

# 在 Oracle® Solaris 11.1 中管理用户帐户和 用户环境

版权所有 © 1998, 2012, Oracle 和/或其附属公司。保留所有权利。

本软件和相关文档是根据许可证协议提供的，该许可证协议中规定了关于使用和公开本软件和相关文档的各种限制，并受知识产权法的保护。除非在许可证协议中明确许可或适用法律明确授权，否则不得以任何形式、任何方式使用、拷贝、复制、翻译、广播、修改、授权、传播、分发、展示、执行、发布或显示本软件和相关文档的任何部分。除非法律要求实现互操作，否则严禁对本软件进行逆向工程设计、反汇编或反编译。

此文档所含信息可能随时被修改，恕不另行通知，我们不保证该信息没有错误。如果贵方发现任何问题，请书面通知我们。

如果将本软件或相关文档交付给美国政府，或者交付给以美国政府名义获得许可证的任何机构，必须符合以下规定：

#### U.S. GOVERNMENT END USERS:

Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

本软件或硬件是为了在各种信息管理应用领域内的一般使用而开发的。它不应被应用于任何存在危险或潜在危险的应用领域，也不是为此而开发的，其中包括可能会产生人身伤害的应用领域。如果在危险应用领域内使用本软件或硬件，贵方应负责采取所有适当的防范措施，包括备份、冗余和其它确保安全使用本软件或硬件的措施。对于因在危险应用领域内使用本软件或硬件所造成的一切损失或损害，Oracle Corporation 及其附属公司概不负责。

Oracle 和 Java 是 Oracle 和/或其附属公司的注册商标。其他名称可能是各自所有者的商标。

Intel 和 Intel Xeon 是 Intel Corporation 的商标或注册商标。所有 SPARC 商标均是 SPARC International, Inc 的商标或注册商标，并应按照许可证的规定使用。AMD、Opteron、AMD 徽标以及 AMD Opteron 徽标是 Advanced Micro Devices 的商标或注册商标。UNIX 是 The Open Group 的注册商标。

本软件或硬件以及文档可能提供了访问第三方内容、产品和服务的方式或有关这些内容、产品和服务的信息。对于第三方内容、产品和服务，Oracle Corporation 及其附属公司明确表示不承担任何种类的担保，亦不对其承担任何责任。对于因访问或使用第三方内容、产品或服务所造成的任何损失、成本或损害，Oracle Corporation 及其附属公司概不负责。

# 目录

---

前言 .....	7
<b>1 管理用户帐户和用户环境（概述） .....</b>	<b>9</b>
管理用户帐户和用户环境方面的新增功能或更改的功能。 .....	9
影响用户帐户管理的安全更改 .....	10
用户管理器 GUI 简介 .....	10
管理编辑器 (pfedit) .....	11
/var/user/\$USER 子目录 .....	11
groupadd 命令更改 .....	11
失败登录计数通知 .....	11
什么是用户帐户和组? .....	12
用户帐户的组成部分 .....	12
用于指定用户名、用户 ID 和组 ID 的准则 .....	17
用户帐户信息和组信息的存储位置 .....	18
passwd 文件中的字段 .....	19
缺省的 passwd 文件 .....	19
shadow 文件中的字段 .....	21
group 文件中的字段 .....	21
缺省的 group 文件 .....	21
用于获取用户帐户信息的命令 .....	23
用于管理用户、角色和组的命令 .....	24
定制用户的工作环境 .....	25
使用站点初始化文件 .....	26
避免引用本地系统 .....	26
Shell 功能 .....	27
Bash Shell 和 ksh93 Shell 历史记录 .....	28
Bash Shell 和 ksh93 Shell 环境变量 .....	29
定制 Bash Shell .....	31

MANPATH 环境变量 .....	31
PATH 环境变量 .....	31
语言环境变量 .....	32
缺省的文件权限 (umask) .....	33
定制用户初始化文件 .....	34
<b>2 使用命令行界面管理用户帐户 (任务) .....</b>	<b>35</b>
使用 CLI 设置和管理用户帐户 .....	35
使用 CLI 设置和管理用户帐户 (任务列表) .....	35
收集用户信息 .....	36
▼ 如何定制用户初始化文件 .....	37
▼ 如何更改所有角色的帐户缺省值 .....	37
设置用户帐户的准则 .....	38
▼ 如何添加用户 .....	39
▼ 如何修改用户 .....	41
▼ 如何删除用户 .....	42
▼ 如何添加组 .....	42
▼ 如何共享作为 ZFS 文件系统创建的起始目录 .....	43
手动挂载用户的起始目录 .....	44
<b>3 使用用户管理器 GUI 管理用户帐户 (任务) .....</b>	<b>45</b>
用户管理器 GUI 简介 .....	45
启动用户管理器 GUI .....	46
"User Manager" (用户管理器) 面板布局 .....	46
选择缺省名称服务范围 and 类型 .....	47
承担角色或更改用户凭证 .....	48
使用用户管理器 GUI 添加、修改和删除用户和角色 .....	49
▼ 如何使用用户管理器 GUI 添加用户或角色 .....	49
▼ 如何使用用户管理器 GUI 修改用户或角色 .....	51
使用用户管理器 GUI 删除用户或角色 .....	51
使用用户管理器 GUI 管理高级设置 .....	52
使用用户管理器 GUI 管理组 .....	53
使用用户管理器 GUI 管理角色 .....	53
使用用户管理器 GUI 管理权限配置文件 .....	55
使用用户管理器 GUI 管理授权 .....	56

索引 .....59



# 前言

---

《在 Oracle Solaris 11.1 中管理用户帐户和用户环境》是文档集的一部分，该文档集包含 Oracle Solaris 系统管理信息中的重要部分。该指南包含基于 SPARC 和基于 x86 的系统的信息。

本书假设您已经完成以下任务：

- 安装了 Oracle Solaris 软件
- 设置了任何计划使用的网络软件

对于 Oracle Solaris，系统管理员可能感兴趣的新增功能在相应各章中名为“... 的新增功能”的各节中进行了介绍。

---

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。

有关支持的系统，请参见 [Oracle Solaris OS: Hardware Compatibility Lists](#) (Oracle Solaris OS: 硬件兼容性列表)。

---

## 目标读者

本书适用于所有负责对运行 Oracle Solaris 发行版的一个或多个系统进行管理的人员。要使用本书，您应当具备 1 到 2 年的 UNIX 系统管理经验。参加 UNIX 系统管理培训课程可能会对您有所帮助。

## 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 <code>ls -a</code> 列出所有文件。 machine_name% you have mail.
<b>AaBbCc123</b>	用户键入的内容，与计算机屏幕输出的显示不同	machine_name% <b>su</b> Password:
<i>aabbcc123</i>	要使用实名或值替换的命令行占位符	删除文件的命令为 <code>rm filename</code> 。
<i>AaBbCc123</i>	保留未译的新词或术语以及要强调的词	这些称为 <i>Class</i> 选项。 <b>注意</b> ：有些强调的项目在联机时以粗体显示。
<b>新词术语强调</b>	新词或术语以及要强调的词	<b>高速缓存</b> 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#

# 管理用户帐户和用户环境（概述）

---

以下是本章中信息的列表：

- 第 9 页中的“管理用户帐户和用户环境方面的新增功能或更改的功能。”
- 第 12 页中的“什么是用户帐户和组？”
- 第 18 页中的“用户帐户信息和组信息的存储位置”
- 第 24 页中的“用于管理用户、角色和组的命令”
- 第 25 页中的“定制用户的工作环境”

有关管理用户帐户和用户环境的任务相关信息，请参见第 2 章，使用命令行界面管理用户帐户（任务）和第 3 章，使用用户管理器 GUI 管理用户帐户（任务）。

## 管理用户帐户和用户环境方面的新增功能或更改的功能。

以下是本发行版中新增或更改的功能：

- 第 10 页中的“影响用户帐户管理的安全更改”
- 第 10 页中的“用户管理器 GUI 简介”
- 第 11 页中的“管理编辑器 (pfedit)”
- 第 11 页中的“/var/user/\$USER 子目录”
- 第 11 页中的“groupadd 命令更改”
- 第 11 页中的“失败登录计数通知”

