Trusted Solaris Installation and Configuration

Trusted Solaris 2.5.1

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

Part No: 805-8026-10
Revision A, August 1998

THE NETWORK IS THE COMPUTER™

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

Sun, Sun Microsystems, the Sun logo, SunSoft, SunDocs, SunExpress, and SunOS, OpenWindows, NFS, Sun Ultra, Ultra, JumpStart, Solaris, AnswerBook, AnswerBook logo, Solstice, Solstice AdminSuite, Solstice AdminTools, Solstice Autoclient, Solstice CacheOS, Disksuite, ToolTalk, X11 / NeWS, Trusted NeWSprint, IPC, OpenBoot, SHIELD, XView, SunInstall, and Trusted Solaris are trademarks, registered trademarks, or service marks of Sun Microsystems, Inc. in the U.S. and other countries. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc . X / Open® is a registered trademark and "X" device is a trademark of X / Open Company Limited, Netscape is a trademark of Netscape Communications Corporation, and PostScript is a trademark of Adobe Systems, Incorporated.

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

RESTRICTED RIGHTS: Use, duplication, or disclosure by the U.S. Government is subject to restrictions of FAR 52.227-14(g)(2)(6 / 87) and FAR 52.227-19(6 / 87), or DFAR 252.227-7015(b)(6 / 95) and DFAR 227.7202-3(a).

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

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

Sun, Sun Microsystems, le logo Sun, SunSoft, SunDocs, SunExpress, et Solaris SunOS, OpenWindows, NFS, Sun Ultra, Ultra, JumpStart, AnswerBook, AnswerBook logo, Solstice, Solstice AdminSuite, Solstice AdminTools, Solstice Autoclient, Solstice CacheOS, Disksuite, ToolTalk, X11 / NeWS, Trusted NeWSprint, IPC, OpenBoot, SHIELD, XView, SunInstall, et Trusted Solaris sont des marques de fabrique ou des marques déposées, ou marques de service, de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pays. Toutes les marques SPARC sont utilisées sous licence et sont des marques de fabrique ou des marques déposées de SPARC International, Inc. aux Etats-Unis et dans d'autres pays. Les produits portant les marques SPARC sont basés sur une architecture développée par Sun Microsystems, Inc. .X / Open® est une marque enregistrées et "X" device est une marque de X / Open Company Limited, Netscape est une marque de Netscape Communications Corporation, et PostScript est une marque de Adobe Systems, Incorporated.

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

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

Contents

Figures

Tables

About This Book

Who is the Audience?

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

Implement Trusted Solaris in Accordance with Site Security

Successfully installing and configuring Trusted Solaris consistent with site security requires understanding the security features of Trusted Solaris and your site security policy. Before attempting to install Trusted Solaris, read Chapter 1, “Overview” for the steps to implement your site security when installing and configuring the Trusted Solaris environment at your 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. "Install the Trusted Solaris Software." on page 11 describes the methods; the task maps beginning on page 16 outline the steps.

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

Planning a Secure Installation

Chapter 1, "Overview" *page 1*

Common Installation and Configuration Procedures

Chapter 2, "Basic Procedures" *page 21*

Installing Trusted Solaris

Chapter 3, "Installing a Workstation" *page 53*

Configuring the NIS+ Root Master

Chapter 5, "Configuring the NIS+ Root Master" *page 71*

Configuring a Non-Networked Workstation

Chapter 4, "Configuring a Workstation without the NIS+ Name Service" *page 63*

Configuring NIS+ Clients

Chapter 6, "Configuring a NIS+ Client" *page 97*

Installing NIS+ Clients Over the Network

Chapter 7, “Preparing to Install Trusted Solaris Over a Network”	*page 107*
Chapter 6, “Configuring a NIS+ Client”	*page 97*
Chapter 3, “Installing a Workstation”	*page 53*

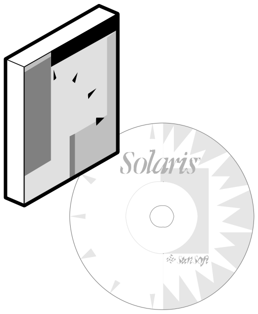
Installing and Configuring NIS+ Clients Using Custom JumpStart

Chapter 8, “Preparing Custom JumpStart Installations”	*page 129*
Chapter 9, “Using Optional Custom JumpStart Features”	*page 173*
Chapter 3, “Installing a Workstation”	*page 53*

Configuring and Booting Diskless Clients

Chapter 10, “Configuring Diskless Clients”	*page 189*

Related Books



The following books contain information useful when installing Trusted Solaris software.

Books from Sun Microsystems

- *Trusted Solaris 2.5.1 Release Notes* – Describes late-breaking news about installing Trusted Solaris software including known problems.
- *Solaris 1.x to 2.x Transition Guide,* PN802-5399 – Describes transition issues including backing up 4.1.x files before installing Solaris software, and restoring files after Solaris software is installed. Applicable to the Trusted Solaris environment.
- *System Administration Guide, Volume I: Solaris 2.5* PN802-5416 – Describes basic administrative tasks in Solaris 2.5.1, such as creating and mounting file systems.
- *System Administration Guide, Volume II: Solaris 2.5* PN802-5417 – Describes more advanced administrative tasks in Solaris 2.5.1, such as configuring printing.

- *Solstice AdminSuite 2.3 Administration Guide*, PN805-3026 – Describes the basic applications that Trusted Solaris 2.5.1 uses to administer the network. Trusted Solaris 2.5.1 has modified the applications; the modifications are described in *Trusted Solaris Administrator's Procedures*.
- *TCP/IP and Data Communications Administration Guide*, Chapter 3, "Planning Your Network" – Describes how to set up a network. Required for networked sites only.
- *NFS Administration Guide*, PN802-1963 – Describes how to administer a networked file system. Recommended for a network installation.
- *NIS+ and DNS Setup and Configuration Guide*, PN802-1964 – Describes how to set up and configure a NIS+ domain. Required for networked sites.
- *NIS+ and FNS Administration Guide*, PN802-5542 – Describes how to administer and troubleshoot a NIS+ domain. Recommended for networked sites.
- *Trusted Solaris Administrator's Procedures* – Describes administration tasks in detail.
- *Trusted Solaris Audit Administration* – Describes auditing one or more Trusted Solaris workstations.
- *Trusted Solaris Label Administration* – Describes labels and includes a copy of *Compartmented Mode Workstation Labeling: Encodings Format* issued by the U.S. government.

Books from Elsewhere

- *Your site security policy document*

  Describes the security policy and security procedures at your site.

- *Solaris Common Desktop Environment: Advanced User's and System Administrator's Guide*

  Describes the Common Desktop Environment.

- *The administrator guide for your currently installed operating system.*

  Describes how to back up system files. See the *Trusted Solaris 2.5.1 Transition Guide* for any compatibility issues.

- *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, glossary items, or words to be emphasized	Read Chapter 6 in *User’s Guide*. These are called *.copy_files*. You *must* be root to do this.
`Italic Type`	Used in examples: replace with an appropriate value	`Password:` ***`password`***

Which Trusted Solaris Prompts Indicate Particular Environments

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

Overview 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. The first section, "The Big Picture", is written for administrators new to the Trusted Solaris operating environment. The next section, "Differences from Solaris 2.5.1 Installation and Configuration", addresses specific differences from base Solaris, and was written with experienced Solaris administrators in mind. The third section, "Installation Results from an Administrator's Perspective", describes the security features in effect after a workstation is installed. Appendix C, "Checklists for Configuring and Installing Trusted Solaris" provides a summary of steps.

Customers interested in localizing their site, see "For International Customers" on page 6. Customers interested in running an *evaluated configuration,* see "Understand Your Site's Security Policy." on page 3.

1

The Big Picture

This section outlines the following steps to install and configure the Trusted Solaris operating environment.

- "Understand the Trusted Solaris Environment."
- "Understand Your Site's Security Policy."
- "Devise an Administration Strategy."
- "Devise a Label Strategy."
- "Plan Workstation Hardware and Capacity."
- "Plan Your Network."
- "Plan Auditing."
- "Devise an Installation and Configuration Strategy."
- "Collect Information."
- "Back Up the Workstation."
- "Install the Trusted Solaris Software."
- "Configure the Software."

1 Understand the Trusted Solaris Environment.

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

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

To familiarize yourself with the Trusted Solaris environment, you should at a minimum read the *Trusted Solaris User's Guide* and *Trusted Solaris Administration Overview*. You should also be familiar with the rest of the documentation set, which is described in the *Trusted Solaris Documentation Roadmap*. It is highly recommended that you attend a “Trusted Solaris for System Administrators” course, available from SunEd University. Ask your Sun account representative to help you schedule it.

2 Understand Your Site’s Security Policy.

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

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

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

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

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

3 Devise an Administration Strategy.

In place of superuser, the Trusted Solaris environment provides three trusted *administrative roles* for managing the environment:

- The *security administrator* is responsible for security-related tasks, such as setting up and assigning sensitivity labels, configuring auditing, and setting password policy.
- The *system administrator* is responsible for the non-security aspects of setup, maintenance, and general administration.
- The root *role* is mainly responsible for installing application software after the initial Trusted Solaris installation, in contrast to root's broader responsibilities in traditional UNIX environments.

There is also a less trusted role called "oper" for operator, that is responsible for backing up files. Since the environment is configurable, you can use these default roles, modify them, or create your own roles according to your security needs.

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

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

4 Devise a Label Strategy.

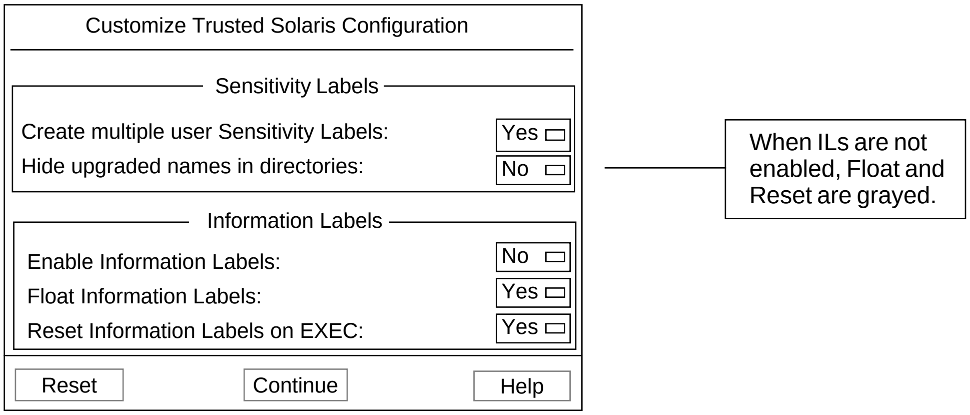
Planning labels requires setting up a hierarchy of sensitivity levels and a categorization of information in your environment. The "label encodings" file contains this type of information for your organization. You can use one of the *label_encodings files* supplied on the Trusted Solaris CDROM, modify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

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

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

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

Planning labels also involves planning label configuration. The Trusted Solaris installation program offers label configuration options, as shown in the following figure.



Customize Trusted Solaris Configuration

Sensitivity Labels

Create multiple user Sensitivity Labels: Yes

Hide upgraded names in directories: No

Information Labels

Enable Information Labels: No

Float Information Labels: Yes

Reset Information Labels on EXEC: Yes

When ILs are not enabled, Float and Reset are grayed.

Figure 1-1 Trusted Solaris Label Configuration Options

Prior to installation, you need to make the following decisions regarding the use of labels:

- Single- or multiple-label environment – If all of your non-administrative users can operate at the same security label, select a single-label system. Multiple-label environments are required for the FB1 level. If you want a no-label system, select single-label, and then hide the labels for all users.
- Hide or display upgraded names in directories – If you want to prevent a user (or intruder) from viewing the names of files or directories at higher levels than the current sensitivity label, choose this option.
- Enable or disable information labels – If dissemination of information at the wrong level is potentially a major security problem, you should enable information labels. Information labels are disabled by default.

- Float information labels or leave up to user – If you enable information labels, you can let users decide at which level a document comprising data at different information labels should be tagged or you can force the resulting document to be tagged at the highest information label in the transaction.
- Reset information labels on EXEC – You can let child processes be tagged at the information label of the parent EXECing them or you can let the child process be classified at the default (minimum) information label.

After installation, you can make the following label configuration display changes using the Solstice AdminSuite User Manager:

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

For International Customers

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

5 Plan Workstation Hardware and Capacity.

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

The following table lists the hardware and capacity required to run a Trusted Solaris environment. For a complete list of supported hardware and peripherals, see Appendix D, "Supported Hardware Components".

Table 1-1 Hardware Requirements

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

Memory over the minimum is required on Trusted Solaris 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
- Run at more than one sensitivity label
- Are used by users who can assume an administrative role

Similarly, disk space requirements are greater 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 the larger software clusters: Developer and Entire.
- Run at more than one label
- Are used by users who can assume an administrative role

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

- Name and IP address
- Ethernet address (for network installations)
- Sun architecture (for network installations)
- Root password
- PROM security level: maintenance password only, or boot password
- PROM password
- What devices may be attached to the workstation
- Which users may use the workstation
- Which printers at what labels may the workstation access

6 Plan Your Network.

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

For help in planning network hardware, see *TCP/IP and Data Communications Administration Guide*, Chapter 3, "Planning Your Network".

As in any client-server network, you need to identify hosts by their function (server or client) and configure the software appropriately. The following table lists servers you may need to create and their function. For more information, see the *System Administration Guide, Volume I* for Solaris 2.5 releases.

Table 1-2 Possible Servers in a Trusted Solaris Environment

Create …	If You Plan to …
Audit data server	Enable auditing
Audit administration server	Analyze the audit trail
Boot server	Install on a subnet
File server	Centrally locate files for general use
Install server	Install over the network or use Custom JumpStart scripts
DNS server	Resolve internet names and addresses outside your local network
Home directory server	Enable remote mounting of users' home directories.
Mail server	Funnel mail to end user workstations from a central location
Network gateway	Operate an *open network*
NIS+ root master (Name Server)	Establish a NIS+ domain

Table 1-2 Possible Servers in a Trusted Solaris Environment

Create …	If You Plan to …
NIS+ replicas	Establish a NIS+ domain
NIS+ subdomain masters	Establish a NIS+ subdomain
OS server	Serve diskless clients
Print server	Print hard copy

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*
- *NIS+ and DNS Setup and Configuration Guide*
- *User Accounts, Printers, and Mail Administration*

OS servers are covered in the *Solstice AdminSuite 2.3 Administration Guide*.

Additional Planning for Open Networks

If your network is open to other networks, you need to specify accessible domains and workstations, and identify which Trusted Solaris hosts will serve as gateways to access them. You need to identify the Trusted Solaris *accreditation range* for these gateways, and the *sensitivity label* at which data from other hosts may be viewed. Trusted Solaris software recognizes five labeled host types, including Trusted Solaris (`sun_tsol`), and provides eight templates by default, as shown in the following table.

Table 1-3 Templates Provided with Trusted Solaris Network Software

Host Type	Template Name	Purpose
Unlabeled	`unlab`	For hosts or networks that send unlabeled packets, for example, SUN workstations running Solaris software
Labeled		
Trusted Solaris 2.5.1 (`sun_tsol`)	`tsol`	For Trusted Solaris 2.5.1 hosts or networks
	`tsol_1`	For TS2.5.1 hosts or networks that label packets with the RIPSO security option

Table 1-3 Templates Provided with Trusted Solaris Network Software

Host Type	Template Name	Purpose
	`tsol_2`	For TS2.5.1 hosts or networks that label packets with the CIPSO security option
TSIX	`tsix`	For TSIX(RE1.1) hosts or networks
MSIX	`msix`	For hosts or networks that run Trusted Solaris 1.2 software
CIPSO	`cipso`	For hosts or networks that send CIPSO packets
RIPSO	`ripso`	For hosts or networks that send RIPSO packets

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

For more information on the security administration of servers, file systems, and network interfaces, see *Trusted Solaris Administrator's Procedures*.

7 Plan Auditing.

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

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

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

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

8 Devise an Installation and Configuration Strategy.

The Trusted Solaris software is initially loaded by root. Since root cannot log into the Trusted Solaris environment, a pseudo-user named “install” has been provided for the first part of the configuration process. Subsequent configuration is a two-person process (by default) using the security administrator and the system administrator roles. Once the roles have been assigned to users, and the workstation is rebooted, the software enforces task division by role.

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

In a networked environment, consider installing and configuring workstations in the order NIS+ master, other NIS+ servers, other servers, and finally end user workstations.

9 Collect Information.

Each role needs to gather the information for the tasks particular to the role. There are blank copies of worksheets for your site’s installation and configuration specifics in Appendix B, “Worksheets for Configuring and Installing Trusted Solaris”.

Completed sample worksheets are in Appendix F, “Example Worksheets”.

10 Back Up the Workstation.

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

11 Install the Trusted Solaris Software.

Installing Trusted Solaris can be done interactively using CDROMs, over the network, or with Custom JumpStart scripts. The first two workstations, the NIS+ root master and the install server (if you wish to do network or Custom JumpStart installs), must be installed interactively; subsequent workstations can be installed using the server. Installing over the network requires network setup; the installation program prompts the install team for needed information. Using Custom JumpStart requires some knowledge of Bourne shell scripting to automate installation; however, you can write scripts where no human interaction with the installation program is required.

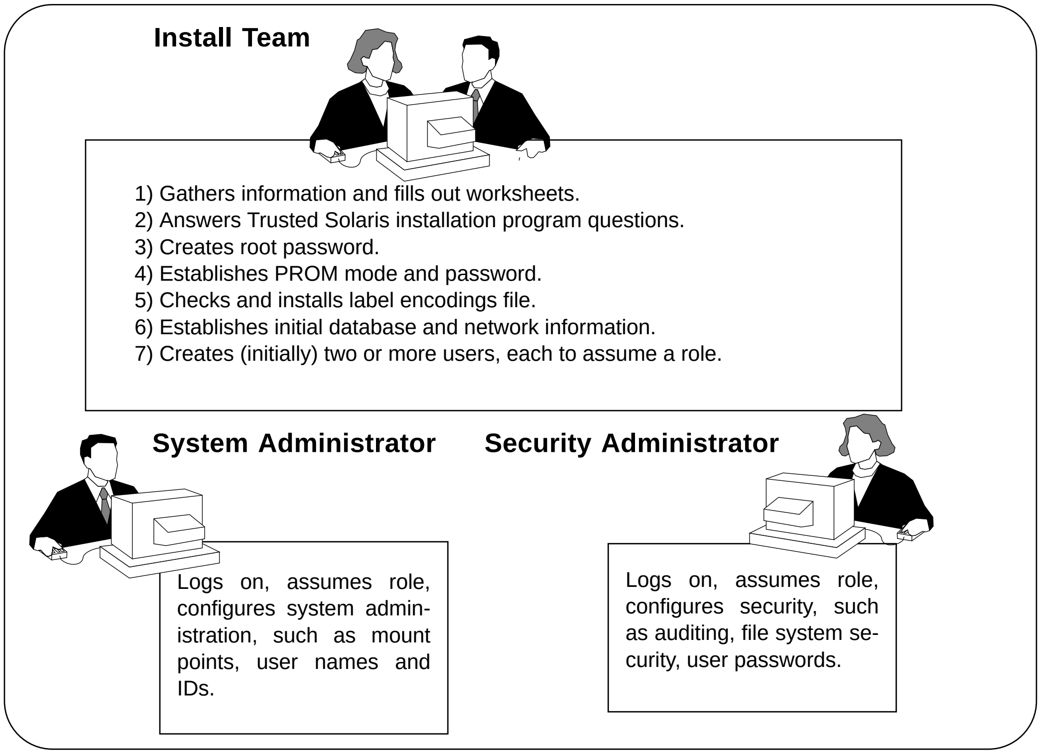
♦ **Use the task maps to guide you through the different installation methods.**

Task Map: Interactive CDROM Installations	*page 16*
Task Map: Network Installations	*page 17*
Task Map: Network Custom JumpStart Installations	*page 18*
Task Map: CDROM + Diskette Custom JumpStart Installations	*page 19*
Task Map: Diskless Booting	*page 20*

For security reasons, the installation program does not offer some of the options that are available for Solaris 2.5.1 software. See "Differences from Solaris 2.5.1 Installation and Configuration" on page 14 for details.

12 Configure the Software.

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



1) Gathers information and fills out worksheets.
2) Answers Trusted Solaris installation program questions.
3) Creates root password.
4) Establishes PROM mode and password.
5) Checks and installs label encodings file.
6) Establishes initial database and network information.
7) Creates (initially) two or more users, each to assume a role.

Logs on, assumes role, configures system administration, such as mount points, user names and IDs.

Logs on, assumes role, configures security, such as auditing, file system security, user passwords.

Figure 1-2 Two Roles Administering a Workstation

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

The security administrator sets up auditing, protects file systems, sets device policy, and protects users, among other tasks. The system administrator shares and mounts file systems and creates users, among other tasks.

Differences from Solaris 2.5.1 Installation and Configuration

Two products that are unbundled in the Solaris environment are bundled in the Trusted Solaris environment. CDE is the only desktop supported and installed by Trusted Solaris software, and the Solstice™ AdminSuite™ GUIs manage local and network administrative databases.

Some options that are available when installing Solaris 2.5.1 software are not available when installing Trusted Solaris software. Specifically,

- No factory JumpStart™. Custom JumpStart support with Trusted Solaris configuration options is provided.
- No remote filesystem mounting during installation. File systems are mounted after installation.
- Upgrading, from Trusted Solaris 2.5 software only, is possible.
- Volume Manager is not supported.
- Solstice™ AutoClient™ or dataless clients are not supported.
- 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.

Installation Results from an Administrator's Perspective

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

- Auditing is enabled.
- A SUN *label_encodings file* is configured and installed.
- The *Common Desktop Environment* (CDE) creates four labeled workspaces.
- Three *administrative role*s secadmin, admin, and root are defined.
- A shell called the *profile shell* is assigned by default as the initial shell for the administrative roles. A profile shell recognizes security-relevant commands.
- A trusted editor is available to administrators for modifying local administrative files. It is implemented as a CDE action named Admin Editor.

- The Solstice AdminSuite GUIs are available to *administrative roles* to administer user, *execution profile*, and other system databases.
- Trusted Solaris-defined CDE actions to view and edit local administrative files in a trusted editor are available to users in administrative roles.
- The Device Allocation Manager manages attached devices.
- One non-administrative role, oper, is defined.
- Several execution profiles are defined to delimit the actions that users and roles can execute. They are defined in the Trusted Solaris database, `tsolprof`.
- A Trusted Solaris-defined database, `tsoluser`, handles users, roles, and their system and security information.
- Three Trusted Solaris-defined databases, `tnidb`, `tnrhtp`, and `tnrhdb`, handle trusted networking.

