Oracle® Solaris Trusted Extensions 配置指南

文件号码 E22295
2011 年 8 月

ORACLE

120418@25097

目录

图

表

前言

《Oracle Solaris Trusted Extensions 配置指南》介绍在 Solaris 操作系统 (Solaris OS) 中配置 Trusted Extensions 的过程。该指南还介绍如何准备 Solaris 系统以支持 Trusted Extensions 的安全安装。

注 – 此 Oracle Solaris 发行版支持使用 SPARC 和 x86 系列处理器体系结构的系统。支持的系统可以在 Oracle Solaris OS: Hardware Compatibility Lists (`http://www.oracle.com/webfolder/technetwork/hcl/index.html`)（Oracle Solaris OS：硬件兼容性列表）中找到。本文档列举了在不同类型的平台上进行实现时的所有差别。

在本文档中，这些与 x86 相关的术语表示以下含义：

- x86 泛指 64 位的 x86 兼容产品系列。
- x64 特指 64 位的 x86 兼容 CPU。

若想了解本发行版支持哪些系统，请参见 Oracle Solaris OS: Hardware Compatibility Lists（Oracle Solaris OS：硬件兼容性列表）。

目标读者

本指南的目标读者为配置 Trusted Extensions 软件的有经验的系统管理员和安全管理员。您的站点安全策略所需的信任级别和您的专业水平决定了可执行配置任务的人选。

实施站点安全

要在系统中成功配置 Trusted Extensions 以与站点安全策略保持一致，需要了解 Trusted Extensions 的安全功能和站点的安全策略。开始之前，请阅读第 1 章，Trusted Extensions 的安全规划，查看有关如何在配置软件时确保站点安全的信息。

Trusted Extensions 和 Solaris 操作系统

Trusted Extensions 在 Solaris OS 之上运行。由于 Trusted Extensions 软件可以修改 Solaris OS，所以 Trusted Extensions 可能需要对 Solaris 安装选项进行特定设置。有关详细信息，请参见第 3 章，将 Trusted Extensions 软件添加到 Solaris OS（任务）。此外，Trusted Extensions 指南对 Solaris 指南进行了补充。作为管理员，您需要访问 Solaris 指南和 Trusted Extensions 指南。

本书的结构

第 1 章，Trusted Extensions 的安全规划，介绍在一个或多个 Solaris 系统中配置 Trusted Extensions 软件时需要考虑的安全问题。

第 2 章，Trusted Extensions 的配置任务列表，包含用于将 Trusted Extensions 软件添加到 Solaris 系统的任务列表。

第 3 章，将 Trusted Extensions 软件添加到 Solaris OS（任务），提供为安装 Trusted Extensions 软件准备 Solaris 系统的说明。还包含启用 Trusted Extensions 的说明。

第 4 章，配置 Trusted Extensions（任务），提供在带有显示器的系统中配置 Trusted Extensions 软件的说明。

第 5 章，为 Trusted Extensions 配置 LDAP（任务），提供为 Trusted Extensions 配置 LDAP 的说明。

第 6 章，配置具有 Trusted Extensions 的无显示系统（任务），介绍如何在无显示系统中配置和管理 Trusted Extensions 软件。

附录 A，站点安全策略，讨论站点安全策略并将 Trusted Extensions 放在更广泛的组织和站点安全环境中。

附录 B，使用 CDE 操作在 Trusted Extensions 中安装区域，介绍如何使用 Trusted CDE 操作配置有标签区域。

附录 C，Trusted Extensions 的配置核对表，为初始设置团队提供配置核对表。

词汇表，定义本指南中使用的特定术语和短语。

Trusted Extensions 指南丛书的结构

下表列出了 Trusted Extensions 指南丛书所涵盖的所有主题和每个指南所针对的目标读者。

指南标题	主题	目标读者
《Solaris Trusted Extensions Transition Guide》	已过时。概述了 Trusted Solaris 8 软件、Solaris 10 软件和 Trusted Extensions 软件之间的差异。 对于本发行版，Solaris OS 的新增功能文档中提供了 Trusted Extensions 更改的概述。	所有
《Solaris Trusted Extensions Reference Manual》	已过时。提供了 Trusted Extensions 发行版 Solaris 10 11/06 和 Solaris 10 8/07 的 Trusted Extensions 手册页。 对于本发行版，Trusted Extensions 手册页是随 Solaris 手册页提供的。	所有
《Oracle Solaris Trusted Extensions 用户指南》	介绍了 Trusted Extensions 的基本功能。本指南包含一个词汇表。	最终用户、管理员、开发者
《Solaris Trusted Extensions Installation and Configuration for Solaris 10 11/06 and Solaris 10 8/07 Releases 》	已过时。介绍了如何为 Trusted Extensions 发行版 Solaris 10 11/06 和 Solaris 10 8/07 计划、安装和配置 Trusted Extensions。	管理员、开发者
《Oracle Solaris Trusted Extensions 配置指南》	从 Solaris 10 5/08 发行版开始，介绍了如何启用和初始配置 Trusted Extensions。取代了《Solaris Trusted Extensions Installation and Configuration》。	管理员、开发者
《Oracle Solaris Trusted Extensions 管理员规程》	说明了如何执行特定的管理任务。	管理员、开发者
《Trusted Extensions Developer's Guide》	说明了如何使用 Trusted Extensions 来开发应用程序。	开发者、管理员
《Trusted Extensions Label Administration》	提供了有关如何在标签编码文件中指定标签组件的信息。	管理员
《Compartmented Mode Workstation Labeling: Encodings Format 》	介绍了标签编码文件中使用的语法。该语法实施各种规则来为系统实现良构的标签。	管理员

相关的安装指南

下列指南包含准备 Trusted Extensions 软件时非常有用的信息。

《Oracle Solaris 10 8/11 Installation Guide: Basic Installations 》－提供有关 Solaris OS 安装选项的指导

《Oracle Solaris 10 8/11 Installation Guide: Custom JumpStart and Advanced Installations》－提供有关安装方法和配置选项的指导

《Oracle Solaris 10 8/11 Installation Guide: Planning for Installation and Upgrade》－提供有关安装 Solaris OS 升级版本的指导

相关的参考文档

您站点的安全策略文档—介绍您站点的安全策略以及安全规程

《Solaris 公用桌面环境：高级用户和系统管理员指南》－介绍公用桌面环境 (Common Desktop Environment, CDE)

当前所安装操作系统的管理员指南—介绍如何备份系统文件

相关的第三方 Web 站点引用

本文档引用了第三方 URL 以提供其他相关信息。

注 – Oracle 对本文档中提到的第三方 Web 站点的可用性不承担任何责任。对于此类站点或资源中的（或通过它们获得的）任何内容、广告、产品或其他资料，Oracle 并不表示认可，也不承担任何责任。对于因使用或依靠此类站点或资源中的（或通过它们获得的）任何内容、产品或服务而造成的或连带产生的实际或名义损坏或损失，Oracle 概不负责，也不承担任何责任。

文档、支持和培训

有关其他资源，请参见以下 Web 站点：

- 文档 (http://www.oracle.com/technetwork/indexes/documentation/index.html)
- 支持 (http://www.oracle.com/us/support/systems/index.html)
- 培训 (http://www.oracle.com/global/us/education/sun_select_country.html)－选择相应的国家/地区以查看先前的 Sun 产品的培训信息。

Oracle 软件资源

Oracle Technology Network (http://www.oracle.com/technetwork/index.html)（Oracle 技术网）提供了与 Oracle 软件相关的各种资源：

- 可在 Discussion Forums (http://forums.oracle.com)（讨论论坛）上讨论技术问题和解决方案。
- 从 Oracle 示例 (http://www.oracle.com/technology/obe/start/index.html)获取实际操作的逐步教程。
- 下载样例代码 (http://www.oracle.com/technology/sample_code/index.html)。

印刷约定

下表介绍了本书中的印刷约定。

表 P–1 印刷约定

字体或符号	含义	示例
AaBbCc123	命令、文件和目录的名称；计算机屏幕输出	编辑 .login 文件。 使用 ls -a 列出所有文件。 machine_name% you have mail.
AaBbCc123	用户键入的内容，与计算机屏幕输出的显示不同	machine_name% **su** Password:
aabbcc123	要使用实名或值替换的命令行占位符	删除文件的命令为 rm *filename*。
AaBbCc123	保留未译的新词或术语以及要强调的词	这些称为 *Class* 选项。 **注意**：有些强调的项目在联机时以粗体显示。
新词术语强调	新词或术语以及要强调的词	**高速缓存**是存储在本地的副本。 请**勿**保存文件。
《书名》	书名	阅读《用户指南》的第 6 章。

命令中的 shell 提示符示例

下表显示了 Oracle Solaris OS 中包含的缺省 UNIX shell 系统提示符和超级用户提示符。请注意，在命令示例中显示的缺省系统提示符可能会有所不同，具体取决于 Oracle Solaris 发行版。

表 P–2 shell 提示符

shell	提示符
Bash shell、Korn shell 和 Bourne shell	`$`
Bash shell、Korn shell 和 Bourne shell 超级用户	`#`
C shell	`machine_name%`
C shell 超级用户	`machine_name#`

◆ ◆ ◆ 第 1 章

1 Trusted Extensions 的安全规划

Oracle Solaris 的 Trusted Extensions 功能可以在软件中实施您站点的部分安全策略。本章概述了配置软件时安全和管理方面的任务。

在 Trusted Extensions 中规划安全

本节概述了启用和配置 Trusted Extensions 软件之前所需的规划。

有关 Trusted Extensions 配置任务的核对表，请参见附录 C，Trusted Extensions 的配置核对表。如果有兴趣将您的站点本地化，请参见第 21 页中的 “对于 Trusted Extensions 的国际客户”。如果想运行 evaluated configuration（评估配置），请参见第 20 页中的 “了解站点的安全策略”。

了解 Trusted Extensions

启用和配置 Trusted Extensions 包括加载可执行文件、指定站点数据及设置配置变量等多项操作。这需要具备大量的背景知识。Trusted Extensions 软件提供了一个基于以下两种 Oracle Solaris 功能的有标签环境：

- 在大多数 UNIX 环境中指定给超级用户的功能，可由不同的管理角色处理。
- 可将忽略安全策略的功能指定给特定用户和应用程序。

在 Trusted Extensions 中，是由特殊的安全标记来控制数据访问的。这些标记称为标签。标签指定给用户、进程和对象（如数据文件和目录）。除了 UNIX 权限或自主访问控制 (discretionary access control, DAC) 之外，这些标签还可以提供 mandatory access control（强制访问控制）。

了解站点的安全策略

通过 Trusted Extensions，可以有效地将站点的安全策略与 Oracle Solaris OS 进行集成。因此，您需要深入了解策略的范围以及 Trusted Extensions 软件如何实施该策略。经过良好规划的配置必须在以下两点之间取得平衡：站点安全策略一致性和用户在系统上执行操作的便利性。

缺省情况下，Trusted Extensions 配置为针对以下保护配置文件遵守信息技术安全评估通用准则 (ISO/IEC 15408) 保证级别 EAL4：

- 有标签的安全保护配置文件
- 受控访问保护配置文件
- 基于角色的存取控制保护配置文件

要符合这些评估级别，必须将 LDAP 配置为命名服务。请注意，如果执行以下任一一项操作，您的配置可能会不再符合评估标准：

- 更改 `/etc/system` 文件中的内核切换设置。
- 关闭审计或设备分配。
- 更改以下可配置文件中的缺省条目：
  - `/usr/openwin/server/etc/*`
  - `/usr/dt/app-defaults/C/Dt`
  - `/usr/dt/app-defaults/C/Dtwm`
  - `/usr/dt/app-defaults/C/SelectionManager`
  - `/usr/dt/bin/Xsession`
  - `/usr/dt/bin/Xtsolsession`
  - `/usr/dt/bin/Xtsolusersession`
  - `/usr/dt/config/sel_config`
  - `/usr/X11/lib/X11/xserver/TrustedExtensionsPolicy`

有关更多信息，请参见通用准则 Web 站点 (`http://www.commoncriteriaportal.org/`)。

设计 Trusted Extensions 的管理策略

root 用户或系统管理员角色负责启用 Trusted Extensions。您可以创建多个角色来划分多个功能区域之间的管理职责：

- security administrator（安全管理员）负责执行与安全相关的任务，例如设置和指定敏感标签、配置审计以及设置口令策略。
- system administrator（系统管理员）负责非安全方面的设置、维护及常规管理。
- primary administrator（主管理员）负责为安全管理员创建 rights profile（权限配置文件），并在安全管理员和系统管理员没有足够特权的情况下解决各种问题。
- 还可以配置更多受限制的角色。例如，操作员可以负责备份文件。

作为管理策略的一部分，需要确定以下内容：

- 哪些用户执掌哪些管理职责
- 允许哪些非管理用户运行可信应用程序，即允许哪些用户在必要时忽略安全策略
- 哪些用户可以访问哪些数据组

设计标签策略

规划标签需要设置敏感度级别的分层结构和系统信息的分类。label_encodings 文件包含您站点的此类信息。您可以使用随 Trusted Extensions 软件提供的 label_encodings 文件之一。也可以修改所提供的某个文件，或者创建新的特定于您的站点的 label_encodings 文件。该文件必须包含特定于 Oracle 的本地扩展，至少包含 COLOR NAMES 部分。

注意 – 如果由您提供 label_encodings 文件，应在系统验证标签之前准备好最终版本的文件。该文件应位于可移除介质上。在启用 Trusted Extensions 服务后执行首次引导期间验证标签。

规划标签还包括规划标签配置。启用 Trusted Extensions 服务后，需要决定系统是必须允许用户采用几个标签登录，还是可以配置为只使用一个用户标签。例如，LDAP 服务器适合采用一个标签区域。对于本地管理服务器的工作，可以创建一个采用最小标签的区域。管理系统时，管理员先登录，然后从用户工作区获取相应角色。

有关更多信息，请参见《Trusted Extensions Label Administration》。另请参阅《Compartmented Mode Workstation Labeling: Encodings Format》。

对于 Trusted Extensions 的国际客户

在本地化 label_encodings 文件时，国际客户必须只本地化标签名称。不得将管理标签名称 ADMIN_HIGH 和 ADMIN_LOW 本地化。所联系的所有带标签主机（不论来自何供应商），其标签名称都必须与 label_encodings 文件中的标签名称一致。

Trusted Extensions 支持的语言环境比 Oracle Solaris OS 少。当您在 Trusted Extensions 不支持的语言环境中操作时，特定于 Trusted Extensions 的文本（例如，有关标签的错误消息）不会转换为当前使用的语言环境。Oracle Solaris 软件会继续被转换为您使用的语言环境。

规划 Trusted Extensions 的系统硬件和容量

系统硬件包括系统本身及其连接设备。此类设备包括磁带机、麦克风、CD-ROM 驱动器以及磁盘组。硬件容量包括系统内存、网络接口以及磁盘空间。

- 按照安装 Oracle Solaris 发行版的建议进行操作，如《Solaris 10 5/09 Installation Guide: Basic Installations》中的"System Requirements and Recommendations"中所述。
- 以下建议适用于 Trusted Extensions 功能：
  - 在以下系统上运行所需的内存要超出最小建议内存：
    - 运行 Solaris Management Console（一种必需的管理 GUI）的系统
    - 在多个敏感标签下运行的系统
    - 可担任管理角色的用户所使用的系统
  - 在以下系统上运行需要更大的磁盘空间：
    - 在多个标签存储文件的系统
    - 其用户可承担管理角色的系统

规划可信网络

有关规划网络硬件方面的帮助，请参见《System Administration Guide: IP Services》中的第 2 章 "Planning Your TCP/IP Network (Tasks)"。

与在任意客户机/服务器网络中一样，您需要按功能为主机（即服务器或客户机）添加标签并配置相应的软件。有关规划的帮助，请参见《Solaris 10 5/09 Installation Guide: Custom JumpStart and Advanced Installations》。

Trusted Extensions 软件识别两种主机类型：有标签主机和无标签主机。每种主机类型均具有缺省的安全模板，如表 1–1 中所示。

表 1–1 Trusted Extensions 中的缺省主机模板

主机类型	模板名称	用途
`unlabeled`	`admin_low`	用于标识可与全局区域通信的不可信主机。这类主机发送不含标签的数据包。有关更多信息，请参见unlabeled system（无标签系统）。
`cipso`	`cipso`	用于标识发送 CIPSO 包的主机或网络。CIPSO 包带有标签。

如果其他网络可以连接到您所在的网络，则需要指定可访问的域和主机。还需要确定将哪些 Trusted Extensions 主机用作网关。您需要为这些网关确定标签的 accreditation range（认可范围），还需要确定可以查看其他主机数据的 sensitivity label（敏感标签）。

`smtnrhtp(1M)` 手册页提供了每种主机类型的完整说明，并附有多个示例。

在 Trusted Extensions 中规划区域

将 Trusted Extensions 软件添加到全局区域中的 Oracle Solaris OS。然后配置有标签的非全局区域。您可以为每个唯一标签创建一个有标签区域，但是不需要为 `label_encodings` 文件中的每个标签创建区域。

配置网络是区域配置的一部分。缺省情况下，会将有标签区域配置为与全局区域通信。另外，也可以将系统上的区域配置为与网络上的其他区域通信。

- 运行桌面显示的 X 服务器只能在全局区域使用。从 Solaris 10 10/08 发行版开始，可以使用回送接口 `lo0` 与全局区域通信。因此，非全局区域可通过 `lo0` 使用桌面显示。
- 缺省情况下，非全局区域不能与不可信主机通信。从 Solaris 10 10/08 发行版开始，可以将每个具有唯一缺省路由的非全局区域配置为不使用全局区域。

Trusted Extensions 区域和 Oracle Solaris 区域

有标签区域与典型的 Oracle Solaris 区域不同。有标签区域主要用于分离数据。在 Trusted Extensions 中，一般用户无法远程登录到有标签区域。到有标签区域的唯一交互接口是通过使用区域控制台。只有 root 用户才能访问区域控制台。

Trusted Extensions 中的区域创建

要创建有标签区域，需要复制整个 Oracle Solaris OS，然后在每个区域中启动 Oracle Solaris OS 的服务。该过程可能会相当耗时。较快的步骤是先创建一个区域，然后复制该区域或克隆该区域的内容。下表介绍了在 Trusted Extensions 中创建区域的选项。

区域创建方法	所需操作	方法特点
从头创建每个有标签区域。	配置、初始化、安装、定制和引导每个有标签区域。	■ 此方法受支持，并且在创建一个或两个额外区域时非常有用。可以对这些区域进行升级。 ■ 此方法相当耗时。

区域创建方法	所需操作	方法特点
通过第一个有标签区域的副本创建其他有标签区域。	配置、初始化、安装和定制一个区域。将此区域用作其他有标签区域的模板。	■ 此方法受支持，并且比从头创建区域的速度要快。可以对这些区域进行升级。如果希望 Oracle 技术支持帮助您解决区域问题，请使用“复制区域”方法。 ■ 此方法使用 UFS。UFS 不为区域提供 Oracle Solaris ZFS 所提供的附加隔离。
通过第一个有标签区域的 ZFS 快照创建其他有标签区域。	从在 Oracle Solaris 安装期间留出的分区设置 ZFS 池。 配置、初始化、安装和定制一个区域。将此区域用作其他有标签区域的 ZFS 快照。	■ 此方法使用 Oracle Solaris ZFS，是最快的方法。此方法将每个区域作为一个文件系统，因此可以比 UFS 提供更多的隔离。ZFS 使用很少的磁盘空间。 ■ 如果要测试 Trusted Extensions 并且可以重新安装区域（而不是升级），此方法可能是一个很好的选择。此方法在其内容不易失的系统上可能非常有用，因为该类系统可以快速重新安装至可用状态。 ■ 此方法**不**受支持。使用此方法创建的区域在更新版本的 OS 发布后**无法升级**。

Oracle Solaris 区域影响软件包的安装和修补。有关更多信息，请参见下列参考：

- 《System Administration Guide: Oracle Solaris Containers-Resource Management and Oracle Solaris Zones》中的第 25 章 “About Packages and Patches on a Solaris System With Zones Installed (Overview)”
- Solaris Zones 和 Solaris Containers 常见问题解答 (`http://hub.opensolaris.org/bin/view/Community+Group+zones/faq`)

规划多级别访问

通常，会将打印和 NFS 配置为多级别服务。要访问多级别服务，正确配置的系统要求每个区域都能够访问一个或多个网络地址。以下配置可提供多级别服务：

- **独占 IP 栈 –** 如同在 Oracle Solaris OS 中一样，为每个区域（包括全局区域）指定一个 IP 地址。缺省情况下，为每个有标签区域创建虚拟网络信息卡 (Virtual Network Information Card, VNIC)。

  此配置的精细之处是为每个区域指定一个单独的网络信息卡 (network information card, NIC)。这种配置可用于使用物理方式分离与每个 NIC 关联的单标签网络。

- **共享 IP 栈** – 指定一个 `all-zones` 地址。在此配置下，系统不能为多级别 NFS 服务器。一个或多个区域可以具有特定于区域的地址。

符合以下两种情况的系统无法提供多级别服务：

- 指定一个 IP 地址，全局区域和有标签区域将共享该地址。
- 没有指定任何特定于区域的地址。

提示 – 如果不允许有标签区域中的用户访问本地多级别打印机，并且不需要起始目录的 NFS 导出，则可以为配置有 Trusted Extensions 的系统指定一个 IP 地址。在此类系统上，不支持多级别打印，而且无法共享起始目录。这种配置通常是在手提电脑上使用。

在 Trusted Extensions 中规划 LDAP 命名服务

如果您不打算安装有标签系统的网络，则可以跳过本节。

如果您打算在系统的网络上运行 Trusted Extensions，则请将 LDAP 用作命名服务。对于 Trusted Extensions，配置系统网络时，需要已置备的 Sun Java System Directory Server（LDAP 服务器）。如果您的站点具备现有的 LDAP 服务器，则可以使用 Trusted Extensions 数据库置备该服务器。要访问该服务器，请在 Trusted Extensions 系统上设置 LDAP 代理。

如果您的站点没有现有的 LDAP 服务器，则在运行 Trusted Extensions 软件的系统上创建一个 LDAP 服务器。第 5 章，为 Trusted Extensions 配置 LDAP（任务）中介绍了相关步骤。

在 Trusted Extensions 中规划审计

缺省情况下，会在安装 Trusted Extensions 时启用审计。因此，缺省情况下，会审计 `root` 登录、屏幕锁定和注销。要审计负责配置系统的用户，可以在配置过程早期创建角色。当这些角色对系统进行配置时，审计记录会包含承担相应角色的登录用户。请参见第 82 页中的 “在 Trusted Extensions 中创建角色和用户”。

在 Trusted Extensions 中规划审计与在 Oracle Solaris OS 中规划审计一样。有关详细信息，请参见《System Administration Guide: Security Services》中的第 VII 部分, “Auditing in Oracle Solaris”。当 Trusted Extensions 添加类、事件和审计标记时，软件不会更改审计的管理方式。对于要审计的 Trusted Extensions 添加项，请参见《Oracle Solaris Trusted Extensions 管理员规程》中的第 18 章 “Trusted Extensions 审计（概述）”。

在 Trusted Extensions 中规划用户安全

Trusted Extensions 软件为用户提供了合理的安全缺省值。表 1–2 中列出了这些安全缺省值。如果列出了两个值，则第一个值为缺省值。安全管理员可以修改这些缺省值以反映站点的安全策略。设置缺省值后，安全管理员可以创建继承这些已建立缺省值的所有用户。有关这些缺省值的关键字和值的说明，请参见 `label_encodings(4)` 和 `policy.conf(4)` 手册页。

表 1–2 Trusted Extensions 用户帐户安全缺省值

文件名	关键字	值
`/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`
`/etc/security/tsol/label_encodings` 的 LOCAL DEFINITIONS 部分	缺省用户安全许可	`CNF: INTERNAL USE ONLY`（CNF：仅供内部使用）
	缺省用户敏感标签	`PUBLIC`

注 – `IDLECMD` 和 `IDLETIME` 变量应用于登录用户的会话。如果登录用户获取了角色，则用户的 `IDLECMD` 和 `IDLETIME` 值将对该角色生效。

系统管理员可以设置一个标准用户模板，该模板可为每个用户设置适当的系统缺省值。例如，缺省情况下每个用户的初始 shell 为 Bourne shell。系统管理员可以设置一个为每个用户提供一个 C shell 的模板。有关更多信息，请参见适用于用户帐户的 Solaris Management Console 联机帮助。

设计 Trusted Extensions 的配置策略

允许 root 用户配置 Trusted Extensions 软件不是一项安全的策略。下面按从最安全到最不安全的顺序介绍了配置策略：

- 两人团队合作配置软件。审计配置过程。

  启用软件时有两个人在计算机上。在配置过程的早期阶段，此团队可以创建角色以及可担任这些角色的本地用户。该团队还可以设置审计来审计角色执行的事件。为用户指定角色且重新引导计算机后，软件会按角色强制划分任务。审计迹可提供配置过程的记录。有关安全配置过程的说明，请参见图 1–1。

  注 – 如果站点安全要求 separation of duty（职责分离），则可信管理员会在创建用户或角色之前完成第 82 页中的 “创建实施职责分离的权限配置文件”。在此定制配置中，由一个角色管理安全性，包括用户的安全属性。另一个角色管理系统和用户的非安全属性。

- 一个人通过指定适当的角色来启用和配置软件。审计配置过程。

  在配置过程的早期阶段，root 用户创建一个本地用户和角色。此用户还可以设置审计来审计角色执行的事件。为本地用户指定角色且重新引导计算机后，软件即会按角色强制划分任务。审计迹可提供配置过程的记录。

- 一个人通过指定适当的角色来启用和配置软件。不审计配置过程。

  通过使用此策略，不会记录配置过程。

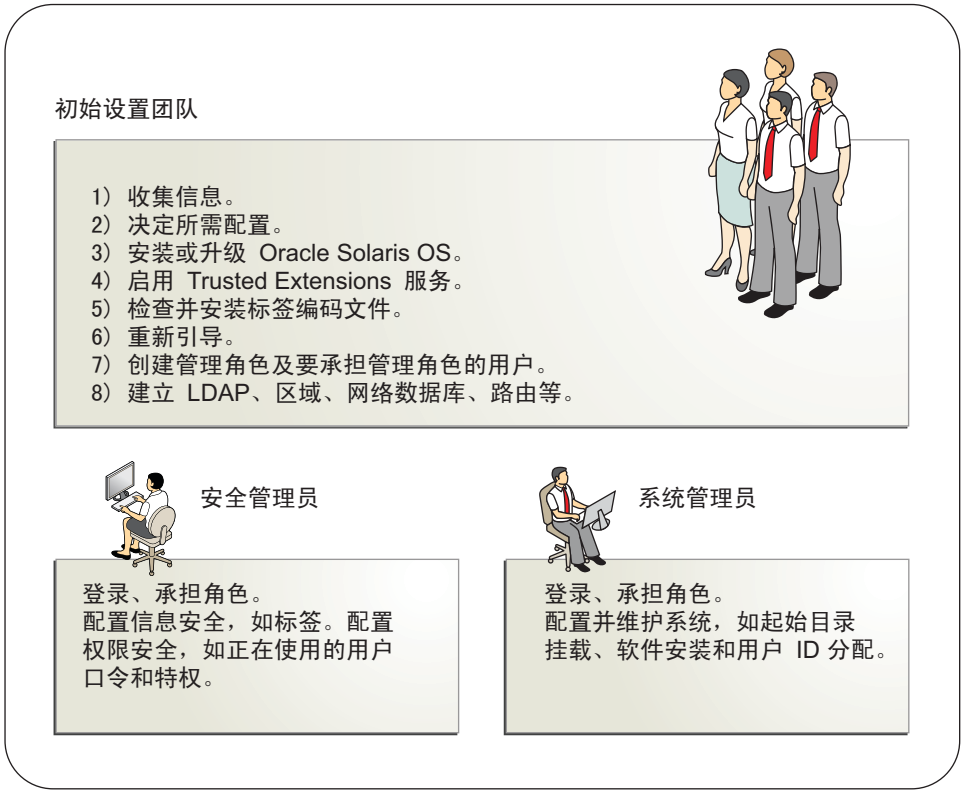
- root 用户启用并配置软件。审计配置过程。

  该团队设置审计以审计 root 在配置期间执行的每个事件。若使用此策略，团队必须确定要审计的事件。审计迹不包括充当 root 的用户的名称。

- root 用户启用并配置软件。

下图显示了根据角色的任务划分。安全管理员需要执行以下任务：配置审计、保护文件系统、设置设备策略、确定哪些程序需要运行特权、保护用户以及其他任务。系统管理员需要执行以下任务：共享和挂载文件系统、安装软件包、创建用户以及其他任务。

图 1–1 管理 Trusted Extensions 系统：按角色任务划分



在启用 Trusted Extensions 之前解决其他问题

配置 Trusted Extensions 之前，必须采取物理措施保护系统，决定将哪些标签附加到区域并解决其他安全问题。有关过程的信息，请参见第 40 页中的 “在启用 Trusted Extensions 之前收集信息并做出决定”。

在启用 Trusted Extensions 之前备份系统

如果系统中存在必须保存的文件，请在启用 Trusted Extensions 服务之前执行备份。最安全的备份文件方法是执行 0 级转储。如果没有执行适当的备份过程，请参见当前操作系统的管理员指南查看相关说明。

启用 Trusted Extensions 的结果（从管理员角度）

启用 Trusted Extensions 软件且重新引导系统后，以下安全功能即可实现。许多功能可由安全管理员进行配置。

- 启用审计。
- 安装并配置 Oracle label_encodings file（label_encodings 文件）。
- 添加两个可信桌面。Solaris Trusted Extensions (CDE) 是 CDE 的可信版本。Solaris Trusted Extensions (JDS) 是 Oracle Java Desktop System 的可信版本。每个窗口环境都会在全局区域中创建 "Trusted Path"（可信路径）工作区。
- 如同在 Oracle Solaris OS 中一样，定义角色的权限配置文件。如同在 Oracle Solaris OS 中一样，不定义角色。

  要使用角色管理 Trusted Extensions，必须创建角色。在配置期间，请创建安全管理员角色。
- 添加三个 Trusted Extensions 网络数据库 `tnrhdb`、`tnrhtp` 和 `tnzonecfg`。通过在 Solaris Management Console 中使用 "Security Templates"（安全模板）工具和 "Trusted Network Zones"（可信网络区域）工具管理这些数据库。
- Trusted Extensions 提供了 GUI 以管理系统。某些 GUI 是 Oracle Solaris GUI 的扩展。
  - 在 Trusted CDE 中，Trusted_Extensions 文件夹中提供了管理操作。其中一些操作是在初始配置 Trusted Extensions 时使用的。《Oracle Solaris Trusted Extensions 管理员规程》中的第 2 章 “Trusted Extensions 管理工具”介绍了这些工具。
  - 通过 `txzonemgr` 脚本，管理员可以配置 Trusted Extensions 区域和网络。有关更多信息，请参见 `txzonemgr(1M)` 手册页。
  - 通过 trusted editor（可信编辑器），管理员可以修改本地管理文件。在 Trusted CDE 中，"Admin Editor"（管理编辑器）操作可调用可信编辑器。
  - 设备分配管理器负责管理连接的设备。
  - Solaris Management Console 提供了基于 Java 的工具，用于管理本地和网络管理数据库。管理可信网络、区域和用户时需要使用这些工具。

