Trusted Extensions 用户指南

文件号码 E36547–02
2012 年 10 月

ORACLE

121210@25097

目录

图

表

前言

《Trusted Extensions 用户指南》是在启用了 Trusted Extensions 功能的 Oracle Solaris 操作系统 (Oracle Solaris OS) 中进行操作的指南。

目标读者

本指南适用于 Trusted Extensions 的所有用户。作为前提条件，您必须熟悉 Oracle Solaris OS 和开源 GNOME 桌面。

此外，您还必须熟悉所在组织的安全策略。

Trusted Extensions 指南丛书的结构

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

指南标题	主题	目标读者
《Trusted Extensions 用户指南》	介绍了 Trusted Extensions 的基本功能。本指南包含一个词汇表。	最终用户、管理员、开发者
《Trusted Extensions 配置和管理》	第 I 部分介绍了如何准备、启用和最初配置 Trusted Extensions。 第 II 部分介绍了如何管理 Trusted Extensions 系统。本指南包含一个词汇表。	管理员、开发者
《Trusted Extensions Developer's Guide》	说明了如何使用 Trusted Extensions 来开发应用程序。	开发者、管理员
《Trusted Extensions Label Administration》	提供了有关如何在标签编码文件中指定标签组件的信息。	管理员
《Compartmented Mode Workstation Labeling: Encodings Format》	介绍了标签编码文件中使用的语法。该语法实施各种规则来为系统实现良构的标签。	管理员

本指南的结构

第 1 章，Trusted Extensions 介绍介绍了在包含 Trusted Extensions 功能的 Oracle Solaris 系统上实施的基本概念。

第 2 章，登录到 Trusted Extensions（任务）介绍了访问和退出 Trusted Extensions 系统的过程。

第 3 章，使用 Trusted Extensions（任务），介绍如何使用 Trusted Extensions。

第 4 章，Trusted Extensions 的元素（参考信息）解释了包含 Trusted Extensions 功能的系统中的关键元素。

词汇表，介绍 Trusted Extensions 中使用的安全术语。

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。

表 P–1 印刷约定 （续）

字体或符号	含义	示例
《书名》	书名	阅读《用户指南》的第 6 章。

命令中的 shell 提示符示例

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

表 P–2 shell 提示符

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

◆ ◆ ◆ 第 1 章

1 Trusted Extensions 介绍

本章介绍了 Trusted Extensions 功能向 Oracle Solaris 操作系统 (Oracle Solaris OS) 中添加的标签和其他安全功能。

什么是 Trusted Extensions？

Trusted Extensions 为 Oracle Solaris 系统提供特殊安全功能。使用这些功能，组织可以在 Oracle Solaris 系统上定义并实施标签安全策略。**安全策略**是规则集合和做法，可以帮助保护站点上的信息和其他资源（例如计算机硬件）。通常，安全规则负责处理诸如谁可以访问哪些信息或者允许谁向可移除介质写入数据之类的问题。**安全做法**是建议的任务执行过程。

下列各节将介绍 Trusted Extensions 中主要的安全功能。正文中会指出哪几项安全功能是可以配置的。

Trusted Extensions 保护系统免受侵入者攻击

Trusted Extensions 向 Oracle Solaris OS 添加了用来防范入侵者的功能。Trusted Extensions 还依赖于 Oracle Solaris 的某些功能，例如口令保护。Trusted Extensions 添加了用于角色的口令更改 GUI。缺省情况下，用户必须获得授权才能使用外围设备，例如麦克风或相机。

限制对可信计算基的访问

术语**可信计算基** (trusted computing base, TCB) 是指 Trusted Extensions 中处理安全性相关事件的部分。TCB 包括软件、硬件、固件、文档和管理规程。只要是可以访问安全性相关文件的实用程序和应用程序都是 TCB 的一部分。管理员会对您与 TCB 之间所有可能的交互操作设置限制。此类交互操作包括执行作业所需的程序、有访问权限的文件以及可能会对安全性产生影响的实用程序。

使用强制访问控制保护信息

如果侵入者设法成功登录到系统中，可以设置进一步的障碍防止其访问信息。可以通过访问控制对文件和其他资源进行保护。与在 Oracle Solaris OS 中一样，访问控制可由信息所有者进行设置。在 Trusted Extensions 中，访问也是由系统进行控制的。有关详细信息，请参见第 17 页中的 “Trusted Extensions 提供自主访问控制和强制访问控制”。

保护外围设备

在 Trusted Extensions 中，管理员控制对本地外围设备（例如磁带机、CD-ROM 驱动器、USB 设备、打印机和麦克风）的访问。可以针对每个用户授予访问权限。该软件使用下述方法限制对外围设备的访问：

- 缺省情况下，设备必须先进行分配，然后才能使用。
- 用户必须拥有授权才能访问控制可移除介质的设备。
- 远程用户无法使用本地设备，例如话筒或 CD-ROM 驱动器。只有本地用户才能分配设备。

阻止欺骗用户的程序

“欺骗”意味着仿冒。有时，入侵者会仿冒登录程序或其他合法程序来拦截口令或其他敏感数据。Trusted Extensions 通过在屏幕顶部显示如下所示的**可信符号**（一个可清楚识别的防篡改图标）来保护用户免受恶意仿冒程序攻击。

图 1–1 可信符号

只要是与可信计算基 (trusted computing base, TCB) 进行交互，就会显示此符号。显示该符号，即可确保安全执行安全性相关事务。不显示该符号，则表示可能存在安全违规。图 1–1 显示了可信符号。

Trusted Extensions 提供自主访问控制和强制访问控制

通过自主访问控制和强制访问控制两项功能，Trusted Extensions 可以控制哪些用户可以访问哪些信息。

自主访问控制

自主访问控制 (discretionary access control, DAC) 是一种软件机制，用于控制用户对文件和目录的访问。DAC 允许所有者根据自己的判断来设置对文件和目录的保护。DAC 的两种形式是 UNIX 权限位和访问控制列表 (access control list, ACL)。

通过权限位，所有者可以按所有者、组和其他用户来设置读、写和执行保护。在传统的 UNIX 系统中，超级用户或 `root` 用户可以覆盖 DAC 保护。而 Trusted Extensions 只允许管理员和授权用户覆盖 DAC。ACL 提供更为精细的访问控制。通过 ACL，所有者可以为特定的用户和特定的组单独指定权限。有关更多信息，请参见《Oracle Solaris 11.1 管理：ZFS 文件系统》中的第 7 章 “使用 ACL 和属性保护 Oracle Solaris ZFS 文件”。

强制访问控制

强制访问控制 (mandatory access control, MAC) 是一种基于标签关系的、由系统强制执行的访问控制机制。系统将敏感标签与创建用来执行程序的所有进程关联起来。MAC 策略使用这种标签来进行访问控制决策。一般情况下，进程无法存储信息，也不能与其他进程进行通信，除非目标标签等同于该进程的标签。MAC 策略允许进程从同一级别标签对象读取数据，或者从较低级别标签对象读取数据。但是，管理员可以创建一个其中仅存在很少较低级别对象或没有较低级别对象的有标签环境。

缺省情况下，MAC 策略对用户不可见。一般用户必须具有对对象的 MAC 访问权限，才能看到这些对象。在任何情况下，用户都不能采取违背 MAC 策略的操作。

敏感标签和安全许可

标签具有以下两个组件：

- 等级，也称**级别**

  此组件表示有层次的安全性级别。对用户来说，等级代表信任的度量；而对数据来说，等级则代表其需要的保护程度。

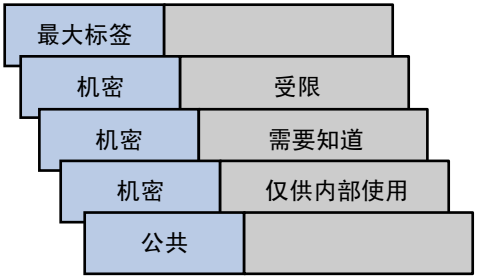
  在美国政府中，等级分为 `TOP SECRET`（绝密）、`SECRET`（秘密）、`CONFIDENTIAL`（机密）和 `UNCLASSIFIED`（未分类）。行业等级不作为标准化的等级。一家公司可以建立唯一的等级。有关示例，请参见图 1–2。左侧的术语代表各个等级，右侧的术语则代表各个区间。

- 区间，也称为**类别**

区间代表分组，例如工作组、部门、项目或主题。一个等级不一定要具有区间。在图 1–2 中，Confidential（机密）等级具有三个专有的区间。Public（公共）等级和 Max Label（最大标签）则不具有区间。如图所示，该组织定义了五个标签。

Trusted Extensions 维护两种类型的标签：**敏感标签**和**安全许可**。系统可以许可用户在一个或多个敏感标签下工作。**用户安全许可**标签，这种特殊的标签用于确定允许用户工作的最高级别的标签。另外，每位用户都具有最小敏感标签。缺省情况下，登录到多级别桌面会话期间将使用此标签。登录后，用户可以选择在此范围内的其他标签下工作。可以为用户指定 Public（公共）作为最小敏感标签，指定 Confidential: Need to Know（机密：需要知道）作为安全许可。第一次登录时，桌面工作区位于 Public（公共）标签下。在会话过程中，用户可以在 Confidential: Internal Use Only（机密：仅供内部使用）和 Confidential: Need to Know（机密：需要知道）中创建工作区。

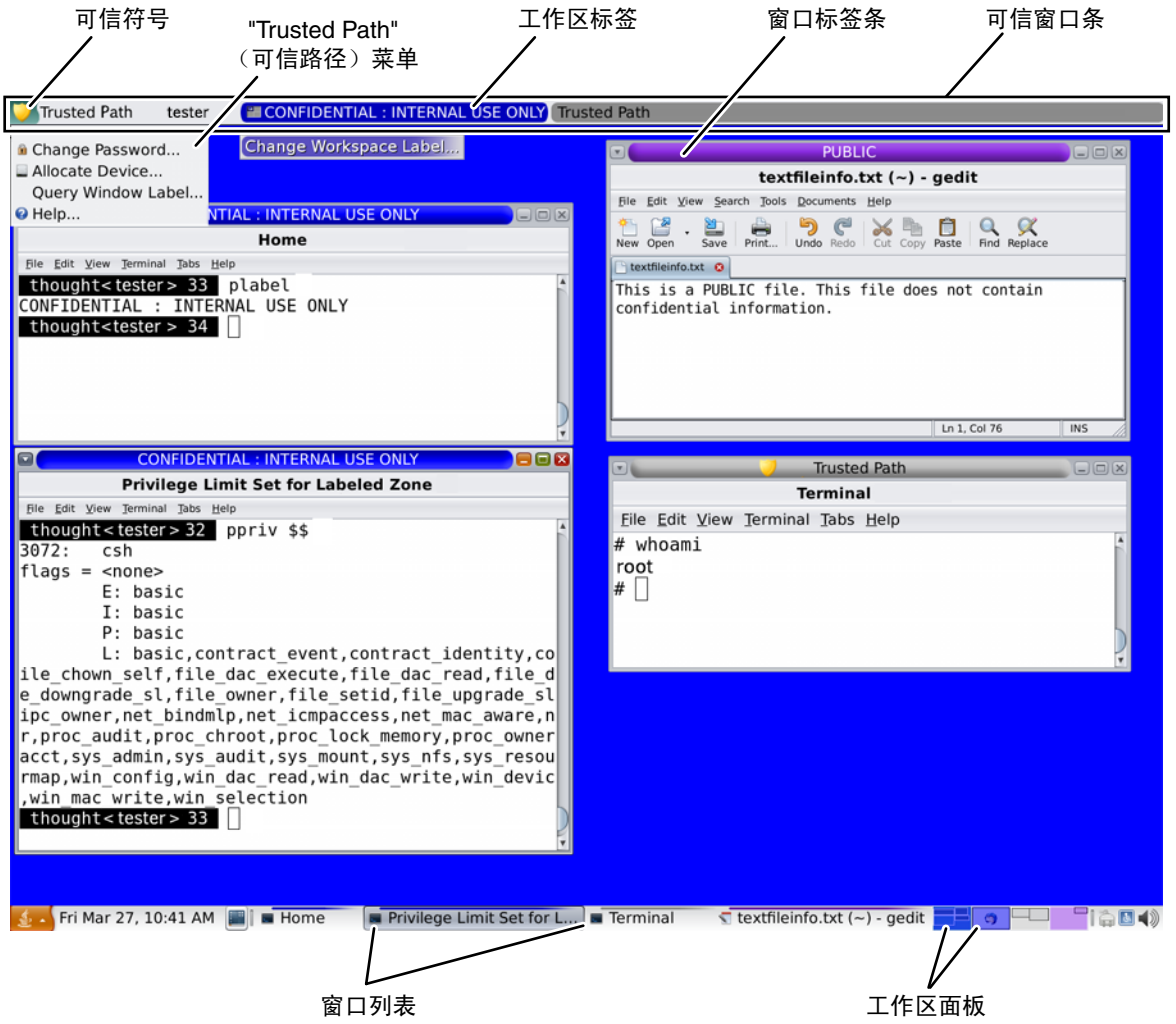
图 1–2 典型行业敏感标签



在配置有 Trusted Extensions 的系统中，所有主体和对象都具有标签。**主体**是一个主动实体，通常为进程。进程促使信息在对象之间流动或更改系统状态。**对象**是包含或接收数据的被动实体，例如数据文件、目录、打印机或其他设备。在某些情况下，进程可以是对象，例如当您对进程使用 kill 命令时。

