users on page 48
  - Determining if two-person installation is a site security requirement
  - Directing the system administrator to create one user or two users
  - Assigning the admin role to the correct user
- Planning role assignments for users (see *Trusted Solaris Administrator's Procedures*)
- Planning software access (see *Trusted Solaris Administrator's Procedures*)
- Planning the users (see *Trusted Solaris Administrator's Procedures*)

The system administrator oversees:

- Under auditing:
  - Plan a Network of Audit File Systems on page 26
- Planning Workstation Hardware on page 38
- Planning Workstation Use on page 41
- Planning Network Administration on page 32
- Finishing Up the Planning on page 52
- Following the security administrator's direction to create one or two users to assume the roles secadmin and admin
- Assigning the role secadmin to the correct user ID

After the install team assigns the Trusted Solaris roles `secadmin` and `admin` to the first two users created on the first workstation, Trusted Solaris software enforces the two-role task division. Before the software enforces task division, the security administrator is responsible for ensuring the security of the installation.

Gathering Information

The planning sections encourage the system administrator and security administrator to fill out worksheets with the information they gather. Blank copies of the worksheets are in Appendix B, "Worksheets for Configuring and Installing Trusted Solaris". Sample filled-out worksheets are in Appendix F, "Example Worksheets". There are summary sheets in Appendix C, "Checklists for Configuring and Installing Trusted Solaris" to track overall progress.

Planning Labels and Clearances

Labels identify the sensitivity of work being done at your site. *Clearances* identify the upper bound of labels that a particular user, role, or workstation can access. A file named `label_encodings` contains the labels and clearances. A placeholder file that you replace is stored in the `/etc/security/tsol` directory.

The security administrator is responsible for labels and clearances.

The following planning section offers a high-level view. A full description of planning and administering labels is in *Trusted Solaris Label Administration*.

Overview of Planning Labels and Clearances

▼ Plan Label Configuration

- **Decide the label configuration for all workstations.**
  Use your site security policy, Table 2-1 on page 19, and Table 2-2 on page 20 to help you determine your site's label configuration.

The Trusted Solaris installation program presents you with label configuration defaults, as shown in Figure 2-1.

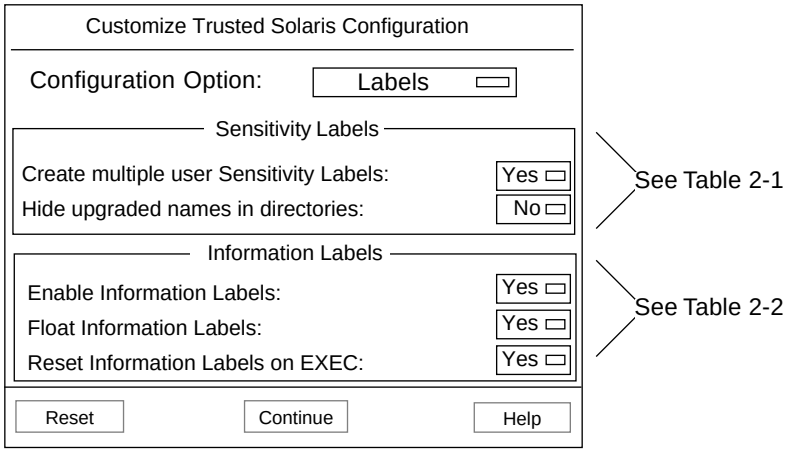


Figure 2-1 Label Configuration Defaults

Note – All Trusted Solaris workstations in your NIS+ domain should use the same label configuration.

Table 2-1 lists factors affecting your sensitivity label configuration choices.

Table 2-1 Choosing a Sensitivity Label Configuration

Choose	Because	Comments
Multiple... No	Your site runs at a single label.	This is sometimes known as a System High configuration.
	Your site runs with no sensitivity labels.	In order to run as a no-label site, you will prevent sensitivity labels from being visible to your users when setting up the user accounts.
	Your site runs with information labels only.	You will prevent sensitivity labels from being visible to your users when setting up the user accounts.

Table 2-1 Choosing a Sensitivity Label Configuration

Multiple … Yes	Your site runs with more than one user label.	Choose whether to hide upgraded names.
Hide Upgraded Names - Yes	Prevent users from viewing files that have a higher label than the label of the directory.	Advantage: provides tighter security Disadvantage: can be confusing to users who expect to see the file

Table 2-2 lists factors affecting your information label configuration choices.

Table 2-2 Choosing an Information Label Configuration

Choose	**Because**	**Comments**
Enable ILs - Yes	Your site does not use sensitivity labels, it uses information labels only. Your site uses sensitivity labels and information labels.	You have further IL configuration choices.
Enable ILs - No	Your site does not use information labels.	End of your choices.
Float ILs - Yes	Your site policy requires that whenever an object is accessed, the IL of the calling process must be reflected in the object's label.	Advantage: Files and objects automatically get the correct IL. Disadvantage: ILs accumulate on an object when the object is simply listed by a process that doesn't open it for read or write
Float ILs - No	Your site policy does not require IL floating.	Advantage: Less overhead Disadvantage: An object's IL must be changed manually.
Reset IL upon EXEC - Yes	Your site policy requires that a new process start with a neutral IL.	Advantage: A process does not accumulate ILs, therefore is less likely to inform snoopers of the history of its use. Disadvantage: More overhead
Reset IL upon EXEC - No	Your site policy does not require resetting the IL upon exec.	Advantage: Less overhead. Disadvantage:

Results of Your Choices

Trusted Solaris places your answers in the `/etc/system` file as a set of variable values. For example, if you enable information labels (ILs), Trusted Solaris places the following entry in `/etc/system`:

```
set tsolsys:tsol_enable_ils=1
```

Entries in the `/etc/system` file configure the labels when a workstation is booted.

▼ Plan Label Visibility

♦ **See** *SL visibility* **and** *IL visibility* **in "User Account Characteristics" on page 96 to set label visibility.**
Label visibility is set per user, not per workstation. If ILs are not enabled, they will not be visible.

▼ Prepare Labels and Clearances

1. **Determine the source of the label encodings file:**
   - Government Furnished Information (GFI)
   - Site-created
   - A modified version of the single-label `label_encodings` file provided by the Trusted Solaris installation program.
2. **Create or edit the label encodings file for your site.**
   Table 2-3 on page 22 lists the editing required on your choice of `label_encodings` file.

3. **Establish a procedure that ensures that one label encodings file is used on all workstations on the network.**
   See "Finishing Up the Planning" on page 52 for installation methods that automate the installation of your site's label_encodings file into `/etc/security/tsol/label_encodings`.

Table 2-3 Editing Your `label_encodings` Source File

Choose	Because	Comments
GFI	Your site has one and uses it.	You edit it to contain SUN-specific data to enable it to run on Trusted Solaris workstations. You install it over the placeholder supplied by the Trusted Solaris installation program.
Site-created	Your site uses multiple labels and does not have a GFI version.	
Trusted Solaris single-label file	Your site uses a single label and does not have a GFI or site-created version.	Requires minimal editing of the placeholder Trusted Solaris single-label `label_encodings` file.

A `label_encodings` file customized for your site must be installed on the NIS+ root master before you install and configure other workstations. The Trusted Solaris installation program provides a placeholder `label_encodings` file in the `/etc/security/tsol` directory. You must substitute your site's label encodings file on the NIS+ root master before you install the second workstation.

▼ Read Further

♦ **Use the references in Table 2-4 to plan and administer labels and clearances.**

Table 2-4 References for Planning Labels and Clearances

Use the Reference ...	To Help You ...
Trusted Solaris Label Administration	Administer labels in a Trusted Solaris environment Find examples and explanation of labels and clearances Read sample label_encodings files
Compartmented Mode Workstation Labeling: Encodings Format	Read the source U.S. Government specifications for a label_encodings file

Table 2-4 References for Planning Labels and Clearances

Use the Reference ...	To Help You ...
Your site security policy document.	Determine the appropriate label configuration at your site Determine what labels and clearances to use Determine the source of your `label_encodings` file

▼ Use Worksheets

1. **Enter your label configuration choices in the "NIS+ Root Master Installation Worksheet" on page 223.**
2. **Use the information and worksheets in** *Trusted Solaris Label Administration* **to plan your label encodings file.**

Planning Auditing

Auditing tracks user and kernel activity on a workstation. In a Trusted Solaris network, auditing tracks user and kernel activity on multiple workstations and creates one audit trail for the entire network. By default, auditing is enabled.

The system administrator plans the network of auditing servers and workstations; the security administrator plans the security aspects of auditing.

Note – If your site security policy does not require auditing, and you are not going to audit, skip to Planning the Workstations on page 37.

The following planning section offers a high-level view. A full description of planning and administering auditing is in the *Trusted Solaris Audit Administration* manual.

Overview of Planning Auditing - Security Administrator

Overview of Planning Auditing - System Administrator

▼ Decide Whether to Audit

- **If you decide to audit, continue. Otherwise, go to Planning the Workstations on page 37.**
  Deciding to audit affects the first workstation and every workstation you install, since auditing requires a dedicated and large enough (probably > 200MB) partition per workstation.

▼ Decide What to Audit

1. **Decide what classes of events to audit for success, what classes to audit for failure, and what classes to audit for failure and success.**
   You will enter the classes in the `/etc/security/audit_control` file.
2. **Decide what classes to audit for particular users, in addition or as exceptions to the classes being audited on all workstations.**
   You will enter the classes in the `/etc/security/audit_user` file.

The security administrator decides what events (which Trusted Solaris software has organized into audit classes) to audit. All workstations are audited identically, so once you plan for one workstation, you have planned for them all. See the Appendixes in *Trusted Solaris Audit Administration* for the list of audit classes, and what events belong to what audit classes (called event-class mapping).

▼ Plan a Secure Auditing Environment

1. **Decide who will analyze the audit records.**
   You assign that user an administrative role that includes the execution profile Audit Review. By default, the admin administrative role has the Audit Review execution profile.

2. **Plan to create two audit file systems, a primary and a secondary (backup).**
   You allocate the disk space during installation.

3. **Decide who will back up and archive the audit records.**
   You assign that user the role `oper`.

4. **Decide what security attribute values to use to protect the audit file systems.**
   See Table 2-20 on page 47 for the default Trusted Solaris security attributes on file systems. Once the system administrator creates the file systems, you edit the `/etc/vfstab` file and `/etc/security/tsol/vfstab_adjunct` files to protect them. A `vfstab_adjunct` entry (for an unlabeled file system) is shown in Figure 5-2 on page 101.

5. **Decide what users and roles will be notified by email when the audit subsystem needs attention.**
   You create an `audit_warn` alias into the Aliases database using Solstice_Apps, DB Manager. Its members are the users and roles who should receive email when the audit subsystem needs attention.

▼ Use Worksheets

1. **Assign the role `oper` (for archiving audit records), the role `secadmin` for audit setup (the `Audit Control` profile) and the role `admin` for audit analysis (the `Audit Review` profile) in the appropriate users' User Worksheets.**

2. **In each workstation's worksheet, enter the security attributes you want to use to protect its local audit file system(s).**

Worksheets for planning auditing are in *Trusted Solaris Audit Administration*.

▼ Plan a Network of Audit File Systems

Note – Skip this part if you are installing Trusted Solaris on a workstation without an Ethernet connector or similar network adapter.

The system administrator sets up a network of audit file systems and one central audit administration server.

1. **During installation, allocate disk space on every workstation for a local audit partition (probably > 200MB)**
   The naming convention for a local audit partition is `/etc/security/audit/`*`workstation_name`*
2. **Create audit servers whose file systems are dedicated audit partitions.**
   The naming convention for a several audit partitions on one workstation is `/etc/security/audit/`*`workstation_name`*
   `/etc/security/audit/`*`workstation_name`*`.1`
   `/etc/security/audit/`*`workstation_name`*`.2`, and so on
3. **Assign each workstation a primary audit file system on an audit server.**
4. **Assign each workstation a secondary audit file system on an audit server.**
   You list the primary, secondary, and local audit file systems for a workstation in its `/etc/security/audit_control` file.
5. **Create a central audit administration server, where every audit file system is mounted.**
   Your audit reviewer interprets the audit records and creates reports from the audit administration server. Audit record backup is done from the central audit administration server.

▼ Read Further

- **Use the references in Table 2-5 to plan, configure, and administer auditing for multiple workstations.**

Table 2-5 References for Planning Auditing

Use the Reference	To Help You ...
Trusted Solaris Audit Administration	Configure and administer auditing in a Trusted Solaris environment
Your site security policy document.	Determine your auditing requirements

▼ Use Worksheets

1. **For each workstation, enter the name and size of the workstation's local audit disk partition in its Disk Partitioning Worksheets. Blank worksheets are available for copying from Disk Partition Tables on page 239.**
2. **Use the Auditing Network worksheets in** *Trusted Solaris Audit Administration* **to lay out auditing for your Trusted Solaris network.**

Planning the Network

Note – Skip this section if you are installing Trusted Solaris on a workstation without an Ethernet connector or similar network adapter.

Network planning requires coordination between the security administrator and the system administrator.

Planning Network Security

The security administrator plans network security. The system administrator determines non-Trusted Solaris domain and host IP addresses if the network is open.

Overview of Planning Network Security - Security Administrator

▼ Decide if Network is Open or Closed

- **Use your site security requirements to help you decide if your Trusted Solaris workstations can communicate with non-Trusted Solaris workstations.**

Note – If you choose to have a closed network, you do not need to plan any further. Go to "Planning Network Administration" on page 32.

▼ Plan an Open Network

1. **Get the names and IP addresses of non-Trusted Solaris hosts and subnets from the system administrator.**
2. **Associate non-Trusted Solaris hosts or subnets with templates defined in the `tnrhtp` file.**
   See the `tnrhtp(4TSOL)` man page for a list of defined host types and the available attributes. You can modify the `tnrhtp` for the network or for the local workstation; see *Trusted Solaris Administrator's Procedures* for more information.
3. **Enter in the "Remote Hosts (tnrhdb) Worksheet for NIS+ Root Master" on page 233 the hosts or subnets that *all* Trusted Solaris workstations can communicate with.**
   You enter these subnets and hosts in the NIS+ `tnrhdb` database.
4. **Enter hosts or subnets with which *one or more* Trusted Solaris workstations can communicate in the workstations' "Remote Hosts Worksheet - Local tnrhdb Entries" on page 234.**
   You enter these hosts and subnets in the local `tnrhdb` file of the affected workstation.

Closed and Open Networks

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 Solaris workstations recognize only Trusted Solaris

workstations. Data entry from outside the network is restricted to peripherals attached to Trusted Solaris workstations. Figure 2-2 illustrates the two types of closed networks, one closed physically and the other closed using software.

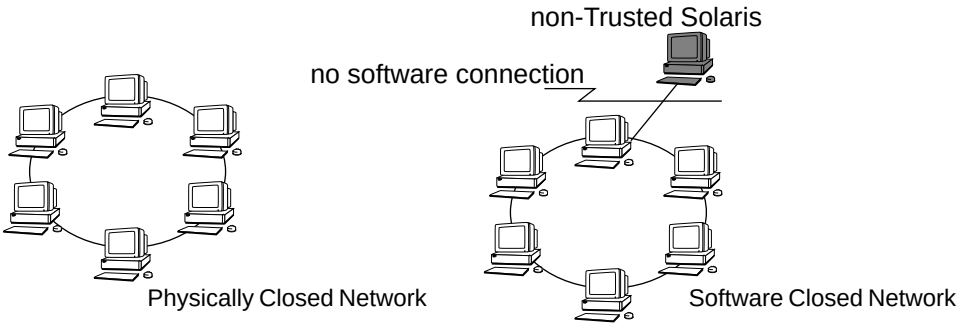


Figure 2-2 Closed Trusted Solaris Networks

Note – If you choose to have a closed network, you do not need to plan any further. Go to "Planning Network Administration" on page 32.

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. A Trusted Solaris workstation can communicate with any non-Trusted Solaris workstation that is defined the NIS+ `tnrhdb` (Trusted Network Remote Host DataBase) or in its local `tnrhdb` database.

Defining a Non-Trusted Solaris Workstation

All workstations that can communicate with each other are defined by an IP address and a `tnrhtp` template name in the `tnrhdb` database. The template definitions include `host_type` and security attributes specific to the host type.

Host type is the Trusted Solaris term for network hosts based on the type of network packet the host sends and receives. Table 2-6 lists the host types that Trusted Solaris workstations recognize.

Table 2-6 Host Types Recognized by Trusted Solaris Network Software

Host Type	Trusted Solaris Term	For Workstation or subnet ...
Unlabeled	`unlabeled`	That sends unlabeled packets, for example, SUN workstations running Solaris software
Labeled		
Trusted Solaris	`sun_tsol`	That runs Trusted Solaris 2.x
TSIX (RE1.1)	`tsix`	That runs TSIX(RE1.1) protocol
MSIX	`msix`	That runs Trusted Solaris 1.2
CIPSO	`cipso`	That sends CIPSO packets
RIPSO	`ripso`	That sends RIPSO packets

Table 2-7 lists the templates provided in the default `tnrhtp` database..

Table 2-7 Templates Provided with Trusted Solaris Network Software

Host Type	Template Name	Purpose
Unlabeled	`unlab`	For unlabeled hosts or networks
Labeled		
Trusted Solaris	`tsol`	For TS2.5 hosts or networks
	`tsol_1`	For TS2.5 hosts or networks that label packets with the RIPSO security option
	`tsol_2`	For TS2.5 hosts or networks that label packets with the CIPSO security option
TSIX (RE1.1)	`tsix`	For TSIX(RE1.1) hosts or networks
MSIX	`msix`	For MSIX hosts or networks
CIPSO	`cipso`	For CIPSO hosts or networks
RIPSO	`ripso`	For RIPSO hosts or networks

See the `tnrhtp(4TSOL)` man page for complete descriptions of each host type with several examples.

Example - Using an Unlabeled Host as a File Server

An unlabeled host, such as a Solaris 2.5.1 workstation serving as a site-wide file server, can serve as a file server for an open Trusted Solaris network. To configure an unlabeled host, or one of its file systems, to be NFS-mounted on a Trusted Solaris workstation, consider the following rules of the trusted network:

- The unlabeled host must be listed in the NIS+ `tnrhdb` table (as `template name=unlab`), or in a particular Trusted Solaris workstation's `tnrhdb` file.
- An unlabeled host entry in the `tnrhdb` overrides the Trusted Solaris security attributes of the workstation's network interface. Table 2-8 shows the list of attributes and default values that apply to an unlabeled host.

Table 2-8 Network Security Defaults for an Unlabeled Host

Security Attribute	**Template Field**	**Default Value, from** `tnidb`
Default Label	def_label	`admin_low` (in hex notation)
Default Clearance	def_cl	`admin_high` (in hex notation)
Default User ID	def_uid	nobody
Default Group ID	def_gid	nobody
Forced Privileges	forced_privs	none

- The file system from an unlabeled host can have Trusted Solaris security attributes specified in the `/etc/security/tsol/vfstab_adjunct` file. However, the attribute values from the `vfstab_adjunct` file are used only if the attributes are not explicitly set in the `tnidb` or `tnrhdb` file for the host.
- Mounted file systems are governed by the Mandatory Access Control (MAC) rule "read down, write equal" (RD/WE).
  Therefore, the files in an unlabeled file system that is mounted at the sensitivity label {C}, can be read by users whose reading process is labeled [C] or higher and can be modified by users whose writing process is [C].

▼ Read Further

♦ **Use the references inTable 2-9 to plan, configure, and administer network security.**

Table 2-9 References for Planning Network Security

Reference	To Help You ...
Trusted Solaris Administrator's Procedures	Configure and administer network hosts.
Your site security policy document.	Determine how open your network can be.

▼ Use Worksheets

Note – Use worksheets only if the network is open.

1. **Using the list of subnet and host addresses provided by the system administrator, enter the IP addresses of hosts or subnets with which all Trusted Solaris workstations can communicate in a worksheet copied from "Remote Hosts (tnrhdb) Worksheet for NIS+ Root Master" on page 233.**
2. **Using the list of subnet and host addresses provided by the system administrator, enter the IP addresses of hosts or subnets with which particular Trusted Solaris workstations can communicate in the "Remote Hosts Worksheet - Local tnrhdb Entries" on page 234.**
   The system administrator collects them in "Determine Names and IP Addresses of Network Hosts" on page 33, and enters them on the Remote Hosts worksheets in Step 1 on page 36.
3. **Enter the hosts and subnets' template names for `host_type`s in the worksheets.**
   You can use the predefined templates for the `host_type` when configuring the network. To modify existing templates and create your own, see *Trusted Solaris Administrator's Procedures*.

Planning Network Administration

The system administrator plans most of network administration. The security aspects of printing and mail are planned by the security administrator.

Overview of Planning Network Administration - System Administrator

Overview of Planning Network Administration - Security Administrator

▼ Plan Network Hardware

Planning the hardware for the network is not covered in this manual.

♦ **Use the references in Table 2-10 to plan network hardware and setup.**

Table 2-10 Planning Network Hardware

What to Plan	Who Plans it	Reference
Physical protections	Security Administrator	Your site security policy document.
Hardware	System Administrator	*TCP/IP and Data Communications Administration Guide*, Chapter 3, “Planning Your Network”

▼ Determine Names and IP Addresses of Network Hosts

♦ **If the security administrator decides on an open network, determine the names and IP addresses of the workstations and subnets that Trusted Solaris workstations can communicate with.**
You and the security administrator will enter these in the appropriate locations during network configuration. You determined the names and addresses of Trusted Solaris workstations in “Collect Basic Information about Each Workstation” on page 43.

▼ Plan NIS+ Domain

1. **Decide the NIS+ domain name, and the name and IP address of the NIS+ root master.**
2. **Decide on the NIS+ replicas and any subdomain masters.**
3. **Decide on the rest of the NIS+ clients.**
   All workstations in the NIS+ domain must be running Trusted Solaris software.

Table 2-11 describes the databases that hold data specific to Trusted Solaris administration. During NIS+ setup, these databases are added to the NIS+ tables in your domain.

Table 2-11 Databases that Contain Trusted Solaris Data

Database	Local File Location	Description
`bootparams`	`/etc/bootparams`	Boot Parameters contains the Trusted Solaris label configuration information you provided during installation
`tnrhdb`	`/etc/security/tsol/tnrhdb`	Trusted Network Remote Host DataBase contains the Trusted Solaris network hosts that all Trusted Solaris workstations can communicate with. After installation, the local file contains your NIS+ subnetaddress, for example, 129.111.111.0
`tnrhtp`	`/etc/security/tsol/tnrhtp`	Trusted Network Remote Host TemPlate contains Trusted Solaris definitions of network host types.
`tsolprof`	`/etc/security/tsol/tsolprof`	Trusted Solaris Profile database contains Trusted Solaris execution profiles, such as Object Management and All
`tsoluser`	`/etc/security/tsol/tsoluser`	Trusted Solaris User database contains Trusted Solaris roles, such as secadmin and admin, and user security information, such as labels and accreditation range

To plan all aspects of your NIS+ domain, see the *NIS+ and DNS Setup and Configuration Guide* in the base Solaris document set.

▼ Plan Servers - References

To plan the system administration aspects of servers, see the administration guides in the base Solaris document set, including:

- *Mail Administration Guide*

- *NIS+ and FNS Administration Guide*
- *User Accounts, Printers, and Mail Administration*

OS servers are covered in the *Solstice AdminSuite 2.1 Administration Guide*.

▼ Plan Network Printer Security

1. **Decide what will be printed on the banner and trailer pages.**
   All ASCII pages are automatically labeled at the top and bottom.
2. **Decide which users are to be authorized to print Postscript.**
   The authorization will be in effect for any printer that the user has access to which prints files within the user's label range. No authorization is required for printing ASCII files.
3. **Decide the label range of each printer.**
   Processes outside the label range of a printer cannot print to it.

Printers in the SPARCprinter family can be attached directly to a print server or to the network itself. Since printers are vulnerable to tampering on the wire between the printer and the network or print server, consider placing printers in the same (locked) room as their print server, or if not being served by a print server, in the same (locked) room where it connects to the network wire.

Setting up printing is covered in detail in *Trusted Solaris Administrator's Procedures*.

▼ Plan Mail Security

- **Decide how to handle mail that arrives at a sensitivity label below the user's minimum label.**
  You use the p (privacy) option in the sendmail configuration file, `/etc/mail/sendmail.cf`. The default is to upgrade `admin_low` mail and send it to the recipient, and to send back mail at other labels.

See the `sendmail(1MTSOL)` man page, especially the TRUSTED SOLARIS DIFFERENCES section.

Setting up mail is covered in detail in *Trusted Solaris Administrator's Procedures*: "How Sendmail Handles Mail Below the Recipient's Minimum SL" and "To Configure Mail Delivery Options for Mail Outside User's Minimum Labels."

▼ Read Further

♦ **Use the references in Table 2-12 to plan mail and printer security.**

Table 2-12 References for Planning Mail and Printer Security

Reference	To Help You ...
Trusted Solaris Administrator's Procedures	Plan, configure, and administer mail and printing.
Your site security policy document.	Determine security requirements for mail and printing.

▼ Use Worksheets

The Job of the System Administrator:

1. **Enter the sunets and host addresses that your Trusted Solaris network can reach.**
   The security administrator uses this to enter security information in worksheets copied from "Remote Hosts Worksheet - Local tnrhdb Entries" on page 234.

   The security administrator's planning task was described earlier, in Step 1 and Step 2 on page 32.

2. **Determine the kind of network packet labeling used by each subnet and host.**
   See Table 2-6 on page 30 for a list of possibilities.

3. **Enter your NIS+ domain servers on the worksheet copied from "Services Provided by Each Workstation" on page 232.**

4. **Enter your printers and their hosts on the worksheet copied from "Services Provided by Each Workstation" on page 232.**

5. **Enter your mail server(s) on the worksheet copied from "Services Provided by Each Workstation" on page 232.**

The Job of the Security Administrator:

1. **Enter security information for printers on the worksheet copied from "Services Provided by Each Workstation" on page 232.**

2. **Enter security information for each mail server on the worksheet copied from "Services Provided by Each Workstation" on page 232.**

Planning the Workstations

Planning the workstations requires coordination between the security administrator and the system administrator.

The system administrator plans the hardware and workstation use; the security administrator plans the workstation security.

Overview of Planning Workstation Hardware - System Administrator

Overview of Planning Workstation Use - System Administrator

Overview of Planning Workstation Security - Security Administrator

2

Planning Workstation Hardware

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

▼ Determine if You Have Required Hardware

♦ **From Table 2-13, determine that you have the hardware required to install Trusted Solaris software on every workstation.**
For a complete list of supported hardware and peripherals, see Appendix D, "Supported Hardware Components".

Table 2-13 Hardware Requirements

Hardware Platform	Minimum Memory	Disk Interfaces	Buses	Devices for Installing Trusted Solaris Software
SPARC® workstation	32 Mbytes	• IPI • SCSI	• VMEbus • Sbus	You must have one of the following devices for installing Trusted Solaris software: • Local CD-ROM drive • Remote CD-ROM drive available over the network • Remote hard disk available over the network plus • 150-megabyte tape drive

▼ Decide Memory Requirements and Disk Space

♦ **For each workstation, decide how much disk space and memory is required.**

Memory Requirements

Trusted Solaris software requires a minimum is 32 Mbytes of virtual memory (physical and swap file/slices). However, a workstation may require more memory, depending on the workstation's use.

Memory requirements are larger on workstations that:

- are used as servers: OS servers, name servers, file servers, audit servers, boot servers
- run graphics or other large applications
- run compilers
- run number-crunching applications

Disk Space Requirements

Disk space requirements are larger on workstations that:

- are used as servers: OS servers, name servers, file servers, audit servers, boot servers
- are used by programmers
- run graphics or other large applications
- store files or large applications locally
- have several smaller disks (for example, ten 104-Mbyte disks will waste more space trying to make things fit than a single 1-GByte disk)
- are installed with larger software groups: developer and entire
  See Table 2-14 for size estimates of Trusted Solaris software groups.

Table 2-14 Software Group Contents and Size

If You Want to Install This Software Group ...	**Which Installs ...**	**Then You Will Need Approximately This Much Disk Space For Trusted Solaris CD ...**
End User System Support	The minimum software required to boot and run Trusted Solaris software including CDE, Solstice AdminSuite, and auditing.	700 Mbytes
Developer System Support	The end user software plus software for developing software including libraries, include files, man pages, and programming tools. Compilers and debuggers are not included.	770 Mbytes
Entire Distribution	The entire Trusted Solaris release (everything on the CD). Compilers and debuggers are not included.	850 Mbytes

▼ Determine Your System Type

♦ **For each workstation, choose its system type.**
During installation you specify the workstation's *system type* to determine where it gets important file systems.

Table 2-15 System Type Choices

Choose	Because	Description
OS server	The workstation will serve diskless clients.	Provides Trusted Solaris operating environment software including services and/or file systems for workstations on the network. For diskless clients, it provides root (/), /usr, and swap file systems.
Standalone	The workstation is: a diskfull client a server the NIS+ root master	Has a local disk and does not require support from an OS server. Workstations that serve other workstations, such as install servers, name servers, file servers, boot servers, and audit servers, as well as diskfull clients are installed as standalone workstations.
Diskless Client	The workstation is a diskless client.	Does not install Trusted Solaris software, but receives file services from an OS server, and does not have a local disk.

Note – For performance reasons, your NIS+ root master should not serve diskless clients. Install the NIS+ root master as a standalone workstation.

A *standalone system* that is non-networked is the only system type in the Trusted Solaris operating environment that does not require you to install the NIS+ name service.

Note – A standalone workstation applies to *both* networked and non-networked systems. Whether networked or non-networked, a standalone workstation has all of its Trusted Solaris software on local hard disk, and does not require services from another system.

Planning Workstation Use

The use of a workstation affects how much disk space and memory it requires, and it affects the order of installation. See Install Workstations in Order on page 53 for the order in which to install workstations.

The system administrator plans workstation use.

▼ Decide Whether Non-Networked Workstation Uses NIS+

If you are installing one workstation, and it is does not have a net connection:

- **Decide whether to use the NIS+ name service.**
  If you decide to use NIS+, go to "Plan NIS+ Domain" on page 34. Otherwise, continue.

A non-networked workstation is not required to use the NIS+ name service, although using NIS+ is recommended.

Advantages of using NIS+ – If you add other workstations later, the domain is already set up. Information is stored in NIS+ tables rather than ASCII text files, so is more secure.

Disadvantages of using NIS+ – Requires time to set up NIS+ domain.

Advantages of using no name service – More disk space and memory available for other tasks.

Disadvantages of using no name service – Requires editing of several ASCII files that correspond to one NIS+ table. May be time-consuming to keep all administrative files synchronized when there are many changes. System information is accessible in plain text files.

If you decide not to use NIS+, go to "Planning Workstation Security" on page 44.

▼ Determine the NIS+ Servers

1. **Decide which workstation will serve as the NIS+ root master.**
   The NIS+ root master requires additional memory and disk space, and it is installed first.
2. **Decide on the NIS+ replicas and any subdomain masters.**

NIS+ servers are the name servers for your Trusted Solaris network, so NIS+ server planning is part of network planning. See Plan NIS+ Domain on page 34 for a fuller description of what needs to be planned, and for references.

▼ Determine the Other Servers

♦ **Determine what servers your domain and users require.**
Table 2-16 lists servers you can create and why you would create them. For more information, see *System Administration Guide, Volume I.*

Table 2-16 Servers to Create, Listed Alphabetically

Create ...	If you plan to ...	Comments
Audit server	Enable auditing	Create as many as you need to serve your audit recording needs
Audit administration server	Enable auditing	One per NIS+ domain is required in order to back up and interpret audit records, and to create audit reports
Boot server	Install over the network	One per subnet is required
		It can be the same as the install server for the install server's domain
File server	Centrally locate files for general use	Can be a Solaris 2.5 (unlabeled) workstation
Install server	Install over the network	One per subnet is required
DNS server	Resolve internet names and addresses outside your local network	Not needed on a closed network.
Home directory server	Enable remote mounting of users' home directories.	Can be the NIS+ root master, but does not have to be.
Mail server	Funnel mail to end user workstations from a central location	You can have some users served by a central mail server, and others not.
OS server	Serve diskless clients	Create as many as you need for your diskless client needs
Print server	Print	Create as many as you need for your printing needs
		The print server for a local printer is the local workstation.

▼ Determine the Network Routers

♦ **Choose a workstation that has at least two interface cards to be the router between another network and the Trusted Solaris network.**
Not required if the security administrator leaves the network closed. See "Planning Network Security" on page 27.

▼ Determine the End User Workstations

♦ **Decide which workstations are end user workstations, their names, and their IP addresses.**

▼ Determine the Shared and Mounted File Systems

1. **For each workstation, decide which file systems it will share.**
2. **For each workstation, determine which shared file systems to mount.**

▼ Collect Basic Information about Each Workstation

♦ **Determine, create, or plan the workstation details listed in Table 2-17:**

Table 2-17 Information to Collect for a Workstation

Information	That You ...
Name	Create or determine.
IP address	Determine.
Ethernet address	Determine from the `banner` command in the PROM (> **`banner`**).
Primary network interface	Select from the list offered during installation.
Network Router	Enter in the file `/etc/defaultrouter` on every workstation. One workstation in the network acts as the interface to another network if your site has an open network. You have as many network routers as you have networks you connect to.

Table 2-17 Information to Collect for a Workstation

Information	That You ...
Sun architecture	Determine from the command `uname -m` in a shell.
Local (backup) audit partition	See "Planning Auditing" on page 23
Primary and secondary audit partitions	See *Trusted Solaris Audit Administration* and "Plan a Network of Audit File Systems" on page 26

▼ Use Worksheets

- **For each server and end user workstation, enter its basic information, file systems to share, and file systems to mount on its worksheet, copied from "Standalone NIS+ Client Installation Worksheet" on page 225.**
  Leave the security information for the security administrator to fill in.

▼ Read Further

- **Use the references in Table 2-5 to plan your workstations and file systems.**
  See the base Solaris document set for planning system administration that is not specific to Trusted Solaris administration, such as planning servers.

Table 2-18 References for Planning Workstation Use

Use the Reference	To Help You ...
Trusted Solaris Audit Administration	Configure auditing in a Trusted Solaris environment
System Administration Guide, Volume I	Plan the servers and file systems.
Mail Administration Guide	Plan mail administration.
TCP/IP and Data Communications Administration Guide, Chapter 4, "Configuring TCP/IP on the Network"	Plan network routing.
Trusted Solaris Administrator's Procedures	Plan and configure your workstations, and handle user, printer, and mail tasks specific to Trusted Solaris software.

Planning Workstation Security

Workstation security includes passwords and security attributes on file systems, network interfaces, and devices. Physical protections, such as locked rooms, are part of wider site security policy and are not covered here.

The security administrator plans workstation security.

▼ Plan Passwords

1. **For each workstation, plan a password for root.**
   "root" is a local user who can access the workstation in single-user mode. The password should be eight alphabetic characters long, and be a nonsense word. Pronounceable nonsense words are easier to remember.

2. **Plan a password for the PROM.**
   The PROM password should be hard to guess, pronounceable, and at least six letters long. Users who know the PROM password can boot the workstation.

