Trusted Extensions Configuration Guide

Part No: 820–3508–15
April 2012

ORACLE

120405@25097

Contents

Preface 13

1 Security Planning for Trusted Extensions 19
Planning for Security in Trusted Extensions 19
Understanding Trusted Extensions 20
Understanding Your Site's Security Policy 20
Planning Who Will Configure Trusted Extensions 21
Devising a Label Strategy 21
Planning System Hardware and Capacity for Trusted Extensions 22
Planning Your Trusted Network 22
Planning Your Labeled Zones in Trusted Extensions 23
Planning for Multilevel Access 25
Planning for the LDAP Naming Service in Trusted Extensions 25
Planning for Auditing in Trusted Extensions 26
Planning User Security in Trusted Extensions 26
Devising a Configuration Strategy for Trusted Extensions 27
Resolving Additional Issues Before Enabling Trusted Extensions 29
Backing Up the System Before Enabling Trusted Extensions 29
Results of Enabling Trusted Extensions From an Administrator's Perspective 30

2 Configuration Roadmap for Trusted Extensions 31
Task Map: Preparing an Oracle Solaris System for Trusted Extensions 31
Task Map: Preparing For and Enabling Trusted Extensions 31
Task Map: Configuring Trusted Extensions 33

3 Adding Trusted Extensions Software to the Oracle Solaris OS (Tasks) 37
Initial Setup Team Responsibilities 37

Installing or Upgrading the Oracle Solaris Operating System for Trusted Extensions 38
▼ Install an Oracle Solaris System to Support Trusted Extensions 38
▼ Prepare an Installed Oracle Solaris System for Trusted Extensions 39
Collecting Information and Making Decisions Before Enabling Trusted Extensions 41
▼ Collect System Information Before Enabling Trusted Extensions 41
▼ Make System and Security Decisions Before Enabling Trusted Extensions 42
Enabling the Trusted Extensions Service 44
▼ Enable Trusted Extensions 44

4 Configuring Trusted Extensions (Tasks) 47
Setting Up the Global Zone in Trusted Extensions 47
▼ Check and Install Your Label Encodings File 48
▼ Enable IPv6 Networking in Trusted Extensions 52
▼ Configure the Domain of Interpretation 52
▼ Create ZFS Pool for Cloning Zones 54
▼ Reboot and Log In to Trusted Extensions 55
▼ Initialize the Solaris Management Console Server in Trusted Extensions 56
▼ Make the Global Zone an LDAP Client in Trusted Extensions 59
Creating Labeled Zones 62
▼ Run the `txzonemgr` Script 63
▼ Configure the Network Interfaces in Trusted Extensions 64
▼ Name and Label the Zone 68
▼ Install the Labeled Zone 70
▼ Boot the Labeled Zone 71
▼ Verify the Status of the Zone 72
▼ Customize the Labeled Zone 74
▼ Copy or Clone a Zone in Trusted Extensions 75
Adding Network Interfaces and Routing to Labeled Zones 77
▼ Add a Network Interface to Route an Existing Labeled Zone 77
▼ Add a Network Interface That Does Not Use the Global Zone to Route an Existing Labeled Zone 79
▼ Configure a Name Service Cache in Each Labeled Zone 83
Creating Roles and Users in Trusted Extensions 84
▼ Create Rights Profiles That Enforce Separation of Duty 85
▼ Create the Security Administrator Role in Trusted Extensions 88

▼ Create a Restricted System Administrator Role 90
▼ Create Users Who Can Assume Roles in Trusted Extensions 90
▼ Verify That the Trusted Extensions Roles Work 93
▼ Enable Users to Log In to a Labeled Zone 95
Creating Home Directories in Trusted Extensions 95
▼ Create the Home Directory Server in Trusted Extensions 95
▼ Enable Users to Access Their Home Directories in Trusted Extensions 96
Adding Users and Hosts to an Existing Trusted Network 98
▼ Add an NIS User to the LDAP Server 98
Troubleshooting Your Trusted Extensions Configuration 100
`netservices limited` Was Run After Trusted Extensions Was Enabled 100
Cannot Open the Console Window in a Labeled Zone 100
Labeled Zone Is Unable to Access the X Server 101
Additional Trusted Extensions Configuration Tasks 103
▼ How to Copy Files to Portable Media in Trusted Extensions 103
▼ How to Copy Files From Portable Media in Trusted Extensions 105
▼ How to Remove Trusted Extensions From the System 106

5 Configuring LDAP for Trusted Extensions (Tasks) 107
Configuring an LDAP Server on a Trusted Extensions Host (Task Map) 107
Configuring an LDAP Proxy Server on a Trusted Extensions Host (Task Map) 108
Configuring the Sun Java System Directory Server on a Trusted Extensions System 109
▼ Collect Information for the Directory Server for LDAP 109
▼ Install the Sun Java System Directory Server 110
▼ Create an LDAP Client for the Directory Server 112
▼ Configure the Logs for the Sun Java System Directory Server 114
▼ Configure a Multilevel Port for the Sun Java System Directory Server 115
▼ Populate the Sun Java System Directory Server 116
Creating a Trusted Extensions Proxy for an Existing Sun Java System Directory Server 119
▼ Create an LDAP Proxy Server 119
Configuring the Solaris Management Console for LDAP (Task Map) 120
▼ Register LDAP Credentials With the Solaris Management Console 120
▼ Enable the Solaris Management Console to Accept Network Communications 121
▼ Edit the LDAP Toolbox in the Solaris Management Console 122
▼ Verify That the Solaris Management Console Contains Trusted Extensions

Information 124

6 Configuring a Headless System With Trusted Extensions (Tasks) 127
Headless System Configuration in Trusted Extensions (Task Map) 127
▼ Enable Remote Login by `root` User in Trusted Extensions 128
▼ Enable Remote Login by a Role in Trusted Extensions 129
▼ Enable Remote Login From an Unlabeled System 131
▼ Use a Remote Solaris Management Console to Administer in the Files Scope 131
▼ Enable the Remote Display of Administrative GUIs 132
▼ Use the `rlogin` or `ssh` Command to Log In and Administer a Headless System in Trusted Extensions 132

A Site Security Policy 135
Creating and Managing a Security Policy 135
Site Security Policy and Trusted Extensions 136
Computer Security Recommendations 136
Physical Security Recommendations 137
Personnel Security Recommendations 138
Common Security Violations 138
Additional Security References 139
U.S. Government Publications 139
UNIX Security Publications 140
General Computer Security Publications 140
General UNIX Publications 140

B Using CDE Actions to Install Zones in Trusted Extensions 143
Associating Network Interfaces With Zones by Using CDE Actions (Task Map) 143
▼ Specify Two IP Addresses for the System by Using a CDE Action 143
▼ Specify One IP Address for the System by Using a CDE Action 145
Preparing to Create Zones by Using CDE Actions (Task Map) 146
▼ Specify Zone Names and Zone Labels by Using a CDE Action 146
Creating Labeled Zones by Using CDE Actions (Task Map) 148
▼ Install, Initialize, and Boot a Labeled Zone by Using CDE Actions 149
▼ Resolve Local Zone to Global Zone Routing in Trusted CDE 152
▼ Customize a Booted Zone in Trusted Extensions 153

▼ Use the Copy Zone Method in Trusted Extensions 155
▼ Use the Clone Zone Method in Trusted Extensions 156

C **Configuration Checklist for Trusted Extensions** 157
Checklist for Configuring Trusted Extensions 157

Glossary 161

Index 169

Figures

FIGURE 1–1 Administering a Trusted Extensions System: Task Division by Role 29
FIGURE 4–1 Solaris Management Console Initial Window 57
FIGURE 4–2 Trusted Extensions Tools in the Solaris Management Console 58

Tables

TABLE 1–1 Default Host Templates in Trusted Extensions 23
TABLE 1–2 Trusted Extensions Security Defaults for User Accounts 27

Preface

The *Trusted Extensions Configuration Guide* provides procedures for configuring Trusted Extensions on the Oracle Solaris operating system (Oracle Solaris OS). This guide also describes preparing the Oracle Solaris system to support a secure installation of Trusted Extensions.

Note – This Oracle Solaris release supports systems that use the SPARC and x86 families of processor architectures. The supported systems appear in the *Oracle Solaris OS: Hardware Compatibility Lists*. This document cites any implementation differences between the platform types.

In this document, these x86 related terms mean the following:

- x86 refers to the larger family of 64-bit and 32-bit x86 compatible products.
- x64 relates specifically to 64-bit x86 compatible CPUs.
- "32-bit x86" points out specific 32-bit information about x86 based systems.

For supported systems, see the *Oracle Solaris OS: Hardware Compatibility Lists*.

Who Should Use This Guide

This guide is for knowledgeable system administrators and security administrators who are configuring Trusted Extensions software. The level of trust that is required by your site security policy, and your level of expertise, determines who can perform the configuration tasks.

Implementing Site Security

Successfully configuring Trusted Extensions on a system in a way that is consistent with site security requires understanding the security features of Trusted Extensions and your site security policy. Before you start, read Chapter 1, "Security Planning for Trusted Extensions," for information about how to ensure site security when configuring the software.

Trusted Extensions and the Oracle Solaris Operating System

Trusted Extensions runs on top of the Oracle Solaris OS. Because Trusted Extensions software can modify the Oracle Solaris OS, Trusted Extensions can require specific settings for Oracle Solaris installation options. For details, see Chapter 3, "Adding Trusted Extensions Software to the Oracle Solaris OS (Tasks)." Also, Trusted Extensions guides supplement Oracle Solaris guides. As administrators, you need access to Oracle Solaris guides and Trusted Extensions guides.

How This Book Is Organized

Chapter 1, "Security Planning for Trusted Extensions," describes the security issues that you need to consider when configuring Trusted Extensions software on one or more Oracle Solaris systems.

Chapter 2, "Configuration Roadmap for Trusted Extensions," contains task maps for adding Trusted Extensions software to Oracle Solaris systems.

Chapter 3, "Adding Trusted Extensions Software to the Oracle Solaris OS (Tasks)," provides instructions on preparing an Oracle Solaris system for Trusted Extensions software. It also includes instructions on enabling Trusted Extensions.

Chapter 4, "Configuring Trusted Extensions (Tasks)," provides instructions on configuring Trusted Extensions software on a system with a monitor.

Chapter 5, "Configuring LDAP for Trusted Extensions (Tasks)," provides instructions on configuring LDAP for Trusted Extensions.

Chapter 6, "Configuring a Headless System With Trusted Extensions (Tasks)," describes how to configure and administer Trusted Extensions software on a headless system.

Appendix A, "Site Security Policy," addresses site security policy and places Trusted Extensions in the context of wider organizational and site security.

Appendix B, "Using CDE Actions to Install Zones in Trusted Extensions," describes how to configure labeled zones by using Trusted CDE actions.

Appendix C, "Configuration Checklist for Trusted Extensions," provides a configuration checklist for the initial setup team.

Glossary defines selected terms and phrases that are used in this guide.

How the Trusted Extensions Guides Are Organized

The following table lists the topics that are covered in the Trusted Extensions guides and the audience for each guide.

Title of Guide	Topics	Audience
Solaris Trusted Extensions Transition Guide	Obsolete. Provides an overview of the differences between Trusted Solaris 8 software, Solaris 10 software, and Trusted Extensions software. For this release, the *What's New* document for Oracle Solaris provides an overview of Trusted Extensions changes.	All
Solaris Trusted Extensions Reference Manual	Obsolete. Provides Trusted Extensions man pages for the Solaris 10 11/06 and Solaris 10 8/07 releases of Trusted Extensions. For this release, Trusted Extensions man pages are included with the Oracle Solaris man pages.	All
Trusted Extensions User's Guide	Describes the basic features of Trusted Extensions. This book contains a glossary.	End users, administrators, developers
Solaris Trusted Extensions Installation and Configuration for Solaris 10 11/06 and Solaris 10 8/07 Releases	Obsolete. Describes how to plan for, install, and configure Trusted Extensions for the Solaris 10 11/06 and Solaris 10 8/07 releases of Trusted Extensions.	Administrators, developers
Trusted Extensions Configuration Guide	Starting with the Solaris 10 5/08 release, describes how to enable and initially configure Trusted Extensions. Replaces *Solaris Trusted Extensions Installation and Configuration for the Solaris 10 11/06 and Solaris 10 8/07 Releases*.	Administrators, developers
Trusted Extensions Administrator's Procedures	Shows how to perform specific administration tasks.	Administrators, developers
Trusted Extensions Developer's Guide	Describes how to develop applications with Trusted Extensions.	Developers, administrators
Trusted Extensions Label Administration	Provides information about how to specify label components in the label encodings file.	Administrators
Compartmented Mode Workstation Labeling: Encodings Format	Describes the syntax used in the label encodings file. The syntax enforces the various rules for well-formed labels for a system.	Administrators

Related Installation Guides

The following guides contain information that is useful when you prepare for Trusted Extensions software.

Oracle Solaris 10 8/11 Installation Guide: Basic Installations – Provides guidance on the installation options for the Oracle Solaris OS

Oracle Solaris 10 8/11 Installation Guide: Custom JumpStart and Advanced Installations – Provides guidance on installation methods and configuration options

Oracle Solaris 10 8/11 Installation Guide: Planning for Installation and Upgrade – Provides guidance on installing an upgrade of the Oracle Solaris OS

Related References

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 (CDE)

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

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` or visit `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` if you are hearing impaired.

Typographic Conventions

The following table describes the typographic conventions that are used in this book.

TABLE P–1 Typographic Conventions

Typeface	Description	Example
`AaBbCc123`	The names of commands, files, and directories, and onscreen computer output	Edit your `.login` file. Use `ls -a` to list all files. `machine_name% you have mail.`

TABLE P–1 Typographic Conventions *(Continued)*

Typeface	Description	Example
AaBbCc123	What you type, contrasted with onscreen computer output	`machine_name%` **`su`** `Password:`
aabbcc123	Placeholder: replace with a real name or value	The command to remove a file is `rm` *filename*.
AaBbCc123	Book titles, new terms, and terms to be emphasized	Read Chapter 6 in the *User's Guide*. A *cache* is a copy that is stored locally. Do *not* save the file. **Note:** Some emphasized items appear bold online.

Shell Prompts in Command Examples

The following table shows the default UNIX system prompt and superuser prompt for shells that are included in the Oracle Solaris OS. Note that the default system prompt that is displayed in command examples varies, depending on the Oracle Solaris release.

TABLE P–2 Shell Prompts

Shell	Prompt
Bash shell, Korn shell, and Bourne shell	`$`
Bash shell, Korn shell, and Bourne shell for superuser	`#`
C shell	`machine_name%`
C shell for superuser	`machine_name#`

◆ ◆ ◆ CHAPTER 1

Security Planning for Trusted Extensions

The Trusted Extensions feature of Oracle Solaris implements a portion of your site's security policy in software. This chapter provides an overview of the security and administrative aspects of configuring the software.

- "Planning for Security in Trusted Extensions" on page 19
- "Results of Enabling Trusted Extensions From an Administrator's Perspective" on page 30

Planning for Security in Trusted Extensions

This section outlines the planning that is required before enabling and configuring Trusted Extensions software.

- "Understanding Trusted Extensions" on page 20
- "Understanding Your Site's Security Policy" on page 20
- "Planning Who Will Configure Trusted Extensions" on page 21
- "Devising a Label Strategy" on page 21
- "Planning System Hardware and Capacity for Trusted Extensions" on page 22
- "Planning Your Trusted Network" on page 22
- "Planning Your Labeled Zones in Trusted Extensions" on page 23
- "Planning for Multilevel Access" on page 25
- "Planning for the LDAP Naming Service in Trusted Extensions" on page 25
- "Planning for Auditing in Trusted Extensions" on page 26
- "Planning User Security in Trusted Extensions" on page 26
- "Devising a Configuration Strategy for Trusted Extensions" on page 27
- "Resolving Additional Issues Before Enabling Trusted Extensions" on page 29
- "Backing Up the System Before Enabling Trusted Extensions" on page 29

For a checklist of Trusted Extensions configuration tasks, see Appendix C, "Configuration Checklist for Trusted Extensions." If you are interested in localizing your site, see "For International Customers of Trusted Extensions" on page 22. If you are interested in running an evaluated configuration, see "Understanding Your Site's Security Policy" on page 20.

Understanding Trusted Extensions

The enabling and configuration of Trusted Extensions involves more than loading executable files, specifying your site's data, and setting configuration variables. Considerable background knowledge is required. Trusted Extensions software provides a labeled environment that is based on two Oracle Solaris features:

- Capabilities that in most UNIX environments are assigned to superuser are handled by discrete administrative roles.
- The ability to override security policy can be assigned to specific users and applications.

In Trusted Extensions, access to data is controlled by special security tags. These tags are called labels. Labels are assigned to users, processes, and objects, such as data files and directories. These labels supply mandatory access control (MAC), in addition to UNIX permissions, or discretionary access control (DAC).

Understanding Your Site's Security Policy

Trusted Extensions effectively enables you to integrate your site's security policy with the Oracle Solaris OS. Thus, you need to have a good understanding of the scope of your policy and how Trusted Extensions software can implement that policy. A well-planned configuration must provide a balance between consistency with your site security policy and convenience for users who are working on the system.

Trusted Extensions is configured by default to conform with the Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408) at Assurance Level EAL4 against the following protection profiles:

- Labeled Security Protection Profile
- Controlled Access Protection Profile
- Role-Based Access Control Protection Profile

To meet these evaluated levels, you must configure LDAP as the naming service. Note that your configuration might no longer conform with the evaluation if you do any of the following:

- Change the kernel switch settings in the `/etc/system` file.
- Turn off auditing or device allocation.
- Change the default entries in public files in the `/usr` directory.

For more information, see the Common Criteria web site (`http://www.commoncriteriaportal.org/`).

Planning Who Will Configure Trusted Extensions

The `root` role or the System Administrator role is responsible for enabling Trusted Extensions. You can create roles to divide administrative responsibilities among several functional areas:

- 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.
- More limited roles can be configured. For example, an operator could be responsible for backing up files.

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

- Which users are handling which administrative responsibilities
- Which non-administrative users are allowed to run trusted applications, meaning which users are permitted to override security policy, when necessary
- Which users have access to which groups of data

Devising a Label Strategy

Planning labels requires setting up a hierarchy of sensitivity levels and a categorization of information on your system. The `label_encodings` file contains this type of information for your site. You can use one of the `label_encodings` files that are supplied with Trusted Extensions software. You could also modify one of the supplied files, or create a new `label_encodings` file that is specific to your site. The file must include the Oracle-specific local extensions, at least the `COLOR NAMES` section.

Caution – If you are supplying a `label_encodings` file, best practice is to have the final version of the file before the labels are verified by the system. Labels are verified during the first boot after the Trusted Extensions service is enabled.

Planning labels also involves planning the label configuration. After enabling the Trusted Extensions service, you need to decide if the system must allow logins at multiple labels, or if the system can be configured with one user label only. For example, an LDAP server is a good candidate to have one labeled zone. For local administration of the server, you would create a zone at the minimum label. To administer the system, the administrator logs in, and from the user workspace assumes the appropriate role.

For more information, see *Trusted Extensions Label Administration*. You can also refer to *Compartmented Mode Workstation Labeling: Encodings Format*.

For International Customers of Trusted Extensions

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

Planning System Hardware and Capacity for Trusted Extensions

System hardware includes the system itself and its attached devices. Such devices include tape drives, microphones, CD-ROM drives, and disk packs. Hardware capacity includes system memory, network interfaces, and disk space.

- Follow the recommendations for installing an Oracle Solaris release, as described in the installation guide for this release and the Installation section of the *Release Notes* for this release.
- Trusted Extensions features can add to those recommendations:
  - Memory beyond the suggested minimum is required on the following systems:
    - Systems that run the Solaris Management Console, a required administrative GUI
    - Systems that run at more than one sensitivity label
    - Systems that are used by users who can assume an administrative role
  - More disk space is required on the following systems:
    - Systems that store files at more than one label
    - Systems whose users can assume an administrative role

Planning Your Trusted Network

For assistance in planning network hardware, see Chapter 2, "Planning Your TCP/IP Network (Tasks)," in *System Administration Guide: IP Services*.

As in any client-server network, you need to identify hosts by their function, that is, server or client, and configure the software appropriately. For assistance in planning, see *Solaris 10 5/09 Installation Guide: Custom JumpStart and Advanced Installations*.

Trusted Extensions software recognizes two host types, cipso and unlabeled. Each host type has a default security template, as shown in Table 1–1.

TABLE 1–1 Default Host Templates in Trusted Extensions

Host Type	Template Name	Purpose
`unlabeled`	`admin_low`	Is used to identify untrusted hosts that can communicate with the global zone. Such hosts send packets that do not include labels. For more information, see unlabeled system.
`cipso`	`cipso`	Is used to identify hosts or networks that send CIPSO packets. CIPSO packets are labeled.

If your network can be reached by other networks, you need to specify accessible domains and hosts. You also need to identify which Trusted Extensions hosts are going to serve as gateways. You need to identify the label accreditation range for these gateways, and the sensitivity label at which data from other hosts can be viewed.

The `smtnrhtp(1M)` man page provides a complete description of each host type with several examples.

Planning Your Labeled Zones in Trusted Extensions

Trusted Extensions software is added to Oracle Solaris in the global zone. You then configure non-global zones that are labeled. You can create one labeled zone for every unique label, though you do not need to create a zone for every label in your `label_encodings` file.

Part of zone configuration is configuring the network. By default, labeled zones are configured to communicate with the global zone. Additionally, you can configure the zones on the system to communicate with other zones on the network.

- The X server that runs the desktop display is available only from the global zone. Starting in the Solaris 10 10/08 release, the loopback interface, `lo0`, can be used to communicate with the global zone. Therefore, the desktop display is available to non-global zones over `lo0`.
- By default, non-global zones cannot communicate with untrusted hosts. Starting in the Solaris 10 10/08 release, you can configure each non-global zone with a unique default route that does not use the global zone.

Trusted Extensions Zones and Oracle Solaris Zones

Labeled zones differ from typical Oracle Solaris zones. Labeled zones are primarily used to segregate data. In Trusted Extensions, regular users cannot remotely log in to a labeled zone. The only interactive interface to a labeled zone is by using the zone console. Only root can gain access to the zone console.

Zone Creation in Trusted Extensions

To create a labeled zone involves copying the entire Oracle Solaris OS, and then starting the services for the Oracle Solaris OS in every zone. The process can be time-consuming. A faster process is to create one zone, then to copy that zone or clone the contents of that zone. The following table describes your options for zone creation in Trusted Extensions.

Zone Creation Method	Effort Required	Characteristics of This Method
Create each labeled zone from scratch.	Configure, initialize, install, customize, and boot each labeled zone.	■ This method is supported, and is useful for creating one or two additional zones. The zones can be upgraded. ■ This method is time-consuming.
Create additional labeled zones from a copy of the first labeled zone.	Configure, initialize, install, and customize one zone. Use this zone as a template for additional labeled zones.	■ This method is supported, and is faster than creating zones from scratch. The zones can be upgraded. Use the Copy Zone method if you want Oracle Support to help you with any zone difficulties. ■ This method uses UFS. UFS does not offer the additional isolation for zones that ZFS offers.
Create additional labeled zones from a ZFS snapshot of the first labeled zone.	Set up a ZFS pool from a partition that you set aside during Oracle Solaris installation. Configure, initialize, install, and customize one zone. Use this zone as a ZFS snapshot for additional labeled zones.	■ This method uses ZFS, and is the fastest method. This method makes every zone a file system, and thus provides more isolation than UFS. ZFS uses much less disk space. ■ If you are testing Trusted Extensions and can reinstall the zones rather than upgrade, this method might be a good choice. This method can be useful on systems whose contents are not volatile, because the system can quickly be reinstalled to a usable state. ■ This method is *not* supported. Zones that are created by using this method *cannot be upgraded* when a later version of the OS is released.

Oracle Solaris zones affect package installation and patching. For more information, see the following references:

- Chapter 25, "About Packages and Patches on a Solaris System With Zones Installed (Overview)," in *System Administration Guide: Oracle Solaris Containers-Resource Management and Oracle Solaris Zones*
- Solaris Zones and Containers FAQ (`http://hub.opensolaris.org/bin/view/Community+Group+zones/faq`)

Planning for Multilevel Access

Typically, printing and NFS are configured as multilevel services. To access multilevel services, a properly configured system requires that every zone be able to access one or more network addresses. The following configurations provide multilevel services:

- **Exclusive IP stack –** As in the Oracle Solaris OS, one IP address is assigned for every zone, including the global zone. By default, a Virtual Network Information Card (VNIC) is created for each labeled zone.

  A refinement of this configuration is to assign a separate network information card (NIC) to each zone. Such a configuration is used to physically separate the single-label networks that are associated with each NIC.
- **Shared IP stack –** One `all-zones` address is assigned. In this configuration, the system cannot be a multilevel NFS server. One or more zones can have zone-specific addresses.

A system that meets the following two conditions cannot provide multilevel services:

- One IP address is assigned that the global zone and the labeled zones share.
- No zone-specific addresses are assigned.

Tip – If users in labeled zones are not supposed to have access to a local multilevel printer, and you do not need NFS exports of home directories, then you can assign one IP address to a system that you configure with Trusted Extensions. On such a system, multilevel printing is not supported, and home directories cannot be shared. A typical use of this configuration is on a laptop.

Planning for the LDAP Naming Service in Trusted Extensions

If you are not planning to install a network of labeled systems, then you can skip this section.

If you plan to run Trusted Extensions on a network of systems, use LDAP as the naming service. For Trusted Extensions. a populated Sun Java System Directory Server (LDAP server) is

required when you configure a network of systems. If your site has an existing LDAP server, you can populate the server with Trusted Extensions databases. To access the server, you set up an LDAP proxy on a Trusted Extensions system.

If your site does not have an existing LDAP server, you create an LDAP server on a system that is running Trusted Extensions software. The procedures are described in Chapter 5, "Configuring LDAP for Trusted Extensions (Tasks)."

Planning for Auditing in Trusted Extensions

By default, auditing is enabled when Trusted Extensions is installed. Therefore, by default, `root` login, screenlock, and logout are audited. To audit the users who are configuring the system, you can create roles early in the configuration process. When these roles configure the system, the audit records include the login user who assumes the role. See "Creating Roles and Users in Trusted Extensions" on page 84.

Planning auditing in Trusted Extensions is the same as in the Oracle Solaris OS. For details, see Part VII, "Auditing in Oracle Solaris," in *System Administration Guide: Security Services*. While Trusted Extensions adds classes, events, and audit tokens, the software does not change how auditing is administered. For Trusted Extensions additions to auditing, see Chapter 18, "Trusted Extensions Auditing (Overview)," in *Trusted Extensions Administrator's Procedures*.

Planning User Security in Trusted Extensions

Trusted Extensions software provides reasonable security defaults for users. These security defaults are listed in Table 1–2. Where two values are listed, the first value is the default. The security administrator can modify these defaults to reflect the site's security policy. After the security administrator sets the defaults, the system administrator can create all the users, who inherit the established defaults. For descriptions of the keywords and values for these defaults, see the `label_encodings(4)` and `policy.conf(4)` man pages.

TABLE 1–2 Trusted Extensions Security Defaults for User Accounts

File name	Keyword	Value
/etc/security/policy.conf	IDLECMD	lock | logout
	IDLETIME	30
	CRYPT_ALGORITHMS_ALLOW	1,2a,md5,5,6
	CRYPT_DEFAULT	_unix_
	LOCK_AFTER_RETRIES	no | yes
	PRIV_DEFAULT	basic
	PRIV_LIMIT	all
	AUTHS_GRANTED	solaris.device.cdrw
	PROFS_GRANTED	Basic Solaris User
LOCAL DEFINITIONS section of /etc/security/tsol/label_encodings	Default User Sensitivity Label	PUBLIC
	Default User Clearance	CNF INTERNAL USE ONLY

Note – The IDLECMD and IDLETIME variables apply to the login user's session. If the login user assumes a role, the user's IDLECMD and IDLETIME values are in effect for that role.

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

Devising a Configuration Strategy for Trusted Extensions

Allowing the root user to configure Trusted Extensions software is not a secure strategy. The following describes the configuration strategy from the most secure strategy to the least secure strategy:

- A two-person team configures the software. The configuration process is audited.

  Two people are at the computer when the software is enabled. Early in the configuration process, this team creates roles, and local users who can assume those roles. The team also sets up auditing to audit events that are executed by roles. After roles are assigned to users,

and the computer is rebooted, the software enforces task division by role. The audit trail provides a record of the configuration process. For an illustration of a secure configuration process, see Figure 1–1.

Note – If site security requires separation of duty, a trusted administrator completes "Create Rights Profiles That Enforce Separation of Duty" on page 85 before creating users or roles. In this customized configuration, one role manages security, including users' security attributes. The other role manages the non-security attributes of systems and users.

- One person enables and configures the software by assuming the appropriate role. The configuration process is audited.

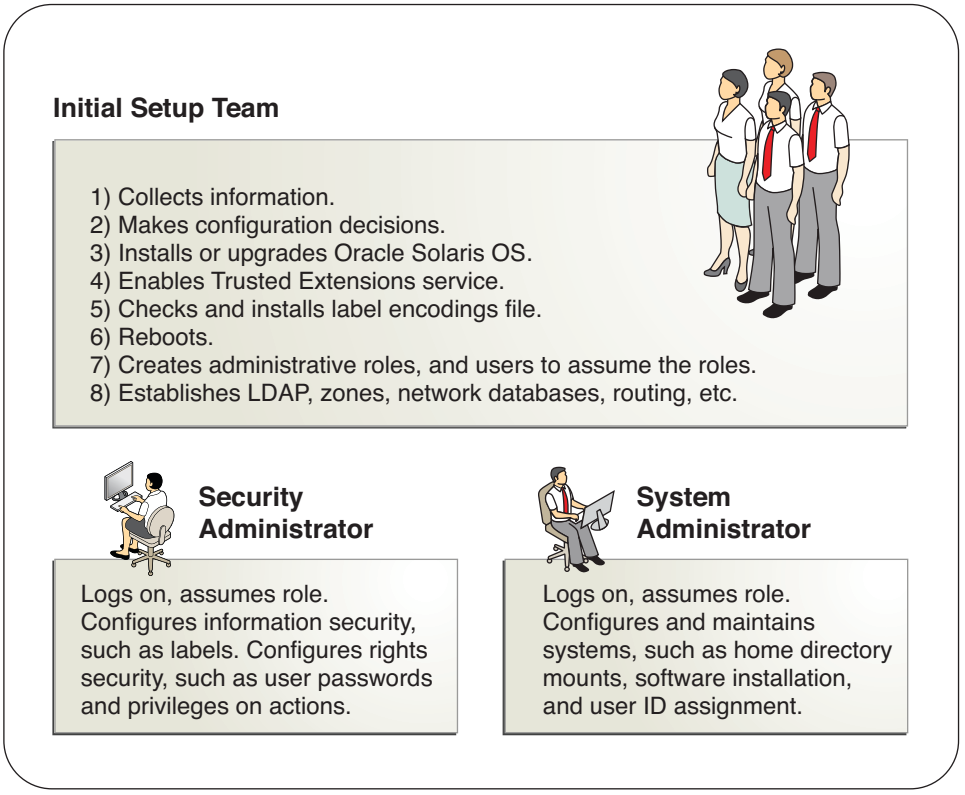
  Early in the configuration process, the `root` user creates a local user and roles. This user also sets up auditing to audit events that are executed by roles. Once roles have been assigned to the local user, and the computer is rebooted, the software enforces task division by role. The audit trail provides a record of the configuration process.
- One person enables and configures the software by assuming the appropriate role. The configuration process is not audited.

  By using this strategy, no record is kept of the configuration process.
- The `root` user enables and configures the software. The configuration process is audited.

  The team sets up auditing to audit every event that `root` performs during configuration. With this strategy, the team must determine which events to audit. The audit trail does not include the name of the user who is acting as `root`.
- The `root` user enables and configures the software.

Task division by role is shown in the following figure. The security administrator configures auditing, protects file systems, sets device policy, determines which programs require privilege to run, and protects users, among other tasks. The system administrator shares and mounts file systems, installs software packages, and creates users, among other tasks.

FIGURE 1–1 Administering a Trusted Extensions System: Task Division by Role



Resolving Additional Issues Before Enabling Trusted Extensions

Before configuring Trusted Extensions, you must physically protect your systems, decide which labels to attach to zones, and resolve other security issues. For the procedures, see "Collecting Information and Making Decisions Before Enabling Trusted Extensions" on page 41.