## 影响用户帐户管理的安全更改

本发行版中更改了以下功能：

- `password` 命令的状态转换提炼。此更改阐明了哪些用户帐户可以锁定，哪些用户帐户不能锁定。主要更改将影响 LK 和 NL 属性定义；主要更改如下：
  - LK 该帐户已锁定。已运行 `passwd -l` 命令，或者由于身份验证失败次数达到了配置的最大允许次数而自动锁定了帐户。请参见 `policy.conf(4)` 和 `user_attr(4)` 手册页。
  - NL 已为非 UNIX 身份验证配置配置了该帐户。运行了 `passwd -N` 命令。从此发行版开始，处于此状态的帐户无法通过运行 `passwd -l` 锁定，也无法通过运行 `passwd -u` 命令解除锁定。
- 限定授权。可以将授权限定为应用于特定对象，如组、区域或文件名。请参见第 11 页中的“管理编辑器 (`pfedit`)”。
- `profiles` 命令已重写，现在可用来管理本地和 LDAP 范围的权限配置文件。不再支持直接编辑基于角色的访问控制 (Role-based Access Control, RBAC) 文件。
- 本发行版提供了在权限配置文件中设置每用户可插拔验证模块 (Pluggable Authentication Module, PAM) 策略 (`pam_policy`) 的功能。`pam_policy` 必须是 `pam_conf(4)` 格式的文件的绝对路径名，或位于 `/etc/security/pam_policy` 文件中的 `pam.conf(4)` 格式的文件名称。请参见 `pam_user_policy(5)`。

除了在权限配置文件中设置 PAM 策略，您也可以使用 `useradd` 或 `usermod` 命令，在用户的 `user_attr` 条目中直接设置 `pam_policy`。请参见示例 2-1。
- 指定有 "User Security"（用户安全）权限配置文件的用户和角色可以创建新的用户帐户，也可以将自己的部分权限委托给其他帐户，而无需成为 `root` 角色。

有关详细信息，请参见《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”。

## 用户管理器 GUI 简介

您现在可以使用 Oracle Solaris 用户管理器图形用户界面 (graphical user interface, GUI) 设置和管理用户、角色以及组。用户管理器 GUI 可在桌面上使用，是 Visual Panels 项目的一部分。在本发行版中，用户管理器 GUI 替代了 Solaris 管理控制台 GUI。可以使用用户管理器 GUI 执行的任务和可以使用 CLI（例如 `useradd`、`usermod`、`userdel`、`roleadd`、`rolemod`、`roledel` 命令）执行的任务本质上是相同的。

有关使用用户管理器 GUI 的说明，请参见第 3 章，使用用户管理器 GUI 管理用户帐户（任务）以及联机帮助。

## 管理编辑器 (pfedit)

在本发行版中，可以使用管理编辑器 (pfedit) 编辑系统文件。如果系统管理员做了定义，则该编辑器的值为 `$EDITOR`。如果未定义编辑器，则该编辑器缺省为 `vi` 命令。

启动编辑器的操作如下所示：

```
$ pfedit system-filename
```

要使用 `pfedit` 命令编辑系统文件，您或您的角色必须对您要编辑的特定文件具有 `solaris.admin.edit/system-filename` 授权。将此 `auth-sysfilename` 指定给现有权限配置文件可简化那些需要组合使用各种服务管理工具 (Service Management Facility, SMF) 命令和常规文件编辑的过程。例如，如果您具有 `solaris.admin.edit/etc/security/audit_warn` 授权，则您可以编辑 `audit_warn` 文件。

可以使用 `pfedit` 命令编辑位于 `/etc` 目录及其子目录中的大部分配置文件，同时也可以编辑应用程序配置文件，例如 GNOME 和 Firefox 文件。**不能使用 `pfedit` 命令编辑可赋予用户大范围控制系统的权力的系统文件，例如 `/etc/security/policy.conf` 文件。您必须具有 `root` 访问权限才能编辑此类文件。请参见 [pfedit\(1M\)](#) 手册页和《[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）”。**

## `/var/user/$USER` 子目录

每当用户登录并使用 `pam_unix_cred` 模块成功验证后，都会显式创建 `/var/user/$USER` 目录（如果该目录尚不存在）。该目录使应用程序能够在主机系统上存储与特定用户相关的持久性数据。`/var/user/$USER` 目录在建立初始凭证后创建，在使用 `su`、`ssh`、`rlogin` 和 `telnet` 命令更改用户时的辅助验证期间也会创建。`/var/user/$USER` 目录无需任何管理。但是，用户应了解该目录的创建方式，目录功能以及在 `/var` 目录中可见。

## groupadd 命令更改

具有 `solaris.group.manage` 授权的管理员可以创建组。在创建组时，系统会将 `solaris.group.assign/groupname` 指定给管理员，这使管理员可以完全控制该组。随后管理员可以根据需要修改或删除该组。有关更多信息，请参见 [groupadd\(1M\)](#) 和 [groupmod\(1M\)](#) 手册页。

## 失败登录计数通知

现在，即使用户帐户未配置为强制实施登录失败，系统也会针对失败的验证通知用户。无法正确验证的用户将看到类似以下有关成功验证的消息：

```
Warning: 2 failed authentication attempts since last successful authentication. The latest at Thu May 24 12:02 2012.
```

要隐藏此类通知，请创建一个 `~/.hushlogin` 文件。

## 什么是用户帐户和组？

本节介绍了以下信息：

- [第 12 页](#)中的“用户帐户的组成部分”
- [第 17 页](#)中的“用于指定用户名、用户 ID 和组 ID 的准则”

一项基本的系统管理任务就是在站点为每个用户设置一个用户帐户。典型的用户帐户包括在没有系统的 `root` 口令的情况下，用户登录和使用系统时所需的信息。[第 12 页](#)中的“用户帐户的组成部分”中介绍了用户帐户组件。

在设置用户帐户时，您可以将用户添加到某个预定义的用户组中。组的典型用途是为文件和目录设置组权限，从而只允许属于该组的那些用户进行访问。

例如，可能有一个目录中包含只应当由少数几个用户访问的机密文件。您可以设置一个名为 `topsecret` 的组，将参与 `topsecret` 项目的用户包括在其中。此外，您可以为 `topsecret` 组设置对 `topsecret` 文件的读取权限。这样，只有 `topsecret` 组中的用户才能够读取这些文件。

**角色**是一种特殊类型的用户帐户，用于为选定的用户授予特殊特权。有关详细信息，请参见《[Oracle Solaris 11.1 管理：安全服务](#)》中的“[基于角色的访问控制（概述）](#)”。

## 用户帐户的组成部分

以下几节介绍了用户帐户的各个组件。

### 用户名（登录名）

用户名也称为**登录名**，使用它用户可以访问其各自的系统和具备适当访问权限的远程系统。必须为所创建的每个用户帐户都选择一个用户名。

建议建立一种标准方法来指定用户名，以便于跟踪它们。而且，用户名应便于用户记忆。在选择用户名时，一个简单的方案就是使用用户名字的首字母和姓氏的前七个字母。例如，`Ziggy Ignatz` 的用户名为 `zignatz`。如果使用此方案会产生重名，则可以使用用户第一个名字的首字母、中间名字的首字母和姓氏的前六个字母。例如，`Ziggy Top Ignatz` 的用户名为 `ztignatz`。

如果使用此方案仍产生重名，请考虑使用下面的方案来创建用户名：

- 用户第一个名字的首字母、中间名字的首字母和姓氏的前五个字母
- 数字 1、2 或 3，依此类推，直到用户名唯一

---

注 – 每个新的用户名都必须不同于系统或者 NIS 或 NIS 域已知的任何邮件别名。否则，邮件可能会传送到使用该别名的用户（而非实际用户）。

---

有关设置用户名（登录名）的详细准则，请参见第 17 页中的“用于指定用户名、用户 ID 和组 ID 的准则”。

## 用户 ID 号

每个用户名都有一个与之相关联的用户标识 (user identification, UID) 号。UID 号在任何用户尝试登录的系统中标识用户名。系统可以使用 UID 号来标识文件和目录的属主。如果在许多不同的系统上为同一个人创建用户帐户，请始终使用相同的用户名和用户 ID 号。这样，用户可以在系统之间方便地移动文件，而不会出现所有权问题。

UID 号必须是一个小于或等于 2147483647 的整数。UID 号是一般用户帐户和特殊系统帐户所必需的。下表列出了为用户帐户和系统帐户保留的 UID 号。

表 1-1 保留的 UID 号

UID 号	用户帐户或登录帐户	说明
0 – 99	root、daemon、bin、sys，等等	保留供操作系统使用
100 – 2147483647	一般用户	通用帐户
60001 和 65534	nobody 和 nobody4	NFS 匿名用户
60002	noaccess	不可信用户

请勿指定 0 到 99 的 UID。保留这些 UID 以供 Oracle Solaris 分配。按照定义，root 总是具有 UID 0，daemon 具有 UID 1，而伪用户 bin 具有 UID 2。此外，您应该为 uucp 登录和伪用户登录（例如，who、tty 和 ttytype）提供较低的 UID，以便使它们出现在 passwd 文件的开头。