3. **In addition, plan whether the PROM mode is secure or full.**
   You use the `eeprom(1MTSOL)` command to enter the PROM mode and password.

   - Choose secure PROM mode when you want to enable only those with the PROM password access to single-user mode.
   - Choose full PROM mode when you want to enable only those with the PROM password access to the PROM.

- Decide when password access to the PROM is required: every time the workstation boots (PROM mode=full), or only for diagnostic procedures (PROM mode=command).

▼ Plan Workstation Label Range

1. **If the workstation should have a label range narrower than the possible label range ([admin_high] to [admin_low]), select its label range from the clearances and labels in your site's `label_encodings` file.**
   See *Trusted Solaris Administrator's Procedures* for the circumstances that would require you to limit a workstation's label range.

Note – Do not limit a workstation's label range before you have tested that the workstation runs well using the full label range.

▼ Plan Network Interface Security

♦ **If the network interface on the workstation should have Trusted Solaris security attribute values more restricted than the default, plan its security attribute values.**
You enter network interface security attribute values in the workstation's `/etc/security/tsol/tnidb` (Trusted Network Interface DataBase) file.

Default Trusted Solaris Network Security Attribute Values

The network interface of every Trusted Solaris workstation is installed by default with the security attributes and values shown in Table 2-19.

Table 2-19 Trusted Solaris Network Security Defaults

Security Attribute	`tnidb` Field	Default Value
Minimum SL	min_sl	`admin_low` (in hex notation)
Maximum SL	max_sl	`admin_high` (in hex notation)
Default Label	def_label	`admin_low` (in hex notation)
Default Clearance	def_cl	`admin_high` (in hex notation)
Default User ID	def_uid	nobody
Default Group ID	def_gid	nobody
Forced Privileges	forced_privs	none

Warning – The loopback and primary interface need the min_sl to be admin_low (in hex) and the max_sl to be admin_high (in hex) for proper functioning.

See the `tnidb(4TSOL)` man page.

▼ Plan File System Security

1. **Identify the file systems whose Trusted Solaris security attributes should be different from the default.**
Workstations whose file systems serve others (file server, audit server, OS server) are likely candidates for security attribute modification.

2. **Decide what values to give each file system's security attributes.**
   You enter file system security attribute values in the workstation's `/etc/security/tsol/vfstab_adjunct` file.

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

Default File System Security Attribute Values

Trusted Solaris software by default protects a file system with security attributes. You can change the values. Table 2-20 shows the security attributes with their default values, listed in the order they are listed in the `vfstab_adjunct` file. See Figure 5-2 on page 101 for a `vfstab_adjunct` entry.

Table 2-20 Trusted Solaris File System-wide Security Attributes

Attribute	Default	Comment
Access ACL	None	Access Control List
Default ACL	None	
Mount Mode	0500	
Attribute Flags	None	
Group Id	Nogroup	
User Id	None	
Information Label	admin_low	
Sensitivity Label	admin_low	
Forced Privilege Set	Empty	
Allowed Privilege Set	Empty	
Lowest SL in Range	admin_low	
Highest SL in Range	admin_high	
MLD prefix	.MLD.	MultiLevel Directory
Audit Preselection Flags	None	

See the `vfstab_adjunct(4TSOL)` man page.

See *Trusted Solaris Administrator's Procedures* for a full description of file system security attributes and how they are used.

▼ Use Worksheets

1. **On the worksheets created by the system administrator for all workstations (see "Use Worksheets" on page 44), enter file system security, network interface security, and label range information.**
2. **Using your own method, create and remember/write down the passwords for root and PROM mode for every workstation on the network.**

▼ Read Further

- **Use the references in Table 2-21 to plan workstation security.**

Table 2-21 References for Workstation Security

Use the Reference	To Help You ...
Trusted Solaris Audit Administration	Configure and administer auditing in a Trusted Solaris environment
Trusted Solaris Label Administration	Configure and administer labeling
Trusted Solaris Administrator's Procedures	Implement workstation security
Your site security policy document.	Determine your security requirements

Planning the First Two Users

The system administrator and security administrator gather information about the first two users. These two users are assigned the roles `secadmin` and `admin`. When the users assume the roles, the Trusted Solaris software enforces two-role task division.

Overview of Planning the First Two Users - System Administrator

▼ Plan User and Role Account Information

1. **Plan Identity and Home information for the user who will be assigned the role admin (system administrator) and the user who will be assigned the role secadmin (security administrator).**
   See Table 2-22 for Identity and Home information required by the User Manager when creating a user.

2. **Plan the Home information of the administrative roles secadmin and admin.**
   See Table 2-22 for Home information to enter for a predefined role in the User Manager.

Table 2-22 Planning User Account Information

User Information the System Administrator Collects		Required Value, if Any
Identity	Login name	*Not a role name or existing user name*
	User ID	*Not a role ID or existing user ID*
	Group	
	Secondary Groups	
	Comment	
	Login Shell	
	User Type	User
Home	Create home directory automatically?	Yes, to create a multilevel directory.
	Home directory pathname	
	Path to setup files (for .cshrc, .login)	
	Default permissions	
	Mail server	
	Autohome setup?	**NO**

▼ Plan User and Role Security

1. **Plan the security aspects of the first two users.**
   See Table 2-23 for the password, idle, label, (execution) profile, and role information required by the User Manager.

Table 2-23 Planning User Security Information

User Information the Security Administrator Collects		Required Value, if Any
Password	Password state	*No more than 8 characters.*
	Minimum days between changing passwords	
	Maximum days between changing passwords	
	Maximum time a user can be inactive	
	Password generation	.
	Account state	1. Locked by system administrator 2. Open by security administrator
	NIS+ credentials?	Yes
Idle	Idle time	
	Idle action: logout or lock screen?	
Labels	Clearance	
	Minimum label	
	View - External or Internal?	
	Sensitivity Label visible or not visible?	
	Information Label visible or not visible?	
Profiles	All, None, others	Enable Logins, Basic Actions, All
Roles	secadmin, admin, root, oper	Assign `secadmin` to the security administrator Assign `admin` to the system administrator

2. **Plan the security aspects of the administrative roles secadmin and admin.** See Table 2-24 for the password and idle information required by the User Manager for the administrative roles. You will not alter label and profile information for the roles.

Table 2-24 Planning Role Security Information

User Information the Security Administrator Collects		Required Value, if Any
Password	Password state	
	Minimum days between changing passwords	
	Maximum days between changing passwords	
	Maximum time a user can be inactive	
	Password generation	
	Account state	Open
	NIS+ credentials?	Yes
Idle	Idle time	
	Idle action: logout or lock screen?	

▼ Read Further

♦ **Use the references inTable 2-25 to plan users at your site.**

Table 2-25 References for Planning Users

Reference	To Help You ...
Trusted Solaris Administration Overview	Get an overview of user management
Trusted Solaris Administrator's Procedures	Administer users
Your site security policy document.	Determine security policy around users: password requirements, idle requirements, and so on

▼ Use Worksheets

1. **Enter the details for each user in a user worksheet copied from the "First User Worksheet" on page 235.**
2. **Enter the details for each role in a role worksheet copied from the "Administrative Role Worksheet - secadmin" on page 237.**

2

Finishing Up the Planning

The system administrator and security administrator coordinate finishing up the planning.

Overview of Finishing Up the Planning

▼ Back up the Workstations

♦ **Before installing, 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.s

▼ Use the Task Maps

♦ **Use the task maps to find the appropriate installation procedure:**

▼ Install Workstations in Order

- **In a networked environment, install and configure workstations in the order:**
  - **i. NIS+ root master**
  - **ii. Workstations that will keep the name service robust, such as NIS+ replicas, NIS+ masters of subdomains**
  - **iii. Workstations that will be used as servers: file servers, network install servers, boot servers, audit servers, OS servers**
  - **iv. Workstations that will be used by end users, both diskfull and diskless**

2

Installing a Workstation 3

This chapter covers how to boot and install a workstation.

Who Does What

Trusted Solaris software is designed to be installed and configured by two people with distinct responsibilities. However, the installation program cannot enforce two-role task division. Task division is enforced by users who can assume Trusted Solaris roles. Since 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.

3

Installing a Workstation

1 Halt the workstation.

If The System Is...	Then ...
Off	**1)** Turn on the system components in the order recommended in the hardware guide. **Caution:** If the workstation starts booting, press L1-A or Stop-A. **2)** Go to Step 2.

On	**1)** If the workstation is running Solaris, enter the following commands:
	`$ su root`
	`# halt`
	2) Go to Step 2.

See “Planning the Workstations” on page 37 for hardware, disk space, and memory requirements.

2 If you are installing from a CDROM, place the Trusted Solaris CD in the workstation’s CDROM drive.

See your hardware manual for instructions.

3 If the screen displays the > prompt instead of the ok prompt, then enter n and press Return.

The screen should now display the ok prompt.

4 Boot the workstation using the appropriate boot command.

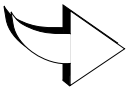
If You Are Booting from a CDROM and If the System You Are Booting Is ...	Then Enter ...
SPARCstation 1 (4/60) SPARCstation 1+ (4/65) SPARCstation SLC™ (4/20) SPARCstation IPC™ (4/40)	`boot sd(0,6,2)`
All other Sun workstations	`boot cdrom`

If You Are Booting Over the Network...	Then Enter ...
From an Install Server	`boot net`
Using Custom JumpStart	`boot net - install`

5 Wait for booting to complete.

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

During the booting phase, OpenWindows is started for the installation program. However, OpenWindows is not used with the Trusted Solaris software after installation.



```
Type b (boot), c (continue), or n (new command mode)
>n
Type help for more information
ok boot cdrom
Rebooting with command: cdrom
Boot device: /sbus/esp@0, 8000000/sd@6, 0:c
File and args:
SunOS Release 5.5.1 Version TS2.5 [UNIX(R) System V Release 4.0]
Copyright (c) 1983-1997, Sun Microsystems, Inc.
WARNING: clock gained 35 days -- CHECK AND RESET THE DATE!
Configuring the /devices directory
Configuring the /dev directory
Starting OpenWindows...
```

6 Be prepared to answer installation program questions.

1. **Use the blank worksheets provided in Appendix B, "Worksheets for Configuring and Installing Trusted Solaris" and the examples in Appendix F, "Example Worksheets" for additional help.**

2. **Be sure to select *None* for the naming service.**
   If you select anything else, you may get errors. Name service configuration is performed after installation. This is true for all installations, including network installations.

3. **To install the End User software cluster, choose Core.**
   Core provides the Common Desktop Environment and Solstice AdminSuite™ tools, which are part of the operating system.

4. **Partition the disks correctly, using the worksheets.**
   Hints:

   On a standalone that will be the home directory server…

   a. **Create an `/export/home` partition large enough for the users' home directories.**
      The `/export/home` partition will be used for user home directories and to hold some files temporarily during configuration.

   On a standalone that will not be a home directory server…

   a. **Create a small `/export` partition to hold some temporary configuration files.**
      You can also use it as a mount point.

   On an OS server…

   a. **Allocate enough space for the clients' root and swap.**
      Follow the suggestions in Chapter 11, "Configuring Diskless Clients".

Note – When you install an OS server, you allocate disk space required for the clients that server will support. Then, *after* the OS server is installed, you will use Host Manager in the Solstice_Apps folder to add the platform support required by those clients.

For audit records...

a. Create at least one partition named `/etc/security/audit/`*`workstation_name`* for audit files, if auditing is a site security requirement.

7 Answer the installation program questions displayed on the screen.

The Welcome to Trusted Solaris screen briefly appears, then the screen turns blue-gray, and a Trusted Solaris Install Console is displayed in the upper left corner. Messages display in the console during installation.

The Trusted Solaris installation program is running.

- If you are installing from a CDROM, the program guides you step by step through installing Trusted Solaris software; it also has online help to answer your questions.
- If you are installing over the network, you will be prompted to answer questions whose answers the installation program cannot find.

After you provide the requested information to the installation program, the actual installation takes from 30 to 60 minutes. The speed of your medium, CDROM or net, determines the installation time.

8 Read the install log.

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

1. Look for successful installation of packages.

2. Ignore messages of the form:

```
WARNING: quick verify of <filename>; wrong mod time.
```

If You Choose Manual Reboot

♦ **To manually reboot your system after the installation, type:**

```
#   halt
ok  boot disk
```

Enter a Root Password

♦ **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.

Configuring a Workstation without the NIS+ Name Service 4

This chapter covers how to configure a workstation to use no name service.

Who Does What

Trusted Solaris software is designed to be installed and configured by two people with distinct responsibilities. Once users who can assume Trusted Solaris roles have been created, and the workstation is rebooted, the software enforces two-role task division. If two-person installation is not a site security requirement, assigning the two administrative roles, secadmin and admin, to one person enables that person to configure both security and system information.

Role - root
Label - admin_low
Shell - profile shell

A box to the left of a configuration procedure, like the one shown here, is used to indicate the role, label, and tool to be used for the procedure. There is a box to the left of procedures where the software enforces role division. There is sometimes more than one box in a procedure when more than one role, tool, or label is required to complete a procedure.

4

Configuring a Non-networked Workstation

A non-networked workstation is configured much like a NIS+ root master, except that `/etc` files are used for administration rather than NIS+ tables.

Use the following procedures to configure either a non-networked workstation or a networked workstation that does not use a name service.

Other setup tasks, such as protecting file systems and securing attached devices are covered in *Trusted Solaris Administrator's Procedures*.

▼ Assume the root Role

♦ **Follow the procedure in "Assume the root Role" on page 71.**

▼ Open a Profile Shell

♦ **Follow the procedure in "Open a Profile Shell" on page 72.**

▼ Protect the Workstation

♦ **Follow the procedure in "Protect the Workstation" on page 73.**

▼ Check the `label_encodings` File

If you are not modifying the `label_encodings` file, and:

- If you are going to access a network without using the NIS+ name service, go to "Set Default Routes" on page 63.

Note – Your `label_encodings` file must be compatible with any Trusted Solaris host you are communicating with.

- If you are not going to access any other workstation, go to "Add administrative roles to three /etc files" on page 64.

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

Caution – If you are planning to install a modified `label_encodings` file, you *must* complete this step before continuing or the installation will fail.

---

1. **Have the medium (tape or diskette) with your site's `label_encodings` file ready to use.**

Role - root
Label - admin_low
Tool - Device Manager
Tool - regular terminal
Tool - Check Encodings

2. **Follow the procedures to allocate the device, check the file, and deallocate the device:**
   a. **"To allocate a device" on page 75**
   b. **"To copy in and check a site-specific label_encodings file" on page 76**
   c. **"To deallocate a device" on page 77**

▼ Set Default Routes

Role - root
Label - admin_low
Action - Set Default Routes

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

♦ **Follow the procedure in "Set Default Routes" on page 78.**

▼ Add the Defaultrouter to the Local Hosts Database

Role - root
Label - admin_low
Tool - Database Manager

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

♦ **Follow the procedure in "Add the Defaultrouter to the Local Hosts Database" on page 79.**

▼ Edit the Trusted Network Files

This task is required only if you plan to access other workstations without using a name service.

Role - root
Label - admin_low
Tool - Database Manager

The `tnrhdb` database should contain:

- this workstation
- every gateway in the `/etc/defaultrouter` file
- every workstation you want to communicate with

♦ **Follow the procedure in "Edit the Trusted Network Files" on page 80.**

▼ Set up DNS

Perform this task only if the security officer has planned for an open network, and you plan to use DNS on a workstation with no name service.

♦ **Follow the procedure in "Set up DNS (Optional)" on page 88.**
You do not need to edit the `nsswitch.conf` file; editing it will have no effect.

▼ Add administrative roles to three `/etc` files

When you operate locally, the Trusted Solaris administrative roles must have their names and passwords in the appropriate `/etc` files. There are three files to modify: passwd, shadow, and tsoluser.

Role - root
Label - admin_low
Shell - regular terminal

1. Save the original files by renaming them to ~.orig.

```
# cd /etc
# cp passwd passwd.orig
# cp passwd.roles passwd.rolesorig
# cp shadow shadow.orig
# cp shadow.roles shadow.roles.orig
#
# cd /etc/security/tsol
#
# cp tsoluser tsoluser.orig
# cp tsoluser.roles tsoluser.roles.orig
```

2. Append each Trusted Solaris file to its corresponding /etc file.

```
# cd /etc
# cat passwd.roles >> passwd
# chmod 600 shadow
# cat shadow.roles >> shadow
# chmod 400shadow
#
# cd /etc/security/tsol
#
# cat tsoluser.roles >> tsoluser
```

3. Modify other /etc files as necessary.

Caution – Do not edit the files: tsolprof, tsoluser, passwd, or shadow. After booting, you will modify these using the Solstice_Apps tools, User Manager and Profile Manager.

▼ Set Device Policy on Secondary Network Interfaces

Note – Ignore this procedure if the workstation has only one network interface.

♦ **Follow the procedure "Set Device Policy on Additional Network Interfaces" on page 89.**

▼ Reboot the system

1. **Right click the CDE front panel.**
2. **Select Shut Down from the menu.**
3. **Confirm that you want to shut down the machine.**
4. **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
```

▼ Update Role Credentials and Passwords

The passwords and credentials of the roles admin, secadmin, and oper must be updated using the User Manager.

- **Follow the procedure in "Update Role Credentials and Passwords" on page 91, *with the following exception*: substitute None for the Naming Service when bringing up User Manager (Step 4 on page 91).**

▼ Add Users to Administer the System

- **Follow the procedure in "Add Users to Administer the System" on page 95, *with the following exception*: continue to use None for the Naming Service of User Manager.**

▼ Verify that Users and Administrative Roles Work

- **Follow the procedure in "Verify that Users and Administrative Roles Work" on page 97.**

▼ Set up Auditing

If your site security requirements do not include auditing, disable it. The security administrator is responsible for the decision to disable auditing.

- **To disable auditing, follow the procedure in "To disable auditing" on page 99.**

▼ To configure auditing

Role - secadmin
Label - admin_low
Various tools

- **Use the audit worksheets and the procedures in the** *Trusted Solaris Audit Administration* **manual to configure auditing on each workstation.**

▼ Mount Unlabeled File Systems

Role - secadmin
Label - admin_low
Action- Set Mount Attributes

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

- **Log in as a user who can assume the role secadmin and follow the procedure in "Mount Unlabeled File Systems (Optional)" on page 100.**

▼ Create Mount Points

Role - admin
Label - admin_low
Action- Set Mount Points

Perform this task only if you plan to access other workstations without using a name service.

- **In the role admin, follow the procedure in "Create Mount Points" on page 101.**

▼ Export Shared Directories

Role - admin
Label - admin_low
Action- Share Filesystems

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

- **In the role admin, follow the procedure in "Export Shared Directories" on page 102.**

▼ Delete the User `install`

Role - admin
Label - admin_low
Tool - User Manager

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

1. **Log on as a user assigned the role admin and assume the role.**
2. **In the role workspace, open the User Manager.**
3. **Choose None for the Name Service, and All for the Filter.**
4. **Select the user `install` in the list.**
5. **Choose the Edit > Delete menu item, and then click OK.**
   You do not need to click the selections in the dialog.

Configuring the NIS+ Root Master 5

This chapter covers how to configure NIS+ root master, the first workstation you install at your site in a networked environment.

Who Does What

Trusted Solaris software is designed to be installed and configured by two people with distinct responsibilities. Once users who can assume Trusted Solaris roles have been created, and the workstation is rebooted, the software enforces two-role task division. If two-person installation is not a site security requirement, assigning the two administrative roles, secadmin and admin, to one person enables that person to configure both security and system information.

Role - root
Label - admin_low
Shell - profile shell

A box to the left of a configuration procedure, like the one shown here, is used to indicate the role, label, and tool to be used for the procedure. There is a box to the left of procedures where the software enforces role division. When more than one role, tool, or label is required to complete a procedure, there is a box for every change of role, tool, or label.

5

Configuring the NIS+ Root Master

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 for the NIS+ workstation itself.

Overview – To configure the NIS+ root master:

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

▼ Assume the root Role

At most sites, two or more administrators, an *install team*, are present when configuring the workstation. “You”, in the following procedures, refers to the install team. You assume the role `root` to configure the workstation before the Trusted Solaris software enforces two-role (secadmin and admin) task division.

▼ To log on and assume a role

1. **Log on to the workstation as the user `install`.**
   a. **Enter `install` as the user name and press the Return key.**
   b. **Enter `install` for the password.**
      The Enable Logins dialog is displayed.
   c. **Click OK to dismiss the dialog.**
      The Message Of the Day dialog is displayed.
   d. **Click OK to dismiss the dialog.**

You are in a CDE workspace (see Figure 5-1). The Trusted Stripe below the Front Panel shows the Input Information Label and the Window Sensitivity Label.

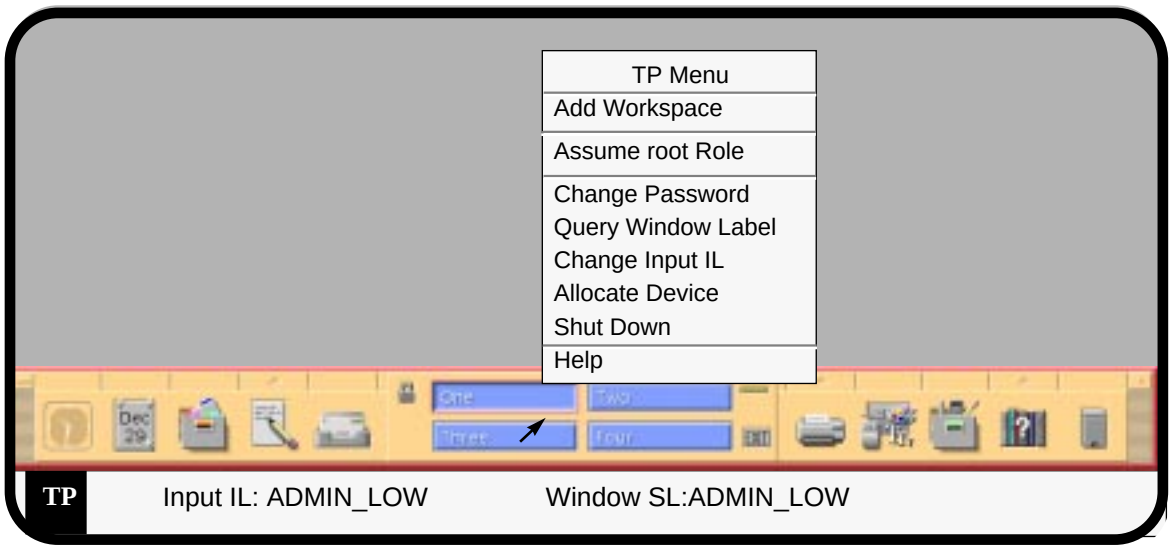


Figure 5-1 Assuming the root role from the Trusted Path Menu

2. **Assume the role root.**

   a. **Click the right mouse button in the middle of the Front Panel.**

   b. **Choose Assume root Role from the menu.**

   c. **At the password prompt, enter the password you created for root.**

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

▼ Open a Profile Shell

The profile shell [`pfsh(1MTSOL)`] is a special shell that enables execution of security-relevant commands. Such commands require privilege. The shell inherits the required privileges from the role's execution profile, hence the name *profile shell*.

▼ To launch a terminal

1. **Click the left mouse button on the triangle above the pad icon on the Front Panel.**
   A subpanel is displayed that includes an icon of a terminal.

2. **Click the terminal icon once.**
   A terminal is displayed. You use the terminal to enter commands when configuring the workstation.

Note – The Options menu enables you to customize the appearance of the window. Customizations are not saved.

▼ To open a profile shell that recognizes privilege

♦ **Enter the `pfsh` command.**
This changes the shell to a profile shell that recognizes privileges.

```
# pfsh
```

▼ To list the commands available to this profile shell

♦ **Enter the `clist` command.**
To view the entire list, pipe the command through `more`.

The `clist` command lists the commands available in a profile shell.

```
# clist | more
```

If the shell does not recognize the `clist` command, it is not a profile shell. If it prints a list of commands, it is a profile shell.

Role - root
Label - admin_low
Shell - profile shell

▼ To see process and privilege information in the profile shell

♦ **To see the process label, enter the `plabel(1TSOL)` command.**

```
# plabel
pid: ADMIN_LOW [ADMIN_LOW]
```

It returns the label of the process, ADMIN_LOW[ADMIN_LOW].

♦ **To see what privileges have been accorded to root in the profile shell, enter the `ppriv(1TSOL)` command.**

```
# ppriv
pid: none
```

While configuring the workstation, you will be running processes with no privileges at the label ADMIN_LOW[ADMIN_LOW], in the root role.

▼ Protect the Workstation

Access to the workstation as root should require a password; you used the password just now to assume the root role. For security, access to the PROM should also require a password.

▼ To set the PROM mode and password

Role - root
Label - admin_low
Shell - profile shell

♦ **In the profile shell, enter the PROM security mode.**
Choose the value `command` or `full` (see the `eeprom(1MTSOL)` 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
```

You are not prompted to enter a PROM password if the workstation already has one. To change the password, run the command:

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

At the next boot, the new PROM security mode and password will go into effect.

Caution – Do not forget this password. The hardware is rendered 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*.

▼ Check the `label_encodings` File

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

- Skip to “Set Default Routes” on page 78 if you are not modifying the `label_encodings` file.

You can edit the placeholder `label_encodings` file that the Trusted Solaris installation program installed. If you choose not to use the default `label_encodings` file shipped with the system, check that your `label_encodings` file works on the NIS+ master before copying the file to every workstation you install.

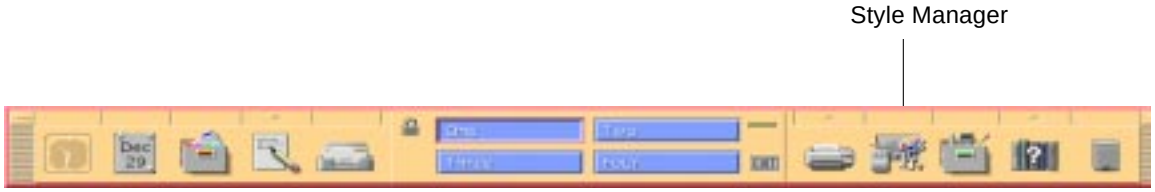
Caution – If you are planning to install a modified `label_encodings` file, you *must* complete this step before continuing or the installation will fail.

1. **Have the medium (tape or diskette) with your site's `label_encodings` file ready to use.**
2. **Follow the procedure "To allocate a device".**

▼ To allocate a device

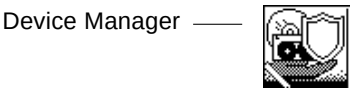
Role - root
Label - admin_low
Tool - Device Manager

1. **Allocate the tape or diskette drive using the Device Allocation Manager.**
   a. **Click the left mouse button on the triangle above the Style Manager icon on the Front Panel.**



   A subpanel is displayed that includes the Device Manager icon.

   b. **Click the Device Manager icon once.**



   c. **Double-click the device to be allocated.**
   mag_tape_0 allocates a tape device.
   floppy_0 allocates a diskette.

   d. **Click OK in the label builder; the file you load will be labeled admin_low.**

2. **Place the tape or diskette in the appropriate drive.**

▼ To copy in and check a site-specific `label_encodings` file

Role - root
Label - admin_low
Shell - profile shell

1. First, copy the file installed by Trusted Solaris to a new name.

```
# cd /etc/security/tsol
# cp label_encodings label_encodings.orig
```

2. Copy the site `label_encodings` file from a tape or diskette.

a. For a tape, use the following `tar(1TSOL)` commands:

```
# pwd
/etc/security/tsol
# tar tv
# tar xv label_encodings
```

b. For a diskette, use the following `tar` commands:

```
# tar tvf /dev/diskette
# tar xvf /dev/diskette label_encodings
```

Role - root
Label - admin_low
Action - Check Encodings

3. Check the syntax of the new `label_encodings` file using the Check Encodings action in the System_Admin folder in the Application Manager.

a. Click the Application Manager icon on the Front Panel.

Application Manager 

b. Double-click the System_Admin icon.


System_Admin

c. Double-click the Check Encodings action.


Check Encodings

d. In the dialog box, enter the full path name of the file, `/etc/security/tsol/label_encodings`.

4. Read the contents of the Check Encodings dialog box that is displayed.
The `chk_encodings(1MTSOL)` command checks the syntax of the file as the editor exits.

a. If it reports no errors, continue.

b. If it reports errors, resolve them before continuing.
For detailed procedures and explanation, please see the *Trusted Solaris Label Administration* manual.

Caution – You *must not* continue if your label_encodings file does not pass the Check Encodings test.

5. Read the new `label_encodings` file by pressing the right mouse button on the workspace background and choosing Restart Workspace Manager.

Your `label_encodings` file is now in effect.

You will copy the `label_encodings` file to the `/export/tmp` directory in "Copy Configuration Files for Distribution to Clients" on page 103.

6. Follow the procedure "To deallocate a device".

▼ To deallocate a device

Role - root
Label - admin_low
Tool - Device Manager

1. Deallocate the tape or diskette drive using the Device Allocation Manager.

a. Double-click the device to be deallocated.
A window appears listing devices being deallocated.

b. When prompted, press the Return key to dismiss the window.

2. Remove the tape or diskette from the drive.

3. Click the top left button and select Close to close the Device Allocation Manager window.

▼ Set Default Routes

This task is required only if the security officer has planned for an open network.

Note – A workstation cannot be its own default router (gateway). The NIS+ master can be a router for its clients, but it cannot be a router for itself.

This is the simplest method for setting up static routers. If your machine or site must access a complex network of gateways, the file `tsolgateways(4TSOL)` offers more control over routing. See the *Trusted Solaris Administrator's Procedures* manual and the man page for how to set up and use an `/etc/tsolgateways` file.

Role - root
Label - admin_low
Action - Set Default Routes

1. **Open the Application Manager by clicking once with the mouse on the Application Manager icon on the Front Panel.**

2. **Double-click the System_Admin icon.**


System_Admin

3. **Double-click the appropriate action: the Set Default Routes action.**
   An empty `/etc/defaultrouter` file appears in the trusted editor (`adminvi`).


Set Default Routes

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

4. **Enter the name of the workstation that you want to use to connect this Trusted Solaris network to another network, write the file and exit the editor.**
   For example, if a workstation named `trustworthy` is going to be your default router, enter its name in the `defaultrouter` file.

```
trustworthy
```

   If there is more than one router, enter them all, one per line. When you write the file and exit the Set Default Routes action, the file is saved to `/etc/defaultrouter`.

5. **If the workstation has more than one network interface, set them up now.**
   See the *TCP/IP and Data Communications Administration Guide*, Chapter 4, "Configuring TCP/IP on the Network" in the Solaris 2.5 document set.

▼ Add the Defaultrouter to the Local Hosts Database

Every workstation in the `/etc/defaultrouter` file must be in the local Hosts database.

▼ To open a Solstice_Apps database

Role - root
Label - admin_low
Tool - Database Manager

1. **Open the Solstice_Apps folder in the Application Manager.**

2. **Open the Database Manager by double-clicking its icon.**

3. **In the Load window, choose None for the Naming Service.**

4. **Select Hosts from the list of databases, then press the Return key to open it.**
   You are now editing a local copy of the `hosts` database.

The list of known hosts is displayed. The local workstation should already be in the database.

▼ To modify a Solstice_Apps database

1. **Enter every host in the `/etc/defaultrouter` file in the Hosts database.**
   a. **To add a host, its IP address, any aliases, and a comment about the host, choose Edit > Add.**
   b. **To modify the IP address, alias, or comment in an existing entry, select the entry and choose Edit > Modify.**
   c. **To change a mis-entered host name, select the entry, choose Edit > Delete, then add the correct new entry using Edit > Add.**
2. **Choose File > Exit to exit the Database Manager after saving your changes.**

▼ Edit the Trusted Network Files

The trusted network remote host database (`tnrhdb`) file enables the workstation to communicate with other hosts. It should include the IP addresses of the workstations on your network and the IP addresses of any other hosts that your Trusted Solaris 2.5 network can communicate with. The security administrator determines what networks can contact the Trusted Solaris 2.5 network; the system administrator collects the IP addresses.

To edit the `tnrhdb`, go to “To edit the tnrhdb database” on page 82.
You may want to do “To edit the tnrhtp database (optional)” first.

Note – You can change the network details later. For customizing the `tnrhdb` and its associated templates database, `tnrhtp`, see *Trusted Solaris Administration Tasks*.

▼ To edit the `tnrhtp` database (optional)

This example adds a new host type, unlab_conf, to the tnrhtp database. This procedure is a prerequisite to mounting an unlabeled host at the label Confidential. “Mount Unlabeled File Systems (Optional)” on page 100 completes the setup.

Role - root
Label - admin_low
Tool - Database Manager

1. **Open the Tnrhtp database in the Database Manager.**
   Follow the procedure in "To open a Solstice_Apps database" on page 79.
   a. **Choose None for the Naming Service.**
   b. **Scroll down to Tnrhtp, select it, and press the Return key to open it.**
      You are now editing a local copy of the `tnrhtp` database.
2. **Select the template `unlab`, and view the entry using Edit > Modify.**
3. **Click Cancel, then choose Edit > Add from the Tnrhtp menu.**
4. **In the Template Manager (Add) window, create an unlabeled host type named unlab_conf, no UID, no GID, no forced privileges, with an admin_high clearance and a CMW label of Admin_Low[Confidential].**
   a. **Enter `unlab_conf` for the template name.**
   b. **Select `Unlabeled` from the list of Host Types.**
   c. **Click the Def! button to use the defaults for User ID, Group ID, and Forced Privileges.**
      The button is to the right of each attribute.
   d. **Click the Clearance button to set the default clearance to `admin_high`.**
      The default clearance must dominate the default label. The label `admin_high` dominates all labels.
      i. **In the label builder, type `admin_high` in the Update With field.**
      ii. **Click the Update button to the right of the field.**
      The clearance in the top field changes to `admin_high`.
      iii. **Click OK.**
   e. **Click the Label button to set the default CMW label to `Admin_Low[Confidential]`.**
      If you are following this example with a different label_encodings file, select a low sensitivity label available to users. The sensitivity label admin_low is not available to users.
      i. **In the label builder, remove admin_high from the Update With field.**
      ii. **Click the SL button.**
      iii. **Click a low user sensitivity label, such as Confidential.**
      The [Sensitivity Label] in the CMW label field reflects your change.

iv. **Click the IL button.**

v. **Click a low information label, such as Unclassified.**
If your label_encodings file has no ILs for the sensitivity label, leave the IL at admin_low. The CMW label might read Admin_Low[Public], for example.

vi. **Click OK.**

5. **Close the Tnrhtp database by selecting File > Exit when you are done.**
The Database Manager does error checking and notifies the kernel cache about changes.

▼ To edit the `tnrhdb` database

Role - root
Label - admin_low
Tool - Database Manager

1. **Open the Database Manager by following the procedure in "To open a Solstice_Apps database" on page 79.**

   a. **Choose None for the Naming Service.**

   b. **Scroll down to Tnrhdb, select it, and press the Return key to open it.**
   You are now editing a local copy of the `tnrhdb` database.