Task Map: Interactive CDROM Installations

Activity	Description	Read	
Gather information	**Plan**	Chapter 1, “Overview”	page 1
	Use worksheets to gather answers to questions asked by the Trusted Solaris installation program.	Appendix B, “Worksheets for Configuring and Installing Trusted Solaris”	page 207
Back up your files	**Save important data**	***Your current workstation backup procedures***	
Install Trusted Solaris software	**Install from local CDROM** Boot and install Trusted Solaris software.	Chapter 3, “Installing a Workstation”	page 53
	Do one of:		
Configure Trusted Solaris software	**Configure NIS+ master** Configure and create a NIS+ master.	Chapter 5, “Configuring the NIS+ Root Master”	page 71
	Configure non-networked workstation Configure Trusted Solaris local administrative files.	Chapter 4, “Configuring a Workstation without the NIS+ Name Service”	page 63
	Configure NIS+ client Configure and create a NIS+ client.	Chapter 6, “Configuring a NIS+ Client”	page 97

Figure 1-3 Task Map for Interactive CDROM Installations

Task Map: Network Installations

Activity	Description	Read	
Gather information	**Plan**	Chapter 1, “Overview”	page 1
	Use worksheets to plan server configurations.	Appendix B, “Worksheets for Configuring and Installing Trusted Solaris”	page 207
Use a NIS+ client …	**Start with a configured NIS+ client (See “Task Map: Interactive CDROM Installations”)**	Chapter 6, “Configuring a NIS+ Client”	page 97
… as network server	**Set up install server and boot server on the network** Set up servers for network installations.	Chapter 7, “Preparing to Install Trusted Solaris Over a Network”	page 107
Install Trusted Solaris software over the net	**From another system on the network** Type `boot net`	Chapter 3, “Installing a Workstation”	page 53
	Do one of:		
Configure Trusted Solaris software	**Configure NIS+ client** Configure and create a NIS+ client.	Chapter 6, “Configuring a NIS+ Client”	page 97
	Configure non-networked workstation Configure Trusted Solaris local administrative files.	Chapter 4, “Configuring a Workstation without the NIS+ Name Service”	page 63

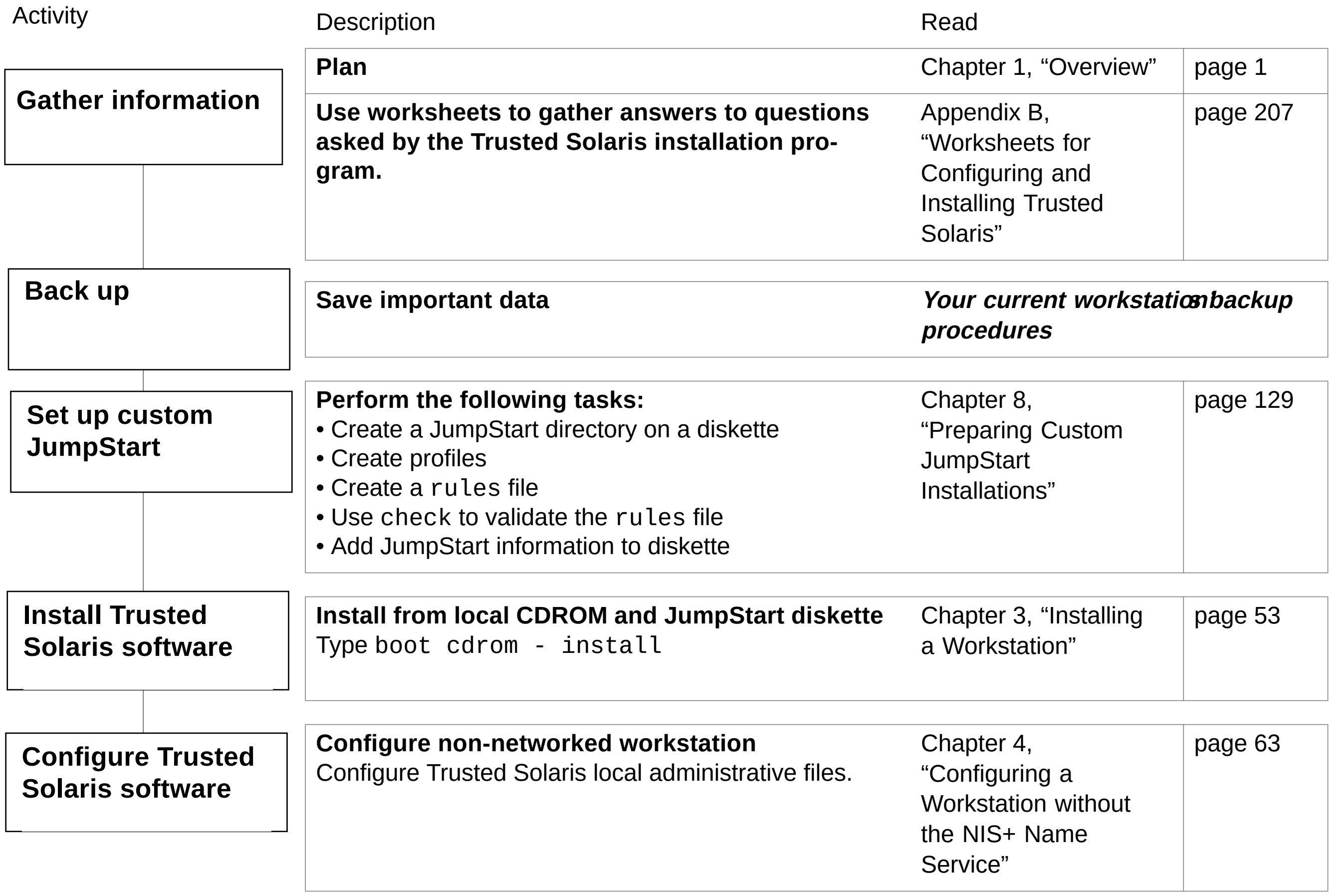
Figure 1-4 Task Map for Network Installations

Task Map: Network Custom JumpStart Installations

Activity	Description	Read	
Gather information	**Plan**	Chapter 1, “Overview”	page 1
	Use worksheets to plan workstation configurations.	Appendix B, “Worksheets for Configuring and Installing Trusted Solaris”	page 207
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 107
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 129
Install Trusted Solaris software	**From another system on the network** Type `boot net - install`	Chapter 3, “Installing a Workstation”	page 53
Configure Trusted Solaris Software	**Configure each custom JumpStart client** Finish configuring a NIS+ client.	Chapter 6, “Configuring a NIS+ Client”	page 97

Figure 1-5 Task Map for Network Custom JumpStart Installations

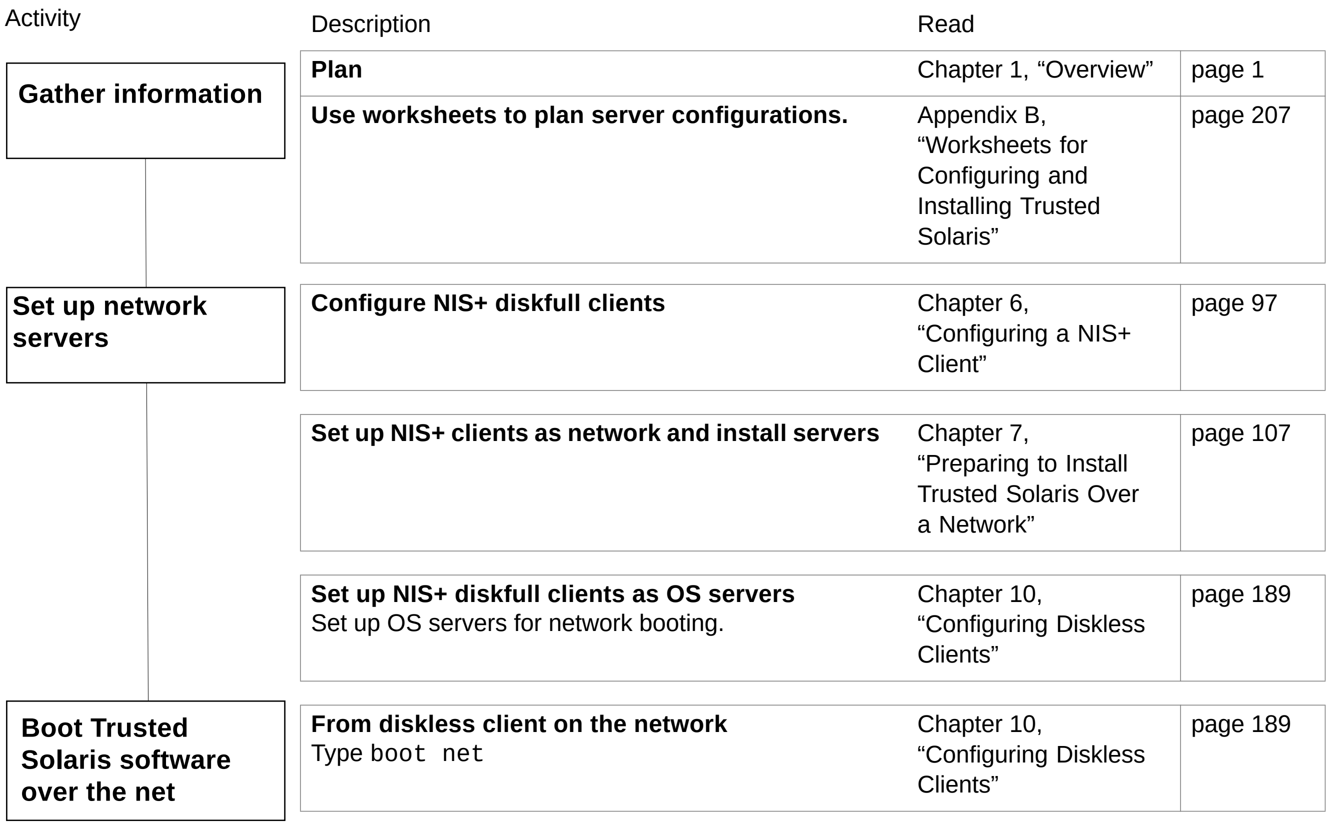
Task Map: CDROM + Diskette Custom JumpStart Installations



Activity	Description	Read	
Gather information	**Plan**	Chapter 1, “Overview”	page 1
	Use worksheets to gather answers to questions asked by the Trusted Solaris installation program.	Appendix B, “Worksheets for Configuring and Installing Trusted Solaris”	page 207
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 129
Install Trusted Solaris software	**Install from local CDROM and JumpStart diskette** Type `boot cdrom - install`	Chapter 3, “Installing a Workstation”	page 53
Configure Trusted Solaris software	**Configure non-networked workstation** Configure Trusted Solaris local administrative files.	Chapter 4, “Configuring a Workstation without the NIS+ Name Service”	page 63

Figure 1-6 Task Map for CDROM Custom JumpStart Installations

Task Map: Diskless Booting



Activity	Description	Read	
Gather information	**Plan**	Chapter 1, “Overview”	page 1
	Use worksheets to plan server configurations.	Appendix B, “Worksheets for Configuring and Installing Trusted Solaris”	page 207
Set up network servers	**Configure NIS+ diskfull clients**	Chapter 6, “Configuring a NIS+ Client”	page 97
	Set up NIS+ clients as network and install servers	Chapter 7, “Preparing to Install Trusted Solaris Over a Network”	page 107
	Set up NIS+ diskfull clients as OS servers Set up OS servers for network booting.	Chapter 10, “Configuring Diskless Clients”	page 189
Boot Trusted Solaris software over the net	**From diskless client on the network** Type `boot net`	Chapter 10, “Configuring Diskless Clients”	page 189

Figure 1-7 Task Map for Diskless Clients

Basic Procedures 2

This chapter covers common administrative procedures when installing and configuring a Trusted Solaris workstation.

Role, Label, and Tool

Role - root
Label - admin_low
Profile shell

A box to the left of a procedure, like the one shown here, is used to indicate the role, label, and tool to be used for the procedure. When more than one role, tool, or label is required, there is a box at every change of role, tool, or label. The *profile shell* is the shell of all administrative roles.

2

List of Basic Procedures

Overview – The following are common procedures when installing and configuring a Trusted Solaris workstation.

How to Log In

The predefined user `install` logs in immediately after installation to configure the workstation.

▼ To Log In as the User "Install"

At most sites, two or more administrators, an *install team*, are present when configuring the workstation. "You", in the following procedure, refers to the install team.

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

   a. **Enter `install` as the user name and press the Return key.**
   The Password dialog box is displayed.

   b. **Enter `install` for the password.**
   The Enable Logins dialog is displayed.

   c. **Click OK to enable logins and dismiss the dialog.**
   The Message Of the Day dialog is displayed; the label is ADMIN_LOW.

   d. **Click OK to dismiss the dialog.**

The Trusted Solaris screen appears briefly.

Then you are in a CDE workspace like the one shown below. The Trusted Stripe below the front panel shows the Input Information Label (if ILs are enabled) and the Window Sensitivity Label.

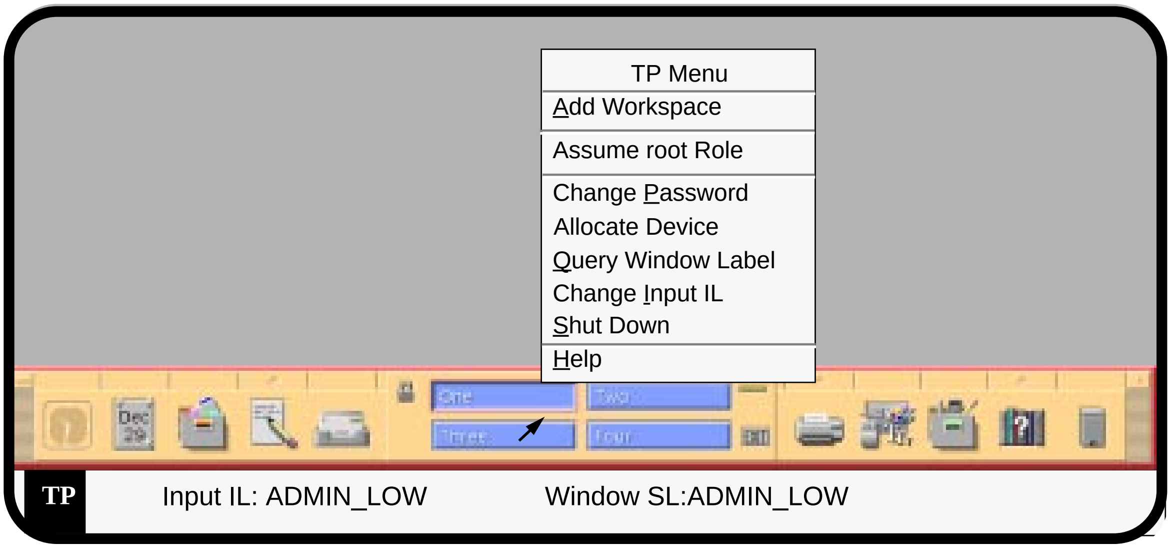


Figure 2-1 The Initial Front Panel and Trusted Path Menu

▼ To Log In as a Regular User

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

2. **Enter your password.**

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

The Enable Logins dialog 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 on page 90). To fix, give the user the Enable Login profile, or have someone else log in and enable logins.

3. **Click OK to enable logins and dismiss the dialog.**
   The Message Of the Day dialog is displayed. In a multilevel session, you can choose to log in at the lowest label in your label range, or to restrict your session to a single label.

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

Once the login process is complete, the Trusted Solaris screen appears briefly, and you are in a CDE session with four workspaces, similar to the one in Figure 2-1. If your user account is configured to display labels, the label of your session (*a* user account *cannot* be ADMIN_LOW) will show in the Trusted Stripe.

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

How to Assume a Role

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

▼ To Assume a Role

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

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

3. **Assume a role from the roles displayed on the TP (Trusted Path) menu, shown in Figure 2-1.**

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

   b. **At the password prompt, enter the password for the role.**
   The password for root is the password you entered for root at the final stage of installation.

How to Launch a Terminal

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

▼ 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.**
   The terminal is displayed with the user or role’s default shell.

How to Open a Profile Shell

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

Note – The default shell of all administrative roles (root, secadmin, and admin) is a profile shell.

▼ To Open a Profile Shell in an Administrative Role

♦ **Launch a terminal.**
The terminal is displayed with the profile shell.

▼ To Open a Profile Shell as a User or Non-Administrative Role

1. **Launch a terminal.**

2. **Type `pfsh` in the terminal to change the shell to a profile shell, if the profile shell has not been assigned as your default shell.**

```
# pfsh
```

▼ To List the Commands Available to a Profile Shell

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

```
# 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 - any
Label - any
Profile shell

▼ To See Process and Privilege Information in a Profile Shell

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

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

If the `plabel` command is in your profile, the label of the process is displayed.

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

```
# ppriv
pid:  none
```

If the `ppriv` command is in your profile, the privileges available to commands run in the profile shell are displayed.

How to Create an Admin_High Workspace

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

1. **Click the right menu button for the TP menu.**

2. **Choose Change Workspace SL from the menu, and select the workspace Sensitivity Label ADMIN_HIGH.**

3. **Click OK.**
   Actions, terminals, commands and windows originating from the workspace after it is relabeled run at the label of the workspace.

How to Protect the PROM

For security, access to the PROM should also require a password.

To Set the PROM Mode and Password

Role - root
Label - admin_low
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
```

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

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

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

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

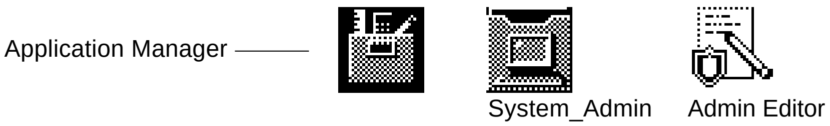
How to Limit Boot-Time Network Contacts

For security, access to other `tsol` hosts can be limited at boot-time. See *Trusted Solaris Administrator's Procedures* for more information on the implications of the boot-time network databases' (`tnrhtp` and `tnrhdb`) defaults.

▼ To Edit the Boot-Time Network Databases

Role - root *or* secadmin
Label - admin_low
Action - Admin Editor

1. **Double-click the Admin Editor action in the System_Admin folder.**



2. **Enter the file name `/etc/security/tsol/boot/tnrhdb`.**
   The file appears in the trusted editor (`adminvi`).

3. **Replace `0.0.0.0` with the address of the NIS+ master or the non-networked workstation.**
   For example, if the IP address of the NIS+ master is 129.150.150.2, then enter:

```
# Loaded at initial boot time only.
# Should be replaced by regular entries after boot.
#
129.150.150.2:tsol
~
“/etc/security/tsol/boot/tnrhdb” 7 lines, 159 characters
```

Note – The above is an example only. Enter the address of *your* NIS+ master.

How to Copy Files To and From a Portable Medium

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

To Copy One or More Files to a Tape or Diskette

Role - ***administrative***
Label - ***appropriate***
Profile shell

1. **First, allocate the appropriate device at the correct label using the Device Allocation action, and insert a clean tape or diskette.**
   Do not mount the device.

```
Do you want device_n mounted: (y,n)? n
```

   For a fuller description, see “To Allocate a Device” on page 32.

2. **Copy the files using the** `tar(1TSOL)` **command.**
   For example, when copying files from an `/export…` directory:

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

3. **Copy the files to a diskette using the** `tar(1TSOL)` **command.**
   For example, when copying files from an `/export…` directory:

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

4. **Deallocate the device before continuing.**
   For the procedure, see “To Deallocate a Device” on page 33.

Note – Remember to physically affix a label to the medium with the sensitivity label and information label of the copied files.

To Copy One or More Files from a Tape or Diskette

It is safe practice to rename the original Trusted Solaris file before copying in a file to replace it.

Role - ***administrative***
Label - admin_low
Profile shell

1. **If the workstation has a file of the same name, copy it to a new name and remove the original.**
   For example, to replace the default `label_encodings` file, do the following in the role `root`.

```
# cd /etc/security/tsol
# cp -p label_encodings label_encodings.orig
# rm label_encodings
```

Note – The `-p` option to the `cp(1)` command preserves the correct file permissions.

2. **Allocate the appropriate device using the Device Allocation action and insert the tape or diskette. Do not mount the device.**

```
Do you want device_n mounted: (y,n)? n
```

   For a fuller description, see “To Allocate a Device” on page 32.

3. **Copy the new file from a tape using the `tar(1TSOL)` command with the `-T` function modifier.**
   For example, when copying in a site `label_encodings` file:

```
# pwd
/etc/security/tsol
# tar tvT
-r--r--r--  3/3 sys sys   72 Aug 27 14:29 label_encodings(A)
-r--r--r--+ 3/3 sys sys 7292 Aug 27 14:29 label_encodings
# tar xvT label_encodings
```

4. **Copy the new file from a diskette using the `tar(1TSOL)` command with the `-T` function modifier.**

5. **For example, when copying in a site `label_encodings` file:**

```
# tar tvfT /dev/diskette
# tar xvfT /dev/diskette label_encodings
```

6. **Deallocate the device before continuing.**
   This is described in "To Deallocate a Device" on page 33.

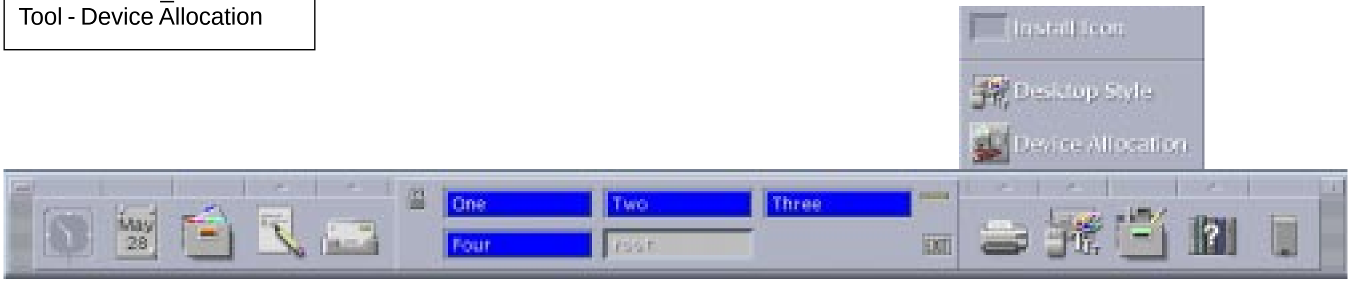
How to Allocate and Deallocate a Device

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

▼ To Allocate a Device

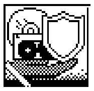
Role - root
Label - admin_low
Tool - Device Allocation

1. **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 Allocation icon.

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



Device Allocation

3. **Double-click the device to be allocated from the list of available devices.**
   mag_tape_0 allocates a tape device.
   floppy_0 allocates a diskette.

4. **Click OK in the label builder that appears.**
   The file you load will be labeled at the label of your workspace. For most installation tasks, the files are labeled admin_low.

Note – Depending on the value of Label View in your `/etc/system` file, a substitute label name may display for the administrative label admin_low.

---

5. **Follow the directions in the window that is displayed.**

6. **If the device can be mounted, answer the question:**

```
Do you want device_n mounted: (y,n)?
```

   For most installation tasks, mount the CDROM, and do not mount a tape or diskette.

▼ To Deallocate a Device

Role - root
Label - admin_low
Tool - Device Allocation

1. **Go to the workspace where the Device Allocation action is displayed.**
   If it is not displayed, click the Device Allocation icon on the Front Panel.

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

3. **Follow the directions in the window that appears.**
   A mounted device is automatically unmounted when it is deallocated.

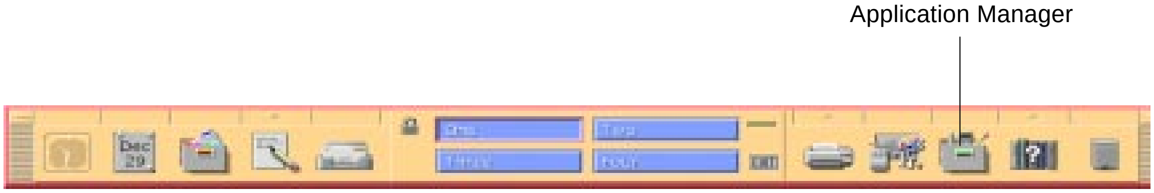
4. **To close the Device Allocation window, click the top left button and select Close.**

How to Open the Application Manager

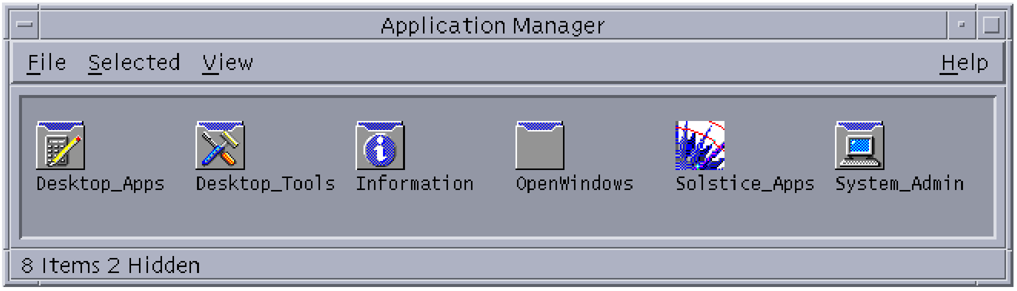
The Application Manager is a front panel action. It contains two folders that hold administrative applications, System_Admin and Solstice_Apps.

To Open the Application Manager

♦ **Single-click the Application Manager on the Front Panel.**



The Application Manager window appears, with several folders.



How to Use the Solstice_Apps Folder

The Solstice_Apps folder holds applications that are used when configuring and maintaining a Trusted Solaris environment. These applications handle local files and their corresponding NIS+ table databases.

The following programs are accessible through the Solstice_Apps folder and are used when configuring a Trusted Solaris workstation:

- Host Manager - for setting up network installation.
- User Manager - for administering users.

- Database Manager - for administering the following databases. One database is only a local database; the others are both local and NIS+ databases.

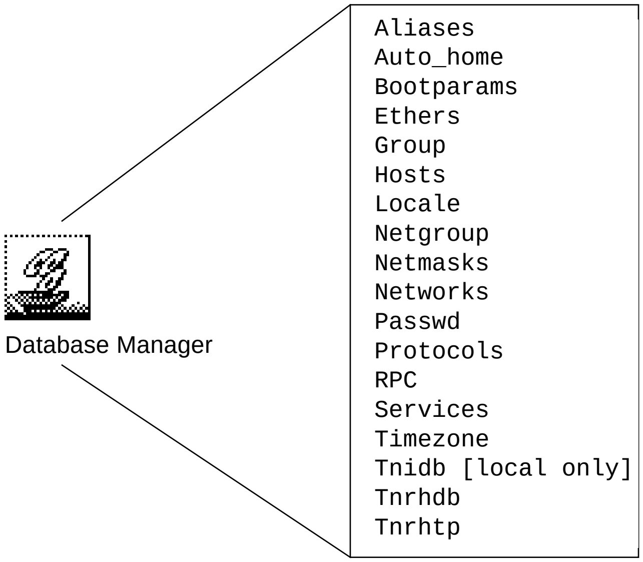
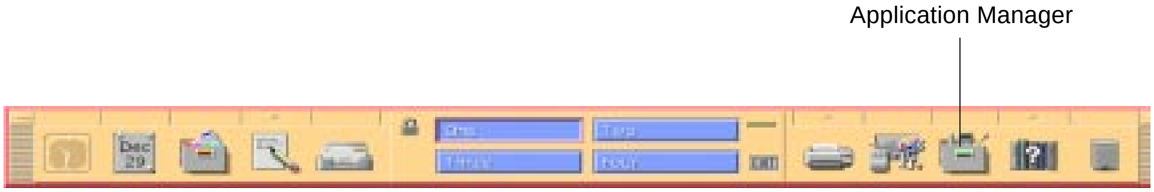


Figure 2-2 Databases Managed by the Database Manager in Solstice_Apps

▼ To Open and Modify a Solstice_Apps Database

1. **Single-click the Application Manager on the Front Panel.**

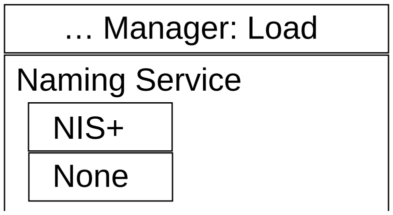


2. **Double-click the Solstice_Apps folder.**

3. **Open a Solstice_Apps Manager by double-clicking its icon, for example, one of -**

   Database Manager   Host Manager   User Manager

4. **In the Load window choose None or NIS+ for the Naming Service.**



… Manager: Load

Naming Service

NIS+

None

   Choose None if you want the changes to be in a local file, or if you are on a workstation that is not running the NIS+ naming service.
   Choose NIS+ for the Naming Service if you want the changes to be in a NIS+ table, seen by all workstations on the network.

