Trusted Extensions 配置和管理

文件号码 E36732–02
2012 年 10 月

ORACLE

121210@25097

目录

前言 19

第 1 部分 Trusted Extensions 的初始配置 23

1 Trusted Extensions 的安全规划 25
在 Trusted Extensions 中规划安全 25
了解 Trusted Extensions 26
了解站点的安全策略 26
规划配置 Trusted Extensions 的人员 26
设计标签策略 27
规划 Trusted Extensions 的系统硬件和容量 27
规划可信网络 28
在 Trusted Extensions 中规划有标签区域 28
规划多级别服务 30
在 Trusted Extensions 中规划 LDAP 命名服务 30
在 Trusted Extensions 中规划审计 31
在 Trusted Extensions 中规划用户安全 31
为 Trusted Extensions 成立一个安装团队 32
在启用 Trusted Extensions 之前解决其他问题 33
在启用 Trusted Extensions 之前备份系统 33
启用 Trusted Extensions 的结果（从管理员角度） 34

2 Trusted Extensions 的配置任务列表 35
任务列表：准备和启用 Trusted Extensions 35
任务列表：选择 Trusted Extensions 配置 35
任务列表：使用提供的缺省设置配置 Trusted Extensions 36
任务列表：配置 Trusted Extensions 以满足站点要求 36

3 将 Trusted Extensions 功能添加到 Oracle Solaris（任务） 39
初始设置团队的职责 39
准备 Oracle Solaris 系统和添加 Trusted Extensions 39
▼ 安全安装 Oracle Solaris 系统 39
▼ 准备已安装的 Oracle Solaris 系统以使用 Trusted Extensions 40
▼ 将 Trusted Extensions 软件包添加到 Oracle Solaris 系统 41
在启用 Trusted Extensions 之前解决安全问题 42
▼ 在启用 Trusted Extensions 之前确保系统硬件安全并做出安全决策 42
启用 Trusted Extensions 服务并登录 43
▼ 启用 Trusted Extensions 并重新引导 43
▼ 登录到 Trusted Extensions 44

4 配置 Trusted Extensions（任务） 47
在 Trusted Extensions 中设置全局区域 47
▼ 如何检查并安装标签编码文件 48
▼ 如何在 Trusted Extensions 中配置 IPv6 CIPSO 网络 50
▼ 如何配置其他系统解释域 50
创建有标签区域 51
▼ 如何创建缺省 Trusted Extensions 系统 51
▼ 如何以交互方式创建有标签区域 52
▼ 如何将标签指定给两个区域工作区 54
在 Trusted Extensions 中配置网络接口 55
▼ 如何在所有区域中共享单个 IP 地址 56
▼ 如何将 IP 实例添加到有标签区域中 57
▼ 如何将虚拟网络接口添加到有标签区域 58
▼ 如何将 Trusted Extensions 系统连接到其他 Trusted Extensions 系统 59
▼ 如何为每个有标签区域配置单独的名称服务 60
在 Trusted Extensions 中创建角色和用户 61
▼ 如何在 Trusted Extensions 中创建 "Security Administrator"（安全管理员）角色 62
▼ 如何创建 "System Administrator"（系统管理员）角色 63
▼ 如何在 Trusted Extensions 中创建可以承担角色的用户 63
▼ 如何检验 Trusted Extensions 角色是否有效 66
▼ 如何使用户能够登录到有标签区域 66
在 Trusted Extensions 中创建集中起始目录 67
▼ 如何在 Trusted Extensions 中创建起始目录服务器 67

▼如何让用户登录每个 NFS 服务器来访问每个标签下的远程起始目录 68
▼如何通过在每个服务器上配置自动挂载程序来使用户能够访问其远程起始目录 ... 68
Trusted Extensions 配置故障排除 69
▼如何将桌面面板移到屏幕底部 69
其他 Trusted Extensions 配置任务 70
▼如何创建有标签辅助区域 71
▼如何创建和共享多级别数据集 72
▼如何在 Trusted Extensions 中将文件复制到便携介质 74
▼如何在 Trusted Extensions 中从便携介质复制文件 75
▼如何从系统中删除 Trusted Extensions 76

5 为 Trusted Extensions 配置 LDAP（任务） 77
在 Trusted Extensions 网络上配置 LDAP（任务列表） 77
在 Trusted Extensions 系统上配置 LDAP 代理服务器（任务列表） 78
在 Trusted Extensions 系统上配置 Oracle Directory Server Enterprise Edition 78
▼收集用于 LDAP 的 Directory Server 的信息 78
▼安装 Oracle Directory Server Enterprise Edition 79
▼为 Directory Server 创建 LDAP 客户机 81
▼配置 Oracle Directory Server Enterprise Edition的日志 82
▼为 Oracle Directory Server Enterprise Edition配置多级别端口 84
▼置备 Oracle Directory Server Enterprise Edition 84
为现有 Oracle Directory Server Enterprise Edition创建 Trusted Extensions 代理 86
▼创建 LDAP 代理服务器 86
创建 Trusted Extensions LDAP 客户机 87
▼使全局区域成为 Trusted Extensions 中的客户机 87

第 2 部分 Trusted Extensions 的管理 91

6 Trusted Extensions 管理概念 93
Trusted Extensions 和 Oracle Solaris OS 93
Trusted Extensions 和 Oracle Solaris OS 之间的相似之处 93
Trusted Extensions 和 Oracle Solaris OS 之间的不同之处 94
多显示端系统和 Trusted Extensions 桌面 95
Trusted Extensions 的基本概念 95

Trusted Extensions 保护 95
Trusted Extensions 与访问控制 96
Trusted Extensions 软件中的标签 97
角色和 Trusted Extensions 100

7 Trusted Extensions 管理工具 101
Trusted Extensions 的管理工具 101
`txzonemgr` 脚本 102
设备管理器 102
Trusted Extensions 中的选择管理器 103
Trusted Extensions 中的标签生成器 103
Trusted Extensions 中的命令行工具 104
Trusted Extensions 中的配置文件 104

8 Trusted Extensions 系统上的安全要求（概述） 105
配置安全功能 105
Trusted Extensions 中的角色 105
用于配置安全功能的 Trusted Extensions 接口 106
Trusted Extensions 对 Oracle Solaris 安全功能的扩展 106
独有的 Trusted Extensions 安全功能 107
安全要求实施 107
用户和安全要求 107
电子邮件使用指南 108
口令实施 108
信息保护 109
口令保护 109
组管理操作 109
用户删除操作 109
更改数据的安全级别时的规则 110
`sel_config` 文件 112

9 执行 Trusted Extensions 中的常见任务 113
Trusted Extensions 管理员入门（任务列表） 113
▼ 如何进入 Trusted Extensions 的全局区域 114

▼ 如何退出 Trusted Extensions 的全局区域 114
Trusted Extensions 中的常见任务（任务列表） 115
▼ 如何更改 root 的口令 115
▼ 如何在有标签区域强制实施新的本地用户口令 116
▼ 如何重新获得对桌面当前焦点的控制权 116
▼ 如何获取标签的十六进制等效值 117
▼ 如何通过标签的十六进制形式获取可读标签 118
▼ 如何在系统文件中更改安全缺省值 119

10 Trusted Extensions 中的用户、权限和角色（概述） 121
Trusted Extensions 中的用户安全功能 121
管理员针对用户的职责 122
系统管理员针对用户的职责 122
安全管理员针对用户的职责 122
在 Trusted Extensions 中创建用户之前要做的决策 123
Trusted Extensions 中的缺省用户安全属性 123
label_encodings 文件缺省值 123
Trusted Extensions 中的 policy.conf 文件缺省值 124
Trusted Extensions 中的可配置用户属性 124
必须为用户指定的安全属性 124
Trusted Extensions 中的用户安全属性指定 125
.copy_files 和 .link_files 文件 126

11 在 Trusted Extensions 中管理用户、权限和角色（任务） 129
针对安全性定制用户环境（任务列表） 129
▼ 如何修改缺省用户标签属性 130
▼ 如何修改 policy.conf 缺省值 130
▼ 如何在 Trusted Extensions 中为用户配置启动文件 131
▼ 如何在 Trusted Extensions 中登录到故障安全会话 134
管理用户和权限（任务列表） 134
▼ 如何修改用户的标签范围 135
▼ 如何创建权限配置文件以实现方便的授权 135
▼ 如何收缩用户的特权集 136
▼ 如何防止锁定用户帐户 137
▼ 如何允许用户更改数据的安全级别 137

▼ 如何从 Trusted Extensions 系统删除用户帐户 138

12 Trusted Extensions 中的远程管理（任务） 139
Trusted Extensions 中的远程管理 139
Trusted Extensions 中用于管理远程系统的方法 140
在 Trusted Extensions 中配置和管理远程系统（任务列表） 141
▼ 启用对远程 Trusted Extensions 系统的远程管理 141
▼ 如何对 Trusted Extensions 系统配置 Xvnc 以进行远程访问 143
▼ 如何登录和管理远程 Trusted Extensions 系统 145

13 在 Trusted Extensions 中管理区域 149
Trusted Extensions 中的区域 149
Trusted Extensions 中的区域和 IP 地址 150
区域和多级别端口 150
Trusted Extensions 中的区域和 ICMP 151
全局区域进程和有标签区域 151
有标签主区域和有标签辅助区域 152
Trusted Extensions 中的区域管理实用程序 153
管理区域（任务列表） 153
▼ 如何显示就绪或正在运行区域 154
▼ 如何显示挂载的文件的标签 155
▼ 如何对通常在有标签区域中不可见的文件进行回送挂载 156
▼ 如何禁用较低级别文件的挂载 157
▼ 如何从有标签区域共享 ZFS 数据集 158
▼ 如何在有标签区域中允许重新为文件设置标签 160

14 在 Trusted Extensions 中管理和挂载文件 161
Trusted Extensions 中的可能挂载项 161
用于已挂载文件系统的 Trusted Extensions 策略 162
用于单级别数据集的 Trusted Extensions 策略 162
用于多级别数据集的 Trusted Extensions 策略 163
MAC 读写策略无特权覆盖 163
在 Trusted Extensions 中共享和挂载文件系统的结果 164
在全局区域中共享和挂载文件 164

在有标签区域中共享和挂载文件 165
mlslabel 属性和挂载单级别文件系统 165
需要为文件重新设置标签的多级别数据集 166
挂载来自其他系统的多级别数据集 167
Trusted Extensions 中的 NFS 服务器和客户机配置 167
在 Trusted Extensions 中创建起始目录 168
在 Trusted Extensions 中更改自动挂载程序 168
Trusted Extensions 软件和 NFS 协议版本 169
备份、共享和挂载有标签文件（任务列表） 170
▼ 如何在 Trusted Extensions 中备份文件 170
▼ 如何在 Trusted Extensions 中恢复文件 171
▼ 如何从有标签区域共享文件系统 171
▼ 如何在有标签区域中对文件进行 NFS 挂载 173
▼ 如何解决 Trusted Extensions 中的挂载故障 174

15 可信网络（概述） 175
可信网络 175
Trusted Extensions 数据包 176
Trusted Extensions 多播包 176
可信网络通信 177
Trusted Extensions 中的网络命令 178
Trusted Extensions 中的网络配置数据库 179
可信网络安全属性 179
Trusted Extensions 中的网络安全属性 180
安全模板中的主机类型和模板名称 180
安全模板中的缺省标签 181
安全模板中的系统解释域 181
安全模板中的标签范围 182
安全模板中的辅助标签 182
可信网络回退机制 182
Trusted Extensions 中的路由概述 184
路由背景 184
Trusted Extensions 中的路由表项 184
Trusted Extensions 认可检查 185
Trusted Extensions 中的路由管理 186

在 Trusted Extensions 中选择路由器 187
Trusted Extensions 中的网关 187
Trusted Extensions 中的路由命令 188
有标签 IPsec 的管理 188
受 IPsec 保护的交换的标签 188
IPsec 安全关联的标签扩展 189
IKE 的标签扩展 190
隧道模式 IPsec 下的标签和认可 190
有关标签扩展的保密性和完整性保护 191

16 在 Trusted Extensions 中管理网络（任务） 193
为主机和网络设置标签（任务） 193
查看现有安全模板（任务） 193
创建安全模板（任务） 196
将主机添加到安全模板（任务） 198
限制可以访问可信网络的主机（任务） 205
配置路由和多级别端口（任务） 209
▼ 如何添加缺省路由 209
▼ 如何为区域创建多级别端口 210
配置有标签 IPsec（任务列表） 212
▼ 如何在多级别 Trusted Extensions 网络中应用 IPsec 保护 212
▼ 如何通过不可信网络配置隧道 214
可信网络故障排除（任务列表） 216
▼ 如何检验系统的接口是否已启动 216
▼ 如何调试 Trusted Extensions 网络 217
▼ 如何调试客户机与 LDAP 服务器的连接 220

17 Trusted Extensions 和 LDAP（概述） 223
在 Trusted Extensions 中使用 LDAP 命名服务 223
本地管理的 Trusted Extensions 系统 224
Trusted Extensions LDAP 数据库 224
Trusted Extensions 中的 LDAP 命名服务快速参考 225

18 Trusted Extensions 中的多级别邮件（概述） 227
多级别邮件服务 227
Trusted Extensions 邮件功能 227

19 管理有标签打印（任务） 229
标签、打印机和打印 229
Oracle Solaris 10 和 Oracle Solaris 11 中的 Trusted Extensions 打印之间的差别 230
在 Trusted Extensions 中限制对打印机和打印作业信息的访问 231
有标签的打印机输出 231
安全信息的 PostScript 打印 235
Trusted Extensions 打印界面（参考信息） 235
在 Trusted Extensions 中管理打印（任务） 236
配置有标签打印（任务列表） 236
▼ 如何配置多级别打印服务器及其打印机 237
▼ 如何配置网络打印机 239
▼ 如何将区域配置为单级别打印服务器 239
▼ 如何允许 Trusted Extensions 客户机访问打印机 240
▼ 如何为打印机配置受限制的标签范围 242
在 Trusted Extensions 中减少打印限制（任务列表） 243
▼ 如何删除标题页和篇尾页 243
▼ 如何为无标签的打印服务器指定标签 244
▼ 如何允许特定用户和角色不标记打印输出 245

20 Trusted Extensions 中的设备（概述） 247
通过 Trusted Extensions 软件提供的设备保护 247
设备标签范围 248
标签范围对设备的影响 248
设备访问策略 248
Device-Clean（设备清除）脚本 249
设备管理器 GUI 249
Trusted Extensions 中的设备安全保障 250
Trusted Extensions 中的设备（参考信息） 251

21 管理 Trusted Extensions 的设备（任务） 253
在 Trusted Extensions 中操作设备（任务列表） 253
在 Trusted Extensions 中使用设备（任务列表） 254
在 Trusted Extensions 中管理设备（任务列表） 254
▼ 如何在 Trusted Extensions 中配置设备 255
▼ 如何在 Trusted Extensions 中撤销或回收设备 258
▼ 如何在 Trusted Extensions 中保护不可分配的设备 259
▼ 如何在 Trusted Extensions 中添加 Device_Clean （设备清除）脚本 260
在 Trusted Extensions 中定制设备授权（任务列表） 261
▼ 如何创建新的设备授权 261
▼ 如何在 Trusted Extensions 中将特定于站点的授权添加到设备 264
▼ 如何指定设备授权 264

22 Trusted Extensions 审计（概述） 267
Trusted Extensions 和审计 267
Trusted Extensions 中的按角色审计管理 267
角色的审计管理职责 268
Trusted Extensions 中的审计任务 268
Trusted Extensions 审计参考 268
Trusted Extensions 审计类 269
Trusted Extensions 审计事件 269
Trusted Extensions 审计令牌 270
Trusted Extensions 审计策略选项 272
Trusted Extensions 对审计命令的扩展 272

23 Trusted Extensions 中的软件管理 273
将软件添加到 Trusted Extensions 273
Oracle Solaris 软件的安全机制 274
评估软件是否符合安全要求 274

A 站点安全策略 277
创建和管理安全策略 277
站点安全策略和 Trusted Extensions 278
计算机安全建议 278

物理安全建议 279
人员安全建议 280
常见安全违规 280
其他安全参考信息 281
美国政府出版物 281
UNIX 安全出版物 281
一般计算机安全出版物 282
一般 UNIX 出版物 282

B Trusted Extensions 的配置核对表 283
用于配置 Trusted Extensions 的核对表 283

C Trusted Extensions 管理快速参考 287
Trusted Extensions 中的管理接口 287
由 Trusted Extensions 扩展的 Oracle Solaris 接口 288
Trusted Extensions 中更为严厉的安全缺省值 289
Trusted Extensions 中的受限选项 289

D Trusted Extensions 手册页列表 291
按字母顺序排列的 Trusted Extensions 手册页 291
Trusted Extensions 修改的 Oracle Solaris 手册页 295

词汇表 299

索引 305

图

图 1–1 管理 Trusted Extensions 系统：按角色划分的任务 33
图 6–1 Trusted Extensions 多级别桌面 96
图 15–1 典型的 Trusted Extensions 路由和路由表项 187
图 19–1 有标签打印作业的典型标题页 232
图 19–2 篇尾页的差别 232
图 19–3 在正文页顶部和底部打印的作业标签 233
图 19–4 正文页以横向模式打印时，作业的标签以纵向模式打印 234
图 20–1 用户打开的设备管理器 249
图 22–1 有标签系统中的典型审计记录结构 269

表

表 1–1 Trusted Extensions 中的缺省主机模板 28
表 1–2 Trusted Extensions 用户帐户安全缺省值 31
表 6–1 标签关系的示例 98
表 7–1 Trusted Extensions 管理工具 101
表 8–1 将文件改为新标签的条件 110
表 8–2 将选定项改为新标签的条件 111
表 10–1 `policy.conf` 文件中的 Trusted Extensions 安全缺省值 124
表 10–2 创建用户后指定的安全属性 124
表 15–1 Trusted Extensions 主机地址和回退机制项 183
表 19–1 CUPS – LP 差异 230
表 19–2 `tsol_separator.ps` 文件中的可配置值 234
表 22–1 Trusted Extensions 审计令牌 270

前言

《Trusted Extensions 配置和管理》提供了用于在 Oracle Solaris 操作系统 (Oracle Solaris OS) 上启用和初始配置 Trusted Extensions 功能的过程。本指南还提供了用于在 Trusted Extensions 系统上管理用户、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。

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 用户指南》中所述。
- 如何在站点角色之间划分管理任务

Trusted Extensions 和 Oracle Solaris 操作系统

Trusted Extensions 在 Oracle Solaris OS 之上运行。由于 Trusted Extensions 软件可以修改 Oracle Solaris OS，所以 Trusted Extensions 可能需要对 Oracle Solaris 安装选项进行特定设置。本指南的第 I 部分介绍如何准备 Oracle Solaris OS 以使用 Trusted Extensions、如何启用 Trusted Extensions 以及如何初始配置该软件。本指南的第 II 部分介绍如何管理系统的独特 Trusted Extensions 功能。

相关的参考文档

在此库中发布的 Oracle Solaris 指南。

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

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

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	`#`
C shell	`machine_name%`
C shell 超级用户	`machine_name#`

第 1 部分

Trusted Extensions 的初始配置

本部分中各章节介绍如何准备 Oracle Solaris 系统以运行 Trusted Extensions。这些章节介绍了如何启用 Trusted Extensions 以及初始配置任务。

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

第 2 章，Trusted Extensions 的配置任务列表，提供用于在 Oracle Solaris 系统上配置 Trusted Extensions 软件的任务列表。

第 3 章，将 Trusted Extensions 功能添加到 Oracle Solaris（任务），提供准备 Oracle Solaris 系统以使用 Trusted Extensions 软件的说明。本章介绍了如何启用 Trusted Extensions 以及如何登录。

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

第 5 章，为 Trusted Extensions 配置 LDAP（任务），提供在 Trusted Extensions 系统上配置 LDAP 命名服务的说明。

◆ ◆ ◆ 第 1 章

1 Trusted Extensions 的安全规划

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

- 第 25 页中的 “在 Trusted Extensions 中规划安全”
- 第 34 页中的 “启用 Trusted Extensions 的结果（从管理员角度）”

在 Trusted Extensions 中规划安全

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

- 第 26 页中的 “了解 Trusted Extensions”
- 第 26 页中的 “了解站点的安全策略”
- 第 26 页中的 “规划配置 Trusted Extensions 的人员”
- 第 27 页中的 “设计标签策略”
- 第 27 页中的 “规划 Trusted Extensions 的系统硬件和容量”
- 第 28 页中的 “规划可信网络”
- 第 28 页中的 “在 Trusted Extensions 中规划有标签区域”
- 第 30 页中的 “规划多级别服务”
- 第 30 页中的 “在 Trusted Extensions 中规划 LDAP 命名服务”
- 第 31 页中的 “在 Trusted Extensions 中规划审计”
- 第 31 页中的 “在 Trusted Extensions 中规划用户安全”
- 第 32 页中的 “为 Trusted Extensions 成立一个安装团队”
- 第 33 页中的 “在启用 Trusted Extensions 之前解决其他问题”
- 第 33 页中的 “在启用 Trusted Extensions 之前备份系统”

有关 Trusted Extensions 配置任务的核对表，请参见附录 B，Trusted Extensions 的配置核对表。如果有兴趣将您的站点本地化，请参见第 27 页中的 “对于 Trusted Extensions 的国际客户”。如果想运行 evaluated configuration（评估配置），请参见第 26 页中的 “了解站点的安全策略”。

了解 Trusted Extensions

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

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

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

了解站点的安全策略

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

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

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

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

- 更改 /etc/system 文件中的内核切换设置。
- 关闭审计或设备分配。
- 更改 /usr 目录下公共文件中的缺省项。

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

规划配置 Trusted Extensions 的人员

root 角色或 "System Administrator"（系统管理员）角色负责启用 Trusted Extensions。您可以创建多个角色来划分多个功能区域之间的管理职责：

- security administrator（安全管理员）负责执行与安全相关的任务，例如设置和指定敏感标签、配置审计以及设置口令策略。
- system administrator（系统管理员）负责非安全方面的设置、维护及常规管理。

- 还可以配置更多受限制的角色。例如，操作员可以负责备份文件。

作为管理策略的一部分，需要确定以下内容：

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

设计标签策略

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

注意 – 如果由您提供 `label_encodings` 文件，最佳做法是在系统验证标签之前安装好最终版本的文件。在启用 Trusted Extensions 服务后执行首次引导期间验证标签。在创建您的第一个区域或网络模板之后，对 `label_encodings` 文件所做的任何更改必须适应现有的区域和模板。

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

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

对于 Trusted Extensions 的国际客户

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

规划 Trusted Extensions 的系统硬件和容量

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

- 遵循有关安装 Oracle Solaris 发行版的建议，如《安装 Oracle Solaris 11.1 系统》以及该发行版的《发行说明》的“安装”部分所述。
- 以下建议适用于 Trusted Extensions 功能：

- 在以下系统上运行所需的内存要超出最小建议内存：
  - 在多个敏感标签下运行的系统
  - 可承担管理角色的用户所使用的系统
- 在以下系统上运行需要更大的磁盘空间：
  - 在多个标签存储文件的系统
  - 其用户可承担管理角色的系统

规划可信网络

有关规划网络硬件的帮助，请参见《配置和管理 Oracle Solaris 11.1 网络》中的第 1 章 “规划网络部署”。

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

表 1–1 Trusted Extensions 中的缺省主机模板

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

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

有关如何为主机、网关和网络设置标签，请参见第 16 章，在 Trusted Extensions 中管理网络（任务）。在初始设置之后，执行为远程系统指定标签操作。

在 Trusted Extensions 中规划有标签区域

将 Trusted Extensions 软件添加到全局区域中的 Oracle Solaris。然后配置有标签的非全局区域。您可以为每个唯一标签创建一个或多个有标签区域，但不需要为 `label_encodings` 文件中的每个标签创建区域。使用提供的脚本，可以轻松地为 `label_encodings` 文件中的缺省用户标签和缺省用户安全许可创建两个有标签区域。

在创建有标签区域之后，一般用户可以使用配置的系统，但这些用户将无法访问其他系统。要进一步隔离在同一标签下运行的服务，可以创建辅助区域。有关更多信息，请参见第 152 页中的 “有标签主区域和有标签辅助区域”。

- 在 Trusted Extensions 中，连接到 X 服务器的本地传输是 UNIX 域套接字。缺省情况下，X 服务器不会侦听 TCP 连接。
- 缺省情况下，非全局区域不能与不可信主机通信。您必须指定每个区域可以访问的显式远程主机 IP 地址或网络掩码。

Trusted Extensions 区域和 Oracle Solaris Zones

Trusted Extensions 区域（即，有标签区域）是 Oracle Solaris Zones 的**标记**。有标签区域主要用于分离数据。在 Trusted Extensions 中，一般用户不能远程登录到有标签区域（从另一个可信系统的同等有标签区域中登录除外）。授权管理员可以从全局区域访问有标签区域。有关区域标记的更多信息，请参见 `brands(5)` 手册页。

Trusted Extensions 中的区域创建

Trusted Extensions 中的区域创建类似于 Oracle Solaris 中的区域创建。Trusted Extensions 提供 `txzonemgr` 脚本以指导您完成该过程。该脚本具有几个命令行选项，可用于自动创建有标签区域。有关更多信息，请参见 `txzonemgr(1M)` 手册页。

访问有标签区域

在正确配置的系统中，每个区域都必须能够使用网络地址与共享同一标签的其他区域进行通信。通过以下配置，有标签区域可以对其他有标签区域进行访问：

- **all-zones 接口** – 指定一个 `all-zones` 地址。在此缺省配置中，只需要一个 IP 地址。每个区域（全局区域和有标签区域）可以通过此共享地址与远程系统上的相同有标签区域进行通信。

  此配置的精细之处在于为全局区域创建第二个 IP 实例，以便专门使用。这个第二个实例不是一个 `all-zones` 地址。此 IP 实例可以用于托管多级别服务，或提供通往专用子网的路由。

- **IP 实例** – 与在 Oracle Solaris OS 中一样，为每个区域（包括全局区域）指定一个 IP 地址。区域共享 IP 栈。在最简单的情况下，所有区域共享同一个物理接口。

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

  更精细之处在于除 IP 实例之外，每个区域使用一个或多个 `all-zones` 接口。该配置提供了使用内部接口（例如 `vni0`）访问全局区域的选项，因此可保护全局区域免遭远程攻击。例如，在全局区域中 `vni0` 实例上绑定多级别端口的特权服务只能由使用共享栈的区域在内部进行访问。

- **专用 IP 栈** – 与在 Oracle Solaris 中一样，为每个区域（包括全局区域）指定一个 IP 地址。为每个有标签区域创建一个虚拟网络接口卡 (virtual network interface card, VNIC)。

此配置的精细之处在于通过一个单独的网络接口创建每个 VNIC。这种配置可用于使用物理方式分离与每个 NIC 关联的单标签网络。配置有专用 IP 栈的区域无法使用 `all-zones` 接口。

限制到有标签区域的应用程序

缺省情况下，有标签区域共享全局区域的名称服务并具有全局区域的配置文件的只读副本，包括 `/etc/passwd` 和 `/etc/shadow` 文件。如果您打算从有标签区域安装应用程序到该区域，并且软件包将用户添加到该区域，您需要在该区域中有这些文件的可写副本。

`pkg:/service/network/ftp` 等软件包可创建用户帐户。要通过在有标签区域中运行 `pkg` 命令来安装该软件包，需要在该区域中运行单独的 `nscd` 守护进程，并需要为区域指定专用 IP 地址。有关更多信息，请参见第 60 页中的 “如何为每个有标签区域配置单独的名称服务”。

规划多级别服务

缺省情况下，Trusted Extensions 不提供多级别服务。大多数服务可轻松地配置为区域到区域服务，即，单标签服务。例如，每个有标签区域都可以连接到以有标签区域的标签运行的 NFS 服务器。

如果您的站点需要多级别服务，最好在至少具有两个 IP 地址的系统上配置这些服务。可以将多级别服务需要的多级别端口指定给与全局区域关联的 IP 地址。有标签区域可以使用 `all-zones` 地址来访问这些服务。

提示 – 如果有标签区域中的用户不得访问多级别服务，则您可以为系统指定一个 IP 地址。该 Trusted Extensions 配置通常是在手提电脑上使用。

在 Trusted Extensions 中规划 LDAP 命名服务

如果您不打算安装有标签系统的网络，则可以跳过本节。如果您打算使用 LDAP，则在添加第一个有标签区域之前，您的系统必须配置为 LDAP 客户机。

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

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

在 Trusted Extensions 中规划审计

缺省情况下，会在第一次引导 Trusted Extensions 时启用审计。因此，缺省情况下会审计 `login/logout` 类中的所有事件。要审计负责配置系统的用户，可以在配置过程早期创建角色。当这些角色对系统进行配置时，审计记录会包含承担相应角色的登录用户。请参见第 61 页中的 “在 Trusted Extensions 中创建角色和用户”。

在 Trusted Extensions 中规划审计与在 Oracle Solaris OS 中规划审计一样。有关详细信息，请参见《Oracle Solaris 11.1 管理：安全服务》中的第 VII 部分, “在 Oracle Solaris 中审计”。当 Trusted Extensions 添加类、事件和审计令牌时，软件不会更改审计的管理方式。有关要审计的 Trusted Extensions 添加项，请参见第 22 章，Trusted Extensions 审计（概述）。

在 Trusted Extensions 中规划用户安全

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

表 1–2 Trusted Extensions 用户帐户安全缺省值

文件名	关键字	值
`/etc/security/policy.conf`	`IDLECMD`	`lock|logout`
	`IDLETIME`	`30`
	`CRYPT_ALGORITHMS_ALLOW`	`1,2a,md5,5,6`
	`CRYPT_DEFAULT`	`sha256`
	`LOCK_AFTER_RETRIES`	`no|yes`
	`PRIV_DEFAULT`	`basic`
	`PRIV_LIMIT`	`all`
	`AUTHS_GRANTED`	`solaris.device.cdrw`
	`CONSOLE_USER`	`Console User`
	`PROFS_GRANTED`	`Basic Solaris User`
`/etc/security/tsol/label_encodings` 的 LOCAL DEFINITIONS 部分	Default User Clearance	`CNF: INTERNAL USE ONLY`（CNF：仅供内部使用）
	Default User Sensitivity Label	`PUBLIC`

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

系统管理员可以设置一个标准用户模板，该模板可为每个用户设置适当的系统缺省值。例如，缺省情况下每个用户的初始 shell 为 bash shell。系统管理员可以设置一个为每个用户提供一个 pfbash shell 的模板。

为 Trusted Extensions 成立一个安装团队

下面按从最安全到最不安全的顺序介绍了配置策略：

- 两人团队合作配置软件。审计配置过程。

  启用软件时有两个人在计算机上。在配置过程的早期阶段，此团队可以创建独立的角色以及可承担这些角色的本地用户。该团队还可以设置审计来审计角色执行的事件。在为用户分配角色并重新引导计算机之后，用户将登录并承担受限制的角色。软件强制实施按角色进行任务划分。审计迹可提供配置过程的记录。有关安全配置过程的说明，请参见图 1–1。

- 一个人通过指定适当的角色来启用和配置软件。审计配置过程。

  在配置过程的早期阶段，root 角色创建了附加角色。root 角色还可以设置审计来审计角色执行的事件。在为初始用户指定这些附加角色并重新引导计算机之后，用户将登录并承担适当角色以执行当前任务。审计迹可提供配置过程的记录。

- 一个人通过承担 root 角色来启用和配置软件。不审计配置过程。

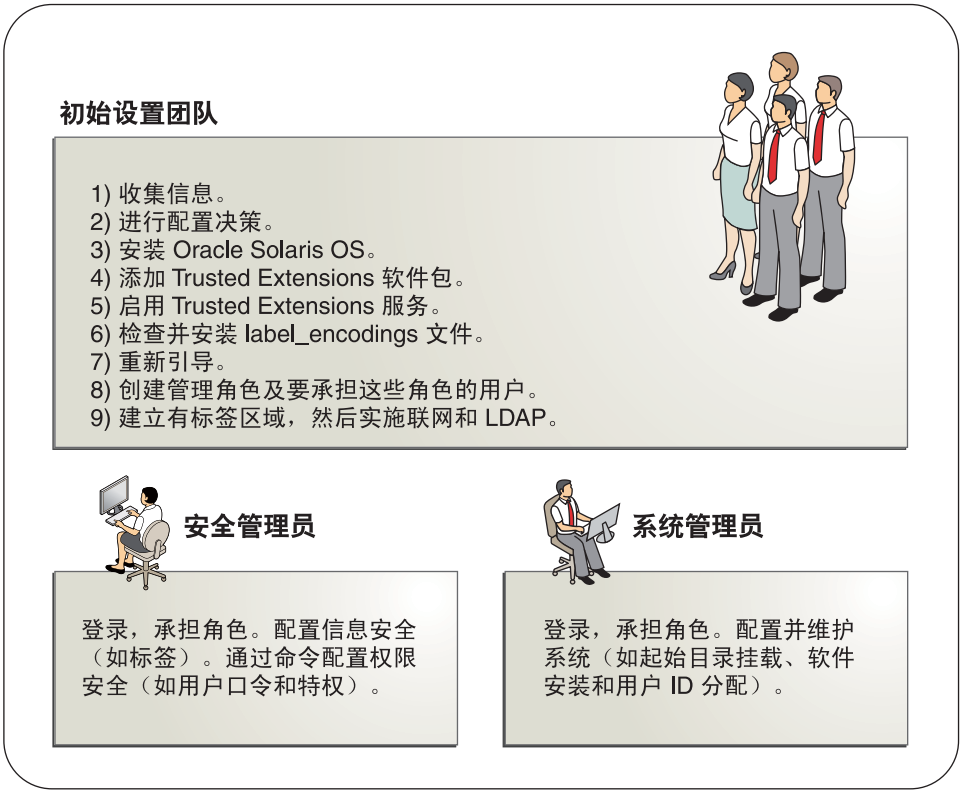
  通过使用此策略，不会记录配置过程。

- 初始设置团队将 root 角色更改为用户。

  不会在软件中记录充当 root 的用户的名称。无显示系统的远程管理可能需要该设置。

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

图 1–1 管理 Trusted Extensions 系统：按角色划分的任务



在启用 Trusted Extensions 之前解决其他问题

配置 Trusted Extensions 之前，必须采取物理措施保护系统，决定将哪些标签附加到区域并解决其他安全问题。有关过程，请参见第 42 页中的 “在启用 Trusted Extensions 之前解决安全问题”。

在启用 Trusted Extensions 之前备份系统

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

启用 Trusted Extensions 的结果（从管理员角度）

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

- 安装并配置 Oracle label_encodings file（label_encodings 文件）。
- 可信桌面 Solaris Trusted Extensions (GNOME) 创建有标签窗口环境，可在全局区域中提供管理工作区。这些工作区受可信路径（在可信窗口条中可见）保护。
- 与在 Oracle Solaris OS 中一样，定义角色的权限配置文件。与在 Oracle Solaris OS 中一样，`root` 是唯一定义的角色。

  要使用附加角色管理 Trusted Extensions，必须创建角色。在配置期间，请创建安全管理员角色。
- 添加三个 Trusted Extensions 网络数据库 `tnrhdb`、`tnrhtp` 和 `tnzonecfg`。使用 `tncfg` 命令，管理员可以查看和修改这些可信数据库。
- Trusted Extensions 提供了 GUI 以管理系统。有关完整列表，请参见第 7 章，Trusted Extensions 管理工具。
  - 通过 `txzonemgr` 脚本，管理员可以配置 Trusted Extensions 区域和网络。有关更多信息，请参见 `txzonemgr(1M)` 手册页。
  - "Device Manager"（设备管理器）管理所连接设备的分配和标签设置。

◆ ◆ ◆ 第 2 章

Trusted Extensions 的配置任务列表

本章概述了用于启用和配置 Oracle Solaris 的 Trusted Extensions 功能的任务。

注意 – 如果您要远程启用和配置 Trusted Extensions，请在引导至 Trusted Extensions 环境之前，仔细查看第 12 章，Trusted Extensions 中的远程管理（任务）。

任务列表：准备和启用 Trusted Extensions

要准备系统并启用 Trusted Extensions，请完成以下任务。

任务	参考
■ 准备现有的 Oracle Solaris 安装以使用 Trusted Extensions ■ 安装 Oracle Solaris OS 时考虑 Trusted Extensions。	■ 第 40 页中的 “准备已安装的 Oracle Solaris 系统以使用 Trusted Extensions” ■ 第 39 页中的 “安全安装 Oracle Solaris 系统”
收集信息，然后针对您的系统和 Trusted Extensions 网络做出决策。	第 42 页中的 “在启用 Trusted Extensions 之前解决安全问题”
启用 Trusted Extensions。	第 43 页中的 “启用 Trusted Extensions 并重新引导”

任务列表：选择 Trusted Extensions 配置

使用以下任务列表中的方法之一，在您的系统中配置 Trusted Extensions。

任务	参考
创建演示 Trusted Extensions 系统。	第 36 页中的 “任务列表：使用提供的缺省设置配置 Trusted Extensions”

任务	参考
创建企业 Trusted Extensions 系统。	第 36 页中的 “任务列表：配置 Trusted Extensions 以满足站点要求”
在远程系统上配置 Trusted Extensions。	启用 Trusted Extensions，但不重新引导。按照第 12 章，Trusted Extensions 中的远程管理（任务）中的说明执行操作。然后，继续按照针对带有显示器的系统的说明执行操作。
在 Oracle 的 Sun Ray 服务器上配置 Trusted Extensions。	请参见《Sun Ray Server Software 4.1 Installation and Configuration Guide for the Solaris Operating System》。有关 Sun Ray 5 发行版的信息，请参见 the Sun Ray Server 4.2 and Sun Ray Connector 2.2 Documentation (`http://wikis.sun.com/display/SRS/Home`)（Sun Ray Server 4.2 和 Sun Ray Connector 2.2 文档）Web 站点。该服务器和客户机共同构成 Sun Ray 5 软件包。 要配置初始客户机服务器通信，请参见第 193 页中的 “为主机和网络设置标签（任务）”。

任务列表：使用提供的缺省设置配置 Trusted Extensions

对于缺省配置，请依序执行以下任务。

任务	参考
装入 Trusted Extensions 软件包。	第 41 页中的 “将 Trusted Extensions 软件包添加到 Oracle Solaris 系统”
启用 Trusted Extensions 并重新引导。	第 43 页中的 “启用 Trusted Extensions 并重新引导”
登录。	第 44 页中的 “登录到 Trusted Extensions”
创建两个有标签区域。	第 51 页中的 “如何创建缺省 Trusted Extensions 系统” 或第 52 页中的 “如何以交互方式创建有标签区域”
为区域创建有标签工作区。	第 54 页中的 “如何将标签指定给两个区域工作区”

任务列表：配置 Trusted Extensions 以满足站点要求

提示 – 对于安全配置过程，请在过程的早期阶段创建角色。

以下任务列表显示了任务顺序。

- 需要执行第 51 页中的 “创建有标签区域”中的任务。
- 根据站点的要求，执行其他配置任务。

任务	参考
配置全局区域。	第 47 页中的 “在 Trusted Extensions 中设置全局区域”
配置有标签区域。	第 51 页中的 “创建有标签区域”
要与其他系统进行通信，请设置网络。	第 55 页中的 “在 Trusted Extensions 中配置网络接口”
配置 LDAP 命名服务。 **注 –** 如果未使用 LDAP，请跳过。	第 5 章，为 Trusted Extensions 配置 LDAP（任务）
完成系统配置。	第 2 部分

◆ ◆ ◆ 第 3 章

将 Trusted Extensions 功能添加到 Oracle Solaris（任务）

本章介绍了如何在 Oracle Solaris 系统中准备和启用 Trusted Extensions 服务。本章包含以下主题：

- 第 39 页中的 “初始设置团队的职责”
- 第 39 页中的 “准备 Oracle Solaris 系统和添加 Trusted Extensions”
- 第 42 页中的 “在启用 Trusted Extensions 之前解决安全问题”

初始设置团队的职责

Trusted Extensions 功能设计为由两名具有不同分工的人员进行配置。此任务分工可按角色执行。由于不同的角色和其他用户都是安装之后才创建的，因此建立一个至少有两名人员的initial setup team（初始设置团队）来负责启用和配置 Trusted Extensions 是一个不错的做法。

准备 Oracle Solaris 系统和添加 Trusted Extensions

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

- 要正确支持 Trusted Extensions，您必须安全安装底层 Oracle Solaris OS。有关影响 Trusted Extensions 的 Oracle Solaris 安装选项的信息，请参见第 39 页中的 “安全安装 Oracle Solaris 系统”。
- 如果已经在使用 Oracle Solaris OS，请检查当前的配置是否符合 Trusted Extensions 的要求。有关影响 Trusted Extensions 的因素，请参见第 40 页中的 “准备已安装的 Oracle Solaris 系统以使用 Trusted Extensions”。

▼ 安全安装 Oracle Solaris 系统

此任务适用于 Oracle Solaris 的全新安装。如果是在进行升级，请参见第 40 页中的 “准备已安装的 Oracle Solaris 系统以使用 Trusted Extensions”。

1. **安装 Oracle Solaris OS 时，请创建用户帐户和 root 角色帐户。**
   在 Trusted Extensions 中，您使用 root 角色以及创建的角色来配置系统。

2. **首次登录到 Oracle Solaris 时，请将口令指定给 root 角色帐户。**

   a. **打开终端窗口。**

   b. **承担 root 角色。**
      在出现提示时，提供不同于用户帐户口令的口令。

```
% su -
Your password has expired. Create a new password.
Enter new password:      Type a password for root
Retype the password:      Retype the root password
#
```

      指定至少包含六个字母数字字符的口令。口令必须难以猜出，从而减少通过试猜口令而让有敌意的人获取未经授权访问的机会。

接下来的步骤 继续执行第 41 页中的 “将 Trusted Extensions 软件包添加到 Oracle Solaris 系统”中的相关操作。

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

此任务适用于已在使用中、而且计划要在其上运行 Trusted Extensions 的 Oracle Solaris 系统。

开始之前 您必须在全局区域中承担 root 角色。

1. **如果您的系统上安装了非全局区域，则请将其删除。**
   Trusted Extensions 有标签标记是区域的专用标记。请参阅 brands(5) 和 trusted_extensions(5) 手册页。

2. **如果您的系统没有 root 口令，则请创建一个。**

注 – 用户不得将其口令透露给他人，因为这可能会让他人有权访问用户数据，并将无法唯一标识该人，或者无法追究其责任。请注意，这种泄露可能是直接的，比如用户故意将自己的口令泄露给他人；也可能是间接的，比如，因为写下了口令或选择了不安全的口令。Oracle Solaris 阻止使用不安全的口令，但无法阻止用户泄露自己的口令或将其写下。

接下来的步骤 继续执行第 41 页中的 “将 Trusted Extensions 软件包添加到 Oracle Solaris 系统”中的相关操作。

▼ 将 Trusted Extensions 软件包添加到 Oracle Solaris 系统

开始之前 您已完成第 40 页中的 “准备已安装的 Oracle Solaris 系统以使用 Trusted Extensions”或第 39 页中的 “安全安装 Oracle Solaris 系统”。

您必须指定有 "Software Installation"（软件安装）权限配置文件。

1. **以初始用户身份登录后，在终端窗口中承担 root 角色。**

```
% su -
Enter Password:       Type root password
#
```

2. **下载并安装 Trusted Extensions 软件包。**

使用命令行或软件包管理器 GUI。

- **在终端窗口中，使用 pkg install 命令。**

```
$ pkg install system/trusted/trusted-extensions
```

要安装可信语言环境，请指定语言环境的短名称。例如，使用以下命令可安装日文语言环境：

```
$ pkg install system/trusted/locale/ja &
```

- **在终端窗口中，启动软件包管理器 GUI。**

```
$ packagemanager &
```

a. **选择 Trusted Extensions 软件包。**

i. **显示 "Desktop (GNOME)"（桌面 (GNOME)）类别下的类别。**

ii. **选择 Trusted Extensions 类别。**

iii. **在软件包列表中，单击 trusted-extensions 对应的复选框。**

iv. **可选在软件包列表中，单击要安装的任何语言环境对应的复选框。**

b. **要添加软件包，请单击 "Install/Update"（安装/更新）图标。**

在启用 Trusted Extensions 之前解决安全问题

对于要配置 Trusted Extensions 的每个系统，需要做出一些配置决策。例如，您需要确定是安装缺省 Trusted Extensions 配置还是定制配置。

▼ 在启用 Trusted Extensions 之前确保系统硬件安全并做出安全决策

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

1 **确定系统硬件需要得到何种安全程度的保护。**

在安全站点，将对每个 Oracle Solaris 系统执行此步骤。

- 对于 SPARC 系统，选择 PROM 安全级别并提供口令。
- 对于 x86 系统，保护 BIOS。
- 在所有系统中，使用口令保护 `root`。

2 **准备 `label_encodings` 文件。**

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

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

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

对于缺省 `label_encodings` 文件，标签如下所示，且区域名称类似于以下内容：

完整标签名称	建议的区域名称
`PUBLIC`	`public`
`CONFIDENTIAL: INTERNAL USE ONLY`	`internal`
`CONFIDENTIAL: NEED TO KNOW`	`needtoknow`
`CONFIDENTIAL: RESTRICTED`	`restricted`

注 – 自动配置方法将创建 `public` 和 `internal` 区域。

4 **确定何时创建角色。**

您的站点的安全策略可能会要求您通过承担某个角色来管理 Trusted Extensions。如果是这样，或者如果您要配置系统来满足某个已评估配置的条件，您就必须在配置过程的早期阶段创建这些角色。

如果不要求您通过使用不同角色来配置系统，您可以选择以 `root` 角色配置系统。这种配置方式不太安全。`root` 角色可以在系统上执行所有任务，而其他角色通常执行一组受到更多限制的任务。因此，由您创建的角色执行的配置更容易控制。

5 **确定每个系统和网络的其他安全问题。**

例如，您可能会考虑下列安全问题：

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

启用 Trusted Extensions 服务并登录

在 Oracle Solaris OS 中，Trusted Extensions 是由服务管理工具 (Service Management Facility, SMF) 管理的一种服务。该服务的名称是 `svc:/system/labeld:default`。缺省情况下，`labeld` 服务被禁用。

注 – 您的 Trusted Extensions 系统具有直接连接的位映射显示屏幕（如手提电脑或工作站）时，不需要网络就可运行桌面。需要进行网络配置才能与其他系统进行通信。

▼ 启用 Trusted Extensions 并重新引导

`labeld` 服务向通信端点添加标签。例如，会为以下项添加标签：

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

开始之前 您已完成第 39 页中的 “准备 Oracle Solaris 系统和添加 Trusted Extensions”和第 42 页中的 “在启用 Trusted Extensions 之前解决安全问题”中的任务。

您必须在全局区域中承担 `root` 角色。

1 **将面板从屏幕顶部移至屏幕底部。**

注意 – 如果您无法移动面板，您可能在登录到 Trusted Extensions 后无法访问桌面的主菜单或面板。

a. **打开 "Terminal"（终端）窗口并转到 `/etc/gconf/2` 目录。**

```
# cd /etc/gconf/2
```

b. **激活这两个 `trusted-extensions-desktop` 。**

```
# cp local-trusted-extensions-desktop-defaults.path.inactive \
local-trusted-extensions-desktop-defaults.path
# cp local-trusted-extensions-desktop-mandatory.path.inactive \
local-trusted-extensions-desktop-mandatory.path
```

2 **打开终端窗口并启用 `labeld` 服务。**

```
# svcadm enable -s labeld
```

`labeld` 服务将标签添加到系统，并启动设备分配服务。

注意 – 在光标返回到提示符之前，不要在系统上执行其他任务。

3 **验证是否已启用该服务。**

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

注意 – 如果您要远程启用和配置 Trusted Extensions，请仔细查看第 12 章，Trusted Extensions 中的远程管理（任务）。在配置系统以允许远程管理之前，不要执行重新引导。如果未配置 Trusted Extensions 系统以进行远程管理，您将无法从远程系统对其进行访问。

4 **重新引导系统。**

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

接下来的步骤 继续执行第 44 页中的 “登录到 Trusted Extensions”中的相关操作。

▼ 登录到 Trusted Extensions

登录后，您将在全局区域中，这是识别和执行强制访问控制 (mandatory access control, MAC) 的环境。

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

开始之前 您已完成第 43 页中的 “启用 Trusted Extensions 并重新引导”。

1. **使用在安装期间创建的用户帐户登录。**

   在登录对话框中，键入 *username*，然后键入口令。

   用户不得将其口令透露给他人，因为这可能会让他人有权访问用户数据，并将无法唯一标识该人，或者无法追究其责任。请注意，这种泄露可能是直接的，比如用户故意将自己的口令泄露给他人；也可能是间接的，比如，因为写下了口令或选择了不安全的口令。Trusted Extensions 阻止使用不安全的口令，但无法阻止用户泄露自己的口令或将其写下。

2. **使用鼠标关闭 "Status"（状态）窗口和 "Clearance"（安全许可）窗口。**

3. **关闭显示标签 PUBLIC 没有匹配区域的对话框。**

   承担 root 角色后，将创建区域。

4. **承担 root 角色。**

   a. **在可信窗口条中，单击您的名称。**

      此时下拉式菜单中将显示 root 角色。

   b. **选择 root 角色。**

      如果出现提示，请为该角色创建一个新口令。

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

接下来的步骤 继续执行以下操作之一：

- 要配置缺省系统，请转至第 51 页中的 “创建有标签区域”
- 要在创建有标签区域之前定制系统，请转至第 47 页中的 “在 Trusted Extensions 中设置全局区域”。
- 如果您的系统没有显示图形，请转至第 12 章，Trusted Extensions 中的远程管理（任务）。

◆ ◆ ◆ 第 4 章

4 配置 Trusted Extensions（任务）

本章介绍了如何在具有监视器的系统上配置 Trusted Extensions。要正常运行，Trusted Extensions 软件需要配置标签和区域。也可以配置网络通信、角色和可承担角色的用户。

- 第 47 页中的 “在 Trusted Extensions 中设置全局区域”
- 第 51 页中的 “创建有标签区域”
- 第 61 页中的 “在 Trusted Extensions 中创建角色和用户”
- 第 67 页中的 “在 Trusted Extensions 中创建集中起始目录”
- 第 69 页中的 “Trusted Extensions 配置故障排除”
- 第 70 页中的 “其他 Trusted Extensions 配置任务”

有关其他配置任务，请参见第 2 部分。

在 Trusted Extensions 中设置全局区域

要定制 Trusted Extensions 配置，请执行以下任务列表中的过程。要安装缺省配置，请转至第 51 页中的 “创建有标签区域”。

任务	说明	参考
保护硬件。	要求输入口令才能更改硬件设置，以保护硬件。	《Oracle Solaris 11.1 管理：安全服务》中的“控制对系统硬件的访问（任务）”
配置标签。	**必须**为您的站点配置标签。如果打算使用缺省 `label_encodings` 文件，可以跳过此步骤。	第 48 页中的 “如何检查并安装标签编码文件”
配置 IPv6 网络。	启用与 Trusted Extensions IPv6 CIPSO 网络的兼容性。	第 50 页中的 “如何在 Trusted Extensions 中配置 IPv6 CIPSO 网络”
更改 DOI。	指定值不是 1 的系统解释域 (Domain of Interpretation, DOI)。	第 50 页中的 “如何配置其他系统解释域”

任务	说明	参考
配置 LDAP 服务器。	配置 Trusted Extensions LDAP 目录服务器。	第 5 章，为 Trusted Extensions 配置 LDAP（任务）
配置 LDAP 客户机。	使此系统成为 Trusted Extensions LDAP 目录服务器的客户机。	第 87 页中的 “使全局区域成为 Trusted Extensions 中的客户机”

▼ 如何检查并安装标签编码文件

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

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

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

注意 – 在继续之前，**必须**成功安装标签，否则配置将失败。

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

要编辑 `label_encodings` 文件，您必须承担 `root` 角色。

1. **将 `label_encodings` 文件复制到磁盘上。**

   要从便携介质复制，请参见第 75 页中的 “如何在 Trusted Extensions 中从便携介质复制文件”。

2. **在终端窗口中，检查文件的语法。**

   a. **运行 `chk_encodings` 命令。**

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

   b. **读取输出结果并执行以下操作之一：**

   - **解决错误。**

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

- **使该文件成为活动的 `label_encodings` 文件。**

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

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

示例 4–1 **检查命令行上的 `label_encodings` 语法**

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

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

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

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

---> VERSION = MYCOMPANY LABEL ENCODINGS  2.0 10/10/2010

---> CLASSIFICATIONS <---

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

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

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

```
# cp /var/encodings/label_encodings2 /etc/security/tsol/label.encodings.10.10.10
# cd /etc/security/tsol
# cp label_encodings label_encodings.tx.orig
# cp label.encodings.10.10.10 label_encodings
```