Backing Up the System Before Enabling Trusted Extensions

If your system has files that must be saved, perform a backup before enabling the Trusted Extensions service. 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.

Results of Enabling Trusted Extensions From an Administrator's Perspective

After the Trusted Extensions software is enabled and the system is rebooted, the following security features are in place. Many features are configurable by the security administrator.

- Auditing is enabled.
- An Oracle label_encodings file is installed and configured.
- Two trusted desktops are added. Solaris Trusted Extensions (CDE) is the trusted version of CDE. Solaris Trusted Extensions (JDS) is the trusted version of the Sun Java Desktop System. Each windowing environment creates Trusted Path workspaces in the global zone.
- As in the Oracle Solaris OS, rights profiles for roles are defined. As in the Oracle Solaris OS, roles are not defined.

  To use roles to administer Trusted Extensions, you must create the roles. During configuration, you create the Security Administrator role.
- Three Trusted Extensions network databases, `tnrhdb`, `tnrhtp`, and `tnzonecfg` are added. The databases are administered by using the Security Templates tool and the Trusted Network Zones tool in the Solaris Management Console.
- Trusted Extensions provides GUIs to administer the system. Some GUIs are extensions to an Oracle Solaris GUI.
  - In Trusted CDE, administrative actions are provided in the Trusted_Extensions folder. Some of these actions are used when you initially configure Trusted Extensions. The tools are introduced in Chapter 2, "Trusted Extensions Administration Tools," in *Trusted Extensions Administrator's Procedures*.
  - The `txzonemgr` script enables administrators to configure Trusted Extensions zones and networking. For more information, see the `txzonemgr(1M)` man page.
  - A trusted editor enables administrators to modify local administrative files. In Trusted CDE, the Admin Editor action invokes a trusted editor.
  - The Device Allocation Manager manages attached devices.
  - The Solaris Management Console provides Java-based tools to manage local and network administrative databases. The use of these tools is required for managing the trusted network, zones, and users.

◆ ◆ ◆ CHAPTER 2

Configuration Roadmap for Trusted Extensions

This chapter outlines the tasks for enabling and configuring Trusted Extensions software.

Task Map: Preparing an Oracle Solaris System for Trusted Extensions

Ensure that the Oracle Solaris OS on which you plan to run Trusted Extensions supports the features of Trusted Extensions that you plan to use. Complete one of the two tasks that are described in the following task map.

Task	For Instructions
Prepare an existing or upgraded Oracle Solaris installation for Trusted Extensions.	"Prepare an Installed Oracle Solaris System for Trusted Extensions" on page 39
Install the Oracle Solaris OS with Trusted Extensions features in mind.	"Install an Oracle Solaris System to Support Trusted Extensions" on page 38

Task Map: Preparing For and Enabling Trusted Extensions

To prepare a Trusted Extensions system before configuring it, complete the tasks that are described in the following task map.

Task	For Instructions
Complete the preparation of your Oracle Solaris system.	"Task Map: Preparing an Oracle Solaris System for Trusted Extensions" on page 31

Task	For Instructions
Back up your system.	For a Trusted Solaris 8 system, back up the system as described in the documentation for your release. A labeled backup can be restored to each identically labeled zone.
	For an Oracle Solaris system, see *System Administration Guide: Basic Administration*.
Gather information and make decisions about your system and your Trusted Extensions network.	"Collecting Information and Making Decisions Before Enabling Trusted Extensions" on page 41
Enable Trusted Extensions.	"Enable Trusted Extensions" on page 44
Configure the system.	For a system with a monitor, see "Task Map: Configuring Trusted Extensions" on page 33.
	For a headless system, see "Headless System Configuration in Trusted Extensions (Task Map)" on page 127.
	For a Sun Ray, see *Sun Ray Server Software 4.1 Installation and Configuration Guide for the Solaris Operating System*. For the Sun Ray 5 release, see the Sun Ray Server 4.2 and Sun Ray Connector 2.2 Documentation (`http://www.oracle.com/technetwork/server-storage/sunrayproducts/overview/index.html?ssSourceSiteId=ocomen`) web site. Together, this server and client comprise the *Sun Ray 5* package. To configure initial client-server communication, see "Configuring Trusted Network Databases (Task Map)" in *Trusted Extensions Administrator's Procedures*.
	For a laptop, go to the OpenSolaris Community: Security web page (`http://hub.opensolaris.org/bin/view/Community+Group+security/`). Click Trusted Extensions. On the Trusted Extensions page under Laptop Configurations, click `Laptop instructions`.
	To prevent networks from communicating with the global zone, configure the `vni0` interface. For an example, see the `Laptop instructions`. Starting in the Solaris 10 10/08 release, you do not need to configure the `vni0` interface. By default, the `lo0` interface is an `all-zones` interface. For dhcp to work with Trusted Extensions, other laptop instructions still apply.

Task Map: Configuring Trusted Extensions

For a secure configuration process, create roles early. The order of tasks when roles configure the system is shown in the following task map.

1. Configure the global zone.

Tasks	For Instructions
Protect machine hardware by requiring a password to change hardware settings.	"Controlling Access to System Hardware" in *System Administration Guide: Security Services*
Configure labels. Labels *must* be configured for your site. If you plan to use the default `label_encodings` file, you can skip this task.	"Check and Install Your Label Encodings File" on page 48
If you are running an IPv6 network, you modify the `/etc/system` file to enable IP to recognize labeled packets.	"Enable IPv6 Networking in Trusted Extensions" on page 52
If the CIPSO Domain of Interpretation (DOI) of your network nodes is different from 1, specify the DOI in the `/etc/system` file.	"Configure the Domain of Interpretation" on page 52
If you plan to use a ZFS snapshot to clone zones, create the ZFS pool.	"Create ZFS Pool for Cloning Zones" on page 54
Boot to activate a labeled environment. Upon login, you are in the global zone. The system's `label_encodings` file enforces mandatory access control (MAC).	"Reboot and Log In to Trusted Extensions" on page 55
Initialize the Solaris Management Console. This GUI is used to label zones, among other tasks.	"Initialize the Solaris Management Console Server in Trusted Extensions" on page 56
Create the Security Administrator role and other roles that you plan to use locally. You create these roles just as you would create them in the Oracle Solaris OS. You can delay this task until the end. For the consequences, see "Devising a Configuration Strategy for Trusted Extensions" on page 27.	"Creating Roles and Users in Trusted Extensions" on page 84 "Verify That the Trusted Extensions Roles Work" on page 93

Skip the next set of tasks if you are using local files to administer the system.

2. Configure a naming service.

Tasks	For Instructions
If you plan to use files to administer Trusted Extensions, you can skip the following tasks.	No configuration is required for the files naming service.
If you have an existing Sun Java System Directory Server (LDAP server), add Trusted Extensions databases to the server. Then make your first Trusted Extensions system a proxy of the LDAP server. If you do not have an LDAP server, then configure your first system as the server.	Chapter 5, "Configuring LDAP for Trusted Extensions (Tasks)"
Manually set up an LDAP toolbox for the Solaris Management Console. The toolbox can be used to modify Trusted Extensions attributes on network objects.	"Configuring the Solaris Management Console for LDAP (Task Map)" on page 120
For systems that are not the LDAP server or proxy server, make them an LDAP client.	"Make the Global Zone an LDAP Client in Trusted Extensions" on page 59
In the LDAP scope, create the Security Administrator role and other roles that you plan to use. You can delay this task until the end. For the consequences, see "Devising a Configuration Strategy for Trusted Extensions" on page 27.	"Creating Roles and Users in Trusted Extensions" on page 84 "Verify That the Trusted Extensions Roles Work" on page 93

3. Create labeled zones.

Tasks	For Instructions
Run the `txzonemgr` command. Follow the menus to configure the network interfaces, then create and customize the first labeled zone. Then, copy or clone the rest of the zones.	"Creating Labeled Zones" on page 62
Or, use Trusted CDE actions.	Appendix B, "Using CDE Actions to Install Zones in Trusted Extensions"
(Optional) After all zones are successfully customized, add zone-specific network addresses and default routing to the labeled zones.	"Adding Network Interfaces and Routing to Labeled Zones" on page 77

The following tasks might be necessary in your environment.

4. Complete system setup.

Tasks	For Instructions
Identify additional remote hosts that require a label, one or more multilevel ports, or a different control message policy.	"Configuring Trusted Network Databases (Task Map)" in *Trusted Extensions Administrator's Procedures*
Create a multilevel home directory server, then automount the installed zones.	"Creating Home Directories in Trusted Extensions" on page 95
Configure auditing, mount file systems, and perform other tasks before enabling users to log in to the system.	*Trusted Extensions Administrator's Procedures*
Add users from an NIS environment to your LDAP server.	"Add an NIS User to the LDAP Server" on page 98
Add a host and its labeled zones to the LDAP server.	"Configuring Trusted Network Databases (Task Map)" in *Trusted Extensions Administrator's Procedures*

◆ ◆ ◆ CHAPTER 3

Adding Trusted Extensions Software to the Oracle Solaris OS (Tasks)

This chapter describes how to prepare the Oracle Solaris OS for Trusted Extensions software. This chapter also describes the information you need before enabling Trusted Extensions. Instructions on how to enable Trusted Extensions is also provided.

- "Initial Setup Team Responsibilities" on page 37
- "Installing or Upgrading the Oracle Solaris Operating System for Trusted Extensions" on page 38
- "Collecting Information and Making Decisions Before Enabling Trusted Extensions" on page 41
- "Enabling the Trusted Extensions Service" on page 44

Initial Setup Team Responsibilities

Trusted Extensions software is designed to be enabled and configured by two people with distinct responsibilities. However, the Oracle Solaris installation program does not enforce this two-role task division. Instead, task division is enforced by roles. Because roles and users are not created until after installation, it is a good practice to have an initial setup team of at least two people present to enable and configure Trusted Extensions software.

Installing or Upgrading the Oracle Solaris Operating System for Trusted Extensions

The choice of Oracle Solaris installation options can affect the use and security of Trusted Extensions:

- To properly support Trusted Extensions, you must install the underlying Oracle Solaris OS securely. For Oracle Solaris installation choices that affect Trusted Extensions, see "Install an Oracle Solaris System to Support Trusted Extensions" on page 38.
- If you have been using the Oracle Solaris OS, check your current configuration against the requirements for Trusted Extensions. For configuration choices that affect Trusted Extensions, see "Prepare an Installed Oracle Solaris System for Trusted Extensions" on page 39.

▼ Install an Oracle Solaris System to Support Trusted Extensions

This task applies to fresh installations of the Oracle Solaris OS. If you are upgrading, see "Prepare an Installed Oracle Solaris System for Trusted Extensions" on page 39.

- **When installing the Oracle Solaris OS, take the recommended action on the following installation choices.**

  The choices follow the order of Oracle Solaris installation questions. Installation questions that are not mentioned in this table do not affect Trusted Extensions.

Oracle Solaris Option	Trusted Extensions Behavior	Recommended Action
NIS naming service NIS+ naming service	Trusted Extensions supports files and LDAP for a naming service. For host name resolution, DNS can be used.	Do not choose NIS or NIS+. You can choose None, which is equivalent to files. Later, you can configure LDAP to work with Trusted Extensions.
Upgrade	Trusted Extensions installs labeled zones with particular security characteristics.	If you are upgrading, go to "Prepare an Installed Oracle Solaris System for Trusted Extensions" on page 39.
`root` password	Administration tools in Trusted Extensions require passwords. If the `root` user does not have a password, then `root` cannot configure the system.	Provide a `root` password. Do not change the default `crypt_unix` password encryption method. For details, see "Managing Password Information" in *System Administration Guide: Security Services*.

Oracle Solaris Option	Trusted Extensions Behavior	Recommended Action
Developer Group	Trusted Extensions uses the Solaris Management Console to administer the network. The End User group and smaller groups do not install the packages for the Solaris Management Console.	On any system that you plan to use to administer other systems, do not install the End User, Core, or Reduced Networking Group.
Custom Install	Because Trusted Extensions installs zones, you might need more disk space in partitions than the default installation supplies.	Choose Custom Install, and lay out the partitions. Consider adding extra swap space for roles. If you plan to clone zones, create a 2000 MB partition for the ZFS pool. For auditing files, best practice is to create a dedicated partition.

▼ Prepare an Installed Oracle Solaris System for Trusted Extensions

This task applies to Oracle Solaris systems that have been in use, and on which you plan to run Trusted Extensions. Also, to run Trusted Extensions on an upgraded Oracle Solaris system, follow this procedure. Other tasks that might modify an installed Oracle Solaris system can be done during Trusted Extensions configuration.

Before You Begin Trusted Extensions cannot be enabled in some Oracle Solaris environments:

- If your system is part of a cluster, Trusted Extensions cannot be enabled on the system.
- The enabling of Trusted Extensions in an alternate boot environment (BE) is not supported. Trusted Extensions can only be enabled in the current boot environment.

1 If non-global zones are installed on your system, remove them.

Or, you can re-install the Oracle Solaris OS. If you are going to re-install the Oracle Solaris OS, follow the instructions in "Install an Oracle Solaris System to Support Trusted Extensions" on page 38.

Trusted Extensions use branded zones.

2 If your system does not have a `root` password, create one.

Administration tools in Trusted Extensions require passwords. If the `root` user does not have a password, then `root` cannot configure the system.

Use the default `crypt_unix` password encryption method for the `root` user. For details, see "Managing Password Information" in *System Administration Guide: Security Services*.

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

3 If you plan to administer the site from this system, add the Oracle Solaris packages for the Solaris Management Console.

Trusted Extensions uses the Solaris Management Console to administer the network. If your system was installed with the End User group or a smaller group, the system does not have the packages for the Solaris Management Console.

4 If you have created an `xorg.conf` file, you need to modify it.

Add the following line to the end of the Module section in the `/etc/X11/xorg.conf` file.

```
load "xtsol"
```

Note – By default, the `xorg.conf` file does not exist. Do nothing if this file does not exist.

5 In the Solaris 10 9/09 and Solaris 10 9/10 releases, if your system is part of an Oracle Solaris Cluster configuration, you can enable Trusted Extensions in the cluster.

Note – Applications must run only in Oracle Solaris Cluster zone clusters.

For more information about Oracle Solaris Cluster support of Trusted Extensions, see "How to Prepare for Trusted Extensions Use With Zone Clusters" in Chapter 7, "Creating Non-Global Zones and Zone Clusters" in the *Oracle Solaris Cluster Software Installation Guide*.

6 If you are upgrading a Trusted Extensions system, read the following before upgrading the system:

- Chapter 1, "What's New in the Solaris 10 10/08 Release," in *Solaris 10 What's New*
- *Solaris 10 10/08 Release Notes*

Tip – To find pertinent information, search for the string `Trusted Extensions`.

7 If you plan to clone zones, create a partition for the ZFS pool.

To decide on your zone creation method, see "Planning Your Labeled Zones in Trusted Extensions" on page 23.

8 **If you plan to install labeled zones on this system, check that your partitions have sufficient disk space for zones.**

Most systems that are configured with Trusted Extensions install labeled zones. Labeled zones can require more disk space than the installed system has set aside.

However, some Trusted Extensions systems do not require that labeled zones be installed. For example, a multilevel printing server, a multilevel LDAP server, or a multilevel LDAP proxy server do not require labeled zones to be installed. These systems might not need the extra disk space.

9 **(Optional) Add extra swap space for roles.**

Roles administer Trusted Extensions. Consider adding extra swap for role processes.

10 **(Optional) Dedicate a partition for audit files.**

Trusted Extensions enables auditing by default. For audit files, best practice is to create a dedicated partition.

11 **(Optional) To run a hardened configuration, run the `netservices limited` command before you enable Trusted Extensions.**

```
# netservices limited
```

Collecting Information and Making Decisions Before Enabling Trusted Extensions

For each system on which Trusted Extensions is going to be configured, you need to know some information, and make some decisions about configuration. For example, because you are going to create labeled zones, you might want to set aside disk space where the zones can be cloned as a ZFS file system. ZFS provides additional isolation for the zones.

▼ Collect System Information Before Enabling Trusted Extensions

1 **Determine the system's main hostname and IP address.**

The hostname is the name of the host on the network, and is the global zone. On an Oracle Solaris system, the `getent` command returns the hostname, as in:

```
# getent hosts machine1
192.168.0.11   machine1
```

2 **Determine the IP address assignments for labeled zones.**

A system with two IP addresses can function as a multilevel server. A system with one IP address must have access to a multilevel server in order to print or perform multilevel tasks. For a discussion of IP address options, see "Planning for Multilevel Access" on page 25.

Most systems require a second IP address for the labeled zones. For example, the following is a host with a second IP address for labeled zones:

```
# getent hosts machine1-zones
192.168.0.12   machine1-zones
```

3 **Collect LDAP configuration information.**

For the LDAP server that is running Trusted Extensions software, you need the following information:

- The name of the Trusted Extensions domain that the LDAP server serves
- The IP address of the LDAP server
- The LDAP profile name that will be loaded

For an LDAP proxy server, you also need the password for the LDAP proxy.

▼ Make System and Security Decisions Before Enabling Trusted Extensions

For each system on which Trusted Extensions is going to be configured, make these configuration decisions before enabling the software.

1 **Decide how securely the system hardware needs to be protected.**

At a secure site, this step has been done for every installed Oracle Solaris system.

- For SPARC systems, a PROM security level and password has been provided.
- For x86 systems, the BIOS is protected.
- On all systems, `root` is protected with a password.

2 **Prepare your `label_encodings` file.**

If you have a site-specific `label_encodings` file, the file must be checked and installed before other configuration tasks can be started. If your site does not have a `label_encodings` file, you can use the default file that Sun supplies. Sun also supplies other `label_encodings` files, which you can find in the `/etc/security/tsol` directory. The Sun files are demonstration files. They might not be suitable for production systems.

To customize a file for your site, see *Trusted Extensions Label Administration*.

3 From the list of labels in your `label_encodings` file, make a list of the labeled zones that you need to create.

The following table lists the label names and suggested zone names for the default `label_encodings` file.

Label	Zone Name
PUBLIC	public
CONFIDENTIAL : INTERNAL	internal
CONFIDENTIAL : NEED TO KNOW	needtoknow
CONFIDENTIAL : RESTRICTED	restricted

For ease of NFS mounting, the zone name of a particular label must be identical on every system. Some systems, such as multilevel print servers, do not need to have labeled zones installed. However, if you do install labeled zones on a print server, the zone names must be identical to the zone names of other systems on your network.

4 Decide when to create roles.

Your site's security policy can require you to administer Trusted Extensions by assuming a role. If so, or if you are configuring the system to satisfy criteria for an evaluated configuration, you must create roles early in the configuration process.

If you are not required to configure the system by using roles, you can choose to configure the system as superuser. This method of configuration is less secure. Audit records do not indicate which user was superuser during configuration. Superuser can perform all tasks on the system, while a role can perform a more limited set of tasks. Therefore, configuration is more controlled when being performed by roles.

5 Choose a zone creation method.

You can create zones from scratch, copy zones, or clone zones. These methods differ in speed of creation, disk space requirements, and robustness. For the trade-offs, see "Planning Your Labeled Zones in Trusted Extensions" on page 23.

6 Plan your LDAP configuration.

Using local files for administration is practical for non-networked systems.

LDAP is the naming service for a networked environment. A populated LDAP server is required when you configure several machines.

- If you have an existing Sun Java System Directory Server (LDAP server), you can create an LDAP proxy server on a system that is running Trusted Extensions. The multilevel proxy server handles communications with the unlabeled LDAP server.

- If you do not have an LDAP server, you can configure a system that runs Trusted Extensions software as a multilevel LDAP server.

7 Decide other security issues for each system and for the network.

For example, you might want to consider the following security issues:

- Determine which devices can be attached to the system and allocated for use.
- Identify which printers at what labels are accessible from the system.
- Identify any systems that have a limited label range, such as a gateway system or a public kiosk.
- Identify which labeled systems can communicate with particular unlabeled systems.

Enabling the Trusted Extensions Service

Starting in the Solaris 10 5/08 release, Trusted Extensions is a service that is managed by the service management facility (SMF). The name of the service is `svc:/system/labeld:default`. By default, the `labeld` service is disabled.

▼ Enable Trusted Extensions

The `labeld` service attaches labels to communications endpoints. For example, the following are labeled:

- All zones and the directories and files within each zone
- All processes including window processes
- All network communications

Before You Begin You have completed the tasks in "Installing or Upgrading the Oracle Solaris Operating System for Trusted Extensions" on page 38 and "Collecting Information and Making Decisions Before Enabling Trusted Extensions" on page 41.

1 On an Oracle Solaris system, enable the `labeld` service.

```
# svcadm enable -s svc:/system/labeld:default
```

The `labeld` service adds labels to the system and starts the auditing service and device allocation. Do not perform other tasks until the cursor returns to the prompt.

2 Verify that the service is enabled.

```
# svcs -x labeld
svc:/system/labeld:default (Trusted Extensions)
 State: online since weekday month date hour:minute:second year
   See: labeld(1M)
Impact: None.
```

Note – The labels do not appear until after you reboot the system. "Setting Up the Global Zone in Trusted Extensions" on page 47 includes tasks that you might want to perform before rebooting.

Troubleshooting The following message indicates that you are not running an Oracle Solaris release that supports Trusted Extensions as a service: `svcs: Pattern 'labeld' doesn't match any instances`.

To run Trusted Extensions on an Oracle Solaris system that does not support the `labeld` service, follow the instructions in the *Solaris Trusted Extensions Installation and Configuration* guide.

◆ ◆ ◆ CHAPTER 4

Configuring Trusted Extensions (Tasks)

This chapter covers how to configure Trusted Extensions on a system with a monitor. To work properly, Trusted Extensions software requires configuration of the following: labels, zones, the network, users who can assume roles, roles, and tools.

- "Setting Up the Global Zone in Trusted Extensions" on page 47
- "Creating Labeled Zones" on page 62
- (Optional) "Adding Network Interfaces and Routing to Labeled Zones" on page 77
- "Creating Roles and Users in Trusted Extensions" on page 84
- "Creating Home Directories in Trusted Extensions" on page 95
- "Adding Users and Hosts to an Existing Trusted Network" on page 98
- "Troubleshooting Your Trusted Extensions Configuration" on page 100
- "Additional Trusted Extensions Configuration Tasks" on page 103

For other configuration tasks, see *Trusted Extensions Administrator's Procedures*.

Setting Up the Global Zone in Trusted Extensions

Before setting up the global zone, you must make decisions about your configuration. For the decisions, see "Collecting Information and Making Decisions Before Enabling Trusted Extensions" on page 41.

Task	Description	For Instructions
Protect the hardware.	Hardware can be protected by requiring a password to change hardware settings.	"Controlling Access to System Hardware" in *System Administration Guide: Security Services*
Configure labels.	Labels *must* be configured for your site. If you plan to use the default `label_encodings` file, you can skip this step.	"Check and Install Your Label Encodings File" on page 48

Task	Description	For Instructions
For IPv6, modify the `/etc/system` file.	If you are running an IPv6 network, you modify the `/etc/system` file to enable IP to recognize labeled packets.	"Enable IPv6 Networking in Trusted Extensions" on page 52
For a DOI whose value is not 1, modify the `/etc/system` file.	If the CIPSO Domain of Interpretation (DOI) of your network nodes is different from 1, specify the DOI in the `/etc/system` file.	"Configure the Domain of Interpretation" on page 52
Create space for a ZFS snapshot.	If you plan to use a ZFS snapshot to clone zones, create the ZFS pool. Perform this task if you are going to clone the first zone to create the rest of the labeled zones.	"Create ZFS Pool for Cloning Zones" on page 54
Reboot and log in.	Upon login, you are in the global zone, which is an environment that recognizes and enforces mandatory access control (MAC).	"Reboot and Log In to Trusted Extensions" on page 55
Initialize the Solaris Management Console.	Trusted Extensions adds tools to the Solaris Management Console for administering users, roles, zones, and the network.	"Initialize the Solaris Management Console Server in Trusted Extensions" on page 56
Configure LDAP.	If you are using the LDAP naming service, set up the LDAP service.	Chapter 5, "Configuring LDAP for Trusted Extensions (Tasks)"
	If you have set up the LDAP service, make this system an LDAP client.	"Make the Global Zone an LDAP Client in Trusted Extensions" on page 59

▼ Check and Install Your Label Encodings File

Your encodings file must be compatible with any Trusted Extensions host with which you are communicating.

Note – Trusted Extensions installs a default `label_encodings` file. This default file is useful for demonstrations. However, this file might not be a good choice for your use. If you plan to use the default file, you can skip this procedure.

- If you are familiar with encodings files, you can use the following procedure.
- If you are not familiar with encodings files, consult *Trusted Extensions Label Administration* for requirements, procedures, and examples.

Caution – You *must* successfully install labels before continuing, or the configuration will fail.

Before You Begin You are the security administrator. The security administrator is responsible for editing, checking, and maintaining the `label_encodings` file. If you plan to edit the `label_encodings` file, make sure that the file itself is writable. For more information, see the `label_encodings(4)` man page.

1. **Insert the media with the `label_encodings` file into the appropriate device.**
2. **Copy the `label_encodings` file to the disk.**
3. **Check the syntax of the file and make it the active `label_encodings` file.**

   - **In Trusted JDS, check and install the file from the command line.**

     a. **Open a terminal window.**

     b. **Run the `chk_encodings` command.**

        ```
        # /usr/sbin/chk_encodings /full-pathname-of-label-encodings-file
        ```

     c. **Read the output and do one of the following:**

        - **Resolve errors.**

          If the command reports errors, the errors *must* be resolved before continuing. For assistance, see Chapter 3, "Making a Label Encodings File (Tasks)," in *Trusted Extensions Label Administration*

        - **Make the file the active `label_encodings` file.**

          ```
          # cp /full-pathname-of-label-encodings-file \
           /etc/security/tsol/label.encodings.site
          # cd /etc/security/tsol
          # cp label_encodings label_encodings.tx.orig
          # cp label.encodings.site label_encodings
          ```

Caution – Your `label_encodings` file *must* pass the `chk_encodings` test before you continue.

   - **In Trusted CDE, use the Check Encodings action.**

     a. **Open the Trusted_Extensions folder.**

        Click mouse button 3 on the background.

     b. **From the Workspace menu, choose Applications → Application Manager.**

c. Double-click the Trusted_Extensions folder icon.

d. Double-click the Check Encodings action.

In the dialog box, type the full path name to the file:

/full-pathname-of-label-encodings-file

The `chk_encodings` command is invoked to check the syntax of the file. The results are displayed in the Check Encodings dialog box.

e. Read the contents of the Check Encodings dialog box and do one of the following:

- **Resolve errors.**

  If the Check Encodings action reports errors, the errors *must* be resolved before continuing. For assistance, see Chapter 3, "Making a Label Encodings File (Tasks)," in *Trusted Extensions Label Administration*.

- **Click `Yes` to make the file the active `label_encodings` file.**

  The Check Encodings action creates a backup copy of the original file, then installs the checked version in `/etc/security/tsol/label_encodings`. The action then restarts the label daemon.

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

4 Check the syntax of the file and make it the active `label_encodings` file.

Use the command line.

a. Open a terminal window.

b. Run the `chk_encodings` command.

```
# /usr/sbin/chk_encodings /full-pathname-of-label-encodings-file
```

c. Read the output and do one of the following:

- **Resolve errors.**

  If the command reports errors, the errors *must* be resolved before continuing. For assistance, see Chapter 3, "Making a Label Encodings File (Tasks)," in *Trusted Extensions Label Administration*

- **Make the file the active `label_encodings` file.**

  ```
  # cp /full-pathname-of-label-encodings-file \
   /etc/security/tsol/label.encodings.site
  # cd /etc/security/tsol
  # cp label_encodings label_encodings.tx.orig
  # cp label.encodings.site label_encodings
  ```

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

Example 4–1 Checking label_encodings Syntax on the Command Line

In this example, the administrator tests several `label_encodings` files by using the command line.

```
# /usr/sbin/chk_encodings /var/encodings/label_encodings1
No errors found in /var/encodings/label_encodings1
# /usr/sbin/chk_encodings /var/encodings/label_encodings2
No errors found in /var/encodings/label_encodings2
```

When management decides to use the `label_encodings2` file, the administrator runs a semantic analysis of the file.

```
# /usr/sbin/chk_encodings -a /var/encodings/label_encodings2
No errors found in /var/encodings/label_encodings2

---> VERSION = MYCOMPANY LABEL ENCODINGS  2.0 10/10/2006

---> CLASSIFICATIONS <---

   Classification 1: PUBLIC
   Initial Compartment bits: 10
   Initial Markings bits: NONE

---> COMPARTMENTS AND MARKINGS USAGE ANALYSIS <---
...
---> SENSITIVITY LABEL to COLOR MAPPING <---
...
```

The administrator prints a copy of the semantic analysis for her records, then moves the file to the `/etc/security/tsol` directory.

```
# cp /var/encodings/label_encodings2 /etc/security/tsol/label.encodings.10.10.06
# cd /etc/security/tsol
# cp label_encodings label_encodings.tx.orig
# cp label.encodings.10.10.06 label_encodings
```

Finally, the administrator verifies that the `label_encodings` file is the company file.

```
# /usr/sbin/chk_encodings -a /etc/security/tsol/label_encodings | head -4
No errors found in /etc/security/tsol/label_encodings

---> VERSION = MYCOMPANY LABEL ENCODINGS  2.0 10/10/2006
```

▼ Enable IPv6 Networking in Trusted Extensions

CIPSO options do not have an Internet Assigned Numbers Authority (IANA) number to use in the IPv6 Option Type field of a packet. The entry that you set in this procedure supplies a number to use on the local network until IANA assigns a number for this option. Trusted Extensions disables IPv6 networking if this number is not defined.

To enable an IPv6 network in Trusted Extensions, you must add an entry in the `/etc/system` file.

- **Type the following entry into the `/etc/system` file:**

  ```
  set ip:ip6opt_ls = 0x0a
  ```

Troubleshooting

- If error messages during boot indicate that your IPv6 configuration is incorrect, correct the entry:
  - Check that the entry is spelled correctly.
  - Check that the system has been rebooted after adding the correct entry to the `/etc/system` file.
- If you install Trusted Extensions on an Oracle Solaris system that currently has IPv6 enabled, but you fail to add the IP entry in `/etc/system`, you see the following error message: `t_optmgmt: System error: Cannot assign requested address` *time-stamp*
- If you install Trusted Extensions on an Oracle Solaris system that does not have IPv6 enabled, and you fail to add the IP entry in `/etc/system`, you see the following types of error messages:
  - `WARNING: IPv6 not enabled via /etc/system`
  - `Failed to configure IPv6 interface(s): hme0`
  - `rpcbind: Unable to join IPv6 multicast group for rpc broadcast` *broadcast-number*

▼ Configure the Domain of Interpretation

All communications to and from a system that is configured with Trusted Extensions must follow the labeling rules of a single CIPSO Domain of Interpretation (DOI). The DOI that is used in each message is identified by an integer number in the CIPSO IP Option header. By default, the DOI in Trusted Extensions is `1`.

If your DOI is not `1`, you must add an entry to the `/etc/system` file and modify the `doi` value in the default security templates.

1. **Type your DOI entry into the `/etc/system` file:**

   ```
   set default_doi = n
   ```

This positive, non-zero number must match the DOI number in the `tnrhtp` database for your node and for the systems that your node communicates with.

2 Before adding the `tnrhtp` database to your LDAP server, modify the `doi` value in the default entries and all entries for local addresses.

Trusted Extensions provides two templates in the `tnrhtp` database, `cipso` and `admin_low`. If you have added entries for local addresses, also modify these entries.

a. Open the `tnrhtp` database in the trusted editor.

```
# /usr/dt/bin/trusted_edit /etc/security/tsol/tnrhtp
```

In Solaris Trusted Extensions (CDE), you can instead use the Admin Editor action in the Trusted_Extensions folder in the Application Manager.

b. Copy the `cipso` template entry to another line.

```
cipso:host_type=cipso;doi=1;min_sl=ADMIN_LOW;max_sl=ADMIN_HIGH
cipso:host_type=cipso;doi=1;min_sl=ADMIN_LOW;max_sl=ADMIN_HIGH
```

c. Comment out one of the `cipso` entries.

```
#cipso:host_type=cipso;doi=1;min_sl=ADMIN_LOW;max_sl=ADMIN_HIGH
cipso:host_type=cipso;doi=1;min_sl=ADMIN_LOW;max_sl=ADMIN_HIGH
```

d. Modify the `doi` value in the uncommented `cipso` entry.

