Trusted Extensions 管理员规程

文件号码 E38868
2013 年 1 月

ORACLE

130221@25097

目录

图

表

前言

《Trusted Extensions 管理员规程》介绍在 Oracle Solaris 操作系统 (Oracle Solaris OS) 中配置 Trusted Extensions 的过程。本指南还提供了用于管理通过 Trusted Extensions 软件设置标签的用户、区域、设备和主机的过程。

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》（《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 位和 32 位的 x86 兼容产品系列。
- x64 特指 64 位的 x86 兼容 CPU。
- “32 位 x86”指出了有关基于 x86 的系统的特定 32 位信息。

有关支持的系统，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和管理 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。

管理员应当熟悉 Oracle Solaris 管理。此外，管理员还应当了解以下事项：

- Trusted Extensions 的安全功能和您的站点安全策略
- 使用配置有 Trusted Extensions 的主机的基本概念和过程，如《Trusted Extensions User's Guide》中所述。
- 如何在站点角色之间划分管理任务

Trusted Extensions 指南丛书的结构

下表列出了 Trusted Extensions 指南中涵盖的主题以及每个指南的目标读者。

指南标题	主题	目标读者
《Trusted Extensions User's Guide》	介绍了 Trusted Extensions 的基本功能。该书包含一个词汇表。	最终用户、管理员、开发者
《Trusted Extensions Configuration Guide》	从 Solaris 10 5/08 发行版开始，介绍了如何启用和初始配置 Trusted Extensions。替代了《Solaris Trusted Extensions Installation and Configuration for the Solaris 10 11/06 and Solaris 10 8/07 Releases》。	管理员、开发者
《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

相关的系统管理指南

以下指南包含对您准备和运行 Trusted Extensions 软件非常有用的信息。

书名	主题
《Oracle Solaris 管理：基本管理》	用户帐户和组、服务器和客户机支持、关闭和启动系统、管理服务以及管理软件（软件包和修补程序）
《系统管理指南：高级管理》	终端和调制解调器、系统资源（磁盘配额、记帐和 crontab）、系统进程以及 Solaris 软件问题疑难解答
《System Administration Guide: Devices and File Systems》	可移除介质、磁盘和设备、文件系统以及备份和还原数据
《Oracle Solaris 管理：IP 服务》	TCP/IP 网络管理、IPv4 和 IPv6 地址管理、DHCP（动态主机配置协议）、Ipsec（Internet 协议安全）、IKE（Internet 密钥交换）、Solaris IP 过滤器、移动 IP、IP 网络多路径 (IP Network Multipathing, IPMP) 以及 IPQoS
《系统管理指南：名称和目录服务（DNS、NIS 和 LDAP）》	DNS、NIS 和 LDAP 命名和目录服务，包括从 NIS 转换到 LDAP 以及从 NIS+ 转换到 LDAP

书名	主题
《系统管理指南：网络服务》	Web 高速缓存服务器、与时间相关的服务、网络文件系统（NFS 和 Autofs）、邮件、SLP（服务定位协议）和 PPP（点对点协议）
《System Administration Guide: Security Services》	审计、设备管理、文件安全、BART（基本审计和报告工具）、Kerberos 服务、PAM（可插拔验证模块）、Solaris 加密框架、权限、RBAC（基于角色的存取控制）、SASL（简单身份认证和安全层）和 Solaris 安全 Shell
《系统管理指南：Oracle Solaris Containers－资源管理和 Oracle Solaris Zones》	资源管理主题项目和任务、扩展记帐、资源控制、公平份额调度器 (Fair Share Scheduler, FSS)、使用资源上限设置守护进程 (rcapd) 的物理内存控制，以及资源池；使用 Solaris Zones 软件分区技术和 lx 标记区域的虚拟功能
《Oracle Solaris ZFS 管理指南》	ZFS（Zettabyte 文件系统）存储池以及文件系统的创建和管理、快照、克隆、备份、使用访问控制列表 (Access Control List, ACL) 保护 ZFS 文件、在安装区域的 Solaris 系统中使用 ZFS、仿真卷以及故障排除和数据恢复
《系统管理指南：打印》	Solaris 打印主题和任务，使用服务、工具、协议和技术来设置及管理打印服务和打印机

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。对于第三方内容、产品和服务，Oracle Corporation 及其附属公司明确表示不承担任何种类的担保，亦不对其承担任何责任。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。

获取 Oracle 支持

Oracle 客户可以通过 My Oracle Support 获取电子支持。有关信息，请访问 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info，或访问 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs（如果您听力受损）。

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	#

表 P–2 shell 提示符 （续）

shell	提示符
C shell	machine_name%
C shell 超级用户	machine_name#

◆ ◆ ◆ 第 1 章

1 Trusted Extensions 管理概念

本章介绍如何管理配置有 Trusted Extensions 软件的系统。

Trusted Extensions 软件和 Oracle Solaris OS

Trusted Extensions 软件向运行 Solaris 操作系统 (Oracle Solaris OS) 的系统添加标签。标签实现**强制访问控制** (Mandatory Access Control, MAC)。MAC 与自主访问控制 (Discretionary Access Control, DAC) 一起保护系统主体（进程）和对象（数据）。Trusted Extensions 软件提供处理标签配置、标签指定和标签策略的界面。

Trusted Extensions 和 Oracle Solaris OS 之间的相似之处

Trusted Extensions 软件使用 Oracle Solaris OS 的权限配置文件、角色、审计、特权或其他安全功能。您可将 Oracle Solaris 安全 Shell (Solaris Secure Shell, SSH)、BART、Oracle Solaris 加密框架、IPsec 和 IP 过滤器与 Trusted Extensions 配合使用。

- 如同在 Oracle Solaris OS 中一样，可限制用户只使用执行其作业所需的应用程序。可授权其他用户执行更多作业。
- 如同在 Oracle Solaris OS 中一样，可将以前指定给超级用户的功能指定给单独的独立“角色”。
- 如同在 Oracle Solaris OS 中一样，特权可以保护进程。还可使用区域来分隔进程。
- 如同在 Oracle Solaris OS 中一样，可以对系统上的事件进行审计。
- Trusted Extensions 使用 Oracle Solaris OS 的系统配置文件，例如 `policy.conf` 和 `exec_attr`。

Trusted Extensions 和 Oracle Solaris OS 之间的不同之处

Trusted Extensions 软件扩展了 Oracle Solaris OS。以下列表进行了概述。有关快速参考，请参见附录 A，Trusted Extensions 管理快速参考。

- Trusted Extensions 使用称为**标签**的特殊安全标记控制对数据的访问。标签提供**强制访问控制** (Mandatory Access Control, MAC)。MAC 保护是对 UNIX 文件权限或自主访问控制 (Discretionary Access Control, DAC) 的补充。标签将直接指定给用户、区域、设备、窗口和网络端点。标签将隐式指定给进程、文件和其他系统对象。

  MAC 不会被一般用户覆盖。Trusted Extensions 要求一般用户在有标签区域中进行操作。缺省情况下，有标签区域中没有用户或进程可以覆盖 MAC。

  与在 Oracle Solaris OS 中一样，可以覆盖 MAC 时，可将覆盖安全策略的能力指定给特定进程或用户。例如，可授权用户更改文件的标签。此类操作会升级或降级该文件中信息的敏感度。
- Trusted Extensions 会添加到现有配置文件和命令中。例如，Trusted Extensions 会添加审计事件、授权、特权和权限配置文件。
- 一些在 Oracle Solaris 系统上可选的功能在 Trusted Extensions 系统上是必需的。例如，区域和角色在配置有 Trusted Extensions 的系统上是必需的。
- 一些在 Oracle Solaris 系统上可选的功能在 Trusted Extensions 系统上是建议使用的。例如，在 Trusted Extensions 中，`root` 用户必须转变为 `root` 角色。
- Trusted Extensions 可以更改 Oracle Solaris OS 的缺省行为。例如，在配置有 Trusted Extensions 的系统上，缺省情况下会启用审计。另外，设备分配是必需的。
- Trusted Extensions 可缩小 Oracle Solaris OS 中可用选项的范围。例如，在配置有 Trusted Extensions 的系统上，不支持 NIS+ 命名服务。此外，在 Trusted Extensions 中，所有区域都是有标签区域。与 Oracle Solaris OS 不同，有标签区域必须使用相同的用户 ID 池和组 ID 池。此外，Trusted Extensions 中的有标签区域可以共享一个 IP 地址。
- Trusted Extensions 提供两个桌面的可信版本。要在有标签环境中工作，Trusted Extensions 的桌面用户必须使用以下桌面之一：
  - **Solaris Trusted Extensions (CDE)** – 是公用桌面环境 (Common Desktop Environment, CDE) 的可信版本。可简称为 Trusted CDE。
  - **Solaris Trusted Extensions (JDS)** – 是 Java Desktop System，发行版 *number* 的可信版本。可简称为 Trusted JDS。
- Trusted Extensions 提供其他图形用户界面 (Graphical User Interface, GUI) 和命令行界面 (Command Line Interface, CLI)。例如，Trusted Extensions 提供设备分配管理器以管理设备。另外，`updatehome` 命令可用于将启动文件放置到每个标签的一般用户起始目录中。

- Trusted Extensions 要求使用特定的 GUI 进行管理。例如，在配置有 Trusted Extensions 的系统上，Solaris Management Console 可用于管理用户、角色和网络。同样，在 Trusted CDE 中，管理编辑器用于编辑系统文件。
- Trusted Extensions 限制用户可以看到的内容。例如，用户无法看到自己不能分配的设备。
- Trusted Extensions 限制用户的桌面选项。例如，会允许用户的工作站停止活动一段有限的时间，屏幕才会锁定。

多显示端系统和 Trusted Extensions 桌面

如果多显示端 Trusted Extensions 系统的显示器是以水平方向配置的，则可信窗口条会伸展横跨显示器。如果这些显示器是以垂直方向配置的，则可信窗口条会显示在最下方的显示器中。

不同的工作区显示在多显示端系统的显示器上时，Trusted CDE 和 Trusted JDS 会以不同方式呈现可信窗口条。

- 在 Trusted JDS 桌面上，每个显示器显示一个可信窗口条。
- 在 Trusted CDE 桌面上，会有一个可信窗口条显示在主显示器上。

注意 – 如果另一个可信窗口条显示在 Trusted CDE 多显示端系统上，该窗口条不是由操作系统生成的。您的系统上可能有未经授权的程序。

请立即与安全管理员联系。要确定正确的可信窗口条，请参见第 66 页中的 “如何重新获得对桌面当前焦点的控制权”。

Trusted Extensions 的基本概念

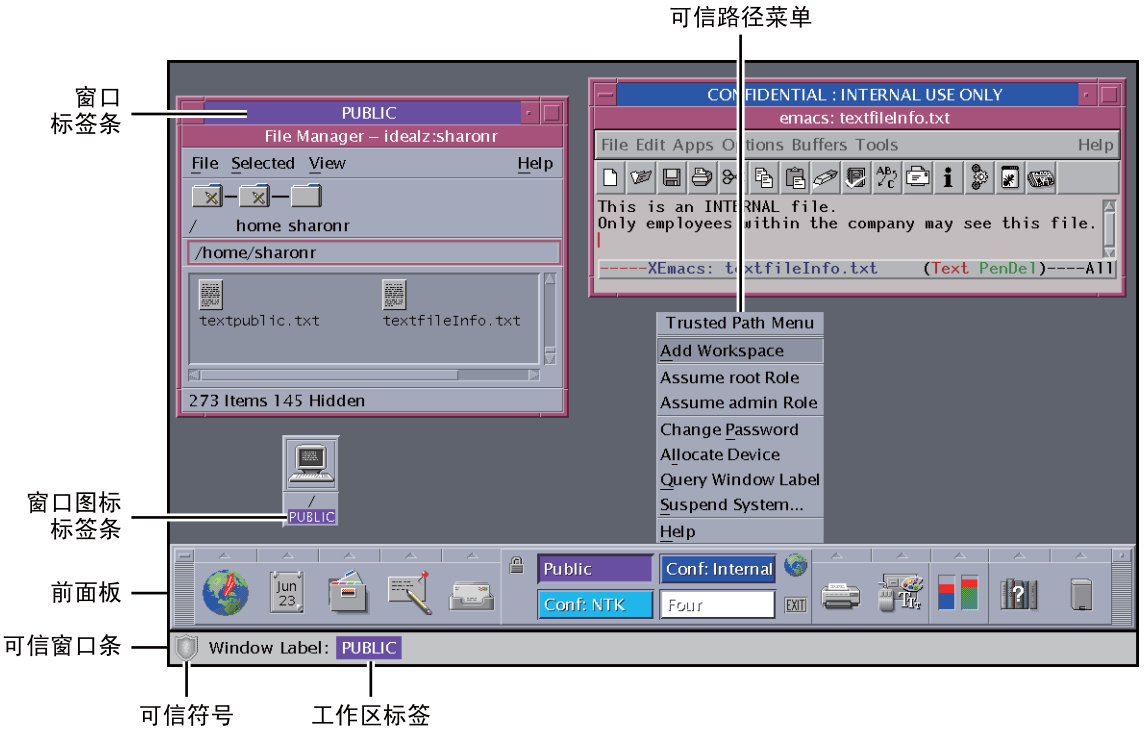
Trusted Extensions 软件会向 Oracle Solaris 系统添加标签。还会添加有标签桌面和可信应用程序，例如标签生成器和设备分配管理器。对于用户和管理员而言，本节中的概念都是了解 Trusted Extensions 所必需的。《Trusted Extensions User's Guide》中会为用户介绍这些概念。

Trusted Extensions 保护

Trusted Extensions 软件增强了 Oracle Solaris OS 的保护功能。Oracle Solaris OS 使用需要口令的用户帐户保护对系统的访问。您可以要求这些口令定期更改或具有一定长度等。角色需要附加口令才能执行管理任务。附加验证可限制由于侵入者猜到 root 用户口令所造成的破坏，因为角色不能作为登录帐户使用。Trusted Extensions 通过将用户和角色限制在批准的标签范围内而提供更进一步的保护。该标签范围限制用户和角色可以访问的信息。

Trusted Extensions 软件会显示 "Trusted Path"（可信路径）符号，是显示在可信窗口条左侧的明显、防篡改的标志。在 Trusted CDE 中，可信窗口条位于屏幕底部。在 Trusted JDS 中，可信窗口条位于屏幕顶部。"Trusted Path"（可信路径）符号符号会在用户使用与安全相关的系统部分时给予指示。如果用户正运行可信应用程序时，没有显示此符号，应立即检查该应用程序版本的真实性。如果未显示可信窗口条，则此桌面不可信。有关桌面显示样例，请参见图 1–1。

图 1–1 Trusted Extensions 多级别 CDE 桌面



与安全最为相关的软件，即可信计算基 (Trusted Computing Base, TCB)，在全局区域中运行。一般用户不能进入全局区域或查看其资源。用户能够与 TCB 软件进行交互，与他们更改口令时一样。只要用户与 TCB 进行交互，"Trusted Path"（可信路径）符号就会出现。

Trusted Extensions 与访问控制

Trusted Extensions 软件通过自主访问控制 (Discretionary Access Control, DAC) 和强制访问控制 (Mandatory Access Control, MAC) 保护信息和其他资源。DAC 是由所有者根据自

己的判断设置的传统 UNIX 权限位和访问控制列表。MAC 是系统自动强制执行的一种机制。MAC 通过检查事务中进程和数据的标签来控制所有事务。

用户的**标签**表示允许该用户运行以及该用户选择操作的敏感度级别。典型的标签有 `Secret`（秘密）或 `Pubic`（公共）。标签确定允许用户访问的信息。MAC 和 DAC 都可被 Oracle Solaris OS 中的特殊权限覆盖。**特权**是指可授予进程的特殊特权。**授权**是指可由管理员授予用户和角色的特殊权限。

作为管理员，您需要根据您站点的安全策略，向用户提供有关适当过程的培训以保护他们的文件和目录。此外，对于允许升级或降级标签的任何用户，您需要指导他们何时适合进行升级或降级。

角色和 Trusted Extensions

在运行 Oracle Solaris 软件但没有 Trusted Extensions 的系统上，角色是可选的。在配置有 Trusted Extensions 的系统上，角色是必需的。该系统由 "System Administrator"（系统管理员）角色和 "Security Administrator"（安全管理员）角色管理。在某些情况下，会使用 `root` 角色。

如同在 Oracle Solaris OS 中一样，权限配置文件是角色功能的基础。Trusted Extensions 提供两个权限配置文件，信息安全和用户安全。这两个配置文件定义安全管理员角色。

Trusted Extensions 中角色可用的程序具有特殊属性，即**可信路径属性**。该属性指示此程序是 TCB 的一部分。从全局区域中启动程序时，可以使用可信路径属性。

有关角色的信息，请参见《System Administration Guide: Security Services》中的第 III 部分, “Roles, Rights Profiles, and Privileges”。

Trusted Extensions 软件中的标签

标签和安全许可位于 Trusted Extensions 中强制访问控制 (Mandatory Access Control, MAC) 的中心。它们定义哪些用户可以访问哪些程序、文件和目录。标签和安全许可包括一个**等级**组件以及零个或多个**区间**组件。等级组件表示有层次的安全性级别，例如 `TOP SECRET` 或 `CONFIDENTIAL`。区间组件表示可能需要访问通用信息主体的一组用户。一些典型的区间类型包括项目、部门或物理位置。标签可由授权用户读取，但在内部，标签会像数字一样进行处理。数字及其可读版本在 `label_encodings` 文件中进行定义。

Trusted Extensions 在所有尝试的安全相关事务中起中介所用。该软件会将访问实体（通常是进程）的标签与被访问的实体（通常是文件系统对象）的标签进行比较。然后，软件会根据哪个标签处于**支配地位** *(dominant)* 来允许或禁止事务。标签还可用于确定对其他系统资源的访问，例如可分配的设备、网络、帧缓存器和其他主机。

标签之间的支配关系

如果满足下面两个条件，表示一个实体的标签**支配**另一个标签：

- 第一个实体的标签的等级组件等于或高于第二个实体的等级。安全管理员将数字指定给 label_encodings 文件中的等级。软件比较这些数字以确定支配关系。
- 第一个实体中的区间集包括第二个实体的所有区间。

如果两个标签具有相同的等级和相同的区间集合，则表明这两个标签**相等**。如果两个标签相等，它们互相支配，而且允许访问。

如果一个标签具有较高等级，或者如果它具有相同等级并且其区间是第二个标签的区间的超集，或者两种情况兼具，表示第一个标签**严格支配**第二个标签。

如果没有一个标签支配另一个标签，表示这两个标签**不相交**或**不可比**。

下表提供了有关支配关系的标签比较示例。在此示例中，NEED_TO_KNOW 是高于 INTERNAL 的等级。存在三个区间：Eng、Mkt 和 Fin。

表 1–1 标签关系的示例

标签 1	关系	标签 2
NEED_TO_KNOW Eng Mkt	（严格）支配	INTERNAL Eng Mkt
NEED_TO_KNOW Eng Mkt	（严格）支配	NEED_TO_KNOW Eng
NEED_TO_KNOW Eng Mkt	（严格）支配	INTERNAL Eng
NEED_TO_KNOW Eng Mkt	支配（等同于）	NEED_TO_KNOW Eng Mkt
NEED_TO_KNOW Eng Mkt	不相交	NEED_TO_KNOW Eng Fin
NEED_TO_KNOW Eng Mkt	不相交	NEED_TO_KNOW Fin
NEED_TO_KNOW Eng Mkt	不相交	INTERNAL Eng Mkt Fin

管理标签

Trusted Extensions 提供两个用作标签或安全许可的特殊管理标签：ADMIN_HIGH 和 ADMIN_LOW。这些标签用于保护系统资源，而且是供管理员而非一般用户使用。

ADMIN_HIGH 是最高级别标签。ADMIN_HIGH 支配系统中所有其他标签，并且可用于保护系统数据（例如管理数据库或审计迹）以免被读取。您必须位于全局区域中才能读取标签为 ADMIN_HIGH 的数据。

ADMIN_LOW 是最低级别标签。ADMIN_LOW 受系统中所有其他标签的支配，包括一般用户的标签。强制访问控制不允许用户将数据写入标签低于用户标签的文件。因此，一般用户可以读取但不可修改标签 ADMIN_LOW 级别的文件。ADMIN_LOW 通常用于保护共享的公共可执行文件，例如 /usr/bin 中的文件。

标签编码文件

系统的所有标签组件（即等级、区间和关联的规则）都存储在 ADMIN_HIGH 文件中，即 label_encodings 文件。该文件位于 /etc/security/tsol 目录中。安全管理员为站点设置 label_encodings 文件。标签编码文件包含：

- **组件定义**—等级、区间、标签和安全许可的定义，包括所需组合和约束条件的各项规则
- **认可范围定义**—为整个系统和一般用户定义可用标签集合的安全许可和最小标签的规格
- **打印规范**—有关打印标题、尾页、页眉、页脚和有关打印机输出的其他安全功能的标识和处理信息
- **定制**—包括标签颜色代码和其他 省值在内的本 定义

有关更多信息，请参见 label_encodings(4) 手册页。还可以参阅《Trusted Extensions Label Administration》和《Compartmented Mode Workstation Labeling: Encodings Format》了解详细信息。

标签范围

标签范围是指用户可在该处运行的潜在可用标签集合。用户和资源都有标签范围。可由标签范围保护的资源包括可分配的设备、网络、接口、帧缓存器和命令或操作等。标签范围由范围顶部的安全许可以及底部的最小标签定义。

范围并不一定包括位于最大和最小标签之间的所有标签组合。label_encodings 文件中的规则可取消某些组合的资格。标签必须**格式正确**（即被标签编码文件中的所有适用规则所允许），才能包含在范围之中。

但是，安全许可不一定要格式正确。例如，假定 label_encodings 文件在某个标签中禁止区间 Eng、Mkt 和 Fin 的任意组合。INTERNAL Eng Mkt Fin 将是有效的安全许可，但不是有效的标签。作为安全许可，此组合将允许用户访问标签为 INTERNAL Eng、INTERNAL Mkt 和 INTERNAL Fin 的文件。

帐户标签范围

将安全许可和最小标签指定给用户时，您也就定义了允许用户在其中进行操作的**帐户标签范围**的上界和下界。以下等式描述了帐户标签范围，使用 ≤ 指示“受支配于或相同于”：

最小标签 ≤ 允许标签 ≤ 安全许可

因此，只要该标签可以支配最小标签，则将允许用户在由安全许可支配的任意标签下进行操作。如果没有明确设置用户的安全许可或最小标签，则 label_encodings 文件中定义的缺省值将生效。

可为用户指定安全许可和最小标签，从而允许他们在多个标签或单个标签下执行操作。用户的安全许可和最小标签相等时，用户只能在一个标签下执行操作。

会话范围

会话范围是指 Trusted Extensions 会话过程中用户可用的标签集合。会话范围必须位于用户的帐户标签范围内以及为系统设置的标签范围内。登录时，如果用户选择单标签会话模式，会话范围限制为该标签。如果用户选择多标签会话模式，用户所选择的标签会成为会话安全许可。会话安全许可定义会话范围的上界。用户的最小标签定义下界。用户在最小标签的工作区中开始会话。会话过程中，用户可切换到会话范围内任何标签的工作区。

标签保护什么以及标签显示在何处

标签显示在桌面上以及在桌面上执行的输出（例如打印机输出）上。

- **应用程序**—应用程序启动进程。这些进程以启动应用程序的工作区的标签运行。有标签区域中的应用程序，将在区域的标签下将其作为一个文件为其设置标签。
- **设备**—流过设备的数据通过设备分配和设备标签范围进行控制。要使用设备，用户必须位于设备的标签范围内，而且被授权分配设备。
- **文件系统挂载点**—每个挂载点都有一个标签。可使用 `getlabel` 命令查看标签。
- **网络接口**—IP 地址（主机）具有描述其标签范围的模板。无标签主机也具有缺省标签。
- **打印机与打印**—打印机具有标签范围。标签打印在正文页上。标签、处理信息和其他安全信息打印在标题页和篇尾页上。要在 Trusted Extensions 中配置打印，请参见第 15 章，管理有标签打印（任务）和《Trusted Extensions Label Administration》中的“Labels on Printed Output”。
- **进程**－将为进程设置标签。进程以进程源自的工作区的标签运行。可通过使用 `plabel` 命令查看进程的标签。
- **用户**—将为用户指定缺省标签和标签范围。用户工作区的标签指示用户进程的标签。
- **窗口**—可在桌面窗口的顶部看到标签。桌面的标签也由颜色指示。颜色显示在桌面切换上以及窗口标题栏的上方。

  窗口移动到带不同标签的工作区时，窗口会保持其原始的标签。
- **区域**—每个区域都有唯一的标签。区域拥有的文件和目录处于该区域的标签级别。有关更多信息，请参见 `getzonepath(1)` 手册页。

◆ ◆ ◆ 第 2 章

Trusted Extensions 管理工具

本章介绍了 Trusted Extensions 中可用的工具、工具位置以及工具所针对的数据库。

Trusted Extensions 的管理工具

配置有 Trusted Extensions 的系统上的管理功能使用的许多工具与 Oracle Solaris OS 中可用的工具相同。Trusted Extensions 还提供了安全性增强的工具。管理工具仅可供角色工作区中的角色使用。

在角色工作区内，您可以访问受信任的命令、操作、应用程序和脚本。下表概述了这些管理工具。

表 2–1 Trusted Extensions 管理工具

工具	说明	更多信息
`/usr/sbin/txzonemgr`	提供了一个用于创建、安装、初始化和引导区域的基于菜单的向导。该脚本替代了用来管理区域的 Trusted CDE 操作。 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` 使用 `zenity` 命令。	请参见《Trusted Extensions Configuration Guide》中的“Creating Labeled Zones”。 另请参见 `zenity`(1) 手册页。

表 2–1 Trusted Extensions 管理工具 （续）

工具	说明	更多信息
在 Trusted CDE 中，"Application Manager" 文件夹中的 "Trusted_Extensions" 文件夹中的操作	用于编辑 Solaris Management Console 不管理的本地文件，如 /etc/system。某些操作运行脚本，如 "Install Zone"（安装区域）操作。	请参见第 32 页中的 “Trusted CDE 操作”和第 51 页中的 “如何在 Trusted Extensions 中启动 CDE 管理操作”。
在 Trusted CDE 中，"Device Allocation Manager"（设备分配管理器） 在 Solaris Trusted Extensions (JDS) 中，"Device Manager"（设备管理器）	用于管理设备的标签范围以及分配设备或取消分配设备。	请参见第 35 页中的 “设备分配管理器”和第 213 页中的 “在 Trusted Extensions 中操作设备（任务列表）”。
Solaris Management Console	用于配置用户、角色、权限、主机、区域和网络。该工具可以更新本地文件或 LDAP 数据库。 该工具还可以启动 dtappsession 传统应用程序。	有关基本功能，请参见《Oracle Solaris 管理：基本管理》中的第 2 章 “使用 Solaris Management Console（任务）”。有关特定于 Trusted Extensions 的信息，请参见第 36 页中的 “Solaris Management Console 工具”。
Solaris Management Console 命令，如 smuser 和 smtnzonecfg	是 Solaris Management Console 的命令行接口。	有关列表，请参见表 2–4。
"Label Builder"（标签生成器）	也是一个用户工具。在程序要求您选择标签时出现。	有关示例，请参见第 85 页中的 “如何在 Solaris Management Console 中修改用户的标签范围”。
Trusted Extensions 命令	用于执行 Solaris Management Console 工具或 CDE 操作未涵盖的任务。	有关管理命令的列表，请参见表 2–5。

txzonemgr 脚本

从 Solaris 10 5/08 发行版开始，使用 txzonemgr 脚本来配置有标签区域。该 zenity(1) 脚本显示一个标题为 "Labeled Zone Manager"（有标签区域管理器）对话框。该 GUI 显示动态确定的菜单，该菜单仅针对有标签区域的当前配置状态显示有效选项。例如，如果区域已有标签，则不显示 "Label"（标签）菜单项。

Trusted CDE 操作

下表列出了 Trusted Extensions 中的角色可以运行的 CDE 操作。可从 "Trusted_Extensions" 文件夹访问这些 Trusted CDE 操作。可从 CDE 桌面上的 "Application Manager" 文件夹访问 "Trusted_Extensions" 文件夹。

表 2–2 Trusted CDE 中的管理操作及其用途，以及关联的权限配置文件

操作名称	操作的用途	缺省的权限配置文件
"Add Allocatable Device"（添加可分配设备）	通过向设备数据库添加条目来创建设备。请参见 add_allocatable(1M)。	"Device Security"（设备安全）
"Admin Editor"（管理编辑器）	编辑指定的文件。请参见第 52 页中的 “如何在 Trusted Extensions 中编辑管理文件”。	"Object Access Management"（对象访问管理）
"Audit Classes"（审计类）	编辑 audit_class 文件。请参见 audit_class(4)。	"Audit Control"（审计控制）
"Audit Control"（审计控制）	编辑 audit_control 文件。请参见 audit_control(4)。	"Audit Control"（审计控制）
"Audit Events"（审计事件）	编辑 audit_event 文件。请参见 audit_event(4)。	"Audit Control"（审计控制）
"Audit Startup"（审计启动）	编辑 audit_startup.sh 脚本。请参见 audit_startup(1M)。	"Audit Control"（审计控制）
"Check Encodings"（检查编码）	对指定的编码文件运行 chk_encodings 命令。请参见 chk_encodings(1M)。	"Object Label Management"（对象标签管理）
"Check TN Files"（检查 TN 文件）	对 tnrhdb、tnrhtp 和 tnzonecfg 数据库运行 tnchkdb 命令。请参见 tnchkdb(1M)。	"Network Management"（网络管理）
"Configure Selection Confirmation"（配置选择确认）	编辑 /usr/dt/config/sel_config 文件。请参见 sel_config(4)。	"Object Label Management"（对象标签管理）
"Create LDAP Client"（创建 LDAP 客户机）	使全局区域成为某个现有 LDAP 目录服务的 LDAP 客户机。	"Information Security"（信息安全）
"Edit Encodings"（编辑编码）	编辑指定的 label_encodings 文件并运行 chk_encodings 命令。请参见 chk_encodings(1M)。	"Object Label Management"（对象标签管理）
"Name Service Switch"（名称服务转换）	编辑 nsswitch.conf 文件。请参见 nsswitch.conf(4)。	"Network Management"（网络管理）
"Set DNS Servers"（设置 DNS 服务器）	编辑 resolv.conf 文件。请参见 resolv.conf(4)。	"Network Management"（网络管理）
"Set Daily Message"（设置日常消息）	编辑 /etc/motd 文件。登录时，该文件的内容显示在 "Last Login"（上次登录）对话框中。	"Network Management"（网络管理）
"Set Default Routes"（设置缺省路由）	指定缺省静态路由。	"Network Management"（网络管理）
"Share Filesystems"（共享文件系统）	编辑 dfstab 文件。不运行 share 命令。请参见 dfstab(4)。	"File System Management"（文件系统管理）

以下操作是在区域创建过程中由初始设置团队使用的操作。可以使用其中的某些操作进行维护和故障排除。

表 2–3 Trusted CDE 中的安装操作及其用途，以及关联的权限配置文件

操作名称	操作的用途	缺省的权限配置文件
"Clone Zone"（克隆区域）	基于现有区域的 ZFS 快照创建有标签区域。	"Zone Management"（区域管理）
"Copy Zone"（复制区域）	基于现有区域创建有标签区域。	"Zone Management"（区域管理）
"Configure Zone"（配置区域）	将标签与区域名称相关联。	"Zone Management"（区域管理）
"Initialize Zone for LDAP"（为 LDAP 初始化区域）	为将区域作为 LDAP 客户机进行引导而初始化区域。	"Zone Management"（区域管理）
"Install Zone"（安装区域）	安装有标签区域所需的系统文件。	"Zone Management"（区域管理）
"Restart Zone"（重新启动区域）	重新启动已引导的区域。	"Zone Management"（区域管理）
"Share Logical Interface"（共享逻辑接口）	为全局区域设置一个接口，并为有标签区域另外设置一个共享的接口。	"Network Management"（网络管理）
"Share Physical Interface"（共享物理接口）	设置一个由全局区域和有标签区域共享的接口。	"Network Management"（网络管理）
"Shut Down Zone"（关闭区域）	关闭某个已安装的区域。	"Zone Management"（区域管理）
"Start Zone（"启动区域）	引导某个已安装的区域并为该区域启动服务。	"Zone Management"（区域管理）
"Zone Terminal Console"（区域终端控制台）	打开控制台以查看已安装区域中的进程。	"Zone Management"（区域管理）

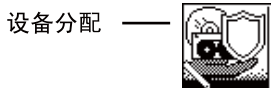
设备分配管理器

设备是一种连接到计算机的物理外设，或者是一种称为**伪设备**的软件模拟设备。因为设备提供了一种用于在系统中导入和导出数据的方法，因此必须对设备进行控制以便正确地保护数据。Trusted Extensions 使用设备分配和设备标签范围来控制流经设备的数据。

具有标签范围的设备示例如下：帧缓存器、磁带机、磁盘和 CD-ROM 驱动器、打印机和 USB 设备。

用户通过 "Device Allocation Manager"（设备分配管理器）分配设备。"Device Allocation Manager"（设备分配管理器）挂载设备，运行一个清除脚本来准备设备并执行分配。完成后，用户通过 "Device Allocation Manager"（设备分配管理器）执行以下操作来取消分配设备：运行另一个清除脚本，卸载并取消分配设备。

图 2–1 Trusted CDE 中的 "Device Allocation Manager"（设备分配管理器）图标



可以通过使用 "Device Allocation Manager"（设备分配管理器）中的 "Device Administration"（设备管理）工具来管理设备。一般用户无法访问 "Device Administration"（设备管理）工具。

注 – 在 Solaris Trusted Extensions (JDS) 中，该 GUI 被命名为 "Device Manager"（设备管理器），"Device Administration"（设备管理）按钮被命名为 "Administration"（管理）。

图 2–2 "Device Allocation Manager"（设备分配管理器）GUI

有关 Trusted Extensions 中的设备保护的更多信息，请参见第 17 章，管理 Trusted Extensions 的设备（任务）。

Solaris Management Console 工具

在 Solaris Management Console 中，可以访问基于 GUI 的管理工具的工具箱。通过这些工具，您可以编辑各种配置数据库中的项目。在 Trusted Extensions 中，Solaris Management Console 是用户、角色和可信网络数据库的管理接口。

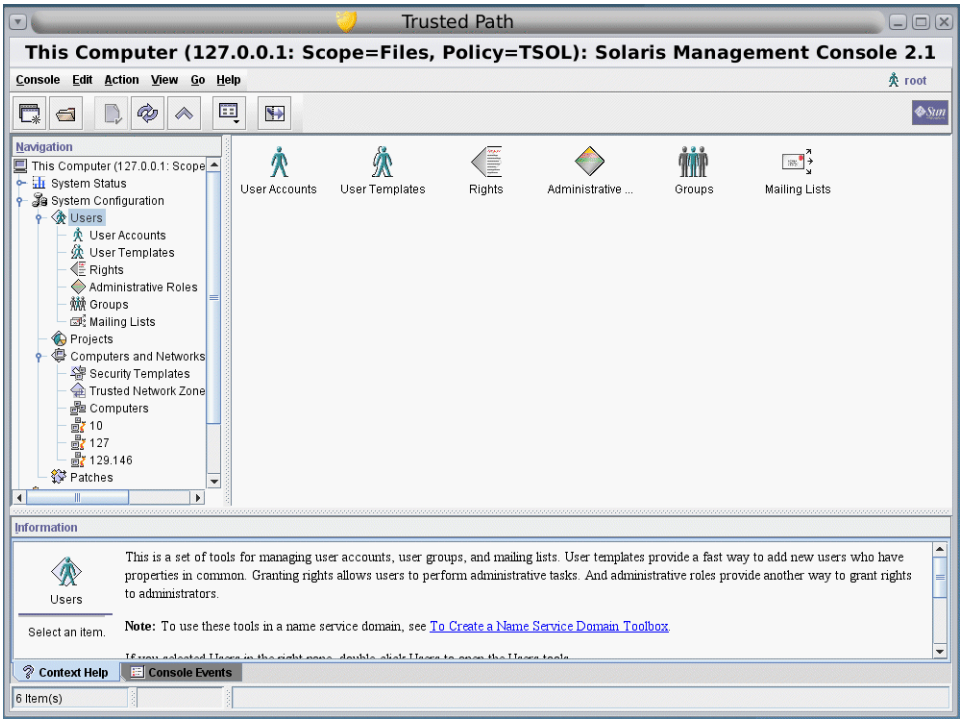
Trusted Extensions 扩展了 Solaris Management Console：

- Trusted Extensions 修改了 Solaris Management Console "Users"（用户）工具集合。有关工具集合的简介，请参见《Oracle Solaris 管理：基本管理》中的第 2 章 “使用 Solaris Management Console（任务）”。
- Trusted Extensions 向 "Computers and Networks"（计算机和网络）工具集合中添加了 "Security Templates"（安全模板）工具和 "Trusted Network Zones"（可信网络区域）工具。

Solaris Management Console 工具根据作用域和安全策略收集到了相应的**工具箱**中。为管理 Trusted Extensions，Trusted Extensions 提供了 `Policy=TSOL` 的工具箱。可以根据作用域（即根据命名服务）来访问工具。可用的作用域有本地主机和 LDAP。

下图显示了 Solaris Management Console。一个 `Scope=Files` 的 Trusted Extensions 工具箱已装入，且 "Users"（用户）工具集合已打开。

图 2–3 Solaris Management Console 中的典型 Trusted Extensions 工具箱



Solaris Management Console 中的 Trusted Extensions 工具

Trusted Extensions 向以下三个工具中添加了可配置的安全属性：

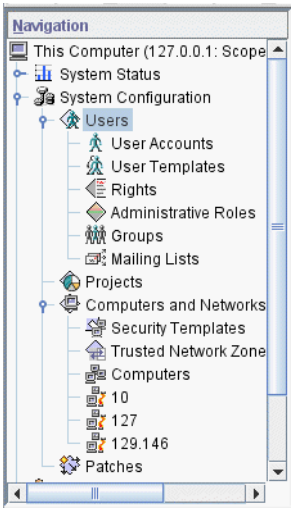
- **"User Accounts"（用户帐户）工具**－是用于更改用户标签、更改用户的标签视图和控制帐户使用的管理接口。
- **"Administrative Roles"（管理角色）工具**－是用于更改角色的标签范围和空闲时的屏幕锁定行为的管理接口。
- **"Rights"（权限）工具**－包含了可以指定给权限配置文件的 CDE 操作。可以为这些操作指定安全属性。

Trusted Extensions 向 "Computers and Networks"（计算机和网络）工具集合中添加了以下两种工具：

- **"Security Templates"（安全模板）工具** – 是用于管理主机和网络的各个标签方面的管理接口。此工具修改 `tnrhtp` 和 `tnrhdb` 数据库、强制实现语法正确性并使用更改更新内核。
- **"Trusted Network Zones"（可信网络区域）工具** – 是用于管理区域的各个标签方面的管理接口。此工具修改 `tnzonecfg` 数据库、强制实现语法正确性并使用更改更新内核。

图 2–4 显示了 "Users"（用户）工具集合处于突出显示状态的 "Files"（文件）工具箱。Trusted Extensions 工具显示在 "Computers and Networks"（计算机和网络）工具集合下。

图 2–4 Solaris Management Console 中的 "Computers and Networks"（计算机和网络）工具集合



"Security Templates"（安全模板）工具

安全模板描述了可以指定给一组主机的安全属性集合。使用 "Security Templates"（安全模板）工具，您可以方便地将安全属性的特定组合指定给一组主机。这些属性控制着数据的打包、传输和解释方式。指定给同一模板的主机具有相同的安全设置。

主机是在 "Computers"（计算机）工具中定义的。主机的安全属性是在 "Security Templates"（安全模板）工具中指定的。"Modify Template"（修改模板）对话框包含两个选项卡：

- **"General"（常规）选项卡** – 描述了模板。包括模板名称、主机类型、缺省标签、系统解释域 (Domain of Interpretation, DOI)、认可范围和离散的敏感标签集合。
- **"Hosts Assigned to Template"（指定给模板的主机）选项卡** – 列出了网络上您已经指定给该模板的所有主机。

第 12 章，可信网络（概述）中更详细地说明了可信的联网和安全模板。

"Trusted Network Zones"（可信网络区域）工具

"Trusted Network Zones"（可信网络区域）工具标识您的系统上的区域。初始状态下，会列出全局区域。在添加区域及其标签时，区域名称将显示在窗格中。区域创建通常发生在系统配置期间。标签指定、多级别端口配置和标签策略是在该工具中配置的。有关详细信息，请参见第 10 章，在 Trusted Extensions 中管理区域（任务）。

与 Solaris Management Console 的客户机-服务器通信

通常，Solaris Management Console 客户机**远程地**管理系统。在使用 LDAP 作为命名服务的网络上，Solaris Management Console 客户机连接到运行 LDAP 服务器的 Solaris Management Console 服务器。下图显示了该配置。

图 2–5 使用 LDAP 服务器管理网络的 Solaris Management Console 客户机

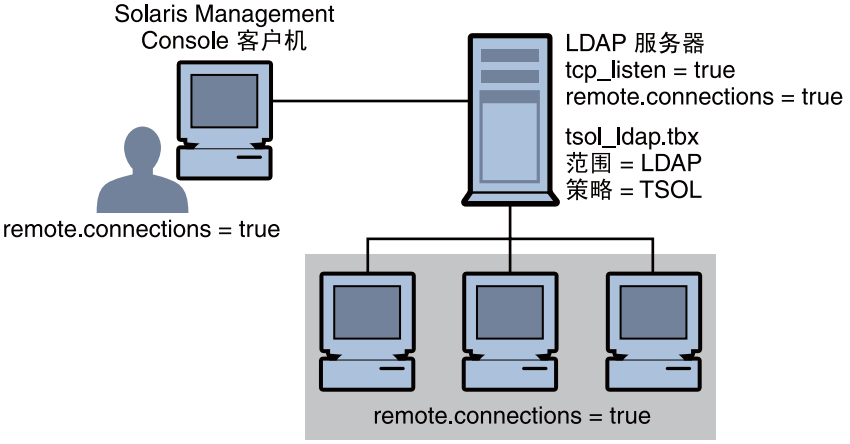
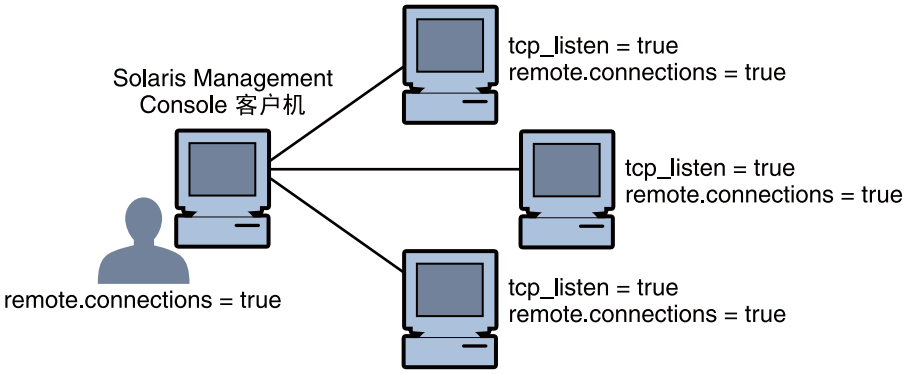


图 2–6 显示了未配置有 LDAP 服务器的网络。管理员为每个远程系统配置了一个 Solaris Management Console 服务器。

图 2–6 管理网络上的各个远程系统的 Solaris Management Console 客户机

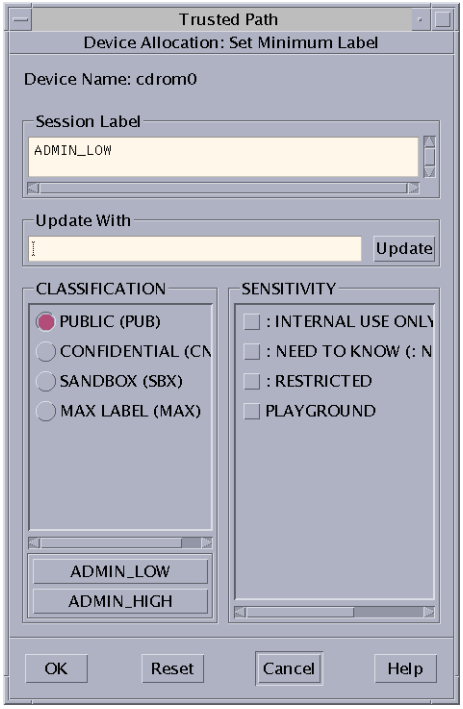


Solaris Management Console 文档

Solaris Management Console 文档的主要来源是其联机帮助。上下文有关帮助绑定到当前选定的功能，且显示在信息窗格中。展开的帮助主题可通过 "Help"（帮助）菜单或单击上下文有关帮助中的链接来访问。有关详细信息，请参见《Oracle Solaris 管理：基本管理》中的第 2 章 “使用 Solaris Management Console（任务）”。另请参见《Oracle Solaris 管理：基本管理》中的“使用 RBAC 和 Solaris 管理工具（任务列表）”。

Trusted Extensions 中的标签生成器

程序要求您指定标签时，标签生成器 GUI 将执行您选择的有效标签或安全许可。例如，登录期间会显示标签生成器（请参见《Trusted Extensions User's Guide》中的第 2 章 “Logging In to Trusted Extensions (Tasks)”）。更改工作区标签时，或者在 Solaris Management Console 中将标签指定给用户、区域或网络接口时，也会显示标签生成器。为新设备指定标签范围时会显示以下标签生成器。



在标签生成器中，"Classification"（等级）列中的组件名称对应于 `label_encodings` 文件中的 `CLASSIFICATIONS` 部分。"Sensitivity"（敏感度）列中的组件名称对应于 `label_encodings` 文件中的 `WORDS` 部分。

Trusted Extensions 中的命令行工具

《Trusted Extensions Reference Manual》中包含了 Trusted Extensions 特有的命令。《Oracle Solaris Reference Manual》中包含了 Trusted Extensions 修改的 Oracle Solaris 命令。`man` 命令可找到所有命令。

下表列出了 Trusted Extensions 特有的命令。命令是以手册页格式列出的。

表 2–4 Trusted Extensions 的用户命令和管理命令

手册页	Trusted Extensions 修改	更多信息
`add_allocatable(1M)`	通过将设备添加到设备分配数据库使得设备可供分配。缺省情况下，可移除设备都是可分配的。	第 215 页中的 “如何在 Trusted Extensions 中配置设备”
`atohexlabel(1M)`	将标签转换为十六进制格式。	第 66 页中的 “如何获取标签的十六进制等效值”

表 2–4 Trusted Extensions 的用户命令和管理命令 （续）

手册页	Trusted Extensions 修改	更多信息
chk_encodings(1M)	检查 label_encodings 文件的完整性。	《Trusted Extensions Label Administration》中的“How to Debug a label_encodings File”
dtappsession(1)	通过使用 "Application Manager"（应用程序管理器）打开一个远程 Trusted CDE 会话。	第 8 章，Trusted Extensions 中的远程管理（任务）
getlabel(1)	显示所选文件或目录的标签。	第 115 页中的 “如何显示挂载的文件的标签”
getzonepath(1)	显示特定区域的完整路径名。	《Trusted Extensions Developer’s Guide》中的“Acquiring a Sensitivity Label”
hextoalabel(1M)	将十六进制的标签转换为其可阅读的等效体。	第 67 页中的 “如何通过标签的十六进制形式获取可读标签”
plabel(1)	显示当前进程的标签。	请参见手册页。
remove_allocatable(1M)	通过从设备分配数据库中删除设备的条目来阻止设备分配。	第 215 页中的 “如何在 Trusted Extensions 中配置设备”
setlabel(1)	重新为所选项设置标签。需要 solaris.label.file.downgrade 或 solaris.label.file.upgrade 授权。这些授权位于 "Object Label Management"（对象标签管理）权限配置文件中。	有关等效的 GUI 过程，请参见《Trusted Extensions User’s Guide》中的“How to Move Files Between Labels in Trusted CDE”。
smtnrhdb(1M)	管理本地 tnrhdb 数据库或命名服务数据库中的条目。	有关使用 Solaris Management Console 的等效过程，请参见第 155 页中的 “配置可信网络数据库（任务列表）”。
smtnrhtp(1M)	管理本地 tnrhtp 数据库或命名服务数据库中的条目。	请参见手册页。
smtnzonecfg(1M)	管理本地 tnzonecfg 数据库中的条目。	有关使用 Solaris Management Console 的等效过程，请参见第 123 页中的 “如何为区域创建多级别端口”。
tnchkdb(1M)	检查 tnrhdb 和 tnrhtp 数据库的完整性。	第 170 页中的 “如何检查可信网络数据库的语法”
tnctl(1M)	在内核中缓存网络信息。	第 171 页中的 “如何将内核高速缓存与可信网络数据库同步”
tnd(1M)	执行可信的网络守护进程。	第 171 页中的 “如何将内核高速缓存与可信网络数据库同步”
tninfo(1M)	显示内核级的网络信息和统计信息。	第 170 页中的 “如何将可信网络数据库信息与内核高速缓存进行比较”。

表 2–4 Trusted Extensions 的用户命令和管理命令 （续）

手册页	Trusted Extensions 修改	更多信息
updatehome(1M)	为当前标签更新 .copy_files 和 .link_files。	第 81 页中的 “如何在 Trusted Extensions 中为用户配置启动文件”

下表列出了 Trusted Extensions 修改或扩展的 Oracle Solaris 命令。命令是以手册页格式列出的。

表 2–5 Trusted Extensions 修改的用户命令和管理命令

手册页	Trusted Extensions 修改	更多信息
allocate(1)	添加相应选项以清除已分配的设备，以及将设备分配给特定区域。在 Trusted Extensions 中，一般用户不能使用此命令。	《Trusted Extensions User’s Guide》中的“How to Allocate a Device in Trusted Extensions”
deallocate(1)	添加相应选项以清除设备，以及从特定区域中取消分配设备。在 Trusted Extensions 中，一般用户不能使用此命令。	《Trusted Extensions User’s Guide》中的“How to Allocate a Device in Trusted Extensions”
list_devices(1)	添加 -a 选项以显示设备属性，如授权和标签。添加 -d 选项以显示已分配的设备类型的缺省属性。添加 -z 选项以显示可以分配给有标签区域的可用设备。	请参见手册页。
tar(1)	添加 -T 选项以归档和提取有标签的文件和目录。	第 133 页中的 “如何在 Trusted Extensions 中备份文件”和第 133 页中的 “如何在 Trusted Extensions 中恢复文件”
auditconfig(1M)	添加 windata_down 和 windata_up 审计策略选项。	《System Administration Guide: Security Services》中的“How to Configure Audit Policy”
auditreduce(1M)	添加 -l 选项以按标签选择审计记录。	《System Administration Guide: Security Services》中的“How to Select Audit Events From the Audit Trail”
automount(1M)	修改 auto_home 映射的名称和内容以涵盖较高级别标签中的区域名称和区域可见性。	第 130 页中的 “在 Trusted Extensions 中更改自动挂载程序”
ifconfig(1M)	添加 all-zones 选项使接口可供系统上的每个区域使用。	第 174 页中的 “如何检验主机的接口是否已启动”
netstat(1M)	添加 -R 选项来为套接字和路由表条目显示扩展的安全属性。	第 174 页中的 “如何调试 Trusted Extensions 网络”
route(1M)	添加 -secattr 选项以显示路由的安全属性：cipso、doi、max_sl 和 min_sl。	第 168 页中的 “如何配置具有安全属性的路由”

Trusted Extensions 中的远程管理

可以通过使用 ssh 命令、dtappsession 程序或 Solaris Management Console 来远程管理配置有 Trusted Extensions 的系统。如果站点安全策略允许，您可以对 Trusted Extensions 主机进行配置以允许从非 Trusted Extensions 主机登录，但是该配置安全性较低。有关更多信息，请参见第 8 章，Trusted Extensions 中的远程管理（任务）。

◆ ◆ ◆ 第 3 章

Trusted Extensions 管理员入门（任务）

本章介绍了如何管理配置有 Trusted Extensions 的系统。

Trusted Extensions 的新增功能

Solaris 10 1/13 – 在此发行版中，Trusted Extensions 向打印子系统添加审计事件。请阅读 `/etc/security/audit_event` 文件了解可信打印事件、`AUE_print_request`、`AUE_print_request_ps`、`AUE_print_request_unlabeled` 和 `AUE_print_request_nobanner` 的定义。

Solaris 10 10/08 – 在此发行版中，Trusted Extensions 提供了以下功能：

- Trusted Extensions 共享的 IP 栈允许缺省路由将各个有标签区域相互隔离，并与全局区域隔离。
- 回送接口 `lo0` 是一个 `all-zones` 接口。
- 可通过角色来实施职责分离。"System Administrator"（系统管理员）角色负责创建用户，但不能指定口令。"Security Administrator"（安全管理员）角色负责指定口令，但不能创建用户。有关详细信息，请参见《Trusted Extensions Configuration Guide》中的“Create Rights Profiles That Enforce Separation of Duty”。
- 本指南在附录 B，Trusted Extensions 手册页列表中提供了 Trusted Extensions 手册页的列表。

Solaris 10 5/08 – 在此发行版中，Trusted Extensions 提供了以下功能：

- 服务管理工具 (Service Management Facility, SMF) 将 Trusted Extensions 作为 `svc:/system/labeld` 服务进行管理。缺省情况下，`labeld` 服务被禁用。启用此服务时，仍须配置和重新引导系统，以实施 Trusted Extensions 安全策略。