最后，管理员检验 `label_encodings` 文件是否为公司文件。

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

---> VERSION = MYCOMPANY LABEL ENCODINGS  2.0 10/10/2010
```

接下来的步骤 必须重新引导系统，才可创建有标签区域。

▼ 如何在 Trusted Extensions 中配置 IPv6 CIPSO 网络

对于 IPv6，Trusted Extensions 将通用体系结构标签 IPv6 安全选项 (Common Architecture Label IPv6 Security Option, CALIPSO) 用作安全标签协议。不需要进行配置。如果必须与运行过时 Trusted Extensions IPv6 CIPSO 协议的系统进行通信，请执行此过程。要与其他 CALIPSO 系统通信，请勿执行此过程。

注意 – 将 CALIPSO 用作 IPv6 协议的系统无法与使用过时 TX IPv6 CIPSO 协议的任何系统进行通信，因为这些协议不兼容。

过时的 Trusted Extensions IPv6 CIPSO 选项没有 Internet 号码分配机构 (Internet Assigned Numbers Authority, IANA) 编号可供在包的 "IPv6 Option Type"（IPv6 选项类型）字段中使用。您在此过程中设置的项会提供一个可在本地网络中使用的编号。

开始之前 如果必须与使用专用但过时的 Trusted Extensions IPv6 CIPSO 安全标签选项的系统进行通信，请执行此过程。

您是全局区域中的 `root` 角色。

- **将以下项键入到 `/etc/system` 文件中：**

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

故障排除 如果在引导过程中出现错误消息，指出 IPv6 CIPSO 配置不正确，请更正该项。例如，拼写错误的项会生成以下消息：`sorry, variable 'ip6opt_1d' is not defined in the 'ip' module. Verify that the entry is spelled correctly`。

- 更正项。
- 检验将正确的项添加到 `/etc/system` 文件后是否重新引导了系统。

接下来的步骤 必须重新引导系统，才可创建有标签区域。

▼ 如何配置其他系统解释域

如果您的站点未使用值为 1 的系统解释域 (Domain of Interpretation, DOI)，必须修改每个 security template（安全模板）中的 `doi` 值。有关更多信息，请参见第 181 页中的 “安全模板中的系统解释域”。

开始之前 您是全局区域中的 `root` 角色。

- **在缺省安全模板中指定 DOI 值。**

```
# tncfg -t cipso set doi=n
# tncfg -t admin_low set doi=n
```

注 – 每个安全模板都必须指定 DOI 值。

另请参见
- 第 180 页中的 “Trusted Extensions 中的网络安全属性”
- 第 196 页中的 “如何创建安全模板”

接下来的步骤 如果打算使用 LDAP，请转至第 5 章，为 Trusted Extensions 配置 LDAP（任务）。必须配置 LDAP，才可创建有标签区域。

否则，继续执行第 51 页中的 “创建有标签区域”中的相关操作。

创建有标签区域

本节中的说明用于配置有标签区域。可选择自动创建两个有标签区域或手动创建区域。

注 – 如果打算使用 LDAP，请转至第 5 章，为 Trusted Extensions 配置 LDAP（任务）。必须配置 LDAP，才可创建有标签区域。

任务	说明	参考
1a. 创建缺省 Trusted Extensions 配置。	`txzonemgr -c` 命令会从 `label_encodings` 文件创建两个有标签区域。	第 51 页中的 “如何创建缺省 Trusted Extensions 系统”
1b. 使用 GUI 创建缺省 Trusted Extensions 配置。	`txzonemgr` 脚本会创建一个 GUI，用于在配置系统时提供相应的任务。	第 52 页中的 “如何以交互方式创建有标签区域”
1c. 手动分步完成区域创建过程。	`txzonemgr` 脚本会创建一个 GUI，用于在配置系统时提供相应的任务。	第 52 页中的 “如何以交互方式创建有标签区域”
2. 创建一个有效的有标签环境。	在缺省配置中，将两个工作区的标签设置为 `PUBLIC` 和 `INTERNAL USE ONLY`。	第 54 页中的 “如何将标签指定给两个区域工作区”
3.（可选）连接到网络中的其他系统。	配置有标签区域网络接口，并将全局区域和有标签区域连接到其他系统。	第 55 页中的 “在 Trusted Extensions 中配置网络接口”

▼ 如何创建缺省 Trusted Extensions 系统

使用此过程可创建含有两个有标签区域的有效 Trusted Extensions 系统。尚未将远程主机指定给系统的安全模板，因此系统无法与任何远程主机进行通信。

开始之前 您已完成第 44 页中的 “登录到 Trusted Extensions”。您已承担 `root` 角色。

1. **在第四个工作区中打开一个终端窗口。**

2. **可选查看 `txzonemgr` 手册页。**

   ```
   # man txzonemgr
   ```

3. **创建缺省配置。**

   ```
   # /usr/sbin/txzonemgr -c
   ```

   此命令将 Oracle Solaris OS 和 Trusted Extensions 软件复制到区域、创建区域的快照、为原始区域设置标签，然后使用快照创建第二个有标签区域。将引导区域。

   - 第一个有标签区域基于 `label_encodings` 文件中的 `Default User Sensitivity Label`（缺省用户敏感标签）值。
   - 第二个有标签区域基于 `label_encodings` 文件中的 `Default User Clearance`（缺省用户安全许可）值。

   此步骤可能需要大约 20 分钟。要安装区域，脚本将针对有标签区域使用全局区域的 root 口令。

接下来的步骤 要使用 Trusted Extensions 配置，请转至第 54 页中的 “如何将标签指定给两个区域工作区”。

▼ 如何以交互方式创建有标签区域

您不必为 `label_encodings` 文件中的每个标签创建一个区域，但您可以这样做。管理 GUI 会枚举可在此系统上为其创建区域的标签。在此过程中，您将创建两个有标签区域。如果您使用 Trusted Extensions `label_encodings` 文件，将创建缺省 Trusted Extensions 配置。

开始之前 您已完成第 44 页中的 “登录到 Trusted Extensions”。您已承担 `root` 角色。

您尚未创建区域。

1. **运行不带任何选项的 `txzonemgr` 命令。**

   ```
   # txzonemgr &
   ```

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

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

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

2 选择以下方法之一安装区域：

- **要创建两个有标签区域，请从对话框中选择 `public and internal zones`（公共区域和内部区域）。**
  - 第一个有标签区域基于 `label_encodings` 文件中的 `Default User Sensitivity Label`（缺省用户敏感标签）值。
  - 第二个有标签区域基于 `label_encodings` 文件中的 `Default User Clearance`（缺省用户安全许可）值。

  a. 应答提示以标识系统。

  如果 `public`（公共）区域使用专用 IP 栈，或者该区域具有在 DNS 中定义的 IP 地址，请使用在 DNS 中定义的主机名。否则，使用系统的名称。

  b. 请勿应答提供 root 口令的提示。

  root 口令在系统安装时进行了设置。此提示的输入将失败。

  c. 出现区域登录提示时，键入用户登录名和口令。

  然后，运行 `svcs -x` 命令以检验是否是否配置了所有的服务。如果未显示任何消息，则说明已配置所有的服务。

  d. 从区域注销并关闭窗口。

  出现提示时，键入 "exit"，然后从 "Zone Console"（区域控制台）选择 "Close"（关闭）窗口。

  在另一个窗口中，第二个区域安装已完成。该区域是基于快照构建的，因此构建速度很快。

  e. 登录到第二个区域控制台并检验所有的服务是否正在运行。

  ```
  # svcs -x
  #
  ```

  如果未显示任何消息，则说明已配置所有的服务。将显示 "Labeled Zone Manager"（有标签区域管理器）。

  f. 双击 "Labeled Zone Manager"（有标签区域管理器）中的内部区域。

  选择 "Reboot"（重新引导），然后单击 "Cancel"（取消）按钮返回到主屏幕。所有区域都正在运行。无标签快照未在运行。

- **要手动创建区域，请选择 "Main Menu"（主菜单），然后选择 "Create a Zone"（创建区域）。**

  按照提示进行操作。GUI 将引导您完成区域创建过程。

  创建和引导区域后，可返回到全局区域以创建更多区域。这些区域都是基于快照创建的。

示例 4–2 **创建另一个有标签区域**

在此示例中，管理员通过缺省 `label_encodings` 文件创建受限区域。

首先，管理员以交互式模式打开 `txzonemgr` 脚本。

```
# txzonemgr &
```

接着，管理员导航到全局区域，并创建名为 `restricted`（受限）的区域。

```
Create a new zone:restricted
```

然后，管理员应用正确的标签。

```
Select label:CNF : RESTRICTED
```

管理员从列表中选择 "Clone"（克隆）选项，随后选择 `snapshot`（快照）作为新区域的模板。

`restricted`（受限）区域可用后，管理员单击 "Boot"（引导）来引导第二个区域。

要能够访问 `restricted`（受限）区域，管理员将 `label_encodings` 文件中的 `Default User Clearance`（缺省用户安全许可）值更改为 `CNF RESTRICTED`（CNF 受限）。

▼ 如何将标签指定给两个区域工作区

此过程将创建两个有标签工作区，并在每个有标签工作区中打开一个有标签窗口。此任务完成后，您将具有一个有效的未联网 Trusted Extensions 系统。

开始之前 您已完成第 51 页中的 “如何创建缺省 Trusted Extensions 系统”或第 52 页中的 “如何以交互方式创建有标签区域”。

您是初始用户。

1. **创建一个 `PUBLIC`（公共）工作区。**

   `PUBLIC`（公共）工作区的标签与 `Default User Sensitivity Label`（缺省用户敏感标签）对应。

   a. **切换到第二个工作区。**

b. **右键单击并选择 "Change Workspace Label"（更改工作区标签）。**

c. **选择 "PUBLIC"（公共）并单击 "OK"（确定）。**

2 **在出现提示时提供您的口令。**
您位于 PUBLIC（公共）工作区中。

3 **打开终端窗口。**
窗口标签为 PUBLIC（公共）。

4 **创建一个 "INTERNAL USE ONLY"（仅供内部使用）工作区。**
如果您使用特定于站点的 label_encodings 文件，将基于 Default User Clearance（缺省用户安全许可）的值创建工作区。

a. **切换到第三个工作区。**

b. **右键单击并选择 "Change Workspace Label"（更改工作区标签）。**

c. **选择 "INTERNAL USE ONLY"（仅供内部使用）并单击 "OK"（确定）。**

5 **在出现提示时提供您的口令。**
您位于 INTERNAL（内部）工作区中。

6 **打开终端窗口。**
窗口标签为 Confidential: Internal Use Only（机密：仅供内部使用）。

您的系统已可供使用。您有两个用户工作区和一个角色工作区。在该配置中，有标签区域将与全局区域使用同一个 IP 地址与其他系统进行通信。之所以可以这样做，是因为在缺省情况下，它们将该 IP 地址作为 all-zones 接口共享。

接下来的步骤 如果您打算使 Trusted Extensions 系统与其他系统进行通信，请转至第 55 页中的 “在 Trusted Extensions 中配置网络接口”。

在 Trusted Extensions 中配置网络接口

您的 Trusted Extensions 系统具有直接连接的位映射显示屏幕（如手提电脑或工作站）时，不需要网络就可运行桌面。但是，需要进行网络配置才能与其他系统进行通信。通过使用 txzonemgr GUI，可以轻松配置有标签区域和全局区域以连接到其他系统。有关有标签区域的配置选项的说明，请参见第 29 页中的 “访问有标签区域”。以下任务列表介绍了网络配置任务，并提供了指向这些任务的链接。

任务	说明	参考
为一般用户配置缺省系统。	系统有一个 IP 地址并使用 `all-zones` 接口在有标签区域与全局区域之间进行通信。将使用同一 IP 地址与远程系统进行通信。	第 56 页中的 “如何在所有区域中共享单个 IP 地址”
将 IP 地址添加到全局区域中。	系统有多个 IP 地址，并使用全局区域的专用 IP 地址访问专用子网。有标签区域无法访问此子网。	第 56 页中的 “如何在所有区域中共享单个 IP 地址”
将 IP 地址指定给每个区域（如果区域共享 IP 栈）。	系统有多个 IP 地址。在最简单的情况下，区域共享一个物理接口。	第 57 页中的 “如何将 IP 实例添加到有标签区域中”
针对每个区域将 `all-zones` 接口添加到 IP 实例。	系统可以为其有标签区域提供特权服务，这些服务是受保护的，可免受远程攻击。	第 57 页中的 “如何将 IP 实例添加到有标签区域中”
将 IP 地址指定给每个区域（如果 IP 栈是专用的）。	为每个区域（包括全局区域）指定一个 IP 地址。为每个有标签区域创建 VNIC。	第 58 页中的 “如何将虚拟网络接口添加到有标签区域”
将区域连接到远程区域。	此任务用于配置有标签区域和全局区域的网络接口，以访问同一标签下的远程系统。	第 59 页中的 “如何将 Trusted Extensions 系统连接到其他 Trusted Extensions 系统”
针对每个区域运行单独的 `nscd` 守护进程。	在每个子网都具有其自己的名称服务器的环境中，此任务用于针对每个区域配置一个 `nscd` 守护进程。	第 60 页中的 “如何为每个有标签区域配置单独的名称服务”

▼ 如何在所有区域中共享单个 IP 地址

通过此过程，系统中的每个区域可以使用一个 IP 地址（即全局区域的 IP 地址），以访问其他有相同标签的区域或主机。此配置是缺省配置。如果以不同方式配置了网络接口，并希望将系统恢复为缺省网络配置，则必须完成此过程。

开始之前 您必须在全局区域中承担 `root` 角色。

1. **运行不带任何选项的 `txzonemgr` 命令。**

   ```
   # txzonemgr &
   ```

   此时将在 "Labeled Zone Manager"（有标签区域管理器）中显示区域列表。有关此 GUI 的信息，请参见第 52 页中的 “如何以交互方式创建有标签区域”。

2. **双击全局区域。**

3. **双击 "Configure Network Interfaces"（配置网络接口）。**

   此时将显示接口列表。查找列有以下特征的接口：

   - 类型为 `phys`
   - 您的主机名对应的 IP 地址

- 状态为 up

4 **选择与您的主机名对应的接口。**

5 **从命令列表中，选择 "Share with Shared-IP Zones"（与共享 IP 的区域进行共享）。**
所有区域均可使用此共享 IP 地址与相应标签下的远程系统进行通信。

6 **单击 "Cancel"（取消），返回到区域命令列表。**

接下来的步骤 要配置系统的外部网络，请转至第 59 页中的 “如何将 Trusted Extensions 系统连接到其他 Trusted Extensions 系统”。

▼ 如何将 IP 实例添加到有标签区域中

如果使用共享 IP 栈和每区域地址，且计划将有标签区域连接到网络上其他系统中的有标签区域，需要执行此过程。

在此过程中，将为一个或多个有标签区域创建 IP 实例（即，每区域地址）。有标签区域使用其每区域地址与网络上有相同标签的区域进行通信。

开始之前 您必须在全局区域中承担 `root` 角色。

此时将在 "Labeled Zone Manager"（有标签区域管理器）中显示区域列表。要打开此 GUI，请参见第 52 页中的 “如何以交互方式创建有标签区域”。必须停止要配置的有标签区域。

1 **在 "Labeled Zone Manager"（有标签区域管理器）中，双击要向其添加 IP 实例的有标签区域。**

2 **双击 "Configure Network Interfaces"（配置网络接口）。**
此时将显示配置选项列表。

3 **选择 "Add an IP instance"（添加 IP 实例）。**

4 **如果您的系统有多个 IP 地址，请选择具有所需接口的项。**

5 **对于此有标签区域，提供 IP 地址和前缀计数。**
例如，键入 `192.168.1.2/24`。如果不附加前缀计数，系统将提示您输入网络掩码。针对此示例的等效网络掩码为 `255.255.255.0`。

6 **单击 "OK"（确定）。**

7 **要添加缺省路由器，请双击刚刚添加的项。**
在出现提示时，键入路由器的 IP 地址，然后单击 "OK"（确定）。

注 – 要删除或修改缺省路由器，请删除该项，然后重新创建 IP 实例。

---

8 **单击 "Cancel"（取消），返回到区域命令列表。**

接下来的步骤 要配置系统的外部网络，请转至第 59 页中的 “如何将 Trusted Extensions 系统连接到其他 Trusted Extensions 系统”。

▼ 如何将虚拟网络接口添加到有标签区域

如果使用专用 IP 栈和每区域地址，且计划将有标签区域连接到网络上其他系统中的有标签区域，需要执行此过程。

在此过程中，将创建 VNIC 并将其指定给有标签区域。

开始之前 您必须在全局区域中承担 `root` 角色。

此时将在 "Labeled Zone Manager"（有标签区域管理器）中显示区域列表。要打开此 GUI，请参见第 52 页中的 “如何以交互方式创建有标签区域”。必须停止要配置的有标签区域。

1 **在 "Labeled Zone Manager"（有标签区域管理器）中，双击要向其添加虚拟接口的有标签区域。**

2 **双击 "Configure Network Interfaces"（配置网络接口）。**
此时将显示配置选项列表。

3 **双击 "Add a virtual interface (VNIC)"（添加虚拟接口 (VNIC)）。**
如果您的系统有多个 VNIC 卡，将显示多个选项。选择具有所需接口的项。

4 **指定主机名，或指定 IP 地址和前缀计数。**
例如，键入 `192.168.1.2/24`。如果不附加前缀计数，系统将提示您输入网络掩码。针对此示例的等效网络掩码为 `255.255.255.0`。

5 **要添加缺省路由器，请双击刚刚添加的项。**
在出现提示时，键入路由器的 IP 地址，然后单击 "OK"（确定）。

注 – 要删除或修改缺省路由器，请删除该项，然后重新创建 VNIC。

6 **单击 "Cancel"（取消），返回到区域命令列表。**

此时将显示 VNIC 项。系统指定了 *zonename_n* 名称，如 `internal_0`。

接下来的步骤 要配置系统的外部网络，请转至第 59 页中的 “如何将 Trusted Extensions 系统连接到其他 Trusted Extensions 系统”。

▼ 如何将 Trusted Extensions 系统连接到其他 Trusted Extensions 系统

在此过程中，将通过添加 Trusted Extensions 系统可以连接到的远程主机来定义 Trusted Extensions 网络。

开始之前 将显示 "Labeled Zone Manager"（有标签区域管理器）。要打开此 GUI，请参见第 52 页中的 “如何以交互方式创建有标签区域”。您是全局区域中的 `root` 角色。

1 **在 "Labeled Zone Manager"（有标签区域管理器）中，双击全局区域。**

2 **选择 "Add Multilevel Access to Remote Host"（添加对远程主机的多级别访问）。**

   a. **键入另一个 Trusted Extensions 系统的 IP 地址。**

   b. **在另一个 Trusted Extensions 系统上运行相应的命令。**

3 **单击 "Cancel"（取消），返回到区域命令列表。**

4 **在 "Labeled Zone Manager"（有标签区域管理器）中，双击有标签区域。**

5 **选择 "Add Access to Remote Host"（添加对远程主机的访问）。**

   a. **键入另一个 Trusted Extensions 系统上有相同标签的区域的 IP 地址。**

   b. **在另一个 Trusted Extensions 系统的区域中运行相应的命令。**

另请参见

- 第 15 章，可信网络（概述）
- 第 193 页中的 “为主机和网络设置标签（任务）”

▼ 如何为每个有标签区域配置单独的名称服务

此操作过程可在每个有标签区域中配置单独的名称服务守护进程 (nscd)。此配置支持满足以下条件的环境：其中的每个区域都连接到一个以区域的标签运行的子网，并且该子网拥有自己的用于该标签的命名服务器。在有标签区域中，如果您打算安装需要使用该标签的用户帐户的软件包，可能需要针对每个区域配置单独的名称服务。有关背景信息，请参见第 30 页中的 “限制到有标签区域的应用程序”和第 123 页中的 “在 Trusted Extensions 中创建用户之前要做的决策”。

开始之前 将显示 "Labeled Zone Manager"（有标签区域管理器）。要打开此 GUI，请参见第 52 页中的 “如何以交互方式创建有标签区域”。您是全局区域中的 root 角色。

1. **在 "Labeled Zone Manager"（有标签区域管理器）中，选择 "Configure per-zone name service"（配置每区域名称服务），然后单击 "OK"（确定）。**

   注 – 此选项规定为在初始系统配置过程中使用一次。

2. **配置每个区域的 nscd 服务。**

   有关帮助，请参见 nscd(1M) 手册页。

3. **重新引导系统。**

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

   重新引导后，将在每个区域中为承担 root 角色在步骤 1 中运行 "Labeled Zone Manager"（有标签区域管理器）的用户配置帐户。其他特定于有标签区域的帐户必须手动添加到区域中。

   注 – 仍从全局区域管理 LDAP 系统信息库中存储的帐户。

4. **对于每个区域，检验路由和名称服务守护进程。**

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

   ```
   zone-name # svcs -x name-service/cache
   svc:/system/name-service/cache:default (name service cache)
    State: online since September 10, 2012  10:10:12 AM PDT
      See: nscd(1M)
      See: /var/svc/log/system-name-service-cache:default.log
   Impact: None.
   ```

   b. **检验通往子网的路由。**

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

示例 4–3 从每个有标签区域中删除名称服务高速缓存

针对每个区域测试一个名称服务守护进程之后，系统管理员决定从有标签区域中删除名称服务守护进程，仅在全局区域中运行守护进程。要将系统恢复为缺省名称服务配置，管理员将打开 `txzonemgr` GUI，选择全局区域，再选择 `Unconfigure per-zone name service`（取消配置每区域名称服务），然后选择 `OK`（确定）。此选择将删除每个有标签区域中的 `nscd` 守护进程。之后，管理员重新引导系统。

接下来的步骤 为每个区域配置用户和角色帐户时，您有三个选项。

- 可以在多级别 LDAP 目录服务器中创建 LDAP 帐户。
- 可以在单独的 LDAP 目录服务器（每个标签一个服务器）中创建 LDAP 帐户。
- 可以创建本地帐户。

在每个有标签区域中单独配置名称服务守护进程意味着所有用户都需要输入口令。用户必须对自身进行验证以获取对其任一有标签区域（包括与其缺省标签对应的区域）的访问权限。此外，管理员必须在每个区域中本地创建帐户，或者帐户必须存在于区域为 LDAP 客户机的 LDAP 目录中。

在全局区域中的帐户运行 "Labeled Zone Manager"（有标签区域管理器）`txzonemgr` 的特殊情况下，帐户的信息将复制到有标签区域，以便至少此帐户能够登录到每个区域。缺省情况下，此帐户为初始用户帐户。

在 Trusted Extensions 中创建角色和用户

在 Trusted Extensions 中创建角色的过程与在 Oracle Solaris中创建角色的过程相同。但对于评估配置，需要 "Security Administrator"（安全管理员）角色。

任务	说明	参考
创建安全管理员角色。	创建一个要处理与安全相关的任务的角色。	第 62 页中的 “如何在 Trusted Extensions 中创建 "Security Administrator"（安全管理员）角色”
创建系统管理员角色。	创建一个要处理与安全无关的系统管理任务的角色。	第 63 页中的 “如何创建 "System Administrator"（系统管理员）角色”
创建承担管理角色的用户。	创建可以承担角色的一个或多个用户。	第 63 页中的 “如何在 Trusted Extensions 中创建可以承担角色的用户”
检验角色是否可以执行其任务。	测试角色。	第 66 页中的 “如何检验 Trusted Extensions 角色是否有效”
使用户能够登录到有标签区域。	启动 `zones`（区域）服务，使一般用户能够登录。	第 66 页中的 “如何使用户能够登录到有标签区域”

▼ 如何在 Trusted Extensions 中创建 "Security Administrator"（安全管理员）角色

开始之前 您是全局区域中的 root 角色。

1. **要创建角色，请使用 roleadd 命令。**

   有关该命令的信息，请参见 roleadd(1M) 手册页。

   可以使用下列信息作为参考：

   - Role name（角色名称）－secadmin
   - -c Local Security Officer

     请勿提供专有信息。
   - -m *home-directory*
   - -u *role-UID*
   - -S *repository*
   - -K *key=value*

     指定 "Information Security"（信息安全）和 "User Security"（用户安全）权限配置文件。

   注 – 对于所有管理角色，请使用管理标签作为标签范围、审计 pfexec 命令的使用、设置 lock_after_retries=no，且不设置口令失效日期。

   ```
   # roleadd -c "Local Security Officer" -m \
   -u 110 -K profiles="Information Security,User Security" -S files \
   -K lock_after_retries=no \
   -K min_label=ADMIN_LOW -K clearance=ADMIN_HIGH secadmin
   ```

2. **提供角色的初始口令。**

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

   指定至少包含六个字母数字字符的口令。安全管理员角色的口令以及所有口令都必须难以猜出，从而减少通过试猜口令而让有敌意的人获取未经授权访问的机会。

3. **创建其他角色时，使用 "Security Administrator"（安全管理员）角色作为参考。**

   可能的角色包括：

   - admin 角色－System Administrator（系统管理员）权限配置文件
   - oper 角色－Operator（操作员）权限配置文件

示例 4–4 在 LDAP 中创建 "Security Administrator"（安全管理员）角色

对第一个系统配置 "local Security Administrator"（本地安全管理员）角色后，管理员会在 LDAP 系统信息库中创建 "Security Administrator"（安全管理员）角色。在该方案中，LDAP 客户机可由在 LDAP 中定义的 "Security Administrator"（安全管理员）角色进行管理。

```
# roleadd -c "Site Security Officer" -d server1:/rpool/pool1/BayArea/secadmin
-u 111 -K profiles="Information Security,User Security" -S ldap \
-K lock_after_retries=no -K audit_flags=lo,ex:no \
-K min_label=ADMIN_LOW -K clearance=ADMIN_HIGH secadmin
```

管理员提供角色的初始口令。

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

接下来的步骤 要将本地角色分配给本地用户，请参见第 63 页中的 “如何在 Trusted Extensions 中创建可以承担角色的用户”。

▼ 如何创建 "System Administrator"（系统管理员）角色

开始之前 您是全局区域中的 root 角色。

1. **将 "System Administrator（系统管理员）"权限配置文件指定给角色。**

```
# roleadd -c "Local System Administrator" -m -u 111  -K audit_flags=lo,ex:no\
-K profiles="System Administrator" -K lock_after_retries=no \
-K min_label=ADMIN_LOW -K clearance=ADMIN_HIGH sysadmin
```

2. **提供角色的初始口令。**

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

▼ 如何在 Trusted Extensions 中创建可以承担角色的用户

在站点安全策略允许的情况下，可以选择创建能承担多个管理角色的用户。

为保证可以创建用户，"System Administrator"（系统管理员）角色负责创建用户和指定初始口令，而 "Security Administrator"（安全管理员）角色则负责指定与安全相关的属性（如角色）。

开始之前 您必须在全局区域中承担 root 角色。或者，如果强制执行职责分离，必须存在可承担 "Security Administrator"（安全管理员）和 "System Administrator"（系统管理员）不同角色的用户以承担其角色，并执行此过程中的相应步骤。

1. **创建用户。**

   root 角色或 "System Administrator"（系统管理员）角色执行此步骤。

   请勿在注释中放置专有信息。

   ```
   # useradd -c "Second User" -u 1201 -d /home/jdoe jdoe
   ```

2. **创建用户后，修改用户的安全属性。**

   root 角色或 "Security Administrator"（安全管理员）角色执行此步骤。

   注 – 对于可承担角色的用户，请关闭帐户锁定，且不设置口令失效日期。同时，审计 pfexec 命令的使用。

   ```
   # usermod -K lock_after_retries=no -K idletime=5 -K idlecmd=lock \
   -K audit_flags=lo,ex:no jdoe
   ```

   注 – 用户承担角色后，idletime 和 idlecmd 的值继续有效。有关更多信息，请参见第 124 页中的 “Trusted Extensions 中的 policy.conf 文件缺省值”。

3. **指定至少包含六个字母数字字符的口令。**

   ```
   # passwd jdoe
   New Password:       Type password
   Re-enter new Password:      Retype password
   ```

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

4. **将角色分配给用户。**

   root 角色或 "Security Administrator"（安全管理员）角色执行此步骤。

   ```
   # usermod -R oper jdoe
   ```

5 **定制用户的环境。**

a. **指定方便授权。**

在检查了站点安全策略以后，可能需要向您的首批用户授予 "Convenient Authorizations"（方便授权）权限配置文件。使用此配置文件，用户可以分配设备、进行无标签打印、远程登录以及关闭系统。要创建配置文件，请参见第 135 页中的 “如何创建权限配置文件以实现方便的授权”。

b. **定制用户初始化文件。**

请参见第 129 页中的 “针对安全性定制用户环境（任务列表）”。

c. **创建多级别副本和链接文件。**

在多级别系统上，可以为用户和角色设置一些文件，这些文件列出要复制或链接到其他标签的用户初始化文件。有关更多信息，请参见第 126 页中的 “.copy_files 和 .link_files 文件”。

示例 4–5 使用 useradd 命令创建本地用户

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

该用户将具有比缺省标签范围更广的标签范围。因此，root 角色确定用户的最小标签和安全许可标签的十六进制格式。

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

其次，root 角色参考表 1–2，然后创建用户。管理员将用户的起始目录放置到 /export/home1，而不是缺省的 /export/home 中。

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

接着，root 角色指定初始口令。

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

最后，root 角色将 "Security Administrator"（安全管理员）角色添加到用户的定义中。该角色是在第 62 页中的 “如何在 Trusted Extensions 中创建 "Security Administrator"（安全管理员）角色”中创建的。

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

▼ 如何检验 Trusted Extensions 角色是否有效

要检验每个角色，请承担相应的角色。然后，执行只有该角色可以执行的任务，并尝试不允许该角色执行的任务。

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

1. **对于每个角色，以可以承担相应角色的用户身份登录。**
2. **承担角色。**

   在以下可信窗口条中，用户名为 `tester`。

   a. **在可信窗口条中，单击您的用户名。**

   b. **从分配给您的角色列表中，选择一个角色。**
3. **测试该角色。**

   有关更改用户属性所需的授权，请参见 `passwd(1)` 手册页。

   - "System Administrator"（系统管理员）角色应该能够创建用户和修改需要 `solaris.user.manage` 授权的用户属性，如用户的登录 shell。"System Administrator"（系统管理员）角色应该不能更改需要 `solaris.account.setpolicy` 授权的用户属性。
   - "Security Administrator"（安全管理员）角色应该能够更改需要 `solaris.account.setpolicy` 授权的用户属性。"Security Administrator"（安全管理员）应该不能创建用户或更改用户的登录 shell。

▼ 如何使用户能够登录到有标签区域

重新引导系统时，必须重新建立设备与底层存储之间的关联。

开始之前 您已经创建了至少一个有标签的区域。配置系统后，您已重新引导。您可承担 `root` 角色。

1. **登录并承担 `root` 角色。**

2 检查区域服务的状态。

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

3 重新启动服务。

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

4 注销。

一般用户现在可以登录了。他们的会话位于有标签区域中。

在 Trusted Extensions 中创建集中起始目录

在 Trusted Extensions 中，用户需要访问其从中工作的每个标签的起始目录。缺省情况下，在每个区域运行的自动挂载程序会自动创建起始目录。然而，如果您使用 NFS 服务器集中起始目录，必须在每个标签下为您的用户启用起始目录访问权限。

▼ 如何在 Trusted Extensions 中创建起始目录服务器

开始之前 您是全局区域中的 root 角色。

1 **将 Trusted Extensions 软件添加到起始目录服务器，并配置其有标签区域。**

因为用户的每个标签都需要一个可登录的起始目录，因此请在每个用户标签下创建一个起始目录服务器。例如，如果您创建缺省配置，则为 PUBLIC 标签创建一个起始目录服务器，为 INTERNAL 标签创建一个服务器。

2 **对于每个有标签区域，请遵循第 173 页中的“如何在有标签区域中对文件进行 NFS 挂载”中介绍的自动挂载过程。然后，返回到此过程。**

3 **检验是否已创建起始目录。**

a. **从起始目录服务器注销。**

b. **以一般用户身份登录到起始目录服务器。**

c. **在登录区域中，打开一个终端。**

d. **在终端窗口中，检验用户的起始目录是否存在。**

e. **为用户可在其中工作的每个区域创建工作区。**

f. **在每个区域中，打开一个终端窗口来检验用户的起始目录是否存在。**

4. **从起始目录服务器注销。**

▼ 如何让用户登录每个 NFS 服务器来访问每个标签下的远程起始目录

在此过程中，通过让用户直接登录到每个起始目录服务器来允许用户在每个标签下创建一个起始目录。在中央服务器中创建每个起始目录后，用户可从任何系统访问其起始目录。

或者，作为管理员，您可以通过运行脚本并修改自动挂载程序来在每个起始目录服务器中创建挂载点。有关此方法，请参见第 68 页中的 “如何通过在每个服务器上配置自动挂载程序来使用户能够访问其远程起始目录”。

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

- **使用户能够直接登录到每个起始目录服务器。**
  通常，已针对每个标签创建一个 NFS 服务器。

  a. **指示每个用户以服务器的标签登录到每个 NFS 服务器。**

  b. **登录成功后，指示用户从服务器注销。**
     登录成功后，用户的起始目录将显示在服务器的标签下。

  c. **指示用户从其常规工作站登录。**
     可从起始目录服务器获得其缺省标签对应的起始目录。当用户更改了某个会话的标签，或者从不同的标签添加了工作区时，将挂载该标签的用户起始目录。

接下来的步骤 用户可在登录期间从标签生成器选择不同的标签，从不同于缺省标签的其他标签登录。

▼ 如何通过在每个服务器上配置自动挂载程序来使用户能够访问其远程起始目录

在此过程中，将运行用于在每个 NFS 服务器上为起始目录创建挂载点的脚本。然后，在服务器的标签下修改 `auto_home` 项，以添加挂载点。然后，用户即可登录。

开始之前 已经将 Trusted Extensions 域的起始目录服务器配置为 LDAP 客户机。已使用带有 `-S ldap` 选项的 `useradd` 命令在 LDAP 服务器上创建用户帐户。您必须是 `root` 角色。

1. **编写一个脚本，以便为每个用户创建起始目录挂载点。**

样例脚本进行了以下假设：

- LDAP 服务器是不同于 NFS 起始目录服务器的服务器。
- 客户机系统也是不同的系统。
- hostname 项指定区域的外部 IP 地址，即其标签对应的 NFS 起始目录服务器。
- 该脚本将在为该标签下的客户机提供服务的区域中的 NFS 服务器上运行。

```
#!/bin/sh
hostname=$(hostname)
scope=ldap

for j in $(getent passwd|tr ' ' _); do
    uid=$(echo $j|cut -d: -f3)
    if [ $uid -ge 100 ]; then
        home=$(echo $j|cut -d: -f6)
        if [[ $home == /home/* ]]; then
            user=$(echo $j|cut -d: -f1)
            echo Updating home directory for $user
            homedir=/export/home/$user
            usermod -md ${hostname}:$homedir -S $scope $user
            mp=$(mount -p|grep  " $homedir zfs" )
            dataset=$(echo $mp|cut -d" " -f1)
            if [[ -n $dataset ]]; then
                zfs set sharenfs=on $dataset
            fi
        fi
    fi
done
```

2 **在每个 NFS 服务器上，在为该标签下的客户机提供服务的有标签区域中运行前面的脚本。**

Trusted Extensions 配置故障排除

错误配置的桌面会阻止使用系统。

▼ 如何将桌面面板移到屏幕底部

注 – 桌面面板的缺省位置位于屏幕顶部。但在 Trusted Extensions 中，可信窗口条会覆盖屏幕顶部。因此，面板必须位于工作区的一侧或底部。缺省工作区具有两个桌面面板。

开始之前 您必须承担 root 角色，才能更改系统的桌面面板位置。

1 **如果屏幕底部有一个可见桌面面板，请执行以下操作之一：**

- **使用鼠标右键将 applet 添加到可见面板。**

- **执行以下步骤，将第二个隐藏的桌面面板移到屏幕底部。**

2 **否则，创建底部桌面面板，以仅用于您的登录，或用于系统的所有用户。**

- **要仅针对您的登录移动面板，请编辑起始目录中的 `top_panel_screen` *n* 文件。**

  a. **转到定义面板位置的文件所在的目录。**

  ```
  % cd $HOME/.gconf/apps/panel/toplevels
  % ls
  %gconf.xml    bottom_panel_screen0/   top_panel_screen0/
  % cd top_panel_screen0
  % ls
  %gconf.xml             top_panel_screen0/
  ```

  b. **编辑 `%gconf.xml` 文件，该文件定义了顶部面板的位置。**

  ```
  % vi %gconf.xml
  ```

  c. **找到所有的定位行，并将字符串 `top` 替换为 `bottom`。**

  例如，使定位行显示为类似于下面的内容：

  ```
  /toplevels/orientation" type="string">
                  <stringvalue>bottom</stringvalue>
  ```

- **要针对系统的所有用户移动面板，请修改桌面配置。**

  在终端窗口中，以 `root` 角色执行以下命令：

  ```
  # export SETUPPANEL="/etc/gconf/schemas/panel-default-setup.entries"
  # export TMPPANEL="/tmp/panel-default-setup.entries"
  # sed 's/<string>top<\/string>/<string>bottom<\/string>/' $SETUPPANEL > $TMPPANEL
  # cp $TMPPANEL $SETUPPANEL
  # svcadm restart gconf-cache
  ```

3 **从系统注销，然后再次登录。**

如果您有多个桌面面板，面板会在屏幕底部堆叠。

其他 Trusted Extensions 配置任务

对于配置 Trusted Extensions 系统以满足要求，以下任务很有用。通过最后一项任务，可以将 Trusted Extensions 功能从 Oracle Solaris 系统中删除。

任务	说明	参考
通知用户站点是否安全。	在登录时显示一条安全消息。	《Oracle Solaris 11 安全准则》中的“如何在标题文件中放置安全消息” 《Oracle Solaris 11 安全准则》中的“如何在桌面登录屏幕中放置安全消息”

任务	说明	参考
创建一个有标签区域，以包含使用与现有区域标签相同的标签运行的服务。	使用与主区域标签相同的标签创建辅助区域。	第 71 页中的 “如何创建有标签辅助区域”
创建数据集以保存所有标签下的目录和文件。	创建并挂载一个重新设置文件标签开销最低的数据集。	第 72 页中的 “如何创建和共享多级别数据集”
在每个标签下创建一个起始目录服务器。	创建多个起始目录服务器，每个标签对应一个起始目录服务器。或者，创建多级别起始目录服务器。	第 67 页中的 “如何在 Trusted Extensions 中创建起始目录服务器”
创建可以承担角色的初始用户。	创建在承担角色时可以担负系统管理职责的可信用户。	第 63 页中的 “如何在 Trusted Extensions 中创建可以承担角色的用户”
删除 Trusted Extensions。	从系统中删除 Trusted Extensions 和所有可信数据。此外，使系统做好在没有 Trusted Extensions 的情况下运行 Oracle Solaris 的准备。	第 76 页中的 “如何从系统中删除 Trusted Extensions”

▼ 如何创建有标签辅助区域

有标签辅助区域可用于将服务隔离在不同区域中，但仍允许服务使用同一标签运行。有关更多信息，请参见第 152 页中的 “有标签主区域和有标签辅助区域”。

开始之前 主区域必须存在。辅助区域必须具有专用 IP 地址，并且不能要求使用桌面。

您必须在全局区域中承担 `root` 角色。

1. **创建辅助区域。**

   您可以使用命令行或 `txzonemgr` 有标签区域 GUI。

   - **使用命令行。**

     ```
     # tncfg -z secondary-label-service primary=no
     # tncfg -z secondary-label-service label=public
     ```

   - **使用 `txzonemgr`。**

     ```
     # txzonemgr &
     ```

     导航至创建新区域的菜单（或选项），然后按照提示执行操作。

     注 – 必须以前缀形式输入网络掩码。例如，`255.255.254.0` 网络掩码要求使用 23 前缀。

2. **验证区域是否是辅助区域。**

   ```
   # tncfg -z zone info primary
       primary=no
   ```

示例 4–6 为公共脚本创建区域

在以下示例中，管理员隔离出一个用于运行脚本和批处理作业的公共区域。

```
# tncfg -z public-scripts primary=no
# tncfg -z public-scripts label=public
```

▼ 如何创建和共享多级别数据集

当降级或升级信息时，多级别数据集是很有用的容器。有关更多信息，请参见第 166 页中的 “需要为文件重新设置标签的多级别数据集”。对于多级别 NFS 文件服务器为大量 NFS 客户机提供使用许多标签的文件，多级别数据集也很有用。

开始之前 要创建多级别数据集，您必须在全局区域中承担 `root` 角色。

1 创建多级别数据集。

```
# zfs create -o mountpoint=/multi -o multilevel=on rpool/multi
```

`rpool/multi` 是在全局区域的 `/multi` 上挂载的多级别数据集。

要限制数据集的上限标签范围，请参见示例 4–7。

2 验证是否已挂载多级别数据集以及挂载点是否具有 `ADMIN_LOW` 标签。

```
# getlabel /multi
/multi: ADMIN_LOW
```

3 保护父文件系统。

为池中的所有文件系统将以下 ZFS 属性设置为 `off`：

```
# zfs set devices=off rpool/multi
# zfs set exec=off rpool/multi
# zfs set setuid=off rpool/multi
```

4 可选设置池的压缩属性。

通常，压缩是在 ZFS 中的文件系统级别设置的。但是，由于此池中的所有文件系统都是数据文件，因此会在顶级数据集为池设置压缩。

```
# zfs set compression=on rpool/multi
```

另请参见《Oracle Solaris 11.1 管理：ZFS 文件系统》中的“ZFS 压缩、重复数据删除和加密属性之间的交互”。

5 为要包含在多级别数据集中的每个标签创建顶层目录。

```
# cd /multi
# mkdir public internal
# chmod 777 public internal
# setlabel PUBLIC public
# setlabel "CNF : INTERNAL" internal
```

6 **使用 LOFS 在已批准具有访问权限的每个有标签区域中挂载多级别数据集。**

例如，以下 zonecfg 命令系列可在 public 区域中挂载数据集。

```
# zonecfg -z public
zonecfg:public> add fs
zonecfg:public:fs> set dir=/multi
zonecfg:public:fs> set special=/multi
zonecfg:public:fs> set type=lofs
zonecfg:public:fs> end
zonecfg:public> exit
```

多级别数据集允许在与挂载区域标签相同的标签处写入文件以及读取较低级别的文件。可以查看和设置挂载文件的标签。

7 **要使用 NFS 与其他系统共享多级别数据集，请执行以下操作：**

a. **将全局区域中的 NFS 服务设置成多级别服务。**

```
# tncfg -z global add mlp_private=2049/tcp
# tncfg -z global add mlp_private=111/udp
# tncfg -z global add mlp_private=111/tcp
```

b. **重新启动 NFS 服务。**

```
# svcadm restart nfs/server
```

c. **共享多级别数据集。**

```
# share /multi
```

已挂载 NFS 的多级别数据集允许在与挂载区域标签相同的标签处写入文件以及读取较低级别的文件。无法可靠地查看或设置已挂载文件的标签。有关更多信息，请参见第 167 页中的 “挂载来自其他系统的多级别数据集”。

示例 4–7 使用低于 ADMIN_HIGH 的最高级别标签创建多级别数据集

在以下示例中，管理员将使用低于缺省值 ADMIN_HIGH 的上界标签或最高级别标签创建多级别数据集。创建数据集时，管理员在 mslabel 属性中指定标签上界。此上界可阻止全局区域进程在多级别数据集中创建任何文件或目录。只有有标签区域才能在数据集中创建目录和文件。由于 multilevel 属性为 on，因此 mlslabel 属性会为单标签数据集设置上界而非标签。

```
# zfs create -o mountpoint=/multiIUO -o multilevel=on \
-o mlslabel="CNF : INTERNAL" rpool/multiIUO
```

然后，管理员登录到每个有标签区域，在已挂载数据集中以该标签创建目录。

```
# zlogin public
# mkdir /multiIUO
# chmod 777 /multiIUO
# zlogin internal
# mkdir /multiIUO
# chmod 777 /multiIUO
```

重新引导区域后，多级别数据集以挂载区域的标签对已授权用户可见。

接下来的步骤 要使用户能够对文件重新设置标签，请参见第 160 页中的 “如何在有标签区域中允许重新为文件设置标签”。

有关重新设置文件标签的说明，请参见《Trusted Extensions 用户指南》中的“如何升级多级别数据集中的数据”和《Trusted Extensions 用户指南》中的“如何降级多级别数据集中的数据”。

▼ 如何在 Trusted Extensions 中将文件复制到便携介质

复制到便携介质时，使用信息的敏感标签来标记介质。

注 – 在 Trusted Extensions 配置期间，`root` 角色可能会使用便携介质将 `label_encodings` 文件传输到所有系统。使用 `Trusted Path`（可信路径）标记介质。

开始之前 要复制管理文件，您必须在全局区域中承担 `root` 角色。

1. **分配相应的设备。**

   使用 Device Manager（设备管理器），然后插入一个干净的介质。有关详细信息，请参见《Trusted Extensions 用户指南》中的“如何在 Trusted Extensions 中分配设备”。

   文件浏览器将显示干净介质的内容。

2. **打开另外一个文件浏览器。**

3. **导航到要复制的文件所在的文件夹。**

4. **对于每个文件，执行以下操作：**

   a. **突出显示文件的图标。**

   b. **将文件拖到便携介质的文件浏览器中。**

5. **对设备取消分配。**

   有关详细信息，请参见《Trusted Extensions 用户指南》中的“如何在 Trusted Extensions 中对设备取消分配”。

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

注 – 请记住在包含所复制文件敏感标签的介质上粘上一个实体标签。

示例 4–8 **使所有系统上的配置文件保持相同**

系统管理员需要确保每个系统都配置了相同的设置。因此，在配置的第一个系统中，管理员将创建一个在重新引导后不能被删除的目录。在该目录中，管理员将放入必须在所有系统上相同或非常相似的文件。

例如，管理员将针对该站点修改 `policy.conf` 文件、缺省 `login` 和 `passwd` 文件。因此，管理员将以下文件复制到永久性目录。

```
# mkdir /export/commonfiles
# cp  /etc/security/policy.conf \
# cp  /etc/default/login \
# cp  /etc/default/passwd \
# cp  /etc/security/tsol/label_encodings \
/export/commonfiles
```

管理员使用 Device Manager（设备管理器）在全局区域中分配 CD-ROM，将文件传输到 CD，并粘贴 `Trusted Path`（可信路径）标签。

▼ 如何在 Trusted Extensions 中从便携介质复制文件

安全的做法是替换文件之前，先重命名原始 Trusted Extensions 文件。在配置系统时，`root` 角色会重命名和复制管理文件。

开始之前 要复制管理文件，您必须在全局区域中承担 `root` 角色。

1. **分配相应的设备。**

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

   文件浏览器将显示内容。

2. **插入包含管理文件的介质。**

3. **如果系统有同名文件，请在原始文件名的基础上组成新名称。**

   例如，在原始文件末尾加上 `.orig`：

   ```
   # cp /etc/security/tsol/label_encodings /etc/security/tsol/label_encodings.orig
   ```

4. **打开一个文件浏览器。**

5. **导航到所需的目标目录，如 `/etc/security/tsol`。**

6 **对于要复制的每个文件，执行以下操作：**

   a. **在挂载介质的文件浏览器中，突出显示文件的图标。**

   b. **然后，将文件拖至第二个文件浏览器的目标目录中。**

7 **对设备取消分配。**

   有关详细信息，请参见《Trusted Extensions 用户指南》中的“如何在 Trusted Extensions 中对设备取消分配”。

8 **系统提示时，弹出并移除介质。**

▼ 如何从系统中删除 Trusted Extensions

您必须执行特定步骤，才能从 Oracle Solaris 系统中删除 Trusted Extensions 功能。

开始之前 您是全局区域中的 `root` 角色。

1 **在要保留的有标签区域中对任何数据进行归档。**

   对于便携介质，将带有区域敏感标签的物理贴纸贴粘到每个归档区域。

2 **从系统中删除有标签区域。**

   有关详细信息，请参见《Oracle Solaris 11.1 管理：Oracle Solaris Zones、Oracle Solaris 10 Zones 和资源管理》中的“如何删除非全局区域”。

3 **禁用 Trusted Extensions 服务。**

```
# svcadm disable labeld
```

4 **可选重新引导系统。**

5 **配置系统。**

   可能需要为您的 Oracle Solaris 系统配置各种服务。可能项包括基本网络、命名服务和文件系统挂载。

◆ ◆ ◆ 第 5 章

为 Trusted Extensions 配置 LDAP（任务）

本章介绍了如何配置 Oracle Directory Server Enterprise Edition (Directory Server) 以便与 Trusted Extensions 结合使用。Directory Server 提供 LDAP 服务。LDAP 是适用于 Trusted Extensions 的受支持的命名服务。最后一节第 87 页中的 “创建 Trusted Extensions LDAP 客户机”介绍了如何配置 LDAP 客户机。

配置 Directory Server 时，您有两种选择。可以在 Trusted Extensions 系统上配置一个 LDAP 服务器，也可以使用现有的某个服务器并通过使用 Trusted Extensions 代理服务器来与其连接。

要配置 LDAP 服务器，请遵循以下任务列表之一中的说明：

- 第 77 页中的 “在 Trusted Extensions 网络上配置 LDAP（任务列表）”
- 第 78 页中的 “在 Trusted Extensions 系统上配置 LDAP 代理服务器（任务列表）”

在 Trusted Extensions 网络上配置 LDAP（任务列表）

任务	说明	参考
设置 Trusted Extensions LDAP 服务器。	如果您没有现有的 Oracle Directory Server Enterprise Edition，请将第一个 Trusted Extensions 系统用作 Directory Server。此系统上没有有标签区域。 其他 Trusted Extensions 系统是此服务器的客户机。	第 78 页中的 “收集用于 LDAP 的 Directory Server 的信息” 第 79 页中的 “安装 Oracle Directory Server Enterprise Edition” 第 82 页中的 “配置 Oracle Directory Server Enterprise Edition的日志”
向服务器添加 Trusted Extensions 数据库。	使用 Trusted Extensions 系统文件中的数据置备 LDAP 服务器。	第 84 页中的 “置备 Oracle Directory Server Enterprise Edition”
将所有其他 Trusted Extensions 系统配置为此服务器的客户机。	配置具有 Trusted Extensions 的其他系统时，使该系统成为此 LDAP 服务器的客户机。	第 87 页中的 “使全局区域成为 Trusted Extensions 中的客户机”

在 Trusted Extensions 系统上配置 LDAP 代理服务器（任务列表）

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

任务	说明	参考
向服务器添加 Trusted Extensions 数据库。	Trusted Extensions 网络数据库 `tnrhdb` 和 `tnrhtp` 需要添加至 LDAP 服务器。	第 84 页中的 “置备 Oracle Directory Server Enterprise Edition”
设置 LDAP 代理服务器。	将一个 Trusted Extensions 系统用作其他 Trusted Extensions 系统的代理服务器。这些其他系统使用此代理服务器访问 LDAP 服务器。	第 86 页中的 “创建 LDAP 代理服务器”
将代理服务器配置为具有多级别 LDAP 端口。	使 Trusted Extensions 代理服务器从特定标签与 LDAP 服务器进行通信。	第 84 页中的 “为 Oracle Directory Server Enterprise Edition配置多级别端口”
将所有其他 Trusted Extensions 系统配置为 LDAP 代理服务器的客户机。	配置具有 Trusted Extensions 的其他系统时，使该系统成为 LDAP 代理服务器的客户机。	第 87 页中的 “使全局区域成为 Trusted Extensions 中的客户机”

在 Trusted Extensions 系统上配置 Oracle Directory Server Enterprise Edition

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

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

注 – 如果不将此 LDAP 服务器用作 NFS 服务器或 Sun Ray 客户机的服务器，那么您不需要在此服务器上安装任何有标签区域。

▼ 收集用于 LDAP 的 Directory Server 的信息

- **确定以下各项的值。**

  这些项按其在系统安装向导中的出现顺序列出。

安装向导提示	操作或信息
Oracle Directory Server Enterprise Edition *version*	
Administrator User ID（管理员用户 ID）	缺省值为 `admin`。
Administrator Password（管理员口令）	创建一个口令，如 `admin123`。
Directory Manager DN（目录管理员 DN）	缺省值为 `cn=Directory Manager`。
Directory Manager Password（目录管理员口令）	创建一个口令，如 `dirmgr89`。
Directory Server Root（Directory Server 根目录）	缺省值为 `/var/Sun/mps`。如果安装了代理软件，以后还会使用此路径。
Server Identifier（服务器标识符）	缺省值是本地系统。
Server Port（服务器端口）	如果计划使用 Directory Server 来为客户机系统提供标准 LDAP 命名服务，请使用缺省值 `389`。 如果计划使用 Directory Server 来支持代理服务器的后续安装，请输入一个非标准端口，如 `10389`。
Suffix（后缀）	包括您的域组件，如 `dc=example-domain,dc=com` 中所示。
Administration Domain（管理域）	为与后缀相对应而构造，如 `example-domain.com` 中所示。
System User（系统用户）	缺省值为 `root`。
System Group（系统组）	缺省值为 `root`。
Data Storage Location（数据存储位置）	缺省值为 `Store configuration data on this server`（**将配置数据存储在此服务器上**）。
Data Storage Location（数据存储位置）	缺省值为 `Store user data and group data on this server`（**将用户数据和组数据存储在此服务器上**）。
Administration Port（管理端口）	缺省值为服务器端口。更改缺省值的建议约定为 *software-version* 的 `1000` 倍。对于软件版本 `5.2`，此约定将得到端口 `5200`。

▼ 安装 Oracle Directory Server Enterprise Edition

可以从 Sun 软件产品的 Oracle Web 站点 (`http://www.oracle.com/us/sun/sun-products-map-075562.html`) 中获取 Directory Server 软件包。

开始之前 您的 Trusted Extensions 系统上安装了一个全局区域。系统上没有带标签的区域。您必须在全局区域中承担 root 角色。

Trusted Extensions LDAP 服务器是为使用 pam_unix 向 LDAP 系统信息库进行验证的客户机配置的。使用 pam_unix 时，口令操作由客户机确定，因此口令策略也由客户机确定。说得明确一点，也就是不使用由 LDAP 服务器设置的策略。有关可在客户机上设置的口令参数，请参见《Oracle Solaris 11.1 管理：安全服务》中的"管理口令信息"。有关 pam_unix 的信息，请参见 pam.conf(4) 手册页。

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

---

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

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

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

2. **从 Sun 软件产品的 Oracle Web 站点 (http://www.oracle.com/us/sun/sun-products-map-075562.html) 中下载 Oracle Directory Server Enterprise Edition 软件包。**

   选择适用于您平台的最新软件。

3. **安装 Directory Server 软件包。**

   使用第 78 页中的 "收集用于 LDAP 的 Directory Server 的信息"中的信息来回答问题。有关问题、缺省值以及建议答案的完整列表，请参见《Oracle Solaris Administration: Naming and Directory Services》中的第 11 章 "Setting Up Oracle Directory Server Enterprise Edition With LDAP Clients (Tasks)"和《Oracle Solaris Administration: Naming and Directory Services》中的第 12 章 "Setting Up LDAP Clients (Tasks)"。

4. **可选将 Directory Server 的环境变量添加到您的路径。**

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

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

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

6. **启用 cacaoadm 程序，并验证是否已启用此程序。**

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

7 **确保每次引导时 Directory Server 都会启动。**

Directory Server 的 SMF 服务的模板包含在 Oracle Directory Server Enterprise Edition软件包中。

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