有关设置 UID 的其他准则，请参见第 17 页中的“用于指定用户名、用户 ID 和组 ID 的准则”。

与用户名（登录名）一样，应采用一个方案来指定唯一的 UID 号。某些公司会指定唯一的员工编号。这样，管理员可以在员工编号的基础上添加一个编号，以便为每个员工创建一个唯一的 UID 号。

为了最大限度地降低安全风险，应当避免重新使用已删除帐户的 UID。如果必须重新使用某个 UID，请“彻底清除以前的帐户”，以便新用户不会受到先前用户属性集的影响。例如，先前的用户可能会因包含在打印机拒绝列表中而被拒绝访问打印机。但是，该属性对于新用户可能并不适合。

## 使用较大的用户 ID 和组 ID

可以为 UID 和组 ID (group ID, GID) 指定带符号整数的最大值，即 2147483647。

下表说明了 UID 和 GID 限制。

表 1-2 较大 UID 和 GID 的限制摘要

UID 或 GID	限制
262144 或更大	使用具有缺省归档格式的 <code>cpio</code> 命令复制文件的用户，会看到系统针对每个文件都返回一条错误消息。而且，归档中的 UID 和 GID 被设置为 <code>nobody</code> 。
2097152 或更大	使用具有 <code>-H odc</code> 格式的 <code>cpio</code> 命令或者使用 <code>pax -x cpio</code> 命令复制文件的用户，会看到系统针对每个文件都返回一条错误消息。而且，归档中的 UID 和 GID 被设置为 <code>nobody</code> 。
1000000 或更大	使用 <code>ar</code> 命令的用户，其归档中的 UID 和 GID 设置为 <code>nobody</code> 。
2097152 或更大	使用 <code>tar</code> 命令、 <code>cpio -H ustar</code> 命令或 <code>pax -x tar</code> 命令的用户，其 UID 和 GID 设置为 <code>nobody</code> 。

## UNIX 组

组是指可共享文件和其他系统资源的用户的集合。例如，参与同一个项目的用户可以形成一个组。组在以前称作 UNIX 组。

每个组都必须有名称、组标识 (group identification, GID) 号和一个属于该组的用户名的列表。GID 号用来在系统内部标识组。

用户可属于以下两种组：

- **主组**—这是操作系统指定给由用户所创建的文件的组。每个用户都必须属于一个主组。
- **补充组**—这是用户所属的除主组之外的一个或多个组。用户最多可以属于 1024 个补充组。

有关设置组名的详细准则，请参见第 17 页中的“用于指定用户名、用户 ID 和组 ID 的准则”。

有时，用户的辅助组并不重要。例如，文件的所有权反映主组，而不反映任何辅助组。但是，其他应用程序可能会依赖用户的辅助组成员身份。例如，用户必须是 `sysadmin` 组（组 14）的成员才能使用以前的 Solaris 发行版中的 `Admintool` 软件。但是，即使组 14 为用户当前的主组，也没有关系。

`groups` 命令可列出用户所属的组。用户一次只能有一个主组。但是，用户可以使用 `newgrp` 命令，将其主组临时更改为它所属的任何其他组。

添加用户帐户时，必须为用户指定一个主组或接受缺省组 `staff`（组 10）。该主组应当已经存在。如果主组不存在，请按 `GID` 号指定主组。用户名不会添加到主组中。如果将用户名添加到主组中，列表可能会变得太长。要想将用户指定给一个新的辅助组，必须先创建一个新的辅助组并为其指定一个 `GID` 号。

组可能是系统上的本地组，也可能通过某个名称服务进行管理。为了简化对组的管理，应当使用名称服务（如 `NIS`）或目录服务（如 `LDAP`）。使用这些服务可以集中管理组中所有成员身份。

## 用户口令

可以在添加用户时为用户指定口令。或者，也可以强制用户在首次登录到系统时指定口令。虽然用户名是公开的，但是口令必须保密，只能是用户自己知道。应当为每个用户帐户都指定一个口令。

用户口令必须遵循下面的语法：

- 口令长度至少必须与 `/etc/passwd` 文件中 `PASSLENGTH` 变量所标识的值相符。缺省情况下，该值设为 6。

在本发行版中，缺省口令散列算法已更改为 `SHA256`。因此，与以前的 `Oracle Solaris` 发行版不同，本发行版中不再有针对用户口令的八字符限制。八字符限制仅应用于使用较旧 `crypt_unix(5)` 算法的口令，为了向下兼容现有的 `passwd` 文件项和 `NIS` 映射，保留了该算法。

口令的最大字符数取决于算法：要么是用于旧口令的 `crypt_unix` 算法，要么是用于所有其他情况的 `SHA256` 算法。如果口令更改来自现有口令，且其为 `crypt_unix` 口令，则最大长度将设置为 8，除非 `policy.conf` 文件要求更改口令算法。

新口令必须在口令算法允许的最大字符数内符合复杂性规则。因此，如果使用 `crypt_unix` 算法，当键入一个包含 20 个字符的口令时，该口令必须在前 8 个字符内符合复杂性规则。如果口令算法是任一其他算法，则口令必须在输入的完整口令内符合复杂性规则，在本示例中为 20。

- 每一个口令都必须满足配置的复杂性约束，这些约束在 `/etc/default/passwd` 文件中指定。
- 每个口令都不得为配置的字典的成员，如 `/etc/default/passwd` 文件中所指定的那样。
- 对于支持口令历史记录检查的名称服务中的用户帐户，如果定义了先前的口令历史记录，则新口令不得包含在先前的口令历史记录中。

`passwd(1)` 手册页详细介绍了口令规则。

为了使计算机系统更加安全，用户应定期更改其口令。为了实现较高级别的安全，应当要求用户每六周更改一次口令。对于较低级别的安全来说，每三个月更改一次口令

就足够了。系统管理登录名（例如 `root` 和 `sys`）应当每月更改一次，或者应当在知道 `root` 口令的员工离开公司或者换岗时进行更改。

许多计算机安全性破坏都涉及到猜测合法用户的口令。应当确保用户避免使用名词、姓名、登录名和其他只需了解该用户的一些情况就有可能猜到的口令。

最好选择如下口令：

- 短语 (`beammeup`)。
- 由短语中每个单词的前几个字母组成的无意义的单词。例如，用 `swotrB` 来替换 `SomeWhere Over The RainBow`。
- 用数字或字符替换字母的单词。例如，用 `sn00py` 来替换 `snoopy`。

请勿选择如下口令：

- 您的姓名（从前向后拼、从后向前拼或混杂在一起）
- 家庭成员的姓名或宠物的名字
- 汽车驾照编号
- 电话号码
- 社会安全号码
- 员工编号
- 与爱好或兴趣有关的单词
- 季节主题，如 `Santa in December`
- 字典中的任何单词

## 起始目录

起始目录是文件系统的一部分，分配给用户以用于存储专用文件。为起始目录分配的空间量取决于用户所创建的文件种类、大小和数量。

起始目录可以位于用户的本地系统上，也可以位于远程文件服务器上。在任一情况下，都应当按照惯例创建 `/export/home/username` 形式的起始目录。对于较大的站点，应当将起始目录存储到服务器上。请为每个用户使用一个单独的文件系统。例如，`/export/home/alice` 或 `/export/home/bob`。通过为每个用户创建单独的文件系统，您可以根据每个用户的需求设置属性或特性。

通常，无论用户的起始目录位于何处，用户都能够通过名为 `/home/username` 的挂载点访问其起始目录。如果起始目录是通过使用 `AutoFS` 挂载的，系统将不允许您在任何系统上的 `/home` 挂载点下面创建任何目录。当 `AutoFS` 处于活动状态时，系统能够识别 `/home` 的特殊状态。有关自动挂载起始目录的更多信息，请参见《在 `Oracle Solaris 11.1` 中管理网络文件系统》中的“`Autofs` 管理的任务概述”。

要从网络上的任何位置使用起始目录，应当始终用 `$HOME`（而非 `/export/home/username`）来引用起始目录。`/export/home/username` 与计算机有关。另外，在用户的起始目录中创建的任何符号链接都应使用相对路径（例如，`../..../x/y/x`），这样，无论起始目录挂载在何处，这些链接都有效。

有关使用 CLI 创建用户帐户时如何添加起始目录的更多信息，请参见第 38 页中的“设置用户帐户的准则”。

## 命名服务

如果要管理大型站点的用户帐户，则可能需要考虑使用名称服务或目录服务，如 LDAP 或 NIS。使用名称服务或目录服务，可以集中存储用户帐户信息，而不是将用户帐户信息存储到每个系统的 `/etc` 文件中。当针对用户帐户使用了某种名称服务或目录服务时，用户可以使用同一个用户帐户从一个系统移动到另一个系统，而不必在每个系统上都复制这些用户帐户的信息。使用命名服务或目录服务还可以确保用户帐户信息保持一致。