5. **If you are loading a database managed by the Database Manager, select the database and press Return.**

6. **To modify entries:**

- **To add an entry, choose Edit > Add.**
- **To modify an existing entry, select the entry and choose Edit > Modify.**
- **To change an entry, select the entry, choose Edit > Delete, then add the correct entry using Edit > Add.**

7. **Choose File > Exit to exit the database after saving your changes.**

▼ To Modify the Password for a Role or User Account

The install team in the role `root` initially modifies the secadmin, admin, and oper passwords. The install team also gives the first users their passwords.

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

Role - secadmin
Label - admin_low
Tool - User Manager

1. **In the User Manager, select a user or role and press the Return key.**
2. **Select from the list of users and press the Return key.**
3. **Click the Password… button.**
   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.**
4. **Make sure that the value of Status is Open.**

Note – Use the status Always Open for all administrative roles, and for the user who can assume the secadmin role. Do not set password expiration dates on administrative roles.

5. **Make sure that the Cred Table Setup box is checked.**
6. **Set other password information for the account.**
   See *Trusted Solaris Administrator's Procedures* for a fuller explanation.
7. **Exit the Password dialog and save the information.**
   a. **Click OK.**
   b. **Click Done.**

▼ To Customize Idle Time

Note – The idle time for a role is not calculated. Roles time out when their user's session times out.

Role - secadmin
Label - admin_low
Tool - User Manager

1. **In User Manager, select a user, not a role.**

2. **Click the Idle… button.**

3. **Press the Idle button labeled 5 mins.**

4. **Choose a convenient setting in keeping with your site security policy.**
   The options are to lock the screen or to log the role out; different time lengths are possible.

5. **Click OK, then Done.**

▼ To Delete a Local User

Role - admin
Label - admin_low
Tool - User Manager

1. **In the role admin, open the User Manager as a local database.**
   The user "install" is defined locally.

2. **Select the user to be deleted, such as "install".**

3. **Select Edit > Delete.**
   For the user "install", you do not have a home directory or mail files to delete. Other local users may have home directories and mail files to delete.

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

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

4. **Close the User Manager by selecting File > Exit when you are done.**

How to Use the System_Admin Folder

The System_Admin folder contains CDE actions for administering a single workstation. These actions do not overlap with the databases in Solstice_Apps. Double-clicking an action causes the action to run. An action that modifies a file invokes the Admin Editor, a trusted editor that prevents the file from being renamed. To create a file, invoke the Admin Editor and supply the name of the new file. Actions also run executables and may elicit input from the administrator.

The following actions are accessible from the System_Admin folder.

Table 2-1 Administrative Actions in the System_Admin Folder

Action or Administrative File Name	**Action Icon Label**
`/etc/nsswitch.conf`	Name Service Switch
`/etc/resolv.conf`	Set DNS Servers
`/etc/vfstab`	Set Mount Points
`/etc/defaultrouter`	Set Default Routes
`/etc/dfs/dfstab`	Share Filesystems
`/etc/mail/sendmail.cf`	Set Mail Options
`/etc/motd`	Set Daily Message
`/etc/security/audit_class`	Audit Classes
`/etc/security/audit_control`	Audit Control
`/etc/security/audit_event`	Audit Events
`/etc/security/audit_startup`	Audit Startup
`/etc/security/audit_user`	Audit Users
`/etc/security/tsol/label_encodings`	Edit Encodings
`/etc/security/tsol/vfstab_adjunct`	Set Mount Attributes
`/etc/tsolgateways`	Set TSOL Gateways
`/usr/dt/config/sel_config`	Configure Selection …
Create or edit any file	Admin Editor
Add allocatable device	Add Allocatable Device
Verify syntax of `label_encodings` file	Check Encodings
Check local `tnrhdb` and `tnrhtp` files	Check TN Files
Check NIS+ `tnrhdb` and `tnrhtp` databases	Check TN NIS+ Tables
Create NIS+ client	Create NIS+ Client
Establish root NIS+ domain	Create NIS+ Server

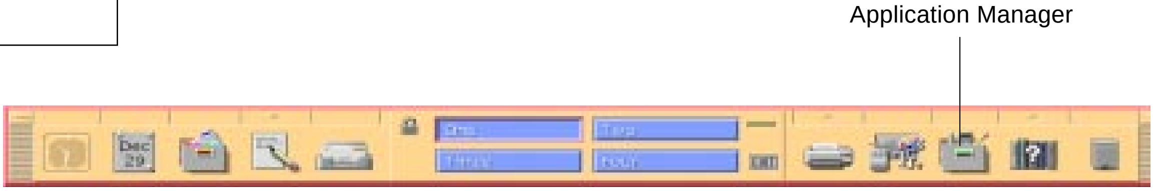
Table 2-1 Administrative Actions in the System_Admin Folder

Populate NIS+ tables	Populate NIS+ Tables
View internal representation of a NIS+ table	View Table Attributes
View contents a NIS+ table	View Table Contents

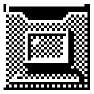
▼ To Run a System_Admin Action

Role - root
Label - admin_low
Action -…

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



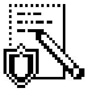
2. **Double-click the System_Admin icon.**


System_Admin

3. **Double-click the appropriate action.**

To Create or Open a File from the Trusted Editor

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


Admin Editor

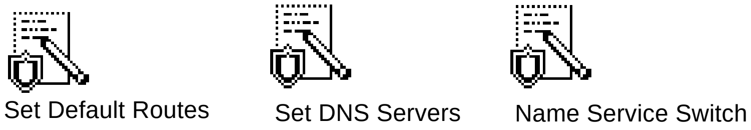
A prompt appears for you to specify the file to be opened.

2. **Enter the name of the file to be opened.**
If the file exists, it is opened.
If the file does not exist, it is created.

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

To Open a File that has a Defined Action

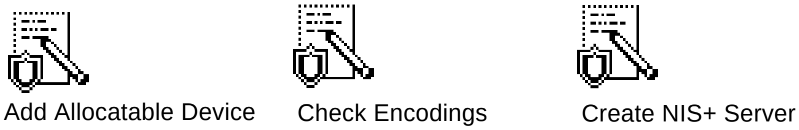
1. **To open a file that has its own action, double-click the action.**
   The file associated with the action (see Table 2-1 on page 39) appears in the trusted editor.



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

To Run a Script from the System_Admin Folder

1. **To run an script that has its own action, double-click the action.**
   When the script requires input, the prompts are displayed.



2. **Follow the instructions.**
   The script is finished when all prompt windows have been dismissed.

How to Add Network Interfaces

For every network interface, a file `/etc/`*`hostname.interface`* file must exist. The installation program creates the file for the primary interface only.

Note – If this procedure is done by the install team before the roles `secadmin` and `admin` have been credentialed, they use `root` to do the procedure.

To Determine the Network Interfaces

Role - admin
Label - admin_low
Profile shell

1. **Use the** `prtconf` **command to find the network interfaces.**

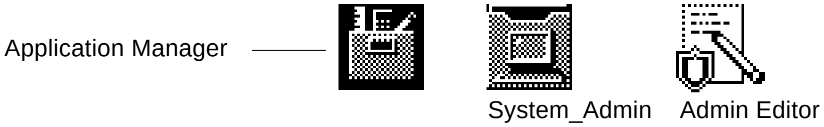
```
# prtconf | grep instance
…    le, instance #0
     qe2, instance #0
     qe3, instance #0
…
```

2. **List the secondary interfaces.**
   The primary interface was configured during installation; its file exists.

To Create the Network Interface Files

Role - secadmin
Label - admin_low
Action - Admin Editor

1. **For each secondary interface, open a file named** `/etc/`*`hostname.interface`* **in the Admin Editor.**
   See "To Run a System_Admin Action" on page 40 if you are unfamiliar with the steps.



   For example, if the host `grebe-118` is a secondary interface and uses a quad ethernet card, the file name is `/etc/grebe-118.qe`.

   a. **In the file, enter the hostname associated with the interface, such as** `grebe-118`**.**

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

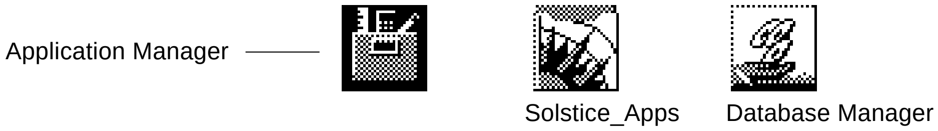
   c. **Change the permissions on the file to 644.**

```
$ chmod 644 /etc/hostname.interface
```

   For example, for the file named `/etc/grebe-118.qe`:.

```
# chmod 644 /etc/grebe-118.qe
```

2. **Add every interface to the local `/etc/hosts` file using the Database Manager with no naming service.**
   See "To Open and Modify a Solstice_Apps Database" on page 35 if you are unfamiliar with editing the Hosts database.



3. **Add every interface to the local `tnrhdb` file using the Database Manager with no naming service.**

How to Share a File System

Administrators access the `/etc/dfs/dfstab` file through the Share Filesystems action in the System_Admin folder.

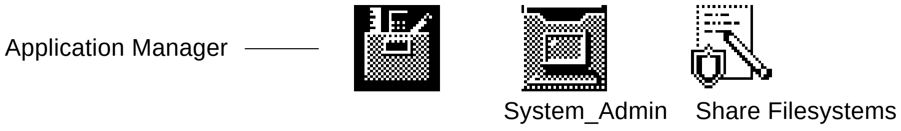
Caution – Do not use proprietary names for shared file systems. The names of shared file systems are visible to every user.

▼ To Share Home Directories and Other Filesystems

Perform this procedure on the home directory or on a file server. If the directory is being shared before the `secadmin` and `admin` roles are credentialed, the install team performs the procedure in the role `root`.

Role - admin
Label - admin_low
Action- Share Filesystems

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



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

a. **Enter the file system to be shared, and any relevant options.**
For example, to share home directories:

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

For example, to share a network install directory:

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

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

Role - admin
Label - admin_low
Profile shell

2. **Run the** share(1MTSOL) **command to share the file systems.**
For example, to share home directories:

```
$ share /export/home
```

For example, to share a network install directory:

```
$ share /export/install/tsolfiles
$ share /jumpstart
```

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

3. **Check that the directories are shared.**

▼ To Check That a Directory Is Shared

Role - admin
Label - admin_low
Profile shell

1. **Run the command** showmount -e**:**

```
$ showmount -e
```

a. **If it returns an export list, the directory is shared, as in:**

```
export list for install_server:
/export/install/tsolfiles
/jumpstart
```

b. **If it returns the following error, start the nfs.server daemon.**

```
showmount: server: RPC: Program not registered
```

▼ To Start the nfs.server Daemon

Role - admin
Label - admin_high
Profile shell

1. **Start the nfs server program in an admin_high shell.**
   See "How to Create an Admin_High Workspace" on page 27 if you are unsure of how to run at the label admin_high.

```
$ /etc/init.d/nfs.server stop
$ /etc/init.d/nfs.server start
```

Role - admin
Label - admin_low
Profile shell

2. **Return to the admin_low shell to check that the directory is shared.**
   For example, when home directories are shared:

```
$ showmount -e
export list for home_directory_server:
/export/home   (everyone)
```

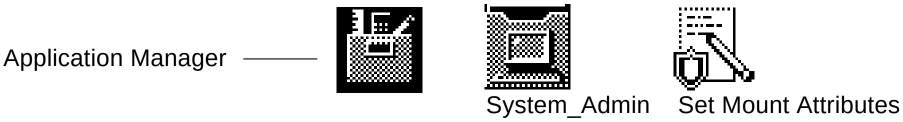
How to Set the Label on an Unlabeled File System

The security administrator uses the System_Admin folder to access the `/etc/security/tsol/vfstab_adjunct` file.

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 2-3 shows a `vfstab_adjunct` entry for an unlabeled, remote file system, `/cpublic`, being mounted at the label Confidential ([C]) on a Trusted Solaris 2.5.1 network.

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

Figure 2-3 Modified `vfstab_adjunct` Entry

Every file in the `/cpublic` file system will be protected at the label Confidential.

Note – This example requires the security administrator to have created a new template. See “To Edit the Tnrhtp Database (Example)” on page 79.

How to Mount a File System

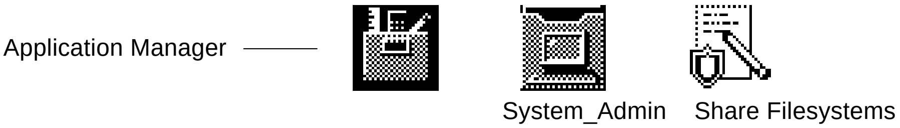
Administrators access the `/etc/vfstab` file through the System_Admin folder, and create the mount points in a profile shell.

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

▼ To Mount a Labeled or Unlabeled File System

Role - admin
Label - admin_low
Action - Set Mount Points

1. **Run the Set Mount Points action from the System_Admin folder in the Application Manager.**



The Set Mount Points action opens the /etc/vfstab file.

For example, the grebe:/opt/tools file system will be mounted every time the workstation is booted.

```
    grebe:/opt/tools - /opt/tools nfs  -  yes    bg,intr,soft
```

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

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

Role - admin
Label - admin_low
Profile shell

```
$ mkdir -p /opt/tools
$ mount /opt/tools
```

The following is a sample entry in the vfstab file for /cpublic, an unlabeled file system:

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

How to Update the Commands in a Role’s Profile

When setting up a network or custom JumpStart install, some required commands are not available to the role because they are not in a profile assigned to the role. To add commands, programs, or scripts to the role’s profile, you modify the “Custom *Rolename* Role” profile. For example, to add a command to the profile shell of the role root, you modify the Custom Root Role profile.

▼ To Add a Command to a Role’s Profile

Role - secadmin
Label - admin_low
Tool - Profile Manager

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

2. **Open the Profile Manager from the Solstice_Apps folder using the NIS+ naming service.**

3. **Load the “Custom *Rolename* Role” into the Profile Manager.**

4. **In the Commands view, type the pathname to the command.**
   For example, to access the Trusted Solaris CDROM, enter:

```
Pathname: /cdrom/cdrom0
```

5. **From the list of Excluded commands, choose the command to be added to the profile.**
   To continue the above example, add `setup_install_server` to the Included list.

6. **Give the command all privileges and save the Custom *Rolename* Role profile.**

▼ To Verify That a Command is in a Role’s Profile

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

Role - root
Label - admin_low
Profile shell

2. **Assume the role, launch a new terminal.**

3. **Verify that the new profile is in effect in the new terminal by using the `clist(1MTSOL)` command.**
   For example, to verify the command in the preceding example:

```
# clist -p | grep setup_install_server
It should display: /cdrom/cdrom0/setup_install_server: all
# clist -i | grep setup_install_server
It should display: none none /cdrom/cdrom0/setup_install_server
```

▼ To Remove a Command from a Role’s Profile

Role - secadmin
Label - admin_low
Tool - Profile Manager

1. **Load the “Custom *Rolename* Role” into the Profile Manager.**
2. **In the Commands view, locate and select the pathname to the command.**
3. **From the list of Included commands, double-click the command to be removed from the profile.**
   This moves the command to the Excluded list.
4. **Save the Custom *Rolename* Role profile.**

How to Upgrade from the Trusted Solaris 2.5 Release

The Trusted Solaris 2.5.1 installation program offers an Upgrade option. The option replaces files that you configured for your site in the Trusted Solaris 2.5 environment. Therefore, certain upgraded files must be replaced with your customized files for the system to run as expected. Further configuration for the Trusted Solaris 2.5.1 release is also required.

▼ To Install with the Upgrade Option

1. **Select the Upgrade option after system identification has completed during installation.**
   The steps of the installation program are described in Chapter 3, “Installing a Workstation”.
2. **Read the upgrade log.**

Before reboot, the upgrade log is in `/a/var/sadm/system/logs/upgrade_log`. After reboot, the upgrade log is in `/var/sadm/system/logs/upgrade_log`.

3. **Manually reboot the system.**
   The procedure is described in Step 9 on page 61.
4. **Continue with “To Configure After Upgrade”.**

▼ To Configure After Upgrade

1. **Follow the instructions in** `upgrade_cleanup` (mentioned in the `upgrade_log`)**.**

Before reboot, the cleanup log is in
`/a/var/sadm/system/data/upgrade_cleanup`
After reboot, the cleanup log is in
`/var/sadm/system/data/upgrade_cleanup`.

For example, in the `upgrade_cleanup` log, you may see the following:

```
/etc/init.d/sysetup: existing file renamed to
/etc/init.d/sysetup:2.5
/etc/system: existing file preserved, the new version was
installed as /etc/system.new
/a/etc/security/tsol/tnrhtp: existing file preserved, the new
version was installed as /a/etc/security/tsol/tnrhtp.new
/a/etc/security/tsol/tnrhdb: existing file preserved, the new
version was installed as /a/etc/security/tsol/tnrhdb.new
```

Note – Files ending in `.new` are files installed from the Trusted Solaris 2.5.1 upgrade program. File ending in `:2.5` are files from the previous release.

a. **Compare the file with the new/renamed version.**
For example, compare `/etc/init.d/sysetup` to `/etc/init.d/sysetup:2.5`.

```
# diff /etc/init.d/sysetup /etc/init.d/sysetup:2.5
```

b. **Decide on the best course of action for your site and do it.**

c. **Repeat for all files mentioned in the `upgrade_cleanup` log.**

2. **Remove your static routing file if you plan to use dynamic routing.**
The static routing files are `/etc/defaultrouter` or `/etc/tsolgateways`. A static routing file was required in the Trusted Solaris 2.5 release.

3. **Check all configuration files.**
   See the appropriate "Configuring …" chapter for the role, tool, and label for modifying these files. Files to check include at least the following:

Local Files to Check after Upgrade	Notes
`/etc/security/tsol/label_encodings`	
`/etc/defaultrouter`	Remove for dynamic routing.
`/etc/tsolgateways`	Remove for dynamic routing.
`/etc/`*`hostname.interface`*	Check secondary network interfaces.
`/etc/security/tsol/tnrhtp|tnrhdb|tnidb`	Check trusted network files.
`/etc/security/tsol/boot/tnrhdb`	Check trusted network boot-time file.
`/etc/hosts`	Check the local hosts file.
`/etc/resolv.conf`	Check the DNS Servers file.
`/etc/nsswitch.conf`	Check the NIS+ switches file.
`/etc/auto*`	Check the files for automounting.
`/etc/vfstab`	Check the file for mount points.
`/etc/vfstab_adjunct`	Check the file for mount point attributes.
`/etc/dfs/dfstab`	Check the file for exported file systems.
`/etc/security/audit_*`	Check the audit configuration files.

4. **Reboot when configuration is complete.**

How to End a Session

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

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

▼ To Lock the Screen

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

▼ To Log Out

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

▼ To Reboot the Workstation

1. **Right click the CDE front panel and select Shut Down from the TP (Trusted Path) menu.**
   The menu appears when the user or role is authorized to shut down the workstation.
2. **Confirm the shutdown.**
3. **Enter** `boot` **at the** `ok` **prompt or** `b` **at the** `>` **prompt:**

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

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

Installing a Workstation 3

This chapter provides procedures to boot and install a workstation. The procedures cover booting and installing –

- From a Trusted Solaris CDROM.
- Over the network from a Trusted Solaris image on hard disk, plus system identification files created by an administrator.
- From a CDROM and custom JumpStart diskette.
- Over the network from a Trusted Solaris image on hard disk, plus custom JumpStart profiles tailored to your site.

The procedures in this chapter should be done on the workstation that is being installed.

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.

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)** On a Trusted Solaris 2.5 workstation: **`Shut Down the workstation from the TP menu.`** **2)** Go to Step 2.

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

See “Plan Workstation Hardware and Capacity.” on page 6 for hardware, disk space, and memory requirements.

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

See your hardware manual for instructions.

4 Boot the workstation using the appropriate boot command.

To Boot From a CDROM:

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`

To Boot From a CDROM with a Custom JumpStart diskette:

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`.

To Boot Over a Network:

If You Are Booting ...	Then Enter ... [1]
From a server on the network	`boot net`
From a server on the network and have customized JumpStart profiles for the site	`boot net - install`

A space is required between the minus sign and `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. The following screen provides an example of what you 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 TS2.5.1 [UNIX(R) System V Release
4.0]
Copyright (c) 1983-1998, Sun Microsystems, Inc.
WARNING: clock gained 35 days -- CHECK AND RESET THE DATE!
Configuring the /devices directory
Configuring the /dev directory
Starting OpenWindows...
```

The following screen provides an example of a custom JumpStart booting sequence.

```
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_5.1_sparc/s0/export/exec/kvm/sparc.sun4c.Trust
ed Solaris_2.5.1
SunOS Release 5.5.1 Version TS2.5.1 [UNIX(R) System V Release 4.0]
Copyright (c) 1983-1998, 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 Be prepared to answer installation program questions.

See Appendix F, "Example Worksheets" for sample answers. You can copy the blank worksheets provided in Appendix B, "Worksheets for Configuring and Installing Trusted Solaris" to record your answers.

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 Trusted Solaris CDROM, the program guides you step by step through installing Trusted Solaris software; it also has online help to answer your questions.
- If you have correctly set up a custom JumpStart installation, you are not prompted for information.
- If you have correctly set up a network installation, you will be prompted for information after system identification is completed.

Installation Program Questions

--------- System identification starts here---------

1. Name of workstation

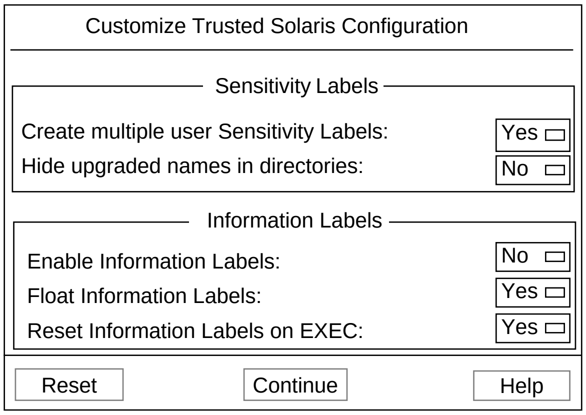
2. Is it networked?

a. Its primary network interface

b. Its IP address

c. Its Name Service
[*None* for the NIS+ root master]
[NIS+ for clients]

3. Trusted Solaris Configuration options



Customize Trusted Solaris Configuration

Sensitivity Labels

Create multiple user Sensitivity Labels: Yes

Hide upgraded names in directories: No

Information Labels

Enable Information Labels: No

Float Information Labels: Yes

Reset Information Labels on EXEC: Yes

4. On a subnet?

a. Its subnet mask

5. Time zone

6. Date and time

--------- System identification completed ---------

--------- *Checks for JumpStart scripts appear in the upper left console window* ---------

7. Upgrade or Install?

You can upgrade from the Trusted Solaris 2.5 release only.

If you are upgrading, please read "How to Upgrade from the Trusted Solaris 2.5 Release" on page 49.

8. **System type**
   The following table describes the two choices in the Trusted Solaris environment.

Table 3-1 System Type Choices

Choose	Because	Description
OS server	The workstation will serve diskless clients.	Provides Trusted Solaris operating environment software including services and file systems for workstations on the network. For diskless clients, it provides all file systems.
Standalone	The workstation is: a diskfull client a server	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.

Notes

- 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+ naming service.
- Diskless clients are installed using the Host Manager in the Solstice_Apps folder. See Chapter 10, “Configuring Diskless Clients”.

9. **Software group**
   The groups Core and End User are identical in the Trusted Solaris environment.

   a. **Customize the installation?**

10. **Disks to use.**

    a. **Preserve the format of any of the disks?**

    b. **Auto-layout file system?**

i. **Which file systems to auto-layout?**

c. **Customize the size of the partitions? YES**
Hints:

On *all workstations*, for audit records…

i. **If auditing is a site security requirement, create at least one audit partition named** `/etc/security/audit/`*`workstation_name`*.

On *all workstations*, for users who can assume a role…

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

On a *standalone* that will be the *home directory server*…

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

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

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

On an *OS server*…

i. **Allocate enough space for the clients' root and swap.**
See the sample worksheet, "OS Server Installation Program Example" on page 258.

Note – When you install an OS server, you allocate the disk space that is required for the clients that that server will support. Then, *after* the OS server is installed, you configure the clients (Chapter 10, "Configuring Diskless Clients").