Make this value the same as the `default_doi` value in the `/etc/system` file.

```
#cipso:host_type=cipso;doi=1;min_sl=ADMIN_LOW;max_sl=ADMIN_HIGH
cipso:host_type=cipso;doi=n;min_sl=ADMIN_LOW;max_sl=ADMIN_HIGH
```

e. Change the `doi` value for the `admin_low` entry.

```
#admin_low:host_type=unlabeled;min_sl=ADMIN_LOW;max_sl=ADMIN_HIGH;doi=1;def_label=ADMIN_LOW
admin_low:host_type=unlabeled;min_sl=ADMIN_LOW;max_sl=ADMIN_HIGH;doi=n;def_label=ADMIN_LOW
```

You are finished when every `doi` value in every entry in the `tnrhtp` database is the same.

Troubleshooting If the `/etc/system` file sets a `default_doi` value other than `1`, and a security template for this system sets a value that does not match this `default_doi` value, then messages similar to the following are displayed on the system console during interface configuration:

- `NOTICE: er10 failed: 10.17.1.12 has wrong DOI 4 instead of 1`
- `Failed to configure IPv4 interface(s): er10`

Interface configuration failure can result in login failure:

- `Hostname: unknown`
- `unknown console login: root`
- `Oct 10 10:10:20 unknown login: pam_unix_cred: cannot load hostname Error 0`

To correct the problem, boot the system into single-user mode and correct the security templates as described in this procedure.

See Also For more information about the DOI, see "Network Security Attributes in Trusted Extensions" in *Trusted Extensions Administrator's Procedures*.

To change the `doi` value in the security templates that you create, see "How to Construct a Remote Host Template" in *Trusted Extensions Administrator's Procedures*.

To use the editor of your choice as the trusted editor, see "How to Assign the Editor of Your Choice as the Trusted Editor" in *Trusted Extensions Administrator's Procedures*.

▼ Create ZFS Pool for Cloning Zones

If you plan to use an ZFS snapshot as your zone template, you need to create a ZFS pool from a ZFS file or a ZFS device. This pool holds the snapshot for cloning each zone. You use the `/zone` device for your ZFS pool.

Before You Begin You have set aside disk space during Oracle Solaris installation for a ZFS file system. For details, see "Planning Your Labeled Zones in Trusted Extensions" on page 23.

1 Unmount the `/zone` partition.

During installation, you created a `/zone` partition with sufficient disk space of about 2000 MBytes.

```
# umount /zone
```

2 Remove the `/zone` mount point.

```
# rmdir /zone
```

3 Comment out the `/zone` entry in the `vfstab` file.

a. Prevent the `/zone` entry from being read.

Open the `vfstab` file in an editor. Prefix the `/zone` entry with a comment sign.

```
#/dev/dsk/cntndnsn  /dev/dsk/cntndnsn  /zone  ufs  2  yes  -
```

b. Copy the disk slice, c*n*t*n*d*n*s*n*, to the clipboard.

c. Save the file, and close the editor.

4 Use the disk slice to re-create `/zone` as a ZFS pool.

```
# zpool create -f zone cntndnsn
```

For example, if your `/zone` entry used disk slice `c0t0d0s5`, then the command would be the following:

```
# zpool create -f zone c0t0d0s5
```

5 Verify that the ZFS pool is healthy.

Use one of the following commands:

```
# zpool status -x zone
pool 'zone' is healthy

# zpool list
NAME     SIZE     USED   AVAIL   CAP   HEALTH   ALTROOT
/zone    5.84G   80K    5.84G    7%   ONLINE   -
```

In this example, the initial setup team reserved a 6000 MByte partition for zones. For more information, see the `zpool(1M)` man page.

▼ Reboot and Log In to Trusted Extensions

At most sites, two or more administrators, who serve as an initial setup team, are present when configuring the system.

Before You Begin Before you first log in, become familiar with the desktop and label options in Trusted Extensions. For details, see Chapter 2, "Logging In to Trusted Extensions (Tasks)," in *Trusted Extensions User's Guide*.

1 Reboot the system.

```
# /usr/sbin/reboot
```

If your system does not have a graphical display, go to Chapter 6, "Configuring a Headless System With Trusted Extensions (Tasks)."

2 Log in to either the Solaris Trusted Extensions (CDE) or the Solaris Trusted Extensions (JDS) desktop as superuser.

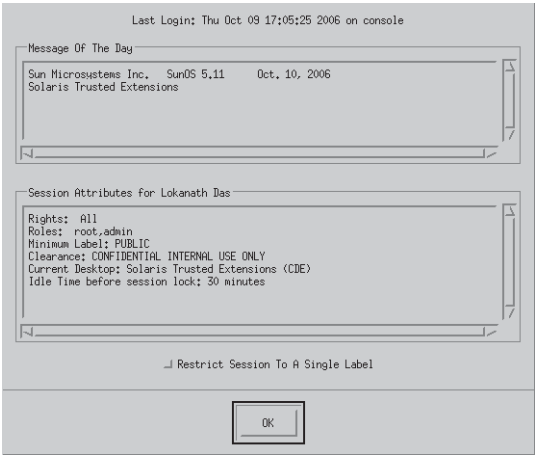
a. In the login window, select one of the trusted desktops.

The Trusted CDE desktop contains actions that are useful when configuring the system. Starting in the Solaris 10 10/08 release, the `txzonemgr` script is the preferred program for configuring the system.

b. In the login dialog box, type `root` and the root password.

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

3 **Read the information in the Last Login dialog box.**



Then click OK to dismiss the box.

4 **Read the Label Builder.**

Click OK to accept the default label.

Once the login process is complete, the Trusted Extensions screen appears briefly, and you are in a desktop session with four workspaces. The `Trusted Path` symbol is displayed in the trusted stripe.

Note – You must log off or lock the screen before leaving a system unattended. Otherwise, a person can access the system without having to pass identification and authentication, and that person would not be uniquely identified or accountable.

▼ Initialize the Solaris Management Console Server in Trusted Extensions

This procedure enables you to administer users, roles, hosts, zones, and the network on this system. On the first system that you configure, only the `files` scope is available.

Before You Begin You must be superuser.

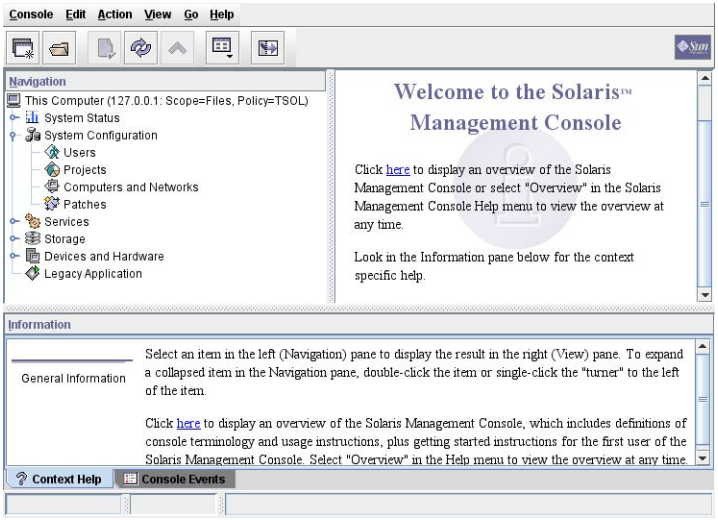
To use the LDAP toolbox on the LDAP server from a Solaris Management Console that is running on a client, you must complete all of the tasks in "Configuring the Solaris Management Console for LDAP (Task Map)" on page 120.

1 **Start the Solaris Management Console.**

```
# /usr/sbin/smc &
```

Note – The first time the Solaris Management Console is started, it performs several registration tasks. These tasks can take a few minutes.

FIGURE 4–1 Solaris Management Console Initial Window



2 **Do one of the following if toolbox icons do not appear in the Solaris Management Console:**

- **If the Navigation pane is not visible:**

  a. **In the Open Toolbox dialog box that is displayed, click Load next to this system's name under Server.**

     If this system does not have the recommended amount of memory and swap, it might take a few minutes for the toolboxes to display. For recommendations, see "Installing or Upgrading the Oracle Solaris Operating System for Trusted Extensions" on page 38.

  b. **From the list of toolboxes, select a toolbox whose `Policy=TSOL`.**

     Figure 4–2 shows a This Computer (*this-host*: `Scope=Files, Policy=TSOL`) toolbox. Trusted Extensions modifies tools under the System Configuration node.

Caution – Do not choose a toolbox that has no policy. Toolboxes without a listed policy do not support Trusted Extensions.

Your toolbox choice depends on which scope you want to influence.

- To edit local files, choose the Files scope.
- To edit LDAP databases, choose the LDAP scope.

  After you complete all of the tasks in "Configuring the Solaris Management Console for LDAP (Task Map)" on page 120, the LDAP scope is available.

c. Click Open.

- **If the Navigation pane is visible, but the toolbox icons are stop signs:**

  a. Exit the Solaris Management Console.

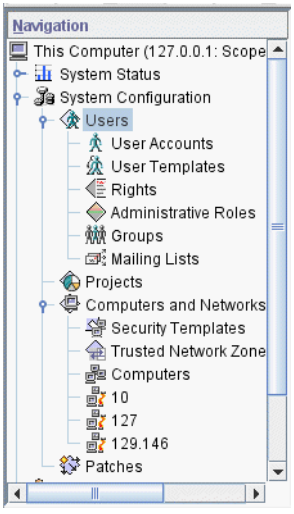
  b. Restart the Solaris Management Console.

  ```
  # /usr/sbin/smc &
  ```

3 If you have not yet done so, select a toolbox whose `Policy=TSOL`.

The following figure shows a This Computer (*this-host*: `Scope=Files, Policy=TSOL`) toolbox. Trusted Extensions modifies tools under the System Configuration node.

FIGURE 4–2 Trusted Extensions Tools in the Solaris Management Console



4 **(Optional) Save the current toolbox.**

Saving a `Policy=TSOL` toolbox enables a Trusted Extensions toolbox to load by default. Preferences are saved per role, per host. The host is the Solaris Management Console server.

a. **From the Console menu, choose Preferences.**

The Home toolbox is selected.

b. **Define a `Policy=TSOL` toolbox as the Home toolbox.**

Put the current toolbox in the Location field by clicking the Use Current Toolbox button.

c. **Click OK to save the preferences.**

5 **Exit the Solaris Management Console.**

See Also For an overview of the Trusted Extensions additions to the Solaris Management Console, see "Solaris Management Console Tools" in *Trusted Extensions Administrator's Procedures*. To use the Solaris Management Console to create security templates, see "Configuring Trusted Network Databases (Task Map)" in *Trusted Extensions Administrator's Procedures*.

▼ Make the Global Zone an LDAP Client in Trusted Extensions

For LDAP, this procedure establishes the naming service configuration for the global zone. If you are not using LDAP, you can skip this procedure.

Starting in the Solaris 10 5/08 release, if you are in a Solaris Trusted Extensions (CDE) workspace, you can use the `txzonemgr` script or a Trusted CDE action to create an LDAP client. If you are in a Solaris Trusted Extensions (JDS) workspace, you must use the `txzonemgr` script.

Note – If you plan to set up a name server in each labeled zone, you are responsible for establishing the LDAP client connection to each labeled zone.

Before You Begin The Sun Java System Directory Server, that is, the LDAP server, must exist. The server must be populated with Trusted Extensions databases, and this system must be able to contact the server. So, the system that you are configuring must have an entry in the `tnrhdb` database on the LDAP server, or this system must be included in a wildcard entry before you perform this procedure.

If an LDAP server that is configured with Trusted Extensions does not exist, you must complete the procedures in Chapter 5, "Configuring LDAP for Trusted Extensions (Tasks)," before you perform this procedure.

1 **If you are using DNS, modify the `nsswitch.ldap` file.**

   a. **Save a copy of the original `nsswitch.ldap` file.**

      The standard naming service switch file for LDAP is too restrictive for Trusted Extensions.

      ```
      # cd /etc
      # cp nsswitch.ldap nsswitch.ldap.orig
      ```

   b. **Change the `nsswitch.ldap` file entries for the following services.**

      The correct entries are similar to the following:

      ```
      hosts:    files dns ldap

      ipnodes:    files dns ldap

      networks:   ldap files
      protocols:  ldap files
      rpc:        ldap files
      ethers:     ldap files
      netmasks:   ldap files
      bootparams: ldap files
      publickey:  ldap files

      services:   files
      ```

      Note that Trusted Extensions adds two entries:

      ```
      tnrhtp:    files ldap
      tnrhdb:    files ldap
      ```

   c. **Copy the modified `nsswitch.ldap` file to `nsswitch.conf`.**

      ```
      # cp nsswitch.ldap nsswitch.conf
      ```

2 **Perform one of the following steps to create an LDAP client.**

   - **Run the `txzonemgr` script and answer the prompts about LDAP.**

     The Create LDAP Client menu item configures the global zone only.

     a. **Follow the instructions in "Run the `txzonemgr` Script" on page 63.**

        The title of the dialog box is Labeled Zone Manager.

     b. **Select Create LDAP Client.**

     c. **Answer the following prompts and click OK after each answer:**

        ```
        Enter Domain Name:                          Type the domain name
        Enter Hostname of LDAP Server:              Type the name of the server
        Enter IP Address of LDAP Server servername:     Type the IP address
        Enter LDAP Proxy Password:                  Type the password to the server
        Confirm LDAP Proxy Password:                Retype the password to the server
        Enter LDAP Profile Name:                    Type the profile name
        ```

d. Confirm or cancel the displayed values.

```
Proceed to create LDAP Client?
```

When you confirm, the `txzonemgr` script adds the LDAP client. Then, a window displays the command output.

- **In a Trusted CDE workspace, find and use the Create LDAP Client action.**

a. Navigate to the Trusted_Extensions folder by clicking mouse button 3 on the background.

b. From the Workspace menu, choose Applications → Application Manager.

c. Double-click the Trusted_Extensions folder icon.

This folder contains actions that set up interfaces, LDAP clients, and labeled zones.

d. Double-click the Create LDAP Client action.

Answer the following prompts:

`Domain Name:`	*Type the domain name*
`Hostname of LDAP Server:`	*Type the name of the server*
`IP Address of LDAP Server:`	*Type the IP address*
`LDAP Proxy Password:`	*Type the password to the server*
`Profile Name:`	*Type the profile name*

e. Click OK.

The following completion message appears:

```
global zone will be LDAP client of LDAP-server
System successfully configured.

*** Select Close or Exit from the window menu to close this window ***
```

f. Close the action window.

3 In a terminal window, set the `enableShadowUpdate` parameter to `TRUE`.

```
# ldapclient -v mod -a enableShadowUpdate=TRUE \
> -a adminDN=cn=admin,ou=profile,dc=domain,dc=suffix
System successfully configured
```

The Create LDAP Client action and the `txzonemgr` script run the `ldapclient init` command only. In Trusted Extensions, you must also modify an initialized LDAP client to enable shadow updates.

4 Verify that the information on the server is correct.

a. Open a terminal window, and query the LDAP server.

```
# ldapclient list
```

The output looks similar to the following:

```
NS_LDAP_FILE_VERSION= 2.0
NS_LDAP_BINDDN= cn=proxyagent,ou=profile,dc=domain-name
...
NS_LDAP_BIND_TIME= number
```

b. Correct any errors.

If you get an error, create the LDAP client again and supply the correct values. For example, the following error can indicate that the system does not have an entry on the LDAP server:

```
LDAP ERROR (91): Can't connect to the LDAP server.
Failed to find defaultSearchBase for domain domain-name
```

To correct this error, you need to check the LDAP server.

Example 4–2 Using Host Names After Loading a resolv.conf File

In this example, the administrator wants a particular set of DNS servers to be available to the system. The administrator copies a `resolv.conf` file from a server on a trusted net. Because DNS is not yet active, the administrator uses the server's IP address to locate the server.

```
# cd /etc
# cp /net/10.1.1.2/export/txsetup/resolv.conf resolv.conf
```

After the `resolv.conf` file is copied and the `nsswitch.conf` file includes `dns` in the `hosts` entry, the administrator can use host names to locate systems.

Creating Labeled Zones

The `txzonemgr` script steps you through all the following tasks that configure labeled zones.

Caution – You must be running the Solaris 10 8/07 release of Trusted Extensions or a later release to use the `txzonemgr` procedures. Or, you must install all patches for the Solaris 10 11/06 release.

If you are running the Solaris 10 11/06 release without current patches, use the procedures in Appendix B, "Using CDE Actions to Install Zones in Trusted Extensions," to configure the labeled zones.

The instructions in this section configure labeled zones on a system that has been assigned at most two IP addresses. For other configurations, see the configuration options in "Task Map: Preparing For and Enabling Trusted Extensions" on page 31.

Task	Description	For Instructions
1. Run the `txzonemgr` script.	The `txzonemgr` script creates a GUI that presents the appropriate tasks as you configure your zones.	"Run the `txzonemgr` Script" on page 63
2. Manage network interfaces in the global zone.	Configure interfaces in the global zone, or create logical interfaces and configure them in the global zone.	"Configure the Network Interfaces in Trusted Extensions" on page 64
3. Name and label the zone.	Name the zone with a version of its label, and assign the label.	"Name and Label the Zone" on page 68
4. Install and boot the zone.	Install the packages in the zone. Configure services in the zone. A Zone Terminal Console enables you to view the activity in the zone.	"Install the Labeled Zone" on page 70 "Boot the Labeled Zone" on page 71
5. Verify the status of the zone.	Verify that the labeled zone is running, and that the zone can communicate with the global zone.	"Verify the Status of the Zone" on page 72
6. Customize the zone.	Remove unwanted services from the zone. If the zone is going to be used to create other zones, remove information that is specific to this zone only.	"Customize the Labeled Zone" on page 74
7. Create the rest of the zones.	Use the method that you have chosen to create your second zone. For a discussion of zone creation methods, see "Planning Your Labeled Zones in Trusted Extensions" on page 23.	"Copy or Clone a Zone in Trusted Extensions" on page 75
8. (Optional) Add zone-specific network interfaces.	To effect network isolation, add one or more network interfaces to a labeled zone. Typically, such configurations are used to isolate labeled subnets.	"Adding Network Interfaces and Routing to Labeled Zones" on page 77

▼ Run the txzonemgr Script

This script steps you through the tasks to properly configure, install, initialize, and boot labeled zones. In the script, you name each zone, associate the name with a label, install the packages to create a virtual OS, and then boot the zone to start services in that zone. The script includes copy zone and clone zone tasks. You can also halt a zone, change the state of a zone, and add zone-specific network interfaces.

This script presents a dynamically-determined menu that displays only valid choices for the current circumstances. For instance, if the status of a zone is configured, the Install zone menu item is not displayed. Tasks that are completed do not display in the list.

Before You Begin You are superuser.

If you plan to clone zones, you have completed the preparation for cloning zones. If you plan to use your own security templates, you have created the templates.

1 Open a terminal window in the global zone.

2 **Run the `txzonemgr` script.**

```
# /usr/sbin/txzonemgr
```

The script opens the `Labeled Zone Manager` dialog box. This `zenity` dialog box prompts you for the appropriate tasks, depending on the current state of your installation.

To perform a task, you select the menu item, then press the Return key or click OK. When you are prompted for text, type the text then press the Return key or click OK.

Tip – To view the current state of zone completion, click Return to Main Menu in the Labeled Zone Manager.

▼ Configure the Network Interfaces in Trusted Extensions

Note – If you are configuring your system to use DHCP, refer to the laptop instructions in the Trusted Extensions section of OpenSolaris Community: Security web page (`http://hub.opensolaris.org/bin/view/Community+Group+security/`).

Starting in the Solaris 10 10/08 release, if you are configuring a system where each labeled zone is on its own subnet, you can skip this step and continue with "Name and Label the Zone" on page 68. You add the network interfaces for each labeled zone in "Add a Network Interface to Route an Existing Labeled Zone" on page 77, after you have finished installing and customizing the zones.

In this task, you configure the networking in the global zone. You must create exactly one `all-zones` interface. An `all-zones` interface is shared by the labeled zones and the global zone. The shared interface is used to route traffic between the labeled zones and the global zone. To configure this interface, do one of the following:

- Create a logical interface from a physical interface, then share the physical interface.

  This configuration is the simplest to administer. Choose this configuration when your system has been assigned two IP addresses. In this procedure, the logical interface becomes the global zone's specific address, and the physical interface is shared between the global zone and the labeled zones.

- Share a physical interface

  Choose this configuration when your system has been assigned one IP address. In this configuration, the physical interface is shared between the global zone and the labeled zones.

- Share a virtual network interface, `vni0`

Choose this configuration when you are configuring DHCP, or when each subnetwork is at a different label. For a sample procedure, refer to the laptop instructions in the Trusted Extensions section of OpenSolaris Community: Security web page (`http://hub.opensolaris.org/bin/view/Community+Group+security/`).

Starting in the Solaris 10 10/08 release, the loopback interface in Trusted Extensions is created as an all-zones interface. Therefore, you do not need to create a `vni0` shared interface.

To add zone-specific network interfaces, finish and verify zone creation before adding the interfaces. For the procedure, see "Add a Network Interface to Route an Existing Labeled Zone" on page 77.

Before You Begin You are superuser in the global zone.

The Labeled Zone Manager is displayed. To open this GUI, see "Run the `txzonemgr` Script" on page 63.

1 In the Labeled Zone Manager, select Manage Network Interfaces and click OK.

A list of interfaces is displayed.

Note – In this example, the physical interface was assigned a host name and an IP address during installation.

---

2 Select the physical interface.

A system with one interface displays a menu similar to the following. The annotation is added for assistance:

```
vni0                          Down      Virtual Network Interface
eri0 global 10.10.9.9 cipso Up      Physical Interface
```

a. Select the `eri0` interface.

b. Click OK

3 Select the appropriate task for this network interface.

You are offered three options:

```
View Template       Assign a label to the interface
Share       Enable the global zone and labeled zones to use this interface
Create Logical Interface       Create an interface to use for sharing
```

- **If your system has one IP address, go to Step 4.**
- **If your system has two IP addresses, go to Step 5.**

4 **On a system with one IP address, share the physical interface.**

In this configuration, the host's IP address applies to all zones. Therefore, the host's address is the `all-zones` address. This host cannot be used as a multilevel server. For example, users cannot share files from this system. The system cannot be an LDAP proxy server, an NFS home directory server, or a print server.

a. **Select Share and click OK.**

b. **Click OK in the dialog box that displays the shared interface.**

```
eri0  all-zones  10.10.9.8  cipso  Up
```

You are successful when the physical interface is an `all-zones` interface. Continue with "Name and Label the Zone" on page 68.

5 **On a system with two IP addresses, create a logical interface.**

Then, share the physical interface.

This is the simplest Trusted Extensions network configuration. In this configuration, the main IP address can be used by other systems to reach any zone on this system, and the logical interface is zone-specific to the global zone. The global zone can be used as a multilevel server.

a. **Select Create Logical Interface and click OK.**

Dismiss the dialog box that confirms the creation of a new logical interface.

b. **Select Set IP address and click OK.**

c. **At the prompt, specify the host name for the logical interface and click OK.**

For example, specify `machine1-services` as the host name for the logical interface. The name indicates that this host offers multilevel services.

d. **At the prompt, specify the IP address for the logical interface and click OK.**

For example, specify `10.10.9.2` as the IP address for the logical interface.

e. **Select the logical interface again and click OK.**

f. **Select Bring Up and click OK.**

The interface is displayed as `Up`.

```
eri0    global       10.10.9.1   cipso   Up
eri0:1  global       10.10.9.2   cipso   Up
```

g. **Share the physical interface.**

i. **Select the physical interface and click OK.**

ii. Select Share and click OK.

```
eri0    all-zones    10.10.9.1   cipso   Up
eri0:1  global       10.10.9.2   cipso   Up
```

You are successful when at least one interface is an `all-zones` interface.

Example 4–3 Viewing the /etc/hosts File on a System With a Shared Logical Interface

On a system where the global zone has a unique interface and labeled zones share a second interface with the global zone, the `/etc/hosts` file appears similar to the following:

```
# cat /etc/hosts
...
127.0.0.1  localhost
192.168.0.11 machine1 loghost
192.168.0.12 machine1-services
```

In the default configuration, the `tnrhdb` file appears similar to the following:

```
# cat /etc/security/tsol/tnrhdb
...
127.0.0.1:cipso
192.168.0.11:cipso
192.168.0.12:cipso
0.0.0.0:admin_low
```

If the `all-zones` interface is not in the `tnrhdb` file, the interface defaults to `cipso`.

Example 4–4 Displaying the Shared Interface on a Trusted Extensions System With One IP Address

In this example, the administrator is not planning to use the system as a multilevel server. To conserve IP addresses, the global zone is configured to share its IP address with every labeled zone.

The administrator selects Share for the `hme0` interface on the system. The software configures all zones to have logical NICs. These logical NICs share a single physical NIC in the global zone.

The administrator runs the **`ifconfig -a`** command to verify that the physical interface `hme0` on network interface `192.168.0.11` is shared. The value `all-zones` is displayed:

```
lo0: flags=2001000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4,VIRTUAL> mtu 8232 index 1
        inet 127.0.0.1 netmask ff000000
hme0: flags=1000843<BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
        all-zones
        inet 192.168.0.11 netmask fffffe00 broadcast 192.168.0.255
```

Starting in the Solaris 10 10/08 release, the loopback interface in Trusted Extensions is created as an all-zones interface.

```
lo0: flags=2001000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4,VIRTUAL> mtu 8232 index 1
        all-zones
        inet 127.0.0.1 netmask ff000000
hme0: flags=1000843<BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
        all-zones
        inet 192.168.0.11 netmask fffffe00 broadcast 192.168.0.255
```

The administrator also examines the contents of the `/etc/hostname.hme0` file:

```
192.168.0.11 all-zones
```

▼ Name and Label the Zone

You do not have to create a zone for every label in your `label_encodings` file, but you can. The administrative GUIs enumerate the labels that can have zones created for them on this system.

Before You Begin You are superuser in the global zone. The Labeled Zone Manager dialog box is displayed. To open this GUI, see "Run the `txzonemgr` Script" on page 63. You have configured the network interfaces in the global zone.

You have created any security templates that you need. A security template defines, among other attributes, the label range that can be assigned to a network interface. The default security templates might satisfy your needs.

- For an overview of security templates, see "Network Security Attributes in Trusted Extensions" in *Trusted Extensions Administrator's Procedures*.
- To use the Solaris Management Console to create security templates, see "Configuring Trusted Network Databases (Task Map)" in *Trusted Extensions Administrator's Procedures*.

1 In the Labeled Zone Manager, select Create a new zone and click OK.

You are prompted for a name.

a. Type the name for the zone.

Tip – Give the zone a name that is similar to the zone's label. For example, the name of a zone whose label is `CONFIDENTIAL: RESTRICTED` would be `restricted`.

For example, the default `label_encodings` file contains the following labels:

```
PUBLIC
CONFIDENTIAL: INTERNAL USE ONLY
CONFIDENTIAL: NEED TO KNOW
CONFIDENTIAL: RESTRICTED
SANDBOX: PLAYGROUND
MAX LABEL
```

Although you could create one zone per label, consider creating the following zones:

- On a system for all users, create one zone for the `PUBLIC` label and three zones for the `CONFIDENTIAL` labels.
- On a system for developers, create a zone for the `SANDBOX: PLAYGROUND` label. Because `SANDBOX: PLAYGROUND` is defined as a disjoint label for developers, only systems that developers use need a zone for this label.
- Do not create a zone for the `MAX LABEL` label, which is defined to be a clearance.

b. Click OK.

The dialog box displays *zone-name*`: configured` above a list of tasks.

2 To label the zone, choose one of the following:

- **If you are using a customized `label_encodings` file, label the zone by using the Trusted Network Zones tool.**

  a. Open the Trusted Network Zones tool in the Solaris Management Console.

  i. Start the Solaris Management Console.

  ```
  # /usr/sbin/smc &
  ```

  ii. Open the Trusted Extensions toolbox for the local system.

  Choose Console → Open Toolbox.

  Select the toolbox that is named This Computer (*this-host*: `Scope=Files, Policy=TSOL`).

  Click Open.

  iii. Under System Configuration, navigate to Computers and Networks.

  Provide a password when prompted.

  iv. Double-click the Trusted Network Zones tool.

  b. For each zone, associate the appropriate label with the zone name.

  i. Choose Action → Add Zone Configuration.

  The dialog box displays the name of a zone that does not have an assigned label.

  ii. Look at the zone name, then click Edit.

iii. **In the Label Builder, click the appropriate label for the zone name.**

If you click the wrong label, click the label again to deselect it, then click the correct label.

iv. **Save the assignment.**

Click OK in the Label Builder, then click OK in the Trusted Network Zones Properties dialog box.

You are finished when every zone that you want is listed in the panel, or the Add Zone Configuration menu item opens a dialog box that does not have a value for Zone Name.

- **If you are using the default `label_encodings` file, use the Labeled Zone Manager.**

Click Select Label menu item and OK to display the list of available labels.

a. **Select the label for the zone.**

For a zone that is named `public`, you would select the label `PUBLIC` from the list.

b. **Click OK.**

A list of tasks is displayed.

▼ Install the Labeled Zone

Before You Begin You are superuser in the global zone. The zone is configured, and has an assigned network interface.

The Labeled Zone Manager dialog box is displayed with the subtitle *zone-name*`:configured`. To open this GUI, see "Run the `txzonemgr` Script" on page 63.

1 **From the Labeled Zone Manager, select Install and click OK.**

Caution – This process takes some time to finish. Do not perform other tasks while this task is completing.

The system copies packages from the global zone to the non-global zone. This task installs a labeled virtual operating system in the zone. To continue the example, this task installs the `public` zone. The GUI displays output similar to the following.

```
# Labeled Zone Manager: Installing zone-name zone
Preparing to install zone <zonename>
Creating list of files to copy from the global zone
Copying <total> files to the zone
Initializing zone product registry
Determining zone package initialization order.
Preparing to initialize <subtotal> packages on the zone.
```

```
Initializing package <number> of <subtotal>: percent complete: percent

Initialized <subtotal> packages on zone.
Zone <zonename> is initialized.
The file /zone/internal/root/var/sadm/system/logs/install_log
contains a log of the zone installation.
```

Note – Messages such as `cannot create ZFS dataset zone/`*zonename*`: dataset already exists` are informational. The zone uses the existing dataset.

When the installation is complete, you are prompted for the name of the host. A name is supplied.

2 **Accept the name of the host.**

The dialog box displays *zone-name*`:installed` above a list of tasks.

Troubleshooting If warnings that are similar to the following are displayed: `Installation of these packages generated errors: SUNW`*pkgname*, read the install log and finish installing the packages.

▼ Boot the Labeled Zone

Before You Begin You are superuser in the global zone. The zone is installed, and has an assigned a network interface.

The Labeled Zone Manager dialog box is displayed with the subtitle *zone-name*`:installed`. To open this GUI, see "Run the `txzonemgr` Script" on page 63.

1 **In the Labeled Zone manager, select Zone Console and click OK.**

A separate console window appears for the current labeled zone.

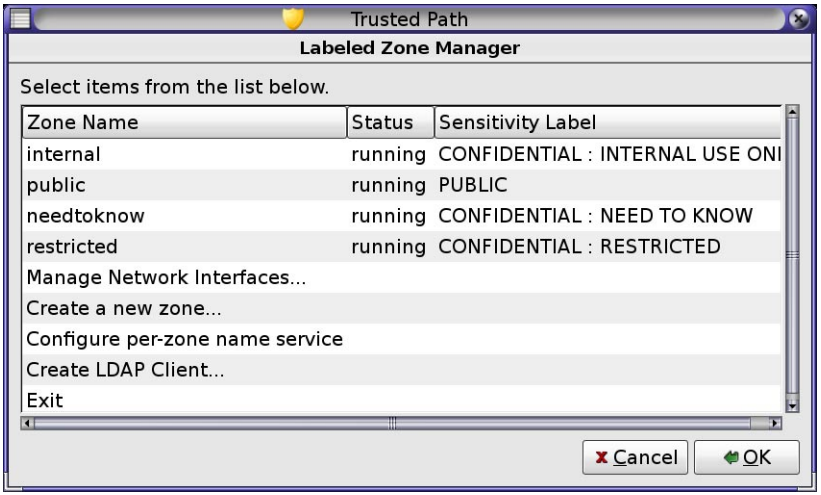
2 **Select Boot.**

The Zone Terminal Console tracks the progress of booting the zone. If the zone is created from scratch, messages that are similar to the following appear in the console:

```
[Connected to zone 'public' console]

[NOTICE: Zone booting up]
...
Hostname: zone-name
Loading smf(5) service descriptions: number/total
Creating new rsa public/private host key pair
Creating new dsa public/private host key pair

rebooting system due to change(s) in /etc/default/init

[NOTICE: Zone rebooting]
```

Caution – Do not perform other tasks while this task is completing.