2. **Use the IP address fallback mechanism to assign one template to all hosts on your Trusted Solaris 2.5 subnet.**

   a. **Enter the subnet IP address and 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.

   b. **For any exceptions on the subnet, enter the exception's IP address and its correct template.**
   For example, `129.150.110.3` **and** `unlab`. This host on the the subnet is an unlabeled host.

3. ***Hint*: To more easily copy the IP addresses from your Hosts database, open the `/etc/hosts` file in the Admin Editor. You can then copy and paste the IP addresses from the editor to the `tnrhdb`.**

4. **Enter the IP address of every host in your `/etc/defaultrouter` file, and assign to each an appropriate template name.**

   a. **To add an IP address and its host type, choose Edit > Add.**

   b. **To modify the host type of an existing IP address - host type entry, select the entry and choose Edit > Modify.**

c. **To change a mis-entered IP address and its host type, select the entry, choose Edit > Delete, then add the correct new entry.**

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

   a. **Enter the fallback designation of each subnet and an appropriate template name for the subnet.**

   b. **Individually assign a different template to any host that is an exception to its subnet's assigned template.**

      Use the details provided by your system administrator, then choose the appropriate template name from the menu. See Table 2-6 on page 30 for host types that are recognized, and Table 2-7 on page 30 for their associated templates.

6. **Close the Tnrhdb database by selecting File > Exit when you are done.** The Database Manager does error checking and notifies the kernel cache of any changes.

7. **Close the `/etc/hosts` file if you used it for copying IP addresses.**

Summary:

The `tnrhdb` database should have an IP address and template name for:

- the NIS+ root master (that is, this host)
- every NIS+ client that will be in the Trusted Solaris 2.5 domain, or its subnet fallback mechanism <*nnn.nnn.nnn*.0>
- every defaultrouter
- every other workstation that the domain can communicate with, or a fallback address for its subnet.

▼ 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.

Overview

- Create a staging area for databases
- Copy and edit staging area files to become NIS+ tables

- Run `nisserver` command in a profile shell
- Run `nispopulate` command in a profile shell
- Run `nisgrpadm` command in a profile shell
- Reboot the workstation
- Update passwords and credentials

▼ To set the stage

Role - root
Label - admin_low
Shell - regular terminal

1. **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 tape, or merely create empty versions of these files, so that the NIS+ tables are all created at once. If you choose not to create these files, you can create them later, but the `nispopulate` command may print out a few warning messages.

```
# cd /etc
# touch bootparams ethers netgroup netmasks timezone
# touch auto_home auto_master
# cp bootparams ethers netgroup netmasks timezone /setup/files
# cp aliases auto_home auto_master /setup/files
# cp group hosts networks protocols rpc services /setup/files
```

Three Trusted Solaris files need to be renamed when copied into the staging area.

```
# cp passwd.roles /setup/files/passwd
# cp shadow.roles /setup/files/shadow
#
# cd /etc/security/tsol
#
# cp tsoluser.roles /setup/files/tsoluser
# cp tsolprof tnrhdb tnrhtp /setup/files
```

3. Check that all the files are now in your staging area; there are 20.

```
# cd /setup/files
# ls | wc -l
20
```

4. Edit the `hosts` file in your staging area.

a. Change the permissions on the file.

```
# chmod u+w /setup/files/hosts
```

Role - root
Label - admin_low
Action - Admin Editor

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

The file already contains the NIS+ root master (that is, this host's address) and its defaultrouter(s).

i. Add every workstation that will be in the Trusted Solaris 2.5 domain.
There is no fallback 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.

ii. **Add every other workstation that the domain can communicate with.**

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

5. **Modify other files in your staging area as necessary.**

Caution – Do not modify the files: `tsolprof`, `tsoluser`, `passwd`, or `shadow`. You will modify these using the Solstice_Apps tools, User Manager and Profile Manager.

There is enough information in your staging area to convert your host to a NIS+ master and then use the Solstice_Apps tools to further configure your system. However, if you are restoring a former NIS+ domain from files, you may want to merge some of your saved files with those in the staging area at this time.

Caution – If you choose to edit 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

Role - root
Label - admin_low
Shell - profile shell

1. **Set up your NIS+ domain name and root master using a profile shell with all privileges.**
   For fuller descriptions of NIS+ setup and administration, see

   - *NIS+ and DNS Setup and Configuration Guide* and
   - *NIS+ and FNS Administration Guide*

   a. **Check that you are in a profile shell.**

```
# clist
```

   b. **If you are not in a profile shell, open one.**

```
# pfsh
```

2. **Enter the** `nisserver` **command**

```
# PATH=$PATH:/usr/lib/nis; export PATH
# nisserver -r -d fully-qualified-domain-name.
```

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

3. **Answer the prompts (y, y, *your-root-password*).**
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.**

```
# nispopulate -F -p /setup/files
```

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

7. **Add the Trusted Solaris roles and system administrators to the NIS+ admin group.**

```
# nisgrpadm -a admin admin secadmin
```

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

8. **Load any additional NIS+ tables you may have backed up.**
Procedures vary depending on the format of the backup and on what types of NIS+ tables they are.

Refer to the *NIS+ and DNS Setup and Configuration Guide* for details of how to load your tables.

▼ Set up DNS (Optional)

For detailed information about DNS, see the *Federated Naming Service Guide.*

If you are using DNS to contact hosts outside of your domain, you must:

Role - root
Label - admin_low
Action - Set DNS Servers

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.

The file looks something like:

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

b. Write the file and exit the editor.

Role - root
Label - admin_low
Action - Name Server Switch

2. Edit the `hosts` entry in the `/etc/nsswitch.conf` file to use DNS.

a. Change the `hosts` entry to:

```
~
#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
~
```

b. Write the file and exit the editor.

▼ Set Device Policy on Additional Network Interfaces

Note – Skip this procedure if the workstation has only one network interface.

The security administrator ensures that every interface is protected with a device policy. The install team protects the interfaces before booting the workstation into multiuser mode.

For more information, read the man page `device_policy(4TSOL)`.

▼ Determine the network interfaces

Role - root
Label - admin_low
Shell - profile shell

1. **Since you have not created an `/etc/hostname.`*`interface`* entry for every interface, use the `prtconf` command.**

```
# prtconf | grep instance
…   le, instance #0
    qe2, instance #0
    qe3, instance #0
…
```

▼ Create the network interface files

Role - root
Label - admin_low
Action - Admin Editor

1. **Open a file named `/etc/`*`hostname.interface`* in the Admin Editor.**
   a. **Double-click the Admin Editor action.**
   b. **Enter the name of the file, such as `/etc/hostname.qe2`.**
2. **In the file, enter the hostname associated with the interface, such as `grebe-118`.**
3. **Repeat Step a, Step b, and Step 2 for every interface.**

▼ Set device policy on secondary network interfaces

1. **Determine the *driver_name*:*minor_name* of each interface using the command** `ls -l /dev/`*`interface_name`*`*`**, as in:**

```
# ls -l /dev/qe*
```

2. **Find the last component of the result.**

```
lrwxrwxrwx   1 root     root          28 Jun  5  1996 /dev/qe
-> ../devices/pseudo/clone@0:qe
```

   The word after the last slash is the *driver_name*; the word after the colon is the *minor_name*. Here, *driver_name:minor_name* would be `clone:qe`.

3. **Open the `/etc/security/tsol/device_policy` file in the Admin Editor.**
   Follow the procedure in "Create the network interface files" on page 89.

4. **Find an entry for `clone:le`.**

5. **Copy and paste the entry.**

6. **Change *driver_name*:*minor_name* in the copied entry to the *driver_name*:*minor_name* of the interface.**
   For example,

```
clone:le        \
        data_mac_policy=DR_MAC_ANY,DW_MAC_ANY       \
        open_priv=sys_net_config

clone:qe        \
        data_mac_policy=DR_MAC_ANY,DW_MAC_ANY       \
        open_priv=sys_net_config
```

Caution – A network interface *must* have the `sys_net_config` privilege.

7. **Create an entry for every unique *driver_name*:*minor_name* combination on the workstation.**

8. **Close the Admin Editor.**

▼ Reboot the workstation

1. **Right click the CDE front panel.**
2. **Select Shut Down from the menu.**
3. **Confirm that you want to shut down the machine.**
4. **Enter** `boot` **at the** `ok` **prompt or** `b` **at the** `>` **prompt:**

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

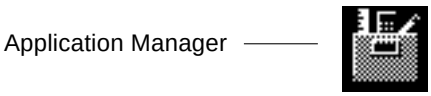
```
Type b (boot), c (continue), or n (new command mode)
> b
```

▼ Update Role Credentials and Passwords

The passwords and credentials of the roles admin, secadmin, and oper must be updated in the new NIS+ domain using the User Manager.

Role - root
Label - admin_low
Tool - User Manager

1. **Log in as install and assume the root role.**
   Follow the procedure in "To log on and assume a role" on page 71.
2. **Open the Application Manager by clicking once with the mouse on the Application Manager icon on the Front Panel.**



3. **Double-click the Solstice_Apps icon, then double-click the User Manager icon.**


Solstice Apps


User Manager

4. **Click OK in the User Manager: Load dialog to use the NIS+ Naming Service and to see all users and roles.**

Trusted Solaris administrative roles and their IDs are listed in the window. These were created from the `tsoluser` file when you ran the `nispopulate` command in "To set up NIS+ with databases from the staging area" on page 86.

5. **Select `oper` from the list of users and press the Return key.**
6. **Click the Password... button to give the role a new password.**
   a. **Press the Password button labeled No password - - setuid only, and select Type In ....**
   b. **Enter a password of no more than eight characters in the Set Password dialog box.**
   c. **Press the Tab key.**
   d. **Re-enter the password and press Return.**
7. **Set other password information for the account.**
   a. **Select the value for Change by.**
   `Type in` means the role types in a password when prompted to change it; `Choose from list` means the password generator generates a list of passwords for the role to choose from.
   b. **Make sure that the value of Status is Open.**
   c. **Make sure that the Cred Table Setup box is checked.**
8. **Exit the Password dialog and save the information.**
   a. **Click OK.**
   b. **Click Done.**
9. **Execute Step 5 through Step 8 for the admin and secadmin roles.**

▼ To customize idle time

By default, the workstation will be in lockscreen mode 5 minutes after a role is not using a workspace. Where site security policy requires a change, modify the idle characteristics for each role.

Role - root
Label - admin_low
Tool - User Manager

1. **Still in User Manager, double-click the role admin.**
2. **Press the Idle button labeled 5 mins.**

3. **Choose a setting in keeping with your site security policy.**
   The options to lock the screen or to log the role out; different time lengths are possible.
4. **Click OK, then Done.**
5. **Update the Idle characteristics for the secadmin and oper roles.**
6. **Close the User Manager by selecting File > Exit when you are done.**

▼ Set up Home Directories

If this workstation is the home directory server:

♦ **Go to "Share Home Directories" on page 93.**

If this workstation is *not* the home directory server, configure the home directory server, reboot it, and mount the home directories before adding users:

▼ Install and configure the home directory server *now*

1. **Go and do:**

Installing a Workstation	*page 56*
Configuring a NIS+ Client: Interactive	*page 105*
Configure the home directory server up through reboot:	
Share Home Directories (on the NIS+ client)	*page 112*
Boot the Workstation (boot the NIS+ client)	*page 113*
Mount Home Directories (on the NIS+ master)	*page 112*

2. **Then, create the first three users on the NIS+ master.**
   Continue with "Add Users to Administer the System" on page 95.

▼ Share Home Directories

Perform this procedure only if the workstation is the home directory server.

Role - root
Label - admin_low
Action- Share Filesystems

1. **Invoke the Share Filesystems action from the System_Admin folder in the Application Manager.**

The Share Filesystems action opens the `/etc/dfs/dfstab` file.

2. **Enter the file system to be shared, and any relevant options.**
For example:

```
share   -F nfs -d "home dirs" /export/home
```

3. **Save the file and close the editor.**

Role - root
Label - admin_low
Shell - regular ter minal

4. **In a terminal, check that the nfs server is running.**

```
# showmount -e
showmount: grebe: RPC: Program not registered
```

5. **If the nfs server is not running, start it.**

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

6. **Check that the home directories are shared.**

```
# showmount -e
export list for grebe:
/export/home (everyone)
```

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

▼ Add Users to Administer the System

Users in the roles of `secadmin` and `admin` will administer the system. The roles already exist. However, users who can assume those roles do not yet exist. Therefore, the role `root` creates at least two users, one per role, and assigns each of them an administrative role. For a detailed description of adding a new user, please see *Trusted Solaris Administrator's Procedures*.

Note – Where site security policy permits, you can choose to create one user who can assume more than one administrative role.

Prerequisite

- The home directory server is either in communication with the NIS+ root master, or it *is* the NIS+ root master.

Overview

- Create one to three users
- Assign the roles `secadmin`, `admin`, and `root`
- Verify that the users can log in and assume their role(s)

▼ To create a user

On the NIS+ master, if you are not in the role root, see "Assume the root Role" on page 71 for details of how to assume the role.

Role - root
Label - admin_low
Tool - User Manager

1. **Open the Application Manager, Solstice_Apps, and then the User Manager (NIS+ Naming Service).**

   See "Update Role Credentials and Passwords" on page 91 for the details of opening the User Manager.

2. **Select Edit > Add.**

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

3. **Create a user who can assume the role secadmin.**
   See Table 5-1 for the information to enter for a user. Read the *Comments* column for guidance. See the *Trusted Solaris Administration Overview* for the details of the User Manager interface.

Note – When creating a user, click to have the User Manager create the (multilevel) home directories, but do not use AutoHome.

Table 5-1 User Account Characteristics

Dialog	Account Characteristic	Comments
Identity	**User name**	
	User ID	(1001 or higher)
	Primary groups	10
	Secondary groups	
	Comment	No proprietary info here.
	Login shell	
	User Type	Normal
Password	**Password generation method**	Assign a password
	Change dates, expiration dates, warnings	
	Change by Type in or Choose from list	
	Status	Open
	Cred Table Setup	Yes, leave it checked. ✓
Home	**Create home directory**	Yes, a multilevel home directory will be created.
	Home directory pathname	*/ mount_path / username*
	Server	*local server*
	Skeleton path	
	Default permissions on home directory	
	Mail server	
	Cred?	Yes, leave it checked. ✓
	AutoHome setup	*NO;* leave it unchecked.
Labels	**Clearance**	*not* ADMIN_HIGH
	Minimum Sensitivity Label	*not* ADMIN_LOW
	Label View	

Table 5-1 User Account Characteristics

	SL visibility **IL visibility**	If your site is a no-label site, choose Hide.
Roles	**Can assume role**	secadmin
Profiles	**Can use profile**	Enable Login, All...
Idle	**Lockscreen or logout** **Time**	

4. **Create another user, one who can assume the administrative role admin.**
5. **Create a third user to assume the role root.**

These three users should each have at least the following profiles:

- Enable Login – user can enable logins after a workstation reboot
- All - user can run basic commands, such as `ls`

After checking your site security policy, you may want to add the profile:

- Convenient Authorizations – user can enable logins, modify cron jobs, print PostScript files, print without labels, remotely log in, and set application search path (CDE)

6. **Close the User Manager.**

See the *Trusted Solaris Administrator's Procedures* manual for how to set up regular users. Setting up users is a two-role, trusted procedure. *The install team should not set up regular users.*

▼ Verify that Users and Administrative Roles Work

1. **Log out.**
   a. **Press the right mouse button on the workspace background and select Log out...from the Workspace Menu, or click the EXIT icon on the Front Panel.**
   b. **When prompted, confirm that you want to log out.**
2. **Log in as a user assigned the role admin.**
   a. **Enter the user name and press the Return key.**

b. **Enter the password and press the Return key.**
The Enable Logins dialog is displayed.

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 profile (see "Profiles" in Table 5-1). To fix, give the user the Enable Login profile, or have someone else log in and enable logins.

c. **Press the Return key to accept the Enable Logins defaults.**

d. **Read the first screen.**
It contains system messages.
In a multilevel system, it offers you the option of restricting the session to a single label.

e. **Click OK to dismiss the dialog.**
The label builder dialog is displayed.

In a no-label or one-label system, it describes your session label.
In a multilabel system, it describes your session clearance.

f. **Click OK to dismiss the label builder dialog.**

You are in a CDE session with four workspaces. The workspace sensitivity label (SL) is your minimum SL, as set up in User Manager.

3. **Assume the role admin from the Trusted Path menu.**
A new workspace named admin at the label admin_low is created for the role.

4. **Open the User Manager.**

5. **Select a user, and press the Return key.**
The dialog boxes that you are not authorized to change are grayed out.

6. **Verify that the user assigned the role secadmin can**

   a. **Log in.**

   b. **Assume the role.**

   c. **Open the User Manager.**

   d. **Select a user, and press the Return key.**

7. **Verify that the user assigned the role root can log in and assume the role.**

a. **Shut down the workstation if you plan to disable auditing (see "To disable auditing" on page 99 for the procedure).**

b. **Log in as a user who can assume the role secadmin if you plan to configure auditing.**

▼ Set up Auditing

If your site security requirements do not include auditing, disable it and go to "Mount Unlabeled File Systems (Optional)" on page 100.

▼ To disable auditing

Role - root
Label - admin_low
Shell - profile shell

1. **Log out using the Shut Down selection from the TP menu, and reboot in single user mode:**

```
Type b (boot), c (continue), or n (new command mode)
> n
PROM password: PROMpassword

> boot -s
```

2. **At the prompt, enter the root password:**

```
Type Ctrl-d to proceed with normal startup,
(or give root password for system maintenance):

rootpassword
```

3. **To disable auditing, open a profile shell, execute the** `bsmunconv(1MTSOL)` **script on the command line, and enter** `y` **when prompted:**

```
# pfsh
# /etc/security/bsmunconv
    This script disables the Basic Security Module (BSM).
    Shall we continue the reversion to a non-BSM system now? [y/n]
y
```

4. **Exit into multiuser mode with auditing disabled:**

```
# exit
```

▼ To configure auditing

Role - secadmin
Label - admin_low
Various tools

- **Use the audit worksheets and the procedures in the** *Trusted Solaris Audit Administration* **manual to configure auditing at your site.**

Note – 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 103.

▼ Mount Unlabeled File Systems (Optional)

You can mount file systems from machines that do not recognize labels for use by the Trusted Solaris 2.5 network. You set the mount to a single label. The following example of mounting an unlabeled host at a single label depends on your having modified the `tnrhtp` file as described in "To edit the tnrhtp database (optional)" on page 80.

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

Role - secadmin
Label - admin_low
Action- Set Mount Attributes

1. **Log in as a user who can assume the role secadmin and assume the role.**
2. **Edit the file** `/etc/security/tsol/vfstab_adjunct` **using the Set Mount Attributes action in the System_Admin folder.**

3. **Copy the template entry, and modify it for the file system to be protected.**

For example, Figure 5-2 shows a `vfstab_adjunct` entry for an unlabeled, remote file system, `/cpublic`, being mounted at the label Confidential ([c]) on a Trusted Solaris 2.5 network.

```
#       Modified template.
#
/cpublic; \
acc_acl=; \
def_acl=; \
mode=; \
attr_flg=; \
gid=; \
uid=; \
ilabel=; \
slabel=C; \
forced=; \
audit_psa=;
#
```

Figure 5-2 Modified `vfstab_adjunct` Entry

Every file in the `/cpublic` file system is read at the label Confidential.

Note – This template mounts an unlabeled file system at Confidential when the `tnrhtp` defines a host type `unlab_conf` as being at the Confidential label. See "To edit the tnrhtp database (optional)" on page 80. To create mount points, see "Create Mount Points".

▼ Create Mount Points

Role - admin
Label - admin_low
Shell - profile shell

1. Create mount points for file systems to be mounted.

```
# mkdir /cpublic
```

Role - admin
Label - admin_low
Action- Set Mount Points

2. **Add the file systems to be mounted to the file `/etc/vfstab` using the Set Mount Points action.**

The following is a sample entry:

```
chincoteague:/cpublic -       /cpublic nfs     -       yes     bg,intr
```

▼ Export Shared Directories

Role - admin
Label - admin_low
Action- Share Filesystems

1. **Log in as a user assigned the role admin and assume the role.**
2. **Invoke the Share Filesystems action, and enter the file system to be exported with any relevant options.**

The following is a sample entry:

```
    share -F nfs -o ro,anon=0 -d "Network Tools" /export/tools
```

The file is saved as `/etc/dfs/dfstab`. The Share Filesystems action does not run the `share(1M)` command.

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

Role - admin
Label - admin_high
Shell - profile shell

3. **To share the file system, either reboot by choosing Shutdown from the TP menu, or start the NFS server from an admin_high profile shell:**

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

Role - admin
Label - admin_low
Shell - profile shell

4. **Run the** `shareall(1M)` **command to share all files in the** `dfstab` **file.**

```
# unshareall
# shareall
```

▼ Copy Configuration Files for Distribution to Clients

Role - root
Label - admin_low
Shell - profile shell

1. **Create a directory named** `tmp` **that cannot be deleted between reboots.**
   Create it in an `/export` subdirectory, such as `/export/tmp`.

```
# mkdir /export/tmp
```

2. **Copy your modified label_encodings file to the** `/export/tmp` **directory.**

```
# cd /etc/security/tsol
# cp label_encodings /export/tmp
```

3. **If you modified other files, copy them to the** `/export/tmp` **directory.**
   For example, a site using DNS and auditing might copy the following files:

```
# cd /etc/security
# cp audit_control /export/tmp
# cp audit_user /export/tmp
# cp audit_startup /export/tmp
# cd /etc
# cp resolv.conf /export/tmp
```

4. **Allocate the tape or diskette device.**
   Follow the procedure in “To allocate a device” on page 75.

5. **Run the** `tar(1TSOL)` **command to copy the contents of the** `/export/tmp` **directory to tape or to diskette.**

a. To copy to tape

```
# cd /export/tmp
# ls
audit_control audit_startup audit_user label_encodings
resolv.conf tnrhtp
# tar cv \
audit_control audit_startup audit_user \
label_encodings resolv.conf tnrhtp
```

b. To copy to diskette

```
# cd /export/tmp
# tar cvf /dev/diskette \
audit_control audit_startup audit_user \
label_encodings resolv.conf tnrhtp
```

c. To eject a diskette

```
# eject
```

6. **Remove the tape or diskette.**

7. **Deallocate the tape or diskette device.**
   Follow the procedure in "To deallocate a device" on page 77.

▼ Delete the User `install`

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

Role - admin
Label - admin_low
Tool - User Manager

♦ **In the role admin, follow the procedure in "Delete the User install" on page 68.**

Configuring a NIS+ Client: Interactive 6

This chapter provides procedures to configure the NIS+ clients at your site interactively, after you have configured the NIS+ root master.

Who Does What

Trusted Solaris software is designed to be installed and configured by two people with distinct responsibilities. Once users who can assume Trusted Solaris roles have been created, and the workstation is rebooted, the software enforces two-role task division. If two-person installation is not a site security requirement, assigning the two administrative roles, secadmin and admin, to one person enables that person to configure both security and system information.

Role - root
Label - admin_low
Shell - profile shell

A box to the left of a configuration procedure, like the one shown here, is used to indicate the role, label, and tool to be used for the procedure. There is a box to the left of procedures where the software enforces role division. There can be more than one box in a procedure when more than one role, tool, or label is required to complete the task.

6

Configuring a NIS+ Client

Configuring a NIS+ client is similar to configuring the NIS+ root master, except that configuration details the client receives from the NIS+ master do not have to be repeated.

Overview – To configure a newly installed NIS+ client:

▼ Log on and Protect the Workstation

Role - root
Label - admin_low
Shell - profile shell

♦ **Follow the procedures in "Assume the root Role" on page 71, in "Open a Profile Shell" on page 72", and in "Protect the Workstation" on page 73.**

▼ Copy Configuration Files from Tape or Diskette

Role - root
Label - admin_low
Shell - profile shell

1. **Copy the files from the tape or diskette of the NIS+ master's configuration files directory to a temporary directory.**
   You made the tape or diskette in section "Copy Configuration Files for Distribution to Clients" on page 103.

Role - root
Label - admin_low
Tool - Device Manager

a. Allocate the appropriate device.
Follow the procedure in "To allocate a device" on page 75.

b. For a tape, use the following `tar(1TSOL)` command:

```
# pwd
/export/tmp
# tar xv
```

c. For a diskette, use the following `tar` command:

```
# tar xvf /dev/diskette
```

2. Remove the tape or diskette and deallocate the device.
Follow the procedure in "To deallocate a device" on page 77.

▼ Copy the NIS+ Master `label_encodings` File

The `label_encodings` file on the client machine must be identical to the one on the NIS+ master. If you are *sure* it is identical, you may skip this step.

Role - root
Label - admin_low
Shell - regular terminal

1. Copy the NIS+ master's `label_encodings` file to the `/etc/security/tsol` directory.

a. Rename the client's `label_encodings` file.

```
# cd /etc/security/tsol
# mv label_encodings label_encodings.orig
```

b. Copy the `/export/tmp/label_encodings` file to `/etc/security/tsol`.

```
# cd /etc/security/tsol
# cp /export/tmp/label_encodings label_encodings
```

2. Check the syntax of the file; follow Step 3 on page 76 in Chapter 5, "Configuring the NIS+ Root Master".

3. **Check the file's label and file permissions.**

   If you are not sure what the appropriate permissions are,

   a. **Verify the file permissions on the NIS+ root master.**

   b. **Then, follow the procedure in "To check a file's label and permissions".**

▼ To check a file's label and permissions

Role - root
Label - admin_low
Shell - profile shell

1. **If a copied file's label is not admin_low[admin_low], set the label and check that it is set correctly.**

```
# setlabel "admin_low[admin_low]" /etc/security/tsol/label_encodings
# getlabel /etc/security/tsol/label_encodings
    label_encodings:  ADMIN_LOW [ADMIN_LOW]
```

2. **Check that the file is owned by user root, group sys, with permissions 0644 (-rw-r--r--).**

```
# ls -l /etc/security/tsol/label_encodings
```

3. **If the file permissions are incorrect, fix them.**

```
# chmod 0644 /etc/security/tsol/label_encodings
# chown root /etc/security/tsol/label_encodings
# chgrp sys  /etc/security/tsol/label_encodings
```

4. **Recheck that the file is owned by user root, group sys, with permissions 0644 (-rw-r--r--).**

```
# ls -l /etc/security/tsol/label_encodings
    -rw-r--r--   1 root   sys    8286 Apr 10 10:20 label_encodings
```

▼ Create and Modify Network Files

1. **Determine the appropriate defaultrouter for the client.**

Table 6-1 Client Defaultrouter Entry

	Client on same subnet	Client on different subnet
NIS+ master has 1 network interface	Enter same defaultrouter as NIS+ master's	Enter defaultrouter for the subnet
NIS+ master has >1 network interface	Enter NIS+ master's other network interface	

Role - root
Label - admin_low
Action - Set Default Routes

2. **Set the defaultrouter for the client.**
   Follow the procedure in "Set Default Routes" on page 78.

Role - root
Label - admin_low
Tool - Database Manager

3. **Add at least two entries to the client's local `hosts` database:**
   a. **Enter the client's defaultrouter.**
   b. **Enter the NIS+ root master.**
      Follow the procedure in "Add the Defaultrouter to the Local Hosts Database" on page 79, and add the NIS+ master, too.

Role - root
Label - admin_low
Action- Set DNS Servers

4. **Enter the DNS servers in `resolv.conf` if your site uses DNS.**
   Follow the procedure in "Set up DNS (Optional)" on page 88.

▼ Edit the `tnrhtp` Database (optional)

You need to do this step only if you assigned a template name for the NIS+ root master that is *not* one of the names supplied by the Trusted Solaris installation program, that is, not one of `tsol`, `tsol_1`, or `tsol_2`.

Note – The `tnrhtp(4TSOL)` template definition and name for the NIS+ master must be identical on the client and master when you run the `nisclient(1M)` command.

Role - root
Label - admin_low
Tool - Database Manager

- **Follow the procedure "To edit the tnrhtp database (optional)" on page 80, substituting your NIS+ master's template name and definition for the one in the procedure.**

▼ Edit the `tnrhdb` Database

Role - root
Label - admin_low
Tool - Database Manager

1. **Enter the IP address and template name (`tsol`) of the subnet into the `tnrhdb(4TSOL)` database.**
   For example, enter a subnet address, such as `129.150.110.0`, and `tsol`. Follow the procedure in "To edit the tnrhdb database" on page 82.
2. **Enter the IP address and host type of the defaultrouter(s).**
   A client with one defaultrouter would have three entries in its `tnrhdb`:
   i. the client and its host type (`tsol`),
   ii. the NIS+ master and its host type (`tsol`) [or its subnet fallback IP address and `tsol`], and
   iii. the defaultrouter and its host type.
3. **Exit the Database Manager.**
   The Database Manager informs the kernel of the network change.

▼ Verify Communication with the NIS+ Master

Role - root
Label - admin_low
Shell - profile shell

1. **Check to see that you can `ping` the NIS+ master.**

```
# ping your-master
```

2. **Check to see that you can `rup` the NIS+ master.**

```
# rup your-master
```

If the `rup(1)` command succeeds, you may proceed. If it fails, debug your network setup until the `rup` command succeeds.

Summary

These NIS+ client files must be compatible with the NIS+ master files:

- /etc/security/tsol/label_encodings
- /etc/security/tsol/tnrhtp

The client's local tnrhdb(4TSOL) 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 defaultrouters, and the client.

In addition, the client's address and name, the NIS+ master's name and address, and the defaultrouter(s)' name and address must be in the local hosts database.

▼ Set up NIS+ Name Services

Note – Skip this step if the client was installed over the network.

Role - root
Label - admin_low
Shell - profile shell

1. **Run the** nisclient(1M) **command in a profile shell.**

```
# /usr/lib/nis/nisclient -i -d fully-qualified-domain. -h master
```

   There is a period after the domain name.

2. **Answer the** nisclient **prompts (y, (*your-master's-ip-address*), nisplus, *your-rootpassword*).**
   You can ignore diagnostics printing out that certain files and directories cannot be located. The files and directories will be created.

▼ Set up DNS

Role - root
Label - admin_low
Action - Set DNS Servers

If you are using DNS to contact hosts outside of your domain, or if you have altered the nsswitch.conf file on the NIS+ master,

♦ **Follow the procedure "Set up DNS (Optional)" on page 88.**

▼ Set up Home Directories

♦ **Do *one* of the following two procedures.**
If this client is the home directory server, "Share Home Directories".
If this client is not the home directory server, "Mount Home Directories".

▼ Share Home Directories

Role - root
Label - admin_low
Action- Share Filesystems

1. **In the role `root`, follow the procedure in "Share Home Directories" on page 93.**
2. **Continue with "Boot the Workstation" on page 113.**
   The rest of the configuration can be done by users who assume administrative roles.

   If you have not yet added users who can assume administrative roles:
3. **Go to the NIS+ root master and continue with "Add Users to Administer the System" on page 95.**

▼ Mount Home Directories

Role - root
Label - admin_low
Action- Set Mount Points

1. **Use the Set Mount Points action to add the file systems to be mounted to the file `/etc/vfstab`.**
   a. **Open the Application Manager from the Front Panel.**
   b. **Double-click the System_Admin folder.**
   c. **Double-click the Set Mount Points action.**
   For example, the `grebe:/export/home` file system will be mounted every time the workstation is booted.

```
grebe:/export/home - /export/home nfs  -  yes    bg,intr,soft
```

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

Role - admin
Label - admin_low
Shell - profile shell

2. **Create the mount point and mount the home directories.**

```
# mkdir -p /export/home
# mount /export/home
```

▼ Set Device Policy on Secondary Network Interfaces

Note – Ignore this procedure if the workstation has only one network interface.

- **Follow the procedure "Set Device Policy on Additional Network Interfaces" on page 89.**

▼ Boot the Workstation

- **Follow the procedure in "Reboot the workstation" on page 91.**

▼ Log in as a User

1. **Log on to the workstation as a user assigned the role secadmin.**

   a. **Enter your user name and press the Return key.**

   b. **Enter your password and press the Return key.**
   The Enable Logins dialog is displayed.

   c. **Press the Return key and read the first screen.**
   It contains system messages.
   In a multilevel system, it offers you the option of restricting the session to a single label.

   d. **Click OK to dismiss the dialog.**
   The label builder dialog is displayed.

   In a no-label or one-label system, it describes your session label.
   In a multilabel system, it describes your session clearance.

   e. **Press the Return key or click OK to dismiss the label builder dialog.**

You are in a CDE session with four workspaces. The workspace sensitivity label (SL) is your minimum SL, as set up in User Manager.

2. **Assume the role secadmin from the Trusted Path menu.**
   A new workspace named admin at the label admin_low is created for the role.

6

▼ Set up Auditing

If your site security requirements do not include auditing, disable it and go to "Mount Unlabeled File Systems (Optional)".

- To disable auditing, follow the procedure in "To disable auditing" on page 99.

Role - secadmin
Label - admin_low
Various tools

♦ **Use the audit worksheets and the procedures in the** *Trusted Solaris Audit Administration* **manual to configure auditing on each workstation.**

Note – To ensure that every workstation and user is audited identically, copy the NIS+ root master's `/etc/security/audit*` configuration files to each workstation (see "Copy Configuration Files from Tape or Diskette" on page 106) and add the correct `dir:` entries. The Audit Control action in the System_Admin folder enables the security administrator to edit the `audit_control` file's `dir:` entries.

▼ Mount Unlabeled File Systems (Optional)

Role - secadmin
Label - admin_low
Action- Set Mount Attributes

♦ **Log in as a user who can assume the role secadmin and follow the procedure in "Mount Unlabeled File Systems (Optional)" on page 100.**

▼ Delete the User `install`

Role - admin
Label - admin_low
Tool - User Manager

♦ **In the role admin, follow the procedure in "Delete the User install" on page 68.**

Preparing to Install Trusted Solaris Over a Network

A typical way to install Trusted Solaris software is to use the installation program to copy the Trusted Solaris CD to the workstation's disk. However, it is uncommon at most sites for every workstation to have its own local CD-ROM drive.

About Installing Trusted Solaris Over a Network

When a workstation does not have a local CDROM drive, you can perform a *network installation*. Network installation means that you install software over the network—from a workstation with the Trusted Solaris CD image on its hard drive to a workstation without a CDROM drive.

Overview – To set up network installation:

Create an Install Server	*page 122*
Create a Trusted Solaris Information Server	*page 124*
Set the Default Date and Time	*page 128*
Add Client Information for a Network Install	*page 129*
Create a Boot Server on a Subnet	*page 136*
Check Device Policy on Secondary Network Interfaces	*page 137*
Reboot the Workstation	*page 137*

7

Servers Required for Network Installation

As shown in Figure 7-1, workstations that install Trusted Solaris software over the network require:

- *Name server (NIS+ root master)* – A workstation that manages a distributed network database (for Trusted Solaris, this is NIS+) containing information about users and hosts on the network.
- *Install server* – A networked workstation with the Trusted Solaris CD image that provides installation services for other workstations.

Note – The install server and NIS+ root master may be the same or separate workstations. For best results, create a separate install server.