## 用户的工作环境

除具有用于创建和存储文件的起始目录外，用户还需要一个环境，使之可以访问完成其工作所需的工具和资源。当用户登录系统时，用户的工作环境由初始化文件确定。这些文件由用户的启动 shell 来定义，具体视发行版的不同而异。

用于管理用户工作环境的一个好的策略是，在用户的起始目录中提供定制的用户初始化文件，例如 `.bash_profile`、`.bash_login`、`.kshrc` 或 `.profile`。

---

注 - 请勿使用系统初始化文件（如 `/etc/profile` 或 `/etc/.login`）来管理用户的工作环境。这些文件驻留在本地系统上，不能进行集中管理。例如，如果使用 AutoFS 从网络上的任何系统挂载用户的起始目录，则必须修改每个系统上的系统初始化文件，以确保用户在系统之间切换时获得一致的环境。

---

有关为用户定制用户初始化文件的详细信息，请参见第 25 页中的“定制用户的工作环境”。

有关如何通过 RBAC 定制用户帐户的信息，请参见《Oracle Solaris 11.1 管理：安全服务》中的“基于角色的访问控制（概述）”了解更多信息。

## 用于指定用户名、用户 ID 和组 ID 的准则

用户名、UID 和 GID 在您的组织（可能跨多个域）中应当是唯一的。

在创建用户名或角色名、UID 和 GID 时，请牢记以下准则：

- **用户名** 一应包含二到八个字母和数字。第一个字符应当为字母。至少有一个字符应当为小写字母。

---

注 – 尽管用户名可以包含句点 (.)、下划线 ( \_ ) 或连字符 (-)，但是由于它们可能会导致某些软件产品出现问题，所以建议不要使用这些字符。

---

- **系统帐户** – 请勿使用包含在缺省文件 `/etc/passwd` 和 `/etc/group` 中的任何用户名、UID 或 GID。请不要使用 0 到 99 的 UID 和 GID。这些数字保留供 Oracle Solaris 进行分配，任何人都不应当使用它们。请注意，此限制还适用于当前未使用的数字。

例如，`gdm` 是为 GNOME Display Manager 守护进程保留的用户名和组名，其他用户不应使用它。有关缺省的 `/etc/passwd` 和 `/etc/group` 项的完整列表，请参见表 1-3 和表 1-4。

请勿将 `nobody` 和 `nobody4` 帐户用于正在运行的进程。这两个帐户是为 NFS 保留的。如果针对正在运行的进程使用这些帐户，可能会产生意外的安全风险。需要以非 `root` 用户身份运行的进程应使用 `daemon` 或 `noaccess` 帐户。

- **系统帐户配置** – 请勿更改缺省系统帐户的配置。这包括更改当前处于锁定状态的系统帐户的登录 shell。但是，为 `root` 帐户设置口令和口令生命周期参数除外。

---

注 – 更改锁定的用户帐户的口令会更改口令，但不再同时解除锁定帐户。现在需要执行一个额外步骤，即使用 `passwd -u` 命令解除锁定帐户。

---

## 用户帐户信息和组信息的存储位置

本节介绍了以下信息：

- 第 19 页中的“`passwd` 文件中的字段”
- 第 19 页中的“缺省的 `passwd` 文件”
- 第 21 页中的“`shadow` 文件中的字段”
- 第 21 页中的“`group` 文件中的字段”
- 第 21 页中的“缺省的 `group` 文件”
- 第 23 页中的“用于获取用户帐户信息的命令”

根据站点策略的不同，用户帐户信息和组信息可以存储在本地系统的 `/etc` 文件中，也可以存储在名称服务或目录服务中，如下所示：

- NIS 名称服务的信息存储在映射中。
- LDAP 目录服务的信息存储在带索引的数据库文件中。

---

注 – 为了避免混淆，通常用文件来指用户帐户和组信息所在的位置，而不用数据库、表或映射。

---

多数用户帐户信息都存储在 `passwd` 文件中。口令信息按如下方式进行存储：

- 如果使用的是 NIS，则存储在 `passwd` 文件中
- 如果使用的是 `/etc` 文件，则存储在 `/etc/shadow` 文件中
- 如果使用的是 LDAP，则存储在 `people` 容器中

使用 LDAP（而非 NIS）时，可以使用口令生命周期。

对于 NIS 和文件，组信息存储在 `group` 文件中。对于 LDAP，组信息存储在 `group` 容器中。

## passwd 文件中的字段

`passwd` 文件中的字段以冒号加以分隔且包含以下信息：

```
username:password:uid:gid:comment:home-directory:login-shell
```

例如：

```
kryten:x:101:100:Kryten Series 4000 Mechanoid:/export/home/kryten:/bin/csh
```

有关 `passwd` 文件中各个字段的完整说明，请参见 [passwd\(1\)](#) 手册页。

## 缺省的 passwd 文件

缺省的 `passwd` 文件包含标准守护进程的项。守护进程是通常在引导时启动的进程，用来执行某些系统范围的任务（如打印、网络管理或端口监视）。

```
root:x:0:0:Super-User:/root:/usr/bin/bash
daemon:x:1:1:/:
bin:x:2:2::/usr/bin:
sys:x:3:3:/:
adm:x:4:4:Admin:/var/adm:
lp:x:71:8:Line Printer Admin:/:
uucp:x:5:5:uucp Admin:/usr/lib/uucp:
nuucp:x:9:9:uucp Admin:/var/spool/uucppublic:/usr/lib/uucp/uucico
dldm:x:15:65:Datalink Admin:/:
netadm:x:16:65:Network Admin:/:
netcfg:x:17:65:Network Configuration Admin:/:
smmsp:x:25:25:SendMail Message Submission Program:/:
listen:x:37:4:Network Admin:/usr/net/nls:
gdm:x:50:50:GDM Reserved UID:/var/lib/gdm:
zfsnap:x:51:12:ZFS Automatic Snapshots Reserved UID:/usr/bin/pfsh
upnp:x:52:52:UPnP Server Reserved UID:/var/coherence:/bin/ksh
xvm:x:60:60:xVM User:/:
mysql:x:70:70:MySQL Reserved UID:/:
openldap:x:75:75:OpenLDAP User:/:
webserverd:x:80:80:WebServer Reserved UID:/:
postgres:x:90:90:PostgreSQL Reserved UID:/usr/bin/pfksk
```

```

svctag:x:95:12:Service Tag UID:/:
unknown:x:96:96:Unknown Remote UID:/:
nobody:x:60001:60001:NFS Anonymous Access User:/:
noaccess:x:60002:60002:No Access User:/:
nobody4:x:65534:65534:SunOS 4.x NFS Anonymous Access User:/:
ftp:x:21:21:FTPD Reserved UID:/:
dhcperv:x:18:65:DHCP Configuration Admin:/:
aiuser:x:60003:60001:AI User:/:
pkg5srv:x:97:97:pkg(5) server UID:/:

```

表 1-3 缺省 passwd 文件中的项

用户名	用户 ID	说明
root	0	为超级用户帐户保留
daemon	1	与例行系统任务相关联的综合系统守护进程
bin	2	与正在运行的系统二进制文件相关联的管理守护进程，用来执行某些例行系统任务
sys	3	与临时目录中的系统日志记录或文件更新相关联的管理守护进程
adm	4	与系统日志记录相关联的管理守护进程
lp	71	为行式打印机守护进程保留
uucp	5	指定给与 uucp 函数关联的守护进程
nuucp	9	指定给与 uucp 函数关联的另一个守护进程
dladm	15	为数据链路管理保留
netadm	16	为网络管理保留
netcfg	17	为网络配置管理保留
smmsp	25	指定给 Sendmail 邮件提交程序守护进程
listen	37	指定给网络侦听器守护进程
gdm	50	指定给 GNOME Display Manager 守护进程
zfsnap	51	为自动快照保留
upnp	52	为 UPnP 服务器保留
xvm	60	为 xVM 用户保留
mysql	70	为 MySQL 用户保留
openldap	75	为 OpenLDAP 用户保留
websrvd	80	为 WebServer 访问保留
postgres	90	为 PostgreSQL 访问保留

表 1-3 缺省 `passwd` 文件中的项 (续)

