



Trusted Solaris Installation and Configuration

Trusted Solaris 7

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

Part Number 805-8056
November 1999

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

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

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

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

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

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

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

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

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

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

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

L'interface d'utilisation graphique OPEN LOOK et SunTM 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 REPENDRE 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

About This Book 19

1. Overview 25

The Big Picture 25

- ▼ Understand the Trusted Solaris Environment. 26
- ▼ Understand Your Site's Security Policy. 26
- ▼ Devise an Administration Strategy. 27
- ▼ Devise a Label Strategy. 28
- ▼ Plan Workstation Hardware and Capacity. 29
- ▼ Plan Your Network. 30
- ▼ Plan Auditing. 32
- ▼ Devise an Installation and Configuration Strategy. 33
- ▼ Collect Information. 33
- ▼ Back Up the Workstation. 33
- ▼ Install the Trusted Solaris Software. 33
- ▼ Configure the Software. 34

Differences from Solaris 7 Installation and Configuration 35

Installation Results from an Administrator's Perspective 35

2. Basic Procedures 37

How to Log In 37

- ▼ To Log In as the User Install 37
- ▼ To Log In as a Regular User 38
- How to Assume a Role 39
- ▼ To Assume a Role 39
- How to Launch a Terminal 40
- ▼ To Launch a Terminal 40
- How to Open a Profile Shell 41
- ▼ To Open a Profile Shell in an Administrative Role 41
- ▼ To Open a Profile Shell as a User or Non-Administrative Role 41
- ▼ To List the Commands Available to a Profile Shell 41
- ▼ To See Process and Privilege Information in a Profile Shell 42
- How to Create an Admin_High Workspace 42
- How to Protect Machine Hardware 43
- ▼ To Set the PROM Mode and Password 43
- ▼ To Protect the BIOS 44
- How to Limit Contact During Booting 44
- How to Copy Files To and From a Portable Medium 44
- ▼ To Copy One or More Files to a Diskette 45
- ▼ To Copy One or More Files from a Diskette 46
- How To Install a Site-Specific Label Encodings File 47
- How to Allocate and Deallocate a Device 48
- ▼ To Allocate a Device 48
- ▼ To Deallocate a Device 49
- How to Open the Application Manager 50
- ▼ To Open the Application Manager 50
- How to Use the Solstice_Apps Folder 50
- ▼ To Open and Modify a Solstice_Apps Database 51
- ▼ To Modify the Password for a Role or User Account 52

▼ To Customize Idle Time	54
▼ To Delete a Local User	54
How to Use the System_Admin Folder	55
▼ To Run a System_Admin Action	57
How to Add Network Interfaces	58
▼ To Determine the Network Interfaces	58
▼ To Create the Network Interface Files	60
How to Share a File System	61
▼ To Share Home Directories and Other Filesystems	61
▼ To Check That a Directory Is Shared	62
▼ To Start the nfs.server Daemon	62
How to Set the Label on an Unlabeled File System	63
How to Mount a File System	64
▼ To Mount a Labeled or Unlabeled File System	64
How to Update the Commands in a Role's Profile	65
▼ To Add a Command to a Role's Profile	65
▼ To Verify That a Command is in a Role's Profile	66
▼ To Remove a Command from a Role's Profile	66
How to End a Session	67
▼ To Lock the Screen	67
▼ To Log Out	67
▼ To Reboot the Workstation	67
3. Installing a Workstation	69
Who Does What	69
System Installation Step by Step	70
▼ IA: Boot from Diskette and Install	70
▼ SPARC: If Solaris workstation is <i>off</i> :	70
▼ SPARC: If Solaris workstation is <i>on</i> :	70

- ▼ SPARC: If Trusted Solaris workstation is *on*: 71
- ▼ Install from a CDROM 71
- ▼ Install over the Network 72
- ▼ Read Booting Messages 72
- ▼ Answer Installation Questions 73
- ▼ Read the Log 75
- ▼ Enter a root Password 76
- Troubleshooting 77
- ▼ Complete OS Server Installation 77
- ▼ Complete Network and JumpStart Installations 77
- 4. Configuring a Workstation without the NIS+ Name Service 79**
 - Who Does What 79
 - Non-Networked Configuration Tasks 79
 - ▼ Log In and Assume the root Role 80
 - ▼ Protect the Workstation 80
 - ▼ Check and Install the label_encodings File 80
 - ▼ Set Up Network Files 81
 - ▼ Add Administrative Roles to Three /etc Files 82
 - ▼ Reboot the Workstation 83
 - ▼ Update Role Passwords 84
 - ▼ Add Users to Administer the System 84
 - ▼ Verify That Users and Administrative Roles Work 85
 - ▼ Mount Unlabeled File Systems 85
 - ▼ Share File Systems 85
 - ▼ Delete the User install 85
- 5. Configuring the NIS+ Root Master 87**
 - Who Does What 87
 - NIS+ Root Master Configuration Tasks 87

▼	Log In and Launch a Terminal	88
▼	Protect the Workstation	89
▼	Check and Install the label_encodings File	89
▼	Set Up Routing	90
▼	Set Up Additional Network Interfaces	92
▼	Add the Static Routing Workstations to the Local Hosts Database	92
▼	Edit the Trusted Network Files	93
▼	Set Up the NIS+ Domain	95
▼	Set Up DNS	100
▼	Reboot the Workstation	101
▼	Update Role Credentials and Passwords	101
▼	Set Up Home Directories	101
▼	Add Users to be Administrators	102
▼	Log Out	105
▼	Verify that Users and Administrative Roles Work	105
▼	Set Up Auditing	106
▼	Set the Label for Unlabeled File Systems (Example)	106
▼	Share File Systems	107
▼	Copy Configuration Files for Distribution to Clients	107
▼	Delete the User install	109
6.	Configuring a NIS+ Client	111
	Who Does What	111
	NIS+ Client Configuration Tasks	111
▼	Log In and Protect the Workstation	112
▼	Copy Configuration Files from the NIS+ Master	112
▼	Copy the NIS+ Master label_encodings File	113
▼	Set Up Static Routing	113
▼	Set Up Secondary Network Interfaces	115

▼	Copy the Tnrhttp Database (Example)	115
▼	Edit the Tnrhdb Database	116
▼	Verify Communication with the NIS+ Master	116
▼	Set Up the NIS+ Name Service	117
▼	Set Up DNS and the Name Service Switch	118
▼	Set Up Home Directories	118
▼	Reboot the Workstation	118
▼	Add Users	119
▼	Finish Configuring the Workstation	119
7.	Preparing to Install Trusted Solaris Over a Network	121
	Servers Required for Network Installation	121
	Setting up Network Installation	122
	Commands You Should Know About	123
▼	Create an Install Server	124
▼	Set the Default Date and Time	125
▼	Add Client Information for a Network Install	126
▼	Check Client Information	131
▼	Create a Boot Server on a Subnet	131
▼	Reboot the Install Server	133
8.	Preparing Custom JumpStart Installations	135
	Definition: Custom JumpStart Installation	135
	Reasons to Choose a Custom JumpStart Installation	136
	Trusted Solaris Differences in Custom JumpStart	136
	Trusted Solaris Custom JumpStart Additions	136
	Trusted Solaris Custom JumpStart Limitations	137
	Prerequisites for a Custom JumpStart Installation	137
	Tasks to Set up Custom JumpStart Installations	137
	What Happens During a Custom JumpStart Installation	139

Networked Custom JumpStart Installation	140
Creating a JumpStart Directory on a Diskette	141
▼ How to Create a JumpStart Directory on a Diskette	141
Creating a JumpStart Directory on a Server	144
▼ How to Create a JumpStart Directory on a Server	144
Enabling Access to the JumpStart Directory	146
▼ How to Enable Access to the JumpStart Directory	146
▼ How to Check Access to the JumpStart Directory	148
Creating a Profile	149
Requirements for Profiles	149
Recommendations for Trusted Solaris Profiles	149
▼ How to Create a Profile	149
Profile Examples	150
Profile Keyword and Profile Value Descriptions	152
How the Size of Swap Is Determined	159
Creating the rules File	160
When Does a System Match a Rule	160
Recommendations for Trusted Solaris Rules	161
▼ How to Create the rules File	161
Rule Examples	163
Important Information About the <code>rules</code> File	164
Rule Keyword and Rule Value Descriptions	165
How the Installation Program Sets the Value of <code>rootdisk</code>	170
Using <code>check</code> to Validate the rules File	171
▼ How to Use <code>check</code> to Validate the rules File	172
Finishing Custom JumpStart	173
▼ Copy JumpStart Files to <code>jumpstart_dir_path</code>	173
▼ Check That All Installation Questions Can Be Answered	174

9.	Using Optional Custom JumpStart Features	177
	Creating Begin Scripts	177
	Important Information About Begin Scripts	178
	Ideas for Begin Scripts	178
	Creating Derived Profiles With Begin Scripts	178
	Creating Finish Scripts	179
	Important Information About Finish Scripts	179
	Ideas for Finish Scripts	179
	▼ Rebooting the Workstation with a Finish Script	180
	Adding Files With Finish Scripts	180
	▼ Create a Finish Script to Add Files after Installation	180
	Customizing the Root Environment	181
	Setting the System's Root Password With Finish Scripts	181
	▼ Create a Finish Script to Set the root Password	182
	Using pfinstall to Test Profiles	183
	Ways to Use pfinstall	183
	▼ How to Use pfinstall to Test a Profile	183
	pfinstall Examples	185
	▼ How to Create a Disk Configuration File for a SPARC System	186
	▼ How to Create a Multiple Disk Configuration File for a SPARC System	188
	IA: Creating a Disk Configuration File on Intel Architecture	190
	▼ How to Create a Disk Configuration File on Intel Architecture	190
	▼ How to Create a Multiple Disk Configuration File on Intel Architecture	194
	Using a Site-Specific Installation Program	198
10.	Configuring Diskless Clients	199
	Prerequisites for Diskless Clients	199
	▼ Install and Configure an OS Server	199
	▼ Access a Trusted Solaris CD Image on a File System	200

▼	Add OS Services	201
▼	Create a Boot Server	203
▼	Reboot the OS Server	203
	Configuring Diskless Clients	203
▼	Add Diskless Clients	203
▼	Ensure that the Client is Known to the NIS+ Master	204
▼	Set up Each Client's Mounts	205
▼	Verify Each Client's tnrdhdb Entries	206
▼	Boot a Diskless Client	206
11.	Where to Find...	209
	For Further Configuration	209
A.	Site Security Policy	211
	Site Security Policy and the Distributed System	212
	Computer Security Recommendations	212
	Physical Security Recommendations	213
	Personnel Security Recommendations	214
	Common Security Violations	215
	Additional Security References	215
	U.S. Government Publications	216
	UNIX Security Publications	216
	General Computer Security Publications	217
	General UNIX Publications	217
B.	Checklists for Configuring and Installing Trusted Solaris	219
	Site Summary Checklist	219
	Background Checklist	219
	Checklist Summaries	219
	Planning Labels	220
	Label Decisions	220

Planning the Network	221
Open Network Security Information	221
NIS+ Domain Information	221
Labels of Communicating Machines	222
Planning Auditing	222
Auditing Security Information	222
Auditing System Information	222
Planning Workstations	223
System Information for Each Machine	223
Security Information for Each Machine	223
C. Sample Custom JumpStart Installation	225
Sample Site Setup	225
▼ Create a JumpStart directory.	226
▼ Share the JumpStart directory.	226
▼ Create the eng_profile profile.	226
▼ Create the marketing_profile profile.	227
▼ Edit the rules file.	227
▼ Execute the check script.	228
▼ Set up the engineering systems for installation.	228
▼ Set up the marketing systems for installation.	229
▼ Boot the systems and install Trusted Solaris software.	230
D. Example Worksheets	231
How to Use the Examples	231
Root NIS+ Master Installation Program Example	231
Root NIS+ Master Disk Partitioning Example	233
Services Provided by Each Workstation Example	234
Standalone Workstation Installation Program Example - Audit Server	235

Standalone Disk Partitioning Example - Audit Server	237
Standalone Workstation Configuration Worksheet - Audit Server	238
OS Server Installation Program Example	239
OS Server Disk Partitioning Example	241
OS Server Configuration Worksheet	242
Remote Hosts Worksheet - Example	244
Remote Hosts (tnrhdb) Worksheet for NIS+ Root Master - Example	244
Remote Hosts (tnrhdb) Worksheet for Individual Workstations - Example	245
User Worksheet Example	246
Glossary	249
Index	265

Tables

TABLE P-1	Typographic Conventions	23
TABLE P-2	Shell Prompts	24
TABLE 1-1	Possible Servers in a Trusted Solaris Environment	30
TABLE 1-2	Templates Provided with Trusted Solaris Network Software	31
TABLE 5-1	User Account Characteristics	103
TABLE 6-1	Client Static Routing Entry	113
TABLE 7-1	Adding Host Information in Host Manager	127
TABLE 8-1	Tasks to Prepare for Custom JumpStart Installations	138
TABLE 8-2	How the Maximum Size of Swap Is Determined	159
TABLE 8-3	How the Trusted Solaris Installation Program Sets rootdisk	170
TABLE 10-1	Adding an OS Server to Host Manager	201
TABLE 10-2	Adding OS Services to an OS Server in Host Manager	202
TABLE 10-3	Diskless Client Information in Host Manager	203

Figures

Figure 1–1	Two Roles Administering a Workstation	34
Figure 2–1	The Enable Logins Dialog	38
Figure 2–2	Databases Managed by the Database Manager in Solstice_Apps	51
Figure 2–3	Load Window for Naming Service	52
Figure 8–1	What Happens During a Custom JumpStart Installation	139
Figure 8–2	How a Custom JumpStart Installation Works: Non-Networked Example	140
Figure C–1	Sample Site Setup	225

About This Book

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

Implement Trusted Solaris in Accordance with Site Security

Successfully installing and configuring Trusted Solaris consistent with site security requires understanding the security features of Trusted Solaris and your site security policy. Before attempting to install Trusted Solaris, read Chapter 1 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 33 describes the methods.

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, such as the *Solaris 7 Sun Hardware Platform Guide*.

Planning a Secure Installation

Chapter 1

Common Installation and Configuration Procedures

Chapter 2

Installing Trusted Solaris

Chapter 3

Configuring the NIS+ Root Master

Chapter 5

Configuring a Non-Networked Workstation

Chapter 4

Configuring NIS+ Clients

Chapter 6

Installing NIS+ Clients Over the Network

Chapter 6, Chapter 3, and Chapter 7

Installing and Configuring NIS+ Clients Using Custom JumpStart

Chapter 8, Chapter 9, and Chapter 3

Configuring and Booting Diskless Clients

Chapter 10

Related Books

The following books contain information useful when installing Trusted Solaris software. The Solaris 7 AnswerBook CD and the Trusted Solaris 7 AnswerBook CD are shipped with the product. Solaris 7 books can be accessed from the Solaris 7 AnswerBook CD.

Books from Sun Microsystems

- *Trusted Solaris 7 Release Notes* — Describes late-breaking news about installing Trusted Solaris software, including known problems.
 - *Solaris Advanced Installation Guide*, 805-3408-10 — Describes interactive installations: network, JumpStart, and custom JumpStart. Contains background information for networked installation.
 - *Solaris 7 Sun Hardware Platform Guide*, 805-4456-10 — Describes hardware supported in the Solaris and Trusted Solaris environments.
 - *Solaris Installation Library*, 805-3643-10 and *Solaris Installation Library*, 805-3644-10 — Describe new features in the Solaris environment, and includes how to install an AnswerBook2 server for the Solaris environment. See *Trusted Solaris Documentation Roadmap* for additional AnswerBook2 server setup required for the Trusted Solaris environment.
 - *Solaris Transition Guide*, 805-3864-10 — 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 7* 805-3728-10 — Describes basic administrative tasks in Solaris 7, such as creating and mounting file systems.
- *System Administration Guide, Volume II: Solaris 7* 805-3728-10 — Describes more advanced administrative tasks in Solaris 7, such as print management.

- *Solstice AdminSuite 2.3 Administration Guide*, 805-3026-10 — Describes the basic applications that Trusted Solaris uses to administer the network. Trusted Solaris has modified the applications; the modifications are described in *Trusted Solaris Administrator's Procedures*.
- "Planning Your Network" in *TCP/IP and Data Communications Administration Guide*, 805-4003-10 — Describes how to set up a network. Required for networked sites only.
- *NFS Administration Guide*, 805-3479-10 — Describes how to administer a networked file system. Recommended for a network installation.
- *Solaris Naming Administration Guide*, 806-1391-10 — Describes how to administer a NIS+ network. Required for networked sites.
- *Solaris Naming Setup and Configuration Guide*, 806-1391-10 — Describes how to set up and configure a NIS+ domain. Required for networked sites.
- *Trusted Solaris Administrator's Procedures* — Describes administration tasks in the Trusted Solaris environment 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.
- *Automating Solaris® Installations: A Custom JumpStart™ Guide.*
By Paul Anthony Kasper and Alan L. McClellan, published by Prentice Hall (SunSoft Press), 1995. Describes how to set up "hands-off" network installations. ISBN 0-13-312505-X

Ordering Sun Documents

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

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

Accessing Sun Documentation Online

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

What Typographic Conventions Mean

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

TABLE P-1 Typographic Conventions

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

TABLE P-1 Typographic Conventions *(continued)*

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

Shell Prompts in Command Examples

The following table shows the default system prompt for the C shell, Bourne shell, and Korn shell, and the prompts for administrative roles.

TABLE P-2 Shell Prompts

Shell	Prompt
C shell prompt	<code>machine_name%</code>
secadmin and admin role prompt	<code>\$</code>
Bourne shell and Korn shell prompt	<code>\$</code>
root role prompt	<code>#</code>

Overview

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

- “The Big Picture” on page 25 — For administrators of the Trusted Solaris operating environment.
- “Differences from Solaris 7 Installation and Configuration” on page 35 — For experienced Solaris administrators. Addresses specific differences from the Solaris operating environment.
- “Installation Results from an Administrator's Perspective” on page 35 — Describes the security features in effect after a workstation is installed.

See Appendix B for a checklist of Trusted Solaris 7 configuration tasks. Customers interested in localizing their site, see “For International Customers” on page 28. Customers interested in running an evaluated configuration, see “Understand Your Site's Security Policy.” on page 26.

The Big Picture

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

- “Understand the Trusted Solaris Environment.” on page 26
- “Devise an Administration Strategy.” on page 27
- “Devise a Label Strategy.” on page 28
- “Plan Workstation Hardware and Capacity.” on page 29

- “Plan Your Network.” on page 30
- “Plan Auditing.” on page 32
- “Devise an Installation and Configuration Strategy.” on page 33
- “Collect Information.” on page 33
- “Back Up the Workstation.” on page 33
- “Install the Trusted Solaris Software.” on page 33
- “Configure the Software.” on page 34

▼ 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*.

▼ Understand Your Site’s Security Policy.

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

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

- Select NIS+ as the naming service.

- Select multiple-label environment operation for the FB1 level. The FC2 level permits single- or multiple-label operation.

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

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

▼ Devise an Administration Strategy.

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.

▼ 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 *Trusted Solaris Label Administration*. You can also refer to *Compartmented Mode Workstation Labeling: Encodings Format*.

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

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

After installation, you can make the following label configuration display changes using 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.

▼ Plan Workstation Hardware and Capacity.

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

Consult the *Solaris 7 Sun Hardware Platform Guide* for a list of hardware that supports the Trusted Solaris environment. Any exceptions are noted in *Trusted Solaris 7 Release Notes*.

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

- 32 MB minimum memory
- Local CDROM 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 (for Intel Architecture: BIOS protection)
- What devices may be attached to the workstation
- Which users may use the workstation
- Which printers at what labels may the workstation access

▼ Plan Your Network.

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

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

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

TABLE 1-1 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 1-1 Possible Servers in a Trusted Solaris Environment *(continued)*

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 *Solaris 7 System Administrator Collection* including:

- *Mail Administration Guide*
- *Solaris Naming Setup and Configuration Guide*
- *System Administration Guide, Volume I*
- *System Administration Guide, Volume II*

OS servers are covered in the *Solstice AdminSuite 2.3 Administration Guide*, and Trusted Solaris-specific administration is covered in *Trusted Solaris Administrator's Procedures*.

Additional Planning for Open Networks

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

TABLE 1-2 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		

TABLE 1-2 Templates Provided with Trusted Solaris Network Software *(continued)*

Host Type	Template Name	Purpose
Trusted Solaris 2.5.1 (sun_tsol)	tsol	For Trusted Solaris 2.5.1 hosts or networks
	tsol_1	For TS2.5.1 and 7 hosts or networks that label packets with the RIPS0 security option
	tsol_2	For TS2.5.1 and 7 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
RIPS0	ripso	For hosts or networks that send RIPS0 packets

The `tnrhttp(4)` 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*.

▼ Plan Auditing.

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

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

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

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

- Read *Trusted Solaris Audit Administration* for step by step assistance.

▼ Devise an Installation and Configuration Strategy.

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

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

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

▼ Collect Information.

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

▼ 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.

▼ 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.

For security reasons, the installation program does not offer some of the options that are available for Solaris 7 software. See “Differences from Solaris 7 Installation and Configuration” on page 35 for details.

▼ Configure the Software.

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

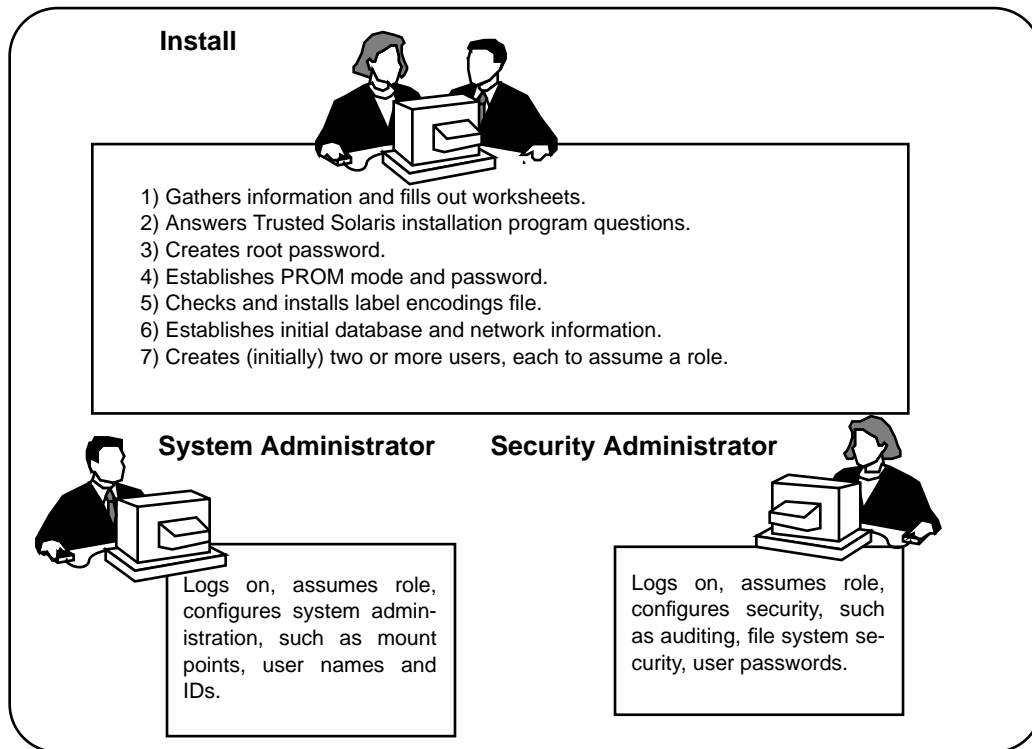


Figure 1-1 Two Roles Administering a Workstation

Once users who can assume the administrative roles are created, the install team reboots the workstation. Further configuration tasks are then 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 7 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 7 software are not available when installing Trusted Solaris 7 software. Specifically,

- No remote filesystem mounting during installation. File systems are mounted after installation.
- Upgrade is not supported.
- Volume Manager is not supported.
- Solstice™ AutoClient™ or dataless clients are not supported.
- NIS+ is the only supported Name Service.
- Web-based browser install is not supported.