- *Trusted Solaris Configuration server* – A networked workstation with the Trusted Solaris configuration values for workstations being installed. Optional for most installations; required for custom JumpStart.
- *Boot server* – A workstation that contains pointers to platform, timezone, and Trusted Solaris configuration values for every workstation to be installed. The install server is often the boot server. Pointers to custom JumpStart installations also are kept on the boot server.

As shown in Figure 7-1, diskless clients that boot Trusted Solaris software over the network also require:

- *OS server* – A workstation that provides Trusted Solaris operating environment software including services and file systems. For diskless clients, OS servers provide the root (/), `/usr`, and swap file systems.

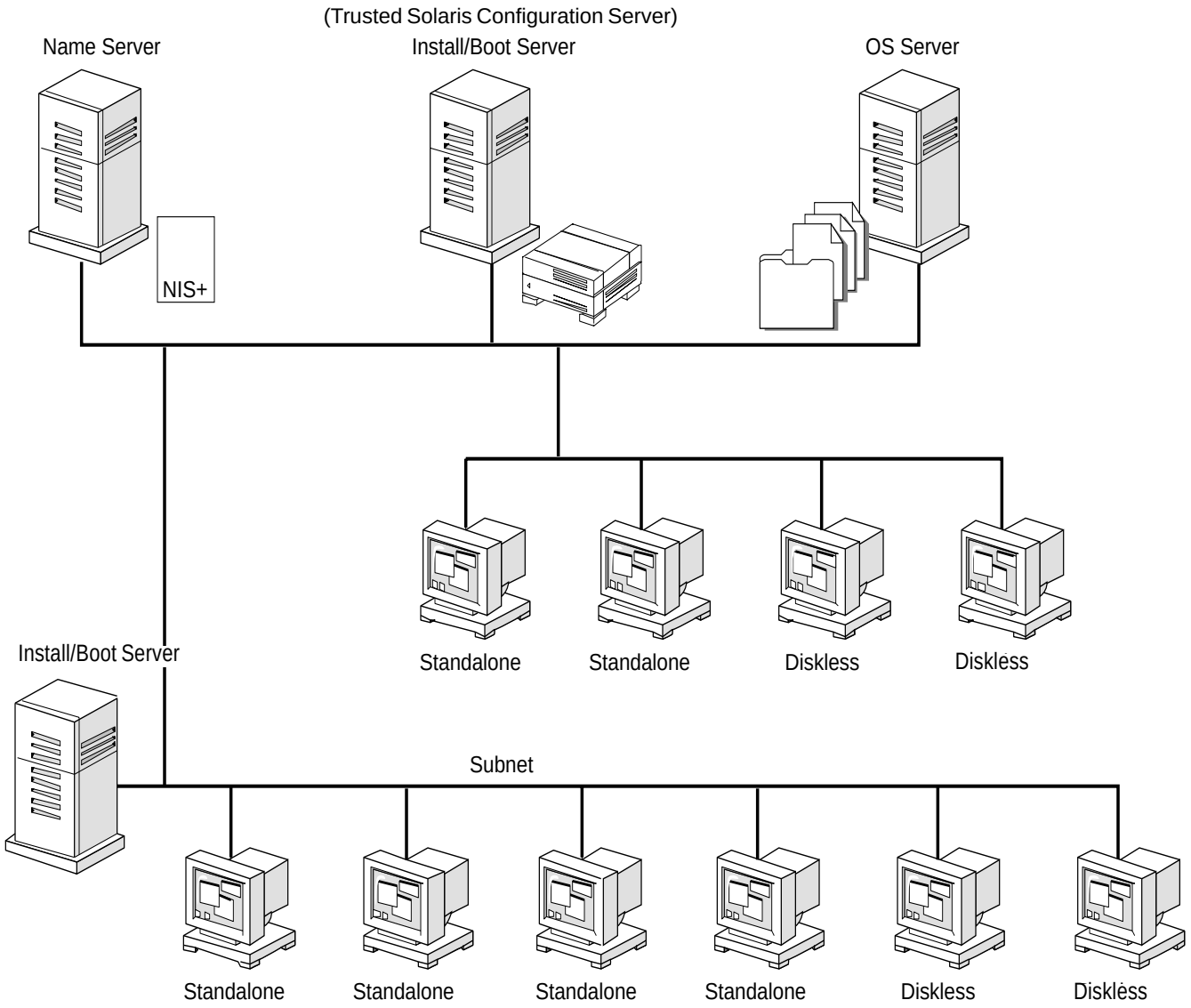


Figure 7-1 Network Installation Servers

7

Setting up Network Installation

To set up your site to install Trusted Solaris software over the network with little user intervention requires the following procedures:

1. **Before configuring servers for network installation, finish the procedure:**

Edit the Trusted Network Files	*page 80*

   Result: The NIS+ root master has the IP address and name of every workstation to be installed in its `hosts` file and their IP address and host type in its `tnrhdb`.

2. **Copy the Trusted Solaris CD image to an install server:**

Create an Install Server	*page 122*

   Result: The Trusted Solaris 2.5 image and booting software is available for network install.

3. **Copy Trusted Solaris configuration information to a server:**

Create a Trusted Solaris Information Server	*page 124*

   Result: The Trusted Solaris 2.5 configuration values are available for network install.

4. **Add client information, such as timezone, platform group, and Trusted Solaris configuration values:**

Add Client Information for a Network Install	*page 129*

   Result: The Trusted Solaris 2.5 installation program system identification questions can be answered without user interaction, including Trusted Solaris configuration values.

5. **Create a boot server for any subnets:**

Create a Boot Server on a Subnet	*page 136*

Result: Clients on the boot server's subnet can be installed from the install server, and get important client information from the boot server.

6. **Check that any secondary network interfaces are configured:**

Check Device Policy on Secondary Network Interfaces *page 137*

Result: Secondary network interfaces are configured for Trusted Solaris policy.

To set up your site to install Trusted Solaris software on workstations over the network with no user intervention, you add JumpStart information:

Preparing Custom JumpStart Installations *page 139*

7

Commands You Should Know About

Table 7-1 shows commands available when setting up network installations.

Table 7-1 Network Installation Commands

Program	Description
`setup_install_server`	A script that copies all or part of the Trusted Solaris CD onto a server's local disk. This enables you to perform network installations from the install server's disk. See the `setup_install_server(1M)` man page for more information.
`add_install_client`	A script that adds client information to a boot server, and adds a pointer to Trusted Solaris configuration information. See the man page `add_install_client(1M)` for details.
Host Manager	A graphical user interface that is available from the Solstice_Apps folder. You can use Host Manager to specify client information for network installation.
`mount`	A command that shows mounted file systems, including the Trusted Solaris CD file system. See the `mount(1MTSOL)` page for more information.
`uname -m`	A command for determining a workstation's platform group (for example, sun4m). This information is required during network installation. See the `uname(1)`man page for more information.
`reset`	A command for resetting the terminal settings and display. It is sometimes useful to use `reset` before booting. Or, if you boot and see a series of error messages about I/O interrupts, press the L1 or STOP and A keys at the same time, and then enter `reset` at the `ok` or > PROM prompt.
`banner`	A command for displaying workstation information, such as model name, Ethernet address, or memory installed. Available only from the `ok` or > PROM prompt.

Files You Should Know About

Table 7-2 shows the `bootparams` database entry and the files that are used to supply label encodings and Trusted Solaris configuration values when installing Trusted Solaris software on a network.

- These files are *recommended* for unscripted network installation, because they reduce the amount of interaction and reduce errors.
- These files are *required* for scripted (Custom JumpStart) network installation.

Table 7-2 Trusted Solaris Network Installation Files

File	Description
`bootparams.org_dir` NIS+ table or *boot_server:*`/etc/bootparams` or `bootparams` local database	The `bootparams` database has been modified for Trusted Solaris installation. It contains an entry, tsol_config=*server:/directory* that is configurable by the system administrator. The entry points to '*server:/directory*, a directory you created and populated with two files.
server:/directory / config_data	The file `config_data` contains Trusted Solaris configuration values that you are otherwise prompted for. You create and edit the file.
server:/directory / label_encodings	Your customized `label_encodings` file is in the directory pointed to by the `tsol_config` entry in the `bootparams` database. New workstations copy the `label_encodings` file from here.

Note – There can be only one `bootparams` database on a subnet. More than one (for example, two workstations where each has a local bootparams database) results in unpredictable behavior.

▼ Create an Install Server

To install workstations over the network, you must have an install server — a workstation with Trusted Solaris software copied to its local disk.

A workstation configured as a NIS+ client can be made into an install server. It must have a local CDROM drive.

Prerequisites:

Installing a Workstation	*page 55*
Configuring a NIS+ Client: Interactive	*page 105*

1. **Log on as a user who can assume the role `root`, and assume the role.**

Role - root
Label - admin_low
Tool - Device Manager

2. **Allocate the CDROM drive and insert the Trusted Solaris CD.**
   Follow the procedure in "To allocate a device" on page 75. The device should be allocated at the label admin_low.

3. **Launch a terminal and open a profile shell with all privileges.**
   Follow the procedure "To get all privileges in a profile shell" on page 123.

Role - root
Label - admin_low
Shell - profile shell
Privileges - all

4. **Mount the Trusted Solaris CD and change the directory to the mounted CD.**

```
# mkdir /cdrom
# mount -F hsfs -o ro /dev/dsk/c0t6d0s0 /cdrom
# cd /cdrom
```

5. **Use the `setup_install_server` command to copy the contents of the Trusted Solaris CD to the install server's local disk.**

```
# ./setup_install_server install_dir_path
```

In this command,

install_dir_path	Specifies the directory where the Trusted Solaris CD image will be copied. You can substitute any directory path.

For example, the following command copies the Trusted Solaris CD image from the Trusted Solaris CD to the `/export/install/ts2.5_sparc` directory on the local disk:

```
./setup_install_server /export/install/ts2.5_sparc
```

The copying takes approximately 30 minutes, depending on the speed of your CDROM drive.

Note – The `setup_install_server` command indicates if there is not enough disk space for the Trusted Solaris CD image. Use the `df -kl` command to determine available disk space.

Role - root
Label - admin_low
Tool - Device Manager

6. **Deallocate the drive and remove the CDROM.**
   Follow the procedure in "To deallocate a device" on page 77.

   Result: The workstation now has the Trusted Solaris CD image on its local disk.

Role - root
Label - admin_low
Shell - profile shell

7. **Exit the privileged profile shell.**
   Follow the procedure in "To exit a profile shell that has all privileges" on page 124.

▼ To get all privileges in a profile shell

Role - root
Label - admin_low
Shell - profile shell
Privileges = all

- **Open a profile shell, and enter a shell command (`sh`, `ksh`, `csh`) in the profile shell.**

```
# pfsh
# sh
# ppriv
pid: all
```

The role root now has all privileges. This is useful for parts of network installation.

Note – The `clist` command is not recognized in a child shell of the profile shell.

▼ To exit a profile shell that has all privileges

♦ **Enter the `exit` command in the privileged profile shell.**

```
# exit
# ppriv
pid: none
# clist
…
list of commands
…
```

You are still in a profile shell. A second call to `exit` returns you to a regular terminal.

♦ **Continue with "Create a Trusted Solaris Information Server".**

▼ Create a Trusted Solaris Information Server

Trusted Solaris label configuration information and the `label_encodings` file for the site can be loaded onto clients automatically during network installation. This simplifies keeping the workstations' label configurations identical.

Note – This procedure is optional for network install, but required for custom JumpStart.

Overview –

- Creating a *server:tsolconfig_dir_path* directory for Trusted Solaris configuration values
- Creating and placing the file `config_data` in *server:tsolconfig_dir_path*
- Copying the `/etc/security/tsol/label_encodings` file from the NIS+ root master to *server:tsolconfig_dir_path*
- Checking the file permissions and labels on *server:tsolconfig_dir_path* and its files

▼ **Set up** *server:tsolconfig_dir_path*

Role - root
Label - admin_low
Shell - regular terminal

1. **Log on to the** *tsolconfig_dir_path* **workstation as a user who can assume the role** `root` **and assume the role.**
   If there is room on the install server, use the install server.

2. **Create and go to the directory.**
   For example,

```
heron# mkdir /export/install/tsolfiles
heron# cd /export/install/tsolfiles
```

3. **Copy the** `label_encodings` **file from** `/etc/security/tsol`**.**
   For example,

```
heron# cp /etc/security/tsol/label_encodings .
```

Role - secadmin
Label - admin_low
Action - Admin Editor

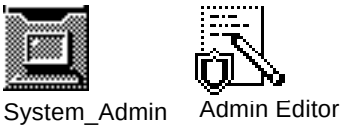
4. **On the** *tsolconfig_dir_path* **workstation, assume the role** `secadmin`**, or log out and have a user who can assume the role** `secadmin` **log on.**
   Admin Editor

5. **In the role** `secadmin`**, use the Admin Editor to create a file named** `config_data` **and enter the Trusted Solaris label configuration settings.**

   a. **Click the Application Manager on the Front Panel.**

Application Manager

   b. **Double-click the System_Admin icon, then double-clickthe Admin Editor icon and enter the file name** `/export/install/tsolfiles/config_data`**.**



c. In the editor, enter Trusted Solaris configuration settings.
For example, the format and the defaults for the Trusted Solaris configuration settings are:

```
multiple_user_sl=yes
enable_il=yes
enable_il_floating=yes
reset_il_on_exec=yes
hide_upgraded_names=no
```

d. Save the file and exit the editor.

Role - secadmin
Label - admin_low
Shell - profile shell

6. Ensure that the *tsolconfig_dir_path* directory and its files have the appropriate protections.

```
$ cd /
$ ls -l /export
```

7. Correct any file protection problems.
For example,

```
$ cd /export/install
$ chmod 0755 tsolfiles
$ chmod 0444 tsolfiles/*
$ chown -R root tsolfiles
$ chgrp -R sys tsolfiles
```

▼ Share *server:tsolconfig_dir_path*

Role - admin
Label - admin_low
Action- Share Filesystems

1. Log in as a user who can assume the role `admin` and assume it.

2. Invoke the Share Filesystems action from the System_Admin folder in the Application Manager.

The Share Filesystems action opens the `/etc/dfs/dfstab` file.

3. **Enter the file system to be shared and any relevant options.**
   For example:

```
share   -F nfs -o ro,anon=0 -d "tsolconfig dir" /export/install/tsolfiles
```

4. **Save the file and close the editor.**

▼ Check that the directory can be shared

Role - admin
Label - admin_low
Shell - profile shell

1. **In the admin role, open a terminal and share the directory.**

```
# share /export/install/tsolfiles
```

2. **If the nfs server is not running:**

```
# showmount -e
showmount: grebe: RPC: Program not registered
```

3. **Start it.**

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

4. **Check that the directory is shared.**

```
# showmount -e
export list for heron:
/export/install/ts2.5_sparc (everyone)
/export/install/tsolfiles   (everyone)
```

Result: Trusted Solaris configuration values are ready for network install.

5. **Continue with “Set the Default Date and Time”.**

▼ Set the Default Date and Time

Note – This procedure is optional for network install, but required for custom JumpStart.

1. **Log on to a Trusted Solaris workstation as a user who can assume the role `admin`, and assume the role.**

Role - admin
Label - admin_low
Tool - Database Manager

2. **Open the Hosts database in the Database Manager using the NIS+ naming service.**

3. **Select the NIS+ root master and press the Return key.**

4. **Add `timehost` as a value of the NIS+ root master's Aliases field.**
   The entry will look like:

   `NIS+_master_host_name` *`IP_address`* `loghost timehost`

5. **Exit the database.**

Result: The date and time will be automatically set during install.

6. **Continue with "Add Client Information for a Network Install".**

▼ Add Client Information for a Network Install

Once you have an install server set up, you then provide basic system information about the workstations (hosts) that you are going to install. You add the Trusted Solaris configuration information to the bootparams database.

You have a choice of two places to enter the information:

- In the NIS+ tables for the network

  From where: You can do this from any workstation.

  How:

Add hosts information to the NIS+ tables	*page 129*
Add bootparams information to the NIS+ tables	*page 131*

  Use this method to have the NIS+ name service provide the client information. This is the most efficient method.

- In the install server's local files

  From where: You can do this from any workstation by remotely logging in to the install server.

  How:

Add host information using the add_install_client command	*page 133*

  Use this method if you have scripts that run the `add_install_client` command for your clients.

  How:

Add host and bootparams information to local databases	*page 135*

  Use this method to keep the network administration information local.

▼ Add hosts information to the NIS+ tables

1. **On the install server, log on as a user who can assume the role `admin`, and assume the role.**

Role - admin
Label - admin_low
Tool - Host Manager

2. **Launch the Host Manager from the Solstice_Apps folder. Select NIS+ for the naming service and click OK.**

3. **If the workstation already exists, select it in the Host Manager main window, choose Edit > Convert > Standalone.**

4. **To add a workstation to be remotely installed, in the Host Manager main window, choose Edit > Add.**

5. **In each entry, enable remote install, complete all fields up to the Boot Server, and click the OK button.**

Table 7-3 Adding Host Information to Host Manager

Entry	Value
Host Name	
IP Address	
Ethernet Address	
System Type	
Timezone Region	
Timezone	
Remote Install	✔ **Enable Remote Install**
Install Server	*install_server_name (entered for you)*
Set Path	`/export/install/ts2.5_sparc`
OS release	*Choose client's platform group and software cluster*
Boot Server	*boot_server_name (if separate server)*
	path to boot file
Profile Server	*IGNORE*

6. **If the Ethernet address field was not filled in, choose the workstation, choose Edit > Modify, and enter the Ethernet address.**

7. **Choose File > Save Changes.**
   The window prints “All changes successful” when finished.
8. **Repeat for all hosts to be installed over the network.**
9. **Exit the Host Manager.**
10. **Continue with “Add bootparams information to the NIS+ tables”.**

▼ Add bootparams information to the NIS+ tables

Follow this procedure to place the pointer to Trusted Solaris configuration values in the `bootparams` NIS+ table.

Note – This procedure is optional for network install, but required for custom JumpStart. If you do not supply the Trusted Solaris files, the install will pause to prompt you for the files.

Role - admin
Label - admin_low
Shell- Database Manager

1. **On the install server, launch the Database Manager.**

   a. **Choose NIS+ for the Naming Service, select Bootparams, and press Return.**
2. **Select a workstation that has not been installed, and choose Edit > Modify.**
3. **Add the keyword=value pair for Trusted Solaris configuration files to the beginning of the entry.**

```
tsol_config=server:tsolconfig_dir_path
```

In this entry,

`tsol_config` Is the Trusted Solaris configuration keyword

server:tsolconfig_dir_path — *server* is the host name of the workstation that contains the Trusted Solaris configuration directory. *tsolconfig_dir_path* is the absolute path name of the directory that contains the Trusted Solaris configuration files.

4. **Make sure to leave a blank after the entry, before the next entry.**

Note – Use the scrollbar to view the entire `bootparams` entry.

For example, the following `bootparams` entry for the workstation `wren` contains a `tsol_config` keyword that points the server to the `/export/install/tsolfiles` directory on `heron`:

```
tsol_config=heron:/export/install/tsolfiles
root=heron:/export/install/ts2.5_sparc/export/exec/kvm/
sparc.TrustedSolaris_2.5
install=heron:/export/install/ts2.5_sparc boottype=:st
```

The install server can now install all hosts. Each workstation will receive essential Trusted Solaris configuration information automatically during installation.

▼ Reboot the Install Server

Between creating the install server and installing clients across the network, you must reboot the server.

1. **Reboot the workstation.**
   Follow the procedure “Reboot the workstation” on page 91.

   Result: The `rpc.tbootparamd` (Trusted bootparams daemon) can now start.

2. **Go to**
   - “Create a Boot Server on a Subnet” on page 136 if you have Trusted Solaris subnets to install.
   - “Check Device Policy on Secondary Network Interfaces” on page 137 if you have additional network interfaces on the install server.

- Otherwise, you can start network installation. Follow the procedure in Chapter 3, “Installing a Workstation”.

▼ Add Client Information Locally

If you choose to add client information locally rather than use the NIS+ tables, use one of the following methods. Do not use either method if you have set up the install server using the NIS+ tables.

▼ Add host information using the `add_install_client` command

Note – If you added hosts and bootparams to NIS+ tables, do not add information locally, as this command does.

1. **Log on to the install server as a user who can assume the role `root`.**

Role - root
Label - admin_low
Shell - profile shell
Privileges - all

2. **As `root`, launch a terminal and open a profile shell with all privileges.**

```
# pfsh
# csh
```

3. **Change to the Trusted Solaris boot information directory.**

```
# cd boot_dir_path
```

For example,

`cd /export/install/ts2.5_sparc` (on an install server)

`cd /export/bootdir` (on a boot server)

4. **Run the `add_install_client` command for every client you plan to install over the network.**

```
# ./add_install_client [-e ethernet_address] \
[-T server:tsolconfig_dir_path]\
-s install_server:install_dir_path host_name platform_group
```

In this command,

`-e`	Specifies the ethernet address.
`-T`	Specifies the Trusted Solaris configuration server.
`-s`	Specifies the install server.
server`:`*tsolconfig_dir_path*	*server* is the host name of the workstation that contains the Trusted Solaris configuration directory. *tsolconfig_dir_path* is the absolute path name of the directory that contains the Trusted Solaris configuration files.
install_server`:`*install_dir_path*	*install_server* is the host name of the install server. *install_dir_path* is the absolute path name of the directory that has the copy of the Trusted Solaris CD image.
host_name	Is the host name of the standalone workstation or the server receiving the network installation. The host must be in the NIS+ name service for this command to work.
platform group	Is the platform group (sun4c, sun4m) of the host being installed. (For a detailed list of platform groups, see Appendix D, "Supported Hardware Components".)

For example, issuing the command:

```
./add_install_client -e 8:0:20:17:22:a4 \
-T heron:/export/install/tsolfiles \
-s heron:/export/install/ts2.5_sparc willet sun4m
```

- creates (if necessary) and copies boot information to the boot server's local `bootparams` database.
- creates (if necessary) and copies ethernet information to the boot server's local `ethers` file.
- points to the Trusted Solaris configuration values directory.

- creates (if necessary) and sets up the `/tftpboot` directory on the boot server with an entry for `willet`, whose platform group is sun4m.
- points the client to platform information on the install server's (`heron`'s) file system, `/export/install.ts2.5_sparc`.

Role - root
Label - admin_low
Shell - profile shell

5. **Remove all privileges from the profile shell.**
   Follow the procedure "To exit a profile shell that has all privileges" on page 124.

Result: The client `willet` can be installed over the network.

Task Complete

Network installation is now ready on network servers that have one network interface.

6. **Go to "Reboot the Install Server" on page 132.**

▼ Add host and bootparams information to local databases

Note – Only use this procedure to keep the network information in local files.

Follow this procedure to place the pointer to Trusted Solaris configuration values in the local `bootparams` file.

1. **Follow the procedure "Add hosts information to the NIS+ tables" on page 129, choosing no naming service before loading the `hosts` database.**
2. **Then continue with "Add bootparams information to the NIS+ tables" on page 131, again choosing no naming service before loading the `bootparams` database.**

Task Complete

Network installation is now ready on network servers that have one network interface.

3. **Go to "Reboot the Install Server" on page 132.**

▼ Create a Boot Server on a Subnet

You can install Trusted Solaris software over the network from any install server on the network. However, a workstation using an install server on another subnet *requires* a separate boot server on its own subnet.

Note – If the boot server and the install server are the same workstation, skip this procedure. Setting up the install server has set up the boot server. Go to "Check Device Policy on Secondary Network Interfaces" on page 137.

1. **Follow Step 1 through Step 4 in "Create an Install Server" on page 122.**

2. **Determine your next step based on whether the boot server uses a local CD-ROM drive or an NFS mount of a Trusted Solaris CD image.**

If the Boot Server Uses ...	Then ...
Local CDROM drive	**1)** Insert the Trusted Solaris CD into the drive. **2)** Go to Step 3.
NFS mount of a Trusted Solaris CD image	**1)** `mount -F nfs -o ro` *server_name*`:`*path* `/mnt` where *server_name*`:`*path* is the host name and absolute path to the Trusted Solaris CD image. **2)** `cd /mnt` **3)** Go to Step 3.

Role - root
Label - admin_low
Shell - profile shell
Privileges - all

3. **Use the `setup_install_server` command with the `-b` option to set up a separate boot server for the subnet.**
   The `setup_install_server -b` command copies all supported platform information to the local disk.

```
# ./setup_install_server -b boot_dir_path
```

In this command,

`-b`	Specifies that the workstation will be set up as a boot server.

boot_dir_path — Specifies the directory where the platform information will be copied. You can substitute any directory path.

For example, the following command copies platform information from the mounted Trusted Solaris CD to the `/export/bootdir/ts2.5_sparc` directory on the boot server:

```
./setup_install_server -b /export/bootdir/ts2.5_sparc
```

The workstation is now is partially configured as a boot server.

Role - root
Label - admin_low
Shell - profile shell

4. **Remove all privileges from the profile shell.**
   Follow the procedure "To exit a profile shell that has all privileges" on page 124.
5. **To fully configure the boot server for Trusted Solaris, follow *one* of the procedures:**
   - "Add bootparams information to the NIS+ tables" on page 131, or
   - "Add host information using the add_install_client command" on page 133.

▼ Check Device Policy on Secondary Network Interfaces

Note – Ignore this procedure if the workstation has only one network interface.

For more information, read the man page `device_policy(4TSOL)`.

♦ **Make sure that you have completed "Set Device Policy on Additional Network Interfaces" on page 89.**

▼ Reboot the Workstation

♦ **Follow the procedure in "Reboot the workstation" on page 91.**

The network servers are now ready for network installation of future clients.

Task Complete

Clients will get platform, ethernet, and other sysid information from network files. If a Trusted Solaris configuration server is set up, they will receive a central `label_encodings` file and their label configuration settings will be identical.

♦ **To install over the net, follow the network installation procedure in:**

Installing a Workstation	*page 56*

You will be prompted for information that is not on the subnet's install or boot server, such as how to partition the disks.

Preparing Custom JumpStart Installations 8

Definition: Custom JumpStart Installation

A custom JumpStart installation automatically installs the Trusted Solaris software on a workstation based on an administrator-defined profile. You can create customized profiles for different types of users.

Note – Appendix E, “Sample Custom JumpStart Installation”, provides an example of how a fictitious site is prepared for custom JumpStart installations.

8

Reasons to Choose a Custom JumpStart Installation

You should choose custom JumpStart installations when you have to install Trusted Solaris software on:

- Many hosts.
- Particular groups of hosts.

For example, the following scenario would be ideal for performing custom JumpStart installations:

- You need to install the Trusted Solaris software on 100 new workstations.
- The engineering group owns 70 out of the 100 new workstations, and its workstations must be installed as standalone workstations with the developer software group.
- The analysis group owns 30 out of the 100 new workstations, and its workstations must be installed as standalone clients with the end user software group.

These installations would be time-consuming and tedious if you chose to perform an interactive installation on each workstation.

Trusted Solaris Differences in Custom JumpStart

Administrators experienced in setting up custom JumpStart installation should note the differences between installing Trusted Solaris and installing Solaris 2.5.1 using custom JumpStart.

Trusted Solaris Custom JumpStart Additions

In the Trusted Solaris environment, administrative jobs are performed by a users in administrative roles. Users in the roles admin and root set up custom JumpStart. Also, devices must be allocated and deallocated for use. So,

- You cannot log in as root. 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.
- Before mounting a CDROM or diskette on an installed workstation, the device must be allocated at a particular label. When the medium is removed, the device must be deallocated.

A Trusted Solaris custom JumpStart must load Trusted Solaris configuration values. See “Create a Trusted Solaris Information Server” on page 124 and “Add Client Information for a Network Install” on page 129 in the previous chapter for adding Trusted Solaris configuration values to a network install.

Trusted Solaris Custom JumpStart Limitations

The following custom JumpStart features are not supported by Trusted Solaris:.

- Mounting remote file systems
- Upgrading from a non-Trusted Solaris 2.x operating system
- Using locales other than U.S. English
- Installing the software clusters: `Core` and `Entire Distribution + OEM`

Prerequisites for a Custom JumpStart Installation

A custom JumpStart installation can be done on a networked or non-networked workstation.

The non-networked workstation must have

- A local diskette drive (for the JumpStart information)
- A local CDROM drive (for the Trusted Solaris image).

The networked workstation must be on a subnet with the following servers:

- An install server (for the Trusted Solaris image)
- A Trusted Solaris configuration server (for Trusted Solaris configuration values)
- A boot server (for boot information on a subnet)
- A JumpStart server (for the JumpStart information).

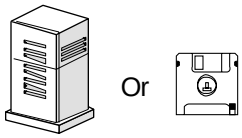
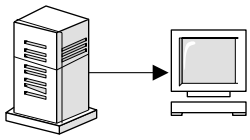
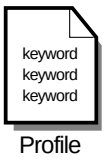
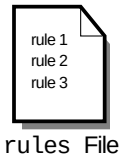
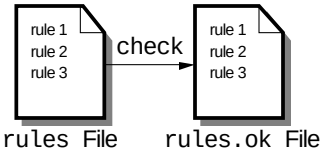
♦ **Follow the procedures to set up the network servers in Chapter 7, “Preparing to Install Trusted Solaris Over a Network”.**

8

Tasks to Set up Custom JumpStart Installations

Table 4-1 shows the tasks that are required to set up custom JumpStart installations.

Table 8-1 Tasks to Prepare for Custom JumpStart Installations

Task		Description
Creating a JumpStart directory on a diskette or on a server		You must create a JumpStart directory to hold the custom JumpStart files. If you are going to use a diskette for custom JumpStart installations, see "Creating a JumpStart Directory on a Diskette" on page 146. If you are going to use a server for custom JumpStart installations, see "Creating a JumpStart Directory on a Server" on page 149.
Enabling all clients to access the JumpStart directory		When you use a server to provide the JumpStart directory, you can enable all clients to access the JumpStart directory. See "Enabling All Systems to Access the JumpStart Directory" on page 151 for detailed information.
Creating profiles		A profile is a text file used as a template by the custom JumpStart installation software. It defines how to install the Trusted Solaris software on a workstation (for example, system type, disk partitioning, software group), and it is named in the `rules` file. See "Creating a Profile" on page 153 for detailed information.
Creating a `rules` file		The `rules` file is 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. See "Creating the rules File" on page 164 for detailed information.
Using `check` to validate the `rules` file		The `rules.ok` file is a generated version of the `rules` file, and it is required by the custom JumpStart installation software to match a workstation to a profile. You *must* use the `check` script to create the `rules.ok` file. See "Using check to Validate the rules File" on page 175 for detailed information.

What Happens During a Custom JumpStart Installation

Figure 8-1 describes what happens after you boot a workstation to perform a custom JumpStart installation.

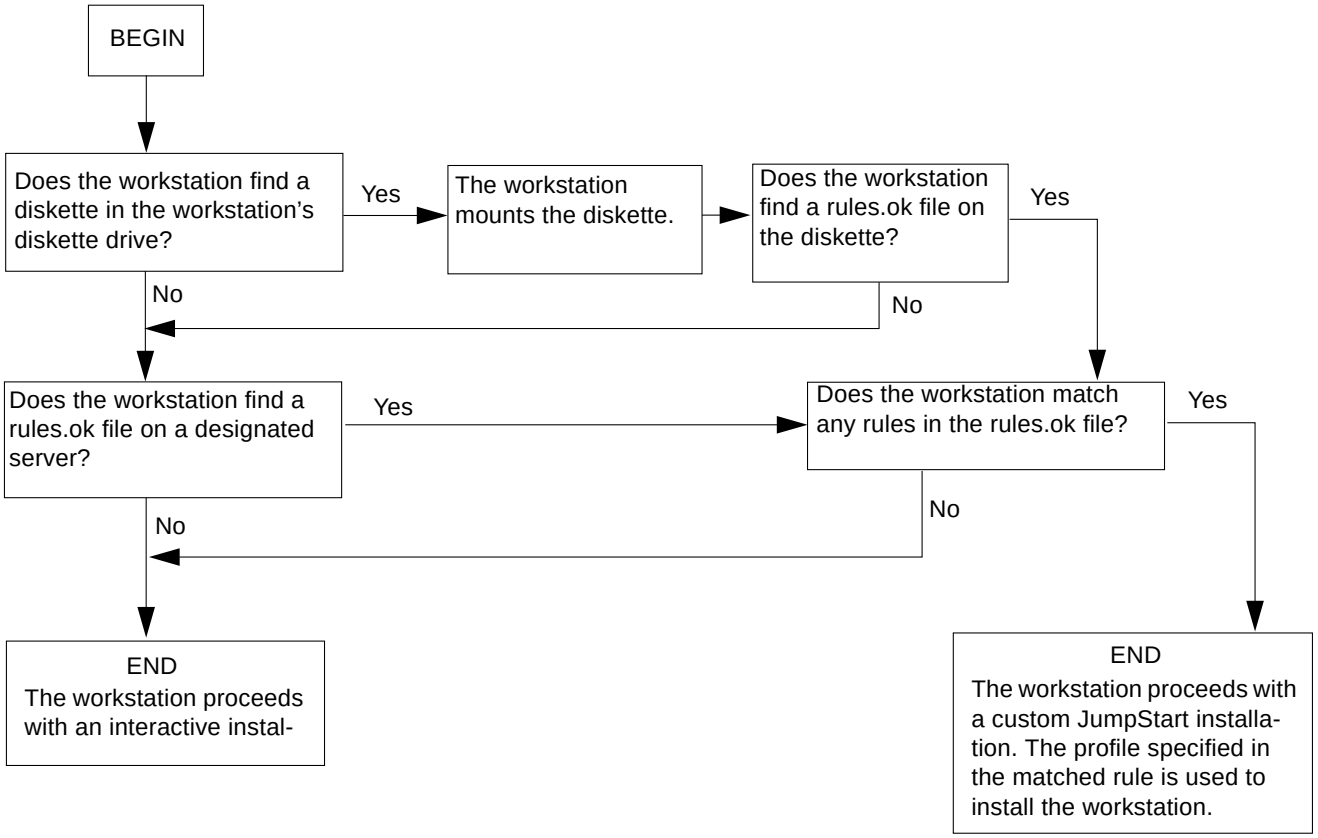


Figure 8-1 What Happens During a Custom JumpStart Installation

Figure 8-2 is an example of how a custom JumpStart installation works on a standalone, non-networked workstation using the workstation's diskette drive.