用户名	用户 ID	说明
<code>svctag</code>	95	为 Service Tag Registry (服务标签注册表) 访问保留
<code>unknown</code>	96	为 NFSv4 ACL 中不可映射的远程用户保留
<code>nobody</code>	60001	为 NFS 匿名访问用户保留
<code>noaccess</code>	60002	为没有访问权限的用户保留
<code>nobody4</code>	65534	为 SunOS 4.x NFS 匿名访问用户保留
<code>ftp</code>	21	为 FTP 访问保留
<code>dhcpcserv</code>	18	为 DHCP 服务器用户保留
<code>aiuser</code>	60003	为 AI 用户保留
<code>pkg5srv</code>	97	为 <code>pkg(5)</code> depot 服务器保留

## shadow 文件中的字段

`shadow` 文件中的字段以冒号加以分隔且包含以下信息：

*username:password:lastchg:min:max:warn:inactive:expire*

缺省的口令散列算法为 SHA256。用户的口令散列类似于以下内容：

`$5$cgQk2iUy$AhHtVGx5Qd0.W3NCKjikb8.KhOiA4DpxsW55sP0UnYD`

有关 `shadow` 文件中各个字段的完整说明，请参见 [shadow\(4\)](#) 手册页。

## group 文件中的字段

`group` 文件中的字段以冒号加以分隔且包含以下信息：

*group-name:group-password:gid:user-list*

例如：

`bin::2:root,bin,daemon`

有关 `group` 文件中各个字段的完整说明，请参见 [group\(4\)](#) 手册页。

## 缺省的 group 文件

缺省的 `group` 文件包含下列系统组，这些组支持某些系统范围的任务，如打印、网络管理或电子邮件。其中的大部分组在 `passwd` 文件中都有相应的项。

```

root::0:
other::1:root
bin::2:root,daemon
sys::3:root,bin,adm
adm::4:root,daemon
uucp::5:root
mail::6:root
tty::7:root,adm
lp::8:root,adm
nuucp::9:root
staff::10:
daemon::12:root
sysadmin::14:
games::20:
smmsp::25:
gdm::50:
upnp::52:
xvm::60:
netadm::65:
mysql::70:
openldap::75:
webservd::80:
postgres::90:
slocate::95:
unknown::96:
nobody::60001:
noaccess::60002:
nogroup::65534:
ftp::21
pkg5srv::97:

```

表 1-4 缺省的 group 文件项

组名	组 ID	说明
root	0	超级用户组
other	1	可选的组
bin	2	与正在运行的系统二进制文件相关联的管理组
sys	3	与系统日志记录或临时目录相关联的管理组
adm	4	与系统日志记录相关联的管理组
uucp	5	与 uucp 函数相关联的组
mail	6	电子邮件组
tty	7	与 tty 设备相关联的组
lp	8	行式打印机组
nuucp	9	与 uucp 函数相关联的组
staff	10	一般的管理组
daemon	12	与例行系统任务相关联的组

表 1-4 缺省的 group 文件项 (续)

组名	组 ID	说明
sysadmin	14	对系统管理员有用的管理组
smmsp	25	Sendmail 邮件提交程序的守护进程
gdm	50	为 GNOME Display Manager 守护进程保留的组
upnp	52	为 UPnP 服务器保留的组
xvm	60	为 xVM 用户保留的组
netadm	65	为网络管理保留的组
mysql	70	为 MySQL 用户保留的组
openldap	75	为 OpenLDAP 用户保留
webserverd	80	为 WebServer 访问保留的组
postgres	90	为 PostgreSQL 访问保留的组
slocate	95	为 Secure Locate (安全定位) 访问保留的组
unknown	96	为 NFSv4 ACL 中不可映射远程组保留的组
nobody	60001	为匿名 NFS 访问指定的组
noaccess	60002	为需要通过某个应用程序访问系统 (而不进行实际登录) 的用户或进程指定的组
nogroup	65534	为不是已知组中成员的用户指定的组
ftp	21	为 FTP 访问指定的组
pkg5srv	97	指定给 pkg(5) depot 服务器的组

## 用于获取用户帐户信息的命令

下表介绍了系统管理员用来获取有关用户帐户的信息的命令。这些信息存储在 `/etc` 目录内的各个文件中。使用这些命令获取用户帐户信息优于使用 `cat` 命令查看类似信息。

表 1-5 用于获取用户相关信息的命令

命令	说明	手册页参考
<code>auths</code>	列出和管理授权。	<code>auths(1)</code>

表 1-5 用于获取用户相关信息的命令 (续)

命令	说明	手册页参考
getent	从管理数据库中获取条目列表。这些信息通常来自于为 <code>/etc/nsswitch.conf</code> 数据库指定的一个或多个源。	<a href="#">getent(1M)</a>
logins	显示关于用户、角色和系统登录的信息。输出受指定的命令选项控制，可以包括用户、角色、系统登录、UID、passwd 帐户字段值、主组、主组 ID、多个组名、多个组 ID、起始目录、登录 shell 和口令生命期参数。	<a href="#">logins(1M)</a>
profiles	列出和管理权限配置文件。	<a href="#">profiles(1)</a>
roles	显示指定给用户的角色。	<a href="#">roles(1)</a>
userattr	显示为 <code>attribute_name</code> 找到的第一个值。如果未指定用户，将从进程的实际用户 ID 中获取。属性名称是在 <code>user_attr(4)</code> 和 <code>prof_attr(4)</code> 中定义的。  注 - 该命令是 Oracle Solaris 11 中新增的命令。	<a href="#">Example 2-1</a>

## 用于管理用户、角色和组的命令

注 - 不再支持 Solaris 管理控制台 GUI 和与此 GUI 关联的 CLI。

以下命令可用于管理用户、角色和组。

表 1-6 用于管理用户、角色和组的命令

命令的手册页	说明	更多信息
<a href="#">useradd(1M)</a>	在本地或在 LDAP 系统信息库中创建用户。	<a href="#">第 39 页中的“如何添加用户”</a>
<a href="#">usermod(1M)</a>	在本地或在 LDAP 系统信息库中更改用户属性。如果用户属性是与安全相关的，例如角色指定，则此任务可能只能由安全管理员或 root 角色来执行。	<a href="#">第 41 页中的“如何修改用户”</a> <a href="#">《Oracle Solaris 11.1 管理：安全服务》中的“如何更改用户的安全属性”</a>

表 1-6 用于管理用户、角色和组的命令 (续)

命令的手册页	说明	更多信息
<code>userdel(1M)</code>	从系统或 LDAP 系统信息库中删除用户。可能涉及其他清除，例如，删除 cron 作业。	第 42 页中的“如何删除用户”
<code>roleadd(1M)</code>	在本地或在 LDAP 系统信息库中管理角色。角色无法登录。用户承担指定的角色来执行管理任务。	《Oracle Solaris 11.1 管理：安全服务》中的“如何创建角色”
<code>rolemod(1M)</code>		《Oracle Solaris 11.1 管理：安全服务》中的“初次配置 RBAC（任务列表）”
<code>roledel(1M)</code>		
<code>groupadd(1M)</code>	在本地或在 LDAP 系统信息库中管理组。	第 42 页中的“如何添加组”
<code>groupmod(1M)</code>		
<code>groupdel(1M)</code>		

## 定制用户的工作环境

本节介绍了以下信息：

- 第 26 页中的“使用站点初始化文件”
- 第 26 页中的“避免引用本地系统”
- 第 27 页中的“Shell 功能”
- 第 28 页中的“Bash Shell 和 ksh93 Shell 历史记录”
- 第 29 页中的“Bash Shell 和 ksh93 Shell 环境变量”
- 第 31 页中的“定制 Bash Shell”
- 第 31 页中的“MANPATH 环境变量”
- 第 31 页中的“PATH 环境变量”
- 第 32 页中的“语言环境变量”
- 第 33 页中的“缺省的文件权限 (umask)”
- 第 34 页中的“定制用户初始化文件”

设置用户的起始目录时，需要为用户的登录 shell 提供用户初始化文件。用户初始化文件是一个 shell 脚本，用来在用户登录系统之后为其设置工作环境。使用用户初始化文件基本上可以执行 shell 脚本所能完成的全部任务。但是，用户初始化文件的主要任务是定义用户工作环境的特征，如用户的搜索路径、环境变量和窗口环境。每个登录 shell 都有其自己的用户初始化文件，下表列出了这些文件。请注意，bash shell 和 ksh93 shell 的缺省用户初始化文件均为 `/etc/skel/local.profile`。

表 1-7 Bash 和 ksh93 用户初始化文件

Shell	用户初始化文件	目的
bash	\$HOME/.bash_profile	定义用户登录时的用户环境
	\$HOME/.bash_login	
	\$HOME/.profile	
ksh93	/etc/profile	定义用户登录时的用户环境
	\$HOME/.profile	
	\$ENV	在文件中定义用户登录时的用户环境，由 Korn shell 的 ENV 环境变量指定