图 1–3 显示了一个典型的多级别 Trusted Extensions 会话。可信窗口条位于顶部。从可信窗口条中调用了 "Trusted Path"（可信路径）菜单。要承担一个角色，请单击用户名来调用角色菜单。底部面板中的工作区切换器显示工作区标签的颜色。底部面板中的窗口列表显示了窗口标签的颜色。

图 1–3 典型的多级别会话



容器和标签

Trusted Extensions 使用容器设置标签。容器也称**区域**。**全局区域**是管理区域，不供用户使用。非全局区域则称为**有标签区域**。有标签区域可供用户使用。全局区域与用户共享一部分系统文件。这些文件显示在有标签区域中时，其标签为 ADMIN_LOW。用户可以读取但不能更改 ADMIN_LOW 文件的内容。

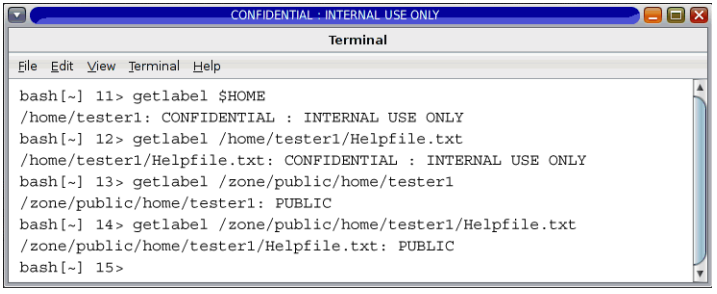
网络通信通过标签进行限制。缺省情况下，各区域间无法互相通信，因为各个区域的标签互不相同。因此，一个区域无法写入到另一个区域中。

但是，管理员可以配置特定区域，使其能够读取其他区域中的特定目录。其他区域可以位于同一台主机上，或者位于远程系统上。例如，可以通过使用自动挂载服务来挂载较低级别区域中的用户起始目录。此类较低级别起始目录挂载的路径名约定包括区域名称，如下所示：

/zone/*name-of-lower-level-zone*/home/*username*

下面显示的终端窗口说明了较低级别起始目录的可见性。如果将自动挂载服务配置为使较低级别区域可读，则登录标签为 Confidential: Internal Use Only（机密：仅供内部使用）的用户即可查看 Public（公共）区域的内容。textfileInfo.txt 文件具有两个版本。Public（公共）区域版本包含可以与公众共享的信息。Confidential: Internal Use Only（机密：仅供内部使用）版本包含仅可在公司内部共享的信息。

图 1–4 从较高级别标签区域查看公共信息



标签和事务

Trusted Extensions 软件管理所有尝试进行的安全性相关事务。该软件将主体标签与对象标签进行比较，然后根据哪个标签具有**支配地位**来允许或禁止事务。如果满足下面两个条件，则认为某个实体的标签可以**支配**另一个实体的标签：

- 第一个实体的标签等级组件等于或高于对象等级。
- 第二个实体的标签中所有的区间都包括在第一个实体的标签中。

如果两个标签具有同一等级和同一组区间，则认为这两个标签是**等同的**。如果标签等同，则这两个标签可以互相支配。因此，允许进行访问。

如果满足以下条件之一，则认为第一个标签**严格支配**第二个标签。

- 第一个标签的等级高于第二个标签的等级
- 第一个标签的等级等于第二个标签的等级，第一个标签包含第二个标签的区间，并且第一个标签还具有其他区间

如果某个标签严格支配另一个标签，则该标签对受支配的标签具有访问权限。

如果任一标签都不支配另一个标签，则认为这两个标签**不相交**。不相交的标签之间不允许进行访问。

例如，请参考下图。

可以根据这些组件创建四个标签：

- TOP SECRET（绝密）
- TOP SECRET A（绝密 A）
- TOP SECRET B（绝密 B）
- TOP SECRET AB（绝密 AB）

TOP SECRET AB（绝密 AB）支配自身并且严格支配其他标签。TOP SECRET A（绝密 A）支配自身并且严格支配 TOP SECRET（绝密）。TOP SECRET B（绝密 B）支配自身并且严格支配 TOP SECRET（绝密）。TOP SECRET A（绝密 A）和 TOP SECRET B（绝密 B）不相交。

在读取事务中，主体的标签必须支配对象的标签。此规则可确保主体的信用级别满足访问对象的要求。即，主体的标签包括被允许来访问对象的所有区间。TOP SECRET A（绝密 A）可以读取 TOP SECRET A（绝密 A）和 TOP SECRET（绝密）数据。同样，TOP SECRET B（绝密 B）可以读取 TOP SECRET B（绝密 B）和 TOP SECRET（绝密）数据。TOP SECRET A（绝密 A）不能读取 TOP SECRET B（绝密 B）数据。TOP SECRET B（绝密 B）也不能读取 TOP SECRET A（绝密 A）数据。TOP SECRET AB（绝密 AB）可以读取所有标签中的数据。

在写入事务中，即主体创建或修改对象时，所得到对象的有标签区域必须等同于主体的有标签区域。不允许从一个区域向其他区域执行写入事务。

在实践中，读取和写入事务中的主体和对象通常具有相同的标签，不必考虑严格支配关系。例如，TOP SECRET A（绝密 A）主体可以创建或修改 TOP SECRET A（绝密 A）对象。在 Trusted Extensions 中，TOP SECRET A（绝密 A）对象位于标签为 TOP SECRET A（绝密 A）的区域中。

下表说明了美国政府标签之间以及一组行业标签之间的支配关系。

表 1–1 Trusted Extensions 中标签关系的示例

	标签 1	关系	标签 2
美国政府标签	TOP SECRET AB（绝密 AB）	（严格）支配	SECRET A（秘密 A）
	TOP SECRET AB（绝密 AB）	（严格）支配	SECRET A B（秘密 A B）
	TOP SECRET AB（绝密 AB）	（严格）支配	TOP SECRET A（绝密 A）

表 1–1 Trusted Extensions 中标签关系的示例 （续）

	标签 1	关系	标签 2
	TOP SECRET AB（绝密 AB）	支配（等同于）	TOP SECRET AB（绝密 AB）
	TOP SECRET AB（绝密 AB）	不相交于	TOP SECRET C（绝密 C）
	TOP SECRET AB（绝密 AB）	不相交于	SECRET C（秘密 C）
	TOP SECRET AB（绝密 AB）	不相交于	SECRET A B C（秘密 A B C）
行业标签	Confidential: Restricted（机密：受限）	支配	Confidential: Need to Know（机密：需要知道）
	Confidential: Restricted（机密：受限）	支配	Confidential: Internal Use Only（机密：仅供内部使用）
	Confidential: Restricted（机密：受限）	支配	Public（公共）
	Confidential: Need to Know（机密：需要知道）	支配	Confidential: Internal Use Only（机密：仅供内部使用）
	Confidential: Need to Know（机密：需要知道）	支配	Public（公共）
	Confidential: Internal（机密：内部）	支配	Public（公共）
	Sandbox（沙箱）	不相交于	所有其他标签

在具有不同标签的文件之间传输信息时，如果您有权更改文件的标签，Trusted Extensions 会显示确认对话框。如果您无权进行此操作，Trusted Extensions 将禁止该事务。安全管理员可以为您授予对信息进行升级或降级的权限。有关更多信息，请参见第 41 页中的“执行可信操作”。

用户保护数据的职责

作为用户，您负责设置权限来保护您的文件和目录。执行后用以设置权限的操作使用一种称为自主访问控制 (discretionary access control, DAC) 的机制。您可以通过使用 `ls -l` 命令或文件浏览器来检查您对文件和目录的权限，如第 3 章，使用 Trusted Extensions（任务）中所述。

强制访问控制 (mandatory access control, MAC) 由系统自动强制执行。如果您有权对带标签的信息进行升级或降级，则您对确保更改信息级别的需要是否合法负有重大责任。

保护数据的另一方面涉及电子邮件。切勿按照来自某位管理员的电子邮件中收到的说明进行操作。例如，如果按照电子邮件中的说明将口令更改为特定的值，将导致发件人可以登录到您的帐户。在受限制的情况下，您可以在按说明进行操作之前先独立验证这些说明。

Trusted Extensions 通过标签分隔信息

Trusted Extensions 通过以下方式将信息分隔在不同的标签中：

- 对所有事务（包括电子邮件）强制执行 MAC。
- 根据标签将多个文件存储在不同区域中。
- 桌面提供有标签工作区。
- 用户可以选择单级别会话或多级别会话。
- 重用对象前删除对象上的数据。

单级别会话或多级别会话

首次登录到 Trusted Extensions 会话时，请指定是在单个标签中还是在多个标签中执行操作。然后，设置**会话安全许可**或**会话标签**。此项设置是您要执行操作的安全级别。

在单级别会话中，您只能访问与您的会话标签相当或者受该标签支配的那些对象。

在多级别会话中，可以访问等同于或低于会话安全许可标签中的信息。可以为不同的工作区指定不同的标签。您还可以在同一标签下有多个工作区。

会话选择示例

表 1–2 提供了一个示例，展示了单级别会话与多级别会话之间的区别。该示例将选择在位于 `CONFIDENTIAL: NEED TO KNOW`（机密：需要知道）(`CNF: NTK`) 的单级别会话中进行操作的用户与选择位于 `CNF: NTK` 的多级别会话的用户进行了对比。

左侧的三列显示了每个用户在登录时的会话选项。请注意，用户针对单级别会话设置**会话标签**，针对多级别会话设置**会话安全许可**。系统会根据您的选择显示正确的label builder（标签生成器）。要查看多级别会话的样例标签生成器，请参见图 3–4。

右侧的两列显示了会话中可用的标签值。“初始工作区标签”列表示用户首次访问系统时的标签。“可用标签”列列出了会话过程中允许用户切换到的标签。

表 1–2 初始标签选择对可用会话标签的影响

用户选择			会话标签值	
会话类型	会话标签	会话安全许可	初始工作区标签	可用标签
单级别别	CNF: NTK	-	CNF: NTK	CNF: NTK
多级别别	-	CNF: NTK	Public（公共）	Public（公共）
				CNF: Internal Use Only（CNF：仅供内部使用）
				CNF: NTK

如表中第一行所示，用户选择了会话标签为 CNF: NTK 的单级别会话。用户的初始工作区标签为 CNF: NTK，该标签也是用户可以在其中执行操作的唯一标签。

如表中第二行所示，用户选择了会话安全许可为 CNF: NTK 的多级别会话。用户的初始工作区标签设置为 Public（公共），因为 Public（公共）是用户的帐户标签范围中可能的最低级别的标签。用户可以切换到 Public（公共）和 CNF: NTK 之间的任何标签。Public（公共）是最小标签，CNF: NTK 是会话安全许可。

有标签工作区

在 Trusted Extensions 桌面上，可通过底部面板右侧的工作区面板来访问工作区。

图 1–5 面板上的有标签工作区

每个工作区具有一个标签。可以将同一标签指定给多个工作区，也可以将不同的标签指定给不同的工作区。在工作区中启动的窗口具有该工作区的标签。该窗口移到其他标签的工作区中时，将保留其原始标签。因此，在多级别会话中，您可以在一个工作区中排列具有不同标签的窗口

对电子邮件事务强制执行 MAC

Trusted Extensions 对电子邮件强制执行 MAC。可以在当前标签下发送和阅读电子邮件，也可以在帐户范围内的某个标签下接收电子邮件。在多级别会话中，可以切换到其他标签中的工作区，在该标签中阅读电子邮件。使用同一个电子邮件阅读程序和同一个登录名。系统仅允许您在当前标签中阅读邮件。

重用对象前删除对象上的数据

Trusted Extensions 通过在重用用户可访问的对象之前自动删除其中的旧信息来防止敏感信息的无意泄漏。例如，再次使用内存和磁盘空间之前要对其中的信息进行清除。如果没有在重用对象之前删除敏感数据，则会造成将数据泄漏给不适当用户的风险。通过解除设备分配，Trusted Extensions 可在将驱动器分配给进程之前清除所有用户可访问的对象。但是，请注意，您必须先手动清除任何可移除存储介质（例如 DVD 和 USB 设备），才能允许其他用户访问该驱动器。