```
# dsadm stop /export/home/ds/instances/your-instance
# dsadm enable-service -T SMF /export/home/ds/instances/your-instance
# dsadm start /export/home/ds/instances/your-instance
```

有关 `dsadm` 命令的信息，请参见 `dsadm`(1M) 手册页。

- **对于代理 Directory Server，请启用此服务。**

```
# dpadm stop /export/home/ds/instances/your-instance
# dpadm enable-service -T SMF /export/home/ds/instances/your-instance
# dpadm start /export/home/ds/instances/your-instance
```

有关 `dpadm` 命令的信息，请参见 `dpadm`(1M) 手册页。

8 **验证您的安装。**

```
# dsadm info /export/home/ds/instances/your-instance
Instance Path:          /export/home/ds/instances/your-instance
Owner:                  root(root)
Non-secure port:        389
Secure port:            636
Bit format:             32-bit
State:                  Running
Server PID:             298
DSCC url:               -
SMF application name:   ds--export-home-ds-instances-your-instance
Instance version:       D-A00
```

故障排除 有关解决 LDAP 配置问题的策略，请参见《在 Oracle Solaris 11.1 中使用命名和目录服务》中的第 13 章 “LDAP 故障排除（参考信息）”。

▼ 为 Directory Server 创建 LDAP 客户机

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

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

开始之前 您是全局区域中的 `root` 角色。

1 **将 Trusted Extensions 软件添加到系统中。**

可以使用 Trusted Extensions Directory Server，或者将 Trusted Extensions 添加到独立的系统中。

2 **在客户机上，在 `name-service/switch` 服务中配置 LDAP。**

a. **显示当前配置。**

```
# svccfg -s name-service/switch listprop config
config                      application
config/value_authorization  astring       solaris.smf.value.name-service.switch
config/default              astring       "files ldap"
config/host                 astring       "files dns"
config/netgroup             astring       ldap
config/printer              astring       "user files ldap"
```

b. **更改以下属性的缺省值：**

```
# svccfg -s name-service/switch setprop config/host = astring: "files ldap dns"
```

3 **在全局区域中，运行 `ldapclient init` 命令。**

在本例中，LDAP 客户机位于 `example-domain.com` 域中。服务器的 IP 地址为 `192.168.5.5`。

```
# ldapclient init -a domainName=example-domain.com -a profileName=default \
> -a proxyDN=cn=proxyagent,ou=profile,dc=example-domain,dc=com \
> -a proxyDN=cn=proxyPassword={NS1}ecc423aad0 192.168.5.5
System successfully configured
```

4 **将服务器的 `enableShadowUpdate` 参数设置为 `TRUE`。**

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

有关 `enableShadowUpdate` 参数的信息，请参见《Oracle Solaris Administration: Naming and Directory Services》中的“enableShadowUpdate Switch”和 `ldapclient`(1M) 手册页。

▼ 配置 Oracle Directory Server Enterprise Edition的日志

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

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

此过程中的设置满足以下要求：

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

开始之前 您必须在全局区域中承担 `root` 角色。

1 配置访问日志。

访问的 *LOG_TYPE* 为 `ACCESS`。用于配置日志的语法如下：

`dsconf set-log-prop` *LOG_TYPE property*:*value*

```
# dsconf set-log-prop ACCESS max-age:3M
# dsconf set-log-prop ACCESS max-disk-space-size:20000M
# dsconf set-log-prop ACCESS max-file-count:100
# dsconf set-log-prop ACCESS max-size:500M
# dsconf set-log-prop ACCESS min-free-disk-space:500M
```

2 配置审计日志。

```
# dsconf set-log-prop AUDIT max-age:3M
# dsconf set-log-prop AUDIT max-disk-space-size:20000M
# dsconf set-log-prop AUDIT max-file-count:100
# dsconf set-log-prop AUDIT max-size:500M
# dsconf set-log-prop AUDIT min-free-disk-space:500M
# dsconf set-log-prop AUDIT rotation-interval:1d
```

缺省情况下，审计日志的轮转时间间隔是一周。

3 配置错误日志。

在此配置中，您将指定要在错误日志中收集的其他数据。

```
# dsconf set-log-prop ERROR max-age:3M
# dsconf set-log-prop ERROR max-disk-space-size:20000M
# dsconf set-log-prop ERROR max-file-count:30
# dsconf set-log-prop ERROR max-size:500M
# dsconf set-log-prop ERROR min-free-disk-space:500M
# dsconf set-log-prop ERROR verbose-enabled:on
```

4 可选进一步配置日志。

您还可以为每个日志配置以下设置：

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

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

▼ 为 Oracle Directory Server Enterprise Edition配置多级别端口

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

开始之前 您必须在全局区域中承担 `root` 角色。

1. **启动 `txzonemgr`。**

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

2. **向全局区域添加一个用于 TCP 协议的多级别端口。**

   端口号为 389。

3. **向全局区域添加一个用于 UDP 协议的多级别端口。**

   端口号为 389。

▼ 置备 Oracle Directory Server Enterprise Edition

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

开始之前 您必须在全局区域中承担 `root` 角色。您的 LDAP 客户机上启用了投影更新。有关先决条件，请参见第 81 页中的 “为 Directory Server 创建 LDAP 客户机”。

1. **为您计划用来置备命名服务数据库的文件创建一个暂存区域。**

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

2. **将样例 `/etc` 文件复制到暂存区域中。**

   ```
   # cd /etc
   # cp aliases group networks netmasks protocols /setup/files
   # cp rpc services auto_master /setup/files

   # cd /etc/security/tsol
   # cp tnrhdb tnrhtp /setup/files
   ```

注意 – 请勿复制 *attr 文件。而是在向 LDAP 系统信息库添加用户、角色和权限配置文件的命令中使用 -S ldap 选项。这些命令可为 user_attr、auth_attr、exec_attr 和 prof_attr 数据库添加条目。有关更多信息，请参见 user_attr(4) 和 useradd(1M) 手册页。

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

4 **在暂存区域中创建区域自动映射。**

```
# cp /zone/public/root/etc/auto_home_public /setup/files
# cp /zone/internal/root/etc/auto_home_internal /setup/files
# cp /zone/needtoknow/root/etc/auto_home_needtoknow /setup/files
# cp /zone/restricted/root/etc/auto_home_restricted /setup/files
```

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

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

```
/setup/files/auto_home_public
 * myNFSserver_FQDN:/zone/public/root/export/home/&

/setup/files/auto_home_internal
 * myNFSserver_FQDN:/zone/internal/root/export/home/&

/setup/files/auto_home_needtoknow
 * myNFSserver_FQDN:/zone/needtoknow/root/export/home/&

/setup/files/auto_home_restricted
 * myNFSserver_FQDN:/zone/restricted/root/export/home/&
```

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

例如，以下命令基于暂存区域中的 hosts 文件置备服务器。

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

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

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

```
# ldapclient -v uninit
```

有关更多信息，请参见 ldapclient(1M) 手册页。

7 **要置备 LDAP 中的 Trusted Extensions 网络数据库，请使用带有 -S ldap 选项的 tncfg 命令。**

有关说明，请参见第 193 页中的 “为主机和网络设置标签（任务）”。

为现有 Oracle Directory Server Enterprise Edition创建 Trusted Extensions 代理

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

▼ 创建 LDAP 代理服务器

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

开始之前 您已经从进行了修改并将 `enableShadowUpdate` 参数设置为 `TRUE` 的一个客户机置备了 LDAP 服务器。有关要求，请参见第 81 页中的 “为 Directory Server 创建 LDAP 客户机”。

此外，您还从 `enableShadowUpdate` 参数设置为 `TRUE` 的一个客户机上将包含 Trusted Extensions 信息的数据库添加到了 LDAP 服务器。有关详细信息，请参见第 84 页中的 “置备 Oracle Directory Server Enterprise Edition”。

您必须在全局区域中承担 `root` 角色。

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

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

以下为样例命令。`ldapclient init` 命令定义代理值。

```
# ldapclient init \
-a proxyDN=cn=proxyagent,ou=profile,dc=west,dc=example,dc=com \
-a domainName=west.example.com \
-a profileName=pit1 \
-a proxyPassword=test1234 192.168.0.1
System successfully configured
```

`ldapclient mod` 命令启用投影更新。

```
# ldapclient mod -a enableShadowUpdate=TRUE \
-a adminDN=cn=admin,ou=profile,dc=west,dc=example,dc=com \
-a adminPassword=admin-password
System successfully configured
```

有关详细信息，请参见《Oracle Solaris Administration: Naming and Directory Services》中的第 12 章 “Setting Up LDAP Clients (Tasks)”。

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

```
# ldaplist -l database
```

故障排除 有关解决 LDAP 配置问题的策略，请参见《在 Oracle Solaris 11.1 中使用命名和目录服务》中的第 13 章 “LDAP 故障排除（参考信息）”。

创建 Trusted Extensions LDAP 客户机

以下过程为现有 Trusted Extensions Directory Server 创建 LDAP 客户机。

▼ 使全局区域成为 Trusted Extensions 中的客户机

此过程在 LDAP 客户机上为全局区域建立 LDAP 命名服务配置。

使用 `txzonemgr` 脚本。

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

开始之前 Oracle Directory Server Enterprise Edition（即 Directory Server）必须存在。该服务器必须置备有 Trusted Extensions 数据库，并且此客户机系统必须能够与该服务器联系。因此，Directory Server 必须已为此客户机指定安全模板。不需要特定的指定，通配符指定已足够。

您必须在全局区域中承担 `root` 角色。

1 **如果使用的是 DNS，请将 `dns` 添加到 `name-service/switch` 配置。**

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

a. 显示当前配置。

```
# svccfg -s name-service/switch listprop config
config                          application
config/value_authorization      astring       solaris.smf.value.name-service.switch
config/default                  astring       files ldap
config/netgroup                 astring       ldap
config/printer                  astring       "user files ldap"
```

b. 将 `dns` 添加到 `host` 属性并刷新该服务。

```
# svccfg -s name-service/switch setprop config/host = astring: "files dns ldap"
# svccfg -s name-service/switch:default refresh
```

c. 验证新配置。

```
# svccfg -s name-service/switch listprop config
config                      application
config/value_authorization  astring       solaris.smf.value.name-service.switch
config/default              astring       files ldap
config/host                 astring       files dns ldap
config/netgroup             astring       ldap
config/printer              astring       "user files ldap"
```

Trusted Extensions 数据库使用缺省配置 `files ldap`，因此未被列出。

2 要创建 LDAP 客户机，请运行不带任何选项的 `txzonemgr` 命令。

```
# txzonemgr &
```

a. 双击全局区域。

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

c. 应答以下提示，并在每次应答后单击 "OK"（确定）：

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

d. 确认或取消显示的值。

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

确认后，`txzonemgr` 脚本将运行 `ldapclient init` 命令。

3 通过启用投影更新来完成客户机配置。

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

4 检验服务器上的信息是否正确。

a. 打开终端窗口，查询 LDAP 服务器。

```
# ldapclient list
```

其输出与以下内容类似：

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

b. 更正所有错误。

如果出现错误，请重新执行步骤 2 至步骤 4。例如，以下错误可能表示系统没有 LDAP 服务器上的项。

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

要更正此错误，需要检查 LDAP 服务器。

第 2 部分

Trusted Extensions 的管理

本部分中各章节介绍如何管理 Trusted Extensions。

第 6 章，Trusted Extensions 管理概念，介绍 Trusted Extensions 功能。

第 7 章，Trusted Extensions 管理工具，介绍特定于 Trusted Extensions 的管理程序。

第 8 章，Trusted Extensions 系统上的安全要求（概述），介绍 Trusted Extensions 中的固定和可配置的安全要求。

第 9 章，执行 Trusted Extensions 中的常见任务，介绍 Trusted Extensions 管理。

第 10 章，Trusted Extensions 中的用户、权限和角色（概述），介绍 Trusted Extensions 中基于角色的访问控制 (role-based access control, RBAC)。

第 11 章，在 Trusted Extensions 中管理用户、权限和角色（任务），提供管理 Trusted Extensions 的一般用户的说明。

第 12 章，Trusted Extensions 中的远程管理（任务），提供远程管理 Trusted Extensions 的说明。

第 13 章，在 Trusted Extensions 中管理区域，提供管理有标签区域的说明。

第 14 章，在 Trusted Extensions 中管理和挂载文件，提供在 Trusted Extensions 中管理挂载、备份系统和其他与文件相关的任务的说明。

第 15 章，可信网络（概述），概述 Trusted Extensions 中的网络数据库和路由。

第 16 章，在 Trusted Extensions 中管理网络（任务），提供在 Trusted Extensions 中管理网络数据库和路由的说明。

第 18 章，Trusted Extensions 中的多级别邮件（概述），介绍 Trusted Extensions 中特定于邮件的问题。

第 19 章，管理有标签打印（任务），提供在 Trusted Extensions 中处理打印的说明。

第 20 章，Trusted Extensions 中的设备（概述），介绍 Trusted Extensions 为 Oracle Solaris 中的设备保护功能提供的扩展。

第 21 章，管理 Trusted Extensions 的设备（任务），提供通过使用设备管理器管理设备的说明。

第 22 章，Trusted Extensions 审计（概述），提供有关审计的特定于 Trusted Extensions 的信息。

第 23 章，Trusted Extensions 中的软件管理，介绍如何管理 Trusted Extensions 系统中的应用程序。

◆ ◆ ◆ 第 6 章

Trusted Extensions 管理概念

本章介绍了如何管理配置有 Trusted Extensions 功能的系统。

- 第 93 页中的 “Trusted Extensions 和 Oracle Solaris OS”
- 第 95 页中的 “Trusted Extensions 的基本概念”

Trusted Extensions 和 Oracle Solaris OS

Trusted Extensions 软件可向运行 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 的权限配置文件、角色、审计、特权以及其他安全功能。您可将安全 Shell、BART、加密框架、IPsec 和 IP 过滤器与 Trusted Extensions 配合使用。在 Trusted Extensions 中可以使用 ZFS 文件系统的所有功能，包括快照和加密。

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。另请参见附录 C，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 系统上处于启用状态。例如，许多配置 Trusted Extensions 的站点要求在创建用户并指定安全属性时进行 separation of duty（职责分离）。
- Trusted Extensions 可以更改 Oracle Solaris 的缺省行为。例如，在配置有 Trusted Extensions 的系统上，要求进行设备分配。
- Trusted Extensions 可缩小 Oracle Solaris 中可用选项的范围。例如，在 Trusted Extensions 中，所有区域都是有标签区域。与 Oracle Solaris 中不同，有标签区域必须使用相同的用户 ID 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 提供了 Oracle Solaris 桌面的多级别版本，即 Solaris Trusted Extensions (GNOME)。该名称可缩略为 Trusted GNOME。
- 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 提供设备管理器 GUI 来管理设备。此外，`updatehome` CLI 可用于将启动文件放在每个标签的用户起始目录中。
- 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，除 `zonecfg` 命令外，还可使用 "Labeled Zone Manager"（有标签区域管理器）管理有标签区域。
- 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。缺省情况下，一般用户无法关闭系统。

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。

但是，当多显示端系统的显示器上显示不同的工作区时，Trusted GNOME 会在每个显示器上显示一个可信窗口条。

Trusted Extensions 的基本概念

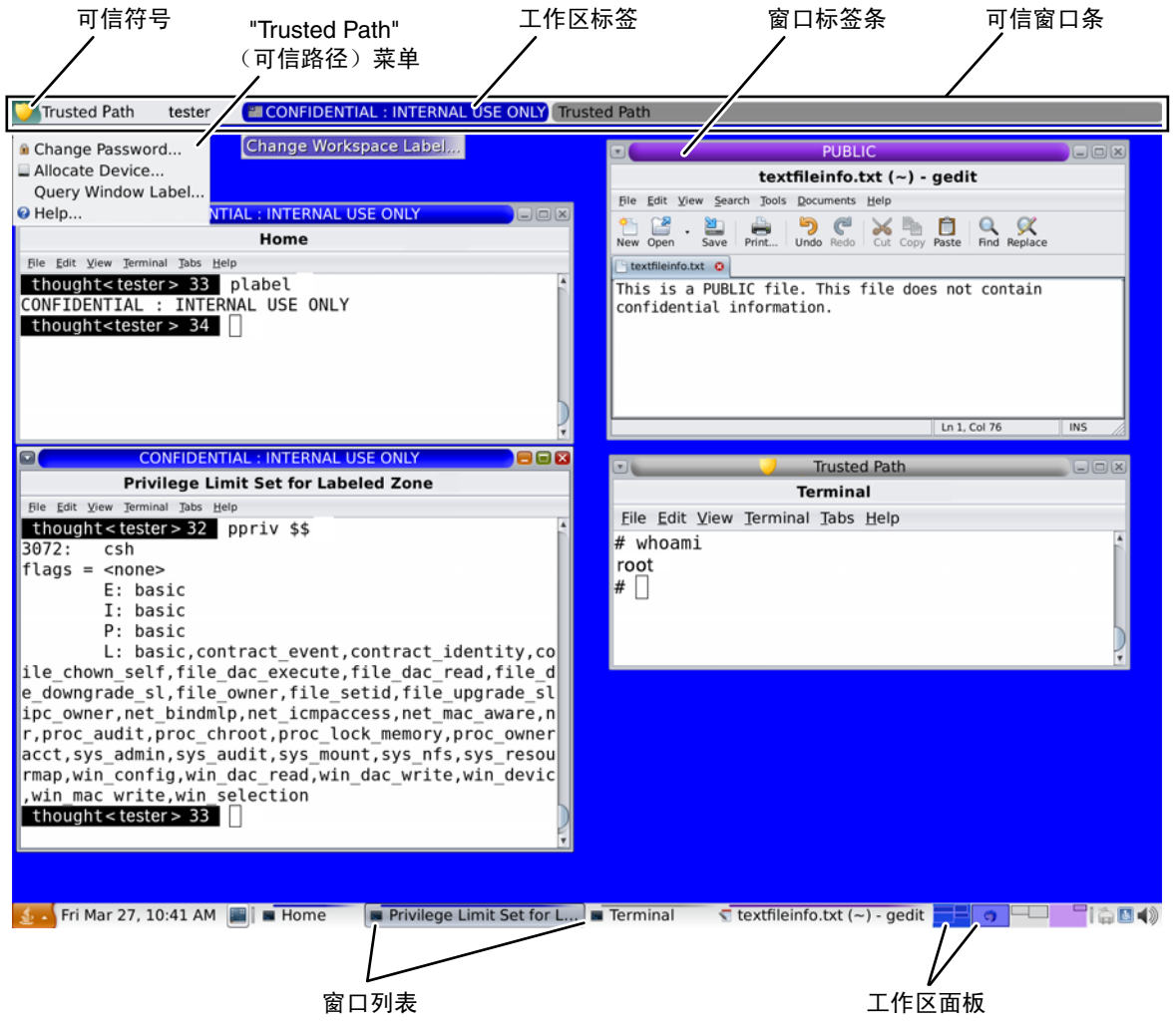
Trusted Extensions 软件会向 Oracle Solaris 系统添加标签。还会添加有标签工作区和可信应用程序，例如标签生成器和设备管理器。对于用户和管理员而言，本节中的概念都是了解 Trusted Extensions 所必需的。《Trusted Extensions 用户指南》中会为用户介绍这些概念。

Trusted Extensions 保护

Trusted Extensions 软件增强了对 Oracle Solaris OS 的保护。Trusted Extensions 可将用户和角色限制在批准的标签范围内。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 GNOME 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 6–1。

图 6–1 Trusted Extensions 多级别桌面



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。用户将受 TCB 软件的限制，例如在更改口令时。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**秘密**或**公共**。标签确定允许用户访问的信息。使用 Oracle Solaris 提供的特殊权限，可以覆盖 MAC 和 DAC。**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。

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`（绝密）到 `SECRET`（秘密），再到 `PUBLIC`（公共）。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、帧缓存器和其他系统。

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 6–1 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。还可以在《Trusted Extensions Label Administration》和《Compartmented Mode Workstation Labeling: Encodings Format》中了解详细信息。

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。
- **IPsec 和 IKE**－IPsec 安全关联和 IKE 规则具有标签。
- **网络接口**－将为 IP 地址（主机）指定描述其标签范围的安全模板。正在进行通信的 Trusted Extensions 系统也将为无标签主机指定缺省标签。
- **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 19 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。颜色将显示在工作区面板和上方的窗口标题栏上，如图 6–1 中所示。

  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。在该窗口中启动的进程会在原始标签下执行。
- **区域**－每个区域都有一个标签。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。

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 "Security Administrator"（安全管理员）角色和安全管理员角色管理。在某些情况下，会使用 `root` 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。

与在 Oracle Solaris 中一样，权限配置文件是角色功能的基础。有关权限配置文件和角色的信息，请参见《Oracle Solaris 11.1 管理：安全服务》中的第 8 章 “使用角色和特权（概述）”。

◆ ◆ ◆ 第 7 章

7 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。

- 第 101 页中的 “Trusted Extensions 的管理工具”
- 第 102 页中的 “txzonemgr 脚本”
- 第 102 页中的 “设备管理器”
- 第 103 页中的 “Trusted Extensions 中的选择管理器”
- 第 103 页中的 “Trusted Extensions 中的标签生成器”
- 第 104 页中的 “Trusted Extensions 中的命令行工具”
- 第 104 页中的 “Trusted Extensions 中的配置文件”

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。

在角色工作区中，可以访问可信的命令、应用程序和脚本。下表概述了这些管理工具。

表 7–1 Trusted Extensions 管理工具

工具	说明	更多信息
/usr/sbin/txzonemgr	创建有标签区域管理器 GUI，用于创建和配置有标签区域（包括网络）。	请参见第 51 页中的 “创建有标签区域”和 txzonemgr(1M) 手册页。
	使用命令行选项可自动创建用户命名的区域。	txzonemgr 是 zenity (1) 脚本。
设备管理器	用于管理设备的标签范围以及分配设备和取消分配设备。	请参见第 102 页中的 “设备管理器”和第 253 页中的 “在 Trusted Extensions 中操作设备（任务列表）”。

表 7–1 Trusted Extensions 管理工具 （续）

工具	说明	更多信息
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 135 页中的 “如何修改用户的标签范围”。
选择管理器	也是一个供有权更改数据安全级别的用户使用的工具。在程序要求您更改数据的安全级别时出现。	要授予用户权限，请参见第 137 页中的 “如何允许用户更改数据的安全级别”。有关图示，请参见《Trusted Extensions 用户指南》中的“如何在具有不同标签的窗口之间移动数据”。
Trusted Extensions 命令	用于执行管理任务	有关管理命令和配置文件的列表，请参见附录 D，Trusted Extensions 手册页列表。

txzonemgr 脚本

/usr/sbin/txzonemgr 命令是区域和网络配置工具，可提供两种模式。

- 作为 CLI，该命令基于现有文件创建有标签区域。当使用 -c 命令选项运行时，CLI 创建并引导两个有标签区域。-d 选项删除所有有标签区域。
- 作为 GUI，该脚本显示标题为 "Labeled Zone Manager"（有标签区域管理器）的对话框。此 GUI 指导您完成创建和引导有标签区域的过程。该脚本包括克隆一个区域以创建快照。此外，该 GUI 还提供网络、命名服务和 LDAP 配置菜单。此脚本处理 IPv4 和 IPv6 地址。

txzonemgr 命令运行 zenity(1) 脚本。"Labeled Zone Manager"（有标签区域管理器）对话框仅显示对有标签区域的当前配置状态有效的选项。例如，如果区域已有标签，则不显示 "Label"（标签）菜单项。

设备管理器

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 Manager"（设备管理器）分配设备。"Device Manager"（设备管理器）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 Manager"（设备管理器）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。

可以通过使用 "Device Manager"（设备管理器）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。

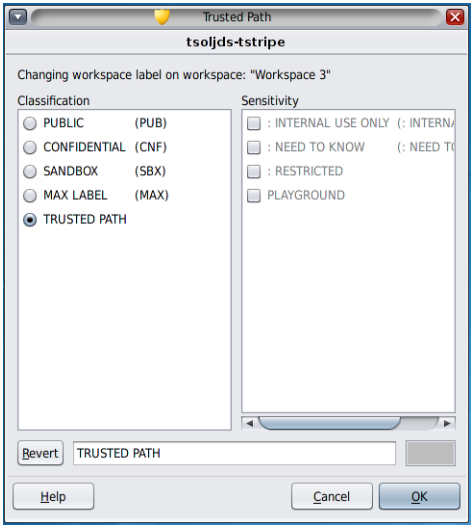
有关 Trusted Extensions 中的设备保护的更多信息，请参见第 21 章，管理 Trusted Extensions 的设备（任务）。

Trusted Extensions 中的选择管理器

当您尝试更改对象或选定项的标签时，将出现选择管理器 GUI。有关更多信息，请参见第 110 页中的 “更改数据的安全级别时的规则”。

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 可让您选择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 用户指南》中的第 2 章 “登录到 Trusted Extensions（任务）”）。更改工作区标签时，或者将标签指定给用户、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 `SENSITIVITY` 部分下的 `WORDS` 部分。

开发者可以通过使用 `tgnome-selectlabel` 命令为他们的应用程序构建标签生成器。键入 `tgnome-selectlabel -h` 可显示联机帮助。另请参见《Trusted Extensions Developer's Guide》中的第 6 章 “Label Builder GUI”。

Trusted Extensions 中的命令行工具

Trusted Extensions 特有的命令和 Trusted Extensions 修改的命令包含在《Oracle Solaris 参考手册》中。man 命令可找到所有命令。有关命令、指向 Trusted Extensions 文档集中示例的链接以及指向手册页的链接的说明，请参见附录 D，Trusted Extensions 手册页列表。

Trusted Extensions 中的配置文件

Trusted Extensions 扩展了 `/etc/inet/ike/config` 文件以包含标签信息。`ike.config(4)` 手册页介绍了 `label_aware` 全局参数和三个阶段 1 转换参数 `single_label`、`multi_label` 和 `wire_label`。

注 – IKE 配置文件包含关键字 `label`，用于使阶段 1 IKE 规则成为特有规则。IKE 关键字 `label` 不同于 Trusted Extensions 标签。

◆ ◆ ◆ 第 8 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。

- 第 105 页中的 “配置安全功能”
- 第 107 页中的 “安全要求实施”
- 第 110 页中的 “更改数据的安全级别时的规则”

配置安全功能

Trusted Extensions 使用的安全功能与 Oracle Solaris 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 的不同之处在于，通常通过承担受限制的角色来管理系统。与在 Oracle Solaris OS 中一样，由 `root` 角色修改配置文件。

Trusted Extensions 中的角色

在 Trusted Extensions 中，角色是用来管理系统的惯用方法。超级用户是 `root` 角色，是执行少数几个任务（例如设置审计标志、更改帐户口令和编辑系统文件）所必需的。创建角色的过程与在 Oracle Solaris 中进行创建的过程一样。

下面的角色是 Trusted Extensions 站点中的典型角色：

- `root` **角色**－在 Oracle Solaris 安装时创建
- **"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**—由初始设置团队在初始配置期间或之后创建

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。

在 Trusted Extensions 中创建角色的过程与 Oracle Solaris 过程相同。缺省情况下，为角色指定管理标签范围 ADMIN_HIGH 到 ADMIN_LOW。

- 有关角色创建的概述，请参见《Oracle Solaris 11.1 管理：安全服务》中的“使用 RBAC（任务）”。
- 要创建角色，请参见《Oracle Solaris 11.1 管理：安全服务》中的“如何创建角色”。

Trusted Extensions 中的角色承担

在可信桌面上，可以通过在用于选择角色的可信窗口条中单击您的用户名来承担指定的角色。确认角色口令后，当前工作区将更改为角色工作区。角色工作区处于全局区域中，并具有可信路径属性。角色工作区是管理工作区。

用于配置安全功能的 Trusted Extensions 接口

在 Trusted Extensions 中，您可以扩展现有安全功能。另外，Trusted Extensions 还提供了独有的安全功能。

Trusted Extensions 对 Oracle Solaris 安全功能的扩展

Oracle Solaris 提供的以下安全机制在 Trusted Extensions 中是可扩展的，如同它们在 Oracle Solaris 中一样：

- **审计类**－有关添加审计类的说明，请参见《Oracle Solaris 11.1 管理：安全服务》中的第 28 章“管理审计（任务）”。

  注 – 要添加**审计事件**的供应商需要联系 Oracle Solaris 代表，以保留事件数目以及获取对审计接口的访问权限。

- **角色和权限配置文件**－有关添加角色和权限配置文件的说明，请参见《Oracle Solaris 11.1 管理：安全服务》中的第 9 章“使用基于角色的访问控制（任务）”。
- **授权**－有关添加新授权的示例，请参见第 261 页中的“在 Trusted Extensions 中定制设备授权（任务列表）”。

与在 Oracle Solaris 中一样，无法扩展特权。

独有的 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。为工作区及其对象设置标签。
- **设备管理器** – 缺省情况下，设备由分配要求来提供保护。设备管理器 GUI 是供管理员和一般用户使用的界面。
- **"Change Password"（更改口令）菜单** – 使用该菜单可以更改用户或角色口令。
- **"Change Workspace Label"（更改工作区标签）菜单** – 多级别会话中的用户可以更改工作区标签。进入不同标签的工作区时，可能要求用户提供口令。
- **"Selection Manager"（选择管理器）对话框** – 多级别会话中的已授权用户可以将信息升级或降级到其他标签。
- **TrustedExtensionsPolicy 文件** – 管理员可以更改 Trusted Extensions 的特有 X 服务器扩展上的策略。有关更多信息，请参见 `TrustedExtensionsPolicy(4)` 手册页。

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。

电子邮件使用指南

使用电子邮件来指导用户执行操作是一种不安全的做法。

请警告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，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) 手册页。
- auth_attr **文件**－包含定制授权。请参见 auth_attr(4) 手册页。
- prof_attr **文件**－包含定制权限配置文件。请参见 prof_attr(4) 手册页。
- exec_attr **文件**－包含站点已添加到权限配置文件的安全属性的命令。请参见 exec_attr(4) 手册页。
- **审计迹**－包含审计服务已收集的审计记录。请参见 audit.log(4) 手册页。

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 root 进行读取。有关更多信息，请参见 shadow(4) 手册页。

组管理操作

"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。
- 决不要重复使用该用户名或用户 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。

- `/usr/share/gnome/sel_config` 文件控制为文件重新设置标签的操作，以及将信息剪切并复制到其他标签的操作。有关更多信息，请参见第 112 页中的 “sel_config 文件”和 `sel_config(4)` 手册页。
- `/usr/bin/tsoljdsselmgr` 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 8–1 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
在多个文件浏览器之间复制和粘贴、剪切和粘贴或者拖放文件	相同标签	相同 UID	无
	降级信息	相同 UID	`solaris.label.file.downgrade`
	升级信息	相同 UID	`solaris.label.file.upgrade`
	降级信息	不同 UID	`solaris.label.file.downgrade`
	升级信息	不同 UID	`solaris.label.file.upgrade`

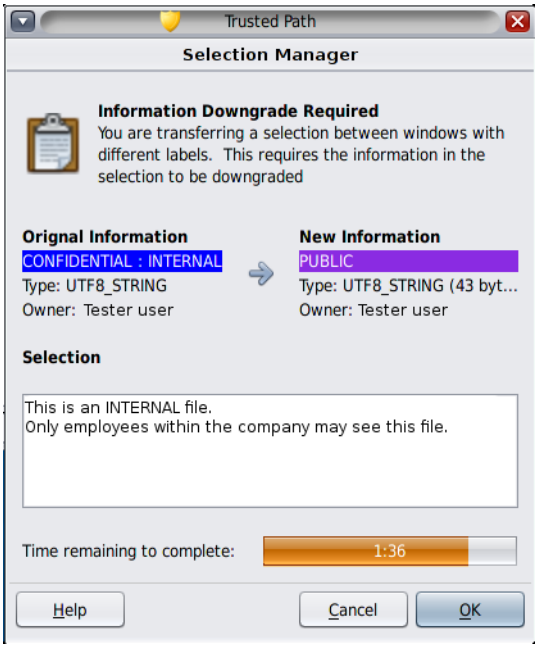
对于窗口或文件中的选定项，应用的是与上述规则不同的规则。拖放**选定项**始终要求标签和所有权与原来相同。在窗口之间的拖放操作中，起中介作用的是 "Selection Manager"（选择管理器）应用程序而不是 `sel_config` 文件。

下表汇总了更改选定项标签时适用的规则。

表 8–2 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
	降级信息	相同 UID	`solaris.label.win.downgrade`
	升级信息	相同 UID	`solaris.label.win.upgrade`
	降级信息	不同 UID	`solaris.label.win.downgrade`
	升级信息	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 提供了一个选择管理器，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，将显示该对话框。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两行选择。



缺省情况下，当数据传输到不同的标签时将显示选择管理器。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 /usr/share/gnome/sel_config 文件以确定选择管理器的行为。

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
- 是否显示选择管理器对话框

◆ ◆ ◆ 第 9 章

9 执行 Trusted Extensions 中的常见任务

本章介绍如何管理 Trusted Extensions 系统，并包含通常在这些系统上执行的任务。

- 第 113 页中的 “Trusted Extensions 管理员入门（任务列表）”
- 第 115 页中的 “Trusted Extensions 中的常见任务（任务列表）”

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 Trusted Extensions 系统。	安全登录。	《Trusted Extensions 用户指南》中的“登录到 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 ■ 使用 Trusted Extensions 手册页	《Trusted Extensions 用户指南》中的“使用有标签系统”
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 用户指南》中的“执行可信操作”
承担角色。	您在全局区域中承担某种角色。所有管理任务都是在全局区域中执行的。	第 114 页中的 “如何进入 Trusted Extensions 的全局区域”
选择用户工作区。	从全局区域中退出。	第 114 页中的 “如何退出 Trusted Extensions 的全局区域”

▼ 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。

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 134 页中的 “如何在 Trusted Extensions 中登录到故障安全会话”。

开始之前 已为您分配一个管理角色。有关指示，请参见第 106 页中的 “在 Trusted Extensions 中创建角色”。

1. **单击可信窗口条中的** *account-name*。

   从列表中选择一个角色。

   有关 Trusted Extensions 桌面功能的位置，请参见图 6–1。有关这些功能的解释，请参见《Trusted Extensions 用户指南》中的第 4 章 “Trusted Extensions 的元素（参考信息）”。

2. **在出现提示时，键入角色口令。**

   验证后，当前工作区会更改为角色工作区。

▼ 如何退出 Trusted Extensions 的全局区域

开始之前 现在您处于全局区域中。

1. **从屏幕底部的桌面面板中选择一个用户工作区。**

2. **或者，单击可信窗口条中的角色名称，然后选择您的用户名。**

   当前工作区会更改为用户工作区。您在此工作区中创建的所有后续窗口均在该用户的用户标签上创建。

   您在角色工作区中创建的窗口继续支持角色标签级别的进程。在这些窗口中启动的进程通过管理特权在全局区域中执行。

   有关更多信息，请参见《Trusted Extensions 用户指南》中的“使用有标签系统”。

Trusted Extensions 中的常见任务（任务列表）

以下任务列表介绍了 Trusted Extensions 中的常见管理过程。

任务	说明	参考
更改 root 的口令。	为 root 角色指定新口令。	第 115 页中的“如何更改 root 的口令”
在有标签区域中反映口令更改。	重新引导口令已更改的区域以更新该区域。	第 116 页中的“如何在有标签区域强制实施新的本地用户口令”
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 116 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 117 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 118 页中的“如何通过标签的十六进制形式获取可读标签”
分配设备。	允许用户分配设备。 使用外围设备向系统添加信息或者从系统中删除信息。	《Oracle Solaris 11.1 管理：安全服务》中的“如何授权用户分配设备” 《Trusted Extensions 用户指南》中的“如何在 Trusted Extensions 中分配设备”
更改系统配置文件。	更改缺省 Trusted Extensions 和 Oracle Solaris 安全值。	第 119 页中的“如何在系统文件中更改安全缺省值”
远程地管理系统。	从远程系统管理 Trusted Extensions 系统。	第 12 章，Trusted Extensions 中的远程管理（任务）

▼ 如何更改 root 的口令

Trusted Extensions 提供了可用于更改口令的 GUI。

1. **承担 root 角色。**
   有关步骤，请参见第 114 页中的“如何进入 Trusted Extensions 的全局区域”。
2. **通过单击可信窗口条中的可信符号，打开 "Trusted Path"（可信路径）菜单。**
3. **选择 "Change Login Password"（更改登录口令）。**
   如果按区域创建单独的口令，则该菜单可以读取 "Change Workspace Password"（更改工作区口令）。
4. **更改口令，然后确认更改。**

▼ 如何在有标签区域强制实施新的本地用户口令

在以下情况下，必须重新引导有标签区域：

- 一个或多个本地用户已更改了口令。
- 所有区域都在使用命名服务高速缓存守护进程 (`nscd`) 的单个实例。
- 使用文件（而非 LDAP）管理系统。

开始之前 您必须指定有 "Zone Security"（区域安全）权限配置文件。

- **要强制实施口令更改，请重新引导用户可以访问的有标签区域。**

  使用以下方法之一：

  - **使用 `txzonemgr` GUI。**

    ```
    # txzonemgr &
    ```

    在 "Labeled Zone Manager"（有标签区域管理器）中，导航到有标签区域，并从命令列表中选择 "Halt"（停止），然后选择 "Boot"（引导）。

  - **在全局区域的终端窗口中，使用区域管理命令。**

    您可以选择关闭或停止系统。

    - `zlogin` 命令完全关闭区域。

      ```
      # zlogin labeled-zone shutdown -i 0
      # zoneadm -z labeled-zone boot
      ```

    - `halt` 子命令绕过关闭脚本。

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

故障排除 要自动更新有标签区域的用户口令，必须配置 LDAP 或每个区域配置一个命名服务。您也可以同时配置这两者。

- 要配置 LDAP，请参见第 5 章，为 Trusted Extensions 配置 LDAP（任务）。
- 每个区域配置一个命名服务要求您具备网络方面的高级技能。有关过程，请参见第 60 页中的 “如何为每个有标签区域配置单独的名称服务”。

▼ 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 9–1 **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 9–2 **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 114 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，请执行以下操作之一：**

  - **要获取敏感标签的十六进制值，请将标签传递到命令。**

    ```
    $ atohexlabel "CONFIDENTIAL : INTERNAL USE ONLY"
    0x0004-08-48
    ```

    字符串不区分大小写，但空格必须确切。例如，以下带引号的字符串返回一个十六进制标签：

    - `"CONFIDENTIAL : INTERNAL USE ONLY"`
    - `"cnf : Internal"`

- "confidential : internal"

以下带引号的字符串返回一个解析错误：

- "confidential:internal"
- "confidential: internal"

- **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 label_encodings 文件中，安全许可标签的等效文本不包括冒号 (:)。

示例 9–3 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

/etc/security 和 /etc/default 目录中的文件包含安全值。有关更多信息，请参见《Oracle Solaris 11.1 管理：安全服务》中的第 3 章 “控制对系统的访问（任务）”。

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 您处于全局区域，并指定有 solaris.admin.edit/*filename* 授权。缺省情况下，root 角色拥有此授权。

- **编辑系统文件。**

  下表列出了安全文件以及可能在这些文件中更改的安全值。前两个文件对 Trusted Extensions 而言是唯一的。

文件	任务	更多信息
/usr/share/gnome/ 中的 sel_config	指定信息移动到其他标签时系统的行为。	sel_config(4) 手册页
/usr/lib/xorg/ 中的 TrustedExtensionsPolicy	修改 X 服务器中标签隔离的 SUN_TSOL 安全策略执行机制。	TrustedExtensionsPolicy(4) 手册页
/etc/default/login	减少允许的口令尝试次数。	请参见《Oracle Solaris 11.1 管理：安全服务》中的“如何监视所有失败的登录尝试”中的示例。 passwd(1) 手册页
/etc/default/kbd	禁用键盘关机。	《Oracle Solaris 11.1 管理：安全服务》中的“如何禁用系统的异常中止序列” **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。 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 10 章

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，请参见第 61 页中的 “在 Trusted Extensions 中创建角色和用户”。

- 第 121 页中的 “Trusted Extensions 中的用户安全功能”
- 第 122 页中的 “管理员针对用户的职责”
- 第 123 页中的 “在 Trusted Extensions 中创建用户之前要做的决策”
- 第 123 页中的 “Trusted Extensions 中的缺省用户安全属性”
- 第 124 页中的 “Trusted Extensions 中的可配置用户属性”
- 第 124 页中的 “必须为用户指定的安全属性”

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 权限配置文件中的命令具有一个标签属性。命令必须在标签范围内或在特定标签执行。
- Trusted Extensions 软件向 Oracle Solaris 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。

有关设置用户和角色的详细信息，请参见以下内容：

- 《在 Oracle Solaris 11.1 中管理用户帐户和用户环境》中的“使用 CLI 设置和管理用户帐户（任务列表）”
- 《Oracle Solaris 11.1 管理：安全服务》中的第 III 部分, “角色、权限配置文件和特权”

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
- 指定初始口令
- 修改除安全属性以外的用户和角色属性

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 `root` 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。

在 Trusted Extensions 中创建用户之前要做的决策

以下决策影响用户可在 Trusted Extensions 中执行的操作，以及需要付出多大的努力。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最初是由初始设置团队配置的。有关缺省值的说明，请参见第 123 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 131 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 USB 设备。

  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 264 页中的 “如何指定设备授权”。要创建更为细化的设备授权集，请参见第 261 页中的 “在 Trusted Extensions 中定制设备授权（任务列表）”。
- 确定是否必须要在有标签区域中单独创建用户帐户。

  缺省情况下，有标签区域共享全局区域名称服务配置。因此，在全局区域中为所有区域创建了用户帐户。有标签区域中的 `/etc/passwd` 和 `/etc/shadow` 文件为全局区域文件的只读视图。同样，LDAP 数据库在有标签区域中为只读。

  从区域中安装到该区域的应用程序可能会要求创建用户帐户，如 `pkg:/service/network/ftp`。要允许特定于区域的应用程序创建用户帐户，必须配置每区域名称服务守护进程，如第 60 页中的 “如何为每个有标签区域配置单独的名称服务”中所述。此类应用程序添加到有标签区域的用户帐户必须由区域管理员手动进行管理。

注 – 存储在 LDAP 中的帐户仍从全局区域进行管理。

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 124 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。他们的决策基于第 27 页中的 “设计标签策略”以及《Trusted Extensions Label Administration》中的示例。

安全管理员为各个用户显式设置的标签值将覆盖 label_encodings 文件中的值。

Trusted Extensions 中的 policy.conf 文件缺省值

/etc/security/policy.conf 文件包含系统的缺省安全值。Trusted Extensions 向此文件中添加了两个关键字。要将值更改为系统范围的值，请将这些 *keyword=value* 对添加到该文件。下表显示了这些关键字的缺省值和可能值。

表 10–1 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	适用于登录用户。
IDLETIME	30	0 至 120 分钟	适用于登录用户。

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。

第 31 页中的 “在 Trusted Extensions 中规划用户安全”提供了包含每个 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

对于可在多个标签登录的用户，您可能希望在每个用户的最小标签起始目录中设置两个帮助应用程序文件 .copy_files 和 .link_files。有关更多信息，请参见第 126 页中的 “.copy_files 和 .link_files 文件”。

必须为用户指定的安全属性

安全管理员可以修改新用户的安全属性。有关包含缺省值的文件的信息，请参见第 123 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 10–2 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	指定后产生的影响
Password（口令）	无	需要	用户具有口令

表 10–2 创建用户后指定的安全属性 （续）

用户属性	缺省值的位置	是否需要操作	指定后产生的影响
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）	内核	可选	将以不同于系统缺省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，请考虑以下信息：

指定口令

帐户创建期间，系统管理员可以为用户帐户指定口令。该初始指定之后，安全管理员或用户可以更改口令。

与在 Oracle Solaris 中一样，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。可以为用户分配多个角色（如果这样做符合您站点的安全策略）。

指定授权
与在 Oracle Solaris OS 中一样，为用户指定授权可将这些授权添加到现有授权。最佳做法是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
与在 Oracle Solaris OS 中一样，权限配置文件的顺序很重要。除了授权以外，配置文件机制使用指定的安全属性的第一个实例的值。有关更多信息，请参见《Oracle Solaris 11.1 管理：安全服务》中的“搜索指定安全属性的顺序”。

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 – 请勿将包含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，所以该权限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，请参见第 136 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修改用户的预选掩码。有关审计的更多信息，请参见《Oracle Solaris 11.1 管理：安全服务》中的第 VII 部分, “在 Oracle Solaris 中审计”和第 22 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 131 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                 .cshrc                  .mime_types
.aliases                .emacs                  .newsrc
.bashrc                 .login                  .signature
.bashrc.user            .mailrc                 .soffice
```

◆ ◆ ◆ 第 11 章

11 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。

- 第 129 页中的 “针对安全性定制用户环境（任务列表）”
- 第 134 页中的 “管理用户和权限（任务列表）”

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。其中的许多任务需要在一般用户登录之前执行。

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 130 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 130 页中的 “如何修改 `policy.conf` 缺省值”
	在系统空闲达到设定的时间量之后，打开屏幕保护程序或注销用户。	示例 11–1
	为系统的所有一般用户删除不必要的特权。	示例 11–2
	阻止在公共资讯服务站的已打印输出中显示标签。	示例 11–3
为用户配置初始化文件。	为所有用户配置启动文件，例如 `.bashrc`、`.cshrc`、`.copy_files` 和 `.soffice`。	第 131 页中的 “如何在 Trusted Extensions 中为用户配置启动文件”
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 134 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。必须将所做更改复制到每个 Trusted Extensions 系统。

注意 – 必须在任何一般用户访问系统之前完成此任务。

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 114 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。**
   有关缺省设置，请参见第 31 页中的 “在 Trusted Extensions 中规划用户安全”中的表 1–2。
2. **在 `label_encodings` 文件中修改用户属性设置。**
3. **将文件的副本分发到每个 Trusted Extensions 系统。**

注意 – `label_encodings` 文件在所有系统上必须都相同。要想了解一种分发方法，请参见第 74 页中的 “如何在 Trusted Extensions 中将文件复制到便携介质”和第 75 页中的 “如何在 Trusted Extensions 中从便携介质复制文件”。

▼ 如何修改 `policy.conf` 缺省值

在 Trusted Extensions 中更改 `policy.conf` 缺省值等同于在 Oracle Solaris 中更改任何安全相关系统文件。使用以下过程可为系统的所有用户更改缺省值。

开始之前 您必须在全局区域中承担 `root` 角色。有关详细信息，请参见第 114 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 10–1。
2. **修改设置。**

示例 11–1 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，`root` 角色将按如下方式将 `IDLECMD` *keyword=value* 对添加到 `/etc/security/policy.conf` 文件：

```
IDLECMD=LOGOUT
```

管理员还想缩短系统在注销之前空闲的时间。因此，root 角色将按如下方式将 IDLETIME *keyword=value* 对添加到 policy.conf 文件：

```
IDLETIME=10
```

现在，系统会在空闲 10 分钟后注销用户。

请注意，如果登录用户承担了某个角色，则用户的 IDLECMD 和 IDLETIME 值将对该角色生效。

示例 11–2 修改每个用户的基本特权集

在本示例中，大型 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，root 角色将从基本特权集中删除 proc_info。将按如下方式对 /etc/policy.conf 文件中的 PRIV_DEFAULT 设置取消注释并进行修改：

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

示例 11–3 为系统的所有用户指定与打印相关的授权

在此示例中，站点安全允许公共资讯服务站计算机在打印时不带标签。在公共资讯服务站中，root 角色修改 /etc/security/policy.conf 文件中的 AUTHS_GRANTED 值。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。管理员进一步修改 policy.conf 条目。

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

重新引导公共资讯服务站后，所有打印作业均不带标签，也没有标题页和篇尾页。

▼ 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 114 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. **在编辑器中，键入 `.copy_files` 文件的完整路径名。**

      ```
      # pfedit /etc/skel/.copy_files
      ```

   b. **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 126 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 11–4。

3. **定制 `.link_files` 文件。**

   a. **在编辑器中，键入 `.link_files` 的完整路径名。**

      ```
      # pfedit /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。**

   - 有关启动文件中包含哪些文件的讨论，请参见《在 Oracle Solaris 11.1 中管理用户帐户和用户环境》中的“定制用户的工作环境”。
   - 有关详细信息，请参见《在 Oracle Solaris 11.1 中管理用户帐户和用户环境》中的“如何定制用户初始化文件”。

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 11–4 为用户定制启动文件

在本示例中，系统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。

系统管理员创建具有以下内容的 .copy_files 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
.bashrc
.bashrc.user
.cshrc
.login
:wq