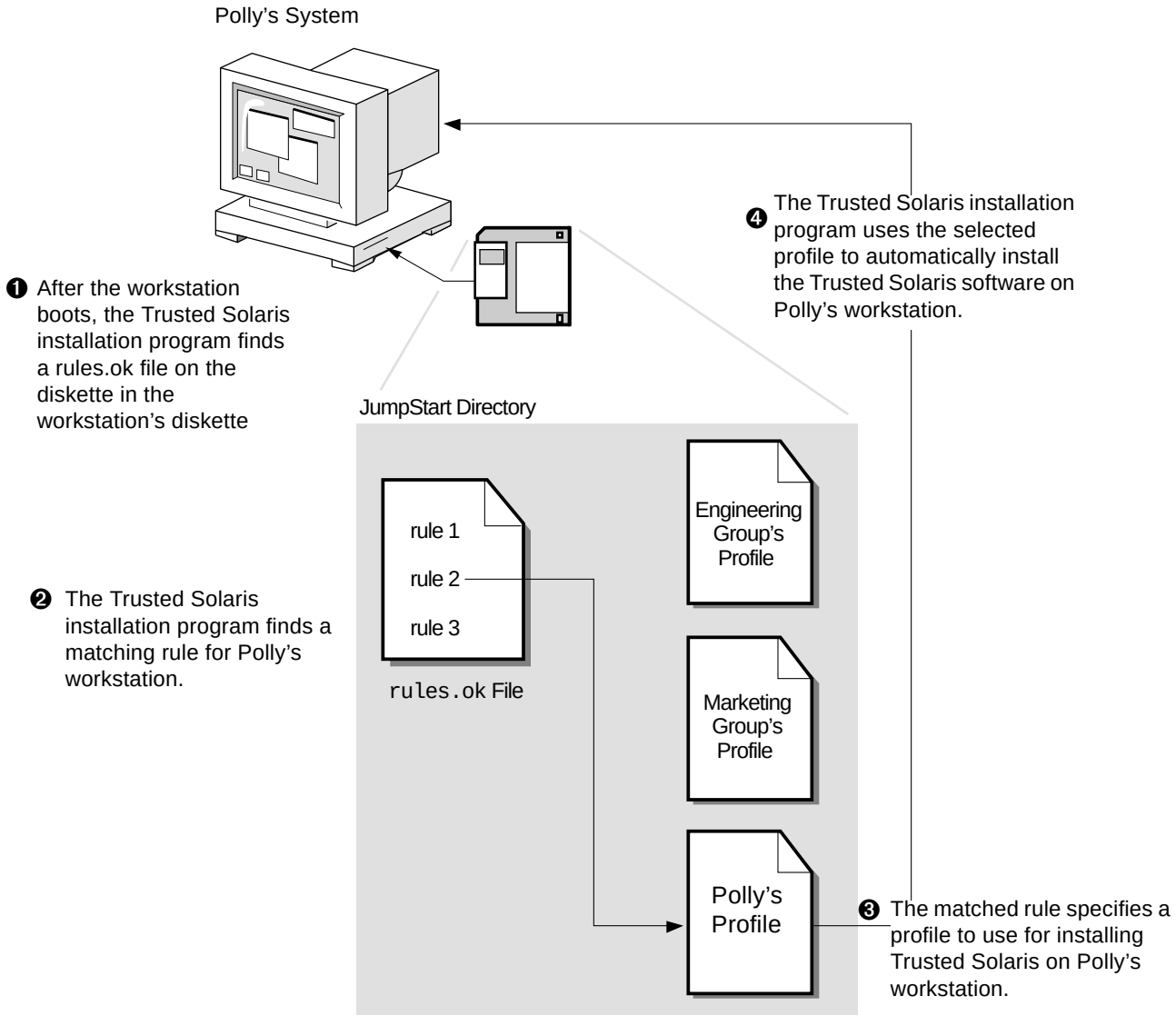


Figure 8-2 How a Custom JumpStart Installation Works: Non-Networked Example

Figure 8-3 is an example of how a custom JumpStart installation works for multiple workstations on a network where different profiles are accessed from a single server.

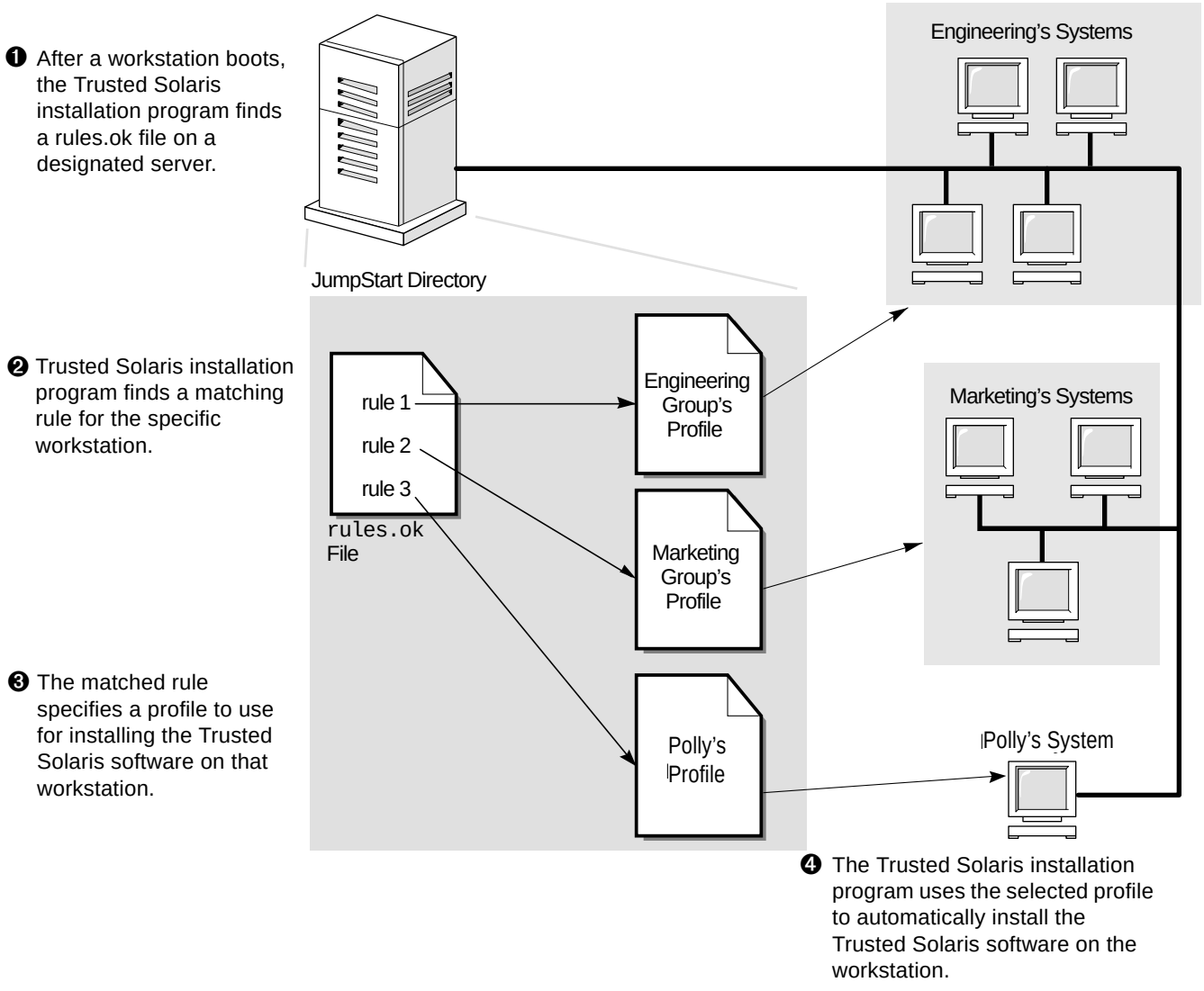


Figure 8-3 How a Custom JumpStart Installation Works: Networked Example

8

Creating a JumpStart Directory on a Diskette

You should use a diskette for a custom JumpStart installation if the workstation:

- Has a diskette drive
- Has a local CDROM drive
- Is *not* connected to a network

When you use a diskette for custom JumpStart installations, the JumpStart directory must be the root directory on the diskette that contains all the essential custom JumpStart installation files (for example, the `rules` file, `rules.ok` file, and profiles). The JumpStart directory should be owned by root and have permissions equal to 755.

Note – Custom JumpStart diskette installation is more limited than network installation. The following information is not available on the diskette, so you will be prompted for it: hostname, name service, Trusted Solaris configuration values, subnet, netmask, timezone, date, and time.

▼ How to Create a JumpStart Directory on a Diskette

Overview – The procedure to create a JumpStart directory on a diskette involves:

- Formatting a diskette (if needed).
- Creating a UFS file system on the diskette (if needed).
- Copying sample custom JumpStart installation files into the diskette's root directory.

Follow this procedure to create a JumpStart directory on a diskette.

1. **Log onto a workstation that has a diskette drive and a CDROM drive and assume the role `root`.**

Role - root
Label - admin_low
Tool - Device Manager

2. **Allocate the diskette drive.**
   Follow the procedure in "To allocate a device" on page 75. The device should be allocated at the label admin_low.

3. **Insert a diskette into the diskette drive.**

4. **If the diskette already has a UFS file system on it, go to Step 8.**
   If the `mount` command fails in Step 8, the diskette does not have a UFS file system on it.

Role - root
Label - admin_low
Shell - profile shell
Privileges - all

5. **Launch a terminal and open a profile shell with all privileges:**

```
# pfsh -c csh
```

6. **Format the diskette:**

```
# fdformat /dev/rdiskette
```

7. **Create a file system on the diskette:**

```
# newfs /dev/rdiskette
```

8. **Create a mount point and mount the diskette:**

```
# mkdir jumpstart_dir_path
# mount -F ufs /dev/diskette jumpstart_dir_path
```

In this command,

jumpstart_dir_path Is the absolute directory path where the diskette is mounted.

For example, the following command would mount a diskette on the `/mnt` directory:

```
mount -F ufs /dev/diskette /jumpstart
```

Note – If the `mount` command fails, go back to Step 6 to format the diskette.

9. **Determine your next step based on where the Trusted Solaris CD image is located.**

If You Want to Use The ...	Then ...
Trusted Solaris CD in the local CDROM drive	**1)** Insert the Trusted Solaris CD into the CDROM drive. **2)** Go to Step 10.
Trusted Solaris CD image on the local disk	**1)** Change the directory to the Trusted Solaris CD image on the local disk. For example: `cd /export/install/ts2.5_sparc` **2)** Go to Step 12.

Role - root
Label - admin_low
Tool - Device Manager

10. **Allocate the CDROM drive.**
Follow the procedure in "To allocate a device" on page 75. The device should be allocated at the label admin_low.

Role - root
Label - admin_low
Shell - profile shell
Privileges - all

11. **Mount the Trusted Solaris CD and change the directory to the mounted CD:**

```
# mount -F hsfs -o ro /dev/dsk/c0t6d0s0 /cdrom
# cd /cdrom
```

12. **Copy the custom JumpStart installation files from the `auto_install_sample` directory on the Trusted Solaris CD into the JumpStart directory (root directory) of the diskette:**

```
# cp -r auto_install_sample/* jumpstart_dir_path
```

Note: *jump_dir_path* is the absolute directory path where the diskette is mounted.

Note – The custom JumpStart installation files must be in the root directory of the diskette.

13. **Deallocate the CDROM drive and the diskette drive.**
Follow the procedure in "To deallocate a device" on page 77.

Task Complete

You have completed creating a JumpStart directory on the diskette. To continue, see "How to Create a Profile" on page 154.

Creating a JumpStart Directory on a Server

If you want to perform custom JumpStart installations by using a server on the network, you must create a JumpStart directory on the server. When you use a server for custom JumpStart installations, the JumpStart directory is a directory on the server that contains all the essential custom JumpStart files (for example, the `rules` file, `rules.ok` file, and profiles). The JumpStart directory should be owned by root and have permissions equal to 755.

▼ How to Create a JumpStart Directory on a Server

Overview – The procedure to create a JumpStart directory on a server involves:

- Creating a directory on the server
- Sharing the directory
- Copying sample custom JumpStart installation files into the directory on the server

Follow this procedure to create a JumpStart directory on a server.

1. **Log on and assume the role `root` on the server where you want the JumpStart directory to reside.**

Role - root
Label - admin_low
Shell - profile shell
Privileges - all

2. **Launch a terminal and open a profile shell with all privileges.**

```
# pfsh -c csh
```

3. **Create the JumpStart directory anywhere on the server:**

```
# mkdir jumpstart_dir_path
```

In this command,

jumpstart_dir_path Is the absolute path of the JumpStart directory.

For example, the following command would create the directory called `jumpstart` in the root file system: `mkdir /jumpstart`

Role - root
Label - admin_low
Action - Share Filesystems

4. Export the directory.

a. Click the Application Manager.

b. Double-click on the System_Admin folder, then double-click on the Share Filesystems action.

c. Add the following entry:

```
share -F nfs -o ro,anon=0 jumpstart_dir_path
```

For example, the following entry would be correct for the example shown in Step 3:

```
share -F nfs -o ro,anon=0 /jumpstart
```

d. Write the file and exit the editor.

Role - root
Label - admin_low
Shell - profile shell
Privileges - all

5. Start the nfs server.

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

6. Share the directory.

```
# unshareall
# shareall
```

7. Determine your next step based on where the Trusted Solaris CD is located.

If You Want to Use The ...	Then ...
Trusted Solaris CD in the local CD-ROM drive	**1)** Insert the Trusted Solaris CD into the CDROM drive. **2)** Go to Step 8.
Trusted Solaris CD image on the local disk	**1)** Change the directory to the Trusted Solaris image on the local disk. For example: `cd /export/install/ts2.5_sparc` **2)** Go to Step 10.

Role - root
Label - admin_low
Tool - Device Manager

8. **Allocate the CDROM drive.**
   Follow the procedure in "To allocate a device" on page 75. The device should be allocated at the label admin_low.

Role - root
Label - admin_low
Shell - profile shell
Privileges - all

9. **Mount the Trusted Solaris CD and change the directory to the mounted CD:**

```
# mount -F hsfs -o ro /dev/dsk/c0t6d0s0 /cdrom
# cd /cdrom
```

10. **Copy the contents of the `auto_install_sample` directory from the Trusted Solaris CD-ROM into the JumpStart directory:**

```
# cp -r auto_install_sample/* jumpstart_dir_path
```

    For example, the following command would copy the `auto_install_sample` directory into the JumpStart directory created in Step 3:

```
cp -r auto_install_sample/* /jumpstart
```

11. **Deallocate the CDROM drive.**
    Follow the procedure in "To deallocate a device" on page 77.

Task Complete

You have completed creating a JumpStart directory on the server. To continue, see "How to Create a Profile" on page 154.

Enabling All Systems to Access the JumpStart Directory

When you create a JumpStart directory on a server, you must make sure workstations can access it during a custom JumpStart installation. There are two ways to do this:

- Using the `-c` option of the `add_install_client` command every time you add a workstation for network installation.

  or

- Enabling all workstations to access the JumpStart directory.

To save you time when adding workstations for network installations, use the following procedure to enable all workstations to access the JumpStart directory from a server.

Note – The following procedure is not necessary if you are using a diskette for the JumpStart directory.

▼ How to Enable All Systems to Access the JumpStart Directory

Overview – The procedure to enable all workstations to access the JumpStart directory from a server involves:

- Editing the `bootparams` database on the boot server

Follow this procedure to enable all workstations to access the JumpStart directory from a server.

1. **On the boot server, log in as a user who can assume the role** `admin`**.**

Role - root
Label - admin_low
Tool - Database Manager

2. **Edit the** `bootparams` **database.**
   a. **Click the Application Manager in the Front Panel.**
   b. **Double-click the Solstice_Apps folder.**
   c. **Double-click the Database Manager.**
   d. **Use the same naming service you used when setting up network install (“Add Client Information for a Network Install” on page 129), and double-click the** `Bootparams` **database.**
3. **For each workstation, add the following entry:**

```
install_config=server:jumpstart_dir_path
```

In this entry,

server	Is the host name of the server where the JumpStart directory is located.
jumpstart_dir_path	Is the absolute path of the JumpStart directory.

For example, the following item in each workstation's bootparams entry would enable the workstation to access the `/jumpstart` directory on the server named `bigbaby`:

```
install_config=bigbaby:/jumpstart
```

Caution – Using this procedure may produce the following error message when booting an install client:
`WARNING: getfile: RPC failed: error 5: (RPC Timed out).`
See page 278 for more details on this error message.

Task Complete

All workstations can now access the JumpStart directory. You no longer need to use the `-c` option of the `add_install_client` command when adding workstations for network installations. . To continue, see "How to Create a Profile" on page 154.

Creating a Profile

A profile is a text file used as a template by the custom JumpStart installation software. It defines how to install the Trusted Solaris software on a workstation (for example, system type, disk partitioning, software group), and it is named in the `rules` file.

A profile consists of one or more profile keywords and their values. Each profile keyword is a command that controls one aspect of how the Trusted Solaris installation program will install the Trusted Solaris software on a workstation. For example, the profile keyword and value

```
system_type   server
```

tells the Trusted Solaris installation program to install the workstation as a server.

Note – If you created the JumpStart directory by using the procedures on page 146 or page 149, example profiles should already be in the JumpStart directory.

Requirements for Profiles

The following are requirements when creating a profile:

- The `install_type` profile keyword is required.
- Only one profile keyword can be on a line.

Recommendations for Trusted Solaris Profiles

Every Trusted Solaris rule should call a finish script. In the script, you can accomplish at least the following two tasks:

- Automatically reboot the workstation.
  See the example in "Rebooting the Workstation with a Finish Script" on page 184.
- For a custom JumpStart diskette installation, install the site's `label_encodings` file in `/etc/security/tsol`.
  See the example in "Adding Files With Finish Scripts" on page 185.

For an example of a rule that calls a finish script, see "Recommendations for Trusted Solaris Rules" on page 164.

▼ How to Create a Profile

Overview – The procedure to create a profile involves:

- Editing a file
- Selecting profile keywords and profile values to define how to install the Trusted Solaris software on a workstation

Follow this procedure to create as many profiles as you need for your site.

Role - secadmin
Label - admin_low
Shell - profile shell

1. **Open a file (the profile) in an editor and give it a descriptive name.**
   You can create a new file or edit one of the sample profiles in the JumpStart directory you created.

   The name of a profile should reflect how it will install the Trusted Solaris software on a workstation (for example, `basic_install`, `eng_profile`, or `mktg_profile`).

2. **Add profile keywords and profile values to the profile.**
   Be aware of these things as you edit the profile:

- "Profile Examples" on page 156 provides some examples of profiles.
- Table 8-2 on page 158 provides the list of valid profile keywords and values.
- You can have as many lines in the profile as necessary to define how to install the Trusted Solaris software on a workstation.
- You can add a comment after the pound sign (#) anywhere on a line. If a line begins with a #, the entire line is a comment line. If a # is specified in the middle of a line, everything after the # is considered a comment. Blank lines are also allowed in a profile.
- The profile keywords and their values *are* case sensitive.
- Profiles should be owned by root and have permissions equal to 644.

3. **Check file permissions by following the procedure "To check a file's label and permissions" on page 108.**

Note – See "Using pfinstall to Test Profiles" on page 188 for detailed information about testing profiles.

Task Complete

This completes the procedure to create a profile. To continue setting up for a custom JumpStart installation, see "How to Create the rules File" on page 165.

8

Profile Examples

The following profile examples describe how you can use different profile keywords and profile values to control how the Trusted Solaris software is installed on a workstation. See Table 8-2 on page 158 for the list of profile keywords and profile values.

```
    # profile keywords      profile values
    # ----------------      -------------------
❶   install_type            initial_install

❷   system_type             standalone

❸   partitioning            default
    filesys                 any 80 swap   # specify size of /swap

❹   cluster                 SUNWCprog
❺   package                 SUNWman delete
    package                 SUNWolman delete
    package                 SUNWxwman delete
    package                 SUNWxwdem add
    package                 SUNWxwdim add
```

❶ This profile keyword is required in every profile.

❷ This profile keyword defines that the workstation will be installed as a standalone workstation.

❸ The file system slices are determined by the software to be installed (`default` value); however, the size of swap is set to 80 Mbytes and it is installed on any disk (`any` value).

❹ The developer software group (`SUNWCprog`) is installed on the workstation.

❺ Because the man pages will be mounted remotely, those packages are selected *not* to be installed on the workstation; however, the packages containing the X Windows demo programs and images are selected to be installed on the workstation.

```
    # profile keywords    profile values
    # ----------------    -------------------
    install_type          initial_install
    system_type           standalone

❶   partitioning          default
    filesys               c0t0d0s0 auto /
    filesys               c0t3d0s1 64 swap
❷   cluster               SUNWCall
```

❶ The file system slices are determined by the software to be installed (`default` value). However, the size of root is based on the selected software (`auto` value) and it is installed on c0t0d0s0, and the size of `swap` is set to 64 Mbytes and it is installed on c0t3d0s1.

❷ The entire distribution software group (`SUNWCall`) is installed on the workstation.

```
    # profile keywords    profile values
    # ----------------    -------------------
    install_type          initial_install
    system_type           standalone

❶   fdisk                 c0t0d0 0x04 delete
❷   fdisk                 c0t0d0 solaris maxfree
❸   cluster               SUNWCall
❹   cluster               SUNWCacc delete
```

❶ All fdisk partitions of type DOSOS16 (04 hexadecimal) are deleted from the c0t0d0 disk.

❷ A Trusted Solaris fdisk partition is created on the largest contiguous free space on the c0t0d0 disk.

❸ The entire distribution software group (`SUNWCall`) is installed on the workstation.

❹ The system accounting utilities (`SUNWCacc`) are selected *not* to be installed on the workstation.

8

Profile Keyword and Profile Value Descriptions

Table 8-2 shows the profile keywords and profile values that you can use in a profile.

Table 8-2 Profile Keyword and Profile Value Descriptions *(1 of 6)*

Profile Keyword	Profile Values and Description
`client_arch`	*karch_value*
	`client_arch` defines that the server will support a different platform group than it uses. If you do not specify `client_arch`, any diskless client must have the same platform group as the server. You must specify `client_arch` once for each platform group. Valid values for *karch_value* are sun4d, sun4c, sun4m, and sun4u. (See Platform Names and Groups on page 247 for a detailed list of the platform names of various workstations.) **Restriction:** `client_arch` can be used only when `system_type` is specified as `server`.
`client_root`	*root_size*
	`client_root` defines the amount of root space (*root_size* in Mbytes) to allocate for each client. If you do not specify `client_root` in a server's profile, the installation software will automatically allocate 15 Mbytes of root space per client. The size of the client root area is used in combination with the `num_clients` keyword to determine how much space to reserve for the `/export/root` file system. **Restriction:** `client_root` can be used only when `system_type` is specified as `server`.
`client_swap`	*swap_size*
	`client_swap` defines the amount of swap space (*swap_size* in Mbytes) to allocate for each diskless client. If you do not specify `client_swap`, 24 Mbytes of swap space is allocated. Example: `client_swap 64` The example defines that each diskless client will have a swap space of 64 Mbytes. **Restriction:** `client_swap` can be used only when `system_type` is specified as `server`.

Table 8-2 Profile Keyword and Profile Value Descriptions *(2 of 6)*

Profile Keyword	Profile Values and Description
`cluster` *(use for software groups)*	*group_name*
	`cluster` designates what software group to add to the workstation. The cluster names for the software groups are: Software Group — *group_name* End user system support — `SUNWCuser` Developer system support — `SUNWCprog` Entire distribution — `SUNWCall` You can specify only one software group in a profile, and it must be specified before other `cluster` and `package` entries. If you do not specify a software group with `cluster`, the end user software group (`SUNWCuser`) is installed on the workstation by default.
`cluster`† *(use for clusters)*	*cluster_name* `[add | delete]`
	`cluster` designates whether a cluster should be added or deleted from the software group that will be installed on the workstation. `add` or `delete` indicates whether the cluster should be added or deleted. If you do not specify `add` or `delete`, the cluster is added by default. *cluster_name* must be in the form `SUNWC`*name*. To view detailed information about clusters and their names, start Admintool on an installed workstation and select Software from the Browse menu.
`dontuse`	*disk_name*
	`dontuse` designates a disk that the Trusted Solaris installation program should *not* use when `partitioning default` is specified. You can specify `dontuse` once for each disk, and *disk_name* must be specified in the form `c`*x*`t`*y*`d`*z* or `c`*y*`d`*z*, for example, `c0t0d0`. By default, the Trusted Solaris installation program uses all the operational disks on the workstation. **Restriction:** You cannot specify the `dontuse` keyword and the `usedisk` keyword in the same profile.

Table 8-2 Profile Keyword and Profile Value Descriptions *(3 of 6)*

Profile Keyword	Profile Values and Description
`filesys` *(use for creating local file systems)*	*slice size* [*file_system*] [*optional_parameters*]
	This instance of `filesys` creates local file systems during the installation. You can specify `filesys` more than once. *slice* - Choose one of the following: • `any` - The Trusted Solaris installation program places the file system on any disk. **Restriction:** `any` cannot be specified when `size` is `existing`, `all`, `free`, *start*:*size*, or `ignore`. • `c`*w*`t`*x*`d`*y*`s`*z* or `c`*x*`d`*y*`s`*z* - The disk slice where the Trusted Solaris installation program places the file system, for example, `c0t0d0s0`. • `rootdisk.s`*n* - The logical name of the disk where the installation program places the root file system. The `s`*n* suffix indicates a specific slice on the disk. *size* - Choose one of the following: • *num* - The size of the file system is set to *num* (in Mbytes). • `existing` - The current size of the existing file system is used. **Note:** When using this value, you can change the name of an existing slice by specifying *file_system* as a different *mount_pt_name*. • `auto` - The size the file system is automatically determined depending on the selected software. • `all` - The specified *slice* uses the entire disk for the file system. When you specify this value, no other file systems can reside on the specified disk. • `free` - The remaining unused space on the disk is used for the file system. **Restriction:** If `free` is used as the value to `filesys`, it must by the last `filesys` entry in a profile. • *start*:*size* - The file system is explicitly partitioned: *start* is the cylinder where the slice begins; *size* is the number of cylinders for the slice.

Table 8-2 Profile Keyword and Profile Value Descriptions *(4 of 6)*

Profile Keyword	Profile Values and Description
`filesys` *(use for creating local file systems)* continued	*slice size* [*file_system*] [*optional_parameters*]
	file_system - You can use this optional value when *slice* is specified as `any` or `cwtxdysz`. If *file_system* is not specified, `unnamed` is set by default, but then you can't specify the *optional_parameters* value. Choose one of the following: • *mount_pt_name* - The file system's mount point name, for example, `/var`. • `swap` - The specified *slice* is used as `swap`. • `overlap` - The specified *slice* is defined as a representation of a disk region (VTOC value is V_BACKUP). By default, slice 2 is an overlap slice that is a representation of the whole disk. **Restriction**: `overlap` can be specified only when *size* is `existing`, `all`, or *start*:*size*. • `unnamed` - The specified *slice* is defined as a raw slice, so *slice* will not have a mount point name. If *file_system* is not specified, `unnamed` is set by default. • `ignore` - The specified *slice* is not used or recognized by the Trusted Solaris installation program. This could be used to ignore a file system on a disk during an installation, so the Trusted Solaris installation program can create a new file system on the same disk with the same name. *optional_parameters* - Choose one of the following: • `preserve` - The file system on the specified *slice* is preserved. **Restriction**: `preserve` can be specified only when *size* is `existing` and *slice* is `cwtxdysz`. • *mount_options* - One or more mount options (`-o` option of the `mount(1MTSOL)` command) that are added to the `/etc/vfstab` entry for the specified *mount_pt_name*. **Note**: If you need to specify more than one mount option, the mount options must be separated by commas and no spaces. For example: `ro,quota`
`install_type`†	`initial_install`
	`install_type` defines the initial installation option. **Restriction**: `install_type` must be the first profile keyword in every profile.
`num_clients`	*client_num*
	When a server is installed, space is allocated for each diskless client's root (`/`) and `swap` file systems. `num_clients` defines the number of diskless clients (*client_num*) that a server will support. If you do not specify `num_clients`, five diskless clients are allocated. **Restriction**: `num_clients` can be used only when `system_type` is specified as `server`.

Table 8-2 Profile Keyword and Profile Value Descriptions *(5 of 6)*

Profile Keyword	Profile Values and Description
`package`†	*package_name* `[add	delete]`
	`package` designates whether a package should be added to or deleted from the software group that will be installed on the workstation. `add` or `delete` indicates whether the package should be added or deleted. If you do not specify `add	delete`, the package is added.  *package_name* must be in the form `SUNW`*name*. Use the `pkginfo -l` command or Admintool (select Software from the Browse menu) on an installed workstation to view detailed information about packages and their names.
`partitioning`	`default	existing	explicit`
	`partitioning` defines how the disks are divided into slices for file systems during the installation. If you do not specify `partitioning`, `default` is set. `default` - The Trusted Solaris installation program selects the disks and creates the file systems on which to install the specified software, except for any file systems specified by the `filesys` keyword. `rootdisk` is selected first; additional disks are used if the specified software does not fit on `rootdisk`. `existing` - The Trusted Solaris installation program uses the existing file systems on the workstation's disks. All file systems except `/`, `/usr`, `/usr/openwin`, `/opt`, and `/var` are preserved. The installation program uses the last mount point field from the file system superblock to determine which file system mount point the slice represents. **Restriction:** When specifying the `filesys` profile keyword with `partitioning existing`, *size* must be `existing`. `explicit` - The Trusted Solaris installation program uses the disks and creates the file systems specified by the `filesys` keywords. If you specify only the root (`/`) file system with the `filesys` keyword, all the Trusted Solaris software will be installed in the root file system. **Restriction:** When you use the `explicit` profile value, you must use the `filesys` profile keyword to specify which disks to use and what file systems to create.
`system_type`	`standalone	server`

Table 8-2 Profile Keyword and Profile Value Descriptions *(6 of 6)*

Profile Keyword	Profile Values and Description
	`system_type` defines the type of workstation being installed. If you do not specify `system_type` in a profile, `standalone` is set by default.
`usedisk`	*disk_name*
	`usedisk` designates a disk that the Trusted Solaris installation program will use when `partitioning default` is specified. You can specify `usedisk` once for each disk, and *disk_name* must be specified in the form `c`*x*`t`*y*`d`*z* or `c`*y*`d`*z*, for example, `c0t0d0`. If you specify the `usedisk` profile keyword in a profile, the Trusted Solaris installation program will only use the disks that you specify with the `usedisk` profile keyword. **Restriction**: You cannot specify the `usedisk` keyword and the `dontuse` keyword in the same profile.

How the Size of Swap Is Determined

If a profile does not explicitly specify the size of swap, the Trusted Solaris installation program determines the maximum size that swap can be, based on the workstation's physical memory. Table 8-3 shows how the maximum size of swap is determined during a custom JumpStart installation.

Table 8-3 How the Maximum Size of Swap Is Determined

Physical Memory (in Mbytes)	Maximum Size of Swap (in Mbytes)
32 - 64	64
64 - 128	64
128 - 512	128
512 >	256

The Trusted Solaris installation program will make the size of swap no more than 20% of the disk where it resides, unless there is free space left on the disk after laying out the other file systems. If free space exists, the Trusted Solaris installation program will allocate the free space to swap up to the maximum size shown in Table 8-3.

Note – Physical memory plus swap space must be a minimum of 64 Mbytes.

Creating the `rules` *File*

The `rules` file is a text file used to create the `rules.ok` file. The `rules` file is a lookup table consisting of one or more rules that define matches between workstation attributes and profiles. For example, the rule

```
karch sun4c - basic_prof -
```

matches a workstation with a sun4c platform name to the `basic_prof` profile, which the Trusted Solaris installation program would use to install the workstation.

Note – If you set up the JumpStart directory by using the procedures on page 146 or page 149, an example `rules` file should already be in the JumpStart directory; the example `rules` file contains documentation and some example rules. If you use the example `rules` file, make sure you comment out the example rules that you will not use.

When Does a System Match a Rule

During a custom JumpStart installation, the Trusted Solaris installation program attempts to match the rules in the `rules.ok` file in order, first rule through the last rule. A rule match occurs when the workstation being installed matches any of the rule values in the rule (as defined in Table 8-5 on page 169). As soon as a workstation matches a rule, the Trusted Solaris installation program stops reading the `rules.ok` file and begins to install the workstation as defined by the matched rule's profile.

Recommendations for Trusted Solaris Rules

Since a workstation installed with custom JumpStart does not automatically reboot, create a rules file whose entries include a finish script that automatically reboots the workstation. An example finish script is in "Rebooting the Workstation with a Finish Script" on page 184. A sample rules file:

```
hostname wren - basic_prof finish.sh
```

matches a workstation whose hostname is `wren` to the `basic_prof` profile, which the Trusted Solaris installation program would use to install the workstation. After installation, the `finish.sh` script would be executed to reboot the workstation.

▼ How to Create the `rules` File

Overview – The procedure to create a `rules` file involves:

- Editing a file
- Selecting rule keywords and rule values for each group of workstations you want to install using custom JumpStart. Any workstations that match the rule keyword and rule value will be installed as specified by the corresponding profile.

Follow this procedure to create a `rules` file.

Role - secadmin
Label - admin_low
Shell - profile shell

1. **Open a file (the `rules` file) in the Admin Editor and name it `rules`.**
   You can create a new file or edit the sample `rules` file provided in the JumpStart directory you created.

2. **Add a rule in the `rules` file for each group of workstations you want to install using custom JumpStart.**
   Be aware of these things as you add rules to the `rules` file:

   - Rule Examples on page 167 provides some examples of rules.
   - Table 8-5 on page 169 provides the list of valid rule keywords and values.
   - The `rules` file must have at least one rule
   - A rule must have at least a rule keyword, a rule value, and a corresponding profile.

   An individual rule in the `rules` file must have the following syntax:

```
[!]rule_keyword rule_value [&& [!]rule_keyword rule_value]...   begin   profile   finish
```

Table 8-4 describes the fields of a rule.

Table 8-4 Field Descriptions of a Rule

Field	Description
!	A symbol used before a rule keyword to indicate negation.
[ ]	A symbol used to indicate an optional expression or field.
...	A symbol used to indicate the preceding expression may be repeated.
rule_keyword	A predefined keyword that describes a general system attribute, such as host name (`hostname`) or memory size (`memsize`). It is used with the `rule` value to match a workstation with the same attribute to a profile. See Table 8-5 on page 169 for the list of `rule` keywords.
rule_value	A value that provides the specific system attribute for the corresponding `rule` keyword. See Table 8-5 on page 169 for the list of `rule` values.
&&	A symbol that must be used to join (logically AND) rule keyword and rule value pairs together in the same rule. During a custom JumpStart installation, a workstation must match every pair in the rule before the rule matches.

Table 8-4 Field Descriptions of a Rule *(Continued)*

Field	Description
begin	A name of an optional Bourne shell script that can be executed before the installation begins. If no begin script exists, you *must* enter a minus sign (-) in this field. All begin scripts must reside in the JumpStart directory. See "Creating Begin Scripts" on page 181 for detailed information on how to create begin scripts.
profile	A name of a text file used as a template that defines how to install Trusted Solaris on a workstation. The information in a profile consists of profile keywords and their corresponding profile values. All profiles must reside in the JumpStart directory. **Note -** There are optional ways to use the profile field, which are described in "Using a Site-Specific Installation Program" on page 196 and "Creating Derived Profiles With Begin Scripts" on page 182.
finish	A name of an optional Bourne shell script that can be executed after the installation completes. If no finish script exists, you *must* enter a minus sign (-) in this field. All finish scripts must reside in the JumpStart directory. See "Creating Finish Scripts" on page 184 for detailed information on how to create finish scripts.