Trusted Extensions 实现安全管理

与传统 UNIX 系统不同，不使用超级用户（root 用户）管理 Trusted Extensions。而是使用具有独立功能的管理角色来管理系统。这样，任何一个用户都不会危及系统的安全。**角色**是具有执行特定任务所需权限的特殊用户帐户，可以访问特定的应用程序。权限包括标签、授权、特权和有效的 UID/GID。

在配置有 Trusted Extensions 的系统上实施以下安全做法：

- 根据使用需要对您授予应用程序访问权限和授权。
- 只有管理员对您授予特殊授权或特殊权限时，您才能执行覆盖安全策略的功能。
- 在多个角色之间划分系统管理职责。

在 Trusted Extensions 中访问应用程序

在 Trusted Extensions 中，您只能访问执行工作所需的程序。与在 Oracle Solaris OS 中一样，管理员通过为您的帐户指定一个或多个权限配置文件来提供访问权限。**权限配置文件**是程序和安全属性的特殊集合。通过这些安全属性，可以成功使用权限配置文件中的程序。

Oracle Solaris OS 提供安全属性，例如**特权**和**授权**。Trusted Extensions 提供标签。如果缺少这些属性中的任何一个属性，都会导致程序或程序的某些部分不能使用。例如，权限配置文件可能包括允许您读取数据库的授权。您可能需要一个包含不同安全属性的权限配置文件，才能修改数据库或读取等级为 Confidential（机密）的信息。

使用包含具有关联安全属性程序的权限配置文件，有助于防止用户误用程序以及损坏系统中的数据。如果需要执行覆盖安全策略的任务，管理员可以为您指定包含必要安全属性的权限配置文件。如果系统不允许您运行特定的任务，请与管理员联系。您可能缺少必需的安全属性。

另外，管理员可能会为您指定配置文件 shell 作为登录 shell。**配置文件** shell 是常见 shell 的特殊版本，可提供对一组特定应用程序和功能的访问权限。配置文件 shell 是 Oracle Solaris OS 的一项功能。有关详细信息，请参见 pfexec(1) 手册页。

注 – 如果尝试运行程序时收到 "Not Found"（未找到）错误消息，或者尝试运行命令时收到 "Not in Profile"（不在配置文件中）错误消息，系统可能还不允许您使用此程序。请与安全管理员联系。

在 Trusted Extensions 中按角色进行管理

Trusted Extensions 建议使用角色进行管理。请确保您知道谁在您的站点上执行哪组职责。下面是常见的角色：

- root 角色－主要用于防止超级用户直接登录。
- 安全管理员角色－执行与安全相关的任务，例如授予设备分配权限、指定权限配置文件以及评估软件程序。
- 系统管理员角色－执行标准的系统管理任务，例如，创建用户、设置起始目录以及安装软件程序。
- 操作员角色－执行系统备份、管理打印机以及挂载可移除介质。

◆ ◆ ◆ 第 2 章

2 登录到 Trusted Extensions（任务）

本章介绍了 Trusted Extensions 系统上的可信桌面以及登录过程。本章包含以下主题：

Trusted Extensions 中的桌面登录

您在 Trusted Extensions 中使用的桌面是受保护的。标签提供了保护的可见信息。应用程序、数据以及您的通信都带有标签。该桌面是 Oracle Solaris 桌面的可信版本。

登录屏幕没有标签。登录过程要求您为会话设立一个标签。选择标签后，桌面、桌面上的窗口以及所有应用程序都将带有标签。此外，影响安全性的应用程序将由可信路径指示符以可见方式进行保护。

Trusted Extensions 登录过程

配置有 Trusted Extensions 的系统上的登录过程类似于 Oracle Solaris 的登录过程。但是，在 Trusted Extensions 中，您需要先检查几个屏幕上与安全相关的信息，然后才能启动桌面会话。下面几节将更为详细地介绍登录过程。以下是简要概述。

1. 身份识别—在 "Username"（用户名）字段中，键入您的用户名。
2. 验证—在 "Password"（口令）字段中，键入您的口令。

   成功完成身份识别和验证后，即可确认您有使用系统的权限。
3. 消息检查和会话类型选择—检查 "Message Of The Day"（当天的消息）对话框中的信息。该对话框显示的是您上次登录的时间、来自管理员的所有消息，以及会话的安全属性。如果您有权限在多个标签下进行操作，则可以指定会话类型，即单级别会话或多级别会话。

注 – 如果系统将您的帐户限制为可以在一个标签下操作，则无法指定会话类型。此限制称为**单标签**或 single-level configuration（单级别配置）。有关示例，请参见第 23 页中的 “会话选择示例”。

4. 标签选择—在 label builder（标签生成器）中，选择您在会话中工作时打算使用的最高安全级别。

注 – 缺省情况下，Trusted Extensions 中不支持一般用户进行远程登录。如果您的管理员已配置了 Oracle Solaris Xvnc 软件，则您可以使用 VNC 客户机来远程显示多级别桌面。有关过程，请参见第 32 页中的 “远程登录 Trusted Extensions”。

登录期间的身份识别和验证

登录期间的身份识别和验证是由 Oracle Solaris OS 处理的。登录屏幕最开始会包含用户名提示。登录过程的这一部分称为**身份识别**。

输入用户名后，将显示口令提示。登录过程的这一部分称为**身份验证**。口令负责验证您的确是已被授权使用该用户名的用户。

口令是一个私有的击键组合，用于向系统验证您的身份。您的口令存储在一个加密的表单中，系统上的其他用户无法访问。您有责任保护好您的口令，避免其他用户使用您的口令进行未经授权的访问。永远不要写下口令或者向其他任何人透露口令，因为如果某个人持有您的口令，则可以访问您的所有数据而不被发现也不被追究责任。您的初始口令是由 security administrator（安全管理员）提供的。

登录期间检查安全属性

安全属性的检查是由 Trusted Extensions 而不是由 Oracle Solaris OS 处理的。登录完成之前，Trusted Extensions 会显示 "Message Of The Day (MOTD)"（当天的消息）对话框。此对话框提供状态信息供您检查。该状态包括过去的信息，比如上次使用系统的时间。还可以为即将开始的会话检查有效的安全属性。如果系统将您的帐户配置为可以在多个标签下进行操作，则您可以选择单级别会话或多级别会话。

然后，可以查看单个标签或者从标签生成器中选择标签和安全许可。

登录到 Trusted Extensions

下列任务会引导您完成登录到 Trusted Extensions 的过程。应在到达桌面之前检查和指定安全信息。

▼ 向系统表明并验证您的身份

1 **在登录屏幕的 "Username"（用户名）字段中，键入您的用户名。**

请务必准确键入管理员指定给您的用户名。请注意拼写和大写。

如果您出现差错，请键入一个虚假口令。"Username"（用户名）字段将出现。

2 **确认您输入的内容。**

按回车键以确认您的用户名。

注意 – 此时将显示登录屏幕，您**绝不**应当看到可信窗口条。如果在您试图登录或解锁屏幕时看到了可信窗口条，请不要键入口令。这表明您可能遭遇了电子欺骗。**电子欺骗**是指侵入者的程序伪装成登录程序来捕获口令。请立即联系 security administrator（安全管理员）。

3 **在口令输入字段中键入口令，然后按回车键。**

为安全起见，字符不会显示在字段中。系统会将登录名和口令与一个授权用户列表进行比较。

故障排除 如果您提供的口令不正确，屏幕上将显示以下消息：

`Authentication failed`（验证失败）

单击 "OK"（确定），关闭错误对话框。重新键入您的用户名，然后键入正确的口令。

▼ 检查消息和选择会话类型

如果您未将自己限制到单个标签，则可以在不同标签下查看数据。您可以在其中进行操作的标签范围的上限由会话安全许可界定，下限则由管理员指定给您的最小标签界定。

1 **检查 MOTD 对话框。**

a. **检查您的上次会话时间是否准确。**

请务必检查有关上次登录的任何可疑事项，例如一天中某个不寻常的时间。如果您有理由相信该时间不准确，请联系 security administrator（安全管理员）。

b. **检查是否有来自管理员的消息。**

"Message of the Day"（当天的消息）字段可能会包含有关计划内维护或安全问题的警告。请务必检查该字段中的信息。

c. **检查会话的安全属性。**

MOTD 对话框会显示您可承担的所有角色、您的最小标签以及其他安全特性。

d. **可选如果您可以登录到多级别会话，请决定是否要登录到单级别会话。**

单击 "Restrict Session to a Single Label"（将会话限制于单一标签）按钮，可登录到单级别会话。

e. **单击 "OK"（确定）。**

2 **请确认您的标签选择。**

此时将显示标签生成器。如果您要在单个标签下登录，标签生成器会描述您的会话标签。在多级别系统中，可以使用标签生成器选择会话安全许可。要查看多级别会话的样例标签生成器，请参见图 3–4。

- **如果没有任何理由，请接受缺省值。**
- **对于多级别会话，请选择安全许可。**

  要更改安全许可，请单击 "Trusted Path"（**可信路径**）安全许可，然后单击您需要的安全许可。

- **对于单级别会话，请选择一个标签。**
  要更改标签，请单击 "Trusted Path"（**可信路径**）标签，然后单击您需要的标签。

3. **单击 "OK"（确定）。**
   可信桌面随即显示。

▼ 排除登录问题故障

1. **如果系统无法识别您的用户名或口令，请咨询管理员。**

2. **如果您的工作站不允许使用您的标签范围，请咨询管理员。**
   可以将工作站限制为仅使用有限的会话安全许可和标签范围。例如，对于位于大厅的工作站，可能仅限使用 PUBLIC（公共）标签。如果您指定的标签或会话安全许可未被接受，请咨询管理员，以确定工作站是否受限。

3. **如果您定制了 shell 初始化文件而且无法登录，您有下面两种选择：**

   - **联系 system administrator（系统管理员）来解决这一情况。**

   - **如果您可以成为 root 用户，可以登录到故障安全会话。**
     在标准登录中，启动时会将 shell 初始化文件作为来源来提供定制环境。在故障安全登录中，会对系统应用缺省值，不会使用任何 shell 初始化文件作为来源。

     在 Trusted Extensions 中，故障安全登录是受保护的。只有 root 帐户可以使用故障安全登录。

     a. **在登录屏幕中键入您的用户名。**

     b. **在屏幕的底部，从桌面菜单中选择 "Solaris Trusted Extensions Failsafe Session"（Solaris Trusted Extensions 故障安全会话）。**

     c. **在系统提示时，提供您的口令。**

     d. **系统提示输入其他口令时，请提供 root 用户的口令。**

远程登录 Trusted Extensions

使用虚拟网络计算 (Virtual Network Computing, VNC)，您可以从手提电脑或家庭计算机访问 Trusted Extensions 中央系统。站点管理员必须将 Oracle Solaris Xvnc 软件配置为在 Trusted Extensions 服务器上运行，将 VNC 查看器配置为在客户机系统上运行。您可以在服务器上安装的标签范围内的任意标签下工作。

▼ 如何登录远程 Trusted Extensions 桌面

开始之前 您的管理员已设置了一个 Xvnc 服务器。有关指针，请参见《Trusted Extensions 配置和管理》中的“如何对 Trusted Extensions 系统配置 Xvnc 以进行远程访问”。

1. **在终端窗口中，连接到 Xvnc 服务器。**

   键入管理员已配置了 Xvnc 的服务器的名称。

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

2. **登录。**

   按照第 29 页中的 “登录到 Trusted Extensions”中的过程操作。

   现在，您可以通过 VNC 查看器在 Trusted Extensions 桌面上工作了。

◆ ◆ ◆ 第 3 章

3 使用 Trusted Extensions（任务）

本章讨论了如何在 Trusted Extensions 的各个工作区中工作。本章包含以下主题：

Trusted Extensions 中的可视桌面安全性

Trusted Extensions 提供了一个多级别桌面。

配置有 Trusted Extensions 的系统仅在登录和屏幕锁定期间不显示可信窗口条。在所有其他时间，可信窗口条都是可见的。

该窗口条位于屏幕顶部。与可信计算基 (trusted computing base, TCB) 交互期间，可信符号将显示在可信窗口条上。例如，更改口令时，就会与 TCB 交互。

如果多显示端 Trusted Extensions 系统的监视器配置为水平显示，则一个可信窗口条会跨监视器显示。但是，如果多显示端系统配置为垂直显示，或者具有单独的桌面（每个监视器一个桌面），则可信窗口条将仅显示在一个监视器上。