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

将定制的文件复制到相应的框架目录中。

```
$ cp .copy_files .link_files .bashrc .bashrc.user .cshrc \
.login .profile .mailrc /etc/skelC
$ cp .copy_files .link_files .ksh .profile .mailrc \
/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. **在登录屏幕中键入用户名。**
2. **在屏幕底部，从桌面菜单中选择 Solaris Trusted Extensions 故障安全会话。**
3. **出现提示时，键入口令。**
4. **提示输入其他口令时，键入 root 口令。**
   现在，您可以调试用户的初始化文件了。

管理用户和权限（任务列表）

在 Trusted Extensions 中，您将承担 "Security Administrator"（安全管理员）角色，以便管理用户、授权、权限和角色。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 135 页中的 “如何修改用户的标签范围”
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 135 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 136 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 137 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 137 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 138 页中的 “如何从 Trusted Extensions 系统删除用户帐户”

▼ 如何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，可登录全局区域的用户也可以查看在特定标签中运行的系统列表。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。

- **执行以下操作之一：**
  - **要扩展用户的标签范围，请指定一个更高级别的安全许可。**

    ```
    # usermod -K min_label=INTERNAL -K clearance=ADMIN_HIGH jdoe
    ```

    也可以通过降低最小标签的级别，来扩展用户的标签范围。

    ```
    # usermod -K min_label=PUBLIC -K clearance=INTERNAL jdoe
    ```

    有关更多信息，请参见 `usermod(1M)` 和 `user_attr(4)` 手册页。
  - **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。**

    ```
    # usermod -K min_label=INTERNAL -K clearance=INTERNAL jdoe
    ```

▼ 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 130 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. **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《Oracle Solaris 11.1 管理：安全服务》中的“如何创建权限配置文件”。

   下列授权可能便于用户使用：

   - `solaris.device.allocate`－授权用户分配外围设备，例如麦克风或 CD-ROM。

     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。

- `solaris.label.file.downgrade`－授权用户降低文件的安全级别。
- `solaris.label.file.upgrade`－授权用户提高文件的安全级别。
- `solaris.label.win.downgrade`－授权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。
- `solaris.label.win.noview`－授权用户移动信息而不查看所移动的信息。
- `solaris.label.win.upgrade`－授权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。
- `solaris.login.remote`－授权用户远程登录。
- `solaris.print.nobanner`－授予用户打印无标题页打印件的权限。
- `solaris.print.unlabeled`－授予用户打印不显示标签的打印件的权限。
- `solaris.system.shutdown`－授权用户关闭系统和关闭区域。

2 **将权限配置文件指定给用户或角色。**

有关逐步操作过程，请参见《Oracle Solaris 11.1 管理：安全服务》中的“如何更改用户的安全属性”。

▼ 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。

- **删除 "basic"（基本）集中的一个或多个特权。**

注意 – 请勿删除 `proc_fork` 或 `proc_exec` 特权。如果没有这些特权，用户无法使用系统。

```
# usermod -K defaultpriv=basic,!proc_info,!proc_session,!file_link_any
```

通过删除 `proc_info` 特权，可以防止用户检查其他用户发起的任何进程。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。

另请参见 有关收集权限配置文件中特权限制的示例，请参见《Oracle Solaris 11.1 管理：安全服务》中的“如何创建权限配置文件”中的示例。

要限制系统中所有用户的特权，请参见示例 11–2。

▼ 如何防止锁定用户帐户

对可承担角色的所有用户执行以下过程。

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

- **对本地用户关闭帐户锁定。**

```
# usermod -K lock_after_retries=no jdoe
```

要对 LDAP 用户关闭帐户锁定，请指定 LDAP 系统信息库。

```
# usermod -S ldap -K lock_after_retries=no jdoe
```

▼ 如何允许用户更改数据的安全级别

可以授权一般用户或角色更改文件和目录或所选文本的安全级别或标签。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 160 页中的 “如何在有标签区域中允许重新为文件设置标签”。

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。

- **将"Object Label Management"（对象标签管理）权限配置文件指定给相应的用户和角色。**

有关逐步操作过程，请参见《Oracle Solaris 11.1 管理：安全服务》中的“如何更改用户的安全属性”。

示例 11–5 允许用户升级而非降级文件标签

"Object Label Management"（对象标签管理）权限配置文件允许用户升级和降级标签。在此示例中，管理员允许可信用户升级数据，但不能将其降级。

管理员创建了一个基于"Object Label Management"（对象标签管理）配置文件的权限配置文件，并删除了新配置文件中的"Downgrade File Label"（降级文件标签）和 "Downgrade DragNDrop or CutPaste Info"（降级 DragNDrop 或 CutPaste 信息）授权。

```
# profiles -p "Object Label Management"
profiles:Object Label Management> set name="Object Upgrade"
profiles:Object Upgrade> info auths
...
```

```
profiles:Object Upgrade> remove auths="solaris.label.file.downgrade,
solaris.label.win.downgrade"
profiles:Object Upgrade> commit
profiles:Object Upgrade> end
```

然后，管理员将配置文件指定给可信用户。

```
# usermod -P +"Object Upgrade" jdoe
```

▼ 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 您必须具有全局区域中的 "System Administrator"（系统管理员）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. **删除用户帐户。**

   ```
   # userdel -r jdoe
   ```

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。

有关其他注意事项，请参见第 109 页中的 “用户删除操作”。

◆ ◆ ◆ 第 12 章

Trusted Extensions 中的远程管理（任务）

本章介绍了如何设置要进行远程管理的 Trusted Extensions 系统，以及如何登录和管理该系统。

- 第 139 页中的 “Trusted Extensions 中的远程管理”
- 第 140 页中的 “Trusted Extensions 中用于管理远程系统的方法”
- 第 141 页中的 “在 Trusted Extensions 中配置和管理远程系统（任务列表）”

注 – 无显示系统和其他远程系统所需的配置方法不满足通过评估的配置的条件。有关更多信息，请参见第 26 页中的 “了解站点的安全策略”。

Trusted Extensions 中的远程管理

远程管理带来了相当大的安全风险，尤其是来自不可信系统中的用户。缺省情况下，Trusted Extensions 不允许从任何系统进行远程管理。

配置网络之前，为所有远程主机指定了 `admin_low` 安全模板，即，将它们识别为无标签主机。配置有标签区域之前，唯一可用的区域是全局区域。在 Trusted Extensions 中，全局区域是管理区域。只有角色才可以访问该区域。具体来说，帐户必须具有从 `ADMIN_LOW` 到 `ADMIN_HIGH` 的标签范围，才能访问全局区域。

在该初始状态下，通过多种机制来保护 Trusted Extensions 系统免受远程攻击。机制包括 `netservices` 值、缺省 `ssh` 策略、缺省登录策略和缺省 PAM 策略。

- 安装时，除安全 shell 之外不会启用任何远程服务来侦听网络。

  但是，由于 `ssh`、登录和 PAM 策略，`root` 或角色无法使用 `ssh` 服务进行远程登录。
- `root` 帐户不能用于远程登录，因为 `root` 是一个角色。角色不能登录，这由 PAM 强制执行。

  即使将 `root` 更改为用户帐户，缺省登录和 `ssh` 策略也会阻止 `root` 用户远程登录。
- 两个缺省 PAM 值可阻止远程登录。

pam_roles 模块拒绝 role 类型的帐户进行本地和远程登录。

Trusted Extensions PAM 模块 pam_tsol_account 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。

因此，与在 Oracle Solaris 系统中一样，必须对远程管理进行配置。Trusted Extensions 添加了两个配置要求，即，访问全局区域所需的标签范围和 pam_tsol_account 模块。

Trusted Extensions 中用于管理远程系统的方法

在 Trusted Extensions 中，您必须使用 安全 Shell 协议以及基于主机的验证，才能访问和管理远程系统。使用基于主机的验证，具有相同名称的用户帐户可以在远程 Trusted Extensions 上承担角色。

使用基于主机的验证时，安全 Shell 客户机会向远程系统（即服务器）发送原始用户名和角色名称。使用该信息，服务器可以将足够的内容传递到 pam_roles 模块以启用角色承担，而无需使用用户帐户登录到服务器。

下面是在 Trusted Extensions 中可以使用的远程管理方法：

- **从 Trusted Extensions 系统进行管理** – 对于最安全的远程管理，两个系统均将它们的对等方指定给 CIPSO 安全模板。请参见示例 12–1。
- **从无标签系统进行管理** – 如果由 Trusted Extensions 系统进行管理不切合实际，可以通过为 PAM 栈中的 pam_tsol_account 模块指定 allow_unlabeled 选项放宽网络协议策略。

  如果放宽该策略，则必须更改缺省安全模板，以便使任意系统都无法访问全局区域。应谨慎使用 admin_low 模板，并且通配符地址 0.0.0.0 不得缺省为 ADMIN_LOW 标签。有关详细信息，请参见第 205 页中的 “如何限定可能会在可信网络上联系的主机”。

在任一管理方案中，要使用 root 角色进行远程登录，必须通过为 pam_roles 模块指定 allow_remote 选项来放宽 PAM 策略。

通常，管理员使用 ssh 命令从命令行管理远程系统。通过 -X 选项，可以使用 Trusted Extensions 管理 GUI。

另外，也可以对远程 Trusted Extensions 配置 Xvnc 服务器。然后，可以使用虚拟网络计算 (Virtual Network Computing, VNC) 连接来显示远程多级别桌面并管理系统。请参见第 143 页中的 “如何对 Trusted Extensions 系统配置 Xvnc 以进行远程访问”。

在 Trusted Extensions 中配置和管理远程系统（任务列表）

将远程系统重新引导至 Trusted Extensions 之前，启用远程管理之后，您可以使用虚拟网络计算 (Virtual Network Computing, VNC) 或 ssh 协议配置系统。

任务	说明	参考
启用对 Trusted Extensions 系统的远程管理。	从指定的 ssh 客户机启用 Trusted Extensions 系统的管理。	第 141 页中的 “启用对远程 Trusted Extensions 系统的远程管理”
启用虚拟网络计算 (Virtual Network Computing, VNC)。	从任何客户机，使用远程 Trusted Extensions 系统上的 Xvnc 服务器向客户机回显服务器的多级别会话。	第 143 页中的 “如何对 Trusted Extensions 系统配置 Xvnc 以进行远程访问”
远程登录 Trusted Extensions 系统。	在远程系统上承担角色以对其进行管理。	第 145 页中的 “如何登录和管理远程 Trusted Extensions 系统”

注 – 请参阅您的安全策略，以确定您的站点上允许的远程管理方法。

▼ 启用对远程 Trusted Extensions 系统的远程管理

在此过程中，您将在 Oracle Solaris 远程系统上启用基于主机的验证，然后再向其添加 Trusted Extensions 功能。远程系统是 安全 Shell 服务器。

开始之前 远程系统随 Oracle Solaris 一起安装，并且您可以访问该系统。您必须是 root 角色。

1. **在这两个系统上，启用基于主机的验证。**

   有关过程，请参见《Oracle Solaris 11.1 管理：安全服务》中的“如何为安全 Shell 设置基于主机的验证”。

   注 – 不要使用 cat 命令。通过 安全 Shell 连接复制和粘贴公钥。如果您的 安全 Shell 客户机不是 Oracle Solaris 系统，请遵循适用于您的平台的有关说明，对 安全 Shell 客户机配置基于主机的验证。

   完成此步骤后，您将在这两个系统上具有可承担 root 角色的用户帐户。为这些帐户分配了相同的 UID、GID 以及角色。此外，您已经生成公钥/私钥对，并共享公钥。

2. **在 安全 Shell 服务器上，放宽 ssh 策略以使 root 能够进行远程登录。**

   ```
   # pfedit /etc/ssh/sshd_config
   ## Permit remote login by root
   PermitRootLogin yes
   ```

   随后的步骤将限制 root 登录到特定的系统和用户。

注 – 由于管理员将承担 root 角色，因此您不需要放宽阻止远程 root 登录的登录策略。

3 在安全 Shell 服务器上，重新启动 ssh 服务。

```
# svcadm restart ssh
```

4 在安全 Shell 服务器上，在 root 的起始目录中，指定用于基于主机的验证的主机和用户。

```
# cd
# pfedit .shosts
client-host username
```

当共享公钥/私钥时，.shosts 文件将使 *client-host* 系统上的 *username* 能够承担服务器上的 root 角色。

5 在安全 Shell 服务器上，放宽两个 PAM 策略。

a. 将 /etc/pam.d/other 复制到 /etc/pam.d/other.orig。

```
# cp /etc/pam.d/other /etc/pam.d/other.orig
```

b. 修改 pam_roles 项以允许通过角色进行远程登录。

```
# pfedit /etc/pam.d/other
...
# Default definition for Account management
# Used when service name is not explicitly mentioned for account management
# ...
#account requisite    pam_roles.so.1
# Enable remote role assumption
account requisite    pam_roles.so.1   allow_remote
...
```

此策略使 *client-host* 系统上的 *username* 能够承担服务器上的角色。

c. 修改 pam_tsol_account 项以允许无标签主机与 Trusted Extensions 远程系统联系。

```
# pfedit /etc/pam.d/other
# Default definition for Account management
# Used when service name is not explicitly mentioned for account management
# ...
#account requisite    pam_roles.so.1
# Enable remote role assumption
account requisite    pam_roles.so.1   allow_remote
#
account required     pam_unix_account.so.1
#account required     pam_tsol_account.so.1
# Enable unlabeled access to TX system
account required     pam_tsol_account.so.1  allow_unlabeled
```

6 测试配置。

a. 在远程系统上打开新的终端。

b. 在 *client-host* 上 *username* 所拥有的窗口中，承担远程系统上的 root 角色。

```
% ssh -l root remote-system
```

7 证明配置正常工作后，在远程系统上启用 Trusted Extensions 并重新引导。

```
# svcadm enable -s labeld
# /usr/sbin/reboot
```

示例 12–1 为远程管理指定 CIPSO 主机类型

在此示例中，管理员将使用 Trusted Extensions 系统来配置远程 Trusted Extensions 主机。为此，管理员将在每个系统上使用 `tncfg` 命令来定义对等系统的主机类型。

remote-system `# tncfg -t cipso add host=192.168.1.12` *Client-host*

client-host `# tncfg -t cipso add host=192.168.1.22` *Remote system*

由于无标签系统也可以配置远程 Trusted Extensions 主机，因此管理员可以在远程主机的 `pam.d/other` 文件中保留 `allow_unlabeled` 选项。

▼ 如何对 Trusted Extensions 系统配置 Xvnc 以进行远程访问

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 服务器。在 Trusted Extensions 中，任何平台上的客户机都可以连接到运行 Trusted Extensions 的 Xvnc 服务器，登录到 Xvnc 服务器，然后显示多级别桌面并在其上工作。

有关更多信息，请参见 `Xvnc`(1) 和 `vncconfig` (1) 手册页。

开始之前 您已经在将用作 Xvnc 服务器的此系统上安装并配置了 Trusted Extensions。此系统上的全局区域具有固定 IP 地址，即，它不使用自动网络配置的配置文件，如 `netcfg`(1M) 手册页中所述。

此系统通过主机名或 IP 地址识别 VNC 客户机。具体来说，`admin_low` 安全模板以显式方式或使用通配符标识可作为此服务器的 VNC 客户机的系统。有关安全配置连接的更多信息，请参见第 205 页中的 “如何限定可能会在可信网络上联系的主机”。

如果当前正在将来 Trusted Extensions Xvnc 服务器的控制台上的 GNOME 会话中运行，则不必启用桌面共享。

您是将来 Trusted Extensions Xvnc 服务器的全局区域中的 `root` 角色。

1 装入或更新 Xvnc 软件。

```
# packagemanager &
```

在软件包管理器 GUI 中，搜索 "vnc" 并从可用的服务器中进行选择。其中一个选项是 TigerVNC X11/VNC 服务器软件。

如果无法打开 GUI，请将本地 root 帐户添加到 X 服务器访问控制列表。以登录到 X 服务器的用户身份运行此命令。

```
% xhost +si:localuser:root
```

有关更多信息，请参见 xhost(1) 和 Xsecurity(5) 手册页。

2 **启用 X Display Manager 控制协议。**

修改 GNOME Display Manager (gdm) 定制配置文件。在 /etc/gdm/custom.conf 文件的 [xdmcp] 标题下键入 Enable=true。

```
[xdmcp]
Enable=true
```

3 **在 /etc/gdm/Xsession 文件大约第 27 行插入以下行。**

提示 – 在进行更改之前保存原始 Xsession 文件的副本。

```
DISPLAY=unix:$(echo $DISPLAY|sed -e s/::ffff://|cut -d: -f2)
```

步骤 2 和步骤 3 中的文件标记有软件包属性 preserve=true。有关此属性对在软件包升级和软件包修复期间修改的文件所产生的影响的信息，请参见 pkg(5) 手册页。

4 **启用 Xvnc 服务器服务。**

```
# svcadm enable xvnc-inetd
```

5 **注销此服务器上的所有活动 GNOME 会话。**

```
# svcadm restart gdm
```

请等待大约一分钟，让桌面管理器重新启动。然后，VNC 客户机可以进行连接。

6 **检验是否已启用 Xvnc 软件。**

```
# svcs | grep vnc
```

7 **在该 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。您可以使用 Oracle Solaris 系统信息库中的 VNC 软件。

8 **可选审计 VNC 连接。**

有关预选每个系统和每个用户的审计事件的信息，请参见《Oracle Solaris 11.1 管理：安全服务》中的“配置审计服务（任务）”。

9 **要在 VNC 客户机上显示 Xvnc 服务器工作区，请执行以下步骤：**

a. **在客户机上的终端窗口中，连接到服务器。**

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

有关命令选项，请参见 vncviewer(1) 手册页。

b. **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 用户指南》中的“登录到 Trusted Extensions”。

示例 12–2 使用 Vino 在测试环境中共享桌面

在本示例中，两个开发者使用 GNOME Vino 服务来共享显示（通过 "Launch"（启动）→ "System"（系统）→ "Preferences"（首选项）→ "Desktop Sharing"（桌面共享）菜单）。除了以上步骤，他们还通过启用 XTEST 扩展来放宽 Trusted Extensions 策略。

```
# pfedit /usr/X11/lib/X11/xserver/TrustedExtensionsPolicy
## /usr/X11/lib/X11/xserver/TrustedExtensionsPolicy file
...
#extension XTEST
extension XTEST
...
```

▼ 如何登录和管理远程 Trusted Extensions 系统

通过该过程，可以使用命令行和 txzonemgr GUI 管理远程 Trusted Extensions 系统。

开始之前 在本地和远程系统上定义相同的用户、角色和角色指定，如第 141 页中的 “启用对远程 Trusted Extensions 系统的远程管理”中所述。

1 **在桌面系统上，使来自远程系统的进程得以显示。**

```
desktop $ xhost + remote-sys
```

2 **确保您是在这两个系统上具有相同名称的用户。**

3 **从一个终端窗口，登录到远程系统。**

使用 ssh 命令登录。

```
desktop $ ssh -X -l identical-username remote-sys
Password:       Type the user's password
remote-sys $
```

-X 选项可使 GUI 得以显示。

4 **在同一终端窗口中，承担在这两个系统上具有相同定义的角色。**

例如，承担 root 角色。

```
remote-sys $ su - root
Password:       Type the root password
```

您现在已在全局区域中。现在，您可以使用此终端窗口从命令行管理远程系统。GUI 将显示在您的屏幕上。有关示例，请参见示例 12–3。

示例 12–3 配置远程系统上的有标签区域

在此示例中，管理员使用 txzonemgr GUI 从有标签桌面系统中配置有标签远程系统上的有标签区域。与在 Oracle Solaris 中一样，管理员通过使用 ssh 命令的 -X 选项使 X 服务器能够访问桌面系统。用户 jandoe 在两个系统上具有相同的定义，可以承担角色 remoterole。

```
TXdesk1 $ xhost + TXnohead4
```

```
TXdesk1 $ ssh -X -l jandoe TXnohead4
Password: Ins1PwD1
TXnohead4 $
```

要访问全局区域，管理员使用 jandoe 帐户承担角色 remoterole。该角色在两个系统上具有相同的定义。

```
TXnohead4 # su - remoterole
Password: abcd1EFG
```

在同一终端中，承担 remoterole 角色的管理员启动 txzonemgr GUI。

```
TXnohead4 $ /usr/sbin/txzonemgr &
```

"Labeled Zone Manager"（有标签区域管理器）将在远程系统上运行，并显示在本地系统上。

示例 12–4 登录到远程有标签区域

管理员想要在 PUBLIC（公共）标签下的远程系统上更改配置文件。

管理员具有两个选项。

- 远程登录到全局区域，显示远程全局区域工作区，然后将工作区更改为 PUBLIC（公共）标签，打开终端窗口，然后编辑文件
- 从 PUBLIC（公共）终端窗口中使用 ssh 命令远程登录到 PUBLIC（公共）区域，然后编辑文件

请注意，如果对于所有区域，远程系统运行一个命名服务守护进程 (nscd)，**并且**远程系统使用文件命名服务，则远程 PUBLIC 区域的口令是上次引导区域时生效的口令。如果更改了远程 PUBLIC（公共）区域的口令，但更改后未引导该区域，则原始口令仍允许访问。

故障排除 如果 `-X` 选项不起作用，您可能需要安装一个软件包。如果未安装 `xauth` 二进制文件，将会禁用 X11 转发。以下命令可装入该二进制文件：**`pkg install pkg:/x11/session/xauth`**。

◆ ◆ ◆ 第 13 章

13 在 Trusted Extensions 中管理区域

本章介绍了非全局区域（即，**有标签**区域）在 Trusted Extensions 系统中的工作方式。此外，还介绍了有标签区域特有的操作过程。

- 第 149 页中的 “Trusted Extensions 中的区域”
- 第 151 页中的 “全局区域进程和有标签区域”
- 第 152 页中的 “有标签主区域和有标签辅助区域”
- 第 153 页中的 “Trusted Extensions 中的区域管理实用程序”
- 第 153 页中的 “管理区域（任务列表）”

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标签，这样就创建了有标签区域。这些标签来自 `label_encodings` 文件。您可以为每个标签创建一个或多个区域，但不是必须如此。系统上具有的标签可能会比有标签区域要多。

在 Trusted Extensions 系统中，全局区域只是一个管理区域。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。

在 Trusted Extensions 系统中，所有的区域都有 *labeled* 标记，并且有标签区域中的所有可写文件和目录都使用该区域的标签。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。

每个区域都是一个独立的 ZFS 文件系统。每个区域都可以具有关联的 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 14 章，在 Trusted Extensions 中管理和挂载文件和第 165 页中的 “mslabel 属性和挂载单级别文件系统”。

Trusted Extensions 中的区域构建于 Oracle Solaris Zones 产品之上。有关参考，请参见《Oracle Solaris 11.1 管理：Oracle Solaris Zones、Oracle Solaris 10 Zones 和资源管理》中的第 II 部分, “Oracle Solaris Zones”。

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。他们考虑了如第 29 页中的 “访问有标签区域”中所述的三种配置，并归纳如下：

- 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 软件获取其 IP 地址的系统，这种缺省配置非常有用。
- 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联网系统，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。

在 Oracle Solaris 中提供了适用于非全局区域的第四种配置，即专用 IP 实例。在这种配置中，一个非全局区域指定有其自己的 IP 实例，并管理其自己的物理接口。每个区域就像是一个独立系统一样运行。有关说明，请参见《Oracle Solaris 11.1 管理：Oracle Solaris Zones、Oracle Solaris 10 Zones 和资源管理》中的“区域网络接口”。

如果在 Trusted Extensions 中配置专用 IP 实例，则每个有标签区域就像是一个独立的**单级别**系统一样运行。Trusted Extensions 的多级别网络功能依赖于共享 IP 栈的功能。本指南假设网络完全由全局区域控制。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 (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。正在进行通信的 Trusted Extensions 系统会为该 IP 地址指定一个安全模板。安全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的标签范围包含包的标签时，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 地址的缺省配置中，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。

有关示例，请参见第 210 页中的 “如何为区域创建多级别端口”。

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 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。要共享有标签文件系统，请参见第 171 页中的 “如何从有标签区域共享文件系统”。

有标签主区域和有标签辅助区域

以特定标签创建的第一个区域是有标签主区域。其标签是唯一的。不能再以该标签创建其他主区域。

辅助区域是使用主区域标签的区域。使用辅助区域，可以将服务隔离在使用同一标签的不同区域中。这些服务可共享网络资源，如名称服务器、打印机和数据库，而无需使用特权。可以具有多个使用同一标签的辅助区域。

具体来说，辅助区域在以下方面不同于主区域：

- 不必为辅助区域指定唯一的标签。
- 辅助区域必须使用专用 IP 网络。

  此限制确保有标签包到达正确的区域。
- 辅助区域未安装 GNOME 软件包。

  辅助区域在 GNOME 可信桌面上不可见。
- 辅助区域不能是 `setlabel` 命令的目标区域。

  如果多个区域使用同一标签，则无法通过此命令解析目标区域。

对于任何标签，最多只能有一个有标签主区域，但可以有任意数量的有标签辅助区域。全局区域是例外。全局区域是唯一可以指定 `ADMIN_LOW` 标签的区域，因此不能具有辅助区域。要创建辅助区域，请参见第 71 页中的 “如何创建有标签辅助区域”和 `zenity`(1) 手册页。

Trusted Extensions 中的区域管理实用程序

可以从命令行执行区域管理任务。不过，管理区域的最简单方法是使用 Trusted Extensions 提供的 shell 脚本 `/usr/sbin/txzonemgr`。此脚本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。有关详细信息，请参见 `txzonemgr`(1M) 和 `zenity`(1) 手册页。

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。此任务列表还提供了指向 Trusted Extensions 中执行的常见操作过程（就像在 Oracle Solaris 系统中的执行一样）的链接。

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 154 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 155 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 156 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 157 页中的 “如何禁用较低级别文件的挂载”

任务	说明	参考
为文件中的标签更改创建多级别数据集。	无需特权，即可对一个 ZFS 数据集中的文件重新设置标签。	第 72 页中的 “如何创建和共享多级别数据集”
配置区域以允许对文件的标签进行更改。	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 160 页中的 “如何在有标签区域中允许重新为文件设置标签”
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 158 页中的 “如何从有标签区域共享 ZFS 数据集”。
配置新的主区域。	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。	请参见第 52 页中的 “如何以交互方式创建有标签区域”。
配置辅助区域。	为隔离不需要桌面的服务创建区域。	第 71 页中的 “如何创建有标签辅助区域”。
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 210 页中的 “如何为区域创建多级别端口” 示例 16–19
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 174 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。	《Oracle Solaris 11.1 管理： Oracle Solaris Zones、Oracle Solaris 10 Zones 和资源管理》中的“如何删除非全局区域”

▼ 如何显示就绪或正在运行区域

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. **运行 `txzonemgr &` 命令。**

   此时 GUI 中将显示区域的名称、状态和标签。

2. **或者，使用 `zoneadm list -v` 命令。**

```
# zoneadm list -v
ID NAME       STATUS     PATH              BRAND       IP
 0 global     running    /                 ipkg        shared
 5 internal   running    /zone/internal    labeled     shared
 6 public     running    /zone/public      labeled     shared
```

   输出不会列出区域的标签。

▼ 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. **在编辑器中，创建 `getmounts` 脚本。**
   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_HIGH
/dev:   ADMIN_HIGH
/system/contract:        ADMIN_HIGH
/proc:                   ADMIN_HIGH
/system/volatile:        ADMIN_HIGH
/system/object:          ADMIN_HIGH
/lib/libc.so.1:          ADMIN_HIGH
/dev/fd:        ADMIN_HIGH
/tmp:           ADMIN_HIGH
/etc/mnttab:    ADMIN_HIGH
/export:        ADMIN_HIGH
/export/home:   ADMIN_HIGH
/export/home/jdoe:   ADMIN_HIGH
/zone/public:        ADMIN_HIGH
/rpool:              ADMIN_HIGH
/zone:               ADMIN_HIGH
/home/jdoe:          ADMIN_HIGH
/zone/public:        ADMIN_HIGH
/zone/snapshot:      ADMIN_HIGH
/zone/internal:      ADMIN_HIGH
...
```

示例 13–1 显示被限制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` 区域的输出样例：

```
# /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/jdoe:   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
```

3 启动区域。

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

示例 13–2 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**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 13–3 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 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 是最低级别标签，安全管理员不对 PUBLIC 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**正在运行**状态。

开始之前 要为区域配置数据集，必须首先停止该区域。您必须在全局区域中承担 root 角色。

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 **挂载点**属性时会设置挂载点的标签。

4. **使该数据集可以共享。**

   ```
   # zfs set sharenfs=on datasetdir/subdir
   ```

5. **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进行添加，会在区域的 /data 处挂载数据集。此步骤可以确保不会在引导区域之前挂载数据集。

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 13–4 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。**被限制**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
```

然后，管理员共享该数据集。

```
# zfs set sharenfs=on 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，管理员引导 needtoknow 区域。

```
# zoneadm -z needtoknow boot
```

现在，可以访问该数据集了。

支配 needtoknow 区域的 restricted 区域中的用户可以通过转到 /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。

▼ 如何在有标签区域中允许重新为文件设置标签

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 必须停止您要配置的区域。您必须具有全局区域中的 "Security Administrator"（安全管理员）角色。

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

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

2. **配置区域以启用标签重新设置。**

   a. **双击该区域。**

   b. **从列表中选择 "Permit Relabeling"（允许重新设置标签）。**

3. **选择 "Boot"（引导）重新启动区域。**

4. **单击 "Cancel"（取消）返回到区域列表。**

   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 137 页中的 “如何允许用户更改数据的安全级别”。

示例 13–5 仅允许从 internal 区域降级

在此示例中，安全管理员使用 `zonecfg` 命令以允许从 `CNF: INTERNAL USE ONLY`（CNF：仅供内部使用）区域对信息进行降级，而不是升级。

```
# zonecfg -z internal set limitpriv=default,file_downgrade_sl
```

示例 13–6 阻止从 internal（内部）区域降级

在此示例中，安全管理员希望在以前用于降级文件的系统上阻止降级 `CNF: INTERNAL USE ONLY`（CNF：仅供内部使用）文件。

管理员使用 "Labeled Zone Manager"（有标签区域管理器）停止 `internal`（内部）区域，然后从 `internal`（内部）区域菜单中选择 "Deny Relabeling"（拒绝重新设置标签）。

◆ ◆ ◆ 第 14 章

在 Trusted Extensions 中管理和挂载文件

本章介绍了共享和挂载文件时使用的 Trusted Extensions 策略以及此策略对多级别数据集的 ZFS 挂载和单级别 ZFS 数据集的 LOFS 和 NFS 挂载的影响。本章还介绍了如何备份和恢复文件。

- 第 161 页中的 “Trusted Extensions 中的可能挂载项”
- 第 162 页中的 “用于已挂载文件系统的 Trusted Extensions 策略”
- 第 164 页中的 “在 Trusted Extensions 中共享和挂载文件系统的结果”
- 第 166 页中的 “需要为文件重新设置标签的多级别数据集”
- 第 167 页中的 “Trusted Extensions 中的 NFS 服务器和客户机配置”
- 第 169 页中的 “Trusted Extensions 软件和 NFS 协议版本”
- 第 170 页中的 “备份、共享和挂载有标签文件（任务列表）”

Trusted Extensions 中的可能挂载项

在 Trusted Extensions 中，有两种 ZFS 数据集可进行挂载。

- **有标签的单级别数据集**和其中驻留或挂载数据的区域具有相同的标签。单级别数据集中的所有文件和目录都使用同一标签。这些数据集是 Trusted Extensions 中的典型数据集。
- **多级别数据集**中可包含使用不同标签的文件和目录。此类数据集能够有效地为使用多个不同标签的 NFS 客户机提供服务，并可以简化为文件重新设置标签的过程。

在 Trusted Extensions 中可以选择以下挂载选项：

- **ZFS 挂载** – 管理员创建的多级别数据集可以通过 ZFS 方式挂载到全局区域。已通过 ZFS 方式挂载的多级别数据集可以通过 LOFS 方式挂载到同一系统中的有标签区域中。

  在有标签区域中，管理员还可以创建单级别数据集并通过 ZFS 方式进行挂载。
- **LOFS 挂载** – 如上一段所述，全局区域可以通过 LOFS 方式将单级别数据集挂载到有标签区域中。挂载的标签是 `ADMIN_LOW`，因此，所有挂载的文件在有标签区域中都处于只读状态。

全局区域还可以通过 LOFS 方式将多级别数据集挂载到有标签区域中。可以修改与区域具有相同标签的已挂载文件。如果具有相应的权限，可为文件重新设置标签。可以查看所处级别低于区域标签级别的已挂载文件。

- **NFS 挂载** – 有标签区域可以挂载使用区域标签的单级别数据集。这些文件可以来自其他有标签区域，也可以来自为其指定了与有标签区域具有相同标签的不可信系统。

  全局区域可以通过 NFS 方式挂载来自另一个 Trusted Extensions 系统的多级别数据集。可以对已挂载的文件进行查看和修改，但不能重新设置标签。此外，只有使用挂载区域标签的文件和目录可返回正确的标签。

  有标签区域可以通过 NFS 方式挂载来自另一个 Trusted Extensions 系统的多级别数据集。无法为已挂载 NFS 的文件重新设置标签，而且这些文件的标签无法通过 `getlabel` 命令确定。但是，MAC 策略可正常运行。可以查看和修改与区域具有相同标签的已挂载文件。可以查看级别较低的文件。

用于已挂载文件系统的 Trusted Extensions 策略

虽然 Trusted Extensions 和 Oracle Solaris 支持相同的文件系统和文件系统管理命令，但 Trusted Extensions 中的已挂载文件系统遵守用于查看和修改有标签数据的强制访问控制 (mandatory access control, MAC) 策略。挂载策略和读写策略会强制实施 MAC 策略以进行标记。

用于单级别数据集的 Trusted Extensions 策略

对于单级别数据集，挂载策略会阻止任何不符合 MAC 的 NFS 挂载或 LOFS 挂载。例如，区域的标签必须能够支配其已挂载的所有文件系统的标签，而且只能使用读写权限挂载带同等标签的文件系统。属于其他区域或 NFS 服务器的任意共享文件系统均使用其所有者的标签进行挂载。

下面汇总了挂载 NFS 的单级别数据集的行为：

- 在全局区域中，可以查看所有已挂载的文件，但只能修改带 `ADMIN_HIGH` 标签的文件。
- 在有标签区域中，可以查看其标签等于或低于区域标签的所有已挂载文件，但只能修改使用区域标签的文件。
- 在不可信系统上，只能查看和修改有标签区域中其标签与不可信系统的指定标签相同的文件系统。

对于已挂载 LOFS 的单级别数据集，可查看已挂载的文件。它们使用 `ADMIN_LOW` 标签，因此不能修改。

用于多级别数据集的 Trusted Extensions 策略

对于多级别数据集，会以文件和目录粒度（而不是文件系统粒度）强制实施 MAC 读写策略。

多级别数据集只能挂载在全局区域中。有标签区域只能通过使用 `zonecfg` 命令指定的 LOFS 挂载点访问多级别数据集。有关过程，请参见第 72 页中的 “如何创建和共享多级别数据集”。全局区域或有标签区域中具有适当特权的进程能够对文件和目录重新设置标签。有关重新设置标签的示例，请参见《Trusted Extensions 用户指南》 。

- 在全局区域中，可以查看多级别数据集中的所有文件。可以修改标记有 `ADMIN_HIGH` 的已挂载文件。
- 在有标签区域中，可通过 LOFS 挂载多级别数据集。可查看与区域具有相同标签或级别低于区域标签的已挂载文件。可以修改与区域具有相同标签的已挂载文件。
- 多级别数据集还可以通过 NFS 从全局区域进行共享。远程客户机可以查看受其网络标签支配的文件，修改具有相同标签的文件。但是，无法为已挂载 NFS 的多级别数据集重新设置标签。有关 NFS 挂载的信息，请参见第 167 页中的 “挂载来自其他系统的多级别数据集”。

有关更多信息，请参见第 166 页中的 “需要为文件重新设置标签的多级别数据集”。

MAC 读写策略无特权覆盖

用于读取和写入文件的 MAC 策略无特权覆盖。如果区域的标签与单级别数据集的标签相同，则只能以读写方式挂载这些数据集。对于只读挂载，区域标签必须支配数据集标签。对于多级别数据集，所有文件和目录必须由 `mlslabel` 属性支配，此属性的缺省值为 `ADMIN_HIGH`。对于多级别数据集，强制在文件和目录级别下实施 MAC 策略。MAC 策略强制实施对所有用户均不可见。用户必须对对象具有 MAC 访问权限，才能看到此对象。

下面汇总了 Trusted Extensions 中适用于单级别数据集的共享和挂载策略 :

- 为了使 Trusted Extensions 系统在其他 Trusted Extensions 系统上挂载文件系统，服务器和客户机必须具有 `cipso` 类型的兼容远程主机模板。
- 为了使 Trusted Extensions 系统从不可信系统挂载文件系统，Trusted Extensions 系统指定给不可信系统的单一标签必须匹配全局区域的标签。

  同样，为了使有标签区域从不可信系统挂载文件系统，Trusted Extensions 系统指定给不可信系统的单一标签必须匹配有挂载区域的标签。
- 可以查看，但是不能修改使用 LOFS 挂载且其标签随挂载区域而异的文件。有关 NFS 挂载的详细信息，请参见第 167 页中的 “Trusted Extensions 中的 NFS 服务器和客户机配置”。

下面汇总了 Trusted Extensions 中适用于多级别数据集的共享和挂载策略：

- 对于要与其他系统共享多级别数据集的 Trusted Extensions 系统，NFS 服务器必须配置为多级别服务。
- 对于要与自身系统上有标签区域共享多级别数据集的 Trusted Extensions 系统，全局区域必须通过 LOFS 方式将数据集挂载到区域中。

  有标签区域对其标签与区域标签匹配的那些已挂载 LOFS 的文件和目录具有写入访问权限，对其支配的文件和目录具有读取访问权限。强制在单个文件和目录级别下实施 MAC 策略。

在 Trusted Extensions 中共享和挂载文件系统的结果

在 Trusted Extensions 中，共享的文件可以简化管理并能够提高效率和速度。MAC 始终有效。

- 通过 NFS 从有标签区域共享单级别数据集－如在 Oracle Solaris 中一样，共享的目录可以简化管理。例如，您可以在一个系统上安装 Oracle Solaris 的手册页，并与其他系统共享手册页目录。
- 通过 LOFS 从全局区域共享多级别数据集－挂载 LOFS 的数据集在将文件从一个标签改为另一个标签时能够提高效率和速度。因为文件是在数据集内部移动的，所以不会使用任何 I/O 操作。
- 通过 NFS 从全局区域共享多级别数据集－NFS 服务器可将包含使用多个标签的文件的多级别数据集共享给多个客户机。此类配置可简化管理并为文件分发提供一个位置。您无需使用带特定标签的服务器为带该标签的客户机提供服务。

在全局区域中共享和挂载文件

在全局区域中挂载文件与在 Oracle Solaris 中挂载文件相同，均遵守 MAC 策略。从全局区域共享的文件会以文件的标签进行共享。因此，全局区域中的文件系统不能有效与其他 Trusted Extensions 系统的全局区域共享，因为所有文件都会以 `ADMIN_LOW` 标签进行共享。全局区域中能够有效与其他系统共享的文件是多级别数据集。

单级别数据集中通过 LOFS 从全局区域共享的文件和目录以 `ADMIN_LOW` 进行共享。例如，全局区域中的 `/etc/passwd` 和 `/etc/shadow` 文件可通过 LOFS 方式挂载到系统上的有标签区域。因为文件的标签是 `ADMIN_LOW`，所以它们在有标签区域中可见且为只读。多级别数据集中的文件和目录可以对象的标签进行共享。

全局区域还可以通过 NFS 共享多级别数据集。在将 NFS 服务配置为使用多级别端口时，客户机可以请求挂载数据集。如果客户机标签位于在 `cipso` 模板中为网络接口（用于处理客户机的 NFS 挂载请求）指定的标签范围内，则请求成功。

需要特别指出的是，全局区域和已挂载文件的行为如下：

- 在 Trusted Extensions 客户机上的全局区域中，共享中的每一项均可读，客户机能够在 ADMIN_HIGH 下写入，就像本地全局区域进程一样。
- 如果客户机是一个有标签区域，则在区域标签与共享文件的标签匹配时，已挂载的文件为可读写文件。
- 如果客户机是一个无标签系统，则在客户机的指定标签与共享文件的标签匹配时，已挂载的文件为可读写文件。
- 使用 ADMIN_LOW 标签的客户机无法挂载数据集。
- 要与同一系统上的有标签区域共享多级别数据集，全局区域可使用 LOFS。

有关查看 NFS 挂载中的文件并为其重新设置标签的更多信息，请参见第 167 页中的 “挂载来自其他系统的多级别数据集”。

在有标签区域中共享和挂载文件

有标签区域可与区域标签的其他系统共享其文件。因此，有标签区域中的文件系统可与其他 Trusted Extensions 系统中使用同一标签的区域共享，并且能够与所指定标签和区域标签相同的不可信系统共享。有关在这些挂载中起中介作用的 ZFS 属性的信息，请参见第 165 页中的 “mlslabel 属性和挂载单级别文件系统”。

全局区域中的 LOFS 挂载在有标签区域中对单级别数据集为只读。对于多级别数据集，对每个文件和目录标签强制实施 MAC 策略（如第 163 页中的 “MAC 读写策略无特权覆盖”中所述）。

mlslabel 属性和挂载单级别文件系统

ZFS 提供安全标签属性 mlslabel，其中包含数据集中数据的标签。mlslabel 属性是可继承的。当 ZFS 数据集具有显式标签时，数据集无法在没有配置 Trusted Extensions 的 Oracle Solaris 系统上挂载。

如果未定义 mlslabel 属性，则缺省值为字符串 none，表明无标签。

当您在有标签区域中挂载 ZFS 数据集时，将出现以下情况：

- 如果没有为数据集设置标签，即，未定义 mlslabel 属性，则 mlslabel 属性的值更改为挂载区域的标签。

  对于全局区域，不会自动设置 mlslabel 属性。如果显式地为数据集 admin_low 设置标签，则数据集必须以只读方式挂载。
- 如果为数据集设置了标签，则内核会检验数据集标签是否与挂载区域的标签匹配。如果标签不匹配，除非区域允许向下读取挂载，否则挂载会失败。如果区域允许向下读取挂载，则较低级别的文件系统以只读方式挂载。

要从命令行设置 mlslabel 属性，请键入类似如下的内容：

```
# zfs set mlslabel=public export/publicinfo
```

要设置初始标签，或将非缺省标签更改为较高级别的标签，需要 file_upgrade_sl 特权。要删除标签（即，将标签设置为 none），需要 file_downgrade_sl 特权。要将非缺省标签更改为较低级别的标签，也需要该特权。

需要为文件重新设置标签的多级别数据集

多级别 ZFS 数据集设计用于包含使用不同标签的文件和目录。每个文件和目录都带有各自的标签，可以在不移动或复制文件的情况下更改这些标签。可在数据集的标签范围内为文件重新设置标签。要创建和共享多级别数据集，请参见第 72 页中的“如何创建和共享多级别数据集”。

通常，数据集中的所有文件和目录的标签与其中挂载此数据集的区域的标签相同。当数据集首次挂载到此区域时，会在名为 mlslabel 的 ZFS 属性中自动记录此标签。这些数据集是**有标签的单级别数据集**。在挂载数据集时，无法更改 mlslabel 属性，即挂载区域无法更改 mlslabel 属性。

设置 mlslabel 属性后，区域的标签必须与数据集的 mlslabel 属性匹配，才能以读写方式将此数据集挂载到此区域中。此外，如果数据集当前已挂载到任何区域（包括全局区域），则它无法挂载到其他任何区域。因为有标签单级别数据集中文件的标签是固定的，所以在使用 setlabel 命令为文件重新设置标签时，此文件实际上会移动到主区域中与目标标签对应的等效路径名中。这种跨区域移动效率可能会很低，并且可能造成混乱。多级别数据集可为重新设置数据标签提供有效的容器。

对于在全局区域中挂载的多级别数据集，mlslabel 属性的缺省值为 ADMIN_HIGH。此值指定数据集的标签范围上界。如果指定较低级别的标签，则只能从其标签受 mlslabel 属性支配的区域写入到数据集。

具有 "Object Label Management"（对象标签管理）权限配置文件的用户或角色使用适当特权升级或降级他们对其具有 DAC 访问权限的文件或目录。有关过程，请参见第 137 页中的“如何允许用户更改数据的安全级别”。

对于用户进程，还适用其他策略约束。

- 缺省情况下，在有标签区域中，无任何进程能够为文件或目录重新设置标签。要启用标签重新设置，请参见第 160 页中的“如何在有标签区域中允许重新为文件设置标签”。要指定更高粒度的控制（例如，允许降级文件但不允许升级文件），请参见示例 13–5。
- 只有目录为空时才可以为其重新设置标签。
- 文件和目录要降级到的标签级别不能低于其所含目录的标签级别。

  要重新设置标签，首先将文件移动到较低级别的目录，然后为其重新设置标签。

- 挂载数据集的区域不能将文件或目录升级到区域标签之上。
- 如果文件当前已由任何区域中的一个进程打开，则无法为其重新设置标签。
- 文件和目录不能升级到数据集的 `mlslabel` 值之上。

挂载来自其他系统的多级别数据集

全局区域可通过 NFS 与 Trusted Extensions 系统和无标签系统共享多级别数据集。数据集可在全局区域和有标签区域中及使用指定标签的无标签系统中挂载。例外情况为 `ADMIN_LOW` 无标签系统。它无法挂载多级别数据集。

使用级别低于 `ADMIN_HIGH` 的标签创建多级别数据集时，可在另一个 Trusted Extensions 系统的全局区域中挂载该数据集，但在该全局区域中只能查看文件，不能修改文件。有标签区域 NFS 挂载来自其他系统的全局区域的多级别数据集时，会存在一些限制。

- 一些限制适用于已挂载 NFS 的多级别数据集。
- Trusted Extensions NFS 客户机仅能看到可写入的文件的正确标签。`getlabel` 命令将较低级别文件的标签错误报告为客户机的标签。MAC 策略有效，因此文件保持只读状态，较高级别文件不可见。
- NFS 服务器忽略客户机可能具有的任何特权。

由于这些限制，对要从其自己的全局区域中获得处理的有标签区域客户机，最好使用 LOFS。NFS 适用于这些客户机，但它们具有一些限制。有关 LOFS 挂载过程，请参见第 72 页中的 “如何创建和共享多级别数据集”。

Trusted Extensions 中的 NFS 服务器和客户机配置

可使较低级别目录对较高级别区域中的用户可见。较低级别目录的 NFS 服务器可以是 Trusted Extensions 系统，也可以是不可信系统。

可信系统需要服务器配置。不可信系统需要客户机配置。

- **关于可信系统的 NFS 服务器配置 –** 要使可信系统中的较低级别目录在有标签区域中可见，需要配置此服务器。
  - 在 NFS 服务器的全局区域中，必须将 NFS 服务配置为多级别服务。
  - 在全局区域中，管理员必须将 `net_bindmlp` 特权添加到有标签区域的 `limitpriv` 中。
  - 在有标签区域中，通过设置 ZFS 文件系统的共享属性导出该文件系统。当有标签区域的状态为 `running` 时，文件系统将在区域的标签级别共享。有关过程，请参见第 171 页中的 “如何从有标签区域共享文件系统”。

- **关于不可信 NFS 服务器的 NFS 客户机配置 –** 因为此服务器不可信，所以 NFS 客户机必须可信。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 173 页中的 “如何在有标签区域中对文件进行 NFS 挂载”。

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`。

注 – `txzonemgr` 脚本假设起始目录挂载为 `/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 168 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。但是，起始目录是在起始目录服务器的全局区域中创建的。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 138 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。要为用户创建起始目录，请参见第 68 页中的 “如何让用户登录每个 NFS 服务器来访问每个标签下的远程起始目录”。

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/*zone-name*/export/home 下，且为只读。auto_home_*zone-name* 映射指定 /zone 路径作为 lofs 重新挂载到 /zone/*zone-name*/home/*username* 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-level* 映射中的 auto_home_public 项：

```
+auto_home_public
*    public-zone-IP-address:/export/home/&
```

txzonemgr 脚本在全局区域中的 auto_master 文件中设置该 PUBLIC 项：

```
+auto_master
/net        -hosts        -nosuid,nobrowse
/home        auto_home    -nobrowse
/zone/public/home      auto_home_public      -nobrowse
```

如果引用了一个起始目录且该名称与 auto_home_*zone-name* 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

Trusted Extensions 软件识别 NFS 版本 3 (NFSv3) 和 NFSv4 上的标签。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。

对于 NFSv3，Trusted Extensions 的行为与 Oracle Solaris 相同。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。有关过程，请参见示例 16–19。

Trusted Extensions 系统还可以与无标签主机共享其单级别数据集。当导出到无标签主机的文件系统的标签与通过导出系统指定给远程主机的标签相同时，该文件系统为**可写**状态。仅当导出到无标签主机的文件系统的标签由指定给远程系统的标签支配时，该文件系统才为**可读**状态。

对于全局区域与运行 NFSv4 服务器的客户机所共享的多级别数据集，MAC 策略所处的粒度是各个文件和目录，而不是整个数据集标签。

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。为 Trusted Solaris 系统指定的标签可确定它对单级别数据集和多级别数据集的访问权限。

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。为远程文件系统的 `mount` 命令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文件系统的常见任务。

任务	说明	参考
备份文件。	保留标签的情况下归档数据。	第 170 页中的 “如何在 Trusted Extensions 中备份文件”
恢复数据。	从备份恢复有标签数据。	第 171 页中的 “如何在 Trusted Extensions 中恢复文件”
共享有标签文件系统。	允许其他系统上的用户访问有标签文件系统。	第 171 页中的 “如何从有标签区域共享文件系统”
挂载有标签区域共享的文件系统。	允许在有标签区域中在同一个标签以读写方式挂载文件系统的内容。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 173 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 起始目录服务器系统上的每个标签访问其起始目录。	第 68 页中的 “如何让用户登录每个 NFS 服务器来访问每个标签下的远程起始目录”
对在较高级别标签工作的用户隐藏较低级别信息。	防止从较高级别查看较低级别的信息。	第 157 页中的 “如何禁用较低级别文件的挂载”
解决文件系统挂载问题。	解决文件系统挂载问题。	第 174 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

开始之前 您必须指定有 "Media Backup"（介质备份）权限配置文件。现在您处于全局区域中。

- **执行保留标签的备份。**

以下命令保留标签。

- 对于主要备份，使用 `zfs send -r | -R` *filesystem*`@snap`

  有关可用方法（包括将备份发送到远程服务器），请参见《Oracle Solaris 11.1 管理：ZFS 文件系统》中的“发送和接收 ZFS 数据”。
- 对于小型备份，使用 `/usr/sbin/tar cT`

  有关 `T` 选项到 `tar` 命令的详细信息，请参见 `tar(1)` 手册页。
- 调用 `zfs` 或 `tar` 备份命令的脚本

▼ 如何在 Trusted Extensions 中恢复文件

开始之前 您是全局区域中的 `root` 角色。

● **恢复有标签备份。**

以下命令可恢复有标签备份。

- 对于主要恢复，使用 `zfs receive -vF` *filesystem*`@snap`

  有关可用方法（包括从远程服务器恢复备份），请参见《Oracle Solaris 11.1 管理：ZFS 文件系统》中的“发送和接收 ZFS 数据”。
- 对于小型恢复，使用 `/usr/sbin/tar xT`

  有关 `T` 选项到 `tar` 命令的详细信息，请参见 `tar(1)` 手册页。
- 调用 `zfs` 或 `tar` 恢复命令的脚本

▼ 如何从有标签区域共享文件系统

要挂载或共享源自有标签区域的目录，请对文件系统设置相应的 ZFS 共享属性，然后重新启动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 您必须指定有 "ZFS File System Management"（ZFS 文件系统管理）权限配置文件。

1. **以将要共享的文件系统的标签创建工作区。**

   有关详细信息，请参见《Trusted Extensions 用户指南》中的“如何在最小标签下添加工作区”。

2. **在区域中，创建文件系统。**

```
# zfs create rpool/wdocs1
```

3 **通过设置 ZFS 共享属性共享文件系统。**

例如，以下一组命令共享编写者的文档文件系统。文件系统共享读写权限，以便编写者可以在该服务器上修改其文档。禁止了 setuid 程序。

```
# zfs set share=name=wdocs1,path=/wdocs1,prot=nfs,setuid=off,
exec=off,devices=off rpool/wdocs1
# zfs set sharenfs=on rpool/wdocs1
```

命令行由于显示的原因进行了换行。

4 **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方法来共享其文件系统。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
  ```

5 **显示从您的系统共享的文件系统。**

在全局区域中以 root 角色运行以下命令：

```
# zfs get all rpool
```

有关更多信息，请参见《Oracle Solaris 11.1 管理：ZFS 文件系统》中的“查询 ZFS 文件系统信息”

6 **要允许客户机挂载共享文件系统，请参见第 173 页中的“如何在有标签区域中对文件进行 NFS 挂载”。**

示例 14–1 以 PUBLIC 标签共享 /export/share 文件系统

对于以标签 PUBLIC 运行的应用程序，系统管理员允许用户读取 public 区域的 /export/reference 文件系统中的文档。

首先，管理员将工作区标签更改为 public 工作区，然后打开终端窗口。在该窗口中，管理员对 /reference 文件系统设置选定的 share 属性。以下命令由于显示的原因进行了换行。

```
# zfs set share=name=reference,path=/reference,prot=nfs,
setuid=off,exec=off,devices=off,rdonly=on rpool/wdocs1
```

然后，管理员共享该文件系统。