您可以使用这些文件作为起点，之后修改这些文件，以创建可为所有用户提供通用工作环境的标准文件集。也可以修改这些文件，以便为不同类型的用户提供工作环境。

有关如何为不同类型的用户创建用户初始化文件集的逐步说明，请参见第 37 页中的“如何定制用户初始化文件”。

## 使用站点初始化文件

用户初始化文件可以由管理员和用户进行定制。此重要任务可以通过位于集中位置且分布在全局的名为**站点初始化文件**的用户初始化文件来完成。使用站点初始化文件，可以不断向用户的工作环境中引入新功能，同时允许用户定制用户初始化文件。

如果您在用户初始化文件中引用站点初始化文件，那么，当用户登录系统时或者当用户启动新 shell 时，对于站点初始化文件进行的所有更新都将自动反映出来。站点初始化文件旨在将系统范围的更改分发到您添加用户时未参与的用户工作环境中。

可以按照定制用户初始化文件的方式定制站点初始化文件。站点初始化文件通常驻留在一台或一组服务器上，并作为第一条语句出现在用户初始化文件中。而且，每个站点初始化文件都必须与引用它的用户初始化文件属于相同类型的 shell 脚本。

要在 bash 或 ksh93 用户初始化文件中引用站点初始化文件，请在用户初始化文件的开头位置插入类似以下内容的一行：

```
. /net/machine-name/export/site-files/site-init-file
```

## 避免引用本地系统

请勿在用户初始化文件中添加对本地系统的具体引用。无论用户登录哪个系统，用户初始化文件中的指令均应为有效指令。

例如：

- 为了使用户的起始目录可在网络上的任何位置使用，请始终用变量 `$HOME` 引用起始目录。例如，使用 `$HOME/bin`，而不使用 `/export/home/username/bin`。当用户登录另一个系统时，`$HOME` 变量将会运行，从而自动挂载起始目录。
- 要访问本地磁盘上的文件，请使用全局路径名，如 `/net/system-name/directory-name`。由 `/net/system-name` 引用的任何目录都可以在用户所登录的系统上自动挂载（假设该系统运行的是 AutoFS）。

## Shell 功能

此 Oracle Solaris 发行版支持以下 shell 功能和行为：

- 在缺省情况下，系统将为在安装 Oracle Solaris 发行版时创建的用户帐户指定 GNU Bourne-Again Shell (bash)。
- 标准系统 shell (bin/sh) 现在是 Korn Shell 93 (ksh93)。
- 缺省的交互式 shell 是 Bourne-again (bash) shell (`/usr/bin/bash`)。
- bash shell 和 ksh93 shell 都提供了命令行编辑功能，这意味着您可以在执行命令之前对其进行编辑。
- 您可以使用几种方式来显示缺省 shell 和路径信息：
  - 使用 `echo $SHELL` 和 `which` 命令：

```
$ grep root /etc/passwd
root:x:0:0:Super-User:/root:/usr/bin/bash
```

```
$ echo $SHELL /usr/bin/bash
$ which ksh93 /usr/bin/ksh93
```

- 使用 `pargs` 命令：

```
~$ pargs -l $$
/usr/bin/i86/ksh93
```

- ksh93 shell 还包含名为 `.sh.version` 的内置变量，其可按如下方式显示：

```
~$ echo ${.sh.version}
Version jM 93u 2011-02-08
```

- 要转到另一个 shell，请键入要使用的 shell 的路径。
- 要退出 shell，请键入 `exit`。

下表介绍了 Oracle Solaris 中支持的 shell 选项。

表 1-8 Oracle Solaris 发行版中的基本 Shell 功能

Shell	路径	注释
Bourne-Again Shell (bash)	<code>/usr/bin/bash</code>	为安装程序创建的用户以及 <code>root</code> 角色使用的缺省 shell。  为通过 <code>useradd</code> 命令创建的用户以及 <code>root</code> 角色使用的缺省（交互式）shell 为 <code>/usr/bin/bash</code> 。缺省路径为 <code>/usr/bin:/usr/sbin</code> 。
Korn Shell	<code>/usr/bin/ksh</code>	<code>ksh93</code> 是本 Oracle Solaris 发行版中的缺省 shell
C Shell 和增强的 C Shell	<code>/usr/bin/csh</code> 和 <code>/usr/bin/tcsh</code>	C Shell 和增强的 C Shell
符合 POSIX 的 Shell	<code>/usr/xpg4/bin/sh</code>	符合 POSIX 的 Shell
Z Shell	<code>/usr/bin/zsh</code>	Z Shell

注 - 缺省情况下，Z Shell (`zsh`) 和增强的 C Shell (`tcsh`) 不会安装在您的系统上。要使用这些 shell 中的任意一种 shell，必须先安装所需的软件包。

## Bash Shell 和 ksh93 Shell 历史记录

`bash` shell 和 `ksh93` shell 都会记录您运行的所有命令的历史记录。此历史记录是按用户保留的，也就是说历史记录在各次登录会话之间是持续保留的，代表您所有的登录会话。

例如，如果您处于 `bash` shell 中，则可以显示已经运行的命令的完整历史记录，如下所示：

```
$ history
1 ls
2 ls -a
3 pwd
4 whoami
.
.
```

要显示一定数目的以前命令，请在该命令中包括一个整数：

```
$ history 2
12 date
13 history
```

有关更多信息，请参见 [history\(1\)](#) 手册页。

## Bash Shell 和 ksh93 Shell 环境变量

bash shell 和 ksh93 shell 存储 shell 识别为环境变量的特殊变量信息。对于 bash shell，要查看当前环境变量的完整列表，请使用 declare 命令：

```
$ declare
BASH=/usr/bin/bash
BASH_ARGC=()
BASH_ARGV=()
BASH_LINENO=()
BASH_SOURCE=()
BASH_VERSINFO=([0]='3' [1]='2' [2]='25' [3]='1'
[4]='release' [5]'
.
.
.
```

对于 ksh93 shell，请使用 set 命令，此命令与 bash shell 的 declare 命令等效。

```
$ set
COLUMNS=80
ENV='$HOME/.kshrc'
FCEDIT=/bin/ed
HISTCMD=3
HZ=''
IFS=$' \t\n'
KSH_VERSION=.sh.version
LANG=C
LINENO=1
.
.
.
```

要为任一 shell 输出环境变量，请使用 echo 或 printf 命令。例如：

```
$ echo $SHELL
/usr/bin/bash
$ printf '$PATH\n'
/usr/bin:/usr/sbin
```

---

**注** - 环境变量在各个会话之间不会持续存在。要设置在各次登录之间保持一致的环境变量，必须在 .bashrc 文件中进行相应的更改。

---

Shell 可以有两种类型的变量：

**环境变量** 指定导出到由 shell 产生的所有进程的变量。export 命令用于导出变量。例如：

```
export VARIABLE=value
```

可以使用 env 命令显示这些设置。环境变量的子集（如 PATH）影响 shell 本身的行为。

Shell（本地）变量 指定仅影响当前 shell 的变量。

在用户初始化文件中，您可以通过更改预定义变量的值或指定其他变量来定制用户的 shell 环境。

下表提供了有关 Oracle Solaris 发行版中可用的 shell 和环境变量的更多详细信息。

表 1-9 Shell 变量和环境变量的说明

变量	说明
CDPATH	设置由 <code>cd</code> 命令使用的变量。如果将 <code>cd</code> 命令的目标目录指定为相对路径名， <code>cd</code> 命令将首先在当前目录（.）中搜索目标目录。如果没有找到目标目录，将继续搜索列在 <code>CDPATH</code> 变量中的路径名，直到找到目标目录并完成目录切换。如果没有找到目标目录，则当前的工作目录保持不变。例如， <code>CDPATH</code> 变量设置为 <code>/home/jean</code> ， <code>/home/jean</code> 下面有两个目录： <code>bin</code> 和 <code>rje</code> 。如果当前的目录是 <code>/home/jean/bin</code> 目录，那么，当您键入 <code>cd rje</code> 时，即使您未指定全路径名，目录也将切换到 <code>/home/jean/rje</code> 。
HOME	设置用户起始目录的路径。
LANG	设置语言环境。
LOGNAME	定义当前登录用户的名称。登录程序会将 <code>LOGNAME</code> 的缺省值自动设置为在 <code>passwd</code> 文件中指定的用户名。您不应当重置此变量，而只应当引用此变量。
MAIL	设置用户邮箱的路径。
MANPATH	设置可用手册页的分层结构。  注 - 从 Oracle Solaris 11 开始，不再需要 <code>MANPATH</code> 环境变量。 <code>man</code> 命令根据 <code>PATH</code> 环境变量设置来确定合适的 <code>MANPATH</code> 。
PATH	按顺序指定多个目录，当用户键入命令时，shell 将在这些目录搜索要运行的程序。如果该目录不在搜索路径中，用户必须键入命令的完整路径名。  在登录过程中，系统会自动定义缺省的 <code>PATH</code> ，并将其设置为 <code>.profile</code> 中指定的路径。  搜索路径的顺序至关重要。如果不同位置中存在相同的命令，将使用首先找到的具有该名称的命令。例如，假设以 shell 语法将 <code>PATH</code> 定义为 <code>PATH=/usr/bin:/usr/sbin:\$HOME/bin</code> ，且 <code>/usr/bin</code> 和 <code>/home/jean/bin</code> 中均有名为 <code>sample</code> 的文件。如果用户键入 <code>sample</code> 命令而未指定其全路径名，则将使用在 <code>/usr/bin</code> 中找到的版本。
PS1	为 <code>bash shell</code> 或 <code>ksh93 shell</code> 定义 shell 提示符。
SHELL	设置由 <code>make</code> 、 <code>vi</code> 和其他工具使用的缺省 shell。