Installation Results from an Administrator's Perspective

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

- Auditing is enabled.
- A SUN label_encodings file is configured and installed.
- CDE creates four labeled workspaces.
- Three administrative roles 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.

Basic Procedures

This chapter covers common administrative procedures when configuring a Trusted Solaris host.

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

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 offers four choices, as shown in Figure 2-1.

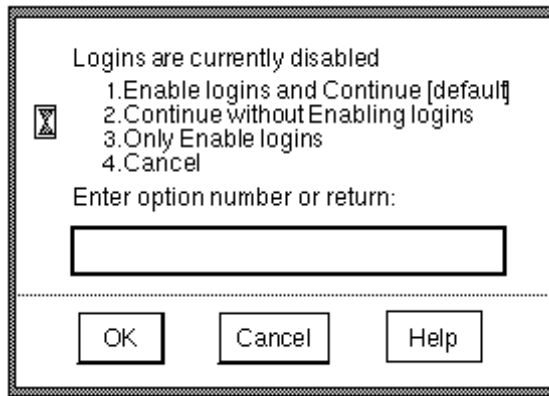


Figure 2-1 The Enable Logins Dialog

- c. **Depending on site security requirements, enter 1 or 2, then click OK.**
The Message Of the Day dialog is displayed; the label is ADMIN_LOW.
- d. **Click OK to dismiss the dialog.**
The Trusted Solaris screen appears briefly; then you are in a CDE workspace.
The trusted stripe below the front panel shows the window sensitivity label.

▼ 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, shown in Figure 2-1, is displayed if you are authorized to enable logins.

If you see the error message:

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

then your user was not assigned the Enable Login profile (see Table 5–1). To fix, give the user the Enable Login profile, or have someone else log in and enable logins.

3. Choose a login option and dismiss the dialog.

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

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

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

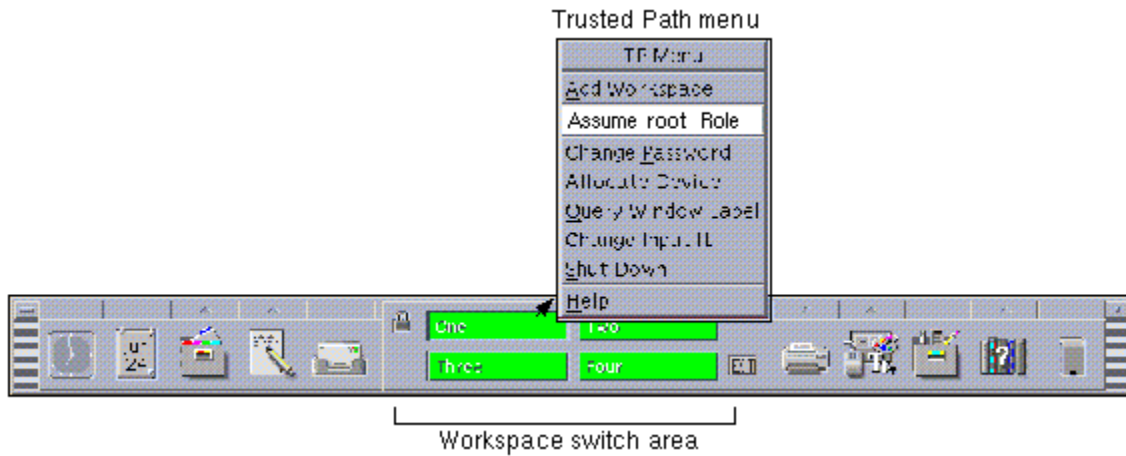
Note - The install team must log off or utilize the lockscreen functionality before leaving a workstation unattended. Otherwise a person may have access to the workstation without having to pass identification and authentication, and that person would not be uniquely identified or accountable.

How to Assume a Role

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

▼ To Assume a Role

1. Log in to the workstation as a user, such as `install`.
2. Right click on the middle of the Front Panel.
3. Assume a role from the roles displayed on the TP (Trusted Path) menu.



- a. Choose **Assume *rolename* Role** from the menu.
- b. At the password prompt, enter the password for the role.
The password for the root role is the password that the install team entered for root at the final stage of installation.

How to Launch a Terminal

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

▼ To Launch a Terminal

- ◆ Right-click on the workstation background and select **Programs > Terminal**.

How to Open a Profile Shell

The profile shell, `pfsh(1M)`, 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 from a role workspace.

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

1. Launch a terminal from a user's or non-administrative role's workspace.
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 and pipe it 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.

▼ To See Process and Privilege Information in a Profile Shell

- ◆ To see the process label, enter the `plabel(1)` command in a profile shell.

```
% plabel
pid: [ADMIN_LOW]
```

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

- ◆ To see what privileges have been accorded to you, enter the `ppriv(1)` command.

```
$ ppriv
pid: none
```

If the `ppriv` command is in your execution 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.

Note - If you are not allowed to change the workspace SL, the Change Workspace SL menu item does not appear.

1. Click the right menu button on the center of the front panel 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 Machine Hardware

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

▼ SPARC: To Set the PROM Mode and Password

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

```
# eeeprom 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:

```
# eeeprom 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*.

▼ IA: To Protect the BIOS

On an Intel machine, the equivalent to protecting the PROM is to protect the BIOS . Refer to your machine's manuals for how to protect the BIOS.

How to Limit Contact During Booting

For greater security, edit the boot-time database,
`/etc/security/tsol/boot/tnrhdb`.

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

- See “Special Boot-time Trusted Network Databases” in *Trusted Solaris Administrator's Procedures* for the security implications of the boot-time network databases.
 - See “Administering the Boot-time Trusted Network Databases” in *Trusted Solaris Administrator's Procedures* for steps to take to modify the boot-time network database defaults.
-

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 Diskette

Note - During installation, the role `root` copies administrative files to and from movable media, at the label `admin_low`.

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

Do you want floppy_0 mounted: (y,n)? **y**

For a fuller description, see “To Allocate a Device” on page 48.

2. **Copy the file to the diskette by double-clicking the File Manager icon in the Front Panel.**
3. **In the File Manager, navigate to the folder that contains the files to be copied, such as `/setup/files`.**
4. **Rename the `label_encodings` file that you are copying.**
For example, name it `label_encodings.site` (for SPARC architecture), or `lblcdsit` (for Intel architecture). Audit system files such as `audit_user`, and routing files such as `nsswitch.conf`, and `resolv.conf` do not need to be renamed.
5. **Choose Open Floppy from the File menu.**
6. **Highlight the icon for the file and drag the file to the floppy disk folder..**
7. **On the floppy disk folder, choose Eject from the File menu.**
8. **Deallocate the device before continuing.**

For the procedure, see “To Deallocate a Device” on page 49.

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

▼ To Copy One or More Files from a Diskette

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

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

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

For a fuller description, see “To Allocate a Device” on page 48.

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

Note - Exception: If the file you are copying is to replace the current `label_encodings` file, do not rename or remove the original file. See “How To Install a Site-Specific Label Encodings File” on page 47 for the full procedure.

3. **Double-click the File Manager icon in the Front Panel and navigate to the desired destination directory, such as `/etc/security/tsol`.**
4. **Choose Open Floppy from the File menu.**
5. **Highlight the icon for the file and drag the file from the floppy disk folder to the destination directory.**
6. **On the floppy disk folder, chose Eject from the File menu.**
7. **If you copied a site version of the label encodings file, see “How To Install a Site-Specific Label Encodings File” on page 47 for the full procedure.**
8. **Deallocate the device before continuing.**
This is described in “To Deallocate a Device” on page 49.

How To Install a Site-Specific Label Encodings File

If you are installing a site-specific `label_encodings` file, consult *Trusted Solaris Label Administration* for requirements, procedures, and suggestions for the label encodings file..

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

1. **Have the medium (diskette) with your site's `label_encodings` file ready to use.**
2. **As root (before roles are verified), or as `secadmin` (after roles have been verified), copy the file to a writable location, such as `/etc/security/tsol/label_encodings.site` using the File Manager.**
If you are unsure of the steps, see “To Copy One or More Files from a Diskette” on page 46.
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 57.

- b. **In the dialog box, enter the full path name of the file:**
`/etc/security/tsol/label_encodings.site`

4. **Read the contents of the Check Encodings dialog box that is displayed.**
The `chk_encodings(1M)` command checks the syntax of the file. If the file passes the check, the action asks whether you want to overwrite the currently-installed `label_encodings` file. If the answer is yes, the action creates a backup copy (naming it `label_encodings.orig`), and installs the checked version.
 - a. **If it reports no errors, continue.**
 - b. **If it reports errors, resolve them before continuing.**

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



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

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

Your `label_encodings` file is now in effect.

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

1. **Click the left mouse button on the triangle above the Style Manager icon on the Front Panel.**

Its Trusted Desktop subpanel includes the Device Allocation icon.

Device Allocation —



2. **Click the Device Allocation icon** **once.**
3. **Double-click the device to be allocated from the list of available devices.**
floppy_0 allocates a diskette.
4. **Click 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/security/label_encodings` 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, answer **y** to mount the device:

▼ To Deallocate a Device

1. Go to the workspace where the Device Allocation action is displayed.
If it is not displayed, click the Device Allocation icon
Device Allocation —  on the Trusted Desktop subpanel, at the same label and in the same role as the one who allocated the device.
2. Double-click the device to be deallocated from the list of allocated devices.
3. 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 an Applications subpanel action. It contains two folders that hold administrative applications, `System_Admin` and `Solstice_Apps`.

▼ To Open the Application Manager

- ◆ Click the arrow above the icon to the left of the mail icon on the Front Panel, and single-click the Applications action.

The Application Manager window appears, with several folders with distinctive icons.

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 a local database only; the others are both local and NIS+ databases.

Profile Manager

For adding and removing commands from a role's execution profile.

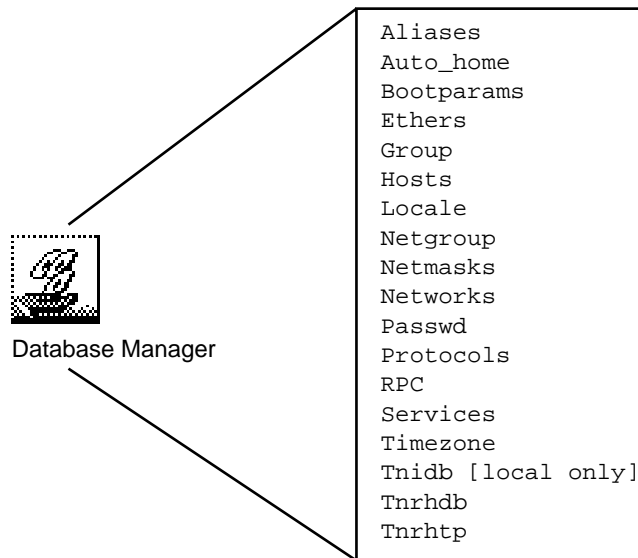


Figure 2-2 Databases Managed by the Database Manager in Solstice_Apps

▼ To Open and Modify a Solstice_Apps Database



1. **Left-click the Applications action.**

The Applications icon is on the Applications subpanel to the left of the mail icon on the front panel.



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

3. **Double-click the appropriate 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

Figure 2-3 Load Window for 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.
 - 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.
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 making 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.

1. As secadmin (as root during installation), at label `admin_low` open the User Manager using the appropriate name service, `NIS+` for a networked installation, `None` for no name service.
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 eight alphanumeric characters in the Set Password dialog box.
 - c. Press the Tab key.
 - d. Re-enter the password and press Return.
4. Make sure that for a user, the value of Status is Open.

Note - For all administrative roles, and for the user who can assume the secadmin role, use the status Always Open. Also, do not set password expiration dates on administrative roles.

5. Make sure that the Cred Table Setup box is checked for networked installations.
6. Set other password information for the account.

See "Managing User Accounts" in *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.

1. As **secadmin** at label `admin_low` 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 user out; different time lengths are possible.
5. Click **OK**, then **Done**.

▼ To Delete a Local User

1. In the role **admin**, label `admin_low`, 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 file renaming.



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. When the icon is the Admin Editor, the action is to edit the file.

Actions in the System_Admin Folder

Add Allocatable Device	Edit /etc/security/tsol/device_maps
Admin Editor	Create or edit any file
AnswerBook2 Admin	Administer AnswerBook2™
Audit Classes	Edit /etc/security/audit_class
Audit Control	Edit /etc/security/audit_control
Audit Events	Edit /etc/security/audit_event
Audit Startup	Edit /etc/security/audit_startup
Audit Users	Edit /etc/security/audit_user
Check Encodings	Check syntax (and install) label_encodings file
Check TN Files	Check local tnrhdb and tnrhtp files
Check TN NIS+ Tables	Check NIS+ tnrhdb and tnrhtp databases
Create NIS+ Client	Create NIS+ client

Create NIS+ Server	Establish root NIS+ domain
Configure Selection ...	Edit /usr/dt/config/sel_config
Edit Encodings	Edit /etc/security/tsol/label_encodings
Eject CD-ROM	Eject CDROM
Eject Floppy	Eject Floppy
Format CD-ROM	Format CDROM
Format Floppy	Format Floppy
Open CD-ROM	Open CDROM
Open Floppy	Open Floppy
Power Manager	Manage auto-shutdown features
Name Service Switch	Edit /etc/nsswitch.conf
Populate NIS+ Tables	Populate NIS+ Tables
Rename Floppy	Rename Floppy
Set Daily Message	Edit /etc/motd
Set Default Routes	Edit /etc/defaultrouter
Set DNS Servers	Edit /etc/resolv.conf
Set Mail Options	Edit /etc/mail/sendmail.cf
Set Mount Attributes	Edit /etc/security/tsol/vfstab_adjunct
Set Mount Points	Edit /etc/vfstab
Set TSOL Gateways	Edit /etc/tsolgateways
Share Filesystems	Edit /etc/dfs/dfstab
Suspend System	Shut down system
System Load	View system load

Terminal Console	Open terminal console
Terminal Remote	Open remote terminal
Terminal Rlogin	Remote login to terminal
View Table Attributes	View internal representation of a NIS+ table
View Table Contents	View contents of a NIS+ table
Watch Errors	Generate error log
X Server Information	X Server information

▼ To Run a System_Admin Action



1. **In an administrative role, open the Application Manager by clicking the icon once with the mouse.**

The Applications icon is on the Applications subpanel to the left of the mail icon on the front panel.



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

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.**

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 its action.**

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

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

To Run a Script from the System_Admin Folder



1. **To run a 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

1. **As role `admin`, at label `admin_low`, use the `prtconf` command to find the network interfaces.**

```
# prtconf | grep instance
... le, instance #0
qe2, instance #0...
```

(continued)

```
qe3, instance #0...
```

2. List the secondary interfaces.

```
# ls /etc/hostname*
hostname.le
```

The primary interface was configured during installation; its file exists.

- ◆ Continue with “To Create the Network Interface Files” on page 60.
- ◆ If you know that you have created an `/etc/hostname.interface` entry for every interface, use the `ifconfig(1M)` command.

```
# ifconfig -a
le0: flags=

863<UP,BROADCAST,NOTRAILERS,RUNNING,MULTICAST> MTU 1500
inet 129.150.118.111 netmask ffffffff0 broadcast 129.150.118.255
ether 8:0:21:62:13:a9
qe2: flags=

863<UP,BROADCAST,NOTRAILERS,RUNNING,MULTICAST> mtu 1500
inet 129.150.117.22 netmask ffffffff0 broadcast 129.150.117.255
ether 8:0:21:64:20:a3
qe3: flags=

863<UP,BROADCAST,NOTRAILERS,RUNNING,MULTICAST> mtu 1500
inet 129.150.119.111 netmask ffffffff0 broadcast 129.150.119.255
ether 8:0:21:52:11:a2
```

- ◆ Continue with “To Create the Network Interface Files” on page 60.

▼ To Create the Network Interface Files



1. **As secadmin, at label `admin_low`, for each secondary interface, open a file named `/etc/hostname.interface` in the Admin Editor.**

See “To Run a System_Admin Action” on page 57 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/hostname.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/hostname.qe`:

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



2. **As secadmin, at label `admin_low`, 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 51 if you are unfamiliar with editing the Hosts database.

3. **As secadmin, at label `admin_low`, add every interface to the local `tnrddb` 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`.



1. **As role `admin`, at label `admin_low`, 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 "netinstall dir" /export/ts7_install/
```

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

2. **As the role `admin`, at label `admin_low`, run the `share(1M)` 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

1. As role **admin**, at label **admin_low**, 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/ts7_sparc
/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

1. In the role **admin**, at label **admin_low**, start the **nfs server** program.

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

2. 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.

1. **Log in as a user who can assume the role secadmin and assume the role.**
2. **As secadmin, at label admin_low, 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, the following example shows a vfstab_adjunct entry for an unlabeled, remote file system, /cpublic, being mounted at the label Confidential ([C]) on a Trusted Solaris 7 network.

EXAMPLE 2-1 vfstab_adjunct Entry for Unlabeled Remote Host

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

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 93.

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



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

1. **As role `admin`, at label `admin_low`, run the Set Mount Points action in the `System_Admin` folder.**

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
```

2. Write the file and exit the editor.
3. As role **admin**, at label `admin_low`, create the mount point and mount the home directories.

```
$ 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 an execution 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

1. Log in as a user who can assume the role `secadmin`.
2. As `secadmin`, at label `admin_low`, 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, type:

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

5. In the list of Excluded commands, double-click the directory /cdrom/cdrom0.
6. 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.
7. 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.
2. Assume the role and launch a terminal from the role's workspace.
3. Verify that the new profile is in effect in the new terminal by using the `clist(1M)` 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

1. As `secadmin`, at label `admin_low`, 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 moved to the Excluded list.
4. Save the Custom *Rolename* Role profile.

How to End a Session

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

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

▼ To Lock the Screen

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

▼ To Log Out

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

▼ To Reboot the Workstation

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

```
Type help for more information
<#2> ok boot
Type b (boot), c (continue), or n (new command mode)
> b
```

Installing a Workstation

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

- From a Trusted Solaris CDROM.
- From a floppy and 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.

System Installation Step by Step

▼ IA: Boot from Diskette and Install

1. Insert the Trusted Solaris Device Assistant diskette into the floppy drive.
2. Choose the install choice of booting from a CDROM.
3. Insert the Trusted Solaris CDROM in the CD drive.

▼ SPARC: If Solaris workstation is *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. If the screen displays the > prompt, enter **n** and press Return to display the ok prompt.

▼ SPARC: If Solaris workstation is *on*:

1. Enter the following commands:

```
$ su root
# halt
```

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

▼ SPARC: If Trusted Solaris workstation is *on*:

1. Shut Down the workstation from the TP menu.
2. If the screen displays the > prompt, enter `n` and press Return to display the ok prompt.

See “Plan Workstation Hardware and Capacity.” on page 29 for hardware, disk space, and memory requirements.

▼ SPARC: Install from a CDROM

See your hardware manual, such as the *Solaris 7 8/99 Sun Hardware Platform Guide* for instructions.

1. Place the Trusted Solaris CD in the workstation’s CDROM drive.
2. Boot the workstation:

```
boot cdrom
```

Note - Use the command

```
boot sd(0,6,2)
```

for SPARCstation 1 (4/60), SPARCstation 1+ (4/65), SPARCstation SLC™ (4/20), and SPARCstation IPC™ (4/40).

3. If you are booting from CDROM *and* with a custom JumpStart diskette, enter:

```
boot cdrom - install
```

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

▼ SPARC: Install over the Network

1. To install from a server on the network, enter:

```
boot net
```

2. To install from a server on the network for a custom JumpStart installation, enter:

```
boot net - install
```

Note - A space is required between the minus sign and install.

▼ Read Booting Messages

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

```
Type b (boot), c (continue), or n (new command mode)
>n
Type help for more information
Ok boot cdrom Rebooting with command: cdrom
Boot device: /sbus/esp@0, 8000000/sd@6, 0:c
File and args:
SunOS Release 5.7 Version Trusted_Solaris_7 [UNIX(R) System V Release
4.0]
Copyright (c) 1983-1999, 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: 1e(0,0,0) - install
2bc00 hostname: sora
```



```

domainname: aviary.eco.org
root server: grebe
root directory:
/export/install/trusted_solaris_7_sparc/s0/export/exec/kvm/sparc.sun4c.Trust
ed Solaris_7
SunOS Release 5.7 Version Trusted_Solaris_7 [UNIX(R) System V Release 4.0]
Copyright (c) 1983-1999, 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.

▼ Answer Installation Questions

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.

See Appendix D for sample answers.

Installation Program Questions

- Select a language and a locale

——— 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]

Caution - Do not choose the options Other or NIS; they do not work in the Trusted Solaris environment.

3. On a subnet?

- a. Its subnet mask

4. Time zone

5. Date and time

——— System identification completed ———

——— *Searches for JumpStart scripts appear in the upper left console window* ———

1. Initial Install

Upgrade is not supported.

2. Allocate client services?

Allocate client services if the workstation will serve diskless clients.

-
- For performance reasons, your NIS+ master should not serve diskless clients.
 - Diskless clients are installed using the Host Manager in the Solstice_Apps folder. See Chapter 10.
-

3. Select the languages that can be displayed onscreen.

4. Software group

- a. The groups Core and End User are identical in the Trusted Solaris environment.
- b. Select To Include Solaris 64-bit support

Note - The 64-bit system will be installed, but your system will boot 32-bit if the Flash PROM needs to be upgraded.

- See “Updating the Flash PROM on the Ultra 1, Ultra 2, Ultra 450, and Sun Enterprise 450 Systems” in *Solaris 7 8/99 Sun Hardware Platform Guide* for how to upgrade the Flash PROM. You do not need to install the Solaris 7 environment for the PROM upgrade; install the Trusted Solaris 7 environment.
-

5. Customize the installation?

6. 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, see “Disk Partitioning Hints” on page 75.
- 7. Begin installation.
- 8. 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.

Disk Partitioning Hints

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

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

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

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

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

- Create an `/export/home` partition large enough for the users’ home directories.

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

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

On an OS server...

- Allocate enough space for the clients’ root and swap. See the sample worksheet, “OS Server Installation Program Example” on page 239

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).

▼ 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`.