- 您的系统使用的 CIPSO 系统解释域 (Domain of Interpretation, DOI) 编号是可配置的。
  - 有关 DOI 的信息，请参见第 145 页中的 “Trusted Extensions 中的网络安全属性”。
  - 要指定不同于缺省值的 DOI，请参见《Trusted Extensions Configuration Guide》中的“Configure the Domain of Interpretation”。
- Trusted Extensions 可以识别 NFS 版本 3 (NFSv3) 以及 NFS 版本 4 (NFSv4) 已挂载文件系统中的 CIPSO 标签。因此，您可以在 Trusted Extensions 系统上将 NFSv3 文件系统挂载为有标签文件系统。要将 udp 用作 NFSv3 中的多级别挂载的基础协议，请参见第 122 页中的 “如何为 NFSv3 Over udp 配置多级别端口”。
- 可以将名称服务高速缓存守护进程 (name service cache daemon, `nscd`) 配置为在每个有标签区域中在区域的标签运行。

管理 Trusted Extensions 时的安全要求

在 Trusted Extensions 中，角色是用来管理系统的惯用方法。通常，不使用超级用户。角色的创建方式与在 Oracle Solaris OS 中一样，且大多数任务都是通过角色执行的。在 Trusted Extensions 中，不使用 `root` 用户来执行管理任务。

下面的角色是 Trusted Extensions 站点中的典型角色：

- `root` **角色**—由初始设置团队创建
- **"Security Administrator"（安全管理员）角色**—由初始设置团队在初始配置期间或之后创建
- **"System Administrator"（系统管理员）角色**—由"Security Administrator"（安全管理员）角色创建

与在 Oracle Solaris OS 中一样，您还可以创建"Primary Administrator"（主管理员）角色、"Operator"（操作员）角色，等等。除 `root` 角色之外，可以在命名服务中管理您创建的任何角色。

与在 Oracle Solaris OS 中一样，只有已指定某个角色的用户可以承担该角色。在 Solaris Trusted Extensions (CDE) 中，您可以从名为 "Trusted Path"（可信路径）的桌面菜单承担某个角色。在 Solaris Trusted Extensions (JDS) 中，如果您的用户名显示在可信窗口条中，您就可以承担角色。单击您的用户名时，将显示角色选项。

在 Trusted Extensions 中创建角色

要管理 Trusted Extensions，您需要创建用于划分系统和安全功能的角色。初始设置团队已在配置过程中创建了"Security Administrator"（安全管理员）角色。有关详细信息，请参见《Trusted Extensions Configuration Guide》中的“Create the Security Administrator Role in Trusted Extensions”。

在 Trusted Extensions 中创建角色的过程与 Oracle Solaris OS 过程相同。如第 2 章，Trusted Extensions 管理工具中所述，Solaris Management Console 是 Trusted Extensions 中用来管理角色的 GUI。

- 有关角色创建的概述，请参见《System Administration Guide: Security Services》中的第 10 章 “Role-Based Access Control (Reference)”和《System Administration Guide: Security Services》中的“Using RBAC (Task Map)”。
- 要创建与超级用户等效的强大角色，请参见《Oracle Solaris 管理：基本管理》中的“创建主管理员角色”。在使用 Trusted Extensions 的站点中，使用 "Primary Administrator"（主管理员）角色可能不符合安全策略。这些站点将把 `root` 转变为角色，并创建"Security Administrator"（安全管理员）角色。
- 要创建 `root` 角色，请参见《System Administration Guide: Security Services》中的“How to Make root User Into a Role”。
- 要使用 Solaris Management Console 创建角色，请参见《System Administration Guide: Security Services》中的“How to Create and Assign a Role by Using the GUI”。

Trusted Extensions 中的角色承担

与 Oracle Solaris OS 不同，Trusted Extensions 在 "Trusted Path"（可信路径）菜单中提供了 "Assume *Rolename* Role"（承担 Rolename 角色）菜单项。在确认角色口令之后，软件将使用可信路径属性激活角色工作区。角色工作区是管理工作区。此类工作区位于全局区域中。

Trusted Extensions 管理员入门（任务列表）

在管理 Trusted Extensions 之前，请熟悉以下过程。

任务	说明	参考
登录。	安全登录。	《Trusted Extensions User’s Guide》中的“Logging In to Trusted Extensions”
在桌面上执行常见用户任务。	这些任务包括： ■ 配置工作区 ■ 使用具有不同标签的工作区 ■ 访问 Trusted Extensions 手册页 ■ 访问 Trusted Extensions 联机帮助	《Trusted Extensions User’s Guide》中的“Working on a Labeled System”
执行需要可信路径的任务。	这些任务包括： ■ 分配设备 ■ 更改口令 ■ 更改工作区的标签	《Trusted Extensions User’s Guide》中的“Performing Trusted Actions”

任务	说明	参考
创建有用的角色。	创建站点的管理角色。在 LDAP 中创建角色是一项一次性任务。 "Security Administrator"（安全管理员）角色是一个很有用的角色。	第 46 页中的 “在 Trusted Extensions 中创建角色” 《Trusted Extensions Configuration Guide》中的“Create the Security Administrator Role in Trusted Extensions”
（可选）使 root 成为角色。	阻止以 root 用户身份进行匿名登录。此任务在每个系统上执行一次。	《System Administration Guide: Security Services》中的“How to Make root User Into a Role”
承担角色。	作为某个角色进入全局区域。所有管理任务都是在全局区域中执行的。	第 48 页中的 “如何进入 Trusted Extensions 的全局区域”
退出角色工作区，并成为一般用户。	离开全局区域。	第 49 页中的 “如何退出 Trusted Extensions 的全局区域”
在本地管理用户、角色、权限、区域和网络。	使用 Solaris Management Console 来管理分布式系统。	第 50 页中的 “如何使用 Solaris Management Console 管理本地系统”
使用 Trusted CDE 操作来管理系统。	使用 "Trusted_Extensions" 文件夹中的管理操作。	第 51 页中的 “如何在 Trusted Extensions 中启动 CDE 管理操作”
编辑管理文件。	在可信编辑器中编辑文件。	第 52 页中的 “如何在 Trusted Extensions 中编辑管理文件”
管理设备分配。	使用 "Device Allocation Manager – Device Administration"（设备分配管理器－设备管理）GUI。	第 214 页中的 “在 Trusted Extensions 中管理设备（任务列表）”

▼ 如何进入 Trusted Extensions 的全局区域

通过承担某个角色，您可以进入 Trusted Extensions 的全局区域。整个系统的管理只能从全局区域进行。只有超级用户或角色可以进入全局区域。

在承担某个角色之后，该角色可以在用户标签创建工作区来编辑有标签区域中的管理文件。

出于故障排除目的，您还可以通过启动故障安全会话进入全局区域。有关详细信息，请参见第 84 页中的 “如何在 Trusted Extensions 中登录到故障安全会话”。

开始之前 您已经创建了一个或多个角色，或者计划作为超级用户进入全局区域。有关指示，请参见第 46 页中的 “在 Trusted Extensions 中创建角色”。

1 **使用一种可信机制。**

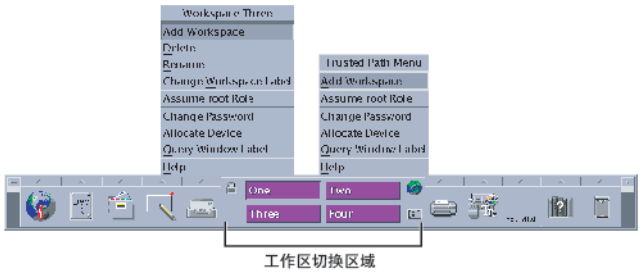
- **在 Solaris Trusted Extensions (JDS) 中，在可信窗口条中单击您的用户名，然后选择一个角色。**

  如果已为您指定了一个角色，则该角色的名称将显示在列表中。

  有关 Trusted Extensions 桌面功能的位置和意义，请参见《Trusted Extensions User's Guide》中的第 4 章 “Elements of Trusted Extensions (Reference)”。

- **在 Solaris Trusted Extensions (CDE) 中，打开 "Trusted Path"（可信路径）菜单。**

  a. **在工作区切换区域上单击鼠标右键。**



  b. **在 "Trusted Path"（可信路径）菜单中选择 "Assume *rolename* Role"（承担 rolename 角色）。**

2 **在出现提示时，键入角色口令。**

在 Trusted CDE 中，将创建一个新的角色工作区，工作区切换按钮将更改为角色桌面的颜色，同时每个窗口上方的标题栏将显示 "Trusted Path"（可信路径）。在 Trusted JDS 中，当前工作区更改为角色工作区。

在 Trusted CDE 中，可通过使用鼠标选择某个一般用户工作区来离开角色工作区。您还可删除上一个角色工作区以退出角色。在 Trusted JDS 中，在可信窗口条中单击角色名，然后在菜单中选择其他角色或用户。该操作将当前工作区更改为新角色或用户的进程。

▼ 如何退出 Trusted Extensions 的全局区域

在 Trusted JDS 和 Trusted CDE 中，用于退出角色的菜单位置不同。

开始之前 现在您处于全局区域中。

- **在这两种桌面上，您都可以单击工作区切换区域中的用户工作区。**
  您还可以通过执行下列操作之一来退出角色工作区，从而退出全局区域：

  - **在 Trusted JDS 中，在可信窗口条中单击您的角色名。**
    单击角色名时，会显示您的用户名和您可承担角色的列表。选择您的用户名后，您在该工作区中创建的所有后续窗口都将以所选用户名进行创建。您之前在当前桌面上创建的窗口将继续显示角色的名称和标签。

    如果选择了另一角色名，您将以另一角色的身份保留在全局区域中。

  - **在 Trusted CDE 中，删除角色工作区。**
    在工作区按钮上单击鼠标右键，然后选择 "Delete"（删除）。这将使您返回您占用的上一个工作区中。

▼ 如何使用 Solaris Management Console 管理本地系统

首次在系统中启动 Solaris Management Console 时，因为要注册工具并创建各种目录，因而会发生延迟。此延迟通常发生在系统配置期间。有关过程，请参见《Trusted Extensions Configuration Guide》中的“Initialize the Solaris Management Console Server in Trusted Extensions”。

要管理远程系统，请参见第 95 页中的“远程管理 Trusted Extensions（任务列表）”。

开始之前 您必须已承担了一个角色。有关详细信息，请参见第 48 页中的“如何进入 Trusted Extensions 的全局区域”。

1. **启动 Solaris Management Console。**
   在 Solaris Trusted Extensions (JDS) 中，使用命令行。

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

   在 Trusted CDE 中，您有三种选择。

   - **在终端窗口中使用 `smc` 命令。**
   - **在前面板的 "Tools"（工具）上拉菜单中，单击 Solaris Management Console 图标。**
   - **在 "Trusted_Extensions" 文件夹中，双击 Solaris Management Console 图标。**

2. **选择 "Console"（控制台）-> "Open Toolbox"（打开工具箱）。**

3. **在列表中，选择相应作用域的 Trusted Extensions 工具箱。**

   Trusted Extensions 工具箱的名称中包含 `Policy=TSOL`。"Files"（文件）作用域将更新当前系统上的本地文件。LDAP 作用域将更新 Oracle Directory Server Enterprise Edition 上的 LDAP 目录。工具箱名称类似于以下内容：

   本计算机（*this-host*: `Scope=Files, Policy=TSOL`）
   本计算机（*ldap-server*: `Scope=LDAP, Policy=TSOL`）

4. **导航至所需的 Solaris Management Console 工具。**

   此时将显示口令提示符。

   对于 Trusted Extensions 已修改的工具，单击 "System Configuration"（系统配置）。

5. **键入口令。**

   有关 Solaris Management Console 工具的更多信息，请参阅联机帮助。有关 Trusted Extensions 修改的工具的简介，请参见第 36 页中的 “Solaris Management Console 工具”。

6. **要关闭 GUI，请在 "Console"（控制台）菜单中选择 "Exit"（退出）。**

▼ 如何在 Trusted Extensions 中启动 CDE 管理操作

1. **承担角色。**

   有关详细信息，请参见第 48 页中的 “如何进入 Trusted Extensions 的全局区域”。

2. **在 Trusted CDE 中，启动 "Application Manager"（应用程序管理器）。**

   a. **在背景上单击鼠标右键以便初启工作区菜单。**

b. **单击 "Applications"（应用程序），然后单击 "Application Manager"（应用程序管理器）菜单项。**

"Trusted_Extensions" 文件夹位于 "Application Manager"（应用程序管理器）中。

3 **打开 "Trusted_Extensions" 文件夹。**

4 **双击相应的图标。**

有关管理操作的列表，请参见第 32 页中的 “Trusted CDE 操作”。

▼ 如何在 Trusted Extensions 中编辑管理文件

管理文件是使用包含审计功能的可信编辑器编辑的。该编辑器还会阻止用户执行 shell 命令，并阻止用户将文件保存为原始文件名之外的任何文件名。

1 **承担角色。**

有关详细信息，请参见第 48 页中的 “如何进入 Trusted Extensions 的全局区域”。

2 **打开一个可信编辑器。**

- **在 Solaris Trusted Extensions (CDE) 中，执行以下操作：**

  a. **要初启编辑器，请在背景上单击鼠标右键以初启工作区菜单。**

  b. **单击 "Applications"（应用程序），然后单击 "Application Manager"（应用程序管理器）菜单项。**

  "Trusted_Extensions" 文件夹位于 "Application Manager"（应用程序管理器）中。

c. **打开 "Trusted_Extensions" 文件夹。**

d. **双击 "Admin Editor"（管理编辑器）操作。**
系统将提示您提供文件名。有关格式，请参见步骤 3 和步骤 4。

- **在 Solaris Trusted Extensions (JDS) 中，执行以下操作：**
  - **可选要使用 `gedit` 作为可信编辑器，请修改 `EDITOR` 变量。**
    有关详细信息，请参见第 64 页中的 “如何将所选的编辑器指定为可信编辑器”。
  - **使用命令行初启可信编辑器。**
    ```
    # /usr/dt/bin/trusted_edit filename
    ```
    必须提供 *filename* 参数。

3 **要创建新文件，请键入新文件的完整路径名。**
保存文件时，编辑器将创建一个临时文件。

4 **要编辑现有文件，请键入现有文件的完整路径名。**

注 – 如果您的编辑器提供了 "Save As"（另存为）选项，请勿使用该选项。请使用编辑器的 "Save"（保存）选项来保存文件。

---

5 **要将文件保存到指定的路径名，请关闭编辑器。**

◆ ◆ ◆ 第 4 章

Trusted Extensions 系统上的安全要求（概述）

本章介绍了配置有 Trusted Extensions 的系统上的可配置安全功能。

可配置的 Oracle Solaris 安全功能

Trusted Extensions 使用的安全功能与 Oracle Solaris OS 提供的安全功能相同，并且增加了一些功能。例如，Oracle Solaris OS 提供了 `eeprom` 保护、口令要求和强大的口令算法、通过将用户锁定在外实现的系统保护，以及禁用键盘关机等功能。

Trusted Extensions 与 Oracle Solaris OS 之间的区别体现在用来修改这些安全缺省值的实际过程。在 Trusted Extensions 中，您通常通过承担某个角色来管理系统。本地设置是通过使用可信编辑器来修改的。会影响用户、角色和主机的网络的更改是在 Solaris Management Console 中进行的。

用于配置安全功能的 Trusted Extensions 接口

本书只提供了具有以下特征的过程：在这些过程中，Trusted Extensions 要求必须使用某个特定的端口来修改安全设置，而在 Oracle Solaris OS 中该端口是可选的。对于 Trusted Extensions 要求使用可信编辑器来编辑本地文件的情况，本书没有再另外提供相应的过程。例如，第 90 页中的 “如何防止锁定用户帐户”过程介绍了如何使用 Solaris Management Console 来更新某个用户帐户以阻止该帐户被锁定。但是，本书没有提供用于设置在整个系统范围内起作用的口令锁定策略的过程。您可以遵循 Oracle Solaris 说明，但不同的是，在 Trusted Extensions 中，您使用可信编辑器来修改系统文件。

Trusted Extensions 对 Oracle Solaris 安全机制的扩展

与在 Oracle Solaris OS 一样，以下 Oracle Solaris 安全机制在 Trusted Extensions 中是可扩展的：

- **审计事件和类**—《System Administration Guide: Security Services》中的第 30 章 “Managing Oracle Solaris Auditing (Tasks)”介绍了如何添加审计事件和审计类。
- **权限配置文件**—《System Administration Guide: Security Services》中的第 III 部分, “Roles, Rights Profiles, and Privileges”介绍了如何添加权限配置文件。
- **角色**—《System Administration Guide: Security Services》中的第 III 部分, “Roles, Rights Profiles, and Privileges”介绍了如何添加角色。
- **授权**－有关添加新授权的示例，请参见第 223 页中的 “在 Trusted Extensions 中定制设备授权（任务列表）”。

与在 Oracle Solaris OS 中一样，特权不可扩展。

Trusted Extensions 安全功能

Trusted Extensions 提供了以下独有的安全功能：

- **标签**－为主体和对象设置标签。为进程设置标签。为区域和网络设置标签。
- **"Device Allocation Manager"（设备分配管理器）**—缺省情况下，设备由分配要求来提供保护。"Device Allocation Manager"（设备分配管理器）GUI 是供管理员和一般用户使用的界面。
- **"Change Password"（更改口令）菜单项**—使用 "Trusted Path"（可信路径）菜单，您可以更改您的用户口令和已承担角色的口令。

安全要求实施

为确保系统安全不会受到危害，管理员需要对口令、文件和审计数据进行保护。用户需要参加培训以便正确履行自己的安全职责。为了与已评估配置的要求一致，请遵循本节中的准则。

用户和安全要求

每个站点的安全管理员要确保对用户进行安全规程方面的培训。安全管理员需要向新员工传达以下规则，并且定期提醒现有员工遵守这些规则：

- 不要将您的口令告诉任何人。

  知道您口令的人可以与您一样访问相同的数据，并且无法被识别，因此无法追究其责任。

- 不要写下口令，也不要将其包含在电子邮件中。
- 选择难以猜测的口令。
- 不要通过电子邮件将您的口令发送给任何人。
- 不要在未锁屏或未注销的情况下离开计算机而使其处于无人看管状态。
- 请记住，管理员不依靠电子邮件向用户发送说明。在与管理员进行确认之前，绝不要按照管理员通过电子邮件发送的说明进行操作。

  请注意，电子邮件中的发件人信息可以伪造。
- 因为您负责维护您创建的文件和目录的访问权限，所以请确保您的文件和目录的权限设置正确。不要允许未经授权的用户读取文件、更改文件、列出目录的内容或者向目录添加内容。

您所在的站点可能会提供其他建议。

电子邮件的使用

使用电子邮件来指导用户执行操作是一种不安全的做法。

请告诉用户不要相信其中包含冒充来自管理员的说明的电子邮件。欺骗性电子邮件可能会被用来诱使用户将口令更改为特定值或者泄漏口令，随后攻击者可以使用该口令登录并危害系统安全。对用户进行警示可以防止发生此情况。

口令实施

在创建新帐户时，"System Administrator"（系统管理员）角色必须指定一个唯一的用户名和用户 ID。为新帐户选择名称和 ID 时，作为管理员的您必须确保用户名和关联 ID 在网络上的任何位置都不重复，并且之前没有使用过。

"Security Administrator"（安全管理员）角色负责指定每个帐户的原始口令，并将该口令告知新帐户的用户。管理口令时，您必须考虑以下信息：

- 对于能够承担"Security Administrator"（安全管理员）角色的用户，请确保将其帐户配置为无法被锁定。此做法可确保当所有其他帐户被锁定时，至少有一个帐户始终可以登录并承担 "Security Administrator"（安全管理员）角色，以便重新打开每个人的帐户。
- 将口令发送给新帐户的用户时，请使用其他任何人都无法窃听的方法。
- 如果您怀疑不应当知道某个帐户口令的某人已经知道了该口令，请更改该口令。
- 在系统生命周期内绝不要重复使用某个用户名或用户 ID。

确保用户名和用户 ID 没有重复使用可以防止在执行下列任务时产生困扰：

- 分析审计记录时，确定哪个用户执行了哪项操作
- 恢复归档文件时，确定哪个用户拥有哪些文件

信息保护

作为管理员，您应当负责为对安全至关重要的文件正确设置和维护自主访问控制 (Discretionary Access Control, DAC) 和强制访问控制 (Mandatory Access Control, MAC) 保护。这些重要文件包括：

- `shadow` **文件**—包含加密的口令。请参见 `shadow(4)`。
- `prof_attr` **数据库**—包含权限配置文件的定义。请参见 `prof_attr(4)`。
- `exec_attr` **数据库**—包含权限配置文件中的命令和操作。请参见 `exec_attr(4)`。
- `user_attr` **文件**—包含指定给本地用户的权限配置文件、特权和授权。请参见 `user_attr(4)`。
- **审计迹**—包含审计服务已收集的审计记录。请参见 `audit.log(4)`

注意 – 因为用于 LDAP 条目的保护机制不受控于 Trusted Extensions 软件实施的访问控制策略，所以绝不要修改缺省的 LDAP 条目，也绝不要修改其访问规则。

口令保护

在本地文件中，口令是受保护的，不允许通过 DAC 来查看口令，也不允许通过 DAC 和 MAC 来修改口令。本地帐户的口令是在 `/etc/shadow` 文件中维护的，该文件只能由超级用户进行读取。有关更多信息，请参见 `shadow(4)` 手册页。

组管理

"System Administrator"（系统管理员）角色需要在本地系统和网络上验证所有组都具有唯一的组 ID (Group ID, GID)。

当某个本地组被从系统中删除时，"System Administrator"（系统管理员）角色必须确保以下内容：

- 具有已删除组的 GID 的所有对象都必须被删除，或者指定给其他组。
- 所有使用已删除组作为其主组的用户必须被重新指定到其他主组。

用户删除操作

当某个帐户被从系统中删除时，"System Administrator"（系统管理员）角色和 "Security Administrator"（安全管理员）角色必须执行以下操作：

- 在每个区域中删除该帐户的起始目录。
- 删除被删除帐户拥有的所有进程或作业：
  - 删除该帐户拥有的所有对象，或者将这些对象的所有权指定给其他用户。
  - 删除以该用户的身份调度的所有 `at` 或 `batch` 作业。有关详细信息，请参见 `at(1)` 和 `crontab(1)` 手册页。
- 绝不要重复使用该用户（帐户）名称或用户 ID。

更改数据的安全级别时的规则

缺省情况下，一般用户可以对文件和选定项执行剪切和粘贴、复制和粘贴以及拖放操作。源和目标必须使用同一标签。

更改文件的标签或者更改文件内的信息的标签需要授权。当用户被授予了更改数据的安全级别授权时，"Selection Manager"（选择管理器）应用程序将充当传输过程中的中间媒介。在 Trusted CDE 中，`/usr/dt/config/sel_config` 文件控制重新为文件设置标签的操作，以及向另一标签进行的信息剪切和复制。在 Trusted JDS 中，`/usr/share/gnome/sel_config` 文件控制这些传输。在 Trusted CDE 中，`/usr/dt/bin/sel_mgr` 应用程序控制窗口之间的拖放操作。如下表所示，重新为选定项设置标签要比重新为文件设置标签受到更严格的限制。

下表汇总了重新为文件设置标签所适用的规则。这些规则涵盖了剪切和粘贴、复制和粘贴以及拖放操作。

表 4–1 将文件改为新标签的条件

事务描述	标签关系	所有者关系	所需授权
在多个文件管理器之间复制和粘贴、剪切和粘贴或者拖放文件	相同标签	相同 UID	无
	降级	相同 UID	`solaris.label.file.downgrade`
	升级	相同 UID	`solaris.label.file.upgrade`
	降级	不同 UID	`solaris.label.file.downgrade`
	升级	不同 UID	`solaris.label.file.upgrade`

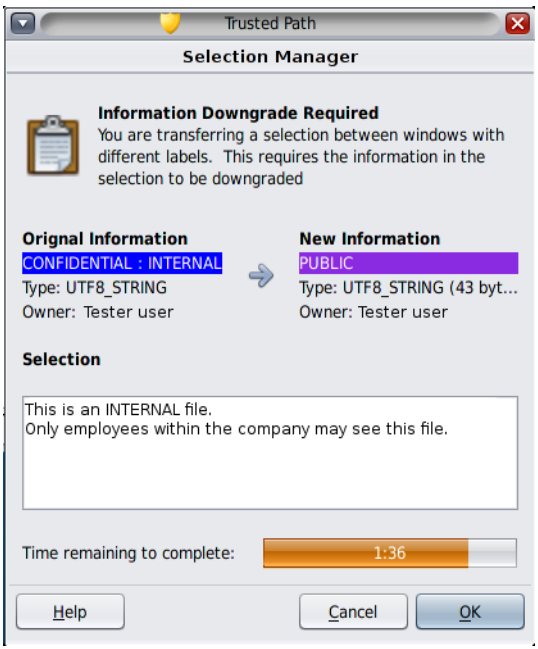
对于窗口或文件中的选定项，应用的是与上述规则不同的规则。拖放**选定项**始终要求标签和所有权与原来相同。在窗口之间的拖放操作中，起中介作用的是 "Selection Manager"（选择管理器）应用程序而不是 `sel_config` 文件。

下表汇总了更改选定项标签时适用的规则。

表 4–2 将选定项改为新标签的条件

事务描述	标签关系	所有者关系	所需授权
在窗口之间复制和粘贴或者剪切和粘贴选定项	相同标签	相同 UID	无
	降级	相同 UID	`solaris.label.win.downgrade`
	升级	相同 UID	`solaris.label.win.upgrade`
	降级	不同 UID	`solaris.label.win.downgrade`
	升级	不同 UID	`solaris.label.win.upgrade`
在窗口之间拖放选定项	相同标签	相同 UID	不适用

Trusted Extensions 提供了一个选择确认器，在标签更改过程中起中介作用。当经授权的用户试图更改文件或选定项的标签时，该窗口将出现。用户有 120 秒的时间来确认操作。要在不使用此窗口的情况下更改数据的安全级别，除了需要“重新设置标签”的授权之外，还需要 `solaris.label.win.noview` 授权。下图显示了窗口中的一个选定项 `zonename`。



缺省情况下，当数据传输到不同的标签时将显示选择确认器。如果某个选择要求做出多个传输决策，则自动回复机制提供了一种一次回复多个传输的方法。有关更多信息，请参见 sel_config(4) 手册页及下面的部分。

sel_config 文件

当操作会升级或降级某一标签时，将检查 sel_config 文件来确定选择确认器的行为。

sel_config 文件定义了以下内容：

- 为其提供自动回复的选择类型的列表
- 特定类型的操作是否可以自动确认
- 是否显示选择确认器对话框

在 Trusted CDE 中，安全管理员角色可以使用 "Trusted_Extensions" 文件夹中的 "Configure Selection Confirmation"（配置选择确认）操作来更改缺省值。新设置在下次登录时生效。在 Solaris Trusted Extensions (JDS) 中，该 CDE 操作不可用。要更改缺省值，请在文本编辑器中修改 /usr/share/gnome/sel_config 文件。

定制 Solaris Trusted Extensions (CDE)

在 Solaris Trusted Extensions (CDE) 中，用户可以向前面板添加操作，还可以定制工作区菜单。Trusted Extensions 软件限制了用户向 CDE 添加程序和命令的能力。

定制前面板

任何人都可以将预先存在的操作从 "Application Manager"（应用程序管理器）拖放到前面板中，只要执行修改的帐户在其配置文件中具有该操作。/usr/dt/ 或 /etc/dt/ 目录中的操作可以添加到前面板中，但是 $HOME/.dt/appconfig 目录中的应用程序不能添加到前面板中。虽然用户可以使用 "Create Action"（创建操作）操作，但他们不能向存储有在系统范围内起作用的操作的目录进行写入。因此，一般用户不能创建可以使用的操作。

在 Trusted Extensions 中，操作的搜索路径已更改。任何个人起始目录中的操作都是最后处理，而不是首先处理。因此，没有人可以定制现有操作。

"Security Administrator"（安全管理员）角色被指定可进行 "Admin Editor"（管理编辑器）操作，因此可以对 /usr/dt/appconfig/types/C/dtwm.fp 文件和前面板子面板的其他配置文件进行任意所需的修改。

定制工作区菜单

工作区菜单是当您在工作区背景上单击鼠标右键时出现的菜单。一般用户可以定制该菜单，并且可以向该菜单添加菜单项。

当允许用户在多个标签工作时，需要满足下列条件：

- 用户必须在全局区域中具有起始目录。

  要保存定制内容，全局区域中的进程必须能够在正确的标签向用户起始目录中进行写入。全局区域进程可向其进行写入的用户起始目录的区域路径类似于以下格式：

  `/zone/`*`zone-name`*`/home/`*`username`*
- 用户必须在一般用户工作区中使用 "Customize Menu"（定制菜单）和 "Add Item to Menu"（向菜单添加菜单项）选项。用户可以为每个标签创建不同的定制内容。
- 当用户承担一个角色时，对工作区菜单所做的更改保持不变。
- 对工作区菜单所做的更改存储在用户在当前标签的起始目录中。已定制的菜单文件是 `.dt/wsmenu`。
- 用户的权限配置文件必须使用户能够运行所需的操作。

  添加到工作区菜单的任何操作都必须由用户的某个权限配置文件进行处理。否则，在调用操作时，操作会失败，并且将显示错误消息。

  例如，任何可执行 "Run"（运行）操作的用户都可以双击可执行文件的图标并使其运行，即使该操作或该操作调用的命令没有包含在帐户的某个权限配置文件中。缺省情况下，没有为角色指定 "Run"（运行）操作。因此，当角色执行任何需要 "Run"（运行）操作的菜单项时，该菜单项会失败。

◆ ◆ ◆ 第 5 章

在 Trusted Extensions 中管理安全要求（任务）

本章介绍了在配置有 Trusted Extensions 的系统上通常会执行的任务。

Trusted Extensions 中的常见任务（任务列表）

下面的任务列表介绍了为 Trusted Extensions 管理员设置工作环境的过程。

任务	说明	参考
更改可信编辑器的编辑器程序。	指定管理文件的编辑器。	第 64 页中的 “如何将所选的编辑器指定为可信编辑器”
更改 root 的口令。	为 root 用户或 root 角色指定新口令。	第 65 页中的 “如何更改 root 的口令”
更改角色的口令。	为您的当前角色指定新口令。	示例 5–2
使用安全注意键组合。	获得鼠标或键盘的控制权。另外，还测试鼠标或键盘是否可信。	第 66 页中的 “如何重新获得对桌面当前焦点的控制权”
确定标签的十六进制数字。	显示文本标签的内部表示形式。	第 66 页中的 “如何获取标签的十六进制等效值”
确定标签的文本表示形式。	显示十六进制标签的文本表示形式。	第 67 页中的 “如何通过标签的十六进制形式获取可读标签”
编辑系统文件。	安全地编辑 Oracle Solaris 或 Trusted Extensions 系统文件。	第 68 页中的 “如何在系统文件中更改安全缺省值”
分配设备。	使用外围设备向系统添加信息或者从系统中删除信息。	《Trusted Extensions User’s Guide》中的“How to Allocate a Device in Trusted Extensions”
远程地管理主机。	从一台远程主机管理 Oracle Solaris 或 Trusted Extensions 主机。	第 8 章，Trusted Extensions 中的远程管理（任务）

▼ 如何将所选的编辑器指定为可信编辑器

可信编辑器使用 $EDITOR 环境变量的值作为其编辑器。

开始之前 您必须是全局区域中的一个角色。

1. **确定 $EDITOR 变量的值。**

   ```
   # echo $EDITOR
   ```

   以下是可能存在的编辑器。也可能没有设置 $EDITOR 变量。

   - /usr/dt/bin/dtpad—是 CDE 提供的编辑器。
   - /usr/bin/gedit—是 Java Desktop System，发行版 *number* 提供的编辑器。Solaris Trusted Extensions (JDS) 是该桌面的可信版本。
   - /usr/bin/vi—是可视编辑器。

2. **设置 $EDITOR 变量的值。**

   - **要永久性地设置该值，请在角色的 shell 初始化文件中修改该值。**

     例如，在角色的起始目录中，修改 Korn shell 的 .kshrc 文件和 C shell 的 .cshrc 文件。

   - **要为当前 shell 设置该值，请在终端窗口中设置该值。**

     例如，在 Korn shell 中，请使用以下命令：

     ```
     # setenv EDITOR=pathname-of-editor
     # export $EDITOR
     ```

     在 C shell 中，请使用以下命令：

     ```
     # setenv EDITOR=pathname-of-editor
     ```

     在 Bourne shell 中，请使用以下命令：

     ```
     # EDITOR=pathname-of-editor
     # export EDITOR
     ```

示例 5–1 指定可信编辑器的编辑器

编辑系统文件时，"Security Administrator"（安全管理员）角色希望使用 vi。承担该角色的用户修改角色的起始目录中的 .kshrc 初始化文件。

```
$ cd /home/secadmin
$ vi .kshrc

## Interactive shell
set -o vi
...
export EDITOR=vi
```

下次任何用户承担 "Security Administrator"（安全管理员）角色时，vi 是可信编辑器。

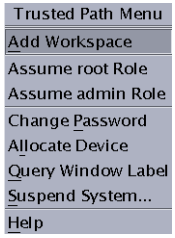
▼ 如何更改 root 的口令

"Security Administrator"（安全管理员）角色有权使用 Solaris Management Console 在任何时候更改任意帐户的口令。但是，Solaris Management Console 无法更改系统帐户的口令。**系统帐户**是 UID 低于 100 的帐户。root 是一个系统帐户，因为它的 UID 为 0。

1. **成为超级用户。**
   如果您的站点已使超级用户成为 root 角色，请承担 root 角色。
2. **在 "Trusted Path"（可信路径）菜单中，选择 "Change Password"（更改口令）。**
   - **在 Trusted JDS 中，单击可信窗口条中的可信符号。**
     从 "Trusted Path"（可信路径）菜单中，选择 "Change Password"（更改口令）。

   - **在 Solaris Trusted Extensions (CDE) 中，打开 "Trusted Path"（可信路径）菜单。**
     a. **在工作区切换区域上单击鼠标右键。**
     b. **在 "Trusted Path"（可信路径）菜单中，选择 "Change Password"（更改口令）。**

3. **更改口令，然后确认更改。**

示例 5–2 更改角色的口令

可承担在 LDAP 中定义的某个角色的任何用户都可以使用 "Trusted Path"（可信路径）菜单来更改该角色的口令。然后，口令将在 LDAP 中针对试图承担该角色的所有用户进行更改。

与在 Oracle Solaris OS 中一样，"Primary Administrator"（主管理员）角色可以使用 Solaris Management Console 更改角色的口令。在 Trusted Extensions 中，"Security Administrator"（安全管理员）角色可以使用 Solaris Management Console 更改其他角色的口令。

▼ 如何重新获得对桌面当前焦点的控制权

“安全注意”键组合可用来中断不可信的应用程序对指针或键盘的抓取。该键组合还可用来验证指针或键盘是否已被可信的应用程序抓取。在已被骗显示多个可信窗口条的多显示端系统中，该键组合可使指针切换到经授权的可信窗口条。

1 **要重新获得对 Sun 键盘的控制权，请使用以下键组合。**

同时按这些键可重新获得对当前桌面焦点的控制权。在 Sun 键盘上，菱形是 Meta 键。

```
<Meta> <Stop>
```

如果抓取（例如指针）不可信，则指针会移动到窗口条。可信指针不会移动到可信窗口条。

2 **如果您使用的不是 Sun 键盘，请使用以下键组合。**

```
<Alt> <Break>
```

在手提电脑中，同时按这些键可重新获得对当前桌面焦点的控制权。

示例 5–3 测试口令提示符是否可信

在使用 Sun 键盘的 x86 系统上，已提示用户输入口令。光标已被抓取，并且位于口令对话框中。要检查该提示是否可信，用户可同时按 <Meta> <Stop> 键。如果指针保留在对话框中，则用户可以判定该口令提示符是可信的。

如果指针移动到了可信窗口条，则用户可判定该口令提示符可能不可信，然后可以与管理员联系。

示例 5–4 强制将指针移动到可信窗口条

在本示例中，用户没有运行任何可信的进程，但无法看到鼠标指针。要将指针移回到可信窗口条的中心，用户需同时按 <Meta> <Stop> 键。

▼ 如何获取标签的十六进制等效值

此过程提供标签的内部十六进制表示形式。此表示形式可安全地用于在公共目录中进行存储。有关更多信息，请参见 `atohexlabel(1M)` 手册页。

开始之前 您必须具有全局区域中的 "Security Administrator"（安全管理员）角色。有关详细信息，请参见第 48 页中的 “如何进入 Trusted Extensions 的全局区域”。

- **要获取标签的十六进制值，请执行下列操作之一。**

  - **要获取敏感标签的十六进制值，请将标签传递到命令。**

    ```
    $ atohexlabel "CONFIDENTIAL : NEED TO KNOW"
    0x0004-08-68
    ```

  - **要获取安全许可的十六进制值，请使用 -c 选项。**

    ```
    $ atohexlabel -c "CONFIDENTIAL NEED TO KNOW"
    0x0004-08-68
    ```

注 – 人类可阅读的敏感标签和安全许可标签是根据 `label_encodings` 文件中的规则构成的。每种类型的标签使用该文件的一个单独部分中的规则。敏感标签和安全许可标签都表达相同的基础级别的敏感度时，这些标签具有相同的十六进制形式。但是，标签可具有不同的人类可阅读形式。接受人类可阅读的标签作为输入的系统接口预期输入一种类型的标签。如果标签类型的文本字符串有所差异，则这些文本字符串无法互换使用。

在缺省的 `label_encodings` 文件中，安全许可标签的等效文本不包括冒号 (:)。

示例 5–5 **使用 `atohexlabel` 命令**

当您以十六进制格式传递有效标签时，命令会返回参数。

```
$ atohexlabel 0x0004-08-68
0x0004-08-68
```

当您传递管理标签时，命令会返回参数。

```
$ atohexlabel admin_high
ADMIN_HIGH
atohexlabel admin_low
ADMIN_LOW
```

故障排除 错误消息 "`atohexlabel parsing error found in <string> at position 0`"（**在位置 `0` 处的 `<string>` 中发现 `atohexlabel` 解析错误**）表明传递到 `atohexlabel` 的 `<string>` 参数不是有效的标签或安全许可。请检查您的键入内容，并检查该标签是否存在于已安装的 `label_encodings` 文件中。

▼ 如何通过标签的十六进制形式获取可读标签

此过程提供了一种方法来修复存储在内部数据库中的标签。有关更多信息，请参见 `hextoalabel(1M)` 手册页。

开始之前 您必须具有全局区域中的 "Security Administrator"（安全管理员）角色。

- **要获取标签的内部表示形式的等效文本，请执行下列步骤之一。**
  - **要获取敏感标签的等效文本，请传递标签的十六进制形式。**

    ```
    $ hextoalabel 0x0004-08-68
    CONFIDENTIAL : NEED TO KNOW
    ```

  - **要获取安全许可的等效文本，请使用 -c 选项。**

    ```
    $ hextoalabel -c 0x0004-08-68
    CONFIDENTIAL NEED TO KNOW
    ```

▼ 如何在系统文件中更改安全缺省值

在 Trusted Extensions 中，安全管理员可以更改或访问系统中的缺省安全设置。

`/etc/security` 和 `/etc/default` 目录中的文件包含安全设置。在 Oracle Solaris 系统中，超级用户可编辑这些文件。有关 Oracle Solaris 的安全信息，请参见《System Administration Guide: Security Services》中的第 3 章 “Controlling Access to Systems (Tasks)”。

注意 – 仅当站点安全策略允许时您才能放宽系统安全缺省值。

开始之前 您必须具有全局区域中的 "Security Administrator"（安全管理员）角色。

- **使用可信编辑器来编辑系统文件。**

  有关详细信息，请参见第 52 页中的 “如何在 Trusted Extensions 中编辑管理文件”。

  下表列出了安全文件以及要在这些文件中更改的安全参数。

文件	任务	更多信息
`/etc/default/login`	减少允许的口令尝试次数。	请参见《System Administration Guide: Security Services》中的“How to Monitor All Failed Login Attempts”中的示例。 `passwd(1)` 手册页
`/etc/default/kbd`	禁用键盘关机。	《System Administration Guide: Security Services》中的“How to Disable a System’s Abort Sequence” **注 –** 在管理员用于调试的主机上，`KEYBOARD_ABORT` 的缺省设置允许访问 `kadb` 内核调试器。有关调试器的更多信息，请参见 `kadb(1M)` 手册页。

文件	任务	更多信息
/etc/security/policy.conf	要求为用户口令使用更强大的算法。 从该主机的所有用户中删除一项基本特权。 将该主机的用户的权限限制到基本的 Solaris 用户授权。	policy.conf(4) 手册页
/etc/default/passwd	要求用户经常更改口令。 要求用户创建差异最大的口令。 要求使用较长的用户口令。 要求使用无法在字典中找到的口令。	passwd(1) 手册页

◆ ◆ ◆ 第 6 章

6 Trusted Extensions 中的用户、权限和角色（概述）

本章介绍了在创建一般用户之前必须做出的基本决定，并提供了用来管理用户帐户的其他背景信息。本章假定初始设置团队已经设置了角色和有限数量的用户帐户。这些用户可以承担用于配置和管理 Trusted Extensions 的角色。有关详细信息，请参见《Trusted Extensions Configuration Guide》中的“Creating Roles and Users in Trusted Extensions”。

Trusted Extensions 中的用户安全功能

Trusted Extensions 软件针对用户、角色或权限配置文件添加了以下安全功能：

- 用户具有一个标签范围，用户可以在此范围内使用系统。
- 角色具有一个标签范围，可以在此范围内使用角色来执行管理任务。
- Trusted Extensions 权限配置文件可以包括 CDE 管理操作。与命令一样，操作可以具有安全属性。
- Trusted Extensions 权限配置文件中的命令和操作具有一个标签属性。命令或操作必须在标签范围内或在特定标签执行。
- Trusted Extensions 软件向 Oracle Solaris OS 定义的特权和授权集中添加了特权和授权。

管理员针对用户的职责

"System Administrator"（系统管理员）角色负责创建用户帐户。"Security Administrator"（安全管理员）角色负责设置帐户的安全属性。

如果您将 Oracle Directory Server Enterprise Edition 用于 LDAP 命名服务，请检查初始设置团队是否配置了 `tsol_ldap.tbx` 工具箱。有关过程，请参见《Trusted Extensions Configuration Guide》中的“Configuring the Solaris Management Console for LDAP (Task Map)”。

有关设置用户和角色的详细信息，请参见以下内容：

- 《Oracle Solaris 管理：基本管理》中的“如何创建第一个角色（主管理员）”
- 《Oracle Solaris 管理：基本管理》中的“设置用户帐户（任务列表）”
- 《System Administration Guide: Security Services》中的第 III 部分, “Roles, Rights Profiles, and Privileges”

系统管理员针对用户的职责

在 Trusted Extensions 中，"System Administrator"（系统管理员）角色负责决定哪些用户可以访问系统。系统管理员负责执行以下任务：

- 添加和删除用户
- 添加和删除角色
- 修改除安全属性以外的用户和角色配置

安全管理员针对用户的职责

在 Trusted Extensions 中，安全管理员角色负责用户或角色的所有安全属性。安全管理员负责执行以下任务：

- 指定和修改用户、角色或权限配置文件的安全属性
- 创建和修改权限配置文件
- 为用户或角色指定权限配置文件
- 为用户、角色或权限指定特权
- 为用户、角色或权限配置文件指定授权
- 从用户、角色或权限配置文件删除特权
- 从用户、角色或权限配置文件删除授权

通常，安全管理员角色负责创建权限配置文件。不过，如果配置文件需要安全管理员角色无法授予的功能，则超级用户或主管理员角色可以创建此配置文件。

在创建权限配置文件之前，安全管理员需要分析新配置文件中是否有任何命令或操作需要特权或授权才能成功。各个命令的手册页列出了可能需要的特权和授权。有关需要特权和授权的操作的示例，请参见 `exec_attr` 数据库。

在 Trusted Extensions 中创建用户之前要做的决策

以下决策影响着用户在 Trusted Extensions 能够执行的操作以及需付出的努力。一些决策与在安装 Oracle Solaris OS 时所做的决策相同。不过，特定于 Trusted Extensions 的决策会影响站点安全性和易用性。

- 决定是否更改 `policy.conf` 文件中的缺省用户安全属性。`label_encodings` 文件中的用户缺省值是由初始设置团队配置的。有关缺省值的说明，请参见第 73 页中的 “Trusted Extensions 中的缺省用户安全属性”。
- 决定要将哪些启动文件（如果有）从每个用户的最小标签起始目录复制或链接至用户的较高级别起始目录。有关过程，请参见第 81 页中的 “如何在 Trusted Extensions 中为用户配置启动文件”。
- 决定用户是否可以访问外围设备，如麦克风、CD-ROM 驱动器和 JAZ 驱动器。

  如果允许某些用户访问，则决定您的站点是否需要额外的授权来满足站点安全性。有关与设备相关的授权的缺省列表，请参见第 227 页中的 “如何指定设备授权”。有关更为细化的设备授权集，请参见第 223 页中的 “在 Trusted Extensions 中定制设备授权（任务列表）”。

Trusted Extensions 中的缺省用户安全属性

`label_encodings` 和 `policy.conf` 文件中的设置共同定义了用户帐户的缺省安全属性。您为用户显式设置的值将覆盖这些系统值。在这些文件中设置的某些值还应用于角色帐户。有关可显式设置的安全属性，请参见第 74 页中的 “Trusted Extensions 中的可配置用户属性”。

`label_encodings` 文件缺省值

`label_encodings` 文件定义了用户的最小标签、安全许可和缺省的标签视图。有关此文件的详细信息，请参见 `label_encodings(4)` 手册页。您的站点的 `label_encodings` 文件是由初始设置团队安装的。他们的决策基于《Trusted Extensions Configuration Guide》中的“Devising a Label Strategy”以及《Trusted Extensions Label Administration》中的示例。

安全管理员在 Solaris Management Console 中为各个用户显式设置的标签值源自 `label_encodings` 文件。显式设置的值将覆盖 `label_encodings` 文件中的值。

Trusted Extensions 中的 `policy.conf` 文件缺省值

Oracle Solaris 的 `/etc/security/policy.conf` 文件包含系统的缺省安全设置。Trusted Extensions 向此文件中添加了两个关键字。如果要更改在系统范围内起作用的值，可以将这些“关键字=值”对添加至此文件。这些关键字是由 Trusted Extensions 实施的。下表显示了这些安全设置的可能值及其缺省值。

表 6–1 policy.conf 文件中的 Trusted Extensions 安全缺省值

关键字	缺省值	可能值	附注
IDLECMD	LOCK	LOCK | LOGOUT	不适用于角色。
IDLETIME	30	0 to 120 minutes	不适用于角色。

policy.conf 文件中定义的授权和权限配置文件是对为各个帐户指定的任何授权和配置文件的**补充**。对于其他字段，个体用户的值将覆盖系统值。

《Trusted Extensions Configuration Guide》中的"Planning User Security in Trusted Extensions"包括了每个 policy.conf 关键字的表。另请参见 policy.conf(4) 手册页。

Trusted Extensions 中的可配置用户属性

Solaris Management Console 2.1 是您用于创建和修改用户帐户的工具。对于可在多个标签登录的用户，您可能还希望在每个用户的最小标签起始目录中设置 .copy_files 和 .link_files 文件。

"User Accounts"（用户帐户）工具在 Solaris Management Console 中的工作方式与在 Oracle Solaris OS 中相同，但有两个例外：

- Trusted Extensions 向用户帐户添加了属性。
- 在 Trusted Extensions 中，起始目录服务器访问需要管理员进行干预。
  - 您按照与在 Oracle Solaris 系统中相同的方式创建起始目录服务器条目。
  - 然后，您和用户执行额外的步骤在每个用户标签挂载起始目录。

如《Oracle Solaris 管理：基本管理》中的"如何用 Solaris Management Console 的 "Users" 工具添加用户"所述，使用向导能够快速创建用户帐户。使用向导之后，您可以修改用户的缺省 Trusted Extensions 属性。

有关 .copy_files 和 .link_files 文件的更多信息，请参见第 76 页中的 ".copy_files 和 .link_files 文件"。

必须为用户指定的安全属性

安全管理员角色必须为新用户指定某些安全属性，如下表所示。有关包含缺省值的文件的信息，请参见第 73 页中的 "Trusted Extensions 中的缺省用户安全属性"。下表显示了可为用户指定的安全属性以及每项指定所产生的影响。

表 6–2 创建用户后指定的安全属性

用户属性	缺省值的位置	是否需要操作	操作的影响
Password（口令）	无	需要	用户具有口令
Roles（角色）	无	可选	用户可以承担角色
Authorizations（授权）	`policy.conf` 文件	可选	用户获得额外的授权
Rights Profiles（权限配置文件）	`policy.conf` 文件	可选	用户获得额外的权限配置文件
Labels（标签）	`label_encodings` 文件	可选	用户获得不同的缺省标签或认可范围
Privileges（特权）	`policy.conf` 文件	可选	用户获得不同的特权集
Account Usage（帐户使用）	`policy.conf` 文件	可选	针对空闲状态下的计算机，用户获得了不同的计算机设置
Audit（审计）	`audit_control` 文件	可选	将以不同于系统审计设置的方式审计用户

Trusted Extensions 中的用户安全属性指定

用户帐户创建之后，安全管理员角色在 Solaris Management Console 中为用户指定安全属性。如果您已经设置了正确的缺省值，则下一步是仅为需要非缺省值的用户指定安全属性。

为用户指定安全属性时，安全管理员会考虑以下信息：

指定口令

安全管理员角色在帐户创建之后为用户帐户指定口令。在此初始指定之后，用户可更改其口令。

在 Oracle Solaris OS 中，可强制用户定期更改其口令。口令生命期选项限制了能够猜测或窃取口令的任何入侵者可能能够非法访问系统的时间长度。此外，设定在更改口令之前需经过的最小时间可防止具有新口令的用户立即恢复为旧口令。有关详细信息，请参见 `passwd(1)` 手册页。

注 – 可以承担角色的用户的口令决不能受制于任何口令生命期约束。

分配角色
用户不是必须具有某个角色不可。可以为单个用户指定多个角色（如果这样做符合您的站点的安全策略）。

指定授权
在 Oracle Solaris OS 中，直接为用户指定授权会将这些授权添加至现有授权。在 Trusted Extensions 中，可将授权添加到一个权限配置文件中，然后将该配置文件指定给用户。

指定权限配置文件
在 Oracle Solaris OS 中，配置文件的顺序至关重要。配置文件机制使用帐户配置文件集中的命令或操作的第一个实例。

您可以按照对您有利的方式使用配置文件的排序顺序。如果您希望命令在运行时使用的安全属性不同于在现有配置文件中为该命令定义的安全属性，可创建一个新的配置文件并包含您希望为该命令指定的安全属性。然后，将此新配置文件插入到现有配置文件之前。

注 – 不要将包含管理操作或管理命令的权限配置文件指定给一般用户。因为一般用户无法进入全局区域，所以该配置文件将不能正常工作。

更改特权缺省值
对于许多站点来说，缺省特权集的限制可能不够严厉。要限制系统上任何一般用户的特权集，请更改 `policy.conf` 文件设置。要更改各个用户的特权集，请使用 Solaris Management Console。有关示例，请参见第 88 页中的 “如何收缩用户的特权集”。

更改标签缺省值
更改用户的标签缺省值会在 `label_encodings` 文件中创建非用户缺省值。

更改审计缺省值
与在 Oracle Solaris OS 中一样，为用户指定审计类会在系统上创建与在 `/etc/security/audit_control` 文件中指定的审计类不同的审计类。有关审计的更多信息，请参见第 18 章，Trusted Extensions 审计（概述）。

`.copy_files` 和 `.link_files` 文件

在 Trusted Extensions 中，这些文件会自动从框架目录**仅**复制到包含帐户的最小标签的区域中。要确保较高级别标签的区域可使用启动文件，用户或管理员必须创建 `.copy_files` 和 `.link_files` 文件。

Trusted Extensions 文件 `.copy_files` 和 `.link_files` 用来帮助将启动文件自动复制或链接至帐户的起始目录的每个标签中。每当用户在新标签创建工作区时，`updatehome` 命令都会读取帐户最小标签的 `.copy_files` 和 `.link_files` 的内容。然后，该命令将列出的每个文件复制或链接到标签级别较高的工作区中。

当用户希望在不同的标签使用稍有差别的启动文件时，.copy_files 文件非常有用。例如，当用户在不同的标签使用不同的邮件别名时，应优先采用复制方式。当启动文件在调用它的任何标签都应相同时，.link-files 文件非常有用。例如，当一台打印机用于所有带标签的打印作业时，应优先采用链接方式。有关示例文件，请参见第 81 页中的 “如何在 Trusted Extensions 中为用户配置启动文件”。

下面列出了一些您可能希望用户能够复制或链接至较高级别标签的启动文件：

- .acrorc
- .aliases
- .cshrc
- .dtprofile
- .emacs
- .login
- .mailrc
- .mime_types
- .newsrc
- .profile
- .signature
- .soffice
- .Xdefaults
- .Xdefaults-*hostname*