3. **Check file permissions by following the procedure "To check a file's label and permissions" on page 108.**

Task Complete

This completes the procedure to create a `rules` file. To validate the `rules` file, see "How to Use check to Validate the rules File" on page 175.

Rule Examples

The following illustration shows several example rules in a `rules` file. Each line has a rule keyword and a valid value for that keyword. The Trusted Solaris installation program scans the `rules` file from top to bottom. When the

Trusted Solaris installation program matches a rule keyword and value with a known workstation, it installs the Trusted Solaris software specified by the profile listed in the profile field.

```
    # rule keywords and rule valuesbegin script  profile    finish script
    # ---------------------------------------- -------    -------------
❶   hostname eng-1                    -          basic_prof     -
❷   network 192.43.34.0 && !model \
    'SUNW,Sun 4_50'                   -          net_prof       -
❸   model SUNW,SPARCstation-LX        -          lx_prof    complete
❹   network 193.144.2.0 && karch sparcsetup      ultra_prof done
❺   any  -                            -          generic_prof   -
```

❶ This rule matches if the workstation's host name is `eng-1`. The `basic_prof` profile is used to install the Trusted Solaris software on the workstation that matches this rule.

❷ The rule matches if the workstation is on subnet 192.43.34.0 and it is *not* a SPARCstation IPX™ (`SUNW,Sun 4_50`). The `net_prof` profile is used to install the Trusted Solaris software on workstations that match this rule.

❸ The rule matches if the workstation is a SPARCstation LX. The `lx_prof` profile and the `complete` finish script are used to install the Trusted Solaris software on workstations that match this rule. This rule also provides an example of rule wrap, which is defined on page 168.

❹ This rule matches if the workstation is on subnet 193.144.2.0 and the workstation is a Sun Ultra. The `setup` begin script, the `ultra_prof` profile, and the `done` finish script are used to install the Trusted Solaris software on workstations that match this rule.

❺ This rule matches any workstation that did not match the previous rules. The `generic_prof` profile is used to install the Trusted Solaris software on workstations that match this rule. If used, `any` should always be in the last rulerule.

Important Information About the `rules` *File*

The following information is important to know about the `rules` file:

- **Name** - The `rules` file *must* have the file name, `rules`.

- `rules.ok` **file** - The `rules.ok` file is a generated version of the `rules` file, and it is required by the custom JumpStart installation software to match a workstation to a profile. You must run the `check` script to create the `rules.ok` file, and the `rules.ok` file should be owned by root and have permissions equal to 644.
- **Comments** - You can add a comment after the pound sign (#) anywhere on a line. If a line begins with a #, the entire line is a comment line. If a # is specified in the middle of a line, everything after the # is considered a comment. Blank lines are also allowed in the `rules` file.

Note – When creating the `rules.ok` file, the `check` script removes all the comment lines, comments at the end of a rule, and blank lines.

- **Rule wrap** - When a rule spans multiple lines, you can let a rule to wrap to a new line, or you can continue a rule on a new line by using a backslash (\) before the carriage return.
- **Rule fields** - The *rule_value*, *begin*, and *finish* fields must have a valid entry or a minus sign (-) to specify that there is no entry.

Rule Keyword and Rule Value Descriptions

Table 8-5 describes the rule keywords and rule values that you can use in the `rules` file.

Table 8-5 Rule Keyword and *Rule Value* Descriptions *(1 of 5)*

Rule Keyword	Rule Values		Description
`any`	minus sign (-)		Match always succeeds.
`arch`	*processor_type*		Matches a workstation's processor type. The `uname -p` command reports the workstation's processor type.
	platform	*processor_type*	
	SPARC	sparc	
`domainname`	*domain_name*		Matches a workstation's domain name, which controls how a name service determines information. If you have a workstation already installed, the `domainname` command reports the workstation's domain name.

Table 8-5 Rule Keyword and *Rule Value* Descriptions *(2 of 5)*

Rule Keyword	Rule Values	Description
`disksize`	*disk_name size_range* *disk_name* - A disk name in the form `cxtydz`, such as `c0t3d0`, or the special word `rootdisk`. `rootdisk` should be used only when trying to match workstations that contain the factory-installed JumpStart software. `rootdisk` is described on page 174. *size_range* - The size of the disk, which must be specified as a range of Mbytes (*xx-xx*).	Matches a workstation's disk (in Mbytes). Example: `disksize c0t3d0 250-300` The example tries to match a workstation with a `c0t3d0` disk that is between 250 and 300 Mbytes. **Note:** When calculating *size_range*, remember that a Mbyte equals 1,048,576 bytes. A disk may be advertised as a "207 Mbyte" disk, but it may have only 207 million bytes of disk space. The Trusted Solaris installation program will actually view the "207 Mbyte" disk as a 197 Mbyte disk because 207,000,000 / 1,048,576 = 197. So, a "207 Mbyte" disk would not match a *size_range* equal to 200-210.
`hostaddress`	*IP_address*	Matches a workstation's IP address.
`hostname`	*host_name*	Matches a workstation's host name. If you have a workstation already installed, the `uname -n` command reports the host name.
`installed`	*slice version* *slice* - A disk slice name in the form `cwtxdysz`, such as `c0t3d0s5`, or the special words `any` or `rootdisk`. If `any` is used, any disk attached to the workstation attempts to match. `rootdisk` should be used only when trying to match workstations that contain the factory-installed JumpStart software. `rootdisk` is described on page 174. *version* - A version name, such as `Trusted_Solaris_2.5`, or the special word `any`. If `any` is used, any Trusted Solaris or SunOS release is matched.	Matches a disk that has a root file system corresponding to a particular version of Trusted Solaris software. **Note:** Factory-installed JumpStart is not supported by Trusted Solaris software.

Table 8-5 Rule Keyword and *Rule Value* Descriptions *(3 of 5)*

Rule Keyword	Rule Values	Description
`karch`	*platform_group* Valid values are sun4d, sun4c, sun4m, and sun4u. (See Appendix D, "Supported Hardware Components" for a detailed list of platform groups and names.)	Matches a workstation's platform name. If you have a workstation already installed, the `arch -k` command or the `uname -m` command reports the workstation's platform group.
`memsize`	*physical_mem* The value must be a range of Mbytes (*xx-xx*) or a single Mbyte value.	Matches a workstation's physical memory size (in Mbytes). Example: `memsize 32-64` The example tries to match a workstation with a physical memory size between 32 and 64 Mbytes. If you have a workstation already installed, the `prtconf` command (line 2) reports the workstation's physical memory size.

Table 8-5 Rule Keyword and *Rule Value* Descriptions *(4 of 5)*

Rule Keyword	Rule Values		Description
`model`	*model_name*		Matches a workstation's model number, which is workstation-dependent and varies by the manufacturer. The list shown may not be complete. If you have a workstation already installed, the `prtconf` command (line 5) reports the workstation's model number. If you have a workstation already installed, the `uname -i` command reports the workstation's model name. **Note:** If the *model_name* contains spaces, the *model_name* must be inside a pair of single quotes ('). For example: `'SUNW,Sun 4_50'`
	System	*model_name*	
	Sun-4/110	Sun 4_100 Series	
	Sun-4/2*xx*	Sun 4_200 Series	
	SPARCstation 1 (4/60)	Sun 4_60	
	SPARCstation 1+ (4/65)	Sun 4_65	
	SPARCstation SLC™ (4/20)	Sun 4_20	
	SPARCstation IPC (4/40)	SUNW,Sun 4_40	
	SPARCstation ELC™ (4/25)	SUNW,SUN 4_25	
	SPARCstation IPX (4/50)	SUNW,Sun 4_50	
	SPARCstation 2 (4/75)	SUNW,SUN 4_75	
	Sun-4/3*xx*	Sun SPARCsystem 300	
	Sun-4/4*xx*	Sun SPARCsystem 400	
	SPARCserver™ 6*xx*	SUNW,SPARCsystem-600	
	SPARCstation 10	SUNW,SPARCstation-10	
	SPARCclassic™ (4/15)	SUNW,SPARCclassic	
	SPARCstation LX (4/30)	SUNW,SPARCstation-LX	
	SPARCcenter™ 1000	SUNW,SPARCserver-1000	
	SPARCcenter 2000	SUNW,SPARCcenter-2000	
	SPARCstation 10 SX	SUNW,SPARCstation-10,SX	
	SPARCstation 20	SUNW,SPARCstation-20	
	SPARCstation 5	SUNW,SPARCstation-5	
	SPARCstation Voyager	SUNW,S240	
	Sun Ultra™ 1	SUNW,Ultra-1	
	Sun UltraServer 1	SUNW,Ultra-1	

Table 8-5 Rule Keyword and *Rule Value* Descriptions *(5 of 5)*

Rule Keyword	Rule Values	Description
`network`	*network_num*	Matches a workstation's network number, which the Trusted Solaris installation program determines by performing a logical AND between the workstation's IP address and the subnet mask. Example: `network 193.144.2.0` The example would match a workstation with a 193.144.2.8 IP address (if the subnet mask were 255.255.255.0).
`osname`	*Trusted_Solaris_version*	Matches a version of Trusted Solaris already installed on a workstation. *Trusted_Solaris_version* is the version of Trusted Solaris environment installed on the workstation: for example, Trusted_Solaris_2.5.
`totaldisk`	*size_range* The value must be specified as a range of Mbytes (*xx-xx*).	Matches the total disk space on a workstation (in Mbytes). The total disk space includes all the operational disks attached to a workstation. Example: `totaldisk 300-500` The example tries to match a workstation with a total disk space between 300 and 500 Mbytes. **Note:** When calculating *size_range*, remember that a Mbyte equals 1048576 bytes. A disk may be advertised as a "207 Mbyte" disk, but it may have only 207 million bytes of disk space. The Trusted Solaris installation program will actually view the "207 Mbyte" disk as a 197 Mbyte disk because 207000000 / 1048576 = 197. So, a "207 Mbyte" disk would not match a *size_range* equal to 200-210.

How the Installation Program Sets the Value of `rootdisk`

`rootdisk` is the logical name of the disk where the root file system is placed during an installation. During a custom JumpStart installation, the Trusted Solaris installation program sets the value of `rootdisk` (that is, the actual disk it represents) depending on various situations; this is described in Table 8-6.

Table 8-6 How the Trusted Solaris Installation Program Sets the Value of `rootdisk`

Situation	**What Happens**
`rootdisk` has *not* been set and a workstation tries to match the following rule: `disksize rootdisk` *size_range* or `installed rootdisk` *version*	`rootdisk` is set to c0t3d0 *or* the first available disk attached to the workstation. After `rootdisk` is set, the workstation tries to match the rule.
If `rootdisk` has been set and the workstation tries to match the following rule. `disksize rootdisk` *size_range* or `installed rootdisk` *version*	The workstation tries to match the rule.
A workstation tries to match the following rule: `installed` *disk version*	If *disk* is found on the workstation with a root file system that matches the specified *version*, the rule matches and `rootdisk` is set to *disk*.
A workstation tries to match the following rule: `installed any` *version*	If any disk is found on the workstation with a root file system that matches the specified *version*, the rule matches and `rootdisk` is set to the found disk. (If there is more than one disk on the workstation that can match, the workstation will match the first disk that is found.)
`rootdisk` has not been set after a workstation matches a rule.	`rootdisk` is set to c0t3d0 *or* the first available disk attached to the workstation.

For the Trusted Solaris installation program to use the value of `rootdisk`, the following conditions must be true in the profile specified for the workstation:

- Default partitioning is used.
- No slice has been explicitly set for the root file system.

Using `check` *to Validate the* `rules` *File*

Before the `rules` file and profiles can be used, you must run the `check` script to validate that these files are set up correctly. The following table shows what the check script does.

Stage	Description
1	The `rules` file is checked for syntax. `check` makes sure that the rule keywords are legitimate, and the *begin*, *class*, and *finish* fields are specified for each rule (the *begin* and *finish* fields may be a minus sign [-] instead of a file name).
2	If no errors are found in the `rules` file, each profile specified in the rules is checked for syntax.
3	If no errors are found, `check` creates the `rules.ok` file from the `rules` file, removing all comments and blank lines, retaining all the rules, and adding the following comment line to the end: `# version=2 checksum=num`

▼ How to Use `check` to Validate the `rules` File

Overview – The procedure to use `check` to validate the `rules` file involves:

- Making sure the check script resides in the JumpStart directory
- Running the check script

Follow this procedure to use `check` to validate the `rules` file.

Role - root
Label - admin_low
Shell - profile shell
Privileges = all

1. Make sure that the `check` script resides in the JumpStart directory.

Note – The `check` script is provided in the `auto_install_sample` directory on the Trusted Solaris CD.

2. **Change the directory to the JumpStart directory:**

```
$ cd jumpstart_dir_path
```

3. **Run the `check` script to validate the `rules` file:**

```
$ ./check [-p path] [-r file_name]
```

In this command,

`-p` *path*	Is the path to the Trusted Solaris 2.5 CD. You can use a Trusted Solaris CD image on a local disk or a mounted Trusted Solaris CD. This option ensures that you are using the most recent version of the `check` script. You should use this option if you are using `check` on a workstation that is running a previous version of Trusted Solaris.
`-r` *file_name*	Specifies a rules file other than the one named `rules`. Using this option, you can test the validity of a rule before integrating it into the `rules` file.

As the `check` script runs, it reports that it is checking the validity of the `rules` file and the validity of each profile. If no errors are encountered, it reports: `The custom JumpStart configuration is ok.`, and creates a file called `rules.ok`.

The rules files is now validated.

Finishing Custom JumpStart

There are two things left to do to set up your JumpStart installation.

- The profiles, rules, and rules.ok files you have customized for JumpStart must be added to *jumpstart_dir_path*.
- Custom JumpStart information must be added to the bootparams database for successful network installation. You should use the same procedure you chose to use to Add Client Information for a Network Install on page 129.

▼ Copy JumpStart Files to *jumpstart_dir_path*

Role - root
Label - admin_low
Shell - profile shell
Privileges = all

1. **Log on as a user who can assume the root role and assume it.**

2. **Launch a terminal, open a profile shell, and open a shell with all privileges.**

```
# pfsh
# csh
```

3. **Change to the JumpStart directory.**
   If the *jumpstart_dir_path* is on a diskette, you must allocate the device first. See "How to Create a JumpStart Directory on a Diskette" on page 146 for the procedure.

```
$ cd jumpstart_dir_path
```

4. **If you are using a working directory rather than the *jumpstart_dir_path* to create custom JumpStart files, copy them to *jumpstart_dir_path*.**
   All of your profiles, the `rules` file, the `rules.ok` file, and the finish script (`finish.sh`) should be copied to *jumpstart_dir_path*.

   For example, the following commands copy the contents of the working directory /export/tmp. All custom JumpStart profiles have followed a convention of using "profile" as the last part of the file name.

```
# cd /export/tmp
# cp *profile jumpstart_dir_path
# cp rules rules.ok jumpstart_dir_path
# cp finish.sh jumpstart_dir_path
```

5. **Check file permissions by following the procedure "To check a file's label and permissions" on page 108.**

File or Directory	Owner	Permissions	Label
jumpstart_dir_path	root	755	admin_low[admin_low]
profiles	root	644	admin_low[admin_low]
rules, rules.ok	root	644	admin_low[admin_low]
finish.sh	root	755	admin_low[admin_low]

6. **Deallocate the diskette drive if the *jumpstart_dir_path* is on a diskette.**

Result: The custom JumpStart files are available to the installation program.

▼ Add JumpStart Options to the `Bootparams` Database

If you are using NIS+ tables for bootparams information:

1. **Follow the procedure "Add hosts information to the NIS+ tables" on page 129, adding the Profile server and the *jumpstart_dir_path* to every host to be installed.**
2. **Make sure you have completed "Add bootparams information to the NIS+ tables" on page 131, which is required for custom JumpStart, but optional for network install.**

If you are using the boot server's local bootparams database:

Either:

- **Follow the procedure "Add host and bootparams information to local databases" on page 135, selecting the no naming service and adding the Profile server to every host to be installed.**

Or:

- **Follow the procedure "To add JumpStart options using the add_install_client command", below.**

▼ To add JumpStart options using the `add_install_client` command

Role - root
Label - admin_low
Shell - profile shell
Privileges = all

♦ **Use the `-c` option to the `add_install_client` command to add JumpStart details to the local `bootparams` database.**

```
# ./add_install_client [-c server:jumpstart_dir_path] [-e ethernet_address] \
[-T server:tsolconfig_dir_path] -s install_server:install_dir_path \
host_name platform_group
```

In this command,

`-c`	Specifies a JumpStart directory for custom JumpStart installations. This option and its arguments are required for custom JumpStart.
server`:`*jumpstart_dir_path*	*server* is the host name of the server on which the JumpStart directory is located. *jumpstart_dir_path* is the absolute path of the JumpStart directory.

For example, issuing the following command on an install/boot server:

```
./add_install_client -e 8:0:20:17:22:a4 \
 -c bigbaby:/export/ts2.5_sparc/jumpstart \
 -T heron:/export/install/tsolfiles \
 -s heron:/export/install/ts2.5_sparc willet sun4m
```

- modifies the local `bootparams` database to look for custom JumpStart information in the `bigbaby:/export/ts2.5_sparc/jumpstart` directory.

The result: The client `willet` can be installed with custom JumpStart. Its Trusted Solaris 2.x image will come from `heron` (as will its boot information and Trusted Solaris configuration information), and its custom JumpStart installation profile will come from `bigbaby`.

Task Complete

To read about the optional features available for custom JumpStart installations, see Chapter 9, “Using Optional Custom JumpStart Features.” To install a workstation using custom JumpStart, go to Chapter 10, “Booting and Installing Trusted Solaris: Custom JumpStart.”

8

Using Optional Custom JumpStart Features 9

This chapter describes the optional features available for custom JumpStart installations, and it is a supplement to Chapter 8, “Preparing Custom JumpStart Installations.” You can use the following optional features to enhance and test custom JumpStart installations:

- Begin scripts
- Finish scripts
- `pfinstall`
- Site-specific installation program

Creating Begin Scripts

A *begin script* is a user-defined Bourne shell script, specified within the `rules` file, that performs tasks before the Trusted Solaris software is installed on the workstation. Begin scripts are used with custom JumpStart installations.

Important Information About Begin Scripts

The following information is important to know about begin scripts:

- Be careful that you do not specify something in the script that would prevent the mounting of file systems onto `/a` during an initial installation. If the Trusted Solaris installation program cannot mount the file systems onto `/a`, an error will occur and the installation will fail.
- Output from the begin script goes to `/var/sadm/begin.log`.
- Begin scripts should be owned by root and have permissions equal to 644.

Ideas for Begin Scripts

You could set up begin scripts to perform the following task:

- Creating derived profiles

Creating Derived Profiles With Begin Scripts

A *derived profile* is a profile that is dynamically created by a begin script during a custom JumpStart installation. Derived profiles are needed when you cannot set up the `rules` file to match specific workstations to a profile (when you need more flexibility than the `rules` file can provide). For example, you may need to use derived profiles for identical workstation models that have different hardware components (for example, workstations that have different frame buffers).

To set up a rule to use a derived profile, you must:

- Set the profile field to an equal sign (=) instead of a profile.
- Set the begin field to a begin script that will create a derived profile depending on which workstation is being installed.

When a workstation matches a rule with the profile field equal to an equal sign (=), the begin script creates the derived profile that is used to install the Trusted Solaris software on the workstation.

An example of a begin script that creates the same derived profile every time is shown below; however, you could add code to this example that would create a different derived profile depending on certain command's output.

```
#!/bin/sh
echo "install_type      initial_install"   > ${SI_PROFILE}
echo "system_type       standalone"       >> ${SI_PROFILE}
echo "partitioning      default"          >> ${SI_PROFILE}
echo "cluster           SUNWCprog"        >> ${SI_PROFILE}
echo "package     SUNWman     delete"      >> ${SI_PROFILE}
echo "package     SUNWolman   delete"      >> ${SI_PROFILE}
echo "package     SUNWxwman   delete"      >> ${SI_PROFILE}
```

As shown above, the begin script must use the `SI_PROFILE` environment variable for the name of the derived profile, which is set to `/tmp/install.input` by default.

Note – If a begin script is used to create a derived profile, make sure there are no errors in it. A derived profile is not verified by the `check` script, because it is not created until the execution of the begin script.

9

Creating Finish Scripts

A *finish script* is a user-defined Bourne shell script, specified within the `rules` file, that performs tasks after the Trusted Solaris software is installed on the workstation, but before the workstation reboots. Finish scripts are used with custom JumpStart installations.

Important Information About Finish Scripts

The following information is important to know about finish scripts:

- The Trusted Solaris installation program mounts the workstation's file systems onto `/a`. The file systems remain mounted on `/a` until the workstation reboots. Therefore, you can use the finish script to add, change, or remove files from the newly installed file system hierarchy by modifying the file systems respective to `/a`.
- Output from the finish script goes to `/var/sadm/finish.log`.
- Finish scripts should be owned by root and have permissions equal to 644.

Ideas for Finish Scripts

You could set up finish scripts to perform the following tasks:

- Installing patches
- Restoring backed up files
- Setting up print servers

The following finish scripts are provided as examples:

- Rebooting the workstation
- Adding files
- Customizing the root environment
- Setting the workstation's root password

Rebooting the Workstation with a Finish Script

Through a finish script, you can reboot the workstation.

1. Add the last line in the example finish script to every finish script you create.

```
#!/bin/sh
/usr/sbin/reboot
```

Adding Files With Finish Scripts

Through a finish script, you can add files from the JumpStart directory to the already installed workstation. This is possible because the JumpStart directory is mounted on the directory specified by the `SI_CONFIG_DIR` variable (which is set to `/tmp/install_config` by default).

Note – You can also replace files by copying files from the JumpStart directory to already existing files on the installed workstation.

The following procedure enables you to create a finish script to add files to a workstation after the Trusted Solaris software is installed on it:

1. Copy all the files you want added to the installed workstation into the JumpStart directory.
2. Insert the following line into the finish script for each file you want copied into the newly installed file system hierarchy.

```
cp ${SI_CONFIG_DIR}/file_name  /a/path_name
```

For example, if you are using a custom JumpStart diskette to install Trusted Solaris, 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/sh
cp ${SI_CONFIG_DIR}/label_encodings  /a/etc/security/tsol
```

9

Customizing the Root Environment

Through a finish script, you can customize files already installed on the workstation. For example, the following finish script customizes the root environment by appending information to the `.cshrc` file in the root directory.

```
#!/bin/sh
#
# Customize root's environment
#
echo "***adding customizations in /.cshrc"
test -f a/.cshrc || {
cat >> a/.cshrc <<EOF
set history=100 savehist=200 filec ignoreeof prompt="\$user@`uname -n`> "
alias cp cp -i
alias mv mv -i
alias rm rm -i
alias ls ls -FC
alias h history
alias c clear
unset autologout
EOF
}
```

Setting the System's Root Password With Finish Scripts

After Trusted Solaris software is installed on a workstation, the workstation reboots. Before the boot process is completed, the workstation prompts for the root password. This means that until someone enters a password, the workstation cannot finish booting.

The `auto_install_sample` directory provides a finish script called `set_root_pw` that sets the root password for you. This allows the initial reboot of the workstation to be completed without prompting for a root password.

The `set_root_pw` file is shown below.

```
#!/bin/sh
#
#       @(#)set_root_pw 1.4 93/12/23 SMI
#
# This is an example bourne shell script to be run after installation.
# It sets the workstation's root password to the entry defined in PASSWD.
# The encrypted password is obtained from an existing root password entry
# in /etc/shadow from an installed machine.

echo "setting password for root"

# set the root password
❶ PASSWD=dKO5IBkSF42lw
#create a temporary input file
❷ cp /a/etc/shadow /a/etc/shadow.orig

mv /a/etc/shadow /a/etc/shadow.orig
nawk -F: '{
❸     if ( $1 == "root" )
          printf"%s:%s:%s:%s:%s:%s:%s:%s:%s\n",$1,passwd,$3,$4,$5,$6,$7,$8,$9
      else
          printf"%s:%s:%s:%s:%s:%s:%s:%s:%s\n",$1,$2,$3,$4,$5,$6,$7,$8,$9
      }' passwd="$PASSWD" /a/etc/shadow.orig > /a/etc/shadow
❹ #remove the temporary file
rm -f /a/etc/shadow.orig
❺ # set the flag so sysidroot won't prompt for the root password
sed -e 's/0# root/1# root/' ${SI_SYS_STATE} > /tmp/state.$$
mv /tmp/state.$$ ${SI_SYS_STATE}
```

There are several things you must do to set the root password in a finish script.

❶ Set the variable `PASSWD` to an encrypted root password obtained from an existing entry in a workstation's `/etc/shadow` file.

❷ Create a temporary input file of `/a/etc/shadow`.

❸ Change the root entry in the `/etc/shadow` file for the newly installed workstation using `$PASSWD` as the password field.

❹ Remove the temporary `/a/etc/shadow` file.

❺ Change the entry from 0 to a 1 in the state file, so that the install team will not be prompted for the root password. The state file is accessed using the variable `SI_SYS_STATE`, whose value currently is `/a/etc/.sysIDtool.state`. (To avoid problems with your scripts if this value changes, always reference this file using `$SI_SYS_STATE`.) The `sed` command shown here contains a tab character after the `0` and after the `1.`

Note – 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.

Using `pfinstall` *to Test Profiles*

When `install_type initial_install` is defined in a profile, you can use the `pfinstall` command to test the profile without actually installing the Trusted Solaris software on a workstation. `pfinstall` shows the results of how a workstation would be installed according to the specified profile, before you actually perform a custom JumpStart installation.

Ways to Use `pfinstall`

`pfinstall(1M)` enables you to test a profile against:

- The workstation's disk configuration where `pfinstall` is being run.
- A disk configuration file that you can create with the `prtvtoc` command. A *disk configuration file* is 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 workstation to test profiles on different sized disks.

▼ How to Use `pfinstall` to Test a Profile

Overview – The procedure to use `pfinstall` to test a profile involves:

- Changing the directory to the JumpStart directory
- Using the `pfinstall` command to test the profile

Follow this procedure to use `pfinstall` to test a profile.

Role - root
Label - admin_low
Shell - profile shell

1. **On an installed and configured Trusted Solaris 2.5 workstation, assume the role `root`.**

2. **Launch a terminal and open a profile shell with all privileges.**

```
# pfsh -c csh
```

Note – The name "profile shell" refers to a shell that recognizes Trusted Solaris *execution profiles*. It does not refer to the profiles being tested here.

3. **To test the profile with a specific system memory size, set `SYS_MEMSIZE` to the specific memory size in Mbytes:**

```
# SYS_MEMSIZE=memory_size
# export SYS_MEMSIZE
```

4. **Change the directory to the JumpStart directory where the profile resides:**

```
$ cd jumpstart_dir_path
```

For example, the following command would change the directory to the `jumpstart` directory on the root file system.

```
cd /jumpstart
```

5. **Run the `pfinstall -d` or `pfinstall -D` command to test the profile:**

Caution – Without the `-d` or `-D` option, `pfinstall` will install the Trusted Solaris software on the workstation by using the specified profile, and the data on the workstation will be overwritten.

```
$ /usr/sbin/install.d/pfinstall -D | -d disk_config [-c path] profile
```

In this command,

`-D`	Tells `pfinstall` to use the current workstation's disk configuration to test the profile against. You must be in the role root to execute `pfinstall` with the `-D` option.
-d *disk_config*	Tells `pfinstall` to use a disk configuration file, *disk_config*, to test the profile against.
`-c` *path*	Is the path to the Trusted Solaris CD. This is required if the Trusted Solaris CD is not mounted on `/cdrom`. (For example, use this option if you copied the Trusted Solaris CD image to disk or mounted the Trusted Solaris CD on a directory other than `/cdrom`).
profile	The name of the profile to test.

Note – You should run `pfinstall` on a workstation running the same version of Trusted Solaris software that will be installed by the profile.

Run `pfinstall` from the directory where the *profile* and *disk_config* files reside (which should be the JumpStart directory). If the *profile* or *disk_config* file is not in the directory where `pfinstall` is run, you must specify the path.

6. **Check to see if the results of `pfinstall` are as you expected. If not, change the profile and go to Step 5.**

Task Complete

You have completed testing the profile. To perform a custom JumpStart installation on a workstation, see Chapter 10, "Booting and Installing Trusted Solaris: Custom JumpStart".

`pfinstall` *Examples*

Below are some examples of using `pfinstall` to test the `basic_prof` profile against the `104_test` disk configuration file:

```
/usr/sbin/install.d/pfinstall -D basic_prof

/usr/sbin/install.d/pfinstall -d 104_test basic_prof

/usr/sbin/install.d/pfinstall -D -c /export/install/ts2.5_sparc basic_prof
```

▼ How to Create a Disk Configuration File for a SPARC System

A disk configuration file is a file that represents a structure of a disk (for example, bytes/sector, flags, slices). Disk configuration files enable you to use `pfinstall(1M)` from a single workstation to test profiles on different sized disks.

Overview – The procedure to create a disk configuration file for a SPARC workstation involves:

- Locating a SPARC workstation with a disk that you want to test a profile against
- Using the `prtvtoc(1M)` command to create the disk configuration file

Follow this procedure to create a disk configuration file.

1. **Locate a workstation with a disk that you want to test a profile against.**
2. **Log on as a user who can assume the role `root` and assume it.**

Role - root
Label - admin_low
Shell - profile shell
Privileges - all

3. **Launch a terminal and open a profile shell with all privileges.**
4. **Determine the device name for the workstation's disk.**
5. **Redirect the output of `prtvtoc` to create the disk configuration file:**

```
$ prtvtoc /dev/rdsk/device_name > disk_config
```

In this command,

`/dev/rdsk/`*device_name*	Is the device name of the workstation's disk. *device_name* must be in the form `c`*w*`t`*x*`d`*y*`s2` or `c`*x*`d`*y*`s2`. **Note:** Slice 2 must be specified in *device_name*.
disk_config	Is the disk configuration file name.

6. **Copy the disk configuration file to the JumpStart directory:**

```
$ cp disk_config jumpstart_dir_path
```

Task Complete

You have completed creating a disk configuration file. The following page provides an example of creating a disk configuration file.

The following example creates a disk configuration file, `104_test`, on a workstation with a 104-Mbyte disk, whose device name is c0t3d0s2.

```
$ prtvtoc /dev/rdsk/c0t3d0s2 > 104_test
```

In this example, the `104_test` file contains the following information:

```
# cat 104_test
* /dev/rdsk/c0t3d0s2 partition map
*
* Dimensions:
*     512 bytes/sector
*      35 sectors/track
*       6 tracks/cylinder
*     210 sectors/cylinder
*    1019 cylinders
*     974 accessible cylinders
*
* Flags:
*   1: unmountable
*  10: read-only
*
*                          First     Sector    Last
* Partition  Tag  Flags    Sector    Count   Sector  Mount Directory
       0      2    00          0     16170     16169
       1      3    00      16170     28140     44309
       2      5    00          0    204540    204539
       6      4    01      44310    160230    204539
```

▼ How to Create a Multiple Disk Configuration File for a SPARC System

If you need to test a profile on multiple disks, you can concatenate disk configuration files together to create multiple disk configuration scenarios.

Overview – The procedure to create a multiple disk configuration file for a SPARC workstation involves:

- Concatenating two or more disk configuration files into one file
- Changing the target numbers of the disks (if needed)

The following procedure creates a disk configuration file to test a profile on two 104-Mbyte disks:

1. **Concatenate the `104_test` file with itself and save the output to another file:**

```
$ cat 104_test 104_test > dual_104_test
```

2. **Edit the disk configuration file so that each disk device name has a different target number.**

For example, the `dual_104_test` file is shown as follows:

```
# cat dual_104_test
❶ * /dev/rdsk/c0t3d0s2 partition map
*
* Dimensions:
*     512 bytes/sector
*      35 sectors/track
*       6 tracks/cylinder
*     210 sectors/cylinder
*    1019 cylinders
*     974 accessible cylinders
*
* Flags:
*   1: unmountable
*  10: read-only
*
*                           First     Sector    Last
* Partition  Tag  Flags    Sector    Count    Sector  Mount Directory
       0      2    00          0     16170     16169
       1      3    00      16170     28140     44309
       2      5    00          0    204540    204539
       6      4    01      44310    160230    204539
❷ * /dev/rdsk/c0t0d0s2 partition map
*
* Dimensions:
*     512 bytes/sector
*      35 sectors/track
*       6 tracks/cylinder
*     210 sectors/cylinder
*    1019 cylinders
*     974 accessible cylinders
*
* Flags:
*   1: unmountable
*  10: read-only
*
*                           First     Sector    Last
* Partition  Tag  Flags    Sector    Count    Sector  Mount Directory
       0      2    00          0     16170     16169
       1      3    00      16170     28140     44309
       2      5    00          0    204540    204539
       6      4    01      44310    160230    204539
```

Because `dual_104_test` file was created by concatenating itself, the following editing was required:

❶ The first disk device name was left as is

❷ The second disk device name was changed from `/dev/rdsk/c0t3d0s2` to `/dev/rdsk/c0t0d0s2` so it has a unique target number.

You have completed creating a multiple disk configuration file.

Using a Site-Specific Installation Program

Through the use of begin and finish scripts, sites with special requirements can install the Trusted Solaris software by creating their own installation program. When a minus sign (`-`) is specified in the profile field, the begin and finish scripts control how the workstation is installed, instead of the profile and the Trusted Solaris installation program.

For example, if the following rule would match, the `x_install.beg` begin script and the `x_install.fin` finish script would install the workstation named `wren` (the Trusted Solaris installation program would not be used):

```
hostname wren x_install.beg - x_install.fin
```

Booting and Installing Trusted Solaris: Custom JumpStart 10

This chapter provides a procedure to boot a workstation and perform a custom JumpStart installation using profiles you have created to install Trusted Solaris software. Trusted Solaris software is automatically installed on the workstation after you boot the workstation.

The procedure in this chapter should be done on the workstation that is being installed.

1 Follow the instructions before you boot the workstation:

If The System Is ...	Then ...
Off	**1)** Turn on the system components in the order recommended in the hardware guide. **Caution:** If the workstation starts booting, press L1-A or Stop-A. **2)** Go to Step 2.

On	**1)** If the workstation is running Trusted Solaris, enter the following commands:
	`$ su root`
	`# halt`
	2) Go to Step 2.

2 If the screen displays the > prompt instead of the ok prompt, then enter n and press Return.

The screen should now display the `ok` prompt.

3 For a network custom JumpStart::

If You Are Booting ...	Then Enter ... [1]
From a server on the network	`boot net - install`

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

4 For a cdrom and diskette JumpStart:

If You Are Booting ...	Then Enter ... [1]
From a local CDROM drive and have placed a custom JumpStart diskette in the diskette drive	`boot cdrom - install`

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

5 Wait for booting to be completed.

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

```
Type b (boot), c (continue), or n (new command mode)
>n
Type help for more information
ok boot net - install
Booting from: le(0,0,0) - install
2bc00 hostname: sora
domainname: aviary.eco.org
root server: grebe
root directory:
/export/install/trusted_solaris_2_5_sparc/s0/export/exec/kvm/sparc.sun4c.Trusted
 Solaris_2.5
SunOS Release 5.5.1 Version TS2.5 [UNIX(R) System V Release 4.0]
Copyright (c) 1983-1997, Sun Microsystems, Inc.
Configuring the /devices directory
Configuring the /dev directory
Searching for JumpStart directory...using heron:/jumpstart
Starting OpenWindows...
```

Note – The booting phase will last for a few minutes.

6 If prompted, provide information about the workstation.

If you have correctly set up the network installation, Trusted Solaris configuration files, and custom JumpStart rules and profiles, you should not be prompted for information.

7 Wait as the Trusted Solaris installation program automatically installs the Trusted Solaris software on the workstation.

You're done for awhile; installing Trusted Solaris software can take between 30 minutes and 2 hours, depending on the speed of your network.

8 If you installed Trusted Solaris on an OS server and allocated space for diskless clients, use the Host Manager to complete the setup of these clients.

The Trusted Solaris installation program only allocates space for clients during an initial installation. The Host Manager completes client setup by providing their required directories. See the Chapter 11, “Configuring Diskless Clients”.

9 Check that all Trusted Solaris configuration tasks are complete.

There is an overview of individual workstation configuration tasks in Chapter 6, “Configuring a NIS+ Client: Interactive”.

Task Complete

For pointers to administration references, see Chapter 12, “Where to Find….”

Configuring Diskless Clients 11

Configuring diskless clients for Trusted Solaris software is similar to configuring them for Solaris 2.5.1. The clients boot from an OS server configured with services for the clients' architecture, plus disk space for their files.

Prerequisites for Diskless Clients

In order to boot, a diskless client requires:

- access to a Trusted Solaris CD image on a hard disk
- an OS server

▼ Install and Configure an OS Server

An OS server is a *system type*. In an interactive installation from the Trusted Solaris CD, the Trusted Solaris installation program prompts you for whether you want to install a standalone or an OS server. When an OS server is installed over the network, its entry in the Host Manager indicates that it is an OS server.

An OS server can be partitioned during installation with space for clients.

Path 1 - Create OS Server during Installation

1. Choose the OS server system type during installation:

Installing a Workstation	*page 56*

2. Use the OS server worksheets during installation:

OS Server Installation Worksheet	*page 229*
OS Server Disks for Partitioning	*page 230*
OS Server Installation Program Example	*page 270*
OS Server Disk Partitioning Example	*page 272*

Path 2 - Convert Standalone to OS Server

The workstation must have disk space for clients.

1. Choose the Standalone system type during installation:

Installing a Workstation	*page 56*

2. Use the OS server worksheets for partitioning:

OS Server Installation Worksheet	*page 229*
OS Server Disks for Partitioning	*page 230*
OS Server Installation Program Example	*page 270*
OS Server Disk Partitioning Example	*page 272*

3. Add the (still Standalone) workstation to the NIS+ network:

Configuring a NIS+ Client: Interactive	*page 105*

▼ Access a Trusted Solaris CD Image on a File System

The OS server needs access to the Trusted Solaris CD image on hard disk. You can mount an existing install server's Trusted Solaris CD image, or you can copy the Trusted Solaris CD image to the OS server.

1. **On the workstation that is going to be the OS server, log on as a user who can assume the `root` role, and assume it.**

Role - root
Label - admin_low
Shell - profile shell
Privileges - all

Either:

- **Follow the procedure "Create an Install Server" on page 122.**
  This will copy the Trusted Solaris CD image to one of the OS server's hard disks.

Or:

- **As root, mount a Trusted Solaris CD image that has been copied to an install server:**

Role - root
Label - admin_low
Shell - regular terminal

a. Create a mount points for the file system to be mounted.