注意 – 如果在多显示端系统上显示了第二个可信窗口条，则该窗口条不是由操作系统生成的。您的系统上可能有未经授权的程序。

请立即与安全管理员联系。要确定正确的可信窗口条，请参见第 39 页中的 “如何找到鼠标指针”。

有关桌面的应用程序、菜单、标签和功能的详细信息，请参见第 4 章，Trusted Extensions 的元素（参考信息）。

Trusted Extensions 注销过程

已登录但一直处于无人使用状态的工作站会导致安全风险。请养成习惯在离开工作站之前要确保工作站的安全性。如果打算很快返回，则请锁定屏幕。在大多数站点上，屏幕在指定的闲置时长后会自动锁定。如果预计会离开一小段时间，或者预计他人将使用您的工作站，请注销。

使用有标签系统

注意 – 如果工作区中没有可信窗口条，请联系security administrator（安全管理员）。您的系统可能存在严重问题。

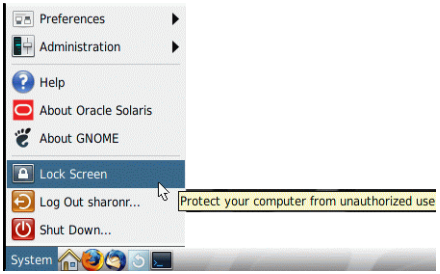
在登录期间或者锁定屏幕后，可信窗口条绝对不应显示。如果在这种情况下仍然显示了可信窗口条，请立即与管理员联系。

▼ 如何锁定屏幕以及如何取消锁定屏幕

如果要暂时离开工作站，请锁定屏幕。

1. **从主菜单中选择 "Lock Screen"（锁定屏幕）。**

图 3–1 选择 "Lock Screen"（锁定屏幕）



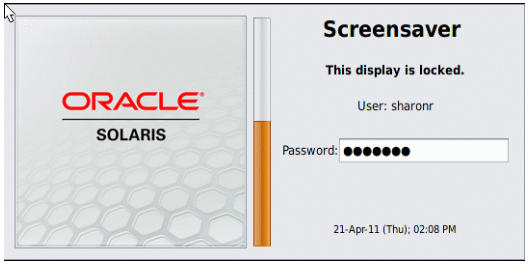
屏幕变黑。此时，只有您才能再次登录。

注 – 屏幕锁定时不得显示可信窗口条。如果确实显示了窗口条，请立即通知 security administrator（安全管理员）。

---

2 **要取消锁定屏幕，请执行以下操作：**

a. **移动鼠标，直到 "Screensaver"（屏幕保护程序）对话框可见。**



如果 "Screensaver"（屏幕保护程序）对话框没有出现，请按回车键。

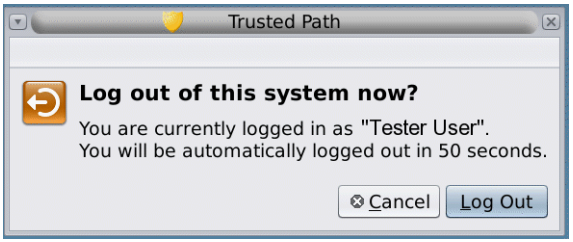
b. **键入口令。**

此操作将使会话恢复为锁屏之前的状态。

▼ 如何注销 Trusted Extensions

在大多数站点上，屏幕在指定的闲置时长后会自动锁定。如果预计离开工作站片刻，或者预计他人使用您的工作站，请注销。

1. **要注销 Trusted Extensions，请从主菜单中选择 "Log Out *your-name*"（注销 your-name）。**



2. **确认您要注销，或者单击 "Cancel"（取消）。**

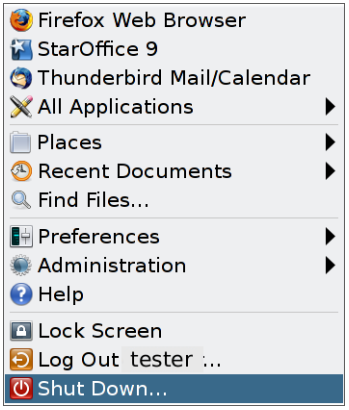
▼ 如何关闭系统

注销是结束 Trusted Extensions 会话的常规方式。如果需要关闭工作站，请使用执行以下过程。

注 – 如果您不在控制台上，则无法关闭系统。例如，VNC 客户机无法关闭系统。

开始之前 必须已为您指定了 "Maintenance and Repair"（维护和修复）权限配置文件。

- **从主菜单中选择 "Shut Down"（关闭）。**



确认关闭。

注 – 缺省情况下，键盘组合 Stop-A (L1-A) 在 Trusted Extensions 中不可用。安全管理员可以更改此缺省设置。

▼ 如何在有标签工作区中查看文件

要查看您的文件，请使用在 Oracle Solaris 系统中的桌面上使用的相同应用程序。如果正在多个标签下执行操作，则只有位于工作区标签的文件才是可见的。

- **打开一个终端窗口或文件浏览器。**
  - **打开终端窗口并列出起始目录的内容。**
    在背景上单击鼠标右键。从菜单中选择 "Open Terminal"（打开终端）。
  - **在桌面或桌面面板上单击 "Home"（起始）文件夹。**
    该文件夹将在文件浏览器中打开。文件浏览器应用程序将在与当前工作区相同的标签下打开。该应用程序仅提供具有其标签的那些文件的访问权限。有关查看具有不同标签的文件的详细信息，请参见第 19 页中的 “容器和标签”。要在一个工作区中查看不同标签下的文件，请参见第 48 页中的 “如何将窗口移动到其他工作区”。

▼ 如何访问 Trusted Extensions 手册页

- **在 Oracle Solaris 发行版中，在一个终端窗口中查看 `trusted_extensions(5)` 手册页。**

```
% man trusted_extensions
```

有关特定于 Trusted Extensions 的用户命令的列表，请参见《Trusted Extensions 配置和管理》中的附录 D “Trusted Extensions 手册页列表”。这些手册页也可以从 Oracle 的文档 Web 站点 (`http://www.oracle.com/technetwork/indexes/documentation/index.html`)获得。

▼ 如何访问每个标签下的初始化文件

如果希望具有较低级别标签的文件在较高级别的标签下可见，可将该文件链接到或复制到其他标签，这样很有用。链接的文件仅在较低级别的标签下可写。复制的文件在每个标签下都是唯一的，并可以在每个标签下进行修改。有关更多信息，请参见《Trusted Extensions 配置和管理》中的“.copy_files 和 .link_files 文件”。

开始之前 必须登录到多级别会话。站点的安全策略必须允许进行链接。

请与管理员合作修改这些文件。

1. **确定要链接到其他标签的初始化文件。**

2. **创建或修改 ~/.link_files 文件。**

   键入条目，每行键入一个文件。可以指定起始目录中子目录的路径，但是不能使用前导斜杠。所有路径都必须位于起始目录内。

3. **确定要复制到其他标签的初始化文件。**

   如果您的应用程序始终写入到具有特定名称的文件，并且需要在不同的标签下分开放置数据，则复制初始化文件很有用。

4. **创建或修改 ~/.copy_files 文件。**

   键入条目，每行键入一个文件。可以指定起始目录中子目录的路径，但是不能使用前导斜杠。所有路径都必须位于起始目录内。

示例 3–1 创建 .copy_files 文件

在此示例中，用户希望为每个标签定制多个初始化文件。在她的组织中，公司的 Web 服务器的访问等级为 Restricted（受限）。因此，她以 Restricted（受限）级别在 .mozilla 文件中设置不同的初始设置。同样，她在 Restricted（受限）级别上具有特殊的模板和别名。因此，她在 Restricted（受限）级别修改 .aliases 和 .soffice 初始化文件。在最低级别标签下创建 .copy_files 文件后，她可以轻松地修改这些文件。

```
% vi .copy_files
# Copy these files to my home directory in every zone
.aliases
.mozilla
.soffice
```

示例 3–2 创建 .link_files 文件

在此示例中，用户希望在所有标签下使用同样的邮件缺省值和 shell 缺省值。

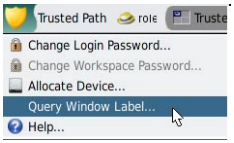
```
% vi .link_files
# Link these files to my home directory in every zone
.cshrc
.mailrc
```

故障排除 这些文件没有处理异常的安全措施。两个文件中的重复条目或者其他标签下已经存在的文件条目可能会导致错误。

▼ 如何交互显示窗口标签

此操作对于识别部分隐藏窗口的标签可能很有用。

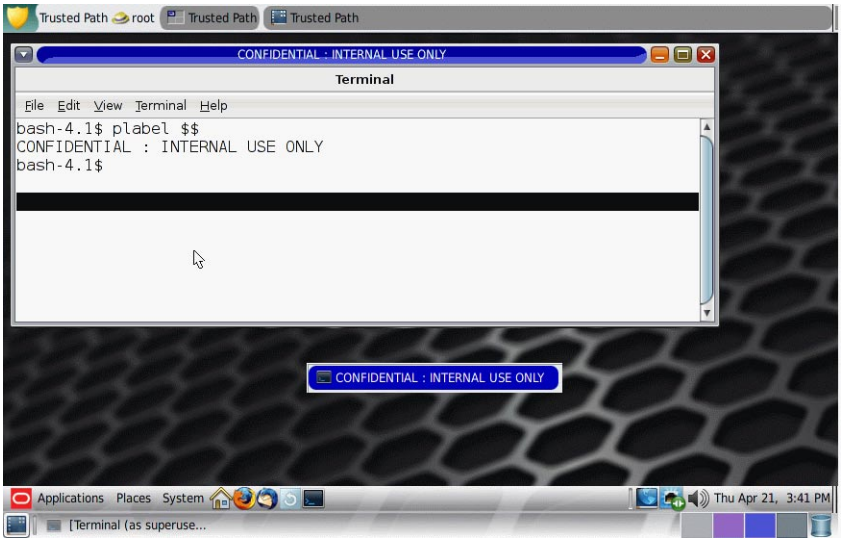
1 **在 "Trusted Path"（可信路径）菜单中，选择 "Query Window Label"（查询窗口标签）。**



2 **在屏幕周围移动指针。**

将在屏幕中心处的一个小矩形框内显示指针所处区域的标签。

图 3–2 查询窗口标签操作



3 **单击鼠标按钮，结束操作。**

▼ 如何找到鼠标指针

不可信的应用程序可能会获得键盘或鼠标指针的控制权。通过找到指针，您可以重新获得对桌面焦点的控制权。

1. **要重新获得对 Sun 键盘的控制权，请按 Meta-Stop。**

   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，空格键两侧的菱形键是 Meta 键。

   如果对键盘或鼠标指针的抓取不可信，则指针将移动到可信窗口条。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，请按 Alt-Break。**

示例 3–3 将鼠标指针强制移动到可信窗口条

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。为将指针移至可信窗口条的中央，用户同时按下 Meta-Stop 键。

示例 3–4 找到真正的可信窗口条

在其监视器配置为在每个监视器上显示一个单独桌面的多显示端 Trusted Extensions 系统上，用户在每个监视器上都看到了一个可信窗口条。因此，这表明 Trusted Extensions 之外的某个程序生成了可信窗口条。当多显示端系统被配置为在每个监视器上显示一个单独桌面时，只应显示一个可信窗口条。

用户应停止工作并立即与安全管理员联系。然后，用户可以通过将鼠标指针置于一个不可信位置（例如，置于工作区背景上）来找到真正的可信窗口条。当用户同时按下 Alt-Break 键时，指针会移动到由 Trusted Extensions 生成的可信窗口条中。

▼ 如何在 Trusted Extensions 中执行常见的桌面任务

某些常见任务会受标签和安全性影响。Trusted Extensions 会特别影响以下任务：

- 清空垃圾箱
- 查找日历事件

1. **清空垃圾箱。**

   在桌面上的 "Trash Can"（垃圾箱）图标上单击鼠标右键。选择 "Empty Trash"（清空垃圾箱），然后进行确认。

   注 – 垃圾箱仅包含工作区标签下的文件。当敏感信息处于垃圾箱中时，请尽快删除这些信息。

   ---

2. **查找每个标签下的日历事件。**

   日历只显示已打开日历工作区的标签下事件。

   - **在多级别会话中，从具有不同标签的每个工作区中打开日历。**

- 在单级别会话中，注销。然后，在不同的标签下登录以查看该标签下的日历事件。

3 **在每个标签下保存一个定制桌面。**
可以为登录的每个标签定制工作区配置。

a. **配置桌面。**

注 – 用户可以保存桌面配置。角色不能保存桌面配置。

---

i. **从主菜单中，单击 "System"（系统）> "Preferences"（首选项）> "Appearance"（外观）。**

ii. **排列窗口，设置字体字号，以及执行其他定制操作。**

b. **要保存当前的桌面，请单击主菜单。**

i. **单击 "System"（系统）> "Preferences"（首选项）> "Startup Applications"（启动应用程序）。**

ii. **单击 "Options"（选项）选项卡。**

iii. **单击 "Remember currently running applications"（记住目前正在运行的应用程序），然后关闭对话框。**

下次在此标签下登录时，将在此配置中恢复您的桌面。

执行可信操作

以下与安全性相关的任务需要可信路径。

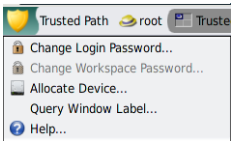
注意 – 尝试执行安全性相关操作时，如果缺少可信符号，请立即与 security administrator（安全管理员）联系。您的系统可能存在严重问题。