When the four default zones are configured and booted, the Labeled Zone Manager displays the zones as follows:



Troubleshooting Sometimes, error messages are displayed and the zone does not reboot. In the Zone Terminal Console, press the Return key. If you are prompted to type y to reboot, type y and press the Return key. The zone reboots.

Next Steps If this zone was copied or cloned from another zone, continue with "Verify the Status of the Zone" on page 72.

If this zone is the first zone, continue with "Customize the Labeled Zone" on page 74.

▼ Verify the Status of the Zone

Note – The X server runs in the global zone. Each labeled zone must be able to connect with the global zone to use the X server. Therefore, zone networking must work before a zone can be used. For background information, see "Planning for Multilevel Access" on page 25.

1 Verify that the zone has been completely started.

a. In the *zone-name*: Zone Terminal Console, log in as root.

```
hostname console login: root
Password:       Type root password
```

b. In the Zone Terminal Console, verify that critical services are running.

```
# svcs -xv
svc:/application/print/server:default (LP print server)
 State: disabled since Tue Oct 10 10:10:10 2006
Reason: Disabled by an administrator.
   See: http://sun.com/msg/SMF-8000-05
   See: lpsched(1M)
...
```

The `sendmail` and `print` services are not critical services.

c. Verify that the zone has a valid IP address.

```
# ifconfig -a
```

For example, the following output shows an IP address for the `hme0` interface.

```
# ...
 hme0: flags=1000843<BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
         all-zones
         inet 192.168.0.11 netmask fffffe00 broadcast 192.168.0.255
```

d. (Optional) Verify that the zone can communicate with the global zone.

i. Set the `DISPLAY` variable to point to the X server

```
# DISPLAY=global-zone-hostname:n.n
# export DISPLAY
```

ii. From the terminal window, display a GUI.

For example, display a clock.

```
# /usr/openwin/bin/xclock
```

If the clock at the label of the zone does not appear, the zone networking has not been configured correctly. For debugging suggestions, see "Labeled Zone Is Unable to Access the X Server" on page 101.

iii. Close the GUI before continuing.

2 From the global zone, check the status of the labeled zones.

```
# zoneadm list -v
ID NAME         STATUS         PATH                BRAND   IP
 0 global       running        /                   native  shared
 3 internal     running        /zone/internal      native  shared
 4 needtoknow   running        /zone/needtoknow    native  shared
 5 restricted   running        /zone/restricted    native  shared
```

Next Steps You have completed configuring the labeled zone. To add zone-specific network interfaces to the zones or to establish default routing per labeled zone, continue with "Adding Network Interfaces and Routing to Labeled Zones" on page 77. Otherwise, continue with "Creating Roles and Users in Trusted Extensions" on page 84.

▼ Customize the Labeled Zone

If you are going to clone zones or copy zones, this procedure configures a zone to be a template for other zones. In addition, this procedure configures a zone that has not been created from a template for use.

Before You Begin You are superuser in the global zone. You have completed "Verify the Status of the Zone" on page 72.

1 In the Zone Terminal Console, disable services that are unnecessary in a labeled zone.

If you are copying or cloning this zone, the services that you disable are disabled in the new zones. The services that are online on your system depend on the service manifest for the zone. Use the `netservices limited` command to turn off services that labeled zones do not need.

a. Remove many unnecessary services.

```
# netservices limited
```

b. List the remaining services.

```
# svcs
...
STATE        STIME      FMRI
online       13:05:00   svc:/application/graphical-login/cde-login:default
...
```

c. Disable graphical login.

```
# svcadm disable svc:/application/graphical-login/cde-login
# svcs cde-login
STATE        STIME      FMRI
disabled     13:06:22   svc:/application/graphical-login/cde-login:default
```

For information about the service management framework, see the `smf(5)` man page.

2 In the Labeled Zone Manager, select Halt to halt the zone.

3 Before continuing, verify that the zone is shut down.

In the *zone-name*: Zone Terminal Console, the following message indicates that the zone is shut down.

```
[ NOTICE: Zone halted]
```

If you are not copying or cloning this zone, create the remaining zones in the way that you created this first zone. Otherwise, continue with the next step.

4 **If you are using this zone as a template for other zones, do the following:**

a. **Remove the `auto_home_`*zone-name* file.**

In a terminal window in the global zone, remove this file from the *zone-name* zone.

```
# cd /zone/zone-name/root/etc
# ls auto_home*
auto_home  auto_home_zone-name
# rm auto_home_zone-name
```

For example, if the `public` zone is the template for cloning other zones, remove the `auto_home_public` file:

```
# cd /zone/public/root/etc
# rm auto_home_public
```

b. **If you plan to clone this zone, create the ZFS snapshot in the next step, then continue with "Copy or Clone a Zone in Trusted Extensions" on page 75.**

c. **If you plan to copy this zone, complete Step 6, then continue with "Copy or Clone a Zone in Trusted Extensions" on page 75.**

5 **To create a zone template for cloning the remaining zones, select Create Snapshot and click OK.**

Caution – The zone for the snapshot must be in a ZFS file system. You created a ZFS file system for the zone in "Create ZFS Pool for Cloning Zones" on page 54.

6 **To verify that the customized zone is still usable, select Boot from the Labeled Zone Manager.**

The Zone Terminal Console tracks the progress of booting the zone. Messages that are similar to the following appear in the console:

```
[Connected to zone 'public' console]

[NOTICE: Zone booting up]
...
Hostname: zonename
```

Press the Return key for a login prompt. You can log in as root.

▼ Copy or Clone a Zone in Trusted Extensions

Before You Begin You have completed "Customize the Labeled Zone" on page 74.

The Labeled Zone Manager dialog box is displayed. To open this GUI, see "Run the `txzonemgr` Script" on page 63.

1 **Create the zone.**

For details, see "Name and Label the Zone" on page 68.

2 **Continue with your zone creation strategy by choosing one of the following methods:**

You will repeat these steps for every new zone.

- **Copy the zone that you just labeled.**

  a. **In the Labeled Zone Manager, select Copy and click OK.**

  b. **Select the zone template and click OK.**

  A window displays the copying process. When the process completes, the zone is installed.

  If the Labeled Zone Manager displays *zone-name*: `configured`, continue with the next step. Otherwise, continue with Step e.

  c. **Select the menu item Select another zone, and click OK.**

  d. **Select the newly installed zone and click OK.**

  e. **Complete "Boot the Labeled Zone" on page 71.**

  f. **Complete "Verify the Status of the Zone" on page 72.**

- **Clone the zone that you just labeled.**

  a. **In the Labeled Zone Manager, select Clone and click OK.**

  b. **Select a ZFS snapshot from the list and click OK.**

  For example, if you created a snapshot from `public`, select the `zone/public@snapshot`.

  When the cloning process completes, the zone is installed. Continue with Step c.

  c. **Open a Zone Console and boot the zone.**

  For instructions, see "Boot the Labeled Zone" on page 71.

  d. **Complete "Verify the Status of the Zone" on page 72.**

Next Steps

- When you have completed "Verify the Status of the Zone" on page 72 for every zone, and you want each zone to be on a separate physical network, continue with "Add a Network Interface to Route an Existing Labeled Zone" on page 77.
- If you have not yet created roles, continue with "Creating Roles and Users in Trusted Extensions" on page 84.
- If you have already created roles, continue with "Creating Home Directories in Trusted Extensions" on page 95.

Adding Network Interfaces and Routing to Labeled Zones

The following tasks support environments where each zone is connected to a separate physical network.

Task	Description	For Instructions
EITHER 1a: Add a network interface to each labeled zone and use the global zone to reach the external network.	Connects each labeled zone to a separate physical network. The labeled zones use the network routing that the global zone provides.	"Add a Network Interface to Route an Existing Labeled Zone" on page 77
OR 1b: Add a network interface to each labeled zone with a default route.	Connects each zone to a separate physical network. The labeled zones do *not* use the global zone for routing.	"Add a Network Interface That Does Not Use the Global Zone to Route an Existing Labeled Zone" on page 79
2. Create a name service cache in each labeled zone.	Configures a name service daemon for each zone.	"Configure a Name Service Cache in Each Labeled Zone" on page 83

▼ Add a Network Interface to Route an Existing Labeled Zone

This procedure adds zone-specific network interfaces to existing labeled zones. This configuration supports environments where each labeled zone is connected to a separate physical network. The labeled zones use the network routing that the global zone provides.

Note – The global zone must configure an IP address for every subnet in which a non-global zone address is configured.

Before You Begin You are superuser in the global zone.

For every zone, you have completed the tasks in "Creating Labeled Zones" on page 62.

1 In the global zone, type the IP addresses and hostnames for the additional network interfaces into the `/etc/hosts` file.

Use a standard naming convention, such as adding *-zone-name* to the name of the host.

```
## /etc/hosts in global zone
10.10.8.2    hostname-zone-name1
10.10.8.3    hostname-global-name1
10.10.9.2    hostname-zone-name2
10.10.9.3    hostname-global-name2
```

2 **For the network for each interface, add entries to the `/etc/netmasks` file.**

```
## /etc/netmasks in global zone
10.10.8.0 255.255.255.0
10.10.9.0 255.255.255.0
```

For more information, see the `netmasks(4)` man page.

3 **In the global zone, plumb the zone-specific physical interfaces.**

a. **Identify the physical interfaces that are already plumbed.**

```
# ifconfig -a
```

b. **Configure the global zone addresses on each interface.**

```
# ifconfig interface-nameN1 plumb
# ifconfig interface-nameN1 10.10.8.3 up
# ifconfig interface-nameN2 plumb
# ifconfig interface-nameN2 10.10.9.3 up
```

c. **For each global zone address, create a `hostname.`*interface-nameN* file.**

```
# /etc/hostname.interface-nameN1
10.10.8.3
# /etc/hostname.interface-nameN2
10.10.9.3
```

The global zone addresses are configured immediately upon system startup. The zone-specific addresses are configured when the zone is booted.

4 **Assign a security template to each zone-specific network interface.**

If the gateway to the network is not configured with labels, assign the `admin_low` security template. If the gateway to the network is labeled, assign a `cipso` security template.

You can create security templates of host type `cipso` that reflect the label of every network. For the procedures to create and assign the templates, see "Configuring Trusted Network Databases (Task Map)" in *Trusted Extensions Administrator's Procedures*.

5 **Halt every labeled zone to which you plan to add a zone-specific interface.**

```
# zoneadm -z zone-name halt
```

6 **Start the Labeled Zone Manager.**

```
# /usr/sbin/txzonemgr
```

7 **For each zone where you want to add a zone-specific interface, do the following:**

a. **Select the zone.**

b. **Select Add Network.**

c. **Name the network interface.**

d. Type the IP address of the interface.

8 In the Labeled Zone Manager for every completed zone, select Zone Console.

9 Select Boot.

10 In the Zone Console, verify that the interfaces have been created.

```
# ifconfig -a
```

11 Verify that the zone has a route to the gateway for the subnet.

```
# netstat -rn
```

Troubleshooting To debug zone configuration, see the following:

- Chapter 30, "Troubleshooting Miscellaneous Solaris Zones Problems," in *System Administration Guide: Oracle Solaris Containers-Resource Management and Oracle Solaris Zones*
- "Troubleshooting Your Trusted Extensions Configuration" on page 100
- "Troubleshooting the Trusted Network (Task Map)" in *Trusted Extensions Administrator's Procedures*

▼ Add a Network Interface That Does Not Use the Global Zone to Route an Existing Labeled Zone

This procedure sets zone-specific default routes for existing labeled zones. In this configuration, the labeled zones do *not* use the global zone for routing.

The labeled zone must be plumbed in the global zone before the zone is booted. However, to isolate the labeled zone from the global zone, the interface must be in the `down` state when the zone is booted. For more information, see Chapter 17, "Non-Global Zone Configuration (Overview)," in *System Administration Guide: Oracle Solaris Containers-Resource Management and Oracle Solaris Zones*.

Note – A unique default route must be configured for every non-global zone that is booted.

Before You Begin You are superuser in the global zone.

For every zone, you have completed the tasks in "Creating Labeled Zones" on page 62. You are using either the `vni0` interface or the `lo0` interface to connect the labeled zones to the global zone.

1. **For every network interface, determine its IP address, netmask, and default router.**

   Use the `ifconfig -a` command to determine the IP address and netmask. Use the `zonecfg -z zonename info net` command to determine if a default router has been assigned.

2. **Create an empty `/etc/hostname.`*interface* file for each labeled zone.**

   ```
   # touch /etc/hostname.interface
   # touch /etc/hostname.interface:n
   ```

   For more information, see the `netmasks(4)` man page.

3. **Plumb the network interfaces of the labeled zones.**

   ```
   # ifconfig zone1-network-interface plumb
   # ifconfig zone2-network-interface plumb
   ```

4. **Verify that the labeled zone's interfaces are in the `down` state.**

   ```
   # ifconfig -a
   zone1-network-interface  zone1-IP-address  down
   zone2-network-interface  zone2-IP-address  down
   ```

   The zone-specific addresses are configured when the zone is booted.

5. **For the network for each interface, add entries to the `/etc/netmasks` file.**

   ```
   ## /etc/netmasks in global zone
   192.168.2.0 255.255.255.0
   192.168.3.0 255.255.255.0
   ```

   For more information, see the `netmasks(4)` man page.

6. **Assign a security template to each zone-specific network interface.**

   Create security templates of host type `cipso` that reflect the label of every network. To create and assign the templates, see "Configuring Trusted Network Databases (Task Map)" in *Trusted Extensions Administrator's Procedures*.

7. **Run the `txzonemgr` script, and open a separate terminal window.**

   In the Labeled Zone Manager, you will add the network interfaces for the labeled zones. In the terminal window, you will display information about the zone and set the default router.

8. **For every zone to which you are going to add a zone-specific network interface and router, complete the following steps:**

   a. **In the terminal window, halt the zone.**

      ```
      # zoneadm -z zone-name halt
      ```

   b. **In the Labeled Zone Manager, do the following:**

      i. **Select the zone.**

ii. **Select Add Network.**

iii. **Name the network interface.**

iv. **Type the IP address of the interface.**

v. **In the terminal window, verify the zone configuration.**

```
# zonecfg -z zone-name info net
net:   address: IP-address
       physical: zone-network-interface
       defrouter not specified
```

c. **In the terminal window, configure the default router for the labeled zone's network.**

```
# zonecfg -z zone-name
zonecfg:zone-name > select net address=IP-address
zonecfg:zone-name:net> set defrouter=router-address
zonecfg:zone-name:net> end
zonecfg:zone-name > verify
zonecfg:zone-name > commit
zonecfg:zone-name > exit
#
```

For more information, see the zonecfg(1M) man page and "How to Configure the Zone" in *System Administration Guide: Oracle Solaris Containers-Resource Management and Oracle Solaris Zones*.

d. **Boot the labeled zone.**

```
# zoneadm -z zone-name boot
```

e. **In the global zone, verify that the labeled zone has a route to the gateway for the subnet.**

```
# netstat -rn
```

A routing table is displayed. The destination and interface for the labeled zone is different from the entry for the global zone.

9 **To remove the default route, select the zone's IP address, then remove the route.**

```
# zonecfg -z zone-name

zonecfg:zone-name > select net address=zone-IP-address
zonecfg:zone-name:net> remove net defrouter=zone-default-route
zonecfg:zone-name:net>  info net
net:
   address: zone-IP-address
   physical: zone-network-interface
   defrouter not specified
```

Example 4–5 Setting a Default Route for a Labeled Zone

In this example, the administrator routes the Secret zone to a separate physical subnet. Traffic to and from the Secret zone is not routed through the global zone. The administrator uses the Labeled Zone Manager and the `zonecfg` command, then verifies that routing works.

The administrator determines that `qfe1` and `qfe1:0` are not currently in use. and creates a mapping for two labeled zones. `qfe1` is the designated interface for the Secret zone.

```
Interface IP Address    Netmask        Default Router
qfe1     192.168.2.22 255.255.255.0 192.168.2.2
qfe1:0   192.168.3.33 255.255.255.0 192.168.3.3
```

First, the administrator creates the `/etc/hostname.qfe1` file and configures the `/etc/netmasks` file.

```
# touch /etc/hostname.qfe1

# cat /etc/netmasks
## /etc/netmasks in global zone
192.168.2.0 255.255.255.0
```

Then, the administrator plumbs the network interface and verifies that the interface is down.

```
# ifconfig qfe1 plumb
# ifconfig -a
```

Then, in the Solaris Management Console, the administrator creates a security template with a single label, Secret, and assigns the IP address of the interface to the template.

The administrator halts the zone.

```
# zoneadm -z secret halt
```

The administrator runs the `txzonemgr` script to open the Labeled Zone Manager.

```
# /usr/sbin/txzonemgr
```

In the Labeled Zone Manager, the administrator selects the Secret zone, selects Add Network, and then selects a network interface. The administrator closes the Labeled Zone Manager.

On the command line, the administrator selects the zone's IP address, then sets its default route. Before exiting the command, the administrator verifies the route and commits it.

```
# zonecfg -z secret
zonecfg: secret > select net address=192.168.6.22
zonecfg: secret:net> set defrouter=192.168.6.2
zonecfg: secret:net> end
zonecfg: secret > verify
zonecfg: secret > commit
zonecfg: secret > info net
```

```
  net:
     address: 192.168.6.22
     physical: qfe1
     defrouter: 192.168.6.2
zonecfg: secret > exit
#
```

The administrator boots the zone.

```
# zoneadm -z secret boot
```

In a separate terminal window in the global zone, the administrator verifies the sending and receiving of packets.

```
# netstat -rn
Routing Table: IPv4
  Destination           Gateway           Flags  Ref     Use  Interface
-------------------- -------------------- ----- ----- ------- ---------
default              192.168.5.15         UG        1    2664 qfe0
192.168.6.2          192.168.6.22         UG        1     240 qfe1
192.168.3.3          192.168.3.33         U         1     183 qfe1:0
127.0.0.1            127.0.0.1            UH        1     380 lo0
...
```

▼ Configure a Name Service Cache in Each Labeled Zone

This procedure enables you to separately configure a name service daemon (`nscd`) in each labeled zone. This configuration supports environments where each zone is connected to a subnetwork that runs at the label of the zone, and the subnetwork has its own name server for that label.

Note – This configuration does not satisfy the criteria for an evaluated configuration. In an evaluated configuration, the `nscd` daemon runs only in the global zone. Doors in each labeled zone connect the zone to the global `nscd` daemon.

Before You Begin You are superuser in the global zone. `root` must not yet be a role. You have successfully completed "Add a Network Interface to Route an Existing Labeled Zone" on page 77.

This configuration requires that you have advanced networking skills. If LDAP is your naming service, you are responsible for establishing the LDAP client connection to each labeled zone. The `nscd` daemon caches the name service information, but does not route it.

1 If you are using LDAP, verify a route to the LDAP server from the labeled zone.

In a terminal window in every labeled zone, run the following command:

zone-name `# netstat -rn`

2. **In the global zone, start the Labeled Zone Manager.**

   ```
   # /usr/sbin/txzonemgr
   ```

3. **Select the Configure per-zone name service, and click OK.**

   This option is intended to be used once, during initial system configuration.

4. **Configure each zone's `nscd` service.**

   For assistance, see the `nscd(1M)` and `nscd.conf(4)` man pages.

5. **Reboot the system.**

6. **For every zone, verify the route and the name service daemon.**

   a. **In the Zone Console, list the `nscd` service.**

      ```
      zone-name # svcs -x name-service-cache
      svc:/system/name-service-cache:default (name service cache)
       State: online since October 10, 2010  10:10:10 AM PDT
         See: nscd(1M)
         See: /etc/svc/volatile/system-name-service-cache:default.log
      Impact: None.
      ```

   b. **Verify the route to the subnetwork.**

      ```
      zone-name # netstat -rn
      ```

7. **To remove the zone-specific name service daemons, do the following in the global zone:**

   a. **Open the Labeled Zone Manager.**

   b. **Select Unconfigure per-zone name service, and click OK.**

      This selection removes the `nscd` daemon in every labeled zone.

   c. **Reboot the system.**

Creating Roles and Users in Trusted Extensions

If you are already using administrative roles, you might want to add a Security Administrator role. For sites that have not yet implemented roles, the procedure for creating them is similar to the procedure in the Oracle Solaris OS. Trusted Extensions adds the Security Administrator role and requires the use of the Solaris Management Console to administer a Trusted Extensions domain.

If site security requires two people to create user and role accounts, create custom rights profiles and assign them to roles to enforce *separation of duty*.

Task	Description	For Instructions
Create three rights profiles that are more restrictive than default profiles.	Creates rights profiles to manage users. These profiles are more restrictive than the default profiles that manage users.	"Create Rights Profiles That Enforce Separation of Duty" on page 85
Create a security administrator role.	Creates a security administrator role that handles security-relevant tasks.	"Create the Security Administrator Role in Trusted Extensions" on page 88
Create a system administrator role that cannot set a user password.	Creates a system administrator role and assigns to it a restricted System Administrator rights profile.	"Create a Restricted System Administrator Role" on page 90
Create users to assume the administrative roles.	Creates one or more users who can assume roles.	"Create Users Who Can Assume Roles in Trusted Extensions" on page 90
Verify that the roles can perform their tasks.	Tests the roles in various scenarios.	"Verify That the Trusted Extensions Roles Work" on page 93
Enable users to log in to a labeled zone.	Starts the `zones` service so that regular users can log in.	"Enable Users to Log In to a Labeled Zone" on page 95

▼ Create Rights Profiles That Enforce Separation of Duty

Skip this procedure if separation of duty is not a site security requirement. If your site requires separation of duty, you must create these rights profiles and roles before you populate the LDAP server.

This procedure creates rights profiles that have discrete capabilities to manage users. When you assign these profiles to distinct roles, two roles are required to create and configure users. One role can create users, but cannot assign security attributes. The other role can assign security attributes, but cannot create users. When you log in to the Solaris Management Console in a role that is assigned one of these profiles, only the appropriate tabs and fields are available to the role.

Before You Begin You must be superuser, in the `root` role, or in the Primary Administrator role. When you start this procedure, the Solaris Management Console must be closed.

1 Create copies of the default rights profiles that affect user configuration.

a. Copy the `prof_attr` file to the `prof_attr.orig` file.

b. Open the `prof_attr` file in the trusted editor.

```
# /usr/dt/bin/trusted_edit /etc/security/prof_attr
```

c. Copy the three rights profiles and rename the copies.

```
System Administrator:::Can perform most non-security...
Custom System Administrator:::Can perform most non-security...

User Security:::Manage passwords...
Custom User Security:::Manage passwords...

User Management:::Manage users, groups, home...
Custom User Management:::Manage users, groups, home...
```

d. Save the changes.

e. Verify the changes.

```
# grep ^Custom  /etc/security/prof_attr
Custom System Administrator:::Can perform most non-security...
Custom User Management:::Manage users, groups, home...
Custom User Security:::Manage passwords...
```

Copying a rights profile rather than modifying it enables you to upgrade the system to a later Oracle Solaris release and retain your changes. Because these rights profiles are complex, modifying a copy of the default profile is less prone to error than building the more restrictive profile from scratch.

2 Start the Solaris Management Console.

```
# /usr/sbin/smc &
```

3 Select the This Computer (*this-host*: `Scope=Files, Policy=TSOL`) toolbox.

4 Click System Configuration, then click Users.

You are prompted for your password.

5 Type the appropriate password.

6 Double-click Rights.

7 Modify the Custom User Security rights profile.

You restrict this profile from creating a user.

a. Double-click Custom User Security.

b. Click the Authorizations tab, then perform the following steps:

i. From the Included list, remove the `Manage Users and Roles` authorization.

The following User Accounts rights remain:

```
Audit Controls
Label and Clearance Range
Change Password
```

```
View Users and Roles
Modify Extended Security Attributes
```

ii. **Add the Manage Privileges right to the Included list.**

c. **Click OK to save your changes.**

8 **Modify the Custom User Management profile.**

You restrict this profile from setting a password.

a. **Double-click Custom User Management.**

b. **Click the Authorizations tab, then perform the following steps:**

i. **Drag the scrollbar for the Included list to User Accounts.**

ii. **From the Included list, remove the `Modify Extended Security Attributes` authorization.**

The following User Accounts rights remain:

```
Manage Users and Roles
View Users and Roles
```

c. **Save your changes.**

9 **Modify the Custom System Administrator rights profile.**

The User Management profile is a supplementary profile in this profile. You prevent the system administrator from setting a password.

a. **Double-click Custom System Administrator.**

b. **Click the Supplementary Rights tab, then perform the following steps:**

i. **Remove the User Management rights profile.**

ii. **Add the Custom User Management rights profile.**

iii. **Move the Custom User Management rights profile above the All rights profile.**

c. **Save your changes.**

Next Steps To prevent the default profiles from being used, see Step 7 in "Verify That the Trusted Extensions Roles Work" on page 93 after you verify that the custom profiles enforce separation of duty.

▼ Create the Security Administrator Role in Trusted Extensions

Role creation in Trusted Extensions is identical to role creation in the Oracle Solaris OS. However, in Trusted Extensions, a Security Administrator role is required. To create a local Security Administrator role, you can also use the command-line interface, as in Example 4–6.

Before You Begin You must be superuser, in the `root` role, or in the Primary Administrator role.

To create the role on the network, you must have completed "Configuring the Solaris Management Console for LDAP (Task Map)" on page 120.

1. **Start the Solaris Management Console.**

   ```
   # /usr/sbin/smc &
   ```

2. **Select the appropriate toolbox.**

   - **To create the role locally, use This Computer (*this-host*: `Scope=Files, Policy=TSOL`).**
   - **To create the role in the LDAP service, use This Computer (*ldap-server*: `Scope=LDAP, Policy=TSOL`).**

3. **Click System Configuration, then click Users.**

   You are prompted for your password.

4. **Type the appropriate password.**

5. **Double-click Administrative Roles.**

6. **From the Action menu, choose Add Administrative Role.**

7. **Create the Security Administrator role.**

   Use the following information as a guide:

   - Role name – `secadmin`
   - Full name – `Security Administrator`
   - Description – Site Security Officer *No proprietary information here.*
   - Role ID Number – ≥100
   - Role shell – Administrator's Bourne (profile shell)
   - Create a role mailing list – Leave the checkbox selected.
   - Password and confirm – Assign a password of at least 6 alphanumeric characters.

The password for the Security Administrator role, and all passwords, must be difficult to guess, thus reducing the chance of an adversary gaining unauthorized access by attempting to guess passwords.

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

- Available and Granted Rights – Information Security, User Security
  - If site security does not require separation of duty, select the Information Security and the default User Security rights profiles.
  - If site security requires separation of duty, select the Information Security and the Custom User Security rights profiles.
- Home Directory Server – *home-directory-server*
- Home Directory Path – /*mount-path*
- Assign Users– This field is automatically filled in when you assign a role to a user.

8 After creating the role, check that the settings are correct.

Select the role, then double-click it.

Review the values in the following fields:

- Available Groups – Add groups if required.
- Trusted Extensions Attributes – Defaults are correct.

  For a single-label system where the labels must not be visible, choose Hide for Label: Show or Hide.
- Audit Excluded and Included – Set audit flags only if the role's audit flags are exceptions to the system settings in the `audit_control` file.

9 To create other roles, use the Security Administrator role as a guide.

For examples, see "How to Create and Assign a Role by Using the GUI" in *System Administration Guide: Security Services*. Give each role a unique ID, and assign to the role the correct rights profile. Possible roles include the following:

- admin Role – `System Administrator` Granted Rights
- primaryadmin Role – `Primary Administrator` Granted Rights
- oper Role – `Operator` Granted Rights

Example 4–6 Using the roleadd Command to Create a Local Security Administrator Role

In this example, the `root` user adds the Security Administrator role to the local system by using the `roleadd` command. For details, see the `roleadd(1M)` man page. The `root` user consults Table 1–2 before creating the role. At this site, separation of duty is not required to create a user.

```
# roleadd -c "Local Security Administrator" -d /export/home1 \
-u 110 -P "Information Security,User Security" -K lock_after_retries=no \
-K idletime=5 -K idlecmd=lock -K labelview=showsl \
-K min_label=ADMIN_LOW -K clearance=ADMIN_HIGH secadmin
```

The `root` user provides an initial password for the role.

```
# passwd -r files secadmin
New Password:            <Type password>
Re-enter new Password:     <Retype password>
passwd: password successfully changed for secadmin
#
```

To assign the role to a local user, see Example 4–7.

▼ Create a Restricted System Administrator Role

Skip this procedure if separation of duty is not a site security requirement.

In this procedure, you assign a more restrictive rights profile to the System Administrator role.

Before You Begin You must be superuser, in the `root` role, or in the Primary Administrator role.

You have completed "Create Rights Profiles That Enforce Separation of Duty" on page 85. You are using the same toolbox that you used to create the rights profile.

1. **In the Solaris Management Console, create the System Administrator role.**
   For assistance, see "Create the Security Administrator Role in Trusted Extensions" on page 88.
2. **Assign the Custom System Administrator rights profile to the role.**
3. **Save the changes.**
4. **Close the Solaris Management Console.**

▼ Create Users Who Can Assume Roles in Trusted Extensions

To create a local user, you can use the command-line interface, as in Example 4–7, instead of the following procedure. Where site security policy permits, you can choose to create a user who can assume more than one administrative role.

For secure user creation, the System Administrator role creates the user, and the Security Administrator role assigns security-relevant attributes, such as a password.

Before You Begin You must be superuser, in the `root` role, in the Security Administrator role, or in the Primary Administrator role. The Security Administrator role has the least amount of privilege that is required for user creation.

The Solaris Management Console is displayed. For details, see "Create the Security Administrator Role in Trusted Extensions" on page 88.

1. **Double-click User Accounts in the Solaris Management Console.**
2. **From the Action menu, choose Add User → Use Wizard.**

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

3. **Follow the online help.**

   You can also follow the procedures in "How to Add a User With the Solaris Management Console's Users Tool" in *System Administration Guide: Basic Administration*.

4. **After creating the user, double-click the created user to modify the settings.**

   Note – For users who can assume roles, make the user account Always Available, and do not set password expiration dates.

   Ensure that the following fields are correctly set:

   - Description – No proprietary information here.
   - Password and confirm – Assign a password of at least 6 alphanumeric characters.

     Note – When the initial setup team chooses a password, the team must select a password that is difficult to guess, thus reducing the chance of an adversary gaining unauthorized access by attempting to guess passwords.

   - Account Availability – Always Available.
   - Trusted Extensions Attributes – Defaults are correct.

     For a single-label system where the labels must not be visible, choose Hide for Label: Show or Hide.
   - Account Usage – Set Idle time and Idle action.

     Lock account – Set to No for any user who can assume a role.

5. **Close the Solaris Management Console.**

6 **Customize the user's environment.**

a. **Assign convenient authorizations.**

After checking your site security policy, you might want to grant your first users the Convenient Authorizations rights profile. With this profile, you can enable users to allocate devices, print PostScript files, print without labels, remotely log in, and shut down the system. To create the profile, see "How to Create a Rights Profile for Convenient Authorizations" in *Trusted Extensions Administrator's Procedures*.

b. **Customize user initialization files.**

See Chapter 7, "Managing Users, Rights, and Roles in Trusted Extensions (Tasks)," in *Trusted Extensions Administrator's Procedures*.

Also see "Managing Users and Rights With the Solaris Management Console (Task Map)" in *Trusted Extensions Administrator's Procedures*.

c. **Create multilabel copy and link files.**

On a multilabel system, users and roles can be set up with files that list user initialization files to be copied or linked to other labels. For more information, see ".copy_files and .link_files Files" in *Trusted Extensions Administrator's Procedures*.

Example 4–7 Using the useradd Command to Create a Local User

In this example, the `root` user creates a local user who can assume the Security Administrator role. For details, see the `useradd(1M)` and `atohexlabel(1M)` man pages.