```
# mkdir -p /export/install/ts2.5_sparc
```

Role - root
Label - admin_low
Action- Set Mount Points

b. Add the file systems to be mounted to the file `/etc/vfstab`.

i. Open the Application Manager.

ii. Double-click the System_Admin folder.

iii. Invoke the Set Mount Points action, and enter the `vfstab` entry.
For example,

```
heron:/export/install/ts2.5_sparc - /export/install/ts2.5_sparc nfs - yes bg,intr,soft
```

iv. Save the file and exit the editor.

Role - root
Label - admin_low
Shell - profile shell
Privileges - all

c. Mount the file system as root in a shell with all privileges.

```
# pfsh -c csh
# mount /export/install/ts2.5_sparc
```

▼ Add OS Services

1. **On the workstation that is going to be the OS server, log on as a user who can assume the `admin` role., and assume it.**

Role - admin
Label - admin_low
Tool - Host Manager

2. **Open the Host Manager.**
   a. **Click the Application Manager on the Front Panel.**
   b. **Double-click Solstice_Apps.**
   c. **Double-click Host Manager, with the NIS+ Naming Service.**
3. **If there is already a Host Manager entry for the OS Server, and its Type is OS Server:**
   a. **Select the entry and choose Edit > Modify.**
   b. **Click Add... under OS Services and go to Step 5:Step b.**
4. **If there is a Host Manager entry for the OS Server, but its Type is *not* OS Server:**
   a. **Select the host.**
   b. **Choose Edit > Convert > to OS Server.**
   c. **Click Add... under OS Services and go to Step 5:Step b.**
5. **If there is no Host Manager entry for the OS server, choose Edit > Add.**

Note – In the Host Manager, the word Solaris stands for Trusted Solaris.

   a. **Fill in the following information about the OS server:**

Table 11-1 Adding an OS Server to Host Manager

Entry	Value
Host Name	
IP Address	
Ethernet Address	
System Type	**OS server**
Timezone Region	
Timezone	
Remote Install	**Do not select unless you plan to re-install the OS server over the network.**
OS Services	**Add...**

b. In the Add OS Services dialog, fill in the information:

Table 11-2 Adding OS Services to an OS Server in Host Manager

Entry	Value
Set Media Path	`/export/install/ts2.5_sparc`
Software Groups	Per platform, choose what software cluster to run. *DO NOT CHOOSE CORE.* End User installs the Trusted Solaris equivalent of Core.
Platforms	Choose a platform.

▼ Create a Boot Server

The boot server provides boot information for the diskless clients. If you want a boot server separate from the install server, create it. The boot server must be on the same subnet as the diskless clients:

Create a Boot Server on a Subnet *page 136*

Configuring Diskless Clients

Each diskless client requires an entry in the Host Manager. Use NIS+ to centrally administer the diskless clients. And create a home directory entry in the client's `vfstab` file.

▼ Add Diskless Clients

1. **On the workstation that is going to be the OS server, log on as a user who can assume the `admin` role, and assume it.**

Role - admin
Label - admin_low
Tool - Host Manager

2. **Open the Host Manager from the Solstice_Apps folder in the Application Manager.**

3. **Add each diskless client as an entry in the Host Manager.**
   If the client exists already, delete it and re-create it. A diskfull client cannot be converted to diskless.

Table 11-3 Diskless Client Information in Host Manager

Entry	Value
Host Name	
IP Address	
Ethernet Address	
System Type	**Diskless**
Timezone Region	
Timezone	
File Server	*(OS server entered for you)*
OS Release	*Select the platform for the client.*
Root Path	/export/root
Swap Path	/export/swap
Swap Size	> 64 MB

4. **Save the changes.**
   Files for the client will be created in `/export/root/clientname`. Adding a diskless client takes from 15 to 30 minutes per client.

▼ Ensure that the Client is Known to the NIS+ Master

1. **Log on to the NIS+ master as a user who can assume the role `root` and assume the role.**

Role - root
Label - admin_low
Shell - regular terminal

2. **Make sure that the client information in the kernel cache and the `tnrhdb` table is correct.**
   a. **Launch a terminal.**
   b. **Look for the client's IP address or a fallback address in the kernel cache.**

```
# tninfo -h
```

c. **Check that the information is in the tnrhdb NIS+ table.**

```
# niscat tnrhdb.org_dir | more
```

Role - root
Label - admin_low
Shell - profile shell
Privileges - all

3. **If the client is in the `tnrhdb` file correctly, but is not in the kernel cache, update the kernel in a profile shell with all privileges.**

```
# pfsh
# csh
# cd /etc/security/tsol
# tnctl -T tnrhtp
# tnctl -H tnrhdb
# tninfo -h
```

Role - root
Label - admin_low
Shell - regular terminal

4. **In a regular terminal, run the command `nistntime`.**

```
# exit [from csh]
# exit [from the profile shell]
# /usr/lib/nis/nistntime tnrhtp
# /usr/lib/nis/nistntime tnrhdb
```

5. **If the client is not in the `tnrhdb` file correctly, open the Database Manager with the NIS+ naming service, choose `tnrhdb`, and enter the client or the fallback mechanism for the client's subnet.**
   When you exit the Database Manager, the `tnrhdb` and the kernel cache are updated.

▼ Set up Each Client's Home Directory

1. **On the OS server, log on as a user who can assume the `root` role, and assume it.**

Role - root
Label - admin_low
Tool - Admin Editor

2. **Open the Admin Editor from the System_Admin folder, with the file `/export/root/`*`clientname`*`/etc/vfstab`.**
   You will do this once per client.

3. **Create a home directory entry in the `vfstab` file. You can add other mount points as well.**
   For example,

```
<home_dir_server>:/export/home - /export/home nfs - yes     bg,intr,soft
squirrel:/export/tools - /export/tools nfs - yes bg,intr,soft
```

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

Role - root
Label - admin_low
Shell - profile shell
Privileges - all

5. **In a profile shell with all privileges, create the mount points in the client's root directory.**

```
# pfsh
# csh
# cd /export/root/clientname
# mkdir -p export/home
# mkdir -p export/tools
```

▼ Reboot the OS Server

♦ **Choose Shut Down from the Trusted Path menu, confirm, then boot the server when the prompt appears.**

Booting Diskless Clients

When booting for the first time, provide a root password.

▼ Boot a Diskless Client

1. **At the `ok` prompt, type `boot net`.**
2. **When booting for the first time, provide and confirm a root password.**

Result: The diskless client is ready for use by a normal user.

See *Trusted Solaris Administrator's Procedures* for the procedure to remove a diskless client.

Where to Find… 12

- *Trusted Solaris Administration Overview* – Introduces you to Trusted Solaris concepts, the user interface, and administration tasks.
- *Trusted Solaris Label Administration* – Introduces you to labels, and gives extensive examples of how to set them up, check them, and centrally administer them.
- *Trusted Solaris Audit Administration* – Introduces you to auditing, and describes the procedures for enabling auditing on one workstation or on a network of workstations, preselecting what to audit, collecting the auditing records, filtering the records, and analyzing them from a centrral location.
- *TCP/IP and Data Communications Administration Guide,* Chapter 3, "Planning Your Network" – Describes how to set up a network. Required for networked sites only.
- *System Administration Guide, Volume I: Solaris 2.5* – Describes basic administrative tasks in Solaris 2.5.1, such as creating and mounting file systems.
- *System Administration Guide, Volume II* – Describes more advanced administrative tasks in Solaris 2.5.1, such as configuring printing.
- *NIS+ and DNS Setup and Configuration Guide* – Describes how to set up and configure a NIS+ domain. Required for networked sites.
- *Trusted Solaris Administrator's Procedures* – Steps you through administrative procedures, such as adding users and configuring printers. Includes worksheets for creating or modifying roles and execution profiles.

12

Table 12-1 shows the Solaris and Trusted Solaris documentation that you may need to configure and administer Trusted Solaris workstations. For a complete description of all the Trusted Solaris 2.5 documentation, refer to the *Trusted Solaris Documentation Roadmap.*

Table 12-1 Where to Go for Configuration and Administration Tasks

Information Needed	**Manual Title**	**Part Number**
Configuring printing	*System Administration Guide, Volume II :Solaris 2.5* *Trusted Solaris Administrator's Procedures*	*802-2003-10* *805-8008-05*
Setting up user accounts	*Trusted Solaris Administrator's Procedures*	*805-8008-05*
Setting up mail accounts	*Trusted Solaris Administrator's Procedures*	*805-8008-05*
Installing software	*System Administration Guide, Volume I Solaris 2.5* *Trusted Solaris Administrator's Procedures*	*802-2002-10* *805-8008-05*
Halting a workstation	*Trusted Solaris Administrator's Procedures*	*805-8008-05*
Boot files	*System Administration Guide, Volume I*	*802-2002-10*
Adding workstations to a network	*Trusted Solaris Administrator's Procedures*	*805-8008-05*
Accessing remote files and workstations	*System Administration Guide, Volume I*	*802-2002-10*
Administering file systems	*System Administration Guide, Volume I*	*802-2002-10*
Setting up system security	*Trusted Solaris Installation and Configuration* *System Administration Guide, Volume II*	*805-8009-05* *802-2003-10*
CD-ROM and diskette drives	*System Administration Guide, Volume I*	*802-2002-10*
Setting up printers	*System Administration Guide, Volume II* *Trusted Solaris Administrator's Procedures*	*802-2003-10* *805-8008-05*

Table 12-1 Where to Go for Configuration and Administration Tasks

Information Needed	**Manual Title**	**Part Number**
Increasing your workstation's performance	*System Administration Guide, Volume II*	*802-2003-10*
Managing disk use	*System Administration Guide, Volume II*	*802-2003-10*
Examining and changing system information	*System Administration Guide, Volume II*	*802-2003-10*
Examining and changing security information	*Trusted Solaris Administrator's Procedures*	*805-8008-05*
Using crontabs	*System Administration Guide, Volume II*	*802-2003-10*
Adding and maintaining peripherals	*Trusted Solaris Administrator's Procedures*	*805-8008-05*
Accessing devices	*Trusted Solaris Administrator's Procedures*	*805-8008-05*
Setting up disks	*System Administration Guide, Volume II*	*802-2003-10*
Terminals and modems, disk drives, tape drives, service access facility, connecting devices to serial port, format utility	*System Administration Guide, Volume II*	*802-2003-10*
Using system administration tools	*Trusted Solaris Administrator's Procedures* *Solstice AdminSuite 2.1 User's Guide*	*805-8008-05* *802-5363-10*
Customizing CDE	*Common Desktop Environment: Advanced User's and System Administrator's Guide*	*order from Addison-Wesley*

12

Site Security Policy A

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 top-level 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 SYSTEM_LOW and SYSTEM_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.

Hayes, Frank, "Is Your System Safe?" *UNIXWORLD*, June 1990.

Wood, Patrick H., and Stephen Kochan, *UNIX System Security*, Hayden Books, Indianapolis, IN, 1986.

A

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.

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.

Leffler, Samuel J., M.K. McKusick, M.J. Karels, and J.S. Quarterman, *The Design and Implementation of the 4.3 BSD UNIX Operating System*, Addison-Wesley, Reading, MA, 1989.

Nemeth, Evi, Garth Snyder, and Scott Seebas, *UNIX System Administration Handbook*, Prentice Hall, Englewood Cliffs, NJ, 1989.

Worksheets for Configuring and Installing Trusted Solaris

B

Purpose

The worksheet templates help you plan the details required to install and configure the workstations and users at your site.

See Appendix F, "Example Worksheets" for sample completed worksheets.

B

How to Use the Worksheets

♦ **Fill out the information before installing and configuring at your site.**

The worksheets provide the details of how you installed and configured your site. They should be protected with care, locked away from unauthorized users, and used to help debug system problems when they occur.

NIS+ Root Master Installation Worksheet

Dialog Box Title	Contents	Answer
Host name		
Networked?	Yes | No	
IP address		
Ethernet address		
Primary network interface	Interfaces of workstation.	
Name service	NIS+ | None	**None**
Trusted Solaris configuration	Multiple user Sensitivity Labels?	
	Hide Upgraded Names?	
	Enable ILs?	
	Float ILs?	
	Reset ILs upon EXEC?	
Subnet	Yes | No	
Subnet mask	255.255.255.0	
Time zone	Offset from GMT | Geographical	
Date and Time		
System type	Standalone | OS server | ~~Dataless~~	**Standalone**
Software group	Core (End user) | Developer | Entire	
Customize?	Yes | No	
Disk(s) to use	Disks visible to the workstation.	
Preserve?	Disks to leave as they are.	**No**
Auto-layout file systems?	Yes | No	
File systems to auto-layout*	`/, /usr, /var, /opt, swap`	
Customize?	Yes | No	**Yes**
Customize Disks*		*
Begin installation	Yes | No	
Reboot	Yes | No	
Root password		

- ***Use the "NIS+ Root Master's Disk Partition Tables" on page 224 for planning and partitioning disks.**

B

NIS+ Root Master's Disk Partition Tables

Disk	Slice	Mount point	Size	Disk	Slice	Mount point	Size
c t d	**s0**			c t d	**s0**		
	s1				**s1**		
	s2	entire disk			**s2**	entire disk	
	s3				**s3**		
	s4				**s4**		
	s5				**s5**		
	s6				**s6**		
	s7				**s7**		

Disk	Slice	Mount point	Size	Disk	Slice	Mount point	Size
c t d	**s0**			c t d	**s0**		
	s1				**s1**		
	s2	entire disk			**s2**	entire disk	
	s3				**s3**		
	s4				**s4**		
	s5				**s5**		
	s6				**s6**		
	s7				**s7**		

- **Need help? See "Root NIS+ Master Disk Partitioning Example" on page 263.**
- **Go to "Disk Partition Tables" on page 239 and following for more disk partitioning blanks.**
- **See "Common Disk Sizes and Amount Available for Partitions" on page 238 for information on how much disk is available for formatting for several standard sizes of disks.**

NIS+ Root Master's Configuration Worksheet

System Administrator Information		**Security Officer Information**
Name		**root password**
IP address	. . .	**PROM mode**
Ethernet address	: : : : :	**PROM password**
Sun architecture	sun_____	
Network interfaces		
Mount Points		**Security Information**

Standalone NIS+ Client Installation Worksheet

Dialog Box Title	**Contents**	**Answer**
Host name		
Networked?	Yes | No	**Yes**
IP address		
Ethernet address		
Primary network interface	Interfaces of workstation.	
Name service	NIS+ | None	**NIS+**
Domain Name		
Name server	Find | Specify	
Name server information	Prompts for name and IP address	
Trusted Solaris configuration		◆
Subnet	Yes | No	◆
Subnet mask	255.255.255.0	◆

Time zone	Offset from GMT | Geographical	
Date and Time		
System type	Standalone | OS server | ~~Dataless~~	
Software group	Core (End user) | Developer | Entire	
Customize?	Yes | No	
Disk(s) to use	Disks visible to the workstation.	
Preserve?	Disks to leave as they are.	**No**
Auto-layout file systems?	Yes | No	
File systems to auto-layout*	`/, /usr, /var, /opt, swap`	
Customize?	Yes | No	**Yes**
Customize Disks*		*****
Begin installation	Yes | No	
Reboot	Yes | No	
Root password		

- **Answer Trusted Solaris configuration (◆), Subnet (◆), and Subnet mask (◆) questions with the answers you used for the NIS+ root master.**
- **Use the Disk Partition Table Worksheets on page 238 for planning and entering disk partitioning.**

Standalone NIS+ Client Disks for Partitioning

Disk	Slice	Mount point	Size	Disk	Slice	Mount point	Size
c t d	**s0**			c t d	**s0**		
	s1				**s1**		
	s2	entire disk			**s2**	entire disk	
	s3				**s3**		
	s4				**s4**		
	s5				**s5**		
	s6				**s6**		
	s7				**s7**		

Standalone NIS+ Client Configuration Worksheet

System Administrator Information		**Security Officer Information**
Name		**root password**
IP address	. . .	**PROM mode**
Ethernet address	: : : : :	**PROM password**
Sun architecture	sun_____	
Network interfaces		

Mount Points (For local file systems)	**Security Attributes**

Mount Points (For remote file systems)

Audit File Systems		
Primary	:/etc/security/audit/	/files
Secondary	:/etc/security/audit/	/files

B

System Administrator Information	Security Officer Information
Local	/etc/security/audit/ /files
Mail Server	
Attached Devices	
Remote Printers	

OS Server Installation Worksheet

Dialog Box Title	Contents	Answer
Host name		
Networked?	Yes | No	**Yes**
IP address		
Ethernet address		
Primary network interface	Interfaces of workstation.	
Name service	NIS+ | None	**None**
Trusted Solaris configuration		◆
Subnet	Yes | No	◆
Subnet mask	255.255.255.0	◆
Time zone	Offset from GMT | Geographical	
Date and Time		
System type	Standalone | OS server | Diskless	**OS Server**
Platform support	sun4c | sun4d | sun4m | sun4u	
Client space allocation	root = , swap= , number of clients=	
Software group	Core (End user) | Developer | Entire	
Customize?	Yes | No	**No**
Disk(s) to use	Disks visible to the workstation.	
Preserve?	Disks to leave as they are.	**No**
Auto-layout file systems?	Yes | No	
File systems to auto-layout*	`/, /usr, /var, /opt, swap`	*
Begin installation	Yes | No	
Reboot	Yes | No	
Root password		

- **Answer Trusted Solaris configuration (◆), Subnet (◆), and Subnet mask (◆) questions with the answers you used for the NIS+ root master.**
- **Use the Disk Partition Table Worksheets on page 238 for planning and entering disk partitioning.**

B

OS Server Disks for Partitioning

Disk	Slice	Mount point	Size	Disk	Slice	Mount point	Size
c t d	**s0**			c t d	**s0**		
	s1				**s1**		
	s2	entire disk			**s2**	entire disk	
	s3				**s3**		
	s4				**s4**		
	s5				**s5**		
	s6				**s6**		
	s7				**s7**		

Disk	Slice	Mount point	Size	Disk	Slice	Mount point	Size
c t d	**s0**			c t d	**s0**		
	s1				**s1**		
	s2	entire disk			**s2**	entire disk	
	s3				**s3**		
	s4				**s4**		
	s5				**s5**		
	s6				**s6**		
	s7				**s7**		

Disk	Slice	Mount point	Size	Disk	Slice	Mount point	Size
c t d	**s0**			c t d	**s0**		
	s1				**s1**		
	s2	entire disk			**s2**	entire disk	
	s3				**s3**		
	s4				**s4**		
	s5				**s5**		
	s6				**s6**		
	s7				**s7**		

OS Server Configuration Worksheet

System Administrator Information		Security Officer Information
Name		**root password**
IP address	. . .	**PROM mode**
Ethernet address	: : : : :	**PROM password**
Sun architecture	sun_____	
Network interfaces		
Mount Points (For local file systems)		**Security Attributes**
	/export/root /export/swap	
Mount Points (For remote file systems)		
Audit File Systems		
Primary	:/etc/security/audit/ /files	
Secondary	:/etc/security/audit/ /files	
Local	/etc/security/audit/ /files	
Mail Server		
Attached Devices		
Remote Printers		

B

Services Provided by Each Workstation

Use	Workstation Name	IP address	Shared File Systems	Security Information
NIS+ workstations				
NIS+ root master				
Network routers				
File Servers (Shares file systems for mounting by end user workstations)				
Audit Servers (Shares all audit file systems for mounting by audit administration server and user workstations)				
			/etc/security/audit/	
			/etc/security/audit/	
			/etc/security/audit/	
			/etc/security/audit/	
			/etc/security/audit/	
Audit Administration Server (Shares no file systems; mounts all audit file systems)				
			None	
OS Servers for Diskless Clients (Shares file systems for mounting by diskless clients)				
			/export/root	
			/export/swap	
Install Server (Shares file system that contains Trusted Solaris image)				

Use	Workstation Name	IP address	Shared File Systems	Security Information
Boot Server (One per NIS+ subdomain)				
Mail Server (Share /var/mail file system)				
Print Servers				

Remote Hosts (`tnrhdb`*) Worksheet for NIS+ Root Master*

System Administrator Information		Security Officer Information
Name **IP address** **Host_type** **Use**		**Template**
Name **IP address** **Host_type** **Use**		**Template**
Name **IP address** **Host_type** **Use**		**Template**
Name **IP address** **Host_type** **Use**		**Template**

B

Remote Hosts Worksheet - Local `tnrhdb` *Entries*

System Administrator Information	Security Officer Information
Workstation name	
Remote host **IP address** **Host_type** **Use**	**Template**
Workstation name	
Remote host **IP address** **Host_type** **Use**	**Template**
Workstation name	
Remote host **IP address** **Host_type** **Use**	**Template**
Workstation name	
Remote host **IP address** **Host_type** **Use**	**Template**
Workstation name	
Remote host **IP address** **Host_type** **Use**	**Template**
Workstation name	
Remote host **IP address** **Host_type** **Use**	**Template**

First User Worksheet

User (will assume role `secadmin`**):**		
Identity	User name	
	User ID	
	Primary Group	
	Secondary Groups	
	Comment	
	Login Shell	
	User Type	Normal
Home	Create home dir automatically?	Yes
	Home directory	
	Path to setup files	
	Default permissions	
	Mail server	
	Cred?	Yes, leave it checked
	AutoHome setup?	*NO*
Password	Password generation method	
	Minimum days between changing passwords	
	Maximum days between changing passwords	
	Maximum time a user can be inactive	
	Status	Open
	NIS+ credentials?	Yes
Idle	Idle time	
	Idle action: logout | lock screen	
Labels	Clearance	
	Minimum label	
	View - External or Internal?	
	Sensitivity Label visible or not visible?	
	Information Label visible or not visible?	
Profiles	All | Convenient Authorizations | ...	All, Enable Login, Convenient ...
Roles	secadmin | admin | root	secadmin

B

Second User Worksheet

User (will assume role `admin`**):**		
Identity	User name	
	User ID	
	Primary Group	
	Secondary Groups	
	Comment	
	Login Shell	
	User Type	Normal
Home	Create home dir automatically?	Yes
	Home directory	
	Path to setup files	
	Default permissions	
	Mail server	
	Cred?	Yes, leave it checked
	AutoHome setup?	*NO*
Password	Password generation method	
	Minimum days between changing passwords	
	Maximum days between changing passwords	
	Maximum time a user can be inactive	
	Status	Open
	NIS+ credentials?	Yes
Idle	Idle time	
	Idle action: logout | lock screen	
Labels	Clearance	
	Minimum label	
	View - External or Internal?	
	Sensitivity Label visible or not visible?	
	Information Label visible or not visible?	
Profiles	All | Convenient Authorizations | ...	All, Enable Login, Convenient ...
Roles	secadmin | admin | root	admin

Administrative Role Worksheet - secadmin

Role: secadmin		
Password	Password generation method	
	Minimum days between changing passwords	
	Maximum days between changing passwords	
	Maximum time a user can be inactive	
	Status	Open
	NIS+ credentials?	Yes
Idle	Idle time	
	Idle action: logout | lock screen	
Labels		
	View - External or Internal?	
	Sensitivity Label visible or not visible?	
	Information Label visible or not visible?	

Administrative Role Worksheet - admin

Role: admin		
Password	Password generation method	
	Minimum days between changing passwords	
	Maximum days between changing passwords	
	Maximum time a user can be inactive	
	Status	Open
	NIS+ credentials?	Yes
Idle	Idle time	
	Idle action: logout | lock screen	
Labels		
	View - External or Internal?	
	Sensitivity Label visible or not visible?	
	Information Label visible or not visible?	

B

Disk Partition Table Worksheets

♦ **Copy and fill out the disk partitioning worksheets on the following pages when planning or formatting disks.**
Table B-1 shows common disk sizes and the amount available for partitioning.

Table B-1 Common Disk Sizes and Amount Available for Partitions

Disk Size	Size of Entire Disk (MB)
2.1G	1980
1.5G	1034
1.3G	1270
1.05G	1002
424MB	404
124MB	99

Disk Partition Tables

Workstation Name: _____

Disk	Slice	Mount point	Size	Disk	Slice	Mount point	Size
c t d	**s0**			c t d	**s0**		
	s1				**s1**		
	s2	entire disk			**s2**	entire disk	
	s3				**s3**		
	s4				**s4**		
	s5				**s5**		
	s6				**s6**		
	s7				**s7**		

Disk	Slice	Mount point	Size	Disk	Slice	Mount point	Size
c t d	**s0**			c t d	**s0**		
	s1				**s1**		
	s2	entire disk			**s2**	entire disk	
	s3				**s3**		
	s4				**s4**		
	s5				**s5**		
	s6				**s6**		
	s7				**s7**		

Disk	Slice	Mount point	Size	Disk	Slice	Mount point	Size
c t d	**s0**			c t d	**s0**		
	s1				**s1**		
	s2	entire disk			**s2**	entire disk	
	s3				**s3**		
	s4				**s4**		
	s5				**s5**		
	s6				**s6**		
	s7				**s7**		

B

Checklists for Configuring and Installing Trusted Solaris

C

What is in the Checklists

The checklists provide an overall view of what to plan before installing and configuring multiple workstations with Trusted Solaris software at your site. They also provide a record of completing a planning task and a pointer to the procedures to carry out the plan.

How to Use the Checklists

The checklists are for planning and for reference. Fill out the information in the worksheets in Appendix B, "Worksheets for Configuring and Installing Trusted Solaris", then check the task off the list before installing and configuring at your site. The worksheets in Appendix B, "Worksheets for Configuring and Installing Trusted Solaris" collect the details of the site; the checklists provide an overall view of what to remember when installing and configuring the workstations at your site, and a record of doing so.

C

Site Summary Checklist

The following checklist summarizes what you have done at your site. Where indicated, there are separate worksheets to plan particular site features, such as the workstations.

	Background for Planning	Comments
☐	Read *Trusted Solaris Administration Overview*	
☐	Understand my site security requirements	
☐	Read Appendix A, "Site Security Policy"	

	Planning	Checklist summaries	Detail worksheets
☐	Labels	*Planning Labels* on *page 243*	See *Trusted Solaris Label Administration*
☐	Network	*Planning the Network* on *page 244*	"Remote Hosts (tnrhdb) Worksheet for NIS+ Root Master" on page 233
			"Services Provided by Each Workstation" on page 232
☐	Auditing	*Planning Auditing* on *page 245*	See *Trusted Solaris Audit Administration*
☐	Workstations	*Planning Workstations* on *page 246*	"Services Provided by Each Workstation" on page 232
☐	First Two Users		"First User Worksheet" on page 235
			"Second User Worksheet" on page 236
☐	Administrative Roles		"Administrative Role Worksheet - secadmin" on page 237
			"Administrative Role Worksheet - admin" on page 237
☐	Users, Roles and Profiles		See *Trusted Solaris Administrator's Procedures*

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.

Planning before Installation	**Decision**		**Enter on:**
☐ Choosing a label_encodings file 1) GFI 2) Site-specific 3) Modified Trusted Solaris single-label 4) Modified Trusted Solaris multilabel			Worksheets copied from *Trusted Solaris Label Administration*
☐ Deciding Trusted Solaris configuration			"NIS+ Root Master Installation Worksheet" on page 223.
Create multiple user Sensitivity Labels:	Yes	No	
Hide upgraded names in directories:	Yes	No	
Enable Information Labels:	Yes	No	
Float Information Labels:	Yes	No	
Reset Information Labels on EXEC:	Yes	No	

Planning before Configuration	**Decision**	**Enter on:**
☐ Deciding which users cannot see labels		Worksheets copied from *Trusted Solaris Administrator's Procedures*

C

Planning the Network

Planning	Decision
❑ Network security if open: 1) Accessible domains 2) Accessible workstations 3) TS workstations that have access to non-TS ones	
❑ Identifying the NIS+ master	
❑ Identifying the NIS+ replicas	
❑ Identifying the NIS+ subdomain masters	
❑ Identifying the OS server(s) for diskless clients	
❑ Identifying the file server(s)	
❑ Identifying the audit servers	
❑ Identifying the audit administration server	
❑ Identifying the print servers	
❑ Identifying the mail servers	
❑ Identifying other workstations on the network	
❑ Determining the label range of each workstation's network interfaces	
❑ Determining the label(s) applied to incoming data from unlabeled workstations	

Planning Auditing

Note – Use this worksheet only if you have decided to audit.

	Decisions made about	For details, see ...
❑	Classes of events to audit for success	
❑	Classes of events to audit for failure	
❑	Classes of events to audit for both	
❑	Users/roles with additional auditing & for what	
❑	Primary and secondary audit partitions for each workstation	
❑	Size of audit partitions	
❑	Who has access to the audit administration server	
❑	Who has access to the audit servers	
❑	Who is responsible for audit archiving and when	

This function	is done by ...	user(s)
audit backup and archive		
audit review		

C

Planning Workstations

	Identified machine, name, and IP address of ...	For details, see ...
❑	NIS+ workstations (root master, replicas, subdomain masters)	
❑	Servers	
❑	End user workstations	
❑	Network routers	

	Tasks finished	For details, see ...
❑	root passwords	
❑	PROM security level	
❑	PROM passwords	
❑	Workstations with limited accreditation range	
❑	Workstations that can have attached devices	
❑	Workstation assignment to users	
❑	Workstation access to printers	

Supported Hardware Components D

Platform Names and Groups

Table D-1 shows the platform names of various hardware platforms. When installing across a network, providing platform group information reduces the number of prompts from the Trusted Solaris installation program.

- Use `uname -i` to determine a system's platform name.
- Use `uname -m` to determine a system's platform group.

Table D-1 Platform Names and Groups

System	Platform Name	Platform Group
SPARCstation 1	SUNW,Sun_4_60	sun4c
SPARCstation1+	SUNW,Sun_4_65	sun4c
SPARCstation SLC	SUNW,Sun_4_20	sun4c
SPARCstation ELC	SUNW,Sun_4_25	sun4c
SPARCstation IPC	SUNW,Sun_4_40	sun4c
SPARCstation IPX	SUNW,Sun_4_50	sun4c
SPARCstation 2	SUNW,Sun_4_75	sun4c
SPARCcenter 1000	SUNW,SPARCserver-1000	sun4d
SPARCcenter 2000	SUNW,SPARCcenter-2000	sun4d

D

Table D-1 Platform Names and Groups

System	Platform Name	Platform Group
SPARCstation 5	SUNW,SPARCstation-5	sun4m
SPARCstation 10	SUNW,SPARCstation-10	sun4m
SPARCstation 10SX	SUNW,SPARCstation-10,SX	sun4m
SPARCstation 20	SUNW,SPARCstation-20	sun4m
SPARCserver6xx	SUNW,SPARCsystem-600	sun4m
SPARCstation LX	SUNW,SPARCstation-LX	sun4m
SPARCstation LX+	SUNW,SPARCstation-LX+	sun4m
SPARCclassic	SUNW,SPARCclassic	sun4m
SPARCclassic X	SUNW,SPARCclassic-X	sun4m
SPARCengine EC3	SUNW,SPARCengine-EC-3	sun4m
SPARCstation Voyager	SUNW,S240	sun4m
Sun Ultra 1 Sun UltraServer 1	SUNW,Ultra-1	sun4u
Other SPARC systems	See your hardware vendor documentation for platform name information.	

SBus Components

Table D-2 shows the SBus components supported in Trusted Solaris 2.5.

Table D-2 SBus Components

Component name
SBus Fast SCSI-2/Buffered Ethernet Card (FSBE/S)
SBus SCSI/Buffered Ethernet Card (SBE/S)
SBus SCSI Host Adapter
SBus Differential Fast/Wide Intelligent SCSI-2 Host Adapter (DWIS/S)
SBus Single-Ended Fast/Wide Intelligent SCSI-2 Host Adapter (SWIS/S)
SBus Quad Ethernet Controller (SQEC)

Table D-2 SBus Components

Component name
SBus FastEthernet Adapter SBus Card
Token Ring Interface/SBus (TRI/S) for Solaris 2.x
PCMCIA Interface/SBus Card

Frame Buffers and Graphics Accelerators

Table D-3 shows the frame buffers and graphics cards supported in Trusted Solaris 2.5.

Table D-3 Frame Buffers and Graphics Accelerators

Component name
24-bit True Color (S24 Frame Buffer)
GX 8-bit Accelerated Graphics
TurboGX 8-bit Accelerated Graphics
TurboGXplus 8-bit Accelerated Graphics
ZX 24-bit Color Accelerated Graphics
TurboZX 24-bit Color Accelerated Graphics
(4-Mbyte and 8-Mbyte) SX 24-bit Color Accelerated Graphics
cgthree
Creator
Creator 3D

Input Devices

Table D-4 shows the input devices supported in Trusted Solaris 2.5.

Table D-4 Input Devices

Component name
SunButtons : 32 key function I/O device
SunDials : 8-Dial Interactive Graphics I/O device for 3-D

D

Printers

Table D-5 shows the printers supported in Trusted Solaris 2.5.

Table D-5 Printers

Component name
SPARCprinter E Laser Printer
SPARCprinter EC Color Laser Printer
Other laser printers

Video and Multimedia Options

Table D-6 shows the video options supported in Trusted Solaris 2.5.

Table D-6 Video Options

Component name	Specific Authorization Required?
SunVideo Realtime Video Board	yes
Multimedia Kit, Camera	yes

Sample Custom JumpStart Installation

E

This example shows a set of steps a system administrator would take to do a custom JumpStart installation for a fictitious site.

Sample Site Setup

Figure E-1 shows the sample site setup for this example.

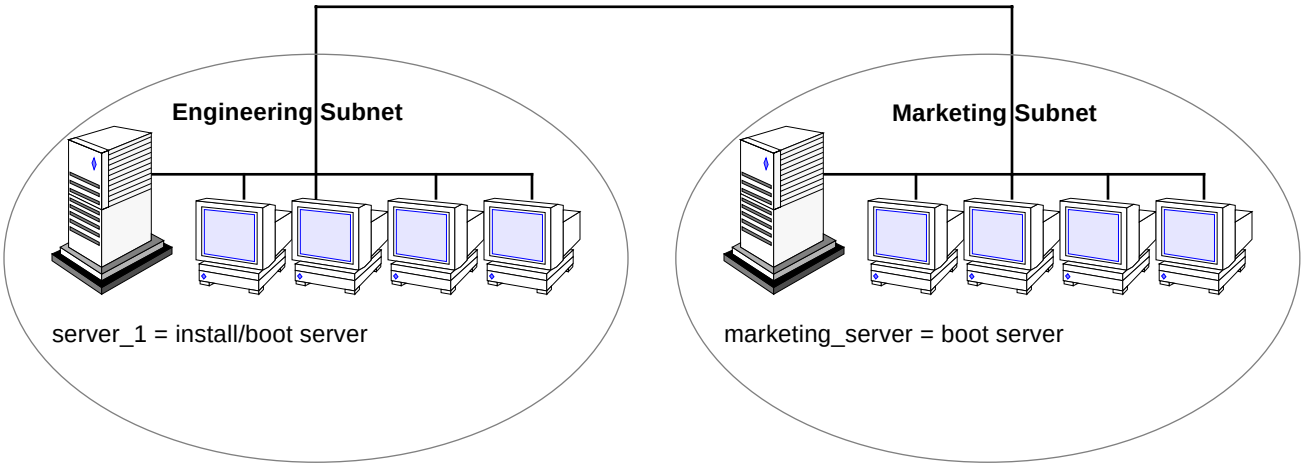


Figure E-1 Sample Site Setup

At this fictitious site:

- The engineering group is on its own subnet. This group uses 32-Mbyte Sun IPX systems for software development.
- The marketing group is on its own subnet. This group uses 16-Mbyte Sun ELC systems for running word processing, spreadsheets, and other office tools.
- The site uses NIS+. The Ethernet addresses, IP addresses, and host names are in NIS+ tables.
- The engineering server named `server_1` has a copy of Trusted Solaris 2.5 software on its local disk in a directory named `/export/install`. Both the engineering and marketing groups will install Trusted Solaris software over the network from `server_1`.

1 Create a JumpStart directory.

Role - admin
Label - admin_low
Shell - profile shell

The system administrator sets up a JumpStart directory on the install server, `server_1`. This directory will hold files necessary for a custom JumpStart installation of Trusted Solaris software. The easiest way to set up this directory is to copy the sample directory from the copy of the Trusted Solaris CD that has been put in `/export/install`.