1. Look for successful installation of packages.

2. Ignore messages of the form:

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

▼ Enter a root Password



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

♦ 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.

Troubleshooting

Errors you encounter during installation are described and debugged in the Troubleshooting section of the *Solaris 7 Installation Collection* (see <http://docs.sun.com/ab2/coll.241.4>).

▼ Complete OS Server Installation

If you installed an OS Server system type, allocated space for diskless clients, and selected the initial installation option, you are not finished.



◆ Use the Host Manager to complete the setup of these clients, as described in Chapter 10.

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.

▼ Complete Network and JumpStart Installations

For pointers to administration books, see Chapter 11.

1. Check that all Trusted Solaris configuration tasks are complete.

For an overview of individual workstation configuration tasks, see Chapter 6.

Configuring a Workstation without the NIS+ Name Service

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

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

Who Does What

Trusted Solaris software is designed to be installed and configured by an install team. Once the team has created users who can assume Trusted Solaris roles, and has rebooted the workstation, the software enforces 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.

Non-Networked Configuration Tasks

A non-networked workstation or a networked workstation that does not use a name service is configured much like a NIS+ root master, except that `/etc` files are used for administration rather than NIS+ tables.

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

If you are configuring the workstation to satisfy criteria for an evaluated configuration, please read “Understand Your Site’s Security Policy.” on page 26

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

- “Log In and Assume the root Role” on page 80
- “Protect the Workstation” on page 80
- “Check and Install the label_encodings File ” on page 80
- “Set Up Network Files” on page 81
- “Add Administrative Roles to Three /etc Files” on page 82
- “Reboot the Workstation” on page 83
- “Update Role Passwords” on page 84
- “Add Users to Administer the System” on page 84
- “Verify That Users and Administrative Roles Work” on page 85
- “Mount Unlabeled File Systems” on page 85
- “Share File Systems” on page 85
- “Delete the User install” on page 85

▼ 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 37 if you are unfamiliar with the steps.

▼ Protect the Workstation

1. **Protect the PROM or the BIOS.**

See “How to Protect Machine Hardware” on page 43 if you are unfamiliar with the steps.

2. **Limit contact with other workstations when booting.**

See the explanation and reference in “How to Limit Contact During Booting” on page 44.

▼ 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 82.
- 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 81.

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, the file must conform to requirements detailed in *Trusted Solaris Label Administration*. Read on.

1. See “How To Install a Site-Specific Label Encodings File” on page 47 for the full procedure.
 - a. Run the Check Encodings action from the System_Admin folder to install the modified `label_encodings` file.



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

- b. Read the new `label_encodings` file into your environment by clicking the right mouse button on the workspace background and choosing Windows > Restart Workspace Manager.

▼ 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.

- ◆ **If you are going to use static routing, set it up.**
Follow the procedure in “Set Up Routing” on page 90.



- ◆ **If you are using static routing, open the Database Manager and 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 92.



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

For a detailed list of steps, see “Set Up DNS” on page 100. Do not edit the `nsswitch.conf` file.

- ◆ **Using the Database Manager, enter the details of every workstation that this workstation may contact in the `tnrhdb(4)` 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 51 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 94.

- ◆ **Configure any secondary network interfaces.**

Follow the steps in “How to Add Network Interfaces” on page 58 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`.

- 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
```

- 2. Add the contents of each `*.roles` file to its corresponding `/etc` file.**



- a. Using the Admin Editor, 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`. To write out an edited `shadow` file, you must use the Admin Editor command `:wq!`, since the file is write-protected.



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 67.

▼ Update Role Passwords

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



2. Open the User Manager from `Solstice_Apps` using `None` for the Naming Service, 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 52 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

1. Add users who will assume administrative roles. Follow the outline provided in Table 5-1.

See “To Open and Modify a `Solstice_Apps` Database” on page 51 if you are unfamiliar with the User Manager.

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 105 to ensure that every role is working.

▼ 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.

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 106 if you are unsure of the steps.

2. **Mount the file system.**

If you are unfamiliar with the steps, see “How to Mount a File System” on page 64.

▼ Share File Systems

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

- ◆ **Share the file systems that other workstations may access.**

Follow the procedure in “How to Share a File System” on page 61 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.

- ◆ **Use the User Manager to delete the user install.**

See “To Delete a Local User” on page 54 if you are unfamiliar with deleting users.

Configuring the NIS+ Root Master

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

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

Who Does What

Trusted Solaris software is designed to be installed and configured by an install team. Once the team has created users who can assume Trusted Solaris roles, and has rebooted the workstation, the software enforces 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.

NIS+ Root Master Configuration Tasks

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

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

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

If you are configuring a site that satisfies criteria for an evaluated configuration, please read “Understand Your Site’s Security Policy.” on page 26.

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

- “Log In and Launch a Terminal” on page 88
- “Protect the Workstation” on page 89
- “Check and Install the label_encodings File” on page 89
- “Set Up Routing” on page 90
- “Set Up Additional Network Interfaces” on page 92
- “Edit the Trusted Network Files” on page 93
- “Set Up the NIS+ Domain” on page 95
- “Set Up DNS” on page 100
- “Reboot the Workstation” on page 101
- “Update Role Credentials and Passwords” on page 101
- “Set Up Home Directories” on page 101
- “Add Users to be Administrators” on page 102
- “Verify that Users and Administrative Roles Work” on page 105
- “Set Up Auditing” on page 106
- “Set the Label for Unlabeled File Systems (Example)” on page 106
- “Share File Systems” on page 107
- “Copy Configuration Files for Distribution to Clients” on page 107
- “Delete the User install” on page 109

▼ Log In and Launch a Terminal

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

See “How to Log In” on page 37 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 40 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

1. Protect the PROM or the BIOS.

See “How to Protect Machine Hardware” on page 43 if you are unfamiliar with the steps.

2. Limit network contact during booting.

See the explanation and reference in “How to Limit Contact During Booting” on page 44.

▼ 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 90 if you are not modifying the label_encodings file and you have an open network.
- Skip to “Edit the Trusted Network Files” on page 93 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 the default `label_encodings` file, check that your `label_encodings` file works on the NIS+ master before copying the file to every workstation you install.

1. See “How To Install a Site-Specific Label Encodings File” on page 47 for the full procedure.
 - a. Run the Check Encodings action from the `System_Admin` folder to install the modified `label_encodings` file.



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

- b. Read the new `label_encodings` file into your environment by clicking the right mouse button on the workspace background and choosing `Windows > Restart Workspace Manager`.

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 107.

▼ 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).

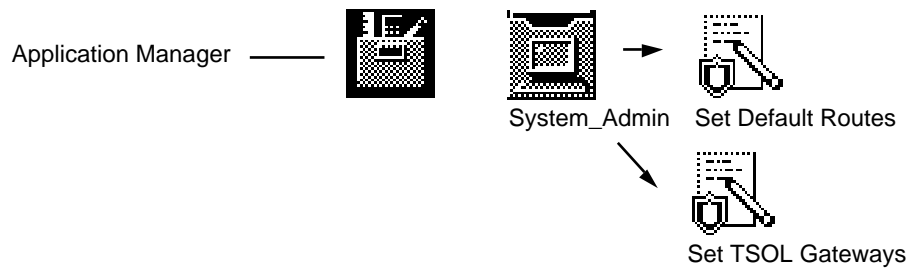
Note - If you plan to use dynamic routing, skip this procedure.

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 “Routing” in *Trusted Solaris Administrator's Procedures* and the `tsolgateways(4)` 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” on page 91.



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 58 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

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

See “To Open a File that has a Defined Action” on page 58 if you are unfamiliar with using trusted actions.

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

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

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 “Managing Devices” in *Trusted Solaris Administrator's Procedures* if you need to add a new hardware device to the `device_policy(4)` 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 the Solaris environment. For further information on basic setup, see “Configuring TCP/IP on the Network” in *TCP/IP and Data Communications Administration Guide* in the *Solaris 7 System Administrator Collection*.

▼ 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 51 if you are unfamiliar with editing the Hosts database.

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 7 network can communicate. The security administrator determines what networks can contact the Trusted Solaris 7 network; for a list of host types, see Table 1–2. The system administrator collects the IP addresses.

If you plan to mount file systems from unlabeled hosts at a label available to users, or enable communications using services such as `ftp`, or route through an unlabeled host, do “To Edit the Tnrhttp Database (Example)” on page 93 first. Otherwise, go to “To Edit the Tnrhdb Database ” on page 94.

You can change the network details later. For customizing the `tnrhdb` and its associated templates database, `tnrhttp`, see “Creating Entries in the Trusted Network Databases” in *Trusted Solaris Administrator's Procedures*.

To Edit the Tnrhttp Database (Example)

This example adds a new template, `unlab_userlabel`, to the `tnrhttp(4)` 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 106 completes the setup.

1. **Open the Tnrhttp database in the Database Manager using no naming service.**
See “To Open and Modify a Solstice_Apps Database” on page 51 if you are unfamiliar with the steps.
2. **Choose Edit > Add from the Tnrhttp menu.**
3. **In the Template Manager (Add) window, create a new template with the an unlabeled host type named `unlab_userlabel`, 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_userlabel` for the template name.
- b. Select `Unlabeled` from the list of Host Types.
- c. Click the **Defl** 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.
- a. Click the **Label** button to set the default CMW label to `[userlabel]`.
Select a sensitivity label available to users. The sensitivity label `[ADMIN_LOW]` is not available to users.
 - i. Click the **SL** button and click a user sensitivity label, such as **Confidential**.
 - ii. Click OK.

4. Exit the database when the template is complete.

To Edit the Tnrhdb Database

1. Open the Tnrhdb database in the Database Manager using no naming service.
See “To Open and Modify a Solstice_Apps Database” on page 51 if you are unfamiliar with the steps.
2. Use the IP address fallback mechanism to assign one template to all hosts on your Trusted Solaris 7 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 unlabeled. 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 1-2 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 7 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.

To Set the Stage

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

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

```
# mkdir -p /setup/files
```

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

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

```
# cd /etc
# touch bootparams ethers netgroup netmasks timezone
# cp bootparams ethers netgroup netmasks timezone \
aliases auto_home auto_master group hosts networks \
protocols 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
```

(continued)


```
# 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
```

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 57.

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 7 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*

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 58 if you are unfamiliar with using trusted actions.

2. Enter your NIS+ domain name.

This workstation will be the root master. For example,

Domain Name: `aviary.eco.org.`

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

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

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

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

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

5. **Populate the standard NIS+ databases from the /setup/files directory by running the Populate NIS+ Tables action.**
6. **Enter your staging area when prompted.**

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

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

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

8. **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:

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

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

The file looks something like:

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

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

2. **Edit the `hosts` entry in the `/etc/nsswitch.conf` file to use DNS. The action is 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 67.

▼ 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.

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

See “To Log In as the User Install” on page 37 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 51.

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 98.

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 52.

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 61.

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” on page 102, before adding users.

Install and Configure the Home Directory Server *Now*

1. Go and do:

- “System Installation Step by Step” on page 70
- Chapter 6
- Configure the home directory server up through reboot:
 - “Set Up Home Directories” on page 118 (on the NIS+ client and NIS+ master)
 - “Reboot the Workstation” on page 118 (boot the NIS+ client)

2. Then, create the first three users.

Continue with “Add Users to be Administrators” on page 102.

▼ 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.

To Create a User

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	<i>/mount_path/username</i>
	Server	<i>home directory server</i>
	Skeleton path	Yes, use it.

TABLE 5-1 User Account Characteristics *(continued)*

	Default permissions on home directory	
	Mail server	
	Cred?	Yes, leave it checked.
	AutoHome setup	Yes, when networked; No, when non-networked.
Labels	Clearance	<i>not</i> ADMIN_HIGH
	Minimum Sensitivity Label	<i>not</i> ADMIN_LOW
	Label View	
	SL visibility	If your site is a no-label site, choose Hide.
	IL visibility	
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

-
- 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 “Managing User Accounts” in *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.
-
1. 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
```

2. **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.

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

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

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

To Configure Auditing

- ◆ **Follow the *Trusted Solaris Audit Administration* guide to configure auditing at your site.**

Who is audited and for what events should be the same on every workstation. Copy any modified audit configuration files from the NIS+ root master to every NIS+ client using the procedure in “Copy Configuration Files for Distribution to Clients” on page 107.

▼ 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 `tnrhttp` file as described in “To Edit the Tnrhttp Database (Example)” on page 93.

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 63.

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

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

▼ Share File Systems

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 61.

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.

3. **Share the file systems.**

If you are unsure of the commands, see “How to Share a File System” on page 61.

▼ Copy Configuration Files for Distribution to Clients

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 `tnrhttp` 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 tnrhttp /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  tnrhttp
```

To Transfer Files for NIS+ Clients to Diskette

1. Allocate the diskette device.

See “How to Allocate and Deallocate a Device” on page 48 if you are unfamiliar with the steps. Do not mount the device.

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

2. Copy the files to the allocated medium.

For examples of copying files to a portable medium, see “How to Copy Files To and From a Portable Medium” on page 44.

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

▼ Delete the User install

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



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

- ♦ See “To Delete a Local User” on page 54 if you have not deleted a local user in the Trusted Solaris system before.

Configuring a NIS+ Client

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

Who Does What

Trusted Solaris software is designed to be installed and configured by an install team. Once the team has created users who can assume Trusted Solaris roles, and has rebooted the workstation, the software enforces 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.

NIS+ Client Configuration Tasks

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.

Depending on your site configuration and installation method, some procedures can be omitted.

- “Log In and Protect the Workstation” on page 112
- “Copy Configuration Files from the NIS+ Master” on page 112
- “Copy the NIS+ Master label_encodings File” on page 113

- “Set Up Static Routing” on page 113
- “Set Up Secondary Network Interfaces” on page 115
- “Copy the Tnrhttp Database (Example)” on page 115
- “Edit the Tnrhdb Database” on page 116
- “Verify Communication with the NIS+ Master” on page 116
- “Set Up the NIS+ Name Service” on page 117
- “Set Up DNS and the Name Service Switch” on page 118
- “Set Up Home Directories” on page 118
- “Reboot the Workstation” on page 118
- “Add Users” on page 119
- “Finish Configuring the Workstation” on page 119

▼ Log In and Protect the Workstation

1. **Log in as a user who can assume the role root and assume it.**
See “How to Log In” on page 37 if you are unsure of the steps.
2. **Protect the workstation.**
See “How to Protect Machine Hardware” on page 43 if you are unsure of the steps.
3. **Limit contact with other `tsol` hosts if required by site security.**
See “How to Limit Contact During Booting” on page 44 for an explanation and reference.

▼ Copy Configuration Files from the NIS+ Master

You made a diskette with files for the client in “Copy Configuration Files for Distribution to Clients” on page 107.

To Copy Master Files from Diskette

1. **As root, at label `admin_low`, make a temporary directory and go to it.**


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

2. **Copy the files from the diskette.**

See “To Copy One or More Files from a Diskette” on page 46 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.

1. **As root, at label admin_low, copy the NIS+ master’s label_encodings file to the /etc/security/tsol directory.**

Follow the procedure in “To Copy One or More Files from a Diskette” on page 46.



2. **Use the Check Encodings action to check the syntax of the file and install it.**



Caution - The label_encodings file *must* pass the Check Encodings test before you continue.

3. **Read the new label_encodings file into your environment by clicking the right mouse button on the workspace background and choosing Windows > Restart Workspace Manager.**

▼ Set Up Static Routing

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

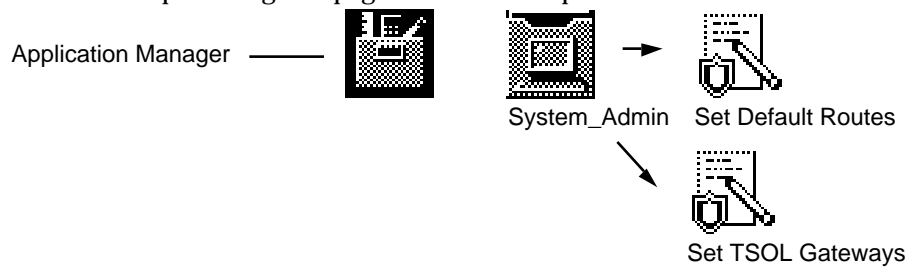
1. **Determine the appropriate static routing for the client.**

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	

2. As root, at label `admin_low`, enter the defaultrouter using the **Set Default Routes** action, or the `tsolgateways` using the **Static Routing Configuration** action.

See “Set Up Routing” on page 90 for more explanation.



3. **Save the file and exit the editor.**
4. As root, at label `admin_low`, 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 51 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 58 if you are unsure of the steps.

▼ Copy the Tnrhttp 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 `tnrhttp(4)` template definition and name for the NIS+ master must be identical on the client and master when you run the `nisclient(1M)` command.

- ◆ **As root, at label `admin_low`, use the File Manager to copy the `tnrhttp` file from the `/export/clientfiles` directory to `/etc/security/tsol/tnrhttp`.**
 - ◆ **As root, copy the original `tnrhttp` file to `tnrhttp.orig`:**

```
# cd /etc/security/tsol/  
# cp tnrhdb tnrhdb.orig  
# rm tnrhdb
```

- ◆ **Double-click the File Manager icon in the Front Panel and navigate to the `/export/clientfiles` directory.**
- ◆ **Open a second File Manager, and navigate to `/etc/security/tsol`.**
- ◆ **Drag the file from the first File Manager to the `/etc/security/tsol` File Manager.**

▼ Edit the Tnrhdb Database

1. As root, at label `admin_low`, use the Database Manager to enter the IP address and template name (`tsol`) of the subnet into the `tnrhdb(4)` database.

For example, enter a subnet address, such as `129.150.110.0`, and `tsol`. See “To Edit the Tnrhdb Database ” on page 94 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`:

- a. The client and its host type (`tsol`),
- b. The NIS+ master and its host type (`tsol`) [or its subnet fallback IP address and `tsol`], and
- c. 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.

1. As root, at label `admin_low`, 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/tnrhttp`

The client's local `tnrhdb(4)` file must have the IP address and host type of the NIS+ master (or the IP address and host type of the subnet), the client's static routers, and the client.

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

▼ Set Up the NIS+ Name Service

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

1. **As root, at label `admin_low`, add the workstation as a NIS+ client using the Create NIS+ Client action in the System_Admin folder.**

See “To Run a Script from the System_Admin Folder” on page 58 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

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.

- ◆ **As root, at label `admin_low`, set up the DNS nameservers and the name service switch by copying the files `resolv.conf` and `nsswitch.conf` from `/export/clientfiles` to the `/etc` directory.**

Make a copy of the original file and use the File Manager, as described for the `tnrhtp` database in Step on page 115.

▼ Set Up Home Directories

- ◆ **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 61.

▼ 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 67.

▼ Add Users

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

- ◆ If you are configuring the home directory server and have not yet added users who can assume administrative roles, return to “Add Users to be Administrators” on page 102.

▼ Finish Configuring the Workstation

If you are configuring a site that satisfies criteria for an evaluated configuration, read “Understand Your Site’s Security Policy.” on page 26

Secadmin Responsibilities

The `secadmin` administrative role handles auditing and security attributes on file systems.

- To configure or to disable auditing, see *Trusted Solaris Audit Administration*.

Note - To ensure that every workstation and user is audited identically, as root at label `admin_low`, copy the NIS+ root master’s `/etc/security/audit*` configuration files to each workstation (see “Copy Configuration Files from the NIS+ Master” on page 112) and enter the correct `dir:` entries as described in *Trusted Solaris Audit Administration*.

- To set security attributes on an unlabeled file system, see “How to Set the Label on an Unlabeled File System” on page 63.

Admin Responsibilities

The `admin` administrative role handles file system management, and user account creation and deletion.

- To share a file system, see “How to Share a File System” on page 61.
- To mount a file system, labeled or unlabeled, see “How to Mount a File System” on page 64.
- To delete the install user, see “To Delete a Local User” on page 54 if you have not deleted a local user in the Trusted Solaris environment before.

Trusted Solaris Administrator’s Procedures provides examples and background.

Preparing to Install Trusted Solaris Over a Network

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

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.

Servers Required for Network Installation

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.

- *Boot server* – A workstation that contains pointers to platform, and timezone 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.

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.

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” on page 93

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 `tnrddb`.

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

- “Create an Install Server” on page 124

Result: The Trusted Solaris 7 image and booting software is available for network install.

3. Add client information such as timezone, and platform group to a network server:

- “Add Client Information for a Network Install” on page 126

Result: The Trusted Solaris 7 installation program system identification questions can be answered without user interaction.

4. Create a boot server for any subnets:

- “Create a Boot Server on a Subnet” on page 131

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:

- Chapter 8

Commands You Should Know About

The following commands and actions enable network installation.

`setup_install_server` A script that copies all or part of the Trusted Solaris CD onto a server's local disk. This enables you to perform network installations from the install server's disk. See the `setup_install_server(1M)` man page for more information.

`add_install_client` A script that adds client information to a boot server. See the man page `add_install_client(1M)` for details.

Host Manager

A graphical user interface that is available from the `Solstice_Apps` folder. You can use Host Manager to specify client information for network installation.

`mount` A command that shows mounted file systems, including the Trusted Solaris CD file system. See the `mount(1M)` page for more information.

`uname -m` A command for determining a workstation's platform group (for example, `sun4m`). This information is required during network installation. See the `uname(1)` man page for more information.

`reset` A command for resetting the terminal settings and display. It is sometimes useful to use `reset` before booting. Or, if you boot and see a series of error messages about I/O interrupts, press the L1 or STOP and A keys at the same time, and then enter `reset` at the ok or > PROM prompt.

banner A command for displaying workstation information, such as model name, Ethernet

address, or memory installed. Available only from the `ok` or `>` PROM prompt.

▼ 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:

- Finish the procedures in Chapter 3.
- Finish the procedures in Chapter 6.
- 1. **Log in as a user who can assume the role `root` and assume it.**
- 2. **As `root`, at label `admin_low`, allocate the CDROM drive, and mount it:**

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

See “To Allocate a Device” on page 48 if you are unsure of the steps.

- 3. **As `secadmin`, at label `admin_low`, 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 65.
- 4. **As `root`, at label `admin_low`, 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 66.
- 5. **As `root`, in the same terminal where the `setup_install_server` command was verified, change to the `cdrom0` directory.**

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

- 6. **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
```

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/ts7_sparc` directory on the local disk:

```
./setup_install_server /export/install/ts7_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.

7. **If there are no boot servers to install, as secadmin at label `admin_low`, 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 66.

8. **As root, at label `admin_low`, deallocate the drive and remove the CDROM.**

See “To Deallocate a Device” on page 49 if you are unsure of the steps.

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

▼ 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`.**
2. **As role `admin`, at label `admin_low`, open the Hosts database using the NIS+ naming service.**

See “To Open and Modify a Solstice_Apps Database” on page 51 if you are unfamiliar with the steps.

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:

<code>NIS+_master_host_name IP_address loghost timehost</code>
--

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” on page 126.**

▼ 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(1M)` 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`.**
2. **As role `admin`, at label `admin_low`, launch the Host Manager using the NIS+ naming service.**
See “To Open and Modify a Solstice_Apps Database” on page 51 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. Click the OK button.

TABLE 7-1 Adding Host Information in Host Manager

Entry	Value
Host Name	
IP Address	
Ethernet Address	
System Type	
Timezone Region	
Timezone	
Remote Install	4 Enable Remote Install
Install Server	<i>install_server_name (entered for you)</i>
Set Path	<i>/export/install/ts7_sparc (sample)</i>
OS release	<i>Choose client's platform group and software cluster</i>
	<i>boot_server_name (if separate server)</i>
Boot Server	<i>path to boot file</i>
Profile Server	<i>Enter JumpStart directory (for Custom JumpStart).</i>

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 131.

Add Client Information with the `add_install_client` Command

Note - If you added hosts with the Host Manager, do not add information locally, as this command does.

1. On the install server, as `secadmin` at label `admin_low`, 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/ts7_sparc`.

See “To Add a Command to a Role's Profile” on page 65 for the full procedure.

2. On the install server, as root at label `admin_low`, launch the Name Service Switch action.
3. 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
```

4. 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/ts7_sparc/add_install_client: all
```



```
/export/install/ts7_sparc/rm_install_client: all
```

See “To Verify That a Command is in a Role’s Profile” on page 66 for the full procedure.

5. 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/ts7_sparc
```

6. Run the `add_install_client(1M)` command for every client you plan to install over the network.

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

In this command,

–e Specifies the ethernet address.