表 1-9 Shell 变量和环境变量的说明 (续)

变量	说明
TERMINFO	指定存储备用 <code>terminfo</code> 数据库的目录。可使用 <code>/etc/profile</code> 或 <code>/etc/.login</code> 文件中的 <code>TERMINFO</code> 变量。有关更多信息，请参见 <code>terminfo(4)</code> 手册页。  如果设置了 <code>TERMINFO</code> 环境变量，系统将首先检查由用户定义的 <code>TERMINFO</code> 路径。如果系统在用户定义的 <code>TERMINFO</code> 目录中找不到终端的定义，它将在缺省目录 ( <code>/usr/share/lib/terminfo</code> ) 中搜索终端的定义。如果系统在这两个位置均未找到终端的定义，则将终端标识为“哑终端”。
TERM	定义终端。此变量应当在 <code>/etc/profile</code> 或 <code>/etc/.login</code> 文件中重置。当用户调用编辑器时，系统将查找在该环境变量中定义的同名文件。系统将搜索 <code>TERMINFO</code> 所引用的目录以确定终端的特征。
TZ	设置时区。例如，时区可用于在 <code>ls -l</code> 命令中显示日期。如果没有在用户的环境中设置 <code>TZ</code> ，将使用系统设置。否则，将使用格林威治标准时间。

## 定制 Bash Shell

要定制 Bash Shell，请将信息添加到位于起始目录的 `.bashrc` 文件中。安装 Oracle Solaris 时创建的初始用户具有一个 `.bashrc` 文件，可设置 `PATH`、`MANPATH` 和命令提示符。有关更多信息，请参见 `bash(1)` 手册页。

## MANPATH 环境变量

`MANPATH` 环境变量指定 `man` 命令查找参考手册页的位置。`MANPATH` 是根据用户的 `PATH` 值自动设置的，但它通常包括 `usr/share/man` 和 `usr/gnu/share/man`。

请注意，用户的 `MANPATH` 环境变量可独立于 `PATH` 环境变量进行修改。与用户的 `$PATH` 中的目录关联的手册页位置不是必须具有一对一等效体。

## PATH 环境变量

当用户使用全路径执行命令时，`shell` 将使用该路径来查找此命令。但是，当用户仅指定命令名称时，`shell` 将按 `PATH` 变量指定的顺序在目录中搜索该命令。如果在一个目录中找到了该命令，`shell` 将执行该命令。

缺省路由系统设置。但是，多数用户会通过修改该路径来添加其他命令目录。与设置环境和访问命令或工具的正确版本有关的许多用户问题都是路径定义错误引起的。

## 路径的设置准则

下面是设置有效 PATH 变量的一些准则：

- 如果您的路径中必须包括当前目录 (.)，应将其放置在最后。将当前目录包括在路径中存在安全风险，因为某些具有恶意的人员可能会将有危害性的脚本或可执行文件隐藏在当前目录中。请考虑改用绝对路径名。
- 搜索路径应尽可能短。Shell 会在该路径中搜索每个目录。如果未找到命令，搜索长目录会降低系统性能。
- 搜索路径的读取顺序是从左到右，因此，您应当将常用命令的目录放在路径的开头。
- 确保目录在路径中不重复。
- 尽可能避免搜索大型目录。将大型目录放在路径的末尾处。
- 将本地目录放在 NFS 挂载目录之前，以便减少在 NFS 服务器不响应时“挂起”的几率。此策略还会减少不必要的网络通信流量。

## 语言环境变量

LANG 和 LC 环境变量可以为 shell 指定特定于语言环境的转换和约定。这些转换和约定包括时区、整理顺序、日期格式、时间格式、货币格式和数字格式。另外，还可以使用用户初始化文件中的 stty 命令来指示终端会话是否支持多字节字符。

LANG 变量为给定的语言环境设置所有可能的转换和约定。可以通过以下 LC 变量来分别设置本地化的多个方

面：LC\_COLLATE、LC\_CTYPE、LC\_MESSAGES、LC\_NUMERIC、LC\_MONETARY 和 LC\_TIME。

---

注 – 缺省情况下，Oracle Solaris 11 仅安装基于 UTF-8 的语言环境。

---

下表介绍了核心 Oracle Solaris 11 语言环境的环境变量值。

表 1-10 LANG 和 LC 变量的值

值	语言环境
en_US.UTF-8	英语（美国）(UTF-8)
fr_FR.UTF-8	法语（法国）(UTF-8)
de_DE.UTF-8	德语（德国）(UTF-8)
it_IT.UTF-8	意大利语（意大利）(UTF-8)
ja_JP.UTF-8	日语（日本）(UTF-8)
ko_KR.UTF-8	韩语（韩国）(UTF-8)

表 1-10 LANG 和 LC 变量的值 (续)

值	语言环境
pt_BT.UTF-8	葡萄牙语 (巴西) (UTF-8)
zh_CN.UTF-8	简体中文 (中国) (UTF-8)
es_ES.UTF-8	西班牙语 (西班牙) (UTF-8)
zh_TW.UTF-8	繁体中文 (中国台湾) (UTF-8)

示例 1-1 使用 LANG 变量设置语言环境

在 Bourne shell 或 Korn shell 用户初始化文件中，您将添加如下内容：

```
LANG=de_DE.ISO8859-1; export LANG
```

```
LANG=de_DE.UTF-8; export LANG
```

## 缺省的文件权限 (umask)

创建文件或目录时，为文件或目录指定的缺省文件权限由用户掩码进行控制。用户掩码由用户初始化文件中的 `umask` 命令设置。可以通过键入 `umask` 并按回车键来显示用户掩码的当前值。

用户掩码中包含下列八进制值：

- 第一位用来为用户设置权限
- 第二位用来为组设置权限
- 第三位用来为其他实体设置权限（又称作 `world`）

请注意，如果第一位是零，它将不显示出来。例如，如果用户掩码设置为 `022`，则将显示 `22`。

如需确定要设置的 `umask` 值，请用 `666`（对于文件）或 `777`（对于目录）减去所需的权限值。差值就是要用于 `umask` 命令的值。例如，假设您希望将文件的缺省模式设置为 `644` (`rw-r--r--`)，`666` 与 `644` 的差值 `022` 就是将用作 `umask` 命令参数的值。

还可以使用下表来确定要设置的 `umask` 值。下表显示了为 `umask` 的每个八进制值创建的文件权限和目录权限。

表 1-11 umask 权限的值

umask 八进制值	文件权限	目录权限
0	<code>rw-</code>	<code>rwx</code>
1	<code>rw-</code>	<code>rw-</code>

表 1-11 umask 权限的值 (续)

umask 八进制值	文件权限	目录权限
2	r--	r-x
3	r--	r--
4	-w-	-wx
5	-w-	-w-
6	--x	--x
7	--- (无)	--- (无)

用户初始化文件中的下行用来将缺省的文件权限设置为 `rw-rw-rw-`。

```
umask 000
```

## 定制用户初始化文件

下面是 `.profile` 用户初始化文件的示例。您可以使用此文件定制自己的用户初始化文件。此示例使用了修改特定站点时将需要的系统名称和路径。

示例 1-2 `.profile` 文件

```
(Line 1) PATH=$PATH:$HOME/bin:/usr/local/bin:/usr/gnu/bin:.
(Line 2) MAIL=/var/mail/$LOGNAME
(Line 3) NNTPSERVER=server1
(Line 4) MANPATH=/usr/share/man:/usr/local/man
(Line 5) PRINTER=printer1
(Line 6) umask 022
(Line 7) export PATH MAIL NNTPSERVER MANPATH PRINTER
```