```
# cp -r /export/install/auto_install_sample /jumpstart
```

2 Share the JumpStart directory.

Role - admin
Label - admin_low
Shell - profile shell

The system administrator shares the `/jumpstart` directory so that the `rules` file and profiles are accessible to systems on the network. To accomplish this, the administrator adds the following line to the `/etc/dfs/dfstab` file:

```
share -F nfs -o ro,anon=0 /jumpstart
```

Then, at the command line, the administrator uses the `unshareall` and `shareall` commands:

```
# unshareall
# shareall
```

3 Create the `eng_profile` profile.

Role - admin
Label - admin_low
Tool - favorite editor

The administrator creates a file named `eng_profile` in the `/jumpstart` directory. The `eng_profile` file has the following entries, which define the Trusted Solaris software to be installed on systems in the engineering group.

```
❶ install_type  initial_install
❷ system_type   standalone
❸ partitioning  default
❹ cluster       SUNWCprog
❺ filesys       any 64 swap
```

❶ Specifies that the installation will be treated as an initial installation, as opposed to an upgrade.

❷ Specifies that the engineering systems are standalone systems.

❸ Specifies that the JumpStart software uses default disk partitioning for installing Trusted Solaris software on the engineering systems.

❹ Specifies that the developer's software cluster will be installed.

❺ Specifies that each system in the engineering group will have 64Mbytes of swap space.

4 Create the `marketing_profile` profile.

Role - admin
Label - admin_low
Tool - favorite editor

The administrator creates a file named `marketing_profile` in the `/jumpstart` directory. The `marketing_profile` file has the following entries, which define the Trusted Solaris software to be installed on systems in the marketing group.

```
❶ install_type  initial_install
❷ system_type   standalone
❸ partitioning  default
❹ cluster       SUNWCuser
❺ package       SUNWaudmo
```

❶ Specifies that the installation will be treated as an initial installation, as opposed to an upgrade.

❷ Specifies that the marketing systems are standalone systems.

❸ Specifies that the JumpStart software will use default disk partitioning for installing Trusted Solaris software on the marketing systems.

❹ Specifies that the end user software cluster is to be installed.

❺ Specifies that the audio demo software package is to be added to each system.

5 Edit the `rules` file.

Role - admin
Label - admin_low
Tool - favorite editor

The administrator must define the `rules` file. The Trusted Solaris installation program will use the contents of this file to select the proper installation for each department.

At this site, each department is on its own subnet and network address. The administrator uses this information to control how systems are installed. The engineering department is on subnet 255.222.43.0, and marketing is on 255.222.44.0.

In the `/jumpstart` directory, the administrator edits the `rules` file, deletes all of the example rules, and enters:

```
network 255.222.43.0 - eng_profile    -
network 255.222.44.0 - marketing_profile -
```

Note – These are sample rules in which an administrator uses a network address to identify which systems will be installed with the `eng_profile` and `marketing_profile`, respectively. The administrator could also have chosen to use host names, memory size, or model type as the rule keyword. See "Rule Keyword and Rule Value Descriptions" on page 169 for a complete list of keywords you can use in a `rules` file.

6 Execute the `check` script.

Role - admin
Label - admin_low
Shell - profile shell

After the `rules` and profile files are properly set up, the system administrator runs the `check` script to verify the files.

```
# cd /jumpstart
# ./check
```

When `check` finds no errors, it creates the `rules.ok` file.

7 Set up the engineering systems for installation.

After setting up the `/jumpstart` directory and appropriate files, the administrator sets up the install server to install Trusted Solaris software on the engineering systems.

The administrator first sets up the engineering systems because they are on the same subnet as the install server. On the install server, the administrator uses the `add_install_client` command:

```
# cd /export/install
# ./add_install_client -c server_1:/jumpstart host_eng1 sun4c
# ./add_install_client -c server_1:/jumpstart host_eng2 sun4c
    .
    .
    .
```

In the `add_install_client` command,

`-c`	Specifies the server (`server_1`) and path (`/jumpstart`) to the JumpStart directory.
`host_eng1`	Is the name of a system in the engineering group.
`host_eng2`	Is the name of another system in the engineering group.
`sun4c`	Specifies the platform of the systems that will use `server_1` as an install server. (This is the proper platform name for Sun IPX systems.)

8 Set up the marketing systems for installation.

Systems cannot boot from an install server on a different subnet, so the administrator sets up a boot server on the marketing group's subnet. On a server on the marketing subnet, the administrator inserts a Trusted Solaris CD. The administrator then uses the `setup_install_server` command to copy the boot software from the CD to the marketing server.

```
# cd /cdrom/cdrom0/s0
# ./setup_install_server -b /marketing/boot-dir sun4c
```

In the `setup_install_server` command,

`-b`	Specifies that `setup_install_server` will copy the boot information from the Trusted Solaris CD to the directory named `/marketing/boot-dir`.
`sun4c`	Specifies the platform of the systems that will use this boot server. (This is the proper platform name for Sun ELC systems.)

Next, the administrator sets up the marketing systems to boot from the local boot server and install Trusted Solaris from the remote install server. The administrator 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
    .
    .
    .
```

In the `add_install_client` command,

`-s`	Specifies the install server (`server_1`) and the path to the Trusted Solaris software (`/export/install`).

`-c`	Specifies the server (`server_1`) and path (`/jumpstart`) to the JumpStart directory.
`host_mkt1`	Is the name of a system in the marketing group.
`host_mkt2`	Is the name of another system in the marketing group.
`sun4c`	Specifies the platform of the systems that will use this boot server. (This is the proper platform name for Sun ELC systems.)

9 Boot the systems and install Trusted Solaris software.

The administrator boots the engineering systems by using the following `boot` command at the `ok` (PROM) prompt of each system.

```
ok boot net - install
```

Example Worksheets

F

Purpose

The worksheet examples provide you with samples for setting up your workstations and user-administrators.

The worksheet examples provide you with samples for your workstations, devices, user-administrators, and network.

F

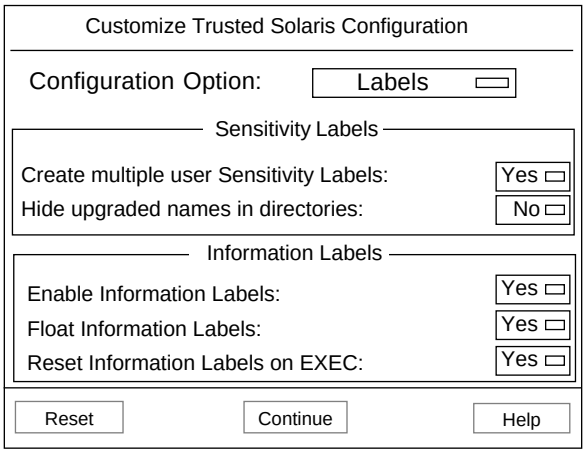
How to Use the Worksheet Examples

Blank worksheets for you to copy and enter your site's details are in Appendix B, "Worksheets for Configuring and Installing Trusted Solaris".

Caution – 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
Host name	grebe	
Networked?	Yes	
IP address	129.159.110.1	
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 root NIS+ master later.
Trusted Solaris Configuration	Continue	Sets the label configuration for all workstations on the Trusted Solaris network.
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 page 280.
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 ID information is automatically given to the installation program, reducing the installer's interaction with the program.

System type	**Standalone**	
Software group	Entire	
Customize?	Yes	Customizing a software group often results in software dependencies; system administration knowledge is required to fix dependencies.

Disk(s) to use	c0t0d0, c0t1d0, c0t3d0, c0t5d0	See “Root NIS+ Master Disk Partitioning Example” on page 263 for the details of the example.
Preserve?	**No**	
Auto-layout file systems?	Yes	Manual layout requires advanced system administration skills.
File systems to auto-layout	`/, /usr, /var`	See “Root NIS+ Master Disk Partitioning Example” on page 263 for examples.
Customize?		Customizing requires advanced system administration skills.
Begin installation		
Reboot	Yes	
Root password	<List it elsewhere>	Workstation security requires a root password.

Root NIS+ Master Disk Partitioning Example

Workstation Name:__grebe__

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	124		**s3**		
	s4				**s4**		
	s5	/opt	100		**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/grebe	1014		**s3**	/swapfile	600
	s4				**s4**		
	s5				**s5**		
	s6				**s6**		
	s7	/etc/security/audit/grebe.1	1014		**s7**	/opt	1380

F

Services Provided by Each Workstation Example

Use	Name	IP address	Shared File Systems	Security Information
NIS+ workstations				
Root NIS+ master	grebe	129.159.110.1	/etc/security/audit/grebe	
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)				
	audacious	129.159.110.7	None	nosuid, nodev, [high]
OS Servers for Diskless Clients (Shares file systems for mounting by diskless clients)				
	hurricane	129.159.110.11	/export/root	
	tornado	129.159.110.12	/export/swap	
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			

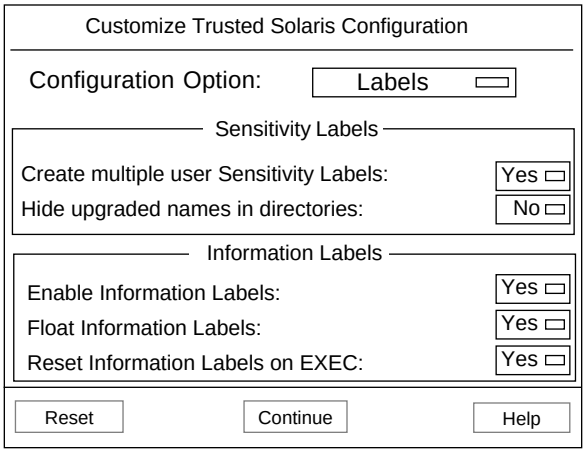
Use	Name	IP address	Shared File Systems	Security Information
Print Servers				
	cirrus cumulus			

F

Standalone Workstation Installation Program Example - Audit Server

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
Host name	willet	
Networked?	Yes	
IP address	129.159.110.3	
Primary network interface	le0	You are not prompted for this unless the workstation has more than one network card.
Name service	**None**	You will configure the workstation as a NIS+ client later.
Trusted Solaris configuration	Continue	Select the same the label configuration as the one for the root NIS+ master.
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 page 280.
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 ID information is automatically given to the installation program, reducing the installer's interaction with the program.

System type	**Standalone**	
Software group	Entire	
Customize?	Yes	Customizing a software group often results in software dependencies; system administration knowledge is required to fix dependencies.
Disk(s) to use	c0t0d0, c0t1d0, c0t3d0, c0t5d0	See "Standalone Disk Partitioning Example - Audit Server" on page 268 for the details of the example.
Preserve?	**No**	Cannot preserve file systems during initial installation.
Auto-layout file systems?	Yes	Manual layout requires advanced system administration skills.
File systems to auto-layout	`/, /usr, /var`	
Customize?		
Customize Disks		See "Standalone Disk Partitioning Example - Audit Server" on page 268 for the details of the example
Begin installation		
Reboot	Yes	
Root password	<List it elsewhere>	Workstation security requires a root password.

F

Standalone Disk Partitioning Example - Audit Server

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

Standalone Workstation Configuration Worksheet - Audit Server

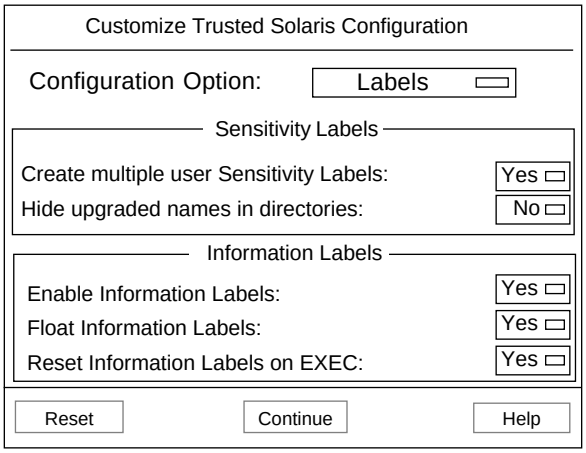
System Administrator Information		**Security Officer Information**	
Name	willet	**root password**	
IP address	129.159.110.3	**PROM mode**	full
Ethernet address	8:0:20:4c:7e:2f	**PROM password**	
Sun architecture	sun4m		
Network interfaces	le0		
Network router	willet-118 le1 (129.159.118.25)		
Mount Points (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/Sol251/		
for TS AnswerBks	/usr/AB/TS25/		
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]
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	grebe		
Attached Devices	CD-ROM (sd6) tape drive (st4)		only usable by those whose profile includes `device_allocate`
Remote Printers			
	cirrus		
	cumulus	Administrator printer [admin_high] only	

F

OS 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
Host name	hurricane	
Networked?	Yes	
IP address	129.159.110.11	
Primary network interface	le0	You are not prompted for this unless the workstation has more than one network card.
Name service	**None**	You will configure the name service later.
Trusted Solaris configuration	Continue	Select the same the label configuration as the one for the root NIS+ master.
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 page 280.
Date and Time		The default is usually the correct clock time.



The answers to the above questions are System ID Information (sysidinfo). When installing over a network, system ID information is automatically given to the installation program, reducing the installer's interaction with the program.

System type	**OS server**	
Platforms supported	sun4c, sun4d, sun4m , sun4u	Choose all platforms that clients require.

Client services	4 clients, root=30, swap=24	When partitioning the disks, provide at least 30MB disk space per client in /export/root, and 24MB of swap space per client in /export/swap. (or make swap = client RAM)
Software group	Entire	
Disk(s) to use	c0t0d0, c0t1d0, c0t3d0, c0t5d0	See OS Server Disk Partitioning Example on page 272 for the details of the example.
Auto-layout file systems?	Yes	
File systems to auto-layout	`/, /usr, /var, /export`	
Preserve existing data?	**No**	There is no upgrade option in this release.
Reboot	Yes	
Root password	<List it elsewhere>	Workstation security requires a root password..

F

OS Server Disk Partitioning Example

Workstation Name: heron

Disk	Slice	Mount point	Size	Disk	Slice	Mount point	Size
c0t0d0	**s0**	/		c0t1d0	**s0**		
	s1	swap			**s1**		
	s2	entire disk	1034		**s2**	entire disk	1980
	s3				**s3**		
	s4	/var			**s4**		
	s5				**s5**		
	s6	/usr			**s6**		
	s7				**s7**	/export/home	

Disk	Slice	Mount point	Size	Disk	Slice	Mount point	Size
c0t3d0	**s0**	/export/root (30/client)	120	c0t5d0	**s0**		
	s1	/export/swap (24/client)	96		**s1**		
	s2	entire disk	1980		**s2**	entire disk	1980
	s3				**s3**		
	s4	/export/exec			**s4**		
	s5				**s5**		
	s6				**s6**		
	s7				**s7**		

OS Server Configuration Worksheet

System Administrator Information		**Security Officer Information**	
Name	heron	**root password**	
IP address	129.159.110.11	**PROM mode**	full
Ethernet address	8:0:20:8a:2d:f	**PROM password**	
Sun architecture	sun4m		
Network interface	le1 (129.159.118.0)		
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/Sol251/		
for TS AnswerBks	/usr/AB/TS25/		
for ManPages	/usr/shar/man		
for CodeMgr	/opt/prog/Code		
for Utilities	/opt/dist/Util		
for Applications	/opt/dist/App		
Audit Mount Points			
Primary	/etc/security/audit/tern.4		nosuid, nodevices, [high]
Secondary	/etc/security/audit/egret.4		nosuid, nodevices, [high]
Local	/etc/security/audit/hurricane		nosuid, nodevices, [high]
Audit File Systems			
Primary	tern:/etc/security/audit/tern.4/files		
Secondary	egret:/etc/security/audit/egret.4/files		
Local	/etc/security/audit/willet/files		
Diskless Clients			
nestling	/export/root/*clientname*...		
babybird	/export/swap/*clientname*...		
juniorbird	/export/root/*clientname*/usr/AB		
tinytweet	/export/root/*clientname*/opt		
smalldove	/export/root/*clientname*/shar		
tinkerbell			

F

System Administrator Information		Security Officer Information
Mail Server	grebe	
Attached Devices	None	
Remote Printers		
	cirrus	
	cumulus	Administrator printer [admin_high] only

*Remote Hosts (*tnrhdb*) Worksheet for NIS+ Root Master - Example*

System Administrator Information		Security Officer Information	
Name	dickinson	**Template**	unlab
IP address	129.159.129.11		
Host_type	unlabeled		
Use	file server		
Name		**Template**	sun_tsol2
IP address	129.159.150.0		
Host_type	sun_tsol		
Use	another TS2.5 domain		
Name	aptitude	**Template**	unlab_conf
IP address	129.159.129.12		
Host_type	unlabeled		
Use	application server		
Name	chincoteague	**Template**	unlab_uncl_write
IP address	129.159.129.10		
Host_type	unlabeled		
Use	print server (unclassified)		

*Remote Hosts (*tnrhdb*) Worksheet for Individual Workstations - Example*

System Administrator Information		Security Officer Information	
Workstation name	grebe **communicates with**		
Remote host	nestleberry	**Template**	ripso_1
IP address	129.159.132.12		
Host_type	RIPSO		
Use	NIS+ man pages		
Workstation name	grebe **communicates with**		
Remote host	diogenes	**Template**	cipso_0
IP address	129.159.132.11		
Host_type	CIPSO		
Use	network diagnostics		

F

User Worksheet Example

User: Katherine Pollit		
Identity	User name	pollitk
	User ID	2001
	Primary Group	staff, admin
	Secondary Groups	analysts
	Comment	Kathy Pollit
	Login Shell	C shell
	User Type	Normal
Home	Create home dir automatically?	Yes
	Home directory	/export/home/pollitk
	Path to setup files	/etc/skel/tsol
	Default permissions	rwxr-----
	Mail server	grebe
	AutoHome setup?	No
Password	Password generation method	Type in
	Minimum days between changing passwords	
	Maximum days between changing passwords	
	Maximum time a user can be inactive	
	Status	Open
	NIS+ credentials?	Yes
Idle	Idle time	120 minutes
	Idle action: logout | lock screen	Lock screen
Labels	Clearance	TS ABLE BAKER
	Minimum label	Confidential
	View - External or Internal?	External
	Sensitivity Label visible or not visible?	visible
	Information Label visible or not visible?	visible
Profiles	All | Nothing | ...	All, Enable Login, Convenient Authorizations
Roles	secadmin | admin | root | oper	secadmin

Troubleshooting G

This appendix describes problems you may encounter when installing Trusted Solaris software, and suggests possible solutions. You may also encounter errors from parts of the underlying Solaris 2.5.1 operating system that remain unmodified. Therefore, check the Troubleshooting section of the installation manual for Solaris 2.5.1 when you encounter a problem installing Trusted Solaris 2.5.

The following table shows common error messages and the page number where you can find causes and possible solutions.

G

Specific Installation Errors

```
WARNING: RPC Timed out
```

Reason Error Occurred

This error occurs when you have two or more servers on a network responding to an install client's boot request. The install client connects to the wrong boot server, and the installation hangs. The following specific problems may cause this error:

- There may be `/etc/bootparams` files on different servers with an entry for this install client.
- There may be multiple `/tftpboot` or `/rplpboot` directory entries for this install client.
- There may be an install client entry in the `/etc/bootparams` file on a server and an entry in another `/etc/bootparams` file enabling all systems to access the profile server. Such an entry would look like this:

`* install_config=`*profile_server*`:`*path*

A line like this in the NIS+ `bootparams` table would also cause this error.

How to Fix the Problem

Examine the network setup:

- Ensure that servers on the network do not have multiple `/etc/bootparams` entries for the install client. If they do, remove duplicate client entries in the `/etc/bootparams` file on all install and boot servers except the one you want the install client to use.
- Ensure that servers on the network do not have multiple `/tftpboot` or `/rplboot` directory entries for the install client. If they do, remove duplicate client entries from the `/tftpboot` or `/rplboot` directories on all install and boot servers except the one you want the install client to use.
- If there's a wildcard entry in the name service `bootparams` map or table (for example, `* install_config=`), delete it and add it to the `/etc/bootparams` file on the boot server.

Time Zones

The next page shows time zones of the world by hours offset from Greenwich Meantime. This may be useful when setting a system's clock during the Solaris installation program.

Figure H-1 reflects Standard Time. If daylight saving time is in effect, add one hour.

H

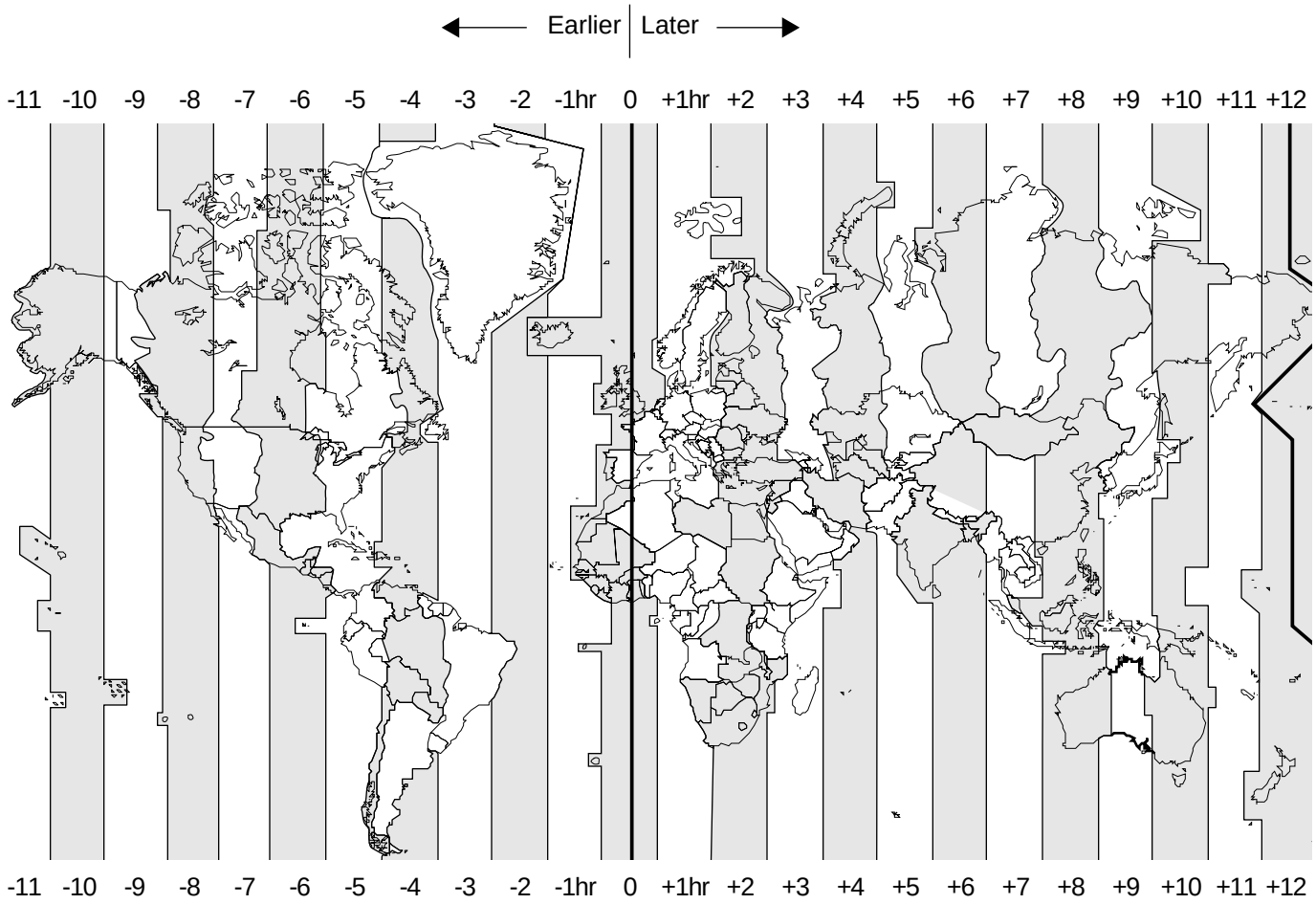


Figure H-1 Greenwich Meantime Map

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 indisviduals and groups, allowing finer-grained control than provided by the standard UNIX *permission bits*.

ACL

See *access control list*.

accreditation range

A set of valid *label*s. See *system accreditation range* and *user accreditation range* for more about the two types of accreditation ranges in the Trusted Solaris environment.

administrative role

A *role* defined in the Trusted Solaris software that gives required *authorization*s, privileged commands, and the Trusted Path *security attribute* to allow the role to perform part of superuser's capabilities, such as backup or auditing. The predefined administrative roles are secadmin, sysadmin, oper, and root.

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. Not all devices are allocatable. Allocatable devices include tape drives, floppy drives, audio devices, and CD-ROM devices. See *device allocation*.

I

allowed privilege set

The allowed set of privileges limits which *privilege*s 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 profile*s. Certain commands require the user to have certain authorizations to succeed. Similar to the use of *privilege* on programs.

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 2.5 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 installation*s.

bootparams file

A file that is consulted when a workstation boots. In Trusted Solaris 2.5, 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.

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 information label followed by a sensitivity label in brackets, in the form: INFORMATION LABEL [SENSITIVITY LABEL].

Common Desktop Environment

The required windowing environment for administering the Trusted Solaris software.

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 2.5 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*.

I

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 officer*.

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 *profile*s on different sized disks.

diskless client

A networked system that does not have its own disk, so it relies completely on an *OS server* for software and file storage. Diskless clients do not have to use the Trusted Solaris installation program, because they use the software that is already installed on an *OS server*.

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* that contains the entire Trusted Solaris release, plus additional hardware support for OEMs. This *software group* is recommended when installing Trusted Solaris software on servers.

/etc

A directory that contains critical system configuration files and maintenance commands.

execution profile

A bundling mechanism for commands and CDE actions and for the *security attribute*s assigned to the commands and CDE actions. Execution 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 execution profiles assigned to that user are in effect, and the user has access to all the commands, CDE actions, and *authorization*s assigned in all of that user's execution 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 root file system and swap for *diskless client*s and the home directories for users on the network. Diskless clients rely on the `/export` file system on an *OS server* to boot and run.

file server

A server that provides the software and file storage for systems on a network.

I

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 *custom JumpStart installations*.

forced privilege set

The forced set of privileges are those placed on a file by the *security officer*. 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.

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*.

information label floating

A conjoining of two *information label*s that occurs when a file or directory with one *information label* is accessed by a process that has another *information label*, the resulting *information label* reflects the combined security level of both *information label*s.

inheritable privilege

The *privilege*s that a process can pass to a program across an execve(2V) 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 *privilege*s 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 2.5 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 CD-ROM 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.

I

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).

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 installation*s, 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 2.5 release does not offer this option; all JumpStart installations in Trusted Solaris 2.5 are *custom JumpStart installation*s.

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 officer* 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; enable or disable information labels; if enabled, enable or disable IL floating and enable or disable resetting IL upon exec. 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 label*s assigned to commands, file systems, and allocatable *device*s, specified by designating a maximum label and a minimum label. For commands, the minimum and maximum labels limit the *sensitivity label*s at which the command may be executed. For file systems, the minimum and maximum labels limit the *sensitivity label*s 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 officer* wishes to restrict to a single label; labels limit the *sensitivity label*s at which *device*s may be allocated and restrict the *sensitivity label*s 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*.

locale

A specific language associated with a region or territory.

I

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*.

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 officer 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 (*SLD*s), 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 *MLD*s. 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 *system*s on a network.

name service

A distributed network database that contains key system information about all the *system*s 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+. Trusted Solaris supports 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 *system*s (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 *root NIS+ master*.

non-networked systems

Systems that are not connected to a network or do not rely on other systems.

/opt

A *file system* that contains the mount points for third-party and unbundled software.

I

OS server

A *system* that provides services to systems on a network. To serve *diskless client*s, an OS server must have disk space set aside for each *diskless client*'s root file system and swap space (`/export/root`, `/export/swap`).

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 *package*s.

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.

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 officer* 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 attribute*s 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 *privilege*s 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.

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*.

role

A role is a user who 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 *root master server*.

root NIS+ master

The workstation that contains the master files for a NIS+ network. Also called a root master or a NIS+ 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 *profile*s.

I

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 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 *process*es, users, files, directories, hosts on the trusted network, allocatable *device*s, and other entities.

security officer

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 attribute*s of all users and workstations so that the software enforces the site's security policy.

security policy

In the Trusted Solaris environment, the set of *DAC*, *MAC*, and *information label*ing 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 (*cluster*s and *package*s). During a Solaris installation, you can install one of the following software groups: core, end user system software, developer system support, or entire distribution.

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 accreditation range

The set of all valid (well-formed) *label*s created according to the rules defined by each site's *security officer* in the *label_encodings file*, plus the two administrative *label*s that are used in every Trusted Solaris environment, ADMIN_LOW and ADMIN_HIGH.

system

Generic name for a workstation. After installation, a system is often called a host.

I

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*, *OS server*, and *diskless client*.

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.

Trusted Network databases

tnrhtp, the Trusted Network Remote Host TemPlate and tnrhdb, the Trusted Network Remote Host DataBase together define the *remote host*s 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, the input information label and window sensitivity label. When either *sensitivity label*s or *information label*s are configured to not be viewable for a user, then the type of label that is viewable is displayed and the other is not. When neither *sensitivity label*s or *information label*s are configured to be displayed for a user, the trusted stripe is reduced to an icon that displays only the trusted path indicator.

tsolprof database

The Trusted SOLaris PROFiles database, accessible either as a file in `/etc/security/tsol/tsolprof` or as a NIS+ table. After configuration, it contains *execution profile*s provided by the Trusted Solaris software.

tsoluser database

The Trusted SOLaris USER database, accessible either as a file in `/etc/security/tsol/tsoluser` or as a NIS+ table. After configuration, it contains *role*s 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 2.5 release.

unlabeled workstation

A workstation that sends unlabeled network packets, such as Solaris 2.5.1.

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 officer*. The rules for well-formed *label*s that define the *system accreditation range* are additionally restricted by the values specified in the ACCREDITATION RANGE section of the site's `label_encodings(4TSOL)` file: the upper bound, the lower bound, the combination constraints and other restrictions.

user clearance

The *clearance* assigned by the *security officer* that sets the upper bound of the set of *label*s 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.

I

/var

A *file system* or directory (on *standalone system*s) 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 CD-ROMs and diskettes. This program is disabled in the Trusted Solaris 2.5 release.

Index

Symbols

A

B

C

D

E

F

G

H

O

P

R

S

T

U

V

W

Z