▼ 如何在 Trusted Extensions 中更改口令

与 Oracle Solaris OS 不同，Trusted Extensions 提供了用于更改口令的 GUI。该 GUI 会抓取指针，直到完成口令操作。要停止已抓取了指针的某个进程，请参见示例 3–5。

1 **从 "Trusted Path"（可信路径）菜单中选择 "Change Login Password"（更改登录口令）或 "Change Workspace Password"（更改工作区口令）。**
要选择该口令菜单项，请在可信窗口条中单击 "Trusted Path"（可信路径）。

图 3–3 "Trusted Path"（可信路径）菜单



注 – 当您的站点在每个区域中运行一个单独的命名服务时，"Trusted Path"（可信路径）菜单项 "Change Workspace Password"（**更改工作区口令**）处于活动状态。

2 **键入当前口令。**

此操作将确认您是否是此用户名的合法用户。出于安全方面的考虑，在键入时不显示口令。

注意 – 键入口令时，请确保光标在 "Change Password"（更改口令）对话框上，并确保已显示可信符号。如果光标不在该对话框上，则可能会无意中将口令键入到其他窗口中，这样其他用户可能会看到口令。如果未显示可信符号，则可能是有人在试图窃取您的口令。请立即与security administrator（安全管理员）联系。

3 **键入新的口令。**

4 **通过重新键入口令对其进行确认。**

注 – 如果您选择了 "Change Password"（**更改口令**）并且您的站点在使用本地帐户，则在区域或系统重新引导之前，您的新口令不会生效。要重新引导区域，必须已为您指定了 "Zone Security"（区域安全）权限配置文件。要重新引导系统，必须已为您指定了 "Maintenance and Repair"（维护和修复）权限配置文件。如果没有为您指定这些配置文件之一，请联系您的系统管理员来安排一次重新引导。

示例 3–5 测试口令提示符是否可信

在具有 Sun 键盘的 x86 系统上，已提示用户输入口令。鼠标指针已被抓取且定位到了口令对话框中。为检查该提示是否可信，用户同时按下 Meta-Stop 键。如果指针保留在对话框中，用户即知道口令提示是可信的。

如果指针没有保留在对话框中，用户即知道口令提示可能不可信。然后，用户必须与管理员联系。

▼ 如何在不同标签下登录

在首次登录后的后续登录会话中出现的第一个工作区的标签可以设置为标签范围内的任何标签。

用户可以为其登录的每个标签配置启动会话特性。

开始之前 必须登录到多级别会话。

1. **在每个标签下创建工作区。**
   有关详细信息，请参见第 47 页中的 “如何在最小标签下添加工作区”。
2. **按照希望的工作区显示方式配置每个工作区。**
3. **转到您在其标签下登录时希望看到的有标签工作区。**
4. **保存此当前工作区。**
   有关详细信息，请参见第 40 页中的 “如何在 Trusted Extensions 中执行常见的桌面任务”。

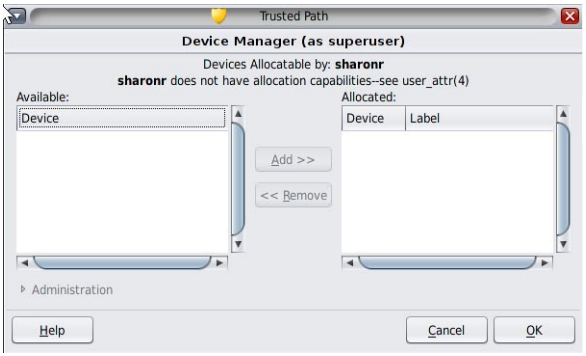
▼ 如何在 Trusted Extensions 中分配设备

通过 "Allocate Device"（分配设备）菜单项，可以挂载和分配设备以专供您使用。如果尝试使用设备而不对其进行分配，则将显示错误消息 "Permission Denied"（权限被拒绝）。

开始之前 您必须具有分配设备的权限。

1. **在 "Trusted Path"（可信路径）菜单中，选择 "Allocate Device"（分配设备）。**
2. **双击要使用的设备。**
   允许您在当前标签下分配的设备将在 "Available Devices:"（可用设备：）下显示。
   - `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

以下对话框指明您无权分配设备：



3 **选择设备。**

将设备从 "Available Devices"（可用设备）列表移动到 "Allocated Devices"（已分配的设备）列表。

- **在 "Available Devices"（可用设备）列表中双击设备名称。**
- **或者，选中该设备，然后单击指向右侧的 "Allocate"（分配）按钮。**

本步骤会启动清除脚本。清除脚本可确保来自其他事务的数据不会保留在介质上。

请注意，当前工作区的标签将应用于设备。传输到设备介质或从其传输的任何数据都必须受此标签支配。

4 **请按照说明进行操作。**

这些说明可以确保介质具有正确的标签。例如，针对麦克风的使用会显示以下说明：

然后，对设备进行挂载。设备名称此时会显示在 "Allocated Devices"（已分配的设备）列表中。此设备现在已分配专供您使用。

故障排除 如果您要使用的设备未显示在列表中，请与管理员联系。设备可能处于错误状态，或者正被他人使用。另外，您也可能没有使用该设备的权限。

如果切换到其他角色工作区或者其他标签下的工作区，则已分配的设备将无法在该标签下工作。要在新标签下使用设备，则需要在初始标签下取消分配该设备，然后在新标签下分配该设备。当您将设备管理器移动到一个不同标签下的工作区时，"Available Devices"（可用设备）和 "Allocated Devices"（已分配的设备）列表将随之更改以反映正确的上下文。

如果文件浏览器窗口未显示，请手动打开该窗口，然后导航到根目录 /。在此目录中，导航到已分配的设备以查看其内容。

▼ 如何在 Trusted Extensions 中对设备取消分配

1. **对设备取消分配。**
   a. **转到显示有 "Device Manager"（设备管理器）的工作区。**
   b. **从已分配设备列表中移动要取消分配的设备。**
2. **移除介质。**
3. **在 "Deallocation"（解除分配）对话框中单击 "OK"（确定）。**
   该设备现在可供其他授权用户使用。

▼ 如何在 Trusted Extensions 中承担角色

与 Oracle Solaris OS 不同，Trusted Extensions 提供了用于承担角色的 GUI。

1. **在可信符号右侧单击您的用户名。**
2. **从菜单中选择角色名称。**
3. **键入角色口令，然后按回车键。**
   此操作将确认您可以合法承担此角色。出于安全方面的考虑，在键入时不显示口令。

注意 – 键入口令时，请确保光标在 "Change Password"（更改口令）对话框上，并确保已显示可信符号。如果光标不在该对话框上，则可能会无意中将口令键入到其他窗口中，这样其他用户可能会看到口令。如果未显示可信符号，则可能是有人在试图窃取您的口令。请立即与security administrator（安全管理员）联系。

接受角色口令后，当前工作区将变为角色工作区。现在您处于全局区域中。您可以执行角色权限配置文件允许您执行的操作。

▼ 如何更改工作区标签

利用在 Trusted Extensions 中设置工作区标签这一功能，可以方便地在同一多级别会话内在不同的标签下工作。

使用此过程可在不同标签下的同一工作区中工作。要创建不同标签的工作区，请参见第 47 页中的“如何在最小标签下添加工作区”。

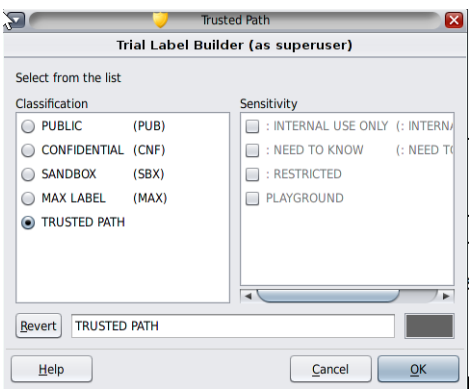
开始之前 必须登录到多级别会话。

1. **单击可信窗口条中的窗口标签。**
   您还可以单击某个工作区面板。

2. **单击 "Change Workspace Label"（更改工作区标签）。**

3. **从标签生成器中选择一个标签。**
   下图显示用户单击 "Trusted Path"（可信路径）按钮。

图 3–4 "Label Builder"（标签生成器）



在单击此按钮后，用户可以从用户标签中进行选择。工作区标签将更改为新标签。在标签以颜色进行编码的系统上，新窗口将用新颜色进行标记。

4. **如果系统提示您输入口令，请提供您的口令。**
   如果您的站点在每个区域中运行一个单独的命名服务，则当用户进入新标签下的工作区时，会提示用户输入口令。

▼ 如何在最小标签下添加工作区

利用在 Trusted Extensions 中设置工作区标签这一功能，可以方便地在同一多级别会话内在不同的标签下工作。您可以在最小标签下添加工作区。

要更改当前工作区的标签，请参见第 46 页中的 “如何更改工作区标签”。

开始之前 必须登录到多级别会话。

1. **要在最小标签下创建工作区，请执行以下操作：**

   a. **在工作区面板上单击鼠标右键。**

   b. **从菜单中选择 "Preferences"（首选项）。**

   c. **在 "Number of Workspaces"（工作区数目）字段中增大数目。**
   将在最小标签下创建新工作区。也可以使用此对话框命名工作区。名称将显示在工具提示中。

   d. **可选为工作区命名。**
   将鼠标悬停在工作区面板上时，其名称将显示在工具提示中。

2. **要更改工作区标签，请选择一个工作区面板并更改其标签。**
   有关详细信息，请参见第 46 页中的 “如何更改工作区标签”。

▼ 如何切换到其他标签下的工作区

开始之前 必须登录到多级别会话。

1. **单击不同颜色的工作区面板。**

2. **如果系统提示您输入口令，请提供您的口令。**
   如果您的站点在每个区域中运行一个单独的命名服务，则当用户进入新标签下的工作区时，会提示用户输入口令。

故障排除 如果登录到单级别会话，则必须先注销才能在不同的标签下工作。然后，在所需的标签下登录。如果允许，则也可以登录到多级别会话。

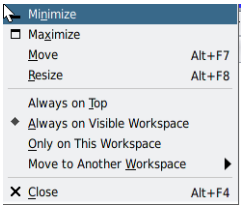
▼ 如何将窗口移动到其他工作区

当您将某个窗口拖动到一个不同标签下的工作区中时，该窗口将保留其原始标签。该窗口中的任何操作都是在该窗口的标签下执行的，而不是在包含该窗口的工作区的标签下执行的。如果希望比较信息，移动窗口很有帮助。您可能还希望在其他标签下使用应用程序，而不在工作区之间移动。

1 **在面板显示屏幕中，将窗口从一个面板拖动到另一个面板。**

已拖动的窗口此时将显示在第二个工作区中。

2 **要在所有工作区中显示该窗口，请从标题栏中的右键菜单中选择 "Always Visible"（始终可见）。**



选定的窗口现在将出现在每个工作区中。

▼ 如何确定文件标签

通常，文件的标签是显而易见的。但是，如果系统允许您查看标签级别低于当前工作区的文件，则文件的标签可能不是显而易见的。特别要指出的是，文件的标签可能与文件浏览器的标签不同。

- **使用文件浏览器。**

提示 – 也可以使用 "Trusted Path"（可信路径）菜单中的 "Query Label"（查询标签）菜单项。

▼ 如何在具有不同标签的窗口之间移动数据

与在 Oracle Solaris 系统上一样，您可以在 Trusted Extensions 中的窗口之间移动数据。但是，数据必须位于同一标签下。在具有不同标签的窗口之间传输信息时，会提升或降低该信息的敏感度。

开始之前 站点的安全策略必须允许这种类型的传输，包含区域必须允许重新标记，而且您必须有权在标签之间移动数据。

因此，管理员必须已经完成以下任务：

- 《Trusted Extensions 配置和管理》中的“如何在有标签区域中允许重新为文件设置标签”
- 《Trusted Extensions 配置和管理》中的“如何允许用户更改数据的安全级别”