–s Specifies the install server.

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, sun4u) of the host being installed. (For a detailed list of

platform groups, see *Solaris 7 Sun Hardware Platform Guide*.)

For example, issuing the command:

```
# ./add_install_client -e 8:0:20:17:22:a4 \  
-s heron:/export/install/ts7_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.
- 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/ts7_sparc.

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

7. As secadmin, at label admin_low, remove the add_install_client script from the Custom Root Role.

See “To Remove a Command from a Role's Profile” on page 66 for the full procedure.

8. Go to “Check Client Information” on page 131.

Remove Client Information with the rm_install_client Command

1. As root, at label admin_low, verify that rm_install_client is in the root profile shell.

```
# clist -p | grep rm_install_client  
It should display:  
/export/install/ts7_sparc/rm_install_client: all
```

2. Change to the Trusted Solaris boot information directory.

```
# cd boot_dir_path
```

3. As root, at label `admin_low`, run the `rm_install_client` command for every client you plan to remove from the network install.

```
# ./rm_install_client host_name
```

4. 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 66 for the full procedure.

▼ Check Client Information

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

1. As role `admin`, at label `admin_low`, 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 pair:

```
install_server=server:install_dir_path
```

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” on page 131.
4. Otherwise, go to “Reboot the Install Server” on page 133.

▼ 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. The install server is the boot server. Go to “Reboot the Install Server” on page 133.

1. Follow Step 1 on page 124 in “Create an Install Server” on page 124.
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 Step 3 on page 132.
NFS mount of a Trusted Solaris CD image	1. As root, <code>mount -F nfs -o ro server_name:path /mnt</code> where <code>server_name:path</code> is the host name and absolute path to the Trusted Solaris CD image. 2. <code>cd /mnt</code> 3. Go to Step Step 6 on page 133.

3. As root, at label `admin_low`, 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 65 and “To Verify That a Command is in a Role’s Profile” on page 66 for the full procedure.

5. Change directory to the Trusted Solaris image.

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

6. **As root, at label `admin_low`, 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/ts7_sparc` directory on the boot server:

```
# ./setup_install_server -b /export/bootdir/ts7_sparc
```

The workstation is now configured as a boot server.

7. **After all boot servers are installed, as `secadmin` at label `admin_low`, 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 66.

▼ 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 67.

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

2. **Follow the network installation procedure, “SPARC: Install over the Network” on page 72 in Chapter 3.**

Clients will get platform, ethernet, and other system identification information from network files.

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

- “How to Create a JumpStart Directory on a Diskette” on page 141
- “How to Create a JumpStart Directory on a Server” on page 144
- “How to Enable Access to the JumpStart Directory” on page 146
- “How to Create a Profile” on page 149
- “How to Create the rules File” on page 161
- “How to Use check to Validate the rules File” on page 172
- “Copy JumpStart Files to jumpstart_dir_path” on page 173
- “Check That All Installation Questions Can Be Answered” on page 174

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 C provides an example of how a fictitious site prepares and uses custom JumpStart installations.

Reasons to Choose a Custom JumpStart Installation

You should choose a custom JumpStart installation 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 7 and installing Solaris 7 using custom JumpStart.

Trusted Solaris Custom JumpStart Additions

In the Trusted Solaris environment, administrative jobs are performed by 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.

Trusted Solaris Custom JumpStart Limitations

The following custom JumpStart features are not supported by Trusted Solaris:

- Mounting remote file systems
- Upgrade
- 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:

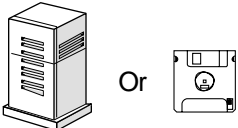
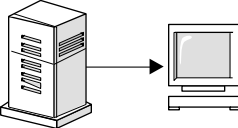

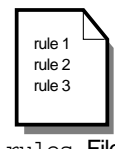
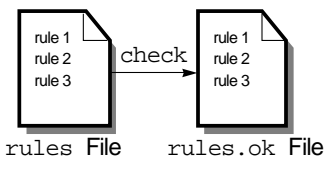
- An install server (for the Trusted Solaris image)
- A Trusted Solaris configuration server (for Trusted Solaris configuration values)
- A boot server (for boot information on a subnet)
- A JumpStart server (for the JumpStart information).

Note - To set up these servers, follow the procedures in Chapter 7.

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 141. If you are going to use a server for custom JumpStart installations, see “Creating a JumpStart Directory on a Server” on page 144.
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 146 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, initial installation option, system type, disk partitioning, software group), and it is named in the <code>rules</code> file. See “Creating a Profile” on page 149 for detailed information.
Creating a rules file		The <code>rules</code> file is a text file used to create the <code>rules.ok</code> file. The <code>rules</code> 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 160 for detailed information.
Using <code>check</code> to validate the rules file		The <code>rules.ok</code> file is a generated version of the <code>rules</code> file, and it is required by the custom JumpStart installation software to match a workstation to a profile. You <i>must</i> use the <code>check</code> script to create the <code>rules.ok</code> file. See “Using <code>check</code> to Validate the rules File” on page 171 for detailed information.

What Happens During a Custom JumpStart Installation

Figure 8–1 describes what happens after you boot a workstation to perform a custom JumpStart installation.

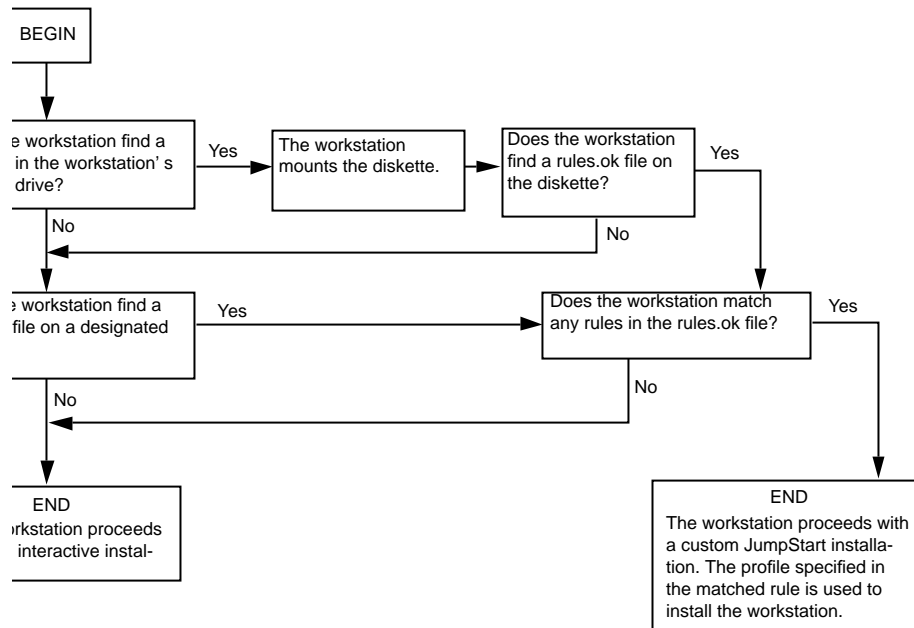


Figure 8–1 What Happens During a Custom JumpStart Installation

The following figure shows an example of how a custom JumpStart installation works on a standalone, non-networked workstation using the workstation's diskette drive.

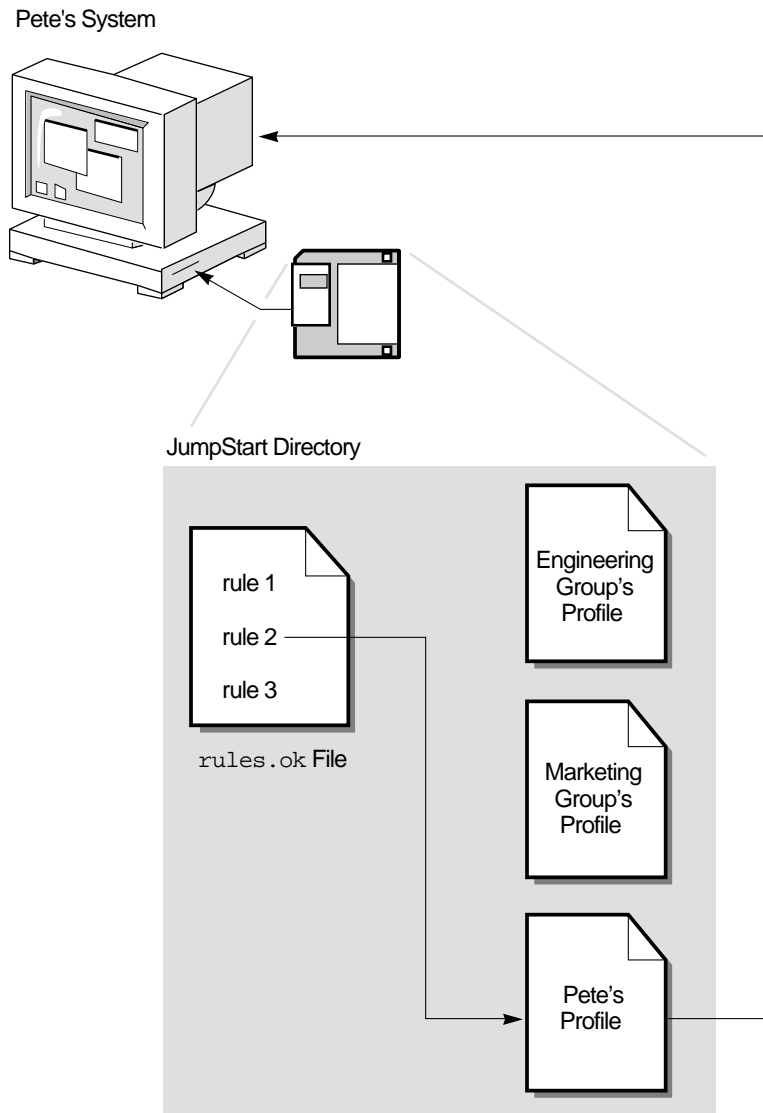


Figure 8-2 How a Custom JumpStart Installation Works: Non-Networked Example

Networked Custom JumpStart Installation

A networked custom JumpStart installation can install multiple workstations with different profiles from from a single server. For example, the JumpStart directory on the server can install workstations in the Engineering group differently from workstations in the Marketing group by using different profiles for machines in those

groups. A profile can also be set up for individual workstations, such as Alison's workstation or Pete's workstation.

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 SPARC workstation that has a diskette drive and a CDROM drive and assume the role root.**
2. **As root, at label `admin_low`, allocate the diskette drive.**

See “To Allocate a Device” on page 48 if you are unsure of the steps. The device should be allocated at the label `admin_low`, and *not* mounted.

```
Do you want floppy_0 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 on page 142.

If the `mount` command fails in Step 7 on page 142, the diskette does not have a UFS file system on it.

5. As root, at label `admin_low`, launch a terminal and format the diskette:

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

6. Create a file system on the diskette:

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

7. As role `admin`, at label `admin_low`, 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 on page 142 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	<ol style="list-style-type: none"> 1. As root, create a mount point at <code>admin_low</code>. For example: <code>mkdir /cdrom</code> 2. Insert the Trusted Solaris CD into the CDROM drive. 3. Go to Step 9 on page 143.
Trusted Solaris CD image on the local disk	<ol style="list-style-type: none"> 1. Change the directory to the Trusted Solaris CD image on the local disk. For example: <code>cd /export/install/ts7_sparc</code> 2. Do Step 11 on page 143.

9. As root, at label `admin_low`, allocate the CDROM drive and mount it.

```
Do you want cdrom_0 mounted: (y,n)? y
```

10. Change the directory to the mounted CD:

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

11. Copy the custom JumpStart installation files from the `jumpstart_sample` directory into the JumpStart directory (root directory) of the diskette:

```
# cp -r Trusted_Solaris_7/Misc/jumpstart_sample/* jumpstart_dir_path
```

- *jumpstart_dir_path* is the absolute directory path where the diskette is mounted.
- The custom JumpStart installation files must be in the root directory of the diskette.

12. Deallocate the CDROM drive and the diskette drive. Label the diskette.

See “To Deallocate a Device” on page 49 if you are unsure of the steps.

You have completed creating a JumpStart directory on the diskette. To continue, see “How to Create a Profile” on page 149.

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.**
2. **As root, at label `admin_low`, 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
```

3. **Share the directory.**

For details, see “How to Share a File System” on page 61.

- 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 on page 144:

```
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	<ol style="list-style-type: none">1. As root, create a mount point at admin_low. For example: mkdir /cdrom2. Insert the Trusted Solaris CD into the CDROM drive.3. Go to Step 6 on page 145.
Trusted Solaris CD image on the local disk	<ol style="list-style-type: none">1. Change the directory to the Trusted Solaris image on the local disk. For example: cd /export/install/ts7_sparc2. Do Step 8 on page 145.

6. **As root, at label admin_low, allocate the CDROM drive and mount it.**

```
Do you want cdrom_0 mounted: (y,n)? y
```

See “To Allocate a Device” on page 48 if you are unsure of the steps.

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

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

8. **As root, at label admin_low, copy the contents of the jumpstart_sample directory into the JumpStart directory:**

```
# cp -r Trusted_Solaris_7/Misc/jumpstart_sample/* jumpstart_dir_path
```

For example, the following command would copy the `jumpstart_sample` directory into the JumpStart directory created in Step 2 on page 144:

```
# cp -r Trusted_Solaris_7/Misc/jumpstart_sample/* /jumpstart
```

9. Deallocate the CDROM drive.

See “To Deallocate a Device” on page 49 if you are unsure of the steps.

You have completed creating a JumpStart directory on the server.

10. Continue with “Enabling Access to the JumpStart Directory” on page 146.

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 126. 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.

Method 1: Host Manager

1. **As role `admin`, at label `admin_low`, 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 126 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. **Choose File > Save Changes.**

When you save the entry, the Host Manager places the information in the `bootparams` database.

4. Repeat for all hosts to be installed with custom JumpStart, then exit the Host Manager.
5. As role `admin`, at label `admin_low`, launch the Database Manager using the same naming service you did for setting up network install.
6. Load the `bootparams` database.
7. 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. As root, at label `admin_low`, go to “Add Client Information with the `add_install_client` Command” on page 128.
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 \
host_name platform_group
```

In this command,

<code>-c</code>	Specifies a JumpStart directory for custom JumpStart installations. This option and its arguments are required for custom JumpStart.
<code>server:jumpstart_dir_path</code>	<code>server</code> is the host name of the server on which the JumpStart directory is located. <code>jumpstart_dir_path</code> is the absolute path of the JumpStart directory.

For example, issuing the following command on an install/boot server modifies the local `bootparams` database to look for custom JumpStart information in the `stork:/jumpstart` directory.:

```
# ./add_install_client -e 8:0:20:17:22:a4 \  
-c stork:/jumpstart \  
-s heron:/export/install/ts7_sparc willet sun4m
```

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 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, as role admin at label `admin_low`, edit the bootparams database.**

For details, see “To Open and Modify a Solstice_Apps Database” on page 51.

2. **Scroll through a host’s entry to locate the keyword=value pairs:**

```
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 pair in the same workstation’s bootparams entry would enable it to access the Trusted Solaris installation image on `heron`.

Together, these keyword=value pairs enable custom JumpStart:

```
install_server=heron:/export/install/ts7_sparc
```

All workstations can now access the JumpStart directory.

3. **Continue with “Creating a Profile” on page 149.**

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 following profile keyword and value indicate to the Trusted Solaris installation program to install the workstation as a server.

```
system_type server
```

Note - If you created the JumpStart directory by using the procedures on “Creating a JumpStart Directory on a Diskette ” on page 141 or “Creating a JumpStart Directory on a Server” on page 144, 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 the following task:

- Automatically reboot the workstation. See the example in “Rebooting the Workstation with a Finish Script” on page 180.

For an example of a rule that calls a finish script, see “Recommendations for Trusted Solaris Rules” on page 161.

▼ 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.

1. As root, at label `admin_low`, open the 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 150 provides some examples of profiles.
- “Profile Keyword and Profile Value Descriptions” on page 152 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 183 for detailed information about testing profiles.

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 161.

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 “Profile Keyword and Profile Value Descriptions” on page 152 for the list of profile keywords and profile values.

```
# profile keywords      profile values
# -----
```

install_type	initial_install
system_type	standalone
partitioning	default
filesystem	any 80 swap # specify size of /swap
cluster	SUNWCprog
package	SUNWman delete
package	SUNWolman delete
package	SUNWxwman delete
package	SUNWxdem add
package	SUNWxdim add

1. This profile keyword is required in every profile.
2. This profile keyword defines that the workstation will be installed as a standalone workstation.
3. 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).
4. The developer software group (SUNWCprog) is installed on the workstation.
5. 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
partitioning	default
filesystem	c0t0d0s0 auto /
filesystem	c0t3d0s1 64 swap
cluster	SUNWCall

1. 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.
2. The entire distribution software group (SUNWCall) is installed on the workstation.

# profile keywords	profile values
# -----	-----
install_type	initial_install
system_type	standalone
fdisk	c0t0d0 0x04 delete
fdisk	c0t0d0 solaris maxfree
cluster	SUNWCall
cluster	SUNWCacc delete

1. All fdisk partitions of type DOSOS16 (04 hexadecimal) are deleted from the c0t0d0 disk.

2. A Trusted Solaris fdisk partition is created on the largest contiguous free space on the c0t0d0 disk.
3. The entire distribution software group (SUNWCall) is installed on the workstation.
4. The system accounting utilities (SUNWCacc) are selected *not* to be installed on the workstation.

# profile keywords	profile values
# -----	-----
install_type	upgrade
package	SUNWbcp delete
package	SUNWolman add
package	SUNWxwman add
cluster	SUNWCumux add
locale	de

1. This profile upgrades a system (SPARC only).
2. The binary compatibility package (SUNWbcp) is selected to be deleted from the system or prevented from being installed.
3. This code ensures that the OpenLook and X Windows man pages and the universal multiplexor software are selected to be installed if they are not installed on the system. (All packages already on the system are automatically upgraded.)
4. The German localization packages are selected to be installed on the system.

Profile Keyword and Profile Value Descriptions

Profile keywords and profile values that you can use in a profile are listed and described below.

Profile Keyword and Profile Value Descriptions

`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 *Solaris 7 Sun Hardware Platform Guide* 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`.

`cluster`

group_name

Use for software groups. `cluster` designates what software group to add to the workstation. The cluster names for the software groups are:

- End user system support: `SUNWCuser`
- Developer system support: `SUNWCprog`
- Entire distribution: `SUNWCall`

You can specify only one software group in a profile, and it must be specified before other `cluster` and `package` entries. If you do not specify a software group with `cluster`, the end user software group (`SUNWCuser`) is installed on the workstation by default.

cluster

cluster_name [add | delete]

Use for clusters.

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 *SUNWCname*.

For Upgrade (not supported for Trusted Solaris 7):

- All clusters already on the system are automatically upgraded.
- If you specify *cluster_name add*, and *cluster_name* is not installed on the system, the cluster is installed.
- If you specify *cluster_name delete*, and *cluster_name* is installed on the system, the package is deleted before the upgrade begins.

dontuse

disk_name

dontuse designates a disk that the Trusted Solaris installation program should not use when partitioning default is specified. You can specify *dontuse* once for each disk, and *disk_name* must be specified in the form *cxydz* or *cydz*, 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.

filesys

slice size [*file_system*] [*optional_parameters*]

Use for creating local file systems.

This instance of *filesys* creates local file systems during the installation. You can specify *filesys* more than once.

slice - Choose one of the following:

<code>any</code>	<p>The Trusted Solaris installation program places the file system on any disk.</p> <p>Restriction: <code>any</code> cannot be specified when size is <code>existing</code>, <code>all</code>, <code>free</code>, <i><code>start:size</code></i>, or <code>ignore</code>.</p>
<code>cwtxdysz</code> or <code>cwdysz</code>	<p>The disk slice where the Trusted Solaris installation program places the file system, for example, <code>c0t0d0s0</code>.</p>
<code>rootdisk.sn</code>	<p>The logical name of the disk where the installation program places the root file system. The <code>.sn</code> suffix indicates a specific slice on the disk.</p>

size - Choose one of the following:

<i>num</i>	<p>The size of the file system is set to <i>num</i> (in Mbytes).</p>
<code>existing</code>	<p>The current size of the existing file system is used.</p> <p>Note: When using this value, you can change the name of an existing slice by specifying <i>file_system</i> as a different <i>mount_pt_name</i>.</p>
<code>auto</code>	<p>The size the file system is automatically determined depending on the selected software.</p>
<code>all</code>	<p>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.</p>
<code>free</code>	<p>The remaining unused space on the disk is used for the file system.</p> <p>Restriction: If <code>free</code> is used as the value to <code>filesys</code>, it must be the last <code>filesys</code> entry in a profile.</p>

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.

file_system - You can use this optional value when *slice* is specified as *any* or *cwtxdysz*. If *file_system* is not specified, *unnamed* is set by default, but then you cannot specify the *optional_parameters* value. Choose one of the following:

mount_pt_name The file system's mount point name, for example, */var*.

swap The specified slice is used as swap.

overlap The specified slice is defined as a representation of a disk region (VTOC value is *V_BACKUP*). By default, slice 2 is an overlap slice that is a representation of the whole disk.

Restriction: *overlap* can be specified only when *size* is existing, *all*, or *start:size*.

unnamed The specified slice is defined as a raw slice, so *slice* will not have a mount point name. If *file_system* is not specified, *unnamed* is set by default.

ignore The specified slice is not used or recognized by the Trusted Solaris installation program. This could be used to ignore a file system on a disk during an installation, so the Trusted Solaris installation program can create a new file system on the same disk with the same name.

optional_parameters - Choose one of the following:

preserve The file system on the specified slice is preserved.

Restriction: *preserve* can be specified only when *size* is existing and *slice* is *cwtxdysz*.

mount_options One or more mount options (*-o* option of the *mount(1M)* 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`.