◆ ◆ ◆ 第 7 章

7 在 Trusted Extensions 中管理用户、权限和角色（任务）

本章提供了在 Trusted Extensions 中配置和管理用户、用户帐户及权限配置文件的过程。

针对安全性定制用户环境（任务列表）

下面的任务列表介绍了在针对所有用户定制系统时或定制各个用户帐户时可以执行的常见任务。

任务	说明	参考
更改标签属性。	为用户帐户修改标签属性，例如最小标签和缺省标签视图。	第 80 页中的 “如何修改缺省用户标签属性”
针对系统的所有用户更改 Trusted Extensions 策略。	更改 `policy.conf` 文件。	第 80 页中的 “如何修改 `policy.conf` 缺省值”
	在经过指定的时间后打开屏幕保护程序。 在系统空闲指定的时间后注销用户。	示例 7–1
	为系统的所有普通用户删除不必要的特权。	示例 7–2
	从公共资讯服务站上的打印输出中删除标签。	示例 7–3
为用户配置初始化文件。	为所有用户配置启动文件，例如 `.cshrc`、`.copy_files` 和 `.soffice`。	第 81 页中的 “如何在 Trusted Extensions 中为用户配置启动文件”

任务	说明	参考
登录到一个故障安全会话。	修复出现故障的用户初始化文件。	第 84 页中的“如何在 Trusted Extensions 中登录到故障安全会话”

▼ 如何修改缺省用户标签属性

您可以在配置第一个系统期间修改缺省用户标签属性。必须将更改复制到每个 Trusted Extensions 主机。

开始之前 您必须具有全局区域中的 "Security Administrator"（安全管理员）角色。有关详细信息，请参见第 48 页中的“如何进入 Trusted Extensions 的全局区域”。

1. **在 `/etc/security/tsol/label_encodings` 文件中查看缺省用户属性设置。**
   有关缺省值，请参见第 73 页中的“`label_encodings` 文件缺省值”。
2. **在 `label_encodings` 文件中修改用户属性设置。**
   请使用可信编辑器。有关详细信息，请参见第 52 页中的“如何在 Trusted Extensions 中编辑管理文件”。在 Trusted CDE 中，您还可以使用 "Edit Label Encodings"（编辑标签编码）操作。有关详细信息，请参见第 51 页中的“如何在 Trusted Extensions 中启动 CDE 管理操作”。

   `label_encodings` 文件应该在所有主机上都相同。
3. **将文件的副本分布到每个 Trusted Extensions 主机。**

▼ 如何修改 `policy.conf` 缺省值

在 Trusted Extensions 中更改 `policy.conf` 缺省值类似于在 Oracle Solaris OS 中更改任何安全相关系统文件。在 Trusted Extensions 中，使用可信编辑器修改系统文件。

开始之前 您必须具有全局区域中的 "Security Administrator"（安全管理员）角色。有关详细信息，请参见第 48 页中的“如何进入 Trusted Extensions 的全局区域”。

1. **在 `/etc/security/policy.conf` 文件中查看缺省设置。**
   有关 Trusted Extensions 关键字，请参见表 6–1。
2. **修改设置。**
   使用可信编辑器来编辑系统文件。有关详细信息，请参见第 52 页中的“如何在 Trusted Extensions 中编辑管理文件”。

示例 7–1 更改系统的空闲设置

在本例中，安全管理员想让空闲的系统返回到登录屏幕。缺省情况下会锁定空闲系统。因此，安全管理员角色将 IDLECMD 关键字=值对添加到 /etc/security/policy.conf 文件中，如下所示：

```
IDLECMD=LOGOUT
```

管理员还想缩短系统在注销之前空闲的时间。因此，安全管理员角色将 IDLETIME 关键字=值对添加到 policy.conf 文件中，如下所示：

```
IDLETIME=10
```

现在，系统会在空闲 10 分钟后注销用户。

示例 7–2 修改每个用户的基本特权集

在本例中，Sun Ray 安装的安全管理员不希望一般用户查看其他 Sun Ray 用户的进程。因此，在配置有 Trusted Extensions 的每个系统上，管理员将从基本特权集中删除 proc_info。对 /etc/policy.conf 文件中的 PRIV_DEFAULT 设置做如下修改：

```
PRIV_DEFAULT=basic,!proc_info
```

示例 7–3 为系统的所有用户指定与打印相关的授权

在本例中，安全管理员通过在计算机的 /etc/security/policy.conf 文件中键入以下内容来允许公共 kiosk 计算机在没有标签的情况下进行打印。在下次引导时，此 kiosk 的所有用户执行的打印作业都会在没有页面标签的情况下打印。

```
AUTHS_GRANTED= solaris.print.unlabeled
```

然后，管理员决定通过删除标题页和篇尾页来节省纸张。她首先在 "Print Manager"（打印管理器）中确保未选中 "Always Print Banners"（始终打印标题）复选框。然后修改 policy.conf 条目以读取以下内容并重新引导。此时，所有打印作业都是无标签的，且没有标题页或篇尾页。

```
AUTHS_GRANTED= solaris.print.unlabeled,solaris.print.nobanner
```

▼ 如何在 Trusted Extensions 中为用户配置启动文件

用户可以以对应于其最小敏感标签的标签将 .copy_files 文件和 .link_files 文件放入其起始目录中。用户还可以修改其最小标签的现有 .copy_files 和 .link_files 文件。管理员角色可以使用此过程来自动化站点的设置。

开始之前 您必须具有全局区域中的 "System Administrator"（系统管理员）角色。有关详细信息，请参见第 48 页中的 “如何进入 Trusted Extensions 的全局区域”。

1. **创建两个 Trusted Extensions 启动文件。**

   将 `.copy_files` 和 `.link_files` 添加到您的启动文件列表中。

   ```
   # cd /etc/skel
   # touch .copy_files .link_files
   ```

2. **定制 `.copy_files` 文件。**

   a. **启动可信编辑器。**

      有关详细信息，请参见第 52 页中的 “如何在 Trusted Extensions 中编辑管理文件”。

   b. **键入 `.copy_files` 文件的完整路径名。**

      ```
      /etc/skel/.copy_files
      ```

   c. **在 `.copy_files` 中键入要复制到用户所有标签起始目录中的文件，每行键入一个文件。**

      可使用 第 76 页中的 “`.copy_files` 和 `.link_files` 文件”作为参考。有关文件样例，请参见示例 7–4。

3. **定制 `.link_files` 文件。**

   a. **在可信编辑器中，键入 `.link_files` 文件的完整路径名。**

      ```
      /etc/skel/.link_files
      ```

   b. **在 `.link_files` 中键入要链接到用户在所有标签的起始目录中的文件，每行键入一个文件。**

4. **为您的用户定制其他启动文件。**

   - 有关启动文件中要包括的内容的讨论，请参见《Oracle Solaris 管理：基本管理》中的“定制用户的工作环境”。
   - 有关详细信息，请参见《Oracle Solaris 管理：基本管理》中的“如何定制用户初始化文件”。
   - 有关示例，请参见示例 7–4。

5. **可选为其缺省 shell 是“配置文件 shell”的用户创建 `skelP` 子目录。**

   `P` 表示 Profile（配置文件）shell。

6. **将定制的启动文件复制到相应的框架目录中。**

7. **创建用户时，请使用相应的 `skel`*X* 路径名。**

   X 表示 shell 名称的开头字母，例如 `B` 代表 Bourne，`K` 代表 Korn，`C` 代表 C shell，`P` 代表 Profile shell。

示例 7–4 为用户定制启动文件

在本例中，安全管理员为每个用户的起始目录配置文件。这些文件在任何用户登录之前已工作。这些文件位于用户的最小标签。在此站点中，用户的缺省 shell 是 C shell。

安全管理员在可信编辑器中创建具有以下内容的 .copy_files 文件和 .link_files 文件：

```
## .copy_files for regular users
## Copy these files to my home directory in every zone
.mailrc
.mozilla
.soffice
:wq

## .link_files for regular users with C shells
## Link these files to my home directory in every zone
.cshrc
.login
.Xdefaults
.Xdefaults-hostname
:wq

## .link_files for regular users with Korn shells
# Link these files to my home directory in every zone
.ksh
.profile
.Xdefaults
.Xdefaults-hostname
:wq
```

在 shell 初始化文件中，管理员确保用户的打印作业会传至有标签的打印机。

```
## .cshrc file
setenv PRINTER conf-printer1
setenv LPDEST  conf-printer1

## .ksh file
export PRINTER conf-printer1
export LPDEST  conf-printer1
```

管理员将修改 .Xdefaults-*home-directory-server* 文件来强制执行 dtterm 命令，以便将 .profile 文件作为新终端的源。

```
## Xdefaults-HDserver
Dtterm*LoginShell: true
```

将定制的文件复制到相应的框架目录中。

```
$ cp .copy_files .link_files .cshrc .login .profile \
.mailrc .Xdefaults .Xdefaults-home-directory-server \
/etc/skelC
$ cp .copy_files .link_files .ksh .profile \
.mailrc .Xdefaults .Xdefaults-home-directory-server \
/etc/skelK
```

故障排除 如果您在最低级别标签创建了一个 `.copy_files` 文件，然后登录到较高级别区域运行 `updatehome` 命令，且该命令失败并出现访问错误，请尝试以下操作：

- 确认您可以从较高级别的区域查看较低级别的目录。

```
higher-level zone# ls /zone/lower-level-zone/home/username
ACCESS ERROR: there are no files under that directory
```

- 如果您无法查看低级别目录，请在较高级别的区域中重新启动自动挂载服务：

```
higher-level zone# svcadm restart autofs
```

除非为主目录使用 NFS 挂载，否则较高级别区域中的自动挂载程序应从 `/zone/`*lower-level-zone*`/export/home/`*username* 回送挂载到 `/zone/`*lower-level-zone*`/home/`*username*。

▼ 如何在 Trusted Extensions 中登录到故障安全会话

在 Trusted Extensions 中，故障安全登录是受保护的。如果一般用户已定制了 shell 初始化文件但现在无法登录，您可以使用故障安全登录来修复用户的文件。

开始之前 您必须知道 `root` 口令。

1. **与在 Oracle Solaris OS 中一样，在登录屏幕上选择 "Options"（选项）–> "Failsafe Session"（故障安全会话）。**
2. **在出现提示时，让用户输入用户名和口令。**
3. **在提示输入 `root` 口令时，输入 `root` 的口令。**

   现在，您可以调试用户的初始化文件了。

使用 Solaris Management Console 管理用户和权限（任务列表）

在 Trusted Extensions 中，必须使用 Solaris Management Console 来管理用户、授权、权限和角色。要管理用户及其安全属性，请承担 "Security Administrator"（安全管理员）角色。下面的任务列表介绍了您为在有标签环境中工作的用户执行的常见任务。

任务	说明	参考
修改用户的标签范围。	修改用户可在其上工作的标签。这些修改可以收缩或扩展 `label_encodings` 文件允许的范围。	第 85 页中的 “如何在 Solaris Management Console 中修改用户的标签范围”

任务	说明	参考
创建权限配置文件以实现方便的授权。	有几种对一般用户可能很有用的授权。为有资格获得这些授权的用户创建配置文件。	第 86 页中的 “如何创建权限配置文件以实现方便的授权”
修改用户的缺省特权集。	从用户的缺省特权集中删除特权。	第 88 页中的 “如何收缩用户的特权集”
防止锁定特定用户的帐户。	可以承担角色的用户必须关闭帐户锁定。	第 90 页中的 “如何防止锁定用户帐户”
使用户能够重新为数据设置标签。	授予用户对信息进行降级或升级的权限。	第 90 页中的 “如何允许用户更改数据的安全级别”
从系统中删除用户。	完全删除用户及其进程。	第 91 页中的 “如何从 Trusted Extensions 系统删除用户帐户”
处理其他任务。	使用 Solaris Management Console 处理非特定于 Trusted Extensions 的任务。	第 92 页中的 “在 Solaris Management Console 中处理其他任务（任务列表）”

▼ 如何在 Solaris Management Console 中修改用户的标签范围

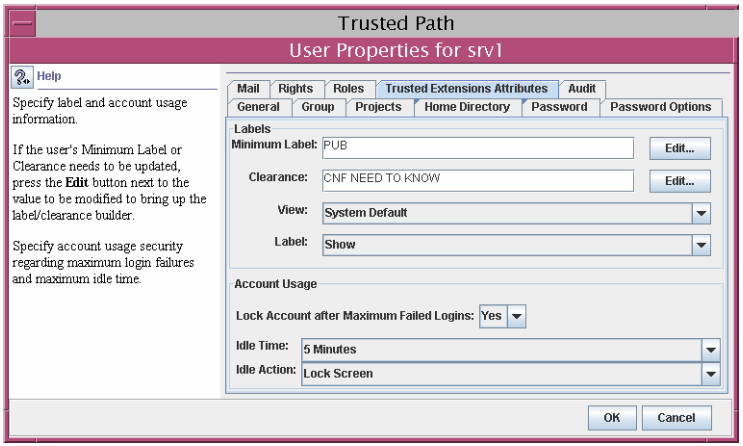
您可能想要扩展用户的标签范围来给予用户对管理应用程序的读取访问权。例如，可以登录到全局区域的用户随后可以运行 Solaris Management Console。该用户可以查看但不能更改内容。

另一方面，您也可能想要收缩用户的标签范围。例如，可以将来宾用户限制到一个标签中。

开始之前 您必须具有全局区域中的 "Security Administrator"（安全管理员）角色。

1. **在 Solaris Management Console 中打开一个 Trusted Extensions 工具箱。**
   请使用具有合适作用域的工具箱。有关详细信息，请参见《Trusted Extensions Configuration Guide》中的“Initialize the Solaris Management Console Server in Trusted Extensions”。
2. **在 "System Configuration"（系统配置）下，导航到 "User Accounts"（用户帐户）。**
   此时可能会显示口令提示符。
3. **键入角色的口令。**
4. **从 "User Accounts"（用户帐户）中选择单个用户。**

5 **单击 "Trusted Extensions Attributes"（Trusted Extensions 属性）选项卡。**



- **要扩展用户的标签范围，请选择一个更高级别的安全许可。**
  您也可以降低最小标签级别。
- **要将标签范围限制为一个标签，请使安全许可等于最小标签。**

6 **要保存更改，请单击 "OK"（确定）。**

▼ 如何创建权限配置文件以实现方便的授权

如果站点安全策略允许，您可能希望创建权限配置文件，该文件包含对可执行需要授权的任务的用户进行的授权。要使特定系统的每个用户得以授权，请参见第 80 页中的“如何修改 policy.conf 缺省值”。

开始之前 您必须具有全局区域中的 "Security Administrator"（安全管理员）角色。

1 **在 Solaris Management Console 中打开一个 Trusted Extensions 工具箱。**
请使用具有合适作用域的工具箱。有关详细信息，请参见《Trusted Extensions Configuration Guide》中的“Initialize the Solaris Management Console Server in Trusted Extensions”。

2 **在 "System Configuration"（系统配置）下，导航到 "Rights"（权限）。**
此时可能会显示口令提示符。

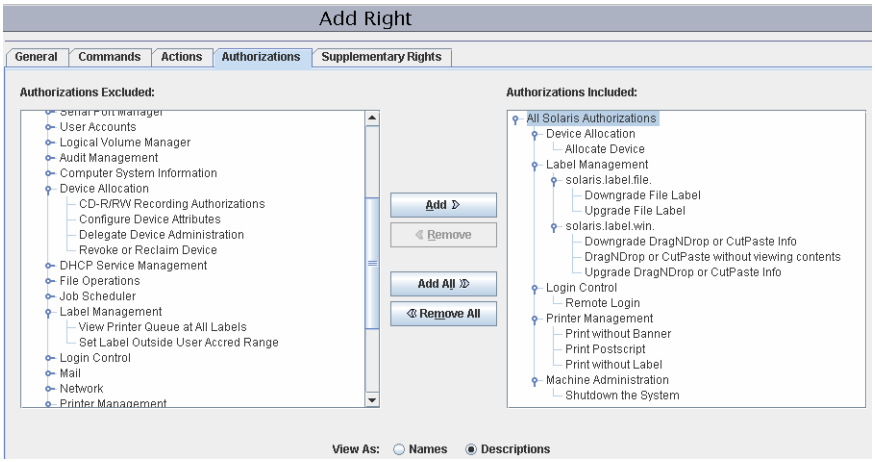
3 **键入角色的口令。**

4 **要添加权限配置文件，请单击 "Action"（操作）–> "Add Right"（添加权限）。**

5 **创建包含以下一种或多种授权的权限配置文件。**

有关逐步操作过程，请参见《System Administration Guide: Security Services》中的"How to Create or Change a Rights Profile"。

在下图中，"Authorizations Included"（包括的授权）窗口显示了可为用户提供方便的授权。



- "Allocate Device"（分配设备）—给予用户分配外围设备（例如麦克风）的授权。

  缺省情况下，Oracle Solaris 用户可以对 CD-ROM 进行读取和写入。不过，在 Trusted Extensions 中，只有可以分配设备的用户能够访问 CD-ROM 驱动器。分配供使用的驱动器需要授权。因此，要在 Trusted Extensions 中对 CD-ROM 进行读取和写入，用户需要 "Allocate Device"（分配设备）授权。
- "Downgrade DragNDrop or CutPaste Info"（降级 DragNDrop 或 CutPaste 信息）—授予用户从较高级别文件选择信息并将所选信息放到较低级别文件中的权限。
- "Downgrade File Label"（降级文件标签）—授予用户降低文件安全级别的权限
- "DragNDrop or CutPaste without viewing contents"（在不查看内容的情况下执行 DragNDrop 或 CutPaste）—授予用户在不查看所移动信息的情况下移动信息的权限。
- "Print Postscript"（打印 Postscript）—授予用户打印 PostScript 文件的权限。
- "Print without Banner"（无标题打印）—授予用户打印无标题页打印件的权限。
- "Print without Label"（无标签打印）—授予用户打印不显示标签的打印件的权限。
- "Remote Login"（远程登录）—授予用户远程登录的权限。
- "Shutdown the System"（关闭系统）—授予用户关闭系统和关闭区域的权限。
- "Upgrade DragNDrop or CutPaste Info"（升级 DragNDrop 或 CutPaste 信息）—授予用户从较低级别文件选择信息并将所选信息放到较高级别文件中的权限。
- "Upgrade File Label"（升级文件标签）—授予用户提高文件安全级别的权限。

6 **将权限配置文件指定给用户或角色。**

有关帮助信息，请参见联机帮助。有关逐步操作过程，请参见《System Administration Guide: Security Services》中的"How to Change the RBAC Properties of a User"。

示例 7–5 为角色指定与打印相关的授权

在下例中，安全管理员允许某个角色执行正文页中没有标签的打印作业。

在 Solaris Management Console 中，安全管理员导航到 "Administrative Roles"（管理性角色）。她查看特定角色中包括的权限配置文件，然后确保与打印相关的授权包含在角色的其中一个权限配置文件中。

▼ 如何收缩用户的特权集

站点安全策略可能要求授予用户的特权要少于缺省情况下指定给用户的特权。例如，在 Sun Ray 系统上使用 Trusted Extensions 的站点，您可能希望阻止用户查看 Sun Ray 服务器上其他用户的进程。

开始之前 您必须具有全局区域中的 "Security Administrator"（安全管理员）角色。

1 **在 Solaris Management Console 中打开一个 Trusted Extensions 工具箱。**

请使用具有合适作用域的工具箱。有关详细信息，请参见《Trusted Extensions Configuration Guide》中的"Initialize the Solaris Management Console Server in Trusted Extensions"。

2 **在 "System Configuration"（系统配置）下，导航到 "User Accounts"（用户帐户）。**

此时可能会显示口令提示符。

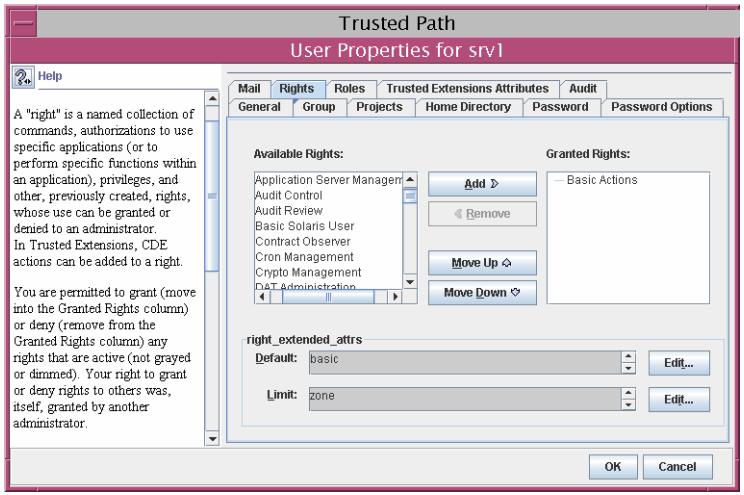
3 **键入角色的口令。**

4 **双击用户的图标。**

5 **删除 "basic"（基本）集中的一个或多个特权。**

a. **双击用户的图标。**

b. 单击 "Rights"（权限）选项卡。

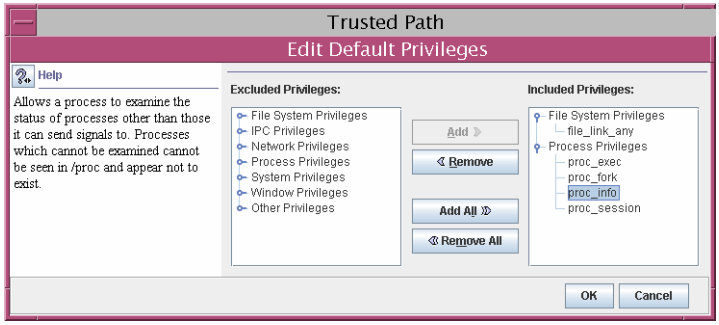


c. 单击 `right_extended_attrs` 字段中 "`basic`"（基本）集右边的 "Edit"（编辑）按钮。

d. 删除 `proc_session` 或 `file_link_any`。

通过删除 `proc_session` 特权，可以防止用户检查其当前会话以外的任何进程。通过删除 `file_link_any` 特权，可以防止用户生成指向不归其所有的文件的硬链接。

注意 – 请勿删除 `proc_fork` 或 `proc_exec` 特权。若没有这些特权，用户将无法使用系统。



6 要保存更改，请单击 "OK"（确定）。

▼ 如何防止锁定用户帐户

Trusted Extensions 扩展了 Solaris Management Console 中的用户安全功能，包括了帐户锁定。为可以承担角色的用户关闭帐户锁定。

开始之前 您必须具有全局区域中的 "Security Administrator"（安全管理员）角色。

1. **启动 Solaris Management Console。**
   请使用具有合适作用域的工具箱。有关详细信息，请参见《Trusted Extensions Configuration Guide》中的"Initialize the Solaris Management Console Server in Trusted Extensions"。
2. **在 "System Configuration"（系统配置）下，导航到 "User Accounts"（用户帐户）。**
   此时可能会显示口令提示符。
3. **键入角色的口令。**
4. **双击用户的图标。**
5. **单击 "Trusted Extensions Attributes"（Trusted Extensions 属性）选项卡。**
6. **在 "Account Usage"（帐户使用情况）会话中，从 "Lock account after maximum failed logins"（达到最大登录失败次数后锁定帐户）旁边的下拉菜单中选择 "No"（否）。**
7. **要保存更改，请单击 "OK"（确定）。**

▼ 如何允许用户更改数据的安全级别

可以授予一般用户或角色更改文件和目录的安全级别或标签的权限。除了具有授权外，该用户或角色还必须配置为以多个标签工作。而且，必须将有标签区域配置为允许重新设置标签。有关过程，请参见第 121 页中的 "如何使文件可以从有标签区域重新设置标签"。

注意 – 更改数据的安全级别是一个特权操作。此任务仅适用于值得信任的用户。

开始之前 您必须具有全局区域中的 "Security Administrator"（安全管理员）角色。

1. **按照第 86 页中的 "如何创建权限配置文件以实现方便的授权"过程创建权限配置文件。**

以下授权允许用户重新为文件设置标签：

- "Downgrade File Label"（降级文件标签）
- "Upgrade File Label"（升级文件标签）

以下授权允许用户重新为文件内信息设置标签：

- "Downgrade DragNDrop or CutPaste Info"（降级 DragNDrop 或 CutPaste 信息）
- "DragNDrop or CutPaste Info Without Viewing"（在不查看内容的情况下 DragNDrop 或 CutPaste 信息）
- "Upgrade DragNDrop or CutPaste Info"（升级 DragNDrop 或 CutPaste 信息）

2 **使用 Solaris Management Console 将配置文件指定给相应的用户和角色。**

有关帮助信息，请使用联机帮助。有关逐步操作过程，请参见《System Administration Guide: Security Services》中的"How to Change the RBAC Properties of a User"。

▼ 如何从 Trusted Extensions 系统删除用户帐户

从系统删除用户时，必须确保同时删除用户的起始目录以及用户拥有的所有对象。作为删除用户拥有的对象的替代方法，您可以将这些对象的所有权变更到一个有效用户。

您还必须确保删除与该用户关联的所有批处理作业。系统上不能保留任何属于已删除用户的对象或进程。

开始之前 您必须具有 "Security Administrator"（安全管理员）角色。

1 **归档用户在每个标签的起始目录。**

2 **归档用户在每个标签的邮件文件。**

3 **在 Solaris Management Console 中删除用户帐户。**

a. **在 Solaris Management Console 中打开一个 Trusted Extensions 工具箱。**

请使用具有合适作用域的工具箱。有关详细信息，请参见《Trusted Extensions Configuration Guide》中的"Initialize the Solaris Management Console Server in Trusted Extensions"。

b. **在 "System Configuration"（系统配置）下，导航到 "User Accounts"（用户帐户）。**

此时可能会显示口令提示符。

c. **键入角色的口令。**

d. **选择要删除的用户帐户，然后单击 "Delete"（删除）按钮。**

   系统将提示您删除用户的起始目录和邮件文件。当您接受提示后，仅会删除用户在全局区域中的起始目录和邮件文件。

4 **在每个有标签区域中，手动删除用户的目录和邮件文件。**

注 – 您应当负责查找和删除用户在所有标签的临时文件，例如 `/tmp` 目录中的文件。

在 Solaris Management Console 中处理其他任务（任务列表）

按照 Oracle Solaris 过程在 Solaris Management Console 中处理任务。您必须是超级用户或承担全局区域中的某个角色。下面的任务列表指出了基本的 Solaris Management Console 任务。

任务	参考
使用 Solaris Management Console 执行管理任务。	《Oracle Solaris 管理：基本管理》中的第 2 章 “使用 Solaris Management Console（任务）”
创建用户。	《Oracle Solaris 管理：基本管理》中的“使用 RBAC 和 Solaris 管理工具（任务列表）”
创建角色。	《System Administration Guide: Security Services》中的“How to Create and Assign a Role by Using the GUI”
修改角色。	《System Administration Guide: Security Services》中的“How to Change the Properties of a Role”
创建或修改权限配置文件。	《System Administration Guide: Security Services》中的“How to Create or Change a Rights Profile”
更改用户的其他安全属性。	《System Administration Guide: Security Services》中的“How to Change the RBAC Properties of a User”
审计角色的操作。	《System Administration Guide: Security Services》中的“How to Audit Roles”
使用 `smprofile list -D` *name-service-type*`:/`*server-name*`/` *domain-name* 列出权限配置文件	《System Administration Guide: Security Services》中的第 9 章 “Using Role-Based Access Control (Tasks)”或 `smprofile`(1M) 手册页

◆ ◆ ◆ 第 8 章

Trusted Extensions 中的远程管理（任务）

本章介绍了如何使用 Trusted Extensions 管理工具来管理远程系统。

Trusted Extensions 中的安全远程管理

缺省情况下，Trusted Extensions 不允许远程管理。如果不可信的远程系统上的用户可以管理配有 Trusted Extensions 的系统，则远程管理将存在重大的安全风险。因此，初始安装的系统上没有启用远程管理选项。

直到配置网络时，才向所有远程主机指定 `admin_low` 安全模板。因此，任何连接都不使用或接受 CIPSO 协议。在该初始状态下，由多种机制来保护系统免受远程攻击。这些机制包括 `netservices` 设置、缺省登录策略和 PAM 策略。

- 将 `netservices` 服务管理工具 (Service Management Facility, SMF) 配置文件设置为 `limited` 时，除了安全 shell 外，不会启用任何远程服务。但是，因登录策略和 PAM 策略的原因，`ssh` 服务不能用于远程登录。
- `root` 帐户不能用于远程登录，因为 `/etc/default/login` 文件中 `CONSOLE` 的缺省策略阻止使用 `root` 帐户进行远程登录。
- 两种 PAM 设置也影响远程登录。

  `pam_roles` 模块始终拒绝 `role` 类型的帐户的本地登录。缺省情况下，该模块也拒绝远程登录。但是，可以通过在系统的 `pam.conf` 条目中指定 `allow_remote` 来将系统配置为接受远程登录。

  此外，`pam_tsol_account` 模块拒绝远程登录到全局区域，除非使用 CIPSO 协议。该策略的目的是由另一个 Trusted Extensions 系统执行远程管理。

要启用远程登录功能，两个系统都必须将其对等方指定给一个 CIPSO 安全模板。如果该方法不可行，可以通过在 pam.conf 文件中指定 allow_unlabeled 选项来放宽网络协议策略。如果放宽了这两个策略中的任意一个，则必须更改缺省网络模板以便使任意计算机都无法访问全局区域。应尽量少用 admin_low 模板，且应该修改 tnrhdb 数据库以便使通配符地址 0.0.0.0 不缺省设置为 ADMIN_LOW 标签。有关详细信息，请参见第 95 页中的 “远程管理 Trusted Extensions（任务列表）”和第 164 页中的 “如何限定可能会在可信网络上联系的主机”。

Trusted Extensions 中用于管理远程系统的方法

通常，管理员使用 rlogin 和 ssh 命令从命令行管理远程系统。也可以使用 Solaris Management Console。在 Trusted CDE 中，dtappsession 程序可以远程启动 Trusted CDE 操作。从 Solaris 10 5/09 发行版开始，用户可以使用虚拟网络计算机 (Virtual Networking Computer, VNC) 远程显示多级别桌面。

下面是在 Trusted Extensions 中可以使用的远程管理方法：

- root 用户可以从终端登录到远程主机。请参见第 96 页中的 “如何在 Trusted Extensions 中从命令行远程登录”。此方法的工作方式与其在 Oracle Solaris 系统上的工作方式相同。此方法不安全。
- 角色可以从角色工作区中的终端登录到远程主机。请参见第 96 页中的 “如何在 Trusted Extensions 中从命令行远程登录”。
- 管理员可以启动远程系统上运行的 Solaris Management Console 服务器。请参见第 98 页中的 “如何从 Trusted Extensions 系统使用 Solaris Management Console 来远程管理系统”。
- 可以使用 dtappsession 命令远程启动 "Trusted_Extensions" 文件夹中的操作。请参见第 97 页中的 “如何使用 dtappsession 来远程管理 Trusted Extensions”。
- 用户可以通过使用 VNC 客户机程序连接到 Trusted Extensions 系统上的 Xvnc 服务器来登录远程的多级别桌面。请参见第 102 页中的 “如何使用 Xvnc 远程访问 Trusted Extensions 系统”。

在 Trusted Extensions 中通过角色进行的远程登录

与在 Oracle Solaris OS 中一样，必须在每个主机上对 /etc/default/login 文件中的一个设置进行更改以允许远程登录。此外，可能还需要更改 pam.conf 文件。在 Trusted Extensions 中，安全管理员负责进行更改。有关过程，请参见《Trusted Extensions Configuration Guide》中的“Enable Remote Login by root User in Trusted Extensions”和《Trusted Extensions Configuration Guide》中的“Enable Remote Login by a Role in Trusted Extensions”。

在 Trusted Extensions 和 Oracle Solaris 主机上，远程登录可能需要（也可能不需要）授权。第 95 页中的 “Trusted Extensions 中的远程登录管理”介绍了需要授权的登录的情况和类型。缺省情况下，角色具有 "Remote Login"（远程登录）授权。

从无标签主机进行的基于角色的远程管理

在 Trusted Extensions 中，用户通过 "Trusted Path"（可信路径）菜单承担角色。然后，角色在可信的工作区中运行。缺省情况下，无法从可信路径以外的路径承担角色。如果站点策略允许，安全管理员可以更改缺省策略。然后，运行 Solaris Management Console 2.1 客户机软件的无标签主机的管理员可以管理可信的主机。

- 要更改缺省策略，请参见《Trusted Extensions Configuration Guide》中的“Enable Remote Login by a Role in Trusted Extensions”。
- 要远程管理系统，请参见第 96 页中的 “如何在 Trusted Extensions 中从命令行远程登录”。

只有远程无标签系统上的用户在 Trusted Extensions 主机上具有用户帐户时才应执行该策略更改。该 Trusted Extensions 用户必须能够承担管理角色。然后，该角色可以使用 Solaris Management Console 来管理远程系统。

注意 – 如果启用了从非 Trusted Extensions 主机进行的远程管理，则管理环境的受保护程度将低于 Trusted Extensions 管理工作区。键入口令和其他安全数据时请务必谨慎。作为预防措施，请先关闭所有不可信的应用程序，然后再启动 Solaris Management Console。

Trusted Extensions 中的远程登录管理

两个 Trusted Extensions 主机之间的远程登录被视为当前登录会话的扩展。

`rlogin` 命令不提示输入口令时不需要授权。如果远程主机上的用户起始目录中的 `/etc/hosts.equiv` 文件或 `.rhosts` 文件列出了用户名或正在尝试从其中进行远程登录的主机，则不需要口令。有关更多信息，请参见 `rhosts(4)` 和 `rlogin(1)` 手册页。

对于所有其他远程登录，包括通过 `ftp` 命令进行的登录，都需要 "Remote Login"（远程登录）授权。

要创建包含 "Remote Login"（远程登录）授权的权限配置文件，请参见第 84 页中的 “使用 Solaris Management Console 管理用户和权限（任务列表）”。

远程管理 Trusted Extensions（任务列表）

下面的任务列表描述了用于管理远程 Trusted Extensions 系统的任务。

任务	说明	参考
使 root 能够远程登录 Trusted Extensions 系统。	使 root 用户能够从有标签系统远程工作。	《Trusted Extensions Configuration Guide》中的“Enable Remote Login by root User in Trusted Extensions”
使某个角色能够远程登录 Trusted Extensions 系统。	允许所有角色从有标签系统进行远程工作。	《Trusted Extensions Configuration Guide》中的“Enable Remote Login by a Role in Trusted Extensions”
启用从无标签系统到 Trusted Extensions 系统的远程登录。	允许任何用户或角色从无标签系统远程工作。	《Trusted Extensions Configuration Guide》中的“Enable Remote Login From an Unlabeled System”
远程登录 Trusted Extensions 系统。	作为一个角色登录 Trusted Extensions 系统。	第 96 页中的 “如何在 Trusted Extensions 中从命令行远程登录”
远程地管理系统。	使用 dtappsession 命令通过 Trusted_Extensions 操作来管理远程系统。	第 97 页中的 “如何使用 dtappsession 来远程管理 Trusted Extensions”
	从 Trusted Extensions 系统中，使用 Solaris Management Console 管理远程主机。	第 98 页中的 “如何从 Trusted Extensions 系统使用 Solaris Management Console 来远程管理系统”
	从有标签系统中，使用 Solaris Management Console 管理远程 Trusted Extensions 主机。	第 99 页中的 “如何从无标签系统使用 Solaris Management Console 来远程管理系统”
管理和使用远程系统	从任何客户机，使用远程 Trusted Extensions 上的 Xvnc 服务器将多级别会话回显到客户机	第 102 页中的 “如何使用 Xvnc 远程访问 Trusted Extensions 系统”
使特定用户能够登录到全局区域。	使用 Solaris Management Console 中的用户和网络工具来使特定用户能够访问全局区域。	第 101 页中的 “在 Trusted Extensions 中如何使特定用户能够远程登录到全局区域”

▼ 如何在 Trusted Extensions 中从命令行远程登录

注 – telnet 命令不能用于远程角色承担，因为此命令不能将主标识和角色标识传递给 pam_roles 模块。

开始之前 用户和角色在本地和远程系统上必须具有相同的定义。

角色必须具有 "Remote Login"（远程登录）授权。缺省情况下，该授权在 "Remote Administration"（远程管理）和 "Maintenance"（维护）以及 "Repair"（修复）权限配置文件中。

安全管理员已经在每个可远程管理的系统上完成了《Trusted Extensions Configuration Guide》中的“Enable Remote Login by a Role in Trusted Extensions”过程。如果可使用无标签系统来管理该系统，则还必须已完成《Trusted Extensions Configuration Guide》中的“Enable Remote Login From an Unlabeled System”过程。

- **从可承担某个角色的用户的工作区中，登录到远程主机。**

  使用 `rlogin` 命令、`ssh` 命令或 `ftp` 命令。

  - 如果使用 `rlogin -l` 或 `ssh` 命令进行登录，则角色的权限配置文件中的所有命令都可用。
  - 如果使用 `ftp` 命令，请参见 `ftp(1)` 手册页以了解可用的命令。

▼ 如何使用 dtappsession 来远程管理 Trusted Extensions

使用 `dtappsession` 程序，管理员可以管理运行 CDE 的远程系统。

当远程系统没有监视器时，`dtappsession` 非常有用。例如，`dtappsession` 经常用于管理大型服务器上的域。有关更多信息，请参见 `dtappsession(1)` 手册页。

开始之前 在有标签系统上，您必须是全局区域中的管理角色。在无标签系统上，您必须承担远程系统上定义的某个角色。然后，您必须从角色的配置文件 shell 运行远程登录。

1. **可选创建一个专用于远程会话的工作区。**

   为避免在远程 CDE 应用程序和本地应用程序之间造成混淆，可以将一个管理角色工作区专用于该过程。有关详细信息，请参见《Trusted Extensions User's Guide》中的“How to Add a Workspace at a Particular Label”。

2. **登录到远程主机。**

   可以使用 `rlogin` 命令或 `ssh` 命令。

   ```
   $ ssh remote-host
   ```

3. **启动远程管理。**

   在终端窗口中，键入 `dtappsession` 命令，后跟本地主机的名称。

   ```
   $ /usr/dt/bin/dtappsession local-host
   ```

   远程主机上运行的 "Application Manager"（应用程序管理器）将显示在本地主机上。同时，还会出现一个 "Exit"（退出）对话框。

4. **管理远程主机。**

   如果您是从 Trusted CDE 中调用了远程会话，则可以使用 "Trusted_Extensions" 文件夹中的操作。

5 **完成后，单击 "Exit"（退出）按钮。**

注意 – 关闭 "Application Manager"（应用程序管理器）不会结束登录会话，因此建议不要采用此操作。

6 **在终端窗口中，退出远程登录会话。**

使用 `hostname` 命令验证您位于本地主机上。

```
$ exit
$ hostname
local-host
```

▼ 如何从 Trusted Extensions 系统使用 Solaris Management Console 来远程管理系统

Solaris Management Console 提供了用来管理用户、权限、角色和网络的远程管理界面。您需要承担某个角色以使用控制台。在此过程中，您在本地系统上运行此控制台并将远程系统指定为服务器。

开始之前 您已完成以下过程：

- 在两个系统上—《Trusted Extensions Configuration Guide》中的“Initialize the Solaris Management Console Server in Trusted Extensions”
- 在远程系统上—《Trusted Extensions Configuration Guide》中的“Enable Remote Login by a Role in Trusted Extensions”和《Trusted Extensions Configuration Guide》中的“Enable the Solaris Management Console to Accept Network Communications”
- 在作为 LDAP 服务器的远程系统上—《Trusted Extensions Configuration Guide》中的“Configuring the Solaris Management Console for LDAP (Task Map)”

1 **在本地系统上，以与在远程系统上具有相同定义的用户身份登录。**

2 **承担您计划用来管理系统的角色。**

3 **以该角色的身份启动 Solaris Management Console。**

有关详细信息，请参见《Trusted Extensions Configuration Guide》中的“Initialize the Solaris Management Console Server in Trusted Extensions”。

a. **在 "Server"（服务器）对话框中，键入远程服务器的名称。**

- **如果您使用 LDAP 作为命名服务，请键入 LDAP 服务器的名称。**
  然后，选择下列作用域之一。
  - **要管理命名服务中的数据库，请选择 `Scope=LDAP` 工具箱。**
    本计算机（*ldap-server*: `Scope=LDAP, Policy=TSOL`）
  - **要管理 LDAP 服务器上的本地文件，请选择 `Scope=Files` 工具箱。**
    本计算机（*ldap-server*: `Scope=Files, Policy=TSOL`）
- **如果您没有使用 LDAP 作为命名服务，请键入要管理的远程系统的名称。**
  然后，选择 `Scope=Files` 工具箱。
  本计算机（*remote-system*: `Scope=Files, Policy=TSOL`）

4 **在 "System Configuration"（系统配置）下选择一个工具。**

当您选定某个工具（例如 "User"（用户））时，对话框将显示 Solaris Management Console 服务器名称、您的用户名、您的角色名和一个用于键入角色口令的位置。请确保各项正确无误。

5 **以在本地和远程系统上具有相同定义的角色身份登录到 Solaris Management Console 服务器。**

键入角色的口令并按 "Login as Role"（以角色身份登录）。现在您即可以使用 Solaris Management Console 来管理系统。

注 – 虽然可以使用 Solaris Management Console 来运行 `dtappsession`，但使用 `dtappsession` 的最简单方法是第 97 页中的 “如何使用 `dtappsession` 来远程管理 Trusted Extensions”中介绍的方法。

▼ 如何从无标签系统使用 Solaris Management Console 来远程管理系统

在此过程中，您在远程系统上运行 Solaris Management Console 客户机和服务器，并在本地系统上显示控制台。

开始之前 Trusted Extensions 系统必须已将标签 `ADMIN_LOW` 指定给本地系统。

注 – 从 Trusted Extensions 系统的角度来看，未运行 CIPSO 协议的系统（如 Trusted Solaris 系统）是无标签系统。

必须将远程系统上的 Solaris Management Console 服务器配置为接受远程连接。有关过程，请参见《Trusted Extensions Configuration Guide》中的“Enable the Solaris Management Console to Accept Network Communications”。

两个系统都必须具有已指定可使用 Solaris Management Console 的同一角色的相同用户。该用户可以具有常规用户的标签范围，但该角色必须具有从 ADMIN_LOW 到 ADMIN_HIGH 的范围。

您必须是全局区域中的管理角色。

1 使本地 X Server 能够显示远程 Solaris Management Console。

```
# xhost + TX-SMC-Server
# echo $DISPLAY
:n.n
```

2 在本地系统上，成为可承担 Solaris Management Console 的某个角色的用户。

```
# su - same-username-on-both-systems
```

3 以该用户的角色身份登录到远程服务器。

```
$ rlogin -l same-rolename-on-both-systems TX-SMC-Server
```

4 确保 Solaris Management Console 使用的环境变量值正确。

a. 设置 DISPLAY 变量的值。

```
$ DISPLAY=local:n.n
$ export DISPLAY=local:n.n
```

b. 将 LOGNAME 变量的值设置为用户名。

```
$ LOGNAME=same-username-on-both-systems
$ export LOGNAME=same-username-on-both-systems
```

c. 将 USER 变量的值设置为角色名。

```
$ USER=same-rolename-on-both-systems
$ export USER=same-rolename-on-both-systems
```

5 以角色身份从命令行启动 Solaris Management Console。

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

6 **在 "System Configuration"（系统配置）下选择一个工具。**

当您选定某个工具（例如 "User"（用户））时，对话框将显示 Solaris Management Console 服务器名称、您的用户名、您的角色名和一个用于键入角色口令的位置。请确保各项正确无误。

7 **以角色身份登录到服务器。**

键入角色的口令并按 "Login as Role"（以角色身份登录）。现在您即可以使用 Solaris Management Console 来管理系统。

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.
```

▼ 在 Trusted Extensions 中如何使特定用户能够远程登录到全局区域

对用户的缺省标签范围和区域的缺省行为进行更改以启用以非角色身份进行的远程登录。您可能希望为使用远程有标签系统的测试者完成此过程。出于安全原因，测试者的系统应当运行与其他用户没有交集的标签。

开始之前 您必须有充足的理由证明该用户需要登录到全局区域。

您必须具有全局区域中的 "Security Administrator"（安全管理员）角色。

1 **要使特定用户能够登录到全局区域，请为这些用户指定管理标签范围。**

使用 Solaris Management Console 将安全许可 `ADMIN_HIGH` 和最小标签 `ADMIN_LOW` 指定给各个用户。有关详细信息，请参见第 85 页中的 “如何在 Solaris Management Console 中修改用户的标签范围”。

用户的有标签区域必须也允许登录。

2 **要启用从有标签区域到全局区域的远程登录，请执行以下操作：**

a. **向全局区域添加一个用于远程登录的多级别端口。**

使用 Solaris Management Console。基于 TCP 协议的端口 513 启用远程登录。有关示例，请参见第 123 页中的 “如何为区域创建多级别端口”。

b. 将 tnzonecfg 更改读入内核。

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

c. 重新启动远程登录服务。

```
# svcadm restart svc:/network/login:rlogin
```

▼ 如何使用 Xvnc 远程访问 Trusted Extensions 系统

虚拟网络计算 (Virtual Network Computing, VNC) 技术将客户机连接到远程服务器，然后在客户机的窗口中显示远程服务器的桌面。Xvnc 是 UNIX 版的 VNC，它基于标准的 X Server。在 Trusted Extensions 中，任何平台上的客户机都可以连接到运行 Trusted Extensions 软件的 Xvnc，登录到 Xvnc 服务器，然后显示多级别桌面并在其上工作。

开始之前 您已在将要用作 Xvnc 服务器的系统上安装并配置了 Trusted Extensions 软件。您已经创建并引导了有标签区域。Xvnc 服务器通过主机名或 IP 地址识别 VNC 客户机。

您在将用作 Xvnc 服务器的系统的全局区域中是超级用户。

1 配置 Xvnc 服务器。

有关更多信息，请参见 Xvnc(1) 和 vncconfig(1)手册页。

注意 – 如果您运行的是 Solaris 10 10/08 或 Solaris 10 5/08 发行版，则在配置服务器之前必须先修补您的系统。对于 SPARC 系统，请安装最新版本的修补程序 125719。对于 x86 系统，请安装最新版本的修补程序 125720。

a. 创建 Xservers 配置目录。

```
# mkdir -p /etc/dt/config
```

b. 将 /usr/dt/config/Xservers 文件复制到 /etc/dt/config 目录。

```
# cp /usr/dt/config/Xservers /etc/dt/config/Xservers
```

c. 编辑 /etc/dt/config/Xservers 文件以启动 Xvnc 程序，而不是 Xserver 或 Xorg。

在本例中，该条目被配置为无需口令即可登录服务器。要成功登录桌面，本地 UID 必须是 none，而不是 console。

在示例中，为便于显示，对条目进行了拆分。该条目必须在一个行上。

```
#   :0  Local local_uid@console root /usr/X11/bin/Xserver :0 -nobanner
  :0  Local local_uid@none root /usr/X11/bin/Xvnc :0 -nobanner
  -AlwaysShared -SecurityTypes None -geometry 1024x768x24 -depth 24
```

注 – 更安全的配置是通过使用 `-SecurityTypes VncAuth` 参数来要求输入口令。`Xvnc(1)` 手册页介绍了口令要求。

d. 重新引导服务器或启动 Xvnc 服务器。

```
# reboot
```

重新引导后，验证 Xvnc 程序是否正在运行。

```
# ps -ef | grep Xvnc
  root  2145  932  0  Jan 18 ?  6:15 /usr/X11/bin/Xvnc :0 -nobanner
  -AlwaysShared -SecurityTypes None -geometry 1024
```

2 在 Trusted Extensions Xvnc 服务器的每个 VNC 客户机上，安装 VNC 客户机软件。

对于客户机系统，您可以选择使用哪种软件。本例中使用了 Sun VNC 软件。

```
# cd SUNW-pkg-directory
# pkgadd -d . SUNWvncviewer
```

3 在 VNC 客户机上的终端窗口中，连接到服务器。

```
% /usr/bin/vncviewer Xvnc-server-hostname
```

4 在所显示的窗口中，键入您的用户名和口令。

继续执行登录过程。有关其余步骤的说明，请参见《Trusted Extensions User's Guide》中的“Logging In to Trusted Extensions”。

如果是以超级用户身份登录到服务器，则您可以立即管理服务器。如果是以用户身份登录到服务器，则您必须承担某个角色才能管理系统。

◆ ◆ ◆ 第 9 章

9 Trusted Extensions 和 LDAP（概述）

本章描述了如何针对配置有 Trusted Extensions 的系统使用 Oracle Directory Server Enterprise Edition（目录服务器）。

在 Trusted Extensions 中使用命名服务

为了在具有多个 Trusted Extensions 系统的一个安全域内实现用户、主机和网络属性的一致性，需使用一个命名服务来分发大多数配置信息。LDAP 是一个命名服务示例。`nsswitch.conf` 文件确定了将使用哪种命名服务。LDAP 是推荐用于 Trusted Extensions 的命名服务。

Directory Server 可以为 Trusted Extensions 和 Oracle Solaris 客户机提供 LDAP 命名服务。该服务器必须包含 Trusted Extensions 网络数据库，并且 Trusted Extensions 客户机必须通过一个多级别端口连接到服务器。安全管理员在配置 Trusted Extensions 时指定多级别端口。

Trusted Extensions 将两个可信网络数据库添加到 LDAP 服务器：`tnrhdb` 和 `tnrhtp`。这些数据库是使用 Solaris Management Console 中的 "Security Templates"（安全模板）工具管理的。`Scope=LDAP, Policy=TSOL` 的一个工具箱将配置更改存储在 Directory Server 上。

- 有关在 Oracle Solaris OS 中使用 LDAP 命名服务的信息，请参见《系统管理指南：名称和目录服务（DNS、NIS 和 LDAP）》。
- 《Trusted Extensions Configuration Guide》中介绍了如何为 Trusted Extensions 客户机设置 Directory Server。通过使用配置有 Trusted Extensions 的 LDAP 代理服务器，可以使 Trusted Extensions 系统成为 Oracle Solaris LDAP 服务器的客户机。

注 – 配置有 Trusted Extensions 的系统不能成为 NIS 或 NIS+ 主机的客户机。

未联网的 Trusted Extensions 系统

如果站点上没有使用命名服务，则管理员必须确保用户、主机和网络的配置信息在所有主机上均相同。如果在一个主机上做了某个更改，则在所有主机上必须做相同的更改。

在未联网的 Trusted Extensions 系统上，配置信息是在 `/etc`、`/etc/security` 和 `/etc/security/tsol` 目录中维护的。您可以使用 "Trusted_Extensions" 文件夹中的操作来修改某些配置信息。可以使用 Solaris Management Console 中的 "Security Templates"（安全模板）工具来修改网络数据库参数。用户、角色和权限是在 "User Accounts"（用户帐户）、"Administrative Roles"（管理角色）和 "Rights"（权限）工具中修改的。`Scope=Files, Policy=TSOL` 的 "This Computer"（本计算机）上的一个工具箱在本地存储配置更改。

Trusted Extensions LDAP 数据库

Trusted Extensions 扩展了 Directory Server 的模式来容纳 `tnrhdb` 和 `tnrhtp` 数据库。Trusted Extensions 定义了两个新属性（`ipTnetNumber` 和 `ipTnetTemplateName`），以及两个新的对象类（`ipTnetTemplate` 和 `ipTnetHost`）。

属性定义如下所示：

```
ipTnetNumber
   ( 1.3.6.1.1.1.1.34 NAME 'ipTnetNumber'
     DESC 'Trusted network host or subnet address'
     EQUALITY caseExactIA5Match
     SYNTAX 1.3.6.1.4.1.1466.115.121.1.26
     SINGLE-VALUE )

ipTnetTemplateName
   ( 1.3.6.1.1.1.1.35 NAME 'ipTnetTemplateName'
     DESC 'Trusted network template name'
     EQUALITY caseExactIA5Match
     SYNTAX 1.3.6.1.4.1.1466.115.121.1.26
     SINGLE-VALUE )
```

对象类定义如下所示：

```
ipTnetTemplate
   ( 1.3.6.1.1.1.2.18 NAME 'ipTnetTemplate' SUP top STRUCTURAL
     DESC 'Object class for Trusted network host templates'
     MUST ( ipTnetTemplateName )
     MAY ( SolarisAttrKeyValue ) )
```

```
ipTnetHost
   ( 1.3.6.1.1.1.2.19 NAME 'ipTnetHost' SUP top AUXILIARY
     DESC 'Object class for Trusted network host/subnet address
           to template mapping'
     MUST ( ipTnetNumber $ ipTnetTemplateName ) )
```

LDAP 中的 cipso 模板定义类似于以下内容：

```
ou=ipTnet,dc=example,dc=example1,dc=exampleco,dc=com
 objectClass=top
 objectClass=organizationalUnit
 ou=ipTnet

 ipTnetTemplateName=cipso,ou=ipTnet,dc=example,dc=example1,dc=exampleco,dc=com
 objectClass=top
 objectClass=ipTnetTemplate
 ipTnetTemplateName=cipso
 SolarisAttrKeyValue=host_type=cipso;doi=1;min_sl=ADMIN_LOW;max_sl=ADMIN_HIGH;

 ipTnetNumber=0.0.0.0,ou=ipTnet,dc=example,dc=example1,dc=exampleco,dc=com
 objectClass=top
 objectClass=ipTnetTemplate
 objectClass=ipTnetHost
 ipTnetNumber=0.0.0.0
 ipTnetTemplateName=internal
```

在 Trusted Extensions 中使用 LDAP 命名服务

在 Trusted Extensions 中管理 LDAP 命名服务的方法与在 Oracle Solaris OS 中管理 LDAP 命名服务的方法相同。下面是实用命令的示例，同时指出了包含更详细信息的参考资料：

- 有关解决 LDAP 配置问题的策略，请参阅《System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)》中的第 13 章 “LDAP Troubleshooting (Reference)”。
- 要对受标签影响的客户机到服务器 LDAP 连接问题进行故障排除，请参见第 177 页中的 “如何调试客户机与 LDAP 服务器的连接”。
- 要对其他客户机到服务器 LDAP 连接问题进行故障排除，请参见《System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)》中的第 13 章 “LDAP Troubleshooting (Reference)”。
- 要显示来自 LDAP 客户机的 LDAP 条目，请键入：