必须登录到多级别会话。

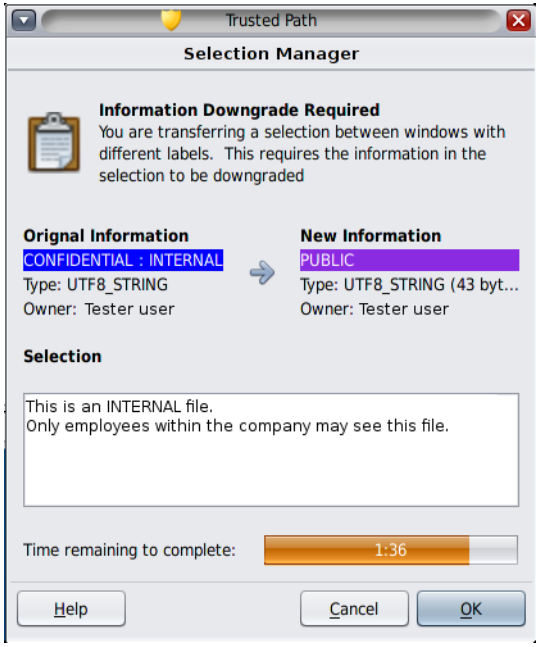
1 **在两个标签下创建工作区。**
有关详细信息，请参见第 47 页中的 “如何在最小标签下添加工作区”。

2 **确认源文件的标签。**
有关详细信息，请参见第 48 页中的 “如何确定文件标签”。

3 **将具有源信息的窗口移动到目标标签下的工作区。**
有关详细信息，请参见第 48 页中的 “如何将窗口移动到其他工作区”。

4 **突出显示要移动的信息，并在目标窗口中粘贴选定内容。**
将显示 "Selection Manager Confirmation"（选择管理器确认）对话框。

图 3–5 "Selection Manager Confirmation"（选择管理器确认）对话框



5 **查看 "Selection Manager Confirmation"（选择管理器确认）对话框，然后确认或取消事务。**

此对话框：

- 描述需要确认事务的原因。
- 确定源文件的标签和所有者。
- 确定目标文件的标签和所有者。
- 确定为传输所选择的数据类型、目标文件类型和数据大小（以字节为单位）。缺省情况下，所选数据以文本格式显示。
- 指示用户可用来完成事务的剩余时间。时间的长短以及是否使用计时器取决于站点的配置。

▼ 如何升级多级别数据集中的数据

Trusted Extensions 中的多级别数据集使重新标记文件这一任务变得简单。有关多级别数据集的更多信息，请参见《Trusted Extensions 配置和管理》中的“需要为文件重新设置标签的多级别数据集”。

开始之前 您必须获得授权才能重新标记文件。您可以对两个或更多标签进行操作，其中一个标签支配另一个标签。

多级别数据集至少挂载在一个有标签区域中，挂载名称在挂载数据集的每个区域中都是相同的，例如 `/multi`。

要允许重新标记，管理员必须已经完成以下任务：

- 《Trusted Extensions 配置和管理》中的“如何创建和共享多级别数据集”
- 《Trusted Extensions 配置和管理》中的“如何在有标签区域中允许重新为文件设置标签”
- 《Trusted Extensions 配置和管理》中的“如何允许用户更改数据的安全级别”

必须登录到多级别会话。

1 **在较高级别标签下创建工作区。**

例如，要将文件从 `PUBLIC` 升级到 `INTERNAL`，请在 `INTERNAL` 标签下创建工作区。

有关详细信息，请参见第 47 页中的 “如何在最小标签下添加工作区”。

2 **打开终端窗口并列出包含要升级的文件的目录。**

在此示例中，文件名为 `temppub1`。

```
$ ls /multi/public
temppub1
```

3 **重新标记该文件。**

```
$ setlabel "cnf : internal" /multi/public/temppub1
```

4 **验证标签更改。**

```
$ getlabel  /multi/public/temppub1
/multi/public/temppub1: "CONFIDENTIAL : INTERNAL USE ONLY"
```

5 **可选将文件移动到目标标签下的目录中。**

```
$ mv /multi/public/temppub1 /multi/internal/temppub1
```

▼ 如何降级多级别数据集中的数据

要降级数据，需要先将文件移动到其目标目录中，然后重新标记该文件。有关说明，请参见《Trusted Extensions 配置和管理》中的“需要为文件重新设置标签的多级别数据集”。

开始之前 您必须获得授权才能对文件进行降级。管理员至少在一个有标签区域中挂载了多级别数据集，且对所有您可以访问的数据集挂载使用了标准名称（例如 `/multi`），并且已允许在该区域中重新标记。

因此，管理员必须已经完成以下任务：

- 《Trusted Extensions 配置和管理》中的“如何创建和共享多级别数据集”
- 《Trusted Extensions 配置和管理》中的“如何在有标签区域中允许重新为文件设置标签”
- 《Trusted Extensions 配置和管理》中的“如何允许用户更改数据的安全级别”

必须登录到多级别会话。

1 **在源文件标签下创建工作区。**

例如，创建 `internal` 工作区。

有关详细信息，请参见第 47 页中的 “如何在最小标签下添加工作区”。

2 **打开终端窗口并打开配置文件 shell。**

```
% pfbash
$
```

3 **可选确认源文件的标签及文件所在目录。**

有关详细信息，请参见第 48 页中的 “如何确定文件标签”。

注 – 如果源文件位于与其父目录相同的标签下，则无法将其就地降级。必须移动文件。移动文件是一种特权操作。

4 **将源文件移动到目标标签下的目录中。**

```
$ mv /multi/internal-directory/file /multi/public-directory
```

5 **将标签更改为目标目录的标签。**

```
$ cd /multi/public-directory
$ setlabel public file
```

6 **可选验证文件是否已重新标记。**

```
$ getlabel /multi/public-directory/file
/multi/public-directory/file: PUBLIC
```

可以在 PUBLIC 标签下编辑文件。

示例 3–6 更改目录的标签

在此示例中，授权用户将重新标记目录。

首先，用户将从目录中移动或删除所有文件。

```
$ getlabel /multi/conf
/multi/conf: CONFIDENTIAL : NEED TO KNOW
$ mv /multi/conf/* /multi/confNTK/temp
```

然后，用户设置目录的标签并验证新标签。

```
$ setlabel "Confidential : Internal Use Only" /multi/conf
getlabel /multi/conf
/multi/conf: "CONFIDENTIAL : INTERNAL USE ONLY"
```

◆ ◆ ◆ 第 4 章

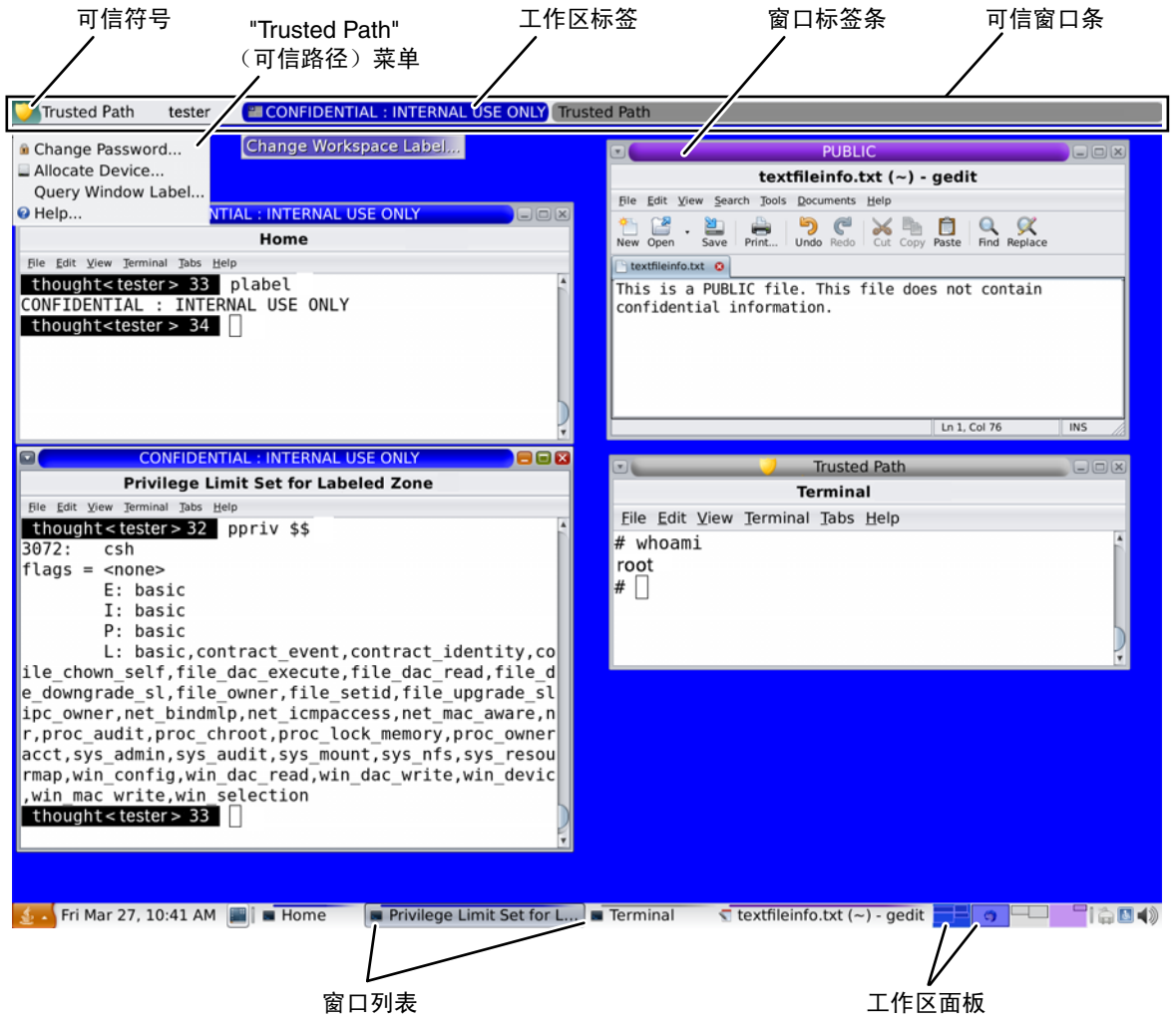
Trusted Extensions 的元素（参考信息）

本章介绍了 Trusted Extensions 的关键元素。本章包含以下主题：

Trusted Extensions 的可见功能

成功完成登录过程后（如第 2 章，登录到 Trusted Extensions（任务）中所述），用户便可以使用 Trusted Extensions 了。使用过程中，用户需要遵守安全限制。特定于 Trusted Extensions 的限制包括系统标签范围、用户安全许可，以及用户是选择单级别会话还是多级别会话。如下图所示，有多项功能使配置有 Trusted Extensions 的系统有别于 Oracle Solaris 系统。

图 4–1 Trusted Extensions 多级别桌面



- **标签显示**—所有窗口、工作区、文件和应用程序都具有一个标签。桌面提供了标签条和用于查看实体标签的其他指示符。
- **可信窗口条**－此窗口条是一种特殊的图形安全机制。在每个工作区中，此窗口条显示在屏幕顶部。
- **从工作区对应用程序的有限访问** – 从工作区中，只能访问您的帐户中允许的那些应用程序。
- **"Trusted Path"（可信路径）菜单**－可以从可信符号访问该菜单。

Trusted Extensions 桌面上的标签

如第 17 页中的 “强制访问控制”中所述，Trusted Extensions 中的所有应用程序和文件都带有标签。Trusted Extensions 在以下位置显示标签：

- 窗口标题栏上方的窗口标签条
- 窗口列表中窗口图标上方的标签颜色条
- 可信窗口条中的窗口标签指示符
- 来自 "Trusted Path"（可信路径）菜单的查询窗口标签指示符，它显示由指针位置指定的窗口或窗口图标的标签

此外，面板的颜色表示工作区的标签。

图 4–2 表示具有不同标签的工作区的面板

图 4–1 显示了标签在 Trusted Extensions 桌面上的显示方式。另外，"Query Window Label"（查询窗口标签）菜单项可用来显示窗口的标签。有关图示，请参见图 3–2。

可信窗口条

可信窗口条显示在屏幕顶部。

图 4–3 桌面上的可信窗口条

可信窗口条的作用是让您可以直观地确认自己处于合法的 Trusted Extensions 会话中。该窗口条可显示您何时在与可信计算基 (trusted computing base, TCB) 进行交互。该窗口条还显示您当前的工作区和当前窗口的标签。可信窗口条不能移动，也不会被其他窗口或对话框遮蔽。

可信窗口条具有以下元素：

- **可信符号** – 在屏幕焦点与安全相关时显示
- **窗口标签** – 当屏幕焦点与安全无关时，显示活动窗口的标签
- **角色标记** – 位于可信符号的右侧，在帐户名称之前，如果帐户是一个角色帐户，会显示一个帽子图标
- **当前帐户名称** – 位于可信符号的右侧，显示工作区中新进程的所有者名称