First, the `root` user determines the hexadecimal format of the user's minimum label and clearance label.

```
# atohexlabel public
0x0002-08-08
# atohexlabel -c "confidential restricted"
0x0004-08-78
```

Next, the `root` user consults Table 1–2, and then creates the user.

```
# useradd -c "Local user for Security Admin" -d /export/home1 \
-K  idletime=10 -K idlecmd=logout -K lock_after_retries=no
-K min_label=0x0002-08-08 -K clearance=0x0004-08-78 -K labelview=showsl jandoe
```

Then, the `root` user provides an initial password.

```
# passwd -r files jandoe
New Password:         <Type password>
Re-enter new Password:      <Retype password>
passwd: password successfully changed for jandoe
#
```

Finally, the `root` user adds the Security Administrator role to the user's definition. The role was created in "Create the Security Administrator Role in Trusted Extensions" on page 88.

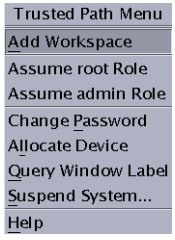
```
# usermod -R secadmin jandoe
```

▼ Verify That the Trusted Extensions Roles Work

To verify each role, assume the role. Then, perform tasks that only that role can perform.

Before You Begin If you have configured DNS or routing, you must reboot after you create the roles and before you verify that the roles work.

1. **For each role, log in as a user who can assume the role.**
2. **Open the Trusted Path menu.**
   - **In Trusted CDE, click the workspace switch area.**

     From the menu, assume the role.
   - **In Trusted JDS, click your user name in the trusted stripe.**

     In the following trusted stripe, the user name is `tester`.

     From the list of roles that are assigned to you, select a role.
3. **In the role workspace, start the Solaris Management Console.**

   ```
   $ /usr/sbin/smc &
   ```
4. **Select the appropriate scope for the role that you are testing.**

5 **Click System Services, and navigate to Users.**

You are prompted for a password.

a. **Type the role password.**

b. **Double-click User Accounts.**

6 **Click a user.**

- The System Administrator role should be able to modify fields under the General, Home Directory, and Group tabs.

  If you configured the roles to enforce separation of duty, then the System Administrator role cannot set the user's initial password.
- The Security Administrator role should be able to modify fields under all tabs.

  If you configured the roles to enforce separation of duty, then the Security Administrator role cannot create a user.
- The Primary Administrator role should be able to modify fields under all tabs.

7 **(Optional) If you are enforcing separation of duty, prevent the default rights profiles from being used.**

Note – When the system is upgraded to a newer version of the Oracle Solaris OS, the System Administrator, User Management, and User Security default profiles are replaced.

In the trusted editor, perform one of the following steps:

- **Remove the three rights profiles from the `prof_attr` file.**

  Removal prevents an administrator from viewing or assigning these profiles. Also, remove the `prof_attr.orig` file.

- **Comment out the three rights profiles in the `prof_attr` file.**

  Commenting out the rights profiles prevents these profiles from being viewed in the Solaris Management Console or from being used in commands that manage users. The profiles and their contents can still be viewed in the `prof_attr` file.

- **Type a different description for the three rights profiles in the `prof_attr` file.**

  Edit the `prof_attr` file to change the description field of these rights profiles. For example, you might replace the descriptions with `Do not use this profile`. This change warns an administrator to not use the profile, but does not prevent the profile from being used.

▼ Enable Users to Log In to a Labeled Zone

When the host is rebooted, the association between the devices and the underlying storage must be re-established.

Before You Begin You have created at least one labeled zone. That zone is not being used for cloning.

1. **Reboot the system.**
2. **Log in as the `root` user.**
3. **Restart the zones service.**

```
# svcs zones
STATE          STIME    FMRI
offline        -        svc:/system/zones:default

# svcadm restart svc:/system/zones:default
```

4. **Log out.**

   Regular users can now log in. Their session is in a labeled zone.

Creating Home Directories in Trusted Extensions

In Trusted Extensions, users need access to their home directories at every label at which the users work. To make every home directory available to the user requires that you create a multilevel home directory server, run the automounter on the server, and export the home directories. On the client side, you can run scripts to find the home directory for every zone for each user, or you can have the user log in to the home directory server.

▼ Create the Home Directory Server in Trusted Extensions

Before You Begin You must be superuser, in the `root` role, or in the Primary Administrator role.

1. **Install and configure the home directory server with Trusted Extensions software.**
   - If you are cloning zones, make sure that you use a ZFS snapshot that has empty home directories.
   - Because users require a home directory at every label that they they can log in to, create every zone that a user can log in to. For example, if you use the default `label_encodings` file, you would create a zone for the `PUBLIC` label.

2. **If you are using UFS and not ZFS, enable the NFS server to serve itself.**

   a. **In the global zone, modify the `automount` entry in the `nsswitch.conf` file.**

      Use the trusted editor to edit the `/etc/nsswitch.conf` file. For the procedure, see "How to Edit Administrative Files in Trusted Extensions" in *Trusted Extensions Administrator's Procedures*.

      ```
      automount: files
      ```

   b. **In the global zone, run the `automount` command.**

3. **For every labeled zone, follow the automount procedure in "How to NFS Mount Files in a Labeled Zone" in *Trusted Extensions Administrator's Procedures*. Then, return to this procedure.**

4. **Verify that the home directories have been created.**

   a. **Log out of the home directory server.**

   b. **As a regular user, log in to the home directory server.**

   c. **In the login zone, open a terminal.**

   d. **In the terminal window, verify that the user's home directory exists.**

   e. **Create workspaces for every zone that the user can work in.**

   f. **In each zone, open a terminal window to verify that the user's home directory exists.**

5. **Log out of the home directory server.**

▼ Enable Users to Access Their Home Directories in Trusted Extensions

Users can initially log in to the home directory server to create a home directory that can be shared with other systems. To create a home directory at every label, each user must log in to the home directory server at every label.

Alternatively, you, as administrator, can create a script to create a mount point for home directories on each user's home system before the user first logs in. The script creates mount points at every label at which the user is permitted to work.

Before You Begin The home directory server for your Trusted Extensions domain is configured.

- **Choose whether to allow direct login to the server, or whether to run a script.**

  - **Enable users to log in directly to the home directory server.**

    a. **Instruct each user to log in to the home directory server.**

       After successful login, the user must log out.

    b. **Instruct each user to log in again, and this time, to choose a different login label.**

       The user uses the label builder to choose a different login label. After successful login, the user must log out.

    c. **Instruct each user to repeat the login process for every label that the user is permitted to use.**

    d. **Instruct the users to log in from their regular workstation.**

       Their home directory for their default label is available. When a user changes the label of a session or adds a workspace at a different label, the user's home directory for that label is mounted.

  - **Write a script that creates a home directory mount point for every user, and run the script.**

```
#!/bin/sh
#
for zoneroot in ‘/usr/sbin/zoneadm list -p | cut -d ":" -f4‘ ; do
    if [ $zoneroot != / ]; then
        prefix=$zoneroot/root/export

        for j in ‘getent passwd|tr ’ ’ _‘ ; do
            uid=‘echo $j|cut -d ":" -f3‘
            if [ $uid -ge 100 ]; then
                gid=‘echo $j|cut -d ":" -f4‘
                homedir=‘echo $j|cut -d ":" -f6‘
                mkdir -m 711 -p $prefix$homedir
                chown $uid:$gid $prefix$homedir
            fi
        done
    fi
done
```

    a. **From the global zone, run this script on the NFS server.**

    b. **Then, run this script on every multilevel desktop that the user is going to log in to.**

Adding Users and Hosts to an Existing Trusted Network

If you have users who are defined in NIS maps, you can add them to your network.

To add hosts and labels to hosts, see the following procedures:

- To add a host, you use the Computers and Networks tool set in the Solaris Management Console. For details, see "How to Add Hosts to the System's Known Network" in *Trusted Extensions Administrator's Procedures*.

  When you add a host to the LDAP server, add all IP addresses that are associated with the host. All-zones addresses, including addresses for labeled zones, must be added to the LDAP server.
- To label a host, see "How to Assign a Security Template to a Host or a Group of Hosts" in *Trusted Extensions Administrator's Procedures*.

▼ Add an NIS User to the LDAP Server

Before You Begin You must be superuser, in the `root` role, or in the Primary Administrator role.

1 From the NIS database, gather the information that you need.

a. Create a file from the user's entry in the `aliases` database.

```
% ypcat -k aliases | grep login-name > aliases.name
```

b. Create a file from the user's entry in the `passwd` database.

```
% ypcat -k passwd | grep "Full Name" > passwd.name
```

c. Create a file from the user's entry in the `auto_home_` database.

```
% ypcat -k auto_home | grep login-name > auto_home_label
```

2 Reformat the information for LDAP and Trusted Extensions.

a. Use the `sed` command to reformat the `aliases` entry.

```
% sed 's/ /:/g' aliases.login-name > aliases
```

b. Use the `nawk` command to reformat the `passwd` entry.

```
% nawk -F: '{print $1":x:"$3":"$4":"$5":"$6":"$7}' passwd.name > passwd
```

c. Use the `nawk` command to create a `shadow` entry.

```
% nawk -F: '{print $1":"$2":6445::::::"}' passwd.name > shadow
```

d. Use the `nawk` command to create a `user_attr` entry.

```
% nawk -F: '{print $1"::::lock_after_retries=yes-or-no;profiles=user-profile, ...;
labelview=int-or-ext,show-or-hide;min_label=min-label;
clearance=max-label;type=normal;roles=role-name,...;
auths=auth-name,..."}' passwd.name > user_attr
```

3 Copy the modified files to the `/tmp` directory on the LDAP server.

```
# cp aliases auto_home_internal passwd shadow user_attr /tmp/name
```

4 Add the entries in the files in Step 3 to the databases on the LDAP server.

```
# /usr/sbin/ldapaddent -D "cn=directory manager" -w DM-password \
-a simple -f /tmp/name/aliases aliases
# /usr/sbin/ldapaddent -D "cn=directory manager" -w DM-password \
-a simple -f /tmp/name/auto_home_internal auto_home_internal
# /usr/sbin/ldapaddent -D "cn=directory manager" -w DM-password \
-a simple -f /tmp/name/passwd passwd
# /usr/sbin/ldapaddent -D "cn=directory manager" -w DM-password \
-a simple -f /tmp/name/shadow shadow
# /usr/sbin/ldapaddent -D "cn=directory manager" -w DM-password \
-a simple -f /tmp/name/user_attr user_attr
```

Example 4–8 Adding a User From an NIS Database to the LDAP Server

In the following example, the administrator adds a new user to the trusted network. The user's information is stored originally in an NIS database. To protect the LDAP server password, the administrator runs the `ldapaddent` commands on the server.

In Trusted Extensions, the new user can allocate devices and assume the Operator role. Because the user can assume a role, the user account does not get locked out. The user's minimum label is `PUBLIC`. The label at which the user works is `INTERNAL`, so `jan` is added to the `auto_home_internal` database. The `auto_home_internal` database automounts `jan`'s home directory with read-write permissions.

- On the LDAP server, the administrator extracts user information from NIS databases.

  ```
  # ypcat -k aliases | grep jan.doe > aliases.jan
  # ypcat passwd | grep "Jan Doe" > passwd.jan
  # ypcat -k auto_home | grep jan.doe > auto_home_internal
  ```

- Then, the administrator reformats the entries for LDAP.

  ```
  # sed 's/ /:/g' aliases.jan > aliases
  # nawk -F: '{print $1":x:"$3":"$4":"$5":"$6":"$7}' passwd.jan > passwd
  # nawk -F: '{print $1":"$2":6445::::::"}' passwd.jan > shadow
  ```

- Then, the administrator creates a `user_attr` entry for Trusted Extensions.

  ```
  # nawk -F: '{print $1"::::lock_after_retries=no;profiles=Media User;
  labelview=internal,showsl;min_label=0x0002-08-08;
  clearance=0x0004-08-78;type=normal;roles=oper;
  auths=solaris.device.allocate"}' passwd.jan > user_attr
  ```

- Then, the administrator copies the files to the `/tmp/jan` directory.

  ```
  # cp aliases auto_home_internal passwd shadow user_attr /tmp/jan
  ```

- Finally, the administrator populates the server with the files in the `/tmp/jan` directory.

```
# /usr/sbin/ldapaddent -D "cn=directory manager" -w a2b3c4d5e6 \
-a simple -f /tmp/jan/aliases aliases
# /usr/sbin/ldapaddent -D "cn=directory manager" -w a2b3c4d5e6 \
-a simple -f /tmp/jan/auto_home_internal auto_home_internal
# /usr/sbin/ldapaddent -D "cn=directory manager" -w a2b3c4d5e6 \
-a simple -f /tmp/jan/passwd passwd
# /usr/sbin/ldapaddent -D "cn=directory manager" -w a2b3c4d5e6 \
-a simple -f /tmp/jan/shadow shadow
# /usr/sbin/ldapaddent -D "cn=directory manager" -w a2b3c4d5e6 \
-a simple -f /tmp/jan/user_attr user_attr
```

Troubleshooting Your Trusted Extensions Configuration

In Trusted Extensions, the labeled zones communicate with the X server through the global zone. Therefore, the labeled zones must have usable routes to the global zone. Also, options that were selected during an Oracle Solaris installation can prevent Trusted Extensions from using interfaces to the global zone.

netservices limited Was Run After Trusted Extensions Was Enabled

Description:

Instead of running the `netservices limited` command before you enabled Trusted Extensions, you ran the command in the global zone afterwards. Therefore, your labeled zones are unable to connect to the X server in the global zone.

Solution:

Run the following commands to open the services that Trusted Extensions requires to communicate between zones:

```
# svccfg -s x11-server setprop options/tcp_listen = true
# svcadm enable svc:/network/rpc/rstat:default
```

Cannot Open the Console Window in a Labeled Zone

Description:

When you attempt to open a console window in a labeled zone, the following error appears in a dialog box:

```
Action:DttermConsole,*,*,*,0 [Error]
Action not authorized.
```

Solution:

Verify that the following two lines are present in each of the zone entries in the `/etc/security/exec_attr` file:

```
All Actions:solaris:act:::*;*;*;*;*:
All:solaris:act:::*;*;*;*;*:
```

If these lines are not present, the Trusted Extensions package that adds these entries was not installed in the labeled zones. In this case, re-create the labeled zones. For the procedure, see "Creating Labeled Zones" on page 62.

Labeled Zone Is Unable to Access the X Server

Description:

If a labeled zone cannot successfully access the X server, you might see messages such as the following:

- `Action failed. Reconnect to Solaris Zone?`
- `No route available`
- `Cannot reach globalzone-`*hostname*`:0`

Cause:

The labeled zones might not be able to access the X server for any of the following reasons:

- The zone is not initialized and is waiting for the `sysidcfg` process to complete.
- The labeled zone's host name is not recognized by the naming service that runs in the global zone.
- No interface is specified as `all-zones`.
- The labeled zone's network interface is down.
- LDAP name lookups fail.
- NFS mounts do not work.

Steps toward a solution:

Do the following:

1. Log in to the zone.

   You can use the `zlogin` command or the Zone Terminal Console action.

   ```
   # zlogin -z zone-name
   ```

   If you cannot log in as superuser, use the `zlogin -S` command to bypass authentication.

2. Verify that the zone is running.

   ```
   # zoneadm list
   ```

   If a zone has a status of `running`, the zone is running at least one process.

3. Address any problems that prevent the labeled zones from accessing the X server.
   - Initialize the zone by completing the `sysidcfg` process.

Run the `sysidcfg` program interactively. Answer the prompts in the Zone Terminal Console, or in the terminal window where you ran the `zlogin` command.

To run the `sysidcfg` process noninteractively, you can do one of the following:

- Specify the Initialize item for the `/usr/sbin/txzonemgr` script.

  The Initialize item enables you to supply default values to the `sysidcfg` questions.

- Write your own `sysidcfg` script.

  For more information, see the `sysidcfg(4)` man page.

- Verify that the X server is available to the zone.

  Log in to the labeled zone. Set the `DISPLAY` variable to point to the X server, and open a window.

  ```
  # DISPLAY=global-zone-hostname:n.n
  # export DISPLAY
  # /usr/openwin/bin/xclock
  ```

  If a labeled window does not appear, the zone networking has not been configured correctly for that labeled zone.

  Note – If you are running Trusted CDE starting with the Solaris 10 5/09 release, see "Resolve Local Zone to Global Zone Routing in Trusted CDE" on page 152.

- Configure the zone's host name with the naming service.

  The zone's local `/etc/hosts` file is not used. Instead, equivalent information must be specified in the global zone or on the LDAP server. The information must include the IP address of the host name that is assigned to the zone.

- No interface is specified as `all-zones`.

  Unless all your zones have IP addresses on the same subnet as the global zone, you might need to configure an `all-zones` (shared) interface. This configuration enables a labeled zone to connect to the X server of the global zone. If you want to restrict remote connections to the X server of the global zone, you can use `vni0` as the `all-zones` address.

  If you do *not* want an `all-zones` interface configured, you must provide a route to the global zone X server for each zone. These routes must be configured in the global zone.

- The labeled zone's network interface is down.

  ```
  # ifconfig -a
  ```

  Use the `ifconfig` command to verify that the labeled zone's network interface is both `UP` and `RUNNING`.

- LDAP name lookups fail.

  Use the `ldaplist` command to verify that each zone can communicate with the LDAP server or the LDAP proxy server. On the LDAP server, verify that the zone is listed in the `tnrhdb` database.
- NFS mounts do not work.

  As superuser, restart `automount` in the zone. Or, add a `crontab` entry to run the `automount` command every five minutes.

Additional Trusted Extensions Configuration Tasks

The following two tasks enable you to transfer exact copies of configuration files to every Trusted Extensions system at your site. The final task enables you to remove Trusted Extensions customizations from an Oracle Solaris system.

▼ How to Copy Files to Portable Media in Trusted Extensions

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

Note – During Trusted Extensions configuration, superuser or an equivalent role copies administrative files to and from portable media. Label the media with `Trusted Path`.

Before You Begin To copy administrative files, you must be superuser or in a role in the global zone.

1. **Allocate the appropriate device.**

   Use the Device Allocation Manager, and insert clean media. For details, see "How to Allocate a Device in Trusted Extensions" in *Trusted Extensions User's Guide*.

   - In Solaris Trusted Extensions (CDE), a *File Manager* displays the contents of the portable media.
   - In Solaris Trusted Extensions (JDS), a *File Browser* displays the contents.

   In this procedure, File Browser is used to refer to this GUI.

2. **Open a second File Browser.**

3. **Navigate to the folder that contains the files to be copied**

   For example, you might have copied files to an `/export/clientfiles` folder.

4 **For each file, do the following:**

   a. **Highlight the icon for the file.**

   b. **Drag the file to the File Browser for the portable media.**

5 **Deallocate the device.**

   For details, see "How to Deallocate a Device in Trusted Extensions" in *Trusted Extensions User's Guide*.

6 **On the File Browser for the portable media, choose Eject from the File menu.**

Note – Remember to physically affix a label to the media with the sensitivity label of the copied files.

Example 4–9 Keeping Configuration Files Identical on All Systems

The system administrator wants to ensure that every machine is configured with the same settings. So, on the first machine that is configured, she creates a directory that cannot be deleted between reboots. In that directory, the administrator places the files that should be identical or very similar on all systems.

For example, she copies the Trusted Extensions toolbox that the Solaris Management Console uses for the LDAP scope, `/var/sadm/smc/toolboxes/tsol_ldap/tsol_ldap.tbx`. She has customized remote host templates in the `tnrhtp` file, has a list of DNS servers, and audit configuration files. She also modified the `policy.conf` file for her site. So, she copies the files to the permanent directory.

```
# mkdir /export/commonfiles
# cp  /etc/security/policy.conf \
/etc/security/audit_control \
/etc/security/audit_startup \
/etc/security/tsol/tnrhtp \
/etc/resolv.conf \
/etc/nsswitch.conf \
/export/commonfiles
```

She uses the Device Allocation Manager to allocate a diskette in the global zone, and transfers the files to the diskette. On a separate diskette, labeled `ADMIN_HIGH`, she puts the `label_encodings` file for the site.

When she copies the files onto a system, she modifies the `dir:` entries in the `/etc/security/audit_control` file for that system.

▼ How to Copy Files From Portable Media in Trusted Extensions

It is safe practice to rename the original Trusted Extensions file before replacing the file. When configuring a system, the `root` role renames and copies administrative files.

Before You Begin To copy administrative files, you must be superuser or in a role in the global zone.

1. **Allocate the appropriate device.**

   For details, see "How to Allocate a Device in Trusted Extensions" in *Trusted Extensions User's Guide*.

   - In Solaris Trusted Extensions (CDE), a *File Manager* displays the contents of the portable media.
   - In Solaris Trusted Extensions (JDS), a *File Browser* displays the contents.

   In this procedure, File Browser is used to refer to this GUI.

2. **Insert the media that contains the administrative files.**

3. **If the system has a file of the same name, copy the original file to a new name.**

   For example, add `.orig` to the end of the original file:

   ```
   # cp /etc/security/tsol/tnrhtp /etc/security/tsol/tnrhtp.orig
   ```

4. **Open a File Browser.**

5. **Navigate to the desired destination directory, such as `/etc/security/tsol`**

6. **For each file that you want to copy, do the following:**

   a. **In the File Browser for the mounted media, highlight the icon for the file.**

   b. **Then, drag the file to the destination directory in the second File Browser.**

7. **Deallocate the device.**

   For details, see "How to Deallocate a Device in Trusted Extensions" in *Trusted Extensions User's Guide*.

8. **When prompted, eject and remove the media.**

Example 4–10 Loading Audit Configuration Files in Trusted Extensions

In this example, roles are not yet configured on the system. The `root` user needs to copy configuration files to portable media. The contents of the media will then be copied to other systems. These files are to be copied to each system that is configured with Trusted Extensions software.

The `root` user allocates the `floppy_0` device in the Device Allocation Manager and responds `yes` to the mount query. Then, the `root` user inserts the diskette with the configuration files and copies them to the disk. The diskette is labeled `Trusted Path`.

To read from the media, the `root` user allocates the device on the receiving host, then downloads the contents.

If the configuration files are on a tape, the `root` user allocates the `mag_0` device. If the configuration files are on a CD-ROM, the `root` user allocates the `cdrom_0` device.

▼ How to Remove Trusted Extensions From the System

To remove Trusted Extensions from your Oracle Solaris system, you perform specific steps to remove Trusted Extensions customizations to the Oracle Solaris system.

1. **As in the Oracle Solaris OS, archive any data in the labeled zones that you want to keep.**

2. **Remove the labeled zones from the system.**

   For details, see "How to Remove a Non-Global Zone" in *System Administration Guide: Oracle Solaris Containers-Resource Management and Oracle Solaris Zones*.

3. **Disable the Trusted Extensions service.**

   ```
   # svcadm disable labeld
   ```

4. **Run the `bsmunconv` command.**

   For the effect of this command, see the `bsmunconv(1M)` man page.

5. **(Optional) Reboot the system.**

6. **Configure the system.**

   Various services might need to be configured for your Oracle Solaris system. Candidates include auditing, basic networking, naming services, and file system mounts.

◆ ◆ ◆ CHAPTER 5

Configuring LDAP for Trusted Extensions (Tasks)

This chapter covers how to configure the Sun Java System Directory Server and the Solaris Management Console for use with Trusted Extensions. The Directory Server provides LDAP services. LDAP is the supported naming service for Trusted Extensions. The Solaris Management Console is the administrative GUI for local and LDAP databases.

You have two options when configuring the Directory Server. You can configure an LDAP server on a Trusted Extensions system, or you can use an existing server and connect to it by using a Trusted Extensions proxy server. Follow the instructions in *one* of the following task maps:

- "Configuring an LDAP Server on a Trusted Extensions Host (Task Map)" on page 107
- "Configuring an LDAP Proxy Server on a Trusted Extensions Host (Task Map)" on page 108

Configuring an LDAP Server on a Trusted Extensions Host (Task Map)

Task	Description	For Instructions
Set up a Trusted Extensions LDAP server.	If you do not have an existing Sun Java System Directory Server, make your first Trusted Extensions system the Directory Server. This system does not have labeled zones installed. The other Trusted Extensions systems are clients of this server.	"Collect Information for the Directory Server for LDAP" on page 109 "Install the Sun Java System Directory Server" on page 110 "Configure the Logs for the Sun Java System Directory Server" on page 114
Add Trusted Extensions databases to the server.	Populate the LDAP server with data from the Trusted Extensions system files.	"Populate the Sun Java System Directory Server" on page 116

Task	Description	For Instructions
Configure the Solaris Management Console to work with the Directory Server.	Manually set up an LDAP toolbox for the Solaris Management Console. The toolbox can be used to modify Trusted Extensions attributes on network objects.	"Configuring the Solaris Management Console for LDAP (Task Map)" on page 120
Configure all other Trusted Extensions systems as clients of this server.	When you configure another system with Trusted Extensions, make the system a client of this LDAP server.	"Make the Global Zone an LDAP Client in Trusted Extensions" on page 59

Configuring an LDAP Proxy Server on a Trusted Extensions Host (Task Map)

Use this task map if you have an existing Sun Java System Directory Server that is running on an Oracle Solaris system.

Task	Description	For Instructions
Add Trusted Extensions databases to the server.	The Trusted Extensions network databases, `tnrhdb` and `tnrhtp`, need to be added to the LDAP server.	"Populate the Sun Java System Directory Server" on page 116
Set up an LDAP proxy server.	Make one Trusted Extensions system the proxy server for the other Trusted Extensions systems. The other Trusted Extensions systems use this proxy server to reach the LDAP server.	"Create an LDAP Proxy Server" on page 119
Configure the proxy server to have a multilevel port for LDAP.	Enable the Trusted Extensions proxy server to communicate with the LDAP server at specific labels.	"Configure a Multilevel Port for the Sun Java System Directory Server" on page 115
Configure the Solaris Management Console to work with the LDAP proxy server.	You manually set up an LDAP toolbox for the Solaris Management Console. The toolbox can be used to modify Trusted Extensions attributes on network objects.	"Configuring the Solaris Management Console for LDAP (Task Map)" on page 120
Configure all other Trusted Extensions systems as clients of the LDAP proxy server.	When you configure another system with Trusted Extensions, make the system a client of the LDAP proxy server.	"Make the Global Zone an LDAP Client in Trusted Extensions" on page 59

Configuring the Sun Java System Directory Server on a Trusted Extensions System

The LDAP naming service is the supported naming service for Trusted Extensions. If your site is not yet running the LDAP naming service, configure a Sun Java System Directory Server (Directory Server) on a system that is configured with Trusted Extensions.

If your site is already running a Directory Server, then you need to add the Trusted Extensions databases to the server. To access the Directory Server, you then set up an LDAP proxy on a Trusted Extensions system.

Note – If you do not use this LDAP server as an NFS server or as a server for Sun Ray clients, then you do not need to install any labeled zones on this server.

▼ Collect Information for the Directory Server for LDAP

- **Determine the values for the following items.**

  The items are listed in the order of their appearance in the Sun Java Enterprise System Install Wizard.

Install Wizard Prompt	Action or Information
Sun Java System Directory Server *version*	
Administrator User ID	The default value is `admin`.
Administrator Password	Create a password, such as `admin123`.
Directory Manager DN	The default value is `cn=Directory Manager`.
Directory Manager Password	Create a password, such as `dirmgr89`.
Directory Server Root	The default value is `/var/Sun/mps`. This path is also used later if the proxy software is installed.
Server Identifier	The default value is the local system.
Server Port	If you plan to use the Directory Server to provide standard LDAP naming services to client systems, use the default value, `389`.
	If you plan to use the Directory Server to support a subsequent installation of a proxy server, enter a nonstandard port, such as `10389`.
Suffix	Include your domain component, as in `dc=example-domain,dc=com`.
Administration Domain	Construct to correspond to the Suffix, as in, `example-domain.com`.

Install Wizard Prompt	Action or Information
System User	The default value is `root`.
System Group	The default value is `root`.
Data Storage Location	The default value is `Store configuration data on this server`.
Data Storage Location	The default value is `Store user data and group data on this server`.
Administration Port	The default value is the Server Port. A suggested convention for changing the default is `software-version TIMES 1000`. For software version 5.2, this convention would result in port `5200`.

▼ Install the Sun Java System Directory Server

The Directory Server packages are available from the Sun Software Gateway web site (`http://www.oracle.com/solaris`).

Before You Begin You are on a Trusted Extensions system with only a global zone installed. The system has no labeled zones.

Trusted Extensions LDAP servers are configured for clients that use `pam_unix` to authenticate to the LDAP repository. With `pam_unix`, the password operations, and therefore the password policy, are determined by the client. Specifically, the policy set by the LDAP server is not used. For the password parameters that you can set on the client, see "Managing Password Information" in *System Administration Guide: Security Services*. For information about `pam_unix`, see the `pam.conf(4)` man page.

Note – The use of `pam_ldap` on an LDAP client is not an evaluated configuration for Trusted Extensions.

---

1 Before you install the Directory Server packages, add the FQDN to your system's hostname entry.

The FQDN is the Fully Qualified Domain Name. This name is a combination of the host name and the administration domain, as in:

```
## /etc/hosts
...
192.168.5.5 myhost myhost.example-domain.com
```

On a system that is running a release prior to the Solaris 10 8/07 release, add IPv4 and IPv6 entries to the `/etc/inet/ipnodes` file. The entries for one system must be contiguous in the file.

If you are not running the latest release of the Oracle Solaris OS, you must have the following patches installed. The first number is a SPARC patch. The second number is an X86 patch.

- 138874–05, 138875–05: Native LDAP, PAM, name-service-switch patch

- 119313-35, 119314-36: WBEM patch
- 121308-21, 121308-21: Solaris Management Console patch
- 119315-20, 119316-20: Solaris Management Applications patch

2 Find the Sun Java System Directory Server packages on the Oracle Sun web site.

a. On the Sun Software Gateway (`http://www.oracle.com/solaris`) page, click the Get It tab.

b. Click the checkbox for the Sun Java Identity Management Suite.

c. Click the Submit button.

d. If you are not registered, register.

e. Log in to download the software.

f. Click the Download Center at the upper left of the screen.

g. Under Identity Management, download the most recent software that is appropriate for your platform.

3 Install the Directory Server packages.

Answer the questions by using the information from "Collect Information for the Directory Server for LDAP" on page 109. For a full list of questions, defaults, and suggested answers, see Chapter 11, "Setting Up Sun Java System Directory Server With LDAP Clients (Tasks)," in *System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)* and Chapter 12, "Setting Up LDAP Clients (Tasks)," in *System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)*.

4 (Optional) Add the environment variables for the Directory Server to your path.

```
# $PATH
/usr/sbin:.../opt/SUNWdsee/dsee6/bin:/opt/SUNWdsee/dscc6/bin:/opt/SUNWdsee/ds6/bin:
/opt/SUNWdsee/dps6/bin
```

5 (Optional) Add the Directory Server man pages to your `MANPATH`.

```
/opt/SUNWdsee/dsee6/man
```

6 Enable the `cacaoadm` program and verify that the program is enabled.

```
# /usr/sbin/cacaoadm enable
# /usr/sbin/cacaoadm start
start: server (pid n) already running
```

7 **Ensure that the Directory Server starts at every boot.**

Templates for the SMF services for the Directory Server are in the Sun Java System Directory Server packages.

- **For a Trusted Extensions Directory Server, enable the service.**

```
# dsadm stop /export/home/ds/instances/your-instance
# dsadm enable-service -T SMF /export/home/ds/instances/your-instance
# dsadm start /export/home/ds/instances/your-instance
```

For information about the `dsadm` command, see the `dsadm`(1M) man page.

- **For a proxy Directory Server, enable the service.**

```
# dpadm stop /export/home/ds/instances/your-instance
# dpadm enable-service -T SMF /export/home/ds/instances/your-instance
# dpadm start /export/home/ds/instances/your-instance
```

For information about the `dpadm` command, see the `dpadm`(1M) man page.

8 **Verify your installation.**

```
# dsadm info /export/home/ds/instances/your-instance
Instance Path:         /export/home/ds/instances/your-instance
Owner:                 root(root)
Non-secure port:       389
Secure port:           636
Bit format:            32-bit
State:                 Running
Server PID:            298
DSCC url:              -
SMF application name:  ds--export-home-ds-instances-your-instance
Instance version:      D-A00
```

Troubleshooting For strategies to solve LDAP configuration problems, see Chapter 13, "LDAP Troubleshooting (Reference)," in *System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)*.