◆ ◆ ◆ 第 2 章

Trusted Extensions 的配置任务列表

本章概述了为启用和配置 Trusted Extensions 软件所需执行的各项任务。

任务列表：准备 Solaris 系统以使用 Trusted Extensions

请确保您计划要在其上运行 &ProductShort 的 Solaris OS 支持您计划要使用的 Trusted Extensions 功能。完成以下任务列表所描述的一项任务。

任务	参考
准备现有的或升级的 Solaris 安装以使用 Trusted Extensions。	第 38 页中的 “准备已安装的 Solaris 系统以使用 Trusted Extensions”
将 Solaris OS 与您考虑要使用的 Trusted Extensions 功能安装在一起。	第 38 页中的 “安装 Solaris 系统以支持 Trusted Extensions”

任务列表：准备和启用 Trusted Extensions

要在配置前准备 Trusted Extensions 系统，请完成以下任务列表中描述的任务。

任务	参考
完成 Solaris 系统的准备。	第 31 页中的 “任务列表：准备 Solaris 系统以使用 Trusted Extensions”
对系统进行备份。	对于 Trusted Solaris 8 系统，请按发行版文档中的描述来备份系统。有标签的备份可还原到与其具有相同标签的区域。
	对于 Solaris 系统，请参见《系统管理指南：基本管理》。
收集信息，然后针对您的系统和 Trusted Extensions 网络做出决策。	第 40 页中的 “在启用 Trusted Extensions 之前收集信息并做出决定”

任务	参考
启用 Trusted Extensions。	第 43 页中的 “启用 Trusted Extensions”
配置系统。	对于有监视器的系统，请参见第 32 页中的 “任务列表：配置 Trusted Extensions”。
	对于无显示系统，请参见第 123 页中的 “Trusted Extensions 中的无显示系统配置（任务列表）”。
	对于 Sun Ray，请参见《Sun Ray Server Software 4.1 Installation and Configuration Guide for the Solaris Operating System》。对于 Sun Ray 5 发行版，请参见 Sun Ray Server 4.2 和 Sun Ray Connector 2.2 文档 (`http://wikis.sun.com/display/SRS/Home`) Web 站点。该服务器和客户机组成了 Sun Ray 5 软件包。 要配置初始客户机-服务器通信，请参见《Oracle Solaris Trusted Extensions 管理员规程》中的“配置可信网络数据库（任务列表）”。
	对于手提电脑，请访问 OpenSolaris 社区：安全性 (`http://hub.opensolaris.org/bin/view/Community+Group+security/`) Web 页。单击 "Trusted Extensions"。在 "Laptop Configurations"（手提电脑配置）下的 Trusted Extensions 页上，单击 "`Laptop instructions`"（**手提电脑说明**）。
	要阻止网络与全局区域进行通信，请配置 `vni0` 接口。有关示例，请参见 `Laptop instructions`（**手提电脑说明**）。 从 Solaris 10 10/08 发行版开始，您无需配置 `vni0` 接口。缺省情况下，`lo0` 接口是一个 `all-zones` 接口。对于与 Trusted Extensions 一起使用的 dhcp，其他手提电脑说明同样适用。

任务列表：配置 Trusted Extensions

为实现安全的配置过程，请及早创建角色。通过角色来配置系统的任务顺序显示在下面的任务列表中。

1. 配置全局区域。

任务	参考
要求需要输入口令才能更改硬件设置，籍此来保护计算机硬件。	《System Administration Guide: Security Services》中的“Controlling Access to System Hardware”
配置标签。**必须**为您的站点配置标签。如果您打算使用缺省的 `label_encodings` 文件，则可以跳过此任务。	第 46 页中的 “检查并安装标签编码文件”
如果您运行的是 IPv6 网络，请修改 `/etc/system` 文件以便使 IP 能够识别有标签的数据包。	第 49 页中的 “在 Trusted Extensions 中启用 IPv6 网络”
如果网络节点的 CIPSO 系统解释域 (Domain of Interpretation, DOI) 与 1 不同，请在 `/etc/system` 文件中指定 DOI。	第 50 页中的 “配置系统解释域”
如果您计划使用 Solaris ZFS 快照来克隆区域，则请创建 ZFS 池。	第 51 页中的 “创建用于克隆区域的 ZFS 池”
引导以激活有标签环境。登录时，您处于全局区域中。系统的 `label_encodings` 文件将实施强制访问控制 (mandatory access control, MAC)。	第 52 页中的 “重新引导并登录到 Trusted Extensions”
初始化 Solaris Management Console。此 GUI 用来为区域添加标签及执行其他任务。	第 54 页中的 “在 Trusted Extensions 中初始化 Solaris Management Console 服务器”
创建安全管理员角色以及计划要在本地使用的其他角色。您可以像在 Solaris OS 中创建角色一样创建这些角色。 您可以推迟执行此任务，在配置过程的最后再执行。有关后果，请参见第 27 页中的 “设计 Trusted Extensions 的配置策略”。	第 82 页中的 “在 Trusted Extensions 中创建角色和用户” 第 90 页中的 “检验 Trusted Extensions 角色是否有效”

如果使用本地文件来管理系统，请跳过接下来的一组任务。

2. 配置命名服务。

	任务	参考
	如果计划使用文件来管理 Trusted Extensions，则可跳过以下任务。	不需要对文件命名服务进行配置。
	如果您具有现有的 Sun Java System Directory Server（LDAP 服务器），请将 Trusted Extensions 数据库添加到该服务器。然后，使您的第一个 Trusted Extensions 系统成为 LDAP 服务器的代理。 如果没有 LDAP 服务器，则将第一个系统配置为服务器。	第 5 章，为 Trusted Extensions 配置 LDAP（任务）
	手动为 Solaris Management Console 设置 LDAP 工具箱。工具箱可用于在网络对象中修改 Trusted Extensions 属性。	第 117 页中的 “为 LDAP 配置 Solaris Management Console（任务列表）”
	对于不是 LDAP 服务器或代理服务器的系统，请使其成为 LDAP 客户机。	第 57 页中的 “使全局区域成为 Trusted Extensions 中的客户机”
	在 LDAP 范围中，创建安全管理员角色和计划要使用的其他角色。 您可以推迟执行此任务，在配置过程的最后再执行。有关后果，请参见第 27 页中的 “设计 Trusted Extensions 的配置策略”。	第 82 页中的 “在 Trusted Extensions 中创建角色和用户” 第 90 页中的 “检验 Trusted Extensions 角色是否有效”

3. 创建有标签区域。

	任务	参考
	运行 `txzonemgr` 命令。 遵循菜单来配置网络接口，然后创建并定制第一个有标签区域。然后，复制或克隆其余的区域。	第 60 页中的 “创建有标签区域”
	或者，使用 Trusted CDE 操作。	附录 B，使用 CDE 操作在 Trusted Extensions 中安装区域
	（可选的）在成功定制所有区域后，为各个有标签区域添加特定于区域的网络地址和缺省路由。	第 74 页中的 “将网络接口和路由添加到有标签区域”

在您的环境中，以下任务可能是必需的。

4. 完成系统设置。

	任务	参考
	确定其他需要标签、一个或多个多级别端口或不同控制消息策略的远程主机。	《Oracle Solaris Trusted Extensions 管理员规程》中的“配置可信网络数据库（任务列表）”
	创建一个多级别起始目录服务器，然后自动挂载所安装的区域。	第 92 页中的 “在 Trusted Extensions 中创建起始目录”
	请先配置审计、挂载文件系统并执行其他任务，然后再允许用户登录到系统。	《Oracle Solaris Trusted Extensions 管理员规程》
	将 NIS 环境中的用户添加到 LDAP 服务器。	第 95 页中的 “将 NIS 用户添加到 LDAP 服务器”
	将主机及其有标签区域添加到 LDAP 服务器。	《Oracle Solaris Trusted Extensions 管理员规程》中的“配置可信网络数据库（任务列表）”

◆ ◆ ◆ 第 3 章

3 将 Trusted Extensions 软件添加到 Solaris OS（任务）

本章介绍了如何准备 Solaris OS 以使用 Trusted Extensions 软件。本章还介绍了在启用 Trusted Extensions 之前所需的信息，并提供了有关如何启用 Trusted Extensions 的说明。

初始设置团队的职责

Trusted Extensions 软件设计为可由两名具有不同分工的人员进行启用和配置。不过，Solaris 安装程序不执行两个角色的任务分工。任务分工是由角色来执行的。由于角色和用户都是安装之后才创建的，所以建立一个至少有两名人员的 initial setup team（初始设置团队）来负责启用和配置 Trusted Extensions 软件是一个不错的做法。

安装或升级 Solaris OS 以使用 Trusted Extensions

Solaris 安装选项的选择会影响 Trusted Extensions 的使用和安全：

- 要正确支持 Trusted Extensions，您必须安全安装基础 Solaris OS。有关影响 Trusted Extensions 的 Solaris 安装选择，请参见第 38 页中的 “安装 Solaris 系统以支持 Trusted Extensions”。
- 如果已经在使用 Solaris OS，请检查当前的配置是否符合 Trusted Extensions 的要求。有关影响 Trusted Extensions 的配置选项，请参见第 38 页中的 “准备已安装的 Solaris 系统以使用 Trusted Extensions”。

▼ 安装 Solaris 系统以支持 Trusted Extensions

此任务适用于 Solaris OS 的全新安装。如果是在进行升级，请参见第 38 页中的 “准备已安装的 Solaris 系统以使用 Trusted Extensions”。

- **安装 Solaris OS 时，请采取针对以下安装选项的建议操作。**

  这些选项遵循了 Solaris 安装问题的顺序。此表中没有提及的安装问题不会影响 Trusted Extensions。

Solaris 选项	Trusted Extensions 行为	建议的操作
NIS 命名服务 NIS+ 命名服务	Trusted Extensions 支持将文件和 LDAP 用于命名服务。对于主机名解析，可使用 DNS。	请勿选择 NIS 或 NIS+。您可以选择 "None"（无），该选项等效于文件。然后，可以对 LDAP 进行配置来与 Trusted Extensions 一起工作。
升级	Trusted Extensions 安装具有特定安全特征的有标签区域。	如果是在进行升级，则请转至第 38 页中的 “准备已安装的 Solaris 系统以使用 Trusted Extensions”。
`root` 口令	Trusted Extensions 中的管理工具要求提供口令。如果 `root` 用户没有口令，则 `root` 无法配置系统。	请提供一个 `root` 口令。请不要更改缺省的 `crypt_unix` 口令加密方式。有关详细信息，请参见《System Administration Guide: Security Services》中的“Managing Password Information”。
开发者组	Trusted Extensions 使用 Solaris Management Console 来管理网络。最终用户组和更小的组将不安装用于 Solaris Management Console 的软件包。	在计划用来管理其他系统的任何系统上，请勿安装最终用户组、核心组或精简网络组。
定制安装	因为 Trusted Extensions 会安装区域，分区中所需的磁盘空间比缺省安装所提供的要多。	选择 "Custom Install"（定制安装），然后安排分区。 请考虑为角色增加额外的交换空间。如果计划要克隆区域，请为 ZFS 池创建一个 2000 MB 大小的分区。 对于审计文件，最佳做法是创建一个专用的分区。

▼ 准备已安装的 Solaris 系统以使用 Trusted Extensions

此任务适用于已在使用中、而且计划要在其上运行 Trusted Extensions 的 Solaris 系统。此外，要在已升级的 Solaris 系统上运行 Trusted Extensions，请执行此过程。其他可能会修改已安装 Solaris 的系统的任务可在 Trusted Extensions 配置过程中完成。

开始之前 在某些 Solaris 环境中无法启用 Trusted Extensions：

- 如果您的系统是群集的一部分，则 Trusted Extensions 无法在系统上启用。
- 不支持在备用的引导环境 (boot environment, BE) 中启用 Trusted Extensions。只能在当前引导环境中启用 Trusted Extensions。

1. **如果您的系统上安装了非全局区域，则请将其删除。**

   或者，您可以重新安装 Solaris OS。如果您要重新安装 Solaris OS，则请按照第 38 页中的“安装 Solaris 系统以支持 Trusted Extensions”中的说明进行操作。

   Trusted Extensions 使用标记区域。

2. **如果您的系统没有 `root` 口令，则请创建一个。**

   Trusted Extensions 中的管理工具要求提供口令。如果 `root` 用户没有口令，则 `root` 无法配置系统。

   对于 `root` 用户，请使用缺省的 `crypt_unix` 口令加密方式。有关详细信息，请参见《System Administration Guide: Security Services》中的“Managing Password Information”。

   注 – 用户绝不要将自己的口令泄露给其他人，否则其他人随后可能会获得对该用户数据的访问权，并且无法被唯一识别或追究责任。请注意，这种泄露可能是直接的，比如用户故意将自己的口令泄露给他人；也可能是间接的，比如，因为写下了口令或选择了不安全的口令。Solaris OS 阻止使用不安全的口令，但无法阻止用户泄露自己的口令或将其写下。

3. **如果计划要使用该系统管理站点，请添加用于 Solaris Management Console 的 Solaris 软件包。**

   Trusted Extensions 使用 Solaris Management Console 来管理网络。如果您的系统安装有最终用户组或更小的组，则系统将不具有用于 Solaris Management Console 的软件包。

4. **如果已经创建了 `xorg.conf` 文件，则需要对其进行修改。**

   将以下行添加到 `/etc/X11/xorg.conf` 文件中 Module 部分的末尾。

   ```
   load "xtsol"
   ```

   注 – 缺省情况下，`xorg.conf` 文件不存在。如果该文件不存在，则无需执行任何操作。

5. **在 Solaris 10 9/09 和 Solaris 10 9/10 发行版中，如果您的系统是 Oracle Solaris Cluster 配置的一部分，您可以在群集中启用 Trusted Extensions。**

   注 – 应用程序只能在 Oracle Solaris Cluster 区域群集中运行。

有关 Trusted Extensions 对 Oracle Solaris Cluster 的支持的更多信息，请参见《Oracle Solaris Cluster Software Installation Guide》的第 7 章“创建非全局区域和区域群集”中的“如何准备将 Trusted Extensions 用于区域群集”。

6 **如果您是在升级 Trusted Extensions 系统，请在升级系统前阅读以下内容：**

- 《Solaris 10 新增功能》中的第 1 章，“Solaris 10 10/08 发行版的新增功能”
- 《Solaris 10 10/08 发行说明》

提示 – 要了解更多相关信息，可搜索字符串 `Trusted Extensions`。

---

7 **如果您计划克隆区域，请为 ZFS 池创建一个分区。**

要确定区域的创建方式，请参见第 23 页中的 “在 Trusted Extensions 中规划区域”。

8 **如果您计划在此系统上安装有标签区域，请检查您的分区是否有足够的磁盘空间用于区域。**

大部分配置有 Trusted Extensions 的系统都安装有标签区域。有标签区域需要的磁盘空间可能比所安装系统留出的磁盘空间多。

不过，某些 Trusted Extensions 系统不要求安装有标签区域。例如，多级别打印服务器、多级别 LDAP 服务器或多级别 LDAP 代理服务器不要求安装有标签区域。这些系统可能不需要额外的磁盘空间。

9 **可选添加用于角色的额外交换空间。**

Trusted Extensions 由角色进行管理。请考虑添加用于角色进程的额外交换空间。

10 **可选为审计文件专用一个分区。**

缺省情况下，Trusted Extensions 会启用审计。对于审计文件，最佳做法是创建一个专用分区。

11 **可选要运行强化的配置，请在启用 Trusted Extensions 之前运行 `netservices limited` 命令。**

```
# netservices limited
```

在启用 Trusted Extensions 之前收集信息并做出决定

对于要在其上配置 Trusted Extensions 的每个系统，您需要了解一些信息，并做出一些有关配置的决定。例如，因为您要创建有标签区域，您可能需要留出磁盘空间，以便在其中将这些区域克隆为 Solaris ZFS 文件系统。Solaris ZFS 为区域提供额外的隔离。

▼ 在启用 Trusted Extensions 之前收集系统信息

1 **确定系统的主要主机名和 IP 地址。**

主机名是主机在网络上的名称，并且是全局区域。在 Solaris 系统上，`getent` 命令会返回主机名，如下所示：

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

2 **确定有标签区域的 IP 地址指定。**

具有两个 IP 地址的系统可用作多级别服务器。具有一个 IP 地址的系统必须拥有对多级别服务器的访问权限才能打印或执行多级别任务。有关 IP 地址选项的论述，请参见第 24 页中的 “规划多级别访问”。

大多数系统要求为有标签区域使用另外的 IP 地址。例如，以下是为有标签区域使用了另外的 IP 地址的主机：

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

3 **收集 LDAP 配置信息。**

对于运行 Trusted Extensions 软件的 LDAP 服务器，您需要以下信息：

- LDAP 服务器所服务的 Trusted Extensions 域的名称
- LDAP 服务器的 IP 地址
- 将装入的 LDAP 配置文件的名称

对于 LDAP 代理服务器，您还需要用于 LDAP 代理的口令。

▼ 在启用 Trusted Extensions 之前做出系统和安全决策

对于要在其上配置 Trusted Extensions 的每个系统，请在启用此软件之前做出这些配置决策。

1 **确定系统硬件需要得到何种安全程度的保护。**

在安全站点中，已经为每个已安装 Solaris 的系统完成了这一步骤。

- 对于 SPARC 系统，已提供了 PROM 安全级别和口令。
- 对于 x86 系统，BIOS 受保护。
- 在所有系统上，通过口令保护 `root`。

2 **准备 `label_encodings` 文件。**

如果您有特定于站点的 `label_encodings` 文件，必须先检查并安装该文件，然后才能开始其他配置任务。如果您的站点没有 `label_encodings` 文件，您可使用 Oracle 提供的缺省文件。Oracle 还提供了其他 `label_encodings` 文件，您可在 `/etc/security/tsol` 目录中找到这些文件。这些 Oracle 文件是演示文件。它们可能不适合用于生产系统。

要为您的站点定制文件，请参见《Trusted Extensions Label Administration》 。

3 **基于 `label_encodings` 文件中的标签列表，制作您需要创建的有标签区域的列表。**

下表列出了缺省 `label_encodings` 文件的标签名和建议的区域名称。

标签	区域名称
PUBLIC	public
CONFIDENTIAL : INTERNAL	internal
CONFIDENTIAL : NEED TO KNOW	needtoknow
CONFIDENTIAL : RESTRICTED	restricted

为便于 NFS 挂载，特定标签的区域名称在每个系统上都必须相同。某些系统，例如多级别打印服务器，不需要安装有标签区域。但是，如果您在打印服务器上安装有标签区域，这些区域名称就必须与您网络上其他系统的区域名称相同。

4 **确定何时创建角色。**

您站点的安全策略可能要求您通过担任角色来管理 Trusted Extensions。如果是这样，或者如果您要配置系统来满足某个已评估配置的条件，您就必须在配置过程的早期阶段创建角色。

如果不要求您通过使用角色来配置系统，您可以选择作为超级用户来配置系统。这种配置方式不太安全。审计记录不会指示在配置过程中哪个用户是超级用户。超级用户可以在系统上执行所有任务，而一个角色只能执行较为有限的一组任务。因此，在通过角色执行配置时可以对配置进行更好的控制。

5 **选择区域创建方式。**

您可以从头创建区域，复制区域或克隆区域。这些方式的创建速度、磁盘空间要求和稳健性各不相同。有关权衡事项，请参见第 23 页中的 “在 Trusted Extensions 中规划区域”。

6 **规划您的 LDAP 配置。**

对于未联网系统，使用本地文件进行管理比较实际。

LDAP 是用于联网环境的命名服务。配置多个计算机时需要一个已置备的 LDAP 服务器。

- 如果您具有现有的 Sun Java System Directory Server（LDAP 服务器），您可在运行 Trusted Extensions 的系统上创建 LDAP 代理服务器。多级别代理服务器处理与无标签 LDAP 服务器的通信。
- 如果您没有 LDAP 服务器，可将运行 Trusted Extensions 软件的一个系统配置为多级别 LDAP 服务器。

7 **确定每个系统和网络的其他安全问题。**

例如，您可能会考虑下列安全问题：

- 确定哪些设备可连接到系统并可供分配使用。
- 确定可从系统访问哪些标签下的哪些打印机。
- 确定具有有限标签范围的任何系统，例如，网关系统或公用资讯服务站。
- 确定哪些有标签系统可以与无标签系统进行通信。

启用 Trusted Extensions 服务

从 Solaris 10 5/08 发行版开始，Trusted Extensions 是由服务管理工具 (service management facility, SMF) 管理的一项服务。该服务的名称是 `svc:/system/labeld:default`。缺省情况下，`labeld` 服务被禁用。

▼ 启用 Trusted Extensions

`labeld` 服务向通信端点添加标签。例如，会为以下项添加标签：

- 所有区域以及每个区域中的目录和文件
- 所有进程，包括窗口进程
- 所有网络通信

开始之前 您已完成第 37 页中的 “安装或升级 Solaris OS 以使用 Trusted Extensions”和第 40 页中的 “在启用 Trusted Extensions 之前收集信息并做出决定”中的任务。

1 **在 Solaris 系统上，启用 `labeld` 服务。**

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

`labeld` 服务向系统添加标签，并启动 Solaris 审计服务和设备分配。在光标返回到提示符之前，不要执行其他任务。

2 **验证是否已启用该服务。**

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

注 – 直到您重新引导系统后，这些标签才会出现。第 45 页中的 “在 Trusted Extensions 中设置全局区域”包括您在重新引导之前可能想要执行的任务。

故障排除 以下消息指示您运行的 Solaris 发行版不支持将 Trusted Extensions 用作一项服务：`svcs: Pattern 'labeld' doesn't match any instances`。

要在不支持 `labeld` 服务的 Solaris 系统上运行 Trusted Extensions，请按照《Solaris Trusted Extensions Installation and Configuration Guide》中的说明进行操作。

◆ ◆ ◆ 第 4 章

4 配置 Trusted Extensions（任务）

本章介绍了如何在具有监视器的系统上配置 Trusted Extensions。要正常工作，Trusted Extensions 软件要求配置以下各项内容：标签、区域、网络、可以承担角色的用户、角色和工具。

- 第 45 页中的 “在 Trusted Extensions 中设置全局区域”
- 第 60 页中的 “创建有标签区域”
- （可选的）第 74 页中的 “将网络接口和路由添加到有标签区域”
- 第 82 页中的 “在 Trusted Extensions 中创建角色和用户”
- 第 92 页中的 “在 Trusted Extensions 中创建起始目录”
- 第 95 页中的 “将用户和主机添加到现有可信网络”
- 第 97 页中的 “Trusted Extensions 配置故障排除”
- 第 100 页中的 “其他 Trusted Extensions 配置任务”

有关其他配置任务，请参见《Oracle Solaris Trusted Extensions 管理员规程》。

在 Trusted Extensions 中设置全局区域

在设置全局区域之前，必须做出有关配置的决定。有关决定的信息，请参见第 40 页中的 “在启用 Trusted Extensions 之前收集信息并做出决定”。

任务	说明	参考
保护硬件。	通过要求输入口令才能更改硬件设置，可以保护硬件。	《System Administration Guide: Security Services》中的“Controlling Access to System Hardware”
配置标签。	**必须**为您的站点配置标签。如果打算使用缺省 `label_encodings` 文件，可以跳过此步骤。	第 46 页中的 “检查并安装标签编码文件”
对于 IPv6，修改 `/etc/system` 文件。	如果您运行的是 IPv6 网络，请修改 `/etc/system` 文件以便使 IP 能够识别有标签的数据包。	第 49 页中的 “在 Trusted Extensions 中启用 IPv6 网络”

任务	说明	参考
对于值不为 1 的 DOI，修改 `/etc/system` 文件。	如果网络节点的 CIPSO 系统解释域 (Domain of Interpretation, DOI) 与 1 不同，请在 `/etc/system` 文件中指定 DOI。	第 50 页中的 “配置系统解释域”
创建 Solaris ZFS 快照的空间。	如果您计划使用 Solaris ZFS 快照来克隆区域，则请创建 ZFS 池。 如果要克隆第一个区域来创建其余有标签区域，请执行此任务。	第 51 页中的 “创建用于克隆区域的 ZFS 池”
重新引导并登录。	登录后，您将在全局区域中，这是识别和执行强制访问控制 (mandatory access control, MAC) 的环境。	第 52 页中的 “重新引导并登录到 Trusted Extensions”
初始化 Solaris Management Console。	Trusted Extensions 会将工具添加到 Solaris Management Console 中以用于管理用户、角色、区域和网络。	第 54 页中的 “在 Trusted Extensions 中初始化 Solaris Management Console 服务器”
配置 LDAP。	如果要使用 LDAP 命名服务，请设置 LDAP 服务。	第 5 章，为 Trusted Extensions 配置 LDAP（任务）
	如果已设置了 LDAP 服务，请将此系统设为 LDAP 客户机。	第 57 页中的 “使全局区域成为 Trusted Extensions 中的客户机”

▼ 检查并安装标签编码文件

您的编码文件必须与正在通信的任何 Trusted Extensions 主机兼容。

注 – Trusted Extensions 会安装缺省 `label_encodings` 文件。此缺省文件可用于演示。但是，此文件可能并不适合您使用。如果打算使用该缺省文件，可以跳过此过程。

- 如果您熟悉编码文件，可以使用以下过程。
- 如果您不熟悉编码文件，请参考《Trusted Extensions Label Administration》以了解相关的要求、过程和示例。

注意 – 在继续之前，**必须**成功安装标签，否则配置将失败。

开始之前 您是安全管理员。security administrator（安全管理员）负责编辑、检查和维护 `label_encodings` 文件。如果打算编辑 `label_encodings` 文件，请确保该文件本身可写入。有关更多信息，请参见 `label_encodings(4)` 手册页。

1. **将包含 `label_encodings` 文件的介质插入到相应的设备中。**
2. **将 `label_encodings` 文件复制到磁盘上。**

3 检查文件的语法，并使其成为活动的 **label_encodings** 文件。

- **在 Trusted JDS 中，通过命令行检查并安装该文件。**

  a. **打开终端窗口。**

  b. **运行 chk_encodings 命令。**

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

  c. **读取输出结果并执行以下操作之一：**

  - **解决错误。**

    如果命令报告了错误，**必须**先解决错误才能继续。有关帮助，请参见《Trusted Extensions Label Administration》中的第 3 章 “Making a Label Encodings File (Tasks)”

  - **使该文件成为活动的 label_encodings 文件。**

  ```
  # 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
  ```

注意 – 您的 label_encodings 文件**必须**通过 chk_encodings 测试，然后才能继续。

- **在 Trusted CDE 中，使用 "Check Encodings"（检查编码）操作。**

  a. **打开 Trusted_Extensions 文件夹。**

  在后台单击鼠标右键。

  b. **从 "Workspace"（工作区）菜单中，选择 "Applications"（应用程序）→ "Application Manager"（应用程序管理器）。**

  c. **双击 Trusted_Extensions 文件夹图标。**

  d. **双击 "Check Encodings"（检查编码）操作。**

  在对话框中键入文件的全路径名：

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

  将调用 chk_encodings 命令以检查文件的语法。结果显示在 "Check Encodings"（检查编码）对话框中。

e. **阅读 "Check Encodings"（检查编码）对话框的内容并执行以下操作之一：**

- **解决错误。**

  如果 "Check Encodings"（检查编码）操作报告了错误，**必须**先解决错误才能继续。有关帮助信息，请参见《Trusted Extensions Label Administration》中的第 3 章 “Making a Label Encodings File (Tasks)”。

- **单击 Yes（是）使该文件成为活动的 `label_encodings` 文件。**

  "Check Encodings"（检查编码）操作会创建原始文件的备份副本，然后将检查后的版本安装在 `/etc/security/tsol/label_encodings` 中。然后，该操作将重新启动标签守护进程。

注意 – 您的 `label_encodings` 文件**必须**通过 "Check Encodings"（检查编码）测试，然后才能继续。

4 **检查文件的语法，并使其成为活动的 `label_encodings` 文件。**

使用命令行。

a. **打开终端窗口。**

b. **运行 `chk_encodings` 命令。**

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

c. **读取输出结果并执行以下操作之一：**

- **解决错误。**

  如果命令报告了错误，**必须**先解决错误才能继续。有关帮助，请参见《Trusted Extensions Label Administration》中的第 3 章 “Making a Label Encodings File (Tasks)”

- **使该文件成为活动的 `label_encodings` 文件。**

```
# 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
```

注意 – 您的 `label_encodings` 文件**必须**通过 "Check Encodings"（检查编码）测试，然后才能继续。

示例 4–1 检查命令行上的 label_encodings 语法

在此示例中，管理员使用命令行来测试多个 `label_encodings` 文件。

```
# /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
```

如果管理层决定使用 label_encodings2 文件，管理员将对该文件运行语义分析。

```
# /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 <---
...
```

管理员打印其记录的语义分析副本，然后将文件移到 /etc/security/tsol 目录。

```
# 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
```

最后，管理员检验 label_encodings 文件是否为公司文件。

```
# /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
```

▼ 在 Trusted Extensions 中启用 IPv6 网络

CIPSO 选项没有 Internet 号码分配机构 (Internet Assigned Numbers Authority, IANA) 编号可供在包的 "IPv6 Option Type"（IPv6 选项类型）字段中使用。在此过程中设置的项会提供一个编号，以在本地网络上使用，直到 IANA 为此选项指定一个编号。如果未定义此编号，Trusted Extensions 将禁用 IPv6 网络。

要在 Trusted Extensions 中启用 IPv6 网络，必须在 /etc/system 文件中添加一个项。

- **将以下项键入到 /etc/system 文件中：**

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

故障排除

- 如果在引导过程中出现错误消息，指出 IPv6 配置不正确，请更正该项：
  - 检查该项的拼写是否正确。

    - 检查在将正确的项添加到 `/etc/system` 文件中后是否重新引导了系统。
- 如果在当前启用了 IPv6 的 Solaris 系统上安装 Trusted Extensions，但未能在 `/etc/system` 中添加 IP 项，则将看到以下错误消息：`t_optmgmt: System error: Cannot assign requested address` *time-stamp*（t_optmgmt: 系统错误: 不能指定所要求的地址 time-stamp）
- 如果在未启用 IPv6 的 Solaris 系统上安装 Trusted Extensions，且未能在 `/etc/system` 中添加 IP 项，则将看到以下类型的错误消息：
    - `WARNING: IPv6 not enabled via /etc/system`（警告：未通过 /etc/system 启用 IPv6）
    - `Failed to configure IPv6 interface(s): hme0`（无法配置 IPv6 接口：hme0）
    - `rpcbind: Unable to join IPv6 multicast group for rpc broadcast` *broadcast-number*（rpcbind: rpc 广播 broadcast-number 无法加入 IPv6 多播组）

▼ 配置系统解释域

与配置有 Trusted Extensions 的系统的所有往来通信都必须遵循单个 CIPSO 系统解释域 (Domain of Interpretation, DOI) 的标记规则。每条消息中使用的 DOI 由 "CIPSO IP Option"（CIPSO IP 选项）头中的整数进行标识。缺省情况下，Trusted Extensions 中的 DOI 为 `1`。