  ```
  $ ldaplist -l
  $ ldap_cachemgr -g
  ```
- 要显示来自 LDAP 服务器的 LDAP 条目，请键入：

  ```
  $ ldap_cachemgr -g
  $ idsconfig -v
  ```
- 要列出 LDAP 管理的主机，请键入：

```
$ ldaplist -l hosts      Long listing
$ ldaplist hosts         One-line listing
```

- 要列出 LDAP 上的目录信息树 (Directory Information Tree, DIT) 中的信息，请键入：

```
$ ldaplist -l services | more
dn: cn=apocd+ipServiceProtocol=udp,ou=Services,dc=exampleco,dc=com
  objectClass: ipService
  objectClass: top
  cn: apocd
  ipServicePort: 38900
  ipServiceProtocol: udp

...
$ ldaplist services name
dn=cn=name+ipServiceProtocol=udp,ou=Services,dc=exampleco,dc=com
```

- 要显示客户机上的 LDAP 服务的状态，请键入：

```
# svcs -xv network/ldap/client
svc:/network/ldap/client:default (LDAP client)
 State: online since date
   See: man -M /usr/share/man -s 1M ldap_cachemgr
   See: /var/svc/log/network-ldap-client:default.log
Impact: None.
```

- 要启动和停止 LDAP 客户机，请键入：

```
# svcadm enable network/ldap/client

# svcadm disable network/ldap/client
```

- 要在 Oracle Directory Server Enterprise Edition 软件 5.2 版中启动和停止 LDAP 服务器，请键入：

```
# installation-directory/slap-LDAP-server-hostname/start-slapd
# installation-directory/slap-LDAP-server-hostname/stop-slapd
```

- 要在 Oracle Directory Server Enterprise Edition 软件 6 版中启动和停止 LDAP 服务器，请键入：

```
# dsadm start /export/home/ds/instances/your-instance
# dsadm stop /export/home/ds/instances/your-instance
```

- 要在 Oracle Directory Server Enterprise Edition 软件 6 版中启动和停止代理 LDAP 服务器，请键入：

```
# dpadm start /export/home/ds/instances/your-instance
# dpadm stop /export/home/ds/instances/your-instance
```

◆ ◆ ◆ 第 10 章

10 在 Trusted Extensions 中管理区域（任务）

本章介绍了非全局区域在配置有 Trusted Extensions 的系统上的工作原理。同时还包括 Trusted Extensions 中区域特有的操作过程。

Trusted Extensions 中的区域

正确配置的 Trusted Extensions 系统包括一个作为操作系统实例的全局区域，以及有一个或多个标签的非全局区域。配置期间，Trusted Extensions 为每个区域附加一个唯一标签，这样就创建了有标签区域。这些标签来自 `label_encodings` 文件。管理员可以为每个标签创建一个区域，但系统对此不作要求。系统上具有的标签可能会比有标签区域要多。有标签区域不可能多于标签。

在 Trusted Extensions 系统上，区域的文件系统通常作为回送文件系统 (loopback file system, lofs) 挂载。有标签区域中的所有可写文件和目录都处于该区域的标签级别。缺省情况下，用户可以查看比用户当前标签级别低的某个标签的区域中的文件。通过该配置，用户可以在比当前工作区标签级别低的标签查看其起始目录。尽管用户可以查看较低级别标签的文件，但不能修改它们。用户只能从与文件具有相同标签的进程修改该文件。

在 Trusted Extensions 中，全局区域是管理区域。有标签区域针对一般用户。区域的标签在用户的认可范围内时用户可以在该区域中工作。

每个区域都有关联的 IP 地址以及安全属性。区域可以配置为多级别端口 (MLP)。此外，区域还可以配置有 Internet 控制信息协议 (Internet Control Message Protocol, ICMP) 广播策略，例如 `ping`。

有关从有标签区域共享目录以及从有标签区域远程挂载目录的信息，请参见 第 11 章，在 Trusted Extensions 中管理和挂载文件（任务）。

Trusted Extensions 中的区域构建于 Oracle Solaris 区域产品之上。有关详细信息，请参见《System Administration Guide: Oracle Solaris Containers-Resource Management and Oracle Solaris Zones》中的第 II 部分, “Zones”。特别注意的是，修补和软件包安装问题会影响 Trusted Extensions。有关详细信息，请参见《System Administration Guide: Oracle Solaris Containers-Resource Management and Oracle Solaris Zones》中的第 25 章 “About Packages and Patches on an Oracle Solaris System With Zones Installed (Overview)”和《System Administration Guide: Oracle Solaris Containers-Resource Management and Oracle Solaris Zones》中的第 30 章 “Troubleshooting Miscellaneous Oracle Solaris Zones Problems”。

Trusted Extensions 中的区域和 IP 地址

您的初始设置团队会为全局区域和有标签区域指定 IP 地址。《Trusted Extensions Configuration Guide》中的“Creating Labeled Zones”中说明了三种类型的配置：

- 系统针对全局区域和所有有标签区域具有一个 IP 地址。

  对于使用 DHCP 软件来获取其 IP 地址的系统，这种配置非常有用。如果没有用户要登录，LDAP 服务器可能会具有此配置。

- 系统具有一个用于全局区域的 IP 地址，以及一个由所有区域（包括全局区域）共享的 IP 地址。任何区域都可以具有唯一地址和共享地址组合。

  对于一般用户将会登录的系统，这种配置非常有用。它还可以用于打印机或 NFS 服务器。此配置可以节省 IP 地址。

- 系统有一个用于全局区域的 IP 地址，而且每个有标签区域都有一个唯一的 IP 地址。

  此配置适用于提供对单级别系统的单独物理网络的访问。通常，每个区域会在与其他有标签区域不同的物理网络上具有一个 IP 地址。由于此配置以单一 IP 实例实现，所以全局区域将控制物理接口并管理全局资源，例如路由表。

引入了非全局区域的专用 IP 实例后，在 Oracle Solaris OS 中可以采用第四种类型的配置：从 Solaris 10 8/07 发行版开始，非全局区域可以指定有自己的 IP 实例，并管理自己的物理接口。在此配置中，每个区域都以类似于独立系统的形式运行。有关说明，请参见《System Administration Guide: Oracle Solaris Containers-Resource Management and Oracle Solaris Zones》中的“Zone Network Interfaces”。

但是在这种配置下，每个有标签区域都以类似于独立的单一标记系统的形式运行。Trusted Extensions 的多级别网络功能依赖于共享 IP 栈的功能。Trusted Extensions 中的管理过程假设联网完全是由全局区域控制的。因此，如果您的初始设置团队已经安装了具有专用 IP 实例的有标签区域，您必须提供或参考站点特定的文档。

区域和多级别端口

缺省情况下，区域之间不能相互发送或接收包。多级别端口 (Multilevel Port, MLP) 可以启用端口上的特定服务，用以接受一定标签范围内的请求，或来自一个标签集合的请求。这些特权服务可以以请求的标签进行回复。例如，您可能想要创建一个可以在所有标签进行侦听的特权 Web 浏览器端口，但是它的回复受标签限制。缺省情况下，有标签区域没有 MLP。

对 MLP 可以接受的包进行限制的标签范围或标签集合基于区域的 IP 地址。在 `tnrhdb` 数据库中为该 IP 地址指定了一个远程主机模板。远程主机模板中的标签范围或标签集合对 MLP 可以接受的包进行限制。

- 针对不同 IP 地址配置，对 MLP 的限制如下：
- 在全局区域具有一个 IP 地址并且每个有标签区域都有一个唯一 IP 地址的系统上，可以向每个区域添加用于特定服务的 MLP。例如，可以对系统进行配置，从而通过 TCP 端口 22 的 `ssh` 服务是全局区域中和每个有标签区域中的 MLP。
- 在典型配置中，为全局区域指定一个 IP 地址，有标签区域与全局区域共享另一个 IP 地址。MLP 添加到一个共享接口后，服务包会路由至定义了 MLP 的有标签区域。仅当有标签区域的远程主机模板包含包的标签时，才会接受该包。如果范围是 `ADMIN_LOW` 到 `ADMIN_HIGH`，将接受所有包。范围较窄会丢弃不在范围内的包。

  一个区域至多可以将一个特定端口定义为共享接口上的 MLP。在前面的方案中，`ssh` 端口配置为非全局区域上的共享 MLP，其他区域都不能接收共享地址上的 `ssh` 连接。但是，全局区域可以定义 `ssh` 端口为专用 MLP，用于接收其区域特定的地址上的连接。
- 在全局区域和有标签区域共享一个 IP 地址的系统中，用于 `ssh` 服务的 MLP 可以添加到一个区域。如果将用于 `ssh` 的 MLP 添加到全局区域，没有任何有标签区域可以添加用于 `ssh` 服务的 MLP。同样，如果将用于 `ssh` 服务的 MLP 添加到有标签区域，全局区域也无法配置有 `ssh` MLP。

有关向有标签区域添加 MLP 的示例，请参见示例 13–16。

Trusted Extensions 中的区域和 ICMP

网络向网络中的系统传送广播消息并发送 ICMP 包。在多级别系统上，这些传送会对每个标签的系统进行泛洪攻击。缺省情况下，有标签区域的网络策略要求仅应在匹配标签接收 ICMP 包。

全局区域进程和有标签区域

在 Trusted Extensions 中，MAC 策略适用于所有进程，包括全局区域中的进程。全局区域中的进程以标签 ADMIN_HIGH 运行。共享全局区域的文件时，以标签 ADMIN_LOW 进行共享。因此，由于 MAC 会阻止标签级别较高的进程修改级别较低对象，全局区域通常不能向 NFS 挂载的系统执行写入操作。

但是，在有限的几种情况下，有标签区域中的操作可以要求全局区域进程修改该区域的文件。

要启用全局区域进程以挂载一个具有读/写权限的远程文件系统，挂载必须在其标签与远程文件系统的标签相同的区域的区域路径下。但是，不能挂载在区域的根路径下。

- 挂载系统必须在与远程文件系统相同的标签具有一个区域。
- 系统必须将远程文件系统挂载在相同有标签区域的区域路径下。

  系统**不能**在有相同标签区域的**区域根路径**下挂载远程文件系统

例如，一个名为 public 的区域，位于标签 PUBLIC（公共）级别。**区域路径**为 /zone/public/。区域路径下的所有目录都处于标签 PUBLIC 级别，如下所示：

```
/zone/public/dev
/zone/public/etc
/zone/public/home/username
/zone/public/root
/zone/public/usr
```

区域路径下的目录中，只有 /zone/public/root 下的文件可以从公共区域看到。仅能从全局区域访问标签 PUBLIC 的所有其他目录和文件。路径 /zone/public/root 是**区域根路径**。

从公共区域管理员的角度看，看到的区域根路径是 /。同样，公共区域管理员无法访问区域路径中的用户起始目录：/zone/public/home/*username* 目录。仅能从全局区域看到该目录。公共区域在区域根路径中将该目录挂载为 /home/ *username*。从全局区域的角度看，看到的挂载是 /zone/public/root/home/*username*。

公共区域管理员可以修改 /home/*username*。用户起始目录下的文件需要修改时，全局区域进程不能使用该路径。全局区域使用区域路径中用户的起始目录 /zone/public/home/*username*。

- 在区域路径 /zone/*zonename*/ 下，但是不在区域根路径 /zone/*zonename*/root 目录下的文件和目录，可以由在 ADMIN_HIGH 标签运行的全局区域进程进行修改。
- 区域根路径 /zone/public/root 下的文件和目录可以由有标签区域管理员修改。

例如，用户在公共区域分配设备时，在标签 ADMIN_HIGH 运行的全局区域进程可以修改区域路径中的 dev 目录：/zone/public/dev。同样，用户保存桌面配置时，桌面配置文件可以由 /zone/public/home/*username* 中的全局区域进程进行修改。最后，要从有标签区域共享文件，全局区域管理员将在区域路径中创建配置文件

dfstab：/zone/public/etc/dfs/dfstab。有标签区域管理员不能访问该文件，也无法从有标签区域共享它。要共享有标签目录，请参见第 133 页中的“如何从有标签区域共享目录”。

Trusted Extensions 中的区域管理实用程序

有些区域管理任务可以从命令行执行。但是最简单的管理区域方法是使用 Trusted Extensions 提供的 GUI：

- 通过使用 Solaris Management Console 中的可信网络区域工具执行区域安全属性的配置。有关该工具的说明，请参见第 39 页中的“"Trusted Network Zones"（可信网络区域）工具”。有关区域配置和创建的示例，请参见《Trusted Extensions Configuration Guide》中的第 4 章 “Configuring Trusted Extensions (Tasks)”和第 123 页中的“如何为区域创建多级别端口”。
- shell 脚本 /usr/sbin/txzonemgr 为创建、安装、初始化和引导区域提供了一个基于菜单的向导。如果要从 Solaris Trusted Extensions (JDS) 管理区域，请使用 txzonemgr 脚本，不要使用 Trusted CDE 操作。txzonemgr 使用 zenity 命令。有关详细信息，请参见 zenity(1) 手册页。
- 在 Trusted CDE 中，可以通过 "Trusted_Extensions" 文件夹中的操作来执行区域的配置和创建。有关操作的说明，请参见第 32 页中的 “Trusted CDE 操作”。有关使用这些操作的过程，请参见第 51 页中的 “如何在 Trusted Extensions 中启动 CDE 管理操作”。

管理区域（任务列表）

以下任务列表说明了特定于 Trusted Extensions 的区域管理任务。本图同时也指出了在 Trusted Extensions 中执行的常见过程；与它们在 Oracle Solaris 系统中的执行一样。

任务	说明	参考
查看所有区域。	在任何标签查看由当前区域支配的区域。	第 114 页中的 “如何显示就绪或正在运行区域”
查看挂载的目录。	在任何标签查看由当前标签支配的目录。	第 115 页中的 “如何显示挂载的文件的标签”
允许一般用户查看 /etc 文件。	回送可以挂载全局区域中的目录或文件，缺省情况下，在有标签区域是无法看到该目录或文件。	第 117 页中的 “如何对通常在有标签区域中不可见的文件进行回送挂载”
防止一般用户从较高级别标签查看较低级别的起始目录。	缺省情况下，可以从较高级别区域看到较低级别目录。禁用一个较低级别区域的挂载时，会禁用所有较低级别区域的挂载。	第 118 页中的 “如何禁用较低级别文件的挂载”

任务	说明	参考
配置区域以允许对文件的标签进行更改。	有标签区域的特权有限。缺省情况下，有标签区域无权允许授权用户重新为文件设置标签。可以修改区域配置以添加该特权。	第 121 页中的“如何使文件可以从有标签区域重新设置标签”
将文件或目录移入有标签区域，或从有标签区域移出。	通过更改文件标签来更改其安全级别。	《Trusted Extensions User's Guide》中的“How to Move Files Between Labels in Trusted CDE”
将 ZFS 数据集附加到一个有标签区域，然后将该数据集共享。	在有标签区域挂载具有读/写权限的 ZFS 数据集，然后以只读形式与较高级别区域共享该数据集。	第 119 页中的“如何从有标签区域共享 ZFS 数据集”。
配置新区域。	在一个当前尚未用作本系统区域标签的标签下创建一个区域。	请参见《Trusted Extensions Configuration Guide》中的“Name and Label the Zone”。 然后，按照初始设置团队用于创建其他区域的过程进行操作。有关步骤，请参见《Trusted Extensions Configuration Guide》中的“Creating Labeled Zones”。
为应用程序创建多级别端口。	多级别端口用于需要多级别输入进入一个有标签区域的程序。	第 122 页中的“如何为 NFSv3 Over udp 配置多级别端口” 第 123 页中的“如何为区域创建多级别端口”
解决 NFS 挂载和访问问题。	调试挂载和区域可能出现的一般访问问题。	第 139 页中的“如何解决 Trusted Extensions 中的挂载故障”
删除有标签区域。	将有标签区域从系统中完全删除。	《System Administration Guide: Oracle Solaris Containers-Resource Management and Oracle Solaris Zones》中的“How to Remove a Non-Global Zone”

▼ 如何显示就绪或正在运行区域

此过程会创建一个 shell 脚本，以显示当前区域以及当前区域配置的所有区域的标签。

开始之前 您必须具有全局区域中的 "System Administrator"（系统管理员）角色。

1. **使用可信编辑器创建 `getzonelabels` 脚本。**
   有关详细信息，请参见第 52 页中的“如何在 Trusted Extensions 中编辑管理文件”。
   提供脚本的路径名，例如 `/usr/local/scripts/getzonelabels`。

2 添加以下内容，然后保存文件：

```
#!/bin/sh
#
echo "NAME\t\tSTATUS\t\tLABEL"
echo "====\t\t======\t\t====="
myzone=‘zonename‘
for i in ‘/usr/sbin/zoneadm list -p‘ ; do
        zone=‘echo $i | cut -d ":" -f2‘
        status=‘echo $i | cut -d ":" -f3‘
        path=‘echo $i | cut -d ":" -f4‘
        if [ $zone != global ]; then
                if [ $myzone = global ]; then
                        path=$path/root/tmp
                else
                        path=$path/export/home
                fi
        fi
        label=‘/usr/bin/getlabel -s $path |cut -d ":" -f2-9‘
        if [ ‘echo $zone|wc -m‘ -lt 8 ]; then
                echo "$zone\t\t$status\t$label"
        else
                echo "$zone\t$status\t$label"
        fi
done
```

3 在全局区域中测试脚本。

```
# getzonelabels
NAME            STATUS          LABEL
====            ======          =====
global          running         ADMIN_HIGH
needtoknow      running         CONFIDENTIAL : NEED TO KNOW
restricted      ready           CONFIDENTIAL : RESTRICTED
internal        running         CONFIDENTIAL : INTERNAL
public          running         PUBLIC
```

从全局区域运行时，脚本显示所有就绪或正在运行区域的标签。下面是从缺省 `label_encodings` 文件创建的区域的全局区域输出：

示例 10–1 显示所有就绪或正在运行区域的标签

在下面的示例中，用户在**内部**区域中运行 `getzonelabels` 脚本。

```
# getzonelabels
NAME            STATUS          LABEL
====            ======          =====
internal        running         CONFIDENTIAL : INTERNAL
public          running         PUBLIC
```

▼ 如何显示挂载的文件的标签

此过程创建一个 shell 脚本，以显示当前区域的已挂载文件系统。从全局区域运行时，该脚本显示每个区域中所有已挂载文件系统的标签。

开始之前 您必须具有全局区域中的 "System Administrator"（系统管理员）角色。

1. **使用可信编辑器创建 `getmounts` 脚本。**
   有关详细信息，请参见第 52 页中的 “如何在 Trusted Extensions 中编辑管理文件”。

   提供脚本的路径名，例如 `/usr/local/scripts/getmounts`。

2. **添加以下内容，然后保存文件：**

```
#!/bin/sh
#
for i in `/usr/sbin/mount -p | cut -d " " -f3` ; do
        /usr/bin/getlabel $i
done
```

3. **在全局区域中测试脚本。**

```
# /usr/local/scripts/getmounts
/:      ADMIN_LOW
/dev:   ADMIN_LOW
/kernel:        ADMIN_LOW
/lib:   ADMIN_LOW
/opt:   ADMIN_LOW
/platform:      ADMIN_LOW
/sbin:  ADMIN_LOW
/usr:   ADMIN_LOW
/var/tsol/doors:        ADMIN_LOW
/zone/needtoknow/export/home:   CONFIDENTIAL : NEED TO KNOW
/zone/internal/export/home:     CONFIDENTIAL : INTERNAL USE ONLY
/zone/restricted/export/home:   CONFIDENTIAL : RESTRICTED
/proc:  ADMIN_LOW
/system/contract:       ADMIN_LOW
/etc/svc/volatile:      ADMIN_LOW
/etc/mnttab:    ADMIN_LOW
/dev/fd:        ADMIN_LOW
/tmp:           ADMIN_LOW
/var/run:       ADMIN_LOW
/zone/public/export/home:  PUBLIC
/root:          ADMIN_LOW
```

示例 10–2 显示 Restricted（受限）区域中文件系统的标签

一般用户从有标签区域运行时，`getmounts` 脚本显示该区域中所有已挂载文件系统的标签。在已经为缺省 `label_encodings` 文件中的每个标签创建了区域的系统中，以下是 `Restricted`（受限）区域的输出：

```
# /usr/local/scripts/getmounts
/:      CONFIDENTIAL : RESTRICTED
/dev:   CONFIDENTIAL : RESTRICTED
/kernel:        ADMIN_LOW
/lib:   ADMIN_LOW
/opt:   ADMIN_LOW
/platform:      ADMIN_LOW
/sbin:  ADMIN_LOW
/usr:   ADMIN_LOW
```

```
/var/tsol/doors:        ADMIN_LOW
/zone/needtoknow/export/home:   CONFIDENTIAL : NEED TO KNOW
/zone/internal/export/home:     CONFIDENTIAL : INTERNAL USE ONLY
/proc:  CONFIDENTIAL : RESTRICTED
/system/contract:       CONFIDENTIAL : RESTRICTED
/etc/svc/volatile:      CONFIDENTIAL : RESTRICTED
/etc/mnttab:    CONFIDENTIAL : RESTRICTED
/dev/fd:        CONFIDENTIAL : RESTRICTED
/tmp:   CONFIDENTIAL : RESTRICTED
/var/run:       CONFIDENTIAL : RESTRICTED
/zone/public/export/home:       PUBLIC
/home/gfaden:   CONFIDENTIAL : RESTRICTED
```

▼ 如何对通常在有标签区域中不可见的文件进行回送挂载

利用此过程，指定有标签区域中的用户可以查看缺省情况下未从全局区域导出的文件。

开始之前 您必须具有全局区域中的 "System Administrator"（系统管理员）角色。

1 停止要更改配置的区域。

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

2 回送挂载文件或目录。

例如，允许普通用户查看 `/etc` 目录中的文件。

```
# zonecfg -z zone-name
 add filesystem
 set special=/etc/filename
 set directory=/etc/filename
 set type=lofs
 add options [ro,nodevices,nosetuid]
 end
 exit
```

注 – 某些文件不为系统使用，所以回送挂载它们没有任何影响。例如，Trusted Extensions 软件不会检查有标签区域中的 `/etc/dfs/dfstab` 文件。有关更多信息，请参见第 128 页中的 “从有标签区域共享文件”。

---

3 启动区域。

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

示例 10–3 回送挂载 `/etc/passwd` 文件

此示例中，安全管理员希望允许测试人员和编程人员检查他们的本地口令是否已经设置。停止 `sandbox`（沙箱）区域后，其配置为回送挂载 `passwd` 文件。然后，重新启动区域。

```
# zoneadm -z sandbox halt
# zonecfg -z sandbox
 add filesystem
    set special=/etc/passwd
    set directory=/etc/passwd
    set type=lofs
    add options [ro,nodevices,nosetuid]
 end
 exit
# zoneadm -z sandbox boot
```

▼ 如何禁用较低级别文件的挂载

缺省情况下，用户可以查看较低级别文件。删除 net_mac_aware 特权，以防止从特定区域查看所有较低级别文件。有关 net_mac_aware 特权的说明，请参见 privileges(5) 手册页。

开始之前 您必须具有全局区域中的 "System Administrator"（系统管理员）角色。

1. **停止要更改配置的区域。**

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

2. **配置区域，防止查看较低级别文件。**

   从区域删除 net_mac_aware 特权。

   ```
   # zonecfg -z zone-name
    set limitpriv=default,!net_mac_aware
    exit
   ```

3. **重新启动区域。**

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

示例 10–4 防止用户查看较低级别文件

在此示例中，安全管理员希望防止一个系统中的用户被混淆。因此，用户只能查看其正在工作的标签的文件。从而，安全管理员可以阻止查看所有较低级别文件。在该系统中，用户无法看到公用文件，除非用户以 PUBLIC（公共）标签工作。此外，用户只能在区域的标签对文件进行 NFS 挂载。

```
# zoneadm -z restricted halt
# zonecfg -z restricted
 set limitpriv=default,!net_mac_aware
 exit
# zoneadm -z restricted boot

# zoneadm -z needtoknow halt
# zonecfg -z needtoknow
 set limitpriv=default,!net_mac_aware
 exit
# zoneadm -z needtoknow boot
```

```
# zoneadm -z internal halt
# zonecfg -z internal
 set limitpriv=default,!net_mac_aware
 exit
# zoneadm -z internal boot
```

因为 PUBLIC（公共）是最低级别标签，安全管理员不对 PUBLIC（公共）区域运行这些命令。

▼ 如何从有标签区域共享 ZFS 数据集

在此过程中，要在有标签区域中挂载一个具有读/写权限的 NFS 数据集。因为所有命令都在全局区域中执行，全局区域管理员可以对向有标签区域添加 ZFS 数据集进行控制。

有标签区域至少要处于 "ready"（就绪）状态下才能共享数据集。区域可以处于 "running"（正在运行）状态。

开始之前 要以数据集配置区域，首先停止该区域。

1 创建 ZFS 数据集。

```
# zfs create datasetdir/subdir
```

数据集的名称可以包括目录，例如 zone/data。

2 在全局区域中，停止有标签区域。

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

3 设置数据集的挂载点。

```
# zfs set mountpoint=legacy datasetdir/subdir
```

如果挂载点与有标签区域相对应，设置 ZFS 的 "mountpoint"（挂载点）属性时会设置挂载点的标签。

4 将数据集作为文件系统添加到区域中。

```
# zonecfg -z labeled-zone-name
# zonecfg:labeled-zone-name> add fs
# zonecfg:labeled-zone-name:dataset> set dir=/subdir
# zonecfg:labeled-zone-name:dataset> set special=datasetdir/subdir
# zonecfg:labeled-zone-name:dataset> set type=zfs
# zonecfg:labeled-zone-name:dataset> end
# zonecfg:labeled-zone-name> exit
```

通过将数据集作为文件系统而添加，会在解释 dfstab 文件之前在区域中的 /data 处挂载该数据集。此步骤可以确保不会在引导区域之前挂载数据集。具体来说，区域引导，挂载数据集，然后解释 dfstab 文件。

5 **共享数据集。**

将数据集文件系统的项添加到 /zone/*labeled-zone-name*/etc/dfs/dfstab 文件。此项还使用 */subdir* 路径名。

```
share  -F nfs  -d "dataset-comment"  /subdir
```

6 **引导有标签区域。**

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

引导区域后，将自动挂载数据集，作为标签为 *labeled-zone-name* 的 *labeled-zone-name* 区域中的读/写挂载点。

示例 10–5 从有标签区域共享和挂载 ZFS 数据集

在此示例中，管理员将一个 ZFS 数据集添加到 needtoknow 区域，然后共享数据集。数据集 zone/data 当前被指定到 /mnt 挂载点。Restricted（受限）区域中的用户可以查看该数据集。

首先，管理员停止区域。

```
# zoneadm -z needtoknow halt
```

因为数据集当前被指定到不同的挂载点，管理员要删除之前的指定，然后设置新的挂载点。

```
# zfs set zoned=off zone/data
# zfs set mountpoint=legacy zone/data
```

接下来，在 zonecfg 交互式接口中，管理员明确将数据集添加到 needtoknow 区域。

```
# zonecfg -z needtoknow
# zonecfg:needtoknow> add fs
# zonecfg:needtoknow:dataset> set dir=/data
# zonecfg:needtoknow:dataset> set special=zone/data
# zonecfg:needtoknow:dataset> set type=zfs
# zonecfg:needtoknow:dataset> end
# zonecfg:needtoknow> exit
```

接下来，管理员修改 /zone/needtoknow/etc/dfs/dfstab 文件以共享数据集，然后引导 needtoknow 区域。

```
## Global zone dfstab file for needtoknow zone
share  -F nfs  -d "App Data on ZFS"  /data

# zoneadm -z needtoknow boot
```

现在，可以访问该数据集了。

Restricted（受限）区域（支配 needtoknow 区域）中的用户可以通过更改到 /data 目录来查看挂载的数据集。从全局区域的角度看，他们使用挂载数据集的完整路径。在此示例中，machine1 是包括有标签区域的系统的主机名。管理员将此主机名指定给非共享 IP 地址。

```
# cd /net/machine1/zone/needtoknow/root/data
```

故障排除 如果尝试从较高级别标签访问数据集时返回错误**找不到**或**无此类文件或目录**，管理员必须通过运行 svcadm restart autofs 命令来重启自动挂载程序服务。

▼ 如何使文件可以从有标签区域重新设置标签

此过程是用户可以重新为文件设置标签的先决条件。

开始之前 您必须具有全局区域中的 "Security Administrator"（安全管理员）角色。

1. **停止要更改配置的区域。**

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

2. **配置区域以启用标签重新设置。**

   向区域添加适当特权。Windows 特权允许用户使用拖放和剪切粘贴操作。

   - **要启用降级，请向区域添加 file_downgrade_sl 特权。**

     ```
     # zonecfg -z zone-name
      set limitpriv=default,win_dac_read,win_mac_read,win_dac_write,
      win_mac_write,win_selection,file_downgrade_sl
      exit
     ```

   - **要启用升级，请向区域添加 sys_trans_label 和 file_upgrade_sl 特权。**

     ```
     # zonecfg -z zone-name
      set limitpriv=default,win_dac_read,win_mac_read,win_dac_write,
      win_mac_write,win_selection,sys_trans_label,file_upgrade_sl
      exit
     ```

   - **要同时启用升级和降级，则需要向区域添加全部三个特权。**

     ```
     # zonecfg -z zone-name
      set limitpriv=default,win_dac_read,win_mac_read,win_dac_write,
      win_mac_write,win_selection,sys_trans_label,file_downgrade_sl,
      file_upgrade_sl
      exit
     ```

3. **重新启动区域。**

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

   对于允许重新设置标签的用户和进程要求，请参见 setflabel(3TSOL) 手册页。要授权用户重新为文件设置标签，请参见第 90 页中的 “如何允许用户更改数据的安全级别”。

示例 10–6 允许从内部区域升级

在此示例中，安全管理员希望允许系统上的授权用户升级文件。通过允许用户升级信息，管理员使他们能够在更高的安全级别保护这些信息。在全局区域中，管理员运行以下区域管理命令。

```
# zoneadm -z internal halt
# zonecfg -z internal
 set limitpriv=default,sys_trans_label,file_upgrade_sl
 exit
# zoneadm -z internal boot
```

现在，授权用户可以从 Internal（内部）区域将 Internal（内部）信息升级到 Restricted（受限）。

示例 10–7 允许从 Restricted（被限制）区域降级

在此示例中，安全管理员希望允许系统上的授权用户将文件降级。因为管理员不向区域添加 Windows 特权，授权用户不能使用文件管理器来重新为文件设置标签。要重新为文件设置标签，用户可以使用 setlabel 命令。

通过允许用户降级信息，管理员允许较低安全级别的用户访问文件。在全局区域中，管理员运行以下区域管理命令。

```
# zoneadm -z restricted halt
# zonecfg -z restricted
 set limitpriv=default,file_downgrade_sl
 exit
# zoneadm -z restricted boot
```

现在，授权用户可以使用 setlabel 命令，从 Restricted（被限制）区域将 Restricted（被限制）信息降级到 Internal（内部）或 Public（公共）。

▼ 如何为 NFSv3 Over udp 配置多级别端口

此过程用于启用通过 udp 的 NFSv3 向下读取挂载。Solaris Management Console 用于添加 MLP。

开始之前 您必须具有全局区域中的 "Security Administrator"（安全管理员）角色。

1. **启动 Solaris Management Console。**

   有关详细信息，请参见第 50 页中的 “如何使用 Solaris Management Console 管理本地系统”。

2. **选择 "Files"（文件）工具箱。**

   工具箱的标题包括 Scope=Files, Policy=TSOL。

3 配置区域和 MLP。

a. 导航到 "Trusted Network Zones"（可信网络区域）工具。

b. 双击全局区域。

c. 为 UDP 协议添加多级别端口：

i. 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）。

ii. 键入端口号 2049，然后单击 "OK"（确定）。

d. 单击 "OK"（确定）保存设置。

4 关闭 Solaris Management Console。

5 更新内核。

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

▼ 如何为区域创建多级别端口

在有标签区域中运行的应用程序需要多级别端口 (Multilevel Port, MLP) 来与区域通信时，使用此过程。在此过程中，一个 Web 代理与区域进行通信。Solaris Management Console 用于添加 MLP。

开始之前 您必须具有全局区域中的 "Security Administrator"（安全管理员）角色。有标签区域必须存在。有关详细信息，请参见《Trusted Extensions Configuration Guide》中的“Creating Labeled Zones”。

1 启动 Solaris Management Console。

有关详细信息，请参见第 50 页中的 “如何使用 Solaris Management Console 管理本地系统”。

2 选择 "Files"（文件）工具箱。

工具箱的标题包括 `Scope=Files, Policy=TSOL`。

3 向计算机列表添加代理主机和网络服务主机。

a. 在 "System Configuration"（系统配置）下，导航到 "Computers and Networks"（计算机和网络）工具。

b. 在 "Computer"（计算机）工具中，单击 "Action"（操作）菜单并选择 "Add Computer"（添加计算机）。

c. 为代理主机添加主机名和 IP 地址。

d. 保存更改。

e. 为网络服务主机添加主机名和 IP 地址。

f. 保存更改。

4 配置区域和 MLP。

a. 导航到 "Trusted Network Zones"（可信网络区域）工具。

b. 选择有标签区域。

c. 在 "MLP Configuration for Local IP Addresses"（本地 IP 地址的 MLP 配置）部分中指定适当的端口/协议字段。

d. 保存更改。

5 对于区域，通过完成以下步骤来定制模板：

a. 导航至 "Security Templates"（安全模板）工具。
单击 "Action"（操作）菜单，选择 "Add Template"（添加模板）。

b. 使用主机名作为模板名称。

c. 指定 CIPSO 作为 "Host Type"（主机类型）。

d. 使用区域的标签作为 "Minimum Label"（最小标签）和 "Maximum Label"（最大标签）。

e. 将区域标签指定给 "Security Label Set"（安全标签集合）。

f. 选择 "Hosts Explicitly Assigned"（明确指定的主机）选项卡。

g. 在 "Add an Entry"（添加项）部分中，添加于区域关联的 IP 地址。

h. 保存更改。

6 关闭 Solaris Management Console。

7 启动区域。

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

8 在全局区域中，为新地址添加路由。

例如，如果区域具有共享 IP 地址，执行以下操作：

```
# route add proxy labeled-zones-IP-address
# route add webservice labeled-zones-IP-address
```

◆ ◆ ◆ 第 11 章

11 在 Trusted Extensions 中管理和挂载文件（任务）

本章介绍了 LOFS 和 NFS 挂载在配置有 Trusted Extensions 的系统上的工作原理。本章还介绍了如何备份和恢复文件。

在 Trusted Extensions 中共享和挂载文件

Trusted Extensions 软件支持与 Oracle Solaris OS 相同的文件系统和文件系统管理命令。Trusted Extensions 还具有非全局区域共享文件功能。此外，Trusted Extensions 对每个非全局区域附加一个唯一的标签。属于该区域的所有文件和目录均挂载在该区域的标签级别。属于其他区域或 NFS 服务器的任意共享文件系统均挂载在所有者的标签级别。Trusted Extensions 阻止任何不符合用于标记的强制访问控制 (Mandatory Access Control, MAC) 策略的挂载。例如，区域的标签必须能够控制其已挂载的所有文件系统标签，而且只能使用读写权限挂载带同等标签的文件系统。

Trusted Extensions 中的 NFS 挂载

Trusted Extensions 中的 NFS 挂载与 Oracle Solaris 挂载类似。差别在于 Trusted Extensions 中挂载有标签区域时使用区域根路径名以及执行 MAC 策略。

Trusted Extensions 中的 NFS 共享与全局区域中的 Oracle Solaris 共享类似。但是，从多级别系统的有标签区域共享文件是 Trusted Extensions 的唯一特性：

- **在全局区域中共享和挂载**—在 Trusted Extensions 系统的全局区域中共享和挂载几乎与 Oracle Solaris OS 中的过程完全相同。对于挂载文件，可使用自动挂载程序、`vfstab` 文件以及 `mount` 命令。对于共享文件，可使用 `dfstab` 文件。
- **有标签区域中的挂载**—在 Trusted Extensions 的有标签区域中挂载文件几乎与在 Oracle Solaris OS 的非全局区域中挂载文件完全相同。对于挂载文件，可使用自动挂载程序、`vfstab` 文件以及 `mount` 命令。在 Trusted Extensions 中，每个有标签区域存在一个唯一的 `automount_home_`*label* 配置文件。
- **有标签区域中的共享**—可使用区域标签的 `dfstab` 文件在区域的标签共享有标签区域中的文件，但这些文件仅对全局区域可见。因此，由全局区域中的全局区域管理员来配置有标签区域以共享文件。此配置文件从其有标签区域看不到。有关更多讨论，请参见第 112 页中的 “全局区域进程和有标签区域”。

标签会影响可以挂载的文件。文件在特定标签共享和挂载。对于需要写入 NFS 挂载的文件的 Trusted Extensions 客户机，必须使用读写权限**与**客户机相同的标签挂载文件。如果在两个 Trusted Extensions 主机之间挂载文件，服务器与客户机必须具有 `cipso` 类型的兼容的远程主机模板。如果在 Trusted Extensions 主机与无标签主机之间挂载文件，可以挂载为 `tnrhdb` 文件中的无标签主机指定的单一标签的文件。可以查看使用 LOFS 挂载的文件，但不能修改。有关 NFS 挂载的详细信息，请参见第 129 页中的 “访问 Trusted Extensions 中 NFS 挂载的目录”。

标签还会影响可以查看哪些目录和文件。缺省情况下，较低级别对象可在用户的环境中使用。因此，在缺省配置中，一般用户可以查看低于用户当前级别的区域中的文件。例如，用户可以从较高级别标签查看其较低级别的起始目录。有关详细信息，请参见第 130 页中的 “在 Trusted Extensions 中创建起始目录”。

如果站点安全性禁止查看较低级别对象，可使较低级别目录对于用户不可见。有关详细信息，请参见第 118 页中的 “如何禁用较低级别文件的挂载”。

Trusted Extensions 中的挂载策略没有 MAC 覆盖。较高级别标签进程永远无法修改可在较低级别标签看到的已挂载文件。此 MAC 策略在全局区域中也有效。全局区域 `ADMIN_HIGH` 进程无法修改较低级别标签的 NFS 挂载的文件，例如 `PUBLIC` 文件或 `ADMIN_LOW` 文件。MAC 策略强制执行缺省配置，并且对一般用户不可见。一般用户无法查看对象，除非他们具有这些对象的 MAC 访问权限。

从有标签区域共享文件

在 Oracle Solaris OS 中，非全局区域无法从其区域中共享目录。但是，在 Trusted Extensions 中，有标签区域可以共享目录。使用位于区域的**根**路径以外的目录，在全局区域中指定可以在有标签区域中共享的目录。有关更多讨论，请参见第 112 页中的 “全局区域进程和有标签区域”。

/zone/*labeled-zone*/*directories*	也称为区域路径。即从全局区域到有标签区域的路径。*labeled-zone* 下的每个记录的标签都与该区域相同。
/zone/*labeled-zone*/root/*directories*	也称为区域根路径。从全局区域的角度来看，是有标签区域的**根**路径。从有标签区域的角度来看，它是区域的根，/ 目录。全局区域不会使用此路径来管理该区域。

要从有标签区域共享目录，全局区域管理员在区域路径的 /etc 目录中创建并修改 dfstab 文件：

```
/zone/labeled-zone/etc/dfs/dfstab
```

此 /etc 目录从有标签区域看不到。此目录与可从该区域看到的 /etc 目录不同：

```
Global zone view: /zone/labeled-zone/root/etc
Labeled zone view of the same directory: /etc
```

此路径中的 dfstab 文件不支持共享有标签目录。

如果有标签区域的状态为 "ready"（**就绪**）或 "running"（**正在运行**），将以该区域的标签级别共享 /zone/*labeled-zone*/etc/dfs/dfstab 文件中列出的文件。有关这一过程，请参见第 133 页中的 “如何从有标签区域共享目录”。

访问 Trusted Extensions 中 NFS 挂载的目录

缺省情况下，NFS 已挂载的文件系统可在导出的文件系统的标签级别看到。如果使用读写权限导出文件系统，该标签的用户可以向文件写入。低于用户当前会话级别标签的 NFS 挂载对于用户可见，但不能对其执行写入操作。即便使用读写权限共享文件系统，挂载系统也只能在挂载的标签向该文件系统执行写入操作。

要使 NFS 挂载的较低级别目录对较高级别区域中的用户可见，NFS 服务器上的全局区域管理员必须导出父目录。将父目录从其标签导出。在客户端，每个区域都必须具有 net_mac_aware 特权。缺省情况下，有标签区域在其 limitpriv 集中包含 net_mac_aware 特权。

- **服务器配置—** 在 NFS 服务器上，导出 dfstab 文件中的父目录。如果父目录位于有标签区域中，则必须在父目录的有标签区域中修改 dfstab 文件。有标签区域的 dfstab 文件仅从全局区域可见。有关这一过程，请参见第 133 页中的 “如何从有标签区域共享目录”。
- **客户机配置—** 必须在初始区域配置期间使用的区域配置文件中指定 net_mac_aware 特权。因此，在除最低级别区域以外的每个区域中，允许查看所有较低级别起始目录的用户都必须具有 net_mac_aware 特权。有关示例，请参见第 135 页中的 “如何在有标签区域中对文件进行 NFS 挂载”。

示例 11–1 提供对较低级别起始目录的访问

在起始目录服务器上，管理员在每个有标签区域中创建并修改 `/zone/`*labeled-zone*`/etc/dfs/dfstab` 文件。`dfstab` 文件使用读写权限导出 `/export/home` 目录。因此，如果在同一标签挂载目录，起始目录可写入。要导出 `PUBLIC`（公共）的 `/export/home` 目录，管理员在起始目录服务器上的 `PUBLIC`（公共）标签创建一个工作区，并从全局区域修改 `/zone/public/etc/dfs/dfstab` 文件。

在客户机上，全局区域的管理员检查除最低级别标签外的每个有标签区域是否都具有 `net_mac_aware` 特权。此特权允许挂载。此特权可在区域配置期间使用 `zonecfg` 命令指定。较低级别起始目录仅供查看。MAC 保护该目录中的文件以防止修改。

在 Trusted Extensions 中创建起始目录

起始目录是 Trusted Extensions 中的一个特例。需要确保在用户能够使用的每个区域中创建起始目录。另外，必须在用户系统上的区域中创建起始目录挂载点。为使 NFS 挂载的起始目录能够正常使用，必须使用目录的常规位置 `/export/home`。在 Trusted Extensions 中，对自动挂载程序进行了修改以处理每个区域中（即每个标签）的起始目录。有关详细信息，请参见第 130 页中的 “在 Trusted Extensions 中更改自动挂载程序”。

创建用户时创建起始目录。在 Trusted Extensions 中，使用 Solaris Management Console (Console) 来创建用户，因此 Console 将创建起始目录。但是，Console 在起始目录服务器的全局区域中创建起始目录。在该服务器上，由 LOFS 挂载目录。如果将起始目录指定为 LOFS 挂载，自动挂载程序会自动创建起始目录。

注 – 如果使用 Console 来删除用户，将仅删除全局区域中该用户的起始目录。不会删除有标签区域中该用户的起始目录。您负责对有标签区域中的起始目录进行归档和删除。有关过程，请参见第 91 页中的 “如何从 Trusted Extensions 系统删除用户帐户”。

但是，自动挂载程序不能在远程 NFS 服务器上自动创建起始目录。用户必须首先登录 NFS 服务器或者需要管理介入。要创建用户的起始目录，请参见《Trusted Extensions Configuration Guide》中的“Enable Users to Access Their Home Directories in Trusted Extensions”。

在 Trusted Extensions 中更改自动挂载程序

在 Trusted Extensions 中，每个标签需要一个单独的起始目录挂载。对 `automount` 命令进行了修改以处理这些有标签的自动挂载。对于每个区域，自动挂载程序 `autofs` 都会挂载一个 `auto_home_` *zone-name* 文件。例如，下面是 `auto_home_global` 文件中全局区域的条目：

```
+auto_home_global
*       -fstype=lofs    :/export/home/&
```

引导允许挂载较低级别区域的区域时，会发生下列情况。较低级别区域的起始目录挂载在 /zone/<**区域名称**>/export/home 下且为只读。auto_home_<**区域名称**> 映射指定 /zone 路径作为 lofs 重新挂载到 /zone/<**区域名称**>/home/<**用户名**> 上的源目录。

例如，下面是从较高级别区域生成的 auto_home_*zone-at-higher-label* 映射中的 auto_home_public 项：

```
+auto_home_public
*       -fstype=lofs    :/zone/public/export/home/&
```

下列是公共区域中的对应项：

```
auto_home_public
*       -fstype=lofs    :/export/home/&
```

如果引用了一个起始目录且该名称与 auto_home_<**区域名称**> 映射中的任意项均不匹配，映射会尝试匹配此回送挂载规范。如果能够满足下列两个条件，该软件会创建起始目录：

1. 此映射查找回送挂载规范的匹配项
2. 起始目录名称与**区域名称**中尚不存在其起始目录的有效用户相匹配

有关自动挂载程序变更的详细信息，请参见 automount(1M) 手册页。

Trusted Extensions 软件和 NFS 协议版本

在 Solaris 10 11/06 和 Solaris 10 8/07 发行版中，Trusted Extensions 仅能识别 NFS 版本 4 (NFSv4) 中的多个标签。从 Solaris 10 5/08 发行版起，Trusted Extensions 软件能够识别 NFS 版本 3 (NFSv3) 和 NFSv4 中的标签。可以使用下列挂载选项集之一：

```
vers=4 proto=tcp
vers=3 proto=tcp
vers=3 proto=udp
```

Trusted Extensions 对于通过 tcp 协议的挂载没有限制。在 NFSv3 和 NFSv4 中，tcp 协议可用于相同标签挂载和向下读取挂载。向下读取挂载需要多级别端口 (Multilevel Port, MLP)。

对于 NFSv3，Trusted Extensions 的行为类似于 Oracle Solaris OS。udp 是 NFSv3 的缺省协议，但是 udp 仅用于初始挂载操作。对于后续 NFS 操作，系统使用 tcp。因此，向下读取挂载在缺省配置中适用于 NFSv3。

在极少数情况下您会具有受限 NFSv3 挂载，以对初始和后续 NFS 操作使用 udp 协议，您必须为使用 udp 协议的 NFS 操作创建 MLP。有关这一过程，请参见第 122 页中的 “如何为 NFSv3 Over udp 配置多级别端口”。

配置有 Trusted Extensions 的主机还可以与无标签的主机共享其自己的文件系统。如果导出到无标签主机的文件或目录的标签等于与可信网络数据库项中的远程主机相关联的标签，该文件或目录为**可写**状态。仅当导出到无标签主机的文件或目录的标签由与远程主机相关联的标签控制，该文件或目录为**可读**状态。

只有单一标签可以与运行某个 Trusted Solaris 软件发行版的系统进行通信。Trusted Extensions 系统和 Trusted Solaris 系统必须为另一个系统指定一个具有无标签主机类型的模板。无标签主机类型必须指定相同的单一标签。作为 Trusted Solaris 服务器的无标签 NFS 客户机，客户机的标签不能为 `ADMIN_LOW`。

使用的 NFS 协议与本地文件系统类型无关。该协议取决于共享计算机的操作系统类型。为 `mount` 命令或在远程文件系统的 `vfstab` 文件中指定的文件系统类型始终为 NFS。

备份、共享和挂载有标签文件（任务列表）

下面的任务列表介绍了用于从有标签文件系统备份和恢复数据的常见任务，以及用于共享和挂载有标签的目录和文件的常见任务。

任务	说明	参考
备份文件。	通过备份来保护数据。	第 133 页中的 “如何在 Trusted Extensions 中备份文件”
恢复数据。	从备份恢复数据。	第 133 页中的 “如何在 Trusted Extensions 中恢复文件”
从有标签区域共享目录的内容。	允许在用户之间共享有标签目录的内容。	第 133 页中的 “如何从有标签区域共享目录”
挂载有标签区域共享的目录的内容。	允许在用于读写的同一标签的区域中挂载目录的内容。当较高级别区域挂载共享的目录时，该目录进行只读挂载。	第 135 页中的 “如何在有标签区域中对文件进行 NFS 挂载”
创建起始目录挂载点。	在每个标签为每位用户创建挂载点。此任务使用户能够在非 NFS 起始目录服务器的系统上访问其起始目录。	《Trusted Extensions Configuration Guide》中的“Enable Users to Access Their Home Directories in Trusted Extensions”
对在较高级别标签工作的用户隐藏较低级别信息。	防止从较高级别窗口查看较低级别信息。	第 118 页中的 “如何禁用较低级别文件的挂载”

任务	说明	参考
解决文件系统挂载问题。	解决文件系统挂载问题。	第 139 页中的“如何解决 Trusted Extensions 中的挂载故障”

▼ 如何在 Trusted Extensions 中备份文件

1. **承担 "Operator"（操作员）角色。**
   此角色包括介质备份权限配置文件。

2. **使用以下备份方法之一：**
   - 对于主要备份，使用 `/usr/lib/fs/ufs/ufsdump`
   - 对于小型备份，使用 `/usr/sbin/tar cT`
   - 调用这些命令中任一个命令的脚本

     例如，Budtool 备份应用程序调用 `ufsdump` 命令。请参见`ufsdump(1M)` 手册页。有关 `T` 选项到 `tar` 命令的详细信息，请参见 `tar(1)` 手册页。

▼ 如何在 Trusted Extensions 中恢复文件

1. **成为 root 用户。**

2. **使用以下方法之一：**
   - 对于主要恢复，使用 `/usr/lib/fs/ufs/ufsrestore`
   - 对于小型恢复，使用 `/usr/sbin/tar xT`
   - 调用这些命令中任一个命令的脚本

   有关 `T` 选项到 `tar` 命令的详细信息，请参见 `tar(1)` 手册页。

注意 – 仅这些命令保留标签。

▼ 如何从有标签区域共享目录

与在 Oracle Solaris OS 中相同，Solaris Management Console 中的挂载和共享工具用于从全局区域中共享和挂载文件。此工具不能用于挂载或共享源自有标签区域的目录。在区域的标签下创建一个 `dfstab` 文件，然后重启该区域以共享有标签目录。

注意 – 对于共享文件系统，请勿使用专有名称。共享文件系统的名称对于每位用户可见。

开始之前 您必须是超级用户或承担文件服务器上全局区域中的 "System Administrator"（系统管理员）角色。

1. **以将要共享的目录的标签创建工作区。**

   有关详细信息，请参见《Trusted Extensions User's Guide》中的"How to Add a Workspace at a Particular Label"。

2. **以该区域的标签创建 `dfstab` 文件。**

   对于将共享目录的每个区域，重复下列步骤：

   a. **在该区域中创建 `/etc/dfs` 目录。**

      ```
      # mkdir -p /zone/zone-name/etc/dfs
      ```

   b. **打开可信编辑器。**

      有关详细信息，请参见第 52 页中的 "如何在 Trusted Extensions 中编辑管理文件"。

   c. **将 `dfstab` 文件的完整路径名键入编辑器中。**

      ```
      # /zone/zone-name/etc/dfs/dfstab
      ```

   d. **添加项以从该区域共享目录。**

      此项从区域根路径的角度描述了该目录。例如，以下项以包含区域的标签共享应用程序的文件：

      ```
      share -F nfs -o ro /viewdir/viewfiles
      ```

3. **对于每个区域，通过启动区域来共享目录。**

   在全局区域中，对每个区域运行下列命令之一。每个区域都可以使用这些方法中的任何一个来共享其目录。实际共享将在每个区域进入**就绪**或**正在运行**状态时发生。

   - **如果该区域不处于正在运行状态且您不希望用户以该区域的标签登录到服务器，可将区域状态设为就绪。**

     ```
     # zoneadm -z zone-name ready
     ```

   - **如果该区域不处于正在运行状态且允许用户以该区域的标签登录到服务器，请引导该区域。**

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

   - **如果该区域已经正在运行，请重新引导该区域。**

     ```
     # zoneadm -z zone-name reboot
     ```

4 显示从您的系统共享的目录。

```
# showmount -e
```

5 要允许客户机挂载导出的文件，请参见第 135 页中的“如何在有标签区域中对文件进行 NFS 挂载”。

示例 11–2 以 PUBLIC 标签共享 /export/share 目录

对于以标签 PUBLIC 运行的应用程序，系统管理员允许用户读取**公共**区域的 /export/share 目录中的文档。名为**公共**的区域以标签 PUBLIC 运行。

首先，管理员创建 public（公共）工作区并编辑 dfstab 文件。

```
# mkdir -p /zone/public/etc/dfs
# /usr/dt/bin/trusted_edit /zone/public/etc/dfs/dfstab
```

在此文件中，管理员添加以下项：

```
## Sharing PUBLIC user manuals
share -F nfs -o ro /export/appdocs
```

管理员离开 public（公共）工作区并返回 "Trusted Path"（可信路径）工作区。由于不允许用户登录此系统，管理员通过将该区域置于就绪状态来共享文件。