```
# zfs set sharenfs=on rpool/reference
```

管理员离开 public 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文件服务器，管理员通过将该区域置于就绪状态来共享文件系统：

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

一旦共享文件系统挂载到用户的系统上，用户便可以访问该共享文件系统。

▼ 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系统可以挂载到 Trusted Extensions 有标签系统上。系统必须具有通往挂载区域标签的文件服务器的路由。

- 要从单标签主机挂载具有读写权限的文件，远程主机的指定标签必须匹配挂载区域的标签。可能有两种远程主机配置。
  - 为不可信远程主机指定与挂载区域一样的标签。
  - 可信远程主机是包含挂载区域标签的多级别服务器。
- 由较高级别区域挂载的文件系统为只读状态。
- 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 相同的挂载界面：

- 缺省情况下，文件系统在引导时挂载。
- 要动态挂载文件系统，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。

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。检验您要挂载的文件系统是否已共享。除非使用自动挂载程序，否则您必须指定有 "File System Management"（文件系统管理）权限配置文件。要从较低级别服务器进行挂载，必须使用 net_mac_aware 特权对该客户机上的区域进行配置。

- **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 用户指南》中的“如何在最小标签下添加工作区”。

  - **动态挂载文件。**

    在有标签区域中，使用 mount 命令。

- 区域引导时挂载文件。
- 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。

▼ 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系统标签的区域中。您必须是 root 角色。

1. **检验 NFS 服务器上的文件系统是否已共享。**
2. **检查 NFS 服务器的安全属性。**

   a. **使用 tninfo 或 tncfg 命令找到服务器的 IP 地址，或包含 NFS 服务器的 IP 地址范围。**
   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。

3. **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。
4. **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 15 章

15 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。

- 第 175 页中的 “可信网络”
- 第 180 页中的 “Trusted Extensions 中的网络安全属性”
- 第 182 页中的 “可信网络回退机制”
- 第 184 页中的 “Trusted Extensions 中的路由概述”
- 第 186 页中的 “Trusted Extensions 中的路由管理”
- 第 188 页中的 “有标签 IPsec 的管理”

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。

可以对在可信系统之间交换的 IP 包设置标签。包上的标签用于对 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。

Trusted Extensions 支持对 IPv4 和 IPv6 包设置标签。

- 对于 IPv4 包，Trusted Extensions 支持商业 IP 安全选项 (Commercial IP Security Option, CIPSO) 标签。
- 对于 IPv6 包，Trusted Extensions 支持通用体系结构标签 IPv6 安全选项 (Common Architecture Label IPv6 Security Option, CALIPSO) 标签。

  如果您必须与 IPv6 CIPSO 网络上的系统进行交互操作，请参见第 50 页中的 “如何在 Trusted Extensions 中配置 IPv6 CIPSO 网络”。

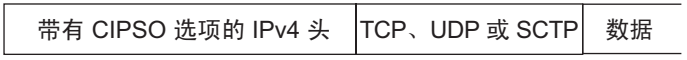
通常，在可信网络上，标签由发送主机生成，并由接收主机处理。然而，可信的路由器也可以在可信网络中转发包时添加或去除标签。在传输之前会将敏感标签映射到 CALIPSO 或 CIPSO 标签。此标签会嵌入到 IP 包中，然后成为**有标签**包。通常，包发送者和包的接收者在同一标签进行操作。

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 数据包包括标签选项。CIPSO 数据包通过 IPv4 网络发送。CALIPSO 包通过 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。



在标准的 IPv6 格式中，带有选项的 IPv6 头后跟 TCP、UDP 或 SCTP 头，然后才是实际的数据。Trusted Extensions 版本的 IPv6 包针对安全属性在 IP 头中使用 CALIPSO 选项。

Trusted Extensions 多播包

Trusted Extensions 可以为一个 LAN 中的多播包添加标签。通过此功能，您可以将有标签多播包发送给以同一标签或多播包标签范围内运行的 CIPSO 或 CALIPSO 系统。在异构 LAN（同时包含有标签和无标签主机）中，多播无法验证多播组的成员。

注意 – 请勿在异构 LAN 中发送有标签多播包。因为这样可能会泄漏有标签信息。

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。`txzonemgr` GUI 和 `tncfg` 命令用于配置网络。

运行 Trusted Extensions 软件的系统支持 Trusted Extensions 系统与以下任一类型主机之间的网络通信：

- 运行 Trusted Extensions 的其他主机
- 运行以下操作系统的主机：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（IPv4 包）和 CALIPSO 标签（IPv6 包）的可信操作系统的主机

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 添加命令并提供 GUI 来管理可信网络。Trusted Extensions 还向 Oracle Solaris 网络命令添加选项。有关这些命令的说明，请参见第 178 页中的 “Trusted Extensions 中的网络命令”。

  这些接口管理三个 Trusted Extensions 网络配置数据库 `tnzonecfg`、`tnrhdb` 和 `tnrhtp`。有关详细信息，请参见第 179 页中的 “Trusted Extensions 中的网络配置数据库 ”。
- Trusted Extensions 将 `tnrhtp` 和 `tnrhdb` 数据库添加到命名服务转换 SMF 服务 `svc:/system/name-service/switch` 的属性。
- 第 1 部分介绍了如何在配置网络时定义区域和主机。有关其他过程，请参见第 16 章，在 Trusted Extensions 中管理网络（任务）。
- Trusted Extensions 扩展 IKE 配置文件 `/etc/inet/ike/config`。有关更多信息，请参见第 188 页中的 “有标签 IPsec 的管理”和 `ike.config(4)` 手册页。

Trusted Extensions 中的网络命令

Trusted Extensions 添加了以下命令来管理可信网络：

- `tncfg`－该命令用于创建、修改和显示 Trusted Extensions 网络的配置。`tncfg -t` 命令用于查看、创建或修改指定的安全模板。`tncfg -z` 命令用于查看或修改指定区域的网络属性。有关详细信息，请参见 `tncfg(1M)` 手册页。
- `tnchkdb`—该命令用于验证可信网络数据库的正确性。每次通过使用 `txzonemgr` 或 `tncfg` 命令来更改安全模板 (`tnrhtp`)、安全模板指定 (`tnrhdb`) 或区域的配置 (`tnzonecfg`) 时都会调用 `tnchkdb` 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。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。搜索的顺序由 `name-service/switch` SMF 服务指定。`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`。

  在 LDAP 网络中，`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：

- `ipadm`－`all-zones` 地址属性使指定的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 `ipadm(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` 用途，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`－与在 Oracle Solaris 中一样，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。
- `ipseckey`－在 Trusted Extensions 中，以下扩展可用于为受 IPsec 保护的包设置标签：`label` *label*、`outer-label` *label* 和 `implicit-label` *label*。有关详细信息，请参见 `ipseckey(1M)` 手册页。

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。`tncfg` 命令是用于访问和修改此数据库的接口。

  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。有关更多信息，请参见 `label_encodings(4)` 手册页。有关多级别端口的讨论，请参见第 150 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。`tncfg` 命令是用于访问和修改此数据库的接口。

  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。然而，当**自适应**主机是发送方时，接收网络接口会将缺省标签指定给传入包。有关安全属性的详细信息，请参见第 180 页中的 “Trusted Extensions 中的网络安全属性”。

- `tnrhdb`－该数据库保存与允许和此系统进行通信的所有主机相对应的 IP 地址和 IP 地址的范围。`tncfg` 命令是用于访问和修改此数据库的接口。

  从 `tnrhtp` 数据库为每个主机或 IP 地址范围指定一个安全模板。模板中的属性定义负责指定主机的属性。

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相同协议和安全属性的主机。

安全属性以模板方式通过管理行为指定给远程系统（主机和路由器）。安全管理员负责管理模板并将其指定给远程系统。如果没有为远程系统指定模板，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：

- 以下四个主机类型之一：`unlabeled`、`cipso`、`adaptive` 或 `netif`。用于网络通信的协议由模板的主机类型确定。请参见第 180 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。

有关更多详细信息，请参见第 180 页中的 “Trusted Extensions 中的网络安全属性”。

Trusted Extensions 中的网络安全属性

随 Trusted Extensions 系统安装了一组缺省安全模板，这些模板用于定义远程主机的标签属性。在 Trusted Extensions 中，均通过安全模板方式为网络上的无标签主机和有标签主机指定安全属性。未指定有模板的主机无法与配置有 Trusted Extensions 的主机进行通信。这些模板在本地存储。

主机可以通过 IP 地址或作为 IP 地址范围的一部分添加到安全模板。有关详细说明，请参见第 182 页中的 “可信网络回退机制”。

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**－定义包是设置 CALIPSO 或 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 系统或网关在此标签进行读取。

  缺省标签属性特定于主机类型 `unlabeled`（无标签）。有关详细信息，请参见第 181 页中的 “安全模板中的缺省标签”。
- **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 `unlabeled`（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。
- **辅助标签集合**－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，添加到具有辅助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。可以指定的最大辅助标签数为四。

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四种主机类型并提供四个缺省模板：

- `cipso` **主机类型**－针对运行有标签可信操作系统的主机。该主机类型支持 CALIPSO 和 CIPSO 标签。

  对于 IPv6，CALIPSO 协议用于指定在 IP 选项字段中传递的安全标签。对于 IPv4，使用 CIPSO 协议。CALIPSO 和 CIPSO 头中的标签从数据的标签自动派生。然后，该派生标签用于在 IP 级别进行安全检查，并标记网络包。
- `unlabeled` **主机类型**－针对使用标准网络协议但不支持有标签选项的主机。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。该主机类型提供缺省标签，以应用于与无标签主机的通信。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。

- `adaptive` **主机类型** – 针对未设置标签但将包发送给有标签系统上特定网络接口的主机的子网。有标签系统将其网络接口缺省标签应用于传入包。

  该主机类型将指定给运行 Oracle Solaris OS 或其他无标签操作系统但期望将数据发送到有标签系统的主机。该主机类型不提供缺省标签。通信标签从接收系统的有标签网络接口派生。该主机类型指定给最终节点系统，而非网关。

  `adaptive` 主机类型可以灵活地规划和缩放可信网络。管理员在提前不知道新系统的缺省标签的情况下，可以使用无标签系统扩展网络。当 `adaptive` 主机配置为将包发送给 `netif` 主机上的有标签网络接口时，该 `netif` 主机上的此接口的缺省标签会将相应的标签指定给传入包。

- `netif` **主机类型** – 针对在 `adaptive` 主机的特定网络接口上接收包的接口的主机名。该主机类型指定给 Trusted Extensions 系统上的接口。`netif` 接口的缺省标签应用于到达包。

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，但是对于常规系统操作来说，安全属性的限制可能不够严厉。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

`unlabeled` 和 `netif` 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**。将这些主机称为“单标签”的技术原因是，这些主机没有 `admin_high` 和 `admin_low` 标签。

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。

如果您的站点使用不同于缺省值的 DOI 值，则必须在每个安全模板中使用该值，如第 50 页中的 “如何配置其他系统解释域”中所述。

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：

- 设置可在主机与远程有标签主机进行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的标签范围内。

- 为通过有标签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。

安全模板中的辅助标签

辅助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，不定义辅助标签集合。

可信网络回退机制

主机 IP 地址可以直接或间接添加到安全模板。直接指定将添加主机的 IP 地址。间接指定将添加包括主机的 IP 地址范围。要与特定主机匹配，可信联网软件首先将查找特定的 IP 地址。如果搜索未找到该主机的特定项，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。有关示例，请参见表 15–1。

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 15–1 Trusted Extensions 主机地址和回退机制项

IP 版本	host_type=cipso 的主机项	覆盖的 IP 地址
IPv4	192.168.118.57	192.168.118.57
	192.168.118.57/32	/32 用于设置 32 固定位的前缀长度。
	192.168.118.128/26	从 192.168.118.0 到 192.168.118.63
	192.168.118.0	192.168.118. 子网上的所有地址。
	192.168.118.0/24	
	192.168.0.0/24	192.168.0. 子网上的所有地址。
	192.168.0.0	192.168. 子网上的所有地址。
	192.168.0.0/16	
	192.0.0.0	192. 子网上的所有地址。
	192.0.0.0/8	
	192.168.118.0/32	主机地址 192.168.118.0。并非地址范围。
	192.168.0.0/32	主机地址 192.168.0.0。并非地址范围。
	192.0.0.0/32	主机地址 192.0.0.0。并非地址范围。
	0.0.0.0/32	主机地址 0.0.0.0。并非地址范围。
	0.0.0.0	所有网络上的所有地址
IPv6	2001\:DB8\:22\:5000\:\:21f7	2001:DB8:22:5000::21f7
	2001\:DB8\:22\:5000\:\:0/52	从 2001:DB8:22:5000::0 到 2001:DB8:22:5fff:ffff:ffff:ffff:ffff
	0\:\:0/0	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。通过将 0.0.0.0/32 项添加到系统的无标签安全模板，您可以使具有特定地址 0.0.0.0 的主机联系系统。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。

要在可为 DHCP 客户机提供服务的 Sun Ray 服务器上创建 tnrhdb 项，请参见示例 16–16。要对可为 DHCP 客户机提供服务的应用程序创建 tnrhdb 项，请参见示例 16–15。0.0.0.0:admin_low 网络是 admin_low 无标签主机模板中的缺省项。有关需要更改此缺省值的安全问题，请查看第 205 页中的 “如何限定可能会在可信网络上联系的主机”。

有关 IPv4 和 IPv6 地址中的前缀长度的更多信息，请参见《配置和管理 Oracle Solaris 11.1 网络》中的“确定网络的 IP 地址寻址格式”和《System Administration Guide: IP Services》中的“IPv6 Addressing Overview”。

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 不同，Trusted Extensions 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。

注 – 期望从 `adaptive` 主机转发包的有标签网关必须使用 `netif` 主机类型模板配置其传入接口。有关 `adaptive` 和 `netif` 主机类型的定义，请参见第 180 页中的 “安全模板中的主机类型和模板名称”。

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辅助标签集合的检查。

认可检查将验证标签范围和 CALIPSO 或 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。仅当从支持标签的主机发送消息时才可以从包获取标签。无法从包获得标签时，从安全模板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，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。
- 对于所有目标，传出包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。
- 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，包将从安全模板继承源主机的缺省标签。否则，包将接收在 CALIPSO 或 CIPSO 选项中指示的标签。
- 针对转发包的检查操作类似于源认可，如下所示：
  - 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。

- 对于所有目标，传出包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。
- 无标签包的标签必须与目标主机的缺省标签相匹配。
- 有标签包的标签必须位于目标主机的标签范围内。
- 期望从 adaptive 主机转发包的有标签网关必须使用 netif 主机类型模板配置其传入接口。有关 adaptive 和 netif 主机类型的定义，请参见第 180 页中的 “安全模板中的主机类型和模板名称”。

目标认可检查

Trusted Extensions 系统接收数据时，软件将执行以下检查：

- 如果传入包没有标签，包将从安全模板继承源主机的缺省标签。否则，包将接收在有标签选项中指示的标签。
- 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。您可以设置可强制实施站点安全策略所需的安全程度的路由。

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。要强制实施该限制，这些站点会将连接到外部网络的网关的网络接口添加到单标签模板。有关 TCP/IP 和路由的更多详细信息，请参见以下内容：

- 《配置和管理 Oracle Solaris 11.1 网络》中的“配置 IPv4 路由器”
- 《配置和管理 Oracle Solaris 11.1 网络》中的“在网络上配置组件系统”
- 《配置和管理 Oracle Solaris 11.1 网络》中的“主要的 TCP/IP 管理任务（任务列表）”
- netcfg(1M) 手册页

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。

- 有标签路由器在包的 IP 选项部分找不到正确类型的信息时会丢弃包。例如，如果有标签路由器在 IP 选项中没有找到所需的有标签选项，或 IP 选项中的 DOI 与目标的认可不一致，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包或丢弃包含有标签选项的包。只有可识别标签的网关（如 Trusted Extensions）可以使用 CALIPSO 或 CIPSO IP 选项的内容来强制执行 MAC。

为了支持可信路由，路由表进行了扩展，以包括 Trusted Extensions 安全属性。第 184 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。

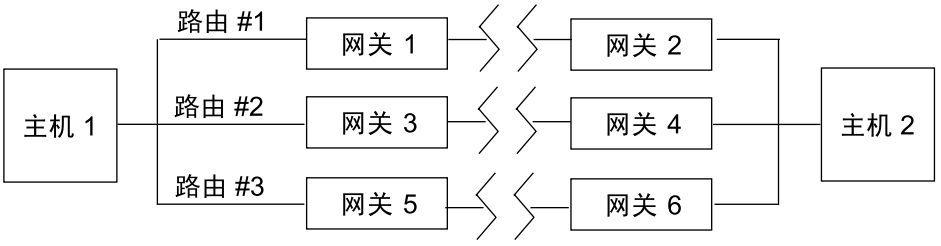
路由软件尝试在路由表中找到通往目标主机的路由。未显式命名主机时，路由软件将查找主机驻留的子网所对应的项。未定义主机和子网时，主机会将包发送至缺省网关（如果定义的话）。可定义多个缺省网关，每个都会被公平对待。

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 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 15–1 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 的安全模板。

Trusted Extensions 中的路由命令

为了针对套接字显示标签和扩展的安全属性，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。

要更改路由表项，Trusted Extensions 将提供以下接口：

- `txzonemgr` GUI 可用于为接口指定缺省路由。
- `route -p` 命令（带有 `add` 或 `delete` 选项）可用于更改路由表项。

有关示例，请参见第 209 页中的 “如何添加缺省路由”。

有标签 IPsec 的管理

Trusted Extensions 系统可以使用 IPsec 来保护有标签网络包。可以使用显式或隐式 Trusted Extensions 标签发送 IPsec 包。使用 CALIPSO 或 CIPSO IP 选项将显式发送标签。使用有标签 IPsec 安全关联 (security association, SA) 将隐式发送标签。此外，具有其他隐式标签的 IPsec 加密包可以通过无标签网络进行传送。

有关一般 IPsec 概念和配置过程的信息，请参见《在 Oracle Solaris 11.1 中保护网络安全》。有关 Trusted Extensions 对 IPsec 过程的修改，请参见第 212 页中的 “配置有标签 IPsec（任务列表）”。

受 IPsec 保护的交换的标签

Trusted Extensions 系统上的所有通信（包括受 IPsec 保护的通信）都必须满足安全标签认可检查。第 185 页中的 “Trusted Extensions 认可检查”中介绍了这些检查。

来自有标签区域中应用程序的 IPsec 包上的必须通过这些检查的标签为**内标签** *(inner label)*、**线标签** *(wire label)*和**密钥管理标签** *(key management label)*：

- **应用程序安全标签**－应用程序驻留区域的标签。
- **内标签 (Inner label)**－应用 IPsec AH 或 ESP 头之前未加密消息数据的标签。正在使用 `SO_MAC_EXEMPT` 套接字选项 (MAC-exempt) 或 multilevel port, MLP（多级别端口）功能时，此标签可能会不同于应用程序安全标签。选择受标签约束的安全关联 (security association, SA) 和 IKE 规则时，IPsec 和 IKE 将使用此内标签 (inner label)。

  缺省情况下，该内标签 (inner label) 与应用程序安全标签相同。通常，两端的应用程序具有相同的标签。但是，对于 MAC-exempt 或 MLP 通信，可能不会满足此条件。IPsec 配置设置可以定义通过网络传递内标签 (inner label) 的方式，即，它们可以定义**线标签** *(wire label)*。IPsec 配置设置无法定义内标签 (inner label) 的值。
- **线标签 (Wire label)**－应用 IPsec AH 或 ESP 头之后加密消息数据的标签。线标签 (wire label) 可能不同于内标签 (inner label)，具体取决于 IKE 和 IPsec 配置文件。
- **密钥管理标签**－无论触发协商的应用程序消息的标签为何，两个节点之间的所有 IKE 协商都在单个标签受到控制。IKE 协商的标签根据每 IKE 规则在 `/etc/inet/ike/config` 文件中进行定义。

IPsec 安全关联的标签扩展

在 Trusted Extensions 系统上使用 IPsec **标签扩展**，以将标签与在安全关联 (security association, SA) 内传输的通信相关联。缺省情况下，IPsec 不使用标签扩展，因此将忽略标签。无论 Trusted Extensions 标签为何，两个系统之间的所有通信都将流经单个 SA。

使用标签扩展，您可以执行以下操作：

- 配置可用于每个 Trusted Extensions 标签的不同 IPsec SA。此配置有效地提供其他机制，用于传递在两个多级别系统之间进行的通信的标签。
- 为不同于未加密形式文本的 IPsec 加密消息文本指定线标签 (on-the-wire label)。此配置支持通过安全性较低的网络传输加密的机密数据。
- 在 IP 包中不使用 CALIPSO 或 CIPSO IP 选项。通过此配置，有标签通信可以遍历标签无感知网络或标签不友好网络。

可以指定是自动通过 IKE（如第 190 页中的 “IKE 的标签扩展”中所述）还是手动通过 `ipseckey` 命令来使用标签扩展。有关标签扩展功能的详细信息，请参见 `ipseckey(1M)` 手册页。

使用标签扩展时，传出通信的 SA 选择将内部敏感标签包括为匹配项的一部分。传入通信的安全标签由已接收包的 SA 的安全标签定义。

IKE 的标签扩展

Trusted Extensions 系统上的 IKE 支持与可识别标签的对等方协商 SA 的标签。在 `/etc/inet/ike/config` 文件中使用以下关键字可控制此机制：

- **label_aware** – 允许 `in.iked` 守护进程使用 Trusted Extensions 标签接口并与对等方协商标签。
- **single_label** – 指明对等方不支持协商 SA 的标签。
- **multi_label** – 指明对等方支持协商 SA 的标签。IKE 为 IKE 在两个节点之间的通信中遇到的每个附加标签创建一个新的 SA。
- **wire_label inner** – 使 `in.iked` 守护进程创建有标签 SA，其中线标签 (wire label) 与内标签 (inner label) 相同。该守护进程正在与 `cipso` 对等方协商时，密钥管理标签为 `ADMIN_LOW`。该守护进程正在与无标签对等方协商时，密钥管理标签为该对等方的缺省标签。遵循常规 Trusted Extensions 规则以在传输包中包含有标签 IP 选项。
- **wire_label** *label* – 使 `in.iked` 守护进程创建有标签 SA，其中线标签 (wire label) 设置为 *label*，而不管内标签 (inner label) 的值为何。`in.iked` 守护进程在指定标签执行密钥管理协商。遵循常规 Trusted Extensions 规则以在传输包中包含有标签 IP 选项。
- **wire_label none** *label* – 导致产生类似于 `wire_label` *label* 的行为，但对 SA 下的传输 IKE 包和数据包隐藏有标签 IP 选项。

有关更多信息，请参见 `ike.config(4)` 手册页。

隧道模式 IPsec 下的标签和认可

应用程序数据包受到隧道模式下的 IPsec 保护时，这些数据包包含多个 IP 头。

外部 IP 头	ESP 或 AH	内部 IP 头	TCP 头	数据

IKE 协议的 IP 头包含与应用程序数据包的外部 IP 头相同的源和目标地址对。

外部 IP 头	UDP 头	IKE 密钥管理协议

Trusted Extensions 将内部 IP 头地址用于内标签 (inner label) 认可检查。Trusted Extensions 使用外部 IP 头地址来执行网线标签和密钥管理标签检查。有关认可检查的信息，请参见第 185 页中的 “Trusted Extensions 认可检查”。

有关标签扩展的保密性和完整性保护

下表说明了 IPsec 保密性和完整性保护如何应用于具有各种标签扩展配置的安全标签。

安全关联	保密性	完整性
无标签扩展	标签在有标签 IP 选项中可见。	有标签 IP 选项中的消息标签受 AH（而不受 ESP）保护。请参见注释。
具有标签扩展	有标签 IP 选项可见，但表示线标签 (wire label)，该标签可能不同于内消息标签 (inner message label)。	特定于标签的 SA 的存在隐式确保了标签完整性。 线上有标签 IP 选项受 AH 保护。请参见注释。
隐藏了标签扩展和有标签 IP 选项	消息标签不可见。	特定于标签的 SA 的存在隐式确保了标签完整性。

注 – 如果可识别标签的路由器在消息通过网络传输时去除或添加有标签 IP 选项，则您无法使用 IPsec AH 完整性保护来保护有标签 IP 选项。对有标签 IP 选项所做的任何修改将使消息无效，并导致受 AH 保护的包在目标处丢弃。

◆ ◆ ◆ 第 16 章

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。

- 第 193 页中的 “为主机和网络设置标签（任务）”
- 第 209 页中的 “配置路由和多级别端口（任务）”
- 第 212 页中的 “配置有标签 IPsec（任务列表）”
- 第 216 页中的 “可信网络故障排除（任务列表）”

为主机和网络设置标签（任务）

仅当 Trusted Extensions 系统已定义其他主机的安全属性后，才可以与这些主机联系。因为远程主机可以包含相似的安全属性，所以 Trusted Extensions 提供了安全模板，您可以将主机添加到这些模板中。

查看现有安全模板（任务）

在为远程主机和网络设置标签之前，请先阅读提供的安全模板，并确保可以访问远程主机和网络。有关说明，请参见以下内容：

- 查看安全模板－第 193 页中的 “如何查看安全模板”
- 确定您的站点是否需要定制的安全模板－第 195 页中的 “如何确定是否需要站点专用安全模板”
- 将系统和网络添加到可信网络中－第 195 页中的 “如何向系统的已知网络添加主机”

▼ 如何查看安全模板

您可以查看安全模板列表以及每个模板的内容。此过程中显示的示例为缺省安全模板。

1 列出可用的安全模板。

```
# tncfg list
   cipso
   admin_low
   adapt
   netif
```

2 查看已列出的模板的内容。

```
# tncfg -t cipso info
   name=cipso
   host_type=cipso
   doi=1
   min_label=ADMIN_LOW
   max_label=ADMIN_HIGH
   host=127.0.0.1/32
```

前面的 cipso 安全模板中的 127.0.0.1/32 项将此系统标识为有标签。当对等方将此系统指定给对等方的远程主机模板（host_type 为 cipso）时，这两个系统可以交换有标签包。

```
# tncfg -t admin_low info
   name=admin_low
   host_type=unlabeled
   doi=1
   def_label=ADMIN_LOW
   min_label=ADMIN_LOW
   max_label=ADMIN_HIGH
   host=0.0.0.0/0
```

前面的 admin_low 安全模板中的 0.0.0.0/0 项允许未显式指定给安全模板的所有主机与此系统联系。这些主机均被标识为无标签。

- 0.0.0.0/0 项的优点在于可以找到在引导时此系统需要的所有主机（例如服务器和网关）。
- 0.0.0.0/0 项的缺点在于此系统网络中的所有主机都可以与此系统联系。要限制哪些主机可与此系统联系，请参见第 205 页中的 “如何限定可能会在可信网络上联系的主机”。

```
# tncfg -t adapt info
   name=adapt
   host_type=adapt
   doi=1
   min_label=ADMIN_LOW
   max_label=ADMIN_HIGH
   host=0.0.0.0/0
```

adapt 模板标识自适应主机，即标识无法具有缺省标签的不可信系统。相反，该主机的标签由其接收可信系统指定。此标签从接收包的 IP 接口的缺省标签派生，该接口由有标签系统的 netif 模板指定。

```
# tncfg -t netif info
   name=netif
   host_type=netif
```

```
doi=1
def_label=ADMIN_LOW
min_label=ADMIN_LOW
max_label=ADMIN_HIGH
host=127.0.0.1/32
```

netif 模板指定可信本地网络接口，**而非**远程主机。netif 模板的缺省标签必须等于具有专用网络接口（其 IP 地址与该模板中的主机地址匹配）的每个区域的标签。此外，与匹配区域接口对应的较低链路只能指定给共享同一标签的其他区域。

▼ 如何确定是否需要站点专用安全模板

- **如果要对您与其进行通信的主机执行以下任一操作，请创建特定于站点的安全模板：**
  - 限定某台主机或一组主机的标签范围。
  - 在非 ADMIN_LOW 的标签下创建单标签主机。
  - 需要无标签主机的非 ADMIN_LOW 缺省标签。
  - 创建可识别一组有限标签的主机。
  - 使用非 1 的 DOI。
  - 将信息从指定的无标签主机发送到信任其可将正确标签指定给这些无标签主机中的包的网络接口。

▼ 如何向系统的已知网络添加主机

将主机和主机组添加到系统的 /etc/hosts 文件之后，系统将能够识别这些主机。只能将已知的主机添加到安全模板中。

开始之前 您是全局区域中的 root 角色。

1. **将各个主机添加到 /etc/hosts 文件中。**

```
# pfedit /etc/hosts

...
192.168.111.121   ahost
```

2. **将一组主机添加到 /etc/hosts 文件中。**

```
# pfedit /etc/hosts

...
192.168.111.0   111-network
```

创建安全模板（任务）

本节包含有关针对以下网络配置创建安全模板的指针或示例：

- DOI 是不同于 1 的值－第 50 页中的 “如何配置其他系统解释域”
- 为可信远程主机指定了特定标签－示例 16–1
- 为不可信远程主机指定了特定标签－示例 16–2

有关满足特定要求的安全模板的更多示例，请参见第 198 页中的 “将主机添加到安全模板（任务）”。

▼ 如何创建安全模板

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，指定有 "Information Security"（信息安全）或 "Network Security"（网络安全）权限配置文件的角色可以修改安全值。"Security Administrator"（安全管理员）角色拥有这些权限配置文件。

1 可选确定非 ADMIN_HIGH 和 ADMIN_LOW 的任何标签的十六进制版本。

对于 PUBLIC 等标签，可以使用标签字符串或十六进制值 (0x0002-08-08) 作为标签值。tncfg 命令接受这两种格式中的任一格式。

```
# atohexlabel "confidential : internal use only"
0x0004-08-48
```

有关更多信息，请参见第 117 页中的 “如何获取标签的十六进制等效值”。

2 不要更改缺省安全模板。

出于支持目的，请勿删除缺省安全模板。

- 您可以复制这些模板，然后对其进行修改。
- 此外，您还可以添加和删除指定给这些模板的主机。有关示例，请参见第 205 页中的 “如何限定可能会在可信网络上联系的主机”。

3 创建安全模板。

tncfg -t 命令提供了三种创建新模板的方法。

- **从头创建安全模板。**

  在交互式模式下使用 tncfg 命令。info 子命令显示在缺省情况下提供的值。使用 Tab 键完成部分属性和值。键入 exit 以完成模板。

```
# tncfg -t newunlabeled
tncfg:newunlabeled> info
   name=newunlabeled
   host_type=unlabeled
   doi=1
   def_label=ADMIN_LOW
   min_label=ADMIN_LOW
   max_label=ADMIN_HIGH
```

```
tncfg:newunlabeled> set m<Tab>
set max_label=" set min_label="
tncfg:newunlabeled> set ma<Tab>
tncfg:newunlabeled> set max_label=ADMIN_LOW
...
tncfg:newunlabeled> commit
tncfg:newunlabeled> exit
```

您也可以在命令行中提供完整的安全模板属性列表。使用分号分隔 `set` 子命令。被忽略的属性接收缺省值。

```
# tncfg -t newunlabeled set host_type=unlabeled;set doi=1; \
set min_label=ADMIN_LOW;set max_label=ADMIN_LOW
```

- **复制现有安全模板，然后对其进行修改。**

```
# tncfg -t cipso
tncfg:cipso> set name=newcipso
tncfg:newcipso> info
name=newcipso
host_type=cipso
doi=1
min_label=ADMIN_LOW
max_label=ADMIN_HIGH
```

已指定给现有安全模板的主机不会复制到新模板中。

- **使用 `export` 子命令创建的模板文件。**

```
# tncfg -f unlab_1 -f template-file
tncfg: unlab_1> set host_type=unlabeled
...
# tncfg -f template-file
```

有关创建源模板以用于导入的示例，请参见 `tncfg(1M)` 手册页。

示例 16–1 为在一个标签下处理包的网关创建安全模板

在此示例中，安全管理员定义一个只能在标签 `PUBLIC` 下传递包的网关。

```
# tncfg -t cipso_public
tncfg:cipso_public> set host_type=cipso
tncfg:cipso_public> set doi=1
tncfg:cipso_public> set min_label="public"
tncfg:cipso_public> set max_label="public"
tncfg:cipso_public> commit
tncfg:cipso_public> exit
```

然后，安全管理员将网关主机添加到安全模板中。有关更多信息，请参见示例 16–3。

示例 16–2 在标签 PUBLIC 下创建无标签安全模板

在此示例中，安全管理员为只能使用 `PUBLIC` 标签收发包的不可信主机创建无标签模板。该模板可能会指定给其文件系统必须由 Trusted Extensions 系统挂载在 `PUBLIC` 标签的主机。

```
# tncfg -t public
tncfg:public> set host_type=unlabeled
tncfg:public> set doi=1
tncfg:public> set def_label="public"
tncfg:public> set min_sl="public"
tncfg:public> set max_sl="public"
tncfg:public> exit
```

然后，安全管理员将主机添加到安全模板中。有关更多信息，请参见示例 16–12。

将主机添加到安全模板（任务）

本节包含有关向安全模板中添加主机的链接和示例。对于间断的 IP 地址，请参见第 198 页中的“如何将主机添加到安全模板”。对于一系列主机，请参见第 203 页中的“如何将一系列主机添加到安全模板”。

本节中的示例说明了以下远程主机标签指定：

- 可信远程网关处理 PUBLIC 通信－示例 16–3
- 不可信远程主机充当单标签路由器－示例 16–4
- 可信远程主机将通信限制为很窄的标签范围－示例 16–5
- 为可信远程主机指定了一组有限标签－示例 16–6
- 为可信远程主机指定了与网络的其余部分没有交集的标签－示例 16–7
- 可信 `netif` 主机对来自 `adapt` 系统的包设置标签－示例 16–8
- 不可信 `adapt` 主机将包发送给 `netif` 主机－示例 16–9
- 可信同构网络在特定标签添加多播地址－示例 16–10
- 从安全模板中删除主机－示例 16–11
- 为不可信远程主机和网络指定了标签－示例 16–12

▼ 如何将主机添加到安全模板

开始之前 必须满足以下几项：

- IP 地址必须存在于 `/etc/hosts` 文件中，或可由 DNS 进行解析。

  有关 `hosts` 文件，请参见第 195 页中的“如何向系统的已知网络添加主机”。

  有关 DNS 的信息，请参见《在 Oracle Solaris 11.1 中使用命名和目录服务》中的第 3 章“管理 DNS（任务）”。
- 标签端点必须匹配。有关规则，请参见第 184 页中的“Trusted Extensions 中的路由概述”。
- 您必须具有全局区域中的 "Security Administrator"（安全管理员）角色。

1 可选验证您是否可以访问要添加的主机名或 IP 地址。

在此示例中，验证是否可以访问 `192.168.1.2`。

```
# arp 192.168.1.2
gateway-2.example.com (192.168.1.2) at 0:0:0:1:ad:cd
```

arp 命令检验主机是否已在系统的 /etc/hosts 文件中定义或者是否可由 DNS 进行解析。

2 **将主机名或 IP 地址添加到安全模板中。**

例如，添加 192.168.1.2 IP 地址。

```
# tncfg -t cipso
tncfg:cipso> add host=192.168.1.2
```

如果要添加之前已添加到其他模板中的主机，系统会通知您将替换该主机的安全模板指定。例如：

```
# tncfg -t cipso
tncfg:cipso> add host=192.168.1.2
192.168.1.2 previously matched the admin_low template
tncfg:cipso> info
...
host=192.168.1.2/32
tncfg:cipso> exit
```

3 **查看已更改的安全模板。**

例如，下面显示了已添加到 cipso 模板的 192.168.1.2 地址：

```
tncfg:cipso> info
...
   host=192.168.1.2/32
```

前缀长度 /32 指示该地址是确切的。

4 **提交更改并退出安全模板。**

```
tncfg:cipso> commit
tncfg:cipso> exit
```

要删除主机项，请参见示例 16–11。

示例 16–3 创建在一个标签下处理包的网关

在示例 16–1 中，管理员创建了一个安全模板，该模板定义了一个只能在标签 PUBLIC 下传递包的网关。在此示例中，安全管理员确保可以解析此网关主机的 IP 地址。

```
# arp 192.168.131.75
gateway-1.example.com (192.168.131.75) at 0:0:0:1:ab:cd
```

arp 命令检验主机是否已在系统的 /etc/hosts 文件中定义或者是否可由 DNS 进行解析。

然后，管理员将 gateway-1 主机添加到安全模板中：

```
# tncfg -t cipso_public
tncfg:cipso_public> add host=192.168.131.75
tncfg:cipso_public> exit
```

系统可以通过 gateway-1 立即收发 public 包。

示例 16–4 创建无标签路由器来路由有标签包

任何 IP 路由器都可以通过 CALIPSO 或 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必须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，但通过该路由器进行的所有直接通信都是以缺省标签 PUBLIC 处理的。

安全管理员从头创建模板。

```
# tncfg -t unl_public_router
tncfg:unl_public_router> set host_type=unlabeled
tncfg:unl_public_router> set doi=1
tncfg:unl_public_router> set def_label="PUBLIC"
tncfg:unl_public_router> set min_label=ADMIN_LOW
tncfg:unl_public_router> set max_label=ADMIN_HIGH
tncfg:unl_public_router> exit
```

然后，管理员将路由器添加到安全模板中。

```
# tncfg -t unl_public_router
tncfg:unl_public_router> add host=192.168.131.82
tncfg:unl_public_router> exit
```

系统可以通过 router-1 立即收发所有标签下的包。

示例 16–5 创建具有有限标签范围的网关

在此示例中，安全管理员创建一个将包限定于较窄标签范围的网关，并添加此网关。

```
# arp 192.168.131.78
gateway-ir.example.com (192.168.131.78) at 0:0:0:3:ab:cd

# tncfg -t cipso_iuo_rstrct
tncfg:cipso_iuo_rstrct> set host_type=cipso
tncfg:cipso_iuo_rstrct> set doi=1
tncfg:cipso_iuo_rstrct> set min_label=0x0004-08-48
tncfg:cipso_iuo_rstrct> set max_label=0x0004-08-78
tncfg:cipso_iuo_rstrct> add host=192.168.131.78
tncfg:cipso_iuo_rstrct> exit
```

系统可以通过 gateway-ir 立即收发标签为 internal 和 restricted 的包。

示例 16–6 在独立标签下创建主机

在此示例中，安全管理员创建一个仅识别两个标签（confidential : internal use only 和 confidential : restricted）的安全模板。所有其他通信都会被拒绝。

首先，安全管理员确保可以解析每台主机的 IP 地址。

```
# arp 192.168.132.21
host-auxset1.example.com (192.168.132.21) at 0:0:0:4:ab:cd
# arp 192.168.132.22
host-auxset2.example.com (192.168.132.22) at 0:0:0:5:ab:cd
# arp 192.168.132.23
host-auxset3.example.com (192.168.132.23) at 0:0:0:6:ab:cd
# arp 192.168.132.24
host-auxset4.example.com (192.168.132.24) at 0:0:0:7:ab:cd
```

然后，管理员需要仔细准确地键入标签。软件按大小写字母和短名称识别标签，但不识别空格间距不准确的标签。例如，标签 `cnf :restricted` 不是有效标签。

```
# tncfg -t cipso_int_and_rst
tncfg:cipso_int_and_rst> set host_type=cipso
tncfg:cipso_int_and_rst> set doi=1
tncfg:cipso_int_and_rst> set min_label="cnf : internal use only"
tncfg:cipso_int_and_rst> set max_label="cnf : internal use only"
tncfg:cipso_int_and_rst> set aux_label="cnf : restricted"
tncfg:cipso_int_and_rst> exit
```

然后，管理员通过使用前缀长度将 IP 地址的范围指定给安全模板。

```
# tncfg -t cipso_int_rstrct
tncfg:cipso_int_rstrct> set host=192.168.132.0/24
```

示例 16–7 为开发者创建有标签主机

在此示例中，安全管理员创建一个 `cipso_sandbox` 模板。此安全模板会指定给可信软件开发者所使用的系统。开发者测试不会影响其他有标签主机，因为标签 `SANDBOX` 与网络上的其他标签不相交。

```
# tncfg -t cipso_sandbox
tncfg:cipso_sandbox> set host_type=cipso
tncfg:cipso_sandbox> set doi=1
tncfg:cipso_sandbox> set min_sl="SBX"
tncfg:cipso_sandbox> set max_sl="SBX"
tncfg:cipso_sandbox> add host=196.168.129.102
tncfg:cipso_sandbox> add host=196.168.129.129
tncfg:cipso_sandbox> exit
```

使用 `196.168.129.102` 和 `196.168.129.129` 系统的开发者可以在标签 `SANDBOX` 下彼此进行通信。

示例 16–8 为 netif 主机创建安全模板

在此示例中，安全管理员创建一个 `netif` 安全模板。此模板将指定给托管 IP 地址 `10.121.10.3` 的有标签网络接口。通过此指定，Trusted Extensions IP 模块会将缺省标签 `PUBLIC` 添加到来自 `adaptive` 主机的所有传入包。

```
# tncfg -t netif_public
tncfg:netif_public> set host_type=netif
tncfg:netif_public> set doi=1
```

```
tncfg:netif_public> set def_label="PUBLIC"
tncfg:netif_public> add host=10.121.10.3
tncfg:netif_public> commit
tncfg:netif_public> exit
```

示例 16–9 为自适应主机创建安全模板

在此示例中，安全管理员提前进行计划。管理员为分别保留公共信息的网络和保留内部信息的网络创建不同的子网。管理员随后定义两个 adapt 主机。为公共子网中的系统指定了 PUBLIC 标签。为内部网络中的系统指定了 IUO 标签。由于对此网络提前进行了计划，因此每个网络使用特定标签保留并传输信息。另一个优点是，当未在预期接口上传送包时，可以轻松调试网络。

```
# tncfg -t adpub_192_168_10
tncfg:adapt_public> set host_type=adapt
tncfg:adapt_public> set doi=1
tncfg:adapt_public> set min_label="public"
tncfg:adapt_public> set max_label="public"
tncfg:adapt_public> add host=192.168.10.0
tncfg:adapt_public> commit
tncfg:adapt_public> exit

# tncfg -t adiuo_192_168_20
tncfg:adapt_public> set host_type=adapt
tncfg:adapt_public> set doi=1
tncfg:adapt_public> set min_label="iuo"
tncfg:adapt_public> set max_label="iuo"
tncfg:adapt_public> add host=192.168.20.0
tncfg:adapt_public> commit
tncfg:adapt_public> exit
```

示例 16–10 发送有标签多播消息

在有标签的同构 LAN 中，管理员选择可通过其使用标签 PUBLIC 发送包的可用多播地址。

```
# tncfg -t cipso_public
tncfg:cipso_public> add host=224.4.4.4
tncfg:cipso_public> exit
```

示例 16–11 从安全模板中删除若干主机

在此示例中，安全管理员从 cipso 安全模板中删除若干主机。管理员使用 info 子命令显示主机，然后键入 remove，再复制并粘贴四个 host= 项。

```
# tncfg -t cipso info
   name=cipso
   host_type=cipso
   doi=1
   min_label=ADMIN_LOW
   max_label=ADMIN_HIGH
```

```
   host=127.0.0.1/32
   host=192.168.1.2/32
   host=192.168.113.0/24
   host=192.168.113.100/25
   host=2001:a08:3903:200::0/56

# tncfg -t cipso
tncfg:cipso> remove host=192.168.1.2/32
tncfg:cipso> remove host=192.168.113.0/24
tncfg:cipso> remove host=192.168.113.100/25
tncfg:cipso> remove host=2001:a08:3903:200::0/56
tncfg:cipso> info
...
   max_label=ADMIN_HIGH
   host=127.0.0.1/32
   host=192.168.75.0/24
```

删除主机后，管理员提交更改并退出安全模板。

```
tncfg:cipso> commit
tncfg:cipso> exit
#
```

▼ 如何将一系列主机添加到安全模板

开始之前 有关要求，请参见第 198 页中的 “如何将主机添加到安全模板”。

1. **要将安全模板指定给子网，请将此子网地址添加到模板中。**

   例如，将两个 IPv4 子网添加到 `cipso` 模板中，然后显示安全模板。

   ```
   # tncfg -t cipso
   tncfg:cipso> add host=192.168.75.0
   tncfg:cipso> add host=192.168.113.0
   tncfg:cipso> info
   ...
   host=192.168.75.0/24
   host=192.168.113.0/24
   tncfg:cipso> exit
   ```

   前缀长度 `/24` 指示地址（以 `.0` 结尾）是子网。

   注 – 如果要添加之前已添加到其他模板中的一系列主机，系统会通知您将替换这些主机的安全模板指定。

   ```
   # tncfg -t cipso
   tncfg:cipso> add host=192.168.113.100/25
   192.168.113.100/25 previously matched the admin_low template
   ```

2 **要将安全模板指定给一系列 IP 地址，请指定 IP 地址和前缀长度。**

在以下示例中，/25 前缀长度涵盖的连续 IPv4 地址为 192.168.113.0 到 192.168.113.127。该地址包括 192.168.113.100。

```
# tncfg -t cipso
tncfg:cipso> add host=192.168.113.100/25
tncfg:cipso> exit
```

在以下示例中，/56 前缀长度涵盖的连续 IPv6 地址为 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。

```
# tncfg -t cipso
tncfg:cipso> add host=2001:a08:3903:200::0/56
tncfg:cipso> info
...
host=2001:a08:3903:200::0/56
tncfg:cipso> exit
```

- 如果项键入错误（如在地址中忽略了 :200），将接收到类似于以下内容的消息：

  ```
  # tncfg -t cipso
  tncfg:cipso> add host=2001:a08:3903::0/56
  Invalid host: 2001:a08:3903::0/56
  ```

- 如果要添加之前已添加到其他模板中的主机，系统会通知您将替换该主机的安全模板指定。例如：

  ```
  # tncfg -t cipso
  tncfg:cipso> add host=192.168.113.100/32
  192.168.113.100/32 previously matched the admin_low template
  tncfg:cipso> info
  ...
  host=192.168.113.100/32
  tncfg:cipso> exit
  ```

  Trusted Extensions 回退机制可以确保此显式指定会覆盖以前的指定，如第 182 页中的 “可信网络回退机制”中所述。

示例 16–12 在标签 PUBLIC 下创建无标签子网

在示例 16–2 中，管理员创建了可为不可信主机指定标签 PUBLIC 的安全模板。在此示例中，安全管理员将一个子网指定给 PUBLIC 标签。指定系统上的用户可以将来自此子网的主机中的文件系统挂载到 PUBLIC 区域。

```
# tncfg -t public
tncfg:public> add host=10.10.0.0/16
tncfg:public> exit
```

可以在标签 PUBLIC 立即访问此子网。

限制可以访问可信网络的主机（任务）

在本节中，通过限制可以访问网络的主机来保护网络。

- 第 205 页中的 “如何限定可能会在可信网络上联系的主机”
- 通过指定要在引导时联系的系统来提高安全性－示例 16–13
- 配置应用服务器以接受来自远程客户机的初始联系信息－示例 16–15。
- 配置有标签 Sun Ray 服务器以接受来自远程客户机的初始联系信息－示例 16–16。

▼ 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 后，`admin_low` 缺省安装模板会定义网络中的每台主机。使用此过程可枚举特定的无标签主机。

每个系统上的本地可信网络值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台远程主机 (`0.0.0.0/0`) 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 `0.0.0.0/0` 通配符项。该项必须替换为引导时系统联系的每台主机对应的项。

例如，在删除 `0.0.0.0/0` 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显式添加到模板中。

如果应用程序最初在主机地址 `0.0.0.0/32` 识别客户机，则必须将 `0.0.0.0/32` 主机项添加到 `admin_low` 模板中。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，这些客户机会作为有标签客户机进行连接。

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都必须存在于 `/etc/hosts` 文件中。

1. **将 `admin_low` 模板指定给在引导时必须联系的每台无标签主机。**
   - 包括在引导时必须联系的每台无标签主机。
   - 包括此系统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。
   - 删除 `0.0.0.0/0` 指定。
2. **将主机添加到 `cipso` 模板中。**

添加在引导时必须联系的每台有标签主机。

- 包括此系统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。
- 包括在引导时必须联系的有标签主机的范围。

有关数据库样例，请参见示例 16–14。

3 检验主机指定是否允许系统进行引导。

示例 16–13 更改 0.0.0.0/0 IP 地址的标签

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 0.0.0.0/0 主机项，并将 0.0.0.0/0 主机项添加到无标签 public 模板中。然后，系统将未特别指定给其他安全模板的任何主机识别为具有 public 安全模板的安全属性的无标签系统。

```
# tncfg -t admin_low info
tncfg:admin_low> remove host=0.0.0.0      Wildcard address
tncfg:admin_low> exit

# tncfg -t public
tncfg:public> set host_type=unlabeled
tncfg:public> set doi=1
tncfg:public> set def_label="public"
tncfg:public> set min_sl="public"
tncfg:public> set max_sl="public"
tncfg:public> add host=0.0.0.0      Wildcard address
tncfg:public> exit
```

示例 16–14 枚举在引导时 Trusted Extensions 系统要联系的系统

在以下示例中，管理员配置具有两个网络接口的 Trusted Extensions 系统的可信网络。此系统与另一个网络以及一些路由器进行通信。将远程主机指定给以下三个模板之一：cipso、admin_low 或 public。对以下命令进行了注释。

```
# tncfg -t cipso
tncfg:admin_low> add host=127.0.0.1      Loopback address
tncfg:admin_low> add host=192.168.112.111      Interface 1 of this host
tncfg:admin_low> add host=192.168.113.111      Interface 2 of this host
tncfg:admin_low> add host=192.168.113.6      File server
tncfg:admin_low> add host=192.168.112.255      Subnet broadcast address
tncfg:admin_low> add host=192.168.113.255      Subnet broadcast address
tncfg:admin_low> add host=192.168.113.1      Router
tncfg:admin_low> add host=192.168.117.0/24      Another Trusted Extensions network
tncfg:admin_low> exit
```

```
# tncfg -t public
tncfg:public> add host=192.168.112.12      Specific network router
tncfg:public> add host=192.168.113.12      Specific network router
tncfg:public> add host=224.0.0.2      Multicast address
tncfg:admin_low> exit

# tncfg -t admin_low
tncfg:admin_low> add host=255.255.255.255      Broadcast address
tncfg:admin_low> exit
```

指定要在引导时联系的主机后，管理员从 admin_low 模板中删除 0.0.0.0/0 项。

```
# tncfg -t admin_low
tncfg:admin_low> remove host=0.0.0.0
tncfg:admin_low> exit
```

示例 16–15 使主机地址 0.0.0.0/32 成为有效的初始地址

在此示例中，安全管理员将应用服务器配置为接受来自潜在客户机的初始连接请求。

管理员配置服务器的可信网络。对服务器和客户机项进行了注释。

```
# tncfg -t cipso info
   name=cipso
   host_type=cipso
   doi=1
   min_label=ADMIN_LOW
   max_label=ADMIN_HIGH
   host=127.0.0.1/32
   host=192.168.128.1/32       Application server address
   host=192.168.128.0/24       Application's client network
     Other addresses to be contacted at boot time

# tncfg -t admin_low info
   name=cipso
   host_type=cipso
   doi=1
   def_label=ADMIN_LOW
   min_label=ADMIN_LOW
   max_label=ADMIN_HIGH
   host=192.168.128.0/24       Application's client network
   host=0.0.0.0/0       Wildcard address
     Other addresses to be contacted at boot time
```

此阶段测试成功后，管理员通过以下方法锁定配置：删除缺省通配符地址 0.0.0.0/0，提交更改，然后添加特定地址。

```
# tncfg -t admin_low info
tncfg:admin_low> remove host=0.0.0.0
tncfg:admin_low> commit
tncfg:admin_low> add host=0.0.0.0/32      For initial client contact
tncfg:admin_low> exit
```

最终 admin_low 配置类似于以下内容：

```
# tncfg -t admin_low
   name=cipso
   host_type=cipso
   doi=1
   def_label=ADMIN_LOW
   min_label=ADMIN_LOW
   max_label=ADMIN_HIGH
   192.168.128.0/24       Application's client network
   host=0.0.0.0/32        For initial client contact
     Other addresses to be contacted at boot time
```

0.0.0.0/32 项仅允许应用程序的客户机访问应用服务器。

示例 16–16 为有标签 Sun Ray 服务器配置有效的初始地址

在此示例中，安全管理员将 Sun Ray 服务器配置为接受来自潜在客户机的初始连接请求。服务器使用专用拓扑和 Sun Ray 服务器缺省设置。