如果您的 DOI 不是 `1`，必须向 `/etc/system` 文件中添加一个项，并修改缺省安全模板中的 `doi` 值。

1 将您的 DOI 项键入到 `/etc/system` 文件中：

```
set default_doi = n
```

这个非零正数必须与节点以及节点与之通信的系统对应的 `tnrhtp` 数据库中的 DOI 编号匹配。

2 在将 `tnrhtp` 数据库添加到 LDAP 服务器之前，修改缺省项以及本地地址的所有项中的 `doi` 值。

Trusted Extensions 在 `tnrhtp` 数据库中提供两个模板，即 `cipso` 和 `admin_low`。如果您添加了本地地址的项，也请修改这些项。

a. 在可信编辑器中，打开 `tnrhtp` 数据库。

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

在 Solaris Trusted Extensions (CDE) 中，可以改用应用程序管理器 Trusted_Extensions 文件夹中的 "Admin Editor"（管理编辑器）操作。

b. 将 `cipso` 模板条目复制到另一行。

```
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. **注释掉其中一个 `cipso` 条目。**

```
#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. **修改取消注释的 `cipso` 条目中的 `doi` 值。**

使此值与 `/etc/system` 文件中的 `default_doi` 值相同。

```
#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. **更改 `admin_low` 条目的 `doi` 值。**

```
#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
```

`tnrhtp` 数据库中每个条目的 `doi` 值都相同时，表示操作完成。

故障排除 如果 `/etc/system` 文件设置的 `default_doi` 值不是 `1`，并且此系统的某个安全模板设置的值与此 `default_doi` 值不匹配，那么，在接口配置过程中，系统控制台上将显示类似如下内容的消息：

- `NOTICE: er10 failed: 10.17.1.12 has wrong DOI 4 instead of 1`（注意: er10 失败: 10.17.1.12 的 DOI 为 4 而不是 1，这是错误的）
- `Failed to configure IPv4 interface(s): er10`（无法配置 IPv4 接口：er10）

接口配置失败可能会导致登录失败：

- `Hostname: unknown`（主机名：未知）
- `unknown console login: root`（未知控制台登录：root）
- `Oct 10 10:10:20 unknown login: pam_unix_cred: cannot load hostname Error 0`（10 月 10 日 10:10:20 未知登录: pam_unix_cred: 无法装入主机名 错误 0）

要更正该问题，请将系统引导至单用户模式，并按此过程所述更正安全模板。

另请参见 有关 DOI 的更多信息，请参见《Oracle Solaris Trusted Extensions 管理员规程》中的“Trusted Extensions 中的网络安全属性”。

要在创建的安全模板中更改 `doi` 值，请参见《Oracle Solaris Trusted Extensions 管理员规程》中的“如何构造远程主机模板”。

要将您选择的编辑器用作可信编辑器，请参见《Oracle Solaris Trusted Extensions 管理员规程》中的“如何将所选的编辑器指定为可信编辑器”。

▼ 创建用于克隆区域的 ZFS 池

如果打算使用 Solaris ZFS 快照作为区域模板，您需要通过 ZFS 文件或 ZFS 设备创建 ZFS 池。此池存放用于克隆每个区域的快照。您将 `/zone` 设备用作 ZFS 池。

开始之前 您已在 Solaris 安装过程中为 ZFS 文件系统留出了磁盘空间。有关详细信息，请参见第 23 页中的 “在 Trusted Extensions 中规划区域”。

1. **卸载 /zone 分区。**

   在安装过程中，您创建了一个 /zone 分区，该分区具有大约 2000 MB 的充足磁盘空间。

   ```
   # umount /zone
   ```

2. **删除 /zone 挂载点。**

   ```
   # rmdir /zone
   ```

3. **注释掉 vfstab 文件中的 /zone 项。**

   a. **阻止读取 /zone 项。**

      在编辑器中打开 vfstab 文件。在 /zone 项前面加上注释符号。

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

   b. **将磁盘分片 c*n* t*n*d*n* s*n* 复制到粘贴板。**

   c. **保存文件，然后关闭编辑器。**

4. **使用磁盘分片重新创建 /zone 作为 ZFS 池。**

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

   例如，如果您的 /zone 项使用磁盘分片 c0t0d0s5，则命令将如下所示：

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

5. **检验 ZFS 池运行状况是否良好。**

   使用以下命令之一：

   ```
   # 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   -
   ```

   在此示例中，初始设置团队为区域保留了一个 6000 MB 的分区。有关更多信息，请参见 zpool(1M) 手册页。

▼ 重新引导并登录到 Trusted Extensions

在大多数站点，在配置系统时，会存在由两个或多个管理员组成的 initial setup team（初始设置团队）。

开始之前 在首次登录之前，请熟悉 Trusted Extensions 中的桌面和标签选项。有关详细信息，请参见《Oracle Solaris Trusted Extensions 用户指南》中的第 2 章 “登录到 Trusted Extensions（任务）”。

1 **重新引导系统。**

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

如果您的系统没有图形显示，请转至第 6 章，配置具有 Trusted Extensions 的无显示系统（任务）。

2 **以超级用户身份登录到 Solaris Trusted Extensions (CDE) 或 Solaris Trusted Extensions (JDS) 桌面。**

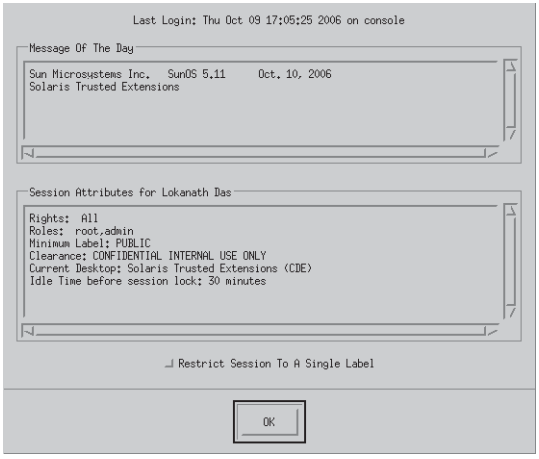
a. **在登录窗口中，选择可信桌面之一。**

Trusted CDE 桌面包含可在配置系统时使用的操作。从 Solaris 10 10/08 发行版开始，`txzonemgr` 脚本是配置系统的首选程序。

b. **在登录对话框中，键入 `root` 和超级用户口令。**

用户不得将其口令透露给他人，因为这可能会让他人有权访问用户数据，并将无法唯一标识该人，或者无法追究其责任。请注意，透露可能是直接的，即用户故意将其口令透露给他人；也可能是间接的，如将口令写下来，或者选择了不安全的口令。Trusted Extensions 软件提供了不安全口令保护，但不能防止用户透露其口令或将口令写下来。

3 **阅读 "Last Login"（上次登录）对话框中的信息。**



然后单击 "OK"（确定）关闭该对话框。

4 **查看标签生成器。**

单击 "OK"（确定）接受缺省标签。

登录过程完成后，会短暂地显示 Trusted Extensions 屏幕，然后您将处于具有四个工作区的桌面会话中。`Trusted Path`（可信路径）符号会显示在 trusted stripe（可信窗口条）中。

注 – 如果要离开系统一段时间，必须注销或锁定屏幕。否则，他人可以在未经识别和验证的情况下访问系统，并且无法唯一标识该人，或者无法追究其责任。

▼ 在 Trusted Extensions 中初始化 Solaris Management Console 服务器

通过此过程，可以管理此系统上的用户、角色、主机、区域和网络。在您配置的第一个系统上，只有 `files`（文件）作用域可用。

开始之前 您必须是超级用户。

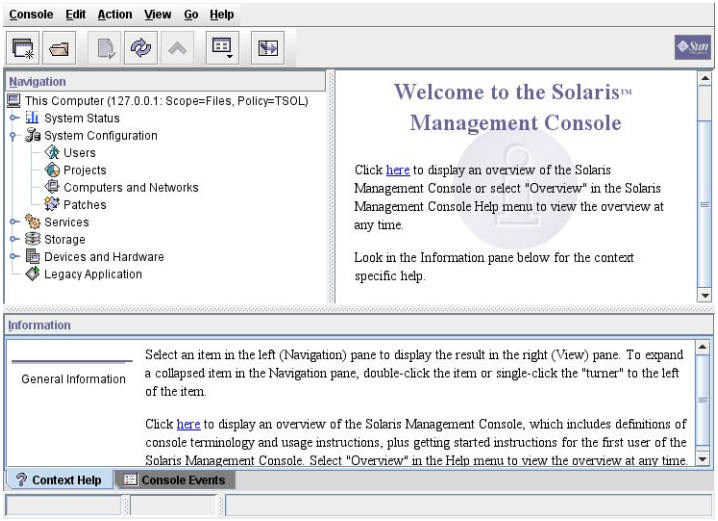
要通过客户机上运行的 Solaris Management Console 使用 LDAP 服务器上的 LDAP 工具箱，您必须完成第 117 页中的 “为 LDAP 配置 Solaris Management Console（任务列表）”中的所有任务。

1 **启动 Solaris Management Console。**

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

注 – 首次启动 Solaris Management Console 时，将执行多个注册任务。这些任务可能要花费几分钟时间。

图 4–1 Solaris Management Console 初始窗口



2 **如果 Solaris Management Console 中未出现工具箱图标，请执行以下操作之一：**

- **如果 "Navigation"（导航）窗格不可见：**

  a. **在显示的 "Open Toolbox"（打开工具箱）对话框中，单击 "Server"（服务器）下此系统名称旁边的 "Load"（装入）。**

  如果此系统不具备所建议的内存和交换量，可能需要几分钟后才能显示工具箱。有关建议，请参见第 37 页中的 “安装或升级 Solaris OS 以使用 Trusted Extensions”。

  b. **从工具箱列表中选择其 `Policy=TSOL` 的工具箱。**

  图 4–2 显示了一个 This Computer (*this-host*: `Scope=Files, Policy=TSOL`) 工具箱。Trusted Extensions 在 "System Configuration"（系统配置）节点下修改工具。

  注意 – 请勿选择没有策略的工具箱。没有列出的策略的工具箱不支持 Trusted Extensions。

  您如何选择工具箱取决于您要影响的作用域。

  - 要编辑本地文件，请选择 "Files"（文件）作用域。
  - 要编辑 LDAP 数据库，请选择 LDAP 作用域。

    完成第 117 页中的 “为 LDAP 配置 Solaris Management Console（任务列表）”中的所有任务后，LDAP 作用域即可用。

  c. **单击 "Open"（打开）。**

- **如果 "Navigation"（导航）窗格可见，但工具箱图标是停止符号：**

  a. **退出 Solaris Management Console。**

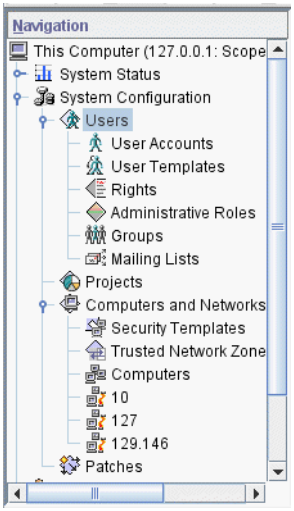
  b. **重新启动 Solaris Management Console。**

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

3. **如果您尚未这样做，请选择 `Policy=TSOL` 的工具箱。**

   下图显示了一个 This Computer (*this-host*: `Scope=Files, Policy=TSOL`) 工具箱。Trusted Extensions 在 "System Configuration"（系统配置）节点下修改工具。

   图 4–2 Solaris Management Console 中的 Trusted Extensions 工具

4. **可选保存当前工具箱。**

   保存 `Policy=TSOL` 工具箱允许在缺省情况下装入 Trusted Extensions 工具箱。首选项是按角色、按主机保存。主机为 Solaris Management Console 服务器。

   a. **从 "Console"（控制台）菜单中，选择 "Preferences"（首选项）。**

      将会选择 "Home"（起始）工具箱。

   b. **定义 `Policy=TSOL` 工具箱作为 "Home"（起始）工具箱。**

      通过单击 "Use Current Toolbox"（使用当前工具箱）按钮，将当前工具箱放入 "Location"（位置）字段。

   c. **单击 "OK"（确定）保存首选项。**

5 **退出 Solaris Management Console。**

另请参见 有关 Solaris Management Console 的 Trusted Extensions 附加内容的概述，请参见《Oracle Solaris Trusted Extensions 管理员规程》中的“Solaris Management Console 工具”。要使用 Solaris Management Console 创建安全模板，请参见《Oracle Solaris Trusted Extensions 管理员规程》中的“配置可信网络数据库（任务列表）”。

▼ 使全局区域成为 Trusted Extensions 中的客户机

对于 LDAP，此过程将建立全局区域的命名服务配置。如果不使用 LDAP，可以跳过此过程。

从 Solaris 10 5/08 发行版开始，如果您位于 Solaris Trusted Extensions (CDE) 工作区，可以使用 `txzonemgr` 脚本或 Trusted CDE 操作来创建一个 LDAP 客户机。如果您位于 Solaris Trusted Extensions (JDS) 或 Solaris Trusted Extensions (GNOME) 工作区中，必须使用 `txzonemgr` 脚本。

注 – 如果打算在每个有标签区域中设置一个名称服务器，则您要负责建立与每个有标签区域的 LDAP 客户机连接。

开始之前 Sun Java System Directory Server（即 LDAP 服务器）必须存在。该服务器必须置备有 Trusted Extensions 数据库，并且此系统必须能够与该服务器联系。因此，要配置的系统必须具有 LDAP 服务器上 `tnrhdb` 数据库中的一个项，或者此系统必须包括在通配符项中，然后再执行此过程。

如果配置有 Trusted Extensions 的 LDAP 服务器不存在，则必须完成第 5 章，为 Trusted Extensions 配置 LDAP（任务）中的过程，然后再执行此过程。

1 **如果要使用 DNS，请修改 `nsswitch.ldap` 文件。**

a. **保存原始 `nsswitch.ldap` 文件的副本。**

LDAP 的标准命名服务转换文件对 Trusted Extensions 具有过多限制。

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

b. **更改以下服务的 `nsswitch.ldap` 文件项。**

正确的项类似如下：

```
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
```

请注意，Trusted Extensions 添加了两项：

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

c. **将修改后的 `nsswitch.ldap` 文件复制到 `nsswitch.conf`。**

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

2 **执行以下步骤之一创建一个 LDAP 客户机。**

- **运行 `txzonemgr` 脚本，并应答有关 LDAP 的提示。**

  "Create LDAP Client"（创建 LDAP 客户机）菜单项仅配置全局区域。

  a. **按照第 61 页中的“运行 `txzonemgr` 脚本”中的说明操作。**

  对话框的标题是 "Labeled Zone Manager"（有标签区域管理器）。

  b. **选择 "Create LDAP Client"（创建 LDAP 客户机）。**

  c. **应答以下提示，并在每次应答后单击 "OK"（确定）：**

```
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. **确认或取消显示的值。**

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

  在确认后，`txzonemgr` 脚本将添加 LDAP 客户机。然后，将在一个窗口中显示命令输出。

- **在 Trusted CDE 工作区中，找到并使用 "Create LDAP Client"（创建 LDAP 客户机）操作。**

  a. **通过在背景上单击鼠标右键，导航到 Trusted_Extensions 文件夹。**

  b. **从 "Workspace"（工作区）菜单中，选择 "Applications"（应用程序）→ "Application Manager"（应用程序管理器）。**

c. **双击 Trusted_Extensions 文件夹图标。**
   此文件夹包含用于设置接口、LDAP 客户机和有标签区域的操作。

d. **双击 "Create LDAP Client"（创建 LDAP 客户机）操作。**
   应答以下提示：

```
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. **单击 "OK"（确定）。**
   此时将显示以下完成消息：

```
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. **关闭操作窗口。**

3 **在终端窗口中，将 enableShadowUpdate 参数设置为 TRUE。**

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

"Create LDAP Client"（创建 LDAP 客户机）操作和 `txzonemgr` 脚本仅运行 `ldapclient init` 命令。在 Trusted Extensions 中，还必须修改已初始化的 LDAP 客户机以启用投影更新。

4 **检验服务器上的信息是否正确。**

a. **打开终端窗口，查询 LDAP 服务器。**

```
# ldapclient list
```

   输出结果类似如下：

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

b. **更正所有错误。**
   如果发生了错误，请重新创建 LDAP 客户机，并提供正确的值。例如，以下错误可能表示系统没有 LDAP 服务器上的项。

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

   要更正此错误，需要检查 LDAP 服务器。

示例 4–2 在装入 resolv.conf 文件后使用主机名

在此示例中，管理员希望系统可以使用一组特定的 DNS 服务器。管理员从可信网络上的某个服务器上复制一个 `resolv.conf` 文件。因为 DNS 尚未处于活动状态，所以管理员使用服务器的 IP 地址来定位服务器。

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

在复制了 `resolv.conf` 文件，并且 `nsswitch.conf` 文件在 `hosts` 项中包含 `dns` 之后，管理员便可以使用主机名来定位系统。

创建有标签区域

`txzonemgr` 脚本会按步骤引导您完成配置有标签区域的以下所有任务。

注意 – 您必须运行 Solaris 10 8/07 发行版的 Trusted Extensions 或更高发行版才能使用 `txzonemgr` 过程。或者，必须为 Solaris 10 11/06 发行版安装所有修补程序。

如果运行的是不具有最新修补程序的 Solaris 10 11/06 发行版，请使用附录 B，使用 CDE 操作在 Trusted Extensions 中安装区域中的过程来配置有标签区域。

本节中的说明介绍在最多指定了两个 IP 地址的系统上配置有标签区域。对于其他配置，请参见第 31 页中的 “任务列表：准备和启用 Trusted Extensions”中的配置选项。

任务	说明	参考
1. 运行 `txzonemgr` 脚本。	`txzonemgr` 脚本会创建一个 GUI，用于在配置区域时提供相应的任务。	第 61 页中的 “运行 `txzonemgr` 脚本”
2. 管理全局区域中的网络接口。	配置全局区域中的接口，或者创建逻辑接口并在全局区域中对其进行配置。	第 62 页中的 “在 Trusted Extensions 中配置网络接口”
3. 命名区域并为其添加标签。	使用某一版本的区域标签命名区域，然后指定标签。	第 65 页中的 “命名区域并为其添加标签”
4. 安装并引导区域。	在区域中安装软件包。在区域中配置服务。通过 Zone Terminal Console（区域终端控制台），可以查看区域中的活动。	第 67 页中的 “安装有标签区域” 第 68 页中的 “引导有标签区域”
5. 检验区域的状态。	检验有标签区域是否在运行，以及该区域是否可与全局区域通信。	第 70 页中的 “检验区域的状态”
6. 定制区域。	从区域中删除不需要的服务。 如果要使用该区域来创建其他区域，请仅删除特定于该区域的信息。	第 71 页中的 “定制有标签区域”

任务	说明	参考
7. 创建其余区域。	使用所选择的方法创建第二个区域。有关区域创建方法的讨论，请参见第 23 页中的 “在 Trusted Extensions 中规划区域”。	第 73 页中的 “在 Trusted Extensions 中复制或克隆区域”
8.（可选的）添加特定于区域的网络接口。	要影响网络隔离，请将一个或多个网络接口添加到某个有标签区域中。通常，此类配置用于隔离有标签子网。	第 74 页中的 “将网络接口和路由添加到有标签区域”

▼ 运行 txzonemgr 脚本

此脚本会按步骤引导您正确完成配置、安装、初始化和引导有标签区域的任务。在该脚本中，您将命名每个区域，将名称与标签关联，安装软件包以创建虚拟 OS，然后引导区域以启动该区域中的服务。此脚本包含复制区域和克隆区域任务。您还可以停止某个区域，更改区域的状态，以及添加特定于区域的网络接口。

此脚本会呈现一个动态确定的菜单，其中仅显示适用于当前环境的有效选项。例如，如果已配置某个区域的状态，则不会显示 “Install zone"（安装区域）菜单项。已完成的任务不会显示在该列表中。

开始之前 您是超级用户。

如果打算克隆区域，则您已完成克隆区域的准备。如果打算使用自己的安全模板，则您已创建相应的模板。

1. **在全局区域中打开一个终端窗口。**

2. **运行 `txzonemgr` 脚本。**

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

   该脚本将打开 "`Labeled Zone Manager`"（有标签区域管理器）对话框。此 `zenity` 对话框会提示您执行相应的任务，具体取决于安装的当前状态。

   要执行某项任务，请选择相应菜单项，然后按回车键或单击 "OK"（确定）。在提示您输入文本时，键入文本，然后按回车键或单击 "OK"（确定）。

提示 – 要查看当前的区域完成状态，请在 "Labeled Zone Manager"（有标签区域管理器）中单击 "Return to Main Menu"（返回到主菜单）。

▼ 在 Trusted Extensions 中配置网络接口

注 – 如果要将系统配置为使用 DHCP，请参阅 OpenSolaris Community: Security Web 页 (`http://hub.opensolaris.org/bin/view/Community+Group+security/`)的 Trusted Extensions 部分中的手提电脑说明。

从 Solaris 10 10/08 发行版开始，如果要配置的系统中的每个有标签区域都在其自己的子网上，则可以跳过此步骤，继续第 65 页中的 “命名区域并为其添加标签”。完成区域的安装和定制后，在第 75 页中的 “添加网络接口以路由现有的有标签区域”中为每个有标签区域添加网络接口。

在此任务中，您将在全局区域中配置网络。必须仅创建一个 `all-zones` 接口。`all-zones` 接口由有标签区域和全局区域共享。共享接口用于在有标签区域和全局区域之间路由通信流量。要配置此接口，请执行以下操作之一：

- 根据某个物理接口创建一个逻辑接口，然后共享该物理接口。

  此配置管理起来最简单。如果为系统指定了两个 IP 地址，请选择此配置。在此过程中，逻辑接口将成为全局区域的特定地址，而物理接口则在全局区域和有标签区域之间共享。

- 共享物理接口

  如果为系统指定了一个 IP 地址，请选择此配置。在此配置中，物理接口在全局区域和有标签区域之间共享。

- 共享虚拟网络接口 `vni0`

  如果要配置 DHCP，或者每个子网位于不同的标签，请选择此配置。有关样例过程，请参阅 OpenSolaris Community: Security Web 页 (`http://hub.opensolaris.org/bin/view/Community+Group+security/`)的 Trusted Extensions 部分中的手提电脑说明。

  从 Solaris 10 10/08 发行版开始，Trusted Extensions 中的回送接口将创建为 all-zones 接口。因此，不需要创建 `vni0` 共享接口。

要添加特定于区域的网络接口，请完成区域创建并进行检验，然后再添加接口。有关过程，请参见第 75 页中的 “添加网络接口以路由现有的有标签区域”。

开始之前 您是全局区域中的超级用户。

将显示 "Labeled Zone Manager"（有标签区域管理器）。要打开此 GUI，请参见第 61 页中的 “运行 `txzonemgr` 脚本”。

1 在 "Labeled Zone Manager"（有标签区域管理器）中，选择 "Manage Network Interfaces"（管理网络接口），然后单击 "OK"（确定）。

此时将显示接口列表。

注 – 在此示例中，安装过程中向物理接口指定了一个主机名和一个 IP 地址。

2 **选择物理接口。**

有一个接口的系统会显示类似如下的菜单。添加了注释以提供帮助：

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

a. **选择 `eri0` 接口。**

b. **单击 "OK"（确定）。**

3 **为此网络接口选择相应的任务。**

提供了三个选项：

```
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
```

- **如果系统有一个 IP 地址，请转到步骤 4。**
- **如果系统有两个 IP 地址，请转到步骤 5。**

4 **在有一个 IP 地址的系统上，共享物理接口。**

在此配置中，主机的 IP 地址应用于所有区域。因此，主机的地址是 `all-zones` 地址。此主机不能用作多级别服务器。例如，用户不能共享此系统中的文件。该系统不能成为 LDAP 代理服务器、NFS 起始目录服务器或打印服务器。

a. **选择 "Share"（共享），然后单击 "OK"（确定）。**

b. **在显示共享接口的对话框中单击 "OK"（确定）。**

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

如果物理接口是一个 `all-zones` 接口，则说明操作成功。继续第 65 页中的 “命名区域并为其添加标签”。

5 **在有两个 IP 地址的系统中，创建一个逻辑接口。**

然后，共享物理接口。

这是最简单的 Trusted Extensions 网络配置。在此配置中，其他系统可使用主 IP 地址来访问此系统中的任何区域，而逻辑接口是全局区域的特定接口。全局区域可用作多级别服务器。

a. **选择 "Create Logical Interface"（创建逻辑接口），然后单击 "OK"（确定）。**

关闭用于确认新逻辑接口创建操作的对话框。

b. **选择 "Set IP address"（设置 IP 地址），然后单击 "OK"（确定）。**

c. **出现提示时，指定逻辑接口的主机名，然后单击 "OK"（确定）。**
   例如，指定 machine1-services 作为逻辑接口的主机名。该名称指示此主机提供多级别服务。

d. **出现提示时，指定逻辑接口的 IP 地址，然后单击 "OK"（确定）。**
   例如，指定 10.10.9.2 作为逻辑接口的 IP 地址。

e. **再次选择逻辑接口，然后单击 "OK"（确定）。**

f. **选择 "Bring Up"（初启），然后单击 "OK"（确定）。**
   该接口将显示为 Up（启用）。

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

g. **共享物理接口。**

   i. **选择物理接口，然后单击 "OK"（确定）。**

   ii. **选择 "Share"（共享），然后单击 "OK"（确定）。**

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

如果至少一个接口是 all-zones 接口，则说明操作成功。

示例 4–3 在有共享逻辑接口的系统上查看 /etc/hosts 文件

在全局区域有唯一接口并且有标签区域与全局区域共享另一个接口的系统上，/etc/hosts 文件的内容类似如下：

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

在缺省配置中，tnrhdb 文件的内容类似如下：

```
# 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
```

如果 all-zones 接口不在 tnrhdb 文件中，则该接口缺省为 cipso。

示例 4–4 在有一个 IP 地址的 Trusted Extensions 系统上显示共享接口

在此示例中，管理员不打算将系统用作多级别服务器。为了节省 IP 地址，将全局区域配置为与每个有标签区域共享其 IP 地址。

管理员为系统上的 `hme0` 接口选择 "Share"（共享）。软件将所有区域配置为具有逻辑 NIC。这些逻辑 NIC 在全局区域中共享一个物理 NIC。

管理员运行 **`ifconfig -a`** 命令来检验网络接口 `192.168.0.11` 上的物理接口 `hme0` 是否已共享。显示的值为 `all-zones`：

```
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
```

从 Solaris 10 10/08 发行版开始，Trusted Extensions 中的回送接口将创建为 all-zones 接口。

```
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
```

管理员还会检查 `/etc/hostname.hme0` 文件的内容。

```
192.168.0.11 all-zones
```

▼ 命名区域并为其添加标签

您不必为 `label_encodings` 文件中的每个标签创建一个区域，但您可以这样做。管理 GUI 会枚举可在此系统上为其创建区域的标签。

开始之前 您是全局区域中的超级用户。将显示 "Labeled Zone Manager"（有标签区域管理器）对话框。要打开此 GUI，请参见第 61 页中的 “运行 txzonemgr 脚本”。您已在全局区域中配置了网络接口。

您已创建了所需的任何安全模板。除了定义其他属性外，安全模板还定义可指定给网络接口的标签范围。缺省安全模板可能会满足您的需要。

- 有关安全模板的概述，请参见《Oracle Solaris Trusted Extensions 管理员规程》中的“Trusted Extensions 中的网络安全属性”。
- 要使用 Solaris Management Console 创建安全模板，请参见《Oracle Solaris Trusted Extensions 管理员规程》中的“配置可信网络数据库（任务列表）”。

1 **在 Labeled Zone Manager（有标签区域管理器）中，选择 "Create a new zone"（新建区域），然后单击 "OK"（确定）。**

此时会提示您输入名称。

a. 键入区域的名称。

提示 – 为区域指定一个与区域标签类似的名称。例如，标签为 CONFIDENTIAL: RESTRICTED（机密：受限）的区域的名称为 restricted（受限）。

例如，缺省 label_encodings 文件包含以下标签：

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

虽然可以每个标签创建一个区域，但是请考虑创建下面的区域：

- 在适用于所有用户的系统上，为 PUBLIC 标签创建一个区域，为 CONFIDENTIAL 标签创建三个区域。
- 在适用于开发者的系统上，为 SANDBOX: PLAYGROUND 标签创建一个区域。对于开发者而言，由于 SANDBOX: PLAYGROUND 定义为不相交标签，所以只有开发者使用的系统需要此标签对应的区域。
- 不要为 MAX LABEL 标签创建区域，该标签定义为安全许可。

b. 单击 "OK"（确定）。

对话框会在任务列表上方显示 *zone-name* :configured（zone-name：已配置）。

2 **要标记区域，请选择以下操作过程之一：**

- **如果要使用定制的 label_encodings 文件，请使用 "Trusted Network Zones"（可信网络区域）工具来标记区域。**

  a. 在 Solaris Management Console 中打开 "Trusted Network Zones"（可信网络区域）工具。

  i. 启动 Solaris Management Console。

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

  ii. 打开本地系统的 Trusted Extensions 工具箱。

  选择 "Console"（控制台）→"Open Toolbox"（打开工具箱）。

选择名为 **This Computer (***this-host***: `Scope=Files, Policy=TSOL`)** 的工具箱。

单击 **"Open"（打开）**。

iii. **在 "System Configuration"（系统配置）下，导航到 "Computers and Networks"（计算机和网络）。**
在出现提示时提供口令。

iv. **双击 "Trusted Network Zones"（可信网络区域）工具。**

b. **对于每个区域，将相应的标签与区域名称相关联。**

i. **选择 "Action"（操作）→"Add Zone Configuration"（添加区域配置）。**
该对话框将显示没有指定的标签的区域名称。

ii. **查看区域名称，然后单击 "Edit"（编辑）。**

iii. **在标签生成器中，针对区域名称单击适当的标签。**
如果单击了错误的标签，请再次单击该标签以将其取消选中，然后单击正确的标签。

iv. **保存指定。**
在标签生成器中单击 "OK"（确定），然后在 "Trusted Network Zones Properties"（可信网络区域属性）对话框中单击 "OK"（确定）。

当所需的每个区域都列在面板中时，或者 "Add Zone Configuration"（添加区域配置）菜单项打开的对话框没有区域名称的值时，则说明您已完成。

- **如果要使用缺省 `label_encodings` 文件，请使用 "Labeled Zone Manager"（有标签区域管理器）。**
单击 "Select Label"（选择标签）菜单项，然后单击 "OK"（确定）以显示可用标签列表。

a. **选择区域的标签。**
对于名为 `public`（公共）的区域，从列表中选择标签 `PUBLIC`（公共）。

b. **单击 "OK"（确定）。**
此时将显示任务列表。

▼ 安装有标签区域

开始之前 您是全局区域中的超级用户。该区域已进行配置，并指定有一个网络接口。

"Labeled Zone Manager"（有标签区域管理器）对话框显示的副标题为 *zone-name*:configured（zone-name：已配置）。要打开此 GUI，请参见第 61 页中的“运行 txzonemgr 脚本”。

1 **从 Labeled Zone Manager（有标签区域管理器）中，选择 "Install"（安装），然后单击 "OK"（确定）。**

注意 – 完成此过程需要花费一些时间。请勿在完成此任务的过程中执行其他任务。

系统会将软件包从全局区域复制到非全局区域。此任务会在该区域中安装一个有标签的虚拟操作系统。为了继续演示示例，此任务将安装 public（公共）区域。GUI 将显示类似如下内容的输出：

```
# 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.
```

注 – 诸如 cannot create ZFS dataset zone/*zonename*: dataset already exists（无法创建 ZFS 数据集合 zone/zonename：数据集合已经存在）之类的消息是信息性的。该区域使用现有的数据集合。