---

11. **Begin installation | Begin upgrade.**

12. **Reboot?**
If you are upgrading, the workstation will not automatically reboot. You must do a manual reboot.

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, diskette, or net, determines the installation time.

8 Read the log.

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

Before reboot, the upgrade log is in `/a/var/sadm/system/logs/upgrade_log`.
After reboot, the upgrade log is in `/var/sadm/system/logs/upgrade_log`.

1. **Look for successful installation of packages.**
2. **Ignore messages of the form:**

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

3. **If you are upgrading, please go to "To Configure After Upgrade" on page 49.**

9 Enter a root password.

Note – The workstation *must* have a root password in order for NIS+ to install correctly.

♦ **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.

♦ **If you manually reboot your system, type:**

```
#   halt
ok  boot disk
```

Then enter a root password at the prompt.

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

10 If you installed 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 10, “Configuring Diskless Clients”.

11 For network and JumpStart installations, check that all Trusted Solaris configuration tasks are complete.

For an overview of individual workstation configuration tasks, see Chapter 6, “Configuring a NIS+ Client”.

Task Complete

For pointers to administration references, see Chapter 11, “Where to Find….”

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

Role, Label, and Tool

Role - root
Label - admin_low
Profile shell

A box to the left of a configuration procedure, like the one to the left, 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.

Note – All administrative roles (root, secadmin, and admin) are supplied with a *profile shell* by default.

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, handling mail, setting up printing, and installing Trusted Solaris 2.5.1 AnswerBook™ are covered in *Trusted Solaris Administrator's Procedures*.

Note – The procedures are not numbered. Depending on how you set up the workstation, some procedures can be omitted.

If you are configuring the workstation to satisfy criteria for an evaluated configuration, please read "Understand Your Site's Security Policy." on page 3.

▼ Log In and Assume the root Role

♦ **Log in as the user `install` and assume the root role.**
See "To Log In as the User "Install"" on page 23 and "To Assume a Role" on page 25 if you are unfamiliar with the steps.

▼ Protect the Workstation

Role - root
Label - admin_low
Profile shell

♦ **Protect the PROM.**
See "How to Protect the PROM" on page 27 if you are unfamiliar with the steps.

Role - root
Label - admin_low
Action - Admin Editor

♦ **Limit contact with other workstations when booting.**
See "How to Limit Boot-Time Network Contacts" on page 28 if you are unfamiliar with the steps.

▼ Check and Install the `label_encodings` File

If you are not installing a site-specific *label_encodings file*, and:

- If you are not going to access any other workstation, skip this step and go to "Add Administrative Roles to Three /etc Files" on page 67.
- If you are going to access a network without using the NIS+ name service, skip this step and go to "Set Up Network Files" on page 66.

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

If you are installing a site-specific `label_encodings` file, read on.

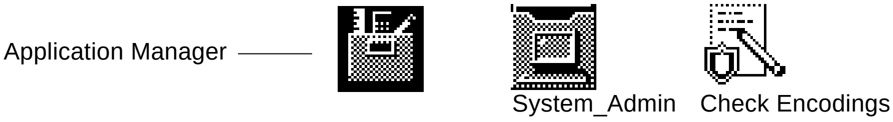
Caution – If you are planning to use a modified `label_encodings` file, you *must* complete this step before continuing or the installation will fail.

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

Role - root
Label - admin_low
Profile shell
Action - Check Encodings

1. **Have the medium (tape or diskette) with your site's `label_encodings` file ready to use.**
2. **Copy in, check the file, and read the file into the environment.**
   See "To Copy One or More Files from a Tape or Diskette" on page 31 if you are unfamiliar with the steps.

3. **Use the Check Encodings action to check the syntax of the file.**
   For more details on using actions, see “To Run a System_Admin Action” on page 40.



Caution – Your label_encodings file *must* pass the Check Encodings test before you continue.

▼ Set Up Network Files

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

Role - root
Label - admin_low
Action - ***various***or none

♦ **If you are going to use static routing, set it up.**
Follow the procedure in “Set Up Routing” on page 75.

Role - root
Label - admin_low
Tool - Database Manager

♦ **If you are using static routing, add the static router(s) to the local Hosts database.**
See the detailed list of steps in “Add the Static Routing Workstations to the Local Hosts Database” on page 78.

Role - root
Label - admin_low
Action - Set DNS Servers

♦ **If your workstation is going to use DNS, enter the nameservers using the Set DNS Servers action.**
For a detailed list of steps, see “Set Up DNS” on page 86. Do not edit the `nsswitch.conf` file.

Role - root
Label - admin_low
Tool - Database Manager

♦ **Enter the details of every workstation that this workstation may contact in the Tnrhdb database. Include the static routers, and any file servers whose file systems you plan to mount.**
See “To Open and Modify a Solstice_Apps Database” on page 35 if you are unfamiliar with accessing the Tnrhdb database. A more detailed explanation of the steps is in “To Edit the Tnrhdb Database” on page 80.

Role - root
Label - admin_low
Action - Admin Editor
Profile shell

♦ **Configure any secondary network interfaces.**
Follow the steps in “How to Add Network Interfaces” on page 41 if you are unfamiliar with setting up network interfaces.

▼ 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
Profile shell

1. **Save the original files by copying them to *.orig.**

```
# cd /etc
# cp -p passwd passwd.orig
# cp -p shadow shadow.orig
#
# cd /etc/security/tsol
#
# cp -p tsoluser tsoluser.orig
```

Role - root
Label - admin_low
Action - Admin Editor

2. **Add the contents of each *.roles file to its corresponding /etc file using the Admin Editor.**

Application Manager —— System_Admin Admin Editor

   a. **Open the file /etc/passwd and go to the end of the file.**

   b. **Read in the file /etc/passwd.roles (the Admin Editor command is :r *filename*).**

   c. **Write and exit the file /etc/passwd.**
   The passwd file now contains its original text and the text of the file passwd.roles.

   d. **To verify, grep for the role secadmin in a profile shell.**

```
# cd /etc
# grep secadmin passwd
secadmin:x:101:14:Security Admin:/etc/security/tsol/home/secadmin:/usr/bin/pfsh
```

   e. **Repeat the above steps for /etc/shadow and shadow.roles, and for /etc/security/tsol/tsoluser and tsoluser.roles.**

Caution – The Trusted Solaris roles *must* be in the local passwd, shadow, and tsoluser files for the Trusted Solaris environment to work. Do not (further) edit the files tsolprof, tsoluser, passwd, or shadow. After booting, you will modify these using the Solstice_Apps tools, User Manager and Profile Manager.

3. **Modify other `/etc` files as necessary.**

▼ Reboot the Workstation

Note – This step is required only if you have set up network files.

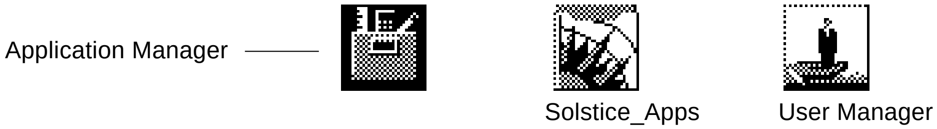
♦ **Shut down the workstation from the TP (Trusted Path) menu.**
For a detailed procedure, see “To Reboot the Workstation” on page 52.

▼ Update Role Passwords

1. **If you rebooted, log in as the user `install` and assume the role `root`.**

Role - root
Label - admin_low
Tool - User Manager

2. **Using None for the Naming Service, open the User Manager and give passwords to the roles secadmin, admin, and oper.**



Follow the steps in “To Modify the Password for a Role or User Account” on page 36 if you are unsure of how to set passwords.

Note – To ensure that the workstation can always be administered, use the status Always Open for every administrative role, and do not set password expiration dates for any administrative role.

3. **Leave the User Manager open.**

▼ Add Users to Administer the System

Role - root
Label - admin_low
Tool - User Manager

1. **Add users who will assume administrative roles.**
   See “To Open and Modify a Solstice_Apps Database” on page 35 if you are unfamiliar with the steps. For suggested entries for user account fields, see Table 5-1 on page 90, “User Account Characteristics”.

Note – To ensure that someone can always log in, use the status Always Open for the user who can assume the secadmin role.

2. **Exit the User Manager when at least the users who can assume the roles secadmin and admin have been created.**

3. **Log out by clicking the EXIT icon on the Front Panel.**

▼ Verify That Users and Administrative Roles Work

♦ **Log in as a user, assume an administrative role, and test it for effectiveness.**
Follow the procedure in “Verify that Users and Administrative Roles Work” on page 92 to ensure that every role is working.

▼ Set Up Auditing

Role - secadmin
Label - admin_low
Various tools

♦ **Disable or configure auditing.**
Read the explanation and follow the procedure in “Set Up Auditing” on page 92 if you are unfamiliar with Trusted Solaris auditing.

Mount Unlabeled File Systems

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

Role - secadmin
Label - admin_low
Action- Set Mount Attributes

1. **Set a label for an unlabeled file system.**
   Read the explanation and follow the procedure in "Set the Label for Unlabeled File Systems (Example)" on page 93 if you are unsure of the steps.

Role - admin
Label - admin_low
Various tools

2. **Mount the file system.**
   If you are unfamiliar with the steps, see "How to Mount a File System" on page 46.

Share File Systems

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

Role - admin
Label - admin_low
Various tools

♦ **Share the file systems that other workstations may access.**
Follow the procedure in "How to Share a File System" on page 43 if you are unfamiliar with sharing file systems.

Delete the User `install`

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

Role - admin
Label - admin_low
Tool - User Manager

♦ **Use the User Manager to delete the user install.**
See "To Delete a Local User" on page 38 if you are unfamiliar with deleting users.

Configuring the NIS+ Root Master 5

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

Who Does What

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

Role - root
Label - admin_low
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. When more than one role, tool, or label is required, there is a box at every change of role, tool, or label.

Note – All Trusted Solaris administrative roles (root, secadmin, and admin) are supplied with a *profile shell* by default.

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, handling mailing, setting up printing, and installing the Trusted Solaris AnswerBook™ are covered in *Trusted Solaris Administrator's Procedures*.

If you are configuring a site that satisfies criteria for an evaluated configuration, please read "Understand Your Site's Security Policy." on page 3.

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

▼ Log In and Launch a Terminal

1. **Log on to the workstation as the user `install`.**
   See "How to Log In" on page 22 if you have not logged in before.

2. **Assume the role 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`.

3. **Launch a terminal.**
   See "To Launch a Terminal" on page 25 if you are unfamiliar with launching a terminal in Solaris or Trusted Solaris. The terminal contains a profile shell, specific to the role `root`.

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

▼ Protect the Workstation

Role - root
Label - admin_low
Profile shell

1. **Protect the PROM.**
   See "How to Protect the PROM" on page 27 if you are unfamiliar with the steps.

Role - root
Label - admin_low
Action - Admin Editor

2. **Edit the boot-time database, `/etc/security/tsol/boot/tnrhdb`.**
   See "How to Limit Boot-Time Network Contacts" on page 28 for details of the steps.

Note – Editing the boot-time databases is required *only if* the default setting is more permissive than your site's security requirements.

▼ Check and Install the `label_encodings` File

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

- Skip to “Set Up Routing” on page 75 if you are not modifying the `label_encodings` file and you have an *open network*.
- Skip to “Edit the Trusted Network Files” on page 78 if you are not modifying the `label_encodings` file and you have a *closed network*.

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

You can edit the `label_encodings` file that the Trusted Solaris installation program installed.

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

If you do not use this file, check that your `label_encodings` file works on the NIS+ master before copying the file to every workstation you install.

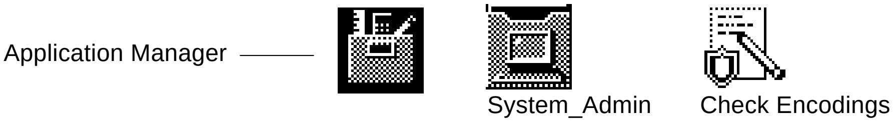
1. **Have the medium (tape or diskette) with your site’s `label_encodings` file ready to use.**

2. **Copy the file to the `/etc/security/tsol` directory.**
   If you are unsure of the steps, see “To Copy One or More Files from a Tape or Diskette” on page 31.

Role - root
Label - admin_low
Action - Check Encodings

3. **Check the syntax of the new `label_encodings` file.**

   a. **Double-click the Check Encodings action in the System_Admin folder in the Application Manager.**
   For more information on using the actions in the System_Admin folder, see “To Run a System_Admin Action” on page 40.



b. **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 – Your `label_encodings` file *must* pass the Check Encodings test before you continue.

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

   Your `label_encodings` file is now in effect.

You will use a copy of the `label_encodings` file on the NIS+ clients. Setting up the copy is covered in "Copy Configuration Files for Distribution to Clients" on page 94.

▼ Set Up Routing

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

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

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

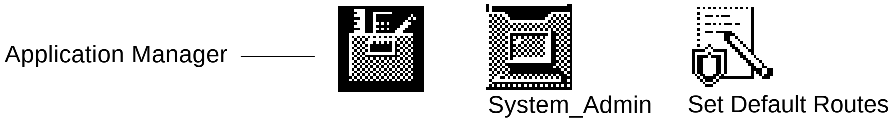
Note – A workstation cannot be its own default router (gateway). A NIS+ master with more than one interface can be a router for its clients, but it cannot be a router for itself.

▼ To Set Up Simple Static Routing

Note – For static routing, do either this procedure, *or* “To Set Up Complex Static Routing”.

Role - root
Label - admin_low
Action - Set Default Routes

1. **Double-click the Set Default Routes action in the System_Admin folder.**
   See “To Open a File that has a Defined Action” on page 41 if you are unfamiliar with using trusted actions.



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

2. **Enter the name of the defaultrouter. If there is more than one, enter them all, one per line.**
   For example, if the workstations `trustworthy` and `forwardho` are routers, enter them, one per line:

```
trustworthy
forwardho
```

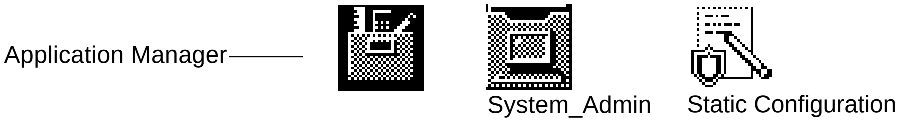
3. **Write the file and exit the editor.**

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

▼ To Set Up Complex Static Routing

Role - root
Label - admin_low
Action - Set TSOL Gateways

1. **Double-click the Static Configuration action in the System_Admin folder.**
   See “To Open a File that has a Defined Action” on page 41 if you are unfamiliar with using trusted actions.



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

2. **Enter the IP address of the net, the name of the gateway and its metric. Repeat for every gateway.**
   For example, if the workstations `trustworthy` and `forwardho` are gateways:

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

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

▼ Set Up Additional Network Interfaces

If the workstation has more than one network interface, set them up now.

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. See *Trusted Solaris Administrator’s Procedures* if you need to add a new hardware device to the `device_policy(4TSOL)` file. The install team ensures that the interfaces are protected before booting the workstation into multiuser mode.

The basic setup of additional network interfaces in Trusted Solaris is identical to their setup in Solaris. For convenience, the steps are included in “How to Add Network Interfaces” on page 41. For further information on basic setup, see the *TCP/IP and Data Communications Administration Guide*, Chapter 4, “Configuring TCP/IP on the Network” in the Solaris 2.5.1 document set.

▼ Add the Static Routing Workstations to the Local Hosts Database

Note – Skip this procedure if the security administrator has planned for dynamic routing or for a closed network.

1. **Open the Hosts database as a local file (using no naming service).**
   See "To Open and Modify a Solstice_Apps Database" on page 35 if you are unfamiliar with editing the Hosts database.

   Application Manager —— Solstice_Apps Database Manager

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

2. **Add the defaultrouter workstation(s) or the tsolgateway workstations as entries to the database.**

3. **Exit the Hosts database when the entries are complete.**

▼ 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 host type and IP addresses of the workstations on your network and the host type and IP addresses of any other subnets and hosts with which your Trusted Solaris 2.5 network can communicate. The security administrator determines what networks can contact the Trusted Solaris 2.5.1 network; for a list of host types, see Table 1-3 on page 9. The system administrator collects the IP addresses.

If you plan to mount file systems from unlabeled hosts at a label available to users, do "To Edit the Tnrhtp Database (Example)" first. Otherwise, go to "To Edit the Tnrhdb Database" on page 80.

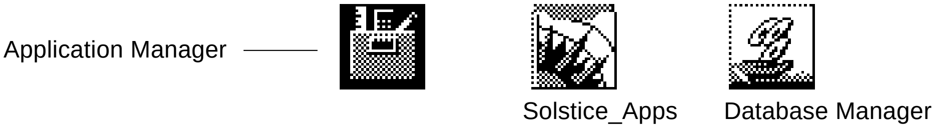
You can change the network details later. For customizing the `tnrhdb` and its associated templates database, `tnrhtp`, see *Trusted Solaris Administrator's Procedures*.

▼ To Edit the Tnrhtp Database (Example)

This example adds a new host type, `unlab_conf`, to the `tnrhtp(4TSOL)` database. This procedure is a prerequisite to mounting an unlabeled host at a user label, such as Confidential. “Set the Label for Unlabeled File Systems (Example)” on page 93 completes the setup.

Role - root
Label - admin_low
Tool - Database Manager

1. **Open the Tnrhtp database in the Database Manager using no naming service.**
   See “To Open and Modify a Solstice_Apps Database” on page 35 if you are unfamiliar with the steps.



2. **Choose Edit > Add from the Tnrhtp menu.**

3. **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[*low_user_label*].**

   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, click** `ADMIN_HIGH`**.**

      ii. **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. **Click the SL button and click a low user sensitivity label, such as Confidential.**

ii. **If** *information labels* **are enabled, click the IL button and click a low information label, such as Unclassified.**
If your label encodings file does not define any ILs for the sensitivity label, leave the IL at ADMIN_LOW. The CMW label might read ADMIN_LOW[PUBLIC], for example.

iii. **Click OK.**

4. **Exit the database when the template is complete.**

▼ To Edit the Tnrhdb Database

Role - root
Label - admin_low
Tool - Database Manager

1. **Open the Tnrhdb database in the Database Manager using no naming service.**
See "To Open and Modify a Solstice_Apps Database" on page 35 if you are unfamiliar with the steps.

Application Manager ——— Solstice_Apps Database Manager

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 subnet is an unlabeled host, an exception to the `tsol` fallback entry.

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` or `/etc/tsolgateways` file, and assign to each an appropriate template name.**

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 1-3 on page 9 for host types and their associated templates provided by Trusted Solaris.

6. **Exit the Tnrhdb database when the entries are complete.**

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 static router (open network only)
- Every other workstation with which the domain can communicate, or a fallback address for its subnet (open network only)

▼ Set Up the NIS+ Domain

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

Overview

- Create a staging area for databases.
- Copy and edit staging area files; they will become NIS+ tables.
- Run `nisserver` command.
- Run `nispopulate` command.
- Run `nisgrpadm` command.
- Reboot the workstation.
- Update passwords and credentials.

To Set the Stage

Role - root
Label - admin_low
Profile shell

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

Three Trusted Solaris files need to be renamed when copied into the staging area. Three others are copied without changing their names.

```
# 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

       WARNING: Command operating outside of the Trusted Path!
   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.**
   For more detailed instructions, see “To Create or Open a File from the Trusted Editor” on page 40.

   Application Manager —— System_Admin Admin Editor

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

      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 with which the domain can communicate.**

      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 User Manager and Profile Manager.

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

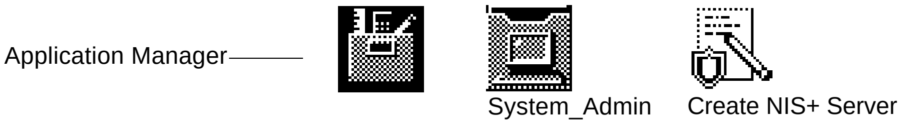
▼ To Set Up NIS+ with Databases from the Staging Area

For fuller descriptions of NIS+ setup and administration, see

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

Role - root
Label - admin_low
Action - Create NIS+ Server

1. **Double-click the Create NIS+ server action in the System_Admin folder.**
   See "To Run a Script from the System_Admin Folder" on page 41 if you are unfamiliar with using trusted actions.



2. **Enter your NIS+ domain name.**
   This workstation will be the root master. For example,

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

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

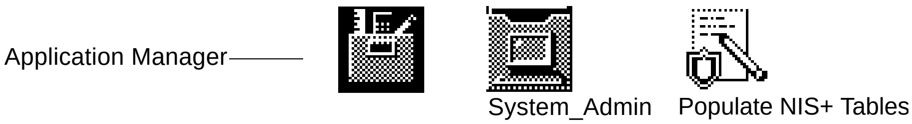
3. **Answer the prompts (y, y, *rootpassword*).**
   You can ignore diagnostics printing out that the file `/etc/defaultdomain` cannot be located. The file will be created.

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

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

Role - root
Label - admin_low
Action - Populate NIS+ Tables

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



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

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

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

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

Role - root
Label - admin_low
Profile shell

8. **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.

9. **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

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

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.**

   Application Manager ——— System_Admin Set DNS Servers

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

      The file looks something like:

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

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

Role - root
Label - admin_low
Action - Name Service Switch

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

   Application Manager ——— System_Admin Name Service Switch

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.**

▼ Reboot the Workstation

♦ **Shut down the workstation from the TP (Trusted Path) menu.**
If you are unfamiliar with rebooting a Trusted Solaris workstation, see "To Reboot the Workstation" on page 52.

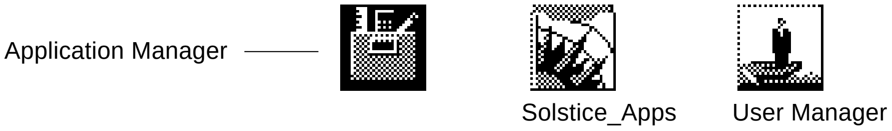
▼ Update Role Credentials and Passwords

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.**
See "To Log In as the User "Install"" on page 23 and "To Assume a Role" on page 25 if you are unsure of the steps.

2. **Open the User Manager using the NIS+ naming service.**
For a more detailed step through the procedure, see "To Open and Modify a Solstice_Apps Database" on page 35.



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 84.

3. **Give each role a new password.**
   If a detailed procedure would be helpful, see “To Modify the Password for a Role or User Account” on page 36.

Note – To ensure that someone can always log in, use the status Always Open for the secadmin role, and for the user who can assume the secadmin role.

▼ Set Up Home Directories

If this workstation is the home directory server, share home directories.

♦ **Share home directories on the home directory server.**
  If you are unfamiliar with how to share file systems, see “How to Share a File System” on page 43.

If this workstation is *not* the home directory server, configure the home directory server, reboot it, and mount the home directories, as detailed in “Install and Configure the Home Directory Server Now**”** , before adding users**.**

▼ Install and Configure the Home Directory Server *Now*

1. **Go and do:**

Installing a Workstation	*page 54*
Configuring a NIS+ Client	*page 97*
Configure the home directory server up through reboot:	
Set Up Home Directories (on the NIS+ client and NIS+ master)	*page 104*
Reboot the Workstation (boot the NIS+ client)	*page 104*

2. **Then, create the first three users.**
   Continue with “Add Users to be Administrators”.

▼ Add Users to be Administrators

The install team in the role `root` creates at least two users, to assume the roles `secadmin` and `admin`. It is also useful to create a user who can assume the role `root`.

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 and the home directories are automounting, or
- The home directory server *is* the NIS+ root master.

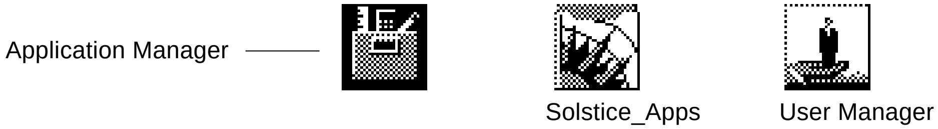
Overview

- 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

Role - root
Label - admin_low
Tool - User Manager

1. **On the home directory server, log in and assume the role root.**
2. **Open the User Manager with the NIS+ Naming Service option.**



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 admin.**

   a. **See Table 5-1 for the information to enter for a user.**
   Make sure you enter information in every dialog.

b. Read the *Comments* column for guidance.
Parentheses enclose suggestions. Requirements or defaults are not enclosed in parentheses.

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**	Assign a password of 8 alphanumeric characters.
	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. In a multilevel system, a multilevel home directory will be created.
	Home directory pathname	/*mount_path*/*username*
	Server	*home directory server*
	Skeleton path	Yes, use it.
	Default permissions on home directory	
	Mail server	
	Cred?	Yes, leave it checked. ✓
	AutoHome setup	Yes, leave it checked. ✓
Labels	**Clearance**	*not* ADMIN_HIGH
	Minimum Sensitivity Label	*not* ADMIN_LOW
	Label View	
	SL visibility	If your site is a no-label site, choose Hide.
	IL visibility	

Table 5-1 User Account Characteristics

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 secadmin.

Note – To ensure that someone can always log in, use the status Always Open for the secadmin role, and for the user who can assume the secadmin role.

5. You may choose to 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 allocate devices, enable logins, print PostScript files, print without labels, remotely log in, and shut down the workstation

6. Close the User Manager

Notes

- Setting up users is a two-role, trusted procedure. *The install team in the role root should set up only the initial administrators.*
- In a multilabel environment, users are set up with a useful file, *.link_files*, from the Skeleton Path.

See *Trusted Solaris User's Guide* and *Trusted Solaris Administrator's Procedures* for details on setting up users and user files.

▼ Log Out

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

Verify that Users and Administrative Roles Work

Bringing up a user in the User Manager confirms that the administrative roles secadmin and admin are working correctly.

1. **For each role, log in and assume the role.**
2. **Open the User Manager and choose the default filter and name service.**
3. **Select a user, and press the Return key.**
   The role admin should be able to modify fields in the dialog boxes Identity and Home.

   The role secadmin should be able to modify fields in the dialog boxes Password, Labels, Profiles, Roles, and Idle Time.
4. **Do the following to verify that the role root is working correctly.**
   a. **Log in and assume the role.**
   b. **Launch a terminal.**
   c. **Find the command** pkgadd(1M) **in the list of commands**:

```
# clist | grep pkgadd
   /usr/sbin/pkgadd
```

5. **Log out, and have a user who can assume the role required for the next task log in.**

Set Up Auditing

The security administrator is responsible for auditing decisions.

Role - secadmin
Label - admin_low
Admin Editor

1. **If site security does not require auditing, disable it.**
   To disable auditing in the Trusted Solaris environment, follow the procedures described in *Trusted Solaris Audit Administration*.
2. **After disabling auditing, go to the next task you plan to do.**

To Configure Auditing

Role - secadmin
Label - admin_low
Various tools

♦ **Use the audit worksheets and the procedures in the** *Trusted Solaris Audit Administration* **guide 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 94.

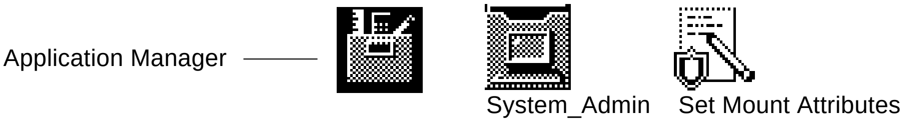
Set the Label for Unlabeled File Systems (Example)

You can mount file systems from workstations that do not recognize labels by setting the label of the mount point 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 (Example)” on page 79.

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.**
   For details of how to edit the file, see “How to Set the Label on an Unlabeled File System” on page 45.



For example, the following entry sets the label Confidential ([C]) on an unlabeled file system, `/cpublic`:

```
/cpublic; \
slabel=C;
```

Share File Systems

Role - admin
Label - admin_low
Action- Share Filesystems

1. **Log in as a user assigned the role admin and assume the role.**

2. **Enter file systems for others to access using the Share Filesystems action.**
   If you are unsure of how to share file systems, see “How to Share a File System” on page 43.

   The following is a sample entry in the `dfstab` file:

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

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_low
Profile shell

3. **Share the file systems.**
   If you are unsure of the commands, see “How to Share a File System” on page 43.

▼ Copy Configuration Files for Distribution to Clients

Role - root
Label - admin_low
Profile shell

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

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

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

```
# cd /etc/security/tsol
# cp -p label_encodings /export/clientfiles
```

Note – The `-p` option to the `cp(1)` command preserves the correct file permissions.

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

```
# cd /etc/security
# cp -p audit_control audit_user audit_startup \
/export/clientfiles
#
# cd /etc/security/tsol
# cp -p tnrhtp /export/clientfiles
#
# cd /etc
# cp -p resolv.conf nsswitch.conf /export/clientfiles
# ls /export/clientfiles
audit_control     audit_user            nsswitch.conf
audit_startup     label_encodings       resolv.conf      tnrhtp
```

▼ To Transfer Files for NIS+ Clients to Tape or Diskette

Role - root
Label - admin_low
Tool - Device Allocation

1. **Allocate the tape or diskette device.**
   See "How to Allocate and Deallocate a Device" on page 32 if you are unfamiliar with the steps. Do not mount the device.

```
Do you want device_n mounted: (y,n)? n
```

2. **Copy the files to the allocated medium.**
   For examples of using the `tar(1TSOL)` command to copy files to a portable medium, see "How to Copy Files To and From a Portable Medium" on page 29.

3. **Deallocate the device and follow the directions in the window.**

▼ 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.

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

♦ **See "To Delete a Local User" on page 38 if you have not deleted a local user in the Trusted Solaris system before.**

Configuring a NIS+ Client 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 an *install team*. Once the team has connected the NIS+ client to the NIS+ master, the software enforces two-role task division. If the client is installed over the net, the roles are enforced at first login.

Role - root
Label - admin_low
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:

Note – The procedures are not numbered. Depending on your site configuration and installation method, some procedures can be omitted.

▼ Log In and Protect the Workstation

Role - root
Label - admin_low
Profile shell

1. **Log in as a user who can assume the role root and assume it.**
   See “How to Log In” on page 22 if you are unsure of the steps.

2. **Protect the workstation.**
   See “How to Protect the PROM” on page 27 if you are unsure of the steps.

3. **Limit contact with other `tsol` hosts if required by site security.**
   See “How to Limit Boot-Time Network Contacts” on page 28 if you are unsure of the steps.

▼ Copy Configuration Files from the NIS+ Master

You made a tape or diskette with files for the client in “Copy Configuration Files for Distribution to Clients” on page 94.

▼ To Copy Master Files from a Tape or Diskette

Role - root
Label - admin_low
Profile shell

1. Make a temporary directory and go to it.

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

Role - root
Label - admin_low
Tool - Device Manager
Profile shell

d. Copy the file from the tape or diskette.

See “To Copy One or More Files from a Tape or Diskette” on page 31 if you are unsure of the steps.

▼ 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
Profile shell

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

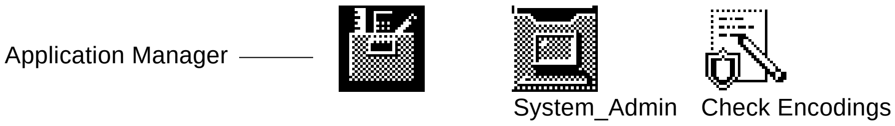
a. Rename the client’s `label_encodings` file.

```
# cd /etc/security/tsol
# cp -p label_encodings label_encodings.orig
# rm label_encodings
```

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

```
# cp -p /export/clientfiles/label_encodings label_encodings
```

2. **Use the Check Encodings action to check the syntax of the file.**
   For more details on using actions, see “To Run a Script from the System_Admin Folder” on page 41.



Caution – Your label_encodings file *must* pass the Check Encodings test before you continue.

▼ Set Up Static Routing

If you set up static routing on the NIS+ master, set it up on the clients.

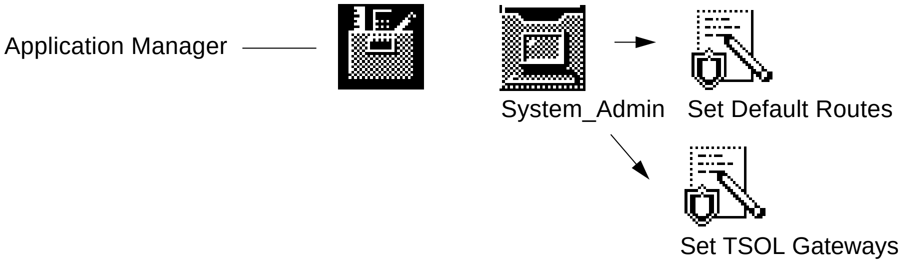
1. **Determine the appropriate static routing for the client.**

Table 6-1 Client Static Routing Entry

	Client on same subnet	**Client on different subnet**
NIS+ master has 1 network interface	Use same entry as NIS+ master’s	Static routing will be slightly different for the subnet
NIS+ master has >1 network interface	Enter NIS+ master’s other network interface(s) in static routing file	

Role - root
Label - admin_low
Action - Set Default Routes
or
Action - Set TSOL Gateways

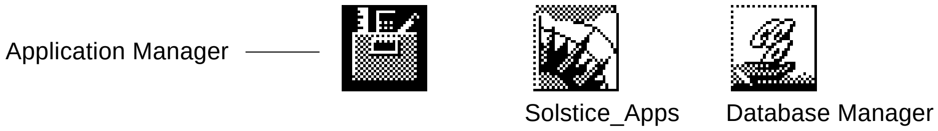
2. **Enter the defaultrouter using the Set Default Routes action, or the tsolgateways using the Static Routing Configuration action.**
   See “Set Up Routing” on page 75 for more explanation.



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

Role - root
Label - admin_low
Tool - Database Manager

4. **Add the static routers and the NIS+ master to the client's local `hosts` database using the Database Manager.**
See "To Open and Modify a Solstice_Apps Database" on page 35 if you are unfamiliar with editing the Hosts database.



5. **Exit the Database Manager.**

▼ Set Up Secondary Network Interfaces

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

♦ **Set up the workstation's network interfaces.**
See "How to Add Network Interfaces" on page 41 if you are unsure of the steps.

▼ Copy the Tnrhtp Database (Example)

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
Profile shell

♦ **Copy the `tnrhtp` file from the `/export/clientfiles` directory to `/etc/security/tsol/tnrhtp`.**

```
# cd /etc/security/tsol
# cp -p tnrhtp tnrhtp.orig
# rm tnrhtp
# cp -p /export/clientfiles/tnrhtp tnrhtp
```

▼ 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`. See “To Edit the Tnrhdb Database” on page 80 if you are unsure of the steps.

2. **Enter the IP address and host type of the static router(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 to inform the kernel of the network change.**

▼ Verify Communication with the NIS+ Master

Note – Skip this procedure if the client specified NIS+ during network install.

Role - root
Label - admin_low
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 static routers, and the client.

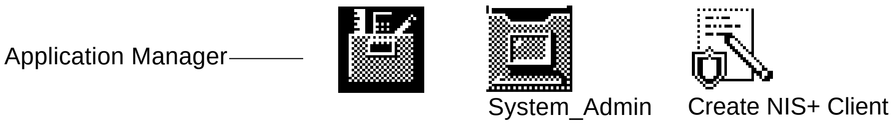
In addition, the client's address and name, the NIS+ master's name and address, and the static routers' names and addresses must be in the local `hosts` database.

▼ Set Up the NIS+ Name Service

Note – Skip this procedure if the client specified NIS+ during network install.

Role - root
Label - admin_low
Action - Create NIS+ Client

1. **Add the workstation as a NIS+ client using the Create NIS+ Client action in the System_Admin folder.**
   See "To Run a Script from the System_Admin Folder" on page 41 if you are unfamiliar with using trusted actions.



   There is a period after the domain name.

2. **Enter the NIS+ domain name and hostname of the root master.**
   For example,

```
Domain Name: aviary.eco.org.
Hostname of NIS+ Master: grebe
```

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

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

4. **Do not reboot when the** `nisclient(1M)` **script prints out:**

```
Once initialization is done, you will need to reboot your machine.
```

You will reboot after setting up DNS. If you are configuring the home directory server, you will reboot after sharing the home directories.

▼ Set Up DNS and the Name Service Switch

Role - root
Label - admin_low
Profile shell

If you are using DNS to contact hosts outside of your domain, or if you have altered the `resolv.conf` and `nsswitch.conf` files on the NIS+ master, set up DNS before rebooting.

♦ **Set up the DNS nameservers and the name service switch by copying the files** `resolv.conf` **and** `nsswitch.conf` **from** `/export/clientfiles` **to the** `/etc` **directory.**

```
# cd /etc
# mv nsswitch.conf nsswitch.conf.orig
# cp -p /export/clientfiles/resolv.conf resolv.conf
# cp -p /export/clientfiles/nsswitch.conf nsswitch.conf
```

▼ Set Up Home Directories

Role - root
Label - admin_low
Action- Share Filesystems

♦ **If this client is the home directory server, share home directories.**
If you are unsure of the steps, see "How to Share a File System" on page 43.

Application Manager —— System_Admin Share Filesystems

▼ Reboot the Workstation

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

♦ **Shut down the workstation from the TP (Trusted Path) menu.**
If you are unfamiliar with rebooting a Trusted Solaris workstation, see "To Reboot the Workstation" on page 52.

▼ Add Users

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

♦ **If you have not yet added users who can assume administrative roles, continue with “Add Users to be Administrators” on page 88.**

▼ Finish Configuring the Workstation

If you are configuring a site that satisfies criteria for an evaluated configuration, please read “Understand Your Site’s Security Policy.” on page 3.

As secadmin

Role - secadmin
Label - admin_low
Various tools

♦ **Log in as a user assigned the role secadmin and assume the role.**

a. To configure auditing, use the audit worksheets and the procedures in *Trusted Solaris Audit Administration***.**

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 the NIS+ Master” on page 99) and enter the correct `dir:` entries as described in *Trusted Solaris Audit Administration*.

b. To disable auditing, follow the procedure in *Trusted Solaris Audit Administration***.**

c. To set security attributes on an unlabeled file system, see “How to Set the Label on an Unlabeled File System” on page 45.

As admin

Role - admin
Label - admin_low
Various tools

♦ **Log in as a user assigned the role admin and assume the role.**

a. To share a file system, see “How to Share a File System” on page 43.

b. To mount a file system, labeled or unlabeled, see “How to Mount a File System” on page 46.

c. **To delete the** `install` **user, see "To Delete a Local User" on page 38 if you have not deleted a local user in the Trusted Solaris environment before.**

Preparing to Install Trusted Solaris Over a Network

7

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:

Servers Required for Network Installation

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

- *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.

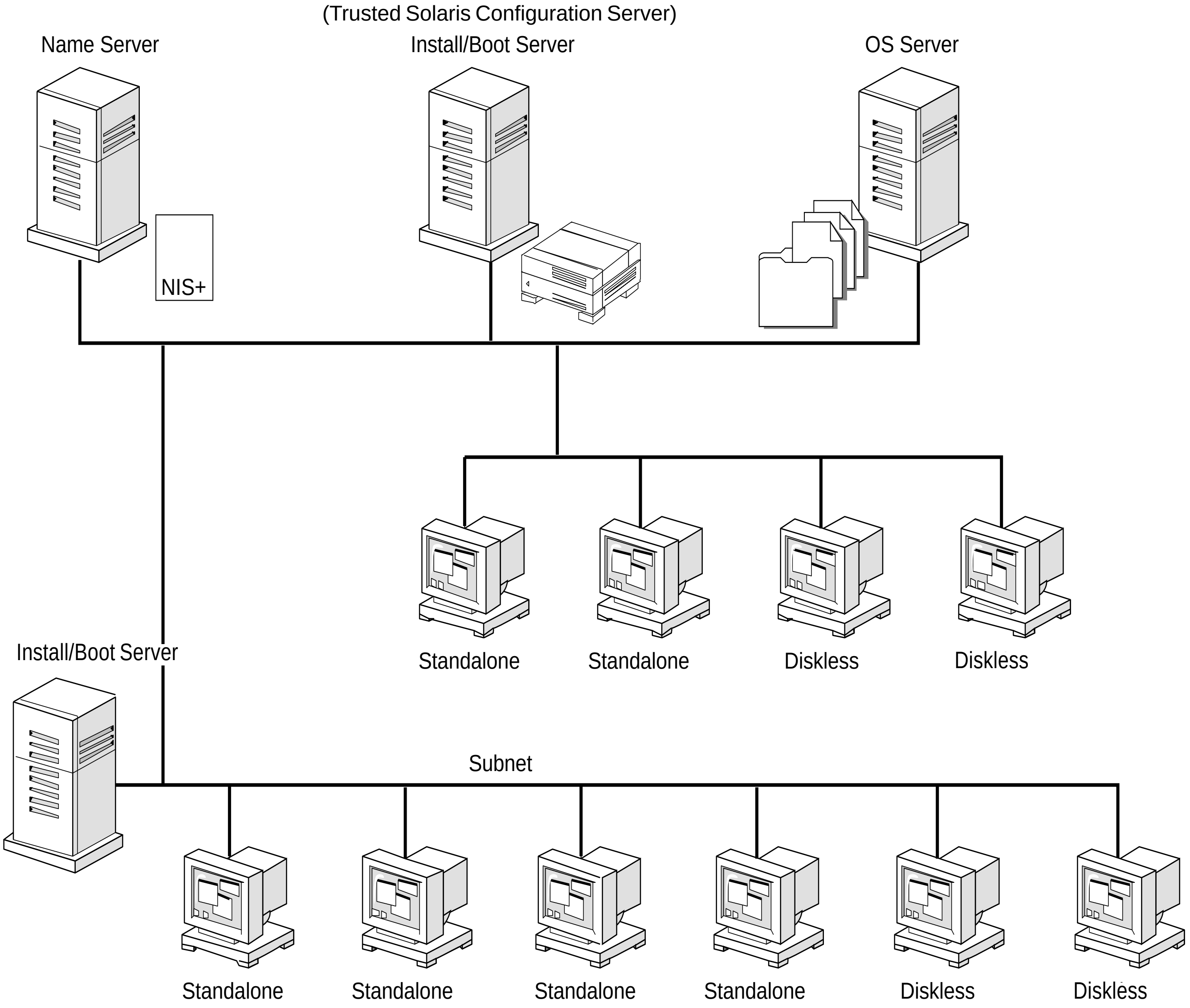


Figure 7-1 Network Installation Servers

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 78*

   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 114*

   Result: The Trusted Solaris 2.5.1 image and booting software is available for network install.

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

Create a Trusted Solaris Configuration Server	*page 116*

   Result: The Trusted Solaris 2.5.1 configuration values are available for network install.

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

Add Client Information for a Network Install	*page 120*

   Result: The Trusted Solaris 2.5.1 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 126*

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

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 129*

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(1MTSOL)` 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(1MTSOL)` 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(1TSOL)` 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.

The following files are

- *recommended* for unscripted network installation, because they reduce the amount of interaction and reduce errors.
- *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 for which you are otherwise prompted. 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. Users who can assume the roles admin, secadmin, and root should be present.

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 53*
Configuring a NIS+ Client	*page 97*

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

Role - root
Label - admin_low
Profile shell

2. **Create a mount point for the CD.**

```
# mkdir /cdrom
```

Role - root
Label - admin_low
Tool - Device Allocation

3. **Allocate the CDROM drive at admin_low, and answer (y):**

```
Do you want cdrom_n mounted: (y,n)? y
```

See “To Allocate a Device” on page 32 if you are unsure of the steps.

Role - secadmin
Label - admin_low
Tool - Profile Manager

4. **As a user who has assumed the role** `secadmin`**, add the** `/cdrom/cdrom0/setup_install_server` **command to the** `root` **role’s profile.**
For the full procedure, see “To Add a Command to a Role’s Profile” on page 48.

Role - root
Label - admin_low
Profile shell

5. **As a user who has assumed the role** `root`**, verify that the command is available to you.**
For the full procedure, see “To Verify That a Command is in a Role’s Profile” on page 48.

6. **In the same terminal where the** `setup_install_server` **command was verified, change to the** `cdrom0` **directory.**

```
# cd /cdrom/cdrom0
```

7. **Use the** `setup_install_server` **command to copy the contents of the CDROM to a permanent location on the install server.**

```
# ./setup_install_server install_dir_path
```

   a. **To verify that the script is running properly, check the following processes.**

```
# ps -ef | grep setup_install_server
# ps -ef | grep find
# ps -ef | grep cpio
# ppriv -p setup_install_server_PID find_PID cpio_PID
ppriv should display: all
```

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/ts2.5.1_sparc` directory on the local disk:

```
./setup_install_server /export/install/ts2.5.1_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 - secadmin
Label - admin_low
Tool - Profile Manager

8. **If there are no boot servers to install, remove the `/cdrom/cdrom0/setup_install_server` script from the Custom Root Role.**
   For the procedure, see "To Remove a Command from a Role's Profile" on page 49.

Role - root
Label - admin_low
Tool - Device Allocation

9. **Assume the role `root` to deallocate the drive and remove the CDROM.**
   See "To Deallocate a Device" on page 33 if you are unsure of the steps.

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

▼ Create a Trusted Solaris Configuration 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 - admin
Label - admin_low
Profile shell

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

2. **Launch a terminal, create a directory and go to it.**
   For example,

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

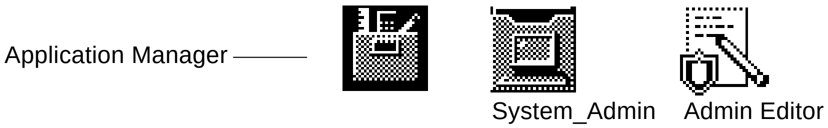
3. **Copy the** `label_encodings` **file from** `/etc/security/tsol`**.**
   For example,

```
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 in.**

5. **In the role** `secadmin`**, use the Admin Editor to create a file named** `tsolconfig_dir_path/config_data`**.**



   For example, the file name would be `/export/install/tsolfiles/config_data`.

   a. **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=no
enable_il_floating=no
reset_il_on_exec=no
hide_upgraded_names=no
```

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

Role - secadmin
Label - admin_low
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 *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 and enter the** ***tsolconfig_dir_path*** **with any relevant options.**
   See "To Open a File that has a Defined Action" on page 41 if you are unfamiliar with the steps.

   Application Manager ——— System_Admin Share Filesystems

   For example:

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

3. **Share the file system.**

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

4. **Check that the file system is shared.**
   If you are unfamiliar with how to check that a file system is shared, see “To Check That a Directory Is Shared” on page 44.

Result: Once the file system is shared, 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 in 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 using the NIS+ naming service.**
   See “To Open and Modify a Solstice_Apps Database” on page 35 if you are unfamiliar with the steps.

Application Manager ——— Solstice_Apps Database Manager

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 also add the Trusted Solaris configuration information.

You have a choice of two methods for entering the information:

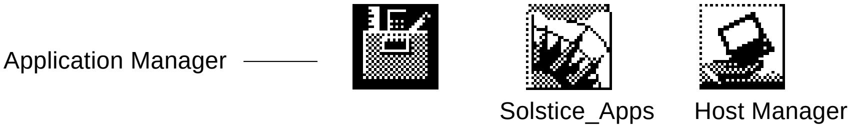
- Using the Host Manager with the NIS+ naming service.
  Use this method to have the NIS+ name service provide the client information. This is the most efficient method.
- Using the `add_install_client(1MTSOL)` command to modify the install server's local files.
  Use this method if you have scripts that run the `add_install_client` command for your clients.

Add Client Information Using the Host Manager

1. **On the install server, log in 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 using the NIS+ naming service.**
   See "To Open and Modify a Solstice_Apps Database" on page 35 if you are unfamiliar with the steps.



3. **If the workstation already exists, select it in the Host Manager main window, choose Edit > Convert > Standalone.**
4. **If the workstation does not already exist, add it by choosing Edit > Add.**
5. **For each workstation, fill out the host information.**
   a. **Enable remote install.**
   b. **Complete all fields up to the Boot Server.**
   c. **Enter the Config Server for Trusted Solaris.**

d. **Click the OK button.**

Table 7-3 Adding Host Information in 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/ts2.5.1_sparc` *`(sample)`*
OS release	*Choose client's platform group and software cluster*
Boot Server	*boot_server_name (if separate server)* *path to boot file*
Profile Server	*Enter JumpStart directory (for Custom JumpStart).*
Config Server	`heron:/export/install/tsolfiles` *`(sample)`* *(for netowrk install, Custom JumpStart)*

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. **Go to "Check Client Information" on page 125.**

Add Client Information with the `add_install_client` Command

Note – If you added hosts and Trusted Solaris configuration information with the Host Manager, do not add information locally, as this command does.

Role - secadmin
Label - admin_low
Tool - Profile Manager

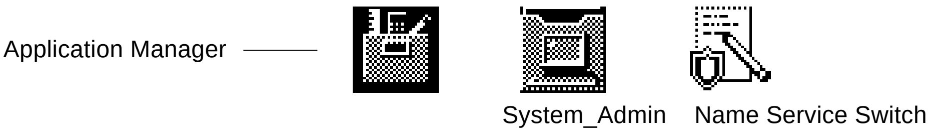
1. **Log in to the install server as a user who can assume the role `secadmin`, assume it, and add the `add_install_client` and `rm_install_client` commands to the `root` role's profile.**
   The path to the commands is *install_dir_path*. For the continuing example, the path is `/export/install/ts2.5.1_sparc`.

   See "To Add a Command to a Role's Profile" on page 48 for the full procedure.

Role - secadmin
Label - admin_low
Action - Name Server Switch

2. **Log in to the install server as a user who can assume the role `root` and assume it.**

3. **Launch the Name Service Switch action in the System_Admin folder.**



4. **Ensure that the value of `ethers` and `bootparams` is `files nisplus`, as in:**

```
ethers:    files nisplus dns
netmasks:  files nisplus dns
bootparams: files nisplus dns
```

Role - root
Label - admin_low
Profile shell

5. **As `root`, verify that the commands `add_install_client` and `rm_install_client` are in your profile.**

```
# clist -p | grep install_client
It should display:
/export/install/ts2.5.1_sparc/add_install_client: all
/export/install/ts2.5.1_sparc/rm_install_client: all
```

See “To Verify That a Command is in a Role’s Profile” on page 48 for the full procedure.

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

```
# cd boot_dir_path
```

For example, if the boot server is also the install server:

```
# cd /export/install/ts2.5.1_sparc
```

7. **Run the** `add_install_client(1MTSOL)` **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/ts2.5.1_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.ts2.5.1_sparc`.