```
# zoneadm -z public ready
```

在用户系统上挂载共享目录后，用户可访问该目录。

▼ 如何在有标签区域中对文件进行 NFS 挂载

在 Trusted Extensions 中，有标签区域管理该区域中的文件挂载。

来自无标签和有标签主机的文件可以挂载到 Trusted Extensions 有标签主机上。

- 要从单一标签主机挂载文件读写，远程主机的指定标签必须与正在挂载文件的区域相同。
- 由较高级别区域挂载的文件为只读状态。
- 在 Trusted Extensions 中，针对每个区域对 auto_home 配置文件进行定制。此文件由区域名称命名。例如，具有全局区域和公共区域的系统具有两个 auto_home 文件，即 auto_home_global 和 auto_home_public。

Trusted Extensions 使用与 Oracle Solaris OS 相同的挂载界面：

- 要在引导时挂载文件，请使用有标签区域中的 /etc/vfstab 文件。
- 要动态挂载文件，请使用有标签区域中的 mount 命令。
- 要自动挂载起始目录，请使用 auto_home_*zone-name* 文件。

- 要自动挂载其他目录，请使用标准自动挂载映射。如果自动挂载映射位于 LDAP 中，可使用 LDAP 命令来管理这些映射。

开始之前 您必须在客户机系统上要挂载的文件标签的区域中。如果您使用的不是自动挂载程序，则您必须是超级用户或承担 "System Administrator"（系统管理员）角色。要从较低级别服务器进行挂载，必须使用 `net_mac_aware` 特权对该区域进行配置。

- **要在有标签区域中对文件进行 NFS 挂载，请执行下列过程。**

  大多数过程都包括以特定标签创建工作区。要创建工作区，请参见《Trusted Extensions User's Guide》中的"How to Add a Workspace at a Particular Label"。

  - **动态挂载文件。**

    在有标签区域中，使用 `mount` 命令。对于动态挂载文件的示例，请参见示例 11–3。

  - **区域引导时挂载文件**

    在有标签区域中，将挂载添加到 `vfstab` 文件。

    有关有标签区域引导时挂载文件的示例，请参见示例 11–4 和示例 11–5。

  - **挂载通过 LDAP 管理的系统的起始目录。**

    a. **在每个标签将用户规范添加到 `auto_home_`*zone-name* 文件。**

    b. **然后，使用这些文件置备 LDAP 服务器上的 `auto_home_`*zone-name* 数据库。**

    有关示例，请参见示例 11–6。

  - **挂载通过文件管理的系统的起始目录。**

    a. **创建和置备 `/export/home/auto_home_`*lowest-labeled-zone-name* 文件。**

    b. **编辑 `/etc/auto_home_`*lowest-labeled-zone-name* 文件以指向新置备的文件。**

    c. **修改每个较高级别区域中的 `/etc/auto_home_`*lowest-labeled-zone-name* 文件，以指向您在步骤 a 中创建的文件。**

    有关示例，请参见示例 11–7。

示例 11–3 使用 `mount` 命令在有标签区域中挂载文件

在此示例中，系统管理员从公共区域挂载远程文件系统。公共区域位于多级别服务器上。

承担 "System Administrator"（系统管理员）角色后，该管理员以标签 `PUBLIC`（公共）创建工作区。在该工作区中，管理员运行 `mount` 命令。

```
# zonename
public
# mount -F nfs remote-sys:/zone/public/root/opt/docs  /opt/docs
```

标签为 PUBLIC 的单一标签文件服务器还包含要挂载的文档：

```
# mount -F nfs public-sys:/publicdocs  /opt/publicdocs
```

remote-sys 文件服务器的公共区域处于 "ready"（就绪）或 "running"（正在运行）状态时，remote-sys 文件成功挂载在此系统上。public-sys 文件服务器处于正在运行状态时，文件成功挂载。

示例 11–4 通过修改 vfstab 文件在有标签区域中挂载文件读写

在此示例中，公共区域引导时，系统管理员以本地系统的公共区域中的 PUBLIC 标签挂载两个远程文件系统。一个文件系统从多级别系统挂载，另一个文件系统从单一标签系统挂载。

承担 "System Administrator"（系统管理员）角色后，该管理员以标签 PUBLIC（公共）创建工作区。在该工作区中，管理员修改该区域中的 vfstab 文件。

```
## Writable books directories at PUBLIC
remote-sys:/zone/public/root/opt/docs  - /opt/docs  nfs  no  yes  rw
public-sys:/publicdocs    - /opt/publicdocs  nfs no yes rw
```

要访问多级别系统的远程有标签区域中的文件，vfstab 项使用远程系统的公共区域的区域根路径 /zone/public/root 作为要挂载的目录的目录路径名。单一标签系统的路径与要在 Oracle Solaris 系统上使用的路径相同。

在终端窗口中，管理员以标签 PUBLIC 挂载该文件。

```
# mountall
```

示例 11–5 通过修改 vfstab 文件在有标签区域中挂载较低级别文件

在此示例中，系统管理员从本地系统的内部区域中的公共区域挂载远程文件系统。承担 "System Administrator"（系统管理员）角色后，管理员以标签 INTERNAL（内部）创建工作区，然后修改该区域中的 vfstab 文件。

```
## Readable books directory at PUBLIC
## ro entry indicates that PUBLIC docs can never be mounted rw in internal zone
remote-sys:/zone/public/root/opt/docs  - /opt/docs  nfs  no  yes  ro
```

要访问远程有标签区域中的文件，vfstab 项使用远程系统的公共区域的区域根路径 /zone/public/root 作为要挂载的目录的目录路径名。

从内部区域中用户的角度看，可在 /opt/docs 处访问该文件。

在终端窗口中，管理员以标签 INTERNAL 挂载该文件。

```
# mountall
```

示例 11–6 在使用 LDAP 管理的网络中挂载有标签的起始目录

在此示例中，系统管理员允许新用户 ikuk 以每个标签访问其起始目录。此站点使用两个起始目录服务器，并使用 LDAP 进行管理。第二个服务器包含用户 jdoe 和 pkai 的起始目录。新用户将添加到此列表。

首先，承担 "System Administrator"（系统管理员）角色后，管理员修改全局区域的 /etc 目录中的 auto_home_*zone-name* 文件，以在第二个起始目录服务器中包含新用户。

```
## auto_home_global file
jdoe   homedir2-server:/export/home/jdoe
pkai   homedir2-server:/export/home/pkai
ikuk   homedir2-server:/export/home/ikuk
*      homedir-server:/export/home/&

## auto_home_internal file
## Mount the home directory from the internal zone of the NFS server
jdoe   homedir2-server:/export/home/jdoe
pkai   homedir2-server:/export/home/pkai
ikuk   homedir2-server:/export/home/ikuk
*      homedir-server:/export/home/&

## auto_home_public
## Mount the home directory from the public zone of the NFS server
jdoe   homedir2-server:/export/home/jdoe
pkai   homedir2-server:/export/home/pkai
ikuk   homedir2-server:/export/home/ikuk
*      homedir-server:/export/home/&
```

其次，为使用户能够以所有标签登录，管理员对所有标签的 auto_home_*zone-name* 文件重复这些编辑操作。

最后，修改此系统上的每个 auto_home_*zone-name* 文件后，管理员使用这些文件将各项添加到 LDAP 数据库。

与 Oracle Solaris OS 类似，/etc/auto_home_*zone-name* 文件中的 +auto_home_public 项将自动挂载程序定向到 LDAP 项。网络中其他系统上的 auto_home_*zone-name* 文件从 LDAP 数据库进行更新。

示例 11–7 在使用文件管理的系统上挂载较低级别起始目录

在此示例中，系统管理员允许用户以每个标签访问其起始目录。站点的标签为 PUBLIC、INTERNAL 和 NEEDTOKNOW。此站点使用两个起始目录服务器，并使用文件进行管理。第二个服务器包含用户 jdoe 和 pkai 的起始目录。

要完成此任务，系统管理员定义公共区域中的公共区域 NFS 起始目录，并将此配置与内部和 needtoknow 区域共享。

首先，承担 "System Administrator"（系统管理员）角色后，该管理员以标签 PUBLIC（公共）创建工作区。在此工作区中，管理员创建新文件 /export/home/auto_home_public。此文件包含所有定制的基于每个用户的 NFS 规范项。

```
## /export/home/auto_home_public file at PUBLIC label
jdoe   homedir2-server:/export/home/jdoe
pkai   homedir2-server:/export/home/pkai
*      homedir-server:/export/home/&
```

第二，管理员修改 /etc/auto_home_public 文件以指向此新文件。

```
## /etc/auto_home_public file in the public zone
## Use /export/home/auto_home_public for the user entries
## +auto_home_public
+ /export/home/auto_home_public
```

此项指示自动挂载程序使用本地文件的内容。

第三，管理员同样修改内部和 needtoknow 区域中的 /etc/auto_home_public 文件。管理员使用对内部和可在 needtoknow 区域看到的公共区域的路径名。

```
## /etc/auto_home_public file in the internal zone
## Use /zone/public/export/home/auto_home_public for PUBLIC user home dirs
## +auto_home_public
+ /zone/public/export/home/auto_home_public

## /etc/auto_home_public file in the needtoknow zone
## Use /zone/public/export/home/auto_home_public for PUBLIC user home dirs
## +auto_home_public
+ /zone/public/export/home/auto_home_public
```

管理员添加新用户 ikuk 时，将添加到 PUBLIC 标签的 /export/home/auto_home_public 文件。

```
## /export/home/auto_home_public file at PUBLIC label
jdoe   homedir2-server:/export/home/jdoe
pkai   homedir2-server:/export/home/pkai
ikuk   homedir2-server:/export/home/ikuk
*      homedir-server:/export/home/&
```

较高级别区域向下读取，从较低级别公共区域获取每个用户的起始目录。

▼ 如何解决 Trusted Extensions 中的挂载故障

开始之前 您必须在要挂载的文件标签的区域中。您必须是超级用户或承担 "System Administrator"（系统管理员）角色。

1. **检查 NFS 服务器的安全属性。**

   在适当作用域内使用 Solaris Management Console 中的安全模板工具。有关详细信息，请参见《Trusted Extensions Configuration Guide》中的"Initialize the Solaris Management Console Server in Trusted Extensions"。

   a. **确认 NFS 服务器的 IP 地址是在一个安全模板中指定的主机。**

      该地址可能是直接指定，或者通过通配符机制间接指定。该地址可以位于有标签模板或无标签模板中。

   b. **检查模板为 NFS 服务器指定的标签。**

      该标签必须与您尝试挂载文件的标签一致。

2. **检查当前区域的标签。**

   如果该标签的级别比已挂载文件系统的标签高，则将无法写入挂载（即便使用读写权限导出了远程文件系统）。您只能以要挂载的标签写入已挂载文件系统。

3. **要从运行 Trusted Solaris 软件早期版本的 NFS 服务器挂载文件系统，请执行以下操作：**

   - **对于 Trusted Solaris 1 NFS 服务器，将 `vers=2` 和 `proto=udp` 选项用于 `mount` 命令。**
   - **对于 Trusted Solaris 2.5.1 NFS 服务器，将 `vers=2` 和 `proto=udp` 选项用于 `mount` 命令。**
   - **对于 Trusted Solaris 8 NFS 服务器，将 `vers=3` 和`proto=udp` 选项用于 `mount` 命令。**

   要从这些服务器中的任何一个挂载文件系统，必须将该服务器指定给一个无标签的模板。

◆ ◆ ◆ 第 12 章

12 可信网络（概述）

本章将向您介绍 Trusted Extensions 中的可信网络概念和机制。

可信网络

Trusted Extensions 为区域、主机以及网络指定安全属性。这些属性将确保在网络上强制执行以下安全功能：

- 在网络通信中正确为数据设置标签。
- 通过本地网络发送或接收数据或挂载文件系统时执行强制访问控制 (Mandatory Access Control, MAC) 规则。
- 将数据路由至远程网络时执行 MAC 规则。
- 将数据路由至区域时执行 MAC 规则。

在 Trusted Extensions 中，网络包受 MAC 保护。标签用于 MAC 决策。用敏感标签以显式或隐式方式为数据设置标签。标签具有 ID 字段、等级或 "level"（级别）字段、以及区间或 "category"（类别）字段。数据必须通过认可检查。该检查确定标签是否格式正确，以及标签是否位于接收主机的认可范围内。位于接收主机认可范围内的格式正确的包将被授予访问权限。

在可信系统之间交换的 IP 包可以添加标签。Trusted Extensions 支持商业 IP 安全选项 (Commercial IP Security Option, CIPSO) 标签。包上的 CIPSO 标签用于对 IP 包进行分类、单独部署以及路由。路由决策比较数据的敏感标签与目标标签。

通常，在可信网络上，标签由发送主机生成，并由接收主机处理。然而，可信的路由器也可以在可信网络中转发包时添加或去除标签。在传输之前会将敏感标签映射到 CIPSO 标签。CIPSO 标签嵌入在 IP 包中。通常，包发送者和包的接收者在同一标签进行操作。

可信网络软件将确保执行 Trusted Extensions 安全策略，即使主题（进程）和对象（数据）位于不同的主机上。Trusted Extensions 网络将在分布式应用程序之间保持 MAC。

Trusted Extensions 数据包

Trusted Extensions 数据包包括 CIPSO 标签选项。数据包可以通过 IPv4 或 IPv6 网络发送。

在标准的 IPv4 格式中，带有选项的 IPv4 头后跟 TCP、UDP 或 SCTP 头，然后才是实际的数据。Trusted Extensions 版本的 IPv4 包针对安全属性在 IP 头中使用 CIPSO 选项。

带有 CIPSO 选项的 IPv4 头	TCP、UDP 或 SCTP	数据

在标准的 IPv6 格式中，带有扩展的 IPv6 头后跟 TCP、UDP 或 SCTP 头，然后才是实际的数据。Trusted Extensions IPv6 包在具有扩展的头中包括多级别安全选项。

带有扩展的 IPv6 头	TCP、UCP 或 SCTP	数据

可信网络通信

Trusted Extensions 支持可信网络上的有标签主机和无标签主机。LDAP 是一种完全受支持的命名服务。利用各种命令和 GUI，可以对网络进行管理。

运行 Trusted Extensions 软件的系统支持 Trusted Extensions 主机与以下任一类型系统之间的网络通信：

- 运行 Trusted Extensions 的其他系统
- 运行以下操作系统的系统：这些操作系统不识别安全属性但支持 TCP/IP，例如 Oracle Solaris 系统、其他 UNIX 系统、Microsoft Windows 和 Macintosh OS 系统
- 运行其他可识别 CIPSO 标签的可信操作系统的系统

正如在 Oracle Solaris OS 中，Trusted Extensions 网络通信和服务可由命名服务进行管理。Trusted Extensions 将以下接口添加到 Oracle Solaris 网络接口：

- Trusted Extensions 将添加三个网络配置数据库：`tnzonecfg`、`tnrhdb` 和 `tnrhtp`。有关详细信息，请参见第 143 页中的 “Trusted Extensions 中的网络配置数据库”。
- Trusted Extensions 版本的命名服务转换文件 `nsswitch.conf` 包括 `tnrhtp` 和 `tnrhdb` 数据库项。可以修改这些项以满足各个站点的配置。

  Trusted Extensions 使用 LDAP 命名服务以集中管理定义主机、网络和用户的配置文件。针对 LDAP 命名服务的可信网络数据库的缺省 `nsswitch.conf` 项如下：

  ```
  # Trusted Extensions
  tnrhtp: files ldap
  tnrhdb: files ldap
  ```

  Oracle Directory Server Enterprise Edition 上的 LDAP 命名服务是 Trusted Extensions 中唯一完全受支持的命名服务。有关在配置有 Trusted Extensions 的系统上使用 LDAP 的信息，请参见第 9 章，Trusted Extensions 和 LDAP（概述）。
- Trusted Extensions 向 Solaris Management Console 添加工具。该控制台用于集中管理区域、主机和网络。第 36 页中的 “Solaris Management Console 工具”中对这些网络工具进行了讲述。

  《Trusted Extensions Configuration Guide》中介绍了如何在配置网络时定义区域和主机。有关其他详细信息，请参见第 13 章，在 Trusted Extensions 中管理网络（任务）。
- Trusted Extensions 添加了用于管理可信联网的命令。Trusted Extensions 还为 Oracle Solaris 网络命令添加了选项。有关这些命令的说明，请参见第 144 页中的 “Trusted Extensions 中的网络命令”。

Trusted Extensions 中的网络配置数据库

Trusted Extensions 会将三个网络配置数据库装入到内核中。将数据从一台主机传输至另一台主机时，在认可检查中使用这些数据库。

- `tnzonecfg`—该本地数据库存储与安全相关的区域属性。每个区域的属性指定区域标签和区域对单级别和多级别端口的访问。另一个属性处理对控制消息的响应，如 `ping`。区域的标签在 `label_encodings` 文件中进行定义。有关详细信息，请参见 `label_encodings(4)` 和 `smtnzonecfg(1M)` 手册页。有关多级别端口的讨论，请参见第 111 页中的 “区域和多级别端口”。
- `tnrhtp`—该数据库存储描述主机和网关的安全属性的模板。`tnrhtp` 可以是本地数据库或存储在 LDAP 服务器上。发送通信时，主机和网关使用目标主机和下一中继站网关的属性强制执行 MAC。接收通信时，主机和网关使用发送者的属性。有关安全属性的详细信息，请参见第 145 页中的 “可信网络安全属性”。有关更多信息，请参见 `smtnrhtp(1M)` 手册页。

- tnrhdb—该数据库存储与获准通信的所有主机相对应的 IP 地址和网络前缀（回退机制）。tnrhdb 可以是本地数据库或存储在 LDAP 服务器上。从 tnrhtp 数据库为每个主机或网络前缀指定一个安全模板。模板中的属性定义负责指定主机的属性。有关更多信息，请参见 smtnrhdb(1M) 手册页。

在 Trusted Extensions 中，已经对 Solaris Management Console 进行了扩展来处理这些数据库。有关详细信息，请参见第 36 页中的 “Solaris Management Console 工具”。

Trusted Extensions 中的网络命令

Trusted Extensions 添加了以下命令来管理可信网络：

- tnchkdb—该命令用于验证可信网络数据库的正确性。更改安全模板 (tnrhtp)、安全模板指定 (tnrhdb) 或区域配置 (tnzonecfg) 时，使用 tnchkdb 命令。修改数据库时，Solaris Management Console 工具将自动运行此命令。有关详细信息，请参见 tnchkdb(1M) 手册页。
- tnctl—该命令可用于更新内核中的可信网络信息。tnctl 还是一个系统服务。使用命令 svcadm restart /network/tnctl 重新启动时可从本地系统上的可信网络数据库刷新内核高速缓存。在 "Files"（文件）作用域内修改数据库时，Solaris Management Console 工具将自动运行此命令。有关详细信息，请参见 tnctl(1M) 手册页。
- tnd—该守护进程会从 LDAP 目录和本地文件中提取 tnrhdb 和 tnrhtp 信息。来自命名服务的信息将根据其在 nsswitch.conf 文件中的顺序装入。tnd 守护进程由 svc:/network/tnd 服务在引导时启动。该服务依赖于 svc:/network/ldap/client。

  tnd 命令还可用于调试和更改轮询间隔。有关详细信息，请参见 tnd(1M) 手册页。
- tninfo—该命令将详细显示可信网络内核高速缓存的当前状态详细信息。输出可以按主机名、区域或安全模板进行过滤。有关详细信息，请参见 tninfo(1M) 手册页。

Trusted Extensions 还向以下 Oracle Solaris 网络命令添加了选项：

- ifconfig—该命令的 all-zones 接口标志使指定接口可用于系统上的每个区域。可向其传送数据的相应区域由与该数据关联的标签决定。有关详细信息，请参见 ifconfig(1M) 手册页。
- netstat －-R 选项扩展了 Oracle Solaris netstat 用途，以显示特定于 Trusted Extensions 的信息，例如多级别套接字和路由表项的安全属性。扩展的安全属性包括对等体的标签以及套接字是特定于某个区域，还是可用于若干区域。有关详细信息，请参见 netstat(1M) 手册页。
- route －-secattr 选项扩展了 Oracle Solaris route 的用途，使其可以显示路由的安全属性。该选项的值具有以下格式：

  min_sl=*label*,max_sl=*label*,doi=*integer*,cipso

  cipso 关键字为可选项，缺省为已设置。有关详细信息，请参见 route(1M) 手册页。

- snoop—正如在 Oracle Solaris OS 中，该命令的 -v 选项可用于显示 IP 头的详细信息。在 Trusted Extensions 中，头包含标签信息。

可信网络安全属性

Trusted Extensions 中的网络管理基于安全模板。安全模板描述了一组具有通用协议和相同安全属性的主机。

安全属性以模板方式通过管理行为指定给系统（主机和路由器）。安全管理员负责管理模板并将其指定给系统。如果没有给某个系统指定模板，则不允许与该系统进行通信。

每个模板都进行了命名，并包含以下内容：

- "Unlabeled"（无标签）主机类型或 CIPSO 主机类型。用于网络通信的协议由模板的主机类型确定。

  主机类型用于确定是否使用 CIPSO 选项并会影响 MAC。请参见第 146 页中的 “安全模板中的主机类型和模板名称”。
- 一组适用于各个主机类型的安全属性。

有关主机类型和安全属性的详细信息，请参见第 145 页中的 “Trusted Extensions 中的网络安全属性”。

Trusted Extensions 中的网络安全属性

Trusted Extensions 安装时随附有一套缺省安全模板。将某模板指定给一台主机时，该模板中的安全值将应用于该主机。在 Trusted Extensions 中，网络上的无标签主机和有标签主机均通过模板方式指定安全属性。未指定安全模板的主机将不可访问。模板可本地存储，或存储在 Oracle Directory Server Enterprise Edition 上的 LDAP 命名服务中。

模板可直接或间接指定给主机。直接指定会将模板指定给特定的 IP 地址。间接指定会将模板指定给包括该主机的网络地址。没有安全模板的主机无法与配置有 Trusted Extensions 的主机进行通信。有关直接指定和间接指定的说明，请参见第 148 页中的 “可信网络回退机制”。

通过使用 Solaris Management Console 中的 "Security Templates"（安全模板）工具修改或创建模板。"Security Templates"（安全模板）工具强制完成模板中的必需字段。哪些字段是必需的取决于主机类型。

每种主机类型都有其自己的一套额外的必需和可选安全属性。以下安全属性均在安全模板中进行指定：

- **主机类型**—定义包是标签为 CIPSO 安全标签还是根本不设置标签。
- **缺省标签**—定义无标签主机的信任级别。无标签主机发送的包由接收 Trusted Extensions 主机或网关在此标签进行读取。

  缺省标签属性特定于无标签主机类型。有关详细信息，请参见 `smtnrhtp(1M)` 手册页和以下各节。
- **DOI**—标识系统解释域的非零正整数。DOI 用于说明哪组标签编码适用于网络通信或网络实体。具有不同 DOI 的标签是不相交的，即使在其他方面是相同的。对于无标签主机，DOI 适用于缺省标签。在 Trusted Extensions 中，缺省值为 `1`。
- **最小标签**—定义标签认可范围的下限。主机和下一中继站网关不会接收低于其模板中指定的最小标签的包。
- **最大标签**—定义标签认可范围的上限。主机和下一中继站网关不会接收高于其模板中指定的最大标签的包。
- **安全标签集合**—可选。为安全模板指定一组独立的安全标签。除了其认可范围由最大和最小标签确定之外，指定给具有安全标签集合的模板的主机还可以发送和接收与该标签集合中任一标签匹配的包。可以指定的最大标签数为四。

安全模板中的主机类型和模板名称

Trusted Extensions 支持可信网络数据库中的两种主机类型并提供两个缺省模板：

- **CIPSO 主机类型**—针对运行可信操作系统的主机。Trusted Extensions 为该主机类型提供名为 `cipso` 的模板。

  通用 IP 安全选项 (Common IP Security Option, CIPSO) 协议用于指定在 IP 选项字段中传递的安全标签。CIPSO 标签从数据的标签自动派生。标记类型 1 用于传递 CIPSO 安全标签。然后，该标签用于在 IP 级别进行安全检查，并标记网络包中的数据。
- **无标签主机类型**—针对使用标准联网协议但不支持 CIPSO 选项的主机。Trusted Extensions 为该主机类型提供名为 `admin_low` 的模板。

  该主机类型将指定给运行 Oracle Solaris OS 或其他无标签操作系统的主机。该主机类型负责提供缺省标签和缺省安全许可，以与无标签主机进行通信。此外，可以指定一个标签范围或一组独立标签，以允许将包发送到无标签网关进行转发。

注意 – `admin_low` 模板提供了使用特定于站点的标签构建无标签模板的示例。虽然安装 Trusted Extensions 需要 `admin_low` 模板，但是安全设置可能不适用于常规系统操作。出于系统维护和支持原因，请保持提供的模板不进行任何修改。

安全模板中的缺省标签

无标签主机类型的模板指定缺省标签。该标签用于控制与其操作系统无法识别标签（如 Oracle Solaris 系统）的主机进行的通信。指定的缺省标签反映适用于该主机及其用户的信任级别。

因为与无标签主机之间的通信本质上仅限于缺省标签，所有这些主机也称为**单标签主机**。

安全模板中的系统解释域

使用同一系统解释域 (Domain of Interpretation, DOI) 的组织在以相同方式解释标签信息和其他安全属性方面达成共识。Trusted Extensions 执行标签比较时，会进行检查以确定 DOI 是否等同。

Trusted Extensions 系统在一个 DOI 值上强制执行标签策略。Trusted Extensions 系统上的所有区域必须在同一 DOI 处运行。对于从使用不同 DOI 的系统接收的包，Trusted Extensions 系统不对其提供异常处理。

如果站点使用的 DOI 值与缺省值不同，必须将此值添加到 `/etc/system` 文件，并在每个安全模板中更改该值。有关初始过程，请参见《Trusted Extensions Configuration Guide》中的“Configure the Domain of Interpretation”。要配置各个安全模板中的 DOI，请参见示例 13–1。

安全模板中的标签范围

最小标签和最大标签属性用于为有标签主机和无标签主机建立标签范围。这些属性用于执行以下操作：

- 设置可在与远程 CIPSO 主机通信时使用的标签范围

  为了将包发送至目标主机，包的标签必须位于在该目标主机安全模板中指定给目标主机的标签范围内。
- 为通过 CIPSO 网关或无标签网关转发的包设置标签范围

  标签范围可在无标签主机类型的模板中进行指定。利用标签范围，主机可以转发不一定处于该主机的标签级别、但是位于指定标签范围内的包。

安全模板中的安全标签集合

安全标签集合最多可定义四个独立标签，远程主机可以在这些标签级别接受、转发或发送包。该属性为可选。缺省情况下，不定义安全标签集合。

可信网络回退机制

tnrhdb 数据库可以直接或间接地为特定主机指定安全模板。直接指定会将模板指定给主机的 IP 地址。间接指定由回退机制处理。可信网络软件首先查找专门将主机 IP 指定给模板的条目。如果软件未找到该主机的特定条目，则将查找“最长匹配位前缀”。当主机的 IP 地址介于具有固定前缀长度的 IP 地址的“最长匹配位前缀”内时，可以间接地将该主机指定给安全模板。

在 IPv4 中，可以由子网进行间接指定。使用 4、3、2 或 1 结尾零 (0) 八位字节进行间接指定时，软件将分别计算 0、8、16 或 24 的前缀长度。表 12–1 中的条目 3 - 6 说明了该回退机制。

还可通过添加斜线 (/) 后跟固定位的数量来设置固定的前缀长度。IPv4 网络地址的前缀长度可以介于 1 – 32 之间。IPv6 网络地址的前缀长度可以介于 1 – 128 之间。

下表提供了回退地址和主机地址示例。如果回退地址集内的某个地址是直接指定的，回退机制不会用于此地址。

表 12–1 tnrhdb 主机地址和回退机制条目

IP 版本	tnrhdb 条目	包含的地址
IPv4	192.168.118.57:cipso	192.168.118.57
	192.168.118.57/32:cipso	/32 用于设置 32 固定位的前缀长度。
	192.168.118.128/26:cipso	从 192.168.118.0 到 192.168.118.63
	192.168.118.0:cipso	192.168.118. 网络上的所有地址
	192.168.118.0/24:cipso	
	192.168.0.0/24:cipso	192.168.0. 网络上的所有地址。
	192.168.0.0:cipso	192.168. 网络上的所有地址
	192.168.0.0/16:cipso	
	192.0.0.0:cipso	192. 网络上的所有地址
	192.0.0.0/8:cipso	
	192.168.0.0/32:cipso	网络地址 192.168.0.0。不是通配符地址。
	192.168.118.0/32:cipso	网络地址 192.168.118.0。不是通配符地址。
	192.0.0.0/32:cipso	网络地址 192.0.0.0。不是通配符地址。
	0.0.0.0/32:cipso	主机地址 0.0.0.0。不是通配符地址。
	0.0.0.0:cipso	所有网络上的所有地址

表 12–1 tnrhdb 主机地址和回退机制条目 （续）

IP 版本	tnrhdb 条目	包含的地址
IPv6	2001\:DB8\:22\:5000\:\:21f7:cipso	2001:DB8:22:5000::21f7
	2001\:DB8\:22\:5000\:\:0/52:cipso	从 2001:DB8:22:5000::0 到 2001:DB8:22:5fff:ffff:ffff:ffff:ffff
	0\:\:0/0:cipso	所有网络上的所有地址

请注意，0.0.0.0/32 地址与特定地址 0.0.0.0 相匹配。在其中文字地址 0.0.0.0 用作源 IP 地址的系统中，tnrhdb 条目 0.0.0.0/32:admin_low 非常有用。例如，在 DHCP 服务器为 DHCP 客户端提供 IP 地址之前，DHCP 客户端可将该服务器作为 0.0.0.0 进行联系。

要在为 DHCP 客户端提供服务的 Sun Ray 服务器上创建 tnrhdb 条目，请参见示例 13–13。因为 0.0.0.0:admin_low 是缺省的通配符条目，因此请参见第 164 页中的 “如何限定可能会在可信网络上联系的主机”，以了解在删除或更改该缺省值时应考虑的问题。

有关 IPv4 和 IPv6 地址中的前缀长度的更多信息，请参见《Oracle Solaris 管理：IP 服务》中的“设计 CIDR IPv4 寻址方案”和《Oracle Solaris 管理：IP 服务》中的“IPv6 寻址概述”。

Trusted Extensions 中的路由概述

在 Trusted Extensions 中，不同网络上主机之间的路由必须在传输中的每个步骤中保持安全性。Trusted Extensions 向 Oracle Solaris OS 中的路由协议添加了扩展安全属性。与 Oracle Solaris OS 不同，该 Trusted Extensions 版本不支持动态路由。有关指定静态路由的详细信息，请参见 route(1M) 手册页中的 -p 选项。

网关和路由器路由包。在此讨论中，术语“网关”和“路由器”可以交换使用。

对于同一子网上主机之间的通信，仅在端点执行认可检查，因为其中没有涉及到路由器。在源主机上将执行标签范围检查。如果接收主机运行的是 Trusted Extensions 软件，还将在目标主机上执行标签范围检查。

源主机和目标主机位于不同的子网上，包将从源主机发送至网关。选定路由后，会在源主机上检查目标主机和下一中继站网关的标签范围。网关将包转发至其中连接了目标主机的网络。包可能会在抵达目标主机之前通过数个网关。

路由背景

在 Trusted Extensions 网关上，在某些情况下执行标签范围检查。在两个无标签主机之间路由包的 Trusted Extensions 系统将比较源主机的缺省标签与目标主机的缺省标签。两个无标签主机共享缺省标签时，将路由包。

每个网关都维护到所有目标主机的路由列表。标准 Oracle Solaris 路由会进行选择以优化路由。Trusted Extensions 提供了其他软件以检查适用于路由选择的安全要求。不满足安全要求的 Oracle Solaris 选择将被跳过。

Trusted Extensions 中的路由表项

Trusted Extensions 中的路由表项可以包含安全属性。安全属性可以包括 `cipso` 关键字。安全属性必须包括最大标签、最小标签和 DOI。

对于不提供安全属性的项，将使用网关安全模板中的属性。

Trusted Extensions 认可检查

Trusted Extensions 软件将针对安全目的确定路由的适用性。该软件在源主机、目标主机以及中间网关上运行一系列称为**认可检查**的测试。

注 – 在以下讨论中，对标签范围的认可检查也意味着对安全标签集合的检查。

认可检查将验证标签范围和 CIPSO 标签信息。从路由表项获取路由的安全属性，该项无安全属性，从网关的安全模板获取。

对于传入通信，如有可能，Trusted Extensions 软件将从包自身获取标签。仅当从支持标签的系统发送消息时才可以从包获取标签。无法从包获得标签时，从可信联网数据库文件将缺省标签指定给消息。然后，在认可检查中使用这些标签。Trusted Extensions 将对传出消息、转发的消息以及传入的消息强制执行若干检查。

源认可检查

对发送进程或发送区域执行以下认可检查：

- 对于所有目标，数据的标签必须位于路由中下一中继站（即第一个中继站）的标签范围内。而且，标签必须包含在第一中继站网关的安全属性内。
- 对于所有目标，传出包的 DOI 必须与目标主机的 DOI 相匹配。DOI 还必须与路由中所有中继站（包括其第一中继站网关）的 DOI 相匹配。
- 目标主机是无标签主机时，必须满足以下条件之一：
  - 发送主机的标签必须与目标主机的缺省标签相匹配。
  - 发送主机被授权执行跨标签通信，发送者的标签支配目标的缺省标签。
  - 发送主机被授权执行跨标签通信，发送者的标签是 `ADMIN_LOW`。即，发送者从全局区域进行发送。

注 – 将消息从一个网络上的主机通过网关发送至另一个网络上的主机时会发生第一中继站检查。

网关认可检查

在 Trusted Extensions 网关系统上，针对下一中继站网关执行以下认可检查：

- 如果传入包没有标签，包将从 `tnrhdb` 条目继承源主机的缺省标签。否则，包将接收指示的 CIPSO 标签。
- 针对转发包的检查操作类似于源认可：
  - 对于所有目标，数据的标签必须位于下一中继站的标签范围内。而且，标签必须包含在下一中继站主机的安全属性内。
  - 对于所有目标，传出包的 DOI 必须与目标主机的 DOI 相匹配。DOI 还必须与下一中继站主机的 DOI 相匹配。
  - 无标签包的标签必须与目标主机的缺省标签相匹配。
  - CIPSO 包的标签必须位于目标主机的标签范围内。

目标认可检查

Trusted Extensions 主机接收数据时，软件将执行以下检查：

- 如果传入包没有标签，包将从 `tnrhdb` 条目继承源主机的缺省标签。否则，包将接收指示的 CIPSO 标签。
- 包的标签和 DOI 必须与目标区域或目标进程的标签和 DOI 一致。进程正在侦听多级别端口的情况除外。侦听进程可以接收包，前提是该进程被授权执行跨标签通信，并且该进程位于全局区域中或者具有的标签可以支配该包的标签。

Trusted Extensions 中的路由管理

Trusted Extensions 支持在网络间路由通信的多种方法。在安全管理员角色中，可以设置路由以强制执行站点安全策略要求的安全程度。

例如，站点可以将本地网络以外的通信限制为单标签。该标签将应用于公用信息。诸如 `UNCLASSIFIED`（未分类）或 `PUBLIC`（公共）等的标签可以指示公共信息。为了强制执行该限制，这些站点会向连接至外部网络的网络接口指定单标签模板。有关 TCP/IP 和路由的更多详细信息，请参见以下内容：

- 《Oracle Solaris 管理：IP 服务》中的“为网络规划路由器”
- 《Oracle Solaris 管理：IP 服务》中的“配置本地网络中的系统”
- 《Oracle Solaris 管理：IP 服务》中的“主要的 TCP/IP 管理任务（任务列表）”
- 《Oracle Solaris 管理：IP 服务》中的“为 DHCP 服务准备网络（任务列表）”

在 Trusted Extensions 中选择路由器

作为路由器，Trusted Extensions 主机提供最高程度的信任。其他类型的路由器可能无法识别 Trusted Extensions 安全属性。无需管理操作，就可将包通过不提供 MAC 安全保护的路由器进行路由。

- CIPSO 路由器在包的 IP 选项部分找不到正确类型的信息时会丢弃包。例如，如果 CIPSO 路由器在 IP 选项中没有找到所需的 CIPSO 选项时，或 IP 选项中的 DOI 与目标的认可不一致时，该路由器会丢弃包。
- 未运行 Trusted Extensions 软件的其他类型路由器可配置为传递或丢弃包含 CIPSO 选项的包。只能识别 CIPSO 的网关（如 Trusted Extensions 提供的）可以使用 CIPSO IP 选项的内容来强制执行 MAC。

为了支持可信路由，Solaris 10 路由表进行了扩展，以包括 Trusted Extensions 安全属性。第 150 页中的 “Trusted Extensions 中的路由表项”中介绍了这些属性。Trusted Extensions 支持静态路由，其中管理员将手动创建路由表项。有关详细信息，请参见 `route(1M)` 手册页中的 `-p` 选项。

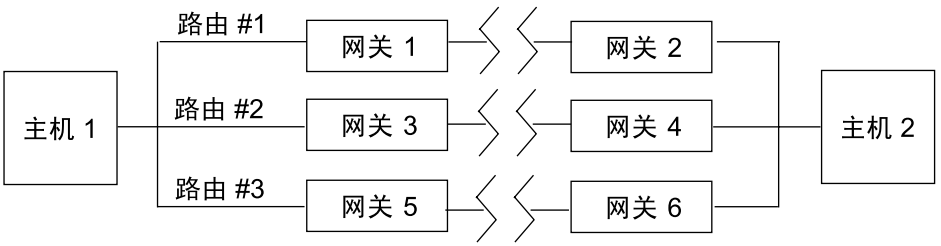
路由软件尝试在路由表中找到通往目标主机的路由。未显式命名主机时，路由软件将查找主机驻留的子网的条目。未定义主机或主机驻留的网络时，主机会将包发送至缺省网关（如果定义）。可定义多个缺省网关，每个都会被公平对待。

在 Trusted Extensions 的此发行版中，安全管理员可手动设置路由，然后在条件变化时手动更改路由表。例如，许多站点都有一个与外界通信的网关。在这些情况中，该单一网关可静态地定义为网络上各个主机上的**缺省值**。Trusted Extensions 的未来发行版中可能会包含动态路由支持。

Trusted Extensions 中的网关

Trusted Extensions 中的路由示例如下所示。该图和表显示了主机 1 和主机 2 之间可能的三种路由。

图 12–1 典型的 Trusted Extensions 路由和路由表项



路由	第一中继站网关	最小标签	最大标签	DOI
#1	网关 1	CONFIDENTIAL	SECRET	1
#2	网关 3	ADMIN_LOW	ADMIN_HIGH	1
#3	网关 5			

- 路由 #1 可以将位于 CONFIDENTIAL 标签范围内的包传输至 SECRET。
- 路由 #2 可以将包从 ADMIN_LOW 传输至 ADMIN_HIGH。
- 路由 #3 不指定路由信息。因此，其安全属性源自网关 5 的 tnrhtp 数据库中的模板。

Trusted Extensions 中的路由命令

为了显示套接字的标签和扩展安全属性，Trusted Extensions 将修改以下 Oracle Solaris 网络命令：

- netstat -rR 命令显示路由表项中的安全属性。
- netstat -aR 命令显示套接字的安全属性。
- route -p 命令（带有 add 或 delete 选项）更改路由表项。

有关详细信息，请参见 netstat(1M) 和 route(1M) 手册页。

有关示例，请参见第 168 页中的 “如何配置具有安全属性的路由”。

◆ ◆ ◆ 第 13 章

13 在 Trusted Extensions 中管理网络（任务）

本章提供了用于保证 Trusted Extensions 网络安全的实施详细信息和过程。

管理可信网络（任务列表）

下表指向适用于常见可信网络操作过程的任务列表。

任务	说明	参考
配置网络数据库。	创建远程主机模板，并将主机指定给这些模板。	第 155 页中的 “配置可信网络数据库（任务列表）”
配置路由并检查内核中的网络数据库和网络信息。	配置静态路由，使有标签包可通过有标签网关和无标签网关到达其目的地。 此外，还显示网络的状态。	第 168 页中的 “在 Trusted Extensions 中配置路由并检查网络信息（任务列表）”
对网络问题进行故障排除。	诊断有关有标签包的网络问题时要采取的步骤。	第 173 页中的 “可信网络故障排除（任务列表）”

配置可信网络数据库（任务列表）

Trusted Extensions 软件包含 `tnrhtp` 和 `tnrhdb` 数据库。这些数据库提供联系系统的远程主机的标签。Solaris Management Console 提供用于管理这些数据库的 GUI。

以下任务列表介绍了创建安全模板并将其应用于主机的任务。

任务	说明	参考
确定您的站点是否需要定制安全模板。	针对站点的安全要求评估现有模板。	第 157 页中的“如何确定是否需要站点专用安全模板”
访问 Solaris Management Console 中的安全模板工具。	访问该工具以修改可信网络数据库。	第 157 页中的“如何打开可信网络工具”
修改安全模板。	通过修改可信网络数据库修改可信网络中安全属性的定义。	第 158 页中的“如何构造远程主机模板”
	将 DOI 更改为异于 1 的值。	示例 13–1
	为将其他主机之间的通信限制于单个标签的有标签主机创建安全模板。	示例 13–2
	为以单标签网关形式运行的无标签主机创建安全模板。	示例 13–3
	为具有限定标签范围的主机创建安全模板。	示例 13–4
	为在其标签范围内指定一组独立标签的主机创建安全模板。	示例 13–5
	为无标签系统和网络指定安全模板。	示例 13–6
	为两个开发者系统创建安全模板。	示例 13–7
向已知网络添加主机。	向可信网络添加系统和网络。	第 162 页中的“如何向系统的已知网络添加主机”
使用通配符项提供远程主机访问。	通过间接将每台主机指定给相同安全模板允许某一 IP 地址范围内的主机与系统进行通信。	示例 13–8 示例 13–9 示例 13–10
在 `tnrhdb` 文件中更改 `admin_low` 通配符项。	通过将通配符项替换为引导时联系的主机的特定地址来提高安全性。	第 164 页中的“如何限定可能会在可信网络上联系的主机”
	通过将通配符项替换为有标签主机网络（作为缺省值）来提高安全性。	示例 13–11
创建主机地址 `0.0.0.0` 项。	配置 Sun Ray 服务器以接受来自远程客户机的初始联系信息。	示例 13–13
指定安全模板。	将模板与某个 IP 地址或连续 IP 地址的列表相关联。	第 163 页中的“如何将安全模板指定给向一台主机或一组主机”

▼ 如何确定是否需要站点专用安全模板

开始之前 您必须具有全局区域中的 "Security Administrator"（安全管理员）角色。

1. **熟悉 Trusted Extensions 模板。**

   阅读本地主机上的 `tnrhtp` 文件。该文件中的注释很有帮助。您也可以在 Solaris Management Console 中查看安全模板工具中的安全属性值。

   - 缺省模板可匹配任何安装。每个模板的标签范围为 `ADMIN_LOW` 到 `ADMIN_HIGH`。
   - `cipso` 模板定义 DOI 为 `1` 的 CIPSO 主机类型。该模板的标签范围为 `ADMIN_LOW` 到 `ADMIN_HIGH`。
   - `admin_low` 模板定义 DOI 为 `1` 的无标签主机。该模板的缺省标签为 `ADMIN_LOW`。该模板的标签范围为 `ADMIN_LOW` 到 `ADMIN_HIGH`。在缺省配置中，将地址 `0.0.0.0` 指定给此模板。因此，所有非 CIPSO 主机会被视为以 `ADMIN_LOW` 安全标签运行的主机。

2. **保留缺省模板。**

   出于支持目的，请勿删除或修改缺省模板。您可以更改已指定给这些缺省模板的主机。有关示例，请参见第 164 页中的 “如何限定可能会在可信网络上联系的主机”。

3. **如果要执行以下任一操作，请创建新模板：**

   - 限定某台主机或一组主机的标签范围。
   - 创建单标签主机。
   - 创建识别几个独立标签的主机。
   - 使用异于 `1` 的不同 DOI。
   - 需要无标签主机的非 `ADMIN_LOW` 缺省标签。

   有关详细信息，请参见第 158 页中的 “如何构造远程主机模板”。

▼ 如何打开可信网络工具

开始之前 您必须位于全局区域中，并充当可以修改网络安全设置的角色。例如，已指定信息安全或网络安全权限配置文件的角色可以修改安全设置。安全管理员角色拥有这些配置文件。

要使用 LDAP 工具箱，必须已完成《Trusted Extensions Configuration Guide》中的“Configuring the Solaris Management Console for LDAP (Task Map)”。

1. **启动 Solaris Management Console。**

   有关详细信息，请参见《Trusted Extensions Configuration Guide》中的“Initialize the Solaris Management Console Server in Trusted Extensions”。

2. **使用相应的工具。**

   - 要修改模板，请使用安全模板工具。

当前定义的所有模板会显示在右窗格中。选择或创建模板时，左窗格中会提供联机帮助。

- 要将一个主机指定给一个模板，请使用安全模板工具。
- 要创建可指定给模板的主机，请使用计算机和网络工具。
- 要将一个标签指定给一个区域，请使用可信网络区域工具。有关 Trusted Extensions 中的区域的更多信息，请参见第 10 章，在 Trusted Extensions 中管理区域（任务）。

▼ 如何构造远程主机模板

开始之前 您必须位于全局区域中，并充当可以修改网络安全设置的角色。例如，已指定信息安全或网络安全权限配置文件的角色可以修改安全设置。安全管理员角色拥有这些配置文件。

1. **在 Solaris Management Console 中，导航到安全模板工具。**

   有关步骤，请参见第 157 页中的“如何打开可信网络工具”。

2. **在 "Computers and Networks"（计算机和网络）下，双击 "Security Templates"（安全模板）。**

   现有模板将显示在 "View"（视图）窗格中。这些模板描述了此系统可以联系的主机的安全属性。这些主机包括正在运行 Trusted Extensions 的 CIPSO 主机和无标签主机。

3. **检查 `cipso` 模板。**

   查看已将该模板指定给哪些主机和哪些网络。

4. **检查 `admin_low` 模板。**

   查看已将该模板指定给哪些主机和哪些网络。

5. **创建模板。**

   如果提供的模板不能充分描述可与此系统通信的主机，请选择 "Add Template from the Action"（从操作中添加模板）菜单。

   使用联机帮助来获得帮助。在将主机指定给这些模板之前，请创建站点需要的所有模板。

6. **可选修改不是缺省模板的现有模板。**

   双击该模板，并使用联机帮助来获得帮助。您可以更改已指定的主机，也可以更改已指定的网络。

示例 13–1 创建具有不同 DOI 值的安全模板

在此示例中，安全管理员的网络具有值异于 1 的 DOI。最初配置系统的团队已完成《Trusted Extensions Configuration Guide》中的“Configure the Domain of Interpretation”。

首先，安全管理员确认 /etc/system 文件中的 DOI 值。

```
# grep doi /etc/system
set default_doi = 4
```

然后，在安全模板工具中，针对管理员创建的每个模板，将 doi 的值设置为 4。对于示例 13–2 中所述的单标签系统，安全管理员会创建以下模板：

```
template: CIPSO_PUBLIC
host_type: CIPSO
doi: 4
min_sl: PUBLIC
max_sl: PUBLIC
```

示例 13–2 创建具有单标签的安全模板

在此示例中，安全管理员要创建一个只能在单标签 PUBLIC（公共）中传递包的网关。管理员在 Solaris Management Console 中使用安全模板工具，创建一个模板并将网关主机指定给该模板。

首先，将网关主机和 IP 地址添加到计算机和网络工具。

```
gateway-1
192.168.131.75
```

然后，在安全模板工具中创建模板。模板中的值如下：

```
template: CIPSO_PUBLIC
host_type: CIPSO
doi: 1
min_sl: PUBLIC
max_sl: PUBLIC
```

该工具为 PUBLIC（公共）提供十六进制值 0X0002-08-08。

最后，按名称和 IP 地址将 gateway-1 主机指定给该模板。

```
gateway-1
192.168.131.75
```

在本地主机上，tnrhtp 项的显示类似如下：

```
cipso_public:host_type=cipso;doi=1;min_sl=0X0002-08-08;max_sl=0X0002-08-08;
```

在本地主机上，tnrhdb 项的显示类似如下：

```
# gateway-1
192.168.131.75:cipso_public
```

示例 13–3 为无标签路由器创建安全模板

任何 IP 路由器都可以通过 CIPSO 标签转发消息，即使该路由器不显式支持标签也是如此。此类无标签路由器需要一个缺省标签来定义需要在哪一个级别上处理与该路由器的连接（或许是用于路由器管理）。在此示例中，安全管理员创建一个可以任何标签转发通信的路由器，但与该路由器的所有直接通信都是以缺省标签 PUBLIC（公共）处理的。

在 Solaris Management Console 中，管理员创建一个模板并将网关主机指定给该模板。

首先，将路由器及其 IP 地址添加到计算机和网络工具。

```
router-1
192.168.131.82
```

然后，在安全模板工具中创建模板。模板中的值如下：

```
Template Name: UNL_PUBLIC
Host Type: UNLABELED
DOI: 1
Default Label: PUBLIC
Minimum Label: ADMIN_LOW
Maximum Label: ADMIN_HIGH
```

该工具为标签提供十六进制值。

最后，按名称和 IP 地址将 router-1 路由器指定给该模板。

```
router-1
192.168.131.82
```

示例 13–4 创建具有有限标签范围的安全模板

在此示例中，安全管理员要创建一个将包限定于较窄标签范围的网关。在 Solaris Management Console 中，管理员创建一个模板并将网关主机指定给该模板。

首先，将主机及其 IP 地址添加到计算机和网络工具。

```
gateway-ir
192.168.131.78
```

然后，在安全模板工具中创建模板。模板中的值如下：

```
Template Name: CIPSO_IUO_RSTRCT
Host Type: CIPSO
DOI: 1
Minimum Label: CONFIDENTIAL : INTERNAL USE ONLY
Maximum Label: CONFIDENTIAL : RESTRICTED
```

该工具为标签提供十六进制值。

最后，按名称和 IP 地址将 gateway-ir 网关指定给该模板。

```
gateway-ir
192.168.131.78
```

示例 13–5 创建具有安全标签集合的安全模板

在此示例中，安全管理员要创建一个仅识别两个标签的安全模板。在 Solaris Management Console 中，管理员创建一个模板并将网关主机指定给该模板。

首先，将每个要使用此模板的主机和 IP 地址添加到计算机和网络工具。

```
host-slset1
192.168.132.21

host-slset2
192.168.132.22

host-slset3
192.168.132.23

host-slset4
192.168.132.24
```

然后，在安全模板工具中创建模板。模板中的值如下：

```
Template Name: CIPSO_PUB_RSTRCT
Host Type: CIPSO
DOI: 1
Minimum Label: PUBLIC
Maximum Label: CONFIDENTIAL : RESTRICTED
SL Set: PUBLIC, CONFIDENTIAL : RESTRICTED
```

该工具为标签提供十六进制值。

最后，使用通配符按钮和一个前缀将 IP 地址范围指定给该模板。

```
192.168.132.0/17
```

示例 13–6 在标签 PUBLIC 上创建无标签模板

在此示例中，安全管理员允许 Oracle Solaris 系统的子网在可信网络中拥有 PUBLIC 标签。该模板具有以下值：

```
Template Name: public
Host Type: Unlabeled
Default Label: Public
Minimum Label: Public
Maximum Label: Public
```

```
DOI: 1

Wildcard Entry: 10.10.0.0
Prefix: 16
```

10.10.0.0 子网上的所有系统均在标签 PUBLIC 上进行处理。

示例 13–7 为开发者创建有标签的模板

在此示例中，安全管理员创建一个 SANDBOX（沙箱）模板。会将此模板指定给可信软件开发者所使用的系统。指定给此模板的两个系统会创建并测试带标签的程序。但是，它们的测试不会影响其他有标签系统，因为标签 SANDBOX（沙箱）与网络上的其他标签不相交。

```
Template Name: cipso_sandbox
Host Type: CIPSO
Minimum Label: SANDBOX
Maximum Label: SANDBOX
DOI: 1