▼ Create an LDAP Client for the Directory Server

You use this client to populate your Directory Server for LDAP. You must perform this task before you populate the Directory Server.

You can create the client temporarily on the Trusted Extensions Directory Server, then remove the client on the server, or you can create an independent client.

1 **Install Trusted Extensions on a system.**

You can use the Trusted Extensions Directory Server, or install Trusted Extensions on a separate system.

Note – If you are not running the latest release of the Oracle Solaris OS, you must have the following patches installed. The first number is a SPARC patch. The second number is an X86 patch.

- 138874–05, 138875–05: Native LDAP, PAM, name-service-switch patch
- 119313-35, 119314-36: WBEM patch
- 121308-21, 121308-21: Solaris Management Console patch
- 119315-20, 119316-20: Solaris Management Applications patch

2 On the client, modify the default `/etc/nsswitch.ldap` file.

The entries in bold indicate the modifications. The file appears similar to the following:

```
# /etc/nsswitch.ldap
#
# An example file that could be copied over to /etc/nsswitch.conf; it
# uses LDAP in conjunction with files.
#
# "hosts:" and "services:" in this file are used only if the
# /etc/netconfig file has a "-" for nametoaddr_libs of "inet" transports.

# LDAP service requires that svc:/network/ldap/client:default be enabled
# and online.

# the following two lines obviate the "+" entry in /etc/passwd and /etc/group.
passwd:     files ldap
group:      files ldap

# consult /etc "files" only if ldap is down.
hosts:      files ldap dns [NOTFOUND=return] files

# Note that IPv4 addresses are searched for in all of the ipnodes databases
# before searching the hosts databases.
ipnodes:    files ldap [NOTFOUND=return] files

networks:   files ldap [NOTFOUND=return] files
protocols:  files ldap [NOTFOUND=return] files
rpc:        files ldap [NOTFOUND=return] files
ethers:     files ldap [NOTFOUND=return] files
netmasks:   files ldap [NOTFOUND=return] files
bootparams: files ldap [NOTFOUND=return] files
publickey:  files ldap [NOTFOUND=return] files

netgroup:   ldap

automount:  files ldap
aliases:    files ldap

# for efficient getservbyname() avoid ldap
services:   files ldap

printers:   user files ldap

auth_attr:  files ldap
prof_attr:  files ldap
```

```
project:    files ldap

tnrhtp:     files ldap
tnrhdb:     files ldap
```

3 **In the global zone, run the `ldapclient init` command.**

This command copies the `nsswitch.ldap` file to the `nsswitch.conf` file.

In this example, the LDAP client is in the `example-domain.com` domain. The server's IP address is `192.168.5.5`.

```
# ldapclient init -a domainName=example-domain.com -a profileNmae=default \
> -a proxyDN=cn=proxyagent,ou=profile,dc=example-domain,dc=com \
> -a proxyDN=cn=proxyPassword={NS1}ecc423aad0 192.168.5.5
System successfully configured
```

4 **Set the server's `enableShadowUpdate` parameter to `TRUE`.**

```
# ldapclient -v mod -a enableShadowUpdate=TRUE \
> -a adminDN=cn=admin,ou=profile,dc=example-domain,dc=com
System successfully configured
```

For information about the `enableShadowUpdate` parameter, see "enableShadowUpdate Switch" in *System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)* and the `ldapclient`(1M) man page.

▼ Configure the Logs for the Sun Java System Directory Server

This procedure configures three types of logs: access logs, audit logs, and error logs. The following default settings are not changed:

- All logs are enabled and buffered.
- Logs are placed in the appropriate `/export/home/ds/instances/`*your-instance*`/logs/`*LOG_TYPE* directory.
- Events are logged at log level 256.
- Logs are protected with `600` file permissions.
- Access logs are rotated daily.
- Error logs are rotated weekly.

The settings in this procedure meet the following requirements:

- Audit logs are rotated daily.
- Log files that are older than 3 months expire.
- All log files use a maximum of 20,000 MBytes of disk space.
- A maximum of 100 log files is kept, and each file is at most 500 MBytes.

- The oldest logs are deleted if less than 500 MBytes free disk space is available.
- Additional information is collected in the error logs.

1 Configure the access logs.

The *LOG_TYPE* for access is `ACCESS`. The syntax for configuring logs is the following:

`dsconf set-log-prop` *LOG_TYPE property*`:`*value*

```
# dsconf set-log-prop ACCESS max-age:3M
# dsconf set-log-prop ACCESS max-disk-space-size:20000M
# dsconf set-log-prop ACCESS max-file-count:100
# dsconf set-log-prop ACCESS max-size:500M
# dsconf set-log-prop ACCESS min-free-disk-space:500M
```

2 Configure the audit logs.

```
# dsconf set-log-prop AUDIT max-age:3M
# dsconf set-log-prop AUDIT max-disk-space-size:20000M
# dsconf set-log-prop AUDIT max-file-count:100
# dsconf set-log-prop AUDIT max-size:500M
# dsconf set-log-prop AUDIT min-free-disk-space:500M
# dsconf set-log-prop AUDIT rotation-interval:1d
```

By default, the rotation interval for audit logs is one week.

3 Configure the error logs.

In this configuration, you specify additional data to be collected in the error log.

```
# dsconf set-log-prop ERROR max-age:3M
# dsconf set-log-prop ERROR max-disk-space-size:20000M
# dsconf set-log-prop ERROR max-file-count:30
# dsconf set-log-prop ERROR max-size:500M
# dsconf set-log-prop ERROR min-free-disk-space:500M
# dsconf set-log-prop ERROR verbose-enabled:on
```

4 (Optional) Further configure the logs.

You can also configure the following settings for each log:

```
# dsconf set-log-prop LOG_TYPE rotation-min-file-size:undefined
# dsconf set-log-prop LOG_TYPE rotation-time:undefined
```

For information about the `dsconf` command, see the `dsconf`(1M) man page.

▼ Configure a Multilevel Port for the Sun Java System Directory Server

To work in Trusted Extensions, the server port of the Directory Server must be configured as a multilevel port (MLP) in the global zone.

1 Start the Solaris Management Console.

```
# /usr/sbin/smc &
```

2. **Select the This Computer (*this-host*: `Scope=Files, Policy=TSOL`) toolbox.**
3. **Click System Configuration, then click Computers and Networks.**
   You are prompted for your password.
4. **Type the appropriate password.**
5. **Double-click Trusted Network Zones.**
6. **Double-click the global zone.**
7. **Add a multilevel port for the TCP protocol:**
   a. **Click Add for the Multilevel Ports for Zone's IP Addresses.**
   b. **Type 389 for the port number, and click OK.**
8. **Add a multilevel port for the UDP protocol:**
   a. **Click Add for the Multilevel Ports for Zone's IP Addresses.**
   b. **Type 389 for the port number.**
   c. **Choose the udp protocol, and click OK.**
9. **Click OK to save the settings.**
10. **Update the kernel.**

```
# tnctl -fz /etc/security/tsol/tnzonecfg
```

▼ Populate the Sun Java System Directory Server

Several LDAP databases have been created or modified to hold Trusted Extensions data about label configuration, users, and remote systems. In this procedure, you populate the Directory Server databases with Trusted Extensions information.

Before You Begin You must populate the database from an LDAP client where shadow updating is enabled. For the prerequisites, see "Create an LDAP Client for the Directory Server" on page 112.

If site security requires separation of duty, complete the following before populating the Directory server:

- "Create Rights Profiles That Enforce Separation of Duty" on page 85
- "Create the Security Administrator Role in Trusted Extensions" on page 88
- "Create a Restricted System Administrator Role" on page 90

1 Create a staging area for files that you plan to use to populate the naming service databases.

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

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

```
# cd /etc
# cp aliases group networks netmasks protocols /setup/files
# cp rpc services auto_master /setup/files

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

If you are running the Solaris 10 11/06 release without patches, copy the `ipnodes` file.

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

3 Remove the `+auto_master` entry from the `/setup/files/auto_master` file.

4 Remove the `?:::::?` entry from the `/setup/files/auth_attr` file.

5 Remove the `::::` entry from the `/setup/files/prof_attr` file.

6 Create the zone automaps in the staging area.

In the following list of automaps, the first of each pair of lines shows the name of the file. The second line of each pair shows the file contents. The zone names identify labels from the default `label_encodings` file that is included with the Trusted Extensions software.

- Substitute your zone names for the zone names in these lines.
- *myNFSserver* identifies the NFS server for the home directories.

```
/setup/files/auto_home_public
 * myNFSserver_FQDN:/zone/public/root/export/home/&

/setup/files/auto_home_internal
 * myNFSserver_FQDN:/zone/internal/root/export/home/&

/setup/files/auto_home_needtoknow
 * myNFSserver_FQDN:/zone/needtoknow/root/export/home/&

/setup/files/auto_home_restricted
 * myNFSserver_FQDN:/zone/restricted/root/export/home/&
```

7 **Add every system on the network to the `/setup/files/tnrhdb` file.**

No wildcard mechanism can be used here. The IP address of every system to be contacted, including the IP addresses of labeled zones, *must* be in this file.

a. **Open the trusted editor and edit `/setup/files/tnrhdb`.**

b. **Add every IP address on a labeled system in the Trusted Extensions domain.**

Labeled systems are of type `cipso`. Also, the name of the security template for labeled systems is `cipso`. Therefore, in the default configuration, a `cipso` entry is similar to the following:

```
192.168.25.2:cipso
```

Note – This list includes the IP addresses of global zones and labeled zones.

c. **Add every unlabeled system with which the domain can communicate.**

Unlabeled systems are of type `unlabeled`. The name of the security template for unlabeled systems is `admin_low`. Therefore, in the default configuration, an entry for an unlabeled system is similar to the following:

```
192.168.35.2:admin_low
```

d. **Save the file, and exit the editor.**

e. **Check the syntax of the file.**

```
# tnchkdb -h /setup/files/tnrhdb
```

f. **Fix any errors before continuing.**

8 **Copy the `/setup/files/tnrhdb` file to the `/etc/security/tsol/tnrhdb` file.**

9 **Use the `ldapaddent` command to populate the Directory Server with every file in the staging area.**

For example, the following command populates the server from the `hosts` file in the staging area.

```
# /usr/sbin/ldapaddent -D "cn=directory manager" \
-w dirmgr123 -a simple -f /setup/files/hosts hosts
```

10 **If you ran the `ldapclient` command on the Trusted Extensions Directory Server, disable the client on that system.**

In the global zone, run the `ldapclient uninit` command. Use verbose output to verify that the system is no longer an LDAP client.

```
# ldapclient -v uninit
```

For more information, see the `ldapclient(1M)` man page.

Creating a Trusted Extensions Proxy for an Existing Sun Java System Directory Server

First, you need to add the Trusted Extensions databases to the existing Directory Server on an Oracle Solaris system. Second, to enable Trusted Extensions systems to access the Directory Server, you then need to configure a Trusted Extensions system to be the LDAP proxy server.

▼ Create an LDAP Proxy Server

If an LDAP server already exists at your site, create a proxy server on a Trusted Extensions system.

Before You Begin You have populated the LDAP server from a client that was modified to set the `enableShadowUpdate` parameter to `TRUE`. For the requirement, see "Create an LDAP Client for the Directory Server" on page 112.

In addition, you have added the databases that contain Trusted Extensions information to the LDAP server from a client where the `enableShadowUpdate` parameter was set to `TRUE`. For details, see "Populate the Sun Java System Directory Server" on page 116.

1 On a system that is configured with Trusted Extensions, create a proxy server.

Note – You must run two `ldapclient` commands. After you run the `ldapclient init` command, you then run the `ldapclient modify` command to set the `enableShadowUpdate` parameter to `TRUE`.

For details, see Chapter 12, "Setting Up LDAP Clients (Tasks)," in *System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)*.

2 Verify that the Trusted Extensions databases can be viewed by the proxy server.

```
# ldaplist -l database
```

Troubleshooting For strategies to solve LDAP configuration problems, see Chapter 13, "LDAP Troubleshooting (Reference)," in *System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)*.

Configuring the Solaris Management Console for LDAP (Task Map)

The Solaris Management Console is the GUI for administering the network of systems that are running Trusted Extensions.

Task	Description	For Instructions
Initialize the Solaris Management Console.	Initialize the Solaris Management Console. This procedure is performed once per system in the global zone.	"Initialize the Solaris Management Console Server in Trusted Extensions" on page 56
Register credentials.	Authenticate the Solaris Management Console with the LDAP server.	"Register LDAP Credentials With the Solaris Management Console" on page 120
Enable remote administration on a system.	By default, a Solaris Management Console client cannot communicate with a Console server on another system. You must explicitly enable remote administration.	"Enable the Solaris Management Console to Accept Network Communications" on page 121
Create the LDAP toolbox.	Create the LDAP toolbox in the Solaris Management Console for Trusted Extensions.	"Edit the LDAP Toolbox in the Solaris Management Console" on page 122
Verify communications.	Verify that Trusted Extensions hosts can become LDAP clients.	"Verify That the Solaris Management Console Contains Trusted Extensions Information" on page 124

▼ Register LDAP Credentials With the Solaris Management Console

Before You Begin You must be the `root` user on an LDAP server that is running Trusted Extensions. The server can be a proxy server.

Your Sun Java System Directory Server must be configured. You have completed one of the following configurations:

- "Configuring an LDAP Server on a Trusted Extensions Host (Task Map)" on page 107
- "Configuring an LDAP Proxy Server on a Trusted Extensions Host (Task Map)" on page 108

1 Register the LDAP administrative credentials.

LDAP-Server `#` **`/usr/sadm/bin/dtsetup storeCred`**
`Administrator DN:` *Type the value for cn on your system*
`Password:` *Type the Directory Manager password*
`Password (confirm):` *Retype the password*

2 List the scopes on the Directory Server.

```
LDAP-Server # /usr/sadm/bin/dtsetup scopes
Getting list of manageable scopes...
Scope 1 file:     Displays name of file scope
Scope 2 ldap:     Displays name of ldap scope
```

Your LDAP server setup determines the scopes that are listed. The LDAP scope is not listed until the LDAP toolbox is edited. The toolbox cannot be edited until after the server is registered.

Example 5–1 Registering LDAP Credentials

In this example, the name of the LDAP server is `LDAP1` and the value for `cn` is the default, `Directory Manager`.

```
# /usr/sadm/bin/dtsetup storeCred
Administrator DN:cn=Directory Manager
Password:abcde1;!
Password (confirm):abcde1;!
# /usr/sadm/bin/dtsetup scopes
Getting list of manageable scopes...
Scope 1 file:/LDAP1/LDAP1
Scope 2 ldap:/LDAP1/cd=LDAP1,dc=example-domain,dc=com
```

▼ Enable the Solaris Management Console to Accept Network Communications

By default, Oracle Solaris systems are not configured to listen on ports that present security risks. Therefore, you must explicitly configure any system that you plan to administer remotely to accept network communications. For example, to administer network databases on the LDAP server from a client, the Solaris Management Console server on the LDAP server must accept network communications.

For an illustration of the Solaris Management Console configuration requirements for a network with an LDAP server, see "Client-Server Communication With the Solaris Management Console" in *Trusted Extensions Administrator's Procedures*.

Before You Begin You must be superuser in the global zone on the Solaris Management Console server system. In this procedure, that system is called the remote system. Also, you must have command line access to the client system as superuser.

1. **On the remote system, enable the system to accept remote connections.**

   The smc daemon is controlled by the wbem service. If the options/tcp_listen property to the wbem service is set to true, the Solaris Management Console server accepts remote connections.

   ```
   # /usr/sbin/svcprop -p options wbem
   options/tcp_listen boolean false
   # svccfg -s wbem setprop options/tcp_listen=true
   ```

2. **Refresh and restart the wbem service.**

   ```
   # svcadm refresh wbem
   # svcadm restart wbem
   ```

3. **Verify that the wbem service is set to accept remote connections.**

   ```
   # svcprop -p options wbem
   options/tcp_listen boolean true
   ```

4. **On the remote system and on any client that needs to access the Solaris Management Console, ensure that remote connections are enabled in the smcserver.config file.**

   a. **Open the smcserver.config file in the trusted editor.**

      ```
      # /usr/dt/bin/trusted_edit /etc/smc/smcserver.config
      ```

   b. **Set the remote.connections parameter to true.**

      ```
      ## remote.connections=false
      remote.connections=true
      ```

   c. **Save the file and exit the trusted editor.**

Troubleshooting If you restart or enable the wbem service, you must ensure that the remote.connections parameter in the smcserver.config file remains set to true.

▼ Edit the LDAP Toolbox in the Solaris Management Console

Before You Begin You must be superuser on the LDAP server. The LDAP credentials must be registered with the Solaris Management Console, and you must know the output of the /usr/sadm/bin/dtsetup scopes command. For details, see "Register LDAP Credentials With the Solaris Management Console" on page 120.

1. **Find the LDAP toolbox.**

   ```
   # cd /var/sadm/smc/toolboxes/tsol_ldap
   # ls *tbx
   tsol_ldap.tbx
   ```

2. **Provide the LDAP server name.**

   a. **Open the trusted editor.**

   b. **Copy and paste the full pathname of the `tsol_ldap.tbx` toolbox as the argument to the editor.**

      For example, the following path is the default location of the LDAP toolbox:

      ```
      /var/sadm/smc/toolboxes/tsol_ldap/tsol_ldap.tbx
      ```

   c. **Replace the scope information.**

      Replace the `server` tags between the `<Scope>` and `</Scope>` tags with the output of the `ldap:/.....` line from the `/usr/sadm/bin/dtsetup scopes` command.

      ```
      <Scope>ldap:/<ldap-server-name>/<dc=domain,dc=suffix></Scope>
      ```

   d. **Replace every instance of `<?server?>` or `<?server ?>` with the LDAP server.**

      ```
      <Name>This Computer (ldap-server-name: Scope=ldap, Policy=TSOL)</Name>
      services and configuration of ldap-server-name.</Description>
      and configuring ldap-server-name.</Description>
      ...
      ```

   e. **Save the file, and exit the editor.**

3. **Refresh and restart the `wbem` service.**

   ```
   # svcadm refresh wbem
   # svcadm restart wbem
   ```

Example 5–2 Configuring the LDAP Toolbox

In this example, the name of the LDAP server is `LDAP1`. To configure the toolbox, the administrator replaces the instances of `<?server ?>` with `LDAP1`.

```
# cd /var/sadm/smc/toolboxes/tsol_ldap
# /usr/dt/bin/trusted_edit /tsol_ldap.tbx
<Scope>ldap:/LDAP1/cd=LDAP1,dc=example-domain,dc=com</Scope

...
<Name>This Computer (LDAP1: Scope=ldap, Policy=TSOL)</Name>
services and configuration of LDAP1.</Description>
and configuring LDAP1.</Description>
...
```

▼ Verify That the Solaris Management Console Contains Trusted Extensions Information

For an illustration of the Solaris Management Console configuration requirements for a network with an LDAP server and for a network without an LDAP server, see "Client-Server Communication With the Solaris Management Console" in *Trusted Extensions Administrator's Procedures*.

Before You Begin You must be logged in to an LDAP client in an administrative role, or as superuser. To make a system an LDAP client, see "Make the Global Zone an LDAP Client in Trusted Extensions" on page 59.

To administer the local system, you must have completed "Initialize the Solaris Management Console Server in Trusted Extensions" on page 56.

To connect to a Console server on a remote system from the local system, you must have completed "Initialize the Solaris Management Console Server in Trusted Extensions" on page 56 on both systems. Also, on the remote system, you must have completed "Enable the Solaris Management Console to Accept Network Communications" on page 121.

To administer the databases in the LDAP naming service from the LDAP client, on the LDAP server you must have completed "Edit the LDAP Toolbox in the Solaris Management Console" on page 122, in addition to the preceding procedures.

1. **Start the Solaris Management Console.**

   ```
   # /usr/sbin/smc &
   ```

2. **Open a Trusted Extensions toolbox.**

   A Trusted Extensions toolbox has the value `Policy=TSOL`.

   - **On a trusted network that uses LDAP as a naming service, perform the following tests:**

     a. **To check that local administrative databases can be accessed, open the following toolbox:**

        `This Computer (`*this-host*`: Scope=Files, Policy=TSOL)`

     b. **To check that the LDAP server's local administrative databases can be accessed, specify the following toolbox:**

        `This Computer (`*ldap-server*`: Scope=Files, Policy=TSOL)`

     c. **To check that the naming service databases on the LDAP server can be accessed, specify the following toolbox:**

        `This Computer (`*ldap-server*`: Scope=LDAP, Policy=TSOL)`

- **On a trusted network that does not use LDAP as a naming service, perform the following tests:**

  a. **To check that local administrative databases can be accessed, open the following toolbox:**

     `This Computer (`*this-host*`: Scope=Files, Policy=TSOL)`

  b. **To check that a remote system's local administrative databases can be accessed, specify the following toolbox:**

     `This Computer (`*remote-system*`: Scope=Files, Policy=TSOL)`

3 **Under System Configuration, navigate to Computers and Networks, then Security Templates.**

4 **Check that the correct templates and labels have been applied to the remote systems.**

Note – When you try to access network database information from a system that is not the LDAP server, the operation fails. The Console allows you to log in to the remote host and open the toolbox. However, when you try to access or change information, the following error message indicates that you have selected `Scope=LDAP` on a system that is not the LDAP server:

```
Management server cannot perform the operation requested.
...
Error extracting the value-from-tool.
The keys received from the client were machine, domain, Scope.
Problem with Scope.
```

Troubleshooting To troubleshoot LDAP configuration, see Chapter 13, "LDAP Troubleshooting (Reference)," in *System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)*.

◆ ◆ ◆ CHAPTER 6

Configuring a Headless System With Trusted Extensions (Tasks)

Configuring and administering Trusted Extensions software on headless systems such as the Netra series requires modifying security settings on the headless system to enable remote access. Administering a remote Trusted Extensions system requires similar setup. To run an administrative GUI, you might need to run the process on the remote system and display the GUI on the desktop system.

For an explanation of the requirements, see Chapter 8, "Remote Administration in Trusted Extensions (Tasks)," in *Trusted Extensions Administrator's Procedures*

Note – The configuration methods that headless and remote systems require do not satisfy the criteria for an evaluated configuration. For more information, see "Understanding Your Site's Security Policy" on page 20.

Headless System Configuration in Trusted Extensions (Task Map)

On headless systems, a console is connected by means of a serial line to a terminal emulator window. The line is typically secured by the `tip` command. Depending on what type of second system is available, you can use one of the following methods to configure a headless system. The methods are listed from more secure to less secure in the following table. These instructions also apply to remote systems.

Task	Description	For Instructions
Enable remote login by the `root` user.	If you are not using LDAP, you must initially log in to the headless system as `root`. If you are using LDAP, you can skip this procedure.	"Enable Remote Login by `root` User in Trusted Extensions" on page 128

Task	Description	For Instructions
Enable remote login.	Enable remote login for a user who can assume the `root` role or another administrative role.	"Enable Remote Login by a Role in Trusted Extensions" on page 129
	Enable the administration of Trusted Extensions systems from an unlabeled system.	"Enable Remote Login From an Unlabeled System" on page 131
	Enable a user to access the global zone on a headless system.	"How to Enable Specific Users to Log In Remotely to the Global Zone in Trusted Extensions" in *Trusted Extensions Administrator's Procedures*
(Optional) Enable the display of administrative GUIs.	Enable administrative GUIs that run on the headless system to display on the desktop system.	"Enable the Remote Display of Administrative GUIs" on page 132
(Optional) Enable virtual network computing (VNC)	From any client, uses the Xvnc server on the remote Trusted Extensions to display a multilevel session back to the client.	"How to Use Xvnc to Remotely Access a Trusted Extensions System" in *Trusted Extensions Administrator's Procedures*
Choose a configuration and administration method to set up the headless system.	Assume a role or become superuser to administer the remote system.	"Use the `rlogin` or `ssh` Command to Log In and Administer a Headless System in Trusted Extensions" on page 132
	Use the Solaris Management Console on the headless system.	"Use a Remote Solaris Management Console to Administer in the Files Scope" on page 131
	If you have no windowing system, you can use serial login as superuser. This procedure is insecure.	No configuration is required.

Note – Consult your security policy to determine which methods of remote administration are permissible at your site.

▼ Enable Remote Login by root User in Trusted Extensions

As in the Oracle Solaris OS, `root` can log in remotely from a labeled system when the `CONSOLE` entry is disabled.

If you plan to administer a remote system by editing local files, use this procedure.

1 **In the trusted editor, comment out the `CONSOLE=` line in the `/etc/default/login` file.**

```
# /usr/dt/bin/trusted_edit /etc/default/login
```

The edited line appears similar to the following:

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

2 **Permit `root` user login over an `ssh` connection.**

Modify the `/etc/ssh/sshd_config` file. By default, `ssh` is enabled on an Oracle Solaris system.

```
# /usr/dt/bin/trusted_edit /etc/ssh/sshd_config
```

The edited line appears similar to the following:

```
PermitRootLogin yes
```

Next Steps To log in as the `root` user from an unlabeled system, you must also complete "Enable Remote Login From an Unlabeled System" on page 131.

To enable remote login by a role, continue with "Enable Remote Login by a Role in Trusted Extensions" on page 129.

▼ Enable Remote Login by a Role in Trusted Extensions

Follow this procedure *only if* you must administer a headless system by using the `rlogin` or `ssh` command.

Configuration errors can be debugged remotely.

Before You Begin If you are using local files to administer the remote system, you have completed "Enable Remote Login by `root` User in Trusted Extensions" on page 128. Then, as the `root` user, perform this task on both systems.

1 **On both systems, identify the other system as a labeled system.**

The desktop system and the headless system must identify each other as using the identical security template. For the procedure, see "How to Assign a Security Template to a Host or a Group of Hosts" in *Trusted Extensions Administrator's Procedures*.

To assign a temporary label, see Example 6–1.

2 **On both systems, create identical users and roles.**

The names and IDs must be identical, and the role must be assigned to the user on both systems. To create users and roles, see "Creating Roles and Users in Trusted Extensions" on page 84.

3 **To contact a remote Solaris Management Console, do the following on both systems:**

a. **Add the other system's host name and IP address to the `/etc/hosts` file.**

```
# /usr/dt/bin/trusted_edit /etc/hosts

127.0.0.1    localhost
192.168.66.66    local-system-name    loghost
192.168.66.12    remote-system-name
```

b. To allow remote role assumption, modify the `pam.conf` file to relax PAM policy.

i. Copy the `/etc/pam.conf` file to `/etc/pam.conf.orig`.

```
# cp /etc/pam.conf /etc/pam.conf.orig
```

ii. In the trusted editor, open the `pam.conf` file.

```
# /usr/dt/bin/trusted_edit /etc/pam.conf
```

iii. Copy the default entries under Account management.

iv. In each copied entry, change `other` to `smcconsole`.

v. To the copied `pam_roles.so.1` entry, add `allow_remote`.

Use the Tab key between fields. This section now appears similar to the following:

```
# Solaris Management Console definition for Account management
#
smcconsole   account requisite   pam_roles.so.1   allow_remote
smcconsole   account required    pam_unix_account.so.1
smcconsole   account required    pam_tsol_account.so.1

# Default definition for Account management
# Used when service name is not explicitly mentioned for account management
#
other   account requisite    pam_roles.so.1
other   account required     pam_unix_account.so.1
other   account required     pam_tsol_account.so.1
```

vi. Save the file and exit the editor.

vii. (Optional) Copy the file to `/etc/pam.conf.site`.

```
# cp /etc/pam.conf /etc/pam.conf.site
```

If you upgrade the system to a later release, you must then evaluate if you should copy the changes from `/etc/pam.conf.site` into the `pam.conf` file.

Example 6–1 Creating a Temporary Definition of a Trusted Extensions Host Type

In this example, the administrator wants to start configuring a remote Trusted Extensions system before the host type definitions are set up. To do so, the administrator uses the `tnctl` command on the remote system to temporarily define the host type of the desktop system:

```
remote-TX# tnctl -h desktop-TX:cipso
```

Later, the administrator wants to reach the remote Trusted Extensions system from a desktop system that is not configured with Trusted Extensions. In this case, the administrator uses the `tnctl` command on the remote system to temporarily define the host type of the desktop system as an unlabeled system that runs at the `ADMIN_LOW` label:

```
remote-TX# tnctl -h desktop-TX:admin_low
```

▼ Enable Remote Login From an Unlabeled System

Before You Begin This procedure is not secure.

You have relaxed PAM policy to allow remote role assumption, as described in "Enable Remote Login by a Role in Trusted Extensions" on page 129.

1 On the trusted system, apply the appropriate security template to the unlabeled system.

Caution – With the default settings, another unlabeled system could log in and administer the remote system. Therefore, you must change the `0.0.0.0` network default from `ADMIN_LOW` to a different label. For the procedure, see "How to Limit the Hosts That Can Be Contacted on the Trusted Network" in *Trusted Extensions Administrator's Procedures*.

2 In the trusted editor, open the `/etc/pam.conf` file.

```
# /usr/dt/bin/trusted_edit /etc/pam.conf
```

3 Find the `smcconsole` entries.

4 Add `allow_unlabeled` to the `tsol_account` module.

Use the Tab key between fields.

```
smcconsole   account required  pam_tsol_account.so.1 allow_unlabeled
```

After your edits, this section appears similar to the following:

```
# Solaris Management Console definition for Account management
#
smcconsole  account  requisite      pam_roles.so.1    allow_remote
smcconsole  account  required       pam_unix_account.so.1
smcconsole  account  required       pam_tsol_account.so.1 allow_unlabeled
```

▼ Use a Remote Solaris Management Console to Administer in the Files Scope

If you are not using LDAP, and you want to use the Solaris Management Console on a remote system, you enable remote connection to the Console. This procedure is not sufficient to enable access for the LDAP scope.

To enable access for the LDAP scope, you must complete all the procedures in "Configuring the Solaris Management Console for LDAP (Task Map)" on page 120.

Before You Begin Both systems are labeled systems.

You have completed the following procedures:

- "Initialize the Solaris Management Console Server in Trusted Extensions" on page 56
- "Enable Remote Login by a Role in Trusted Extensions" on page 129

1. **Complete "Enable the Solaris Management Console to Accept Network Communications" on page 121.**

2. **On the desktop system, become a user that is defined identically on both systems.**

3. **On the desktop system, assume the role that is defined identically on both systems.**

4. **On the desktop system, start the Solaris Management Console.**

   ```
   # /usr/sbin/smc &
   ```

5. **In the Server dialog box, type the name of the headless system.**

   Then, choose the `Scope=Files` toolbox.

   ```
   This Computer (remote-system: Scope=Files, Policy=TSOL)
   ```

▼ Enable the Remote Display of Administrative GUIs

The procedure for remote display on a desktop is identical to the procedure on an Oracle Solaris system that is not configured with Trusted Extensions. This procedure is placed here for convenience.

1. **On the desktop system, enable processes from the headless system to display.**

   a. **Enable the headless system to access the X server on the desktop system.**

      desktop `$ xhost +` *headless-host*

   b. **Determine the value of the desktop's `DISPLAY` variable.**

      desktop `$ echo $DISPLAY`
      `:`*n*`.`*n*

2. **On the headless system, set the `DISPLAY` variable to the desktop system.**

   headless `$ DISPLAY=`*desktop*`:`*n*`.`*n*
   headless `$ export DISPLAY=`*n*`:`*n*

▼ Use the rlogin or ssh Command to Log In and Administer a Headless System in Trusted Extensions

This procedure enables you to use the command line and the `txzonemgr` GUI to administer a headless system as superuser or as a role.

Note – Remote login by using the `rlogin` command is less secure than remote login by using the `ssh` command.

To use the Solaris Management Console to administer a remote system does not require you to use a remote login command. For the procedure, see "How to Remotely Administer Systems by Using the Solaris Management Console From a Trusted Extensions System" in *Trusted Extensions Administrator's Procedures*.

Before You Begin You have completed "Enable Remote Login by a Role in Trusted Extensions" on page 129.

You are a user who is enabled to log in to the headless system with that same user name and user ID, and you can assume the same role on the headless system that you can assume on the desktop system.

1 On the desktop system, enable processes from the headless system to display.

```
desktop $ xhost + headless-host
desktop $ echo $DISPLAY
:n.n
```

2 Ensure that you are the user who is identically defined on both systems.

3 From a terminal window, remotely log in to the headless system.

- **Use the `ssh` command to log in:**

  ```
  desktop $ ssh -l identical-username  headless
  Password:       Type the user's password
  headless $
  ```

- **Or, use the `rlogin` command to log in:**

  ```
  desktop # rlogin headless
  Password:       Type the user's password
  headless $
  ```

4 Assume the role that is defined identically on both systems.

Use the same terminal window. For example, assume the `root` role.