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

Role - secadmin
Label - admin_low
Tool - Profile Manager

8. As `secadmin`**, remove the** `add_install_client` **script from the Custom Root Role.**

See "To Remove a Command from a Role's Profile" on page 49 for the full procedure.

9. Go to "Check Client Information" on page 125.

Remove Client Information with the `rm_install_client` Command

Role - root
Label - admin_low
Profile shell

1. **Log in as a user who can assume the role `root`, assume it, and launch a terminal.**

2. **Verify that `rm_install_client` is in the `root` profile shell.**

```
# clist -p | grep rm_install_client
It should display:
/export/install/ts2.5.1_sparc/rm_install_client: all
```

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

```
# cd boot_dir_path
```

4. **Run the `rm_install_client` command for every client you plan to remove from the network install.**

```
# ./rm_install_client host_name
```

Role - secadmin
Label - admin_low
Tool - Profile Manager

5. **Once all clients are removed, assume the role `secadmin` and remove the `rm_install_client` script from the Custom Root Role.**
   See "To Remove a Command from a Role's Profile" on page 49 for the full procedure.

Check Client Information

Follow this procedure to verify that the `bootparams` file contains the required information.

Role - admin
Label - admin_low
Tool - Database Manager

1. **Open the Database Manager, and choose the appropriate naming service before loading the `bootparams` database.**

2. **Scroll through a host's entry to locate the keyword=value pairs:**
   `tsol_config=`*server:tsolconfig_dir_path*   `install_server=`*server:tinstall_dir_path*

Task
Complete

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

3. **If there are subnets, continue with "Create a Boot Server on a Subnet".**

4. **Otherwise, go to "Reboot the Install Server" on page 128.**

▼ 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 "Reboot the Install Server" on page 128.

1. **Follow Step 1 through Step 2 in "Create an Install Server" on page 114.**

2. **Determine your next step based on whether the boot server uses a local CDROM 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) As** `root`**,** `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 6.

Role - root
Label - admin_low
Tool - Device Allocation

3. **Allocate the CDROM drive.**
   The device should be allocated at the label admin_low and mounted.

```
Do you want cdrom_n mounted: (y,n)? y
```

4. **Check that the** `setup_install_server` **command is in the profile shell.**

```
# clist -p | grep setup_install_server
It should display: /cdrom/cdrom0/setup_install_server: all
```

If the command is not available, place the command in the profile before continuing. See “To Add a Command to a Role’s Profile” on page 48 and “To Verify That a Command is in a Role’s Profile” on page 48 for the full procedure.

5. **Change directory to the Trusted Solaris image.**

```
# cd /cdrom/cdrom0
```

Role - root
Label - admin_low
Profile shell

6. **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/ts2.5.1_sparc` directory on the boot server:

```
# ./setup_install_server -b /export/bootdir/ts2.5.1_sparc
```

The workstation is now configured as a boot server.

Role - secadmin
Label - admin_low
Tool - Profile Manager

7. **After all boot servers are installed , remove the `/cdrom/cdrom0/setup_install_server` script from the Custom Root Role.**
For the procedure, see “To Remove a Command from a Role’s Profile” on page 49.

▼ Reboot the Install Server

Before installing clients across the network, you must reboot the server.

1. **Shut down the install server from the TP (Trusted Path) menu.**
   If you are unfamiliar with rebooting a Trusted Solaris workstation, see "To Reboot the Workstation" on page 52.

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

2. **Follow the network installation procedure, "To Boot Over a Network:" on page 55, in Chapter 3, "Installing a Workstation".**

   Task Complete

   Clients will get platform, ethernet, and other system identification 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.

   The installation program will prompt for information that is not on the 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.

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 2.5.1 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 Configuration Server” on page 116 and “Add Client Information for a Network Install” on page 120 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 2.5 operating environment
- Creating dataless clients

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:

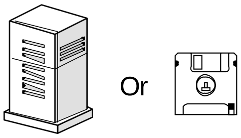
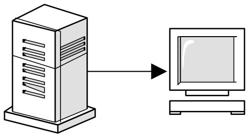
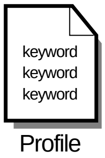
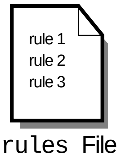
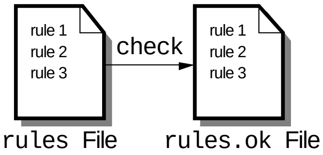
- An install server (for the Trusted Solaris image)
- A Trusted Solaris configuration server (for Trusted Solaris configuration values)
- A boot server (for boot information on a subnet)
- A JumpStart server (for the JumpStart information).

♦ **To set up these servers, follow the procedures in Chapter 7, “Preparing to Install Trusted Solaris Over a Network”.**

Tasks to Set up Custom JumpStart Installations

The following table 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 136. If you are going to use a server for custom JumpStart installations, see “Creating a JumpStart Directory on a Server” on page 139.
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 Access to the JumpStart Directory” on page 141 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 145 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 157 for detailed information.
Using `check` to validate the `rules` file	 rule 1 rule 2 rule 3 check rule 1 rule 2 rule 3 rules File 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* use the `check` script to create the `rules.ok` file. See “Using check to Validate the rules File” on page 169 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.

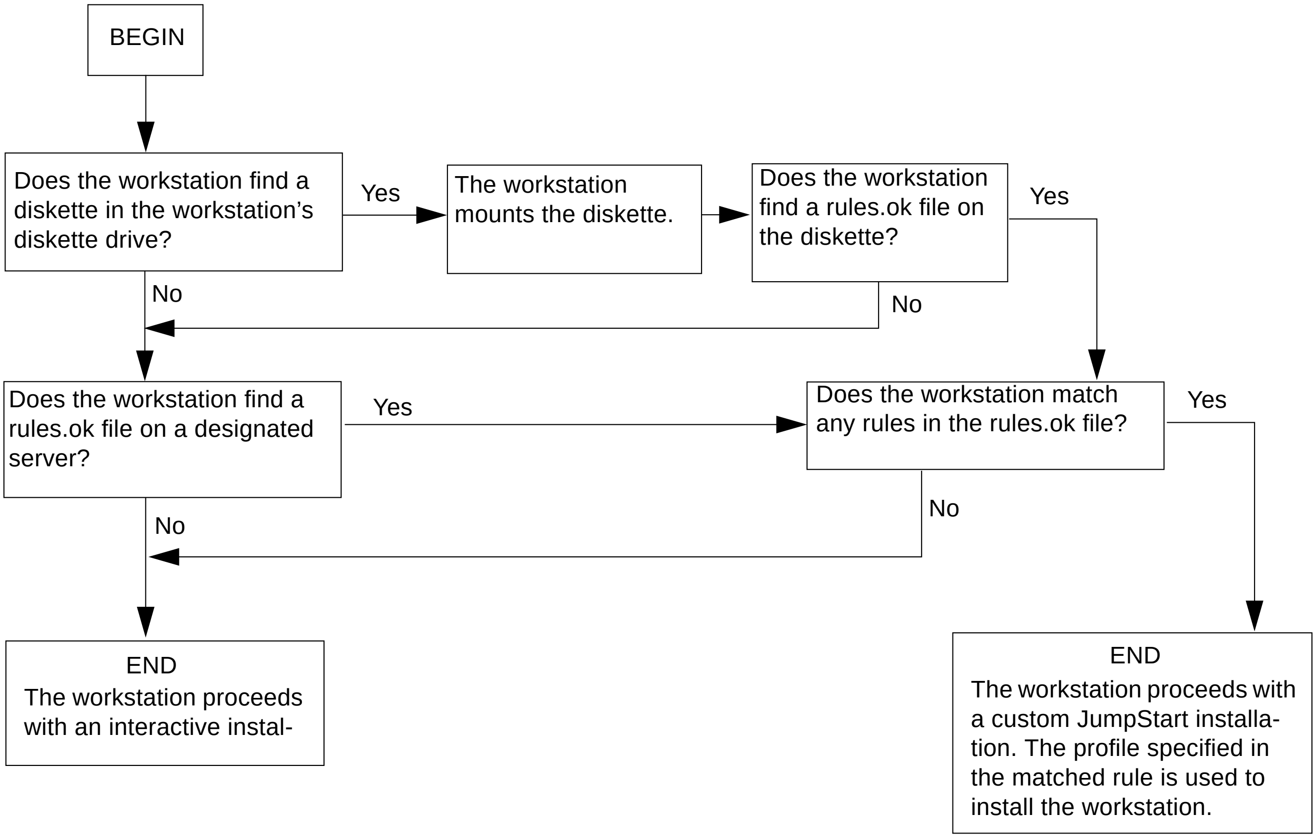

BEGIN
Does the workstation find a diskette in the workstation's diskette drive?
Yes
The workstation mounts the diskette.
Does the workstation find a rules.ok file on the diskette?
Yes
No
No
Does the workstation find a rules.ok file on a designated server?
Yes
Does the workstation match any rules in the rules.ok file?
Yes
No
No
END
The workstation proceeds with an interactive instal-
END
The workstation proceeds with a custom JumpStart installation. The profile specified in the matched rule is used to install the workstation.

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.

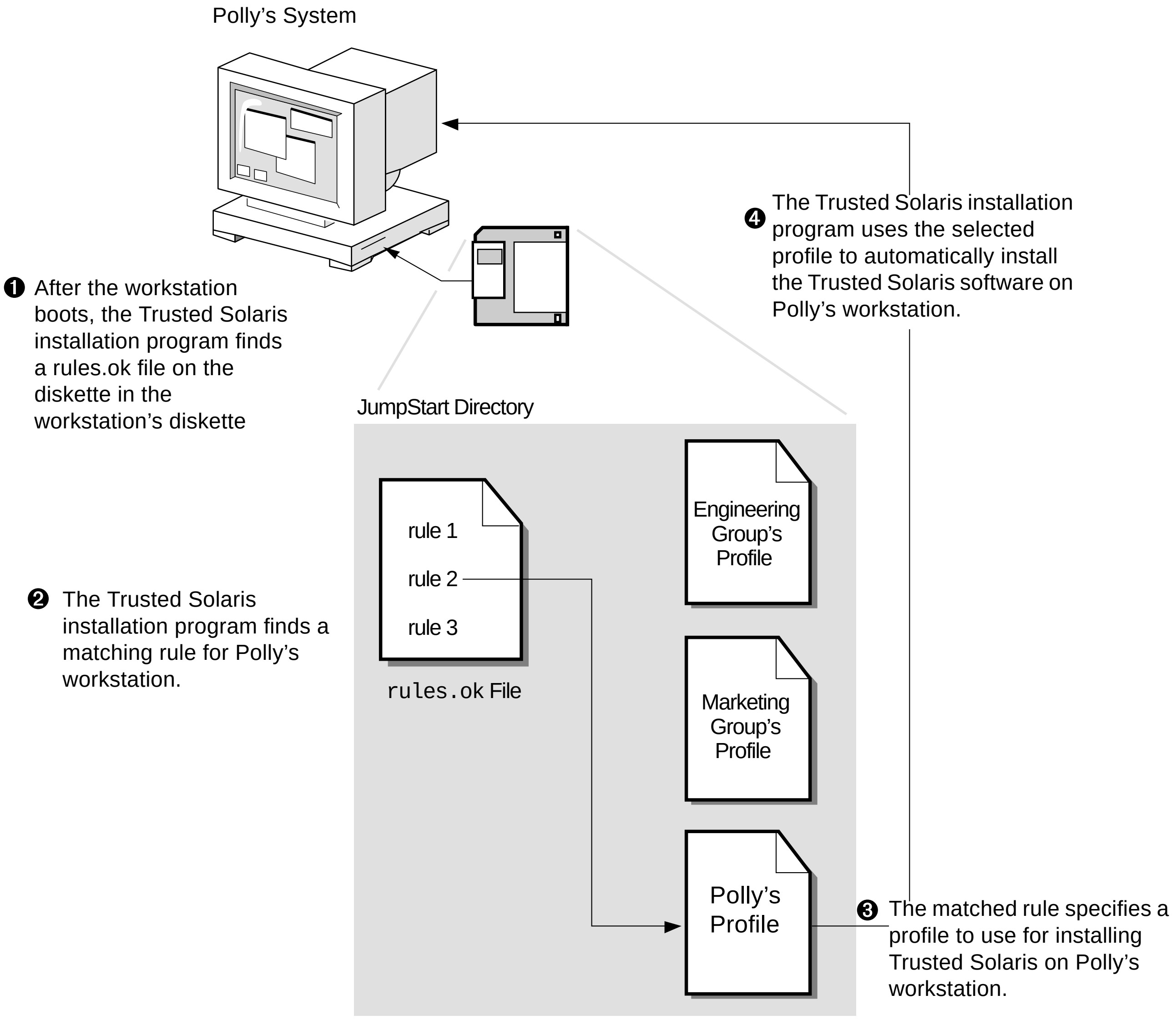
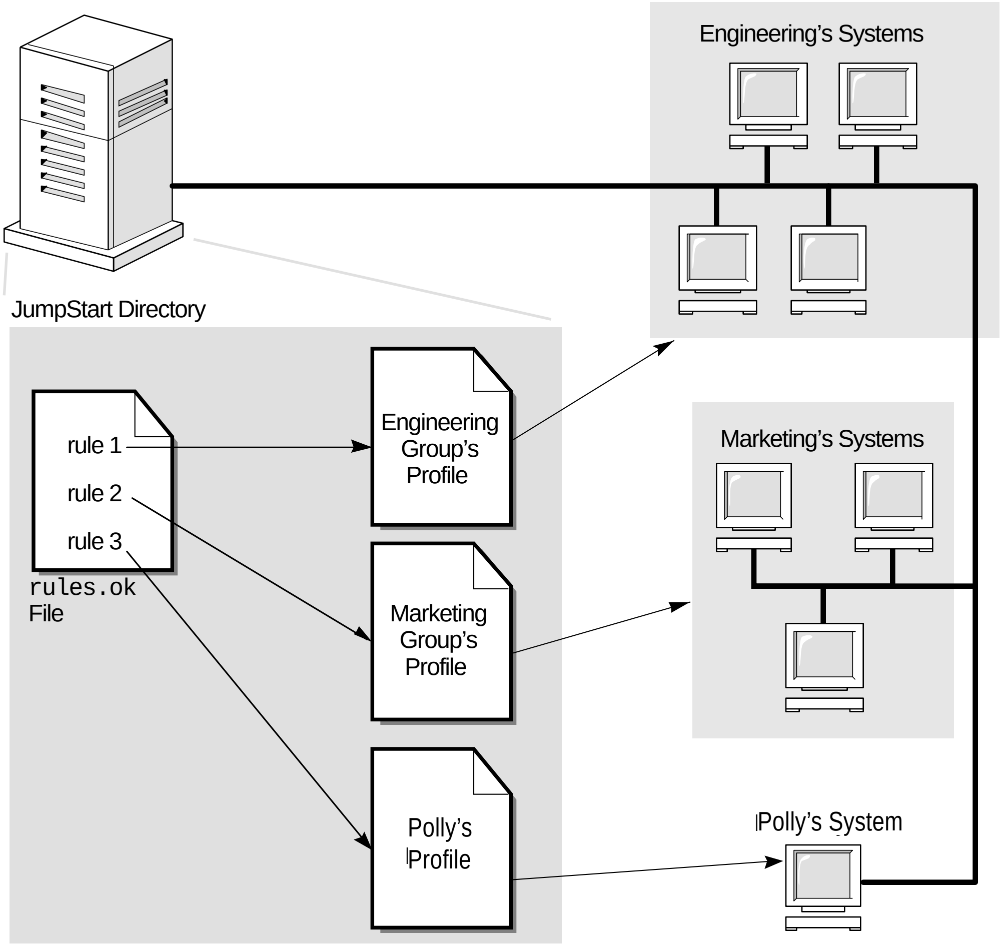

Polly's System
❶ After the workstation boots, the Trusted Solaris installation program finds a rules.ok file on the diskette in the workstation's diskette
❷ The Trusted Solaris installation program finds a matching rule for Polly's workstation.
❸ The matched rule specifies a profile to use for installing Trusted Solaris on Polly's workstation.
❹ The Trusted Solaris installation program uses the selected profile to automatically install the Trusted Solaris software on Polly's workstation.
JumpStart Directory
rule 1
rule 2
rule 3
rules.ok File
Engineering Group's Profile
Marketing Group's Profile
Polly's Profile

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.



❶ After a workstation boots, the Trusted Solaris installation program finds a rules.ok file on a designated server.

❷ The Trusted Solaris installation program finds a matching rule for the specific workstation.

❸ The matched rule specifies a profile to use for installing the Trusted Solaris software on that workstation.

❹ The Trusted Solaris installation program uses the selected profile to automatically install the Trusted Solaris software on the workstation.

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 Allocation

2. **Allocate the diskette drive.**
   See "To Allocate a Device" on page 32 if you are unsure of the steps. The device should be allocated at the label admin_low, and *not* mounted.

```
Do you want floppy_n mounted: (y,n)? n
```

3. **Insert a diskette into the diskette drive.**

4. **If the diskette already has a UFS file system on it, go to Step 7.**
   If the `mount` command fails in Step 7, the diskette does not have a UFS file system on it.

Role - root
Label - admin_low
Profile shell

5. **Launch a terminal and format the diskette:**

```
# fdformat /dev/rdiskette
```

6. **Create a file system on the diskette:**

```
# newfs /dev/rdiskette
```

Role - admin
Label - admin_low
Profile shell

7. **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 `/jumpstart` directory:

```
mount -F ufs /dev/diskette /jumpstart
```

Note – If the `mount` command fails, go back to Step 5 to format the diskette.

8. **Determine your next step based on the location of the Trusted Solaris CD image.**

If You Want to Use the ...	Then ...
Trusted Solaris CD in the local CDROM drive	**1)** As root, create a mount point at admin_low. For example: `mkdir /cdrom` **2)** Insert the Trusted Solaris CD into the CDROM drive. **3)** Go to Step 6.
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/ts2.5.1_sparc` **2)** Go to Step 10.

Role - root
Label - admin_low
Tool - Device Allocation

9. **Allocate the CDROM drive.**
   The device should be allocated at the label admin_low and mounted.

```
Do you want cdrom_n mounted: (y,n)? y
```

10. **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:**

```
# cd /cdrom/cdrom0
# 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.

11. **Deallocate the CDROM drive and the diskette drive. Label the diskette.**
    See "To Deallocate a Device" on page 33 if you are unsure of the steps.

Task
Complete

You have completed creating a JumpStart directory on the diskette. To continue, see "How to Create a Profile" on page 146.

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
Profile shell

2. **Launch a terminal and 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 -p /jumpstart
```

Role - root
Label - admin_low
Action - Share Filesystems

3. **Share the directory.**
For details, see “How to Share a File System” on page 43.

Application Manager — System_Admin Share Filesystems

a. **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 2:

```
share -F nfs -o ro,anon=0 /jumpstart
```

4. **Share the file system.**
For example,

```
# share /jumpstart
```

5. **Determine the next step based on the location of the Trusted Solaris image.**

If You Want to Use The ...	Then ...
Trusted Solaris CD in the local CDROM drive	**1)** As root, create a mount point at admin_low. For example: `mkdir /cdrom` **2)** Insert the Trusted Solaris CD into the CDROM drive. **3)** Go to Step 6.
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/ts2.5.1_sparc` **2)** Go to Step 8.

Role - root
Label - admin_low
Tool - Device Allocation

6. **Allocate the CDROM drive.**
   See “To Allocate a Device” on page 32 if you are unsure of the steps. The device should be allocated at the label admin_low and mounted.

```
Do you want cdrom_n mounted: (y,n)? y
```

Role - root
Label - admin_low
Profile shell

7. **Change the directory to the mounted CD:**

```
$ cd /cdrom/cdrom0
```

Role - root
Label - admin_low
Profile shell

8. **Copy the contents of the** `auto_install_sample` **directory from the Trusted Solaris CDROM 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 2:

```
# cp -r auto_install_sample/* /jumpstart
```

9. **Deallocate the CDROM drive.**
   See “To Deallocate a Device” on page 33 if you are unsure of the steps.

Task Complete

You have completed creating a JumpStart directory on the server.

10. **Continue with “Enabling Access to the JumpStart Directory”.**

Enabling Access to the JumpStart Directory

The JumpStart directory 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 120. You can also directly edit the bootparams database on the install server.

Note – The following procedure is not necessary if you are using a diskette for the JumpStart directory.

▼ How to Enable Access to the JumpStart Directory

Follow the same procedure that you used to set up the network servers in Chapter 7, "Preparing to Install Trusted Solaris Over a Network".

Method 1: Host Manager

Role - admin
Label - admin_low
Tool - Host Manager

1. **Launch the Host Manager using the same naming service you did for setting up network install, and select a workstation.**
   See "Add Client Information Using the Host Manager" on page 120 for a description of the Host Manager interface.

2. **Enter** *jumpstart_dir_path* **as the Profile Server entry and click OK.**
   For example, enter `stork:/jumpstart`.

3. **If you have not already done so, enter** *tsolconfig_dir_path* **as the Config Server entry and click OK.**
   See "Create a Trusted Solaris Configuration Server" on page 116 for how to create a *tsolconfig_dir_path* value.

4. **Choose File > Save Changes.**
   When you save the entry, the Host Manager places the information in the `bootparams` database.

5. **Repeat for all hosts to be installed with custom JumpStart, then exit the Host Manager.**

Role - admin
Label - admin_low
Tool - Database Manager

6. **Launch the Database Manager using the same naming service you did for setting up network install.**

7. **Load the** `bootparams` **database.**

8. **To fully automate custom JumpStart, add an** `ns` **entry before the initial entry. Leave a space between it and the next entry.**

```
ns=nis+_server:nisplus(netmask)
```

For example,

```
ns=grebe:nisplus(255.255.255.0)
```

Method 2: add_install_client Command

1. **Go to “Add Client Information with the add_install_client Command” on page 122.**

Role - root
Label - admin_low
Profile shell

2. **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 stork:/jumpstart \
 -T heron:/export/install/tsolfiles \
 -s heron:/export/install/ts2.5.1_sparc willet sun4m
```

modifies the local `bootparams` database to look for custom JumpStart information in the `stork:/jumpstart` directory.

The result: The client `willet` can be installed with custom JumpStart. Its Trusted Solaris 2.5.1 image will come from `heron` (as will its boot information and Trusted Solaris configuration values), and its custom JumpStart installation profile will come from `stork`.

▼ How to Check Access to the JumpStart Directory

If you want to check the bootparams database file directly:

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

Role - admin
Label - admin_low
Tool - Database Manager

2. **Edit the `bootparams` database.**
   For details, see "To Open and Modify a Solstice_Apps Database" on page 35.

Application Manager —— Solstice_Apps Database Manager

3. **Scroll through a host's entry to locate the keyword=value pairs:**
   `tsol_config=`*server:tsolconfig_dir_path*
   `install_server=`*server:install_dir_path*
   `install_config=`*server:jumpstart_dir_path*

   For example, the following keyword=value pair in a workstation's `bootparams` entry would enable it to access the `/jumpstart` directory on the server named `stork`:

```
install_config=stork:/jumpstart
```

   The following keyword=value pairs in the same workstation's bootparams entry would enable it to access the Trusted Solaris configuration files on heron, and the Trusted Solaris installation image on `heron`. Together, these three keyword=value pairs enable custom JumpStart:

```
tsol_config=heron:/export/install/tsolfiles
install_server=heron:/export/install/ts2.5.1_sparc
```

Note – If you see the following error message when booting an install client: `WARNING: getfile: RPC failed: error 5: (RPC Timed out).` Read page 266 for more details and for how to fix the error.

All workstations can now access the JumpStart directory.

Task Complete

4. **Continue with "Creating a Profile".**

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 136 or page 139, example profiles have been placed 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 176.
- 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 177.

For an example of a rule that calls a finish script, see “Recommendations for Trusted Solaris Rules” on page 158.

▼ 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 - root
Label - admin_low
Profile shell

1. **Open the Admin Editor.**

   Application Manager —— System_Admin Admin Editor

2. **Enter a file name (the profile) to be edited.**
   You can create a new file or edit one of the sample profiles in the JumpStart directory you created. For example,