安装完成后，系统将提示您输入主机的名称。提供一个名称。

2 **接受主机的名称。**

对话框会在任务列表上方显示 *zone-name*:installed（zone-name：已安装）。

故障排除 如果显示类似如下内容的警告：Installation of these packages generated errors: SUNW*pkgname*（安装以下软件包时发生错误：SUNWpkgname），请查看安装日志并完成软件包的安装。

▼ 引导有标签区域

开始之前 您是全局区域中的超级用户。该区域已安装，并指定有一个网络接口。

"Labeled Zone Manager"（有标签区域管理器）对话框显示的副标题为 *zone-name*:installed（zone-name：已安装）。要打开此 GUI，请参见第 61 页中的 “运行 txzonemgr 脚本”。

1 **在 Labeled Zone Manager（有标签区域管理器）中，选择 "Zone Console"（区域控制台），然后单击 "OK"（确定）。**

此时将为当前有标签区域显示一个单独的控制台窗口。

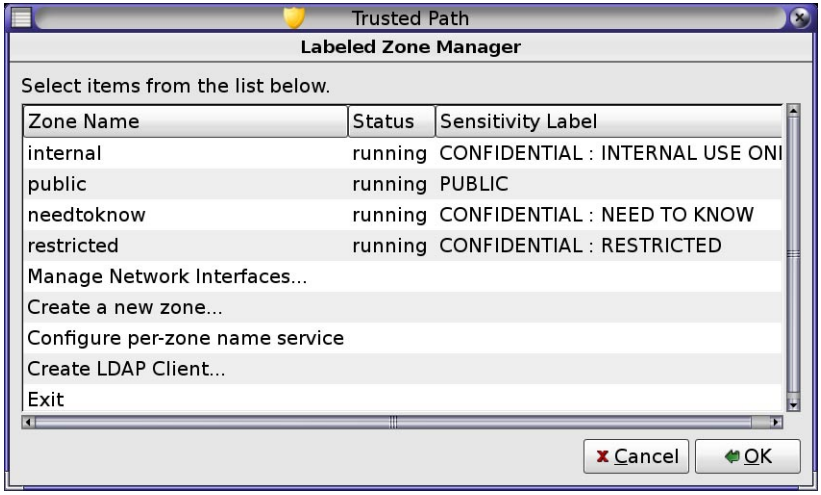
2 **选择 "Boot"（引导）。**

Zone Terminal Console（区域终端控制台）会跟踪区域引导进度。如果区域是从头开始创建的，则将在控制台中显示类似如下内容的消息：

```
[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]
```

注意 – 请勿在完成此任务的过程中执行其他任务。

如果配置并引导了四个缺省区域，Labeled Zone Manager（有标签区域管理器）将按如下所示显示区域：



故障排除 有时，将会显示错误消息，并且区域不会重新引导。在 Zone Terminal Console（区域终端控制台）中，按回车键。如果提示您键入 y 重新引导，请键入 y 并按回车键。区域将会重新引导。

接下来的步骤 如果此区域是从其他区域复制或克隆的，请继续第 70 页中的 “检验区域的状态”。

如果此区域是第一个区域，请继续第 71 页中的 “定制有标签区域”。

▼ 检验区域的状态

注 – X 服务器在全局区域中运行。每个有标签区域必须能够与全局区域相连接才能使用 X 服务器。因此，在可以使用区域之前，区域联网必须正常。有关背景信息，请参见第 24 页中的 “规划多级别访问”。

1 检验区域是否已完全启动。

a. 在“*zone-name*：区域终端控制台”中，以 root 用户身份登录。

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

b. 在 Zone Terminal Console（区域终端控制台）中，检验关键服务是否在运行。

```
# 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)
...
```

`sendmail` 和 `print` 服务不是关键服务。

c. 检验区域是否具有有效 IP 地址。

```
# ifconfig -a
```

例如，以下输出结果显示了 `hme0` 接口的 IP 地址。

```
# ...
 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. 可选检验区域是否可与全局区域通信。

i. 将 DISPLAY 变量设置为指向 X 服务器。

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

ii. **通过终端窗口显示一个 GUI。**

例如，显示一个时钟。

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

如果区域标签处的时钟没有出现，表明区域网络的配置不正确。有关调试建议，请参见第 98 页中的 “有标签区域无法访问 X 服务器”。

iii. **在继续之前关闭该 GUI。**

2 **从全局区域检查有标签区域的状态。**

```
# 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
```

接下来的步骤 您已完成了有标签区域的配置。要将特定于区域的网络接口添加到区域中，或者为每个有标签区域建立缺省路由，请继续第 74 页中的 “将网络接口和路由添加到有标签区域”。否则，请继续第 82 页中的 “在 Trusted Extensions 中创建角色和用户”。

▼ 定制有标签区域

如果要克隆区域或复制区域，此过程可将某个区域配置为其他区域的模板。此外，此过程还可配置尚未根据模板创建的区域以供使用。

开始之前 您是全局区域中的超级用户。您已完成了第 70 页中的 “检验区域的状态”。

1 **在区域终端控制台中，禁用有标签区域中不需要的服务。**

如果要复制或克隆此区域，您禁用的服务将会在新区域中被禁用。在您的系统上处于联机状态的服务依赖于区域的服务清单。使用 `netservices limited` 命令可关闭有标签区域不需要的服务。

a. **删除多数不需要的服务。**

```
# netservices limited
```

b. **列出剩余的服务。**

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

c. **禁用图形登录。**

```
# 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
```

有关服务管理框架的信息，请参见 `smf(5)` 手册页。

2 **在 Labeled Zone Manager（有标签区域管理器）中，选择 "Halt"（停止）以停止区域。**

3 **在继续之前，检验区域是否已关闭。**

在 *zone-name*: Zone Terminal Console（zone-name：区域终端控制台）中，以下消息表明区域已关闭。

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

如果不复制或克隆此区域，请使用创建此第一个区域的方式创建其余的区域。否则，请继续执行下一步。

4 **如果要将此区域用作其他区域的模板，请执行以下操作：**

a. **删除 `auto_home_`*zone-name* 文件。**

在全局区域的终端窗口中，从 *zone-name* 区域删除此文件。

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

例如，如果 `public`（公共）区域是用于克隆其他区域的模板，请删除 `auto_home_public` 文件：

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

b. **如果打算克隆此区域，请在下一步中创建 ZFS 快照，然后继续第 73 页中的“在 Trusted Extensions 中复制或克隆区域”。**

c. **如果打算复制此区域，请完成步骤 6，然后继续第 73 页中的“在 Trusted Extensions 中复制或克隆区域”。**

5 **要创建一个区域模板以用于克隆其余区域，请选择 "Create Snapshot"（创建快照），然后单击 "OK"（确定）。**

注意 – 快照的区域必须在 ZFS 文件系统中。您已在第 51 页中的“创建用于克隆区域的 ZFS 池”中为区域创建了一个 ZFS 文件系统。

---

6 **要检验定制的区域是否仍然可用，请从 "Labeled Zone Manager"（有标签区域管理器）中选择 "Boot"（引导）。**

Zone Terminal Console（区域终端控制台）会跟踪区域引导进度。控制台中会显示类似如下的消息：

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

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

按回车键可出现登录提示。您可以使用 root 用户身份登录。

▼ 在 Trusted Extensions 中复制或克隆区域

开始之前 您已完成了第 71 页中的 “定制有标签区域”。

将显示 "Labeled Zone Manager"（有标签区域管理器）对话框。要打开此 GUI，请参见第 61 页中的 “运行 txzonemgr 脚本”。

1 **创建区域。**

有关详细信息，请参见第 65 页中的 “命名区域并为其添加标签”。

2 **通过选择以下方法之一，继续您的区域创建策略：**

对于每个新区域，您将重复执行这些步骤。

- **复制刚刚添加标签的区域。**

  a. **在 Labeled Zone Manager（有标签区域管理器）中，选择 "Copy"（复制），然后单击 "OK"（确定）。**

  b. **选择区域模板，然后单击 "OK"（确定）。**

  此时一个窗口会显示复制过程。该过程完成后，区域就安装好了。

  如果 Labeled Zone Manager（有标签区域管理器）中显示 *zone-name*: `configured`（zone-name：已配置），请继续执行下一步。否则，请继续执行步骤 e。

  c. **选择菜单项 "Select another zone"（选择另一个区域），然后单击 "OK"（确定）。**

  d. **选择新安装的区域，然后单击 "OK"（确定）。**

  e. **完成第 68 页中的 “引导有标签区域”。**

  f. **完成第 70 页中的 “检验区域的状态”。**

- **克隆刚刚添加标签的区域。**

  a. **在 Labeled Zone Manager（有标签区域管理器）中，选择 "Clone"（克隆），然后单击 "OK"（确定）。**

  b. **从列表中选择一个 ZFS 快照，然后单击 "OK"（确定）。**
  例如，如果您从 `public` 创建了一个快照，请选择 `zone/public@snapshot`。
  克隆过程完成后，区域就安装好了。继续执行步骤 c。

  c. **打开 Zone Console（区域控制台）并引导区域。**
  有关说明，请参见第 68 页中的 “引导有标签区域”。

  d. **完成第 70 页中的 “检验区域的状态”。**

接下来的步骤

- 针对每个区域完成第 70 页中的 “检验区域的状态”后，如果您希望每个区域位于单独的物理网络上，请继续第 75 页中的 “添加网络接口以路由现有的有标签区域”。
- 如果您尚未创建角色，请继续第 82 页中的 “在 Trusted Extensions 中创建角色和用户”。
- 如果您已经创建了角色，请继续第 92 页中的 “在 Trusted Extensions 中创建起始目录”。

将网络接口和路由添加到有标签区域

以下任务支持其中的每个区域都连接到单独物理网络的环境。

任务	说明	参考
要么 1a：将网络接口添加到每个有标签区域，并使用全局区域访问外部网络。	将每个有标签区域连接到单独的物理网络。有标签区域使用全局区域提供的网络路由。	第 75 页中的 “添加网络接口以路由现有的有标签区域”
或者 1b：将网络接口添加到具有缺省路由的每个有标签区域。	将每个区域连接到单独的物理网络。有标签区域**不**使用全局区域进行路由。	第 77 页中的 “添加不使用全局区域的网络接口以路由现有的有标签区域”
2. 在每个有标签区域中创建名称服务高速缓存。	为每个区域配置名称服务守护进程。	第 80 页中的 “在每个有标签区域中配置名称服务高速缓存”

▼ 添加网络接口以路由现有的有标签区域

此过程将特定于区域的网络接口添加到现有的有标签区域中。此配置支持其中的每个有标签区域都连接到单独物理网络的环境。有标签区域使用全局区域提供的网络路由。

注 – 全局区域必须为配置了非全局区域地址的每个子网配置一个 IP 地址。

开始之前 您是全局区域中的超级用户。

对于每个区域，您已完成了第 60 页中的 “创建有标签区域”中的任务。

1 在全局区域中，将附加网络接口的 IP 地址和主机名键入到 `/etc/hosts` 文件中。

使用标准命名约定，例如向主机的名称添加 *-zone-name*。

```
## /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 对于每个接口的网络，请将相应的项添加到 `/etc/netmasks` 文件中。

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

有关更多信息，请参见 `netmasks(4)` 手册页。

3 在全局区域中，检测特定于区域的物理接口。

a. 确定已经检测的物理接口。

```
# ifconfig -a
```

b. 在每个接口上配置全局区域地址。

```
# 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. 对于每个全局区域地址，创建一个 `hostname.`*interface-nameN* 文件。

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

全局区域地址在系统启动时立即进行配置。特定于区域的地址在引导区域时进行配置。

4. **向每个特定于区域的网络接口指定安全模板。**

   如果网络的网关未配置标签，请指定 `admin_low` 安全模板。如果网络的网关配有标签，请指定 `cipso` 安全模板。

   您可以创建主机类型为 `cipso` 的安全模板，以反映每个网络的标签。有关创建和指定模板的过程，请参见《Oracle Solaris Trusted Extensions 管理员规程》中的“配置可信网络数据库（任务列表）”。

5. **停止打算向其添加特定于区域的接口的每个有标签区域。**

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

6. **启动 Labeled Zone Manager（有标签区域管理器）。**

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

7. **对于要在其中添加特定于区域的接口的每个区域，执行以下操作：**

   a. **选择区域。**

   b. **选择 "Add Network"（添加网络）。**

   c. **命名网络接口。**

   d. **键入接口的 IP 地址。**

8. **在每个已完成区域的 Labeled Zone Manager（有标签区域管理器）中，选择 "Zone Console"（区域控制台）。**

9. **选择 "Boot"（引导）。**

10. **在 "Zone Console"（区域控制台）中，检验是否已创建接口。**

    ```
    # ifconfig -a
    ```

11. **检验区域是否有通往子网网关的路由。**

    ```
    # netstat -rn
    ```

故障排除 要调试区域配置，请参见以下内容：

- 《System Administration Guide: Oracle Solaris Containers-Resource Management and Oracle Solaris Zones》中的第 30 章 “Troubleshooting Miscellaneous Solaris Zones Problems”
- 第 97 页中的 “Trusted Extensions 配置故障排除”
- 《Oracle Solaris Trusted Extensions 管理员规程》中的“可信网络故障排除（任务列表）”

▼ 添加不使用全局区域的网络接口以路由现有的有标签区域

此过程为现有的有标签区域设置特定于区域的缺省路由。在此配置中，有标签区域不使用全局区域进行路由。

在引导区域前，必须在全局区域中检测有标签的区域。但是，要将有标签区域与全局区域隔离，在引导区域时接口必须处于 `down`（关闭）状态。有关更多信息，请参见《System Administration Guide: Oracle Solaris Containers-Resource Management and Oracle Solaris Zones》中的第 17 章 “Non-Global Zone Configuration (Overview)”。

注 – 必须为引导的每个非全局区域配置一个唯一缺省路由。

开始之前 您是全局区域中的超级用户。

对于每个区域，您已完成了第 60 页中的 “创建有标签区域”中的任务。您使用 `vni0` 接口或 `lo0` 接口将有标签区域连接到全局区域。

1. **对于每个网络接口，确定其 IP 地址、网络掩码和缺省路由器。**

   使用 `ifconfig -a` 命令确定 IP 地址和网络掩码。使用 `zonecfg -z zonename info net` 命令确定是否指定了缺省路由器。

2. **为每个有标签区域创建一个空 `/etc/hostname.`*interface* 文件。**

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

   有关更多信息，请参见 `netmasks(4)` 手册页。

3. **检测有标签区域的网络接口。**

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

4. **检验有标签区域的接口是否处于 `down`（关闭）状态。**

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

   特定于区域的地址在引导区域时进行配置。

5. **对于每个接口的网络，请将相应的项添加到 `/etc/netmasks` 文件中。**

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

   有关更多信息，请参见 `netmasks(4)` 手册页。

6 **向每个特定于区域的网络接口指定安全模板。**

创建主机类型为 `cipso` 的安全模板，以反映每个网络的标签。要创建和指定模板，请参见《Oracle Solaris Trusted Extensions 管理员规程》中的“配置可信网络数据库（任务列表）”。

7 **运行 `txzonemgr` 脚本，打开一个单独的终端窗口。**

在 Labeled Zone Manager（有标签区域管理器）中，您将为有标签区域添加网络接口。在终端窗口中，您将显示有关区域的信息并设置缺省路由器。

8 **对于要向其添加特定于区域的网络接口和路由器的每个区域，请完成以下步骤：**

a. **在终端窗口中，停止区域。**

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

b. **在 Labeled Zone Manager（有标签区域管理器）中，执行以下操作：**

i. **选择区域。**

ii. **选择 "Add Network"（添加网络）。**

iii. **命名网络接口。**

iv. **键入接口的 IP 地址。**

v. **在终端窗口中，检验区域配置。**

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

c. **在终端窗口中，为有标签区域的网络配置缺省路由器。**

```
# 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
#
```

有关更多信息，请参见 `zonecfg(1M)` 手册页，以及《System Administration Guide: Oracle Solaris Containers-Resource Management and Oracle Solaris Zones》中的“How to Configure the Zone”。

d. **引导有标签区域。**

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

e. 在全局区域中，检验有标签区域是否有通往子网网关的路由。

```
# netstat -rn
```

将会显示一个路由表。有标签区域的目标和接口不同于全局区域的条目。

9 要删除缺省路由，请选择区域的 IP 地址，然后删除路由。

```
# 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
```

示例 4–5 设置有标签区域的缺省路由

在此示例中，管理员将 Secret（秘密）区域路由到单独的物理子网。来往于 Secret（秘密）区域的通信不会通过全局区域进行路由。管理员使用 Labeled Zone Manager（有标签区域管理器）和 `zonecfg` 命令，然后检验路由是否有效。

管理员确定 `qfe1` 和 `qfe1:0` 当前未在使用，并为两个有标签区域创建映射。`qfe1` 是 Secret（秘密）区域的指定接口。

```
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
```

首先，管理员创建 `/etc/hostname.qfe1` 文件并配置 `/etc/netmasks` 文件。

```
# touch /etc/hostname.qfe1

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

接着，管理员检测网络接口并检验接口是否关闭。

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

然后，在 Solaris Management Console 中，管理员创建一个具有单一标签 Secret（秘密）的安全模板，并将接口的 IP 地址指定给模板。

管理员停止区域。

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

管理员运行 `txzonemgr` 脚本打开 Labeled Zone Manager（有标签区域管理器）。

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

在 Labeled Zone Manager（有标签区域管理器）中，管理员依次选择 Secret（秘密）区域、"Add Network"（添加网络）和一个网络接口。管理员关闭 Labeled Zone Manager（有标签区域管理器）。

在命令行上，管理员选择区域的 IP 地址，然后设置其缺省路由。在退出命令之前，管理员检验路由并将其提交。

```
# 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
#
```

管理员引导区域。

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

在全局区域中的单独终端窗口中，管理员检验数据包的发送和接收。

```
# 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
...
```

▼ 在每个有标签区域中配置名称服务高速缓存

通过此过程，可以在每个有标签区域中单独配置名称服务守护进程 (nscd)。此配置支持满足以下条件的环境：其中的每个区域都连接到一个以区域的标签运行的子网，并且该子网拥有自己的用于该标签的名称服务器。

注 – 此配置不满足评估配置的标准。在评估配置中，nscd 守护进程仅在全局区域中运行。每个有标签区域中的通道将区域连接到全局 nscd 守护进程。

开始之前 您是全局区域中的超级用户。root 必须尚未成为角色。您已成功完成了第 75 页中的“添加网络接口以路由现有的有标签区域”。

此配置要求您具备网络方面的高级技能。如果您的命名服务是 LDAP，则您要负责建立与每个有标签区域的 LDAP 客户机连接。nscd 守护进程会缓存名称服务信息，但不会路由该信息。

1 **如果要使用 LDAP，请检验从有标签区域到 LDAP 服务器的路由。**

在每个有标签区域的终端窗口中，运行以下命令：

zone-name **# netstat -rn**

2 **在全局区域中，启动 Labeled Zone Manager（有标签区域管理器）。**

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

3 **选择 "Configure per-zone name service"（配置每区域名称服务），然后单击 "OK"（确定）。**

此选项规定为在初始系统配置过程中使用一次。

4 **配置每个区域的 nscd 服务。**

有关帮助，请参见 nscd(1M) 和 nscd.conf(4) 手册页。

5 **重新引导系统。**

6 **对于每个区域，检验路由和名称服务守护进程。**

a. **在 "Zone Console"（区域控制台）中，列出 nscd 服务。**

```
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. **检验通往子网的路由。**

zone-name **# netstat -rn**

7 **要删除特定于区域的名称服务守护进程，请在全局区域中执行以下操作：**

a. **打开 Labeled Zone Manager（有标签区域管理器）。**

b. **选择 "Unconfigure per-zone name service"（取消配置每区域名称服务），然后单击 "OK"（确定）。**

此选择将删除每个有标签区域中的 nscd 守护进程。

c. **重新引导系统。**

在 Trusted Extensions 中创建角色和用户

如果已经在使用管理角色，则可能需要添加安全管理员角色。对于尚未实施角色的站点，创建角色的过程与 Solaris OS 中的过程类似。Trusted Extensions 添加安全管理员角色，并要求使用 Solaris Management Console 来管理 Trusted Extensions 域。

如果站点安全策略要求两个人来创建用户和角色帐户，请创建定制权限配置文件并将其指定给角色以实施 *separation of duty*（**职责分离**）。

任务	说明	参考
创建三个限制性比缺省配置文件更强的权限配置文件。	创建用于管理用户的权限配置文件。这些配置文件的限制性比管理用户的缺省配置文件更强。	第 82 页中的 “创建实施职责分离的权限配置文件”
创建安全管理员角色。	创建处理安全相关任务的安全管理员角色。	第 85 页中的 “在 Trusted Extensions 中创建安全管理员角色”
创建不能设置用户口令的系统管理员角色。	创建一个系统管理员角色并为其指定受限制的系统管理员权限配置文件。	第 87 页中的 “创建受限系统管理员角色”
创建承担管理角色的用户。	创建可以承担角色的一个或多个用户。	第 88 页中的 “在 Trusted Extensions 中创建可以承担角色的用户”
检验角色是否可以执行其任务。	在各种情况下测试角色。	第 90 页中的 “检验 Trusted Extensions 角色是否有效”
使用户能够登录到有标签区域。	启动 zones（区域）服务，使一般用户能够登录。	第 92 页中的 “使用户能够登录到有标签区域”

▼ 创建实施职责分离的权限配置文件

如果 separation of duty（职责分离）并不是一项站点安全要求，请跳过此过程。如果站点要求职责分离，在置备 LDAP 服务器之前，必须创建这些权限配置文件和角色。

此过程创建具有独立的用户管理功能的权限配置文件。在向不同角色指定这些配置文件时，需要两个角色来创建和配置用户。一个角色可以创建用户，但不能指定安全属性。另一个角色可以指定安全属性，但不能创建用户。当您以指定有其中一个配置文件的角色登录 Solaris Management Console 时，该角色只能使用相应的选项卡和字段。

开始之前 您必须是具有 `root` 角色或主管理员角色的超级用户。启动此过程时，必须关闭 Solaris Management Console。

1 创建影响用户配置的缺省权限配置文件的副本。

a. 将 `prof_attr` 文件复制到 `prof_attr.orig` 文件。

b. **在可信编辑器中，打开 `prof_attr` 文件。**

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

c. **复制三个权限配置文件，并重命名副本。**

```
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. **保存更改。**

e. **检验更改。**

```
# 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...
```

通过复制权限配置文件（而不是修改），可以将系统升级到较新的 Solaris 发行版并保留您的更改。因为这些权限配置文件很复杂，所以与从头开始生成限制性更强的配置文件相比，修改缺省配置文件的副本较不容易出错。

2 **启动 Solaris Management Console。**

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

3 **选择 This Computer (*this-host*: `Scope=Files, Policy=TSOL`) 工具箱。**

4 **单击 "System Configuration"（系统配置），然后单击 "Users"（用户）。**

此时会提示您输入口令。

5 **键入相应的口令。**

6 **双击 "Rights"（权限）。**

7 **修改 "Custom User Security"（定制用户安全）权限配置文件。**

限制此配置文件，防止创建用户。

a. **双击 "Custom User Security"（定制用户安全）。**

b. **单击 "Authorizations"（授权）选项卡，然后执行以下步骤：**

   i. **从 "Included"（包括）列表中，删除 `Manage Users and Roles`（管理用户和角色）授权。**

      以下 "User Accounts"（用户帐户）权限将保留：

      ```
      Audit Controls
      Label and Clearance Range
      Change Password
      View Users and Roles
      Modify Extended Security Attributes
      ```

   ii. **将 "Manage Privileges"（管理特权）权限添加到 "Included"（包括）列表中。**

c. **单击 "OK"（确定）以保存更改。**

8 **修改 "Custom User Management"（定制用户管理）配置文件。**

限制此配置文件，防止设置口令。

a. **双击 "Custom User Management"（定制用户管理）。**

b. **单击 "Authorizations"（授权）选项卡，然后执行以下步骤：**

   i. **拖动 "Included"（包括）列表的滚动条到 "User Accounts"（用户帐户）。**

   ii. **从 "Included"（包括）列表中，删除 `Modify Extended Security Attributes`（修改扩展安全属性）授权。**

      以下 "User Accounts"（用户帐户）权限将保留：

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

c. **保存您的更改。**

9 **修改 "Custom System Administrator"（定制系统管理员）权限配置文件。**

"User Management"（用户管理）配置文件是此配置文件中的一个补充配置文件。防止系统管理员设置口令。

a. **双击 "Custom System Administrator"（定制系统管理员）。**

b. **单击 "Supplementary Rights"（补充权限）选项卡，然后执行以下步骤：**

   i. **删除 "User Management"（用户管理）权限配置文件。**

   ii. **添加 "Custom User Management"（定制用户管理）权限配置文件。**

iii. 将 "Custom User Management"（定制用户管理）权限配置文件移到 "All"（全部）权限配置文件上方。

c. 保存您的更改。

接下来的步骤 在确认定制配置文件实施职责分离之后，要防止使用缺省配置文件，请参见第 90 页中的 “检验 Trusted Extensions 角色是否有效”中的步骤 7。

▼ 在 Trusted Extensions 中创建安全管理员角色

在 Trusted Extensions 中创建角色的过程与在 Solaris OS 中创建角色的过程相同。但是，在 Trusted Extensions 中，安全管理员角色是必需的。要创建本地安全管理员角色，也可以使用命令行界面，如示例 4–6中所示。

开始之前 您必须是具有 `root` 角色或主管理员角色的超级用户。

要在网络上创建角色，必须已完成第 117 页中的 “为 LDAP 配置 Solaris Management Console（任务列表）”。

1. **启动 Solaris Management Console。**

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

2. **选择相应的工具箱。**

   - **要在本地创建角色，请使用 This Computer (*this-host*: `Scope=Files, Policy=TSOL`)。**
   - **要在 LDAP 服务中创建角色，请使用 This Computer (*ldap-server*: `Scope=LDAP, Policy=TSOL`)。**

3. **单击 "System Configuration"（系统配置），然后单击 "Users"（用户）。**

   此时会提示您输入口令。

4. **键入相应的口令。**

5. **双击 "Administrative Roles"（管理角色）。**

6. **从 "Action"（操作）菜单中，选择 "Add Administrative Role"（添加管理角色）。**

7. **创建“安全管理员”角色。**

   请参照以下信息：

   - Role name（角色名称）－`secadmin`
   - Full name（全名）－`Security Administrator`（安全管理员）

- Description（说明）－站点安全管理人员 (Site Security Officer) **不在此处提供专有信息**。
- Role ID Number（角色 ID 号）－≥100
- Role shell（角色 shell）－管理员的 Bourne（配置文件 shell）
- Create a role mailing list（创建角色邮件列表）－使该复选框保持处于选中状态。
- Password and confirm（口令和确认）－指定至少包含 6 个字母数字字符的口令。

  安全管理员角色的口令以及所有口令都必须难以猜出，从而减少通过试猜口令而让有敌意的人获取未经授权访问的机会。

注 – 对于所有管理角色，使帐户始终可用 (Always Available)，不要设置口令失效日期。

- Available and Granted Rights（可用权限和授予权限）—信息安全 (Information Security)、用户安全 (User Security)
  - 如果站点安全策略不要求 separation of duty（职责分离），请选择 "Information Security"（信息安全）和缺省的 "User Security"（用户安全）权限配置文件。
  - 如果站点安全策略要求职责分离，请选择 "Information Security"（信息安全）和 "Custom User Security"（定制用户安全）权限配置文件。
- Home Directory Server（起始目录服务器）－*home-directory-server*
- Home Directory Path（起始目录路径）－*/mount-path*
- Assign Users（指定用户）－此字段会在向用户指定角色时自动填充。

8 在创建角色之后，检查相应设置是否正确。

选择该角色，然后双击它。

检查以下字段中的值：

- Available Groups（可用组）－根据需要添加组。
- Trusted Extensions Attributes（Trusted Extensions 属性）－缺省值正确。

  对于不应显示标签的单标签系统，请为 "Label: Show or Hide"（标签：显示或隐藏）选择 "Hide"（隐藏）。
- Audit Excluded and Included（排除和包括审计）－仅当角色的审计标志未包括在 `audit_control` 文件中的系统设置之内时，才设置审计标志。

9 要创建其他角色，请参照安全管理员角色。

例如，请参见《System Administration Guide: Security Services》中的"How to Create and Assign a Role by Using the GUI"。为每个角色指定一个唯一 ID，并向角色指定正确的权限配置文件。可能的角色包括：

- admin 角色－System Administrator（系统管理员）授予的权限
- primaryadmin 角色－Primary Administrator（主管理员）授权的权限
- oper 角色－Operator（操作员）授予的权限

示例 4–6 使用 roleadd 命令创建本地安全管理员角色

在此示例中，root 用户使用 roleadd 命令将安全管理员角色添加到本地系统中。有关详细信息，请参见 roleadd(1M) 手册页。root 用户在创建角色前要参考表 1–2。在此站点上，创建用户时不需要职责分离。

```
# 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
```

root 用户提供角色的初始口令。

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

要将角色指定给本地用户，请参见示例 4–7。

▼ 创建受限系统管理员角色

如果 separation of duty（职责分离）并不是一项站点安全要求，请跳过此过程。

在此过程中，要将一个限制性更强的权限配置文件指定给系统管理员角色。

开始之前 您必须是具有 root 角色或主管理员角色的超级用户。

您已完成了第 82 页中的 "创建实施职责分离的权限配置文件"。您要使用的工具箱与创建权限配置文件时所用的工具箱相同。

1. **在 Solaris Management Console 中，创建系统管理员角色。**
   有关帮助，请参见第 85 页中的 "在 Trusted Extensions 中创建安全管理员角色"。
2. **将 Custom System Administrator（定制系统管理员）权限配置文件指定给角色。**
3. **保存更改。**

4 **关闭 Solaris Management Console。**

▼ 在 Trusted Extensions 中创建可以承担角色的用户

要创建本地用户，可以使用命令行界面（如示例 4–7 中所示）来代替以下过程。在站点安全策略允许的情况下，可以选择创建能承担多个管理角色的用户。

为保证可以安装创建用户，系统管理员角色负责创建用户，而安全管理员角色则负责指定与安全相关的属性（如口令）。

开始之前 您必须是具有 `root` 角色、安全管理员角色或主管理员角色的超级用户。安全管理员角色拥有创建用户所需的最小特权。

将会显示 Solaris Management Console。有关详细信息，请参见第 85 页中的 “在 Trusted Extensions 中创建安全管理员角色”。

1 **在 Solaris Management Console 中双击 "User Accounts"（用户帐户）。**

2 **从 "Action"（操作）菜单中，选择 "Add User"（添加用户）→ "Use Wizard"（使用向导）。**

注意 – 角色和用户的名称和 ID 来自于同一个池。请勿将现有的名称或 ID 用于添加的用户。

3 **按照联机帮助的说明操作。**

您也可以遵循《System Administration Guide: Basic Administration》中的“How to Add a User With the Solaris Management Console’s Users Tool”的过程。

4 **在创建了用户之后，双击创建的用户以修改设置。**

注 – 对于可以承担角色的用户，使用户帐户始终可用 (Always Available)，不要设置口令失效日期。

确保正确设置以下字段：

- Description（说明）－不在此处提供专有信息。
- Password and confirm（口令和确认）－指定至少包含 6 个字母数字字符的口令。

注 – 初始设置团队选择口令时，必须选择难以猜出的口令，从而减少通过试猜口令而让有敌意的人获取未经授权访问的机会。

- Account Availability（帐户可用性）－始终可用 (Always Available)。
- Trusted Extensions Attributes（Trusted Extensions 属性）－缺省值正确。