- **有标签窗口** – 显示工作区中所有窗口的标签

可信符号

只要您访问 TCB 的任意部分，可信符号就会显示在可信窗口条区域的左侧。

当鼠标指针聚焦在不会影响安全性的窗口或屏幕区域时，可信符号不会显示。可信符号无法仿造。如果您看到了该符号，便可以确定您正在安全地与 TCB 进行交互。

注意 – 如果工作区中没有可信窗口条，请联系security administrator（安全管理员）。您的系统可能存在严重问题。

在登录期间或者锁定屏幕后，可信窗口条绝对不应显示。如果在这种情况下仍然显示了可信窗口条，请立即与管理员联系。

窗口标签指示符

窗口标签指示符显示活动窗口的标签。在多级别会话中，指示符可帮助您识别同一工作区中具有不同标签的窗口。指示符还可以表明您正在与 TCB 交互。例如，当您更改口令时，"Trusted Path"（可信路径）指示符会显示在可信窗口条中。

Trusted Extensions 中的设备安全性

在 Trusted Extensions 中，缺省情况下，设备由设备分配要求来提供安全保护。用户如果未显式获得分配设备的授权，则不能使用设备。已分配的设备不能由其他用户使用。正在使用的具备一个标签的设备不能同时具备另一个标签并被使用，除非为该设备取消分配第一个标签并为其分配另一个标签。

要使用设备，请参见第 43 页中的“如何在 Trusted Extensions 中分配设备”。

Trusted Extensions 中的文件和应用程序

Trusted Extensions 中的所有应用程序都有一个敏感级别，通过其标签进行标识。在所有数据事务中，应用程序都是**主体**。主体必须支配主体尝试访问的**对象**。对象可能是文件，有时也可能是其他进程。应用程序的标签信息显示在窗口标签条中。当窗口处于打开或最小化状态时，标签可见。当指针位于应用程序的窗口中时，应用程序的标签还会显示在可信窗口条中。

在 Trusted Extensions 中，文件是数据事务中的对象。只有应用程序标签能够支配文件标签时，应用程序才能访问文件。可以从与文件具有相同标签的窗口中查看文件。

有些应用程序使用初始化文件来为用户配置环境。您的起始目录中有两个特殊文件，可帮助您访问每个标签的初始化文件。这些文件使得一个标签的应用程序可以使用在另一个标签的目录中生成的初始化文件。这两个特殊的文件为 `.copy_files` 和 `.link_files`。

`.copy_files` 文件

`.copy_files` 文件存储初次切换到较高级别标签工作区时要复制的文件名。此文件存储在最小标签的起始目录中。如果您有一个应用程序始终使用某个特定名称写入起始目录中的某个文件，此文件将非常有用。通过 `.copy_files` 文件，您可以指定应用程序更新每个标签的文件。

`.link_files` 文件

`.link_files` 文件存储当您首次切换到较高级别标签工作区时要链接的文件名。此文件存储在最小标签的起始目录中。如果某个特定文件需要在多个标签上可用，但在每个标签必须具有完全相同的内容，`.link_files` 文件将非常有用。

Oracle Solaris OS 中的口令安全性

用户定期更改口令可缩短入侵者使用非法获取的口令的机会窗口。因此，站点的安全策略可能会要求您定期更改口令。Oracle Solaris OS 可设定口令内容要求并且可实施口令重置要求。下面是可能的重置要求：

- **两次更改之间的最少天数**－防止您或其他人在指定天数内更改口令。
- **两次更改之间的最大天数**－要求您在指定天数后更改口令。
- **处于非活动状态的最大天数**—如果未更改口令，将在处于非活动状态时间达指定天数后锁定帐户。
- **失效日期**—要求您在指定日期之前更改口令。

如果您的管理员实施了上述的某个选项，您在截止日期之前将会收到一封电子邮件，通知您更改口令。

口令可能具有内容方面的条件。在 Oracle Solaris OS 中，口令至少必须满足以下条件：

- 口令必须至少包含 8 个字符。
- 口令必须至少包含两个字母字符以及一个数字字符或一个特殊字符。
- 新口令必须不同于以前的口令。不能使用对旧口令进行颠倒或循环移位而得到的口令。在进行此项比较时，大写字母和小写字母将被同等对待。
- 新口令必须至少包含三个不同于旧口令的字符。在进行此项比较时，大写字母和小写字母将被同等对待。
- 口令必须不容易猜到。不要使用常用词或专有名词。试图入侵帐户的程序和个人可以使用列表来尝试猜测用户的口令。

您可以使用 "Trusted Path"（可信路径）菜单中的 "Change Password"（更改口令）菜单项来更改口令。有关步骤，请参见第 41 页中的 “如何在 Trusted Extensions 中更改口令”。

Trusted Extensions 中的工作区安全性

在 Trusted Extensions 中，工作区和桌面应用程序可以识别标签。应用程序在当前工作区的标签下运行，并仅在打开该应用程序的进程的标签下显示信息。

可信桌面的安全功能的行为和位置如下所述：

- "Trusted Path"（可信路径）菜单位于可信窗口条中。
- 将鼠标悬停在窗口上方时，面板上任务列表中某个窗口的标签名称将显示在一个工具提示中。同样，切换区域中某个工作区的标签名称也将显示在该工具提示中。
- 要更改某个角色，请在可信窗口条中单击帐户名称，然后选择角色。
- 要在特定标签下添加工作区，请选择现有的某个工作区，然后更改其标签。
- 对桌面进行了相应配置，使每个工作区可以反映出您在该工作区中工作时所处于的标签的颜色。底部的窗口条上的面板也显示了标签颜色。

词汇表

access control list, ACL（访问控制列表） Oracle Solaris OS 的安全功能。ACL 对 discretionary access control, DAC（自主访问控制）进行了扩展，它使用应用于特定用户和特定组的权限规范（ACL 条目）的列表。使用 ACL，可以实现比标准 UNIX permissions（权限）所提供的控制更加精细的控制。

access permission（访问权限） 大多数计算机系统的一项安全功能。访问权限向用户授予读取、写入、执行或查看文件或目录名称的权利。另请参见 discretionary access control, DAC（自主访问控制）和 mandatory access control, MAC（强制访问控制）。

account label range（帐户标签范围） 由安全管理员指定给用户或 role（角色）以便在配置有 Trusted Extensions 的系统上工作的标签集合。标签范围的上限由 user clearance（用户安全许可）定义，下限由用户的 minimum label（最小标签）定义。该集合仅包含良构的标签。

accreditation range（认可范围） 准许一类用户或资源使用的标签集合：另请参见 system accreditation range（系统认可范围）、user accreditation range（用户认可范围）、label encodings file（标签编码文件）和 network accreditation range（网络认可范围）。

administrative label（管理性标签） 仅适用于管理性文件的两个特殊标签：`ADMIN_LOW` 和 `ADMIN_HIGH`。`ADMIN_LOW` 是系统中的最低级别标签，未包含任何区间。此标签受系统中的所有标签严格支配。`ADMIN_LOW` 上的信息可供正在 `ADMIN_LOW` 标签下工作的某个 role（角色）中的所有用户读取，但只能由一个用户进行写入。`ADMIN_HIGH` 是系统中的最高级别标签，包含所有区间。此标签严格支配系统中的所有标签。只有在 `ADMIN_HIGH` 上工作的角色中的用户可以读取 `ADMIN_HIGH` 上的信息。管理性标签用作角色和系统的标签或安全许可。另请参见 dominating label（支配标签）。

allocatable device（可分配设备） Oracle Solaris OS 的安全功能。一个可分配设备一次只能由一个用户使用，可以在系统中导入或导出数据。security administrator（安全管理员）决定哪些用户有权访问哪些可分配设备。可分配设备包括磁带机、软盘驱动器、音频设备和 CD-ROM 设备。另请参见 device allocation（设备分配）。

audit ID, AUID（审计 ID） Oracle Solaris OS 的安全功能。审计 ID 代表登录用户。AUID 在用户承担某个角色后会保持不变，因此可用来标识用户以便 auditing（审计）。审计 ID 始终代表用于审计的用户，即使该用户获得了 effective UID/GID（有效 UID/GID）。另请参见 user ID, UID（用户 ID）。

auditing（审计） Oracle Solaris OS 的安全功能。审计是指捕获系统上的用户活动和其他事件，然后将这些信息存储在一组称为**审计迹**的文件中的过程。审计会生成系统活动报告，以便履行站点安全策略。

authorization（授权） Oracle Solaris OS 的安全功能。授权可授予用户执行某项操作的权限，未授权情况下安全策略会禁止该操作。security administrator（安全管理员）为权限配置文件指定授权。然后，将权限配置文件指定给用户或 role（角色）帐户。某些命令和操作要求用户具有必需的授权才能完全发挥作用。另请参见 privilege（特权）。

classification（等级） clearance（安全许可）或 label（标签）的一个组件。等级表示有层次的安全性级别，例如 TOP SECRET（绝密）或 UNCLASSIFIED（未分类）。

clearance（安全许可） 用于定义 label range（标签范围）上界的一个 label（标签）。安全许可具有两个组件：一个 classification（等级）以及零个或多个区间。安全许可无需是 well-formed label（良构的标签）。安全许可定义了理论上的界限，而不一定是实际的标签。另请参见 user clearance（用户安全许可）、session clearance（会话安全许可）和 label encodings file（标签编码文件）。

compartmented mode workstation, CMW（分隔模式工作站） 一种计算系统，它满足了《Security Requirements for System High and Compartmented Mode Workstations》（DIA 文档编号 DDS-2600-5502-87）所定义的对可信工作站的政府要求。确切地说，它为 UNIX 工作站定义了一个基于 X Window System 的可信操作系统。

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）。区间代表可能需要访问该信息的一组用户，例如，工程部或多学科项目团队。

covert channel（隐蔽信道） 不以正常方式进行数据通信的一个通信信道。使用隐蔽信道，进程能够以违反安全策略意图的方式间接地传输信息。

deallocated device（取消分配的设备） Oracle Solaris OS 的安全功能。取消分配的设备是指不再分配给某个用户供其专用的设备。另请参见 device allocation（设备分配）。

device allocation（设备分配） Oracle Solaris OS 的安全功能。设备分配是一种保护 allocatable device（可分配设备）上的信息不被分配有该设备的用户之外的用户访问的机制。设备取消分配后，将运行设备清除脚本来清除设备中的信息，然后设备才可重新供其他用户访问。在 Trusted Extensions 中，设备分配是由 Device Manager（设备管理器）执行的。

Device Manager（设备管理器） Trusted Extensions 的一个可信应用程序。此 GUI 用于配置设备，以及分配和取消分配设备。设备配置包括向设备添加授权要求。

device（设备） 请参见 allocatable device（可分配设备）。

discretionary access control, DAC（自主访问控制） 一种访问控制机制，允许文件或目录的所有者对其他用户授予或拒绝访问权限。所有者可以将读取、写入和执行 permissions（权限）指定给所有者、所有者所属的用户组以及一个名为“其他”的类别（指所有其他未指定的用户）。所有者还可以指定 access control list, ACL（访问控制列表）。通过 ACL，所有者可以将权限明确指定给更多用户和组。与之相对的是 mandatory access control, MAC（强制访问控制）。

disjoint label（没有交集的标签） 请参见 dominating label（支配标签）。

dominating label（支配标签） 当两个标签相比较时，如果其中一个标签的 classification（等级）组件高于或等于另一标签的等级且其 compartment（区间）组件包含另一标签的所有区间组件，则该标签称为支配标签。如果组件都是相同的，则我们可以说这两个标签相互支配，而且是**平等**的。如果一个标签支配另一个标签且标签不是平等的，则我们可以说第一个标签**严格支配**另一个标签。如果两个标签不是平等的且任何一个标签都不处于支配地位，则这两个标签是**没有交集的**。

downgraded label（降级的标签） 一种对象 label（标签），标签值已更改为不再支配标签先前值的一个值。

effective UID/GID（有效 UID/GID） Oracle Solaris OS 的安全功能。有效 ID 在必要时会覆盖实际 ID，以便运行某个特定程序或某个程序的某个选项。当某个命令或操作必须由某个特定用户来运行时（通常是必须由 root 用户运行），security administrator（安全管理员）会在 rights profile（权限配置文件）中为该命令或操作指定有效 UID。有效组 ID 的使用方式与之相同。请注意，与在常规 UNIX 系统中一样，使用 `setuid` 命令时，该命令可能会由于缺少特权而无法正常运行。

evaluatable configuration（可评估配置） 满足一系列政府安全要求标准的计算机系统。另请参见 extended configuration（扩展的配置）。

extended configuration（扩展的配置） 因修改违反了安全策略而不再是 evaluatable configuration（可评估配置）的计算机系统。

fallback mechanism（回退机制） 用于在 `tnrhtp` 数据库中指定 IP 地址的一种快捷方法。对于 IPv4 地址，回退机制将 `0` 识别为子网的通配符。

gateway（网关） 具有一个以上网络接口的主机。此类主机可以用于连接两个或更多个网络。当网关是 Trusted Extensions 主机时，网关可将通信限定到某个特定的标签。