Hostname: DevMachine1
IP Address: 196.168.129.129

Hostname: DevMachine2
IP Address: 196.168.129.102
```

使用这些系统的开发者可以在标签 SANDBOX（沙箱）中彼此进行通信。

▼ 如何向系统的已知网络添加主机

Solaris Management Console 中的计算机工具与 Oracle Solaris OS 中的计算机工具相同。此处提供此过程是为了便于您使用。主机已知后，您可以将这些主机指定给安全模板。

开始之前 您必须拥有可以管理网络的管理员身份。例如，拥有网络管理或系统管理员权限配置文件的角色可以管理网络。

1. **在 Solaris Management Console 中，导航到计算机工具。**
   有关详细信息，请参见第 157 页中的 “如何打开可信网络工具”。
2. **在计算机工具中，确认您要查看网络上的所有计算机。**
3. **添加此系统可能联系的主机。**
   您必须添加此系统可能联系的每台主机，包括任何静态路由器和任何审计服务器。
   a. **从 "Action"（操作）菜单中，选择 "Add Computer"（添加计算机）。**

b. 按名称和 IP 地址标识主机。

c. 可选提供有关主机的其他信息。

d. 要添加主机，请单击 "Apply"（应用）。

e. 完成各项时，单击 "OK"（确定）。

4 添加此系统可能联系的主机组。
使用联机帮助通过网络 IP 地址添加主机组。

▼ 如何将安全模板指定给向一台主机或一组主机

开始之前 您必须具有全局区域中的 "Security Administrator"（安全管理员）角色。

要指定给模板的所有主机必须在计算机和网络工具中存在。有关详细信息，请参见第 162 页中的 “如何向系统的已知网络添加主机”。

1 在 Solaris Management Console 中，导航到安全模板工具。
有关详细信息，请参见第 157 页中的 “如何打开可信网络工具”。

2 双击相应的模板名称。

3 单击 "Hosts Assigned to Template"（指定给模板的主机）选项卡。

4 要将模板指定给单台主机，请执行以下操作：

a. 在 "Hostname"（主机名）字段中，键入主机的名称。

b. 在 "IP Address"（IP 地址）字段中，键入主机的地址。

c. 单击 "Add"（添加）按钮。

d. 要保存更改，请单击 "OK"（确定）。

5 要将模板指定给具有连续地址的一组主机，请执行以下操作：

a. 单击 "Wildcard"（通配符）。

b. 在 "IP Address"（IP 地址）字段中，键入 IP 地址。

c. 在 "Prefix"（前缀）字段中，键入描述连续地址组的前缀。

d. 单击 "Add"（添加）按钮。

e. 要保存更改，请单击 "OK"（确定）。

示例 13–8 将 IPv4 网络作为通配符项添加

在以下示例中，安全管理员将多个 IPv4 子网指定给同一个安全模板。在 "Hosts Assigned to Template"（指定给模板的主机）选项卡中，管理员添加以下通配符项：

```
IP Address: 192.168.113.0
IP address: 192.168.75.0
```

示例 13–9 将 IPv4 主机列表作为通配符项添加

在以下示例中，安全管理员将不沿八位字节边界的连续 IPv4 地址指定给同一安全模板。在 "Hosts Assigned to Template"（指定给模板的主机）选项卡中，管理员添加以下通配符项：

```
IP Address: 192.168.113.100
Prefix Length: 25
```

此通配符项包含地址范围 `192.168.113.0` 到 `192.168.113.127`。该地址包括 `192.168.113.100`。

示例 13–10 将 IPv6 主机列表作为通配符项添加

在以下示例中，安全管理员将连续的 IPv6 地址指定给同一安全模板。在 "Hosts Assigned to Template"（指定给模板的主机）选项卡中，管理员添加以下通配符项：

```
IP Address: 2001:a08:3903:200::0
Prefix Length: 56
```

此通配符项包含地址范围 `2001:a08:3903:200::0` 到 `2001:a08:3903:2ff:ffff:ffff:ffff:ffff`。该地址包括 `2001:a08:3903:201:20e:cff:fe08:58c`。

▼ 如何限定可能会在可信网络上联系的主机

此过程可保护有标签主机免受任意无标签主机的联系。安装 Trusted Extensions 时，此缺省模板会定义网络上的每台主机。使用此过程可枚举特定的无标签主机。

每个系统上的本地 `tnrhdb` 文件用于在引导时联系网络。缺省情况下，未随 CIPSO 模板提供的每台主机由 `admin_low` 模板定义。此模板将未另行定义的每个系统 (`0.0.0.0`) 指定为具有 `admin_low` 缺省标签的无标签系统。

注意 – 缺省 `admin_low` 模板可能会在 Trusted Extensions 网络上造成安全风险。如果站点安全要求加强保护，安全管理员可以在安装系统后删除 `0.0.0.0` 通配符项。该项必须替换为引导期间系统联系的每台主机对应的项。

例如，在删除 `0.0.0.0` 通配符项后，DNS 服务器、起始目录服务器、审计服务器、广播和多播地址以及路由器必须在本地 `tnrhdb` 文件中。

如果应用程序最初识别主机地址 `0.0.0.0` 处的客户机，则您必须将 `0.0.0.0/32:admin_low` 主机项添加到 `tnrhdb` 数据库。例如，要接收来自潜在 Sun Ray 客户机的初始连接请求，Sun Ray 服务器必须包含此项。然后，当服务器识别客户机时，会为客户机提供 IP 地址，这些客户机会作为 CIPSO 客户机进行连接。

开始之前 您必须具有全局区域中的 "Security Administrator"（安全管理员）角色。

要在引导时联系的所有主机必须在计算机和网络工具中存在。

1. **在 Solaris Management Console 中，导航到文件作用域内的安全模板工具。**

   文件作用域可在引导期间保护系统。要访问安全模板工具，请参见第 157 页中的 “如何打开可信网络工具”。

2. **修改指定给 `admin_low` 模板的主机。**

   a. **双击 `admin_low` 模板。**

      引导期间可能会在标签 `ADMIN_LOW` 中联系所添加的每台主机。

   b. **单击 "Hosts Assigned to Template"（指定给模板的主机）选项卡。**

      引导期间可能会在标签 `ADMIN_LOW` 中联系所添加的每台主机。

   c. **添加在引导时必须联系的每台无标签主机。**

      有关详细信息，请参见第 163 页中的 “如何将安全模板指定给向一台主机或一组主机”。

      包括此主机必须通过其进行通信的、未在运行 Trusted Extensions 的每个链路上路由器。

   d. **添加在引导时必须联系的主机范围。**

   e. **删除 `0.0.0.0` 项。**

3. **修改指定给 `cipso` 模板的主机。**

   a. **双击 `cipso` 模板。**

      引导期间可能会联系所添加的每台主机。

b. **单击 "Hosts Assigned to Template"（指定给模板的主机）选项卡。**
   引导期间可能会在标签 ADMIN_LOW 中联系所添加的每台主机。

c. **添加在引导时必须联系的每台有标签主机。**
   有关详细信息，请参见第 163 页中的 “如何将安全模板指定给向一台主机或一组主机”。

   - 包括 LDAP 服务器。
   - 包括此主机必须通过其进行通信的、正在运行 Trusted Extensions 的每个链路上路由器。
   - 确保所有网络接口都已指定给模板。
   - 包括广播地址。

d. **添加在引导时必须联系的主机范围。**

4 **检验主机指定是否允许系统进行引导。**

示例 13–11 更改 0.0.0.0 tnrhdb 项的标签

在此示例中，安全管理员创建一个公共网关系统。管理员从 admin_low 模板中删除 0.0.0.0 项，并将该项指定给名为 public（公共）的无标签模板。然后，系统将未在其 tnrhdb 文件中列出的任何系统识别为具有 public（公共）安全模板的安全属性的无标签系统。

下面描述了一个专为公共网关创建的无标签模板。

```
Template Name: public
Host Type: Unlabeled
Default Label: Public
Minimum Label: Public
Maximum Label: Public
DOI: 1
```

示例 13–12 在 tnrhdb 数据库中枚举引导期间要联系的计算机

以下示例显示本地 tnrhdb 数据库，其中包含具有两个网络接口的 LDAP 客户机对应的项。该客户机与另一个网络以及一些路由器进行通信。

```
127.0.0.1:cipso           Loopback address
192.168.112.111:cipso     Interface 1 of this host
192.168.113.111:cipso     Interface 2 of this host
10.6.6.2:cipso            LDAP server
192.168.113.6:cipso       Audit server
192.168.112.255:cipso     Subnet broadcast address
192.168.113.255:cipso     Subnet broadcast address
```

```
192.168.113.1:cipso         Router
192.168.117.0:cipso         Another Trusted Extensions network
192.168.112.12:public       Specific network router
192.168.113.12:public       Specific network router
224.0.0.2:public            Multicast address
255.255.255.255:admin_low       Broadcast address
```

示例 13–13 使主机地址 0.0.0.0 成为一个有效的 tnrhdb 项

在此示例中，安全管理员配置 Sun Ray 服务器以接受来自潜在客户机的初始连接请求。该服务器使用一个专用拓扑，并在使用缺省值：

```
# utadm -a bge0
```

首先，管理员确定 Solaris Management Console 域名：

```
SMCserver # /usr/sadm/bin/dtsetup scopes
Getting list of managable scopes...
Scope 1 file:/machine1.ExampleCo.COM/machine1.ExampleCo.COM
```

然后，管理员将客户机初始连接项添加到 Sun Ray 服务器的 tnrhdb 数据库。由于管理员正在进行测试，所以缺省通配符地址仍将用于所有未知地址：

```
SunRayServer # /usr/sadm/bin/smtnrhdb \
add -D file:/machine1.ExampleCo.COM/machine1.ExampleCo.COM \
-- -w 0.0.0.0 -p 32 -n admin_low
Authenticating as user: root

Please enter a string value for: password ::
... from machine1.ExampleCo.COM was successful.
```

执行此命令之后，tnhrdb 数据库的显示类似如下。将会突出显示 smtnrhdb 命令的结果：

```
## tnrhdb database
## Sun Ray server address
       192.168.128.1:cipso
## Sun Ray client addresses on 192.168.128 network
       192.168.128.0/24:admin_low
## Initial address for new clients
       0.0.0.0/32:admin_low
## Default wildcard address
0.0.0.0:admin_low
     Other addresses to be contacted at boot
```

```
# tnchkdb -h /etc/security/tsol/tnrhdb
```

此阶段的测试成功之后，管理员通过删除缺省通配符地址使该配置更加安全，检查 tnrhdb 数据库的语法，然后再次进行测试。最终 tnhrdb 数据库的显示类似如下：

```
## tnrhdb database
## Sun Ray server address
       192.168.128.1:cipso
```

```
## Sun Ray client addresses on 192.168.128 network
       192.168.128.0/24:admin_low
## Initial address for new clients
       0.0.0.0/32:admin_low
## 0.0.0.0:admin_low - no other systems can enter network at admin_low
     Other addresses to be contacted at boot
```

在 Trusted Extensions 中配置路由并检查网络信息（ 任务列表 ）

以下任务列表介绍了配置网络以及检验配置的任务。

任务	说明	参考
配置静态路由。	手动说明从一台主机到另一台主机的最佳路由。	第 168 页中的 “如何配置具有安全属性的路由”
检查本地网络数据库的准确性。	使用 `tnchkdb` 命令检查本地网络数据库的语法有效性。	第 170 页中的 “如何检查可信网络数据库的语法”
将网络数据库项与内核高速缓存中的项进行比较。	使用 `tninfo` 命令确定是否已使用最新数据库信息更新内核高速缓存。	第 170 页中的 “如何将可信网络数据库信息与内核高速缓存进行比较”
将内核高速缓存与网络数据库进行同步。	使用 `tnctl` 命令用正在运行的系统上的最新网络数据库信息更新内核高速缓存。	第 171 页中的 “如何将内核高速缓存与可信网络数据库同步”

▼ 如何配置具有安全属性的路由

开始之前 您必须具有全局区域中的 "Security Administrator"（安全管理员）角色。

1. **添加要用于通过可信网络路由包的每个目标主机和网关。**

   地址将被添加到本地 `/etc/hosts` 文件，或添加到 LDAP 服务器上的等效项。使用 Solaris Management Console 中的计算机和网络工具。文件作用域修改 `/etc/hosts` 文件。LDAP 作用域修改 LDAP 服务器上的项。有关详细信息，请参见第 162 页中的 “如何向系统的已知网络添加主机”。

2. **将每个目标主机、网络和网关指定给安全模板。**

   地址将被添加到本地 `/etc/security/tsol/tnrhdb` 文件，或添加到 LDAP 服务器上的等效项。使用 Solaris Management Console 中的安全模板工具。有关详细信息，请参见第 163 页中的 “如何将安全模板指定给向一台主机或一组主机”。

3. **设置路由。**

   在终端窗口中，使用 `route add` 命令指定路由。

第一项设置缺省路由。该项指定在没有为主机或包目的地定义特定路由时要使用的网关地址 192.168.113.1。

```
# route add default 192.168.113.1  -static
```

有关详细信息，请参见 route(1M) 手册页。

4 **设置一个或多个网络项。**

使用 -secattr 标志指定安全属性。

在下面的命令列表中，第二行显示一个网络项。第三行显示标签范围为 PUBLIC（公共）到 CONFIDENTIAL : INTERNAL USE ONLY（机密：仅供内部使用）的网络项。

```
# route add default 192.168.113.36
# route add -net 192.168.102.0 gateway-101
# route add -net 192.168.101.0 gateway-102 \
-secattr min_sl="PUBLIC",max_sl="CONFIDENTIAL : INTERNAL USE ONLY",doi=1
```

5 **设置一个或多个主机项。**

新的第四行显示单标签主机 gateway-pub 对应的主机项。gateway-pub 的标签范围为 PUBLIC（公共）到 PUBLIC（公共）。

```
# route add default 192.168.113.36
# route add -net 192.168.102.0 gateway-101
# route add -net 192.168.101.0 gateway-102 \
-secattr min_sl="PUBLIC",max_sl="CONFIDENTIAL : INTERNAL USE ONLY",doi=1
# route add -host 192.168.101.3 gateway-pub \
-secattr min_sl="PUBLIC",max_sl="PUBLIC",doi=1
```

示例 13–14 添加标签范围为 CONFIDENTIAL : INTERNAL USE ONLY（机密：仅供内部使用）到 CONFIDENTIAL : RESTRICTED（机密：受限）的路由

以下 route 命令将 IP 地址为 192.168.115.0，网关为 192.168.118.39 的主机添加到路由表。标签范围为 CONFIDENTIAL : INTERNAL USE ONLY（机密：仅供内部使用）到 CONFIDENTIAL : RESTRICTED（机密：受限），DOI 为 1。

```
$ route add -net 192.168.115.0 192.168.118.39 \
-secattr min_sl="CONFIDENTIAL : INTERNAL USE ONLY",max_sl="CONFIDENTIAL : RESTRICTED",doi=1
```

可使用 netstat -rR 命令显示所添加主机的结果。在下面的摘录中，用省略号 (...) 代替了其他路由。

```
$ netstat -rRn
...
192.168.115.0        192.168.118.39        UG       0      0
       min_sl=CNF : INTERNAL USE ONLY,max_sl=CNF : RESTRICTED,DOI=1,CIPSO
...
```

▼ 如何检查可信网络数据库的语法

tnchkdb 命令可检查每个网络数据库的语法是否准确。在使用安全模板工具或可信网络区域工具时，Solaris Management Console 会自动运行此命令。通常，您运行此命令来检查要配置为供将来使用的数据库文件的语法。

开始之前 您必须位于全局区域中，并充当可以检查网络设置的角色。安全管理员角色和 "Security Administrator"（安全管理员）角色可以检查这些设置。

- **在终端窗口中，运行 tnchkdb 命令。**

```
$ tnchkdb [-h tnrhdb-path] [-t tnrhtp-path] [-z tnzonecfg-path]
checking /etc/security/tsol/tnrhtp ...
checking /etc/security/tsol/tnrhdb ...
checking /etc/security/tsol/tnzonecfg ...
```

示例 13–15 测试某个试用网络数据库的语法

在此示例中，安全管理员在测试一个网络数据库文件的可能用途。最初，管理员使用了错误的选项。检查的结果显示在 tnrhdb 文件的行上：

```
$ tnchkdb -h /opt/secfiles/trial.tnrhtp
checking /etc/security/tsol/tnrhtp ...
checking /opt/secfiles/trial.tnrhtp ...
line 12: Illegal name: min_sl=ADMIN_LOW;max_sl=ADMIN_HIGH
line 14: Illegal name: min_sl=ADMIN_LOW;max_sl=ADMIN_HIGH
checking /etc/security/tsol/tnzonecfg ...
```

当安全管理员使用 -t 选项检查该文件时，该命令确认试用 tnrhtp 数据库的语法准确无误：

```
$ tnchkdb -t /opt/secfiles/trial.tnrhtp
checking /opt/secfiles/trial.tnrhtp ...
checking /etc/security/tsol/tnrhdb ...
checking /etc/security/tsol/tnzonecfg ...
```

▼ 如何将可信网络数据库信息与内核高速缓存进行比较

网络数据库包含的信息可能未缓存在内核中。此过程可检查相应信息是否完全相同。使用 Solaris Management Console 更新网络时，会用网络数据库信息更新内核高速缓存。tninfo 命令在测试期间以及进行调试时很有用。

开始之前 您必须位于全局区域中，并充当可以检查网络设置的角色。安全管理员角色和 "Security Administrator"（安全管理员）角色可以检查这些设置。

- **在终端窗口中，运行 tninfo 命令。**

- `tninfo -h` *hostname* 显示指定主机的 IP 地址和模板。
- `tninfo -t` *templatename* 显示以下信息：

  ```
  template: template-name
  host_type: either CIPSO or UNLABELED
  doi: 1
  min_sl: minimum-label
  hex: minimum-hex-label
  max_sl: maximum-label
  hex:maximum-hex-label
  ```

- `tninfo -m` *zone-name* 显示区域的多级别端口 (Multilevel Port, MLP) 配置。

示例 13–16 显示主机的多级别端口

在本示例中，系统配置有多个有标签区域。所有区域共用同一 IP 地址。某些区域还配置有特定于区域的地址。在此配置中，用于 Web 浏览的 TCP 端口（端口 `8080`）是公共区域中共享接口上的一个 MLP。管理员还将 `telnet` TCP 端口 `23` 设置为公共区域中的一个 MLP。由于这两个 MLP 位于共享接口上，所以其他区域（包括全局区域）都不能在端口 `8080` 和 `23` 的共享接口上接收包。

此外，`ssh` TCP 端口（端口 `22`）是公共区域中的每区域 MLP。公共区域的 `ssh` 服务可以在地址标签范围内特定于区域的地址接收任何包。

以下命令显示公共区域的 MLP：

```
$ tninfo -m public
private: 22/tcp
shared:  23/tcp;8080/tcp
```

以下命令显示全局区域的 MLP。请注意，端口 `23` 和 `8080` 不能为全局区域中的 MLP，因为全局区域与公共区域共用同一地址。

```
$ tninfo -m global
private: 111/tcp;111/udp;514/tcp;515/tcp;631/tcp;2049/tcp;
         6000-6003/tcp;38672/tcp;60770/tcp;
shared:  6000-6003/tcp
```

▼ 如何将内核高速缓存与可信网络数据库同步

尚未用可信网络数据库信息更新内核时，您可以采用多种方式更新内核高速缓存。在使用安全模板工具或可信网络区域工具时，Solaris Management Console 会自动运行此命令。

开始之前 您必须具有全局区域中的 "Security Administrator"（安全管理员）角色。

- **要将内核高速缓存与网络数据库同步，请运行以下命令之一：**
  - **重新启动 `tnctl` 服务。**

注意 – 请勿对从 LDAP 服务器获取可信网络数据库信息的系统使用此方法。本地数据库信息将会覆盖从 LDAP 服务器获取的信息。

```
$ svcadm restart  svc:/network/tnctl
```

此命令将来自本地可信网络数据库的所有信息读入到内核中。

- **针对最近添加的项更新内核高速缓存。**

  ```
  $ tnctl -h hostname
  ```

  此命令仅将来自所选择选项的信息读入到内核中。有关选项的详细信息，请参见示例 13–17 和 `tnctl`(1M) 手册页。

- **修改 `tnd` 服务。**

  注 – `tnd` 服务仅在 `ldap` 服务运行的情况下才运行。

  - **更改 `tnd` 轮询间隔。**

    这不会更新内核高速缓存。但是，您可以缩短轮询间隔以更频繁地更新内核高速缓存。有关详细信息，请参见 `tnd`(1M) 手册页中的示例。

  - **刷新 `tnd`。**

    此服务管理工具 (Service Management Facility, SMF) 命令可出发使用对可信网络数据库进行的最近更改对内核进行立即更新。

    ```
    $ svcadm refresh svc:/network/tnd
    ```

  - **使用 SMF 重新启动 `tnd`。**

    ```
    $ svcadm restart svc:/network/tnd
    ```

注意 – 避免运行 `tnd` 命令来重新启动 `tnd`。此命令可能会中断当前成功进行的通信。

示例 13–17 使用最新的 `tnrhdb` 项更新内核

在此示例中，管理员向本地 `tnrhdb` 数据库添加了三个地址。首先，管理员删除了 `0.0.0.0` 通配符项。

```
$ tnctl -d -h 0.0.0.0:admin_low
```

接着，管理员查看 `/etc/security/tsol/tnrhdb` 数据库中最后三项的格式：

```
$ tail /etc/security/tsol/tnrhdb
#\:\:0:admin_low
```

```
127.0.0.1:cipso
#\:\:1:cipso
192.168.103.5:admin_low
192.168.103.0:cipso
0.0.0.0/32:admin_low
```

然后，管理员更新内核高速缓存：

```
$ tnctl -h 192.168.103.5
tnctl -h 192.168.103.0
tnctl -h 0.0.0.0/32
```

最后，管理员检验内核高速缓存是否已更新。第一项的输出类似如下：

```
$ tninfo -h 192.168.103.5
IP Address: 192.168.103.5
Template: admin_low
```

示例 13–18 更新内核中的网络信息

在此示例中，管理员使用公共打印服务器更新可信网络，然后检查内核设置是否正确。

```
$ tnctl -h public-print-server
$ tninfo -h public-print-server
IP Address: 192.168.103.55
Template: PublicOnly
$ tninfo -t PublicOnly
================================
Remote Host Template Table Entries
--------------------------------
template: PublicOnly
host_type: CIPSO
doi: 1
min_sl: PUBLIC
hex: 0x0002-08-08
max_sl: PUBLIC
hex: 0x0002-08-08
```

可信网络故障排除（任务列表）

以下任务列表介绍了调试网络的任务。

任务	说明	参考
确定为什么两台主机不能通信。	检查单系统上的接口是否已经启动。	第 174 页中的“如何检验主机的接口是否已启动”
	两台主机不能彼此通信时使用调试工具。	第 174 页中的“如何调试 Trusted Extensions 网络”

任务	说明	参考
确定为什么 LDAP 客户机不能访问 LDAP 服务器。	解决 LDAP 服务器和客户机之间的连接丢失问题。	第 177 页中的 “如何调试客户机与 LDAP 服务器的连接”

▼ 如何检验主机的接口是否已启动

如果您的系统不能按预期方式与其他主机进行通信，请使用此过程。

开始之前 您必须位于全局区域中，并充当可以检查网络设置的角色。安全管理员角色和 "Security Administrator"（安全管理员）角色可以检查这些设置。

1. **检验系统的网络接口是否已启动。**

   以下输出结果显示该系统有两个网络接口，即 `hme0` 和 `hme0:3`。两个接口都未启动。

   ```
   # ifconfig -a
   ...
   hme0: flags=1000843<BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
            inet 192.168.0.11 netmask ffffff00 broadcast 192.168.0.255
   hme0:3 flags=1000843<BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
            inet 192.168.0.12 netmask ffffff00 broadcast 192.168.0.255
   ```

2. **如果接口未启动，请使其启动，然后检验其是否已启动。**

   以下输出结果显示两个接口都已启动。

   ```
   # ifconfig hme0 up
   # ifconfig -a
   ...
   hme0: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,...
   hme0:3 flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,..
   ```

▼ 如何调试 Trusted Extensions 网络

要调试两台应当进行通信但未进行通信的主机，您可以使用 Trusted Extensions 和 Solaris 调试工具。例如，提供了诸如 `snoop` 和 `netstat` 之类的 Oracle Solaris 网络调试命令。有关详细信息，请参见 `snoop(1M)` 和 `netstat(1M)` 手册页。有关特定于 Trusted Extensions 的命令，请参见表 2–4。

- 有关联系有标签区域的问题，请参见第 113 页中的 “管理区域（任务列表）”。
- 有关调试 NFS 挂载的信息，请参见第 139 页中的 “如何解决 Trusted Extensions 中的挂载故障”。
- 有关调试 LDAP 通信的信息，请参见第 177 页中的 “如何调试客户机与 LDAP 服务器的连接”。

开始之前 您必须位于全局区域中，并充当可以检查网络设置的角色。安全管理员角色或 "Security Administrator"（安全管理员）角色可以检查这些设置。

1 **要排除 tnd 守护进程故障，请更改轮询间隔并收集调试信息。**

注 – tnd 服务仅在 ldap 服务运行的情况下才运行。

有关详细信息，请参见 tnd(1M) 手册页。

2 **检查无法通信的主机是否正在使用同一命名服务。**

a. **在每台主机上，检查 nsswitch.conf 文件。**

i. **检查 nsswitch.conf 文件中 Trusted Extensions 数据库的值。**

例如，在使用 LDAP 管理网络的站点上，相应的项类似如下：

```
# Trusted Extensions
tnrhtp: files ldap
tnrhdb: files ldap
```

ii. **如果值不同，请更正 nsswitch.conf 文件。**

要修改这些项，系统管理员可使用 "Name Service Switch"（名称服务转换）操作。有关详细信息，请参见第 51 页中的 “如何在 Trusted Extensions 中启动 CDE 管理操作”。此操作会保留所需的 DAC 和 MAC 文件权限。

b. **检查是否已配置 LDAP 命名服务。**

```
$ ldaplist -l
```

c. **检查两台主机是否都位于 LDAP 命名服务中。**

```
$ ldaplist -l hosts | grep hostname
```

3 **检查是否正确定义了每台主机。**

a. **使用 Solaris Management Console 检验这些定义。**

- 在安全模板工具中，检查每台主机是否都已指定给与其他主机的安全模板兼容的安全模板。
- 对于无标签系统，检查缺省标签指定是否正确。
- 在可信网络区域工具中，检查是否已经正确配置多级别端口 (Multilevel Port, MLP)。

b. **使用命令行检查内核中的网络信息是否为最新。**

检查每台主机内核高速缓存中的指定是否与网络上以及其他主机上的分配相匹配。

要在传输过程中获取源主机、目标主机和网关主机的安全信息，请使用 tninfo 命令。

- **显示给定主机的 IP 地址和所指定的安全模板。**

  ```
  $ tninfo -h hostname
  IP Address: IP-address
  Template: template-name
  ```

- **显示模板定义。**

  ```
  $ tninfo -t template-name
  template: template-name
  host_type: one of CIPSO or UNLABELED
  doi: 1
  min_sl: minimum-label
  hex: minimum-hex-label
  max_sl: maximum-label
  hex: maximum-hex-label
  ```

- **显示区域的 MLP。**

  ```
  $ tninfo -m zone-name
  private: ports-that-are-specific-to-this-zone-only
  shared: ports-that-the-zone-shares-with-other-zones
  ```

4 修复任何不正确的信息。

- 要更改或检查网络安全信息，请使用 Solaris Management Console 工具。有关详细信息，请参见第 157 页中的“如何打开可信网络工具”。
- 要更新内核高速缓存，请在信息已过时的主机上重新启动 tnctl 服务。留出一些时间以允许此进程完成。然后，刷新 tnd 服务。如果刷新失败，请尝试重新启动 tnd 服务。有关详细信息，请参见第 171 页中的“如何将内核高速缓存与可信网络数据库同步”。

注 – tnd 服务仅在 ldap 服务运行的情况下才运行。

重新引导会清除内核高速缓存。在引导时，会使用数据库信息置备高速缓存。nsswitch.conf 文件确定是使用本地数据库还是 LDAP 数据库置备内核。

5 收集传输信息以帮助您进行调试。

- **检验您的路由配置。**

  使用 route 命令的 get 子命令。

  ```
  $ route get [ip] -secattr sl=label,doi=integer
  ```

  有关详细信息，请参见 route(1M) 手册页。

- **查看包中的标签信息。**

  使用 `snoop -v` 命令。

  `-v` 选项显示包标头的详细信息，包括标签信息。此命令提供大量详细信息，因此您可能需要限定此命令检查的包。有关详细信息，请参见 snoop(1M) 手册页。

- **查看路由表项和套接字的安全属性。**

  在 `netstat -a|-r` 命令中使用 `-R` 选项。

  `-aR` 选项显示套接字的扩展安全属性。`-rR` 选项显示路由表项。有关详细信息，请参见 netstat(1M) 手册页。

▼ 如何调试客户机与 LDAP 服务器的连接

在 LDAP 服务器上错误配置客户机项可能会妨碍客户机与服务器进行通信。同样，在客户机上错误配置文件可能会妨碍通信。尝试调试客户机/服务器通信问题时，请检查以下项和文件。

开始之前 在 LDAP 客户机上，您必须充当全局区域中的安全管理员角色。

1. **检查 LDAP 服务器以及 LDAP 服务器网关所对应的远程主机模板是否正确。**

   ```
   # tninfo -h LDAP-server
   # route get LDAP-server
   # tninfo -h gateway-to-LDAP-server
   ```

   如果远程主机模板指定不正确，请使用 Solaris Management Console 中的安全模板工具将主机指定给正确的模板。

2. **检查并更正 `/etc/hosts` 文件。**

   您的系统、系统上有标签区域的接口、LDAP 服务器的网关和 LDAP 服务器必须列在该文件中。可能还会有更多项。

   查找重复的项。删除其他系统上属于有标签区域的任何项。例如，如果 `Lserver` 是 LDAP 服务器的名称，`LServer-zones` 是有标签区域的共享接口，请从 `/etc/hosts` 中删除 `LServer-zones`。

3. **如果您在使用 DNS，请检查并更正 `resolv.conf` 文件中的项。**

   ```
   # more resolv.conf
   search list of domains
   domain domain-name
   nameserver IP-address

   ...
   nameserver IP-address
   ```

4. **检查 `nsswitch.conf` 文件中的 `tnrhdb` 和 `tnrhtp` 项是否准确。**

5 检查是否在服务器上正确配置了客户机。

```
# ldaplist -l tnrhdb client-IP-address
```

6 检查是否在 LDAP 服务器上正确配置了有标签区域的接口。

```
# ldaplist -l tnrhdb client-zone-IP-address
```

7 检验您是否可以从当前运行的所有区域 `ping` LDAP 服务器。

```
# ldapclient list
...
NS_LDAP_SERVERS= LDAP-server-address
# zlogin zone-name1 ping LDAP-server-address
LDAP-server-address is alive
# zlogin zone-name2 ping LDAP-server-address
LDAP-server-address is alive
...
```

8 配置 LDAP 并重新引导。

a. 有关过程，请参见《 Trusted Extensions Configuration Guide 》中的“Make the Global Zone an LDAP Client in Trusted Extensions”。

b. 在每个有标签区域中，将区域重建为 LDAP 服务器的客户机。

```
# zlogin zone-name1
# ldapclient init \
-a profileName=profileName \
-a domainName=domain \
-a proxyDN=proxyDN \
-a proxyPassword=password  LDAP-Server-IP-Address
# exit
# zlogin zone-name2 ...
```

c. 停止所有区域，锁定文件系统，然后重新引导。

如果您在使用 Oracle Solaris ZFS，请先停止区域并锁定文件系统，然后再重新引导。如果未在使用 ZFS，您可以在不停止区域和锁定文件系统的情况下重新引导。

```
# zoneadm list
# zoneadm -z zone-name halt
# lockfs -fa
# reboot
```

◆ ◆ ◆ 第 14 章

Trusted Extensions 中的多级别邮件（概述）

本章介绍了配置有 Trusted Extensions 的系统上的安全和多级别邮件程序。

多级别邮件服务

Trusted Extensions 可为任何邮件应用程序提供多级别邮件。一般用户启动其邮件程序时，应用程序将以用户的当前标签打开。如果用户在多级别系统中操作，他们可能要链接或复制其邮件程序初始化文件。有关详细信息，请参见第 81 页中的 “如何在 Trusted Extensions 中为用户配置启动文件”。

Trusted Extensions 邮件功能

在 Trusted Extensions 中，"System Administrator"（系统管理员）角色根据 Oracle Solaris 的《系统管理指南：高级管理》和《Oracle Solaris 管理：IP 服务》中的说明设置和管理邮件服务器。此外，安全管理员确定需要如何配置 Trusted Extensions 邮件功能。

以下几个方面的邮件管理特定于 Trusted Extensions：

- `.mailrc` 文件处于用户的最小标签。

  因此，以多个标签工作的用户在较高级别标签没有 `.mailrc` 文件，除非将最小标签目录中的 `.mailrc` 文件复制或链接到各个较高目录中。

  安全管理员角色或各个用户可以将 `.mailrc` 文件添加到 `.copy_files` 或 `.link_files`。有关这些文件的说明，请参见 `updatehome(1M)` 手册页。有关配置建议，请参见第 76 页中的 “`.copy_files` 和 `.link_files` 文件”。
- 邮件阅读器可以在系统上以每个标签运行。需要执行一些配置来将邮件客户端连接到服务器。

例如，要将 Mozilla 邮件用于多级别邮件，您需要以每个标签配置 Mozilla 邮件客户端以指定邮件服务器。每个标签的邮件服务器可以相同或不同，但必须指定服务器。

- Solaris Management Console 中的 "Mailing Lists"（邮件列表）工具用于管理邮件别名。

  根据所选的 Solaris Management Console 工具箱作用域，您可以更新本地的 `/etc/aliases` 文件或 Oracle Directory Server Enterprise Edition 上的 LDAP 条目。

- Trusted Extensions 软件先检查主机和用户标签，然后才发送或转发邮件。
  - 该软件检查邮件是否在主机的认可范围内。此列表和第 13 章，在 Trusted Extensions 中管理网络（任务）中介绍了这些检查。
  - 该软件检查邮件是否在帐户的安全许可和最小标签之间。
  - 用户可以阅读在其认可范围内接收的电子邮件。在一个会话期间，用户只能以其当前标签阅读邮件。

    要通过电子邮件联系一般用户，管理角色必须从用户可以阅读的标签的工作区中发送邮件。用户的缺省标签通常是上佳选择。

◆ ◆ ◆ 第 15 章

管理有标签打印（任务）

本章介绍如何使用 Trusted Extensions 软件配置有标签打印。它还介绍如何配置没有标签设置选项的打印作业。

标签、打印机和打印

Trusted Extensions 软件使用标签来控制打印机访问。标签用于控制对打印机的访问以及对有关已排队打印作业的信息的访问。该软件还对已打印的输出进行标记。为正文页设置标签，并为必需的标题页和篇尾页设置标签。标题页和篇尾页还可以包含处理说明。

系统管理员处理基本的打印机管理。安全管理员角色管理打印机安全，这包括标签和有标签输出的处理方式。这些管理员按照基本的 Oracle Solaris 打印机管理过程进行操作，然后他们为打印服务器和打印机指定标签。

Trusted Extensions 软件同时支持单级别打印和多级别打印。多级别打印仅在全局区域中实现。要使用全局区域的打印服务器，有标签区域必须具有与全局区域不同的主机名称。获取不同主机名称的一种方法是，为有标签区域指定 IP 地址。该地址应与全局区域的 IP 地址不同。

在 Trusted Extensions 中限制对打印机和打印作业信息的访问

使用 Trusted Extensions 软件配置的系统上的用户和角色以其会话的标签创建打印作业。打印作业只能在识别该标签的打印机上打印。标签必须处于打印机的标签范围内。

用户和角色可以查看其标签与会话标签相同的打印作业。在全局区域中，角色可以查看其标签由区域标签控制的作业。

使用 Trusted Extensions 软件配置的打印机在打印机输出上打印标签。由无标签打印服务器管理的打印机不在打印机输出上打印标签。这样的打印机具有与其无标签服务器相同的标签。例如，可以在 LDAP 命名服务的 `tnrhdb` 数据库中为 Oracle Solaris 打印服务器指定任意标签。用户然后可以在 Oracle Solaris 打印机上打印该任意标签的作业。与 Trusted Extensions 打印机一样，那些 Oracle Solaris 打印机只能从按照已指定给打印机服务器的标签工作的用户那里接受打印作业。

有标签的打印机输出

Trusted Extensions 在正文页以及标题页和篇尾页上打印安全信息。该信息来自 `label_encodings` 文件和 `tsol_separator.ps` 文件。

安全管理员可以执行以下操作，以修改用于设置标签和向打印机输出添加处理指令的缺省设置：

- 本地化或定制标题页和篇尾页上的文本
- 指定要在正文页上或标题页和篇尾页的各个字段中打印的替代标签
- 更改或忽略任何文本或标签

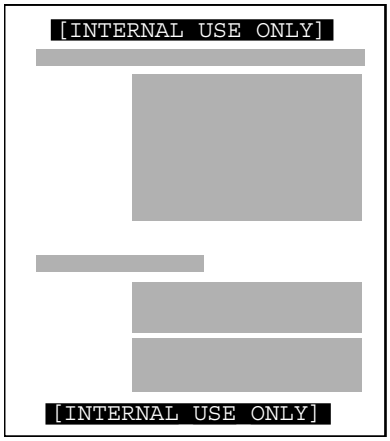
安全管理员还可以配置用户帐户以使用不在输出上打印标签的打印机。也可以授权用户有选择地不在打印机输出上打印标题或标签。

有标签正文页

缺省情况下，在每个正文页的顶部和底部打印 "Protect As"（保护为）等级。当来自作业标签的等级与 `minimum protect as classification` 进行比较时，"Protect As"（保护为）等级是主要的等级。`minimum protect as classification` 在 `label_encodings` 文件中定义。

例如，如果用户登录到 "Internal Use Only"（仅供内部使用）会话，则该用户的打印作业使用该标签。如果 `label_encodings` 文件中的 `minimum protect as classification` 为 "Public"（公共），则在正文页上打印 "Internal Use Only"（仅供内部使用）标签。

图 15–1 在正文页顶部和底部打印的作业标签



有标签的标题页和篇尾页

下图显示了缺省标题页以及缺省篇尾页的不同之处。标注将对各部分进行标识。请注意，篇尾页使用不同的外线。

打印作业上显示的文本、标签和警告是可配置的。也可以使用其他语言的文本替换此文本以进行本地化。

图 15–2 有标签打印作业的典型标题页

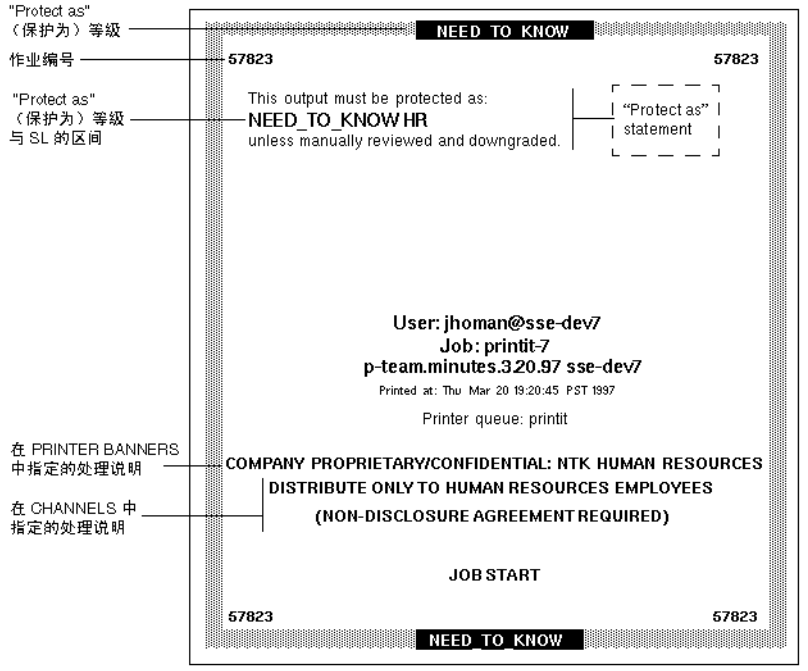
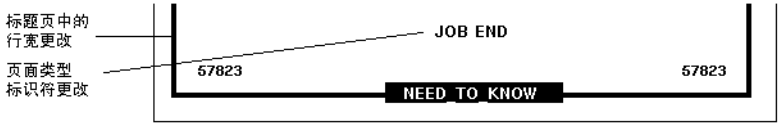


图 15–3 篇尾页的差别



下表显示了安全管理员可通过修改 `/usr/lib/lp/postscript/tsol_separator.ps`文件进行更改的可信打印的各个方面。

注 – 要本地化或国际化已打印的输出，请参见 `tsol_separator.ps` 文件中的注释。

表 15–1 tsol_separator.ps 文件中的可配置值

输出	缺省值	如何定义	更改
PRINTER BANNERS	/Caveats Job_Caveats	/Caveats Job_Caveats	请参见《Trusted Extensions Label Administration》中的“Specifying Printer Banners”。
CHANNELS	/Channels Job_Channels	/Channels Job_Channels	请参见《Trusted Extensions Label Administration》中的“Specifying Channels”。
标题页和篇尾页顶部的标签	/HeadLabel Job_Protect def	请参见 /PageLabel 说明。	与更改 /PageLabel 相同。 另请参见《Trusted Extensions Label Administration》中的“Specifying the Protect As Classification”。
正文页顶部和底部的标签	/PageLabel Job_Protect def	比较作业标签和 label_encodings 文件中的 minimum protect as 等级。打印处于较高支配地位的等级。 如果打印作业的标签有区间，则包含区间。	更改 /PageLabel 定义以指定其他值。 或者，键入您选择的字符串。 或者，不打印任何内容。
"Protect as"（保护为）等级语句中的文本和标签	/Protect Job_Protect def /Protect_Text1 () def /Protect_Text2 () def	请参见 /PageLabel 说明。 标签上方显示的文本。 标签下方显示的文本。	与更改 /PageLabel 相同。 将 Protect_Text1 和 Protect_Text2 中的 () 替换为文本字符串。

安全信息的 PostScript 打印

Trusted Extensions 中有标签的打印依赖于 Solaris 打印中的功能。在 Oracle Solaris OS 中，打印机型号脚本处理标题页的创建。要实现标记，打印机型号脚本首先将打印作业转换为 PostScript 文件。然后，对 PostScript 文件进行处理，在正文页上插入标签以及创建标题页和篇尾页。

Solaris 打印机型号脚本还可以将 PostScript 转换为打印机的本机语言。如果打印机接受 PostScript 输入，则 Oracle Solaris 软件会将作业发送到打印机。如果打印机不接受 PostScript 输入，则软件将 PostScript 格式转换为光栅图像。然后将光栅图像转换为适当的打印机格式。

由于 PostScript 软件用于打印标签信息，因此缺省情况下用户无法打印 PostScript 文件。此限制可防止知识渊博的 PostScript 程序员创建用于修改打印机输出上标签的 PostScript 文件。

安全管理员角色可以通过将 Print Postscript 授权指定给角色帐户和值得信任的用户来覆盖此限制。仅当可以信任帐户不会对打印机输出上的标签进行电子欺骗时才指定授权。此外，允许用户打印 PostScript 文件必须与站点的安全策略一致。

打印机型号脚本

打印机型号脚本使特定型号的打印机可以提供标题页和篇尾页。Trusted Extensions 提供了以下四个脚本：

- tsol_standard－用于直接连接的 PostScript 打印机，例如通过并行端口连接的打印机
- tsol_netstandard－用于网络可访问的 PostScript 打印机
- tsol_standard_foomatic－用于不打印 PostScript 格式的直接连接的打印机
- tsol_netstandard_foomatic－用于不打印 PostScript 格式的网络可访问的打印机

当打印机驱动程序名称以 Foomatic 开头时，会使用 foomatic 脚本。Foomatic 驱动程序是 PostScript 打印机驱动程序 (PostScript Printer Driver, PPD)。

注 – 将打印机添加到有标签区域时，缺省情况下在 "Print Manager"（打印管理器）中指定 "Use PPD"（使用 PPD）。然后使用 PPD 将标题页和篇尾页转换为打印机语言。

其他转换过滤器

转换过滤器将文本文件转换为 PostScript 格式。过滤器的程序是由打印机守护进程运行的可信程序。可以信任由已安装的任何过滤器程序转换为 PostScript 格式的文件已具有真实的标签以及标题页和篇尾页文本。

Oracle Solaris 软件提供了站点需要的大多数转换过滤器。站点的 "Security Administrator"（安全管理员）角色可以安装其他过滤器。然后可以信任这些过滤器已具有真实的标签以及标题页和篇尾页。要添加转换过滤器，请参见《System Administration Guide: Printing》中的第 7 章 “Customizing LP Printing Services and Printers (Tasks)”。

Trusted Extensions 与 Trusted Solaris 8 打印的互操作性

具有兼容的 label_encodings 文件且将彼此识别为使用 CIPSO 模板的 Trusted Solaris 8 和 Trusted Extensions 系统可以互相使用以进行远程打印。下表介绍了如何设置系统以允许打印。缺省情况下，用户无法列出或取消其他 OS 的远程打印服务器上的打印作业。（可选）可以授权用户这样做。

源系统	打印服务器系统	操作	结果
Trusted Extensions	Trusted Solaris 8	配置打印—在 Trusted Extensions `tnrhdb` 中，为 Trusted Solaris 8 打印服务器指定具有适当标签范围的模板。标签可能是 CIPSO 或无标签。	Trusted Solaris 8 打印机可以从 Trusted Extensions 系统打印处于打印机的标签范围内的作业。
Trusted Extensions	Trusted Solaris 8	授权用户－在 Trusted Extensions 系统上，创建一个添加所需授权的配置文件。为用户指定该配置文件。	Trusted Extensions 用户可以列出或取消他们发送到 Trusted Solaris 8 打印机的打印作业。 用户无法查看或删除不同标签的作业。
Trusted Solaris 8	Trusted Extensions	配置打印—在 Trusted Solaris 8 `tnrhdb` 中，为 Trusted Extensions 打印服务器指定具有适当标签范围的模板。标签可能是 CIPSO 或无标签。	Trusted Extensions 打印机可以从 Trusted Solaris 8 系统打印处于打印机的标签范围内的作业。
Trusted Solaris 8	Trusted Extensions	授权用户－在 Trusted Solaris 8 系统上，创建一个添加所需授权的配置文件。为用户指定该配置文件。	Trusted Solaris 8 用户可以列出或取消他们发送到 Trusted Extensions 打印机的打印作业。 用户无法查看或删除不同标签的作业。

Trusted Extensions 打印界面（参考信息）

扩展了以下用户命令以符合 Trusted Extensions 安全策略：

- `cancel`－调用者必须等于打印作业的标签才能取消作业。缺省情况下，一般用户只能取消自己的作业。
- `lp`－Trusted Extensions 添加 `-o nolabels` 选项。用户必须有权在没有标签的情况下打印。同样，用户必须有权使用 `-o nobanner` 选项。
- `lpstat`－调用者必须等于打印作业的标签才能获取作业的状态。缺省情况下，一般用户只能查看自己的打印作业。

扩展了以下管理命令以符合 Trusted Extensions 安全策略。在 Oracle Solaris OS 中，这些命令只能由包含 "Printer Management"（打印机管理）权限配置文件的角色运行。

- `lpmove` – 调用者必须等于打印作业的标签才能移动作业。缺省情况下，一般用户只能移动他们自己的打印作业。
- `lpadmin` – 在全局区域中，此命令适用于所有作业。在有标签区域中，调用者必须支配打印作业的标签才能查看作业，必须等于该标签才能更改作业。

  Trusted Extensions 将打印机型号脚本添加到 `-m` 选项。Trusted Extensions 添加 `-o nolabels` 选项。
- `lpsched` – 在全局区域中，此命令始终会成功。在 Oracle Solaris OS 中，使用 `svcadm` 命令来启用、禁用、启动或重新启动打印服务。在有标签区域中，调用者必须等于打印服务的标签才能更改打印服务。有关服务管理工具的详细信息，请参见 `smf(5)`、`svcadm(1M)` 和 `svcs(1)` 手册页。

Trusted Extensions 将 `solaris.label.print` 授权添加到打印机管理权限配置文件。需要有 `solaris.print.unlabeled` 授权才能打印没有标签的正文页。

在 Trusted Extensions 中管理打印（任务列表）

在完成 Oracle Solaris 打印机设置之后，执行配置打印的 Trusted Extensions 过程。以下任务列表提供了指向负责管理有标签打印的主要任务的链接。

任务	说明	参考
为有标签的输出配置打印机。	使用户可以打印到 Trusted Extensions 打印机。已用标签标记打印作业。	第 188 页中的 “配置有标签打印（任务列表）”
从打印机输出中删除可见的标签。	使用户可以在特定的标签打印到 Oracle Solaris 打印机。未用标签标记打印作业。 或者，阻止标签在 Trusted Extensions 打印机上打印。	第 200 页中的 “在 Trusted Extensions 中减少打印限制（任务列表）”

配置有标签打印（任务列表）

以下任务列表介绍了与有标签打印相关的常见配置过程。

注 – 打印机客户机只能打印处于 Trusted Extensions 打印服务器的标签范围内的作业。

任务	说明	参考
从全局区域配置打印。	在全局区域中创建多级别打印服务器。	第 189 页中的 “如何配置多级别打印服务器及其打印机”

任务	说明	参考
为系统网络配置打印。	在全局区域中创建多级别打印服务器，并使有标签区域可以使用打印机。	第 191 页中的“如何为 Sun Ray 客户机配置网络打印机”
在与有标签系统相同的子网中为无标签系统配置打印。	使无标签系统可以使用网络打印机。	第 194 页中的“如何在有标签系统上配置级联打印”
从有标签区域配置打印。	为有标签区域创建单标签打印服务器。	第 196 页中的“如何为单标签打印配置区域”
配置多级别打印客户机。	将 Trusted Extensions 主机连接到打印机。	第 198 页中的“如何允许 Trusted Extensions 客户机访问打印机”
限制打印机的标签范围。	将 Trusted Extensions 打印机限制为很窄的标签范围。	第 199 页中的“如何为打印机配置受限制的标签范围”

▼ 如何配置多级别打印服务器及其打印机

由 Trusted Extensions 打印服务器管理的打印机会在正文页、标题页和篇尾页上打印标签。这样的打印机可以打印处于打印机服务器的标签范围内的作业。可以访问打印服务器的任何 Trusted Extensions 主机都可以使用连接到该服务器的打印机。

开始之前 确定 Trusted Extensions 网络的打印服务器。您必须承担此打印机服务器上全局区域中的 "Security Administrator"（安全管理员）角色。

1. **启动 Solaris Management Console。**

   有关详细信息，请参见第 50 页中的“如何使用 Solaris Management Console 管理本地系统”。

2. **选择 "Files"（文件）工具箱。**

   工具箱的标题包括 `Scope=Files, Policy=TSOL`。

3. **通过使用打印服务器端口 515/tcp 配置全局区域，启用多级别打印。**

   通过将一个多级别端口 (Multilevel Port, MLP) 添加到全局区域，为打印服务器创建该端口。

   a. **导航到 "Trusted Network Zones"（可信网络区域）工具。**

   b. **在 "Multilevel Ports for Zone's IP Addresses"（区域 IP 地址的多级别端口）中，添加 515/tcp。**

   c. **单击 "OK"（确定）。**

4 **定义所连接的每个打印机的特征。**

使用命令行。"Print Manager"（打印管理器）GUI 在全局区域中不起作用。

```
# lpadmin -p printer-name -v /dev/null \
-o protocol=tcp -o dest=printer-IP-address:9100 -T PS -I postscript
# accept printer-name
# enable printer-name
```

5 **为连接到打印服务器的每个打印机指定打印机型号脚本。**

型号脚本将激活指定打印机的标题页和篇尾页。

有关脚本的说明，请参见第 186 页中的 “打印机型号脚本”。如果打印机的驱动程序名称以 Foomatic 开头，则指定其中一个 foomatic 型号脚本。在一行上，使用以下命令：

```
$ lpadmin -p printer \
 -m { tsol_standard | tsol_netstandard |
      tsol_standard_foomatic | tsol_netstandard_foomatic }
```

如果 ADMIN_LOW 到 ADMIN_HIGH 的缺省打印机标签范围是每个打印机可接受的，则标签配置已完成。

6 **在允许打印的每个有标签区域中，配置打印机。**

将全局区域的 all-zones IP 地址用作打印服务器。

a. **以 root 身份登录到有标签区域的区域控制台。**

```
# zlogin -C labeled-zone
```

b. **向该区域添加打印机。**

```
# lpadmin -p printer-name -s all-zones-IP-address
```

c. **可选将打印机设置为缺省打印机。**

```
# lpadmin -d printer-name
```

7 **在每个区域中，测试打印机。**

注 – 从 Solaris 10 7/10 发行版开始，具有管理标签 ADMIN_HIGH 或 ADMIN_LOW 的文件在打印输出的正文上打印 ADMIN_HIGH。会使用 label_encodings 文件中的最高级别标签和区间为标题页和篇尾页设置标签。

以 root 身份和一般用户身份，执行以下步骤：

a. **从命令行打印纯文本文件。**

b. **从应用程序（如 Beehive）、浏览器和编辑器打印文件。**

c. **验证标题页、篇尾页和安全标题是否正确打印。**

另请参见
- **限制打印机标签范围** – 第 199 页中的“如何为打印机配置受限制的标签范围”
- **阻止有标签的输出** – 第 200 页中的“在 Trusted Extensions 中减少打印限制（任务列表）”
- **将此区域用作打印服务器** – 第 198 页中的“如何允许 Trusted Extensions 客户机访问打印机”

▼ 如何为 Sun Ray 客户机配置网络打印机

此过程在具有单个 `all-zones` 接口的 Sun Ray 服务器上配置 PostScript 打印机。使打印机变为可供此服务器的 Sun Ray 客户机的所有用户使用。初始配置发生在全局区域中。配置全局区域后，将每个有标签区域配置为使用打印机。

开始之前 您必须登录到 Trusted CDE 中的多级别会话。

1. **在全局区域中，为网络打印机指定 IP 地址。**
   有关说明，请参见《System Administration Guide: Printing》中的第 5 章 “Setting Up Printers by Using LP Print Commands (Tasks)”。

2. **启动 Solaris Management Console。**
   - 有关说明，请参见《Trusted Extensions Configuration Guide》中的“Initialize the Solaris Management Console Server in Trusted Extensions”。
   - 选择 `Scope=Files, Policy=TSOL` 工具箱并登录。

3. **为 `admin_low` 模板指定打印机。**
   a. **在 "Computers and Networks"（计算机和网络）工具中，双击 "Security Templates"（安全模板）。**
   b. **双击 `admin_low`。**
   c. **在 "Hosts Assigned to Template"（为模板指定的主机）选项卡中，添加打印机的 IP 地址。**
      有关更多信息，请阅读左窗格中的联机帮助。

4. **将打印机端口添加到全局区域的共享接口。**
   a. **在 "Computers and Networks"（计算机和网络）工具中，双击 "Trusted Network Zones"（可信网络区域）。**
   b. **双击 `global`。**

c. **在 "Multilevel Ports for Shared IP Addresses"（共享 IP 地址的多级别端口）列表中，添加端口 515、协议 tcp。**

5 **验证 Solaris Management Console 指定的内容是否在内核中。**