  对于不应显示标签的单标签系统，请为 "Label: Show or Hide"（标签：显示或隐藏）选择 "Hide"（隐藏）。
- Account Usage（帐户使用）－设置空闲时间和空闲操作。

  Lock account（锁定帐户）－对于可以承担角色的任何用户设置为 "No"（否）。

5 **关闭 Solaris Management Console。**

6 **定制用户的环境。**

a. **指定方便授权。**

   在检查了站点安全策略以后，可能需要向您的首批用户授予 "Convenient Authorizations"（方便授权）权限配置文件。使用此配置文件，用户可以分配设备、打印 PostScript 文件、进行无标签打印、远程登录以及关闭系统。要创建配置文件，请参见《Oracle Solaris Trusted Extensions 管理员规程》中的“如何创建权限配置文件以实现方便的授权”。

b. **定制用户初始化文件。**

   请参见《Oracle Solaris Trusted Extensions 管理员规程》中的第 7 章 “在 Trusted Extensions 中管理用户、权限和角色（任务）”。

   另请参见《Oracle Solaris Trusted Extensions 管理员规程》中的“使用 Solaris Management Console 管理用户和权限（任务列表）”。

c. **创建多标签副本和链接文件。**

   在多标签系统上，可以为用户和角色设置一些文件，这些文件列出要复制或链接到其他标签的用户初始化文件。有关更多信息，请参见《Oracle Solaris Trusted Extensions 管理员规程》中的“.copy_files 和 .link_files 文件”。

示例 4–7 使用 useradd 命令创建本地用户

在此示例中，`root` 用户创建一个可承担安全管理员角色的本地用户。有关详细信息，请参见 `useradd(1M)` 和 `atohexlabel(1M)` 手册页。

首先，`root` 用户确定用户的最小标签和安全许可标签的十六进制格式。

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

其次，root 用户参考表 1–2，然后创建用户。

```
# 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
```

接着，root 用户提供初始口令。

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

最后，root 用户将安全管理员角色添加到用户的定义中。该角色是在第 85 页中的 “在 Trusted Extensions 中创建安全管理员角色”中创建的。

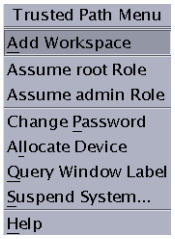
```
# usermod -R secadmin jandoe
```

▼ 检验 Trusted Extensions 角色是否有效

要检验每个角色，请承担相应的角色。然后，执行只有该角色可以执行的任务。

开始之前 如果您配置了 DNS 或路由，则必须在创建角色之后，检验该角色是否有效之前，进行重新引导。

1. **对于每个角色，以可以承担相应角色的用户身份登录。**
2. **打开 "Trusted Path"（可信路径）菜单。**
   - **在 Trusted CDE 中，单击工作区切换区域。**



   从菜单中选择并承担相应角色。

- **在 Trusted JDS 中，单击可信窗口条中您的用户名。**
  在以下可信窗口条中，用户名为 `tester`。

  从指定给您的角色列表中，选择一个角色。

3. **在角色工作区中，启动 Solaris Management Console。**

   ```
   $ /usr/sbin/smc &
   ```

4. **为要测试的角色选择相应的作用域。**

5. **单击 "System Services"（系统服务），然后导航到 "Users"（用户）。**
   此时会提示您输入口令。

   a. **键入角色的口令。**

   b. **双击 "User Accounts"（用户帐户）。**

6. **单击某个用户。**

   - 系统管理员角色应该能够修改 "General"（常规）、"Home Directory"（起始目录）和 "Group"（组）选项卡下的字段。
     如果您配置了可实施 separation of duty（职责分离）的角色，则系统管理员角色将无法设置用户的初始口令。
   - 安全管理员角色应该能够修改所有选项卡下的字段。
     如果您配置了可实施职责分离的角色，则安全管理员角色将无法创建用户。
   - 主管理员角色应该能够修改所有选项卡下的字段。

7. **可选如果要实施职责分离，请防止使用缺省权限配置文件。**

注 – 当系统升级到较新版本的 Solaris OS 时，System Administrator（系统管理员）、User Management（用户管理）和 User Security（用户安全）缺省配置文件将被替换。

在可信编辑器中，执行以下步骤之一：

- **从 `prof_attr` 文件中删除三个权限配置文件。**
  通过删除权限配置文件，可以防止管理员查看或指定这些配置文件。此外，还要删除 `prof_attr.orig` 文件。

- **在 prof_attr 文件中注释掉三个权限配置文件。**
  通过注释掉权限配置文件，可以防止在 Solaris Management Console 中查看这些配置文件，或者防止在管理用户的命令中使用这些配置文件。仍可在 prof_attr 文件中查看这些配置文件及其内容。

- **在 prof_attr 文件中为三个权限配置文件键入不同的说明。**
  编辑 prof_attr 文件以更改这些权限配置文件的说明字段。例如，可以将说明替换为 Do not use this profile（不要使用此配置文件）。这种更改可警告管理员不要使用该配置文件，但并不防止使用该配置文件。

▼ 使用户能够登录到有标签区域

重新引导主机时，必须重新建立设备与底层存储之间的关联。

开始之前 您已经创建了至少一个有标签的区域。该区域将不用于进行克隆。

1. **重新引导系统。**
2. **以 root 用户身份登录。**
3. **重新启动区域服务。**

```
# svcs zones
STATE          STIME    FMRI
offline        -        svc:/system/zones:default

# svcadm restart svc:/system/zones:default
```

4. **注销。**
   一般用户现在可以登录了。他们的会话位于有标签区域中。

在 Trusted Extensions 中创建起始目录

在 Trusted Extensions 中，用户需要访问其从中工作的每个标签的起始目录。要使每个起始目录可供用户使用，需要创建一个多级别起始目录服务器，在该服务器上运行自动挂载程序，并导出起始目录。在客户端，可以运行脚本来为每个用户找到每个区域的起始目录，也可以让用户登录到起始目录服务器。

▼ 在 Trusted Extensions 中创建起始目录服务器

开始之前 您必须是具有 root 角色或主管理员角色的超级用户。

1. **使用 Trusted Extensions 软件安装并配置起始目录服务器。**
   - 如果您要克隆区域，请确保使用具有空起始目录的 Solaris ZFS 快照。
   - 因为用户在其可以登录到的每个标签都需要一个起始目录，所以请创建用户可以登录到的每个区域。例如，如果使用缺省 label_encodings 文件，则要为 PUBLIC（公共）标签创建一个区域。
2. **如果要使用 UFS，但不使用 Solaris ZFS，请使 NFS 服务器能够为自身提供服务。**
   a. **在全局区域中，修改 nsswitch.conf 文件中的 automount 条目。**
      使用可信编辑器编辑 /etc/nsswitch.conf 文件。有关过程，请参见《Oracle Solaris Trusted Extensions 管理员规程》中的“如何在 Trusted Extensions 中编辑管理文件”。
      ```
      automount: files
      ```
   b. **在全局区域中，运行 automount 命令。**
3. **对于每个有标签区域，请遵循《 Oracle Solaris Trusted Extensions 管理员规程 》中的“如何在有标签区域中对文件进行 NFS 挂载”中介绍的自动挂载过程。然后，返回到此过程。**
4. **检验是否已创建起始目录。**
   a. **从起始目录服务器注销。**
   b. **以一般用户身份登录到起始目录服务器。**
   c. **在登录区域中，打开一个终端。**
   d. **在终端窗口中，检验用户的起始目录是否存在。**
   e. **为用户可在其中工作的每个区域创建工作区。**
   f. **在每个区域中，打开一个终端窗口来检验用户的起始目录是否存在。**
5. **从起始目录服务器注销。**

▼ 在 Trusted Extensions 中使用户能够访问其起始目录

用户可以在最初时登录到起始目录服务器来创建可与其他系统共享的起始目录。要为每个标签创建一个起始目录，每个用户必须登录到每个标签的起始目录服务器。

或者，也可以管理员身份创建一个脚本，以便在用户首次登录前在每个用户的主系统上创建起始目录的挂载点。该脚本会在用户可以工作的每个标签创建挂载点。

开始之前 已配置 Trusted Extensions 域的起始目录服务器。

- **选择是允许直接登录到服务器，还是运行脚本。**
  - **使用户能够直接登录到起始目录服务器。**
    a. **指示每个用户登录到起始目录服务器。**
       成功登录后，该用户必须注销。
    b. **指示每个用户重新登录，但这次要选择不同的登录标签。**
       用户使用标签生成器来选择不同的登录标签。成功登录后，该用户必须注销。
    c. **指示每个用户针对允许该用户使用的每个标签重复登录过程。**
    d. **指示用户从其常规工作站登录。**
       用户缺省标签的用户起始目录可用。当用户更改了某个会话的标签，或者从不同的标签添加了工作区时，将挂载该标签的用户起始目录。
  - **编写一个脚本，以便为每个用户创建起始目录挂载点，然后运行该脚本。**

```
#!/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. **从全局区域中，在 NFS 服务器上运行此脚本。**
    b. **然后，在用户要登录的每个多级别桌面上运行此脚本。**

将用户和主机添加到现有可信网络

如果您有在 NIS 映射中定义的用户，可以将其添加到您的网络中。

要将主机和标签添加到主机中，请参见以下过程：

- 要添加主机，可使用 Solaris Management Console 中的 "Computers and Networks"（计算机和网络）工具集合。有关详细信息，请参见《Oracle Solaris Trusted Extensions 管理员规程》中的“如何向系统的已知网络添加主机”。

  将某个主机添加到 LDAP 服务器时，请添加与该主机关联的所有 IP 地址。必须将所有区域地址（包括有标签区域的地址）添加到 LDAP 服务器。
- 为主机添加标签，请参见《Oracle Solaris Trusted Extensions 管理员规程》中的“如何将安全模板指定给向一台主机或一组主机”。

▼ 将 NIS 用户添加到 LDAP 服务器

开始之前 您必须是具有 `root` 角色或主管理员角色的超级用户。

1 从 NIS 数据库收集需要的信息。

a. 根据 `aliases` 数据库中的相应用户项创建一个文件。

```
% ypcat -k aliases | grep login-name > aliases.name
```

b. 根据 `passwd` 数据库中的相应用户项创建一个文件。

```
% ypcat -k passwd | grep "Full Name" > passwd.name
```

c. 根据 `auto_home_` 数据库中的相应用户项创建一个文件。

```
% ypcat -k auto_home | grep login-name > auto_home_label
```

2 为 LDAP 和 Trusted Extensions 重新设置信息格式。

a. 使用 `sed` 命令重新设置 `aliases` 项的格式。

```
% sed 's/ /:/g' aliases.login-name > aliases
```

b. 使用 `nawk` 命令重新设置 `passwd` 项的格式。

```
% nawk -F: '{print $1":x:"$3":"$4":"$5":"$6":"$7}' passwd.name > passwd
```

c. 使用 `nawk` 命令创建一个 `shadow` 项。

```
% nawk -F: '{print $1":"$2":6445::::::"}' passwd.name > shadow
```

d. 使用 `nawk` 命令创建一个 `user_attr` 项。

```
% 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 **将修改后的文件复制到 LDAP 服务器上的 /tmp 目录。**

```
# cp aliases auto_home_internal passwd shadow user_attr /tmp/name
```

4 **将步骤 3 中文件中的项添加到 LDAP 服务器上的数据库中。**

```
# /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
```

示例 4–8 将 NIS 数据库中的用户添加到 LDAP 服务器

在以下示例中，管理员向可信网络中添加了一个新用户。该用户的信息原来存储在 NIS 数据库中。为了保护 LDAP 服务器口令，管理员在服务器上运行了 `ldapaddent` 命令。

在 Trusted Extensions 中，该新用户可以分配设备并承担操作员角色。因为该用户可以承担角色，因此用户帐户不会被锁定。用户的最小标签为 `PUBLIC`（公共）。用户工作所在的标签为 `INTERNAL`（内部），因此将 `jan` 添加到 `auto_home_internal` 数据库。`auto_home_internal` 数据库自动挂载具有读写权限的 `jan` 的起始目录。

- 在 LDAP 服务器上，管理员从 NIS 数据库中提取用户信息。

```
# 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
```

- 然后，管理员为 LDAP 重新设置项的格式。

```
# 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
```

- 接着，管理员为 Trusted Extensions 创建 `user_attr` 项。

```
# 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
```

- 随后，管理员将文件复制到 `/tmp/jan` 目录。

```
# cp aliases auto_home_internal passwd shadow user_attr /tmp/jan
```

- 最后，管理员用 `/tmp/jan` 目录中的文件置备服务器。

```
# /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
```

Trusted Extensions 配置故障排除

在 Trusted Extensions 中，有标签区域通过全局区域与 X 服务器通信。因此，有标签区域必须有通往全局区域的可用路由。此外，在 Solaris 安装过程中选择的选项可能会防止 Trusted Extensions 使用通往全局区域的接口。

在启用 Trusted Extensions 之后运行了 netservices limited

说明：

不是在启用 Trusted Extensions 之前运行 `netservices limited` 命令，而是之后在全局区域中运行了该命令。因此，您的有标签区域无法连接到全局区域中的 X 服务器。

解决方案：

运行以下命令以打开 Trusted Extensions 在区域间通信所需的服务：

```
# svccfg -s x11-server setprop options/tcp_listen = true
# svcadm enable svc:/network/rpc/rstat:default
```

无法在有标签区域中打开控制台窗口

说明：

尝试在有标签区域中打开控制台窗口时，对话框中出现了以下错误：

```
Action:DttermConsole,*,*,*,0 [Error]
Action not authorized.
```

解决方案：

检验 `/etc/security/exec_attr` 文件中每个区域的项中是否存在以下两行：

```
All Actions:solaris:act:::*;*;*;*;*:
All:solaris:act:::*;*;*;*;*:
```

如果不存在这些行，表明未在该有标签区域中安装添加这些项的 Trusted Extensions 软件包。在这种情况下，请重新创建有标签区域。有关过程，请参见第 60 页中的“创建有标签区域”。

有标签区域无法访问 X 服务器

说明：

如果某个有标签区域不能成功访问 X 服务器，可能会显示如下消息：

- `Action failed. Reconnect to Solaris Zone?`（操作失败。是否重新连接到 Solaris Zone？）
- `No route available`（没有可用路由）
- `Cannot reach globalzone-`*`hostname`*` :0`（无法访问 globalzone-hostname: 0）

原因：

有标签区域可能因以下任何原因而无法访问 X 服务器：

- 区域未初始化，正在等待 `sysidcfg` 进程完成。
- 有标签区域的主机名未被全局区域中运行的命名服务识别。
- 未将任何接口指定为 `all-zones`。
- 有标签区域的网络接口已关闭。
- LDAP 名称查找失败。
- NFS 挂载无效。

解决步骤：

请执行以下操作：

1. 登录到区域。

   可以使用 `zlogin` 命令或 Zone Terminal Console（区域终端控制台）操作。

   ```
   # zlogin -z zone-name
   ```

   如果无法以超级用户身份登录，请使用 `zlogin -S` 命令来跳过验证。

2. 检验区域是否正在运行。

   ```
   # zoneadm list
   ```

   如果某个区域的状态为 `running`（运行），则表明该区域至少正在运行一个进程。

3. 解决防止有标签区域访问 X 服务器的任何问题。
   - 通过完成 `sysidcfg` 进程初始化区域。

     以交互方式运行 `sysidcfg` 程序。应答 Zone Terminal Console（区域终端控制台）或运行 `zlogin` 命令的终端窗口中的提示。

要以非交互方式运行 sysidcfg 进程，可以执行以下操作之一：

- 为 /usr/sbin/txzonemgr 脚本指定 "Initialize"（初始化）项。

  通过 "Initialize"（初始化）项，可以向 sysidcfg 问题提供缺省值。

- 编写您自己的 sysidcfg 脚本。

  有关更多信息，请参见 sysidcfg(4) 手册页。

- 检验 X 服务器对区域可用。

  登录到有标签区域。将 DISPLAY 变量设置为指向 X 服务器，然后打开一个窗口。

  ```
  # DISPLAY=global-zone-hostname:n.n
  # export DISPLAY
  # /usr/openwin/bin/xclock
  ```

  如果未显示有标签窗口，表明该有标签区域的区域网络配置不正确。

  注 – 如果运行的是 Solaris 10 5/09 发行版或更高版本的 Trusted CDE，请参见第 145 页中的 “在 Trusted CDE 中解析本地区域与全局区域间的路由”。

- 通过命名服务配置区域的主机名。

  不使用该区域的本地 /etc/hosts 文件，而是必须在全局区域中或 LDAP 服务器上指定等效信息。该信息必须包括指定给区域的主机名的 IP 地址。

- 未将任何接口指定为 all-zones。

  除非您的所有区域在与全局区域相同的子网上有 IP 地址，否则可能需要配置一个 all-zones（共享）接口通过这种配置，有标签区域可以连接到全局区域的 X 服务器。如果需要限制与全局区域 X 服务器的远程连接，可以使用 vni0 作为 all-zones 地址。

  如果**不**希望配置 all-zones 接口，必须为每个区域提供通往全局区域 X 服务器的路由。必须在全局区域中配置这些路由。

- 有标签区域的网络接口已关闭。

  ```
  # ifconfig -a
  ```

  使用 ifconfig 命令检验有标签区域的网络接口处于 UP 和 RUNNING 状态。

- LDAP 名称查找失败。

  使用 ldaplist 命令检验每个区域都可以与 LDAP 服务器或 LDAP 代理服务器通信。在 LDAP 服务器上，检验该区域是否已在 tnrhdb 数据库中列出。

- NFS 挂载无效。

  以超级用户身份在区域中重新启动 automount。或者，添加一个 crontab 项以便每隔五分钟运行一次 automount 命令。

其他 Trusted Extensions 配置任务

通过以下两项任务，可以将配置文件的完整副本传输至您站点上的每个 Trusted Extensions 系统。通过最后一项任务，可以将 Trusted Extensions 定制内容从 Solaris 系统中删除。

▼ 如何在 Trusted Extensions 中将文件复制到便携介质

复制到便携介质时，使用信息的敏感标签来标记介质。

注 – 在 Trusted Extensions 配置过程中，超级用户或等效角色会向便携介质和从便携介质复制管理文件。使用 `Trusted Path`（可信路径）标记介质。

开始之前 要复制管理文件，您必须是超级用户，或者在全局区域中承担了角色。

1. **分配相应的设备。**

   使用设备分配管理器，然后插入一个干净的介质。有关详细信息，请参见《Oracle Solaris Trusted Extensions 用户指南》中的“如何在 Trusted Extensions 中分配设备”。

   - 在 Solaris Trusted Extensions (CDE) 中，*File Manager*（文件管理器）会显示便携介质的内容。
   - 在 Solaris Trusted Extensions (JDS) 中，*File Browser*（文件浏览器）会显示内容。

   在此过程中，使用 File Browser（文件浏览器）来指代此 GUI。

2. **打开另外一个 File Browser（文件浏览器）。**

3. **导航到要复制的文件所在的文件夹。**

   例如，可能已将文件复制到 `/export/clientfiles` 文件夹。

4. **对于每个文件，执行以下操作：**

   a. **突出显示文件的图标。**

   b. **将文件拖到便携介质的 File Browser（文件浏览器）中。**

5. **对设备解除分配。**

   有关详细信息，请参见《Oracle Solaris Trusted Extensions 用户指南》中的“如何在 Trusted Extensions 中对设备解除分配”。

6. **在便携介质的 File Browser（文件浏览器）上，从 "File"（文件）菜单中选择 "Eject"（弹出）。**

注 – 请记住在包含所复制文件敏感标签的介质上粘上一个实体标签。

示例 4–9 使所有系统上的配置文件保持相同

系统管理员需要确保每台计算机配置了相同的设置。因此，在配置的第一台计算机上，要创建一个在重新引导后不会被删除的目录。在该目录中，管理员将放入应在所有系统上相同或非常相似的文件。

例如，管理员复制 Solaris Management Console 用于 LDAP 作用域的 Trusted Extensions 工具箱 `/var/sadm/smc/toolboxes/tsol_ldap/tsol_ldap.tbx`。管理员在 `tnrhtp` 文件中定制了远程主机模板，有一个 DNS 服务器以及审计配置文件的列表。管理员还修改了其站点的 `policy.conf` 文件。因此，管理员将这些文件复制到永久目录。

```
# 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
```

管理员使用设备分配管理器在全局区域中分配软盘，并将文件传输到该软盘上。在一个有 `ADMIN_HIGH` 标签的单独软盘上，管理员放入站点的 `label_encodings` 文件。

管理员将文件复制到某个系统上时，针对该系统修改了 `/etc/security/audit_control` 文件中的 `dir:` 条目。

▼ 如何在 Trusted Extensions 中从便携介质复制文件

在替换原始 Trusted Extensions 文件之前，可以安全地对其进行重命名。在配置系统时，`root` 角色会重命名和复制管理文件。

开始之前 要复制管理文件，您必须是超级用户，或者在全局区域中承担了角色。

1. **分配相应的设备。**

   有关详细信息，请参见《Oracle Solaris Trusted Extensions 用户指南》中的“如何在 Trusted Extensions 中分配设备”。

   - 在 Solaris Trusted Extensions (CDE) 中，*File Manager*（文件管理器）会显示便携介质的内容。
   - 在 Solaris Trusted Extensions (JDS) 中，*File Browser*（文件浏览器）会显示内容。

   在此过程中，使用 File Browser（文件浏览器）来指代此 GUI。

2. **插入包含管理文件的介质。**

3. **如果系统有同名文件，请在原始文件名的基础上组成新名称。**
   例如，在原始文件末尾加上 `.orig`：
   ```
   # cp /etc/security/tsol/tnrhtp /etc/security/tsol/tnrhtp.orig
   ```
4. **打开一个 File Browser（文件浏览器）。**
5. **导航到所需的目标目录，如 `/etc/security/tsol`。**
6. **对于要复制的每个文件，执行以下操作：**
   a. **在挂载介质的 File Browser（文件浏览器）中，突出显示文件的图标。**
   b. **然后，将文件拖至第二个 File Browser（文件浏览器）的目标目录中。**
7. **对设备解除分配。**
   有关详细信息，请参见《Oracle Solaris Trusted Extensions 用户指南》中的“如何在 Trusted Extensions 中对设备解除分配”。
8. **系统提示时，弹出并移除介质。**

示例 4–10 在 Trusted Extensions 中装入审计配置文件

在此示例中，系统上尚未配置角色。`root` 用户需要将配置文件复制到便携介质上。然后，可将该介质的内容复制到其他系统上。这些文件将被复制到配置有 Trusted Extensions 软件的每个系统上。

`root` 用户在设备分配管理器中分配 `floppy_0` 设备，并对挂载查询做出 `yes`（是）响应。随后，`root` 用户插入包含配置文件的软盘，并将配置文件复制到磁盘上。该软盘带有 `Trusted Path`（可信路径）标签。

为了从介质中读取，`root` 用户在接收主机上分配设备，然后下载内容。

如果配置文件位于磁带上，`root` 用户将分配 `mag_0` 设备。如果配置文件位于 CD-ROM 上，`root` 用户将分配 `cdrom_0` 设备。

▼ 如何从系统中删除 Trusted Extensions

要从 Solaris 系统中删除 Trusted Extensions，要执行特定的步骤来删除 Solaris 系统中的 Trusted Extensions 定制内容。

1. **如同在 Solaris OS 中一样，对需要保留的有标签区域的所有数据进行归档。**

2. **从系统中删除有标签区域。**

   有关详细信息，请参见《System Administration Guide: Oracle Solaris Containers-Resource Management and Oracle Solaris Zones》中的"How to Remove a Non-Global Zone"。

3. **禁用 Trusted Extensions 服务。**

   ```
   # svcadm disable labeld
   ```

4. **运行 bsmunconv 命令。**

   有关此命令的效果，请参见 bsmunconv(1M) 手册页。

5. **可选重新引导系统。**

6. **配置系统。**

   可能需要为您的 Solaris 系统配置各种服务。候选项包括审计、基本联网、命名服务和文件系统挂载。

◆ ◆ ◆ 第 5 章

为 Trusted Extensions 配置 LDAP（任务）

本章介绍了如何配置 Sun Java System Directory Server 和 Solaris Management Console 以便与 Trusted Extensions 一起使用。Directory Server 提供 LDAP 服务。LDAP 是适用于 Trusted Extensions 的受支持的命名服务。Solaris Management Console 是本地数据库和 LDAP 数据库的管理 GUI。

配置 Directory Server 时，您有两种选择。可以在 Trusted Extensions 系统上配置一个 LDAP 服务器，也可以使用现有的某个服务器并通过使用 Trusted Extensions 代理服务器来与其连接。请按照下列任务列表之一中的说明执行操作：

- 第 105 页中的 “在 Trusted Extensions 主机上配置 LDAP 服务器（任务列表）”
- 第 106 页中的 “在 Trusted Extensions 主机上配置 LDAP 代理服务器（任务列表）”

在 Trusted Extensions 主机上配置 LDAP 服务器（任务列表）

任务	说明	参考
设置 Trusted Extensions LDAP 服务器。	如果您没有现有的 Sun Java System Directory Server，请将第一个 Trusted Extensions 系统用作 Directory Server。此系统尚未安装有标签区域。 其他 Trusted Extensions 系统是此服务器的客户机。	第 107 页中的 “收集用于 LDAP 的 Directory Server 的信息” 第 108 页中的 “安装 Sun Java System Directory Server” 第 112 页中的 “配置 Sun Java System Directory Server 的日志”
向服务器添加 Trusted Extensions 数据库。	使用 Trusted Extensions 系统文件中的数据置备 LDAP 服务器。	第 114 页中的 “置备 Sun Java System Directory Server”
配置 Solaris Management Console 以便与 Directory Server 一起使用。	手动为 Solaris Management Console 设置 LDAP 工具箱。工具箱可用于在网络对象中修改 Trusted Extensions 属性。	第 117 页中的 “为 LDAP 配置 Solaris Management Console（任务列表）”

任务	说明	参考
将所有其他 Trusted Extensions 系统配置为此服务器的客户机。	配置具有 Trusted Extensions 的其他系统时，使该系统成为此 LDAP 服务器的客户机。	第 57 页中的 “使全局区域成为 Trusted Extensions 中的客户机”

在 Trusted Extensions 主机上配置 LDAP 代理服务器（任务列表）

如果在 Oracle Solaris 系统上具有一个正在运行的现有 Sun Java System Directory Server，请使用此任务列表。

任务	说明	参考
向服务器添加 Trusted Extensions 数据库。	Trusted Extensions 网络数据库 `tnrhdb` 和 `tnrhtp` 需要添加至 LDAP 服务器。	第 114 页中的 “置备 Sun Java System Directory Server”
设置 LDAP 代理服务器。	将一个 Trusted Extensions 系统用作其他 Trusted Extensions 系统的代理服务器。其他 Trusted Extensions 系统使用此代理服务器访问 LDAP 服务器。	第 116 页中的 “创建 LDAP 代理服务器”
将代理服务器配置为具有多级别 LDAP 端口。	使 Trusted Extensions 代理服务器从特定标签与 LDAP 服务器进行通信。	第 113 页中的 “为 Sun Java System Directory Server 配置多级别端口”
配置 Solaris Management Console 以便与 LDAP 代理服务器一起使用。	手动为 Solaris Management Console 设置 LDAP 工具箱。工具箱可用于在网络对象中修改 Trusted Extensions 属性。	第 117 页中的 “为 LDAP 配置 Solaris Management Console（任务列表）”
将所有其他 Trusted Extensions 系统配置为 LDAP 代理服务器的客户机。	配置具有 Trusted Extensions 的其他系统时，使该系统成为 LDAP 代理服务器的客户机。	第 57 页中的 “使全局区域成为 Trusted Extensions 中的客户机”

在 Trusted Extensions 系统上配置 Sun Java System Directory Server

LDAP 命名服务是适用于 Trusted Extensions 的受支持的命名服务。如果您的站点尚未运行 LDAP 命名服务，请在配置有 Trusted Extensions 的系统上配置 Sun Java System Directory Server (Directory Server)。

如果您的站点已经在运行 Directory Server，则您需要向服务器添加 Trusted Extensions 数据库。为访问 Directory Server，您需要在 Trusted Extensions 系统上设置一个 LDAP 代理。

注 – 如果不使用此 LDAP 服务器作为 NFS 服务器或 Sun Ray 客户机的服务器，则不需要在此服务器上安装任何有标签区域。

▼ 收集用于 LDAP 的 Directory Server 的信息

- **确定以下各项的值。**

  这些项按其在 Oracle Java Enterprise System 安装向导中的出现顺序列出。

安装向导提示	操作或信息
Sun Java System Directory Server *version*（Sun Java System Directory Server 版本）	
Administrator User ID（管理员用户 ID）	缺省值为 `admin`。
Administrator Password（管理员口令）	创建一个口令，如 `admin123`。
Directory Manager DN（目录管理员 DN）	缺省值为 `cn=Directory Manager`。
Directory Manager Password（目录管理员口令）	创建一个口令，如 `dirmgr89`。
Directory Server Root（Directory Server 根目录）	缺省值为 `/var/Sun/mps`。如果安装了代理软件，以后还会使用此路径。
Server Identifier（服务器标识符）	缺省值是本地系统。
Server Port（服务器端口）	如果计划使用 Directory Server 来为客户机系统提供标准 LDAP 命名服务，请使用缺省值 `389`。 如果计划使用 Directory Server 来支持代理服务器的后续安装，请输入一个非标准端口，如 `10389`。
Suffix（后缀）	包括您的域组件，如 `dc=example-domain,dc=com` 中所示。
Administration Domain（管理域）	为与后缀相对应而构造，如 `example-domain.com` 中所示。
System User（系统用户）	缺省值为 `root`。
System Group（系统组）	缺省值为 `root`。
Data Storage Location（数据存储位置）	缺省值为 `Store configuration data on this server`（**将配置数据存储在此服务器上**）。

安装向导提示	操作或信息
Data Storage Location（数据存储位置）	缺省值为 `Store user data and group data on this server`（**将用户数据和组数据存储在此服务器上**）。
Administration Port（管理端口）	缺省值为服务器端口。更改缺省值的建议约定为**软件版本的 `1000` 倍**。对于软件版本 5.2，此约定将得到端口 `5200`。

▼ 安装 Sun Java System Directory Server

可从 Sun Software Gateway Web 站点 (`http://www.oracle.com/solaris`)获取 Directory Server 软件包。

开始之前 您的 Trusted Extensions 系统上仅安装了一个全局区域。系统上没有带标签的区域。

Trusted Extensions LDAP 服务器是为使用 `pam_unix` 向 LDAP 系统信息库进行验证的客户机配置的。使用 `pam_unix` 时，口令操作由客户机确定，因此口令策略也由客户机确定。说得明确一点，也就是不使用由 LDAP 服务器设置的策略。有关可在客户机上设置的口令参数，请参见《系统管理指南：安全性服务》中的“管理口令信息”。有关 `pam_unix` 的信息，请参见 `pam.conf(4)` 手册页。

注 – LDAP 客户机上 `pam_ldap` 的使用是 Trusted Extensions 的未经评估的配置。

1 在安装 Directory Server 软件包之前，将 FQDN 添加至您的系统的主机名条目。

FQDN 是指 Fully Qualified Domain Name（全限定域名）。此名称是主机名和管理域的组合，如下例所示：

```
## /etc/hosts
...
192.168.5.5 myhost myhost.example-domain.com
```

在运行 Solaris 10 8/07 之前的发行版的系统上，将 IPv4 和 IPv6 项添加到 `/etc/inet/ipnodes` 文件中。一个系统的项在文件中必须是连续的。

如果未运行最新发行版的 Solaris OS，则必须安装以下修补程序。第一个编号是 SPARC 修补程序。第二个编号是 X86 修补程序。

- 138874–05、138875–05：Native LDAP、PAM、名称服务转换器修补程序
- 119313-35、119314-36：WBEM 修补程序
- 121308-21、121308-21：Solaris Management Console 修补程序
- 119315-20、119316-20：Solaris Management Applications 修补程序

2 在 Oracle Sun Web 站点中找到 Sun Java System Directory Server 软件包。

a. 在 Sun Software Gateway (`http://www.oracle.com/solaris`) 页面中，单击 "Get It"（获取）选项卡。

b. 单击 "Sun Java Identity Management Suite" 的复选框。

c. 单击 "Submit"（提交）按钮。

d. 如果您尚未注册，则进行注册。

e. 登录以便下载软件。

f. 单击屏幕左上角的 "Download Center"（下载中心）。

g. 在 "Identity Management"（身份管理）下，下载适用于您的平台的最新软件。

3 安装 Directory Server 软件包。

使用第 107 页中的 “收集用于 LDAP 的 Directory Server 的信息”中的信息来回答问题。有关问题、缺省值以及建议答案的完整列表，请参见《系统管理指南：命名和目录服务（DNS、NIS 和 LDAP）》中的第 11 章 “为使用 LDAP 客户机设置 Sun Java System Directory Server（任务）”以及《系统管理指南：命名和目录服务（DNS、NIS 和 LDAP）》中的第 12 章 “设置 LDAP 客户机（任务）”。

4 可选将 Directory Server 的环境变量添加到您的路径。

```
# $PATH
/usr/sbin:.../opt/SUNWdsee/dsee6/bin:/opt/SUNWdsee/dscc6/bin:/opt/SUNWdsee/ds6/bin:
/opt/SUNWdsee/dps6/bin
```

5 可选将 Directory Server 手册页添加到您的 `MANPATH`。

```
/opt/SUNWdsee/dsee6/man
```

6 启用 `cacaoadm` 程序，并验证是否已启用此程序。

```
# /usr/sbin/cacaoadm enable
# /usr/sbin/cacaoadm start
start: server (pid n) already running
```

7 确保每次引导时 Directory Server 都会启动。

Directory Server 的 SMF 服务的模板包含在 Sun Java System Directory Server 软件包中。

- 对于 Trusted Extensions Directory Server，请启用此服务。

  ```
  # 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
  ```

  有关 `dsadm` 命令的信息，请参见 `dsadm`(1M) 手册页。

- 对于代理 Directory Server，请启用此服务。

  ```
  # 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
  ```

有关 dpadm 命令的信息，请参见 dpadm(1M) 手册页。

8 **验证您的安装。**

```
# 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
```

故障排除 有关解决 LDAP 配置问题的策略，请参见《系统管理指南：命名和目录服务（DNS、NIS 和 LDAP）》中的第 13 章 “LDAP 疑难解答（参考）”.