<code>install_type</code>	<p><code>initial_install</code> <code>upgrade</code></p> <p><code>install_type</code> defines whether to perform the initial installation option or upgrade option on the system. (Upgrade is not supported for Trusted Solaris 7).</p> <p>Restriction: <code>install_type</code> must be the first profile keyword in every profile.</p>
<code>locale</code>	<p><i>locale_name</i></p> <p><code>locale</code> 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 <code>\$LANG</code> environment variable.</p> <p>The English localization packages are installed by default. You can specify <code>locale</code> once for each localization you need to support.</p>
<code>num_clients</code>	<p><i>client_num</i></p> <p>When a server is installed, space is allocated for each diskless client's root (<code>/</code>) and swap file systems. <code>num_clients</code> defines the number of diskless clients (<i>client_num</i>) that a server will support. If you do not specify <code>num_clients</code>, five diskless clients are allocated.</p> <p>Restriction: <code>num_clients</code> can be used only when <code>system_type</code> is specified as <code>server</code>.</p>
<code>package</code>	<p><i>package_name</i> [<code>add</code> <code>delete</code>]</p> <p><code>package</code> designates whether a package should be added to or deleted from the software group that will be installed on the workstation. <code>add</code> or <code>delete</code> indicates whether the package should be added or deleted. If you do not specify <code>add</code> <code>delete</code>, the package is added.</p> <p><i>package_name</i> must be in the form <code>SUNWname</code>. Use the <code>pkginfo -l</code> command on an installed workstation to</p>

view detailed information about packages and their names.

For Upgrade (not supported for Trusted Solaris 7):

- 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.

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 `cwtxdy` or `cwdy`, 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. The following table shows how the maximum size of swap is determined during a custom JumpStart installation.

TABLE 8-2 How the Maximum Size of Swap Is Determined

Physical Memory (in Mbytes)	Maximum Size of Swap (in Mbytes)
32 - 64	64
64 - 128	64

TABLE 8-2 How the Maximum Size of Swap Is Determined (continued)

Physical Memory (in Mbytes)	Maximum Size of Swap (in Mbytes)
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 8-2.

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 “Creating a JumpStart Directory on a Diskette ” on page 141 or “Creating a JumpStart Directory on a Server” on page 144, 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 “Rule Keyword and Rule Value Descriptions” on page 165). 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 180. 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.

1. As secadmin, at label `admin_low`, open the Admin Editor.

See “To Create or Open a File from the Trusted Editor” on page 57 if you are unfamiliar with the steps.

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 163 provides some examples of rules.
- “Rule Keyword and Rule Value Descriptions” on page 165 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
```

The fields of a rule are described below:

Field Descriptions of a Rule

!	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.
&&	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.
<i>rule_keyword</i>	A predefined keyword that describes a general system attribute, such as host name (<code>hostname</code>) or memory size (<code>memsize</code>). It is used with the <code>rule_value</code> to match a workstation with the same attribute to a profile. See “Rule Keyword and Rule Value Descriptions” on page 165 for the list of <code>rule</code> keywords.
<i>rule_value</i>	A value that provides the specific system attribute for the corresponding <code>rule</code> keyword. See “Rule Keyword and Rule Value Descriptions” on page 165 for the list of <code>rule</code> values.

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 177 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 198 and “Creating Derived Profiles With Begin Scripts” on page 178.

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 179 for detailed information on how to create finish scripts.

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 172.

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 values  begin script  profile      finish script
# -----
hostname eng-1                  -            basic_prof  -
```

```

network 192.43.34.0 && !model \
'SUNW,Sun 4_50' - net_prof -
model SUNW,SPARCstation-LX - lx_prof complete
network 193.144.2.0 && karch sparc setup ultra_prof done
any - generic_prof -

```

1. 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.
2. 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.
3. 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 "Important Information About the `rules` File" on page 164.
4. 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.
5. 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 rule.

Important Information About the `rules` File

The following information is important to know about the `rules` file:

Name	The <code>rules</code> file <i>must</i> have the file name, <code>rules</code> .
<code>rules.ok</code> file	The <code>rules.ok</code> file is a generated version of the <code>rules</code> file, and it is required by the custom JumpStart installation software to match a workstation to a profile. You must run the <code>check</code> script to create the <code>rules.ok</code> file, and the <code>rules.ok</code> 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 <code>rules</code> 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

The rule keywords and rule values that you can use in the `rules` file are listed and described below.

Rule Keyword and Rule Value Descriptions

any

minus sign (-)

Match always succeeds.

arch

processor_type

Matches a workstation's processor type. The `uname -p` command reports the workstation's processor type.

For example, `SPARC` is a platform; `sparc` is a *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(1M)` command reports the workstation's domain name.

disksize

disk_name size_range

- *disk_name* — A disk name in the form `cxydz`, 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 Table 8-3.
- *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 less than 207 million bytes of disk space. The Trusted Solaris installation program will actually view the “207 Mbyte” disk as a 197 Mbyte disk because $207,000,000 / 1,048,576 = 197$. So, a “207 Mbyte” disk would not match a *size_range* equal to 200-210.

hostaddress

IP_address

Matches a workstation's IP address.

hostname

host_name

Matches a workstation's host name.

If you have a workstation already installed, the `uname -n` command reports the host name.

installed

slice version

- *slice* - A disk slice name in the form `cwtxdysz`, such as `c0t3d0s5`, or the special words `any` or `rootdisk`. If `-any` is used, any disk attached to the workstation attempts to match. `rootdisk` should be used only when trying to match workstations that contain the factory-installed JumpStart software. `rootdisk` is described on Table 8-3.
- *version* - A version name, such as `Trusted_Solaris_7`, 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 may not be supported by Trusted Solaris software.

`karch`

platform_group

Matches a workstation's platform name.

Valid values are `sun4d`, `sun4c`, `sun4m`, and `sun4u`. (See *Solaris 7 Sun Hardware Platform Guide*.)

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

Matches a workstation's physical memory size (in Mbytes). The value must be a range of Mbytes (`xx-xx`) or a single Mbyte value.

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(1M)` command reports the workstation's physical memory size in line 2. Run the command in the role `admin`.

`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 reports the workstation's model number in line 5.

If you have a workstation already installed, the `uname -i` command reports the workstation's model name.

For example, a system name is different from a *model_name*:

System Name	Model Name
SPARCstation 1 (4/60)	Sun 4_60
SPARCstation IPX (4/50)	SUNW,Sun_4_50
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 Voyager	SUNW,S240
Sun Ultra™ 1	SUNW,Ultra-1
Sun UltraServer 1	SUNW,Ultra-1
Sun UltraServer 2	SUNW,Ultra-2

Note: If the *model_name* contains spaces, the *model_name* must be inside a pair of single quotes ('). For example:
'SUNW,Sun 4_60'

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 software already installed on a workstation. *Trusted_Solaris_version* is the version of the Trusted Solaris environment installed on the workstation: for example, Trusted Solaris 2.5.1.

totaldisk

size_range

Matches the total disk space on a workstation (in Mbytes). The total disk space includes all the operational disks attached to a workstation. The value must be specified as a range of Mbytes (xx-xx).

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 the following table.

TABLE 8-3 How the Trusted Solaris Installation Program Sets `rootdisk`

Situation	What Happens
A system contains the factory-installed JumpStart software. (This applies to some SPARC systems only).	<code>rootdisk</code> is set to the disk that contains the factory-installed JumpStart software before the system tries to match any rules.
<code>rootdisk</code> has <i>not</i> been set and a workstation tries to match the following rule:	<code>rootdisk</code> is set to <code>c0t3d0</code> or the first available disk attached to the workstation.
<code>disksize rootdisk size_range</code>	After <code>rootdisk</code> is set, the workstation tries to match the rule.
or	
<code>installed rootdisk version</code>	

TABLE 8-3 How the Trusted Solaris Installation Program Sets rootdisk *(continued)*

Situation	What Happens
<p>If <code>rootdisk</code> has been set and the workstation tries to match the following rule.</p> <p><code>disksize rootdisk <i>size_range</i></code></p> <p>or</p> <p><code>installed rootdisk <i>version</i></code></p>	<p>The workstation tries to match the rule.</p>
<p>A workstation tries to match the following rule:</p> <p><code>installed <i>disk version</i></code></p>	<p>If <i>disk</i> is found on the workstation with a root file system that matches the specified <i>version</i>, the rule matches and <code>rootdisk</code> is set to <i>disk</i>.</p>
<p>A workstation tries to match the following rule:</p> <p><code>installed any <i>version</i></code></p>	<p>If any disk is found on the workstation with a root file system that matches the specified <i>version</i>, the rule matches and <code>rootdisk</code> 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.)</p>
<p><code>rootdisk</code> has not been set after a system matches a rule and the system is going to be upgraded (which is defined in the profile).</p>	<p><code>rootdisk</code> is set to the first disk found with a root file system that matches an upgradable version of Trusted Solaris software. If no disk is found, the system proceeds with an interactive installation.</p>
<p><code>rootdisk</code> has not been set after a workstation matches a rule.</p>	<p><code>rootdisk</code> is set to <code>c0t3d0</code> or the first available disk attached to the workstation.</p>

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(1M)` command to validate that these files are set up correctly. The check script performs the following steps:

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 the `check` command 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.

1. As root, at label `admin_low`, make sure that the `check` script resides in the JumpStart directory.

Note - The `check` script is provided in the `jumpstart_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 7 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. **As root, at label `admin_low`, 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 141 for the procedure.

```
# cd jumpstart_dir_path
```

2. **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
```

3. Check file permissions.

File or Directory	Owner	Permissions	Label
<i>jumpstart_dir_path</i>	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]

4. As root, at label `admin_low`, 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 124
- “Set the Default Date and Time” on page 125
- “Add Client Information for a Network Install” on page 126
- “How to Create a JumpStart Directory on a Server” on page 144 or “How to Create a JumpStart Directory on a Diskette” on page 141
- “How to Enable Access to the JumpStart Directory” on page 146
- “How to Create a Profile” on page 149
- “How to Create the rules File” on page 161

- “Copy JumpStart Files to jumpstart_dir_path” on page 173

To read about the optional features available for custom JumpStart installations, see Chapter 9.

To install a workstation using custom JumpStart, use the appropriate booting procedure in Chapter 3.

Using Optional Custom JumpStart Features

- “How to Use `pfinstall` to Test a Profile” on page 183
- “SPARC: How to Create a Disk Configuration File for a SPARC System” on page 186
- “IA: How to Create a Disk Configuration File on Intel Architecture” on page 190
- “SPARC: How to Create a Multiple Disk Configuration File for a SPARC System” on page 188
- “IA: How to Create a Multiple Disk Configuration File on Intel Architecture” on page 194

This chapter describes the optional features available for custom JumpStart installations, and it is a supplement to Chapter 8. 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.

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
- Adding entries to the automount map

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.

- ◆ **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:

▼ Create a Finish Script to Add Files after Installation

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 `jumpstart_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
PASSWD=dKO5IBkSF42lw
#create a temporary input file
cp /a/etc/shadow /a/etc/shadow.orig

mv /a/etc/shadow /a/etc/shadow.orig
nawk -F: '{
  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
#remove the temporary file
rm -f /a/etc/shadow.orig
# 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.

▼ Create a Finish Script to Set the root Password

1. **Set the variable `PASSWD` to an encrypted root password obtained from an existing entry in a workstation's `/etc/shadow` file.**
2. **Create a temporary input file of `/a/etc/shadow`.**
3. **Change the root entry in the `/etc/shadow` file for the newly installed workstation using `$PASSWD` as the password field.**

4. 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

The procedure to use `pfinstall` to test a profile involves testing the command in the JumpStart directory.

1. On an installed and configured Trusted Solaris workstation, log in as a user who can assume the role root.

2. As root at label `admin_low`, 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 profiles. 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:

```
$ /usr/sbin/install.d/pfinstall -D | -d disk_config [-c path] 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.

In this command,

<code>-D</code>	Tells <code>pfinstall</code> to use the current workstation's disk configuration to test the profile against. You must be in the role <code>root</code> to execute <code>pfinstall</code> with the <code>-D</code> option.
<code>-d <i>disk_config</i></code>	Tells <code>pfinstall</code> to use a disk configuration file, <i>disk_config</i> , to test the profile against.
<code>-c <i>path</i></code>	Is the path to the Trusted Solaris CD. This is required if the Trusted Solaris CD is not mounted on <code>/cdrom</code> . (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 <code>/cdrom</code>).
<i>profile</i>	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 Step 5 on page 184.

You have completed testing the profile. To perform a custom JumpStart installation on a workstation, see Chapter 3.

pfinstall Examples

Below are some examples of using `pfinstall(1M)` 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/ts7_sparc -basic_prof
```

▼ SPARC: 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` 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 `prtvtoc(1M)` workstation with a disk that you want to test a profile against
- Using the 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.**
3. **As root at label `admin_low`, 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/rdisk/device_name > disk_config
```

In this command,
`/dev/rdisk/device_name`

Is the device name of the workstation's disk.
device_name must be in the form `cwtxdys2` or `cwdys2`.

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
```

You have completed 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/rdisk/c0t3d0s2 > 104_test
```

In this example, the 104_test file contains the following information:

```
# cat 104_test
* /dev/rdisk/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
```

▼ SPARC: 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
* /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
```

(continued)

```

*
*
*           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
* /dev/rdisk/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

```

(continued)

6	4	01	44310	160230	204539
---	---	----	-------	--------	--------

Because `dual_104_test` file was created by concatenating itself, the following editing was required:

- The first disk device name was left as is.
- The second disk device name was changed from `/dev/rdisk/c0t3d0s2` to `/dev/rdisk/c0t0d0s2` so it has a unique target number.

You have completed creating a multiple disk configuration file.

IA: Creating a Disk Configuration File on Intel Architecture

The following procedures enable you to use the `-d` option of the `pfinstall` command to test custom JumpStart installations for Intel architecture.

▼ IA: How to Create a Disk Configuration File on Intel Architecture

A disk configuration file represents a disk structure (for example, bytes/sectors, flags, slices), and it enables you to use `pfinstall` from a single system to test profiles against different sized disks. Disk configuration files for an Intel architecture system must also contain information about a disk's `fdisk` partitions.

Overview – Creating a disk configuration file for an Intel architecture system involves:

- Locating an Intel architecture system with a disk that you want to test a profile against
- Saving the output of the `prtvtoc` command to a file
- Saving the output of the `fdisk` command to a file
- Concatenating the two files to create a disk configuration file

Follow this procedure to create a disk configuration file for an Intel architecture system:

1. Locate an Intel architecture system with a disk that you want to test a profile against.
2. Determine the device name for the system's disk.
3. Redirect the output of the following `prtvtoc` command to a file:

```
# prtvtoc /dev/rdisk/device_name > file1
```

where `/dev/rdisk/device_name` is the device name of the system's disk, and `file1` is the file that contains the output of the `prtvtoc` command. `device_name` must be in the form `cwtxdyp0` or `cxryp0`. Partition 0 must be specified in `device_name`.

4. Save the output of the following `fdisk` command to a file:

```
# fdisk -R -d -n /dev/rdisk/device_name 2>file2
```

Note - This version of the `fdisk` command may not be supported in the next release.

where `/dev/rdisk/device_name` is the device name of the system's disk. `file2` is the file that contains the output of the `fdisk` command. `device_name` must be in the form `cwtxdyp0` or `cxryp0`. Partition 0 must be specified in `device_name`.

5. Concatenate the two files to create a disk configuration file:

```
# cat file1 file2 > disk_config
```

Note - The output of the `prtvtoc` command must be first in a disk configuration file for an Intel architecture system.

6. Copy the disk configuration file to the JumpStart directory:

```
# cp disk_config jumpstart_dir_path
```

You have created a disk configuration file for an Intel architecture system. The following page provides an example of creating a disk configuration file. This example creates a disk configuration file, `500_test`, on an Intel architecture system with a 500-Mbyte disk.

First, you would save the output of the prtvtoc command to a file:

```
# prtvtoc /dev/rdisk/c0t0d0p0 > output1
```

The output1 file is shown as follows:

```
* /dev/rdisk/c0t0d0p0 partition map
*
* Dimensions:
*   512 bytes/sector
*   79 sectors/track
*   7 tracks/cylinder
*   553 sectors/cylinder
*   1481 cylinders
*   1479 accessible cylinders
*
* Flags:
*   1: unmountable
*   10: read-only
*
*
* Partition  Tag  Flags      First      Sector      Last
* Partition  Tag  Flags      Sector    Count      Sector  Mount Directory
*   0         2    00         553    194103    194655
*   1         3    01    194656     65807    260462
*   2         6    00         0     819546    819545
*   3         6    00    260463     50876    311338
*   4         6    00    311339     72996    384334
*   6         4    00    384335    434105    818439
*   8         1    01         0         553         552
```

Second, you would save the output of the fdisk command to a different file:

```
# fdisk -R -d -n /dev/rdisk/c0t0d0p0 2>output2
```

The output2 file is shown as follows:

```
fdisk physical geometry:
cylinders[1855] heads[7] sectors[79] sector size[512] blocks[1025815] mbytes[500]

fdisk virtual (HBA) geometry:
cylinders[500] heads[64] sectors[32] sector size[512] blocks[1024000] mbytes[500]

fdisk table on entry:

SYSID ACT BHEAD BSECT BEG CYL    EHEAD ESECT ENDCYL    RELSECT    NUMSECT
6      0   1     1     0      63    32    99      32      204768
```

(continued)

130	128	0	1	100	63	96	243	204800	819200
100	0	0	0	0	0	0	0	100	100
100	0	0	0	0	0	0	0	100	100

Finally, you would concatenate the two files (output1 and output2) together to create the disk configuration file named 500_test.

```
# cat output1 output2 > 500_test
```

The 500_test file is shown as follows:

```
* /dev/rdisk/c0t0d0p0 partition map
*
* Dimensions:
*   512 bytes/sector
*   79 sectors/track
*   7 tracks/cylinder
*   553 sectors/cylinder
*   1481 cylinders
*   1479 accessible cylinders
*
* Flags:
*   1: unmountable
*  10: read-only
*
*
*           First   Sector   Last
* Partition Tag  Flags   Sector   Count   Sector Mount Directory
*   0      2   00      553   194103  194655
```

(continued)

1	3	01	194656	65807	260462
2	6	00	0	819546	819545
3	6	00	260463	50876	311338
4	6	00	311339	72996	384334
6	4	00	384335	434105	818439
8	1	01	0	553	552

fdisk physical geometry:

cylinders[1855] heads[7] sectors[79] sector size[512] blocks[1025815] mbytes[500]

fdisk virtual (HBA) geometry:

cylinders[500] heads[64] sectors[32] sector size[512] blocks[1024000] mbytes[500]

fdisk table on entry:

SYSID	ACT	BHEAD	BSECT	BEGCYL	EHEAD	ESECT	ENDCYL	RELSECT	NUMSECT
6	0	1	1	0	63	32	99	32	204768
130	128	0	1	100	63	96	243	204800	819200
100	0	0	0	0	0	0	0	100	100
100	0	0	0	0	0	0	0	100	100

▼ IA: How to Create a Multiple Disk Configuration File on Intel Architecture

If you need to test a profile on multiple disks, you can concatenate disk configuration files together to create multiple disk configuration scenarios.

Creating a multiple disk configuration file for an Intel architecture system involves:

- Concatenating two or more disk configuration files to create a multiple disk configuration file
- Changing the target numbers of disks in the multiple disk configuration file

Note - Disk device target numbers must be unique on a system.

The following procedure creates a multiple disk configuration file. (The procedure uses the 500_test file from the previous procedure.)

1. Concatenate a disk configuration file with itself and save it to a file.

The new file becomes the multiple disk configuration file. For example, the following command creates a multiple disk configuration file named dual_500_test:

```
$ cat 500_test 500_test > dual_500_test
```

2. Edit the disk configuration file so that each disk device name has a different target number.

The dual_500_test file is shown as follows:

```
* /dev/rdisk/c0t0d0p0 partition map
*
* Dimensions:
*   512 bytes/sector
*   79 sectors/track
*   7 tracks/cylinder
*   553 sectors/cylinder
*   1481 cylinders
*   1479 accessible cylinders
*
* Flags:
*   1: unmountable
*  10: read-only
*
*
*           First      Sector      Last
* Partition Tag  Flags   Sector      Count      Sector  Mount Directory
0         2    00      553    194103    194655
```

(continued)

```

1      3      01      194656      65807      260462
2      6      00           0      819546      819545
3      6      00      260463      50876      311338
4      6      00      311339      72996      384334
6      4      00      384335      434105      818439
8      1      01           0        553        552

fdisk physical geometry:
cylinders[1855] heads[7] sectors[79] sector size[512] blocks[1025815] mbytes[500]

fdisk virtual (HBA) geometry:
cylinders[500] heads[64] sectors[32] sector size[512] blocks[1024000] mbytes[500]

fdisk table on entry:

SYSID ACT BHEAD BSECT BEG CYL    EHEAD ESECT ENDCYL    RELSECT    NUMSECT
6      0   1     1     0        63    32    99        32        204768
130    128 0     1    100       63    96   243       204800    819200
100    0   0     0     0         0     0     0        100        100
100    0   0     0     0         0     0     0        100        100

* /dev/rdsk/c0t1d0p0 partition map
*
* Dimensions:
*      512 bytes/sector
*      79 sectors/track
*      7 tracks/cylinder
*      553 sectors/cylinder
*      1481 cylinders
*      1479 accessible cylinders
*

```

(continued)

```

* Flags:
*   1: unmountable
*  10: read-only
*
*
*           First      Sector      Last
* Partition Tag  Flags   Sector      Count      Sector  Mount Directory
0         2    00        553    194103    194655
1         3    01    194656     65807    260462
2         6    00          0    819546    819545
3         6    00    260463     50876    311338
4         6    00    311339     72996    384334
6         4    00    384335    434105    818439
8         1    01          0      553      552

fdisk physical geometry:
cylinders[1855] heads[7] sectors[79] sector size[512] blocks[1025815] mbytes[500]

fdisk virtual (HBA) geometry:
cylinders[500] heads[64] sectors[32] sector size[512] blocks[1024000] mbytes[500]

fdisk table on entry:
SYSID ACT BHEAD BSECT BEGCVL   EHEAD ESECT ENDCYL   RELSECT   NUMSECT
6      0   1    1     0      63   32    99      32      204768
130    128 0    1    100     63   96   243     204800  819200
100    0   0    0     0      0    0    0      100     100
100    0   0    0     0      0    0    0      100     100

```

Because the dual_500_test file was created by concatenating itself, it required editing as follows:

The first disk device name was left as is

The second disk device name was changed from `/dev/rdisk/c0t0d0p0` to `/dev/rdisk/c0t1d0p0` so it has a unique target number.

You have created a multiple disk configuration file for an Intel architecture system.

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

Configuring a diskless client for Trusted Solaris software is similar to configuring them for the Solaris 7 environment. The *Solstice AdminSuite 2.3 Administration Guide* lists the procedures. 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

- ♦ **Choose the OS server system type during installation, and configure disk space for diskless clients.**

- “System Installation Step by Step” on page 70

Path 2 - Convert Standalone to OS Server

The workstation must have disk space for clients. 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`.

1. **Choose the Standalone system type during installation and leave room (or add disks) for diskless clients.**
2. **Add the (still Standalone) workstation to the NIS+ network:**
 - Chapter 6

▼ 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.**

Either:

- ♦ **Follow the procedure “Create an Install Server” on page 124.**

This will copy the Trusted Solaris CD image to one of the OS server's hard disks.

Or:

- ♦ **As root, at label `admin_low`, mount a Trusted Solaris CD image that has been copied to an install server:**

1. **Add the file systems to be mounted to the file `/etc/vfstab`.**

For example,

```
heron:/export/install/ts7_sparc - /export/install/ts7_sparc nfs - yes bg,intr,soft
```


2. As role **admin**, at label **admin_low**, create a mount point for the file system to be mounted.