```
# utadm -a net0
```

然后，管理员配置服务器的可信网络。对服务器和客户机项进行了注释。

```
# tncfg -t cipso info
   name=cipso
   host_type=cipso
   doi=1
   min_label=ADMIN_LOW
   max_label=ADMIN_HIGH
   host=127.0.0.1/32
   host=192.168.128.1/32       Sun Ray server address
   host=192.168.128.0/24       Sun Ray client network
     Other addresses to be contacted at boot time

# tncfg -t admin_low info
   name=cipso
   host_type=cipso
   doi=1
   def_label=ADMIN_LOW
   min_label=ADMIN_LOW
   max_label=ADMIN_HIGH
   host=192.168.128.0/24       Sun Ray client network
   host=0.0.0.0/0       Wildcard address
     Other addresses to be contacted at boot time
```

此阶段测试成功后，管理员通过以下方法锁定配置：删除缺省通配符地址 0.0.0.0/0，提交更改，然后添加特定地址。

```
# tncfg -t admin_low info
tncfg:admin_low> remove host=0.0.0.0
tncfg:admin_low> commit
```

```
tncfg:admin_low> add host=0.0.0.0/32      For initial client contact
tncfg:admin_low> exit
```

最终 admin_low 配置类似于以下内容：

```
# tncfg -t admin_low
   name=cipso
   host_type=cipso
   doi=1
   def_label=ADMIN_LOW
   min_label=ADMIN_LOW
   max_label=ADMIN_HIGH
   192.168.128.0/24       Sun Ray client network
   host=0.0.0.0/32        For initial client contact
     Other addresses to be contacted at boot time
```

0.0.0.0/32 项仅允许 Sun Ray 客户机访问服务器。

配置路由和多级别端口（任务）

通过静态路由，有标签包可以通过有标签网关和无标签网关到达其目的地。通过 MLP，应用程序可以使用一个入口点访问所有区域。

▼ 如何添加缺省路由

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

已将每个目标主机、网络和网关添加到安全模板。有关详细信息，请参见第 198 页中的 “如何将主机添加到安全模板”和第 203 页中的 “如何将一系列主机添加到安全模板”。

1. **使用 txzonemgr GUI 创建缺省路由。**

   ```
   # txzonemgr &
   ```

2. **双击要设置其缺省路由的区域，然后双击其 IP 地址项。**

   如果此区域有多个 IP 地址，请选择具有所需接口的项。

3. **在出现提示时，键入路由器的 IP 地址，然后单击 "OK"（确定）。**

注 – 要删除或修改缺省路由器，请删除该项，然后重新创建 IP 项并添加路由器。如果此区域只有一个 IP 地址，必须删除 IP 实例才能删除该项。

示例 16–17 使用 route 命令为全局区域设置缺省路由

在此示例中，管理员使用 route 命令为全局区域创建缺省路由。

```
# route add default 192.168.113.1 -static
```

▼ 如何为区域创建多级别端口

可以将专用和共享 MLP 添加到有标签区域和全局区域。

如果在有标签区域中运行的某应用程序需要使用多级别端口 (multilevel port, MLP) 与区域进行通信，将使用此过程。在此过程中，一个 Web 代理与区域进行通信。

开始之前 您必须在全局区域中承担 `root` 角色。系统必须至少具有两个 IP 地址，并且有标签区域已停止。

1. **将代理主机和 Web 服务主机添加到 `/etc/hosts` 文件。**

```
## /etc/hosts file
...
proxy-host-name  IP-address
web-service-host-name IP-address
```

2. **配置区域。**

例如，将 `public` 区域配置为识别标签显式设置为 `PUBLIC` 的包。对于此配置，安全模板命名为 `webprox`。

```
# tncfg -t webprox
tncfg:public> set name=webprox
tncfg:public> set host_type=cipso
tncfg:public> set min_label=public
tncfg:public> set max_label=public
tncfg:public> add host=mywebproxy.oracle.com      host name associated with public zone
tncfg:public> add host=10.1.2.3/16      IP address of public zone
tncfg:public> exit
```

3. **配置 MLP。**

例如，Web 代理服务可能会通过 `8080/tcp` 接口与 `PUBLIC` 区域进行通信。

```
# tncfg -z public add mlp_shared=8080/tcp
# tncfg -z public add mlp_private=8080/tcp
```

4. **要将 MLP 添加到内核中，请引导区域。**

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

5. **在全局区域中，为新地址添加路由。**

要添加路由，请执行第 209 页中的 “如何添加缺省路由”中的相关操作。

示例 16–18 使用 `txzonemgr` GUI 配置 MLP

管理员打开 "Labeled Zone Manager"（有标签区域管理器）来配置 Web 代理服务。

```
# txzonemgr &
```

管理员双击 PUBLIC（公共）区域，然后双击 Configure Multilevel Ports（配置多级别端口）。然后，管理员选择并双击 Private interfaces（专用接口）行。选择更改为类似于以下内容的项字段：

```
Private interfaces:111/tcp;111/udp
```

管理员通过分号分隔符开始 Web 代理项输入

```
Private interfaces:111/tcp;111/udp;8080/tcp
```

完成专用项后，管理员在 Shared interfaces（共享接口）字段中键入 Web 代理。

```
Shared interfaces:111/tcp;111/udp;8080/tcp
```

弹出消息指示 public（公共）区域的多级别端口将在下次引导区域时处于活动状态。

示例 16–19 通过 udp 为 NFSv3 配置专用多级别端口

在此示例中，管理员通过 udp 启用 NFSv3 向下读取挂载。管理员可以选择使用 tncfg 命令。

```
# tncfg -z global add mlp_private=2049/udp
```

txzonemgr GUI 提供了定义 MLP 的另一种方式。

在 "Labeled Zone Manager"（有标签区域管理器）中，管理员双击 global（全局）区域，然后双击 Configure Multilevel Ports（配置多级别接口）。在 MLP 菜单中，管理员选择并双击 Private interfaces（专用接口）行，然后添加端口/协议。

```
Private interfaces:111/tcp;111/udp;8080/tcp
```

弹出消息指示 global（全局）区域的多级别端口将在下次引导时处于活动状态。

示例 16–20 显示系统的多级别端口

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
```

配置有标签 IPsec（任务列表）

以下任务列表介绍了用于将标签添加到 IPsec 保护中的任务。

任务	说明	参考
结合使用 Trusted Extensions 和 IPsec。	将标签添加到 IPsec 保护。	第 212 页中的“如何在多级别 Trusted Extensions 网络中应用 IPsec 保护”
通过不可信网络结合使用 Trusted Extensions 和 IPsec。	通过无标签网络传送有标签 IPsec 包。	第 214 页中的“如何通过不可信网络配置隧道”

▼ 如何在多级别 Trusted Extensions 网络中应用 IPsec 保护

在此过程中，在两个 Trusted Extensions 系统上配置 IPsec 以处理以下情况：

- 这两个系统分别为 enigma 和 partym，都是在多级别网络中运行的多级别 Trusted Extensions 系统。
- 对应用程序数据进行加密和保护，以防在网络中进行未经授权的更改。
- 数据的安全标签以 CALIPSO 或 CIPSO IP 选项的形式显示，供 enigma 和 partym 系统之间路径中的多级别路由器和安全设备使用。
- enigma 和 partym 交换的安全标签受到保护，以免受到未经授权的更改。

开始之前 您是全局区域中的 root 角色。

1. **将 enigma 和 partym 主机添加到 cipso 安全模板中。**

   按照第 193 页中的“为主机和网络设置标签（任务）”中的过程进行操作。使用主机类型为 cipso 的模板。

2. **为 enigma 和 partym 系统配置 IPsec。**

   有关过程，请参见《在 Oracle Solaris 11.1 中保护网络安全》中的“如何使用 IPsec 保证两个系统之间的通信安全”。将 IKE 用于密钥管理，如以下步骤中所述。

3 **将标签添加到 IKE 协商。**

按照《在 Oracle Solaris 11.1 中保护网络安全》中的“如何使用预先共享的密钥配置 IKE”中的过程进行操作，然后修改 `ike/config` 文件，如下所示：

a. **将关键字 `label_aware`、`multi_label` 和 `wire_label inner` 添加到 `enigma` 系统的 `/etc/inet/ike/config` 文件中。**

生成的文件将类似于以下内容。突出显示标签添加项。

```
    ### ike/config file on enigma, 192.168.116.16
    ## Global parameters
    #
## Use IKE to exchange security labels.
    label_aware
  #
       ## Defaults that individual rules can override.
    p1_xform
          { auth_method preshared oakley_group 5 auth_alg sha encr_alg 3des }
    p2_pfs 2
    #
  ## The rule to communicate with partym
      # Label must be unique
    { label "enigma-partym"
          local_addr 192.168.116.16
          remote_addr 192.168.13.213
          multi_label
          wire_label inner
          p1_xform
           { auth_method preshared oakley_group 5 auth_alg sha1 encr_alg aes }
          p2_pfs 5
    }
```

b. **将相同关键字添加到 `partym` 系统的 `ike/config` 文件中。**

```
    ### ike/config file on partym, 192.168.13.213
    ## Global Parameters
    #
## Use IKE to exchange security labels.
    label_aware
    #
        p1_xform
          { auth_method preshared oakley_group 5 auth_alg sha encr_alg 3des }
    p2_pfs 2
    ## The rule to communicate with enigma
    # Label must be unique
    { label "partym-enigma"
          local_addr 192.168.13.213
          remote_addr 192.168.116.16
          multi_label
          wire_label inner
    p1_xform
           { auth_method preshared oakley_group 5 auth_alg sha1 encr_alg aes }
        p2_pfs 5
    }
```

4 **如果在网络中无法使用 CALIPSO 或 CIPSO IP 选项的 AH 保护，请使用 ESP 验证。**

使用 `/etc/inet/ipsecinit.conf` 文件中的 `encr_auth_algs`（而非 `auth_algs`）来处理验证。ESP 验证不包含 IP 头和 IP 选项，但验证 ESP 头后面的所有信息。

```
{laddr enigma raddr partym} ipsec {encr_algs any encr_auth_algs any sa shared}
```

注 – 您也可以将标签添加到受证书保护的系统中。公钥证书在 Trusted Extensions 系统的全局区域中进行管理。完成《在 Oracle Solaris 11.1 中保护网络安全》中的“使用公钥证书配置 IKE”中的过程后按同样的方式修改 `ike/config` 文件。

▼ 如何通过不可信网络配置隧道

此过程在两个 Trusted Extensions VPN 网关系统之间通过公共网络配置 IPsec 隧道。此过程中使用的示例基于《在 Oracle Solaris 11.1 中保护网络安全》中的“用于保护 VPN 的 IPsec 任务的网络拓扑说明”中说明的配置。

假设对此说明进行以下修改：

- `10` 子网是多级别可信网络。CALIPSO 或 CIPSO IP 选项安全标签在这些 LAN 上可见。
- `192.168` 子网是在 `PUBLIC` 标签下运行的单标签不可信网络。这些网络不支持 CALIPSO 或 CIPSO IP 选项。
- `euro-vpn` 和 `calif-vpn` 之间的有标签通信受到保护，以免受到未经授权的更改。

开始之前 您是全局区域中的 `root` 角色。

1 **按照第 193 页中的“为主机和网络设置标签（任务）”中的过程进行操作来定义以下内容：**

a. **将 `10.0.0.0/8` IP 地址添加到有标签安全模板中。**

使用主机类型为 `cipso` 的模板。保留缺省标签范围（`ADMIN_LOW` 到 `ADMIN_HIGH`）。

b. **将 `192.168.0.0/16` IP 地址添加到标签 `PUBLIC` 下的无标签安全模板中。**

使用无标签主机类型的模板。将缺省标签设置为 `PUBLIC`。保留缺省标签范围（`ADMIN_LOW` 到 `ADMIN_HIGH`）。

c. **将 `Calif-vpn` 和 `Euro-vpn` 的面向 Internet 的地址 `192.168.13.213` 与 `192.168.116.16` 添加到 `cipso` 模板中。**

保留缺省标签范围。

2 **创建 IPsec 隧道。**

按照《在 Oracle Solaris 11.1 中保护网络安全》中的“如何在隧道模式下使用 IPsec 保护 VPN”中的过程进行操作。将 IKE 用于密钥管理，如以下步骤中所述。

3 **将标签添加到 IKE 协商。**

按照《在 Oracle Solaris 11.1 中保护网络安全》中的“如何使用预先共享的密钥配置 IKE”中的过程进行操作，然后修改 `ike/config` 文件，如下所示：

a. **将关键字 `label_aware`、`multi_label` 和 `wire_label none PUBLIC` 添加到 `euro-vpn` 系统的 `/etc/inet/ike/config` 文件中。**

生成的文件将类似于以下内容。突出显示标签添加项。

```
        ### ike/config file on euro-vpn, 192.168.116.16
    ## Global parameters
    #
## Use IKE to exchange security labels.
    label_aware
    #
        ## Defaults that individual rules can override.
    p1_xform
          { auth_method preshared oakley_group 5 auth_alg sha encr_alg 3des }
    p2_pfs 2
    #
   ## The rule to communicate with calif-vpn
       # Label must be unique
    { label "eurovpn-califvpn"
          local_addr 192.168.116.16
          remote_addr 192.168.13.213
          multi_label
          wire_label none PUBLIC
          p1_xform
           { auth_method preshared oakley_group 5 auth_alg sha1 encr_alg aes }
          p2_pfs 5
        }
```

b. **将相同关键字添加到 `calif-vpn` 系统的 `ike/config` 文件中。**

```
    ### ike/config file on calif-vpn, 192.168.13.213
    ## Global Parameters
    #
## Use IKE to exchange security labels.
    label_aware
    #
        p1_xform
          { auth_method preshared oakley_group 5 auth_alg sha encr_alg 3des }
    p2_pfs 2
    ## The rule to communicate with euro-vpn
    # Label must be unique
    { label "califvpn-eurovpn"
          local_addr 192.168.13.213
          remote_addr 192.168.116.16
          multi_label
          wire_label none PUBLIC
    p1_xform
           { auth_method preshared oakley_group 5 auth_alg sha1 encr_alg aes }
```

```
        p2_pfs 5
}
```

注 – 您也可以将标签添加到受证书保护的系统中。完成《在 Oracle Solaris 11.1 中保护网络安全》中的“使用公钥证书配置 IKE”中的过程后按同样的方式修改 `ike/config` 文件。

可信网络故障排除（ 任务列表 ）

以下任务列表介绍了可帮助您调试 Trusted Extensions 网络的任务。

任务	说明	参考
确定系统和远程主机无法进行通信的原因。	检查单系统上的接口是否已经启动。	第 216 页中的 “如何检验系统的接口是否已启动”
	当系统和远程主机彼此之间不能通信时使用调试工具。	第 217 页中的 “如何调试 Trusted Extensions 网络”
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 220 页中的 “如何调试客户机与 LDAP 服务器的连接”

▼ 如何检验系统的接口是否已启动

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属性值的角色。"Security Administrator"（安全管理员）角色和 "System Administrator"（系统管理员）角色可以检查这些值。

1 检验系统的网络接口是否已启动。

可以使用 "Labeled Zone Manager"（有标签区域管理器）GUI 或 `ipadm` 命令显示系统的接口。

- **打开 "Labeled Zone Manager"（ 有标签区域管理器 ），然后双击需要的区域。**

  ```
  # txzonemgr &
  ```

  选择 "Configure Network Interfaces"（配置网络接口），并检验此区域的 `Status`（状态）列的值是否为 `Up`（启动）。

- **或者，使用 `ipadm show-addr` 命令。**

  ```
  # ipadm show-addr
  ...
  ADDROBJ           TYPE      STATE       ADDR
  ```

```
lo0/v4          static    ok           127.0.0.1/8
net0/_a         dhcp      down         10.131.132.133/23
net0:0/_a       dhcp      down         10.131.132.175/23
```

net0 接口的值应为 ok。有关 ipadm 命令的更多信息，请参见 ipadm(1M) 手册页。

2 **如果接口未启动，请将其启动。**

a. **在 "Labeled Zone Manager"（有标签区域管理器）GUI 中，双击接口处于关闭状态的区域。**

b. **选择 "Configure Network Interfaces"（配置网络接口）。**

c. **双击状态为 Down（关闭）的接口。**

d. **选择 "Bring Up"（初启），然后单击 "OK"（确定）。**

e. **单击 "Cancel"（取消）或 "OK"（确定）。**

▼ 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，可以使用 Trusted Extensions 和 Oracle 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，请参见附录 D，Trusted Extensions 手册页列表。

- 有关联系有标签区域的问题，请参见第 153 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 174 页中的 “如何解决 Trusted Extensions 中的挂载故障”。

开始之前 您必须位于全局区域中，并充当可以检查网络属性值的角色。"Security Administrator"（安全管理员）角色或 "System Administrator"（系统管理员）角色可以检查这些值。只有 root 角色可以编辑文件。

1 **检查无法通信的主机是否正在使用同一命名服务。**

a. **在每个系统上，检查 name-service/switch SMF 服务中 Trusted Extensions 数据库的值。**

```
# svccfg -s name-service/switch listprop config
config/value_authorization  astring  solaris.smf.value.name-service.switch
config/default              astring  ldap
...
config/tnrhtp               astring  "files ldap"
config/tnrhdb               astring  "files ldap"
```

b. 如果不同主机上具有不同的值，请更正违例主机上的值。

```
# svccfg -s name-service/switch setprop config/tnrhtp="files ldap"
# svccfg -s name-service/switch setprop config/tnrhdb="files ldap"
```

c. 然后，在这些主机上重新启动命名服务守护进程。

```
# svcadm restart name-service/switch
```

2 通过显示传输中的源、目标和网关主机来检验是否已正确定义每台主机。

使用命令行检查网络信息是否正确。检验每台主机上的指定是否与网络中其他主机上的指定匹配。根据要查看的内容，使用 `tncfg` 命令、`tninfo` 命令或 `txzonemgr` GUI。

- **显示模板定义。**

  `tninfo -t` 命令以字符串和十六进制格式显示标签。

  ```
  $ 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
  ```

- **显示模板以及指定给该模板的主机。**

  `tncfg -t` 命令以字符串格式显示标签并列出指定的主机。

  ```
  $ tncfg -t template info
     name=<template-name>
     host_type=<one of cipso or unlabeled>
     doi=1
     min_label=<minimum-label>
     max_label=<maximum-label>
     host=127.0.0.1/32            /** Localhost **/
     host=192.168.1.2/32          /** LDAP server **/
     host=192.168.1.22/32         /** Gateway to LDAP server **/
     host=192.168.113.0/24        /** Additional network **/
     host=192.168.113.100/25            /** Additional network **/
     host=2001:a08:3903:200::0/56     /** Additional network **/
  ```

- **显示特定主机的 IP 地址和所指定的安全模板。**

  `tninfo -h` 命令显示指定主机的 IP 地址以及所指定的安全模板的名称。

  ```
  $ tninfo -h hostname
  IP Address: IP-address
  Template: template-name
  ```

  `tncfg get host=` 命令显示定义指定主机的安全模板名称。

  ```
  $ tncfg get host=hostname|IP-address[/prefix]
  template-name
  ```

- **显示区域的多级别端口 (multilevel port, MLP)。**

  `tncfg -z` 命令在每一行列出一个 MLP。

  ```
  $ tncfg -z zone-name info [mlp_private | mlp_shared]
  mlp_private=<port/protocol-that-is-specific-to-this-zone-only>
  mlp_shared=<port/protocol-that-the-zone-shares-with-other-zones>
  ```

  `tninfo -m` 命令在一行中列出专用 MLP，在另一行中列出共享 MLP。使用分号分隔 MLP。

  ```
  $ tninfo -m zone-name
  private: ports-that-are-specific-to-this-zone-only
  shared: ports-that-the-zone-shares-with-other-zones
  ```

  要以 GUI 形式显示 MLP，请使用 `txzonemgr` 命令。双击区域，然后选择 "Configure Multilevel Ports"（配置多级别端口）。

3. **修复任何不正确的信息。**

   a. **要更改或检查网络安全信息，请使用可信网络管理命令 `tncfg` 和 `txzonemgr`。要检验数据库的语法，请使用 `tnchkdb` 命令。**

   例如，以下输出显示未定义模板名称 `internal_cipso`：

   ```
   # tnchkdb
        checking /etc/security/tsol/tnrhtp ...
        checking /etc/security/tsol/tnrhdb ...
   tnchkdb: unknown template name: internal_cipso at line 49
   tnchkdb: unknown template name: internal_cipso at line 50
   tnchkdb: unknown template name: internal_cipso at line 51
        checking /etc/security/tsol/tnzonecfg ...
   ```

   该错误表明未使用 `tncfg` 和 `txzonemgr` 命令创建和指定 `internal_cipso` 安全模板。

   要进行修复，请将 `tnrhdb` 文件替换为原始文件，然后使用 `tncfg` 命令创建并指定安全模板。

   b. **要清除内核高速缓存，请重新引导。**

   在引导时，会使用数据库信息置备高速缓存。SMF 服务 `name-service/switch` 决定是使用本地数据库还是使用 LDAP 数据库来置备内核。

4. **收集传输信息以帮助进行调试。**

   a. **检验您的路由配置。**

   ```
   $ route get [ip] -secattr sl=label,doi=integer
   ```

   有关详细信息，请参见 `route(1M)` 手册页。

   b. **查看包中的标签信息。**

   ```
   $ snoop -v
   ```

   `-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。

c. 查看路由表项和套接字的安全属性。

```
$ netstat -aR
```

-aR 选项显示套接字的扩展安全属性。

```
$ netstat -rR
```

-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。

a. 使用 tncfg 或 tninfo 命令查看信息。

```
# tncfg get host=LDAP-server
# tncfg get host=gateway-to-LDAP-server

# tninfo -h LDAP-server
# tninfo -h gateway-to-LDAP-server
```

b. 确定通往服务器的路由。

```
# route get LDAP-server
```

如果模板指定不正确，请将主机添加到正确的模板。

2 检查并更正（如有必要）/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 文件中删除 LServer-zones。

3 如果使用的是 DNS，请检查 svc:/network/dns/client 服务的配置。

```
# svccfg -s dns/client listprop config
config                      application
config/value_authorization  astring       solaris.smf.value.name-service.dns.switch
config/nameserver           astring       192.168.8.25 192.168.122.7
```

4 要更改值，请使用 **svccfg** 命令。

```
# svccfg -s dns/client setprop config/search = astring: example1.domain.com
# svccfg -s dns/client setprop config/nameserver = net_address: 192.168.8.35
# svccfg -s dns/client:default refresh
# svccfg -s dns/client:default validate
# svcadm enable dns/client
# svcadm refresh name-service/switch
# nslookup some-system
Server:         192.168.135.35
Address:        192.168.135.35#53

Name:   some-system.example1.domain.com
Address: 10.138.8.22
Name:   some-system.example1.domain.com
Address: 10.138.8.23
```

5 检验 **name-service/switch** 服务中的 **tnrhdb** 和 **tnrhtp** 项是否正确。

在以下输出中，未列出 tnrhdb 和 tnrhtp 项。因此，这些数据库将按该顺序使用缺省的 files ldap 命名服务。

```
# svccfg -s name-service/switch listprop config
config                          application
config/value_authorization      astring       solaris.smf.value.name-service.switch
config/default                  astring       "files ldap"
config/host                     astring       "files dns"
config/netgroup                 astring       ldap
```

6 检查是否在服务器上正确配置了客户机。

```
# ldaplist -l tnrhdb client-IP-address
```

7 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
```

8 检验您是否可以从当前运行的所有区域联系 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
...
```

9 配置 LDAP 并重新引导。

a. 有关过程，请参见第 87 页中的“使全局区域成为 Trusted Extensions 中的客户机”。

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. 停止所有区域并重新引导。

```
# zoneadm list
zone1
zone2
,
,
,
# zoneadm -z zone1 halt
# zoneadm -z zone2 halt
.
.
.
# reboot
```

可以改用 `txzonemgr` GUI 来停止有标签区域。

◆ ◆ ◆ 第 17 章

17 Trusted Extensions 和 LDAP（概述）

本章介绍了如何针对配置有 Trusted Extensions 的系统使用 Oracle Directory Server Enterprise Edition（LDAP 服务器）。

- 第 223 页中的 “在 Trusted Extensions 中使用 LDAP 命名服务”
- 第 225 页中的 “Trusted Extensions 中的 LDAP 命名服务快速参考”

在 Trusted Extensions 中使用 LDAP 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。`svc:/system/name-service/switch` 服务确定要使用的命名服务。LDAP 是推荐用于 Trusted Extensions 的命名服务。

LDAP 服务器可以为 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。安全管理员在系统配置期间指定多级别端口。

通常，在全局区域中为全局区域配置此多级别端口。因此，有标签区域无法对 LDAP 目录进行写入访问。相反，有标签区域通过在网络上其自身系统或其他可信系统中运行的多级别代理服务发送读取请求。Trusted Extensions 也支持每个标签一个目录服务器的 LDAP 配置。当用户每个标签有不同的凭证时，需要此类配置。

Trusted Extensions 将两个可信网络数据库添加到 LDAP 服务器：`tnrhdb` 和 `tnrhtp`。

- 有关在 Oracle Solaris 中使用 LDAP 命名服务的信息，请参见《Oracle Solaris Administration: Naming and Directory Services》中的第 III 部分, “LDAP Naming Services”。
- 第 5 章，为 Trusted Extensions 配置 LDAP（任务）中介绍了如何设置用于 Trusted Extensions 的 LDAP 服务器。通过使用配置有 Trusted Extensions 的代理，Trusted Extensions 系统可以成为 Oracle Solaris LDAP 服务器的客户机。

- 第 87 页中的 “创建 Trusted Extensions LDAP 客户机”中介绍了如何设置 Trusted Extensions LDAP 服务器的客户机。

本地管理的 Trusted Extensions 系统

如果站点上没有使用分布式的命名服务，则管理员必须确保用户、系统和网络的配置信息在所有系统上均相同。如果在一个系统上做了某个更改，则在所有系统上必须做相同的更改。

在本地管理的 Trusted Extensions 系统上，在 `/etc`、`/etc/security` 和 `/etc/security/tsol` 目录中的文件中通过 `name-service/switch` SMF 服务中的配置属性来维护配置信息。

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
```

Trusted Extensions 中的 LDAP 命名服务快速参考

在 Trusted Extensions 中管理 LDAP 命名服务的方法与在 Oracle Solaris 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，请参见《在 Oracle Solaris 11.1 中使用命名和目录服务》中的第 13 章 “LDAP 故障排除（参考信息）”。
- 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 220 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《在 Oracle Solaris 11.1 中使用命名和目录服务》中的第 13 章 “LDAP 故障排除（参考信息）”。
- 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软件的版本 6 或 7 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软件的版本 6 或 7 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 18 章

18 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。

- 第 227 页中的 “多级别邮件服务”
- 第 227 页中的 “Trusted Extensions 邮件功能”

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 131 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 管理：网络服务》中的第 13 章 “邮件服务（任务）”中的说明设置并管理邮件服务器。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(1)` 手册页。有关配置建议，请参见第 126 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 Thunderbird 邮件用于多级别邮件，您需要以每个标签配置 Thunderbird 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。

- 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。该列表和第 185 页中的 “Trusted Extensions 认可检查”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 19 章

19 管理有标签打印（任务）

本章介绍如何使用 Trusted Extensions 来配置有标签打印。还介绍如何在没有标签设置选项的情况下配置 Trusted Extensions 打印作业。

- 第 229 页中的 “标签、打印机和打印”
- 第 236 页中的 “配置有标签打印（任务列表）”
- 第 243 页中的 “在 Trusted Extensions 中减少打印限制（任务列表）”

标签、打印机和打印

Trusted Extensions 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。该软件还对打印输出设置标签。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。管理员按照基本的 Oracle Solaris 打印机管理过程进行操作。需要进行配置才能应用标签、限制打印作业的标签范围、配置要打印的有标签区域以及放宽打印限制。

Trusted Extensions 同时支持多级别打印和单级别打印。缺省情况下，在 Trusted Extensions 系统的全局区域中配置的打印服务器可以打印所有范围的标签，也就是说，该打印服务器是多级别的。可访问该打印服务器的任何有标签区域或系统都可以打印到连接的打印机。有标签区域可支持单级别打印。区域可以通过全局区域连接打印机，也可以将区域配置为打印服务器。使用该标签的任何区域都可以访问有标签区域，因此它的打印服务器可以在连接的打印机上打印。也可以通过在已指定任意标签的无标签系统上使用打印服务器来进行单级别打印。这些打印作业将进行无标签的打印。

Oracle Solaris 10 和 Oracle Solaris 11 中的 Trusted Extensions 打印之间的差别

Oracle Solaris 10 的缺省打印协议是 LP 打印服务。Oracle Solaris 11 的缺省系统是通用 UNIX 打印系统 (Common UNIX Printing System, CUPS)。有关 Oracle Solaris 中 CPU 的全面指南，请参见《在 Oracle Solaris 11.1 中配置和管理输出》。下表列出了 CUPS 和 LP 打印协议之间的显著差异。

表 19–1 CUPS – LP 差异

差异区域	CUPS	LP
IANA 端口号	631	515
打印面	单面	双面
层叠打印	必须在打印服务器上共享打印机	必须配置通往打印机的路由
访问网络打印机	必须能够成功对打印机和打印服务器的 IP 地址执行 `ping` 操作	必须配置通往打印机的路由
远程打印作业	无法在无标签的情况下打印	可以在无标签的情况下打印
向客户机添加远程打印机	`lpadmin -p` *printer-name* `-E \ -v ipp://`*print-server-IP-address*`/printers/`*printer-name-on-server*	`lpadmin -p` *printer-name* `\ -s` *server-name*
启用并接受打印服务器	`lpadmin -E` 选项	`accept` 和 `enable` 命令
PostScript 保护	缺省情况下提供	需要授权
禁用标题页和篇尾页	`-o job-sheets=none` 选项	`-o nobanner` 选项
`lp -d` *printer* `file1 file2`	每个打印作业一个标题页和一个篇尾页	打印作业中每个文件一个标题页和一个篇尾页
作业页面上的标签方向	始终纵向	始终为作业的方向

打印服务	`svc:/application/cups/scheduler`
	`.../in-lpd:default`
		`svc:/application/print/service-selector`
		`.../server`
		`.../rfc1179`
		`.../ipp-listener`
		`svc:/network/device-discovery/printers:snmp`

在 Trusted Extensions 中限制对打印机和打印作业信息的访问

配置有 Trusted Extensions 的系统上的用户和角色以其会话的标签创建打印作业。只有识别该标签的打印服务器才接受这些打印作业。此标签必须在打印服务器的标签范围内。

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。

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。信息来自 `/etc/security/tsol/label_encodings` 文件和 `/usr/lib/cups/filter/tsol_separator.ps` 文件。在所有页面的顶部和底部，长度超过 80 个字符的标签在打印时都会被截断。该截断通过箭头 (->) 指示。即使正文页以横向打印，页眉和页脚标签也以纵向打印。有关示例，请参见图 19–4。

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。安全管理员可以配置以下内容：

- 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

定向到无标签打印机的用户可以打印不带标签的输出。用户位于具有其自己的打印服务器的有标签区域中时，如果向用户指定 `solaris.print.unlabeled` 授权，则他们可以打印不带标签的输出。可将角色配置为打印不带标签的输出到由 Trusted Extensions 打印服务器控制的本地打印机。有关帮助，请参见第 243 页中的 “在 Trusted Extensions 中减少打印限制（任务列表）”。

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。有关这些部分中的文本源的解释，请参见《Trusted Extensions Label Administration》中的第 4 章 “Labeling Printer Output (Tasks)”。请注意，篇尾页使用不同的外线。

图 19–1 有标签打印作业的典型标题页

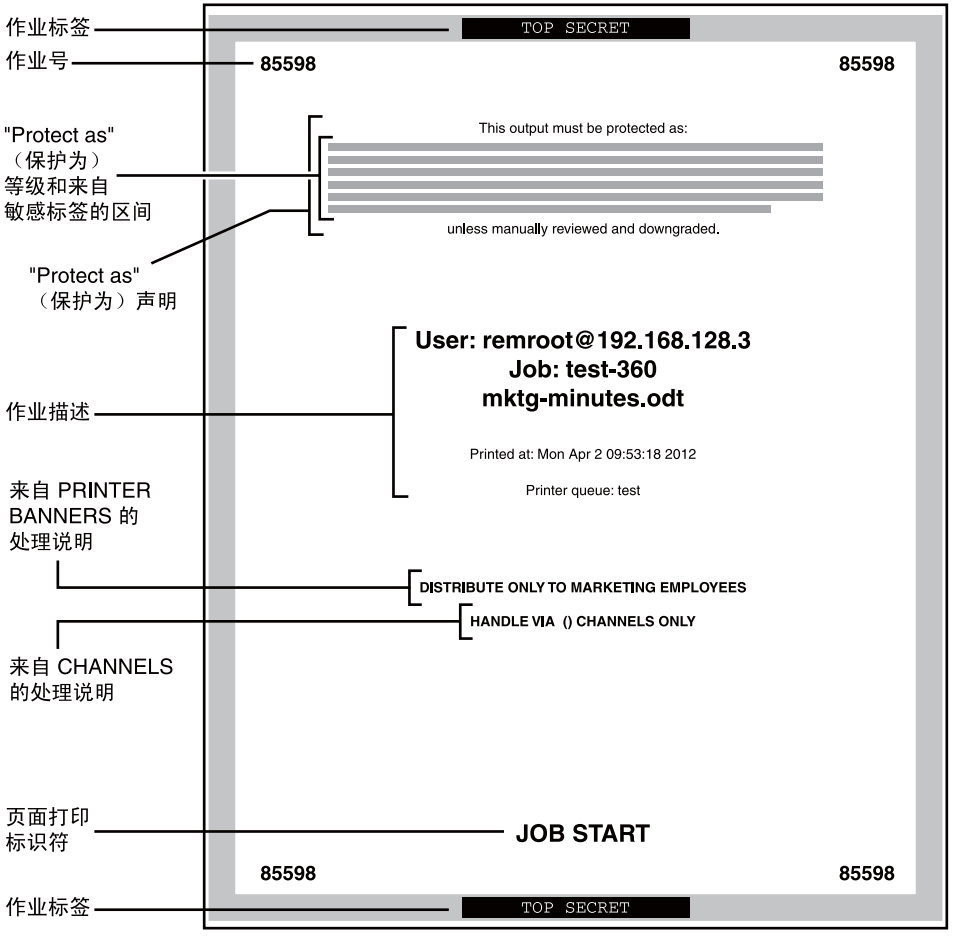
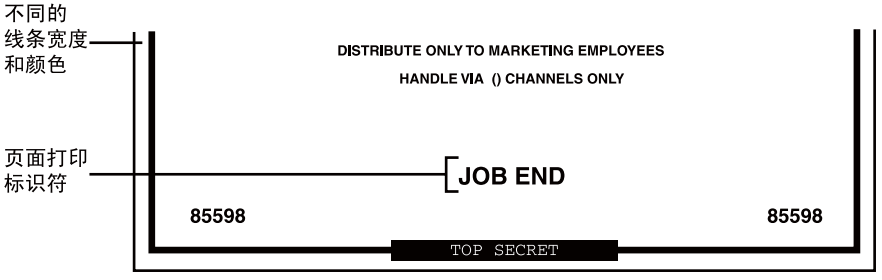


图 19–2 篇尾页的差别

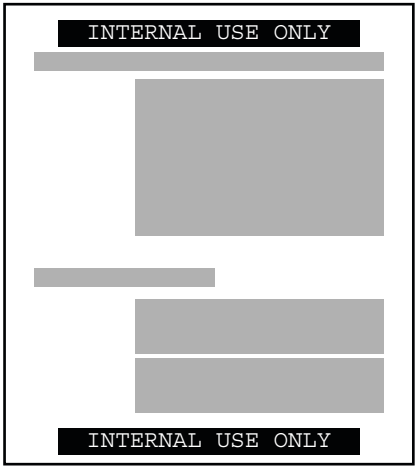


有标签正文页

缺省情况下，将在每个正文页的顶部和底部打印 "Protect as"（保护为）等级。作业标签的等级与 `minimum protect as` 等级相比，"Protect as"（保护为）等级是处于支配地位的等级。`minimum protect as` 等级在 `label_encodings` 文件中定义。

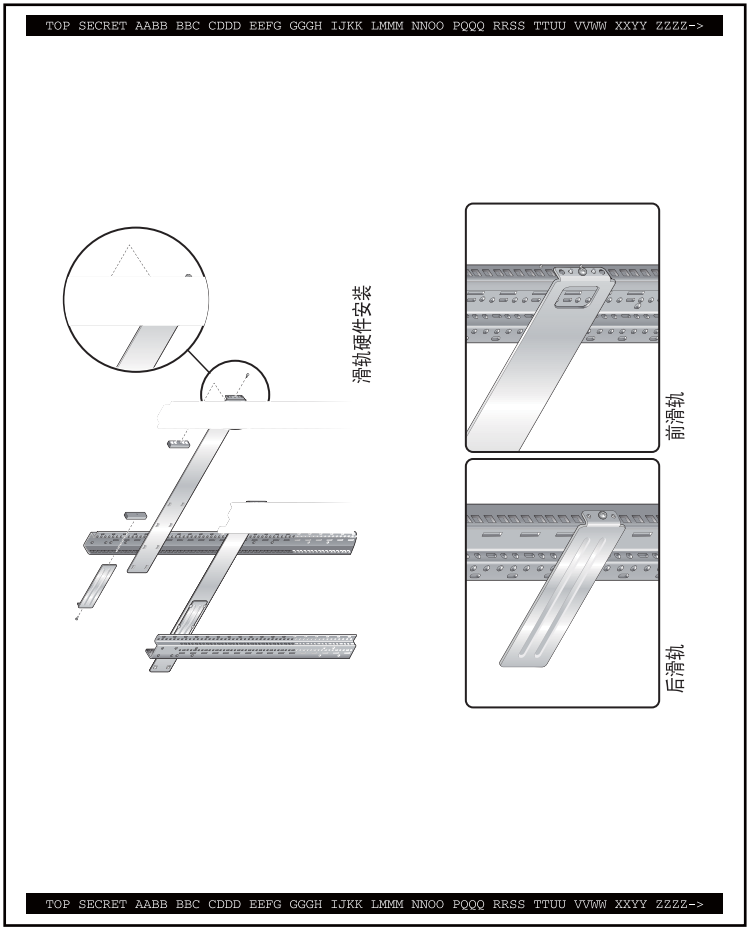
例如，如果用户登录到 `Internal Use Only` 会话，则该用户的打印作业使用该标签。如果 `label_encodings` 文件中的 `minimum protect as` 等级是 `Public`，则在正文页上打印 `Internal Use Only` 标签。

图 19–3 在正文页顶部和底部打印的作业标签



正文页以横向模式打印时，标签以纵向模式打印。下图显示了以横向模式打印的正文页，它的 "Protect as"（保护为）标签扩展至页面边界之外。此标签截断至 80 个字符。

图 19–4 正文页以横向模式打印时，作业的标签以纵向模式打印



tsol_separator.ps 配置文件

下表显示了安全管理员可通过修改 /usr/lib/cups/filter/tsol_separator.ps 文件进行更改的可信打印的各个方面。

表 19–2 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”。

表 19–2 tsol_separator.ps 文件中的可配置值 （续）

输出	缺省值	如何定义	更改
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 Oracle Solaris 打印中的功能。在 Oracle Solaris OS 中，job-sheets 选项处理标题页创建。为了执行标签设置操作，过滤器将打印作业转换为 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。

注 – CUPS 将阻止对 PostScript 文件进行任何改动。因此，有经验的 PostScript 程序员不能创建可修改打印输出上的标签的 PostScript 文件。

Trusted Extensions 打印界面（参考信息）

Trusted Extensions 将添加以下打印授权来实施 Trusted Extensions 安全策略。会在打印服务器上检查这些授权。因此，远程用户（如有标签区域中的用户）不能通过授权检查。

- solaris.print.admin－允许角色管理打印
- solaris.print.list－允许角色查看不属于该角色的打印作业
- solaris.print.nobanner－允许角色打印全局区域中没有标题页和篇尾页的作业

- `solaris.print.unlabeled` － 允许角色打印全局区域中没有页标签的作业

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。一般用户只能取消他们自己的作业。
- `lp` － 打印没有标签的正文页的 `-o nolabel` 选项需要 `solaris.print.unlabeled` 授权。打印没有标题页或篇尾页的 `-o job-sheets=none` 选项需要 `solaris.print.nobanner` 授权。
- `lpstat` － 调用者必须等于打印作业的标签才能获取作业的状态。一般用户只能查看他们自己的打印作业。

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。
- `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。

在 Trusted Extensions 中管理打印（ 任务 ）

完成 Oracle Solaris 打印机设置后，您可以执行 Trusted Extensions 的配置打印过程。这些过程中包含某些基本设置。有关更多信息，请参见《在 Oracle Solaris 11.1 中配置和管理输出》中的第 2 章 “使用 CUPS 设置打印机（任务）”。以下链接指向管理有标签打印的主要任务：

- 第 236 页中的 “配置有标签打印（任务列表）”
- 第 243 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。

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 237 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
配置网络打印机。	共享打印机。	第 239 页中的“如何配置网络打印机”
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 239 页中的“如何将区域配置为单级别打印服务器”
配置多级别打印客户机。	将 Trusted Extensions 主机连接到打印机。	第 240 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 242 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

连接到 Trusted Extensions 打印服务器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。如果该打印机被共享，则可以访问该打印服务器的所有 Trusted Extensions 主机都可以使用该共享打印机。

开始之前 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. **确定打印机的品牌和型号。**

   ```
   # lpinfo -m | grep printer-manufacturer
   ```

   例如，以下语法可找到所有 Xerox 打印机：

   ```
   # lpinfo -m | grep Xerox
   gutenprint.5.2://xerox-able_1406/expert Xerox Able 1406 - CUPS+Gutenprint v5.2.4
   gutenprint.5.2://xerox-able_1406/simple Xerox Able 1406 - CUPS+Gutenprint v5.2.4 ...
   gutenprint.5.2://xerox-dc_400/expert Xerox Document Centre 400 - ...
   gutenprint.5.2://xerox-dc_400/simple Xerox Document Centre 400 - ...
   gutenprint.5.2://xerox-dp_4508/expert Xerox DocuPrint 4508 - ...
   gutenprint.5.2://xerox-dp_4508/simple Xerox DocuPrint 4508 - ...
   ...
   ```

2. **定义所连接的每个打印机的特征。**

   ```
   # lpadmin -p printer-name -E -v socket://printer-IP-address -m printer-make-and-model
   -
   ```

   `-E` 选项允许指定的打印机接受打印请求队列。它还将激活或启用打印机。

3. **要创建网络打印机，请共享打印机。**

   ```
   # lpadmin -p printer-name -o printer-is-shared=true
   ```

   要阻止其他系统使用该打印机，请跳过此步骤。

4 **显示打印机缺省设置。**

```
# lpoptions -p printer-name
```

5 **调整缺省设置。**

例如，您可以打印双面和双联本。

提示 – 可以使用 CUPS Web 界面来配置打印机：Home - CUPS version-number (`http://localhost:631`)。

---

6 **为连接到打印服务器的每台打印机配置有标签的标题页和篇尾页。**

```
# lpadmin -p printer-name -o job-sheets=labeled
```

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。

7 **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. **添加打印机。**

```
# lpadmin -p zone-printer-name -E \
-v ipp://global-zone-IP-address/printers/printer-name-in-global-zone
```

c. **可选将打印机设置为缺省打印机。**

```
# lpadmin -d zone-printer-name
```

8 **在每个有标签区域中，测试打印机。**

以 `root` 身份和一般用户身份，执行以下步骤：

a. **从命令行打印文本和 PostScript 文件。**

```
# lp /etc/motd ~/PostScriptTest.ps
% lp $HOME/file1.txt $HOME/PublicTest.ps
```

b. **从应用程序（如邮件、Oracle OpenOffice、Adobe Reader 和浏览器）打印文件。**

c. **验证标题页、篇尾页和正文页标签是否正确打印。**

另请参见

- **限制打印机标签范围 –** 第 242 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 243 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 240 页中的 “如何允许 Trusted Extensions 客户机访问打印机”

▼ 如何配置网络打印机

如果某台打印机被共享，则可以访问打印服务器的所有 Trusted Extensions 主机都可以使用该共享打印机。

开始之前 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. **定义您的网络打印机的特征。**

   按照第 237 页中的 “如何配置多级别打印服务器及其打印机”中的步骤 1 到步骤 6 来配置您的网络打印机。

   在步骤 3 中共享打印机后，可访问该打印机的网络上的所有系统都可以打印到该打印机。

2. **测试网络打印机。**

   以 `root` 身份和一般用户身份，从使用该打印服务器的系统执行以下步骤：

   a. **从命令行打印文本和 PostScript 文件。**

   ```
   # lp /etc/motd ~/PostScriptTest.ps
   % lp $HOME/file1.txt $HOME/PublicTest.ps
   ```

   b. **从应用程序（如邮件、Oracle OpenOffice、Adobe Reader 和浏览器）打印文件。**

   c. **验证标题页、篇尾页和正文页标签是否正确打印。**

另请参见

- **限制打印机标签范围** – 第 242 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 243 页中的 “在 Trusted Extensions 中减少打印限制（任务列表）”

▼ 如何将区域配置为单级别打印服务器

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 用户指南》中的“如何在最小标签下添加工作区”。

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 用户指南》中的“如何更改工作区标签”。

3 **定义所连接的每个打印机的特征。**

按照第 237 页中的 “如何配置多级别打印服务器及其打印机”中的步骤 1 到步骤 6 来配置您的区域打印机。

已连接的打印机只能打印区域标签的作业。

4 **测试打印机。**

注 – 出于安全原因，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. **从命令行打印文本和 PostScript 文件。**

```
# lp /etc/motd ~/PostScriptTest.ps
% lp $HOME/file1.txt $HOME/PublicTest.ps
```

b. **从应用程序（如邮件、Oracle OpenOffice、Adobe Reader 和浏览器）打印文件。**

c. **验证标题页、篇尾页和正文页标签是否正确打印。**

另请参见

- **阻止有标签的输出 —** 第 243 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 240 页中的 “如何允许 Trusted Extensions 客户机访问打印机”

▼ 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共享打印机的访问。
- 对于有标签区域，添加对连接到其系统的全局区域的共享打印机的访问。
- 对于有标签区域，添加对为其配置同一标签远程区域的共享打印机的访问。
- 对于有标签区域，添加对连接到其他系统上全局区域的共享打印机的访问。

开始之前 打印服务器已配置有标签范围或单个标签。此外，已配置并共享连接到打印服务器的打印机。有关详细信息，请参见以下内容：

- 第 237 页中的 “如何配置多级别打印服务器及其打印机”
- 第 239 页中的 “如何将区域配置为单级别打印服务器”
- 第 244 页中的 “如何为无标签的打印服务器指定标签”

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

1. **验证是否能够对打印机执行 ping 命令。**

   ```
   # ping printer-IP-address
   ```

   如果此命令失败，则存在网络连接问题。请修复连接问题，然后返回到此过程。有关帮助，请参见第 216 页中的“可信网络故障排除（任务列表）”。

2. **完成使系统能够访问打印机的一个或多个过程。**

   - **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. **添加对连接到远程 Trusted Extensions 打印服务器的打印机的访问。**

     ```
     $ lpadmin -p printer-name -E \
     -v ipp://print-server-IP-address/printers/printer-name-on-server
     ```

   - **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 用户指南》中的“如何更改工作区标签”。

     b. **添加对打印机的访问。**

     ```
     $ lpadmin -p printer-name -E \
     -v ipp://print-server-IP-address/printers/printer-name-on-print-server
     ```

   - **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。**

     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 -p printer-name -E \
     -v ipp://zone-print-server-IP-address/printers/printer-name-on-zone-print-server
     ```

   - **将有标签区域配置为使用无标签打印服务器打印无安全信息的输出。**

     有关说明，请参见第 244 页中的“如何为无标签的打印服务器指定标签”。

3. **测试打印机。**

注 – 出于安全原因，具有管理标签 ADMIN_HIGH 或 ADMIN_LOW 的文件在打印输出的正文页上打印 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，测试可以访问全局区域的所有帐户和可以访问有标签区域的所有帐户是否可以打印。

a. **从命令行打印文本和 PostScript 文件。**

```
# lp /etc/motd ~/PostScriptTest.ps
% lp $HOME/file1.txt $HOME/PublicTest.ps
```

b. **从应用程序（如邮件、Oracle OpenOffice、Adobe Reader 和浏览器）打印文件。**

c. **验证标题页、篇尾页和正文页标签是否正确打印。**

▼ 如何为打印机配置受限制的标签范围

打印机的缺省标签范围为 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 Manager"（设备管理器）。**
   从 "Trusted Path"（可信路径）菜单中选择 "Allocate Device"（分配设备）选项。
2. **单击 "Administration"（管理）按钮以显示 "Device Administration"（设备管理）对话框。**
3. **如果打印机已列于对话框中并连接到系统，则查找打印机的名称。**
   否则，请单击 "Add"（添加）按钮，并为新打印机键入名称。
4. **单击 "Configure"（配置）按钮以显示 "Device Configuration"（设备配置）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 103 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 Manager"（设备管理器）。

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。	阻止在全局区域的打印输出上打印安全信息。	第 243 页中的 “如何删除标题页和篇尾页”
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。未用标签标记打印作业。	第 244 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。	打印到无标签打印服务器。 指定禁止标签设置操作的打印授权。	第 244 页中的 “如何为无标签的打印服务器指定标签” 第 245 页中的 “如何允许特定用户和角色不标记打印输出”
隐藏标题页和篇尾页。	删除标题页和篇尾页，从而删除这些页面上的其他安全信息。	第 243 页中的 “如何删除标题页和篇尾页”
指定打印授权。	授权特定用户和角色打印没有标签的作业。	第 245 页中的 “如何允许特定用户和角色不标记打印输出”

▼ 如何删除标题页和篇尾页

`job-sheets` 选项设置为 `none` 的打印机不打印标题页或篇尾页。

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

- **在适当的标签，将打印机配置为无标题页或篇尾页。**

```
$ lpadmin -p print-server-IP-address -o job-sheets=none,none
```

或者，可以指定一次 `none`。