▼ 为 Directory Server 创建 LDAP 客户机

您将使用此客户机来置备您用于 LDAP 的 Directory Server。在置备 Directory Server 之前必须执行此任务。

您可以在 Trusted Extensions Directory Server 上临时创建客户机，然后在服务器上删除此客户机，您也可以创建独立的客户机。

1 **在系统上安装 Trusted Extensions。**

可以使用 Trusted Extensions Directory Server，或者在一个独立的系统上安装 Trusted Extensions。

注 – 如果未运行最新发行版的 Solaris OS，则必须安装以下修补程序。第一个编号是 SPARC 修补程序。第二个编号是 X86 修补程序。

- 138874–05、138875–05：Native LDAP、PAM、名称服务转换器修补程序
- 119313-35、119314-36：WBEM 修补程序
- 121308-21、121308-21：Solaris Management Console 修补程序
- 119315-20、119316-20：Solaris Management Applications 修补程序

---

2 **在客户机上，修改缺省的 /etc/nsswitch.ldap 文件。**

以粗体显示的条目表示所做的修改。该文件应类似于以下内容：

```
# /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 **在全局区域中，运行 `ldapclient init` 命令。**

此命令将 `nsswitch.ldap` 文件复制到 `nsswitch.conf` 文件中。

在本例中，LDAP 客户机位于 `example-domain.com` 域中。服务器的 IP 地址为 `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 **将服务器的 `enableShadowUpdate` 参数设置为 `TRUE`。**

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

有关 enableShadowUpdate 参数的信息，请参见《系统管理指南：命名和目录服务（DNS、NIS 和 LDAP）》中的“enableShadowUpdate 开关”以及 ldapclient(1M) 手册页。

▼ 配置 Sun Java System Directory Server 的日志

此过程将配置三种类型的日志：访问日志、审计日志和错误日志。将不会更改以下缺省设置：

- 启用并缓冲所有日志。
- 将日志放置在相应的 /export/home/ds/instances/*your-instance*/logs/*LOG_TYPE* 目录中。
- 以日志级别 256 记录事件。
- 使用 600 文件权限保护日志。
- 访问日志每天轮转一次。
- 错误日志每周轮转一次。

此过程中的设置满足以下要求：

- 审计日志每天轮转一次。
- 超过 3 个月的日志文件将过期。
- 所有日志文件最多可使用 20,000 MB 磁盘空间。
- 最多可保留 100 个日志文件，且每个文件最多 500 MB。
- 如果可用的空闲磁盘空间小于 500 MB，则删除最旧的日志。
- 在错误日志中收集其他信息。

1 配置访问日志。

访问的 *LOG_TYPE* 为 ACCESS。用于配置日志的语法如下：

```
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 配置审计日志。

```
# 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
```

缺省情况下，审计日志的轮转时间间隔是一周。

3 **配置错误日志。**

在此配置中，您将指定要在错误日志中收集的其他数据。

```
# 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 **可选进一步配置日志。**

您还可以为每个日志配置以下设置：

```
# dsconf set-log-prop LOG_TYPE rotation-min-file-size:undefined
# dsconf set-log-prop LOG_TYPE rotation-time:undefined
```

有关 `dsconf` 命令的信息，请参见 `dsconf`(1M) 手册页。

▼ 为 Sun Java System Directory Server 配置多级别端口

要在 Trusted Extensions 中工作，必须在全局区域中将 Directory Server 的服务器端口配置为多级别端口 (multilevel port, MLP)。

1 **启动 Solaris Management Console。**

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

2 **选择 This Computer (*this-host*: `Scope=Files, Policy=TSOL`) 工具箱。**

3 **单击 "System Configuration"（系统配置），然后单击 "Computers and Networks"（计算机和网络）。**

此时会提示您输入口令。

4 **键入相应的口令。**

5 **双击 "Trusted Network Zones"（可信网络区域）。**

6 **双击全局区域。**

7 **为 TCP 协议添加多级别端口：**

a. **单击 "Add for the Multilevel Ports for Zone's IP Addresses"（为区域的 IP 地址添加多级别端口）。**

b. **键入端口号 389，然后单击 "OK"（确定）。**

8 为 UDP 协议添加多级别端口：

a. 单击 "Add for the Multilevel Ports for Zone's IP Addresses"（为区域的 IP 地址添加多级别端口）。

b. 键入端口号 389。

c. 选择 udp 协议，然后单击 "OK"（确定）。

9 单击 "OK"（确定）以保存设置。

10 更新内核。

```
# tnctl -fz /etc/security/tsol/tnzonecfg
```

▼ 置备 Sun Java System Directory Server

已创建或修改了多个 LDAP 数据库，用以保存有关标签配置、用户和远程系统的 Trusted Extensions 数据。在此过程中，您将使用 Trusted Extensions 信息置备 Directory Server 数据库。

开始之前 必须从启用了投影更新的 LDAP 客户机置备数据库。有关先决条件，请参见第 110 页中的 “为 Directory Server 创建 LDAP 客户机”。

如果站点安全要求 separation of duty（职责分离），请在置备 Directory server 之前完成以下操作：

- 第 82 页中的 “创建实施职责分离的权限配置文件”
- 第 85 页中的 “在 Trusted Extensions 中创建安全管理员角色”
- 第 87 页中的 “创建受限系统管理员角色”

1 为您计划用来置备命名服务数据库的文件创建一个暂存区域。

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

2 将样例 /etc 文件复制到暂存区域中。

```
# 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
```

如果您运行的是没有修补程序的 Solaris 10 11/06 发行版，请复制 ipnodes 文件。

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

3 **从 /setup/files/auto_master 文件中删除 +auto_master 条目。**

4 **Remove the ?:::::? entry from the /setup/files/auth_attr file.**

5 **从 /setup/files/prof_attr 文件中删除 :::: 条目。**

6 **在暂存区域中创建区域自动映射。**

在以下自动映射列表中，每一对行中的第一行显示了文件的名称。每一对行中的第二行显示了文件内容。区域名称标识 Trusted Extensions 软件中包含的缺省 label_encodings 文件中的标签。

- 使用您的区域名称替换这些行中的区域名称。
- *myNFSserver* 标识 NFS 服务器的起始目录。

```
/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 **将网络上的每个系统都添加到 /setup/files/tnrhdb 文件中。**

此处不可使用任何通配符机制。**必须**将要与之通信的每个系统的 IP 地址（包括有标签区域的 IP 地址）包含在此文件中。

a. **打开可信编辑器，并编辑 /setup/files/tnrhdb。**

b. **将有标签系统上的每个 IP 地址添加到 Trusted Extensions 域中。**

有标签系统的类型为 cipso。此外，有标签系统的安全模板的名称为 cipso。因此，在缺省配置中，cipso 条目类似于以下内容：

```
192.168.25.2:cipso
```

注 – 此列表包括全局区域和有标签区域的 IP 地址。

c. **添加域可与之进行通信的所有无标签系统。**

无标签系统的类型为 `unlabeled`。无标签系统的安全模板的名称为 `admin_low`。因此，在缺省配置中，无标签系统的条目类似于以下内容：

```
192.168.35.2:admin_low
```

d. **保存文件后退出编辑器。**

e. **检查文件的语法。**

```
# tnchkdb -h /setup/files/tnrhdb
```

f. **修复所有错误之后再继续。**

8 **将 `/setup/files/tnrhdb` 文件复制为 `/etc/security/tsol/tnrhdb` 文件。**

9 **通过 `ldapaddent` 命令，使用暂存区域中的所有文件置备 Directory Server。**

例如，以下命令基于暂存区域中的 `hosts` 文件置备服务器。

```
# /usr/sbin/ldapaddent -D "cn=directory manager" \
-w dirmgr123 -a simple -f /setup/files/hosts hosts
```

10 **如果在 Trusted Extensions Directory Server 上运行 `ldapclient` 命令，则会在该系统上禁用客户机。**

在全局区域中，运行 `ldapclient uninit` 命令。使用详细输出来验证该系统不再是 LDAP 客户机。

```
# ldapclient -v uninit
```

有关更多信息，请参见 `ldapclient(1M)` 手册页。

为现有 Sun Java System Directory Server 创建 Trusted Extensions 代理

首先，您需要将 Trusted Extensions 数据库添加到 Solaris 系统上的现有 Directory Server 中。然后，为使 Trusted Extensions 系统能够访问 Directory Server，您需要将一个 Trusted Extensions 系统配置为 LDAP 代理服务器。

▼ 创建 LDAP 代理服务器

如果您的站点中已存在 LDAP 服务器，请在一个 Trusted Extensions 系统上创建代理服务器。

开始之前 您已经从进行了修改并将 `enableShadowUpdate` 参数设置为 `TRUE` 的一个客户机置备了 LDAP 服务器。有关要求，请参见第 110 页中的 “为 Directory Server 创建 LDAP 客户机”。

此外，您还从 enableShadowUpdate 参数设置为 TRUE 的一个客户机上将包含 Trusted Extensions 信息的数据库添加到了 LDAP 服务器。有关详细信息，请参见第 114 页中的“置备 Sun Java System Directory Server”。

1 **在配置有 Trusted Extensions 的系统上，创建代理服务器。**

注 – 必须运行两个 ldapclient 命令。运行 ldapclient init 命令之后，运行 ldapclient modify 命令来将 enableShadowUpdate 参数设置为 TRUE。

有关详细信息，请参见《系统管理指南：命名和目录服务（DNS、NIS 和 LDAP）》中的第 12 章“设置 LDAP 客户机（任务）”。

2 **验证代理服务器是否可查看 Trusted Extensions 数据库。**

```
# ldaplist -l database
```

故障排除 有关解决 LDAP 配置问题的策略，请参阅《系统管理指南：命名和目录服务（DNS、NIS 和 LDAP）》中的第 13 章“LDAP 疑难解答（参考）”.

为 LDAP 配置 Solaris Management Console（任务列表）

Solaris Management Console 是用于管理运行有 Trusted Extensions 的系统网络的 GUI。

任务	说明	参考
初始化 Solaris Management Console。	初始化 Solaris Management Console。在全局区域中，为每个系统执行一次此过程。	第 54 页中的“在 Trusted Extensions 中初始化 Solaris Management Console 服务器”
注册凭证。	向 LDAP 服务器验证 Solaris Management Console。	第 118 页中的“向 Solaris Management Console 注册 LDAP 凭证”
在系统上启用远程管理。	缺省情况下，Solaris Management Console 客户机无法与其他系统上的 Console 服务器进行通信。您必须显式启用远程管理。	第 118 页中的“使 Solaris Management Console 接受网络通信”
创建 LDAP 工具箱。	在 Solaris Management Console for Trusted Extensions 中创建 LDAP 工具箱。	第 119 页中的“在 Solaris Management Console 中编辑 LDAP 工具箱”
验证通信。	验证 Trusted Extensions 主机是否可成为 LDAP 客户机。	第 120 页中的“验证 Solaris Management Console 是否包含 Trusted Extensions 信息”

▼ 向 Solaris Management Console 注册 LDAP 凭证

开始之前 您必须是在运行 Trusted Extensions 的 LDAP 服务器上的 root 用户。服务器可以是代理服务器。

必须配置 Sun Java System Directory Server。您已经完成了以下一种配置：

- 第 105 页中的“在 Trusted Extensions 主机上配置 LDAP 服务器（任务列表）”
- 第 106 页中的“在 Trusted Extensions 主机上配置 LDAP 代理服务器（任务列表）”

1 注册 LDAP 管理凭证。

```
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 在 Directory Server 上列出范围。

```
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
```

LDAP 服务器的设置决定了所列出的范围。编辑 LDAP 工具箱之前，LDAP 范围不会列出。注册服务器之后，才可编辑工具箱。

示例 5–1 注册 LDAP 凭证

在本例中，LDAP 服务器的名称为 LDAP1，cn 的值为缺省值 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
```

▼ 使 Solaris Management Console 接受网络通信

缺省情况下，Solaris 系统未配置为在存在安全风险的端口上进行侦听。因此，您必须显式将您计划远程管理的任何系统配置为接受网络通信。例如，要从客户机管理 LDAP 服务器上的网络数据库，LDAP 服务器上的 Solaris Management Console 服务器必须接受网络通信。

有关包含 LDAP 服务器的网络的 Solaris Management Console 配置要求说明，请参见《Oracle Solaris Trusted Extensions 管理员规程》中的“与 Solaris Management Console 的客户机-服务器通信”。

开始之前 您必须是 Solaris Management Console 服务器系统上的全局区域中的超级用户。在此过程中，该系统称为远程系统。此外，您必须具有作为超级用户通过命令行访问客户机系统的权限。

1. **在远程系统上，使系统接受远程连接。**

   `smc` 守护进程是由 `wbem` 服务控制的。如果 `wbem` 服务的 `options/tcp_listen` 属性设置为 `true`，则 Solaris Management Console 服务器将接受远程连接。

   ```
   # /usr/sbin/svcprop -p options wbem
   options/tcp_listen boolean false
   # svccfg -s wbem setprop options/tcp_listen=true
   ```

2. **刷新并重新启动 `wbem` 服务。**

   ```
   # svcadm refresh wbem
   # svcadm restart wbem
   ```

3. **验证 `wbem` 服务是否设置为接受远程连接。**

   ```
   # svcprop -p options wbem
   options/tcp_listen boolean true
   ```

4. **在远程系统以及需要访问 Solaris Management Console 的任何客户机上，确保在 `smcserver.config` 文件中启用了远程连接。**

   a. **在可信编辑器中，打开 `smcserver.config` 文件。**

      ```
      # /usr/dt/bin/trusted_edit /etc/smc/smcserver.config
      ```

   b. **将 `remote.connections` 参数设置为 `true`。**

      ```
      ## remote.connections=false
      remote.connections=true
      ```

   c. **保存文件后退出可信编辑器。**

故障排除 如果重新启动或启用了 `wbem` 服务，必须确保 `smcserver.config` 文件中的 `remote.connections` 参数仍然设置为 `true`。

▼ 在 Solaris Management Console 中编辑 LDAP 工具箱

开始之前 您必须是 LDAP 服务器上的超级用户。必须向 Solaris Management Console 注册了 LDAP 凭证，且必须了解 `/usr/sadm/bin/dtsetup scopes` 命令的输出。有关详细信息，请参见第 118 页中的 “向 Solaris Management Console 注册 LDAP 凭证”。

1. **找到 LDAP 工具箱。**

   ```
   # cd /var/sadm/smc/toolboxes/tsol_ldap
   # ls *tbx
   tsol_ldap.tbx
   ```

2. **提供 LDAP 服务器名称。**

   a. **打开可信编辑器。**

   b. **将 `tsol_ldap.tbx` 工具箱的完整路径名作为参数复制并粘贴到编辑器中。**

   例如，以下路径是 LDAP 工具箱的缺省位置：

   ```
   /var/sadm/smc/toolboxes/tsol_ldap/tsol_ldap.tbx
   ```

   c. **替换范围信息。**

   使用 `/usr/sadm/bin/dtsetup scopes` 命令中 `ldap:/.....` 行的输出替换 `<Scope>` 与 `</Scope>` 标记之间的 `server` 标记。

   ```
   <Scope>ldap:/<ldap-server-name>/<dc=domain,dc=suffix></Scope>
   ```

   d. **使用 LDAP 服务器替换 `<?server?>` 或 `<?server ?>` 的每个实例。**

   ```
   <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. **保存文件后退出编辑器。**

3. **刷新并重新启动 `wbem` 服务。**

   ```
   # svcadm refresh wbem
   # svcadm restart wbem
   ```

示例 5–2 配置 LDAP 工具箱

在本例中，LDAP 服务器的名称为 `LDAP1`。为配置工具箱，管理员将使用 `LDAP1` 替换 `<?server ?>` 的实例。

```
# 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>
...
```

▼ 验证 Solaris Management Console 是否包含 Trusted Extensions 信息

有关包含 LDAP 服务器的网络以及未包含 LDAP 服务器的网络的 Solaris Management Console 配置要求说明，请参见《Oracle Solaris Trusted Extensions 管理员规程》中的“与 Solaris Management Console 的客户机-服务器通信”。

开始之前 您必须以管理性角色或超级用户身份登录 LDAP 客户机。要使系统成为 LDAP 客户机，请参见第 57 页中的 “使全局区域成为 Trusted Extensions 中的客户机”。

要管理本地系统，您必须已经完成第 54 页中的 “在 Trusted Extensions 中初始化 Solaris Management Console 服务器”。

要从本地系统连接至远程系统上的 Console 服务器，您必须已经在这两个系统上完成第 54 页中的 “在 Trusted Extensions 中初始化 Solaris Management Console 服务器”。此外，在远程系统上，您必须已经完成第 118 页中的 “使 Solaris Management Console 接受网络通信”。

要从 LDAP 客户机管理 LDAP 命名服务中的数据库，除了前面的过程之外，在 LDAP 服务器上您必须已经完成第 119 页中的 “在 Solaris Management Console 中编辑 LDAP 工具箱”。

1. **启动 Solaris Management Console。**

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

2. **打开 Trusted Extensions 工具箱。**

   Trusted Extensions 工具箱具有值 `Policy=TSOL`。

   - **在使用 LDAP 作为命名服务的可信网络中，执行以下测试：**

     a. **要检查是否可访问本地管理数据库，请打开以下工具箱：**

        `This Computer (`*this-host*`: Scope=Files, Policy=TSOL)`

     b. **要检查是否可访问 LDAP 服务器的本地管理数据库，请指定以下工具箱：**

        `This Computer (`*ldap-server*`: Scope=Files, Policy=TSOL)`

     c. **要检查是否可访问 LDAP 服务器上的命名服务数据库，请指定以下工具箱：**

        `This Computer (`*ldap-server*`: Scope=LDAP, Policy=TSOL)`

   - **在不使用 LDAP 作为命名服务的可信网络中，执行以下测试：**

     a. **要检查是否可访问本地管理数据库，请打开以下工具箱：**

        `This Computer (`*this-host*`: Scope=Files, Policy=TSOL)`

     b. **要检查是否可访问远程系统的本地管理数据库，请指定以下工具箱：**

        `This Computer (`*remote-system*`: Scope=Files, Policy=TSOL)`

3. **在 "System Configuration"（系统配置）下，依次导航至 "Computers and Networks"（计算机和网络）、"Security Templates"（安全模板）。**

4. **检查是否为远程系统应用了正确的模板和标签。**

注 – 当您尝试从不是 LDAP 服务器的系统访问网络数据库信息时，该操作将失败。通过控制台，您可以登录到远程主机并打开工具箱。不过，当您尝试访问或更改信息时，以下错误消息指出您在不是 LDAP 服务器的系统上选择了 `Scope=LDAP`。

```
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.
```

故障排除 要排除 LDAP 配置故障，请参见《系统管理指南：命名和目录服务（DNS、NIS 和 LDAP）》中的第 13 章 “LDAP 疑难解答（参考）”。

◆ ◆ ◆ 第 6 章

6 配置具有 Trusted Extensions 的无显示系统（任务）

在无显示系统（例如 Netra 系列）上配置和管理 Trusted Extensions 软件需要修改无显示系统上的安全设置以启用远程访问。管理远程 Trusted Extensions 系统也需要类似的设置。要运行管理 GUI，您可能需要在远程系统上运行该过程并在桌面系统上显示 GUI。

有关要求的说明，请参见《Oracle Solaris Trusted Extensions 管理员规程》中的第 8 章 “Trusted Extensions 中的远程管理（任务）”

注 – 无显示系统和远程系统所需的配置方法不满足通过评估的配置的条件。有关更多信息，请参见第 20 页中的 “了解站点的安全策略”。

Trusted Extensions 中的无显示系统配置（任务列表）

在无显示系统上，控制台通过串行线路连接到终端仿真窗口。通常会使用 `tip` 命令来确保线路的安全。根据可用的另一系统的类型，可以使用下列方法之一来配置无显示系统。下表中按照安全性从高到低的顺序列出了这些方法。这些说明也适用于远程系统。

任务	说明	参考
以 `root` 用户身份启用远程登录。	如果未使用 LDAP，则必须以 `root` 用户身份初始登录到无显示系统。如果在使用 LDAP，则可以跳过此过程。	第 124 页中的 “在 Trusted Extensions 中，以 `root` 用户身份启用远程登录”

任务	说明	参考
启用远程登录。	为可以担任 root 角色或其他管理角色的用户启用远程登录。	第 125 页中的 “在 Trusted Extensions 中以某个角色启用远程登录”
	启用从无标签系统对 Trusted Extensions 系统的管理。	第 127 页中的 “启用从无标签系统进行的远程登录”
	使用户可以在无显示系统上访问全局区域。	《Oracle Solaris Trusted Extensions 管理员规程》中的“在 Trusted Extensions 中如何使特定用户能够远程登录到全局区域”
（可选的）启用管理 GUI 的显示。	使在无显示系统上运行的管理 GUI 显示在桌面系统上。	第 128 页中的 “启用管理 GUI 的远程显示”
（可选的）启用虚拟网络计算 (virtual network computing, VNC)	在任何客户机上，使用远程 Trusted Extensions 上的 Xvnc 服务器向客户机回显多级别会话。	《Oracle Solaris Trusted Extensions 管理员规程》中的“如何使用 Xvnc 远程访问 Trusted Extensions 系统”
选择一种配置和管理方法来设置无显示系统。	担任某个角色或成为超级用户以管理远程系统。	第 128 页中的 “在 Trusted Extensions 中使用 rlogin 或 ssh 命令登录和管理无显示系统”
	使用无显示系统上的 Solaris Management Console。	第 127 页中的 “使用远程 Solaris Management Console 在文件范围内进行管理”
	如果您没有窗口系统，可以以超级用户身份使用串行登录。此过程不安全。	无需任何配置。

注 – 请参阅您的安全策略，以确定您的站点上允许的远程管理方法。

▼ 在 Trusted Extensions 中，以 root 用户身份启用远程登录

与在 Solaris OS 中一样，当 CONSOLE 登录被禁用时，root 可以从有标签系统远程登录。

如果您打算通过编辑本地文件来管理远程系统，请使用以下过程。

1 **在可信编辑器中，注释掉 /etc/default/login 文件中的 CONSOLE= 行。**

```
# /usr/dt/bin/trusted_edit /etc/default/login
```

编辑后的行显示如下：

```
#CONSOLE=/dev/console
```

2 **允许 root 用户通过 ssh 连接进行登录。**

修改 /etc/ssh/sshd_config 文件。缺省情况下，ssh 在 Solaris 系统上处于启用状态。

```
# /usr/dt/bin/trusted_edit /etc/ssh/sshd_config
```

编辑后的行显示如下：

```
PermitRootLogin yes
```

接下来的步骤 要以 root 用户身份从无标签系统登录，还必须完成第 127 页中的 “启用从无标签系统进行的远程登录”。

要以某个角色启用远程登录，请继续执行第 125 页中的 “在 Trusted Extensions 中以某个角色启用远程登录”。

▼ 在 Trusted Extensions 中以某个角色启用远程登录

仅当您必须通过 rlogin 或 ssh 命令管理无显示系统时，才需执行此过程。

可以远程调试配置错误。

开始之前 如果您使用本地文件来管理远程系统，并且已完成了第 124 页中的 “在 Trusted Extensions 中，以 root 用户身份启用远程登录”。那么，请以 root 用户身份在两个系统上都执行以下任务。

1 **在两个系统上，互相将对方标识为有标签系统。**

桌面系统和无显示系统必须互相标识为使用相同的安全模板。有关过程，请参见《Oracle Solaris Trusted Extensions 管理员规程》中的“如何将安全模板指定给向一台主机或一组主机”。

要指定临时标签，请参见示例 6–1。

2 **在两个系统上，创建相同的用户和角色。**

名称和 ID 必须相同，并且必须为这两个系统上的同一用户指定同一角色。要创建用户和角色，请参见第 82 页中的 “在 Trusted Extensions 中创建角色和用户”。

3 **要联系远程 Solaris Management Console，请在两个系统上执行以下操作：**

a. **将对方系统的主机名和 IP 地址添加到 /etc/hosts 文件中。**

```
# /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. 要允许远程角色担任，请修改 pam.conf 文件以放宽 PAM 策略。

i. 将 /etc/pam.conf 文件复制为 /etc/pam.conf.orig。

```
# cp /etc/pam.conf /etc/pam.conf.orig
```

ii. 在可信编辑器中，打开 pam.conf 文件。

```
# /usr/dt/bin/trusted_edit /etc/pam.conf
```

iii. 复制帐户管理下的缺省条目。

iv. 在每个复制的条目中，将 other 更改为 smcconsole。

v. 向复制的 pam_roles.so.1 条目添加 allow_remote。

在字段之间使用 Tab 键。现在，此部分将显示如下：

```
# 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. 保存文件后退出编辑器。

vii. 可选将文件复制为 /etc/pam.conf.site。

```
# cp /etc/pam.conf /etc/pam.conf.site
```

如果要将系统升级到更高的发行版，则随后必须评估是否应将 /etc/pam.conf.site 中的更改复制到 pam.conf 文件中。

示例 6–1 创建 ProductShort; 主机类型的临时定义

在本示例中，管理员想在设置主机类型定义之前开始配置远程 ProductShort; 系统。为此，管理员在远程系统上使用 tnctl 命令来临时定义桌面系统的主机类型：

```
remote-TX# tnctl -h desktop-TX:cipso
```

然后，管理员想要从尚未配置 ProductShort; 的桌面系统连接到远程 ProductShort; 系统。在本例中，管理员在远程系统上使用 tnctl 命令将桌面系统的主机类型临时定义为从 ADMIN_LOW 标签运行的无标签系统：

```
remote-TX# tnctl -h desktop-TX:admin_low
```

▼ 启用从无标签系统进行的远程登录

开始之前 此过程不安全。

如第 125 页中的 “在 Trusted Extensions 中以某个角色启用远程登录”中所述，您已放宽 PAM 策略以允许远程角色担任。

1 **在可信系统上，向无标签系统应用合适的安全模板。**

注意 – 使用缺省设置时，另一无标签系统可以登录和管理远程系统。因此，您必须将 `0.0.0.0` 网络缺省值从 `ADMIN_LOW` 更改为一个不同的标签。有关过程，请参见《Oracle Solaris Trusted Extensions 管理员规程》中的“如何限定可能会在可信网络上联系的主机”。

2 **在可信编辑器中，打开 `/etc/pam.conf` 文件。**

```
# /usr/dt/bin/trusted_edit /etc/pam.conf
```

3 **找到 `smcconsole` 条目。**

4 **将 `allow_unlabeled` 添加到 `tsol_account` 模块。**

在字段之间使用 Tab 键。

```
smcconsole   account required  pam_tsol_account.so.1 allow_unlabeled
```

编辑之后，此部分将显示如下：

```
# 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
```

▼ 使用远程 Solaris Management Console 在文件范围内进行管理

如果未使用 LDAP，并且希望在远程系统上使用 Solaris Management Console，请启用到控制台的远程连接。此过程不足以启用 LDAP 范围的访问。

要启用 LDAP 范围的访问，必须完成第 117 页中的 “为 LDAP 配置 Solaris Management Console（任务列表）”中的所有过程。

开始之前 两个系统都是有标签的系统。

您已完成以下过程：

- 第 54 页中的 “在 Trusted Extensions 中初始化 Solaris Management Console 服务器”
- 第 125 页中的 “在 Trusted Extensions 中以某个角色启用远程登录”

1. **完成第 118 页中的 “使 Solaris Management Console 接受网络通信”。**

2. **在桌面系统上，成为在两个系统上具有相同定义的用户。**

3. **在桌面系统上，担任在两个系统上具有相同定义的角色。**

4. **在桌面系统上，启动 Solaris Management Console。**

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

5. **在 "Server"（服务器）对话框中，键入无显示系统的名称。**

   然后，选择 `Scope=Files` 工具箱。

   ```
   This Computer (remote-system: Scope=Files, Policy=TSOL)
   ```

▼ 启用管理 GUI 的远程显示

用于在桌面上启用远程显示的过程与在未配置 ProductShort; 的 Solaris 系统上使用的过程相同。为方便起见，下面提供了该过程。

1. **在桌面系统上，使来自无显示系统的进程得以显示。**

   a. **使无显示系统能够访问桌面系统上的 X 服务器。**

      desktop `$` **`xhost +`** *headless-host*

   b. **确定桌面的 `DISPLAY` 变量的值。**

      desktop `$` **`echo $DISPLAY`**
      `:`*n*`.`*n*

2. **在无显示系统上，将 `DISPLAY` 变量设置为桌面系统。**

   headless `$ DISPLAY=`*desktop*`:`*n*`.`*n*
   headless `$ export DISPLAY=`*n*`:`*n*

▼ 在 Trusted Extensions 中使用 rlogin 或 ssh 命令登录和管理无显示系统

在此过程中，您可以使用命令行和 `txzonemgr` GUI 以超级用户或某个角色的身份管理无显示系统。

注 – 使用 `rlogin` 命令进行远程登录不如使用 `ssh` 命令进行远程登录安全。

使用 Solaris Management Console 管理远程系统不需要使用远程登录命令。有关过程，请参见《Oracle Solaris Trusted Extensions 管理员规程》中的“如何从 Trusted Extensions 系统使用 Solaris Management Console 来远程管理系统”。

开始之前 已完成第 125 页中的 “在 Trusted Extensions 中以某个角色启用远程登录”。

您是可以使用该同一用户名和用户 ID 登录到无显示系统的用户，您可以在无显示系统上担任与桌面系统上相同的角色。

1. **在桌面系统上，使来自无显示系统的进程得以显示。**