```
$ mkdir -p /export/install/ts7_sparc
```

3. Mount the file system.

```
# mount /export/install/ts7_sparc
```

▼ Add OS Services

1. On the workstation that is going to be the OS server, as role **admin** at label **admin_low**, open the **Host Manager** with the **NIS+ Naming Service**.
2. 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 4 on page 201.
3. 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 4 on page 201.
4. 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	<i>Do not select unless you plan to re-install the OS server over the network.</i>
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/ts7_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” on page 131

▼ 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.**
 2. **As role admin at label `admin_low`, open the Host Manager with the NIS+ Naming Service.**
1. **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	

TABLE 10-3 Diskless Client Information in Host Manager *(continued)*

System Type	Diskless
Timezone Region	
Timezone	
File Server	<i>(OS server is already entered for you.)</i>
OS Release	<i>Select the platform for the client.</i>
Root Path	/export/root
Swap Path	/export/swap
Swap Size	> 64 MB

2. 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.
2. As root, at label `admin_low`, 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
```

3. If the client is in the `tnrhdb` file correctly, but is not in the kernel cache, update the kernel.

```
# cd /etc/security/tsol
# tntctl -T tnrhtp
# tntctl -H tnrhdb
```

- 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, as root at label `admin_low`, open the Admin Editor from the `System_Admin` folder, with the file `/export/root/clientname/etc/vfstab`. You will do this once per client.

2. 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
```

3. Write the file and exit the editor.
4. As root, at label `admin_low`, 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, as root at label `admin_low`, 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.
2. 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
```

▼ Boot a Diskless Client

When booting for the first time, provide the client with a root password.

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...

Books in the Trusted Solaris document set and other reference books for setting up workstations are briefly described in “Related Books” on page 21 of this book. The following books contain information about configuration and maintenance.

For Further Configuration

To configure the AnswerBook2 server for access to Solaris and Trusted Solaris 7 AnswerBooks, see the *Trusted Solaris Documentation Roadmap*.

Trusted Solaris Administrator's Procedures, 805-8055-10, is the first book to check for configuration information on:

- Accessing devices
- Accessing remote files and workstations
- Adding and maintaining peripherals
- Adding workstations to a network
- Administering file systems
- Configuring printing
- Examining and changing security information
- Examining and changing system information
- Installing software
- Setting up disks (labeled)
- Setting up mail accounts
- Setting up printers

- Setting up system security
- Setting up user accounts
- Using crontabs
- Using system administration tools
- Using Trusted Solaris boot files

System Administration Guide, Volume I: Solaris 7, 805-3727-10 contains basic information, such as:

- Administering file systems
- Using boot files

System Administration Guide, Volume II: Solaris 7, 805-3728-10 contains advanced topics for system administrators:

- Examining and changing system information
- Increasing performance
- Managing disk use
- Setting up disks (unlabeled)
- Solaris system security
- Using crontabs (basic)

Solstice AdminSuite 2.3 Administration Guide, 805-3026-10, describes the tools in Solstice_Apps. They have been modified for Trusted Solaris, so see *Trusted Solaris Administrator's Procedures* and the CDE online help for the modifications.

CDE has been modified in the Trusted Solaris environment, so read the CDE online help and *Trusted Solaris Administrator's Procedures* for Trusted Solaris-specific information.

Site Security Policy

Each Trusted Solaris site is unique and must determine its own security policy. Perform the following tasks when creating and managing a security policy.

- Establish a security team. The security team should have representation from toplevel management, personnel management, computer system management and administrators, and facilities management. The team should review Trusted Solaris administrators' policies and procedures, and recommend general security policies that apply to all system users.
- Educate management and administration personnel about the site security policy. All personnel involved in the management and administration of the site should be educated about the security policy. Security policies should not be made available to ordinary users since this policy information has direct bearing on the security of the computer systems.
- Educate users about Trusted Solaris and the policy. All users must be familiar with the Trusted Solaris User's Guide. Because the users are usually the first to know when a system is not functioning normally, the user should become acquainted with the system and report any problems to a system administrator. A secure environment needs the users to notify the system administrators immediately if they notice:
 - A discrepancy in the last login time that is reported at the beginning of each session
 - An unusual change to file data
 - A lost or stolen human-readable printout
 - The inability to operate a user function
- Enforce the security policy. If the security policy is not followed and enforced, the data contained in Trusted Solaris will not be secure. Procedures should be established to record any problems and the measures that were taken to resolve the incidents.

- Review the security policy. The security team should perform a periodic review of the security policy and all incidents that occurred since the last review. Adjustments to the policy can then lead to increased security.

Site Security Policy and the Distributed System

The security administrator should design the distributed system based on the site's security policy. The security policy dictates configuration decisions regarding such things as:

- How much auditing will be done for all users in the system and for which classes of events
- How much auditing will be done for users in roles and for which classes of events
- How audit data will be managed, archived, and reviewed
- Which labels will be used in the system and whether the ADMIN_LOW and ADMIN_HIGH labels will be viewable by ordinary users
- Which user clearances will be assigned to individuals
- Which devices (if any) will be allocatable by which normal users
- Which label ranges are defined for machines, printers, and other devices
- Whether the Trusted Solaris system will be used in an evaluated configuration or in an extended configuration.

Computer Security Recommendations

The following list of guidelines provides some things to consider when developing a security policy for your site.

- The maximum label of the Trusted Solaris distributed system (the highest label in the user accreditation range) should not be greater than the maximum security level of work being done at the site.
- System reboots, power failures, and shutdowns should all be recorded manually in a site log.
- File-system damage should be documented and all affected files should be analyzed for potential security-policy violations.
- Operating manuals and administrator documentation should be restricted to individuals with a valid need for access to that information.

- Unusual or unexpected behavior of any Trusted Solaris software should be reported and documented, and the cause should be determined.
- If possible, at least two individuals should administer Trusted Solaris. One should be assigned security administrator authorization for security-related decisions, and the other should be assigned the system administrator authorization for computer management tasks.
- A regular backup routine should be established.
- Authorizations should be assigned only to users who need them and who can be trusted to use them properly.
- Privileges should be assigned to programs only when the program needs the privileges to do its work, and only when the programs have been scrutinized and proven to be trustworthy in their use of privilege. Review the privileges on existing Trusted Solaris programs for a guide to setting privileges on new programs.
- Audit information should be reviewed and analyzed regularly. Any irregular events should be noted and investigated to determine the cause of the event.
- The number of administration IDs should be minimized. The install user account should be disabled after an authorized security administrator user is established.
- The number of set user ID and set group ID programs should be minimized. Setuid/setgid programs should be employed only in protected subsystems.
- An administrator should regularly verify that normal users have a valid login shell.
- An administrator should regularly verify that normal users have valid user ID values and not system administration ID values.
- Consider TEMPEST shielded equipment and fiber-optic network cables to reduce electronic radiation emitted from computer equipment.
- Only certified technicians should open and close TEMPEST equipment to ensure its ability to shield electromagnetic radiation.

Physical Security Recommendations

- Restrict access to the Trusted Solaris system. The most secure locations are generally interior rooms that are not on the ground floor.
- Monitor and document access to Trusted Solaris.
- Secure computer equipment to large objects such as tables and desks to prevent theft. When equipment is secured to a wooden item, increase the strength of the item by adding metal plates.

- Consider removable storage media for sensitive information. Lock up all removable media when not in use.
- Store system backups and archives in a secure location separate from the location of the Trusted Solaris system.
- Restrict physical access to the backup and archival media in the same manner as access to the Trusted Solaris system.
- Install a high-temperature alarm in the computer facility to indicate when the temperature is outside of the range of the manufacturer's specifications. A suggested range is 10°C to 32°C (50°F to 90°F).
- Install a water alarm in the computer facility to indicate water on the floor, in the subfloor cavity, and in the ceiling.
- Install a smoke alarm to indicate fire.
- Install a fire-suppression system.
- Install a humidity alarm to indicate too much or too little humidity.
- Consider TEMPEST shielding if machines do not have it. TEMPEST shielding may be appropriate for facility walls, floors, and ceilings.
- Check for physical gaps that allow entrance to the facility or the rooms containing computer equipment. Look for openings under raised floors, in suspended ceilings, in roof ventilation equipment, and in adjoining walls between original and secondary additions.
- Prohibit eating, drinking, and smoking in computer facilities or near computer equipment. Establish areas where these activities can occur without threat to the computer equipment.
- Protect architectural drawings and diagrams of the computer facility.
- Restrict the use of building diagrams, floor maps, and photographs of the computer facility.

Personnel Security Recommendations

- Inspect packages, documents, and storage media entering and leaving a secure site.
- Require identification badges on all personnel and visitors at all times.
- Use identification badges that are difficult to copy or counterfeit.
- Establish areas that are prohibited for visitors and clearly mark the areas.
- Escort visitors at all times.

Common Security Violations

Because no computer is 100% secure, a computer facility is only as secure as the people who use it. The limitations of an administrator are directly related to the actions of all individuals involved with the use of computer equipment and its facilities. Although most actions that violate security are easily resolved by careful users or additional equipment, the following list gives examples of problems that can occur:

- Users give passwords to other individuals who should not have access to the computer system.
- Users write down passwords and lose or leave the passwords in nonsecure locations.
- Users set their passwords to easily guessed words or names.
- Users learn passwords by watching other users when they enter a password.
- Unauthorized users remove, replace, or physically tamper with hardware.
- Users leave their workstations or terminals unattended without locking the screen.
- Users change the permissions on a file to allow other users to read the file.
- Users change the labels on a file to allow other users to read the file.
- Users discard sensitive hardcopy documents without shredding them or leave sensitive hardcopy documents in insecure locations.
- Users leave access doors unlocked.
- Users lose their keys.
- Users do not lock up removable storage media.
- Computer screens are visible through exterior windows.
- Network cables are tapped.
- Electronic eavesdropping captures signals emitted from computer equipment.
- Power outages, surges, and spikes destroy data.
- Earthquakes, floods, tornadoes, hurricanes, and lightning destroy data.
- External electromagnetic radiation interference such as sun-spot activity scrambles files.

Additional Security References

As a trusted administrator, you should become familiar with the standards established by various government agencies. Government publications describe in

detail the standards, policies, methods, and terminology associated with computer security.

Other publications listed here are guides for system administrators of UNIX systems and are useful in gaining a thorough understanding of UNIX security problems and solutions. Some publications listed here describe successful attempts to penetrate computer systems around the world and illustrate real threats to computer security. These publications emphasize the importance of computer systems managed by knowledgeable and capable administrators.

U.S. Government Publications

Computer Security Requirements, Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments, DoD, CSC-STD-003-85, 1985.

Department of Defense Password Management Guideline, DoD, CSC-STD-002-85, 1985.

Department of Defense Trusted Computer System Evaluation Criteria (TCSEC)
National Computer Security Center, DoD 520.28-STD, 1985.

Graubart, Richard D., J.L. Berger, and John P.L. Woodward, *Compartmented Mode Workstations Evaluation Criteria, Version 1*, DIA DDS-2600-6243-91, Mitre, Bedford, Massachusetts, March 1991.

Personal Computer Security Considerations, National Computer Security Center, NCSC-WA-002-85, 1985.

Technical Rationale behind CSC-STD-003-85 Computer Security Requirements, Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments, DoD, CSC-STD-004-85, 1985.

Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria, National Computer Security Center, NCSC-TG-005 Version 1, 1987.

Woodward, John P.L., *Security Requirements for System High and Compartmented Mode Workstations*, DIA DDS-2600-5502-87, Mitre, Bedford, Massachusetts, November 1987.

UNIX Security Publications

Farrow, Rik, *UNIX System Security*, Addison-Wesley, Reading, MA, 1991.

Garfinkel, Simson, and Gene Spafford, *Practical UNIX Security*, O'Reilly & Associates, Inc., Sebastopol, CA, 1991.

Gregory, Peter, *Solaris Security*, Sun Microsystems Press, September 1999.

Hayes, Frank, "Is Your System Safe?" *UNIXWORLD*, June 1990.

Wood, Patrick H., and Stephen Kochan, *UNIX System Security*, Hayden Books, Indianapolis, IN, 1986.

General Computer Security Publications

Denning, Peter J., *Computers under Attack: Intruders, Worms and Viruses*, ACM Press, Addison-Wesley, Reading, MA, 1990.

Farrow, Rik, "Inside the Internet Worm," *UNIXWORLD*, June 1990.

Hafner, Katie, and John Markroff, *Cyberpunk: Outlaws and Hackers on the Computer Frontier*, Simon & Schuster, New York, NY, 1991.

Levy, Steven, *Hackers: Heroes of the Computer Revolution*, Dell Books, New York, NY, 1984.

McAfee, John, and C. Haynes, *Computer Viruses, Worms, Data Diddlers, Killer Programs, and Other Threats to Your System*, St. Martin's Press, New York, NY, 1989.

Page, Bob, "A Report on the Internet Worm," University of Lowell, Computer Science Department, November 1988.

Russell, Deborah, and G.T. Gangemi, Sr., *Computer Security Basics*, O'Reilly & Associates, Inc., Sebastopol, CA, 1990.

"Special Report: Computer Security and the Internet", *Scientific American*, October 1998. pp 95–117. Contains articles on hackers, firewalls, encryption, digital signatures, and Java, with extensive bibliographies.

Seeley, Donn, "A Tour of the Worm," University of Utah Department of Computer Science, Technical Report, November 1988.

Spafford, Eugene H., "The Internet Worm: Crisis and Aftermath," *Communications of the ACM*, June 1989.

Stoll, Cliff, *The Cuckoo's Egg*, Doubleday, Garden City, NY, 1989.

Thompson, Ken, "Reflections on Trusting Trust," 1983 ACM Turing Award Lecture, *Communications of the ACM*, August 1984.

General UNIX Publications

Bach, Maurice J., *The Design of the UNIX Operating System*, Prentice Hall, Englewood Cliffs, NJ, 1986.

Kobert, Jeannie Johnstone, *Guide To High Availability: Configuring boot/root/swap*, Sun Microsystems Press, September 1999.

Nemeth, Evi, Garth Snyder, and Scott Seebas, *UNIX System Administration Handbook*, Prentice Hall, Englewood Cliffs, NJ, 1989.

Winsor, Janice, *Solaris 7 Reference*, Sun Microsystems Press, September 1999.

Checklists for Configuring and Installing Trusted Solaris

The checklists are for planning and for reference. They provide an overall view of what to remember when installing and configuring the workstations at your site, and a record of doing so.

Site Summary Checklist

The following checklists summarize what you have done at your site. Where indicated, there are separate worksheets to plan particular site features, such as servers and labels.

Background Checklist

- Read *Trusted Solaris Administration Overview*.
- Understand site security requirements.
- Read Appendix A.

Checklist Summaries

Labels

See *Trusted Solaris Label Administration*. For highlights, see “Planning Labels” on page 220.

Network	See “Planning the Network” on page 221.
Auditing	See <i>Trusted Solaris Audit Administration</i> . For highlights, see “Planning Auditing” on page 222.
Workstations and Servers	See “Planning Workstations” on page 223.
First Users	See Table 5–1.
Administrative Roles	See “Update Role Credentials and Passwords” on page 101 for password and account locking considerations.
Users, Roles and Profiles	See <i>Trusted Solaris Administrator’s Procedures</i> .
Printers	See <i>Trusted Solaris Administrator’s Procedures</i> and “Planning Workstations” on page 223.

Planning Labels

Planning labels requires extensive knowledge. *Trusted Solaris Label Administration* describes in detail the modifications required to the `label_encodings` file you choose.

Label visibility exceptions are implemented per user when creating users.

Label visibility exceptions per workstation can be done but are not recommended. See *Trusted Solaris Label Administration* for why and how.

Note - When localizing a `label_encodings` file, localize the label names only. However, the names `ADMIN_HIGH` and `ADMIN_LOW` *must not* be localized. All labeled workstations that you contact must have label names that match the label names in the Trusted Solaris `label_encodings` file.

Label Decisions

- | | |
|---|--|
| Choose a <code>label_encodings</code> file | <ol style="list-style-type: none"> 1. GFI 2. Site-specific 3. Modified Trusted Solaris single-label 4. Modified Trusted Solaris multilabel |
|---|--|

Decide Trusted Solaris configuration	Create multiple user Sensitivity Labels — Yes, default ■ Hide upgraded names in directories — No, default
Decide label visibility	Visible to each user, default

Planning the Network

The first decision to make is whether to have an open network or a closed network.

Open Network Security Information

If the network is open:

- Identify accessible domains
- Identify accessible workstations
- Identify Trusted Solaris workstations that can access to unlabeled workstations or domains

NIS+ Domain Information

For the NIS+ domain:

1. Identify the NIS+ master
2. Identify the NIS+ replicas
3. Identify the NIS+ subdomain masters
4. Identify the the OS servers for diskless clients
5. Identify the file servers
6. Identify the audit servers
7. Identify the print servers
8. Identify the mail servers
9. Identify network routers/gateways
10. Identify end user workstations
11. Identify other workstations on the network

Labels of Communicating Machines

Identify the labels at which machines can communicate.

- Determine the label range of each workstation's network interfaces
- Determine the label(s) applied to incoming data from unlabeled workstations

Planning Auditing

Planning auditing can require extensive knowledge. *Trusted Solaris Audit Administration* describes in detail how to set up auditing.

Auditing Security Information

Auditing security decisions include:

- Classes of events to audit for success
- Classes of events to audit for failure
- Classes of events to audit for both
- Users/roles with what additional auditing
- Who has access to the audit administration server
- Who has access to the audit servers
- Who has the execution profile for audit file backup
- Who has the execution profile for audit file review

Auditing System Information

Auditing system decisions include:

- Primary and secondary audit partitions for each workstation
- Size of audit partitions

Planning Workstations

System Information for Each Machine

List the system information for each workstation/server in the Trusted Solaris network:

- name
- kernel architecture
- IP address

Security Information for Each Machine

Determine the security information for each workstation/server in the Trusted Solaris network:

- root password
- PROM/BIOS security level
- PROM/BIOS password
- Attached peripherals permitted?
- Access to printers
- Access to unlabeled domains

Sample Custom JumpStart Installation

This example shows a set of steps an install team would take to do a custom JumpStart installation for a fictitious site.

Sample Site Setup

The following figure shows the sample site setup for this example.

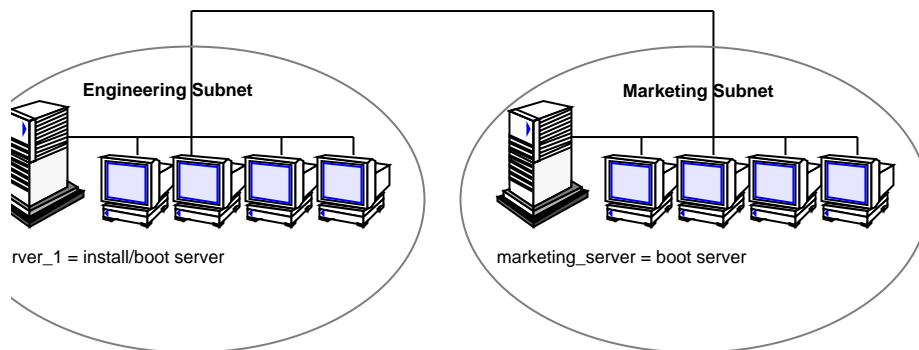


Figure C-1 Sample Site Setup

At this fictitious site:

- The engineering group is on its own subnet. This group uses 32-Mbyte Sun Ultra systems for software development.
- The marketing group is on its own subnet. This group uses 32-Mbyte Sun IPX 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 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`.

▼ Create a JumpStart directory.

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`. As root at the label `ADMIN_LOW`:

```
# cp -r /export/install/jumpstart_sample /jumpstart
```

▼ Share the JumpStart directory.

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 in the role `admin` at the label `ADMIN_LOW` 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
```

Then, at the command line, the administrator in the role `admin` at the label `ADMIN_LOW` uses the `unshareall` and `shareall` commands:

```
# unshareall
# shareall
```

▼ Create the `eng_profile` profile.

The security administrator in the role `root` at the label `ADMIN_LOW` using the Admin Editor action, 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.

```
install_type  initial_install
system_type   standalone
partitioning  default
```

```
cluster      SUNWCprog
fileysys     any 128 swap
```

1. Specifies that the installation will be treated as an initial installation.
2. Specifies that the engineering systems are standalone systems.
3. Specifies that the JumpStart software uses default disk partitioning for installing Trusted Solaris software on the engineering systems.
4. Specifies that the developer's software cluster will be installed.
5. Specifies that each system in the engineering group will have 128 Mbytes of swap space.

▼ Create the marketing_profile profile.

An administrator in the role `root` at the label `ADMIN_LOW` using the Admin Editor 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.

```
install_type    initial_install
system_type     standalone
partitioning    default
cluster         SUNWCuser
package         SUNWaudmo
```

1. Specifies that the installation will be treated as an initial installation, as opposed to an upgrade.
2. Specifies that the marketing systems are standalone systems.
3. Specifies that the JumpStart software will use default disk partitioning for installing Trusted Solaris software on the marketing systems.
4. Specifies that the end user software cluster is to be installed.
5. Specifies that the audio demo software package is to be added to each system.

▼ Edit the rules file.

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 in the role `secadmin` at the label `ADMIN_LOW` using the Admin Editor 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 165 for a complete list of keywords you can use in a rules file.

▼ Execute the check script.

After the rules and profile files are properly set up, the system administrator runs the `check(1M)` script to verify the files. At the label `ADMIN_LOW` in a profile shell (`pfsh(1M)`), as role `admin`:

```
$ cd /jumpstart
$ ./check
```

When `check` finds no errors, it creates the `rules.ok` file.

▼ Set up the engineering systems for installation.

After setting up the `/jumpstart` directory and appropriate files, the administrator sets up the install server to install Trusted Solaris software on the engineering systems.

The administrator first sets up the engineering systems because they are on the same subnet as the install server. On the install server, the administrator in the role `root` at the label `ADMIN_LOW` uses the `add_install_client(1M)` command:

```
# cd /export/install
# ./add_install_client -c server_1:/jumpstart host_eng1 sun4u
# ./add_install_client -c server_1:/jumpstart host_eng2 sun4u
.
.
.
```

In the `add_install_client` command,

<code>-c</code>	Specifies the server (<code>server_1</code>) and path (<code>/jumpstart</code>) 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.
sun4u	Specifies the platform of the systems that will use <code>server_1</code> as an install server. (This is the proper platform name for Sun Ultra systems.)

▼ Set up the marketing systems for installation.

Systems cannot boot from an install server on a different subnet, so the administrator sets up a boot server on the marketing group's subnet. On a server on the marketing subnet, the administrator inserts a Trusted Solaris CD. The administrator in the role root at the label `ADMIN_LOW` then uses the `setup_install_server(1M)` 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,

<code>-b</code>	Specifies that <code>setup_install_server</code> will copy the boot information from the Trusted Solaris CD to the directory named <code>/marketing/boot-dir</code> .
<code>sun4c</code>	Specifies the platform of the systems that will use this boot server. (This is the proper platform name for Sun IPX systems.)

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. At the label `admin_low`, 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,

<code>-s</code>	Specifies the install server (<code>server_1</code>) and the path to the Trusted Solaris software (<code>/export/install</code>).
-----------------	---

<code>-c</code>	Specifies the server (<code>server_1</code>) and path (<code>/jumpstart</code>) to the JumpStart directory.
<code>host_mkt1</code>	Is the name of a system in the marketing group.
<code>host_mkt2</code>	Is the name of another system in the marketing group.
<code>sun4c</code>	Specifies the platform of the systems that will use this boot server. (This is the proper platform name for Sun IPX systems.)

▼ Boot the systems and install Trusted Solaris software.

The install team boots the engineering systems by using the following `boot(1M)` command at the `ok (PROM)` prompt of each system.