```
# tninfo -h printer-IP-address
   IP address= printer-IP-address
   Template = admin_low

# tninfo -m global
   private: 111/tcp;111/udp;513/tcp;515/tcp;631/tcp;2049/tcp;6000-6050/tcp;
7007/tcp;7010/tcp;7014/tcp;7015/tcp;32771/tcp;32776/ip
   shared: 515/tcp;6000-6050/tcp;7007/tcp;7010/tcp;7014/tcp;7015/tcp
```

注 – 其他专用和共享多级别端口 (Multilevel Port, MLP)（如 6055 和 7007）支持 Sun Ray 要求。

---

6 **确认在全局区域中启用了打印服务。**

```
# svcadm enable print/server
# svcadm enable rfc1179
```

7 **如果系统是使用 netservices limited 安装的，请允许打印机访问网络。**

rfc1179 服务必须侦听除 localhost 之外的地址。LP 服务仅侦听指定管道。

```
# inetadm -m svc:/application/print/rfc1179:default bind_addr=''
# svcadm refresh rfc1179
```

注 – 如果正在运行 netservices open，则前面的命令将生成以下错误：`"Error: "inetd" property group missing"`（**错误：**`"inetd"` **属性组缺失**）。

---

8 **使所有用户可以打印 PostScript。**

在可信编辑器中，创建 /etc/default/print 文件并添加以下行：

```
PRINT_POSTSCRIPT=1
```

诸如 Beehive 之类的应用程序以及 gedit 将创建 PostScript 输出。

9 **将所有 LP 过滤器添加到打印服务。**

在全局区域中，运行此 C Shell 脚本：

```
csh
    cd /etc/lp/fd/
    foreach a (*.fd)
        lpfilter -f $a:r -F $a
    end
```

10 **在全局区域中添加打印机。**

使用命令行。"Print Manager"（打印管理器）GUI 在全局区域中不起作用。

```
# lpadmin -p printer-name -v /dev/null -m tsol_netstandard \
-o protocol=tcp -o dest=printer-IP-address:9100 -T PS -I postscript
```

```
# accept printer-name
# enable printer-name
```

11 可选将打印机设置为缺省打印机。

```
# lpadmin -d printer-name
```

12 在每个有标签区域中，配置打印机。

将全局区域的 `all-zones` IP 地址用作打印服务器。如果 `all-zones` NIC 是虚拟网络接口 (virtual network interface , vni)，请将 vni 的 IP 地址用作 `-s` 选项的参数。

a. 以 root 身份登录到有标签区域的区域控制台。

```
# zlogin -C labeled-zonename
```

b. 向该区域添加打印机。

```
# lpadmin -p printer-name -s global-zone-shared-IP-address
```

c. 可选将打印机设置为缺省打印机。

```
# lpadmin -d printer-name
```

13 在每个区域中，测试打印机。

注 – 从 Solaris 10 7/10 发行版开始，具有管理标签 `ADMIN_HIGH` 或 `ADMIN_LOW` 的文件在打印输出的正文上打印 `ADMIN_HIGH`。会使用 `label_encodings` 文件中的最高级别标签和区间为标题页和篇尾页设置标签。

以 `root` 身份和一般用户身份，执行以下步骤：

a. 从命令行打印纯文本文件。

b. 从应用程序（如 Beehive）、浏览器和编辑器打印文件。

c. 验证标题页、篇尾页和安全标题是否正确打印。

示例 15–1 确定网络打印机的打印机状态

在此示例中，管理员从全局区域和有标签区域验证网络打印机的状态。

```
global # lpstat -t
    scheduler is running
    system default destination: math-printer
    system for _default: trusted1 (as printer math-printer)
    device for math-printer: /dev/null
    character set
    default accepting requests since Feb 28 00:00 2008
    lex accepting requests since Feb 28 00:00 2008
    printer math-printer is idle. enabled since Feb 28 00:00 2008. available.
```

```
Solaris1# lpstat -t
   scheduler is not running
   system default destination: math-printer
   system for _default: 192.168.4.17 (as printer math-printer)
   system for math-printer: 192.168.4.17
   default accepting requests since Feb 28 00:00 2008
   math-printer accepting requests since Feb 28 00:00 2008
   printer _default is idle. enabled since Feb 28 00:00 2008. available.
   printer math-printer is idle. enabled since Feb 28 00:00 2008. available.
```

▼ 如何在有标签系统上配置级联打印

级联打印提供了从 Windows 桌面会话到 Trusted Extensions 有标签区域接口的打印功能，其中物理接口的区域 IP 地址充当打印假脱机程序。位于物理接口的区域 IP 地址上的多级别端口 (Multilevel Port, MLP) 侦听器与 Trusted Extensions 打印子系统进行通信，并打印具备适当的有标签标题表单和篇尾表单的文件。

此过程使与有标签系统位于同一子网中的有标签系统可以使用有标签的网络打印机。`rfc1179` 服务处理级联打印。必须在允许级联打印的每个有标签区域中执行此过程。

开始之前 至此已完成第 191 页中的“如何为 Sun Ray 客户机配置网络打印机”。

1. **以 root 身份登录到有标签区域的区域控制台。**

   ```
   # zlogin -C labeled-zonename
   ```

2. **取消 `rfc1179` 服务与打印/服务器服务的相关性。**

   ```
   labeled-zone # cat <<EOF | svccfg
         select application/print/rfc1179
         delpg lpsched
         end
      EOF

   labeled-zone # svcadm refresh application/print/rfc1179
   ```

3. **确保启用了 `rfc1179` 服务。**

   ```
   labeled-zone # svcadm enable rfc1179
   ```

4. **如果有标签区域是使用 `netservices limited` 安装的，请允许打印机访问网络。**

   `rfc1179` 服务必须侦听除 `localhost` 之外的地址。LP 服务仅侦听指定管道。

   ```
   # inetadm -m svc:/application/print/rfc1179:default bind_addr=''
   # svcadm refresh rfc1179
   ```

注 – 如果正在运行 `netservices open`，则前面的命令将生成以下消息：`"Error: "inetd" property group missing"`（**错误：**`"inetd"` **属性组缺失**）。

5 从有标签区域配置级联打印。

labeled-zone `#` `lpset -n system -a spooling-type=cascade` *printer-name*

此命令将更新区域的 `/etc/printers.conf` 文件。

6 测试与该标签区域位于同一子网上的 Oracle Solaris 系统。

例如，测试 `Solaris1` 系统。此系统与 `internal` 区域位于同一子网上。配置参数如下所示：

- `math-printer` IP 地址是 192.168.4.6
- `Solaris1` IP 地址是 192.168.4.12
- `internal` 区域 IP 地址是 192.168.4.17

```
Solaris1# uname -a
SunOS Solaris1 Generic_120011-11 sun4u sparc SUNW,Sun-Blade-1000
Solaris1# lpadmin -p math-printer -s 192.168.4.17
Solaris1# lpadmin -d math-printer

Solaris1# lpstat -t
   scheduler is not running
   system default destination: math-printer
   system for _default: 192.168.4.17 (as printer math-printer)
   system for math-printer: 192.168.4.17
   default accepting requests since Feb 28 00:00 2008
   math-printer accepting requests since Feb 28 00:00 2008
   printer _default is idle. enabled since Feb 28 00:00 2008. available.
   printer math-printer is idle. enabled since Feb 28 00:00 2008. available.
```

- **测试 `lp` 命令。**

  ```
  Solaris1# lp /etc/hosts
     request id is math-printer-1 (1 file)
  ```

- **从应用程序（如 Beehive）和浏览器测试打印。**

7 测试与该有标签区域位于同一子网上的 Windows 2003 服务器。

a. 在 Windows 服务器上设置打印机。

使用 "Start"（开始）菜单 -> "Settings"（设置）-> "Printers & Faxes GUI"（打印机和传真 GUI）。

指定以下打印机配置：

- "Add A Printer"（添加打印机）
- "Local Printer attached to this computer"（连接到此计算机的本地打印机）
- "Create a new port"（创建新端口）－标准 TCP/IP 端口

- "Printer Name or IP Address"（打印机名称或 IP 地址）－192.168.4.17，即有标签区域的 IP 地址
- "Port Name"（端口名称）－接受缺省值
- "Additional Port Information Required"（所需的其他端口信息）－接受缺省值
  - "Device Type"（设备类型）= "Custom"（定制）
  - "Settings – Protocol"（设置 - 协议）= LPR
  - "LPR Settings – Queue Name"（LPR 设置 - 队列名称)= math-printer，即 UNIX 队列名称
  - "LPR Byte Counting Enabled"（LPR 字节计数已启用）

通过指定制造商、型号、驱动程序和其他打印机参数来完成打印机提示。

8 通过从应用程序中选择打印机来测试打印机。

例如，测试与 `internal` 区域位于同一子网上的 `winserver` 系统。配置参数如下所示：

- `math-printer` IP 地址是 192.168.4.6
- `winserver` IP 地址是 192.168.4.200
- `internal` 区域 IP 地址是 192.168.4.17

```
winserver C:/> ipconfig
Windows IP Configuration
   Ethernet adapter TP-NIC:
      Connection-specific DNS Suffix  . :
      IP Address. . . . . . . . . . . . : 192.168.4.200
      Subnet Mask . . . . . . . . . . . : 255.255.255.0
      Default Gateway . . . . . . . . . : 192.168.4.17
```

▼ 如何为单标签打印配置区域

开始之前 区域不得与全局区域共享 IP 地址。您必须具有全局区域中的 "System Administrator"（系统管理员）角色。

1 添加工作区。

有关详细信息，请参见《Trusted Extensions User's Guide》中的"How to Add a Workspace at a Particular Label"。

2 将新工作区的标签更改为将作为该标签的打印服务器的区域的标签。

有关详细信息，请参见《Trusted Extensions User's Guide》中的"How to Change the Label of a Workspace"。

3 **定义所连接的打印机的特征。**

a. **在区域的标签，启动 "Print Manager"（打印管理器）。**

缺省情况下，"Use PPD"（使用 PPD）复选框处于选中状态。系统为打印机查找适当的驱动程序。

b. **可选要指定其他打印机驱动程序，请执行以下操作：**

i. **移除 "Use PPD"（使用 PPD）的复选标记。**

ii. **定义使用其他驱动程序的打印机的品牌和型号。**

在 "Print Manager"（打印管理器）中，您提供前两个字段的值后，"Print Manager"（打印管理器）将提供驱动程序名称。

```
Printer Make        manufacturer
Printer Model       manufacturer-part-number
Printer Driver      automatically filled in
```

4 **为连接到区域的每个打印机指定打印机型号脚本。**

型号脚本将激活指定打印机的标题页和篇尾页。

有关脚本的选择，请参见第 186 页中的 “打印机型号脚本”。如果打印机的驱动程序名称以 `Foomatic` 开头，则指定其中一个 foomatic 型号脚本。使用以下命令：

```
$ lpadmin -p printer -m model
```

已连接的打印机只能打印区域标签的作业。

5 **测试打印机。**

注 – 从 Solaris 10 7/10 发行版开始，具有管理标签 `ADMIN_HIGH` 或 `ADMIN_LOW` 的文件在打印输出的正文上打印 `ADMIN_HIGH`。会使用 `label_encodings` 文件中的最高级别标签和区间为标题页和篇尾页设置标签。

以 `root` 身份和一般用户身份，执行以下步骤：

a. **从命令行打印纯文本文件。**

b. **从应用程序（如 Beehive）、浏览器和编辑器打印文件。**

c. **验证标题页、篇尾页和安全标题是否正确打印。**

另请参见 **阻止有标签的输出 —** 第 200 页中的 “在 Trusted Extensions 中减少打印限制（任务列表）”

▼ 如何允许 Trusted Extensions 客户机访问打印机

最初，只有在其中配置打印服务器的区域才可以打印到该打印服务器的打印机。系统管理员必须为其他区域和系统显式添加对那些打印机的访问。可能性如下所示：

- 对于全局区域，添加对连接到其他系统上全局区域的打印机的访问。
- 对于有标签区域，添加对连接到其系统的全局区域的打印机的访问。
- 对于有标签区域，添加对为其配置同一标签远程区域的打印机的访问。
- 对于有标签区域，添加对连接到其他系统上全局区域的打印机的访问。

开始之前 打印服务器已配置有标签范围或单个标签，且连接到它的打印机已进行配置。有关详细信息，请参见以下内容：

- 第 189 页中的 “如何配置多级别打印服务器及其打印机”
- 第 196 页中的 “如何为单标签打印配置区域”
- 第 202 页中的 “如何为无标签的打印服务器指定标签”

您必须承担全局区域中的 "Security Administrator"（安全管理员）角色，或者能够承担该角色。

1 完成允许系统访问打印机的过程。

- **对不是打印服务器的系统上的全局区域进行配置，使其使用其他系统的全局区域访问打印机。**

  a. 在无法访问打印机的系统上，承担 "Security Administrator"（安全管理员）角色。

  b. 添加对连接到 Trusted Extensions 打印服务器的打印机的访问。

  ```
  $ lpadmin -s printer
  ```

- **将有标签区域配置为使用其全局区域访问打印机。**

  a. 将角色工作区的标签更改为有标签区域的标签。

  有关详细信息，请参见《Trusted Extensions User's Guide》中的“How to Change the Label of a Workspace”。

  b. 添加对打印机的访问。

  ```
  $ lpadmin -s printer
  ```

- **将有标签区域配置为使用其他系统的有标签区域访问打印机。**

  各区域的标签必须完全相同。

  a. 在无法访问打印机的系统上，承担 "Security Administrator"（安全管理员）角色。

b. 将角色工作区的标签更改为有标签区域的标签。

有关详细信息，请参见《Trusted Extensions User's Guide》中的"How to Change the Label of a Workspace"。

c. 添加对连接到远程有标签区域的打印服务器的打印机的访问。

```
$ lpadmin -s printer
```

- **将有标签区域配置为使用无标签打印服务器访问打印机。**

  区域的标签必须与打印服务器的标签完全相同。

  a. 在无法访问打印机的系统上，承担 "Security Administrator"（安全管理员）角色。

  b. 将角色工作区的标签更改为有标签区域的标签。

  有关详细信息，请参见《Trusted Extensions User's Guide》中的"How to Change the Label of a Workspace"。

  c. 添加对连接到任意有标签打印服务器的打印机的访问。

  ```
  $ lpadmin -s printer
  ```

2 测试打印机。

从 Solaris 10 7/10 发行版开始，具有管理标签 ADMIN_HIGH 或 ADMIN_LOW 的文件将在打印输出的正文上打印 ADMIN_HIGH。会使用 label_encodings 文件中的最高级别标签和区间为标题页和篇尾页设置标签。

在每个客户机上，测试全局区域中的 root 和角色以及有标签区域中的 root、角色和一般用户是否可以打印。

a. 从命令行打印纯文本文件。

b. 从应用程序（如 Beehive）、浏览器和编辑器打印文件。

c. 验证标题页、篇尾页和安全标题是否正确打印。

▼ 如何为打印机配置受限制的标签范围

缺省的打印机标签范围为 ADMIN_LOW 到 ADMIN_HIGH。此过程缩小了由 Trusted Extensions 打印服务器控制的打印机的标签范围。

开始之前 您必须具有全局区域中的 "Security Administrator"（安全管理员）角色。

1. 启动 "Device Allocation Manager"（设备分配管理器）。
   - 从 "Trusted Path"（可信路径）菜单中选择 "Allocate Device"（分配设备）选项。
   - 在 Trusted CDE 中，从前面板上的 "Tools"（工具）子面板启动 "Device Allocation Manager"（设备分配管理器）操作。
2. 单击 "Device Administration"（设备管理）按钮以显示 "Device Allocation: Administration"（设备分配：管理）对话框。
3. 为新打印机键入名称。
   如果打印机已连接到系统，则查找打印机的名称。
4. 单击 "Configure"（配置）按钮以显示 "Device Allocation: Configuration"（设备分配：配置）对话框。
5. 更改打印机的标签范围。
   a. 单击 "Min Label"（最小标签）按钮以更改最小标签。
      从标签生成器中选择一个标签。有关标签生成器的信息，请参见第 40 页中的 “Trusted Extensions 中的标签生成器”。
   b. 单击 "Max Label"（最大标签）按钮以更改最大标签。
6. 保存更改。
   a. 在 "Configuration"（配置）对话框中单击 "OK"（确定）。
   b. 在 "Administration"（管理）对话框中单击 "OK"（确定）。
7. 关闭 "Device Allocation Manager"（设备分配管理器）。

在 Trusted Extensions 中减少打印限制（任务列表）

以下任务是可选的。它们降低了 Trusted Extensions 软件在安装时缺省提供的打印安全性。

任务	说明	参考
将打印机配置为不对输出进行标记。	防止在正文页上打印安全信息，并删除标题页和篇尾页。	第 201 页中的 “如何从已打印的输出删除标签”

任务	说明	参考
在没有带标签输出的情况下，在单个标签下配置打印机。	使用户可以在特定的标签打印到 Oracle Solaris 打印机。未用标签标记打印作业。	第 202 页中的 “如何为无标签的打印服务器指定标签”
删除正文页的可见标签。	修改 `tsol_separator.ps` 文件以阻止从 Trusted Extensions 主机发送的所有打印作业上的有标签正文页。	第 202 页中的 “如何从所有打印作业中删除页标签”
隐藏标题页和篇尾页。	授权特定用户打印没有标题页和篇尾页的作业。	第 203 页中的 “如何为特定用户隐藏标题页和篇尾页”
使可信用户可以打印没有标签的作业。	授权特定系统的特定用户或所有用户打印无标签作业。	第 203 页中的 “如何使特定用户可以隐藏页标签”
启用 PostScript 文件打印。	授权特定系统的特定用户或所有用户打印 PostScript 文件。	第 204 页中的 “如何使用户可以在 Trusted Extensions 中打印 PostScript 文件”
指定打印授权。	使用户可以跳过缺省打印限制。	第 86 页中的 “如何创建权限配置文件以实现方便的授权” 第 80 页中的 “如何修改 `policy.conf` 缺省值”

▼ 如何从已打印的输出删除标签

没有 Trusted Extensions 打印机型号脚本的打印机不打印有标签的标题页或篇尾页。正文页也不包括标签。

开始之前 您必须具有全局区域中的 "Security Administrator"（安全管理员）角色。

- **在适当的标签，执行以下操作之一：**
  - **从打印服务器，完全停止标题打印。**

    ```
    $ lpadmin -p printer -o nobanner=never
    ```

    仍为正文页设置标签。
  - **将打印机型号脚本设置为 Oracle Solaris 脚本。**

    ```
    $ lpadmin -p printer  \
    -m { standard | netstandard | standard_foomatic | netstandard_foomatic }
    ```

    在已打印的输出上将不出现标签。

▼ 如何为无标签的打印服务器指定标签

Oracle Solaris 打印服务器是无标签的打印服务器，可以为其指定一个标签，以便 Trusted Extensions 能够以该标签访问打印机。连接到无标签打印服务器的打印机只能打印已经指定给打印服务器的标签的作业。打印的作业没有标签或篇尾页，并可能没有标题页。如果打印的作业具有标题页，则该页将不包含任何安全信息。

可以将 Trusted Extensions 系统配置为将作业提交到由无标签打印服务器管理的打印机。用户可以在安全管理员为打印服务器所指定标签的无标签打印机上打印作业。

开始之前 您必须具有全局区域中的 "Security Administrator"（安全管理员）角色。

1. **在适当的作用域中打开 Solaris Management Console。**

   有关详细信息，请参见《Trusted Extensions Configuration Guide》中的“Initialize the Solaris Management Console Server in Trusted Extensions”。

2. **在 "System Configuration"（系统配置）下，导航到 "Computers and Networks"（计算机和网络）工具。**

   在出现提示时提供口令。

3. **为打印服务器指定无标签的模板。**

   有关详细信息，请参见第 163 页中的 “如何将安全模板指定给向一台主机或一组主机”。

   选择一个标签。以该标签工作的用户可以将打印作业发送到打印服务器标签的 Oracle Solaris 打印机。打印的页没有标签，且标题页和篇尾页也不是打印作业的一部分。

示例 15–2 将公共打印作业发送到无标签的打印机

对普通公众可用的文件适合打印到无标签的打印机。在此示例中，市场材料的编写人员需要生成在页面顶部和底部上不打印标签的文档。

安全管理员为 Oracle Solaris 打印服务器指定无标签主机类型模板。在示例 13–6 中对该模板进行了介绍。模板的任意标签是 `PUBLIC`（公共）。打印机 `pr-nolabel1` 已连接到此打印服务器。来自 `PUBLIC`（公共）区域中用户的打印作业在 `pr-nolabel1` 打印机上打印，且没有标签。根据打印机的设置，作业可能具有也可能没有标题页。标题页不包含安全信息。

▼ 如何从所有打印作业中删除页标签

此过程可防止 Trusted Extensions 打印机上的所有打印作业在打印作业的正文页上包括可见标签。

开始之前 您必须具有全局区域中的 "Security Administrator"（安全管理员）角色。

1. **编辑 `/usr/lib/lp/postscript/tsol_separator.ps` 文件。**
   请使用可信编辑器。有关详细信息，请参见第 52 页中的 “如何在 Trusted Extensions 中编辑管理文件”。

2. **查找 `/PageLabel` 的定义。**
   查找以下行：

   ```
   %% To eliminate page labels completely, change this line to
   %% set the page label to an empty string: /PageLabel () def
   /PageLabel Job_PageLabel def
   ```

   注 – 值 `Job_PageLabel` 在您的站点上可能有所不同。

3. **将 `/PageLabel` 的值替换为一对空括号。**

   ```
   /PageLabel () def
   ```

▼ 如何使特定用户可以隐藏页标签

此过程使授权用户或角色可以在 Trusted Extensions 打印机上打印作业，但每个正文页的顶部和底部都没有标签。对用户可以在其上工作的所有标签均隐藏其页标签。

开始之前 您必须具有全局区域中的 "Security Administrator"（安全管理员）角色。

1. **确定允许谁打印没有页标签的作业。**

2. **授权那些用户和角色打印没有页标签的作业。**
   为那些用户和角色指定包括 "Print without Label"（无标签打印）授权的权限配置文件。有关详细信息，请参见第 86 页中的 “如何创建权限配置文件以实现方便的授权”。

3. **指示用户或角色使用 `lp` 命令提交打印作业：**

   ```
   % lp -o nolabels staff.mtg.notes
   ```

▼ 如何为特定用户隐藏标题页和篇尾页

开始之前 您必须具有全局区域中的 "Security Administrator"（安全管理员）角色。

1. **创建包括 "Print without Banner"（无标题打印）授权的权限配置文件。**
   将该配置文件指定给允许在没有标题页和篇尾页的情况下打印的每个用户或角色。

   有关详细信息，请参见第 86 页中的 “如何创建权限配置文件以实现方便的授权”。

2. **指示用户或角色使用 `lp` 命令提交打印作业：**

   ```
   % lp -o nobanner staff.mtg.notes
   ```

▼ 如何使用户可以在 Trusted Extensions 中打印 PostScript 文件

开始之前 您必须具有全局区域中的 "Security Administrator"（安全管理员）角色。

- **使用以下三种方法之一，使用户可以打印 PostScript 文件：**
  - **要在系统上启用 PostScript 打印，请修改 `/etc/default/print` 文件。**
    a. **创建或修改 `/etc/default/print` 文件。**
       请使用可信编辑器。有关详细信息，请参见第 52 页中的 “如何在 Trusted Extensions 中编辑管理文件”。
    b. **键入以下条目：**
       ```
       PRINT_POSTSCRIPT=1
       ```
    c. **保存文件并关闭编辑器。**
  - **要授权所有用户从系统打印 PostScript 文件，请修改 `/etc/security/policy.conf` 文件。**
    a. **修改 `policy.conf` 文件。**
       请使用可信编辑器。有关详细信息，请参见第 52 页中的 “如何在 Trusted Extensions 中编辑管理文件”。
    b. **添加 `solaris.print.ps` 授权。**
       ```
       AUTHS_GRANTED=other-authorizations,solaris.print.ps
       ```
    c. **保存文件并关闭编辑器。**
  - **要使用户或角色可以从任何系统打印 PostScript 文件，请仅为这些用户和角色提供适当的授权。**
    将包括 `Print Postscript` 授权的配置文件指定给这些用户和角色。有关详细信息，请参见第 86 页中的 “如何创建权限配置文件以实现方便的授权”。

示例 15–3 从公共系统启用 PostScript 打印

在以下示例中，安全管理员已将公共资讯服务站约束为以 `PUBLIC` 标签操作。系统还具有几个用于打开感兴趣主题的图标。可以打印这些主题。

安全管理员在系统上创建了 `/etc/default/print` 文件。该文件具有一个启用 PostScript 文件打印的条目。没有用户需要 `Print Postscript` 授权。

```
# vi /etc/default/print

# PRINT_POSTSCRIPT=0
PRINT_POSTSCRIPT=1
```

◆ ◆ ◆ 第 16 章

Trusted Extensions 中的设备（概述）

本章介绍了 Trusted Extensions 为设备保护功能提供的扩展。

通过 Trusted Extensions 软件提供的设备保护

在 Oracle Solaris 系统上，可通过分配和授权机制来保护设备。缺省情况下，一般用户无需获得授权即可访问设备。配置有 Trusted Extensions 功能的系统采用 Oracle Solaris OS 的设备保护机制。

但是，缺省情况下，Trusted Extensions 要求设备在分配后才能使用并且用户获得授权后才能使用设备。此外，设备还受标签保护。Trusted Extensions 为管理员提供了用来管理设备的图形用户界面 (Graphical User Interface, GUI)。用户也使用该界面来分配设备。

注 – 在 Trusted Extensions 中，用户无法使用 `allocate` 和 `deallocate` 命令。用户必须使用 "Device Allocation Manager"（设备分配管理器）。在 Solaris Trusted Extensions (JDS) 中，该 GUI 的标题为 "Device Manager"（设备管理器）。

有关 Oracle Solaris 中的设备保护的信息，请参见《System Administration Guide: Security Services》中的第 4 章 “Controlling Access to Devices (Tasks)”。

在配置有 Trusted Extensions 的系统中，由两个角色进行设备保护。

- "System Administrator"（系统管理员）角色控制对外围设备的访问。

  系统管理员使设备成为可分配的。系统管理员使之不可分配的设备不能被任何人使用。可分配的设备只能由经授权的用户进行分配。

- "Security Administrator"（安全管理员）角色限制可以在哪些标签访问设备并设置设备策略。安全管理员决定向哪个用户授予分配设备的权限。

Trusted Extensions 软件提供的设备控制机制的主要特征如下：

- 缺省情况下，Trusted Extensions 系统中未经授权的用户不能分配如磁带机、CD-ROM 驱动器、磁盘驱动器等设备。

  具有 "Allocate Device"（分配设备）授权的一般用户可以在用户分配设备的标签导入或导出信息。
- 直接登录后，用户可调用 "Device Allocation Manager"（设备分配管理器）来分配设备。要远程分配设备，用户必须具有对全局区域的访问权限。通常情况下，只有角色具有对全局区域的访问权限。
- 安全管理员可对每个设备的标签范围进行限制。一般用户只能访问设备标签范围中包括允许用户使用的标签的设备。缺省的设备标签范围为 `ADMIN_LOW` 到 `ADMIN_HIGH`。
- 对于可分配的设备和不可分配的设备，都可对其标签范围进行限制。不可分配的设备包括帧缓存器和打印机等等。

设备标签范围

为防止用户复制敏感信息，每个可分配的设备都有一个标签范围。要使用某个可分配的设备，用户当前必须在设备标签范围内的某个标签工作。否则，用户不能分配设备。当设备被分配到用户时，用户的当前标签应用于导入或导出的数据。当设备被取消分配时，会显示导出数据的标签。用户必须以物理方式为包含导出数据的介质设置标签。

标签范围对设备的影响

为限制通过控制台进行直接登录访问，安全管理员可以在帧缓存器上设置一个限制性的标签范围。

例如，可以指定一个限制性的标签范围来限制对公众可访问系统的访问。标签范围可确保用户只能在帧缓存器标签范围中的标签访问系统。

如果主机具有一台本地打印机，则打印机上的限制性标签范围可以限制能够在该打印机上打印的作业。

设备访问策略

Trusted Extensions 遵循与 Oracle Solaris 一样的设备策略。安全管理员可以更改缺省策略或定义新策略。`getdevpolicy` 命令用于检索设备策略信息，`update_drv` 命令用于更改

设备策略。有关更多信息，请参见《System Administration Guide: Security Services》中的“Configuring Device Policy (Task Map)”。另请参见 getdevpolicy(1M) 和 update_drv(1M) 手册页。

Device-Clean（设备清除）脚本

当分配或取消分配设备时，会运行一个 device-clean（设备清除）脚本。Oracle Solaris 提供了用于磁带机、CD-ROM 驱动器和磁盘驱动器的脚本。如果在您的站点中向系统添加了可分配的设备类型，所添加的设备可能需要这些脚本。要查看现有的脚本，请转到 /etc/security/lib 目录。有关更多信息，请参见《System Administration Guide: Security Services》中的“Device-Clean Scripts”。

对于 Trusted Extensions 软件，device-clean（设备清除）脚本必须满足特定的要求。device_clean(5) 手册页中描述了这些要求。

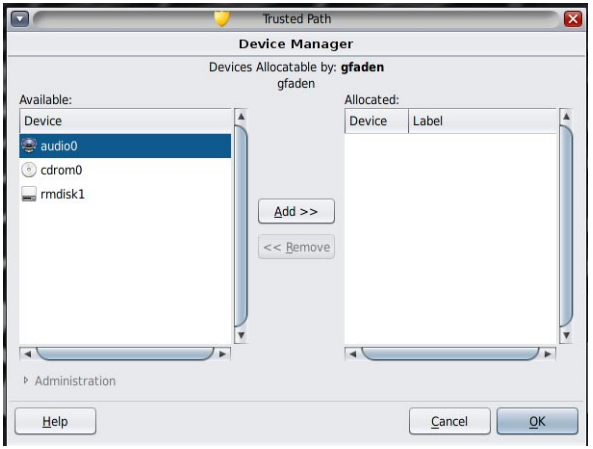
"Device Allocation Manager"（设备分配管理器）GUI

"Device Allocation Manager"（设备分配管理器）供管理员用来管理可分配的设备和不可分配的设备。一般用户也可使用 "Device Allocation Manager"（设备分配管理器）来分配和取消分配设备。前提是这些用户必须具有 "Allocate Device"（分配设备）授权。在 Solaris Trusted Extensions (CDE) 工作区中，可从前面板打开 "Device Allocation Manager"（设备分配管理器）。图标显示如下：

设备分配 

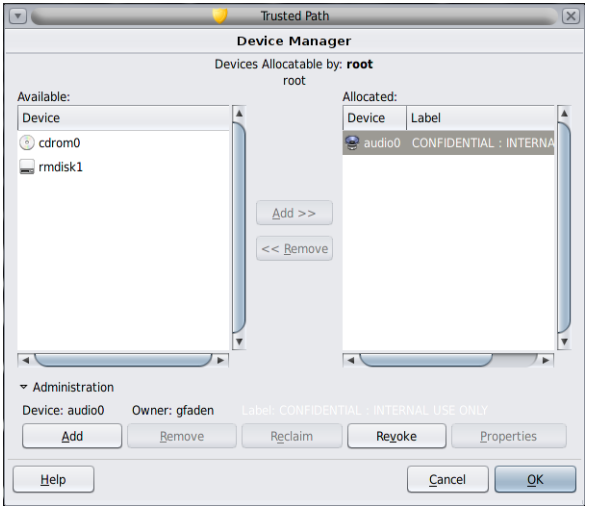
在 Solaris Trusted Extensions (JDS) 工作区中，该 GUI 的名称为 "Device Manager"（设备管理器）。可以通过从 "Trusted Path"（可信路径）菜单选择 "Allocate Device"（分配设备）来启动该 GUI。在 Trusted CDE 中，也可以从 "Trusted Path"（可信路径）菜单启动该 GUI。下图显示了由可以分配**音频**设备的用户打开的 "Device Allocation Manager"（设备分配管理器）GUI。

图 16–1 用户打开的 "Device Allocation Manager"（设备分配管理器）GUI



如果用户没有被授予分配设备权限，则他们看到的是一个空列表。另外，空列表也可能表明可分配的设备当前已由另一用户分配或处于错误状态。如果用户在 "Available"（可用）设备列表中没有找到设备，请与相关管理员联系。

"Device Administration"（设备管理）功能可供拥有对设备进行管理所需的一个或两个（即全部）授权的角色使用。管理授权包括 "Configure Device Attributes"（配置设备属性）和 "Revoke or Reclaim Device"（撤销或回收设备）。下图显示了 "Device Allocation Administration"（设备分配管理）对话框。



在 Solaris Trusted Extensions (JDS) 中，"Device Administration"（设备管理）按钮的名称为 "Administration"（管理）。

Trusted Extensions 中的设备安全保障

安全管理员决定哪些用户可以分配设备并确保被授权使用设备的用户经过培训。管理员确信该用户可以完成以下任务：

- 正确地标记和处理包含导出敏感信息的任何介质，确保这些信息不会被不应看到这些信息的任何人使用。

  例如，如果磁盘中存储的信息的标签为 `NEED TO KNOW ENGINEERING`，则导出信息的人员必须以物理方式为磁盘添加 `NEED TO KNOW ENGINEERING` 标签。该磁盘必须存放在只有需要获悉相关信息的工程组成员能够访问的位置。
- 确保为从这些设备中的介质导入（读取）的信息正确地维护标签。

  经授权用户必须在与要被导入的信息的标签匹配的标签分配设备。例如，如果用户分配了一个标签为 `PUBLIC` 的磁盘驱动器，则用户必须仅导入标签为 `PUBLIC` 的信息。

安全管理员还要负责强制用户遵守这些安全要求。

Trusted Extensions 中的设备（参考信息）

Trusted Extensions 设备保护功能使用 Oracle Solaris 接口和 Trusted Extensions 接口。

有关 Oracle Solaris 命令行接口的信息，请参见《System Administration Guide: Security Services》中的“Device Protection (Reference)”。

不能访问 "Device Allocation Manager"（设备分配管理器）的管理员可以通过使用命令行来管理可分配的设备。`allocate` 和 `deallocate` 命令具有管理选项。有关示例，请参见《System Administration Guide: Security Services》中的“Forcibly Allocating a Device”和《System Administration Guide: Security Services》中的“Forcibly Deallocating a Device”。

有关 Trusted Extensions 命令行接口的信息，请参见 `add_allocatable(1M)` 和 `remove_allocatable(1M)` 手册页。

◆ ◆ ◆ 第 17 章

管理 Trusted Extensions 的设备（任务）

本章介绍了如何在配置有 Trusted Extensions 的系统上管理和使用设备。

在 Trusted Extensions 中操作设备（任务列表）

以下任务列表中提供了相应链接，这些链接指向管理员和用户用于操作外围设备的任务列表。

任务	说明	参考
使用设备。	以某个角色或一般用户的身份使用设备。	第 214 页中的 “在 Trusted Extensions 中使用设备（任务列表）”
管理设备。	为一般用户配置设备。	第 214 页中的 “在 Trusted Extensions 中管理设备（任务列表）”
定制设备授权。	"Security Administrator"（安全管理员）角色创建新授权、将它们添加到设备、将它们置于一个权限配置文件中并将该配置文件指定给用户。	第 223 页中的 “在 Trusted Extensions 中定制设备授权（任务列表）”

在 Trusted Extensions 中使用设备（任务列表）

在 Trusted Extensions 中，所有角色都有权分配设备。与用户类似，角色必须使用 "Device Allocation Manager"（设备分配管理器）。Oracle Solaris 的 `allocate` 命令在 Trusted Extensions 中无法使用。以下任务列表中提供了相应链接，这些链接指向用于在 Trusted Extensions 中使用设备的用户过程。

任务	参考
分配和取消分配设备。	《Trusted Extensions User's Guide》中的"How to Allocate a Device in Trusted Extensions" 《Trusted Extensions User's Guide》中的"Workspace Switch Area"
使用便携介质传输文件。	《Trusted Extensions Configuration Guide》中的"How to Copy Files From Portable Media in Trusted Extensions" 《Trusted Extensions Configuration Guide》中的"How to Copy Files to Portable Media in Trusted Extensions"

在 Trusted Extensions 中管理设备（任务列表）

以下任务列表描述了在您的站点上保护设备的过程。

任务	说明	参考
设置或修改设备策略。	更改访问设备所需的特权。	《System Administration Guide: Security Services》中的"Configuring Device Policy (Task Map)"
授予用户分配设备的授权。	"Security Administrator"（安全管理员）角色将包含 "Allocate Device"（分配设备）授权的权限配置文件指定给用户。	《System Administration Guide: Security Services》中的"How to Authorize Users to Allocate a Device"
	"Security Administrator"（安全管理员）角色将包含特定于站点的授权的配置文件指定给用户。	第 223 页中的 "在 Trusted Extensions 中定制设备授权（任务列表）"
配置设备。	选择安全功能来保护设备。	第 215 页中的 "如何在 Trusted Extensions 中配置设备"

任务	说明	参考
撤销或回收设备。	使用 "Device Allocation Manager"（设备分配管理器）使设备可供用户使用。	第 218 页中的“如何在 Trusted Extensions 中撤销或回收设备”
	使用 Oracle Solaris 命令使设备可供用户使用或使其不可供用户使用。	《System Administration Guide: Security Services》中的“Forcibly Allocating a Device” 《System Administration Guide: Security Services》中的“Forcibly Deallocating a Device”
阻止访问可分配设备。	提供对设备的细粒度访问控制。	示例 17–4
	拒绝所有人访问可分配设备。	示例 17–1
保护打印机和帧缓存器。	确保不可分配的设备不可分配。	第 219 页中的“如何在 Trusted Extensions 中保护不可分配的设备”
配置串行登录设备。	启用通过串行端口的登录。	第 220 页中的“如何配置用于登录的串行线路”
使 CD 播放器程序可供使用。	使音频播放器程序在插入音乐 CD 时自动打开。	第 221 页中的“如何在 Trusted CDE 中配置音频播放器程序以便使用”
阻止 "File Manager"（文件管理器）显示。	阻止在已分配某个设备后显示 "File Manager"（文件管理器）。	第 222 页中的“如何阻止在分配设备后显示 "File Manager"（文件管理器）”
使用新的 device-clean（设备清除）脚本。	将新脚本放置在合适的位置。	第 223 页中的“如何在 Trusted Extensions 中添加 Device_Clean （设备清除）脚本”

▼ 如何在 Trusted Extensions 中配置设备

缺省情况下，可分配设备的标签范围是从 `ADMIN_LOW` 到 `ADMIN_HIGH`，并且必须在分配后才可使用。另外，用户必须获得授权才能分配设备。这些缺省值是可以更改的。

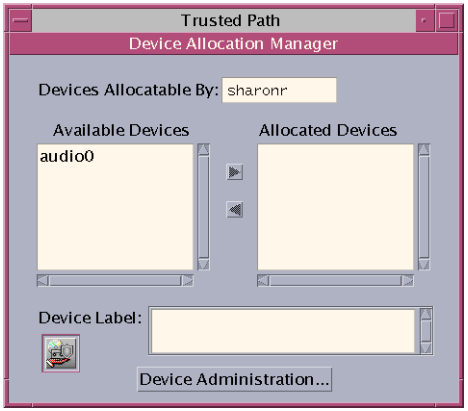
以下设备可供分配使用：

- `audio`*n*－指示麦克风和扬声器
- `cdrom`*n*－指示 CD-ROM 驱动器
- `floppy`*n*－指示磁盘驱动器
- `mag_tape`*n*－指示磁带机（流化处理）
- `rmdisk`*n*－指示可移除磁盘（如 JAZ 或 ZIP 驱动器）或者 USB 可热插拔介质

开始之前 您必须具有全局区域中的 "Security Administrator"（安全管理员）角色。

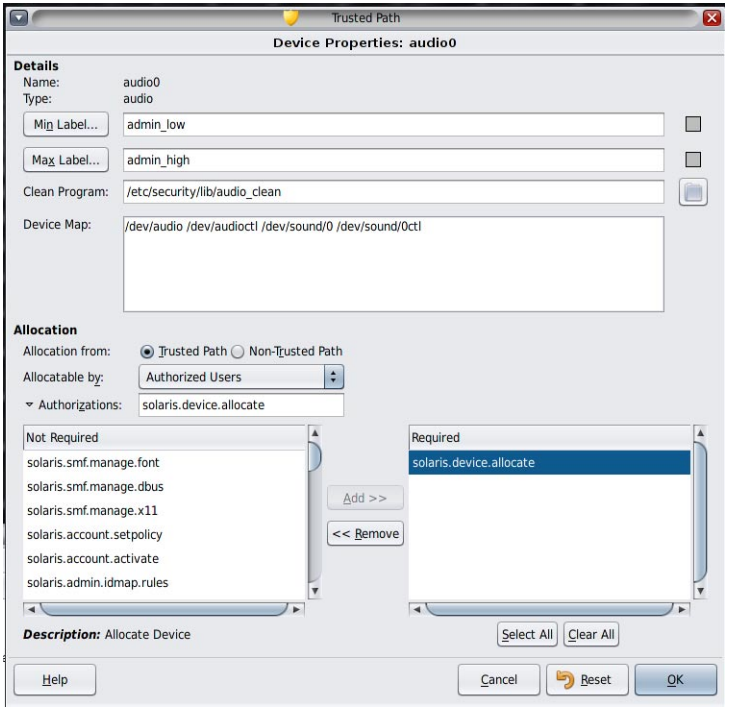
1 从 "Trusted Path"（可信路径）菜单中，选择 "Allocate Device"（分配设备）。

"Device Allocation Manager"（设备分配管理器）随即出现。



2 查看缺省安全设置。

单击 "Device Administration"（设备管理），然后突出显示设备。下图显示了 root 角色正在查看的音频设备。



3 **可选限制设备上的标签范围。**

a. **设置最小标签。**

单击 "Min Label"（最小标签）按钮。从标签生成器中选择一个最小标签。有关标签生成器的信息，请参见第 40 页中的 “Trusted Extensions 中的标签生成器”。

b. **设置最大标签。**

单击 "Max Label..."（最大标签...）按钮。从标签生成器中选择一个最大标签。

4 **指定设备是否可以在本地分配。**

在 "Device Allocation Configuration"（设备分配配置）对话框中，在 "For Allocations From Trusted Path"（对于从可信路径进行的分配）下，从 "Allocatable By"（可由以下用户分配）列表中选择一个选项。缺省情况下，会选中 "Authorized Users"（经授权的用户）。因此，设备是可分配的，且用户必须已被授权。

- **要使设备不可分配，请单击 "No Users"（无用户）。**

  在配置打印机、帧缓存器或其他不可分配的设备时，请选择 "No Users"（无用户）。

- **要使设备可分配，但不需要授权，请单击 "All Users"（所有用户）。**

5 **指定设备是否可以远程分配。**

在 "For Allocations From Non-Trusted Path"（对于从非可信路径进行的分配）部分中，从 "Allocatable By"（可由以下用户分配）列表中选择一个选项。缺省情况下，会选中 "Same As Trusted Path"（与可信路径相同）。

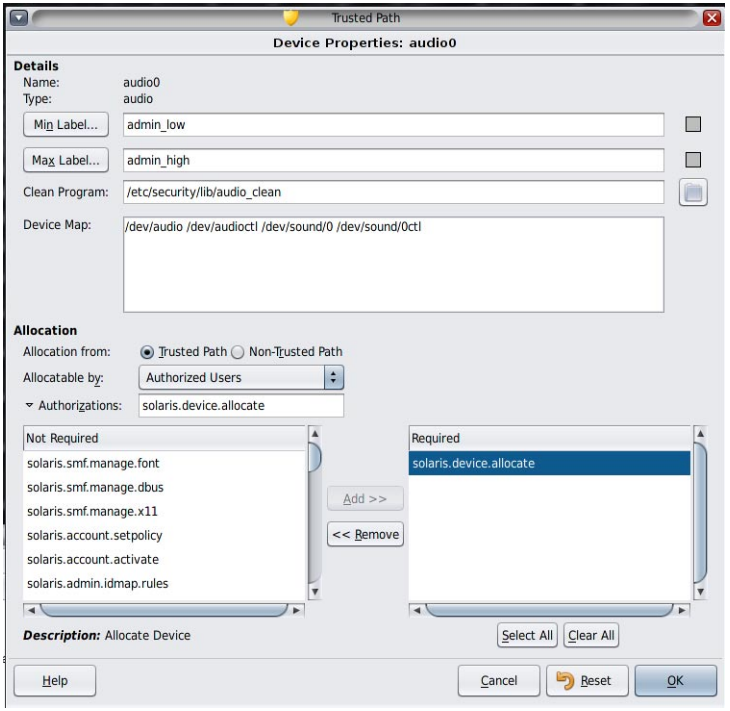
- **如果需要用户授权，请选择 "Allocatable by Authorized Users"（可由经授权的用户分配）。**

- **要使设备不可供远程用户分配，请选择 "No Users"（无用户）。**

- **要使设备可供任何人分配，请选择 "All Users"（所有用户）。**

6 **如果设备是可分配的，并且您的站点已创建了新的设备授权，请选择相应的授权。**

下面的对话框显示了需要 `solaris.device.allocate` 授权才能分配 `cdrom0` 设备。



要创建和使用特定于站点的设备授权，请参见第 223 页中的“在 Trusted Extensions 中定制设备授权（任务列表）”。

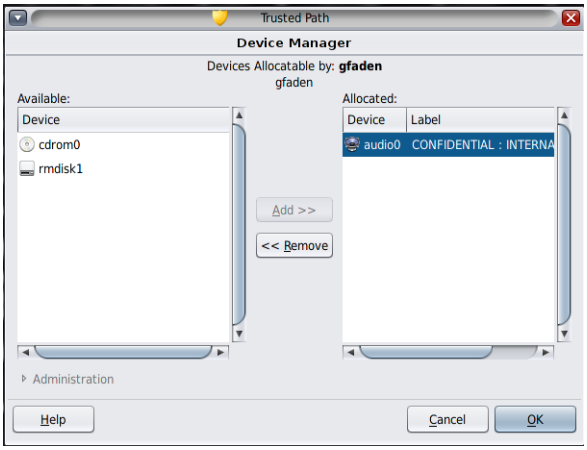
7 **要保存更改，请单击 "OK"（确定）。**

▼ 如何在 Trusted Extensions 中撤销或回收设备

如果某个设备没有在 "Device Allocation Manager"（设备分配管理器）中列出，则它可能已被分配，或者可能处于分配错误状态。系统管理员可以恢复此设备，使其可用。

开始之前 您必须具有全局区域中的 "System Administrator"（系统管理员）角色。此角色包含 `solaris.device.revoke` 授权。

1 从 "Trusted Path"（可信路径）菜单中，选择 "Allocate Device"（分配设备）。
在下图中，音频设备已分配给某个用户。



2 单击 "Device Administration"（设备管理）按钮。

3 检查设备的状态。
选择设备名称，并检查 "State"（状态）字段。

- 如果 "State"（状态）字段是 "Allocate Error State"（分配错误状态），请单击 "Reclaim"（回收）按钮。
- 如果 "State"（状态）字段是 "Allocated"（已分配），请执行以下操作之一：
  - 请求 "Owner"（所有者）字段中的用户取消分配设备。
  - 通过单击 "Revoke"（撤销）按扭强制解除分配设备。

4 关闭 "Device Allocation Manager"（设备分配管理器）。

▼ 如何在 Trusted Extensions 中保护不可分配的设备

对于帧缓存器和打印机，最常使用 "Device Configuration"（设备配置）对话框的 "Allocatable By"（可由以下用户分配）部分中的 "No Users"（无用户）选项，这些设备不必分配即可使用。

开始之前 您必须具有全局区域中的 "Security Administrator"（安全管理员）角色。

1 从 "Trusted Path"（可信路径）菜单中，选择 "Allocate Device"（分配设备）。

2. **在 "Device Allocation Manager"（设备分配管理器）中，单击 "Device Administration"（设备管理）按钮。**

3. **选择新的打印机或帧缓存器。**

   a. **要使设备不可分配，请单击 "No Users"（无用户）。**

   b. **可选限制设备上的标签范围。**

      i. **设置最小标签。**

         单击 "Min Label..."（最小标签...）按钮。从标签生成器中选择一个最小标签。有关标签生成器的信息，请参见第 40 页中的 “Trusted Extensions 中的标签生成器”。

      ii. **设置最大标签。**

         单击 "Max Label..."（最大标签...）按钮。从标签生成器中选择一个最大标签。

示例 17–1 阻止远程分配音频设备

"Allocatable By"（可由以下用户分配）部分中的 "No Users"（无用户）选项可阻止远程用户在远程系统上收听对话。

安全管理员在 "Device Allocation Manager"（设备分配管理器）中按以下方式配置音频设备：

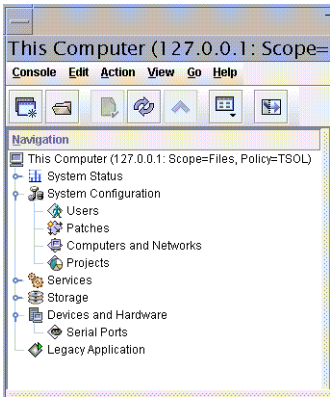
```
Device Name: audio
For Allocations From: Trusted Path
Allocatable By: Authorized Users
Authorizations: solaris.device.allocate

Device Name: audio
For Allocations From: Non-Trusted Pathh
Allocatable By: No Users
```

▼ 如何配置用于登录的串行线路

开始之前 您必须具有全局区域中的 "Security Administrator"（安全管理员）角色。

1. **在 "Files"（文件）作用域中打开 Solaris Management Console。**

图 17–1 Solaris Management Console 中的串行端口工具



2 **在 "Devices and Hardware"（设备和硬件）下，导航到 "Serial Ports"（串行端口）。**
在出现提示时提供口令。按照联机帮助来配置串行端口。

3 **要更改缺省标签范围，请打开 "Device Allocation Manager"（设备分配管理器）。**
缺省标签范围是从 `ADMIN_LOW` 到 `ADMIN_HIGH`。

示例 17–2 限制串行端口的标签范围

创建串行登录设备之后，安全管理员将串行端口的标签范围限制为单个标签 `Public`（公共）。管理员在 "Device Administration"（设备管理）对话框中设置以下值。

```
Device Name: /dev/term/[a|b]
Device Type: tty
Clean Program: /bin/true
Device Map: /dev/term/[a|b]
Minimum Label: Public
Maximum Label: Public
Allocatable By: No Users
```

▼ 如何在 Trusted CDE 中配置音频播放器程序以便使用

以下过程可以使音频播放器在用户插入音乐 CD 时自动在 Trusted CDE 工作区中打开。有关用户的操作过程，请参见《Trusted Extensions User's Guide》中的“How to Allocate a Device in Trusted Extensions”中的示例。

注 – 在 Trusted JDS 工作区中，用户指定可移除介质的行为时所使用的方法与在非可信工作区中使用的方法相同。

开始之前 您必须具有全局区域中的 "System Administrator"（系统管理员）角色。

1. **编辑 `/etc/rmmount.conf` 文件。**

   请使用可信编辑器。有关详细信息，请参见第 52 页中的 “如何在 Trusted Extensions 中编辑管理文件”。

2. **将您的站点的 CD 播放器程序添加到文件中的 `cdrom` 操作。**

   `action` *media* `action_`*program*`.so` *path-to-program*

示例 17–3 **配置音频播放器程序以便使用**

在下面的示例中，系统管理员使 `workman` 程序可供系统的所有用户使用。`workman` 程序是一个音频播放器程序。

```
# /etc/rmmount.conf file
action cdrom action_workman.so /usr/local/bin/workman
```

▼ 如何阻止在分配设备后显示 "File Manager"（文件管理器）

缺省情况下，挂载设备时会显示 "File Manager"（文件管理器）。如果正在挂载的设备没有文件系统，您可能希望阻止 "File Manager"（文件管理器）显示。

开始之前 您必须具有全局区域中的 "System Administrator"（系统管理员）角色。

1. **编辑 `/etc/rmmount.conf` 文件。**

   请使用可信编辑器。有关详细信息，请参见第 52 页中的 “如何在 Trusted Extensions 中编辑管理文件”。

2. **找到以下 `filemgr` 操作：**

   ```
   action cdrom action_filemgr.so
   action floppy action_filemgr.so
   ```

3. **注释掉相应的操作。**

   以下示例显示已经为 `cdrom` 和 `diskette` 设备注释掉 `action_filemgr.so` 操作。

   ```
   # action cdrom action_filemgr.so
   # action floppy action_filemgr.so
   ```

   在分配 CDROM 或磁盘时，"File Manager"（文件管理器）不会显示。

▼ 如何在 Trusted Extensions 中添加 Device_Clean（设备清除）脚本

如果在创建设备时没有指定 device_clean （设备清除）脚本，则会使用缺省脚本 /bin/true。

开始之前 准备一个具有如下功能的脚本：清除物理设备中的所有可用数据，并且在成功时返回 0。对于具有可移除介质的设备，如果用户没有弹出介质，脚本会尝试执行此操作。如果介质没有弹出，脚本会将设备置于分配错误状态。有关要求的详细信息，请参见 device_clean(5) 手册页。

您必须在全局区域中承担 root 角色。

1. **将脚本复制到 /etc/security/lib 目录中。**
2. **在 "Device Administration"（设备管理）对话框中，指定脚本的完整路径。**
   a. **打开 "Device Allocation Manager"（设备分配管理器）。**
   b. **单击 "Device Administration"（设备管理）按钮。**
   c. **选择设备的名称，然后单击 "Configure"（配置）按钮。**
   d. **在 "Clean Program"（清除程序）字段中，键入脚本的完整路径。**
3. **保存您的更改。**

在 Trusted Extensions 中定制设备授权（任务列表）

下面的任务列表描述了在您的站点更改设备授权的过程。

任务	说明	参考
创建新的设备授权。	创建特定于站点的授权。	第 224 页中的 “如何创建新的设备授权”
将授权添加到设备。	将特定于站点的授权添加到选定设备。	第 226 页中的 “如何在 Trusted Extensions 中将特定于站点的授权添加到设备”
将设备授权指定给用户和角色。	使用户和角色能够使用新授权。	第 227 页中的 “如何指定设备授权”

▼ 如何创建新的设备授权

如果一个设备不需要授权，那么缺省情况下，所有用户都能使用此设备。如果需要授权，则只有经授权的用户才能使用此设备。

要拒绝对可分配设备的所有访问，请参见示例 17–1。

开始之前 您必须具有全局区域中的 "Security Administrator"（安全管理员）角色。

1. **编辑 `auth_attr` 文件。**

   请使用可信编辑器。有关详细信息，请参见第 52 页中的 “如何在 Trusted Extensions 中编辑管理文件”。

2. **为新授权创建一个标题。**

   使用您的组织的反序 Internet 域名，后跟可选的其他任意组件，如您公司的名称。以点分隔组件。使用点结束标题名。

   domain-suffix`.`*domain-prefix*`.`*optional*`.:::`*Company* `Header::help=`*Company*`.html`

3. **添加新的授权条目。**

   添加授权，每行一个授权。在示例中，为了便于显示，对行进行了拆分。授权包括 `grant` 授权，它使得管理员能够指定新的授权。

   ```
   domain-suffix.domain-prefix.grant:::Grant All Company Authorizations::
   help=CompanyGrant.html
   domain-suffix.domain-prefix.grant.device:::Grant Company Device Authorizations::
   help=CompanyGrantDevice.html
   domain-suffix.domain-prefix.device.allocate.tape:::Allocate Tape Device::
   help=CompanyTapeAllocate.html
   domain-suffix.domain-prefix.device.allocate.floppy:::Allocate Floppy Device::
   help=CompanyFloppyAllocate.html
   ```

4. **保存文件并关闭编辑器。**

5. **如果要使用 LDAP 作为命名服务，请更新 Oracle Directory Server Enterprise Edition（目录服务器）上的 `auth_attr` 条目。**

   有关信息，请参见 `ldapaddent(1M)` 手册页。

6. **将新授权添加到相应的权限配置文件。然后，将配置文件指定给用户和角色。**

   使用 Solaris Management Console。承担 "Security Administrator"（安全管理员）角色，然后执行《System Administration Guide: Security Services》中的“How to Create or Change a Rights Profile” Oracle Solaris 过程。

7. **使用授权来限制对磁带机和磁盘驱动器的访问。**

   在 "Device Allocation Manager"（设备分配管理器）中，将新授权添加到所需授权列表中。有关过程，请参见第 226 页中的 “如何在 Trusted Extensions 中将特定于站点的授权添加到设备”。

示例 17–4 创建细粒度设备授权

NewCo 的安全管理员需要为公司构建细粒度设备授权。

首先，管理员编写以下帮助文件，并将这些文件置于 /usr/lib/help/auths/locale/C 目录中：

```
Newco.html
NewcoGrant.html
NewcoGrantDevice.html
NewcoTapeAllocate.html
NewcoFloppyAllocate.html
```

然后，管理员在 auth_attr 文件中为 newco.com 的所有授权添加一个标题。

```
# auth_attr file
com.newco.:::NewCo Header::help=Newco.html
```

接下来，管理员向文件中添加授权条目：

```
com.newco.grant:::Grant All NewCo Authorizations::
help=NewcoGrant.html
com.newco.grant.device:::Grant NewCo Device Authorizations::
help=NewcoGrantDevice.html
com.newco.device.allocate.tape:::Allocate Tape Device::
help=NewcoTapeAllocate.html
com.newco.device.allocate.floppy:::Allocate Floppy Device::
help=NewcoFloppyAllocate.html
```

在示例中，为了便于显示，对行进行了拆分。

auth_attr 条目创建了以下授权：

- 用于授予所有 NewCo 授权的授权
- 用于授予 NewCo 设备授权的授权
- 用于分配磁带机的授权
- 用于分配磁盘驱动器的授权

示例 17–5 创建可信路径和非可信路径授权

缺省情况下，"Allocate Devices"（分配设备）授权允许从可信路径和可信路径外进行分配。

在下面的示例中，站点安全策略要求限制远程 CD-ROM 分配。安全管理员创建了 com.someco.device.cdrom.local 授权。该授权适用于使用可信路径分配的 CD-ROM 驱动器。com.someco.device.cdrom.remote 授权适用于少数用户，他们可以在可信路径外分配 CD-ROM 驱动器。

安全管理员创建帮助文件、将授权添加到 auth_attr 数据库、将授权添加到设备，然后将授权置于权限配置文件中。配置文件被指定给允许分配设备的用户。

- 下面是 auth_attr 数据库条目：

```
com.someco.:::SomeCo Header::help=Someco.html
com.someco.grant:::Grant All SomeCo Authorizations::
help=SomecoGrant.html
com.someco.grant.device:::Grant SomeCo Device Authorizations::
help=SomecoGrantDevice.html
com.someco.device.cdrom.local:::Allocate Local CD-ROM Device::
help=SomecoCDAllocateLocal.html
com.someco.device.cdrom.remote:::Allocate Remote CD-ROM Device::
help=SomecoCDAllocateRemote.html
```

- 下面是 "Device Allocation Manager"（设备分配管理器）分配：

  "Trusted Path"（可信路径）允许经授权的用户在分配本地 CD-ROM 驱动器时使用 "Device Allocation Manager"（设备分配管理器）。

  ```
  Device Name: cdrom_0
  For Allocations From: Trusted Path
  Allocatable By: Authorized Users
  Authorizations: com.someco.device.cdrom.local
  ```

  "Non-Trusted Path"（非可信路径）允许用户使用 `allocate` 命令远程分配设备。

  ```
  Device Name: cdrom_0
  For Allocations From: Non-Trusted Path
  Allocatable By: Authorized Users
  Authorizations: com.someco.device.cdrom.remote
  ```

- 下面是权限配置文件条目：

  ```
  # Local Allocator profile
  com.someco.device.cdrom.local

  # Remote Allocator profile
  com.someco.device.cdrom.remote
  ```

- 下面是适用于经授权的用户的权限配置文件：

  ```
  # List of profiles for regular authorized user
  Local Allocator Profile
  ...