```
desktop $ xhost + headless-host
desktop $ echo $DISPLAY
:n.n
```

2. **确保您是在这两个系统上具有相同定义的用户。**

3. **从一个终端窗口，远程登录到无显示系统。**

   - **使用 `ssh` 命令登录：**

```
desktop $ ssh -l identical-username  headless
Password:       Type the user's password
headless $
```

   - **或者，使用 `rlogin` 命令登录：**

```
desktop # rlogin headless
Password:       Type the user's password
headless $
```

4. **担任在两个系统上具有相同定义的角色。**

   使用同一终端窗口。例如，担任 `root` 角色。

```
headless $ su - root
Password:       Type the root password
```

   您现在已在全局区域中。现在，您可以使用此终端从命令行管理无显示系统。

5. **使无显示系统上的进程显示在桌面系统上。**

注 – 通过使用 `ssh -X` 命令登录，还可以显示远程 GUI。有关更多信息，请参见 `ssh(1)` 手册页。有关示例，请参见示例 6–2。

```
headless $  DISPLAY desktop:n.n
headless $ export DISPLAY=n:n
```

现在即可以使用 Trusted Extensions GUI 管理无显示系统。例如，启动 `txzonemgr` GUI：

```
headless $ /usr/sbin/txzonemgr
```

"Labeled Zone Manager"（有标签区域管理器）将在远程系统上运行，并显示在桌面系统上。

6 可选访问 Trusted CDE 操作。

要打开并安全关闭 Application Manager，请参见《Oracle Solaris Trusted Extensions 管理员规程》中的"如何使用 dtappsession 来远程管理 Trusted Extensions"。

示例 6–2 配置无显示系统上的有标签区域

在本例中，管理员使用 `txzonemgr` GUI 从有标签桌面系统上配置有标签无显示系统上的有标签区域。与在 Solaris OS 中一样，管理员通过使用 `ssh` 命令及 `-X` 选项使 X 服务器能够访问桌面系统。用户 `install1` 在两个系统上具有相同的定义，可以担任角色 `remoterole`。

```
TXdesk1 $ xhost + TXnohead4
TXdesk1 $ whoami
install1

TXdesk1 $ ssh -X -l install1 TXnohead4
Password: Ins1PwD1
TXnohead4 $
```

为连接到全局区域，管理员担任了角色 `remoterole`。该角色在两个系统上具有相同的定义。

```
TXnohead4 # su - remoterole
Password: abcd1EFG
```

然后，管理员启动 `txzonemgr` GUI。

```
TXnohead4 $ /usr/sbin/txzonemgr &
```

"Labeled Zone Manager"（有标签区域管理器）将在无显示系统上运行，并显示在桌面系统上。

◆ ◆ ◆ 附 录 A

站点安全策略

本附录讨论了站点安全策略问题，并推荐了用于进一步了解相关信息的参考书籍和 Web 站点：

创建和管理安全策略

每个 Trusted Extensions 站点都是唯一的，并且必须确定自己的安全策略。在创建和管理安全策略时需执行下列任务。

- 成立安全团队。安全团队需要包括来自最高管理层、人事管理人员、计算机系统管理人员与管理员以及装置管理人员的代表。该团队必须审核 Trusted Extensions 管理员的策略和规程，并建议适用于所有系统用户的一般安全策略。
- 向管理和行政管理人员进行有关站点安全策略的培训。参与站点的管理和行政管理的所有人员都必须接受有关安全策略的培训。安全策略绝对不可供一般用户使用，因为此策略信息直接关系到计算机系统的安全性。
- 对用户进行 Trusted Extensions 软件和安全策略方面的培训。所有用户都必须熟悉《Oracle Solaris Trusted Extensions 用户指南》。因为用户通常是第一个知道系统运行不正常的人，所以用户必须了解系统并将所有问题报告给系统管理员。安全的环境要求用户在发现任何下列问题时立即通知系统管理员：
  - 在每个会话开始时报告的上次登录时间与实际不符。
  - 文件数据发生异常更改
  - 人可阅读的打印输出材料丢失或被盗
  - 无法执行某个用户功能

- 执行安全策略。如果没有遵守和执行安全策略，则配置有 Trusted Extensions 的系统中包含的数据就不安全。必须设定规程来记录所有问题和已采取的用来解决事故的措施。
- 定期审核安全策略。安全团队必须定期审核安全策略以及自从上次审核之后发生的所有事故。然后可调整策略以提高安全性。

站点安全策略和 Trusted Extensions

安全管理员必须基于站点的安全策略设计 Trusted Extensions 网络。安全策略决定了配置决策，例如：

- 对于所有用户，对哪些类别的事件进行何种程度的审计
- 对于各个角色中的用户，对哪些类型的事件进行何种程度的审计
- 如何管理、归档和审核审计数据
- 在系统中使用哪些标签以及一般用户是否可以查看 `ADMIN_LOW` 和 `ADMIN_HIGH` 标签
- 将哪些用户安全许可指定给个人
- 哪些一般用户可以分配哪些设备（如果有）
- 为系统、打印机和其他设备定义哪些标签
- 是否是在可评估配置中使用 Trusted Extensions

计算机安全建议

在为站点制定安全策略时，请考虑以下指导准则列表。

- 将配置有 Trusted Extensions 的系统的最大标签指定为不大于在站点上执行的工作的最大安全级别。
- 手动将系统重新引导、电源故障和关机事件记录到站点日志中。
- 记录文件系统损坏并分析所有受影响的文件是否存在可能的安全策略违规。
- 将操作手册和管理员文档限制为仅可供确实需要访问这些信息的个人使用。
- 报告并记录任何 Trusted Extensions 软件的异常行为，并确定原因。
- 如果可能，至少指定两个人来管理配置有 Trusted Extensions 的系统。向一个人指定安全相关决策方面的安全管理员授权。向另一个人指定系统管理任务方面的安全管理员授权。
- 建立常规备份例程。
- 只向需要授权且可以信任他们能正确使用授权的人指定授权。
- 只有在程序需要特权来执行其工作、并且经仔细审查后证明这些程序对特权的使用值得信任，才向其指定特权。审核现有 Trusted Extensions 程序上的特权，并将其做法作为在新程序上设置特权的指南。
- 定期审核并分析审计信息。调查所有不正常的事件，以确定导致事件的原因。

- 最大程度地减少管理 ID 的数量。
- 最大程度地减少 setuid 和 setgid 程序的数量。使用授权、特权和角色来执行程序并防止滥用。
- 确保管理员定期验证一般用户拥有有效的登录 shell。
- 确保管理员必须定期验证一般用户拥有有效的用户 ID 值而非系统管理 ID 值。

物理安全建议

在为站点制定安全策略时，请考虑以下指导准则列表。

- 限制对配置有 Trusted Extensions 的系统的访问。最安全的位置一般是不处于一楼的内部房间。
- 监视并记录对配置有 Trusted Extensions 的系统的访问。
- 将计算机设备固定在大型物体（如桌椅）上以防被盗。如果设备固定在木制物件上，请通过添加金属板增强物体的强度。
- 考虑使用可移除存储介质来存储敏感信息。当可移除介质未在使用中时，请锁定所有这些介质。
- 将系统备份和归档存储在系统位置之外的其他安全位置。
- 采用与限制对系统的访问相同的方式来限制对备份和归档介质的物理访问。
- 在计算机装置中安装高温报警器，以在温度超出制造商规范的范围时进行指示。建议范围为 10°C 到 32°C（50°F 到 90°F）。
- 在计算机装置中安装漏水报警器，以在地板上、底层地板中以及天花板中出现漏水时进行指示。
- 安装烟雾报警器以指示起火情况，并安装灭火系统。
- 安装湿度报警器以指示湿度过高或者过低情况。
- 如果计算机没有安装 TEMPEST 屏蔽层，考虑安装一个。TEMPEST 屏蔽层可能适合用于装置的墙面、地板和天花板。
- 只允许由获得认证的技师打开和关闭 TEMPEST 设备以确保该设备屏蔽电磁辐射的能力。
- 检查是否存在允许进入计算机设备所在装置或房间的物理缺口。检查活动式地板下、吊顶天花板中、房顶通风设备中以及原始物体与二次增建物之间的邻墙中是否有开口。
- 严禁在计算机装置内或计算机设备旁边进食、饮水和吸烟。划定出可以在其中进行这些活动而不会对计算机设备造成威胁的专门区域。
- 保护计算机装置的建筑图和图表。
- 限制对计算机装置的建筑图、地板地图和照片的使用。

人员安全建议

在为站点制定安全策略时，请考虑以下指导准则列表。

- 在人员到达安全站点时和离开安全站点前对软件包、文档和存储介质进行检查。
- 始终要求所有职员和访客出示个人身份胸卡。
- 使用难以复制或伪造的个人身份胸卡。
- 划定禁止访客进入的区域，并将这些区域清晰标记出来。
- 始终陪同访客。

常见安全违规

由于没有任何计算机是完全安全的，所以计算机装置是否安全取决于使用它的人。谨慎的用户或其他设备可轻松避免大部分违反安全的操作。不过，以下列表提供了可能发生的问题的示例：

- 用户将口令告诉了对系统不应当具有访问权的其他个人。
- 用户写下了口令，并将口令遗失或留在了不安全的位置。
- 用户将自己的口令设置为很容易被猜出的字词或容易被猜出的名字。
- 用户看到其他用户键入口令并记住了口令。
- 未经授权的用户拆除、更换或以物理方式损坏硬件。
- 用户使其系统处于无人看管状态且没有锁定屏幕。
- 用户更改文件的权限来允许其他用户阅读文件。
- 用户更改文件的标签来允许其他用户阅读文件。
- 用户没有用碎纸机碎掉敏感的硬拷贝文档就将它们丢弃，或将敏感的硬拷贝文档留在不安全的位置。
- 用户没有锁好出入门。
- 用户丢失了钥匙。
- 用户没有锁定可移除的存储介质。
- 计算机屏幕可通过外窗被看到。
- 网络电缆被搭接。
- 电子窃听设备捕获到计算机设备发射出的信号。
- 停电、电涌和电力激增破坏了数据。
- 地震、洪水、龙卷风、飓风和闪电破坏了数据。
- 外部电磁辐射干扰（例如太阳黑子活动）扰乱了文件。

其他安全参考信息

政府出版物详细介绍了与计算机安全相关的标准、政策、方法和术语。此处列出的其他出版物是适用于 UNIX 系统的系统管理员的指南，对于透彻了解 UNIX 安全问题和解决方案十分有用。

Web 上也提供了很多资源。需要特别指出的是，CERT (`http://www.cert.org`) Web 站点向公司和用户发出关于软件中的安全漏洞的警报。SANS 协会 (`http://www.sans.org/`) 提供培训、大量术语词汇表和 Internet 上排名靠前的威胁的更新列表。

美国政府出版物

美国政府在 Web 上提供了它的许多出版物。美国国家标准与技术局 (National Institute of Standards and Technology, NIST) 的计算机安全资源中心 (CSRC, Computer Security Resource Center) 发布关于计算机安全的文章。以下是可以从 NIST 站点 (`http://csrc.nist.gov/index.html`)下载的出版物样例。

- 《计算机安全介绍：NIST 手册》。SP 800-12，1995 年 10 月。
- 《Standard Security Label for Information Transfer》。FIPS-188，1994 年 9 月。
- 由 Marianne Swanson 和 Barbara Guttman 合著的《Generally Accepted Principles and Practices for Securing Information Technology Systems》。SP 800-14，1996 年 9 月。
- 由 Miles Tracy、Wayne Jensen 和 Scott Bisker 合著的《Guidelines on Electronic Mail Security》。SP 800-45，2002 年 9 月。E.7 部分涉及了安全地为邮件配置 LDAP。
- Mark Wilson 和 Joan Hash 合著的《Building an Information Technology Security Awareness and Training Program》。SP 800-50，2003 年 10 月。包括了一个非常有用的词汇表。
- 由 Karen Scarfone、Tim Grance 和 Kelly Masone 合著的《Computer Security Incident Handling Guide》。SP 800-61，2008 年 3 月。E.7 部分涉及了安全地为邮件配置 LDAP。
- 由 Karen Scarfone、Wayne Jansen 和 Miles Tracy 合著的《Guide to General Server Security》。SP 800-123，2008 年 7 月。
- Murugiah Souppaya、John Wack 和 Karen Kent 合著的《Security Configuration Checklists Program for IT Products》。SP 800-70，2005 年 5 月。

UNIX 安全出版物

Oracle Corporation 安全工程师《Solaris 10 Security Essentials》Prentice Hall，2009。

由 John Chirillo 和 Edgar Danielyan 合著的《Sun Certified Security Administration for Solaris 9 & 10 Study Guide》。McGraw-Hill/Osborne 出版，2005。

由 Simson Garfinkel、Gene Spafford 和 Alan Schwartz 合著的《Practical UNIX and Internet Security, 3rd Edition》。O'Reilly & Associates, Inc, Sebastopol, CA 出版，2006。

一般计算机安全出版物

由 Glenn M. Brunette 和 Christoph L. 合著的《Toward Systemically Secure IT Architectures》。Oracle Corporation 出版，2005 年 6 月。

由 Charlie Kaufman、Radia Perlman 和 Mike Speciner 合著的《Network Security: Private Communication in a Public World, 2nd Edition》。Prentice-Hall 出版，2002。

由 Charles P. Pfleeger 和 Shari Lawrence Pfleeger 合著的《Security in Computing》。Prentice Hall PTR 出版，2006。

《Privacy for Pragmatists: A Privacy Practitioner's Guide to Sustainable Compliance》。Oracle Corporation 出版，2005 年 8 月。

由 Mark Rhodes-Ousley、Roberta Bragg 和 Keith Strassberg 合著的《Network Security: The Complete Reference》。McGraw-Hill/Osborne 出版，2004。

Cliff Stoll 编著的《The Cuckoo's Egg》。Doubleday 出版，1989。

一般 UNIX 出版物

Maurice J. Bach 编著的《The Design of the UNIX Operating System》。Prentice Hall, Englewood Cliffs, NJ 出版，1986。

Evi Nemeth、Garth Snyder 和 Scott Seebas 合著的《UNIX System Administration Handbook》。Prentice Hall, Englewood Cliffs, NJ 出版，1989。

◆ ◆ ◆ 附 录 B

使用 CDE 操作在 Trusted Extensions 中安装区域

本附录介绍如何使用 Trusted CDE 操作在 Trusted Extensions 中配置有标签区域。如果您运行的是不带修补程序的 Solaris 10 11/06 发行版，或者您已熟悉这些操作，请使用 Trusted CDE 操作。要使用 `txzonemgr` 脚本，请参见第 60 页中的 “创建有标签区域”。

使用 CDE 操作将网络接口与区域关联（任务列表）

请仅执行以下任务之一。有关折衷方案，请参见第 24 页中的 “规划多级别访问”。

任务	说明	参考
共享逻辑接口。	将全局区域映射到一个 IP 地址，将有标签区域映射到其他 IP 地址。	第 137 页中的 “使用 CDE 操作为系统指定两个 IP 地址”
共享物理接口。	将所有区域映射到一个 IP 地址。	第 139 页中的 “使用 CDE 操作为系统指定一个 IP 地址”

▼ 使用 CDE 操作为系统指定两个 IP 地址

在此配置中，主机的地址仅应用于全局区域。有标签区域与全局区域共享第二个 IP 地址。

开始之前 您是全局区域中的超级用户。系统已经指定有两个 IP 地址。您位于 Trusted CDE 工作区中。

1 **导航到 Trusted_Extensions 文件夹。**

   a. **在后台单击鼠标右键。**

   b. **从 "Workspace"（工作区）菜单中，选择 "Applications"（应用程序）→"Application Manager"（应用程序管理器）。**

   c. **双击 Trusted_Extensions 文件夹图标。**
      此文件夹包含用于设置接口、LDAP 客户机和有标签区域的操作。

2 **双击 "Share Logical Interface"（共享逻辑接口）操作并回答提示。**

注 – 系统必须已经指定有两个 IP 地址。对于此操作，请提供第二个地址以及该地址对应的主机名。第二个地址是共享地址。

```
Hostname:       Type the name for your labeled zones interface
IP Address:     Type the IP address for the interface
```

此操作会为主机配置多个 IP 地址。全局区域的 IP 地址是主机的名称。有标签区域的 IP 地址采用不同的主机名。此外，有标签区域的 IP 地址与全局区域共享。使用此配置时，有标签区域能够访问网络打印机。

提示 – 对有标签区域使用标准命名约定。例如，将 `-zones` 添加到主机名中。

---

3 **可选在终端窗口中，检验操作的结果。**

```
# ifconfig -a
```

例如，以下输出结果显示了有标签区域的网络接口 `192.168.0.12` 上的共享逻辑接口 `hme0:3`。`hme0` 接口是全局区域的唯一 IP 地址。

```
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
```

从 Solaris 10 10/08 发行版开始，回送接口 `lo0` 也是 `all-zones` 接口：

```
 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
...
```

▼ 使用 CDE 操作为系统指定一个 IP 地址

在此配置中，主机的地址将应用于所有区域，包括有标签区域。

开始之前 您是全局区域中的超级用户。您位于 Trusted CDE 工作区中。

1. **导航到 Trusted_Extensions 文件夹。**

   a. **在后台单击鼠标右键。**

   b. **从 "Workspace"（工作区）菜单中，选择 "Applications"（应用程序）→"Application Manager"（应用程序管理器）。**

   c. **双击 Trusted_Extensions 文件夹图标。**
      此文件夹包含用于设置接口、LDAP 客户机和有标签区域的操作。

2. **双击 "Share Physical Interface"（共享物理接口）操作。**
   此操作会为主机配置一个 IP 地址。全局区域不具有唯一地址。此系统不能用作多级别打印服务器或 NFS 服务器。

3. **可选在终端窗口中，检验操作的结果。**

   ```
   # ifconfig -a
   ```

   共享物理接口操作将所有区域配置为具有逻辑 NIC。这些逻辑 NIC 在全局区域中共享一个物理 NIC。

   例如，以下输出结果显示了所有区域的网络接口 `192.168.0.11` 上的共享物理接口 `hme0`。

   ```
   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
   ```

   从 Solaris 10 10/08 发行版开始，回送接口 `lo0` 也是 `all-zones` 接口：

   ```
     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
   ...
   ```

准备使用 CDE 操作创建区域（任务列表）

以下任务列表介绍了准备系统以创建区域的任务。有关区域创建方法的讨论，请参见第 23 页中的“在 Trusted Extensions 中规划区域”。

任务	说明	参考
1. 命名每个区域，并将区域名称与区域标签关联起来。	使用某一版本的区域标签命名每个有标签区域，然后将该名称与 Solaris Management Console 中的标签相关联。	第 140 页中的“使用 CDE 操作指定区域名称和区域标签”
2. 在创建区域前配置网络。	为每台主机上的网络接口指定一个标签，然后进行进一步的配置。	《Oracle Solaris Trusted Extensions 管理员规程》中的“配置可信网络数据库（任务列表）”

▼ 使用 CDE 操作指定区域名称和区域标签

您不必为 `label_encodings` 文件中的每个标签创建一个区域，但您可以这样做。`tnzonecfg` 数据库会枚举可在此系统中为其创建区域的标签。

1. **导航到 Trusted_Extensions 文件夹。**
   a. **在后台单击鼠标右键。**
   b. **从 "Workspace"（工作区）菜单中，选择 "Applications"（应用程序）→"Application Manager"（应用程序管理器）。**
   c. **双击 Trusted_Extensions 文件夹图标。**
2. **对于每个区域，对区域进行命名。**
   a. **双击 "Configure Zone"（配置区域）操作。**
   b. **在出现提示时，提供名称。**

   提示 – 为区域指定一个与区域标签类似的名称。例如，标签为 `CONFIDENTIAL : INTERNAL USE ONLY` 的区域的名称可以为 `internal`。
3. **对每个区域重复 "Configure Zone"（配置区域）操作。**

   例如，缺省 `label_encodings` 文件包含以下标签：

```
PUBLIC
CONFIDENTIAL: INTERNAL USE ONLY
CONFIDENTIAL: NEED TO KNOW
```

```
CONFIDENTIAL: RESTRICTED
SANDBOX: PLAYGROUND
MAX LABEL
```

虽然您可以运行 "Configure Zone"（配置区域）操作六次来为每个标签创建一个区域，但是请考虑创建下面的区域：

- 在适用于所有用户的系统上，为 PUBLIC 标签创建一个区域，为 CONFIDENTIAL 标签创建三个区域。
- 在适用于开发者的系统上，为 SANDBOX: PLAYGROUND 标签创建一个区域。对于开发者而言，由于 SANDBOX: PLAYGROUND 定义为不相交标签，所以只有开发者使用的系统需要此标签对应的区域。
- 不要为 MAX LABEL 标签创建区域，该标签定义为安全许可。

4 打开 "Trusted Network Zones"（可信网络区域）工具。

Solaris Management Console 中的工具旨在防止用户错误。这些工具可检查语法错误，并自动以正确的顺序运行命令来更新数据库。

a. 启动 Solaris Management Console。

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

b. 打开本地系统的 Trusted Extensions 工具箱。

i. 选择 "Console"（控制台）→"Open Toolbox"（打开工具箱）。

ii. 选择名为 This Computer (*this-host*: Scope=Files, Policy=TSOL) 的工具箱。

iii. 单击 "Open"（打开）。

c. 在 "System Configuration"（系统配置）下，导航到 "Computers and Networks"（计算机和网络）。

在出现提示时提供口令。

d. 双击 "Trusted Network Zones"（可信网络区域）工具。

5 对于每个区域，将相应的标签与区域名称相关联。

a. 选择 "Action"（操作）→"Add Zone Configuration"（添加区域配置）。

该对话框将显示没有指定的标签的区域名称。

b. 查看区域名称，然后单击 "Edit"（编辑）。

c. **在标签生成器中，针对区域名称单击适当的标签。**

如果单击了错误的标签，请再次单击该标签以将其取消选中，然后单击正确的标签。

d. **保存指定。**

在标签生成器中单击 "OK"（确定），然后在 "Trusted Network Zones Properties"（可信网络区域属性）对话框中单击 "OK"（确定）。

当所需的每个区域都列在面板中时，或者 "Add Zone Configuration"（添加区域配置）菜单项打开的对话框没有区域名称的值时，则说明您已完成。

故障排除 如果 "Trusted Network Zones Properties"（可信网络区域属性）对话框不提示您要创建的区域，则要么是区域网络配置文件不存在，要么是您已经创建了该文件。

- 检查区域网络配置文件是否尚不存在。在面板中查找相应名称。
- 如果该文件不存在，请运行 "Configure Zone"（配置区域）操作以提供区域名称。然后，重复步骤 5 以创建该文件。

使用 CDE 操作创建有标签的区域（任务列表）

可以为可信网络区域配置数据库中的每项创建一个区域。您通过运行 "Configure Zone"（配置区域）操作在第 140 页中的 “使用 CDE 操作指定区域名称和区域标签”中生成相应项。

应用程序管理器中的 Trusted_Extensions 文件夹包含以下用于创建有标签区域的操作：

- 配置区域－针对每个区域名称创建区域配置文件
- 安装区域－将正确的软件包和文件系统添加到区域
- 区域终端控制台－提供用于在区域中查看事件的窗口
- 针对 LDAP 初始化区域－使区域成为 LDAP 客户机，并准备区域以便进行引导
- 启动区域－引导区域，然后启动所有服务管理框架 (service management framework, SMF) 服务器
- 关闭区域－将区域的状态从 "Started"（已启动）更改为 "Halted"（已停止）

任务的完成顺序如下。

任务	说明	参考
1. 安装并引导一个区域。	创建第一个有标签区域。安装软件包，使区域成为 LDAP 客户机，然后启动区域中的所有服务。	第 143 页中的 “使用 CDE 操作安装、初始化并引导有标签区域”

任务	说明	参考
2. 定制区域。	删除不需要的服务。如果您打算复制或克隆区域，请删除特定于区域的信息。	第 147 页中的 “在 Trusted Extensions 中定制引导的区域”
3. 创建其他区域。	使用以下方法之一创建其他区域。您可在第 41 页中的 “在启用 Trusted Extensions 之前做出系统和安全决策”中选择方法。	
	从头开始创建每个区域。	第 143 页中的 “使用 CDE 操作安装、初始化并引导有标签区域” 第 145 页中的 “在 Trusted CDE 中解析本地区域与全局区域间的路由” 第 147 页中的 “在 Trusted Extensions 中定制引导的区域”
	将第一个有标签区域复制到其他标签。对所有区域重复进行该操作。	第 148 页中的 “在 Trusted Extensions 中使用复制区域方法”
	使用 ZFS 快照从第一个有标签区域克隆其他区域。	第 149 页中的 “在 Trusted Extensions 中使用克隆区域方法”

▼ 使用 CDE 操作安装、初始化并引导有标签区域

由于创建区域涉及复制整个操作系统，所以该过程很耗时。较快的过程是创建一个区域，使该区域成为其他区域的模板，然后复制或克隆该区域模板。

开始之前 您已完成第 140 页中的 “使用 CDE 操作指定区域名称和区域标签”。

如果使用 LDAP 作为命名服务，则您已完成第 57 页中的 “使全局区域成为 Trusted Extensions 中的客户机”。

如果要克隆区域，则您已完成第 51 页中的 “创建用于克隆区域的 ZFS 池”。在以下过程中，您将安装所准备的区域。

1 在 Trusted_Extensions 文件夹中，双击 "Install Zone"（安装区域）操作。

a. 键入要安装的区域的名称。

此操作会创建一个有标签的虚拟操作系统。完成此步骤需要花费一些时间。"Install Zone"（安装区域）正在运行时请勿执行其他任务。

```
# 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. 打开控制台以监视已安装区域中的事件。

i. 双击 "Zone Terminal Console"（区域终端控制台）操作。

ii. 键入刚安装的区域的名称。

2 初始化区域。

- **如果您在使用 LDAP，请双击 "Initialize Zone for LDAP"（针对 LDAP 初始化区域）操作。**

  ```
  Zone name:                    Type the name of the installed zone
  Host name for the zone:       Type the host name for this zone
  ```

  例如，在具有共享逻辑接口的系统上，值将类似如下：

  ```
  Zone name:              public
  Host name for the zone: machine1-zones
  ```

  此操作会使有标签区域成为一个为全局区域提供服务的相同 LDAP 服务器的 LDAP 客户端。出现以下信息时说明此操作已完成：

  ```
  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 ***
  ```

- **如果您未在使用 LDAP，请通过执行以下步骤之一手动初始化区域。**

  Trusted Extensions 中的手动过程与 Solaris OS 的过程相同。如果系统至少有一个 `all-zones` 接口，则所有区域的主机名必须与全局区域的主机名匹配。通常，在区域初始化期间对问题的回答与对全局区域的回答相同。

  通过执行以下操作之一提供主机信息：

  - **在步骤 3 中启动区域后，回答区域终端控制台中有关系统特征的问题。**

    您的回答将用于置备区域中的 `sysidcfg` 文件。

注 – 您必须确保 Trusted CDE 桌面中存在从有标签区域到全局区域的路由。有关过程，请参见第 145 页中的 “在 Trusted CDE 中解析本地区域与全局区域间的路由”。

- **在步骤 3 中引导区域之前，在区域的 `/etc` 目录中放置一个定制 `sysidcfg` 文件。**

3. **双击 "Start Zone"（启动区域）操作。**

   回答提示。

   ```
   Zone name:      Type the name of the zone that you are configuring
   ```

   此操作会引导区域，然后启动在该区域中运行的所有服务。有关服务的详细信息，请参见 `smf(5)` 手册页。

   "Zone Terminal Console"（区域终端控制台）会跟踪区域引导进度。控制台中会显示类似如下的消息：

   ```
   [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. **监视控制台输出。**

   在继续第 147 页中的 “在 Trusted Extensions 中定制引导的区域”之前，请确保已重新引导区域。以下控制台登录提示表明已重新引导区域。

   ```
   hostname console login:
   ```

故障排除 对于 "Install Zone"（安装区域）：如果显示类似如下的警告：`Installation of these packages generated errors: SUNW`*pkgname*，请阅读安装日志并完成软件包安装。

▼ 在 Trusted CDE 中解析本地区域与全局区域间的路由

要使每个区域可访问 Trusted CDE，必须解析 `DISPLAY` 变量。在 Trusted CDE 中，要解析该变量，有标签区域的节点名称、全局区域的节点名称和 all-zones 接口的节点名称必须解析为相同的名称。

开始之前 您正在使用 Trusted CDE 并在手动初始化有标签的区域。

1 **通过使用以下方法之一使 Trusted CDE 可显示在区域的标签下。**

- **方法 1：使 X 服务器可与其他系统进行通信**

  在此配置中，有标签区域可通过全局区域中的 X 服务器访问其他系统。

  a. **确保 `/etc/nodename` 文件指定系统的名称。**

  ```
  ## /etc/nodename
  machine1
  ```

  b. **确保 `/etc/hosts` 文件指定系统的名称。**

  ```
  ## /etc/hosts
  192.168.2.3  machine1 loghost
  ```

  要使 ToolTalk 服务正常工作，系统的名称必须位于 `loghost` 所在的同一行上。

  c. **确保 `/etc/hostname.`*interface* 文件指定系统的名称。**

  在此配置中，`machine1` 是 Trusted CDE 的 all-zones 接口。

  ```
  ## /etc/hostname.bge0
  machine1 all-zones
  ```

- **方法 2：将 X 服务器通信限制于本地系统。**

  在此配置中，有标签区域可以与本地系统上的 X 服务器进行通信。但是，本地 X 服务器与网络上的其他系统之间不存在路由。相应路由必须使用其他接口。

  a. **确保 `/etc/nodename` 文件指定系统的名称。**

  ```
  ## /etc/nodename
  machine1
  ```

  b. **确保 `/etc/hosts` 文件指定系统的名称。**

  从 Solaris 10 10/08 发行版开始，`lo0` 是 all-zones 接口。在这种情况下，该文件的显示类似如下：

  ```
  ## /etc/hosts
  127.0.0.1  localhost  machine1 loghost
  ```

  您也可以使用 `vni0` 接口。

  要使 ToolTalk 服务正常工作，系统的名称必须位于 `loghost` 所在的同一行上。

- **方法 3：采用其他方式解析 `DISPLAY` 变量，例如，每个区域逻辑接口上的可路由地址。**

  有关该过程，请参见第 74 页中的 “将网络接口和路由添加到有标签区域”。

2 **要引导区域，请返回到第 143 页中的 “使用 CDE 操作安装、初始化并引导有标签区域”中的步骤 3。**

▼ 在 Trusted Extensions 中定制引导的区域

如果要克隆区域，此过程可将某个区域配置为其他区域的模板。此外，此过程还可配置区域以供使用。

1 确保区域已完全启动。

a. 在“*zone-name*：区域终端控制台”中，以 root 用户身份登录。

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

b. 检查该区域是否正在运行。

状态 `running` 表示至少一个进程正在区域中运行。