```
ok boot net - install
```

Example Worksheets

The worksheet examples provide you with samples for your workstations, devices, user-administrators, and network.



Caution - These are examples only. Do *not* use the IP addresses, names, and other details as they are written here.

How to Use the Examples

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.

Subnet?	Yes	If your LAN is part of a larger network, say yes.
Subnet mask	255.255.255.0	Check that the default is the appropriate mask for your site.
Time zone	Geographical, US Pacific	A time zone map is provided on the www .
Date and Time		The default provided is usually the correct clock time.
The answers to the above questions are System ID Information (sysidinfo). When installing over a network, system information is automatically given to the installation program, reducing the installer's interaction with the program.		
Install	Install	Upgrade is not supported for this release.
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 233 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 233
Customize?		Customizing requires advanced system administration skills.
Customize Disks		See "Root NIS+ Master Disk Partitioning Example" on page 233
Begin installation		

Reboot	Yes	
Root password	<i>List it elsewhere</i>	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/utills/cmgr	
for Man Pages	ada	129.159.110.5	/opt/utills/man	
for Utilities	ada	129.159.118.5	/opt/utills/	
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]

Use	Name	IP address	Shared File Systems	Security Information
	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			
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	
Subnet?	Yes	If your LAN is part of a larger network, say yes.
Subnet mask	255.255.255.0	Check that the default is the appropriate mask for your site.
Time zone	Geographical, US Pacific	A time zone map is provided on the www.
Date and Time		The default provided is usually the correct clock time.
The answers to the above questions are System ID Information (sysidinfo). When installing over a network, system information is automatically given to the installation program, reducing the installer's interaction with the program.		
Install	Install	Upgrade is not supported for this release.
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 237 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 237 for the details of the example.
Begin installation		
Reboot	Yes	
Root password	<i>List it elsewhere</i>	Workstation security requires a root password.

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

Disk	Slice	Mount point	Size	Disk	Slice	Mount point	Size
	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)			

System Administrator Information		Security Officer Information
for Sol AnswerBks	/usr/AB/Sol7/	
for TS AnswerBks	/usr/AB/TS7/	
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	
Subnet?	Yes	If your LAN is part of a larger network, say yes.
Subnet mask	255.255.255.0	Check that the default is the appropriate mask for your site.
Time zone	Geographical US Pacific	A time zone map is provided on the WWW.
Date and Time		The default is usually the correct clock time.
The answers to the above questions are System ID Information (sysidinfo). When installing over a network, system information is automatically given to the installation program, reducing the installer's interaction with the program.		
Install	Install	Upgrade is not supported for this release.
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 241 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	<i>List it elsewhere</i>	Workstation security requires a root password.

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		
s7		

s6		
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/Sol7/		
for TS AnswerBks	/usr/AB/TS7/		
for ManPages	/usr/shar/man		
for CodeMgr	/opt/prog/Code		
for Utilities	/opt/dist/Util		
for Applications	/opt/dist/App		
Audit Mount Points			

System Administrator Information		Security Officer Information	
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/ <i>clientname</i> ...		
babybird	/export/swap/ <i>clientname</i> ...		
juniorbird	/export/root/ <i>clientname</i> /usr/AB		
tinytweet	/export/root/ <i>clientname</i> /opt		
smalldove	/export/root/ <i>clientname</i> /shar		
tinkerbelle			
Mail Server	grebe		
Attached Devices	None		
Remote Printers	cirrus		
	cumulus	Administrator printer [admin_high] only	

Remote Hosts Worksheet - Example

Trusted Solaris 7 Host Type = tsol;		Unlabeled Host Type = unlabeled; unlabeled_conf;	
Name	grebe	Name	dickinson
IP address	129.159.110.1	IP address	129.159.129.11
Name	willet	Name	
IP address	129.159.110.2	IP address	
Name	sora	Name	
IP address	129.159.110.3	IP address	
Name		Name	
IP address		IP address	
Name		Name	
IP address		IP address	
Name		Name	
IP address		IP address	

Remote Hosts (tnrhdb) Worksheet for NIS+ Root Master - Example

System Administrator Information		Security Administrator Information	
Name	dickinson	Template	unlab
IP address	129.159.129.11		
Host_type	unlabeled		
Use	file server		

System Administrator Information		Security Administrator Information	
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		

System Administrator Information		Security Officer Information
Host_type	CIPSO	
Use	network diagnostics	

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

User: Katherine Pollit		
	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

Glossary

access control list	One type of discretionary access control based on a list of entries that the owner can specify for a file or directory. An access control list (ACL) can restrict or permit access to any number of individuals and groups, allowing finer-grained control than provided by the standard UNIX permission bits.
accreditation range	A set of sensitivity labels that are approved for a class of users or resources. See also workstation accreditation range and user accreditation range.

ACL

See access control list

accreditation range	A set of valid labels. See accreditation range and user accreditation range for more about the two types of accreditation ranges in the Trusted Solaris environment.
administrative role	A role defined in the Trusted Solaris software that gives required authorizations, 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 privileges a process can use. A process that runs a program that has a forced privilege set

limits that program to the forced privileges that are also in the process' allowed privilege set.

authorization	A right granted to a user or role to perform an action that would otherwise not be allowed by the Trusted Solaris security policy. Authorizations are granted in execution profiles. Certain commands require the user to have certain authorizations to succeed. Similar to the use of privilege on programs.
application search path	In CDE the search path used by the system to find applications and certain configuration information. The application search path is controlled by a trusted role.
AutoClient system	A system type that caches all of its needed system software from an OS server. Because it contains no permanent data, an AutoClient is a field replaceable unit (FRU). It requires a small local disk for swapping and for caching its individual root (/) and /usr file systems from an OS server. Trusted Solaris does not support autoclients.
begin script	A user-defined Bourne shell script, specified within the rules file, that performs tasks before the Trusted Solaris software is installed on the system. Begin scripts can be used only with custom JumpStart installations.
bootparams file	A file that is consulted when a workstation boots. In Trusted Solaris, the bootparams file contains a keyword=value entry that points the boot server to the Trusted Solaris label configuration for the workstation. A workstation can have a local bootparams file (/etc/bootparams), or it can use the bootparams NIS+ table. See bootparams(4).
boot server	A server that provides boot services to workstations on the same subnet. A boot server is required if you plan to push Trusted Solaris information from a central location to every workstation in the system. If the install server is on a different subnet than the workstations that need to install the Trusted Solaris software, you must create a boot server for that subnet.
CDE	See Common Desktop Environment.
clearance	The upper bound of the set of labels at which a user may work, whose lower bound is the minimum label assigned by the security administrator. There are two types of clearance, the session clearance and the user clearance.

client	A workstation connected to a network.
closed network	A <i>closed network</i> is a network of Trusted Solaris workstations that is cut off from any non-Trusted Solaris workstation. The cutoff can be physical, where there is no wire that extends past the Trusted Solaris network. The cutoff can be in the software, where the Trusted Solarisworkstations recognize only Trusted Solarisworkstations. Data entry from outside the network is restricted to peripherals attached to Trusted Solarisworkstations.
cluster	A logical grouping of software packages. The Trusted Solaris software is divided into four main software groups, which are each composed of clusters and packages.
CMW label	Consists of an 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 <i>copied</i> to the user's home directory at other labels, when those directories are created. See also .link_files.
core	A software group that contains the minimum software required to boot and run the Solaris operating environment on a system. It includes some networking software and the drivers required to run the OpenWindows environment; it does not include the windowing software. Trusted Solaris does not offer a core software group, since the Common Desktop Environment is the required administration environment.
core file	A file that contains a picture of the state of a system when it crashed. Also called a core dump.
custom JumpStart installation	A type of installation in which the Trusted Solaris software is automatically installed on a system based on a customized profile. You can customize profiles for different types of users.
DAC	See discretionary access control.

derived profile	A profile that is dynamically created by a begin script during a custom JumpStart installation.
device	Devices include printers, workstations, tape drives, floppy drives, audio devices, and internal pseudo terminal devices. Devices are subject to the read equal write equal MAC policy.
device allocation	A mechanism for protecting the information on an allocatable device from access by anybody except the user who allocates the device. Until a device is deallocated, no one but the user who allocated a device can access any information associated with the device. For a user to allocate a device, that user must have been granted the device allocation authorization by the security administrator.
developer system support	A software group that contains the End User System Support software group plus the libraries, include files, man pages, and programming tools for developing software.
discretionary access control	The type of access granted or denied by the owner of a file or directory at the discretion of the owner. The Trusted Solaris environment provides two kinds of discretionary access controls (DAC): permission bits and access control list.
disk configuration file	A file that represents a structure of a disk (for example, bytes/sector, flags, slices). Disk configuration files enable you to use <code>pfinstall</code> from a single system to test profiles 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: <code>tundra.mpk.ca.us</code>). As you read a domain name from left to right, the component names identify more general (and usually remote) areas of administrative authority.

end user system support	A software group that contains the core software group plus the recommended software for an end user, including OpenWindows and DeskSet software.
entire distribution	A software group that contains the entire Trusted Solaris release.
entire distribution plus OEM support	A software group contains the entire Trusted Solaris release, plus additional hardware support for OEMs. This software group is recommended when installing Trusted Solaris software on servers.
EISA	Extended Industry Standard Architecture. A type of bus on x86 systems. EISA bus standards are “smarter” than ISA bus systems, and attached devices can be automatically detected when they have been configured via the “EISA configurator” program supplied with the system. See ISA.
/etc	A directory that contains critical system configuration files and maintenance commands.
evaluated configuration	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. The evaluating body for the Trusted Solaris 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 attributes 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 authorizations 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 <code>/export</code> file system can contain the root file system and swap for diskless clients and the home directories for users on the network. Diskless clients rely on the <code>/export</code> file system on an OS server to boot and run.
fdisk partition	A logical partition of a disk drive dedicated to a particular operating system on x86 systems. During the Solaris installation program, you must set up at least one Solaris fdisk partition on an

x86 system. x86 systems are designed to support up to four different operating systems on each drive; each operating system must reside on a unique fdisk partition.

file server	A server that provides the software and file storage for systems on a network.
file privilege set	These sets are the allowed and forced privileges specified for use by executable files (programs). The allowed set limits which privileges a process can use, whether the privileges are forced on the executable file or inherited (see inheritable privileges). Any privileges in the forced privilege set are available to any process that invokes the program, as long as they are also in the allowed set.
file system	A collection of files and directories that, when set into a logical hierarchy, make up an organized, structured set of information. File systems can be mounted from your local system or a remote system.
finish script	A user-defined Bourne shell script, specified within the rules file, that performs tasks after the Trusted Solaris software is installed on the system, but before the system reboots. Finish scripts can be used only with JumpStart installations.
forced privilege set	The forced set of privileges are those placed on a file by the security administrator. Any privileges in the forced privilege set are available to any process that invokes the program, as long as they are also in the allowed privilege set.
GFI	Government Furnished Information. In this manual, it refers to a U.S. government-provided label_encodings file. In order to use a GFI with Trusted Solaris software, you must add the Sun-specific LOCAL DEFINITIONS section to the end of the GFI. Trusted Solaris Label Administration explains the procedure in detail.
host name	The name by which a system is known to other systems on a network. This name must be unique among all the systems within a given domain (usually, this means within any single organization). A host name can be any combination of letters, numbers, and minus sign (-), but it cannot begin or end with a minus sign.
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 <i>advisory label</i> . Trusted Solaris 7 no longer supports information labels.

inheritable privilege	The privileges that a process can pass to a program across an <code>execve()</code> without their being affected by the new program's forced or allowed privilege sets. When a new program is executed by a process, the inheritable set of the process is set to be equal to the inheritable set of the old program. The inheritable set is not affected by the forced or allowed privileges on the currently executing program, which allows privileges to be passed from programs that cannot use them to programs that can.
initial label	The minimum label assigned to a user or role, and the label of the user's initial workspace. It is the lowest label at which the user or role can work.
initial installation option	An option presented during the Trusted Solaris installation program that overwrites the disk(s) with the new version of Trusted Solaris. The initial installation option is the only installation option supported in the Trusted Solaris release.
install server	A server that provides the Trusted Solaris installation image for other systems on a network to boot and install from (also known as a <i>media server</i>). 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	<p>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.</p> <p>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).</p>
ISA	Industry Standard Architecture. A type of bus found in x86 systems. ISA bus systems are "dumb" and provide no mechanism the system can use to detect and configure devices automatically. See EISA.

JumpStart directory	When using a diskette for custom JumpStart installations, the JumpStart directory is the root directory on the diskette that contains all the essential custom JumpStart files. When using a server for custom JumpStart installations, the JumpStart directory is a directory on the server that contains all the essential custom JumpStart files.
JumpStart installation	A type of installation in which the Solaris software is automatically installed on a system by using factory-installed JumpStart software. The Trusted Solaris release does not offer this option; all JumpStart installations in Trusted Solaris are custom JumpStart installations.
kernel architecture	See platform group.
label	A security identifier assigned to a file or directory based on the level at which the information being stored in that file or directory should be protected. Depending on how the security administrator has configured the user, a user may see the complete CMW label, only the sensitivity label portion, only the information label portion, or no labels at all. See <code>label_encodings</code> file.
label configuration	A Trusted Solaris installation choice of: single- or multilabel sensitivity labels; if multilabel, hide or show upgraded file names. Unless circumstances are unusual, label configuration should be identical on all workstations in the Trusted Solaris domain.
labeled workstation	A labeled workstation sends labeled network packets, such as RIPS0, CIPSO, TSIX(RE1.1), and MSIX packets. All Trusted Solaris workstations are labeled workstations.
label_encodings file	The file where the complete CMW label is defined, as are label view, admin_low and admin_high strings, default label visibility, and all other aspects of labels.
label range	A set of sensitivity labels assigned to commands, file systems, and allocatable devices, specified by designating a maximum label and a minimum label. For commands, the minimum and maximum labels limit the sensitivity labels at which the command may be executed. For file systems, the minimum and maximum labels limit the sensitivity labels at which information may be stored on each file system. Trusted Solaris environments have multilabel file systems configured with a label range from the lowest sensitivity label to the highest sensitivity label. Remote hosts that do not recognize labels are assigned a single sensitivity label, along with any other hosts that the security administrator wishes to restrict to a single label; labels limit the sensitivity labels at which devices may be allocated

and restrict the sensitivity labels at which information can be stored or processed using the device.

label view flags	Label view flags control the translation and display of the internal ADMIN_LOW and ADMIN_HIGH labels. A value of External specifies that the actual label ADMIN_LOW displays as the lowest label name in the user accreditation range specified in the label_encodings file, and that the actual label ADMIN_HIGH displays as the highest label name in the user accreditation range. A value of Internal specifies that the ADMIN_LOW and ADMIN_HIGH labels are translated to the Admin Low Name and Admin High Name strings specified in the label_encodings file.
.link_files	An optional setup file in a multilabel environment. The file contains the names of startup files, such as .cshrc or .netscape, that the user environment or user applications require in order for the environment or application to behave well. The files referenced in .link_files are then <i>linked</i> to the user's home directory at other labels, when those directories are created. See also .copy_files.
locale	A specific language associated with a region or territory.
MAC	See mandatory access control.
mandatory access control	Access control based on comparing the sensitivity label of a file, directory, or device to the sensitivity label of the process that is trying to access it. The MAC rule — write up, read down (WURD) — applies when a process at one sensitivity label attempts to read or write to a file at another sensitivity label. The MAC rule — write equal, read down — applies when a process at one sensitivity label attempts to write to a directory at another sensitivity label. The MAC rule — read equal, write equal — applies when a process at one sensitivity label attempts to write to a device at another sensitivity label
MCA	Micro Channel Architecture. A type of bus on x86 systems. The MCA bus provides fast data transfer within the computer, and attached devices can be automatically detected when they have been configured using the reference disk provided by the manufacturer. The MCA bus is not compatible with devices for other buses.
media server	See install server.
minimum label	The lower bound of a user's sensitivity labels and the lower bound of all users' sensitivity labels. The minimum label set by the security administrator when specifying a user's security attributes is the

sensitivity label of the first workspace that comes up after the user's first login. The sensitivity label specified in the minimum label field by the security administrator in the `label_encodings` file sets the lower bound for all users.

MLD	See multilevel directory.
mount	The process of making a remote or local file system accessible by executing the <code>mount</code> 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, <code>/usr</code>).
mount point	A directory on a system where you can mount a file system that exists on the local or a remote system.
multilevel directory	A directory in which information at differing sensitivity label is maintained in separate subdirectories called single-level directories (SLDs), while appearing to most interfaces to be a single directory under a single name. In the Trusted Solaris environment, directories that are used by multiple standard applications to store files at varying labels, such as the <code>/tmp</code> directory, <code>/var/spool/mail</code> , and users' <code>\$HOME</code> directories, are set up to be MLDs. A user working in an MLD sees only files at the sensitivity label of the user's process.
name server	A server that provides a name service to systems on a network.
name service	A distributed network database that contains key system information about all the systems on a network, so the systems can communicate with each other. With a name service, the system information can be maintained, managed, and accessed on a network-wide basis. Sun supports the following name services: NIS (formerly YP) and NIS+. Trusted Solaris supports NIS+. Without a name service, each system has to maintain its own copy of the system information (in the local <code>/etc</code> files).
network installation	A way to install software over the network—from a system with a CDROM drive to a system without a CDROM drive. Network installations require a name server and an install server.
networked systems	A group of workstations (called hosts) connected through hardware and software, so they can communicate and share information; referred to as a local area network (LAN). One or more servers are usually needed when systems are networked.

NIS+	Network Information Service, Plus. The name service for a Trusted Solaris network. NIS+ provides automatic information updating and adds security features such as authorization and authentication.
NIS+ master	See NIS+ root master.
NIS+ root master	The workstation that contains the master files for a NIS+ network. Also called a root master or a NIS+ master.
non-networked systems	Workstations that are not connected to a network or do not rely on other workstations.
open network	An <i>open network</i> is a network of Trusted Solaris workstations that is connected physically to other networks and that uses Trusted Solaris software to communicate with non-Trusted Solaris workstations. Contrast with closed network.
/opt	A file system that contains the mount points for third-party and unbundled software.
OS server	A system that provides services to systems on a network. To serve diskless clients, an OS server must have disk space set aside for each diskless client's root file system and swap space (/export/root, /export/swap). To serve dataless clients, an OS server must provide the /usr file system. To serve autclients, an OS server must provide everything except the individual root (/) and /usr file systems required for swapping and caching.
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 <i>outside the evaluated configuration</i> .
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 <i>packages</i> .
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 <code>uname -m</code> command. A vendor-defined grouping of hardware platforms for the purpose of distributing specific software. Examples of valid platform names are <code>i86pc</code> , <code>sun4c</code> . Often called kernel architecture.
platform name	The output of the <code>uname -i</code> command. For example, the platform name for the SPARCstation IPX is <code>SUNW,Sun_4_50</code> .
privilege	A right granted to a process executing a command that allows the command or one or more of its options to bypass some aspect of security policy. A privilege is only granted by a site's security administrator after the command itself or the person using it has been judged to be able to use that privilege in a trustworthy manner.
process	An action that executes a command on behalf of the user who invokes the command. A process receives a number of security attributes from the user, including the user ID (UID), the group ID (GID), the supplementary group list, and the user's audit ID (AUID). Security attributes received by a process include any privileges available to the command being executed, the process clearance (which is set to be the same as the session clearance), the sensitivity label of the current workspace, and an information label. If the label configuration option <code>RESET IL ON EXEC</code> 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 like a user, except that a role cannot log in. Roles are limited to a particular set of commands and CDE actions. See administrative role.

/ (root)	The file system at the top of the hierarchical file tree on a system. The root directory contains the directories and files critical for system operation, such as the kernel, device drivers, and the programs used to start (boot) a system.
root master	See NIS+ root master.
rule	A series of values that assigns one or more system attributes to a profile.