group ID, GID（组 ID） Oracle Solaris OS 的安全功能。 GID 是一个整数，用于标识具有公有访问权限的一组用户。另请参见 discretionary access control, DAC（自主访问控制）。

host template（主机模板） `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。

host type（主机类型） host（主机）的一种等级。该等级用于网络通信。主机类型的定义存储在 `tnrhtp` 数据库中。主机类型决定了是否使用 CIPSO 网络协议与网络中的其他主机进行通信。**网络协议**是指用于对通信信息进行打包的规则。

host（主机） 连接到网络的一台计算机。

label builder（标签生成器） Trusted Extensions 的一个可信应用程序。通过此 GUI，用户可以选择会话安全许可或会话标签。clearance（安全许可）或 label（标签）必须位于 security administrator（安全管理员）指定给用户的 account label range（帐户标签范围）内。

label encodings file（标签编码文件） 由 security administrator（安全管理员）管理的一个文件。该编码文件包含所有有效安全许可和标签的定义。该文件还定义了 system accreditation range（系统认可范围）和 user accreditation range（用户认可范围），并定义了关于站点上的打印输出的安全信息。

label range（标签范围） 上限由 clearance（安全许可）或最大标签界定、下限由最小标签界定的由良构的标签组成的任意标签集合。标签范围用于实施 mandatory access control, MAC（强制访问控制）。另请参见 label encodings file（标签编码文件）、account label range（帐户标签范围）、accreditation range（认可范围）、network accreditation range（网络认可范围）、session range（会话范围）、system accreditation range（系统认可范围）和 user accreditation range（用户认可范围）。

label view（标签视图） 一项安全功能，它显示 administrative label（管理性标签），或使用未分类的占位符替代管理性标签。例如，如果安全策略禁止显示标签 ADMIN_HIGH 和 ADMIN_LOW，则可以使用标签 RESTRICTED 和 PUBLIC 来替代。

labeled workspace（有标签工作区） 与某个标签关联的一个工作区。有标签工作区会将从该工作区启动的每项活动都标上该工作区的 label（标签）。当用户将某个窗口移动到具有其他标签的工作区时，所移动的窗口会一直保留其原来的标签。可信桌面上的每个工作区都是带标签的。两个工作区可以与同一个标签相关联。

label（标签） 也称为敏感标签。标签用于指示实体的安全级别。实体是指文件、目录、进程、设备或网络接口。实体标签用于确定在特定的事务中是否允许访问该实体。标签具有两个组件：一个 classification（等级）（指示安全层次级别），以及零个或多个区间（定义可在给定等级上访问实体的用户）。另请参见 label encodings file（标签编码文件）。

least privilege（最小特权） 请参见 principle of least privilege（最小特权原则）。

mandatory access control, MAC（强制访问控制） 一种由系统实施的访问控制机制，使用安全许可和标签来实施安全策略。clearance（安全许可）或 label（标签）是一个安全级别。MAC 将用户运行的程序与用户选择在会话中工作时所处的安全级别相关联。然后，MAC 仅允许访问同一级别或更低级别的信息、程序和设备。MAC 还阻止用户对更低级别的文件执行写入操作。没有特殊授权或特权不能覆盖 MAC。与之相对的是 discretionary access control, DAC（自主访问控制）。

minimum label（最小标签） 指定给用户的一个 label（标签），是用户可以工作的标签集合的下界。用户首次开始一个 Trusted Extensions 会话时，最小标签是用户的缺省标签。在登录时，用户可以选择另外一个标签作为初始标签。

此外，它还是授予任何非管理用户的最低级别标签。最小标签由 security administrator（安全管理员）指定，用于定义 user accreditation range（用户认可范围）的下限。

network accreditation range（网络认可范围） 允许 Trusted Extensions 主机在其中进行网络通信的标签集合。该标签集合可以是一个包含四个独立标签的列表。

object（对象） 一个包含或接收数据的被动实体，例如，数据文件、目录、打印机或其他设备。主体对对象执行操作。在某些情况下，process（进程）可以是对象，例如当您向进程发送信号时。

operator（运算符） 可以指定给负责对系统进行备份的用户的 role（角色）。

ordinary user（一般用户） 除了系统的标准安全策略赋予的权限外，不享有允许例外的特殊授权的用户。通常，一般用户不能承担管理 role（角色）。

permissions（权限） 指示允许哪些用户读取、写入或执行文件或目录（文件夹）的一组代码。用户分为所有者、组（所有者所在的组）和其他（其他任何人）。读取权限（由 *r* 表示）允许用户读取文件的内容，如果是目录，则允许列出文件夹中的文件。写入权限（由 *w* 表示）允许用户对文件进行更改，如果是目录，则允许添加或删除文件。执行权限（由 *e* 表示）允许用户运行文件（如果文件是可执行文件）。如果是目录，则执行权限允许用户读取或搜索目录中的文件。也称为 UNIX 权限或权限位。

principle of least privilege（最小特权原则） 该安全准则将用户限制为仅允许使用执行其工作所需的功能。在 Oracle Solaris OS 中，通过按需向程序提供特权来应用该原则。特权是按需提供的，并且仅适用于特定用途。

privileged process（特权进程） Oracle Solaris OS 的安全功能。特权 process（进程）使用所指定的特权来运行。

privilege（特权） Oracle Solaris OS 的安全功能。特权是指由 security administrator（安全管理员）授予某个程序的权限。可以要求使用特权来覆盖安全策略的某个方面。另请参见 authorization（授权）。

process（进程） 一个正在运行的程序。Trusted Extensions 进程具有 Oracle Solaris 安全属性，例如 user ID, UID（用户 ID）、group ID, GID（组 ID）、用户的 audit ID, AUID（审计 ID），以及特权。Trusted Extensions 向每个进程添加一个 label（标签）。

profile shell（配置文件 shell） Oracle Solaris OS 的安全功能。 Bourne shell 的一种版本，用户可以通过它来运行具有安全属性的程序。

profile（配置文件） 请参见 rights profile（权限配置文件）。

reading down（向下读取） subject（主体）所具有的查看它对其 label（标签）具有支配权的 object（对象）的能力。安全策略通常允许向下读取。例如，在 `Secret`（秘密）级别运行的文本编辑器程序可以读取 `Unclassified`（未分类）数据。另请参见 mandatory access control, MAC（强制访问控制）。

rights profile（权限配置文件） Oracle Solaris OS 的安全功能。使用权限配置文件，站点的 security administrator（安全管理员）可以将命令与安全属性捆绑起来。用户授权和特权等属性使得命令得以成功。权限配置文件通常包含相关的任务。配置文件可以指定给用户和角色。

role（角色） Oracle Solaris OS 的安全功能。角色是一个特殊帐户，它为担任该角色的用户提供对具有安全属性的某些应用程序的访问权限，用户执行特定任务时需要访问这些应用程序。

security administrator（安全管理员） 在配置有 Trusted Extensions 的系统上，指定给负责定义和实施安全策略的用户的 role（角色）。安全管理员可以在 system accreditation range（系统认可范围）内的任何标签下工作，可能还有权访问站点上的所有信息。安全管理员可为所有用户和设备配置安全属性。另请参见 label encodings file（标签编码文件）。

security attribute（安全属性） Oracle Solaris OS 的安全功能。实体（例如进程、区域、用户或设备）的与安全相关的一个特性。安全属性包括 user ID, UID（用户 ID）和 group ID, GID（组 ID）等标识值。Trusted Extensions 所特有的属性包括标签和标签范围。请注意，只有特定的一些安全属性适用于一种特定类型的实体。

security policy（安全策略） 包含 DAC、MAC 和标签规则的集合，用于定义可以如何访问信息以及哪些用户可以访问信息。在客户站点上，指的是用于定义在站点上处理的信息的敏感度的规则集合。策略包括用来保护信息免受未经授权访问的措施。

Selection Manager（选择管理器） Trusted Extensions 的一个可信应用程序。当授权用户试图升级或降级信息时，将显示此 GUI。

sensitivity label（敏感标签） 请参见 label（标签）。

session clearance（会话安全许可） 登录时设置的 clearance（安全许可），用于为 Trusted Extensions session（会话）定义标签的上界。如果允许用户设置会话安全许可，则用户可以指定用户的 account label range（帐户标签范围）内的任意值。如果用户帐户是针对强制单级别会话配置的，则会话安全许可设置为由 security administrator（安全管理员）指定的缺省值。另请参见 clearance（安全许可）。

session range（会话范围） 用户在某个 Trusted Extensions 会话期间可访问的标签集合。会话范围的上界由用户的 session clearance（会话安全许可）界定，下限由 minimum label（最小标签）界定。

session（会话） 从登录到 Trusted Extensions 主机到从主机注销之间的时间。trusted stripe（可信窗口条）会出现在所有 Trusted Extensions 会话中，以确认用户当前没有被仿冒系统所欺骗。

single-level configuration（单级别配置） 配置为仅在单个 label（标签）上执行操作的用户帐户。也称为单级别配置。

spoof（电子欺骗） 仿冒某个软件程序以非法获取对系统上信息的访问权限。

strict dominance（严格支配） 请参见 dominating label（支配标签）。

subject（主体） 一个主动实体，通常是代表用户或 role（角色）运行的 process（进程）。主体可导致信息在对象之间流动，还可以更改系统状态。

system accreditation range（系统认可范围） 站点的所有有效标签的集合。该标签集合包括可供站点的 security administrator（安全管理员）和 system administrator（系统管理员）使用的 administrative label（管理性标签）。系统认可范围是在 label encodings file（标签编码文件）中定义的。

system administrator（系统管理员） Oracle Solaris OS 的安全功能。可以将系统管理员 role（角色）指定给负责执行标准系统管理任务（例如设置非安全相关的用户帐户部分）的用户。另请参见 security administrator（安全管理员）。

trusted application（可信应用程序） 被授予了一项或多项特权的应用程序。

trusted computing base, TCB（可信计算基） 配置有 Trusted Extensions 的系统中会影响安全性的部件。TCB 包括软件、硬件、固件、文档和管理规程。可访问安全相关文件的实用程序和应用程序都是可信计算基的部件。

trusted facilities management（可信设备管理） 常规 UNIX 系统中所有与系统管理相关联的活动，加上维护分布式系统和系统所含数据的安全性所需的所有管理活动。

Trusted GNOME 一种有标签的图形桌面，包括一个会话管理器、一个窗口管理器和各种桌面工具。该桌面是一个可完全访问的桌面。

Trusted Path menu（"Trusted Path"（可信路径）菜单） 一个包含 Trusted Extensions 操作的菜单，可通过在前面板的切换区域上按下鼠标右键来显示。菜单选项分为三类：面向工作区的选项、role（角色）担任选项以及与安全相关的任务。

trusted path（可信路径） 指访问允许与 trusted computing base, TCB（可信计算基）进行交互的操作和命令的机制。另请参见 Trusted Path menu（"Trusted Path"（可信路径）菜单）、trusted symbol（可信符号）和 trusted stripe（可信窗口条）。

trusted stripe（可信窗口条） 屏幕保留区域中一个与屏幕同宽的矩形图形。可信窗口条会显示在所有 Trusted Extensions 会话中，以确认有效的 Trusted Extensions 会话。可信窗口条具有两个组件：(1) 一个必需的 trusted symbol（可信符号），用于指示与 trusted computing base, TCB（可信计算基）的交互，(2) 一个 label（标签），用于指示当前窗口或工作区的标签。

trusted symbol（可信符号） 显示在 trusted stripe（可信窗口条）区域左侧的符号。只要用户访问 trusted computing base, TCB（可信计算基）的任何部分，该符号就会显示。

upgraded label（升级的标签） 一种对象 label（标签），标签值已更改为支配标签先前值的一个值。

user accreditation range（用户认可范围） 在特定的站点上，security administrator（安全管理员）可以指定给某个用户的最大标签集合。用户认可范围不包括 administrative label（管理性标签）和仅可供管理员使用的任何标签组合。用户认可范围是在 label encodings file（标签编码文件）中定义的。

user clearance（用户安全许可） 由 security administrator（安全管理员）指定的一个安全许可。用户安全许可定义了用户的 account label range（帐户标签范围）的上界。用户安全许可决定了允许用户在其中工作的最高标签。另请参见 clearance（安全许可）和 session clearance（会话安全许可）。

user ID, UID（用户 ID） Oracle Solaris OS 的安全功能。UID 标识用户以便进行 discretionary access control, DAC（自主访问控制）、mandatory access control, MAC（强制访问控制）和 auditing（审计）。另请参见 access permission（访问权限）。

well-formed label（良构的标签） 可包含在某个范围中的 label（标签），因为 label encodings file（标签编码文件）中的所有适用规则均允许使用该标签。

workspace（工作区） 请参见 labeled workspace（有标签工作区）。

索引