```
File to Edit: /jumpstart/basic_install_profile
```

   The name of a profile should reflect how it will install the Trusted Solaris software on a workstation (for example, `basic_install_profile`, `eng_profile`, or `mktg_profile`).

3. **Add profile keywords and profile values to the profile.**
   Be aware of these things as you edit the profile:

   - “Profile Examples” on page 147 provides some examples of profiles.
   - Table 8-2 on page 150 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.

Note – See “Using pfinstall to Test Profiles” on page 180 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 158.

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 150 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.

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 7)*

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 233 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 7)*

<table>
<tr><th>Profile Keyword</th><th>Profile Values and Description</th></tr>
<tr><td>`cluster`
(use for software groups)</td><td>*group_name*</td></tr>
<tr><td></td><td>`cluster` designates what software group to add to the workstation. The cluster names for the software groups are:
<table><tr><th>Software Group</th><th>*group_name*</th></tr><tr><td>End user system support</td><td>`SUNWCuser`</td></tr><tr><td>Developer system support</td><td>`SUNWCprog`</td></tr><tr><td>Entire distribution</td><td>`SUNWCall`</td></tr></table>
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.</td></tr>
<tr><td>`cluster`[†]
(use for clusters)</td><td>*cluster_name* `[add | delete]`</td></tr>
<tr><td></td><td>`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*.</td></tr>
<tr><td>`dontuse`</td><td>*disk_name*</td></tr>
<tr><td></td><td>`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.</td></tr>
</table>

Table 8-2 Profile Keyword and Profile Value Descriptions *(3 of 7)*

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`. • `cw`*t*`x`*d*`y`*s*`z` or `cx`*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 7)*

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 `c`*w*`t`*x*`d`*y*`s`*z*. 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 `c`*w*`t`*x*`d`*y*`s`*z*. • *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,nodev`
`install_type`†	`initial_install | upgrade`
	`install_type` defines whether to perform the initial installation option or upgrade option on the system. **Restriction:** `install_type` must be the first profile keyword in every profile.

Table 8-2 Profile Keyword and Profile Value Descriptions *(5 of 7)*

<table>
<tr><th>Profile
Keyword</th><th>Profile Values and Description</th></tr>
<tr><td>locale[†]</td><td><i>locale_name</i></td></tr>
<tr><td></td><td>locale designates that the localization packages associated with the selected software should be installed (or added for upgrade) for the specified <i>locale_name</i>. The <i>locale_name</i> values are the same as the values used for the $LANG environment variable. Trusted Solaris 2.5.1 supports the following localizations:
<table>
<tr><th>Language</th><th><i>locale_name</i></th></tr>
<tr><td>Chinese</td><td>zh</td></tr>
<tr><td>French</td><td>fr</td></tr>
<tr><td>German</td><td>de</td></tr>
<tr><td>Italian</td><td>it</td></tr>
<tr><td>Japanese</td><td>ja</td></tr>
<tr><td>Korean</td><td>ko</td></tr>
<tr><td>Latin American</td><td>es</td></tr>
<tr><td>Swedish</td><td>sv</td></tr>
<tr><td>Taiwanese</td><td>zh_TW</td></tr>
</table>
The English localization packages are installed by default. You can specify locale once for each localization you need to support.</td></tr>
<tr><td>num_clients</td><td><i>client_num</i></td></tr>
<tr><td></td><td>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 (<i>client_num</i>) that a server will support. If you do not specify num_clients, five diskless clients are allocated.
<b>Restriction:</b> num_clients can be used only when system_type is specified as server.</td></tr>
</table>

Table 8-2 Profile Keyword and Profile Value Descriptions *(6 of 7)*

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. For Upgrade: • All packages already on the system are automatically upgraded. • If you specify *package_name* `add`, and *package_name* is not installed on the system, the package is installed. • If you specify *package_name* `delete`, and *package_name* is installed on the system, the package is deleted *before* the upgrade begins. • If you specify *package_name* `delete`, and *package_name* is not installed on the system, the package is prevented from being installed if it is part of a cluster that is designated to be installed.

Table 8-2 Profile Keyword and Profile Value Descriptions *(7 of 7)*

Profile Keyword	Profile Values and Description
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
	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 136 or page 139, 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 163). 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 176. 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
Action - Admin Editor

1. **Open the Admin Editor.**
   See "To Create or Open a File from the Trusted Editor" on page 40 if you are unfamiliar with the steps.

   Application Manager —— System_Admin Admin Editor

2. **To edit the sample `rules` file:**

```
File to Edit: /jumpstart/rules
```

3. **To create a `rules` file in `/export/tmp`:**

```
File to Edit: /export/tmp/rules
```

4. **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 161 provides some examples of rules.
   - Table 8-5 on page 163 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 163 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 163 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 173 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 188 and "Creating Derived Profiles With Begin Scripts" on page 174.
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 176 for detailed information on how to create finish scripts.

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 169.

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 162.

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* <u>platform</u> SPARC	 <u>*processor_type*</u> sparc	Matches a workstation's processor type. The `uname -p` command reports the workstation's processor type.
`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 `c`*x*`t`*y*`d`*z*, 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 168. *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 `c`*w*`t`*x*`d`*y*`s`*z*, 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 168. *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. Run the command in the role admin.

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 is not 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_60'`
	System	*model_name*	
	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	
	SPARCserver 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	
	Sun UltraServer 2	SUNW,Ultra-2	
	Sun UltraEnterprise	SUNW,Ultra-Enterprise	

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
Profile shell

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 2.5.1 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

To complete the Custom JumpStart installation the profiles, rules, and rules.ok files you have customized for JumpStart must be added to *jumpstart_dir_path*. Check that all interactive prompts can be answered.

▼ Copy JumpStart Files to *jumpstart_dir_path*

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

Role - root
Label - admin_low
Profile shell

2. **Launch a terminal and 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 136 for the procedure.

```
$ cd jumpstart_dir_path
```

3. **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 finish.sh *profile* rules rules.ok jumpstart_dir_path
```

4. **Check file permissions.**

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]

Role - root
Label - admin_low
Tool - Device Allocation

5. **Deallocate the diskette drive if the *jumpstart_dir_path* is on a diskette.**

Result: The custom JumpStart files are available to the installation program.

▼ Check That All Installation Questions Can Be Answered

A custom JumpStart installation prompts you interactively if the installation program cannot get information that it requires.

♦ **Did you complete the following procedures?**

- “Create an Install Server” on page 114
- “Create a Trusted Solaris Configuration Server” on page 116
- “Set the Default Date and Time” on page 119
- “Add Client Information for a Network Install” on page 120
- “How to Create a JumpStart Directory on a Server” on page 139 or “How to Create a JumpStart Directory on a Diskette” on page 136
- “How to Enable Access to the JumpStart Directory” on page 142
- “How to Create a Profile” on page 146
- “How to Create the rules File” on page 158
- “Copy JumpStart Files to jumpstart_dir_path” on page 171

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 “Boot the workstation using the appropriate boot command.” on page 55 in Chapter 3, “Installing a Workstation”.”

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
```

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.

5. 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
Profile shell

1. **On an installed and configured Trusted Solaris workstation, log in as a user who can assume the role `root` and assume it.**
2. **Launch a terminal and see that the `pfinstall(1M)` command is available in the role's profile shell.**

```
# clist | grep pfinstall
```

Note – The name *profile shell* refers to a shell that recognizes Trusted Solaris *execution profile*s. It does not refer to the machine 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 3, "Installing a Workstation".

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
Profile shell

3. **Launch a terminal and determine the device name for the workstation's disk.**
4. **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 `cwtxdys2` or `cxdys2`.

Note: Slice 2 must be specified in *device_name*.

disk_config Is the disk configuration file name.

5. **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.

Task Complete

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
```

Configuring Diskless Clients 10

Configuring diskless clients for Trusted Solaris software is similar to configuring them for the Solaris 2.5.1 environment. 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
- Solstice AdminSuite databases mounted on `/opt`

▼ Install and Configure an OS Server

An OS server is a *system type*. When you choose the OS server system type during installation, you are prompted to allocate disk space for its diskless clients.

When an OS server is installed over the network rather than interactively, the Host Manager records that it is an OS server.

Path 1 - Create OS Server during Installation

1. **Choose the OS server system type during installation:**

Installing a Workstation	*page 54*

2. **Use the OS server worksheets during installation:**

OS Server Installation Worksheet	*page 215*
OS Server Disks for Partitioning	*page 216*
OS Server Installation Program Example	*page 258*
OS Server Disk Partitioning Example	*page 260*

Path 2 - Convert Standalone to OS Server

The workstation must have disk space for clients.

1. **Choose the Standalone system type during installation.**

2. **Use the OS server worksheets for partitioning.**

3. **Add the (still Standalone) workstation to the NIS+ network:**

Configuring a NIS+ Client	*page 97*

▼ 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 in as a user who can assume the `root` role, and assume it.**

Role - root
Label - admin_low
Profile shell

Either:

♦ **Follow the procedure "Create an Install Server" on page 114.**
This will copy the Trusted Solaris CD image to one of the OS server's hard disks.

Or:

Role - root
Label - admin_low
Action - Set Mount Points

♦ **Mount a Trusted Solaris CD image that has been copied to an install server:**

a. Add the file systems to be mounted to the file `/etc/vfstab`**.**
For example,

```
heron:/export/install/ts2.5.1_sparc - /export/install/ts2.5.1_sparc nfs - yes bg,intr,soft
```

Role - admin
Label - admin_low
Profile shell

b. Create a mount points for the file system to be mounted.

```
# mkdir -p /export/install/ts2.5.1_sparc
```

c. Mount the file system.

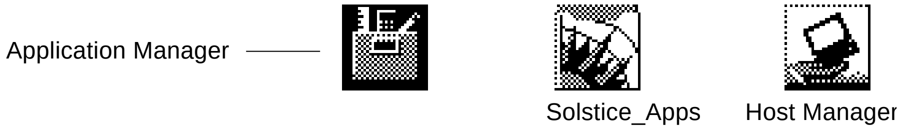
```
# mount /export/install/ts2.5.1_sparc
```

▼ Add OS Services

1. **On the workstation that is going to be the OS server, log in 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 with the NIS+ Naming Service.**



3. **If there is already an 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 an 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 10-1 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 10-2 Adding OS Services to an OS Server in Host Manager

Entry	Value
Set Media Path	`/export/install/ts2.5.1_sparc`
Software Groups	Per platform, choose what software cluster to run. Note that Core and End User are equivalent.
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 126*

▼ Reboot the OS Server

♦ **Choose Shut Down from the Trusted Path menu, confirm, then boot the server when the prompt appears.**

Configuring Diskless Clients

Each diskless client requires an entry in the Host Manager. Use NIS+ to centrally administer the diskless clients.

▼ 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 with the NIS+ Naming Service.**

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 10-3 Diskless Client Information in Host Manager

Entry	Value
Host Name	
IP Address	
Ethernet Address	
System Type	Diskless
Timezone Region	
Timezone	

Table 10-3 Diskless Client Information in Host Manager

File Server	*(OS server is already 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 in to the NIS+ master as a user who can assume the role `root` and assume it.**

Role - root
Label - admin_low
Profile shell

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
Profile shell

3. **If the client is in the `tnrhdb` file correctly, but is not in the kernel cache, update the kernel.**

```
# cd /etc/security/tsol
# tnctl -T tnrhtp
# tnctl -H tnrhdb
```

Role - root
Label - admin_low
Profile shell

a. **Then check the kernel cache and run the command `nistntime`.**

```
# tninfo -h
# /usr/lib/nis/nistntime tnrhtp
# /usr/lib/nis/nistntime tnrhdb
```

4. **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 Mounts

1. **On the OS server, log on as a user who can assume the `root` role, and assume it.**

Role - root
Label - admin_low
Action - 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 an `/opt` entry in the `vfstab` file.**
   The `/opt` mount point enables the client to run Solstice AdminSuite. You can add other mount points as well.

   For example,

```
<server>:/export/opt - /export/opt 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
Profile shell

5. **Create the mount points in the client's root directory.**

```
# cd /export/root/clientname
# mkdir -p export/opt
# mkdir -p export/tools
```

▼ Verify Each Client's tnrhdb Entries

1. **On the OS server, log on as a user who can assume the root role, and assume it.**

Role - root
Label - admin_low
Action - Admin Editor

2. **Open the Admin Editor from the System_Admin folder, with the file** `/export/root/clientname/etc/security/tsol/tnrhdb`**.**
   You will do this once per client.

3. **Correct any entries in the file that are not in the following format:**

```
ip_address:template
nnn.nnn.nnn.nnn:template
```

   For example, the following is a correctly formatted sample entry:

```
129.150.129.7:tsol
```

Booting Diskless Clients

When booting for the first time, provide the client with 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… 11

Books in the Trusted Solaris document set and other reference books for setting up workstations are briefly described in “Related Books” on page xxi of this book. For a complete description of the Trusted Solaris 2.5.1 document set, refer to the *Trusted Solaris Documentation Roadmap*. The following table lists where to find information after installing and configuring your workstations.

Table 11-1 Where to Go for Configuration and Administration Tasks

Information Needed	**Title of Guide**	**Part Number**
Configuring printing	*System Administration Guide, Volume II Solaris 2.5* *Trusted Solaris Administrator's Procedures*	802-2003-10 805-8025-10
Setting up user accounts	*Trusted Solaris Administrator's Procedures*	805-8025-10
Setting up mail accounts	*Trusted Solaris Administrator's Procedures*	805-8025-10
Installing software	*System Administration Guide, Volume I Solaris 2.5* *Trusted Solaris Administrator's Procedures*	802-2002-10 805-8025-10
Boot files	*System Administration Guide, Volume I*	802-2002-10
Adding workstations to a network	*Trusted Solaris Administrator's Procedures*	805-8025-10
Accessing remote files and workstations	*System Administration Guide, Volume II* *Trusted Solaris Administrator's Procedures*	802-2002-10 805-8025-10

Table 11-1 Where to Go for Configuration and Administration Tasks

Information Needed	**Title of Guide**	**Part Number**
Administering file systems	*System Administration Guide, Volume I* *Trusted Solaris Administrator's Procedures*	802-2002-10 805-8025-10
Setting up system security	*Trusted Solaris Administrator's Procedures* *System Administration Guide, Volume II*	805-8025-10 802-2003-10
Setting up printers	*System Administration Guide, Volume II* *Trusted Solaris Administrator's Procedures*	802-2003-10 805-8025-10
Increasing 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* *Trusted Solaris Administrator's Procedures*	802-2003-10 805-8025-10
Examining and changing security information	*Trusted Solaris Administrator's Procedures*	805-8025-10
Using crontabs	*System Administration Guide, Volume II* *Trusted Solaris Administrator's Procedures*	802-2003-10 805-8025-10
Adding and maintaining peripherals	*Trusted Solaris Administrator's Procedures*	805-8025-10
Accessing devices	*Trusted Solaris Administrator's Procedures*	805-8025-10
Setting up disks	*System Administration Guide, Volume II*	802-2003-10
Using system administration tools	*Trusted Solaris Administrator's Procedures* *Solstice AdminSuite 2.3 User's Guide*	805-8025-10 802-5363-10
Customizing CDE	*Solaris Common Desktop Environment: Advanced User's and System Administrator's Guide*	order 48952 from Addison-Wesley

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 ADMIN_LOW and ADMIN_HIGH labels will viewable by ordinary users
- Which user clearances will be assigned to individuals
- Which devices (if any) will be allocatable by which normal users
- Which label ranges are defined for machines, printers, and other devices
- Whether the Trusted Solaris system will be used in an evaluated configuration or in an extended configuration.

Computer Security Recommendations

The following list of guidelines provides some things to consider when developing a security policy for your site.

- The maximum label of the Trusted Solaris distributed system (the highest label in the user accreditation range) should not be greater than the maximum security level of work being done at the site.
- System reboots, power failures, and shutdowns should all be recorded manually in a site log.
- File-system damage should be documented and all affected files should be analyzed for potential security-policy violations.
- Operating manuals and administrator documentation should be restricted to individuals with a valid need for access to that information.
- Unusual or unexpected behavior of any Trusted Solaris software should be reported and documented, and the cause should be determined.
- If possible, at least two individuals should administer Trusted Solaris. One should be assigned security administrator authorization for security-related decisions, and the other should be assigned the system administrator authorization for computer management tasks.
- A regular backup routine should be established.
- Authorizations should be assigned only to users who need them and who can be trusted to use them properly.
- Privileges should be assigned to programs only when the program needs the privileges to do its work, and only when the programs have been scrutinized and proven to be trustworthy in their use of privilege. Review the privileges on existing Trusted Solaris programs for a guide to setting privileges on new programs.
- Audit information should be reviewed and analyzed regularly. Any irregular events should be noted and investigated to determine the cause of the event.
- The number of administration IDs should be minimized. The install user account should be disabled after an authorized security administrator user is established.
- The number of set user ID and set group ID programs should be minimized. Setuid/setgid programs should be employed only in protected subsystems.

- An administrator should regularly verify that normal users have a valid login shell.
- An administrator should regularly verify that normal users have valid user ID values and not system administration ID values.
- Consider TEMPEST shielded equipment and fiber-optic network cables to reduce electronic radiation emitted from computer equipment.
- Only certified technicians should open and close TEMPEST equipment to ensure its ability to shield electromagnetic radiation.

Physical Security Recommendations

- Restrict access to the Trusted Solaris system. The most secure locations are generally interior rooms that are not on the ground floor.
- Monitor and document access to Trusted Solaris.
- Secure computer equipment to large objects such as tables and desks to prevent theft. When equipment is secured to a wooden item, increase the strength of the item by adding metal plates.
- Consider removable storage media for sensitive information. Lock up all removable media when not in use.
- Store system backups and archives in a secure location separate from the location of the Trusted Solaris system.
- Restrict physical access to the backup and archival media in the same manner as access to the Trusted Solaris system.
- Install a high-temperature alarm in the computer facility to indicate when the temperature is outside of the range of the manufacturer's specifications. A suggested range is 10°C to 32°C (50°F to 90°F).
- Install a water alarm in the computer facility to indicate water on the floor, in the subfloor cavity, and in the ceiling.
- Install a smoke alarm to indicate fire.
- Install a fire-suppression system.
- Install a humidity alarm to indicate too much or too little humidity.
- Consider TEMPEST shielding if machines do not have it. TEMPEST shielding may be appropriate for facility walls, floors, and ceilings.

- Check for physical gaps that allow entrance to the facility or the rooms containing computer equipment. Look for openings under raised floors, in suspended ceilings, in roof ventilation equipment, and in adjoining walls between original and secondary additions.
- Prohibit eating, drinking, and smoking in computer facilities or near computer equipment. Establish areas where these activities can occur without threat to the computer equipment.
- Protect architectural drawings and diagrams of the computer facility.
- Restrict the use of building diagrams, floor maps, and photographs of the computer facility.

Personnel Security Recommendations

- Inspect packages, documents, and storage media entering and leaving a secure site.
- Require identification badges on all personnel and visitors at all times.
- Use identification badges that are difficult to copy or counterfeit.
- Establish areas that are prohibited for visitors and clearly mark the areas.
- Escort visitors at all times.

Common Security Violations

Because no computer is 100% secure, a computer facility is only as secure as the people who use it. The limitations of an administrator are directly related to the actions of all individuals involved with the use of computer equipment and its facilities. Although most actions that violate security are easily resolved by careful users or additional equipment, the following list gives examples of problems that can occur:

- Users give passwords to other individuals who should not have access to the computer system.
- Users write down passwords and lose or leave the passwords in nonsecure locations.
- Users set their passwords to easily guessed words or names.
- Users learn passwords by watching other users when they enter a password.

- Unauthorized users remove, replace, or physically tamper with hardware.
- Users leave their workstations or terminals unattended without locking the screen.
- Users change the permissions on a file to allow other users to read the file.
- Users change the labels on a file to allow other users to read the file.
- Users discard sensitive hardcopy documents without shredding them or leave sensitive hardcopy documents in insecure locations.
- Users leave access doors unlocked.
- Users lose their keys.
- Users do not lock up removable storage media.
- Computer screens are visible through exterior windows.
- Network cables are tapped.
- Electronic eavesdropping captures signals emitted from computer equipment.
- Power outages, surges, and spikes destroy data.
- Earthquakes, floods, tornadoes, hurricanes, and lightning destroy data.
- External electromagnetic radiation interference such as sun-spot activity scrambles files.

Additional Security References

As a trusted administrator, you should become familiar with the standards established by various government agencies. Government publications describe in detail the standards, policies, methods, and terminology associated with computer security.

Other publications listed here are guides for system administrators of UNIX systems and are useful in gaining a thorough understanding of UNIX security problems and solutions. Some publications listed here describe successful attempts to penetrate computer systems around the world and illustrate real threats to computer security. These publications emphasize the importance of computer systems managed by knowledgeable and capable administrators.

U.S. Government Publications

Computer Security Requirements, Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments, DoD, CSC-STD-003-85, 1985.

Department of Defense Password Management Guideline, DoD, CSC-STD-002-85, 1985.

Department of Defense Trusted Computer System Evaluation Criteria (TCSEC) National Computer Security Center, DoD 520.28-STD, 1985.

Graubart, Richard D., J.L. Berger, and John P.L. Woodward, *Compartmented Mode Workstations Evaluation Criteria, Version 1*, DIA DDS-2600-6243-91, Mitre, Bedford, Massachusetts, March 1991.

Personal Computer Security Considerations, National Computer Security Center, NCSC-WA-002-85, 1985.

Technical Rationale behind CSC-STD-003-85 Computer Security Requirements, Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments, DoD, CSC-STD-004-85, 1985.

Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria, National Computer Security Center, NCSC-TG-005 Version 1, 1987.

Woodward, John P.L., *Security Requirements for System High and Compartmented Mode Workstations*, DIA DDS-2600-5502-87, Mitre, Bedford, Massachusetts, November 1987.

UNIX Security Publications

Farrow, Rik, *UNIX System Security*, Addison-Wesley, Reading, MA, 1991.

Garfinkel, Simson, and Gene Spafford, *Practical UNIX Security*, O'Reilly & Associates, Inc., Sebastopol, CA, 1991.

Hayes, Frank, "Is Your System Safe?" *UNIXWORLD*, June 1990.

Wood, Patrick H., and Stephen Kochan, *UNIX System Security*, Hayden Books, Indianapolis, IN, 1986.

General Computer Security Publications

Denning, Peter J., *Computers under Attack: Intruders, Worms and Viruses*, ACM Press, Addison-Wesley, Reading, MA, 1990.

Farrow, Rik, "Inside the Internet Worm," *UNIXWORLD*, June 1990.

Hafner, Katie, and John Markroff, *Cyberpunk: Outlaws and Hackers on the Computer Frontier*, Simon & Schuster, New York, NY, 1991.

Levy, Steven, *Hackers: Heroes of the Computer Revolution*, Dell Books, New York, NY, 1984.

McAffe, John, and C. Haynes, *Computer Viruses, Worms, Data Diddlers, Killer Programs, and Other Threats to Your System*, St. Martin's Press, New York, NY, 1989.

Page, Bob, "A Report on the Internet Worm," University of Lowell, Computer Science Department, November 1988.

Russell, Deborah, and G.T. Gangemi, Sr., *Computer Security Basics*, O'Reilly & Associates, Inc., Sebastopol, CA, 1990.

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		
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	**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		

♦ ***See the "NIS+ Root Master's Disk Partition Tables" on page 210 for planning the disk partitions.**

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 251.**
- **Go to “Disk Partition Tables” on page 225 and following for more disk partitioning blanks.**
- **See “Common Disk Sizes and Amount Available for Partitions” on page 224 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_____	**Boot-time network db entry**	
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	*(Needed for network installattion)*	
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		

Need help?

- **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 224 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_____	**Boot-time network db entry**	
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		

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		
Primary network interface	Interfaces of workstation.	
Name service	NIS+ | None	**NIS+**
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		

Need help?

- **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 224 for planning and entering disk partitioning.**

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_____	**Boot-time network db entry**
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**

Remote Hosts Worksheet - Local `tnrhdb` *Entries*

System Administrator Information	Security Officer Information
Workstation name	
Remote host	**Template**
IP address	
Host_type	
Use	
Workstation name	
Remote host	**Template**
IP address	
Host_type	
Use	
Workstation name	
Remote host	**Template**
IP address	
Host_type	
Use	
Workstation name	
Remote host	**Template**
IP address	
Host_type	
Use	
Workstation name	
Remote host	**Template**
IP address	
Host_type	
Use	
Workstation name	
Remote host	**Template**
IP address	
Host_type	
Use	

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?	Yes
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
Roles	secadmin | admin | root	secadmin

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?	Yes
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
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	1444
1.3G	1270
1.05G	1002
424MB	404
124MB	99

B

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**		

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 229*	See *Trusted Solaris Label Administration*
□	Network	*Planning the Network* on *page 230*	"Remote Hosts (tnrhdb) Worksheet for NIS+ Root Master" on page 219
			"Services Provided by Each Workstation" on page 218
□	Auditing	*Planning Auditing* on *page 231*	See *Trusted Solaris Audit Administration*
□	Workstations	*Planning Workstations* on *page 232*	"Services Provided by Each Workstation" on page 218
□	First Users		"First User Worksheet" on page 221
			"Second User Worksheet" on page 222
□	Administrative Roles		"Administrative Role Worksheet - secadmin" on page 223
			"Administrative Role Worksheet - admin" on page 223
□	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.

Note – When localizing a label_encodings file, localize the label names only. However, the names ADMIN_HIGH and ADMIN_LOW *must not* be localized. All labeled workstations that you contact must have label names that match the label names in the Trusted Solaris label_encodings file.

	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 209.
	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*

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		

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
SPARCserver 1000	SUNW,SPARCserver-1000	sun4d
SPARCcenter 2000	SUNW,SPARCcenter-2000	sun4d

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
Sun Ultra 2 Sun UltraServer 2	SUNW,Ultra-2	sun4u
Sun Ultra Enterprise	SUNW,Ultra-4	sun4u
Sun Ultra 5	SUNW,Ultra-5	sun4u
Sun Ultra 10	SUNW,Ultra-10	sun4u
Sun Ultra 30	SUNW,Ultra-30	sun4u
Sun Ultra 50	SUNW,Ultra-50	sun4u
Other SPARC systems	See your hardware vendor documentation for platform name information.	

SBus Components

Table D-2 shows the SBus components supported in the Trusted Solaris 2.5.1 release.

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)
SBus FastEthernet Adapter SBus Card (2.0)
Sun FDDI Dual-Attach SBus Interface (4.0)
PCMCIA Interface/SBus Card

PCI Cards

The following table shows the PCI cards supported in the Trusted Solaris 2.5.1 release.

Table D-3 PCI Cards

Component name
SunFDDI/P 1.0 DAS (X1036A)
SunTRI/P 1.0 Token Ring Interface (X1039A)
Sun Quad FastEthernet PCI Adapter (X1034A)
SunFastEthernet PCI Adapter (X1033A)
SunSwift PCI Adapter (X1032A)
Sun GigabitEthernet PCI Adapter (X1044A)
Sun PGX Card (graphics) (X3660A)

Frame Buffers and Graphics Accelerators

The following table shows the frame buffers and graphics cards supported in the Trusted Solaris 2.5.1 release.

Table D-4 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
Monochrome

Input Devices

The following table shows the input devices supported in the Trusted Solaris 2.5.1 release.

Table D-5 Input Devices

Component name
SunButtons: 32 key function I/O device
SunDials: 8-Dial Interactive Graphics I/O device for 3-D

Printers

The following table shows the printers supported in the Trusted Solaris 2.5.1 release.

Table D-6 Printers

Component name
SPARCprinter E Laser Printer
SPARCprinter EC Color Laser Printer
Other laser printers

SunVideo and Multimedia Options

The following table shows the video options supported in the Trusted Solaris 2.5.1 release.

Table D-7 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.

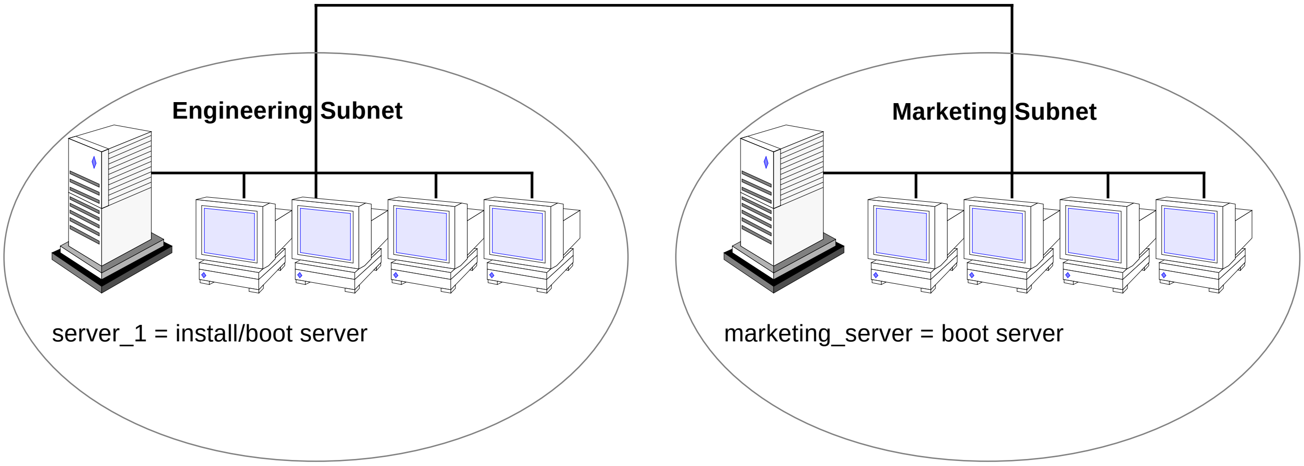

Engineering Subnet
Marketing Subnet
server_1 = install/boot server
marketing_server = boot server

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 2.5.1 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 - root
Label - admin_low
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
Action - Set Mount Points

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 uses the Set Mount Points action in the System_Admin folder to add the following line to the /etc/dfs/dfstab file:

```
share -F nfs -o ro,anon=0 /jumpstart
```

Role - admin
Label - admin_low
Profile shell

Then, at the command line, the administrator uses the unshareall and shareall commands:

```
# unshareall
# shareall
```

3 Create the eng_profile profile.

Role - root
Label - admin_low
Action - Admin Editor

The security 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 - root
Label - admin_low
Action - Admin Editor

An administrator in the role root 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 - secadmin
Label - admin_low
Action - Admin Editor

The security 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 163 for a complete list of keywords you can use in a rules file.

6 Execute the check script.

Role - admin
Label - admin_low
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.

Role - root
Label - admin_low
Profile shell

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 in the role root 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.

Role - root
Label - admin_low
Profile shell

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 in the role root 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.)

Role - root
Label - admin_low
Profile shell

Next, an administrator in the role root 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 install team 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.

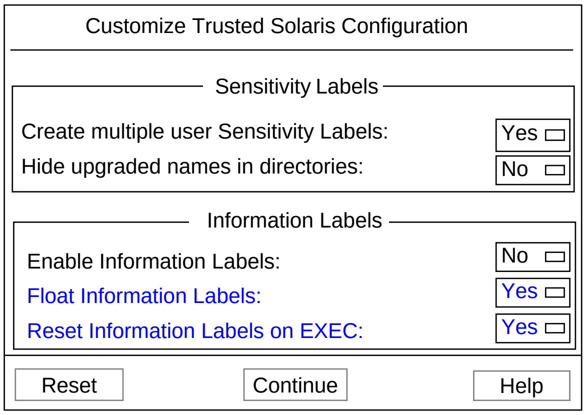
F

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.  Customize Trusted Solaris Configuration Sensitivity Labels Create multiple user Sensitivity Labels: Yes □ Hide upgraded names in directories: No □ Information Labels Enable Information Labels: No □ Float Information Labels: Yes □ Reset Information Labels on EXEC: Yes □ Reset Continue Help
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 268.
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.

Upgrade or Install	Install | Upgrade	Upgrade from Trusted Solaris 2.5 only.
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 251 for the details of the example.
Preserve?	Yes | 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 251 for examples.
Customize?		Customizing requires advanced system administration skills.
Customize Disks		See “Root NIS+ Master Disk Partitioning Example” on page 251 for examples.
Begin installation or upgrade		
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	224		**s3**		
	s4				**s4**		
	s5				**s5**		
	s6	/usr	520		**s6**		410
	s7	/export	10		**s7**	/export/tools	1380

Disk	Slice	Mount point	Size	Disk	Slice	Mount point	Size
c0t3d0	**s0**			c0t5d0	**s0**		
	s1				**s1**		
	s2	entire disk	2028		**s2**	entire disk	1980
	s3	/etc/security/audit/grebe	1014		**s3**	/swapfile	600
	s4				**s4**		
	s5				**s5**		
	s6				**s6**		
	s7	/etc/security/audit/grebe.1	1014		**s7**	/opt	1380

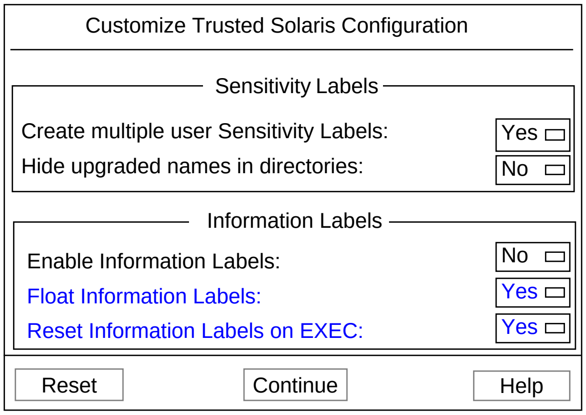
Services Provided by Each Workstation Example

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			

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	NIS+ | None	
Trusted Solaris Configuration	Continue	Select the same the label configuration as the one for the root NIS+ master.  Customize Trusted Solaris Configuration Sensitivity Labels Create multiple user Sensitivity Labels: Yes ▭ Hide upgraded names in directories: No ▭ Information Labels Enable Information Labels: No ▭ Float Information Labels: Yes ▭ Reset Information Labels on EXEC: Yes ▭ Reset Continue Help
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 268.
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.

Upgrade or Install	Install | Upgrade	Upgrade from Trusted Solaris 2.5 only.
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 256 for the details of the example.
Preserve?	Yes | No	
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 256 for the details of the example
Begin installation or upgrade		
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

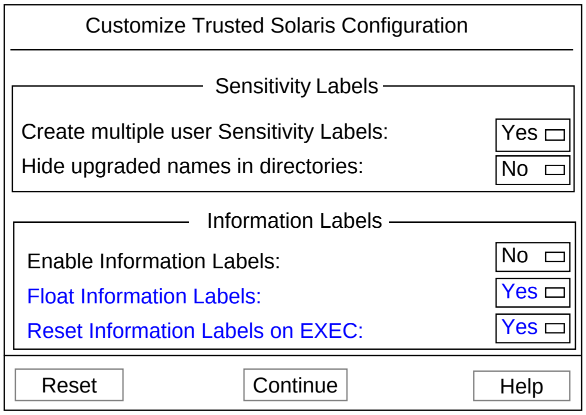
Disk	Slice	Mount point	Size	Disk	Slice	Mount point	Size
c0t3d0	**s0**			c0t5d0	**s0**		
	s1				**s1**		
	s2	entire disk	1980		**s2**	entire disk	1980
	s3	/etc/security/audit/willet.3	990		**s3**	/etc/security/audit/willet	990
	s4				**s4**		
	s5				**s5**		
	s6				**s6**		
	s7	/etc/security/audit/willet.4	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	**Boot-time network db entry**	129.159.110.1:tsol
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	CDROM (sd6) tape drive (st4)		only usable by those whose profile includes `device_allocate`
Remote Printers			
	cirrus		
	cumulus	Administrator printer [admin_high] only	

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	NIS+ | None	
Trusted Solaris Configuration	Continue	Select the same the label configuration as the one for the root NIS+ master.  Customize Trusted Solaris Configuration Sensitivity Labels Create multiple user Sensitivity Labels: Yes Hide upgraded names in directories: No Information Labels Enable Information Labels: No Float Information Labels: Yes Reset Information Labels on EXEC: Yes
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 268.
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.		
Upgrade or Install	Install | Upgrade	Upgrade from Trusted Solaris 2.5 only.
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 260 for the details of the example.
Auto-layout file systems?	Yes	
File systems to auto-layout	`/, /usr, /var, /export`	
Preserve existing data?	Yes | No	
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	**Boot-time network db entry**	129.159.110.1:tsol
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			

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, 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 environment that remain unmodified. Therefore, check the Troubleshooting section of the installation manual for Solaris 2.5.1 when you encounter a problem installing the Trusted Solaris 2.5.1 release.

The following table shows common error messages and the page number where you can find causes and possible solutions.

WARNING: RPC Timed out	*page 266*

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 H

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.

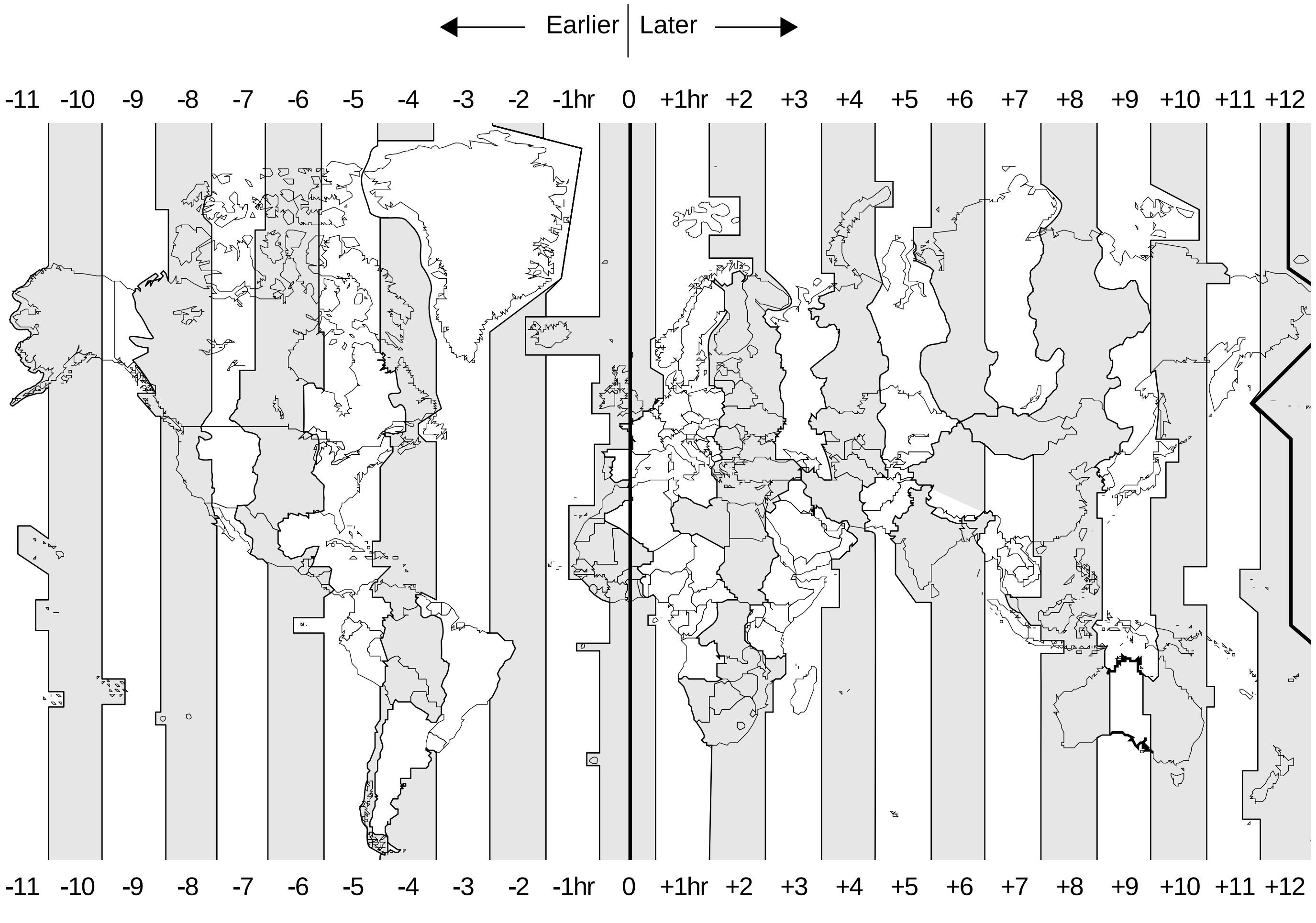


Figure H-1 Greenwich Meantime Map

Glossary I

access control list

One type of *discretionary access control* based on a list of entries that the owner can specify for a file or directory. An access control list (ACL) can restrict or permit access to any number of individuals and groups, allowing finer-grained control than provided by the standard UNIX *permission bits*.

accreditation range

A set of sensitivity labels that are approved for a class of users or resources. See also *workstation accreditation range* and *user accreditation range*.

ACL

See *access control list*.

accreditation range

A set of valid *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. Allocatable devices include tape drives, floppy drives, audio devices, and CDROM devices. See *device allocation*.

allowed privilege set

The allowed set of privileges limits which *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.

application search path

In *CDE*, the search path used by the system to find applications and certain configuration information. The application search path is controlled by a *trusted role*.

AutoClient system

A system type that caches all of its needed system software from an OS server. Because it contains no permanent data, an AutoClient is a field replaceable unit (FRU). It requires a small local disk for swapping and for caching its individual root (`/`) and `/usr` file systems from an OS server. Trusted Solaris 2.5.1 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 2.5.1, the bootparams file contains a keyword=value entry that points the *boot server* to the Trusted Solaris *label configuration* for the workstation. A workstation can have a local bootparams file (`/etc/bootparams`), or it can use the bootparams NIS+ table. See `bootparams(4)`.

boot server

A server that provides boot services to workstations on the same subnet. A boot server is required if you plan to push Trusted Solaris information from a central location to every workstation in the system. If the *install server* is on a different subnet than the workstations that need to install the Trusted Solaris software, you must create a boot server for that subnet.

CDE

See *Common Desktop Environment*.

clearance

The upper bound of the set of labels at which a user may work, whose lower bound is the *minimum label* assigned by the *security administrator*. There are two types of clearance, the session clearance and the *user clearance*.

client

A workstation connected to a network.

closed network

A *closed network* is a network of Trusted Solaris workstations that is cut off from any non-Trusted Solaris workstation. The cutoff can be physical, where there is no wire that extends past the Trusted Solaris network. The cutoff can be in the software, where the Trusted Solaris workstations recognize only Trusted Solaris workstations. Data entry from outside the network is restricted to peripherals attached to Trusted Solaris workstations.

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.

.copy_files

An optional setup file in a multilabel environment. The file contains the names of startup files, such as `.cshrc` or `.netscape`, that the user environment or user applications require in order for the environment or application to behave well. The files referenced in `.copy_files` are then *copied* to the user's home directory at other labels, when those directories are created. See also *.link_files*.

core

A *software group* that contains the minimum software required to boot and run the Solaris operating environment on a system. It includes some networking software and the drivers required to run the OpenWindows environment; it does not include the windowing software. Trusted Solaris 2.5.1 does not offer a core software group, since the Common Desktop Environment is the required administration environment.

core file

A file that contains a picture of the state of a system when it crashed. Also called a core dump.

custom JumpStart installation

A type of installation in which the Trusted Solaris software is automatically installed on a system based on a customized *profile*. You can customize profiles for different types of users.

DAC

See *discretionary access control*.

derived profile

A *profile* that is dynamically created by a *begin script* during a *custom JumpStart installation*.

device

Devices include printers, workstations, tape drives, floppy drives, audio devices, and internal pseudo terminal devices. Devices are subject to the read equal write equal *MAC* policy.

device allocation

A mechanism for protecting the information on an allocatable *device* from access by anybody except the user who allocates the device. Until a device is deallocated, no one but the user who allocated a device can access any information associated with the device. For a user to allocate a device, that user must have been granted the device allocation authorization by the *security administrator*.

developer system support

A software group that contains the End User System Support *software group* plus the libraries, include files, man pages, and programming tools for developing software.

discretionary access control

The type of access granted or denied by the owner of a file or directory at the discretion of the owner. The Trusted Solaris environment provides two kinds of discretionary access controls (DAC): *permission bits* and *access control list*.

disk configuration file

A file that represents a structure of a disk (for example, bytes/sector, flags, slices). Disk configuration files enable you to use `pfinstall` from a single system to test *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.

evaluated configuration

A set of one or more Trusted Solaris workstations which are running in a configuration that has been certified as meeting specific criteria by a certification authority. In the United States, those criteria are the TCSEC and the evaluating and certifying body is the NSA. Internationally, the criteria are the ITSEC. Thee evaluating body for the Trusted Solaris 2.5.1 operating environment is Logica; the certifying authority is UK ITSEC Certification Body.

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.

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 privilege*s). 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 installation*s.

forced privilege set

The forced set of privileges are those placed on a file by the *security administrator*. Any privileges in the forced privilege set are available to any process that invokes the program, as long as they are also in the *allowed privilege set*.

GFI

Government Furnished Information. In this manual, it refers to a U.S. government-provided *label_encodings file*. In order to use a GFI with Trusted Solaris software, you must add the Sun-specific LOCAL DEFINITIONS section to the end of the GFI. *Trusted Solaris Label Administration* explains the procedure in detail.

host name

The name by which a system is known to other systems on a network. This name must be unique among all the systems within a given domain (usually, this means within any single organization). A host name can be any combination of letters, numbers, and minus sign (-), but it cannot begin or end with a minus sign.

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.

I

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 2.5.1 release.

install server

A server that provides the Trusted Solaris installation image for other systems on a network to boot and install from (also known as a *media server*). The Trusted Solaris installation image can reside on the install server's CDROM drive or hard disk.

install team

A team of at least two people who together oversee the installation of a Trusted Solaris workstation. One team member is responsible for security decisions, and the other for system administration decisions.

interactive installation

A type of installation where you have full hands-on interaction with the Trusted Solaris installation program to install the Trusted Solaris software on a system.

IP address

Internet protocol address. A unique number that identifies a networked system so it can communicate via Internet protocols. It consists of four numbers separated by periods. Most often, each part of the IP address is a number between 0 and 225; however, the first number must be less than 224 and the last number cannot be 0.

IP addresses are logically divided into two parts: the network (similar to a telephone area code), and the system on the network (similar to a phone number).

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 2.5.1 release does not offer this option; all JumpStart installations in Trusted Solaris 2.5.1 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 administrator* has configured the user, a user may see the complete *CMW label*, only the *sensitivity label* portion, only the *information label* portion, or no labels at all. See *label_encodings file*.

label configuration

A Trusted Solaris installation choice of: single- or multilabel sensitivity labels; if multilabel, hide or show upgraded file names; 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 administrator* 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*.

.link_files

An optional setup file in a multilabel environment. The file contains the names of startup files, such as `.cshrc` or `.netscape`, that the user environment or user applications require in order for the environment or application to behave well. The files referenced in `.link_files` are then *linkied* to the user's home directory at other labels, when those directories are created. See also *.copy_files*.

locale

A specific language associated with a region or territory.

MAC

See *mandatory access control.*

mandatory access control

Access control based on comparing the *sensitivity label* of a file, directory, or *device* to the *sensitivity label* of the process that is trying to access it. The *MAC* rule write up, read down (WURD) applies when a process at one *sensitivity label* attempts to read or write to a file at another *sensitivity label*. The *MAC* rule write equal, read down applies when a process at one *sensitivity label* attempts to write to a directory at another *sensitivity label*. The *MAC* rule read equal, write equal applies when a process at one *sensitivity label* attempts to write to a *device* at another *sensitivity label.*

media server

See *install server.*

minimum label

The lower bound of a user's sensitivity labels and the lower bound of all users' sensitivity labels. The minimum label set by the *security administrator* when specifying a user's security attributes is the sensitivity label of the first workspace that comes up after the user's first login. The sensitivity label specified in the minimum label field by the *security administrator* in the `label_encodings` file sets the lower bound for all users.

MLD

See *multilevel directory*.

mount

The process of making a remote or local *file system* accessible by executing the `mount` command. To mount a file system, you need a *mount point* on the local system and the name of the file system to be mounted (for example, `/usr`).

mount point

A directory on a system where you can mount a *file system* that exists on the local or a remote system.

multilevel directory

A directory in which information at differing *sensitivity label* is maintained in separate subdirectories called single-level directories (*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 workstations (called hosts) connected through hardware and software, so they can communicate and share information; referred to as a local area network (LAN). One or more servers are usually needed when systems are networked.

NIS+

Network Information Service, Plus. The name service for a Trusted Solaris network. NIS+ provides automatic information updating and adds security features such as authorization and authentication.

NIS+ master

See *root NIS+ master*.

non-networked systems

Workstations that are not connected to a network or do not rely on other workstations.

open network

An *open network* is a network of Trusted Solaris workstations that is connected physically to other networks and that uses Trusted Solaris software to communicate with non-Trusted Solaris workstations.

/opt

A *file system* that contains the mount points for third-party and unbundled software.

OS server

A *system* that provides services to systems on a network. 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`).

outside the evaluated configuration

When software that has been proved to be able satisfy the criteria for an *evaluated configuration*, is configured with settings that do not satisfy security criteria, it is described as being *outside the evaluated configuration*.

package

A functional grouping of files and directories that form a software application. The Trusted Solaris software is divided into four main *software groups*, which are each composed of *clusters* and *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 administrator* after the command itself or the person using it has been judged to be able to use that privilege in a trustworthy manner.

process

An action that executes a command on behalf of the user who invokes the command. A process receives a number of *security 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. The profile shell is the default shell of a *trusted role*.

remote host

A workstation that is not part of the Trusted Solaris NIS+ domain. A remote host can be an *unlabeled workstation* or a *labeled workstation*.

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.

rules.ok file

A generated version of the *rules file*. It is required by the *custom JumpStart installation* software to match a system to a *profile*. You use the `check` script to create the `rules.ok` file.

security administrator

In an organization where sensitive information must be protected, the person or persons who define and enforce the site's *security policy* and who are cleared to access all information being processed at the site. In the Trusted Solaris software environment, an *administrative role* that is assigned to one or more individuals who have the proper *clearance* and whose task is to configure the *security attribute*s of all users and workstations so that the software enforces the site's security policy. In contrast, see *system administrator*.

security attribute

An attribute used in enforcing the Trusted Solaris *security policy*. Various sets of security attributes, both in the base Solaris and the Trusted Solaris environments, are assigned to *process*es, users, files, directories, hosts on the trusted network, allocatable *device*s, and other entities.

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 administrator* 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.

system administrator

In the Trusted Solaris environment, the *trusted role* assigned to the user or users responsible for performing standard system management tasks such as setting up the non-security-relevant portions of user accounts. In contrast, see *security administrator*.

system type

One of several different ways a workstation can be set up to run the Trusted Solaris software. Valid system types are: *standalone system*, *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 administrator*. 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 administrator* 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.

/var

A *file system* or directory (on *standalone systems*) containing system files that are likely to change or grow over the life of the system. These include system logs, `vi` files, mail files, and uucp files.

Volume Management

A program that provides a mechanism to administer and obtain access to the data on CDROMs and diskettes. This program is disabled in the Trusted Solaris 2.5 release.

workstation accreditation range

The set of all valid (well-formed) *label*s created according to the rules defined by each site's *security administrator* in the *label_encodings file*, plus the two administrative *label*s that are used in every Trusted Solaris environment, ADMIN_LOW and ADMIN_HIGH. Also called the *system accreditation range*.

Index