```
# zoneadm list -v
ID NAME         STATUS         PATH
 2 public       running        /
```

c. 检查该区域可与全局区域通信。

X 服务器在全局区域中运行。每个有标签区域必须能够与全局区域相连接才能使用此服务。因此，在可以使用区域之前，区域联网必须正常。有关帮助，请参见第 98 页中的 “有标签区域无法访问 X 服务器”。

2 在区域终端控制台中，禁用有标签区域中不需要的服务。

如果要复制或克隆此区域，您禁用的服务将会在新区域中被禁用。在您的系统上处于联机状态的服务依赖于区域的服务清单。使用 `netservices limited` 命令可关闭有标签区域不需要的服务。

a. 删除多数不需要的服务。

```
# netservices limited
```

b. 列出剩余的服务。

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

c. 禁用图形登录。

```
# 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
```

有关服务管理框架的信息，请参见 `smf(5)` 手册页。

3 **关闭区域。**

选择以下方式之一：

- **运行 "Shut Down Zone"（关闭区域）操作。**

  提供区域的名称。

- **在全局区域的终端窗口中，使用 `zlogin` 命令。**

  ```
  # zlogin zone-name init 0
  ```

  有关更多信息，请参见 `zlogin(1)` 手册页。

4 **检验该区域是否已关闭。**

在“*zone-name*：区域终端控制台”中，以下消息表明区域已关闭。

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

如果不复制或克隆此区域，请使用创建此第一个区域的方式创建其余的区域。

5 **如果要将此区域用作其他区域的模板，请执行以下操作：**

a. **删除 `auto_home_`*zone-name* 文件。**

在全局区域的终端窗口中，从 *zone-name* 区域删除此文件。

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

例如，如果 `public` 区域是用于克隆其他区域的基础，请删除它的 `auto_home` 文件：

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

接下来的步骤

- 如果要复制某个区域，请转至第 148 页中的“在 Trusted Extensions 中使用复制区域方法”。
- 如果要克隆某个区域，请转至第 149 页中的“在 Trusted Extensions 中使用克隆区域方法”。

▼ 在 Trusted Extensions 中使用复制区域方法

开始之前

- 您已完成第 140 页中的“使用 CDE 操作指定区域名称和区域标签”。
- 您已在第 142 页中的“使用 CDE 操作创建有标签的区域（任务列表）”中定制了某个用作克隆模板的区域。
- 您当前未在运行用作克隆模板的区域。
- 显示 Trusted_Extensions 文件夹。

1. **对于要创建的每个区域，双击 "Copy Zone"（复制区域）操作。**

   回答提示。

   ```
   New Zone Name:          Type name of target zone
   From Zone Name:         Type name of source zone
   ```

注意 – 请勿在完成此任务的过程中执行其他任务。

2. **创建区域后，检查每个区域的状态。**

   a. **双击 "Zone Terminal Console"（区域终端控制台）操作。**

   b. **登录到每个区域。**

   c. **完成第 70 页中的“检验区域的状态”。**

▼ 在 Trusted Extensions 中使用克隆区域方法

开始之前

- 您已完成第 140 页中的“使用 CDE 操作指定区域名称和区域标签”。
- 您已完成第 51 页中的“创建用于克隆区域的 ZFS 池”。
- 您已通过完成第 51 页中的“创建用于克隆区域的 ZFS 池”创建了区域模板。
- 您已在第 142 页中的“使用 CDE 操作创建有标签的区域（任务列表）”中定制了某个用作克隆模板的区域。
- 用作克隆模板的区域已关闭。
- 显示 Trusted_Extensions 文件夹。

1. **创建区域模板的 Solaris ZFS 快照。**

   ```
   # cd /
   # zfs snapshot zone/zone-name@snapshot
   ```

   您可以使用此快照来克隆其余的区域。对于名为 `public` 的已配置区域，快照命令如下：

   ```
   # zfs snapshot zone/public@snapshot
   ```

2. **对于要创建的每个区域，双击 "Clone Zone"（克隆区域）操作。**

   回答提示。

   ```
   New Zone Name:          Type name of source zone
   ZFS Snapshot:             Type name of snapshot
   ```

3. **阅读对话框中的信息。**

   ```
   Zone label is <LABEL>
   zone-name is ready for booting
   ```

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

4 **对于每个区域，运行 "Start Zone"（启动区域）操作。**
在运行其他区域的操作之前启动每个区域。

5 **创建区域后，检查每个区域的状态。**

a. **双击 "Zone Terminal Console"（区域终端控制台）操作。**

b. **完成第 70 页中的“检验区域的状态”。**

◆ ◆ ◆ 附 录 C

Trusted Extensions 的配置核对表

此核对表提供了 Trusted Extensions 的主要配置任务的概述。并在主要任务中列出了更小的任务。核对表不能代替本指南中的步骤。

用于配置 Trusted Extensions 的核对表

以下汇总了在站点上启用和配置 Trusted Extensions 所需执行的操作。其中交叉引用了别处介绍的任务。

1. 阅读。
   - 阅读《Oracle Solaris Trusted Extensions 管理员规程》的前五章。
   - 了解站点安全要求。
   - 阅读第 132 页中的 “站点安全策略和 Trusted Extensions”。
2. 准备。
   - 确定 `root` 口令。
   - 确定 PROM 或 BIOS 安全级别。
   - 确定 PROM 或 BIOS 口令。
   - 确定是否允许连接外围设备。
   - 确定是否允许访问远程打印机。
   - 确定是否允许访问无标签的网络。
   - 确定区域创建方法。
3. 启用 Trusted Extensions。
   a. 安装 Oracle Solaris OS。
      - 对于远程管理，请安装开发者群组或更大的 Solaris 软件包组。
      - 对于克隆区域创建方法，请选择 "Custom Install"（定制安装），然后安排 `/zone` 分区。
   b. 启用 Trusted Extensions 服务 `svc:/system/labeld`。
4. 如果使用 IPv6，则为 Trusted Extensions 启用 IPv6。

5. 如果使用不同于 1 的 DOI，请在 /etc/system 和 /etc/security/tsol/tnrhtp 文件中设置 DOI。
6. （可选的）创建用来克隆区域的 ZFS 池。
7. 配置标签。
   a. 完成您的站点的 label_encodings 文件。
   b. 检查并安装该文件。
   c. 重新引导。
8. 为全局区域和有标签区域配置接口。
9. 配置 Solaris Management Console。
10. 配置命名服务。
    - 使用文件命名服务（无需配置）。
    - 或者，配置 LDAP
      a. 创建一个 Trusted Extensions 代理服务器或 Trusted Extensions LDAP 服务器。
      b. 使 Solaris Management Console 服务器能够接受网络连接。
      c. 向 LDAP 注册 Solaris Management Console。
      d. 为 Solaris Management Console 创建 LDAP 工具箱。
11. 为 LDAP 配置网络连接。
    - 在远程主机模板中，将一个 LDAP 服务器或代理服务器指定给 cipso 主机类型。
    - 在远程主机模板中，将本地系统指定给 cipso 主机类型。
    - 使本地系统成为 LDAP 服务器的客户机。
12. 创建有标签区域。
    - 选项 1：使用 txzonemgr script（txzonemgr 脚本） 脚本。
    - 选项 2：使用 Trusted CDE 操作。
      a. 配置有标签区域
         i. 在 Solaris Management Console 中，将区域名称与特定标签进行关联。
         ii. 运行 "Configure Zone"（配置区域）操作。
      b. 运行 "Install Zone"（安装区域）操作。
      c. 运行 "Initialize for LDAP"（为 LDAP 进行初始化）操作。
      d. 运行 "Start Zone"（启动区域）操作。
      e. 定制正在运行的区域。
      f. 运行 "Shut Down Zone"（关闭区域）操作。
      g. 在区域关闭后定制区域。
      h. （可选的）创建 ZFS 快照。
      i. 从头开始创建其余区域，或者通过使用 "Copy Zone"（复制区域）或 "Clone Zone"（克隆区域）操作创建其余区域。

13. 配置网络。请参见《Oracle Solaris Trusted Extensions 管理员规程》中的“配置可信网络数据库（任务列表）”。
    - 标识单标签主机和有限范围主机。
    - 确定要应用于来自无标签主机的传入数据的标签。
    - 定制远程主机模板。
    - 将各个主机指定给模板。
    - 为模板指定子网。
14. 建立静态路由。请参见《Oracle Solaris Trusted Extensions 管理员规程》中的“在 Trusted Extensions 中配置路由并检查网络信息（任务列表）”。
15. 配置本地用户和本地管理角色。
    - 要强制实现职责分离，请创建定制权限配置文件。
    - 创建 "Security Administrator"（安全管理员）角色。
    - 创建一个可以担任安全管理员角色的本地用户。
    - 创建其他角色，以及要担任这些角色的其他本地用户。
16. 在 NFS 服务器上创建起始目录。
    - 在用户可以访问的每个标签处为每个用户创建起始目录。
    - （可选的）阻止用户从其较低级别的起始目录进行读取。
17. 配置打印。请参见《Oracle Solaris Trusted Extensions 管理员规程》中的“在 Trusted Extensions 中管理打印（任务列表）”。
18. 配置设备。请参见《Oracle Solaris Trusted Extensions 管理员规程》中的“在 Trusted Extensions 中操作设备（任务列表）”。
    a. 为角色指定 "Device Management"（设备管理）配置文件或 "System Administrator"（系统管理员）配置文件。
    b. 要使设备可用，请执行以下操作之一：
        - 逐个系统地使设备成为可分配的。
        - 为选定的用户和角色指定 "Allocate Device"（分配设备）授权。
19. 配置 Oracle Solaris 功能。
    - 配置审计。
    - 配置安全设置。
    - 使特定的 LDAP 客户机充当 LDAP 管理系统。
    - 配置 LDAP 中的用户。
    - 配置 LDAP 中的网络角色。
    - 挂载并共享文件系统。请参见《Oracle Solaris Trusted Extensions 管理员规程》中的第 11 章 “在 Trusted Extensions 中管理和挂载文件（任务）”

词汇表

accreditation range（认可范围） 一类用户或资源的获得批准的一组敏感标签。一组有效标签。另请参见 system accreditation range（系统认可范围）和 user accreditation range（用户认可范围）。

administrative role（管理角色） 一种 role（角色），提供必需的授权、特权命令、特权操作和可信路径 security attribute（安全属性），以允许该角色执行管理任务。角色执行一部分 Solaris 超级用户的权能，例如备份或审计。

allocation（分配） 一种机制，用于控制对 device（设备）的访问。请参见 device allocation（设备分配）。

application search path（应用程序搜索路径） 在 CDE 中，system（系统）使用搜索路径来查找应用程序和某些配置信息。应用程序搜索路径由 trusted role（可信角色）控制。

authorization（授权） 授予用户或角色执行某个操作的权限，如果未获得授权，安全策略将不允许执行该操作。授权是在权限配置文件中设置的。特定命令需要用户具备特定授权才能成功执行。例如，要打印 PostScript 文件，需要具有打印 Postscript 授权。

CDE 请参见 Common Desktop Environment（公用桌面环境）。

CIPSO label（CIPSO 标签） 通用 IP 安全选项。CIPSO 是 Trusted Extensions 实施的标签标准。

classification（等级） clearance（安全许可）或 label（标签）的分层组件。等级表示有层次的安全性级别，例如 `TOP SECRET` 或 `UNCLASSIFIED`。

clearance（安全许可） 用户可工作的标签集合的上限。下限是由 security administrator（安全管理员）指定的 minimum label（最小标签）。安全许可可以是两种类型（会话安全许可或 user clearance（用户安全许可））之一。

client（客户机） 连接到网络的系统。

closed network（封闭式网络） 配置有 Trusted Extensions 的系统组成的网络。该网络与任何非 Trusted Extensions 主机分离。这种分离可能是物理的，其中没有网线扩展至 Trusted Extensions 网络之外。这种分离也可能是在软件中实施的，其中 Trusted Extensions 主机只能识别 Trusted Extensions 主机。来自网络之外的数据项将被限制于与 Trusted Extensions 主机连接的外围设备。与 open network（开放式网络）相对。

Common Desktop Environment（公用桌面环境） 用于管理 Trusted Extensions 软件的历史窗口环境。Trusted Extensions 可修改该环境以创建 Trusted CDE。也可以修改 Oracle Java Desktop System 以创建 Trusted JDS。

compartment（区间） label（标签）的一个无层次组件，与 classification（等级）组件结合使用以构成 clearance（安全许可）或 label（标签）。区间代表信息的集合，例如，将供工程部门或多学科项目团队使用。

.copy_files file（.copy_files 文件） 多标签系统上的可选设置文件。此文件包含一系列启动文件，例如 `.cshrc` 或 `.mozilla`，用户环境或用户应用程序需要这些文件以使系统或应用程序正常运行。`.copy_files` 中列出的文件然后会被**复制**到较高级别标签的用户起始目录（如果创建了这些目录）。另请参见 .link_files file（.link_files 文件）。

DAC 请参见 discretionary access control（自主访问控制）。

device allocation（设备分配） 一种机制，用于保护可分配 device（设备）上的信息免受分配该设备的用户之外的任何人访问。在设备被解除分配之前，只有分配设备的用户可以访问与该设备相关的信息。要使用户可以分配某个设备，该用户必须已由 security administrator（安全管理员）授予了设备分配授权。

device（设备） 设备包括打印机、计算机、磁带机、软盘驱动器、CD-ROM 驱动器、DVD 驱动器、音频设备和内部伪终端设备。设备受 read-equal/write-equal MAC 策略约束。对可移除设备（例如 DVD 驱动器）的访问由 device allocation（设备分配）控制。

discretionary access control（自主访问控制） 文件或目录的所有者自主授予或拒绝的访问类型。Trusted Extensions 提供两种自主访问控制 (discretionary access control, DAC)，即 UNIX permission bits（权限位）和 ACL。

domain name（域名） 标识本地网络上的一组系统。域名包括一系列用句点分隔的组件名称（例如：`example1.town.state.country.org`）。在一个域名中，越靠右的组件名称所标识的网域范畴越广（通常指远程区域）。

domain of interpretation, DOI（系统解释域） 在配置有 Trusted Extensions 的 Solaris 系统上，系统解释域用于区分可能定义了相似标签的不同 `label_encodings` 文件。DOI 是一组规则，可将网络包上的安全属性转换为按本地 `label_encodings` 文件表示这些安全属性。当系统具有相同的 DOI 时，它们将共享该组规则，并可以转换有标签的网络包。

domain（域） Internet 命名分层结构的一部分。它代表本地网络上一组共享管理文件的系统。

evaluated configuration（评估配置） 在一个已由认证机构认定为符合特定标准的配置中运行的一个或多个 Trusted Extensions 主机。在美国，这些标准是 TCSEC。评估和认证机构是 NSA。

- Solaris 10 11/06 发行版上配置的 Trusted Extensions 软件通过了通用标准 v2.3 [2005 年 8 月]（ISO 标准）、评估保证级 (Evaluation Assurance Level, EAL) 4 和许多保护框架的认证。
- 通过保证连续性，经过 NSA 认证的 Trusted Extensions 软件已配置在 Solaris 10 5/09 发行版上。

通用标准 v2 (Common Criteria v2, CCv2) 和保护框架通过级别 B1+ 使早期的 TCSEC U.S. 标准过时。美国、英国、加拿大、丹麦、荷兰、德国和法国已签署了 CCv2 互认协议。

Trusted Extensions 配置目标提供与 TCSEC C2 和 B1 级别类似的功能以及一些其他功能。

file system（文件系统） 文件和目录的集合，在设置到逻辑分层结构时，组成一组有条理的结构化信息。可以从本地 system（系统）或远程系统挂载文件系统。

GFI
Government Furnished Information（政府提供的信息）。在本手册中，是指美国政府提供的 label_encodings file（label_encodings 文件）。要将 GFI 用于 Trusted Extensions 软件，必须将 Oracle 专用的 `LOCAL DEFINITIONS` 部分添加到 GFI 的末尾。有关详细信息，请参见《Trusted Extensions Label Administration》中的第 5 章 “Customizing LOCAL DEFINITIONS”。

host name（主机名）
使网络上的其他系统能够识别某个 system（系统）的名称。此名称在给定域内的所有系统之间必须唯一。通常，域标识一个组织。主机名可以是字母、数字和减号 (–) 的任意组合，但不能以减号开头或结尾。

initial label（初始标签）
指定给用户或角色的 minimum label（最小标签），用户初始工作区的标签。初始标签是用户或角色可在其中工作的最低级别标签。

initial setup team（初始设置团队）
一个至少由两人组成的团队，他们一起监视 Trusted Extensions 软件的启用和配置。一名团队成员负责安全决策，另一名成员负责系统管理决策。

IP address（IP 地址）
Internet 协议地址。标识某个联网系统使其可通过 Internet 协议进行通信的唯一数字。在 IPv4 中，该地址由四个以句点分隔的数字组成。IP 地址的每一部分通常是一个 0 到 225 之间的数字。但第一个数字必须小于 224，最后一个数字不能是 0。

IP 地址在逻辑上分为两部分：网络和网络上的 system（系统），网络号类似于电话区号。相对于网络，系统编号类似于电话号码。

label configuration（标签配置）
Trusted Extensions 的单标签或多标签敏感标签安装选项。在大多数情况下，标签配置在您站点上的所有系统上都相同。

label_encodings file（label_encodings 文件）
在该文件中定义完整的 sensitivity label（敏感标签），比如，认可范围、标签视图、缺省标签可见性、缺省用户安全许可以及标签的其他各方面。

label range（标签范围）
指定给命令、区域和可分配设备的一组敏感标签。通过指定最大标签和最小标签来指定范围。对于命令，最小标签和最大标签限定可在其中执行命令的标签。不识别标签的远程主机将被指定单个 sensitivity label（敏感标签），就像 security administrator（安全管理员）想要限制为单个标签的任何其他主机一样。标签范围限定可在其中分配设备的标签，并限定使用设备时可在其中存储或处理信息的标签。

label relationships（标签关系）
在配置有 Trusted Extensions 的 Solaris 系统上，一个标签可以支配另一个标签、等同于另一个标签或与另一个标签不相交。例如，标签 `Top Secret` 可支配标签 `Secret`。对于具有相同 domain of interpretation, DOI（系统解释域）的两个系统，一个系统上的标签 `Top Secret` 等同于另一个系统上的标签 `Top Secret`。

label set（标签集合）
请参见 security label set（安全标签集合）。

labeled host（有标签主机）
一个 labeled system（有标签系统），属于由有标签系统组成的可信网络的一部分。

labeled system（有标签系统）
有标签系统是运行多级别操作系统（例如 Trusted Extensions 或启用了 MLS 的 SELinux）的系统。该系统可以发送和接收在包标头中标有通用 IP 安全选项 (Common IP Security Option, CIPSO) 标签的网络包。

labeled zone（有标签区域） 在配置有 Trusted Extensions 的 Solaris 系统上，会为每个区域指定一个唯一标签。虽然会为全局区域添加标签，但**有标签区域**通常是指指定有标签的非全局区域。相比于 Solaris 系统上未配置标签的非全局区域，有标签区域有两个不同的特征。首先，有标签区域必须使用相同的用户 ID 和组 ID 池。第二，有标签区域可以共享 IP 地址。

label（标签） 指定给某个对象的安全标识符。标签基于该对象中信息应受到保护的级别。根据 security administrator（安全管理员）配置用户的方式，用户可以看到 sensitivity label（敏感标签），或者根本没有标签。标签在 label_encodings file（label_encodings 文件）中进行定义。

.link_files file（.link_files 文件） 多标签系统上的可选设置文件。此文件包含一系列启动文件，例如 `.cshrc` 或 `.mozilla`，用户环境或用户应用程序需要这些文件以使系统或应用程序正常运行。 `.link_files` 中列出的文件然后会被**链接**到较高级别标签的用户起始目录（如果创建了这些目录）。另请参见 .copy_files file（.copy_files 文件）。

MAC 请参见 mandatory access control（强制访问控制）。

mandatory access control（强制访问控制） 这种访问控制基于文件、目录或 device（设备）的 sensitivity label（敏感标签）与正在尝试进行访问的进程的敏感标签的比较。当位于一个标签的进程尝试读取位于较低级别标签的某个文件时，MAC 规则 read equal–read down 适用。当位于一个标签的进程尝试写入位于另一个标签的目录时，MAC 规则 write equal-read down 适用。

minimum label（最小标签） 用户的敏感标签的下界和系统的敏感标签的下界。security administrator（安全管理员）指定用户的安全属性时设置的最小标签是用户首次登录时第一个工作区的敏感标签。security administrator（安全管理员）在 `label_encodings` 文件的最小标签字段指定的敏感标签设置系统的下界。

multilevel desktop（多级别桌面） 在配置有 Trusted Extensions 的 Solaris 系统上，用户可以从特定的标签运行桌面。如果用户被授予从多个标签工作的权限，则该用户可以创建单独的工作区以从各个标签工作。在此多级别桌面上，授权的用户可以在不同标签的窗口之间进行剪切和粘贴，从不同的标签接收邮件，以及在不同标签的工作区中查看和使用标记窗口。

multilevel port, MLP（多级别端口） 在配置有 Trusted Extensions 的 Solaris 系统上，MLP 用于在区域中提供多级别服务。缺省情况下，X 服务器是在全局区域中定义的多级别服务。MLP 是通过端口号和协议指定的。例如，多级别桌面中 X 服务器的 MLP 是通过 6000-6003 和 TCP 指定的。

naming service（命名服务） 一个分布式网络数据库，它包含网络上所有系统的关键系统信息，以便系统能够彼此通信。使用命名服务，可以在网络范围的基础上维护、管理和访问系统信息。Oracle 支持 LDAP 命名服务。如果没有这样的服务，每个 system（系统）必须在本地 `/etc` 文件中维护各自的系统信息副本。

networked systems（联网系统） 通过硬件和软件相连的一组系统，有时称为局域网 (local area network, LAN)。系统联网时通常需要一个或多个服务器。

non-networked systems（非联网系统） 未连接到网络或不依赖于其他主机的计算机。

open network（开放式网络） 由 Trusted Extensions 主机组成的网络，以物理方式连接到其他网络，并使用 Trusted Extensions 软件与非 Trusted Extensions 主机进行通信。与 closed network（封闭式网络）相对。

outside the evaluated configuration（评估配置之外）
在已被证明能够满足 evaluated configuration（评估配置）标准的软件中配置了不满足安全标准的设置时，会将该软件描述为处于**评估配置之外**。

permission bits（权限位）
一种 discretionary access control（自主访问控制）类型，所有者指定一组数位来表示谁可以读取、写入或执行文件或目录。可为每个文件或目录指定三组不同的权限：一组适用于所有者，一组适用于所有者所在的组，一组适用于所有其他情况。

primary administrator（主管理员）
受委托来为组织创建新权限配置文件，以及解决超出 security administrator（安全管理员）和 system administrator（系统管理员）两者能力范围的计算机故障的人员。应当极少地使用此角色。进行初始安全配置后，更多安全站点可以选择不创建此角色，并不为主管理员配置文件指定任何角色。

privilege（特权）
授予正在执行某个命令的进程的权力。完整权限集合描述了系统的全部特权（从基本权能到管理权能）。绕开 security policy（安全策略）的特权（例如在系统上设置时钟）可由站点的 security administrator（安全管理员）授予。

process（进程）
代表调用命令的用户执行命令的操作。进程会接收来自用户的许多安全属性，包括用户 ID (user ID, UID)、组 ID (group ID, GID)、补充组列表和用户的审计 ID (audit ID, AUID)。进程接收的安全属性包括可用于所执行命令的任何特权和当前工作区的 sensitivity label（敏感标签）。

profile shell（配置文件 shell）
识别安全属性（例如特权、授权和特殊 UID 及 GID）的特殊 shell。配置文件 shell 通常会将用户限定于执行较少的命令，但可以允许这些命令以更多的权限运行。配置文件 shell 是 trusted role（可信角色）的缺省 shell。

remote host（远程主机）
与本地系统不同的系统。远程主机可以是 unlabeled host（无标签主机）或 labeled host（有标签主机）。

rights profile（权限配置文件）
适用于命令和 CDE 操作以及指定给这些可执行内容的安全属性的捆绑机制。权限配置文件允许 Solaris 管理员控制谁可以执行哪些命令，以及控制这些命令执行时具有的属性。当用户登录时，指定给该用户的所有权限都将生效，该用户可以访问该用户的所有权限配置文件中指定的所有命令、CDE 操作和授权。

role（角色）
角色与用户类似，只不过角色不能登录。通常，角色用于指定管理权能。角色会被限定于执行一组特定的命令、授权和 CDE 操作。请参见 administrative role（管理角色）。

security administrator（安全管理员）
必须对敏感信息进行保护的组织中，定义并强制实施站点的 security policy（安全策略）的人员。这些人员有权访问站点中所处理的所有信息。在软件中，会将安全管理员 administrative role（管理角色）指定给具有适当 clearance（安全许可）的一个或多个个人。这些管理员配置所有用户和主机的安全属性，以便软件可以强制实施站点的安全策略。与此对比，请参见 system administrator（系统管理员）。

security attribute（安全属性）
用于强制实施 Trusted Extensions security policy（安全策略）的属性。将会为 process（进程）、用户、区域、主机、可分配设备和其他对象指定各种安全属性集合。

security label set（安全标签集合）
为 tnrhtp database（tnrhtp 数据库）项指定一组独立的安全标签。指定给具有安全标签集合的模板的主机可以发送和接收与标签集合中任一标签匹配的包。

security policy（安全策略） Trusted Extensions 主机上，定义可以如何访问信息的 DAC、MAC 和标签设置规则集合。客户站点上，定义该站点上所处理信息敏感度的规则集合，以及用于保护信息免受未经授权的访问的措施。

sensitivity label（敏感标签） 指定给某个对象或过程的安全 label（标签）。该标签用于根据所含数据的安全级别来限定访问。

separation of duty（职责分离） 需要两个管理员或角色来创建和验证用户的安全策略。一个管理员或角色负责创建用户、用户起始目录和其他基本管理内容。另一个管理员或角色负责用户的安全属性，例如口令和标签范围。

Solaris Management Console 基于 Java 的管理 GUI，包含管理程序的 toolbox（工具箱）。大多数系统、网络和用户管理都是通过使用控制台工具箱完成的。

system accreditation range（系统认可范围） 根据 security administrator（安全管理员）在 label_encodings file（label_encodings 文件）中定义的规则创建的所有有效标签的集合，以及在配置有 Trusted Extensions 的每个系统上使用的两个管理标签。这两个管理标签为 `ADMIN_LOW` 和 `ADMIN_HIGH`。

system administrator（系统管理员） Trusted Extensions 中，指定给负责执行标准系统管理任务（例如设置用户帐户的非安全相关部分）的用户的 trusted role（可信角色）。与此对比，请参见 security administrator（安全管理员）。

system（系统） 计算机的通用名称。安装后，网络上的系统通常称为主机。

tnrhdb database（tnrhdb 数据库） 可信网络远程主机数据库。此数据库向远程主机指定一组标签特征。可在 `/etc/security/tsol/tnrhdb` 中以文件的形式访问该数据库，也可通过 LDAP 服务器访问该数据库。

tnrhtp database（tnrhtp 数据库） 可信网络远程主机模板。此数据库定义可指定给远程主机的标签特征集合。可在 `/etc/security/tsol/tnrhtp` 中以文件的形式访问该数据库，也可通过 LDAP 服务器访问该数据库。

toolbox（工具箱） Solaris Management Console 中的程序的集合。在 Trusted Extensions 主机上，管理员使用 `Policy=TSOL` 工具箱。每个工具箱都有在工具箱作用域内可用的程序。例如，"Trusted Network Zones"（可信网络区域）工具，该工具处理系统的 `tnzonecfg` 数据库，仅存在于 `Files` 工具箱中，因为它的作用域始终是本地。用户帐户程序存在于所有工具箱中。要创建本地用户，管理员会使用 `Files` 工具箱；要创建网络用户，管理员会使用 `LDAP` 工具箱。

trusted editor（可信编辑器） 在配置有 Trusted Extensions 的 Solaris 系统上，可信编辑器用于创建和修改管理文件。该编辑器不能修改文件名。此外，使用该编辑器要经过审计，并且将会禁用 shell 转义命令。在 Trusted CDE 中，"Admin Editor"（管理编辑器）操作可启动可信编辑器。在 Trusted JDS 中，`/usr/dt/bin/trusted_edit` 命令可启动可信编辑器。

Trusted Network databases（可信网络数据库） 可信网络远程主机模板 `tnrhtp` 和可信网络远程主机数据库 `tnrhdb` 一起定义可与 Trusted Extensions 通信的远程主机数据库。

trusted path（可信路径） 在配置有 Trusted Extensions 的 Solaris 系统上，可信路径是一种与系统交互时的可靠防篡改方式。可信路径用于确保管理功能不能受到威胁。必须受到保护的用户功能（例如更改口令）也使用可信路径。当可信路径处于活动状态时，桌面会显示防篡改指示器。

trusted role（可信角色） 请参见 administrative role（管理角色）。

trusted stripe（可信窗口条） 一个不能受到欺骗的区域。在 Trusted CDE 中，可信窗口条位于屏幕的底部；在 Trusted JDS 中，可信窗口条位于顶部。可信窗口条提供有关窗口系统状态的可视化反馈：可信路径指示器和窗口 sensitivity label（敏感标签）。当敏感标签配置为不可供用户查看时，可信窗口将缩小为一个仅显示可信路径指示器的图标。

txzonemgr script（txzonemgr 脚本） `/usr/sbin/txzonemgr` 脚本提供一个用于管理有标签区域的简单 GUI。该脚本还提供一些菜单项，这些菜单项适用于联网选项、名称服务选项以及使全局区域成为现有 LDAP 服务器的客户机。`txzonemgr` 由 root 用户在全局区域中运行。

unlabeled host（无标签主机） 发送无标签网络包的联网系统，例如正在运行 Solaris OS 的系统。

unlabeled system（无标签系统） 对于配置有 Trusted Extensions 的 Solaris 系统，无标签系统是未在运行多级别操作系统（例如 Trusted Extensions 或启用了 MLS 的 SELinux）的系统。无标签系统不发送有标签的包。如果正在进行通信的 Trusted Extensions 系统向无标签系统指定了单个标签，则 Trusted Extensions 系统和无标签系统之间的网络通信将从该标签进行。无标签系统也称为“单级别系统”。

user accreditation range（用户认可范围） 一般用户可在 system（系统）中工作的所有可能的标签集合。站点的 security administrator（安全管理员）在 label_encodings file（label_encodings 文件）文件中指定范围。定义 system accreditation range（系统认可范围）的良构标签规则还会受到该文件的 `ACCREDITATION RANGE` 部分的值的限制：上界、下界、组合约束和其他限制。

user clearance（用户安全许可） 设置用户可随时在其中工作的标签集合的上界的 clearance（安全许可）指定的 security administrator（安全管理员）。在任何特定的登录会话期间，用户可以决定接受缺省值或者可以进一步限制该安全许可。

索引

N

R

S

T

U

Z

安

备

编

标

操

出

初

共

故

关

管

规

检

角

日

删

审

使

收

手

添

网

站

帐

针

职

注

准