rules file	A text file used to create the rules.ok file. The <code>rules</code> file is a look-up table consisting of one or more rules that define matches between system attributes and profiles.
rules.ok file	A generated version of the rules file. It is required by the custom JumpStart installation software to match a system to a profile. You use the <code>check</code> script to create the <code>rules.ok</code> file.
security administrator	In an organization where sensitive information must be protected, the person or persons who define and enforce the site's security policy and who are cleared to access all information being processed at the site. In the Trusted Solaris software environment, an administrative role that is assigned to one or more individuals who have the proper clearance and whose task is to configure the security attributes of all users and workstations so that the software enforces the site's security policy. In contrast, see system administrator.
security attribute	An attribute used in enforcing the Trusted Solaris security policy. Various sets of security attributes, both in the base Solaris and the Trusted Solaris environments, are assigned to processes, users, files, directories, hosts on the trusted network, allocatable devices, and other entities.
security policy	In the Trusted Solaris environment, the set of DAC, MAC, and information labeling rules that define how information may be accessed. At a customer site, the set of rules that define the sensitivity of the information being processed at that site and the measures that are used to protect the information from unauthorized access.
sensitivity label	A security label assigned to a file or directory or process, which is used to limit access based on the security level of the data contained.
single-level directory	A directory within an MLD containing files at only a single sensitivity label. When a user working at a particular sensitivity

label changes into an MLD, the user's working directory actually changes to a single-label directory within the MLD, whose sensitivity label is the same as the sensitivity label at which the user is working.

SLD	See single-level directory.
slice	An area on a disk composed of a single range of contiguous blocks. A slice is a physical subset of a disk (except for slice 2, which by convention represents the entire disk). A disk can be divided into eight slices. Before you can create a file system on a disk, you must format it into slices.
software group	A logical grouping of the Solaris software (clusters and packages). During a Solaris installation, you can install one of the following software groups: core, end user system software, developer system support, or entire distribution.
standalone system	A system that has its own / (root) file system, swap space, and /usr file system, which reside on its local disk(s); it does not require boot or software services from an OS server. A standalone system can be connected to a network, but it does not have to be.
subnet	A working scheme that divides a single logical network into smaller physical networks to simplify routing.
subnet mask	A bit mask, which is 32 bits long, used to determine important network or system information from an IP address.
swap space	Disk space used for virtual memory storage when the system does not have enough system memory to handle current processes. Also known as the /swap or swap file system.
system	Generic name for a workstation. After installation, a system is often called a host.
system accreditation range	The set of all valid (well-formed) labels created according to the rules defined by each site's security administrator in the label_encodings file, plus the two administrative labels that are used in every Trusted Solaris environment, ADMIN_LOW and ADMIN_HIGH.
system administrator	In the Trusted Solaris environment, the trusted role assigned to the user or users responsible for performing standard system

management tasks such as setting up the non-security-relevant portions of user accounts. In contrast, see security administrator.

system type	One of several different ways a workstation can be set up to run the Trusted Solaris software. Valid system types are: standalone system, 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 <code>/etc/security/tsol/tnrhdb</code> or as a NIS+ table.
tnrhtp database	The Trusted Network Remote Host TemPlate, accessible either as a file in <code>/etc/security/tsol/tnrhtp</code> 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 hosts that a Trusted Solaris domain can communicate with.
trusted role	See administrative role.
Trusted Solaris installation program	(1) A menu-driven, interactive program that enables you to set up a system and install the Trusted Solaris software on it. (2) Any part of the software that is used to install the Trusted Solaris software on a system.
trusted stripe	A region that cannot be spoofed along the bottom of the screen, which by default provides the following as visual feedback about the state of the window system: a trusted path indicator, the input information label and window sensitivity label. When either sensitivity labels or information labels 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 labels or information labels 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 <code>/etc/security/tsol/tsolprof</code> or as a NIS+ table. After configuration, it contains execution profiles provided by the Trusted Solaris software.
tsoluser database	The Trusted SOLaris USER database, accessible either as a file in <code>/etc/security/tsol/tsoluser</code> or as a NIS+ table. After

configuration, it contains roles provided by the Trusted Solaris software.

upgrade option	An option presented during the Solaris installation program. The upgrade procedure merges the new version of Solaris with existing files on your disk(s), and it saves as many local modifications as possible since the last time Solaris was installed. The upgrade option is not available with the Trusted Solaris 7 release.
unlabeled workstation	A workstation that sends unlabeled network packets, such as Solaris 7.
user accreditation range	The set of all possible labels at which any normal user may work on the system, as defined by each site's security administrator. The rules for well-formed labels that define the system accreditation range are additionally restricted by the values specified in the ACCREDITATION RANGE section of the site's <code>label_encodings(4)</code> file: the upper bound, the lower bound, the combination constraints and other restrictions.
user clearance	The clearance assigned by the security administrator that sets the upper bound of the set of labels at which one particular user may work at any time. The user may decide to accept or further restrict that clearance during any particular login session, when setting the session clearance after log in.
/usr	A file system on a standalone system or server that contains many of the standard UNIX programs. Sharing a large file system with a server rather than maintaining a local copy minimizes the overall disk space required to install and run the Trusted Solaris software on a system.
/var	A file system or directory (on standalone systems) containing system files that are likely to change or grow over the life of the system. These include system logs, <code>vi</code> files, mail files, and <code>uucp</code> 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 7 release.
workstation accreditation range	The set of all valid (well-formed) labels created according to the rules defined by each site's security administrator in the <code>label_encodings</code> file, plus the two administrative labels that are used in every Trusted Solaris environment, <code>ADMIN_LOW</code> and <code>ADMIN_HIGH</code> . Also called the system accreditation range.

Index

Special Characters

- ! (exclamation mark) rule field 162
- # (pound sign)
 - in profiles 150
 - in rules 164
- && (ampersands) rule field 162
- (minus sign) in rules 165, 198
- ... (ellipsis points) rule field 162
- = (equals sign) in profile field 178
- [(brackets) rule field 162
- \ (backslash) in rules 165

A

- accounts
 - creating the first users 102
- adding
 - clusters when upgrading 154
- add_install_client command
 - custom JumpStart example 229, 230
 - example 130, 147, 148
 - install server setup 128, 130
 - JumpStart directory access 148
 - syntax 129, 131, 147
- Admin Editor
 - opening administrative action 55, 58
 - using to create file 57
- administrative actions
 - in Solstice_Apps folder 51
 - in System_Admin folder 57
- administrative roles
 - adding to three /etc files 82
 - verifying during configuration 105

- ampersands (&&) rule field 162
- AND rule field 162
- angle bracket (>) prompt 71
- any
 - rule keyword
 - description and values 165
 - rootdisk matching 171
- Application Manager
 - opening 50
- arch rule keyword 165
- auditing
 - NIS+ client setup 119
 - NIS+ root master setup 106
 - planning 32

B

- backslash (\) in rules 165
- backup
 - before installation 33
- banner command 124
- begin rule field
 - described 163
 - valid entries 165
 - validation 172
- begin scripts
 - creating derived profiles with 178, 179
 - log file 178
 - overview 177
 - permissions 178
 - rule field 163
 - site-specific installation programs 198

- binary compatibility package profile
 - example 152
- boot information
 - copying during custom JumpStart 229
- boot server
 - creating on subnet 131
- booting the workstation
 - during installation 67, 101
 - I/O interrupt error messages 123
 - interactive installation 70
 - resetting terminals and display first 123
- bootparams file
 - enabling JumpStart directory access 148
- Bourne shell scripts in rule fields 163
- brackets rule field 162

C

- CDE sessions
 - ending 67
 - starting the workstation 67
- check script
 - comments and 165
 - derived profiles and 179
 - directory for 172
 - rules file validation 171, 173
 - rules.ok file creation 172
 - starting 172, 175
 - testing rules 173
- checklists for administrators 219
- client_arch profile keyword 152
- client_root profile keyword 153
- client_swap profile keyword 153
- cluster profile keyword
 - description and values 153, 154
 - examples 150, 152
- comments
 - in profiles 150
 - in rules file 165
- concatenating multiple disk configuration files
 - Intel architecture 194
 - Intel architecture systems 198
- configuration files
 - copying for distribution 107
 - creating directory 107
 - SPARC systems
 - for concatenating multiple disks 188, 190

- copying
 - disk configuration file to JumpStart
 - directory 191
- CPUs (processors)
 - rule keywords 165
- credentials
 - giving to roles 101
- custom execution profiles
 - verifying 66
- custom JumpStart installation
 - advantages 136
 - booting and installing
 - booting the system 70, 73
 - described 135
 - diskless clients 77
 - examples 225, 230
 - check script 228
 - engineering systems setup 228
 - JumpStart directory 226
 - marketing systems setup 229, 230
 - networked 141
 - non-networked 139
 - rules file editing 227, 228
 - site setup 225, 226
 - standalone system 139
 - hands-off installation 122
 - requirements 122
 - JumpStart directory 147
 - optional features 177, 198
 - begin scripts 177, 179
 - finish scripts 179, 183
 - overview 177
 - pfinstall command 183, 186
 - site-specific installation
 - programs 198
 - overview 139, 141
 - preparing 135, 175

D

- Database Manager
 - entering local hosts 93
 - modifying tnrdhdb 93, 94
 - modifying tnrdhpt 93, 94
 - using 51
- databases
 - tsoluser 82, 96

- user
 - during installation 82, 96
- default routes
 - setting 91
- defaults
 - derived profile name 179
 - SI_CONFIG_DIR variable 180
 - software group installed 154
- deleting
 - clusters when upgrading 154
- derived profiles 178, 179
- Developer system support software
 - cluster name 153
 - profile example 150
- Device Allocation action
 - using 48
- devices
 - setting device policy 92
- dfstab file 226
- directories
 - changing
 - to JumpStart directory 172
 - to mounted CD 132, 143
 - to Trusted Solaris CD image on local disk 143, 145
 - changing to mounted CD 143
 - changing to Trusted Solaris CD image on local disk 143
- JumpStart
 - adding files 180
 - copying disk configuration files 191
 - copying files 180, 186
 - copying installation files from CD 143, 145
 - creating 137, 226
 - creating for SPARC systems 141, 143
 - enabling access 146, 148
 - install server setup 147
 - permissions 141, 144
 - rules file example 160
 - sharing 226
- disk configuration files
 - copying to JumpStart directory 186, 191

- creating 186
 - Intel architecture 194
 - Intel architecture systems 194
 - Intel architecture 190
 - Intel multiple disks 198
 - SPARC multiple disks 188, 190
 - SPARC systems 186, 188
- creation using prtvtoc 186
- described 183, 186, 190
- diskette
 - copying files from 46
- diskettes
 - copying files to 45
 - copying Trusted Solaris boot diskette 142
 - formatting 142
 - JumpStart directory
 - access 146
 - creating for SPARC systems 141, 143
 - mounting 142
- diskless clients
 - accessing a Trusted Solaris image 200
 - adding 203
 - boot server 203
 - configuring 203
 - platforms 152
 - prerequisites 199
 - providing a root password 206
 - setting up home directories 205
 - swap space 153
- disksize rule keyword
 - description and values 166
 - rootdisk matching 170
- display
 - resetting after I/O interrupts 123
- DNS
 - setup 100
- domainname rule keyword 166
- domains
 - rule keyword 166

E

- ellipsis points (...) rule field 162
- eng_profile example 226
- Entire distribution software
 - cluster name 153
- equals sign (=) in profile field 178

- /etc/bootparams file
 - enabling JumpStart directory access 148
- /etc/dfs/dfstab file 226
- /etc/nsswitch.conf file 100
- /etc/passwd file 82
- /etc/shadow file 82, 182
- exclamation mark (!) rule field 162
- execution profiles
 - updating 65, 67
 - verifying 66
- exporting shared directories 107

F

- fallback mechanism
 - using for network configuration 94
- fdformat command 142
- fdisk command 191
- fdisk profile keyword
 - example 151
- files
 - copying from floppy 46
 - copying to diskette 45
 - distributing label encodings with finish
 - script 181
- files and file systems
 - begin scripts output 178
 - copying
 - JumpStart installation files from
 - CD 143, 145
 - Trusted Solaris boot diskette 142
 - mounting 64
 - setting label 63
 - sharing 61
 - showing if shared 63
- filesys profile keyword
 - description and values 152
 - examples 150, 151
- finish rule field
 - described 163
 - valid entries 165
 - validation 172
- finish scripts
 - adding 180
 - distributing label encodings file 181
 - log file 179
 - rule field 163
- floppy

- copying files from 46
- formatting diskettes 142

H

- hands-off installation
 - requirements 122
- hard disks
 - partitioning
 - examples 150, 152
 - rootdisk values 170, 171
 - size
 - root space 153
 - rule keywords 166, 170
 - swap space
 - diskless client 153
 - maximum size 159
 - profile examples 150, 151
- hardware
 - configuring 20
 - installation requirements 29
 - planning 29, 30
- home directories
 - mounting 65
 - setup 101, 118
 - sharing 61, 62
- Host Manager
 - adding diskless clients 201
 - adding hosts 126, 128, 131, 201
 - described 123
- hostaddress rule keyword 166
- hostname rule keyword
 - description and values 166
 - example 164
- hosts
 - adding for network installation 127
 - entering in network files 90, 95
 - entering in tnrdhdb 94, 95
 - modifying templates 93, 94

I

- I/O interrupt error messages 123
- icons
 - for device allocation 48
 - for System_Admin actions 57
 - using to launch actions 40

- idle time 54
- install server
 - copying Trusted Solaris CD to local disk 123
 - creating 124
 - described 121
 - requirement for network installation 121
- install user
 - deleting 54
- installation
 - boot commands 71
 - initial option 74
 - using DNS 100
 - manual reboot 76
 - memory requirements 29
 - networked workstations
 - division of tasks 69
 - setting date and time 126
 - NIS+ clients 111, 119
 - NIS+ root master 87, 109
 - non-networked workstation 85
 - over networks 121, 133
 - planning 25, 36
 - planning hardware 29
 - root password creation 76
- installed rule keyword
 - description and values 167
 - rootdisk matching 170
- install_config command 148
- install_type profile keyword
 - examples 150, 152
 - requirement 149, 151
 - testing profiles 183, 185
- interactive installation
 - booting the system 70
 - CDROM drive preparation 71
 - networked workstations 69
 - NIS+ root master 87, 109
- IP addresses
 - in tnrdhdb file 93
 - in tsolgateways file 92
 - rule keyword 166

J

- JumpStart directory
 - adding files with finish scripts 180

- copying files
 - disk configuration files 186, 191
 - installation files from CD 143, 145
 - using finish scripts 180
- creating 137
 - diskette for SPARC systems 141, 143
 - example 226
 - server 144, 146
- install server setup 147
- permissions 141, 144
- rules file example 160
- sharing 144, 146, 226
- jumpstart_sample directory
 - check script 172
 - copying files to JumpStart directory 143, 145
 - set_root_pw finish script 182, 183

K

- karch rule keyword 167

L

- label encodings file
 - checking 89
 - copying 107
 - distributing using JumpStart 181
 - localizing 28, 220
 - modifying 48, 89
- labels
 - finding process' current label 42
 - planning 28
 - setting on unlabeled file system 63
- label_encodings file
 - copying to client 112
 - modifying 80
- locale profile keyword
 - example 152
- log files
 - begin scripts output 178
 - finish scripts output 179
 - installation output 75
- logical AND rule field 162

M

- man pages 151, 152

marketing_profile example 227

matching

derived profiles 178

order for rules 161, 163

rootdisk values 170, 171

memory

displaying amount installed 124

rule keyword 164, 167

setting size 184

swap space size and 159

memsize rule keyword

description and values 167

example 164

microprocessors

rule keywords 165

minus sign (-)

in begin and finish scripts 198

in rules 165

model name 124

model rule keyword

description and values 168

example 164

mount command 123, 142

mounting

begin script caution 178

diskettes 142

displaying mounted file systems 123

by Trusted Solaris installation 179

Trusted Solaris CD 132, 143

unlabeled file systems 106

multiple disk configuration file

Intel architecture 194

Intel architecture systems 198

SPARC systems 188, 190

multiple lines in rules 165

N

name server 121

names/naming

derived profile names 179

host name 166

profile names 150

rules file 161, 164

software group cluster names 154

system model names 168

naming service

choosing in Solstice 51

network installation

custom JumpStart installation

example 141

hands-off configuration 122

planning 30, 32

preparation 121, 133

network interfaces

adding 58

network rule keyword

description and values 169

example 164

NIS+ domain

client setup 117

configuring root master 87, 111

setup 100

updating credentials 101

O

ok prompt 71

OS servers

adding 126, 133

converting from standalone 200

described 122

for diskless clients 199

requirement for network installation 122

OS services

adding to network server 201

osname rule keyword 169

output files

begin scripts log 178

finish scripts log 179

installation log 75

P

package profile keyword

examples 151, 152

partitioning

examples 150, 152

fdisk partitions 152

PASSWD variable 182

passwords

modifying 53

root 182, 183

root password creation 76

root password use 88

- updating role passwords 101
- paths
 - check script 172
 - install server setup 129
 - Trusted Solaris server setup 129
- peripheral devices
 - configuring 20
- permissions
 - begin scripts 178
 - finish scripts 179
 - JumpStart directory 141, 144
- pfinstall command 183, 186
- platforms
 - diskless client 152
 - matching system attributes and
 - profiles 160, 161, 163
 - name determination 123
 - rule keywords 167
 - system model names 168
- pound sign (#)
 - in profiles 150
 - in rules 164
- privileges
 - finding process' current set 42
- processors
 - rule keywords 165
- profile keywords 152
 - adding to profiles 150
 - case sensitivity 150
 - client_arch 152
 - client_root 153
 - client_swap 153
 - cluster
 - description and values 153, 154
 - examples 150, 152
- fdisk
 - example 151
- filesys
 - examples 150, 151
- install_type
 - examples 150, 152
 - requirement 149, 151
- locale
 - example 152
- package
 - examples 151, 152
- partitioning
 - examples 150, 151

- system_type
 - examples 150, 152
- profile keywords to profiles
 - adding 150
- Profile Manager
 - updating custom profiles 65, 67
- profile shell
 - opening 41
 - viewing privilege information 42
 - viewing process information 42
- profiles
 - comments in 150
 - creating 137, 149, 150
 - creating derived 178, 179
 - derived profiles 178, 179
 - described 137, 149
 - examples 152
 - eng_profile 226
 - marketing_profile 227
 - short 150
 - matching systems to 160, 161, 163
 - naming 150
 - requirements 149, 150
 - rule field 163
 - testing 183, 185
 - verifying 66
- prompt, changing to ok prompt 71
- prtconf command 58, 168
- prvtoc command
 - disk configuration file creation 186
 - Intel disk configuration file creation 190, 194

R

- reboot
 - workstation during configuration 67, 101
- release of Trusted Solaris software
 - installed rule keyword 167
- release software
 - osname rule keyword 169
- remote host templates
 - creating new template 93
- requirements
 - network installation 122
 - servers 121
 - profiles 149, 150

- reset command 123
- roles
 - updating profiles 65, 67
 - verifying profile contents 66
- root (/) file systems
 - profile example 151
 - value set by installation program 170, 171
- root environment (customizing) 181
- root passwords 182, 183
 - created 76
 - for diskless clients 206
 - used 88
- root role
 - assuming 39
 - updating profiles 65, 67
- rootdisk
 - defined 170
 - value set by installation program 170, 171
- rule keywords 165, 170
 - any
 - description and values 165
 - rootdisk matching 171
 - arch 165
 - disksize
 - description and values 166
 - rootdisk matching 170
 - domainname 166
 - hostaddress 166
 - hostname 164, 166
 - installed
 - description and values 167
 - rootdisk matching 170
 - karch 167
 - memsize 164, 167
 - model 164, 168
 - network 164, 169
 - osname 169
 - totaldisk 170
 - validation 172
- rules
 - derived profiles 178, 179
 - examples 163
 - field descriptions 162, 163
 - matching order 161, 163
 - multiple line rules 165
 - rootdisk matching rules 170, 171

- syntax 162
 - testing validity 173
- rules file
 - adding rules 161, 162
 - comments 164
 - creating 137, 160, 163
 - described 137, 160
 - example 160
 - multiple line rules 165
 - naming 161, 164
 - syntax 162
 - testing rules 173
 - validating using check 137, 171, 173
 - derived profiles and 179
- rules files
 - adding rules 161
 - custom JumpStart example 227, 228
 - testing 228
 - testing rules 173
 - using check 137, 171, 173
 - validating 228
- rules.ok file
 - comments and 165
 - creating 137, 160, 164, 172
 - described 164
 - matching order for rules 161, 163
- rule_keyword rule field 162
- rule_value rule field 163, 165

S

- screens
 - locking 67
- scripts
 - adding finish 180
 - begin scripts 177, 179, 198
 - Bourne shell scripts in rule fields 163
 - creating finish 180
 - distributing label encodings file 181
 - finish scripts 179, 183, 198
 - network installation commands 123
- security
 - common violations 215
 - computer publications 217
 - computer recommendations 212
 - personnel recommendations 214
 - physical recommendations 213

- root password 182, 183
- site security policy 212
- U.S. Government publications 216
- UNIX publications 216
- servers
 - JumpStart directory creation 144, 146
 - name server 121
 - network installation requirements 122
 - requirements for network installation 121
 - root space 153
- setup_install_server command
 - boot server setup 132
 - custom JumpStart example 229
 - described 123
- set_root_pw finish script 182, 183
- shadow file 182
- share command
 - sharing JumpStart directory 226
- shared directories
 - exporting 107
 - starting server daemon 62
- shutdown
 - workstation 67
- site security policy 26, 212, 218
- site-specific installation programs 198
- size
 - hard disk
 - root space 153
 - rule keywords 166, 170
 - memory 164, 167, 184
 - swap space
 - diskless client 153
 - maximum size 159
 - profile examples 151
- SI_CONFIG_DIR variable 180
- SI_PROFILE environment variable 179
- SI_SYS_STATE variable 183
- slices
 - profile examples 150, 151
 - rule keyword 167
- software groups
 - cluster names for profiles 154
 - profile examples 150, 152
 - upgrading 154
- Solstice_Apps folder
 - Host Manager 123
 - using 50, 55
- SPARC systems

- JumpStart directory creation on
 - diskette 141, 144
- square brackets ([]) rule field 162
- standalone systems
 - adding 126
 - custom JumpStart installation
 - example 139
 - profile examples 150, 152
- static routes
 - setting 90
- subnet
 - boot server creation on 131
- SUNWCall group 153
- swap file systems
 - diskless client swap space 153
 - memory size and 159
 - profile examples 151
 - size determination 159
- system information
 - displaying 124
- System_Admin folder
 - using 55, 58
- system_type profile keyword
 - examples 150, 152
- SYS_MEMSIZE variable 184

T

- terminals
 - resetting after I/O interrupts 123
- tnrhdb file
 - configuring 93, 95
- tnrhttp file
 - editing on the client 115
 - modifying 93, 94
- totaldisk rule keyword 170
- troubleshooting 77
 - I/O interrupt messages 123
- trusted network
 - editing local files 93
- Trusted Solaris boot diskette
 - copying to disk 142
- Trusted Solaris CD
 - copying to install server's local disk 123
 - displaying mounted file systems 123
 - image on local disk 143, 145
 - mounting 132, 143

- Trusted Solaris configuration
 - adding users 102
 - copying label encodings file to client 113
 - copying tntrhttp file to the client 115
 - evaluated configuration 26
 - exporting directories 61
 - logging on as a user 38
 - mounting unlabeled file systems 106
 - NIS+ clients 111, 119
 - protecting workstation 43
 - setting static routes 90
 - setting up home directories 101, 118
 - updating credentials 101
 - verifying that roles work 105
 - workstation without NIS+ 79, 85
- Trusted Solaris installation
 - interactive
 - networked workstations 69
 - non-networked workstations 79, 85
 - log files 75
 - methods 33
 - NIS+ clients 111, 119
 - NIS+ root master 87, 109
 - over networks 121, 135
 - preparing custom JumpStart
 - installation 135, 175
 - setting default date and time 126
 - worksheet examples 231, 247
 - workstation without NIS+ 79, 85
- Trusted Solaris software
 - groups
 - cluster names for profiles 154
 - profile examples 150, 152
 - release or version
 - installed rule keyword 167
 - osname rule keyword 169
- tsolgateways
 - setting 92

U

- uname command 123

- UNIX publications
 - general 217
 - security 216
- unlabeled host type
 - creating (example) 93
- upgrade installation
 - profile example 152
 - profile keywords 152, 154
- User Manager
 - deleting local user 54
 - using 51

V

- /var/sadm/begin.log file 178
- /var/sadm/finish.log file 179
- /var/sadm/system/logs/install_log 75
- variables
 - PASSWD 182
 - SI_CONFIG_DIR 180
 - SI_PROFILE 179
 - SI_SYS_STATE 183
 - SYS_MEMSIZE 184
- version of Trusted Solaris software
 - installed rule keyword 167
 - osname rule keyword 169

W

- worksheets
 - examples 231, 247
- workspaces
 - creating at admin_high 43
- workstations
 - booting 67
 - protecting 43
 - screen-locking 67
 - shutting down 67
 - starting 67
- wrapping lines in rules 165