```
headless $ su - root
Password:       Type the root password
```

You are now in the global zone. You can now use this terminal to administer the headless system from the command line.

5 Enable processes on the headless system to display on the desktop system.

Note – You can also display remote GUIs by logging in with the `ssh -X` command. For more information, see the `ssh(1)` man page. For an example, see Example 6–2.

```
headless $  DISPLAY desktop:n.n
headless $ export DISPLAY=n:n
```

You can now administer the headless system by using Trusted Extensions GUIs. For example, start the `txzonemgr` GUI:

```
headless $ /usr/sbin/txzonemgr
```

The Labeled Zone Manager runs on the remote system and displays on the desktop system.

6 (Optional) Access Trusted CDE actions.

To open and safely close the Application Manager, see "How to Remotely Administer Trusted Extensions With dtappsession" in *Trusted Extensions Administrator's Procedures*.

Example 6–2 Configuring Labeled Zones on a Headless System

In this example, the administrator uses the `txzonemgr` GUI to configure labeled zones on a labeled headless system from a labeled desktop system. As in the Oracle Solaris OS, the administrator enables X server access to the desktop system by using the `-X` option to the `ssh` command. The user `install1` is defined identically on both systems, and can assume the role `remoterole`.

```
TXdesk1 $ xhost + TXnohead4
TXdesk1 $ whoami
install1

TXdesk1 $ ssh -X -l install1 TXnohead4
Password: Ins1PwD1
TXnohead4 $
```

To reach the global zone, the administrator assumes the role `remoterole`. This role is defined identically on both systems.

```
TXnohead4 # su - remoterole
Password: abcd1EFG
```

Then, the administrator starts the `txzonemgr` GUI.

```
TXnohead4 $ /usr/sbin/txzonemgr &
```

The Labeled Zone Manager runs on the headless system and displays on the desktop system.

◆ ◆ ◆ APPENDIX A

Site Security Policy

This appendix discusses site security policy issues, and suggests reference books and web sites for further information:

- "Site Security Policy and Trusted Extensions" on page 136
- "Computer Security Recommendations" on page 136
- "Physical Security Recommendations" on page 137
- "Personnel Security Recommendations" on page 138
- "Common Security Violations" on page 138
- "Additional Security References" on page 139

Creating and Managing a Security Policy

Each Trusted Extensions 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 needs to have representation from top-level management, personnel management, computer system management and administrators, and facilities management. The team must review Trusted Extensions 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 must be educated about the security policy. Security policies must not be made available to regular users because this policy information has direct bearing on the security of the computer systems.
- Educate users about Trusted Extensions software and the security policy. All users must be familiar with the *Trusted Extensions User's Guide*. Because the users are usually the first to know when a system is not functioning normally, the user must 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 any of the following:
  - 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 the system that is configured with Trusted Extensions is not secure. Procedures must be established to record any problems and the measures that were taken to resolve the incidents.
- Periodically review the security policy. The security team must 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 Trusted Extensions

The security administrator must design the Trusted Extensions network based on the site's security policy. The security policy dictates configuration decisions, such as the following:

- How much auditing is done for all users and for which classes of events
- How much auditing is done for users in roles and for which classes of events
- How audit data is managed, archived, and reviewed
- Which labels are used in the system and whether the `ADMIN_LOW` and `ADMIN_HIGH` labels will viewable by regular users
- Which user clearances are assigned to individuals
- Which devices (if any) can be allocated by which regular users
- Which label ranges are defined for systems, printers, and other devices
- Whether Trusted Extensions is used in an evaluated configuration or not

Computer Security Recommendations

Consider the following list of guidelines when you develop a security policy for your site.

- Assign the maximum label of a system that is configured with Trusted Extensions to not be greater than the maximum security level of work being done at the site.
- Manually record system reboots, power failures, and shutdowns in a site log.
- Document file system damage, and analyze all affected files for potential security policy violations.
- Restrict operating manuals and administrator documentation to individuals with a valid need for access to that information.
- Report and document unusual or unexpected behavior of any Trusted Extensions software, and determine the cause.

- If possible, assign at least two individuals to administer systems that are configured with Trusted Extensions. Assign one person the security administrator authorization for security-related decisions. Assign the other person the system administrator authorization for system management tasks.
- Establish a regular backup routine.
- Assign authorizations only to users who need them and who can be trusted to use them properly.
- Assign privileges to programs only they need the privileges to do their 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 Extensions programs as a guide to setting privileges on new programs.
- Review and analyze audit information regularly. Investigate any irregular events to determine the cause of the event.
- Minimize the number of administration IDs.
- Minimize the number of setuid and setgid programs. Use authorizations, privileges, and roles to execute the program and to prevent misuse.
- Ensure that an administrator regularly verifies that regular users have a valid login shell.
- Ensure that an administrator must regularly verifies that regular users have valid user ID values and not system administration ID values.

Physical Security Recommendations

Consider the following list of guidelines when you develop a security policy for your site.

- Restrict access to the systems that are configured with Trusted Extensions. The most secure locations are generally interior rooms that are not on the ground floor.
- Monitor and document access to systems that are configured with Trusted Extensions.
- Secure computer equipment to large objects such as tables and desks to prevent theft. When equipment is secured to a wooden object, increase the strength of the object by adding metal plates.
- Consider removable storage media for sensitive information. Lock up all removable media when the media are not in use.
- Store system backups and archives in a secure location that is separate from the location of the systems.
- Restrict physical access to the backup and archival media in the same manner as you restrict access to the systems.
- Install a high-temperature alarm in the computer facility to indicate when the temperature is outside 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, and 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 might be appropriate for facility walls, floors, and ceilings.
- Allow only certified technicians to open and close TEMPEST equipment to ensure its ability to shield electromagnetic radiation.
- Check for physical gaps that allow entrance to the facility or to the rooms that contain 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

Consider the following list of guidelines when you develop a security policy for your site.

- Inspect packages, documents, and storage media when they arrive and before they leave 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 completely secure, a computer facility is only as secure as the people who use it. Most actions that violate security are easily resolved by careful users or additional equipment. However, the following list gives examples of problems that can occur:

- Users give passwords to other individuals who should not have access to the system.
- Users write down passwords, and lose or leave the passwords in insecure locations.
- Users set their passwords to easily guessed words or easily guessed names.
- Users learn passwords by watching other users type a password.
- Unauthorized users remove, replace, or physically tamper with hardware.

- Users leave their systems 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 users 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

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.

The web also provides resources. In particular, the CERT (`http://www.cert.org`) web site alerts companies and users to security holes in the software. The SANS Institute (`http://www.sans.org/`) offers training, an extensive glossary of terms, and an updated list of top threats from the Internet.

U.S. Government Publications

The U.S. government offers many of its publications on the web. The Computer Security Resource Center (CSRC) of the National Institute of Standards and Technology (NIST) publishes articles on computer security. The following are a sample of the publications that can be downloaded from the NIST site (`http://csrc.nist.gov/index.html`).

- *An Introduction to Computer Security: The NIST Handbook*. SP 800-12, October 1995.
- *Standard Security Label for Information Transfer*. FIPS-188, September 1994.
- Swanson, Marianne and Barbara Guttman. *Generally Accepted Principles and Practices for Securing Information Technology Systems*. SP 800-14, September 1996.

- Tracy, Miles, Wayne Jensen, and Scott Bisker. *Guidelines on Electronic Mail Security*. SP 800-45, September 2002. Section E.7 concerns securely configuring LDAP for mail.
- Wilson, Mark and Joan Hash. *Building an Information Technology Security Awareness and Training Program*. SP 800-61, January 2004. Includes a useful glossary.
- Grace, Tim, Karen Kent, and Brian Kim. *Computer Security Incident Handling Guidelines*. SP 800-50, September 2002. Section E.7 concerns securely configuring LDAP for mail.
- Scarfone, Karen,Wayne Jansen, and Miles Tracy. *Guide to General Server Security* SP 800-123, July 2008.
- Souppaya, Murugiah, John Wack, and Karen Kent. *Security Configuration Checklists Program for IT Products*. SP 800-70, May 2005.

UNIX Security Publications

Sun Microsystems Security Engineers. *Solaris 10 Security Essentials*. Prentice Hall, 2009.

Chirillo, John and Edgar Danielyan. *Sun Certified Security Administration for Solaris 9 & 10 Study Guide*. McGraw-Hill/Osborne, 2005.

Garfinkel, Simson, Gene Spafford, and Alan Schwartz. *Practical UNIX and Internet Security, 3rd Edition*. O'Reilly & Associates, Inc, Sebastopol, CA, 2006.

General Computer Security Publications

Brunette, Glenn M. and Christoph L. *Toward Systemically Secure IT Architectures*. Sun Microsystems, Inc, June 2005.

Kaufman, Charlie, Radia Perlman, and Mike Speciner. *Network Security: Private Communication in a Public World, 2nd Edition*. Prentice-Hall, 2002.

Pfleeger, Charles P. and Shari Lawrence Pfleeger. *Security in Computing*. Prentice Hall PTR, 2006.

Privacy for Pragmatists: A Privacy Practitioner's Guide to Sustainable Compliance. Sun Microsystems, Inc, August 2005.

Rhodes-Ousley, Mark, Roberta Bragg, and Keith Strassberg. *Network Security: The Complete Reference*. McGraw-Hill/Osborne, 2004.

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

General UNIX Publications

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

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

◆ ◆ ◆ APPENDIX B

Using CDE Actions to Install Zones in Trusted Extensions

This appendix covers how to configure labeled zones in Trusted Extensions by using Trusted CDE actions. If you are running the Solaris 10 11/06 release without patches, or if you are familiar with these actions, use the Trusted CDE actions. To use the `txzonemgr` script, see "Creating Labeled Zones" on page 62.

- "Associating Network Interfaces With Zones by Using CDE Actions (Task Map)" on page 143
- "Preparing to Create Zones by Using CDE Actions (Task Map)" on page 146
- "Creating Labeled Zones by Using CDE Actions (Task Map)" on page 148

Associating Network Interfaces With Zones by Using CDE Actions (Task Map)

Do only one of the following tasks. For the trade-offs, see "Planning for Multilevel Access" on page 25.

Task	Description	For Instructions
Share a logical interface.	Map the global zone to one IP address, and map the labeled zones to a different IP address.	"Specify Two IP Addresses for the System by Using a CDE Action" on page 143
Share a physical interface.	Map all zones to one IP address.	"Specify One IP Address for the System by Using a CDE Action" on page 145

▼ Specify Two IP Addresses for the System by Using a CDE Action

In this configuration, the host's address applies only to the global zone. Labeled zones share a second IP address with the global zone.

Before You Begin You are superuser in the global zone. The system has already been assigned two IP addresses. You are in a Trusted CDE workspace.

1 Navigate to the Trusted_Extensions folder.

a. Click mouse button 3 on the background.

b. From the Workspace menu, choose Applications → Application Manager.

c. Double-click the Trusted_Extensions folder icon.

This folder contains actions that set up interfaces, LDAP clients, and labeled zones.

2 Double-click the Share Logical Interface action and answer the prompts.

Note – The system must already have been assigned two IP addresses. For this action, provide the second address and a host name for that address. The second address is the shared address.

`Hostname:` *Type the name for your labeled zones interface*
`IP Address:` *Type the IP address for the interface*

This action configures a host with more than one IP address. The IP address for the global zone is the name of the host. The IP address for a labeled zone has a different host name. In addition, the IP address for the labeled zones is shared with the global zone. When this configuration is used, labeled zones are able to reach a network printer.

Tip – Use a standard naming convention for labeled zones. For example, add `-zones` to the host name.

---

3 (Optional) In a terminal window, verify the results of the action.

```
# ifconfig -a
```

For example, the following output shows a shared logical interface, `hme0:3` on network interface `192.168.0.12` for the labeled zones. The `hme0` interface is the unique IP address of the global zone.

```
lo0: flags=2001000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4,VIRTUAL> mtu 8232 index 1
        inet 127.0.0.1 netmask ff000000
        ether 0:0:00:00:00:0
hme0: flags=1000843<BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
        inet 192.168.0.11 netmask fffffe00 broadcast 192.168.0.255
hme0:3 flags=1000843<BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
        all-zones
        inet 192.168.0.12 netmask fffffe00 broadcast 192.168.0.255
```

Starting in the Solaris 10 10/08 release, the loopback interface, `lo0`, is also an `all-zones` interface:

```
  lo0: flags=2001000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4,VIRTUAL> mtu 8232 index 1
         all-zones
         inet 127.0.0.1 netmask ff000000
         ether 0:0:00:00:00:0
...
```

▼ Specify One IP Address for the System by Using a CDE Action

In this configuration, the host's address applies to all the zones, including the labeled zones.

Before You Begin You are superuser in the global zone. You are in a Trusted CDE workspace.

1 Navigate to the Trusted_Extensions folder.

a. Click mouse button 3 on the background.

b. From the Workspace menu, choose Applications → Application Manager.

c. Double-click the Trusted_Extensions folder icon.

This folder contains actions that set up interfaces, LDAP clients, and labeled zones.

2 Double-click the Share Physical Interface action.

This action configures a host with one IP address. The global zone does not have a unique address. This system cannot be used as a multilevel print server or NFS server.

3 (Optional) In a terminal window, verify the results of the action.

```
# ifconfig -a
```

The Share Physical Interface action configures all zones to have logical NICs. These logical NICs share a single physical NIC in the global zone.

For example, the following output shows the shared physical interface, `hme0` on network interface `192.168.0.11` for all the zones.

```
lo0: flags=2001000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4,VIRTUAL> mtu 8232 index 1
       inet 127.0.0.1 netmask ff000000
       ether 0:0:00:00:00:0
hme0: flags=1000843<BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
       all-zones
       inet 192.168.0.11 netmask fffffe00 broadcast 192.168.0.255
```

Starting in the Solaris 10 10/08 release, the loopback interface, `lo0`, is also an `all-zones` interface:

```
lo0: flags=2001000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4,VIRTUAL> mtu 8232 index 1
       all-zones
       inet 127.0.0.1 netmask ff000000
       ether 0:0:00:00:00:0
...
```

Preparing to Create Zones by Using CDE Actions (Task Map)

The following task map describes the tasks for preparing the system for zone creation. For a discussion of zone creation methods, see "Planning Your Labeled Zones in Trusted Extensions" on page 23.

Task	Description	For Instructions
1. Name each zone, and link the zone name to the zone label.	Name each labeled zone with a version of its label, then associate the name with the label in the Solaris Management Console.	"Specify Zone Names and Zone Labels by Using a CDE Action" on page 146
2. Configure the network before creating the zones.	Assign a label to the network interface on every host, and do further configuration.	"Configuring Trusted Network Databases (Task Map)" in *Trusted Extensions Administrator's Procedures*

▼ Specify Zone Names and Zone Labels by Using a CDE Action

You do not have to create a zone for every label in your `label_encodings` file, but you can. The `tnzonecfg` database enumerates the labels that can have zones created for them on this system.

1 Navigate to the Trusted_Extensions folder.

a. Click mouse button 3 on the background.

b. From the Workspace menu, choose Applications → Application Manager.

c. Double-click the Trusted_Extensions folder icon.

2 For every zone, name the zone.

a. Double-click the Configure Zone action.

b. At the prompt, provide a name.

Tip – Give the zone a similar name to the zone's label. For example, the name of a zone whose label is `CONFIDENTIAL : INTERNAL USE ONLY` would be `internal`.

3 Repeat the Configure Zone action for every zone.

For example, the default `label_encodings` file contains the following labels:

```
PUBLIC
CONFIDENTIAL: INTERNAL USE ONLY
CONFIDENTIAL: NEED TO KNOW
CONFIDENTIAL: RESTRICTED
SANDBOX: PLAYGROUND
MAX LABEL
```

Although you could run the Configure Zone action six times to create one zone per label, consider creating the following zones:

- On a system for all users, create one zone for the `PUBLIC` label and three zones for the `CONFIDENTIAL` labels.
- On a system for developers, create a zone for the `SANDBOX: PLAYGROUND` label. Because `SANDBOX: PLAYGROUND` is defined as a disjoint label for developers, only systems that developers use need a zone for this label.
- Do not create a zone for the `MAX LABEL` label, which is defined to be a clearance.

4 Open the Trusted Network Zones tool.

The tools in the Solaris Management Console are designed to prevent user error. These tools check for syntax errors and automatically run commands in the correct order to update databases.

a. Start the Solaris Management Console.

```
# /usr/sbin/smc &
```

b. Open the Trusted Extensions toolbox for the local system.

i. Choose Console → Open Toolbox.

ii. Select the toolbox that is named This Computer (*this-host*: `Scope=Files, Policy=TSOL`).

iii. Click Open.

c. Under System Configuration, navigate to Computers and Networks.

Provide a password when prompted.

d. Double-click the Trusted Network Zones tool.

5 **For each zone, associate the appropriate label with a zone name.**

a. **Choose Action → Add Zone Configuration.**

The dialog box displays the name of a zone that does not have an assigned label.

b. **Look at the zone name, then click Edit.**

c. **In the Label Builder, click the appropriate label for the zone name.**

If you click the wrong label, click the label again to deselect it, then click the correct label.

d. **Save the assignment.**

Click OK in the Label Builder, then click OK in the Trusted Network Zones Properties dialog box.

You are finished when every zone that you want is listed in the panel, or the Add Zone Configuration menu item opens a dialog box that does not have a value for Zone Name.

Troubleshooting If the Trusted Network Zones Properties dialog box does not prompt for a zone that you want to create, either the zone network configuration file does not exist, or you have already created the file.

- Check that the zone network configuration file does not already exist. Look in the panel for the name.
- If the file does not exist, run the Configure Zone action to supply the zone name. Then, repeat Step 5 to create the file.

Creating Labeled Zones by Using CDE Actions (Task Map)

One zone can be created for every entry in the Trusted Network Zone Configuration database. You made the entries in "Specify Zone Names and Zone Labels by Using a CDE Action" on page 146, by running the Configure Zone action.

The Trusted_Extensions folder in the Application Manager contains the following actions that create labeled zones:

- Configure Zone – Creates a zone configuration file for every zone name
- Install Zone – Adds the correct packages and file systems to the zone
- Zone Terminal Console – Provides a window for viewing events in a zone
- Initialize Zone for LDAP – Makes the zone an LDAP client and prepares the zone for booting
- Start Zone – Boots the zone, then starts all the service management framework (SMF) services

- Shut Down Zone – Changes the state of the zone from Started to Halted

The tasks are completed in the following order.

Task	Description	For Instructions
1. Install and boot one zone.	Create the first labeled zone. Install the packages, make the zone an LDAP client, and start all services in the zone.	"Install, Initialize, and Boot a Labeled Zone by Using CDE Actions" on page 149
2. Customize the zone.	Remove unwanted services. If you plan to copy or clone the zone, remove zone-specific information.	"Customize a Booted Zone in Trusted Extensions" on page 153
3. Create the other zones.	Use one of the following methods to create the other zones. You chose the method in "Make System and Security Decisions Before Enabling Trusted Extensions" on page 42.	
	Create each zone from scratch.	"Install, Initialize, and Boot a Labeled Zone by Using CDE Actions" on page 149 "Resolve Local Zone to Global Zone Routing in Trusted CDE" on page 152 "Customize a Booted Zone in Trusted Extensions" on page 153
	Copy the first labeled zone to another label. Repeat for all zones.	"Use the Copy Zone Method in Trusted Extensions" on page 155
	Use a ZFS snapshot to clone the other zones from the first labeled zone.	"Use the Clone Zone Method in Trusted Extensions" on page 156

▼ Install, Initialize, and Boot a Labeled Zone by Using CDE Actions

Because zone creation involves copying an entire operating system, the process is time-consuming. A faster process is to create one zone, make the zone a template for other zones, and then copy or clone that zone template.

Before You Begin You have completed "Specify Zone Names and Zone Labels by Using a CDE Action" on page 146.

If you are using LDAP as your naming service, you have completed "Make the Global Zone an LDAP Client in Trusted Extensions" on page 59.

If you are going to clone zones, you have completed "Create ZFS Pool for Cloning Zones" on page 54. In the following procedure, you install the zone that you prepared.

1 In the Trusted_Extensions folder, double-click the Install Zone action.

a. Type the name of the zone that you are installing.

This action creates a labeled virtual operating system. This step takes some time to finish. Do not do other tasks on the system while Install Zone is running.

```
# zone-name: Install Zone
Preparing to install zone <zone-name>
Creating list of files to copy from the global zone
Copying <total> files to the zone
Initializing zone product registry
Determining zone package initialization order.
Preparing to initialize <subtotal> packages on the zone.
Initializing package <number> of <subtotal>: percent complete: percent

Initialized <subtotal> packages on zone.
Zone <zone-name> is initialized.
The file /zone/internal/root/var/sadm/system/logs/install_log
contains a log of the zone installation.

*** Select Close or Exit from the window menu to close this window ***
```

b. Open a console to monitor events in the installed zone.

i. Double-click the Zone Terminal Console action.

ii. Type the name of the zone that was just installed.

2 Initialize the zone.

- **If you are using LDAP, double-click the Initialize Zone for LDAP action.**

```
Zone name:                  Type the name of the installed zone
Host name for the zone:     Type the host name for this zone
```

For example, on a system with a shared logical interface, the values would be similar to the following:

```
Zone name:              public
Host name for the zone: machine1-zones
```

This action makes the labeled zone an LDAP client of the same LDAP server that serves the global zone. The action is complete when the following information appears:

```
zone-name zone will be  LDAP client of IP-address
zone-name is ready for booting
Zone label is LABEL

*** Select Close or Exit from the window menu to close this window ***
```

- **If you are not using LDAP, initialize the zone manually by doing one of the following steps.**

  The manual procedure in Trusted Extensions is identical to the procedure for the Oracle Solaris OS. If the system has at least one `all-zones` interface, then the hostname for all the zones must match the global zone's hostname. In general, the answers to the questions during zone initialization are the same as the answers for the global zone.

  Supply the host information by doing one of the following:

  - **After you start the zone in Step 3, answer the questions in the Zone Terminal Console about system characteristics.**

    Your answers are used to populate the `sysidcfg` file in the zone.

    Note – You must ensure that a route for the Trusted CDE desktop exists from the labeled zone to the global zone. For the procedure, see "Resolve Local Zone to Global Zone Routing in Trusted CDE" on page 152.

  - **Place a custom `sysidcfg` file in the zone's `/etc` directory before booting the zone in Step 3.**

3. **Double-click the Start Zone action.**

   Answer the prompt.

   `Zone name:` *Type the name of the zone that you are configuring*

   This action boots the zone, then starts all the services that run in the zone. For details about the services, see the `smf(5)` man page.

   The Zone Terminal Console tracks the progress of booting the zone. Messages that are similar to the following appear in the console:

   ```
   [Connected to zone 'public' console]

   [NOTICE: Zone booting up]
   ...
   Hostname: zonename
   Loading smf(5) service descriptions: number/total
   Creating new rsa public/private host key pair
   Creating new dsa public/private host key pair

   rebooting system due to change(s) in /etc/default/init

   [NOTICE: Zone rebooting]
   ```

4. **Monitor the console output.**

   Before continuing with "Customize a Booted Zone in Trusted Extensions" on page 153, make sure that the zone has rebooted. The following console login prompt indicates that the zone has rebooted.

   hostname `console login:`

Troubleshooting For Install Zone: If warnings that are similar to the following are displayed: `Installation of these packages generated errors: SUNW`*pkgname*, read the install log and finish installing the packages.

▼ Resolve Local Zone to Global Zone Routing in Trusted CDE

For every zone to access Trusted CDE, the `DISPLAY` variable must resolve. In Trusted CDE, to resolve the variable, the nodename of the labeled zone, the nodename of the global zone, and the nodename of an all-zones interface must resolve to the identical name.

Before You Begin You are using Trusted CDE and are manually initializing a labeled zone.

1 Enable Trusted CDE to display at the label of a zone by using one of the following methods.

- **Method 1: Enable X server traffic with other systems.**

  In this configuration, the labeled zones can reach other systems through the X server in the global zone.

  a. Ensure that the `/etc/nodename` file specifies the name of the system.

  ```
  ## /etc/nodename
  machine1
  ```

  b. Ensure that the `/etc/hosts` file specifies the name of the system.

  ```
  ## /etc/hosts
  192.168.2.3  machine1 loghost
  ```

  For ToolTalk services to work, the name of the system must be on the same line as `loghost`.

  c. Ensure that the `/etc/hostname.`*interface* file specifies the name of the system.

  In this configuration, `machine1` is the all-zones interface for Trusted CDE.

  ```
  ## /etc/hostname.bge0
  machine1 all-zones
  ```

- **Method 2: Limit X server traffic to the local system.**

  In this configuration, the labeled zones can communicate with the X server on the local system. However, no route exists from the local X server to other systems on the network. The route must use another interface.

  a. Ensure that the `/etc/nodename` file specifies the name of the system.

  ```
  ## /etc/nodename
  machine1
  ```

b. Ensure that the `/etc/hosts` file specifies the name of the system.

Starting with the Solaris 10 10/08 release, `lo0` is an all-zones interface. In this case, the file appears similar to the following:

```
## /etc/hosts
127.0.0.1  localhost  machine1 loghost
```

You can also use the `vni0` interface.

For ToolTalk services to work, the name of the system must be on the same line as `loghost`.

- **Method 3: Resolve the `DISPLAY` variable in another way, such as routable addresses on per-zone logical interfaces.**

  For that procedure, see "Adding Network Interfaces and Routing to Labeled Zones" on page 77.

2 **To boot the zone, return to Step 3 in "Install, Initialize, and Boot a Labeled Zone by Using CDE Actions" on page 149.**

▼ Customize a Booted Zone in Trusted Extensions

If you are going to clone zones, this procedure configures a zone to be a template for other zones. In addition, this procedure configures the zone for use.

1 **Ensure that the zone has been completely started.**

a. In the *zone-name*: Zone Terminal Console, log in as root.

```
hostname console login: root
Password:      Type root password
```

b. Check that the zone is running.

The status `running` indicates that at least one process is running in the zone.

```
# zoneadm list -v
ID NAME        STATUS         PATH
 2 public      running        /
```

c. Check that the zone can communicate with the global zone.

The X server runs in the global zone. Each labeled zone must be able to connect with the global zone to use this service. Therefore, zone networking must work before the zone can be used. For assistance, see "Labeled Zone Is Unable to Access the X Server" on page 101.

2 In the Zone Terminal Console, disable services that are unnecessary in a labeled zone.

If you are copying or cloning this zone, the services that you disable are disabled in the new zones. The services that are online on your system depend on the service manifest for the zone. Use the `netservices limited` command to turn off services that labeled zones do not need.

a. Remove many unnecessary services.

```
# netservices limited
```

b. List the remaining services.

```
# svcs
...
STATE        STIME      FMRI
online       13:05:00   svc:/application/graphical-login/cde-login:default
...
```

c. Disable graphical login.

```
# svcadm disable svc:/application/graphical-login/cde-login
# svcs cde-login
STATE        STIME      FMRI
disabled     13:06:22   svc:/application/graphical-login/cde-login:default
```

For information about the service management framework, see the `smf(5)` man page.

3 Shut down the zone.

Choose one of the following ways:

- **Run the Shut Down Zone action.**

  Provide the name of the zone.

- **In a terminal window in the global zone, use the `zlogin` command.**

  ```
  # zlogin zone-name init 0
  ```

  For more information, see the `zlogin(1)` man page.

4 Verify that the zone is shut down.

In the *zone-name*: Zone Terminal Console, the following message indicates that the zone is shut down:

```
[ NOTICE: Zone halted]
```

If you are not copying or cloning this zone, create the remaining zones in the way that you created this first zone.

5 **If you are using this zone as a template for other zones, do the following:**

a. **Remove the `auto_home_`*zone-name* file.**

In a terminal window in the global zone, remove this file from the *zone-name* zone.

```
cd /zone/zone-name/root/etc
# ls auto_home*
auto_home  auto_home_zone-name
# rm auto_home_zone-name
```

For example, if the `public` zone were the basis for cloning other zones, remove its `auto_home` file:

```
# cd /zone/public/root/etc
# rm auto_home_public
```

Next Steps

- If you are copying a zone, go to "Use the Copy Zone Method in Trusted Extensions" on page 155.
- If you are cloning a zone, go to "Use the Clone Zone Method in Trusted Extensions" on page 156.

▼ Use the Copy Zone Method in Trusted Extensions

Before You Begin

- You have completed "Specify Zone Names and Zone Labels by Using a CDE Action" on page 146.
- You have customized a zone that is the template for cloning in "Creating Labeled Zones by Using CDE Actions (Task Map)" on page 148.
- You are not currently running the zone that is your template for cloning.
- The Trusted_Extensions folder is displayed.

1 **For every zone that you want to create, double-click the Copy Zone action.**

Answer the prompts.

`New Zone Name:`	*Type name of target zone*
`From Zone Name:`	*Type name of source zone*

Caution – Do not perform other tasks while this task is completing.

2 **When the zones are created, check the status of every zone.**

a. **Double-click the Zone Terminal Console action.**

b. **Log in to each zone.**

c. **Complete "Verify the Status of the Zone" on page 72.**

▼ Use the Clone Zone Method in Trusted Extensions

Before You Begin

- You have completed "Specify Zone Names and Zone Labels by Using a CDE Action" on page 146.
- You have completed "Create ZFS Pool for Cloning Zones" on page 54.
- You have created the zone template by completing "Create ZFS Pool for Cloning Zones" on page 54.
- You have customized a zone that is your template for cloning in "Creating Labeled Zones by Using CDE Actions (Task Map)" on page 148.
- The zone that is your template for cloning is shut down.
- The Trusted_Extensions folder is displayed.

1 Create a ZFS snapshot of the zone template.

```
# cd /
# zfs snapshot zone/zone-name@snapshot
```

You use this snapshot to clone the remaining zones. For a configured zone that is named `public`, the snapshot command is the following:

```
# zfs snapshot zone/public@snapshot
```

2 For every zone that you want to create, double-click the Clone Zone action.

Answer the prompts.

```
New Zone Name:          Type name of source zone
ZFS Snapshot:             Type name of snapshot
```

3 Read the information in the dialog box.