  # List of profiles for role or authorized user
  Remote Allocator Profile
  ...
  ```

▼ 如何在 Trusted Extensions 中将特定于站点的授权添加到设备

开始之前 您必须是 "Security Administrator"（安全管理员）角色，或者是具有 "Configure Device Attributes"（配置设备属性）授权的角色。您必须已创建了特定于站点的授权，如第 224 页中的 “如何创建新的设备授权”中所述。

1 执行第 215 页中的 “如何在 Trusted Extensions 中配置设备”过程。

a. 选择一个需要由新授权来保护的设备。

b. **单击 "Device Administration"（设备管理）按钮。**

c. **单击 "Authorizations"（授权）按钮。**
新授权显示在 "Not Required"（非必需）列表中。

d. **将新授权添加到授权的 "Required"（必需）列表中。**

2 **要保存更改，请单击 "OK"（确定）。**

▼ 如何指定设备授权

"Allocate Device"（分配设备）授权允许用户分配设备。"Allocate Device"（分配设备）授权和 "Revoke or Reclaim Device"（撤销或回收设备）授权适用于管理角色。

开始之前 您必须具有全局区域中的 "Security Administrator"（安全管理员）角色。

如果现有的配置文件不适用，安全管理员可以创建新的配置文件。有关示例，请参见第 86 页中的 “如何创建权限配置文件以实现方便的授权”。

- **为用户指定包含 "Allocate Device"（分配设备）授权的权限配置文件。**
有关帮助信息，请参见联机帮助。有关逐步操作过程，请参见《System Administration Guide: Security Services》中的“How to Change the RBAC Properties of a User”。
以下权限配置文件使得角色可以分配设备：
  - "All Authorizations"（所有授权）
  - "Device Management"（设备管理）
  - "Media Backup"（介质备份）
  - "Object Label Management"（对象标签管理）
  - "Software Installation"（软件安装）

  以下权限配置文件使得角色可以撤销或回收设备：
  - "All Authorizations"（所有授权）
  - "Device Management"（设备管理）

  以下权限配置文件使得角色可以创建或配置设备：
  - "All Authorizations"（所有授权）
  - "Device Security"（设备安全）

示例 17–6 指定新的设备授权

在本例中，安全管理员为系统配置新的设备授权，并将包含新授权的权限配置文件指定给可信用户。安全管理员执行以下操作：

1. 按第 224 页中的 “如何创建新的设备授权”中所述创建新的设备授权
2. 在 "Device Allocation Manager"（设备分配管理器）中，将新的设备授权添加到磁带机和磁盘驱动器
3. 将新授权置于 "NewCo Allocation"（NewCo 分配）权限配置文件中
4. 将 "NewCo Allocation"（NewCo 分配）权限配置文件添加到被授权分配磁带机和磁盘驱动器的用户和角色的配置文件中

现在，经授权的用户和角色可以在此系统上使用磁带机和磁盘驱动器了。

◆ ◆ ◆ 第 18 章

18 Trusted Extensions 审计（概述）

本章介绍了 Trusted Extensions 提供的新增审计功能。

Trusted Extensions 和审计

在配置有 Trusted Extensions 软件的系统上，配置和管理审计的方法与在 Oracle Solaris 系统上配置和管理审计的方法相似。不过，存在下面一些差异。

- Trusted Extensions 软件向系统中添加审计类、审计事件、审计令牌和审计策略选项。
- 在 Trusted Extensions 软件中会缺省启用审计。
- 不支持 Oracle Solaris 按区域审计。在 Trusted Extensions 中，所有区域均以相同的方式进行审计。
- Trusted Extensions 提供了管理工具来管理用户的审计特征以及编辑审计文件。
- Trusted Extensions 中使用 "System Administrator"（系统管理员）和 "Security Administrator"（安全管理员）这两个角色来配置和管理审计。

  安全管理员计划要审计的内容以及任何特定于站点的“事件到类”映射。与在 Oracle Solaris OS 中一样，系统管理员为审计文件计划磁盘空间需求、创建审计管理服务器以及安装审计配置文件。

Trusted Extensions 中的按角色审计管理

Trusted Extensions 中的审计要求进行与 Oracle Solaris OS 中相同的规划。有关规划的详细信息，请参见《System Administration Guide: Security Services》中的第 29 章 “Planning for Oracle Solaris Auditing”。

用于审计管理的角色设置

在 Trusted Extensions 中，审计是两个角色的职责。"System Administrator"（系统管理员）角色设置审计存储的磁盘和网络。"Security Administrator"（安全管理员）角色决定要审计的内容，并在审计配置文件中指定该信息。与在 Oracle Solaris OS 中一样，您在软件中创建角色。软件提供了这两个角色的权限配置文件。初始设置团队在初始配置过程中创建了 "Security Administrator"（安全管理员）角色。有关详细信息，请参见《Trusted Extensions Configuration Guide》中的“Create the Security Administrator Role in Trusted Extensions”。

注 – 系统仅记录审计配置文件要求系统记录的安全相关事件（也就是说，只记录预先选择的事件类别）。因此，在进行后续审计检查时可以仅考虑已记录的事件。如果配置不正确，将无法检测到试图破坏系统安全的行为，或者导致管理员无法检测到应为试图破坏安全的行为负责的用户。管理员必须定期分析审计迹，以检查是否存在破坏安全的行为。

Trusted Extensions 中的审计任务

在 Trusted Extensions 中配置和管理审计的过程与 Oracle Solaris 中的过程稍有不同。

- 两个管理角色中的一个在全局区域中执行审计配置。然后，系统管理员将特定的定制审计文件从全局区域复制到每个有标签区域中。通过执行此过程，在全局区域和有标签区域中将以相同的方式对用户操作进行审计。

  有关详细信息，请参见第 231 页中的 “安全管理员的审计任务”和第 231 页中的 “系统管理员的审计任务”

- Trusted Extensions 管理员使用一个可信编辑器来编辑审计配置文件。在 Trusted CDE 中，Trusted Extensions 管理员使用 CDE 操作来调用可信编辑器。有关操作列表，请参见第 32 页中的 “Trusted CDE 操作”。

- Trusted Extensions 管理员使用 Solaris Management Console 来配置特定的用户。可以在此工具中指定特定于用户的审计特征。只有当用户的审计特征与用户使用的系统的审计特征不同时才需要指定用户特征。有关此工具的简介，请参见第 36 页中的 “Solaris Management Console 工具”。

安全管理员的审计任务

以下任务与安全有关，因此属于安全管理员的职责。请遵循 Oracle Solaris 说明，但是请使用 Trusted Extensions 管理工具。

任务	针对 Oracle Solaris 的说明	Trusted Extensions 不同之处
配置审计文件。	《System Administration Guide: Security Services》中的“Configuring Audit Files (Task Map)”	请使用可信编辑器。有关详细信息，请参见第 52 页中的“如何在 Trusted Extensions 中编辑管理文件”。
（可选）更改缺省审计策略。	《System Administration Guide: Security Services》中的“How to Configure Audit Policy”	请使用可信编辑器。
禁用和重新启用审计。	《System Administration Guide: Security Services》中的“How to Disable the Audit Service”	缺省情况下启用审计。
管理审计。	《System Administration Guide: Security Services》中的“Oracle Solaris Auditing (Task Map)”	请使用可信编辑器。 忽略每区域审计任务。

系统管理员的审计任务

以下任务属于系统管理员的职责。请遵循 Oracle Solaris 说明，但是请使用 Trusted Extensions 管理工具。

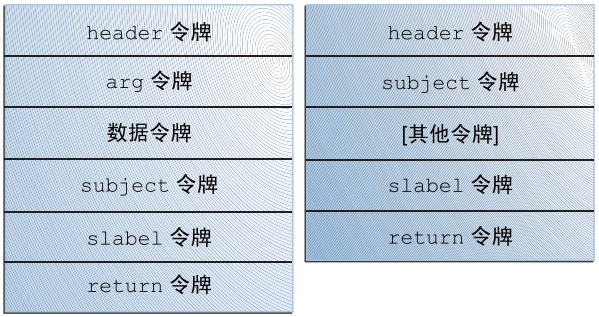
任务	针对 Oracle Solaris 的说明	Trusted Extensions 不同之处
创建一个专用于审计文件的 ZFS 文件系统。 创建一个 `audit_warn` 别名。	《System Administration Guide: Security Services》中的“Managing Audit Records” 《System Administration Guide: Security Services》中的“How to Configure the audit_warn Email Alias”	请在全局区域中执行所有管理。 请使用可信编辑器。
将定制的审计文件复制或回送挂载到有标签区域。	《System Administration Guide: Security Services》中的“Configuring the Audit Service in Zones (Tasks)”	创建有标签区域后，将文件回送挂载或复制到每个有标签区域。 将文件复制到第一个有标签区域中，然后复制该区域。
（可选）分布审计配置文件。	无说明	请参见《Trusted Extensions Configuration Guide》中的“How to Copy Files From Portable Media in Trusted Extensions”。
管理审计。	《System Administration Guide: Security Services》中的“Oracle Solaris Auditing (Task Map)”	忽略每区域审计任务。

任务	针对 Oracle Solaris 的说明	Trusted Extensions 不同之处
按标签选择审计记录。	《System Administration Guide: Security Services》中的“How to Select Audit Events From the Audit Trail”	要按标签选择记录，请使用 `auditreduce` 命令和 `-l` 选项。

Trusted Extensions 审计参考

Trusted Extensions 软件向 Oracle Solaris OS 中添加审计类、审计事件、审计令牌和审计策略选项。多个审计命令进行了扩展来处理标签。下图显示了典型的 Trusted Extensions 内核审计记录和用户级别审计记录。

图 18–1 有标签系统中的典型审计记录结构



Trusted Extensions 审计类

下表中按字母顺序列出了 Trusted Extensions 软件添加到 Oracle Solaris OS 的审计类。这些类列在 `/etc/security/audit_class` 文件中。有关审计类的更多信息，请参见 `audit_class(4)` 手册页。

表 18–1 X Server 审计类

短名称	长名称	审计掩码
xc	X - Object create/destroy（X－对象创建/销毁）	0x00800000
xp	X - Privileged/administrative operations（X－特权/管理操作）	0x00400000
xs	X - Operations that always silently fail, if bad（X－如果出现错误，总是在无提示情况下失败的操作）	0x01000000

表 18–1 X Server 审计类 （续）

短名称	长名称	审计掩码
xx	X - All X events in the xc, xp, and xs classes (metaclass)（X－xc、xp 和 xs 类（元类）中的所有 X 事件）	0x01c00000

X Server 审计事件根据以下标准映射到这些类中：

- **xc** － 该类针对创建或销毁对服务器对象进行审计。例如，该类对 `CreateWindow()` 进行审计。
- **xp** － 该类针对特权的使用进行审计。包括成功的和不成功的特权使用。例如，当一个客户机试图更改另一个客户机的窗口的属性时，将对 `ChangeWindowAttributes()` 进行审计。该类还包括管理例程，如 `SetAccessControl()`。
- **xs** － 当安全属性导致故障时，某些例程在发生故障时不会向客户机返回 X 错误消息，该类将对此类例程进行审计。例如，如果 `GetImage()` 由于缺少特权而无法从窗口进行读取，则它不会返回 `BadWindow` 错误。

  应当选择仅对成功情况审计这些事件。如果针对故障选择了 xs 事件，审计迹中会充满无关记录。
- **xx** － 该类包括所有 X 审计类。

Trusted Extensions 审计事件

Trusted Extensions 软件向系统中添加了审计事件。新的审计事件和这些事件所属的审计类列在 `/etc/security/audit_event` 文件中。Trusted Extensions 的审计事件数目介于 9000 和 10000 之间。有关审计事件的更多信息，请参见 `audit_event(4)` 手册页。

Trusted Extensions 审计令牌

下表中按字母顺序列出了 Trusted Extensions 软件添加到 Oracle Solaris OS 的审计令牌。`audit.log(4)` 手册页中也列出了这些令牌。

表 18–2 Trusted Extensions 审计令牌

令牌名称	说明
第 234 页中的 “`label` 令牌”	敏感标签
第 234 页中的 “`xatom` 令牌”	X 窗口原子标识
第 235 页中的 “`xclient` 令牌”	X 客户机标识
第 235 页中的 “`xcolormap` 令牌”	X 窗口颜色信息
第 235 页中的 “`xcursor` 令牌”	X 窗口光标信息

表 18–2 Trusted Extensions 审计令牌 （续）

令牌名称	说明
第 236 页中的 “xfont 令牌”	X 窗口字体信息
第 236 页中的 “xgc 令牌”	X 窗口图形上下文信息
第 236 页中的 “xpixmap 令牌”	X 窗口像素映射信息
第 236 页中的 “xproperty 令牌”	X 窗口属性信息
第 237 页中的 “xselect 令牌”	X 窗口数据信息
第 238 页中的 “xwindow 令牌”	X 窗口窗口信息

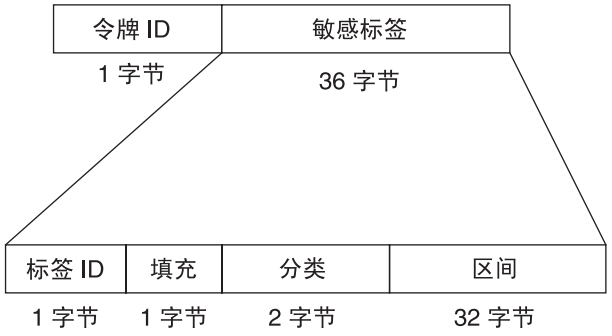
label 令牌

label 令牌包含一个敏感标签。此令牌包含以下字段：

- 令牌 ID
- 敏感标签

下图显示了该令牌的格式。

图 18–2 label 令牌格式



label 令牌由 praudit 命令显示如下：

```
sensitivity label,ADMIN_LOW
```

xatom 令牌

xatom 令牌包含与 X 原子有关的信息。此令牌包含以下字段：

- 令牌 ID
- 字符串长度

- 标识原子的文本字符串

xatom 令牌由 praudit 命令显示如下：

```
X atom,_DT_SAVE_MODE
```

xclient 令牌

xclient 令牌包含与 X 客户机有关的信息。此令牌包含以下字段：

- 令牌 ID
- 客户机 ID

xclient 令牌由 praudit 命令显示如下：

```
X client,15
```

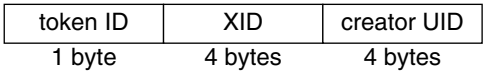
xcolormap 令牌

xcolormap 令牌包含与颜色映射有关的信息。此令牌包含以下字段：

- 令牌 ID
- X Server 标识符
- 创建者的用户 ID

下图显示了该令牌的格式。

图 18–3 xcolormap、xcursor、xfont、xgc、xpixmap 和 xwindow 令牌的格式



xcolormap 令牌由 praudit 命令显示如下：

```
X color map,0x08c00005,srv
```

xcursor 令牌

xcursor 令牌包含与光标有关的信息。此令牌包含以下字段：

- 令牌 ID
- X Server 标识符
- 创建者的用户 ID

图 18–3 显示了该令牌格式。

xcursor 令牌由 praudit 命令显示如下：

```
X cursor,0x0f400006,srv
```

xfont 令牌

xfont 令牌包含与字体有关的信息。此令牌包含以下字段：

- 令牌 ID
- X Server 标识符
- 创建者的用户 ID

图 18–3 显示了该令牌格式。

xfont 令牌由 praudit 命令显示如下：

```
X font,0x08c00001,srv
```

xgc 令牌

xgc 令牌包含与 xgc 有关的信息。此令牌包含以下字段：

- 令牌 ID
- X Server 标识符
- 创建者的用户 ID

图 18–3 显示了该令牌格式。

xgc 令牌由 praudit 命令显示如下：

```
Xgraphic context,0x002f2ca0,srv
```

xpixmap 令牌

xpixmap 令牌包含与像素映射有关的信息。此令牌包含以下字段：

- 令牌 ID
- X Server 标识符
- 创建者的用户 ID

图 18–3 显示了该令牌格式。

xpixmap 令牌由 praudit 命令显示如下：

```
X pixmap,0x08c00005,srv
```

xproperty 令牌

xproperty 令牌包含与窗口的各个属性有关的信息。此令牌包含以下字段：

- 令牌 ID
- X Server 标识符

- 创建者的用户 ID
- 字符串长度
- 标识原子的文本字符串

下图显示了 xproperty 令牌的格式。

图 18–4 xproperty 令牌格式

token ID	XID	creator UID	strlen	string (atom name)
1 byte	4 bytes	4 bytes	2 bytes	N bytes

xproperty 令牌由 praudit 命令显示如下：

```
X property,0x000075d5,root,_MOTIF_DEFAULT_BINDINGS
```

xselect 令牌

xselect 令牌包含在窗口之间移动的数据。此数据包括一个没有既定内部结构的字节流和一个属性字符串。此令牌包含以下字段：

- 令牌 ID
- 属性字符串的长度
- 属性字符串
- 属性类型的长度
- 属性类型字符串
- 用以指定数据的字节数的长度字段
- 包含数据的字节字符串

下图显示了该令牌的格式。

图 18–5 xselect 令牌格式

令牌 ID	属性长度	属性字符串	属性类型长度	属性类型	数据长度	窗口数据
1 字节	2 字节	N 字节	2 字节	N 字节	2 字节	N 字节

xselect 令牌由 praudit 命令显示如下：

```
X selection,entryfield,halogen
```

xwindow 令牌

xwindow 令牌包含与窗口有关的信息。此令牌包含以下字段：

- 令牌 ID
- X Server 标识符
- 创建者的用户 ID

图 18–3 显示了该令牌格式。

xwindow 令牌由 praudit 命令显示如下：

```
X window,0x07400001,srv
```

Trusted Extensions 审计策略选项

Trusted Extensions 向现有的 Oracle Solaris 审计策略选项中添加了两个审计策略选项。可以列出策略以查看添加项：

```
$ auditconfig -lspolicy
...
windata_down Include downgraded window information in audit records
windata_up   Include upgraded window information in audit records
...
```

Trusted Extensions 对审计命令的扩展

auditconfig、auditreduce 和 bsmrecord 命令进行了扩展以处理 Trusted Extensions 信息：

- auditconfig 命令包括了 Trusted Extensions 审计策略。有关详细信息，请参见 auditconfig(1M) 手册页。
- auditreduce 命令添加了 -l 选项，用以根据标签过滤记录。有关详细信息，请参见 auditreduce(1M) 手册页。
- bsmrecord 命令包括了 Trusted Extensions 审计事件。有关详细信息，请参见 bsmrecord(1M) 手册页。

◆ ◆ ◆ 第 19 章

19 Trusted Extensions 中的软件管理（任务）

本章介绍了在配置有 Trusted Extensions 的系统上如何确保第三方软件以可信的方式运行。

将软件添加到 Trusted Extensions

任何可添加到 Oracle Solaris 系统的软件都可以添加到配置有 Trusted Extensions 的系统。此外，还可以添加使用 Trusted Extensions API 的程序。将软件添加到 Trusted Extensions 系统与将软件添加到运行非全局区域的 Oracle Solaris 系统类似。

例如，打包问题会影响安装了非全局区域的系统。软件包参数定义以下内容：

- **软件包的区域作用域**—该作用域决定了可以在其中安装特定软件包的区域的类型。
- **软件包的可见性**—可见性决定了是否必须安装某个软件包以及该软件包是否必须在所有区域中都相同。
- **软件包的限制**—一个限制为是否必须仅在当前区域中安装软件包。

在 Trusted Extensions 中，程序通常安装在全局区域中，供有标签区域中的一般用户使用。有关在区域中安装软件包的详细信息，请参见《System Administration Guide: Oracle Solaris Containers-Resource Management and Oracle Solaris Zones》中的第 25 章 “About Packages and Patches on an Oracle Solaris System With Zones Installed (Overview)”。另请参见 `pkgadd(1M)` 手册页。

在 Trusted Extensions 站点上，系统管理员和安全管理员协同工作来安装软件。安全管理员对软件添加情况进行评估，以确定是否符合安全策略。如果软件需要特权或授权才能成功运行，则 "Security Administrator"（安全管理员）角色将为该软件的用户指定相应的权限配置文件。

从可移除介质导入软件需要授权。具有 "Allocate Device"（分配设备）授权的帐户可以从可移除介质导入或导出数据。数据可能包括可执行代码。一般用户只能在该用户的安全许可内的标签导入数据。

"System Administrator"（系统管理员）角色负责添加安全管理员批准的程序。

Oracle Solaris 针对软件的安全机制

Trusted Extensions 使用与 Oracle Solaris OS 一样的安全机制。这些机制包括：

- **授权**—可以要求某个程序的用户具有特定授权。有关授权的信息，请参见《System Administration Guide: Security Services》中的“Oracle Solaris RBAC Elements and Basic Concepts”。另请参见 `auth_attr(4)` 和 `getauthattr(3SECDB)` 手册页。
- **特权**－可以为程序和进程指定特权。有关特权的信息，请参见《System Administration Guide: Security Services》中的第 8 章 “Using Roles and Privileges (Overview)”。另请参见 `privileges(5)` 手册页。

  `ppriv` 命令提供了一个调试实用程序。有关详细信息，请参见 `ppriv(1)` 手册页。有关对在非全局区域中运行的程序使用此实用程序的说明，请参见《System Administration Guide: Oracle Solaris Containers-Resource Management and Oracle Solaris Zones》中的“Using the ppriv Utility”。
- **权限配置文件**－权限配置文件将安全属性收集在一个地方，以便分配给用户或角色。有关权限配置文件的信息，请参见《System Administration Guide: Security Services》中的“RBAC Rights Profiles”。Trusted Extensions 会为可指定安全属性的可执行文件添加 CDE 操作。
- **可信库**－动态共享的库，供 `setuid`、`setgid` 和只能从可信目录装入的特权程序使用。与在 Oracle Solaris OS 中一样，可使用 `crle` 命令将特权程序的共享库目录添加到可信目录列表中。有关详细信息，请参见 `crle(1)` 手册页。

评估软件是否符合安全要求

如果软件已指定有特权或者以替代用户 ID 或组 ID 运行，则软件即成为**可信的**。可信软件可以绕过 Trusted Extensions 安全策略的各项设置。请注意，您可以将软件设为可信软件，即使它可能不值得信任。安全管理员必须进行仔细的审查，在确认软件以值得信任的方式使用特权后才向软件授予特权。

在可信的系统上，程序分为三类：

- **不需要安全属性的程序** – 某些程序在单级别上运行，而且不需要特权。这些程序可以安装在公共目录（例如 `/usr/local`）中。要进行访问，请在用户和角色的权限配置文件中将这些程序指定为命令。
- **以 root 用户身份运行的程序**—某些程序使用 `setuid 0` 执行。可以在权限配置文件中为这类程序指定有效的 UID `0`。然后，安全管理员将配置文件指定给某个管理角色。

  提示 – 如果应用程序能够以值得信任的方式使用特权，请为应用程序指定所需的特权，而不以 `root` 用户身份执行程序。

- **需要特权的程序**— 某些程序需要特权的原因可能不明显。即使程序没有执行从表面上即能看出违反了系统安全策略的功能，程序也可能在内部执行了违反安全要求的操作。例如，程序可能在使用共享的日志文件，或者程序可能在从 `/dev/kmem` 读取数据。有关安全方面的注意事项，请参见 mem(7D) 手册页。

  有时，内部策略覆盖对于应用程序的正确运转不是特别重要。相反，此种覆盖为用户提供了一项方便的功能。

  如果您的组织可以访问源代码，请检查您是否能够删除要求策略覆盖的操作，而不影响应用程序性能。

创建可信程序时开发者的职责

尽管程序的开发者可以在源代码中操纵特权集，但如果安全管理员没有为程序指定所需的特权，程序也会失败。在创建可信程序时，开发者和安全管理员需要合作。

编写可信程序的开发者必须负责以下事项：

1. 了解程序何时需要特权来执行其工作。
2. 了解并实施用于在程序中安全地使用特权的技术，例如特权包围。
3. 在将特权指定给程序时知道这其中的安全含义。程序不得违反安全策略。
4. 通过使用从可信目录链接到程序的共享库来编译程序。

   有关其他信息，请参见《Oracle Solaris 10 开发者安全性指南》。有关适用于 Trusted Extensions 的代码示例，请参见《Trusted Extensions Developer's Guide》。

安全管理员针对可信程序的职责

安全管理员负责测试和评估新软件。确定软件值得信任后，安全管理员为程序配置权限配置文件和其他安全相关属性。

安全管理员的职责包括以下几项：

1. 确保程序员和程序分发过程是可信的。
2. 通过下面的某个来源，确定程序需要哪些特权：
   - 询问程序员。
   - 搜索源代码，以查明程序期望使用的任何特权。
   - 搜索源代码，查明程序要求其用户具有的任何授权。
   - 在 `ppriv` 命令中使用调试选项，搜索特权使用情况。有关示例，请参见 `ppriv(1)` 手册页。
3. 检查源代码，以确保代码以值得信任的方式使用程序运行所需的特权。

   如果程序未能以值得信任的方式使用特权，且您可以修改程序的源代码，请修改代码。只有十分了解安全性的安全顾问或开发者才能修改代码。修改可以包括特权包围或对授权的检查。

   必须手动指定特权。对于因缺少特权而失败的程序，可以为其指定特权。另一方面，安全管理员可以决定指定一个有效的 UID 或 GID 来使特权成为非必需的。

窗口系统中的可信进程

在 Solaris Trusted Extensions (CDE) 中，以下窗口系统进程是可信的：

- 前面板
- 前面板的子面板
- 工作区菜单
- 文件管理器
- 应用程序管理器

窗口系统的可信进程可供每个人使用，但只有全局区域中的角色能够访问管理操作。

在 "File Manager"（文件管理器）中，如果某个操作未列在帐户的任一配置文件中，则该操作的图标不可见。在工作区菜单中，如果某个操作未列在帐户的任一配置文件中，该操作可见，但在调用该操作时会显示错误。

在 Trusted CDE 中，窗口管理器 `dtwm` 调用 `Xtsolusersession` 脚本。该脚本与窗口管理器配合使用来调用从窗口系统启动的操作。`Xtsolusersession` 脚本在帐户尝试启动某个操作时检查该帐户的权限配置文件。在任一情况下，如果操作列在所指定的权限配置文件中，该操作将以配置文件所指定的安全属性运行。

添加 Trusted CDE 操作

在 Trusted Extensions 中创建和使用 CDE 操作的过程与 Oracle Solaris OS 中的过程类似。有关如何添加操作的信息，请参见《Solaris Common Desktop Environment: Advanced User's and System Administrator's Guide》中的第 4 章 "Adding and Administering Applications"。

与在 Oracle Solaris OS 中一样，可以通过权限配置文件机制来控制对操作的使用。在 Trusted Extensions 中，已在管理角色的权限配置文件中为多个操作指定了安全属性。安全管理员还可以使用 "Rights"（权限）工具来为新操作指定安全属性。

下表总结了在创建和使用操作时 Oracle Solaris 系统和 Trusted Extensions 系统之间的主要差异。

表 19–1 Trusted Extensions 中对 CDE 操作的约束

Oracle Solaris CDE 操作	Trusted CDE 操作
任何人都可以在发起者的起始目录中创建新操作。 新操作自动可供其创建者使用。	仅当某个操作列在指定给用户的权限配置文件中时，该操作才可用。操作的搜索路径有所不同。用户起始目录中的操作是最后而不是最先处理的。因此，没有人可以定制现有操作。 用户可以在其起始目录中创建新操作，但该操作可能不可用。 具有 "All"（全部）配置文件的用户可以使用他们创建的操作。其他情况下，安全管理员必须将新操作的名称添加到帐户的某个权限配置文件中。 要启动操作，用户需使用 "File Manager"（文件管理器）。系统管理员可以将操作放置在公共目录中。
可以将操作拖放到前面板中。	前面板是可信路径的一部分。窗口管理器只能识别位于 `/usr/dt` 和 `/etc/dt` 子目录中的以管理方式添加的操作。即使使用 "All"（全部）配置文件，用户也不能将新操作拖至前面板。窗口管理器不能识别用户的起始目录中的操作。该管理器仅检查公共目录。
如果以 `root` 用户身份运行操作，则操作可以执行特权操作。	如果在指定给用户的权限配置文件中已经为操作指定了特权，则操作可以执行特权操作。
操作不是由 Solaris Management Console 管理的。	操作是在 Solaris Management Console 的 "Rights"（权限）工具中指定给权限配置文件的。如果添加了新操作，则安全管理员可以使这些新操作可供使用。

在 Trusted Extensions 中管理软件（任务）

在 Trusted Extensions 中管理软件与在安装了非全局区域的 Oracle Solaris 系统上管理软件类似。有关区域的详细信息，请参见《System Administration Guide: Oracle Solaris Containers-Resource Management and Oracle Solaris Zones》中的第 II 部分, “Zones”。

▼ 如何在 Trusted Extensions 中添加软件包

开始之前 您必须是可以分配设备的角色。

1 从相应的工作区启动。

- **要将软件包安装在全局区域中，请停留在全局区域中。**

- **要将软件包安装在某个有标签区域中，请以该标签创建一个工作区。**
  有关详细信息，请参见《Trusted Extensions User's Guide》中的"How to Change the Label of a Workspace"。

2. **分配 CD-ROM 驱动器。**
   有关详细信息，请参见《Trusted Extensions User's Guide》中的"How to Allocate a Device in Trusted Extensions"。

3. **安装软件。**
   有关详细信息，请参见《Oracle Solaris 管理：基本管理》中的"软件管理任务所在的位置"。

4. **在完成后，取消分配设备。**
   有关详细信息，请参见《Trusted Extensions User's Guide》中的"How to Allocate a Device in Trusted Extensions"。

▼ 如何在 Trusted Extensions 中安装 Java 归档文件

此过程将一个 Java 归档 (Java archive, JAR) 文件下载到全局区域。从全局区域中，管理员可以使该文件可供一般用户使用。

开始之前 安全管理员已验证 Java 程序的来源是值得信任的，传送方法是安全的，而且程序能够以值得信任的方式运行。

您是全局区域中的 "System Administrator"（系统管理员）角色。在 Trusted CDE 中，"Software Installation"（软件安装）权限配置文件包括对 Java 代码的 "Open"（打开）操作。

1. **将 JAR 文件下载到 `/tmp` 目录中。**
   例如，如果您是在 `http://www.sunfreeware.com` 网站上选择软件，请参阅该网站的 "Solaris `pkg-get` tool" 说明。

2. **打开 "File Manager"（文件管理器），并导航到 `/tmp` 目录。**

3. **双击所下载的文件。**

4. **要安装软件，请回答对话框中的问题。**

5. **阅读安装日志。**

示例 19–1 将 JAR 文件下载到用户标签

为降低安全风险，系统管理员将软件下载到一般用户认可范围内的单个标签。然后，安全管理员以该标签测试 JAR 文件。如果软件通过测试，则安全管理员随后会将该标签降级至 ADMIN_LOW。系统管理员将软件安装到 NFS 服务器上，使其可供所有用户使用。

1. 首先，系统管理员在用户标签创建一个工作区。
2. 在该工作区中，系统管理员下载 JAR 文件。
3. 安全管理员在该标签测试文件。
4. 然后，安全管理员将文件的标签更改为 ADMIN_LOW。
5. 最后，系统管理员将文件复制到其标签为 ADMIN_LOW 的 NFS 服务器。

◆ ◆ ◆ 附 录 A

Trusted Extensions 管理快速参考

Trusted Extensions 接口扩展了 Oracle Solaris OS。本附录提供了它们之间的差异的快速参考。有关接口的详细列表，包括库例程和系统调用，请参见附录 B，Trusted Extensions 手册页列表。

Trusted Extensions 中的管理接口

Trusted Extensions 为其软件提供了接口。以下接口只在 Trusted Extensions 软件正在运行时可用：

`txzonemgr` 脚本
: 提供了一个用于创建、安装、初始化和引导有标签区域的基于菜单的向导。菜单的标题是 "Labeled Zone Manager"（有标签区域管理器）。该脚本还针对联网选项、名称服务器选项以及将全局区域委托到现有 LDAP 服务器提供了菜单项。

Trusted CDE 操作
: 在 Trusted CDE 中，"Workspace Menu"（工作区菜单）–> "Application Manager"（应用程序管理器）–> Trusted_Extensions 中包含了用来配置文件、安装和引导区域以及简化其他 Trusted Extensions 任务的 CDE 操作。对于这些操作执行的任务，请参见第 32 页中的 “Trusted CDE 操作”。Trusted CDE 联机帮助中也介绍了这些操作。

管理编辑器
: 此可信编辑器用于编辑系统文件。在 Trusted CDE 中，"Workspace Menu"（工作区菜单）–> "Application Manager"（应用程序管理器）–> Trusted_Extensions –> "Admin Editor"（管理编辑器）调用 "Admin Editor"（管理编辑器）。在 Trusted JDS 中，可从命令行调用该编辑器。您提供要编辑的文件作为参数，如下所示：

  `/usr/dt/bin/trusted_edit` *filename*

"Device Allocation Manager"（设备分配管理器）
: 在 Trusted Extensions 中，此 GUI 用来管理设备。管理员使用 "Device Administration"（设备管理）对话框来配置设备。

角色和一般用户使用 "Device Allocation Manager"（设备分配管理器）来分配设备。可以从 "Trusted Path"（可信路径）菜单访问此 GUI。

"Label Builder"（标签生成器）
用户可以选择标签或安全许可时将调用此应用程序。角色将标签或标签范围指定给设备、区域、用户或角色时也会显示此应用程序。

"Selection Manager"（选择管理器）
经授权的用户或经授权的角色试图升级或降级信息时将调用此应用程序。

"Trusted Path"（可信路径）菜单
此菜单处理与可信计算基 (Trusted Computing Base, TCB) 的交互。例如，此菜单中有 "Change Password"（更改口令）菜单项。在 Trusted CDE 中，您可以从工作区切换区域访问 "Trusted Path"（可信路径）菜单。在 Trusted JDS 中，您可通过单击可信窗口条左侧的可信符号来访问 "Trusted Path"（可信路径）菜单。

管理命令
Trusted Extensions 提供了用于获取标签和执行其他任务的命令。有关命令列表，请参见第 41 页中的 “Trusted Extensions 中的命令行工具”。

由 Trusted Extensions 扩展的 Oracle Solaris 接口

Trusted Extensions 对现有的 Oracle Solaris 配置文件、命令和 GUI 进行了补充。

管理命令	Trusted Extensions 为选定的 Oracle Solaris 命令添加了选项。有关列表，请参见表 2–5
配置文件	Trusted Extensions 添加了两个特权：`net_mac_aware` 和 `net_mlp`。有关 `net_mac_aware` 的使用，请参见第 129 页中的 “访问 Trusted Extensions 中 NFS 挂载的目录”。
	Trusted Extensions 向 `auth_attr` 数据库添加了授权。
	Trusted Extensions 向 `exec_attr` 数据库添加了可执行文件（包括 CDE 操作）。
	Trusted Extensions 修改了 `prof_attr` 数据库中的现有权限配置文件。它还向数据库添加了配置文件。
	Trusted Extensions 在 `exec_attr` 数据库中为可授权执行的可执行文件添加了 CDE 操作。
	Trusted Extensions 向 `policy.conf` 数据库添加了字段。有关字段，请参见第 73 页中的 “Trusted Extensions 中的 `policy.conf` 文件缺省值”。

	Trusted Extensions 添加了审计令牌、审计事件、审计类和审计策略选项。有关列表，请参见第 232 页中的 “Trusted Extensions 审计参考”。
Solaris Management Console	Trusted Extensions 在 "Computers and Networks"（计算机和网络）工具集合中添加了一个 "Security Templates"（安全模板）工具。 Trusted Extensions 在 "Computers and Networks"（计算机和网络）工具集合中添加了一个 "Trusted Network Zones"（可信网络区域）工具。 Trusted Extensions 向 "Users"（用户）工具和 "Administrative Roles"（管理角色）工具添加了 "Trusted Extensions Attributes"（Trusted Extensions 属性）选项卡。
区域中共享的目录	Trusted Extensions 允许您共享有标签区域中的目录。通过从全局区域创建 `/etc/dfs/dfstab` 文件，可以在区域的标签共享目录。

Trusted Extensions 中更为严厉的安全缺省值

Trusted Extensions 设立了比 Oracle Solaris OS 更为严厉的安全缺省值：

审计　缺省情况下，审计处于启用状态。

管理员可以关闭审计。但是，安装了 Trusted Extensions 的站点通常要求进行审计。

设备　缺省情况下，设备分配处于启用状态。

缺省情况下，设备分配需要授权。因此，缺省情况下，一般用户不能使用可移除介质。

管理员可以取消授权要求。但是，安装了 Trusted Extensions 的站点通常要求使用设备分配授权。

打印　一般用户只能使用打印机标签范围中包括用户的标签的打印机进行打印。

缺省情况下，打印输出具有标题页和篇尾页。这些页和正文页中都包括打印作业的标签。

缺省情况下，用户不能打印 PostScript 文件。

角色　在 Oracle Solaris OS 中可使用角色，但其使用是可选的。在 Trusted Extensions 中，角色是进行正确管理所必需的。

在 Oracle Solaris OS 中，使 root 用户成为角色是可能的。在 Trusted Extensions 中，root 用户成为了角色以便更好地审计谁充当超级用户。

Trusted Extensions 中的受限选项

Trusted Extensions 缩小了 Oracle Solaris 配置选项的范围：

桌面	Trusted Extensions 提供了两种桌面：Solaris Trusted Extensions (CDE) 和 Solaris Trusted Extensions (JDS)。 Trusted Extensions 提供了 Solaris Trusted Extensions (GNOME) 桌面。
命名服务	支持 LDAP 命名服务。所有区域必须由一个命名服务进行管理。
区域	全局区域是一个管理区域。只有 root 用户或角色才能进入全局区域。因此，对 Oracle Solaris 一般用户可用的管理接口对 Trusted Extensions 一般用户不可用。例如，在 Trusted Extensions 中，用户无法初启 Solaris Management Console。 非全局区域是有标签区域。用户在有标签区域中工作。

◆ ◆ ◆ 附 录 B

Trusted Extensions 手册页列表

Trusted Extensions 是 Oracle Solaris OS 的一个配置。本附录提供了包含 Trusted Extensions 信息的 Oracle Solaris 手册页的简短说明。

按字母顺序排列的 Trusted Extensions 手册页

下面的手册页介绍了 Oracle Solaris 系统中的 Trusted Extensions 软件。这些手册页仅适用于配置有 Trusted Extensions 的系统。

Oracle Solaris 手册页	概要
add_allocatable(1M)	向分配数据库添加条目
atohexlabel(1M)	将人可阅读的标签转换为其内部的等效文本
blcompare(3TSOL)	比较二进制标签
blminmax(3TSOL)	确定两个标签的绑定
chk_encodings(1M)	检查标签编码文件语法
dtappsession(1)	启动新的 "Application Manager"（应用程序管理器）会话
fgetlabel(2)	获取文件的标签
getlabel(1)	显示文件的标签
getlabel(2)	获取文件的标签
getpathbylabel(3TSOL)	获取区域路径名
getplabel(3TSOL)	获取进程的标签
getuserrange(3TSOL)	获取用户的标签范围
getzoneidbylabel(3TSOL)	通过区域标签获取区域 ID

getzonelabelbyid(3TSOL)	通过区域 ID 获取区域标签
getzonelabelbyname(3TSOL)	通过区域名称获取区域标签
getzonepath(1)	显示与指定标签对应的区域的根路径
getzonerootbyid(3TSOL)	通过区域根 ID 获取区域根路径名
getzonerootbylabel(3TSOL)	通过区域标签获取区域根路径
getzonerootbyname(3TSOL)	通过区域名称获取区域根路径名
hextoalabel(1M)	将内部文本标签转换为人可阅读的等效体
labelbuilder(3TSOL)	创建基于 Motif 的用户接口，以便交互生成有效标签或安全许可
labelclipping(3TSOL)	转换二进制标签并将标签剪辑至指定的宽度
label_encodings(4)	描述标签编码文件
label_to_str(3TSOL)	将标签转换为人可阅读的字符串
labels(5)	描述 Trusted Extensions 标签属性
libtsnet(3LIB)	是 Trusted Extensions 网络库
libtsol(3LIB)	是 Trusted Extensions 库
m_label(3TSOL)	为新标签分配和释放资源
pam_tsol_account(5)	检查因标签导致的帐户限制
plabel(1)	获取进程的标签
remove_allocatable(1M)	从分配数据库中删除条目
sel_config(4)	是复制、剪切、粘贴和拖放操作的选择规则
setflabel(3TSOL)	将文件移动到具有相应敏感标签的区域
smtnrhdb(1M)	管理 Trusted Extensions 联网数据库中的条目
smtnrhtp(1M)	管理用于 Trusted Extensions 联网的模板数据库中的条目
smtnzonecfg(1M)	管理非全局区域中用于 Trusted Extensions 联网的配置数据库中的条目
str_to_label(3TSOL)	将人可阅读的字符串解析为标签
tnctl(1M)	配置 Trusted Extensions 网络参数
tnd(1M)	是可信的网络守护进程

tninfo(1M)	显示内核级的 Trusted Extensions 网络信息和统计信息
trusted_extensions(5)	介绍 Trusted Extensions
TrustedExtensionsPolicy(4)	是 Trusted Extensions X Server 扩展的配置文件
tsol_getrhtype(3TSOL)	获取 Trusted Extensions 网络信息中的主机类型
updatehome(1M)	更新当前标签的起始目录副本和链接文件
XTSOLgetClientAttributes(3XTSOL)	获取 X 客户机的标签属性
XTSOLgetPropAttributes(3XTSOL)	获取窗口属性的标签属性
XTSOLgetPropLabel(3XTSOL)	获取窗口属性的标签
XTSOLgetPropUID(3XTSOL)	获取窗口属性的 UID
XTSOLgetResAttributes(3XTSOL)	获取窗口或像素图的所有标签属性
XTSOLgetResLabel(3XTSOL)	获取窗口、像素图或色彩表的标签
XTSOLgetResUID(3XTSOL)	获取窗口或像素图的 UID
XTSOLgetSSHeight(3XTSOL)	获取屏幕条的高度
XTSOLgetWorkstationOwner(3XTSOL)	获取工作站的所有权
XTSOLIsWindowTrusted(3XTSOL)	确定窗口是否是由可信的客户机创建的
XTSOLMakeTPWindow(3XTSOL)	使该窗口成为一个 "Trusted Path"（可信路径）窗口
XTSOLsetPolyInstInfo(3XTSOL)	设置多实例信息
XTSOLsetPropLabel(3XTSOL)	设置窗口属性的标签
XTSOLsetPropUID(3XTSOL)	设置窗口属性的 UID
XTSOLsetResLabel(3XTSOL)	设置窗口或像素图的标签
XTSOLsetResUID(3XTSOL)	设置窗口、像素图或色彩表的 UID
XTSOLsetSessionHI(3XTSOL)	为窗口服务器设置会话高敏感标签
XTSOLsetSessionLO(3XTSOL)	为窗口服务器设置会话低敏感标签
XTSOLsetSSHeight(3XTSOL)	设置屏幕条的高度
XTSOLsetWorkstationOwner(3XTSOL)	设置工作站的所有权

Trusted Extensions 修改的 Oracle Solaris 手册页

Trusted Extensions 向下列 Oracle Solaris 手册页添加了信息。

Oracle Solaris 手册页	Trusted Extensions 修改
allocate(1)	添加了相应的选项来支持在区域中分配设备以及在有窗口环境清除该设备
auditconfig(1M)	为有标签信息添加窗口策略
audit_class(4)	添加了 X Server 审计类
audit_event(4)	添加了审计事件
auditreduce(1M)	添加了一个标签选择器
auth_attr(4)	添加了标签授权
automount(1M)	添加了挂载以及由此获得的查看较低级别起始目录的功能
cancel(1)	针对用户取消打印作业的能力添加了标签限制
deallocate(1)	添加了相应的选项来支持在区域中取消分配设备，在有窗口环境中清除该设备，以及指定要取消分配的设备的类型
device_clean(5)	在 Trusted Extensions 中在缺省情况下会调用
exec_attr(4)	将 CDE 操作添加为了一种配置文件对象
getpflags(2)	识别 NET_MAC_AWARE 和 NET_MAC_AWARE_INHERIT 进程标志
getsockopt(3SOCKET)	获取套接字的强制访问控制状态 SO_MAC_EXEMPT
getsockopt(3XNET)	获取套接字的强制访问控制状态 SO_MAC_EXEMPT
ifconfig(1M)	添加了 all-zones 接口
is_system_labeled(3C)	确定系统是否配置有 Trusted Extensions
ldaplist(1)	添加了 Trusted Extensions 网络数据库
list_devices(1)	添加了与设备相关联的属性，如标签
lp(1)	添加了 -nolabels 选项
lpadmin(1M)	针对管理员管理打印的能力添加了标签限制
lpmove(1M)	针对管理员移动打印作业的能力添加了标签限制
lpq(1B)	针对打印队列信息的显示添加了标签限制
lprm(1B)	针对调用者删除打印请求的能力添加了标签限制
lpsched(1M)	针对管理员停止和重新启动打印服务的能力添加了标签限制

lpstat(1)	针对打印服务状态的显示添加了标签限制
netstat(1M)	添加了 -R 选项，用以显示扩展的安全属性
privileges(5)	添加了 PRIV_FILE_DOWNGRADE_SL 等 Trusted Extensions 特权
prof_attr(4)	添加了 "Object Label Management"（对象标签管理）等权限配置文件
route(1M)	添加 -secattr 选项，用以向路由添加扩展的安全属性
setpflags(2)	设置了 NET_MAC_AWARE 每进程标志
setsockopt(3SOCKET)	设置了 SO_MAC_EXEMPT 选项
setsockopt(3XNET)	对套接字设置了强制访问控制 SO_MAC_EXEMPT
smexec(1M)	添加了相应选项来支持 CDE 操作类型
smrole(1M)	添加了相应选项来支持角色的标签
smuser(1M)	添加了相应选项来支持用户的标签和其他安全属性，如允许的空闲时间
socket.h(3HEAD)	支持为无标签的对等方使用 SO_MAC_EXEMPT 选项
tar(1)	在对应于标签的 tar 文件和提取文件中添加了包括标签
tar.h(3HEAD)	添加了在有标签的 tar 文件中使用的属性类型
ucred_getlabel(3C)	添加了基于用户凭证获取标签值的功能
user_attr(4)	添加了特定于 Trusted Extensions 的用户安全属性

索引

A

C

D

E

U

X

Z

安

保

备

本

编

标

不

操

查

差

承

程

串

挂

关

管

认

软

删

商

设

升

使

手

授

数

特

通

图

网