```
$ lpadmin -p print-server-IP-address -o job-sheets=none
```

仍为正文页设置标签。要从正文页删除标签，请参见第 245 页中的“如何允许特定用户和角色不标记打印输出”。

▼ 如何为无标签的打印服务器指定标签

可通过 Trusted Extensions 系统向 Oracle Solaris 打印服务器指定标签以访问使用该标签的打印机。在指定的标签打印无标签的作业。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。用户可以在使用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. **为打印服务器指定无标签的模板。**

   有关详细信息，请参见第 198 页中的“如何将主机添加到安全模板”。

   在指定给无标签模板中打印服务器的标签处工作的用户可以将打印作业发送到使用该标签的 Oracle Solaris 打印机。

2. **在无法访问打印机的系统上，承担 "Security Administrator"（安全管理员）角色。**

3. **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 用户指南》中的“如何更改工作区标签”。

4. **添加对连接到任意有标签打印服务器的打印机的访问。**

   ```
   $ lpadmin -p printer-name -E \
   -v ipp://print-server-IP-address/printers/printer-name-on-print-server
   ```

示例 19–1 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。第 214 页中的“如何通过不可信网络配置隧道”对此模板进行了介绍。模板的任意标签是 `PUBLIC`。打印机 `pr-nolabel1` 已连接到此打印服务器。来自 `PUBLIC` 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。

▼ 如何允许特定用户和角色不标记打印输出

要使用户和角色可以打印无标签作业，需要 "Security Administrator"（安全管理员）的授权，并且提交打印作业时需要已授权用户或角色的操作。

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. **为用户或角色指定打印授权。**

   - **要使用户或角色能够从标题页和篇尾页删除标签，请指定 `solaris.print.nobanner` 授权。**

     ```
     $ usermod -A +solaris.print.nobanner username

     $ rolemod -A +solaris.print.nobanner rolename
     ```

   - **要使用户或角色能够从正文页删除标签，请指定 `solaris.print.unlabeled` 授权。**

     ```
     $ usermod -A +solaris.print.unlabeled username

     $ rolemod -A +solaris.print.unlabeled rolename
     ```

   - **要使用户或角色能够从打印输出删除所有标签，请同时指定上述两种授权。**

     ```
     $ usermod -A +solaris.print.unlabeled,+solaris.print.nobanner username

     $ rolemod -A +solaris.print.unlabeled,+solaris.print.nobanner rolename
     ```

2. **准备打印无标签输出。**

   确保打印机是本地打印机。

   对于用户，这表示用户必须从具有打印服务器的有标签区域打印。角色可从全局区域或有标签区域打印。

3. **要打印无标签输出，请在命令行上指定删除标签的选项。**

   您必须具有打印无标签输出的权限。

   - **要在没有标题的情况下进行打印，请使用 `job-sheets=none` 选项。**

     ```
     $ lp -o job-sheets=none file
     ```

   - **要在正文页上没有标签的情况下进行打印，请使用 `nolabel` 选项。**

     ```
     $ lp -o nolabels file
     ```

   - **要在确保输出上没有标签的情况下进行打印，请同时使用这两个选项。**

     ```
     $ lp -o job-sheets=none -o nolabels file
     ```

◆ ◆ ◆ 第 20 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。

- 第 247 页中的 “通过 Trusted Extensions 软件提供的设备保护”
- 第 249 页中的 “设备管理器 GUI”
- 第 250 页中的 “Trusted Extensions 中的设备安全保障”
- 第 251 页中的 “Trusted Extensions 中的设备（参考信息）”

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 Manager"（设备管理器）。

有关 Oracle Solaris 中的设备保护的信息，请参见《Oracle Solaris 11.1 管理：安全服务》中的第 5 章 “控制对设备的访问（任务）”。

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《Oracle Solaris 11.1 管理：安全服务》中的“配置设备策略（任务列表）”。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《Oracle Solaris 11.1 管理：安全服务》中的“设备清除脚本”。

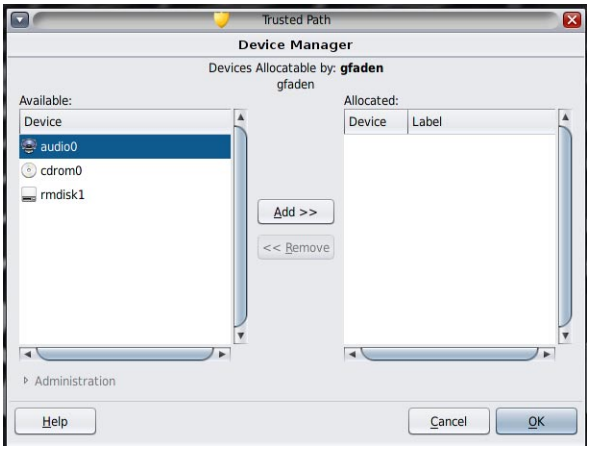
对于 Trusted Extensions 软件，device-clean（设备清除）脚本必须满足特定的要求。`device_clean(5)` 手册页中描述了这些要求。

设备管理器 GUI

设备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。一般用户也可使用设备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。

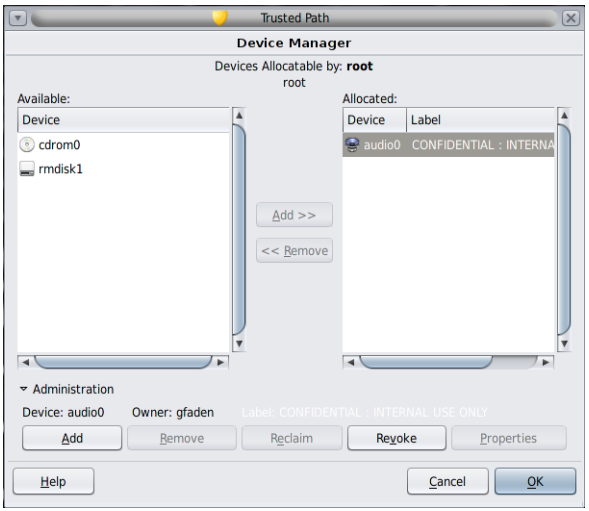
GUI 被称为设备管理器。可以通过从 "Trusted Path"（可信路径）菜单选择 "Allocate Device"（分配设备）来启动该 GUI。下图显示了由可以分配 `audio` 设备的用户打开的设备管理器。

图 20–1 用户打开的设备管理器



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 Devices"（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。



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《Oracle Solaris 11.1 管理：安全服务》中的“设备保护（参考信息）”。

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《Oracle Solaris 11.1 管理：安全服务》中的“如何强制分配设备”和《Oracle Solaris 11.1 管理：安全服务》中的“如何强制取消分配设备”。

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 21 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。

- 第 253 页中的 “在 Trusted Extensions 中操作设备（任务列表）”
- 第 254 页中的 “在 Trusted Extensions 中使用设备（任务列表）”
- 第 254 页中的 “在 Trusted Extensions 中管理设备（任务列表）”
- 第 261 页中的 “在 Trusted Extensions 中定制设备授权（任务列表）”

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 254 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 254 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）角色创建新的设备授权、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 261 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，角色必须使用设备管理器。Oracle Solaris `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 用户指南》中的“如何在 Trusted Extensions 中分配设备”
使用便携介质传输文件。	第 75 页中的 “如何在 Trusted Extensions 中从便携介质复制文件” 第 74 页中的 “如何在 Trusted Extensions 中将文件复制到便携介质”

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。	《Oracle Solaris 11.1 管理：安全服务》中的“配置设备策略（任务列表）”
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。	《Oracle Solaris 11.1 管理：安全服务》中的“如何授权用户分配设备”
	"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 261 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 255 页中的 “如何在 Trusted Extensions 中配置设备”
撤销或回收设备。	使用设备管理器使设备可供用户使用。	第 258 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。	《Oracle Solaris 11.1 管理：安全服务》中的“如何强制分配设备” 《Oracle Solaris 11.1 管理：安全服务》中的“如何强制取消分配设备”
阻止访问可分配设备。	提供对设备的细粒度访问控制。	示例 21–2
	拒绝所有人访问可分配设备。	示例 21–1
保护打印机和帧缓存器。	确保不可分配的设备不可分配。	第 259 页中的 “如何在 Trusted Extensions 中保护不可分配的设备”

任务	说明	参考
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 260 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

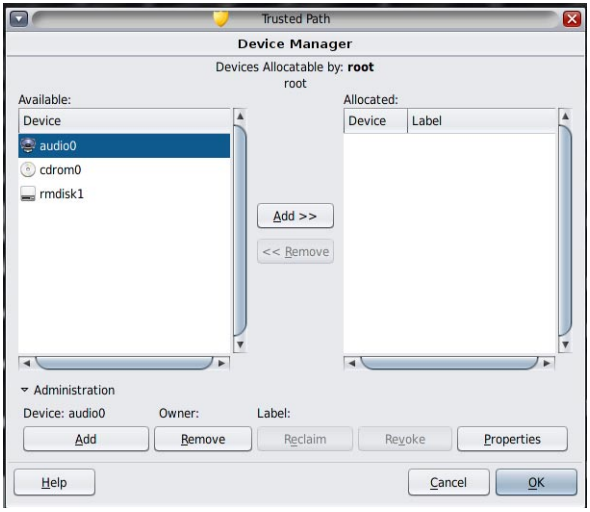
缺省情况下，可分配设备的标签范围是从 ADMIN_LOW 到 ADMIN_HIGH，并且必须在分配后才可使用。另外，用户必须获得授权才能分配设备。这些缺省值是可以更改的。

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

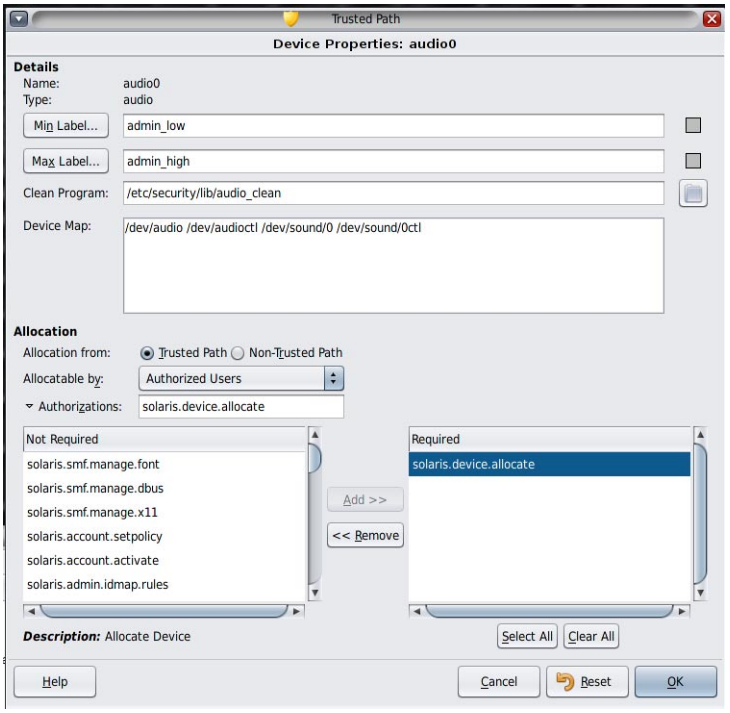
开始之前 您必须具有全局区域中的 "Security Administrator"（安全管理员）角色。

1. **从 "Trusted Path"（可信路径）菜单中，选择 "Allocate Device"（分配设备）。**
   此时将显示 "Device Manager"（设备管理器）。



2 **查看缺省安全设置。**

单击 "Administration"（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 103 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 Configuration"（设备配置）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）。**

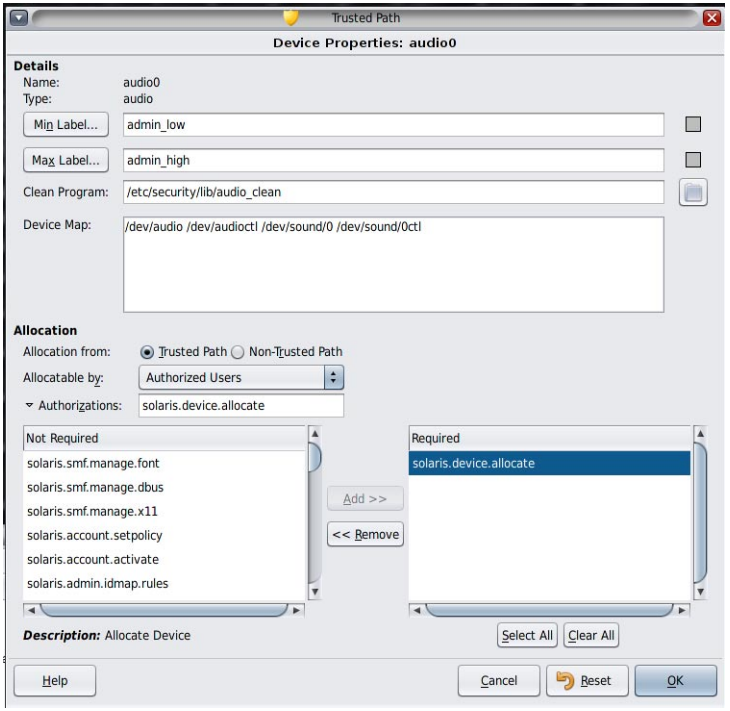
5 指定设备是否可以远程分配。

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）。

- **若需要用户授权，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 261 页中的“在 Trusted Extensions 中定制设备授权（任务列表）”。

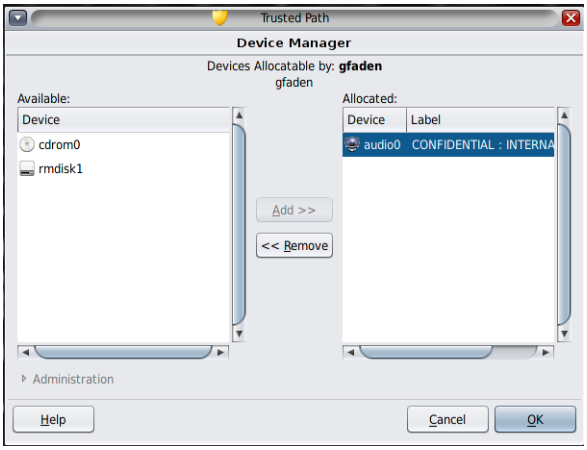
7 **要保存更改，请单击 "OK"（确定）。**

▼ 如何在 Trusted Extensions 中撤销或回收设备

如果某个设备没有在 "Device Manager"（设备管理器）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 "Administration"（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 Manager"（设备管理器）。**

▼ 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 Manager"（设备管理器）中，单击 "Administration"（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 103 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 21–1 **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。

安全管理员在设备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 Properties"（设备属性）对话框中，指定脚本的完整路径。
   a. 打开 "Device Manager"（设备管理器）。
   b. 单击 "Administration"（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 261 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 264 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 264 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 21–1。要创建并使用新授权，请参见示例 21–3。

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. **可选为每一个新的设备授权创建帮助文件。**
   帮助文件为 HTML 格式。命名约定为 *AuthName*`.html`，如 `DeviceAllocateCD.html` 中所示。
2. **创建设备授权。**

```
$ auths add -t "Authorization description" -h /full/path/to/helpfile.html authorization-name
```

3 **将新授权添加到相应的权限配置文件。**

```
$ profiles rights-profile
profiles:rights-profile > add auths="authorization-name"...
```

4 **将配置文件指定给用户和角色。**

```
# usermod -P "rights-profile" username
# rolemod -P "rights-profile" rolename
```

5 **使用授权来限制对选定设备的访问。**

在 "Device Manager"（设备管理器）中，将新授权添加到所需授权列表中。有关过程，请参见第 264 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 21–2 创建细粒度设备授权

在此示例中，NewCo 的安全管理员需要为公司构建细粒度设备授权。

首先，管理员将创建以下帮助文件：

```
Newco.html
NewcoDevAllocateCDVD.html
NewcoDevAllocateUSB.html
```

接下来，管理员将创建一个模板帮助文件，可以基于该文件复制其他帮助文件，然后进行修改。

```
<HTML>
-- Copyright 2012 Newco.  All rights reserved.
-- NewcoDevAllocateCDVD.html
-->
<HEAD>
        <TITLE>Newco Allocate CD or DVD Authorization</TITLE>
</HEAD>
<BODY>
The com.newco.dev.allocate.cdvd authorization enables you to allocate the
CD drive on your system for your exclusive use.
<p>
The use of this authorization by a user other than the authorized account
is a security violation.
<p>
</BODY>
</HTML>
```

创建帮助文件后，管理员使用 `auths` 命令创建每个设备授权。由于授权应用于整个公司，因此管理员将授权置于 LDAP 系统信息库中。该命令包含到帮助文件的路径名。

管理员创建了两个设备授权和一个 Newco 授权标题。

- 一个授权用于授权用户分配 CD-ROM 或 DVD 驱动器。

```
# auths add -S ldap -t "Allocate CD or DVD" \
-h /docs/helps/NewcoDevAllocateCDVD.html com.newco.dev.allocate.cdvd
```

- 一个授权用于授权用户分配 USB 设备。

```
# auths add -S ldap -t "Allocate USB" \
-h /docs/helps/NewcoDevAllocateUSB.html com.newco.dev.allocate.usb
```

- Newco 授权标题标识所有 Newco 授权。

```
# auths add -S ldap -t "Newco Auth Header" \
-h /docs/helps/Newco.html com.newco
```

示例 21–3 创建并指定可信路径和非可信路径设备授权

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 和 DVD 分配。安全管理员创建了 `com.newco.dev.allocate.cdvd.local` 授权。该授权适用于使用可信路径分配的 CD-ROM 和 DVD 驱动器。`com.newco.dev.allocate.cdvd.remote` 授权适用于少数用户，他们可以在可信路径外分配 CD-ROM 或 DVD 驱动器。

安全管理员创建帮助文件、将设备授权添加到 `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。`root` 角色将配置文件指定给允许分配设备的用户。

- 以下命令将设备授权添加到 `auth_attr` 数据库：

```
$ auths add -S ldap -t "Allocate Local DVD or CD" \
-h /docs/helps/NewcoDevAllocateCDVDLocal.html \
com.newco.dev.allocate.cdvd.local
$ auths add -S ldap -t "Allocate Remote DVD or CD" \
-h /docs/helps/NewcoDevAllocateCDVDRemote.html \
com.newco.dev.allocate.cdvd.remote
```

- 下面显示 "Device Manager"（设备管理器）分配：

  CD-ROM 驱动器的本地分配受可信路径保护。

```
Device Name: cdrom_0
For Allocations From: Trusted Path
Allocatable By: Authorized Users
Authorizations: com.newco.dev.allocate.cdvd.local
```

  远程分配不受可信路径保护，因此，远程用户必须可信。最后，管理员将仅为两个角色授权远程分配。

```
Device Name: cdrom_0
For Allocations From: Non-Trusted Path
Allocatable By: Authorized Users
Authorizations: com.newco.dev.allocate.cdvd.remote
```

- 以下命令为这些授权创建 Newco 权限配置文件，并将授权添加到配置文件：

```
$ profiles -S ldap "Remote Allocator"
profiles:Remote Allocator > set desc="Allocate Remote CDs and DVDs"
profiles:Remote Allocator > set help="/docs/helps/NewcoDevRemoteCDVD.html"
profiles:Remote Allocator > add auths="com.newco.dev.allocate.cdvd.remote"
profiles:Remote Allocator > end
profiles:Remote Allocator > exit
```

```
$ profiles -S ldap "Local Only Allocator"
profiles:Local Only Allocator > set desc="Allocate Local CDs and DVDs"
profiles:Local Only Allocator > set help="/docs/helps/NewcoDevLocalCDVD.html"
profiles:Local Only Allocator > add auths="com.newco.dev.allocate.cdvd.local"
profiles:Local Only Allocator > end
profiles:Local Only Allocator > exit
```

- 以下命令将权限配置文件指定给授权的用户。root 角色指定配置文件。在该站点上，仅授权角色可远程分配外围设备。

```
# usermod -P "Local Only Allocator" jdoe
# usermod -P "Local Only Allocator" kdoe

# rolemod -P "Remote Allocator" secadmin
# rolemod -P "Remote Allocator" sysadmin
```

▼ 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 261 页中的“如何创建新的设备授权”中所述。

1. **执行第 255 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 "Administration"（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 135 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。**

  有关逐步操作过程，请参见《Oracle Solaris 11.1 管理：安全服务》中的“如何更改用户的安全属性”。

  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 21–2 显示如何指定授权。

◆ ◆ ◆ 第 22 章

22 Trusted Extensions 审计（概述）

本章介绍了 Trusted Extensions 提供的新增审计功能。

- 第 267 页中的 “Trusted Extensions 和审计”
- 第 267 页中的 “Trusted Extensions 中的按角色审计管理”
- 第 268 页中的 “Trusted Extensions 审计参考”

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。
- 不建议按区域审计，因为在有标签区域中需要 `root` 帐户。
- 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。系统管理员计划审计文件的磁盘空间要求，创建审计管理服务器，并检查审计日志。

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《Oracle Solaris 11.1 管理：安全服务》中的第 27 章 “规划审计”。

角色的审计管理职责

在 Trusted Extensions 中，审计是各个角色的职责。

- `root` 角色为用户和权限配置文件指定审计标志，并编辑系统文件（如 `audit_warn` 脚本）。
- "System Administrator"（系统管理员）角色设置审计存储的磁盘和网络。该角色还可检查审计记录。
- "Security Administrator"（安全管理员）角色决定审计内容并配置审计。初始设置团队通过完成第 62 页中的“如何在 Trusted Extensions 中创建 "Security Administrator"（安全管理员）角色”创建了该角色。

注 – 系统仅记录安全管理员已预选的审计类中的事件。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

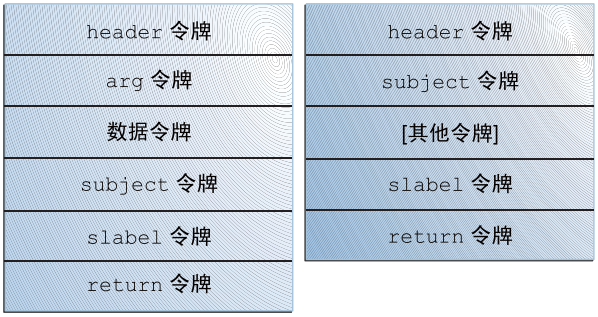
在 Trusted Extensions 中配置和管理审计的过程与 Oracle Solaris 中的过程仅稍有不同。在 Trusted Extensions 中，审计配置在全局区域中执行。由于未配置按区域审计，因此在全局区域和有标签区域中按相同的方式对用户操作执行审计。每个审计事件的标签都包含在审计记录中。

- 安全管理员可选择特定于 Trusted Extensions 的审计策略 `windata_down` 和 `windata_up`。
- 检查审计记录时，系统管理员可按标签选择审计记录。有关更多信息，请参见 `auditreduce(1M)` 手册页。

Trusted Extensions 审计参考

Trusted Extensions 软件向 Oracle Solaris 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 22–1 有标签系统中的典型审计记录结构



Trusted Extensions 审计类

Trusted Extensions 向 Oracle Solaris 中添加 X 窗口审计类。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。

X 服务器审计事件根据以下标准映射到这些类中：

- **xa** – 该类审计对 X 服务器的访问权限，即 X 客户机连接和 X 客户机断开连接。
- **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 的审计令牌。audit.log(4) 手册页中列出了令牌定义。

表 22–1 Trusted Extensions 审计令牌

令牌名称	说明
第 270 页中的 “label 令牌”	敏感标签
第 270 页中的 “xatom 令牌”	X 窗口原子标识
第 270 页中的 “xcolormap 令牌”	X 窗口颜色信息
第 271 页中的 “xcursor 令牌”	X 窗口光标信息
第 271 页中的 “xfont 令牌”	X 窗口字体信息
第 271 页中的 “xgc 令牌”	X 窗口图形上下文信息
第 271 页中的 “xpixmap 令牌”	X 窗口像素映射信息
第 271 页中的 “xproperty 令牌”	X 窗口属性信息
第 271 页中的 “xselect 令牌”	X 窗口数据信息
第 272 页中的 “xwindow 令牌”	X 窗口的窗口信息

label 令牌

label 令牌包含一个敏感标签。

label 令牌由 praudit -x 命令显示如下：

```
<sensitivity_label>ADMIN_LOW</sensitivity_label>
```

xatom 令牌

xatom 令牌标识 X 原子。

xatom 令牌由 praudit 命令显示如下：

```
X atom,_DT_SAVE_MODE
```

xcolormap 令牌

xcolormap 令牌包含有关色彩表使用的信息，包括 X 服务器标识符和创建者的用户 ID。

xcolormap 令牌由 praudit 命令显示如下：

```
<X_colormap xid="0x08c00005" xcreator-uid="srv"/>
```

xcursor 令牌

xcursor 令牌包含有关光标使用的信息，包括 X 服务器标识符和创建者的用户 ID。

xcursor 令牌由 praudit 命令显示如下：

```
X cursor,0x0f400006,srv
```

xfont 令牌

xfont 令牌包含有关字体使用的信息，包括 X 服务器标识符和创建者的用户 ID。

xfont 令牌由 praudit 命令显示如下：

```
<X_font xid="0x08c00001" xcreator-uid="srv"/>
```

xgc 令牌

xgc 令牌包含有关 X 窗口的图形上下文的信息。

xgc 令牌由 praudit 命令显示如下：

```
Xgraphic context,0x002f2ca0,srv

<X_graphic_context xid="0x30002804" xcreator-uid="srv"/>
```

xpixmap 令牌

xpixmap 令牌包含有关像素映射使用的信息，包括 X 服务器标识符和创建者的用户 ID。

xpixmap 令牌由 praudit -x 命令显示如下：

```
<X_pixmap xid="0x2f002004" xcreator-uid="srv"/>
```

xproperty 令牌

xproperty 令牌包含有关窗口的各种属性的信息，如 X 服务器标识符、创建者的用户 ID 以及原子标识符。

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。

xselect 令牌由 praudit 命令显示如下：

```
X selection,entryfield,halogen
```

xwindow 令牌

xwindow 令牌标识 X 服务器和创建者的用户 ID。

xwindow 令牌由 praudit 命令显示如下：

```
<X_window xid="0x07400001" xcreator-uid="srv"/>
```

Trusted Extensions 审计策略选项

Trusted Extensions 向现有的审计策略选项中添加了两个窗口审计策略选项。

```
$ 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 auditrecord 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。
- auditrecord 命令包括了 Trusted Extensions 审计事件。

◆ ◆ ◆ 第 23 章

23 Trusted Extensions 中的软件管理

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

可添加到 Oracle Solaris 系统的任何软件，都可添加到配置有 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。

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。但是，您可以通过在有标签区域中运行 `pkg` 命令在该区域中安装软件包。如果您进行此操作，必须确保该区域可以处理管理帐户和口令提示。有关讨论，请参见第 30 页中的 “限制到有标签区域的应用程序”。有关软件包和区域的详细信息，请参见《Oracle Solaris 11.1 管理：Oracle Solaris Zones、Oracle Solaris 10 Zones 和资源管理》中的第 24 章 “关于安装了区域的 Oracle Solaris 11.1 系统上的自动安装和软件包”。

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 软件的安全机制

Trusted Extensions 使用与 Oracle Solaris 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《Oracle Solaris 11.1 管理：安全服务》中的“RBAC 元素和基本概念”。另请参见 `auth_attr(4)` 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《Oracle Solaris 11.1 管理：安全服务》中的第 8 章 “使用角色和特权（概述）”。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《Oracle Solaris 11.1 管理：Oracle Solaris Zones、Oracle Solaris 10 Zones 和资源管理》中的“使用 ppriv 实用程序”。
- **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《Oracle Solaris 11.1 管理：安全服务》中的“RBAC 权限配置文件”。
- **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 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 11 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。

◆ ◆ ◆ 附 录 A

站点安全策略

本附录讨论了站点安全策略问题，并推荐了用于进一步了解相关信息的参考书籍和 Web 站点：

- 第 278 页中的 “站点安全策略和 Trusted Extensions”
- 第 278 页中的 “计算机安全建议”
- 第 279 页中的 “物理安全建议”
- 第 280 页中的 “人员安全建议”
- 第 280 页中的 “常见安全违规”
- 第 281 页中的 “其他安全参考信息”

创建和管理安全策略

每个 Trusted Extensions 站点都是唯一的，并且必须确定自己的安全策略。在创建和管理安全策略时需执行下列任务。

- 成立安全团队。安全团队需要包括来自最高管理层、人事管理人员、计算机系统管理人员与管理员以及装置管理人员的代表。该团队必须审核 Trusted Extensions 管理员的策略和规程，并建议适用于所有系统用户的一般安全策略。
- 向管理和行政管理人员进行有关站点安全策略的培训。参与站点的管理和行政管理的所有人员都必须接受有关安全策略的培训。安全策略绝对不可供一般用户使用，因为此策略信息直接关系到计算机系统的安全性。
- 对用户进行 Trusted Extensions 软件和安全策略方面的培训。所有用户都必须熟悉《Trusted Extensions 用户指南》。因为用户通常是第一个知道系统运行不正常的人，所以用户必须了解系统并将所有问题报告给系统管理员。安全的环境要求用户在发现任何下列问题时立即通知系统管理员：
  - 在每个会话开始时报告的上次登录时间与实际不符。
  - 文件数据发生异常更改
  - 人可阅读的打印输出材料丢失或被盗
  - 无法执行某个用户功能

- 执行安全策略。如果没有遵守和执行安全策略，则配置有 Trusted Extensions 的系统中包含的数据就不安全。必须设定规程来记录所有问题和已采取的用来解决事故的措施。
- 定期审核安全策略。安全团队必须定期审核安全策略以及自从上次审核之后发生的所有事故。然后可调整策略以提高安全性。

站点安全策略和 Trusted Extensions

安全管理员必须基于站点的安全策略设计 Trusted Extensions 网络。安全策略决定了配置决策，例如：

- 对于所有用户，对哪些类别的事件进行何种程度的审计
- 对于各个角色中的用户，对哪些类型的事件进行何种程度的审计
- 如何管理、归档和审核审计数据
- 在系统中使用哪些标签以及一般用户是否可以查看 `ADMIN_LOW` 和 `ADMIN_HIGH` 标签
- 将哪些用户安全许可指定给个人
- 哪些一般用户可以分配哪些设备（如果有）
- 为系统、打印机和其他设备定义哪些标签
- 是否是在可评估配置中使用 Trusted Extensions

计算机安全建议

在为站点制定安全策略时，请考虑以下指导准则列表。

- 将配置有 Trusted Extensions 的系统的最大标签指定为不大于在站点上执行的工作的最大安全级别。
- 手动将系统重新引导、电源故障和关机事件记录到站点日志中。
- 记录文件系统损坏并分析所有受影响的文件是否存在可能的安全策略违规。
- 将操作手册和管理员文档限制为仅可供确实需要访问这些信息的个人使用。
- 报告并记录任何 Trusted Extensions 软件的异常行为，并确定原因。
- 如果可能，至少指定两个人来管理配置有 Trusted Extensions 的系统。向一个人指定安全相关决策方面的安全管理员授权。向另一个人指定系统管理任务方面的安全管理员授权。
- 建立常规备份例程。
- 只向需要授权且可以信任他们能正确使用授权的人指定授权。
- 只有在程序需要特权来执行其工作、并且经仔细审查后证明这些程序对特权的使用值得信任，才向其指定特权。审核现有 Trusted Extensions 程序上的特权，并将其做法作为在新程序上设置特权的指南。
- 定期审核并分析审计信息。调查所有不正常的事件，以确定导致事件的原因。

- 最大程度地减少管理 ID 的数量。
- 最大程度地减少 setuid 和 setgid 程序的数量。使用授权、特权和角色来执行程序并防止滥用。
- 确保管理员定期验证一般用户拥有有效的登录 shell。
- 确保管理员必须定期验证一般用户拥有有效的用户 ID 值而非系统管理 ID 值。

物理安全建议

在为站点制定安全策略时，请考虑以下指导准则列表。

- 限制对配置有 Trusted Extensions 的系统的访问。最安全的位置一般是不处于一楼的内部房间。
- 监视并记录对配置有 Trusted Extensions 的系统的访问。
- 将计算机设备固定在大型物体（如桌椅）上以防被盗。如果设备固定在木制物件上，请通过添加金属板增强物体的强度。
- 考虑使用可移除存储介质来存储敏感信息。当可移除介质未在使用中时，请锁定所有这些介质。
- 将系统备份和归档存储在系统位置之外的其他安全位置。
- 采用与限制对系统的访问相同的方式来限制对备份和归档介质的物理访问。
- 在计算机装置中安装高温报警器，以在温度超出制造商规范的范围时进行指示。建议范围为 10°C 到 32°C（50°F 到 90°F）。
- 在计算机装置中安装漏水报警器，以在地板上、底层地板中以及天花板中出现漏水时进行指示。
- 安装烟雾报警器以指示起火情况，并安装灭火系统。
- 安装湿度报警器以指示湿度过高或者过低情况。
- 如果计算机没有安装 TEMPEST 屏蔽层，考虑安装一个。TEMPEST 屏蔽层可能适合用于装置的墙面、地板和天花板。
- 只允许由获得认证的技师打开和关闭 TEMPEST 设备以确保该设备屏蔽电磁辐射的能力。
- 检查是否存在允许进入计算机设备所在装置或房间的物理缺口。检查活动式地板下、吊顶天花板中、房顶通风设备中以及原始物体与二次增建物之间的邻墙中是否有开口。
- 严禁在计算机装置内或计算机设备旁边进食、饮水和吸烟。划定出可以在其中进行这些活动而不会对计算机设备造成威胁的专门区域。
- 保护计算机装置的建筑图和图表。
- 限制对计算机装置的建筑图、地板地图和照片的使用。

人员安全建议

在为站点制定安全策略时，请考虑以下指导准则列表。

- 在人员到达安全站点时和离开安全站点前对软件包、文档和存储介质进行检查。
- 始终要求所有职员和访客出示个人身份胸卡。
- 使用难以复制或伪造的个人身份胸卡。
- 划定禁止访客进入的区域，并将这些区域清晰标记出来。
- 始终陪同访客。

常见安全违规

由于没有任何计算机是完全安全的，所以计算机装置是否安全取决于使用它的人。谨慎的用户或其他设备可轻松避免大部分违反安全的操作。不过，以下列表提供了可能发生的问题的示例：

- 用户将口令告诉了对系统不应当具有访问权的其他个人。
- 用户写下了口令，并将口令遗失或留在了不安全的位置。
- 用户将自己的口令设置为很容易被猜出的字词或容易被猜出的名字。
- 用户看到其他用户键入口令并记住了口令。
- 未经授权的用户拆除、更换或以物理方式损坏硬件。
- 用户使其系统处于无人看管状态且没有锁定屏幕。
- 用户更改文件的权限来允许其他用户阅读文件。
- 用户更改文件的标签来允许其他用户阅读文件。
- 用户没有用碎纸机碎掉敏感的硬拷贝文档就将它们丢弃，或将敏感的硬拷贝文档留在不安全的位置。
- 用户没有锁好出入门。
- 用户丢失了钥匙。
- 用户没有锁定可移除的存储介质。
- 计算机屏幕可通过外窗被看到。
- 网络电缆被搭接。
- 电子窃听设备捕获到计算机设备发射出的信号。
- 停电、电涌和电力激增破坏了数据。
- 地震、洪水、龙卷风、飓风和闪电破坏了数据。
- 外部电磁辐射干扰（例如太阳黑子活动）扰乱了文件。

其他安全参考信息

政府出版物详细介绍了与计算机安全相关的标准、政策、方法和术语。此处列出的其他出版物是适用于 UNIX 系统的系统管理员的指南，对于透彻了解 UNIX 安全问题和解决方案十分有用。

Web 上也提供了很多资源。需要特别指出的是，CERT (`http://www.cert.org`) Web 站点向公司和用户发出关于软件中的安全漏洞的警报。SANS 协会 (`http://www.sans.org/`) 提供培训、大量术语词汇表和 Internet 上排名靠前的威胁的更新列表。

美国政府出版物

美国政府在 Web 上提供了它的许多出版物。美国国家标准与技术局 (National Institute of Standards and Technology, NIST) 的计算机安全资源中心 (CSRC, Computer Security Resource Center) 发布关于计算机安全的文章。以下是可以从 NIST 站点 (`http://csrc.nist.gov/index.html`) 下载的出版物样例。

- 《计算机安全介绍：NIST 手册》。SP 800-12，1995 年 10 月。
- 《Standard Security Label for Information Transfer》。FIPS-188，1994 年 9 月。
- 由 Marianne Swanson 和 Barbara Guttman 合著的《Generally Accepted Principles and Practices for Securing Information Technology Systems》。SP 800-14，1996 年 9 月。
- 由 Miles Tracy、Wayne Jensen 和 Scott Bisker 合著的《Guidelines on Electronic Mail Security》。SP 800-45，2002 年 9 月。E.7 部分涉及了安全地为邮件配置 LDAP。
- 由 Mark Wilson 和 Joan Hash 合著的《Building an Information Technology Security Awareness and Training Program》。SP 800-61，2004 年 1 月。包括了一个非常有用的词汇表。
- 由 Karen Scarfone、Tim Grance 和 Kelly Masone 合著的《Computer Security Incident Handling Guide》。SP 800-50，2002 年 9 月。E.7 部分涉及了安全地为邮件配置 LDAP。
- 由 Karen Scarfone、Wayne Jansen 和 Miles Tracy 合著的《Guide to General Server Security》（通用服务器安全指南）。SP 800-123，2008 年 7 月。
- 由 Murugiah Souppaya、John Wack 和 Karen Kent 合著的《Security Configuration Checklists Program for IT Products》（IT 产品安全配置核对表计划）。SP 800-70，2005 年 5 月。

UNIX 安全出版物

Oracle Corporation 安全工程师《Solaris 10 Security Essentials》Prentice Hall，2009。

由 John Chirillo 和 Edgar Danielyan 合著的《Sun Certified Security Administration for Solaris 9 & 10 Study Guide》。McGraw-Hill/Osborne 出版，2005。

由 Simson Garfinkel、Gene Spafford 和 Alan Schwartz 合著的《Practical UNIX and Internet Security, 3rd Edition》。O'Reilly & Associates, Inc, Sebastopol, CA 出版，2006。

一般计算机安全出版物

由 Glenn M. Brunette 和 Christoph L. 合著的《Toward Systemically Secure IT Architectures》。Oracle Corporation 出版，2005 年 6 月。

由 Charlie Kaufman、Radia Perlman 和 Mike Speciner 合著的《Network Security: Private Communication in a Public World, 2nd Edition》。Prentice-Hall 出版，2002。

由 Charles P. Pfleeger 和 Shari Lawrence Pfleeger 合著的《Security in Computing》。Prentice Hall PTR 出版，2006。

《Privacy for Pragmatists: A Privacy Practitioner's Guide to Sustainable Compliance》。Oracle Corporation 出版，2005 年 8 月。

由 Mark Rhodes-Ousley、Roberta Bragg 和 Keith Strassberg 合著的《Network Security: The Complete Reference》。McGraw-Hill/Osborne 出版，2004。

由 Cliff Stoll 编著的《The Cuckoo's Egg》。Doubleday 出版，1989。

一般 UNIX 出版物

由 Maurice J. Bach 编著的《The Design of the UNIX Operating System》。Prentice Hall, Englewood Cliffs, NJ 出版，1986。

由 Evi Nemeth、Garth Snyder 和 Scott Seebas 合著的《UNIX System Administration Handbook》。Prentice Hall, Englewood Cliffs, NJ 出版，1989。

◆ ◆ ◆ 附 录 B

Trusted Extensions 的配置核对表

此核对表提供了 Trusted Extensions 的主要配置任务的概述。并在主要任务中列出了更小的任务。核对表不能代替本指南中的步骤。

用于配置 Trusted Extensions 的核对表

以下汇总了在站点上启用和配置 Trusted Extensions 所需执行的操作。其中交叉引用了别处介绍的任务。

1. 阅读。
   - 阅读第 2 部分的前五章。
   - 了解站点安全要求。
   - 阅读第 278 页中的 “站点安全策略和 Trusted Extensions”。
2. 准备。
   - 确定 `root` 口令。
   - 确定 PROM 或 BIOS 安全级别。
   - 确定 PROM 或 BIOS 口令。
   - 确定是否允许连接外围设备。
   - 确定是否允许访问远程打印机。
   - 确定是否允许访问无标签的网络。
3. 启用 Trusted Extensions。请参见第 43 页中的 “启用 Trusted Extensions 服务并登录”。
   a. 安装 Oracle Solaris OS。
   b. 装入 Trusted Extensions 软件包。
   c. 启用 Trusted Extensions 服务 `svc:/system/labeld`。
   d. 重新引导。
4. （可选）定制全局区域。请参见第 47 页中的 “在 Trusted Extensions 中设置全局区域”。
   a. 如果使用不同于 `1` 的 DOI，请在 `/etc/system` 文件和每个安全模板中设置 DOI。
   b. 检验并安装站点的 `label_encodings` 文件。

c. 重新引导。

5. 添加有标签区域。请参见第 51 页中的 “创建有标签区域”。

   a. 自动配置两个有标签区域。
   b. 手动配置有标签区域。
   c. 创建有标签工作区。

6. 配置 LDAP 命名服务。请参见第 5 章，为 Trusted Extensions 配置 LDAP（任务）。

   创建一个 Trusted Extensions 代理服务器或 Trusted Extensions LDAP 服务器。文件命名服务无需配置。

7. 为全局区域和有标签区域配置接口和路由。请参见第 55 页中的 “在 Trusted Extensions 中配置网络接口”。

8. 配置网络。请参见第 193 页中的 “为主机和网络设置标签（任务）”。

   - 标识单标签主机和有限范围主机。
   - 确定要应用于来自无标签主机的传入数据的标签。
   - 定制安全模板。
   - 将各个主机指定给安全模板。
   - 为安全模板指定子网。

9. 执行进一步配置。

   a. 为 LDAP 配置网络连接。

      - 为所有安全模板中的 `cipso` 主机类型指定 LDAP 服务器或代理服务器。
      - 为所有安全模板中的 `cipso` 主机类型指定 LDAP 客户机。
      - 使本地系统成为 LDAP 服务器的客户机。

   b. 配置本地用户和本地管理角色。请参见第 61 页中的 “在 Trusted Extensions 中创建角色和用户”。

      - 创建 "Security Administrator"（安全管理员）角色。
      - 创建一个可以承担 "Security Administrator"（安全管理员）角色的本地用户。
      - 创建其他角色，以及要承担这些角色的其他本地用户（根据具体情况确定是否创建）。

   c. 在用户可以访问的每个标签下创建起始目录。请参见第 67 页中的 “在 Trusted Extensions 中创建集中起始目录”。

      - 在 NFS 服务器上创建起始目录。
      - 创建可加密的本地 ZFS 起始目录。
      - （可选的）阻止用户从其较低级别的起始目录进行读取。

   d. 配置打印。请参见第 236 页中的 “配置有标签打印（任务列表）”。

   e. 配置设备。请参见第 253 页中的 “在 Trusted Extensions 中操作设备（任务列表）”。

      i. 为角色指定 "Device Management"（设备管理）配置文件或 "System Administrator"（系统管理员）配置文件。

      ii. 要使设备可用，请执行以下操作之一：

- 逐个系统地使设备成为可分配的。
- 为选定的用户和角色指定 "Allocate Device"（分配设备）授权。

f. 配置 Oracle Solaris 功能。

- 配置审计。
- 配置系统安全值。
- 启用特定的 LDAP 客户机以管理 LDAP。
- 配置 LDAP 中的用户。
- 配置 LDAP 中的网络角色。

g. 挂载并共享文件系统。请参见第 14 章，在 Trusted Extensions 中管理和挂载文件。

◆ ◆ ◆ 附 录 C

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 D，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）。此脚本还提供用于网络选项、命名服务选项的菜单项，以及用于使全局区域成为现有 LDAP 服务器的客户机的菜单项。在 Oracle Solaris 11 发行版中，`txzonemgr -c` 命令将跳过用于创建前两个有标签区域的菜单。
Device Manager（设备管理器）	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。

	使用 `tgnome-selectlabel` 实用程序，可以定制标签生成器。请参见《Trusted Extensions Developer's Guide》中的"tgnome-selectlabel Utility"。
"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 (Login/Workspace) Password"（更改（登录/工作区）口令）菜单项。在 Trusted GNOME 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 104 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。有关所有 Trusted Extensions 接口的列表，请参见附录 D，Trusted Extensions 手册页列表。
配置文件	Trusted Extensions 添加了两个特权：`net_mac_aware` 和 `net_mlp`。有关使用 `net_mac_aware` 的信息，请参见第 167 页中的 "Trusted Extensions 中的 NFS 服务器和客户机配置"。
	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。
	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 向 `policy.conf` 数据库添加了字段。有关字段，请参见第 124 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 268 页中的 "Trusted Extensions 审计参考"。

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：

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。

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。

Trusted Extensions 中的受限选项

Trusted Extensions 缩小了 Oracle Solaris 配置选项的范围：

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。

非全局区域是有标签区域。用户在有标签区域中工作。

◆ ◆ ◆ 附 录 D

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 信息的手册页的说明。

- 第 291 页中的 “按字母顺序排列的 Trusted Extensions 手册页”
- 第 295 页中的 “Trusted Extensions 修改的 Oracle Solaris 手册页”

按字母顺序排列的 Trusted Extensions 手册页

以下手册页仅适用于配置有 Trusted Extensions 的系统。说明中包括一些链接，这些链接指向 Trusted Extensions 文档集中这些功能的示例或解释。

Trusted Extensions 手册页	用途和指向其他信息的链接
`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。 请参见第 255 页中的 “如何在 Trusted Extensions 中配置设备”。
`atohexlabel`(1M)	将人可阅读的标签转换为其内部的等效文本。 有关示例，请参见第 117 页中的 “如何获取标签的十六进制等效值”。
`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。

	有关示例，请参见《Trusted Extensions Label Administration》中的“How to Debug a label_encodings File”和示例 4–1。
fgetlabel(2)	获取文件的标签
getlabel(1)	显示所选文件或目录的标签。
	有关示例，请参见第 155 页中的 “如何显示挂载的文件的标签”。
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。
	《Trusted Extensions Developer’s Guide》中的“Acquiring a Sensitivity Label”
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
	有关示例，请参见第 118 页中的 “如何通过标签的十六进制形式获取可读标签”。
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 有关其用途的示例，请参见第 145 页中的 “如何登录和管理远程 Trusted Extensions 系统”。
plabel(1)	获取进程的标签
remove_allocatable(1M)	通过从设备分配数据库中删除设备项来阻止设备分配 有关示例，请参见第 255 页中的 “如何在 Trusted Extensions 中配置设备”。
sel_config(4)	是复制、剪切、粘贴和拖放操作的选择规则 请参见第 110 页中的 “更改数据的安全级别时的规则”。
setflabel(3TSOL)	将文件移动到具有相应敏感标签的区域
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。
str_to_label(3TSOL)	将人可阅读的字符串解析为标签
tncfg(1M)	管理可信网络数据库。用于管理可信网络的 txzonmgr GUI 的备用方法。list 子命令显示网络接口的安全特征。tncfg 提供比 tninfo 命令更完整的信息。 有关许多示例，请参见第 16 章，在 Trusted Extensions 中管理网络（任务）。
tnctl(1M)	配置 Trusted Extensions 网络参数。您也可以使用 tncfg 命令。 有关示例，请参见示例 12–1。
tnd(1M)	启用 LDAP 命名服务时执行可信网络守护进程。
tninfo(1M)	显示内核级的 Trusted Extensions 网络信息和统计信息。 第 217 页中的 “如何调试 Trusted Extensions 网络”。您也可以使用 tncfg 命令和 txzonemgr GUI。

	有关与 tncfg 命令的比较，请参见第 174 页中的 “如何解决 Trusted Extensions 中的挂载故障”。
trusted_extensions(5)	介绍 Trusted Extensions
txzonemgr(1M)	管理有标签区域和网络接口。使用命令行选项可自动创建两个区域。此命令接受配置文件作为输入，并可删除区域。txzonemgr 是 zenity (1) 脚本。 请参见第 51 页中的 “创建有标签区域”和第 216 页中的 “可信网络故障排除（任务列表）”。
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
tgnome-selectlabel 实用程序	用于创建标签生成器 GUI 有关更多信息，请参见《Trusted Extensions Developer’s Guide》中的“tgnome-selectlabel Utility”。
updatehome(1)	更新当前标签的起始目录副本和链接文件 请参见第 131 页中的 “如何在 Trusted Extensions 中为用户配置启动文件”。
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 修改和指向其他信息的链接
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。在 Trusted Extensions 中，一般用户不能使用此命令。 有关用户操作过程的信息，请参见《Trusted Extensions 用户指南》中的“如何在 Trusted Extensions 中分配设备”。
auditconfig(1M)	为有标签信息添加窗口策略、审计类、审计事件和审计令牌。
auditreduce(1M)	添加 `-l` 选项以按标签选择审计记录。 有关示例，请参见《Oracle Solaris 11.1 管理：安全服务》中的“如何从审计迹中选择审计事件”。
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。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。 有关更多信息，请参见第 168 页中的 “在 Trusted Extensions 中更改自动挂载程序”。
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。在 Trusted Extensions 中，一般用户不能使用此命令。

	有关用户操作过程的信息，请参见《Trusted Extensions 用户指南》中的“如何在 Trusted Extensions 中分配设备”。
device_clean(5)	在 Trusted Extensions 中在缺省情况下会调用
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
ikeadm(1M)	为有标签 IKE 进程添加调试标志 0x0400。
ike.config(4)	添加 label_aware 全局参数和三个阶段 1 转换关键字 single_label、multi_label 和 wire_label
in.iked(1M)	支持在全局区域中通过多级别 UDP 端口 500 和 4500 协商有标签安全关联。 另请参见 ike.config(4) 手册页。
ipadm(1M)	添加 all-zones 接口作为永久性属性值。 有关示例，请参见第 216 页中的 “如何检验系统的接口是否已启动”。
ipseckey(1M)	添加 label、outer-label 和 implicit-label 扩展。这些扩展将 Trusted Extensions 标签与在安全关联内传输的通信相关联。
is_system_labeled(3C)	确定系统是否配置有 Trusted Extensions
ldaplist(1)	在 LDAP 中添加 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。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。
netstat(1M)	添加 -R 选项，用以为套接字和路由表项显示扩展的安全属性。 有关示例，请参见第 174 页中的 “如何解决 Trusted Extensions 中的挂载故障”。
pf_key(7P)	将标签添加到 IPsec 安全关联 (security association, SA)
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。添加 -secattr 选项以显示路由的安全属性：cipso、doi、max_sl 和 min_sl。 有关示例，请参见第 174 页中的 “如何解决 Trusted Extensions 中的挂载故障”。
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
socket.h(3HEAD)	支持为无标签的对等方使用 SO_MAC_EXEMPT 选项
tar(1)	添加 -T 选项以归档和提取有标签的文件和目录。 请参见第 170 页中的 “如何在 Trusted Extensions 中备份文件”和第 171 页中的 “如何在 Trusted Extensions 中恢复文件”。
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)	添加特定于 Trusted Extensions 的用户安全属性：idletime、idlecmd、clearance 和 min_label 请参见第 31 页中的 “在 Trusted Extensions 中规划用户安全”。

词汇表

accreditation range（认可范围） 一类用户或资源的获得批准的一组敏感标签。一组有效标签。另请参见 system accreditation range（系统认可范围）和 user accreditation range（用户认可范围）。

administrative role（管理角色） 一种 role（角色），提供必需的授权、特权命令和可信路径 security attribute（安全属性），以允许该角色执行管理任务。角色执行 Oracle Solaris `root` 的一部分权能，例如备份或审计。

allocation（分配） 一种机制，用于控制对 device（设备）的访问。请参见 device allocation（设备分配）。

authorization（授权） 授予用户或角色执行某个操作的权限，如果未获得授权，安全策略将不允许执行该操作。授权是在权限配置文件中设置的。特定命令需要用户具备特定授权才能成功执行。

branded zone（标记区域） 在 Trusted Extensions 中，即有标签的非全局区域。更通俗地说，就是包含非本机操作环境的非全局区域。请参见 `brands(5)` 手册页。

CIPSO label（CIPSO 标签） 通用 IP 安全选项。CIPSO 是 Trusted Extensions 实施的标签标准。

classification（等级） clearance（安全许可）或 label（标签）的分层组件。等级表示有层次的安全性级别，例如 `TOP SECRET`（机密）或 `UNCLASSIFIED`（未分类）。

clearance（安全许可） 用户可工作的标签集合的上限。下限是由 security administrator（安全管理员）指定的 minimum label（最小标签）。安全许可可以是两种类型（会话安全许可或 user clearance（用户安全许可））之一。

client（客户机） 连接到网络的系统。

closed network（封闭式网络） 配置有 Trusted Extensions 的系统组成的网络。该网络与任何非 Trusted Extensions 主机分离。这种分离可能是物理的，其中没有网线扩展至 Trusted Extensions 网络之外。这种分离也可能是在软件中实施的，其中 Trusted Extensions 主机只能识别 Trusted Extensions 主机。来自网络之外的数据项将被限制于与 Trusted Extensions 主机连接的外围设备。与 open network（开放式网络）相对。

compartment（区间） label（标签）的一个无层次组件，与 classification（等级）组件结合使用以构成 clearance（安全许可）或 label（标签）。区间代表信息的集合，例如，将供工程部门或多学科项目团队使用。

.copy_files file（.copy_files 文件） 多标签系统上的可选设置文件。此文件包含一系列启动文件，例如 `.cshrc` 或 `.firefox`，用户环境或用户应用程序需要这些文件以使系统或应用程序正常运行。`.copy_files` 中列出的文件然后会被**复制**到较高级别标签的用户起始目录（如果创建了这些目录）。另请参见 .link_files file（.link_files 文件）。

DAC 请参见 discretionary access control（自主访问控制）。

device allocation（设备分配） 一种机制，用于保护可分配 device（设备）上的信息免受分配该设备的用户之外的任何人访问。在设备被取消分配之前，只有分配设备的用户可以访问与该设备相关的信息。要使用户可以分配某个设备，该用户必须已由 security administrator（安全管理员）授予了设备分配授权。

device（设备） 设备包括打印机、计算机、磁带机、软盘驱动器、CD-ROM 驱动器、DVD 驱动器、音频设备和内部伪终端设备。设备受 read-equal/write-equal MAC 策略约束。对可移除设备（例如 DVD 驱动器）的访问由 device allocation（设备分配）控制。

discretionary access control（自主访问控制） 文件或目录的所有者自主授予或拒绝的访问类型。Trusted Extensions 提供两种自主访问控制 (discretionary access control, DAC)，即 UNIX permission bits（权限位）和 ACL。

domain name（域名） 一组系统的标识。域名包括一系列用句点分隔的组件名称（例如：`example1.town.state.country.org`）。在一个域名中，越靠右的组件名称所标识的网域范畴越广（通常指远程区域）。

domain of interpretation, DOI（系统解释域） 在配置有 Trusted Extensions 的 Oracle Solaris 系统上，系统解释域用于区分可能定义了相似标签的不同 `label_encodings` 文件。DOI 是一组规则，可将网络包上的安全属性转换为按本地 `label_encodings` 文件表示这些安全属性。当系统具有相同的 DOI 时，它们将共享该规则集合，并可以转换有标签的网络包。

domain（域） Internet 命名分层结构的一部分。它代表本地网络上一组共享管理文件的系统。

evaluated configuration（评估配置） 在一个已由认证机构认定为符合特定标准的配置中运行的一个或多个 Trusted Extensions 主机。