```
Zone label is <LABEL>
zone-name is ready for booting

*** Select Close or Exit from the window menu to close this window ***
```

4 For each zone, run the Start Zone action.

Start each zone before running the action for another zone.

5 After the zones are created, check the status of every zone.

a. **Double-click the Zone Terminal Console action.**

b. **Complete "Verify the Status of the Zone" on page 72.**

◆ ◆ ◆ APPENDIX C

Configuration Checklist for Trusted Extensions

This checklist provides an overall view of the major configuration tasks for Trusted Extensions. The smaller tasks are outlined within the major tasks. The checklist does not replace following the steps in this guide.

Checklist for Configuring Trusted Extensions

The following list summarizes what is required to enable and configure Trusted Extensions at your site. Tasks that are covered elsewhere are cross-referenced.

1. Read.
   - Read the first five chapters of *Trusted Extensions Administrator's Procedures*.
   - Understand site security requirements.
   - Read "Site Security Policy and Trusted Extensions" on page 136.
2. Prepare.
   - Decide the `root` password.
   - Decide the PROM or BIOS security level.
   - Decide the PROM or BIOS password.
   - Decide if attached peripherals are permitted.
   - Decide if access to remote printers is permitted.
   - Decide if access to unlabeled networks is permitted.
   - Decide the zone creation method.
3. Enable Trusted Extensions.
   a. Install the Oracle Solaris OS.
      - For remote administration, install the Developer Group or larger group of packages.
      - For the Clone Zone creation method, select Custom Install, then lay out a `/zone` partition.
   b. Enable `svc:/system/labeld`, the Trusted Extensions service.

4. If using IPv6, enable IPv6 for Trusted Extensions.
5. If using a DOI different from `1`, set the DOI in the `/etc/system` and the `/etc/security/tsol/tnrhtp` files.
6. (Optional) Create ZFS pool for cloning zones.
7. Configure labels.
   a. Finalize your site's `label_encodings` file.
   b. Check and install the file.
   c. Reboot.
8. Configure interfaces for the global zone and for labeled zones.
9. Configure the Solaris Management Console.
10. Configure the naming service.
    - Use the files naming service, which requires no configuration.
    - Or, configure LDAP
      a. Create either a Trusted Extensions proxy server or a Trusted Extensions LDAP server.
      b. Enable the Solaris Management Console server to accept network connections.
      c. Register the Solaris Management Console with LDAP.
      d. Create an LDAP toolbox for the Solaris Management Console.
11. Configure network connections for LDAP.
    - Assign an LDAP server or proxy server to the `cipso` host type in a remote host template.
    - Assign the local system to the `cipso` host type in a remote host template.
    - Make the local system a client of the LDAP server.
12. Create labeled zones.
    - OPTION 1: Use txzonemgr script.
    - OPTION 2: Use Trusted CDE actions.
      a. Configure labeled zones
         i. In the Solaris Management Console, associate zone names with particular labels.
         ii. Run the Configure Zone action.
      b. Run the Install Zone action.
      c. Run the Initialize for LDAP action.
      d. Run the Start Zone action.
      e. Customize the running zone.
      f. Run the Shut Down Zone action.
      g. Customize the zone while the zone is shut down.
      h. (Optional) Create a ZFS snapshot.

i. Create the remaining zones from scratch, or by using the Copy Zone or the Clone Zone action.

13. Configure the network. See "Configuring Trusted Network Databases (Task Map)" in *Trusted Extensions Administrator's Procedures*.
    - Identify single-label hosts and limited-range hosts.
    - Determine the labels to apply to incoming data from unlabeled hosts.
    - Customize the remote host templates.
    - Assign individual hosts to templates.
    - Assign subnets to templates.
14. Establish static routing. See "Configuring Routes and Checking Network Information in Trusted Extensions (Task Map)" in *Trusted Extensions Administrator's Procedures*.
15. Configure local users and local administrative roles.
    - To enforce separation of duty, create customized rights profiles.
    - Create the Security Administrator role.
    - Create a local user who can assume the Security Administrator role.
    - Create other roles, and possibly other local users to assume these roles.
16. Create home directories on the NFS server.
    - Create home directories for each user at every label that the user can access.
    - (Optional) Prevent users from reading their lower-level home directories.
17. Configure printing. See "Managing Printing in Trusted Extensions (Task Map)" in *Trusted Extensions Administrator's Procedures*.
18. Configure devices. See "Handling Devices in Trusted Extensions (Task Map)" in *Trusted Extensions Administrator's Procedures*.
    a. Assign the Device Management profile or the System Administrator profile to a role.
    b. To make devices usable, do one of the following:
       - Per system, make devices allocatable.
       - Assign the Allocate Device authorization to selected users and roles.
19. Configure Oracle Solaris features.
    - Configure auditing.
    - Configure security settings.
    - Enable particular LDAP clients to be LDAP administration systems.
    - Configure users in LDAP.
    - Configure network roles in LDAP.
    - Mount and share file systems. See Chapter 11, "Managing and Mounting Files in Trusted Extensions (Tasks)," in *Trusted Extensions Administrator's Procedures*

Glossary

accreditation range A set of sensitivity labels that are approved for a class of users or resources. A set of valid labels. See also system accreditation range and user accreditation range.

administrative role A role that gives required authorizations, privileged commands, privileged actions, and the Trusted Path security attribute to allow the role to perform administrative tasks. Roles perform a subset of superuser's capabilities, such as backup or auditing.

allocation A mechanism by which access to a device is controlled. See device allocation.

application search path In CDE, the search path is used by the system to find applications and certain configuration information. The application search path is controlled by a trusted role.

authorization A right granted to a user or role to perform an action that would otherwise not be allowed by security policy. Authorizations are granted in rights profiles. Certain commands require the user to have certain authorizations to succeed. For example, to print a PostScript file requires the Print Postscript authorization.

CDE See Common Desktop Environment.

CIPSO label Common IP Security Option. CIPSO is the label standard that Trusted Extensions implements.

classification The hierarchical component of a clearance or a label. A classification indicates a hierarchical level of security, for example, `TOP SECRET` or `UNCLASSIFIED`.

clearance The upper limit of the set of labels at which a user can work. The lower limit is the minimum label that is assigned by the security administrator. A clearance can be one of two types, a session clearance or a user clearance.

client A system connected to a network.

closed network A network of systems that are configured with Trusted Extensions. The network is cut off from any non-Trusted Extensions host. The cutoff can be physical, where no wire extends past the Trusted Extensions network. The cutoff can be in the software, where the Trusted Extensions hosts recognize only Trusted Extensions hosts. Data entry from outside the network is restricted to peripherals attached to Trusted Extensions hosts. Contrast with open network.

Common Desktop Environment The historical windowing environment for administering Trusted Extensions software. Trusted Extensions modifies the environment to create Trusted CDE. The Sun Java Desktop System is also modified to create a Trusted JDS.

compartment A nonhierarchical component of a label that is used with the classification component to form a clearance or a label. A compartment represents a collection of information, such as would be used by an engineering department or a multidisciplinary project team.

.copy_files file An optional setup file on a multilabel system. This file contains a list of startup files, such as `.cshrc` or `.mozilla`, that the user environment or user applications require in order for the system or application to behave well. The files that are listed in `.copy_files` are then *copied* to the user's home directory at higher labels, when those directories are created. See also .link_files file.

DAC See discretionary access control.

device Devices include printers, computers, tape drives, floppy drives, CD-ROM drives, DVD drives, audio devices, and internal pseudo terminal devices. Devices are subject to the read equal write equal MAC policy. Access to removable devices, such as DVD drives, are controlled bydevice allocation.

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 that is 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.

discretionary access control The type of access that is granted or that is denied by the owner of a file or directory at the discretion of the owner. Trusted Extensions provides two kinds of discretionary access controls (DAC), UNIX permission bits and ACLs.

domain A part of the Internet naming hierarchy. It represents a group of systems on a local network that share administrative files.

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: `example1.town.state.country.org`). As you read a domain name from left to right, the component names identify more general, and usually remote, areas of administrative authority.

domain of interpretation (DOI) On an Oracle Solaris system that is configured with Trusted Extensions, the domain of interpretation is used to differentiate between different `label_encodings` files that might have similar labels defined. The DOI is a set of rules that translates the security attributes on network packets to the representation of those security attributes by the local `label_encodings` file. When systems have the same DOI, they share that set of rules and can translate the labeled network packets.

evaluated configuration One or more Trusted Extensions hosts that 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. The evaluating and certifying body is the NSA.

- Trusted Extensions software that is configured on the Solaris 10 11/06 release is certified to the Common Criteria v2.3 [August 2005], an ISO standard, to Evaluation Assurance Level (EAL) 4, and against a number of protection profiles.
- Through an Assurance Continuity, the NSA certified Trusted Extensions software that is configured on the Solaris 10 5/09 release.

The Common Criteria v2 (CCv2) and protection profiles make the earlier TCSEC U.S. standard obsolete through level B1+. A mutual recognition agreement for CCv2 has been signed by the United States, the United Kingdom, Canada, Denmark, the Netherlands, Germany, and France.

The Trusted Extensions configuration target provides functionality that is similar to the TCSEC C2 and B1 levels, with some additional functionality.

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.

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 Extensions software, you must add the Sun-specific `LOCAL DEFINITIONS` section to the end of the GFI. For details, see Chapter 5, "Customizing LOCAL DEFINITIONS," in *Trusted Extensions Label Administration*.

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, a domain identifies a 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.

initial label The minimum label assigned to a user or role, and the label of the user's initial workspace. The initial label is the lowest label at which the user or role can work.

initial setup team A team of at least two people who together oversee the enabling and configuration of Trusted Extensions software. One team member is responsible for security decisions, and the other for system administration decisions.

IP address Internet protocol address. A unique number that identifies a networked system so it can communicate by means of Internet protocols. In IPv4, the address consists of four numbers separated by periods. Most often, each part of the IP address is a number between 0 and 225. However, the first number must be less than 224 and the last number cannot be 0.

IP addresses are logically divided into two parts: the network, and the system on the network. The network number is similar to a telephone area code. In relation to the network, the system number is similar to a phone number.

label A security identifier that is assigned to an object. The label is based on the level at which the information in that object should be protected. Depending on how the security administrator has configured the user, a user can see the sensitivity label, or no labels at all. Labels are defined in the label_encodings file.

label configuration A Trusted Extensions installation choice of single-label or multilabel sensitivity labels. In most circumstances, label configuration is identical on all systems at your site.

label_encodings file The file where the complete sensitivity label is defined, as are accreditation ranges, label view, default label visibility, default user clearance, and other aspects of labels.

label range A set of sensitivity labels that are assigned to commands, zones, and allocatable devices. The range is specified by designating a maximum label and a minimum label. For commands, the minimum and maximum labels limit the labels at which the command can be executed. Remote hosts that do not recognize labels are assigned a single sensitivity label, as are any other hosts that the security administrator wants to restrict to a single label. A label range limits the labels at which devices can be allocated and restrict the labels at which information can be stored or processed when using the device.

label relationships On an Oracle Solaris system that is configured with Trusted Extensions, a label can dominate another label, be equal to another label, or be disjoint from another label. For example, the label `Top Secret` dominates the label `Secret`. For two systems with the same domain of interpretation (DOI), the label `Top Secret` on one system is equal to the label `Top Secret` on the other system.

label set See security label set.

labeled host A labeled system that is part of a trusted network of labeled systems.

labeled system A labeled system is a system that is running a multilevel operating system, such as Trusted Extensions or SELinux with MLS enabled. The system can send and receive network packets that are labeled with a Common IP Security Option (CIPSO) in the header of the packet.

labeled zone On an Oracle Solaris system that is configured with Trusted Extensions, every zone is assigned a unique label. Although the global zone is labeled, *labeled zone* typically refers to a non-global zone that is assigned a label. Labeled zones have two different characteristics from non-global zones on an Oracle Solaris system that is not configured with labels. First, labeled zones must use the same pool of user IDs and group IDs. Second, labeled zones can share IP addresses.

.link_files file An optional setup file on a multilabel system. This file contains a list of startup files, such as `.cshrc` or `.mozilla`, that the user environment or user applications require in order for the system or application to behave well. The files that are listed in `.link_files` are then *linked* to the user's home directory at higher labels, when those directories are created. See also .copy_files file.

MAC See mandatory access control.

mandatory access control Access control that is 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, read equal–read down, applies when a process at one label attempts to read a file at a lower label. The MAC rule, write equal-read down, applies when a process at one label attempts to write to a directory at another label.

minimum label The lower bound of a user's sensitivity labels and the lower bound of the system's sensitivity labels. The minimum label set by the security administrator when specifying a user's security attributes is the sensitivity label of the user's first workspace at first login. The sensitivity label that is specified in the minimum label field by the security administrator in the `label_encodings` file sets the lower bound for the system.

multilevel desktop On an Oracle Solaris system that is configured with Trusted Extensions, users can run a desktop at a particular label. If the user is authorized to work at more than one label, the user can create a separate workspace to work at each label. On this multilevel desktop, authorized users can cut and paste between windows at different labels, receive mail at different labels, and view and use labeled windows in workspaces of a different label.

multilevel port (MLP) On an Oracle Solaris system that is configured with Trusted Extensions, an MLP is used to provide multilevel service in a zone. By default, the X server is a multilevel service that is defined in the global zone. An MLP is specified by port number and protocol. For example, the MLP of the X server for the multilevel desktop is specified by 6000-6003 and TCP.

naming service A distributed network database that contains key system information about all the systems on a network, so that the systems can communicate with each other. With a naming service, the system information can be maintained, managed, and accessed on a network-wide basis. Sun supports the LDAP naming service. Without such a service, each system has to maintain its own copy of the system information in the local `/etc` files.

networked systems A group of systems that are connected through hardware and software, sometimes referred to as a local area network (LAN). One or more servers are usually needed when systems are networked.

non-networked systems Computers that are not connected to a network or do not rely on other hosts.

open network A network of Trusted Extensions hosts that is connected physically to other networks and that uses Trusted Extensions software to communicate with non-Trusted Extensions hosts. Contrast with closed network.

outside the evaluated configuration When software that has been proved to be able satisfy the criteria for an evaluated configuration, is configured with settings that do not satisfy security criteria, the software is described as being *outside the evaluated configuration*.

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 the owner's group, and one set for all others.

primary administrator The person who is entrusted to create new rights profiles for the organization, and to fix machine difficulties that are beyond the power of the security administrator and system administrator combined. This role should be assumed rarely. After initial security configuration, more secure sites can choose not to create this role, and not to assign any role the Primary Administrator profile.

privilege Powers that are granted to a process that is executing a command. The full set of privileges describes the full capabilities of the system, from basic capabilities to administrative capabilities. Privileges that bypass security policy, such as setting the clock on a system, can be granted by a site's security administrator.

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 that are available to the command being executed and the sensitivity label of the current workspace.

profile shell A special shell that recognizes security attributes, such as privileges, authorizations, and special UIDs and GIDs. A profile shell typically limits users to fewer commands, but can allow these commands to run with more rights. The profile shell is the default shell of a trusted role.

remote host A different system than the local system. A remote host can be an unlabeled host or a labeled host.

rights profile A bundling mechanism for commands and CDE actions and for the security attributes that are assigned to these executables. Rights profiles allow Oracle Solaris administrators to control who can execute which commands and to control the attributes these commands have when they are executed. When a user logs in, all rights assigned to that user are in effect, and the user has access to all the commands, CDE actions, and authorizations assigned in all of that user's rights profiles.

role A role is like a user, except that a role cannot log in. Typically, a role is used to assign administrative capabilities. Roles are limited to a particular set of commands and authorizations and CDE actions. See administrative role.

security administrator In an organization where sensitive information must be protected, the person or persons who define and enforce the site's security policy. These persons are cleared to access all information that is being processed at the site. In software, the Security Administrator administrative role is assigned to one or more individuals who have the proper clearance. These administrators configure the security attributes of all users and hosts so that the software enforces the site's security policy. In contrast, see system administrator.

security attribute An attribute that is used to enforce Trusted Extensions security policy. Various sets of security attributes are assigned to processes, users, zones, hosts, allocatable devices, and other objects.

security label set Specifies a discrete set of security labels for a tnrhtp database entry. Hosts that are assigned to a template with a security label set can send and receive packets that match any one of the labels in the label set.

security policy On a Trusted Extensions host, the set of DAC, MAC, and labeling rules that define how information can 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 that is assigned to an object or a process. The label is used to limit access according to the security level of the data that is contained.

separation of duty The security policy that two administrators or roles be required to create and authenticate a user. One administrator or role is responsible for creating the user, the user's home directory, and other basic administration. The other administrator or role is responsible for the user's security attributes, such as the password and the label range.

Solaris Management Console A Java-based administrative GUI that contains toolboxes of administrative programs. Most system, network, and user administration is done by using the Console toolboxes.

system Generic name for a computer. After installation, a system on a network is often referred to as a host.

system accreditation range The set of all valid labels that are created according to the rules that the security administrator defines in the label_encodings file, plus the two administrative labels that are used on every system that is configured with Trusted Extensions. The administrative labels are `ADMIN_LOW` and `ADMIN_HIGH`.

system administrator In Trusted Extensions, the trusted role assigned to the user or users who are responsible for performing standard system management tasks such as setting up the non-security-relevant portions of user accounts. In contrast, see security administrator.

tnrhdb database The trusted network remote host database. This database assigns a set of label characteristics to a remote host. The database is accessible either as a file in `/etc/security/tsol/tnrhdb` or from the LDAP server.

tnrhtp database The trusted network remote host template. This database defines the set of label characteristics that a remote host can be assigned. The database is accessible either as a file in `/etc/security/tsol/tnrhtp`, or from the LDAP server.

toolbox A collection of programs in the Solaris Management Console. On a Trusted Extensions host, administrators use `Policy=TSOL` toolboxes. Each toolbox has programs that are usable in the scope of the toolbox. For example, the Trusted Network Zones tool, which handles the system's `tnzonecfg` database, exists only in the `Files` toolbox, because its scope is always local. The User Accounts program exists in all toolboxes. To create a local user, the administrator uses the `Files` toolbox, and to create a network user, the administrator uses the `LDAP` toolbox.

trusted editor On an Oracle Solaris system that is configured with Trusted Extensions, the trusted editor is used to create and modify administrative files. The file name cannot be changed by the editor. Also, use of the editor is audited and shell escape commands are disabled. In Trusted CDE, the Admin Editor action starts the trusted editor. In Trusted JDS, the `/usr/dt/bin/trusted_edit` command starts the trusted editor.

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 Extensions system can communicate with.

trusted path On an Oracle Solaris system that is configured with Trusted Extensions, the trusted path is a reliable, tamper-proof way to interact with the system. The trusted path is used to ensure that administrative functions cannot be compromised. User functions that must be protected, such as changing a password, also use the trusted path. When the trusted path is active, the desktop displays a tamper-proof indicator.

trusted role See administrative role.

trusted stripe A region that cannot be spoofed. In Trusted CDE, the trusted stripe is at the bottom of the screen, and in Trusted JDS the stripe is at the top. The stripe provides visual feedback about the state of the window system: a trusted path indicator and window sensitivity label. When sensitivity labels are configured to not be viewable for a user, the trusted stripe is reduced to an icon that displays only the trusted path indicator.

txzonemgr script The `/usr/sbin/txzonemgr` script provides a simple GUI for managing labeled zones. The script also provides menu items for networking options, name services options, and for clienting the global zone to an existing LDAP server. `txzonemgr` is run by root in the global zone.

unlabeled host A networked system that sends unlabeled network packets, such as a system that is running the Oracle Solaris OS.

unlabeled system To an Oracle Solaris system that is configured with Trusted Extensions, an unlabeled system is a system that is not running a multilevel operating system, such as Trusted Extensions or SELinux with MLS enabled. An unlabeled system does not send labeled packets. If the communicating Trusted Extensions system has assigned to the unlabeled system a single label, then network communication between the Trusted Extensions system and the unlabeled system happens at that label. An unlabeled system is also called a “single-level system”.

user accreditation range The set of all possible labels at which a regular user can work on the system. The site's security administrator specifies the range in the label_encodings file file. The rules for well-formed labels that define the system accreditation range are additionally restricted by the values in the `ACCREDITATION RANGE` section of the 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 a user can work at any time. The user can decide to accept the default, or can further restrict that clearance during any particular login session.

Index

A

accessing the X server, 101–103
accounts
  creating, 84–95
  planning, 26
`Action failed. Reconnect to Solaris Zone?`, 101–103
adding
  default routes for labeled zones, 79–83
  LDAP toolbox, 122–123
  local role with `roleadd`, 89–90
  local user with `useradd`, 92–93
  network databases to LDAP server, 116–118
  `nscd` daemon to every labeled zone, 83–84
  roles, 84–95
  shared network interfaces, 64–68
  Trusted Extensions to an Oracle Solaris system, 44–45
  users by using `lpaddent`, 98–100
  users who can assume roles, 90–93
  zone-specific network interface, 77–79
  zone-specific `nscd` daemon, 83–84
Additional Trusted Extensions Configuration Tasks, 103–106
addresses
  sharing between global and labeled zones, 143–145
  specifying one IP address per system, 67–68, 145–146
administering, remotely by a role, 129–131
administrative actions
  Check Encodings, 48–51
  Clone Zone, 156
administrative actions *(Continued)*
  Configure Zone, 146
  Copy Zone, 155–156
  Create LDAP Client, 59–62
  Initialize Zone for LDAP, 150
  Install Zone, 150
  Share Logical Interface, 144
  Share Physical Interface, 145
  Shut Down Zone, 154
  Start Zone, 151
  Zone Terminal Console, 75, 150, 151
allocating devices
  for copying data, 103–104
  tape drive, 106
Associating Network Interfaces With Zones by Using CDE Actions (Task Map), 143–146
auditing, planning, 26

B

backing up, previous system before installation, 29
booting
  zones, 71–72, 151

C

`Cannot reach global zone`, 101–103
Check Encodings action, 48–51
checking
  `label_encodings` file, 48–51
  roles are working, 93–94

checklists for initial setup team, 157–159
chk_encodings command, 51
Clone Zone action, 156
collecting information
  before enabling Trusted Extensions, 41–42
  for LDAP service, 109–110
configuration files, copying, 103–104
Configure Zone action, 146
configuring
  access to headless Trusted Extensions, 127–134
  as a role or as superuser?, 43
  LDAP for Trusted Extensions, 109–118
  LDAP proxy server for Trusted Extensions clients, 119
  network interfaces, 64–68
  Solaris Management Console for LDAP, 120–125
  Trusted Extensions labeled zones, 62–76, 143–156
  Trusted Extensions software, 47–106
Configuring an LDAP Proxy Server on a Trusted Extensions Host (Task Map), 108
Configuring an LDAP Server on a Trusted Extensions Host (Task Map), 107–108
Configuring the Solaris Management Console for LDAP (Task Map), 120–125
configuring Trusted Extensions
  checklist for install team, 157–159
  headless access, 127–134
  initial procedures, 47–106
  labeled zones, 62–76, 143–156
  task maps, 31–35
console window, troubleshooting not opening, 100–101
Copy Zone action, 155–156
Create a new zone menu item, 68, 75–76
Create LDAP Client action, 59–62
creating
  accounts, 84–95
  accounts during or after configuration, 43
  home directories, 95–97
  home directory server, 95–96
  labeled zones, 62–76
  LDAP client, 59–62
  LDAP proxy server for Trusted Extensions clients, 119
creating *(Continued)*
  LDAP toolbox, 122–123
  local role with roleadd, 89–90
  local user with useradd, 92–93
  roles, 84–95
  users who can assume roles, 90–93
  zones, 62–76, 149–152
Creating Labeled Zones, 62–76
Creating the Labeled Zones by Using CDE Actions (Task Map), 148–156
credentials, registering LDAP with the Solaris Management Console, 120–121

D

deciding
  to configure as a role or as superuser, 43
  to use a Sun-supplied encodings file, 42
decisions to make
  based on site security policy, 136
  before enabling Trusted Extensions, 42–44
default routes, specifying for labeled zones, 79–83
deleting, labeled zones, 106
directories, for naming service setup, 117
disabling, Trusted Extensions, 106
domain of interpretation (DOI), entry in /etc/system file, 52–54
dpadm service, 112
dsadm service, 112

E

enabling
  DOI different from 1, 52–54
  dpadm service, 112
  dsadm service, 112
  IPv6 network, 52
  labeld service, 44–45
  LDAP administration from a client, 121–122
  login to labeled zone, 95
  Trusted Extensions on an Oracle Solaris system, 44–45
encodings file, *See* label_encodings file

error messages
troubleshooting, 45, 101–103
/etc/system file
modifying for DOI different from 1, 52–54
modifying for IPv6 network, 52

F

files
copying from removable media, 105
resolv.conf, 62

H

hardware planning, 22
Headless System Configuration in Trusted Extensions (Task Map), 127–134
home directories
creating, 95–97
creating server for, 95–96
logging in and getting, 96–97

I

initial setup team, checklist for configuring Trusted Extensions, 157–159
Initialize Zone for LDAP action, 150
initializing
Solaris Management Console, 56–59
zones, 150
zones for LDAP, 149–152
Install Zone action, 150
troubleshooting, 152
installation menu
Create a new zone, 68, 75–76
Zone Console, 71
installing
label_encodings file, 48–51
Oracle Solaris OS for Trusted Extensions, 37–45
Sun Java System Directory Server, 109–118
zones, 70–71, 149–152
IPv6
entry in /etc/system file, 52
troubleshooting, 52

L

label_encodings file
checking, 48–51
installing, 48–51
localizing, 22
modifying, 48–51
labeld service, 44–45
disabling, 106
troubleshooting, 45
Labeled Zone Manager, *See* txzonemgr script
labeling
turning on labels, 55–56
zones, 68–70, 146–148
labels
assigning to named zones, 69, 147
on trusted stripe, 56
planning, 21–22
specifying for zones, 68–70, 146–148
laptops, planning, 25
LDAP
enabling administration from a client, 121–122
planning, 25–26
LDAP configuration
creating client, 59–62
for Trusted Extensions, 109–118
Sun Ray servers, and, 109
LDAP server
collecting information for, 109–110
configuring multilevel port, 115–116
configuring naming service, 110–112
configuring proxy for Trusted Extensions clients, 119
creating proxy for Trusted Extensions clients, 119
installing in Trusted Extensions, 110–112
planning for separation of duty, 117
protecting log files, 114–115
registering credentials with Solaris Management Console, 120–121
log files, protecting Directory Server logs, 114–115

logging in
to a home directory server, 96–97
using `rlogin` command, 132–134
login, remote, 129–131
`lpaddent` command, 98–100

M

media, copying files from removable, 105
modifying, `label_encodings` file, 48–51
multilevel server, planning, 25

N

name service cache daemon, *See* `nscd` daemon
names
specifying for zones, 68–70, 146–148
naming
zones, 68–70, 146–148
network, *See* Trusted Extensions network
`No route available`, 101–103
`nscd` daemon, adding to every labeled zone, 83–84

O

Oracle Solaris installation options, requirements, 38–39
Oracle Solaris installed systems, requirements for Trusted Extensions, 39–41

P

planning
See also Trusted Extensions use
account creation, 26
administration strategy, 21
auditing, 26
hardware, 22
labels, 21–22
laptop configuration, 25
LDAP naming service, 25–26
planning *(Continued)*
network, 22–23
NFS server, 25
printing, 25
Trusted Extensions, 19–29
Trusted Extensions configuration strategy, 27–28
zones, 23–25
Preparing to Create Zones by Using CDE Actions (Task Map), 146–148
printing, planning, 25
publications, security and UNIX, 139–141

R

rebooting
activating labels, 55–56
enabling login to labeled zone, 95
registering, LDAP credentials with the Solaris Management Console, 120–121
remote logins, enabling for roles, 129–131
removing, zone-specific `nscd` daemon, 84
removing Trusted Extensions, *See* disabling
requirements for Trusted Extensions
Oracle Solaris installation options, 38–39
Oracle Solaris installed systems, 39–41
`resolv.conf` file, loading during configuration, 62
rights profiles, customizing for separation of duty, 85–87
roadmaps
Task Map: Configuring Trusted Extensions, 33–35
Task Map: Preparing an Oracle Solaris System for Trusted Extensions, 31
Task Map: Preparing For and Enabling Trusted Extensions, 31–32
`roleadd` command, 89–90
roles
adding local role with `roleadd`, 89–90
creating Security Administrator, 88–90
determining when to create, 43
logging in remotely, 129–131
separation of duty, 85–87, 90
verifying they work, 93–94
root passwords, required in Trusted Extensions, 40

routing, specifying default routes for labeled
zones, 79–83

S

screens, initial display, 56
security
initial setup team, 37
publications, 139–141
root password, 40
site security policy, 135–141
Security Administrator role, creating, 88–90
security information, planning for Trusted
Extensions, 29
separation of duty
creating rights profiles, 85–87
planning for, 27–28
planning for LDAP, 117
service management framework (SMF)
`dpadm`, 112
`dsadm`, 112
`labeld` service, 44–45
Share Logical Interface action, 144
Share Physical Interface action, 145
Shut Down Zone action, 154
site security policy
common violations, 138–139
personnel recommendations, 138
physical access recommendations, 137–138
recommendations, 136–137
tasks involved, 135–141
Trusted Extensions configuration decisions, 136
understanding, 20
Solaris Management Console
configuring for LDAP, 120–125
configuring LDAP toolbox, 122–123
enabling LDAP toolbox to be used, 121–122
initializing, 56–59
loading a Trusted Extensions toolbox, 56–59
registering LDAP credentials, 120–121
troubleshooting, 56–59
using Trusted Network Zone Configuration
tool, 69, 147
Solaris Management Console *(Continued)*
working with Sun Java System Directory
Server, 120–125
Start Zone action, 151
starting
zones, 71–72, 151
Sun Java System Directory Server, *See* LDAP server
Sun Ray systems
LDAP servers, and, 109
web site for documentation, 32
`svcs: Pattern 'labeld' doesn't match any
instances`, 45
System Administrator role, restricting, 90

T

tape devices, allocating, 106
Task Map: Configuring Trusted Extensions, 33–35
Task Map: Preparing an Oracle Solaris System for
Trusted Extensions, 31
Task Map: Preparing For and Enabling Trusted
Extensions, 31–32
tasks and task maps
Additional Trusted Extensions Configuration
Tasks, 103–106
Associating Network Interfaces With Zones by
Using CDE Actions (Task Map), 143–146
Configuring an LDAP Proxy Server on a Trusted
Extensions Host (Task Map), 108
Configuring an LDAP Server on a Trusted
Extensions Host (Task Map), 107–108
Configuring the Solaris Management Console for
LDAP (Task Map), 120–125
Creating Labeled Zones, 62–76
Creating the Labeled Zones by Using CDE Actions
(Task Map), 148–156
Headless System Configuration in Trusted
Extensions (Task Map), 127–134
Preparing to Create Zones by Using CDE Actions
(Task Map), 146–148
`tcp_listen=true` LDAP setting, 121–122
toolboxes
adding LDAP server to `tsol_ldap.tbx`, 122–123
loading in Trusted Extensions, 56–59

toolboxes *(Continued)*
Scope=LDAP, 120–121
troubleshooting
accessing X server, 101–103
console window not opening, 100–101
`Installation of these packages generated errors: SUNW`*pkgname*, 71, 152
IPv6 configuration, 52
Oracle Solaris release that supports the `labeld` service, 45
Solaris Management Console, 56–59
Trusted Extensions configuration, 100–103
Trusted Network Zones Properties, 148
Trusted Extensions
See also Trusted Extensions planning
collecting information before enabling, 41–42
decisions to make before enabling, 42–44
differences from Oracle Solaris administrator's perspective, 30
disabling, 106
enabling, 44–45
memory requirements, 22
planning configuration strategy, 27–28
planning for, 19–29
planning hardware, 22
planning network, 22–23
preparing for, 38–41, 41–44
results before configuration, 30
separation of duty, 27–28
two-role configuration strategy, 28
Trusted Extensions configuration
adding network databases to LDAP server, 116–118
changing default DOI value, 52–54
databases for LDAP, 109–118
division of tasks, 37
evaluated configuration, 20
headless systems, 127–134
initial procedures, 47–106
initial setup team responsibilities, 37
labeled zones, 62–76, 143–156
LDAP, 109–118
reboot to activate labels, 55–56
task maps, 31–35
troubleshooting, 100–103
Trusted Extensions network
adding zone-specific interface, 77–79
adding zone-specific `nscd` daemon, 83–84
enabling IPv6, 52
planning, 22–23
removing zone-specific `nscd` daemon, 84
specifying default routes for labeled zones, 79–83
Trusted Extensions requirements
Oracle Solaris installation, 38–39
Oracle Solaris installed systems, 39–41
root password, 40
Trusted Network Zones tool
assigning labels to named zones, 69, 147
troubleshooting, 148
`tsol_ldap.tbx` file, 122–123
`txzonemgr` script, 63–64, 102

U

`useradd` command, 92–93
users
adding from NIS server, 98–100
adding local user with `useradd`, 92–93
creating initial users, 90–93
requiring two roles to create user, 85–87
requiring two roles to create users, 90
`/usr/sbin/txzonemgr` script, 63–64, 102, 148

V

verifying
`label_encodings` file, 48–51
roles are working, 93–94
zone status, 72–73

W

workspaces, initial display, 56

Z

`zenity` script, 63–64
ZFS, unsupported but fast zone creation method, 24
ZFS pools, creating for cloning zones, 54–55
Zone Console, output, 71
Zone Terminal Console action
  output, 75, 151
  using, 150
zones
  adding network interface, 77–79
  adding `nscd` daemon to each labeled zone, 83–84
  associating zone names with labels, 69, 147
  booting, 71–72, 151
  creating, 149–152
  creating ZFS pool for cloning, 54–55
  customizing, 74–75
  deciding creation method, 23–25
  deleting, 106
  enabling login to, 95
  halting, 74
  initializing, 150
  initializing for LDAP, 149–152
  installing, 70–71, 149–152
  isolating with default routes, 79–83
  removing `nscd` daemon from labeled zones, 84
  showing zone activity, 71, 75, 151
  shutting down, 154
  specifying a shared IP address, 143–145
  specifying default routes, 79–83
  specifying labels, 68–70, 146–148
  specifying names, 68–70, 146–148
  specifying one IP address for all zones, 67–68, 145–146
  starting, 151
  troubleshooting access, 101–103
  troubleshooting installation, 71
  `txzonemgr` script, 102
  `/usr/sbin/txzonemgr` script, 63–64, 148
  verifying status, 72–73