Trusted Extensions 软件通过了通用标准 v2.3 [2005 年 8 月]（ISO 标准）、评估保证级 (Evaluation Assurance Level, EAL) 4 和许多保护框架的认证。

file system（文件系统） 文件和目录的集合，在设置到逻辑分层结构时，组成一组有条理的结构化信息。可以从本地 system（系统）或远程系统挂载文件系统。

GFI Government Furnished Information（政府提供的信息）。在本手册中，是指美国政府提供的 label_encodings file（label_encodings 文件）。要将 GFI 用于 Trusted Extensions 软件，必须将 Oracle 专用的 `LOCAL DEFINITIONS` 部分添加到 GFI 的末尾。有关详细信息，请参见《Trusted Extensions Label Administration》中的第 5 章 “Customizing the LOCAL DEFINITIONS Section (Tasks)”。

host name（主机名） 使网络上的其他系统能够识别某个 system（系统）的名称。此名称在给定域内的所有系统之间必须唯一。通常，域标识一个组织。主机名可以是字母、数字和减号 (–) 的任意组合，但不能以减号开头或结尾。

initial label（初始标签） 指定给用户或角色的 minimum label（最小标签），用户初始工作区的标签。初始标签是用户或角色可在其中工作的最低级别标签。

initial setup team（初始设置团队） 一个至少由两人组成的团队，他们一起监视 Trusted Extensions 软件的启用和配置。一名团队成员负责安全决策，另一名成员负责系统管理决策。

IP address（IP 地址）
Internet 协议地址。标识某个联网系统使其可通过 Internet 协议进行通信的唯一数字。在 IPv4 中，该地址由四个以句点分隔的数字组成。IP 地址的每一部分通常是一个 0 到 225 之间的数字。但第一个数字必须小于 224，最后一个数字不能是 0。

IP 地址在逻辑上分为两部分：网络和网络上的 system（系统），网络号类似于电话区号。相对于网络，系统编号类似于电话号码。

label configuration（标签配置）
Trusted Extensions 的单标签或多标签敏感标签安装选项。在大多数情况下，标签配置在您站点上的所有系统上都相同。

label_encodings file（label_encodings 文件）
在该文件中定义完整的 sensitivity label（敏感标签），比如，认可范围、标签视图、缺省标签可见性、缺省用户安全许可以及标签的其他各方面。

label range（标签范围）
指定给命令、区域和可分配设备的一组敏感标签。通过指定最大标签和最小标签来指定范围。对于命令，最小标签和最大标签限定可在其中执行命令的标签。不识别标签的远程主机将被指定单个 sensitivity label（敏感标签），就像 security administrator（安全管理员）想要限制为单个标签的任何其他主机一样。标签范围限定可在其中分配设备的标签，并限定使用设备时可在其中存储或处理信息的标签。

label relationships（标签关系）
在配置有 Trusted Extensions 的 Oracle Solaris 系统上，一个标签可以支配另一个标签、等同于另一个标签或与另一个标签不相交。例如，标签 `Top Secret` 可支配标签 `Secret`。对于具有相同 domain of interpretation, DOI（系统解释域）的两个系统，一个系统上的标签 `Top Secret` 等同于另一个系统上的标签 `Top Secret`。

label set（标签集合）
请参见 security label set（安全标签集合）。

labeled host（有标签主机）
一个 labeled system（有标签系统），属于由有标签系统组成的可信网络的一部分。

labeled system（有标签系统）
有标签系统是运行多级别操作系统（例如 Trusted Extensions 或启用了 MLS 的 SELinux）的系统。该系统可以发送和接收在包标头中标有通用 IP 安全选项 (Common IP Security Option, CIPSO) 标签的网络包。

labeled zone（有标签区域）
在配置有 Trusted Extensions 的 Oracle Solaris 系统上，会为每个区域指定一个标签。虽然会为全局区域添加标签，但**有标签区域**通常是指指定有标签的非全局区域。相比于 Oracle Solaris 系统上未配置标签的非全局区域，有标签区域有两个不同的特征。首先，有标签区域必须使用相同的用户 ID 和组 ID 池。第二，有标签区域可以共享 IP 地址。

label（标签）
指定给某个对象的安全标识符。标签基于该对象中信息应受到保护的级别。根据 security administrator（安全管理员）配置用户的方式，用户可以看到 sensitivity label（敏感标签），或者根本没有标签。标签在 label_encodings file（label_encodings 文件）中进行定义。

.link_files file（.link_files 文件）
多标签系统上的可选设置文件。此文件包含一系列启动文件，例如 `.cshrc` 或 `.firefox`，用户环境或用户应用程序需要这些文件以使系统或应用程序正常运行。 `.link_files` 中列出的文件然后会被**链接**到较高级别标签的用户起始目录（如果创建了这些目录）。另请参见 .copy_files file（.copy_files 文件）。

MAC
请参见 mandatory access control（强制访问控制）。

mandatory access control（强制访问控制） 这种访问控制基于文件、目录或 device（设备）的 sensitivity label（敏感标签）与正在尝试进行访问的进程的敏感标签的比较。当使用某个标签的进程尝试读取使用较低级别标签的某个文件时，适用 MAC 规则 read equal–read down。当使用某个标签的进程尝试写入使用另一个标签的目录时，适用 MAC 规则 write equal-read down。

minimum label（最小标签） 用户的敏感标签的下界和系统的敏感标签的下界。security administrator（安全管理员）指定用户的安全属性时设置的最小标签是用户首次登录时第一个工作区的敏感标签。security administrator（安全管理员）在 `label_encodings` 文件的最小标签字段指定的敏感标签设置系统的下界。

multilevel desktop（多级别桌面） 在配置有 Trusted Extensions 的 Oracle Solaris 系统上，用户可以从特定的标签运行桌面。如果用户被授予从多个标签工作的权限，则该用户可以创建单独的工作区以从各个标签工作。在此多级别桌面上，授权的用户可以在不同标签的窗口之间进行剪切和粘贴，从不同的标签接收邮件，以及在不同标签的工作区中查看和使用标记窗口。

multilevel port, MLP（多级别端口） 在配置有 Trusted Extensions 的 Oracle Solaris 系统上，MLP 用于在区域中提供多级别服务。缺省情况下，X 服务器是在全局区域中定义的多级别服务。MLP 是通过端口号和协议指定的。例如，多级别桌面中 X 服务器的 MLP 是通过 6000-6003 和 TCP 指定的。

naming service（命名服务） 一个分布式网络数据库，它包含网络上所有系统的关键系统信息，以便系统能够彼此通信。如果没有这样的服务，每个 system（系统）必须在本地 `/etc` 文件中维护各自的系统信息副本。

networked systems（联网系统） 通过硬件和软件相连的一组系统，有时称为局域网 (local area network, LAN)。系统联网时通常需要一个或多个服务器。

non-networked systems（非联网系统） 未连接到网络或不依赖于其他主机的计算机。

open network（开放式网络） 由 Trusted Extensions 主机组成的网络，以物理方式连接到其他网络，并使用 Trusted Extensions 软件与非 Trusted Extensions 主机进行通信。与 closed network（封闭式网络）相对。

outside the evaluated configuration（评估配置之外） 在已被证明能够满足 evaluated configuration（评估配置）标准的软件中配置了不满足安全标准的设置时，会将该软件描述为处于**评估配置之外**。

permission bits（权限位） 一种 discretionary access control（自主访问控制）类型，所有者指定一组数位来表示谁可以读取、写入或执行文件或目录。可为每个文件或目录指定三组不同的权限：一组适用于所有者，一组适用于所有者所在的组，一组适用于所有其他情况。

privilege（特权） 授予正在执行某个命令的进程的权力。完整权限集合描述了系统的全部特权（从基本权能到管理权能）。绕开 security policy（安全策略）的特权（例如在系统上设置时钟）可由站点的 security administrator（安全管理员）授予。

process（进程） 代表调用命令的用户执行命令的操作。进程会接收来自用户的许多安全属性，包括用户 ID (user ID, UID)、组 ID (group ID, GID)、补充组列表和用户的审计 ID (audit ID, AUID)。进程接收的安全属性包括可用于所执行命令的任何特权和当前工作区的 sensitivity label（敏感标签）。

profile shell（配置文件 shell） 识别安全属性（例如特权、授权和特殊 UID 及 GID）的特殊 shell。配置文件 shell 通常会将用户限定于执行较少的命令，但可以允许这些命令以更多的权限运行。配置文件 shell 是 trusted role（可信角色）的缺省 shell。

remote host（远程主机） 与本地系统不同的系统。远程主机可以是 unlabeled host（无标签主机）或 labeled host（有标签主机）。

rights profile（权限配置文件） 一种捆绑机制,适用于命令以及指定给这些可执行命令的安全属性。权限配置文件允许 Oracle Solaris 管理员控制谁可以执行哪些命令，以及控制这些命令执行时具有的属性。当用户登录时，指定给该用户的所有权限都将生效，用户可以访问其所有权限配置文件中指定的全部命令和授权。

role（角色） 角色与用户类似，只不过角色不能登录。通常，角色用于指定管理权能。角色会被限定于执行一组特定的命令和授权。请参见 administrative role（管理角色）。

security administrator（安全管理员） 必须对敏感信息进行保护的组织中，定义并强制实施站点的 security policy（安全策略）的人员。这些人员有权访问站点中所处理的所有信息。在软件中，会将安全管理员 administrative role（管理角色）指定给具有适当 clearance（安全许可）的一个或多个个人。这些管理员配置所有用户和主机的安全属性，以便软件可以强制实施站点的安全策略。与此对比，请参见 system administrator（系统管理员）。

security attribute（安全属性） 用于强制实施 Trusted Extensions security policy（安全策略）的属性。将会为 process（进程）、用户、区域、主机、可分配设备和其他对象指定各种安全属性集合。

security label set（安全标签集合） 为 tnrhtp database（tnrhtp 数据库）项指定一组独立的安全标签。指定给具有安全标签集合的模板的主机可以发送和接收与标签集合中任一标签匹配的包。

security policy（安全策略） Trusted Extensions 主机上，定义可以如何访问信息的 DAC、MAC 和标签设置规则集合。客户站点上，定义该站点上所处理信息敏感度的规则集合，以及用于保护信息免受未经授权的访问的措施。

security template（安全模板） `tnrhtp` 数据库中的一条记录，用于定义可访问 Trusted Extensions 网络的一类主机的安全属性。

sensitivity label（敏感标签） 指定给某个对象或过程的安全 label（标签）。该标签用于根据所含数据的安全级别来限定访问。

separation of duty（职责分离） 需要两个管理员或角色来创建和验证用户的安全策略。一个管理员或角色负责创建用户、用户起始目录和其他基本管理内容。另一个管理员或角色负责用户的安全属性，例如口令和标签范围。

system accreditation range（系统认可范围） 根据 security administrator（安全管理员）在 label_encodings file（label_encodings 文件）中定义的规则创建的所有有效标签的集合，以及在配置有 Trusted Extensions 的每个系统上使用的两个管理标签。这两个管理标签为 `ADMIN_LOW` 和 `ADMIN_HIGH`。

system administrator（系统管理员） Trusted Extensions 中，指定给负责执行标准系统管理任务（例如设置用户帐户的非安全相关部分）的用户的 trusted role（可信角色）。与此对比，请参见 security administrator（安全管理员）。

system（系统） 计算机的通用名称。安装后，网络上的系统通常称为主机。

tnrhdb database（tnrhdb 数据库） 可信网络远程主机数据库。此数据库向远程主机指定一组标签特征。该数据库可作为 `/etc/security/tsol/tnrhdb` 中的文件进行访问。

tnrhtp database（tnrhtp 数据库） 可信网络远程主机模板。此数据库定义可指定给远程主机的标签特征集合。该数据库也可作为 `/etc/security/tsol/tnrhtp` 中的文件进行访问。

Trusted Network databases（可信网络数据库） 可信网络远程主机模板 `tnrhtp` 和可信网络远程主机数据库 `tnrhdb` 一起定义可与 Trusted Extensions 通信的远程主机数据库。

trusted path（可信路径） 在配置有 Trusted Extensions 的 Oracle Solaris 系统上，可信路径是一种与系统交互时的可靠防篡改方式。可信路径用于确保管理功能不能受到威胁。必须受到保护的用户功能（例如更改口令）也使用可信路径。当可信路径处于活动状态时，桌面会显示防篡改指示器。

trusted role（可信角色） 请参见 administrative role（管理角色）。

trusted stripe（可信窗口条） 一个不能受到欺骗的区域。在 Trusted GNOME 中，可信窗口条位于顶部。可信窗口条提供有关窗口系统状态的可视化反馈：可信路径指示器和窗口 sensitivity label（敏感标签）。当敏感标签配置为不可供用户查看时，可信窗口将缩小为一个仅显示可信路径指示器的图标。

txzonemgr script（txzonemgr 脚本） `/usr/sbin/txzonemgr` 脚本提供一个用于管理有标签区域的简单 GUI。该脚本还提供用于网络选项的菜单项。`txzonemgr` 由 root 用户在全局区域中运行。

unlabeled host（无标签主机） 发送无标签网络包的联网系统，例如正在运行 Oracle Solaris OS 的系统。

unlabeled system（无标签系统） 对于配置有 Trusted Extensions 的 Oracle Solaris 系统，无标签系统是未在运行多级别操作系统（例如 Trusted Extensions 或启用了 MLS 的 SELinux）的系统。无标签系统不发送有标签的包。如果正在进行通信的 Trusted Extensions 系统向无标签系统指定了单个标签，则 Trusted Extensions 系统和无标签系统之间的网络通信将从该标签进行。无标签系统也称为“单级别系统”。

user accreditation range（用户认可范围） 一般用户可在 system（系统）中工作的所有可能的标签集合。站点的 security administrator（安全管理员）在 label_encodings file（label_encodings 文件）文件中指定范围。定义 system accreditation range（系统认可范围）的良构标签规则还会受到该文件的 `ACCREDITATION RANGE` 部分的值的限制：上界、下界、组合约束和其他限制。

user clearance（用户安全许可） 设置用户可随时在其中工作的标签集合的上界的 clearance（安全许可）指定的 security administrator（安全管理员）。在任何特定的登录会话期间，用户可以决定接受缺省值或者可以进一步限制该安全许可。

索引

数字和符号

"Allocate Device"（分配设备）授权，264–265, 265
"Assume Role"（承担角色）菜单项，114
"Audit Review"（审计检查）配置文件, 检查审计记录，268
"Change Password"（更改口令）菜单项
  说明，107
  用于更改 root 口令，115
"Change Workspace Label"（更改工作区标签）菜单项
  说明，107
"Configure Device Attributes"（配置设备属性）授权，265
"Device Manager"（设备管理器）, 由管理员使用，255–258
"Revoke or Reclaim Device"（撤销或回收设备）授权，264–265, 265
"Security Administrator"（安全管理员）角色
  保护不可分配的设备，259–260
  保障安全性，250
  创建，62–63
  管理用户，134–138
  配置设备，255–258
  启用公共系统中的无标签正文页面，131
"Selection Manager"（选择管理器）, 缺省配置，110–112
"System Administrator"（系统管理员）角色
  创建，63
  管理打印机，229
  回收设备，258–259
  检查审计记录，268
"Trusted Path"（可信路径）菜单, "Assume Role"（承担角色），114

A

ADMIN_HIGH 标签
  mslabel 和，165–166
  顶级管理标签，98
  多级别数据集和，163–164
  角色安全许可，63
  角色和，106
  全局区域进程和区域，151–152
  全局区域中挂载 NFS 的文件，162
  设备和，248
  未本地化，27
  正文页标签和，240
ADMIN_LOW 标签
  保护管理文件，109
ADMIN_LOW标签, 最低级别标签，98
ADMIN_LOW 标签
  挂载文件，164–165
  关于无标签系统挂载的限制，165
Allocate Device（分配设备）授权，135–136
atohexlabel 命令，117–118

C

-c 选项, txzonemgr 脚本，51–52
CD-ROM 驱动器, 访问，248
chk_encodings 命令，49
重新获得对桌面焦点的控制权，116–117

重新设置标签信息，137–138
重新引导
　激活标签，44–45
重新设置数据标签，消除 IO，72–74
重新引导
　允许登录到有标签区域，66–67
.copy_files 文件
　说明，126–127
　为用户设置，131–133

D

DAC，**请参见**自主访问控制 (discretionary access control, DAC)
/dev/kmem 内核映像文件，安全违规，275
device-clean 脚本，添加到设备，260–261
device-clean（设备清除）脚本，要求，249
DOI，远程主机模板，180
Downgrade DragNDrop or CutPaste Info（降级 DragNDrop 或 CutPaste 信息）授权，135–136
Downgrade File Label（降级文件标签）授权，135–136
dpadm 服务，81
DragNDrop or CutPaste without viewing contents（在不查看内容的情况下执行 DragNDrop 或 CutPaste）授权，135–136
dsadm 服务，81
dtsession 命令，运行 updatehome，126–127

E

/etc/default/kbd 文件，如何编辑，119–120
/etc/default/login 文件，如何编辑，119–120
/etc/default/passwd 文件，如何编辑，119–120
/etc/hosts 文件，195
/etc/security/policy.conf 文件
　缺省值，124
　如何编辑，119–120
　修改，130–131
/etc/security/tsol/label_encodings 文件，98
/etc/system 文件，针对 IPv6 CIPSO 网络修改，50

G

getmounts脚本，155

H

hextoalabel 命令，118–119

I

IDLECMD 关键字，更改缺省值，130–131
IDLETIME 关键字，更改缺省值，130–131
IKE，隧道模式下的标签，190
IP 地址
　0.0.0.0 主机地址，183
　可信网络中的回退机制，182
ipadm 命令，178
IPsec
　标签扩展，189
　具有 Trusted Extensions 标签，188–191
　可信交换的标签，188–189
　隧道模式下的标签，190
　有关标签扩展的保护，191
ipseckey 命令，178
IPv6
　/etc/system 文件中的项，50
　故障排除，50

K

kmem 内核映像文件，275

L

label_encodings 文件
　安装，48–49
　本地化，27
　检查，48–49
　内容，98
　认可范围的源，98
　修改，48–49
　有标签打印参考，231–235

label 审计令牌，270
labeld 服务
  禁用，76
  启用，43–44
LDAP
  Trusted Extensions 数据库，223
  故障排除，220–222
  管理命名服务，225–226
  规划，30
  启动代理服务器，226
  启动服务器，226
  适用于 Trusted Extensions 的命名服务，223–225
  停止代理服务器，226
  停止服务器，226
  显示条目，225
LDAP 服务器
  保护日志文件，82–83
  配置多级别端口，84
  配置命名服务，79–81
  收集信息，78–79
  为 Trusted Extensions 客户机创建代理，86–87
  为 Trusted Extensions 客户机配置代理，86–87
  在 Trusted Extensions 上安装，79–81
LDAP 配置
  NFS 服务器, 以及，78
  Sun Ray 服务器, 以及，78
  Trusted Extensions，78–85
  创建客户机，87–89
.link_files 文件
  说明，126–127
  为用户设置，131–133
LOFS, 在 Trusted Extensions 中挂载数据集，161–162

M

MAC, **请参见**强制访问控制 (mandatory access control, MAC)
MLP, **请参见**多级别端口 (multilevel port, MLP)
mlslabel 属性, ADMIN_HIGH 标签和，165–166

N

net_mac_aware特权，157–158
netstat 命令，178, 217
NFS, 在 Trusted Extensions 中挂载数据集，161–162
NFS 服务器, LDAP 服务器, 以及，78
NFS 挂载
  访问较低级别目录，167–169
  在全局和有标签区域中，164–166
nscd 守护进程, 添加到每个有标签区域，60–61

O

Oracle Directory Server Enterprise Edition, **请参见** LDAP 服务器
Oracle Solaris OS
  与 Trusted Extensions 的不同之处，94–95
  与 Trusted Extensions 的相似之处，93
  与 Trusted Extensions 审计的不同之处，267
  与 Trusted Extensions 审计的相似之处，267
Oracle Solaris 安装选项, 要求，39–40
Oracle Solaris 已安装的系统, Trusted Extensions 的要求，40–41

P

policy.conf 文件
  更改 Trusted Extensions 关键字，130–131
  更改缺省值，119–120
  缺省值，124
  如何编辑，130–131
Print without Banner（无标题打印）授权，135–136
Print without Label（无标签打印）授权，135–136
proc_info 特权, 从基本集中删除，131

R

Remote Login（远程登录）授权，135–136
roleadd 命令，62–63
root UID, 应用程序所必需的，274
root 的实际 UID, 应用程序所必需的，274
root 角色, 添加 device_clean 脚本，260–261
root 口令, Trusted Extensions 中的要求，40
route 命令，178

S

Security Administrator（安全管理员）角色
  创建 "Convenient Authorizations"（方便授权）权限配置文件，135–136
  为用户指定授权，135–136
sel_config 文件，112
Shutdown（关闭）授权，135–136
snoop 命令，178, 217
solaris.print.admin, 授权，235–236
solaris.print.list, 授权，235–236
solaris.print.nobanner, 授权，235–236
solaris.print.nobanner 授权，131
solaris.print.unlabeled, 授权，235–236
solaris.print.unlabeled 授权，131
Stop-A, 启用，119–120
Sun Ray 系统
  LDAP 服务器, 以及，78
  防止用户查看他人的进程，131
  客户机联系人的 0.0.0.0/32 地址，205
  启用客户机和服务器之间的初始联系，208
  文档的 Web 站点，36

T

调试, **请参见**故障排除
tncfg 命令
  创建多级别端口，210–212
  说明，178
  修改 DOI 值，50–51
tnchkdb命令, 说明，178
tnctl命令, 说明，178
tnd命令, 说明，178
tninfo 命令, 使用，220
tninfo命令, 说明，178
Trusted Extensions
  另请参见 Trusted Extensions 规划
  IPsec 保护，188–189
  管理的快速参考，287–289
  规划，25–33
  规划配置策略，32
  规划网络，28
  规划硬件，27–28
  禁用，76
  联网，175–191
Trusted Extensions（续）
  内存要求，28
  配置之前的结果，34
  启用，43–44
  手册页快速参考，291–297
  双角色配置策略，32
  添加，41
  显示远程访问，145
  与 Oracle Solaris OS 的不同之处，94–95
  与 Oracle Solaris OS 的相似之处，93
  与 Oracle Solaris 审计的不同之处，267
  与 Oracle Solaris 审计的相似之处，267
  与从 Oracle Solaris 管理员角度看的不同之处，34
  在启用之前做出决策，42–43
  准备，39–41, 42–43
Trusted Extensions 的审计令牌
  label 令牌，270
  xatom 令牌，270
  xcolormap 令牌，270
  xcursor 令牌，271
  xfont 令牌，271
  xgc 令牌，271
  xpixmap 令牌，271
  xproperty 令牌，271
  xselect 令牌，271–272
  xwindow 令牌，272
  列表，270–272
Trusted Extensions 的要求
  Oracle Solaris 安装选项，39–40
  Oracle Solaris 已安装的系统，40–41
Trusted Extensions 管理员入门（任务列表），113–114
Trusted Extensions 配置
  LDAP，78–85
  LDAP 的数据库，78–85
  初始过程，47–76
  初始设置团队的职责，39
  更改缺省 DOI 值，50–51
  故障排除，69–70
  任务分工，39
  任务列表，35–37
  通过评估的配置，26
  向 LDAP 服务器添加网络数据库，84–85
  有标签区域，51–55

Trusted Extensions 配置（续）
远程系统，139–147
重新引导以激活标签，44–45
Trusted Extensions 网络
对 CIPSO 包启用 IPv6，50
规划，28
删除特定于区域的 nscd 守护进程，61
添加特定于区域的 nscd 守护进程，60–61
Trusted Extensions 要求
Oracle Solaris 安装，39–40
Oracle Solaris 已安装的系统，40–41
root 口令，40
Trusted Extensions 中的常见任务（任务列表），115–120
Trusted Extensions 中的审计
X 审计类，269
参考，267–272
规划，31
角色，用于管理，267–268
其他审计策略，272
其他审计令牌，270–272
其他审计事件，269
任务，268
现有审计命令的新增项，272
与 Oracle Solaris 审计的不同之处，267
tsol_separator.ps 文件
定制有标签打印，231–235
可配置的值，234
tsoljdsselmgr 应用程序，110–112
txzonemgr 脚本，154
-c 选项，51–52

U

updatehome 命令，126–127
Upgrade DragNDrop or CutPaste Info（升级 DragNDrop 或 CutPaste 信息）授权，135–136
Upgrade File Label（升级文件标签）授权，135–136
useradd 命令，65–66
/usr/bin/tsoljdsselmgr 应用程序，110–112
/usr/lib/cups/filter/tsol_separator.ps 文件，231–235
/usr/local/scripts/getmounts脚本，155
/usr/sbin/txzonemgr 脚本，51–52, 101, 153, 154
/usr/share/gnome/sel_config 文件，112
utadm 命令，缺省的 Sun Ray 服务器配置，208

V

Vino，共享桌面，145

X

X 审计类，269
xatom 审计令牌，270
xcolormap 审计令牌，270
xcursor 审计令牌，271
xfont 审计令牌，271
xgc 审计令牌，271
xpixmap 审计令牌，271
xproperty 审计令牌，271
xselect 审计令牌，271–272
xwindow 审计令牌，272

Z

zenity 脚本，51–52
ZFS
从较高级别区域查看挂载的只读数据集，159
多级别数据集，72–74, 161–162
快速区域创建方法，29
添加数据集到有标签区域，158–159
在 Trusted Extensions 中挂载数据集，161–162
在有标签区域挂载具有读/写权限的数据集，158–159

安

安全
root 口令，40
出版物，281–282
初始设置团队，39
站点安全策略，277–282
安全标签集合，远程主机模板，180

安全策略
培训用户，107–108
审计，272
用户和设备，250
安全管理员, **请参见** "Security Administrator"（安全管理员）角色
安全管理员角色, 管理打印机安全，229
安全机制
Oracle Solaris，274
可扩展的，106
安全模板
请参见远程主机模板
安全属性，184
修改用户缺省值，130
远程主机的设置，196–198
在路由中使用，209
针对所有用户修改缺省值，130–131
安全信息
为 Trusted Extensions 规划，33
在打印输出上，231–235
安全许可, 标签概述，97
安全注意, 键组合，116–117
安装
`label_encodings` 文件，48–49
Oracle Directory Server Enterprise Edition，78–85
适用于 Trusted Extensions 的 Oracle Solaris OS，39–45

保

保护
不可分配的设备，259–260
带有标签的信息，99–100
较低级别标签的文件不被访问，157–158
任意主机访问的有标签主机，205–209
设备，102–103, 247–249
使设备不被远程分配，260
文件系统（通过使用非专有名称），171

备

备份, 安装之前备份以前的系统，33

本

本地化, 配置有标签的打印输出，234

编

编辑系统文件，119–120
编码文件, **请参见** `label_encodings` 文件

标

标记
打开标签，44–45
区域，52–54
标签
另请参见标签范围
"Change Workspace Label"（更改工作区标签）菜单项，107
IKE SA 的扩展，190
IPsec SA 的扩展，189
IPsec 交换，188–189
打印时没有页标签，245
等级组件，97
概述，97
故障排除，118–119
关系，97–98
规划，27
降级和升级，112
进程的，99–100
良构，99
描述的，96
配置标签更改所适用的规则，112
区间组件，97
确定等效文本，118–119
授予用户或角色更改数据标签的权限，137–138
隧道模式下的认可，190
为区域指定，52–54
显示有标签区域中文件系统的标签，155–156
以十六进制显示，117–118
用户进程的，99
远程主机模板中的缺省值，180
在打印输出上，231–235
在内部数据库中修复，118–119
支配关系，97–98

标签的支配关系，97–98
标签范围
  限制打印机标签范围，242–243
  限制远程访问，139–140
  在打印机上设置，248
  在帧缓存器上设置，248
标签扩展
  IKE 协商，190
  IPsec SA，189
标题页
  典型，231
  篇尾页的差别，231–232
  删除标签，245
  有标签的说明，231–232

不

不可分配的设备
  保护，259–260
  设置标签范围，248
不同之处
  Trusted Extensions 和 Oracle Solaris OS 之间，94–95
  Trusted Extensions 和 Oracle Solaris 审计之间，267
  扩展 Oracle Solaris 接口，288–289

查

查看，**请参见**访问
查看现有安全模板（任务），193–195
查找
  标签的十六进制等效值，117–118
  文本格式的标签等效值，118–119

差

差别，Trusted Extensions 中的管理接口，287–288
差异
  Trusted Extensions 中的缺省值，289
  Trusted Extensions 中的受限选项，289

承

承担，角色，114

程

程序，**请参见**应用程序

出

出版物，安全和 UNIX，281–282

初

初始设置团队，用于配置 Trusted Extensions 的核对表，283–285

创

创建
  LDAP 客户机，87–89
  Trusted Extensions 客户机的 LDAP 代理服务器，86–87
  角色，61–67
  可以承担角色的用户，63–66
  配置时或配置后的帐户，43
  起始目录，67–69，168
  起始目录服务器，67–68
  区域，51–55
  使用 `roleadd` 添加 LDAP 角色，63
  使用 `roleadd` 添加本地角色，62–63
  使用 `useradd` 创建本地用户，65–66
  有标签区域，51–55
  帐户，61–67
  针对设备的授权，261–264
创建有标签区域，51–55

磁

磁盘，访问，248

打

打印
- PostScript，235
- 本地化有标签的输出，234
- 本地语言，234
- 管理，229–236
- 国际化有标签的输出，234
- 和 label_encodings 文件，98
- 来自 Oracle Solaris 打印服务器的公共作业，244
- 没有带标签的标题页和篇尾页，135–136
- 没有页标签，135–136, 245
- 配置标签和文本，234
- 配置多级别有标签输出，237–238, 239
- 配置公共打印作业，244
- 配置有标签区域，239–240
- 使用 Oracle Solaris 打印服务器，244
- 授权，235–236
- 为 Oracle Solaris 打印服务器设置标签，244
- 为打印机客户机配置，240–242
- 限制标签范围，242–243
- 针对公共系统中无标签输出的授权，131
- 阻止输出上的标签，243–244

打印的输出, **请参见**打印
打印机, 设置标签范围，248
打印机输出, **请参见**打印
打印输出, **请参见**打印

代

代理服务器, 启动和停止 LDAP，226

单

单标签
- 登录，99
- 在区域中打印，239–240

导

导出, **请参见**共享
导入, 软件，273

登

登录
- 到起始目录服务器，68
- 使用 ssh 命令，145–147
- 通过角色，105–106
- 远程，141–143

等

等级标签组件，97
等效文本标签, 确定，118–119

定

定制
- label_encodings 文件，98
- 设备授权，264
- 无标签打印，243–245
- 用户帐户，129–134

多

多播包，176
多级别打印
- 配置，237–238, 239
- 由打印客户机访问，240–242

多级别端口 (multilevel port, MLP)
- NFSv3 MLP 的示例，211
- Web 代理 MLP 的示例，210–212
- 管理，211–212

多级别服务器, 规划，30
多级别挂载, NFS 协议版本，169–170
多级别数据集
- 创建，72–74
- 概述，166–167

多头系统, 可信窗口条，95

翻

翻译, **请参见**本地化

防

防止, **请参见**保护

访

访问
- **请参见**计算机访问
- 按标签选择审计记录，268
- 打印机，229–236
- 管理工具，113–114
- 较低级别区域中挂载的 ZFS 数据集（从较高级别区域），159
- 起始目录，149
- 全局区域，114
- 设备，247–249
- 用户访问有标签区域，66–67
- 远程多级别桌面，143–145
- 远程系统，139–147

访问策略
- 强制访问控制 (Mandatory Access Control, MAC)，94
- 设备，248
- 自主访问控制 (Discretionary Access Control, DAC)，93, 94–95

分

分配, 使用设备管理器，249–250
分配错误状态, 纠正，258–259
分配设备, 用于复制数据，74–75
“分配设备”授权，248

服

服务管理框架 (Service Management Framework, SMF)
- `dpadm`，81
- `dsadm`，81
- `labeld` 服务，43–44

更

更改
- `IDLETIME` 关键字，130–131
- 标签更改所适用的规则，112
- 数据的安全级别，137–138
- 系统安全缺省值，119–120
- 用户特权，136
- 由经授权的用户更改标签，137–138

供

供初始设置团队使用的核对表，283–285

工

工具, **请参见**管理工具
工作区
- 全局区域，105–106
- 颜色更改，114
- 指示标签的颜色，100

共

共享
- IP 地址，55
- 使用 Vino，145
- 有标签区域的 ZFS 数据集，158–159

故

故障安全会话, 登录，134
故障排除
- IPv6 配置，50
- LDAP，220–222
- Trusted Extensions 配置，69–70
- 查看较低级别区域中挂载的 ZFS 数据集，159
- 登录失败，134
- 回收设备，258–259
- 检验接口是否已启动，216–217
- 可信网络，217–220
- 网络，216–222

故障排除（续）
已挂载文件系统，174
在内部数据库中修复标签，118–119

挂

挂载
概述，164–166
故障排除，174
回送挂载的文件，156
文件系统，171–173
有标签区域上的 ZFS 数据集，158–159

管

管理
请参见管理
LDAP，223–226
Trusted Extensions 中的审计，267–268
安全模板，198–203, 203–204
打印，236
第三方软件，273–275
对用户的方便授权，135–136
多级别端口，211–212
多级别数据集，164–166
更改信息的标签，137–138
共享文件系统，171–173
具有安全属性的路由，209
可信网络，193–222
面向管理员的快速参考，287–289
区域，153–160
全局区域，114
设备，253–265
设备分配，264–265
设备授权，261–264
使用 txzonemgr 的区域，153
文件
使用标签备份，170–171
使用标签恢复，171
文件系统
概述，162–164
故障排除，174
挂载，173–174
管理（续）
无标签打印，243–245
系统文件，119–120
用户，123, 129–138
用户的启动文件，131–133
用户特权，136
邮件，227–228
有标签 IPsec，212–216
有标签打印，229–245
远程，139–147
远程主机模板，196–198
帐户锁定，137
指定设备授权，264–265
管理标签，98
管理工具
"Labeled Zone Manager"（有标签区域管理器），102
txzonemgr 脚本，102
标签生成器，103
访问，113–114
命令，104
配置文件，104
设备管理器，102–103
说明，101–104
选择管理器，103
管理角色, **请参见**角色
管理区域（任务列表），153–160
管理用户和权限（任务列表），134–138

规

规划
另请参见 Trusted Extensions 使用
LDAP 命名服务，30
Trusted Extensions，25–33
Trusted Extensions 配置策略，32
标签，27
管理策略，26–27
区域，28–30
审计，31
手提电脑配置，30
网络，28
硬件，27–28
帐户创建，31

国
国际化, **请参见**本地化

过
过程, **请参见**任务和任务列表

恢
恢复对桌面焦点的控制，116–117

回
回退机制, 在安全模板中，182

会
会话, 故障安全，134
会话范围，99

计
计算机访问
  管理员职责，109
  限制，248

剪
剪切和粘贴
  和标签，110–112
  配置标签更改所适用的规则，112

检
检查
  `label_encodings` 文件，48–49
  角色有效，66
检验
  `label_encodings` 文件，48–49
  角色有效，66
  接口已启动，216–217

键
键盘关机, 启用，119–120
键组合, 测试抓取是否可信，116–117

降
降级标签, 配置适用于选择确认器的规则，112

脚
脚本
  `getmounts`，155
  `/usr/bin/txzonemgr`，154
  `/usr/sbin/txzonemgr`，101, 153

角
角色
  承担，105–106, 114
  创建，106
  创建安全管理员，62–63
  工作区，105–106
  管理审计，268
  检验它们是否有效，66
  可信应用程序访问权限，101
  离开角色工作区，114
  确定何时创建，43
  使用 `roleadd` 添加 LDAP 角色，63
  使用 `roleadd` 添加本地角色，62–63
  指定权限，126
角色工作区, 全局区域，105–106

接
接口
检验是否已启动，216–217
添加到安全模板中，198–203, 203–204

解
解除分配, 强制，258–259

介
介质, 从可移除文件中复制文件，75

禁
禁用, Trusted Extensions，76

进
进程
标签，99–100
防止用户查看他人的进程，131
用户进程的标签，99

决
决定
使用 Oracle 提供的编码文件，42
通过承担受限制的角色或作为 root 进行配置，43

开
开发者的职责，275

可
可信程序, 定义，274–275
可信窗口条
多显示端系统上，95
将面板移至屏幕底部，69–70
将指针切换到，117
可信的程序, 添加，275
可信路径, 设备管理器，249–250
可信路径属性, 可用时，100
可信网络
0.0.0.0/0 通配符地址，205
0.0.0.0 tnrhdb 项，205–209
标签和 MAC 执行，175–179
概念，175–191
路由示例，187–188
缺省标签配置，185
使用模板，196–198
主机类型，180–181
可信网络故障排除（任务列表），216–222
可信应用程序, 在角色工作区中，101
可信抓取, 键组合，116–117

控
控制, **请参见**限制

口
口令
"Change Password"（更改口令）菜单项，107, 115
测试口令提示符是否可信，117
存储，109
更改 root，115
更改标签时提供，107
更改用户口令，107
在有标签区域中进行更改，116
指定，125

良
良构的标签，99

路

路由，184
  Trusted Extensions 中的命令，188
  表，184, 187
  概念，186
  认可检查，185–186
  使用 route 命令，209
  示例，187–188

面

面板, 移至屏幕底部，69–70

名

名称, 为区域指定，52–54
名称服务高速缓存守护进程, **请参见** nscd 守护进程

命

命令
  使用特权执行，114
  网络故障排除，217
命名, 区域，52–54
命名服务
  LDAP，223–226
  Trusted Extensions 特有的数据库，223
  管理 LDAP，225–226

模

模板, **请参见**远程主机模板

目

目录
  访问低级别，149
  共享，171–173
  挂载，171–173
  命名服务设置，84
目录（**续**）
  授予用户或角色更改标签的权限，137–138

内

内标签 (inner label)，189

配

配置
  Trusted Extensions，47–76
  Trusted Extensions 客户机的 LDAP 代理服务器，86–87
  Trusted Extensions 有标签区域，51–55
  VNIC，58–59
  访问远程 Trusted Extensions，139–147
  具有安全属性的路由，209
  可信网络，193–222
  逻辑接口，57–58
  设备，255–258
  通过承担受限制的角色或作为 root，43
  网络接口，56–57, 59
  为 Trusted Extensions 配置 LDAP，78–85
  用户的启动文件，131–133
  有标签打印，236–243
  针对设备的授权，261–264
配置 Trusted Extensions
  初始过程，47–76
  供初始设置团队使用的核对表，283–285
  任务列表，35–37
  有标签区域，51–55
  远程访问，139–147
配置文件
  请参见权限配置文件
  复制，74–75
  装入，75
配置有标签 IPsec（任务列表），212–216
配置有标签打印（任务列表），236–243

篇

篇尾页, **请参见**标题页

评

评估程序是否符合安全要求，274–275

其

其他 Trusted Extensions 配置任务，70–76

启

启动文件, 用于定制的过程，131–133
启用
- DOI 不同于 1，50–51
- dpadm 服务，81
- dsadm 服务，81
- IPv6 CIPSO 网络，50
- labeld 服务，43–44
- Trusted Extensions 功能，43–44
- 登录到有标签区域，66–67
- 键盘关机，119–120

起

起始目录
- 创建，67–69, 168
- 创建服务器，67–68
- 登录并获取，68
- 访问，149

强

强制访问控制 (mandatory access control, MAC)
- Trusted Extensions 中，96
- 在网络上执行，175–179

区

区间标签组件，97
区域
- net_mac_aware 特权，173–174
- txzonemgr 脚本，51–52

区域（续）
- 创建 MLP，210–212
- 创建辅助区域，71–72
- 从有标签区域中删除 nscd 守护进程，61
- 辅助，152–153
- 管理，149–160
- 全局，149
- 全局区域进程，151–152
- 确定创建方法，28–30
- 删除，76
- 添加 nscd 守护进程到每个有标签区域，60–61
- 为 NFSv3 创建 MLP，211
- 显示文件系统的标签，155–156
- 显示状态，154
- 用于隔离有标签服务，71–72
- 允许登录到，66–67
- 在 Trusted Extensions 中，149–160
- 指定标签，52–54
- 指定名称，52–54
- 主，152–153

全

全局区域
- 进入，114
- 退出，114
- 与有标签区域的区别，149

权

权限
- **请参见**权限配置文件
- 为用户更改缺省值，126

权限配置文件
- Convenient Authorizations（方便授权），135–136
- 包含 "Allocate Device"（分配设备）授权，265
- 包含设备分配授权，265
- 包含新的设备授权，263–264
- 指定，126

热

热键, 重新获得对桌面焦点的控制权，116–117

任

任务和任务列表
- Trusted Extensions 管理员入门（任务列表），113–114
- Trusted Extensions 中的常见任务（任务列表），115–120
- 查看现有安全模板（任务），193–195
- 创建有标签区域，51–55
- 管理区域（任务列表），153–160
- 管理用户和权限，134–138
- 可信网络故障排除（任务列表），216–222
- 配置有标签 IPsec（任务列表），212–216
- 配置有标签打印（任务列表），236–243
- 其他 Trusted Extensions 配置任务，70–76
- 任务列表：配置 Trusted Extensions 以满足站点要求，36–37
- 任务列表：使用提供的缺省设置配置 Trusted Extensions，36
- 任务列表：选择 Trusted Extensions 配置，35–36
- 任务列表：准备和启用 Trusted Extensions，35
- 为主机和网络设置标签（任务），193–209
- 在 Trusted Extensions 网络上配置 LDAP（任务列表），77–78
- 在 Trusted Extensions 系统上配置 LDAP 代理服务器（任务列表），78
- 在 Trusted Extensions 中操作设备（任务列表），253
- 在 Trusted Extensions 中定制设备授权（任务列表），261–265
- 在 Trusted Extensions 中管理打印（任务列表），236
- 在 Trusted Extensions 中管理设备（任务列表），254–261
- 在 Trusted Extensions 中减少打印限制（任务列表），243–245
- 在 Trusted Extensions 中设置远程管理（任务列表），141–147
- 在 Trusted Extensions 中使用设备（任务列表），254

任务和任务列表（**续**）
- 针对安全性定制用户环境（任务列表），129–134

任务列表
- 任务列表：配置 Trusted Extensions 以满足站点要求，36–37
- 任务列表：使用提供的缺省设置配置 Trusted Extensions，36
- 任务列表：选择 Trusted Extensions 配置，35–36
- 任务列表：准备和启用 Trusted Extensions，35

认

认可范围, `label_encodings`文件，98
认可检查，185–186

日

日志文件, 保护 Directory Server 日志，82–83

软

软件
- 导入，273
- 管理第三方，273–275

软件包, Trusted Extensions 功能，41
软盘
- **请参见**磁盘

删

删除
- 打印输出上的标签，243–244
- 特定于区域的 `nscd` 守护进程，61
- 有标签区域，76

删除 Trusted Extensions, **请参见**禁用

商

商业应用程序, 评估，275

设

设备
- Trusted Extensions 中的，247–251
- 保护，102–103
- 保护不可分配的，259–260
- 策略缺省值，248
- 创建新授权，261–264
- 访问，249–250
- 访问策略，248
- 分配，247–249
- 故障排除，258–259
- 管理，253–265
- 回收，258–259
- 配置设备，255–258
- 设置策略，248
- 使用，254
- 使用 "Device Manager"（设备管理器）进行管理，255–258
- 添加 `device_clean` 脚本，260–261
- 添加定制授权，264
- 为不可分配的设备设置标签范围，248
- 阻止远程分配音频，260

设备分配
- 包含分配授权的配置文件，265
- 概述，247–249
- 授权，264–265

设备管理器
- 管理工具，101
- 说明，249–250

升

升级标签, 配置适用于选择确认器的规则，112

收

收集信息, LDAP 服务，78–79

手

手册页, 适用于 Trusted Extensions 管理员的快速参考，291–297

手提电脑, 规划，30

授

授权
- "Allocate Device"（分配设备），264–265, 265
- "Configure Device Attributes"（配置设备属性），265
- "Revoke or Reclaim Device"（撤销或回收设备），264–265, 265
- 包含设备分配授权的配置文件，265
- 被授予，97
- 便于针对用户，135–136
- 创建本地和远程设备授权，263–264
- 创建定制设备授权，262–263
- 定制对设备的授权，264
- 分配设备，248
- 设备分配，264–265
- 授权用户或角色更改标签，137–138
- 添加新的设备授权，261–264
- 无标签打印，243–245
- 指定，126
- 指定设备授权，264–265

数

数据, 有效地重新设置标签，72–74

数据集, **请参见** ZFS

数据库
- LDAP 中的，223
- 可信网络，179

特

特权
- 从基本集中删除 `proc_info`，131
- 收缩用户的，136
- 需要特权的不明显原因，275
- 执行命令时，114

添

添加
- IPsec 保护，212–214
- nscd 守护进程到每个有标签区域，60–61
- Trusted Extensions 软件包，41
- VNIC 接口，58–59
- 多级别数据集，72–74
- 辅助区域，71–72
- 共享网络接口，56–57
- 角色，61–67
- 可以承担角色的用户，63–66
- 逻辑接口，57–58
- 使用 roleadd 添加 LDAP 角色，63
- 使用 roleadd 添加本地角色，62–63
- 使用 useradd 添加本地用户，65–66
- 特定于区域的 nscd 守护进程，60–61
- 网络数据库至 LDAP 服务器，84–85
- 远程主机，59
- 远程主机模板，196–198

通

通配符地址, **请参见**回退机制

网

网关
- 认可检查，185–186
- 示例，187–188

网络
- **请参见** Trusted Extensions 网络
- **请参见**可信网络

网络包，176

网络概念，177

网络数据库
- LDAP 中的，223
- 说明，179

为

为主机和网络设置标签（任务），193–209

文

文件
- .copy_files，126–127, 131–133
- /etc/default/kbd，119–120
- /etc/default/login，119–120
- /etc/default/passwd，119–120
- /etc/security/policy.conf，124, 130–131
- /etc/security/tsol/label_encodings 文件，98
- getmounts，155
- .link_files，126–127, 131–133
- policy.conf，119–120
- /usr/bin/tsoljdsselmgr，110–112
- /usr/lib/cups/filter/tsol_separator.ps，231–235
- /usr/sbin/txzonemgr，101, 153
- /usr/share/gnome/sel_config，112
- 从可移除介质中复制，75
- 从支配标签访问，155–156
- 防止从支配标签访问，157–158
- 回送挂载，156
- 启动，131–133
- 使用标签备份，170–171
- 使用标签恢复，171
- 授予用户或角色更改标签的权限，137–138
- 重新为特权设置标签，160

文件和文件系统
- 共享，171–173
- 挂载，171–173
- 命名，171

文件系统
- NFS 挂载，164–166
- 共享，162–164
- 在全局和有标签区域中共享，164–166
- 在全局和有标签区域中挂载，164–166

文件系统的名称，171

无

无标签打印, 配置，243–245

系

系统解释域 (domain of interpretation, DOI), 修改，50–51

系统文件
label_encodings，48–49
sel_config，112
tsol_separator.ps，245
编辑，119–120

显
显示
每个区域的状态，154
有标签区域中文件系统的标签，155–156

线
线标签 (wire label)，189

限
限定, 网络上定义的主机，205–209
限制
打印机标签范围，242–243
打印机访问（使用标签），230–231, 231
对打印机的访问（使用标签），230–231, 231
对全局区域的访问，106
对设备的访问，247–249
访问较低级别文件，157–158
基于标签限制对计算机的访问，248
较低级别文件的挂载，157–158
远程访问，139–140

相
相似之处
Trusted Extensions 和 Oracle Solaris OS 之间，93
Trusted Extensions 和 Oracle Solaris 审计之间，267

修
修改, label_encodings 文件，48–49

虚
虚拟网络计算 (Virtual Network Computing, VNC), **请参见**运行 Trusted Extensions 的 Xvnc 系统

选
选择
请参见选择
按标签选择审计记录，268
选择管理器, 配置适用于选择确认器的规则，112

颜
颜色, 指示工作区的标签，100

要
要做的决策
基于站点安全策略，278
在启用 Trusted Extensions 之前，42–43

一
一般用户, **请参见**用户

音
音频设备, 阻止远程分配，260

应
应用程序
可信的和值得信任的，274–275
评估安全性，275
启用客户机和服务器之间的初始网络联系，207
应用程序安全标签，189

硬

硬件规划，27–28

用

用户
- "Change Password"（更改口令）菜单项，107
- "Change Workspace Label"（更改工作区标签）菜单项，107
- 安全培训，107, 109, 250
- 创建，122
- 创建初始用户，63–66
- 打印，229–236
- 登录到故障安全会话，134
- 定制环境，129–134
- 防止查看他人的进程，131
- 防止帐户锁定，137
- 访问打印机，229–236
- 访问设备，247–249
- 分配角色，125
- 更改缺省特权，126
- 规划，123
- 恢复对桌面焦点的控制，116–117
- 会话范围，99
- 进程的标签，99
- 启动文件，131–133
- 删除某些特权，136
- 删除时的注意事项，109
- 设置框架目录，131–133
- 使用 `.copy_files` 文件，131–133
- 使用 `.link_files` 文件，131–133
- 使用 `useradd` 添加本地用户，65–66
- 使用设备，254
- 授权，135–136
- 修改安全缺省值，130
- 针对所有用户修改安全缺省值，130–131
- 指定标签，126
- 指定口令，125
- 指定权限，126
- 指定授权，126

邮

邮件
- Trusted Extensions 中的实现，227–228
- 多级别，227
- 管理，227–228

有

有标签 IPsec, **请参见** IPsec
有标签打印
- 标题页，231–232
- 删除标签，135–136
- 无标题页，135–136
- 正文页，233

有标签多播包，176
有标签区域, **请参见**区域
有标签区域管理器, **请参见** `txzonemgr` 脚本

远

远程多级别桌面, 访问，143–145
远程管理
- 方法，140
- 缺省值，139–140

远程系统, 针对角色承担进行配置，141–143
远程主机, 使用 `tnrhdb` 中的回退机制，182
远程主机模板
- `0.0.0.0/0` 通配符指定，205
- Sun Ray 服务器的项，205
- 创建，196–198
- 将系统添加到，198–203, 203–204
- 指定，198–204

运

运行 Trusted Extensions 的 Xvnc 系统
- 远程访问，140, 143–145

在

在 Trusted Extensions 网络上配置 LDAP（任务列表），77–78
在 Trusted Extensions 系统上配置 LDAP 代理服务器（任务列表），78
在 Trusted Extensions 中操作设备（任务列表），253
在 Trusted Extensions 中定制设备授权（任务列表），261–265
在 Trusted Extensions 中挂载数据集，161–162
在 Trusted Extensions 中管理打印（任务列表），236
在 Trusted Extensions 中管理设备（任务列表），254–261
在 Trusted Extensions 中减少打印限制（任务列表），243–245
在 Trusted Extensions 中设置远程管理（任务列表），141–147
在 Trusted Extensions 中使用设备（任务列表），254
在内部数据库中, 修复标签，118–119

站

站点安全策略
- Trusted Extensions 配置决策，278
- 常见违规，280
- 建议，278–279
- 了解，26
- 人员建议，280
- 涉及的任务，277–282
- 物理访问建议，279

帐

帐户
- **另请参见**角色
- **另请参见**用户
- 创建，61–67
- 规划，31

帐户锁定, 为可承担角色的用户防止，137

针

针对安全性定制用户环境（任务列表），129–134

正

正文页
- `ADMIN_HIGH` 标签，240
- 无标签，245
- 有标签的说明，233

值

值得信任的程序，274–275

指

指定
- 将特权指定给用户，126
- 权限配置文件，126

主

主机
- 添加到 `/etc/hosts` 文件，195
- 添加到安全模板中，198–203, 203–204
- 网络概念，177
- 指定模板，198–204

主机类型
- 联网，176, 180–181
- 模板和协议表，180–181
- 远程主机模板，180

注

注销, 要求，130–131

桌

桌面
登录到故障安全会话，134
工作区颜色更改，114
将面板移至屏幕底部，69–70
使用 Vino 共享，145
远程访问多级，143–145

自

自主访问控制 (discretionary access control, DAC)，96

组

组
安全要求，109
删除时的注意事项，109
组件定义，`label_encodings` 文件，98

最

最大标签，远程主机模板，180
最小标签，远程主机模板，180