1. 定义用户的 shell 搜索路径。
2. 设置用户邮件文件的路径。
3. 定义用户的时间/时钟服务器。
4. 定义用户的手册页搜索路径。
5. 定义用户的缺省打印机。
6. 设置用户的缺省文件创建权限。
7. 设置所列出的环境变量。

## 使用命令行界面管理用户帐户（任务）

---

本章提供了有关使用命令行界面 (Command-Line Interface, CLI) 设置和管理用户帐户的基本信息。

有关管理用户帐户和用户环境的概述信息，请参见第 1 章，[管理用户帐户和用户环境（概述）](#)。

有关使用用户管理器图形用户界面 (graphical user interface, GUI) 管理用户和角色的信息，请参见第 3 章，[使用用户管理器 GUI 管理用户帐户（任务）](#)。

### 使用 CLI 设置和管理用户帐户

以下任务介绍了如何使用 CLI 设置和管理用户帐户。

### 使用 CLI 设置和管理用户帐户（任务列表）

任务	说明	参考
收集用户信息。	使用标准表单收集用户信息有助于组织用户信息。	第 36 页中的“收集用户信息”
定制用户初始化文件。	您可以设置用户初始化文件，以便为新用户提供一致的环境。	第 37 页中的“如何定制用户初始化文件”
更改所有角色的帐户缺省值。	更改所有角色的缺省起始目录和框架目录。	第 37 页中的“如何更改所有角色的帐户缺省值”
创建一个用户帐户。	使用您设置的帐户缺省值，通过 <code>useradd</code> 命令创建一个本地用户。	第 39 页中的“如何添加用户”
修改用户帐户。	修改系统上的用户登录信息。	第 41 页中的“如何修改用户”

任务	说明	参考
删除用户帐户。	使用 <code>userdel</code> 命令删除用户帐户。	第 42 页中的“如何删除用户”
创建然后指定用于执行管理任务的角色。	使用您设置的帐户缺省值创建一个本地角色，以便用户可以执行特定的管理命令或任务。	《Oracle Solaris 11.1 管理：安全服务》中的“如何创建角色” 《Oracle Solaris 11.1 管理：安全服务》中的“如何指定角色”
创建一个组。	使用 <code>groupadd</code> 命令创建新组。	第 42 页中的“如何添加组”
为用户帐户添加安全属性。	在设置本地用户帐户后，您可以添加所需的安全属性。	《Oracle Solaris 11.1 管理：安全服务》中的“如何更改用户的安全属性”
共享某个用户的起始目录。	您必须共享用户的起始目录，以便可以从用户的系统远程挂载该目录。	第 43 页中的“如何共享作为 ZFS 文件系统创建的起始目录”
手动挂载用户的起始目录。	通常，您无需手动挂载作为 ZFS 文件系统创建的用户起始目录。起始目录在它创建时和从 SMF 本地文件系统服务引导时会自动挂载。	第 44 页中的“手动挂载用户的起始目录”

## 收集用户信息

在设置用户帐户时，您可以创建类似于以下表单的表单，用于在设置用户帐户之前收集用户的相关信息。

项	说明
用户名：	
角色名：	
配置文件或授权：	
UID：	
主组：	
辅助组：	
注释：	
缺省 Shell：	
口令状态和更新：	

项	说明
起始目录的路径名:	
挂载方法:	
起始目录的权限:	
邮件服务器:	
添加到下列邮件别名中:	
桌面系统名称:	

## ▼ 如何定制用户初始化文件

- 1 承担 `root` 角色或拥有 "User Management" ( 用户管理 ) 权限配置文件的角色。

```
$ su -
Password:
#
```

请参见《Oracle Solaris 11.1 管理：安全服务》中的“如何使用指定给您的管理权限”。

- 2 为每种类型的用户创建一个框架目录。

```
# mkdir /shared-dir/skel/user-type
```

`shared-dir` 可供网络上的其他系统使用的目录名称。

`user-type` 要用来存储某种类型用户的初始化文件的目录名称。

- 3 将缺省的用户初始化文件复制到为不同类型的用户创建的目录中。

- 4 编辑每种用户类型的用户初始化文件，并根据系统需要定制这些文件。

有关用户初始化文件定制方法的详细说明，请参见第 25 页中的“定制用户的工作环境”。

- 5 设置用户初始化文件的权限。

```
# chmod 744 /shared-dir/skel/user-type/*
```

- 6 验证用户初始化文件的权限是否正确。

```
# ls -la /shared-dir/skel/*
```

## ▼ 如何更改所有角色的帐户缺省值

在下面的过程中，管理员已定制了一个 `roles` 目录。管理员更改所有角色的缺省起始目录和框架目录。

- 1 承担 **root** 角色或拥有 "User Management" ( 用户管理 ) 权限配置文件的角色。  
请参见 《Oracle Solaris 11.1 管理：安全服务》 中的“如何使用指定给您的管理权限”。

- 2 创建一个定制的角色目录。例如：

```
# roleadd -D
group=other,1 project=default,3 basedir=/home
skel=/etc/skel shell=/bin/pfsh inactive=0
expire= auths= profiles=All limitpriv=
defaultpriv= lock_after_retries=
```

- 3 更改所有角色的缺省起始目录和框架目录。例如：

```
# roleadd -D -b /export/home -k /etc/skel/roles
# roleadd -D
group=staff,10 project=default,3 basedir=/export/home
skel=/etc/skel/roles shell=/bin/sh inactive=0
expire= auths= profiles= roles= limitpriv=
defaultpriv= lock_after_retries=
```

将来可使用 **roleadd** 命令在 `/export/home` 中创建起始目录，并从 `/etc/skel/roles` 目录填充角色的环境。

## 设置用户帐户的准则

请注意以下有关使用 CLI 设置用户帐户的准则：

- 在此发行版中，用户帐户将创建为 Oracle Solaris ZFS 文件系统。作为管理员，当您创建用户帐户时，您将为用户提供他们自己的文件系统和 ZFS 数据集。使用 **useradd** 和 **roleadd** 命令创建的每个起始目录将作为单个 ZFS 文件系统放置在 `/export/home` 文件系统中，形成该用户的起始目录。因此，用户可以对自己的起始目录进行备份，创建起始目录的 ZFS 快照，以及通过 ZFS 快照替换当前起始目录中的文件。
- 要设置用户帐户，您必须承担 **root** 角色或拥有相应权限配置文件的角色，例如 "User Management" ( 用户管理 ) 权限配置文件。请参见 《Oracle Solaris 11.1 管理：安全服务》 中的“如何使用指定给您的管理权限”。
- 使用 **useradd** 命令创建用户帐户时，必须在命令语法中指定 **-m** 选项。否则，不会为用户创建起始目录。

例如，以下命令将为用户 `jdoe` 创建起始目录：

```
# useradd -m jdoe
```

但是，以下语法不会为用户创建起始目录：

```
# useradd jdoe
```

注 - 该规则的唯一例外是您希望用 `pam_zfs_key` 模块为用户创建加密的起始目录。在这种情况下，**不要在 `useradd` 命令中指定 `-m` 选项**。请参见 [pam\\_zfs\\_key\(5\)](#) 和 [zfs\\_encrypt\(1M\)](#) 手册页。

- 仅当随 `-d` 选项一起指定了 `hostname:/pathname` 时，`useradd` 命令才会在 `auto_home` 映射中创建条目。否则，指定的路径名会更新为 `passwd` 数据库中用户的起始目录，而不会创建 `auto_home` 映射条目。仅当启用了 `autofs` 服务时，才会挂载 `auto_home` 自动挂载程序映射中指定的起始目录。  
例如，如果按如下所示指定 `-d` 选项创建用户，则所创建的用户不包含 `auto_home` 条目，且 `passwd` 条目指定 `/export/home/user1` 作为用户的起始目录：  

```
# useradd -d /export/home/user1 user1
```

但是，如果按如下所示使用 `-d` 选项创建用户，则用户将具有 `auto_home` 条目，且 `passwd` 数据库将包含 `/home/user1`，指示依赖于 `autofs` 服务：  

```
# useradd -d localhost:/export/home/user1 user1
```
- 如果起始目录的路径名中指定了远程主机，例如 `foobar:/export/home/jdoe`，则 `jdoe` 的起始目录必须在 `foobar` 系统上创建。缺省路径名为 `localhost:/export/home/username`。
- 当文件系统是一个 ZFS 数据集时（Oracle Solaris 11 的所有文件系统都如此），用户的起始目录是作为子 ZFS 数据集创建的，并且将创建快照所需的 ZFS 权限委托给用户。如果指定的路径名未对应于某个 ZFS 数据集，则系统将创建常规目录。如果指定 `-S ldap` 选项，则 `auto_home` 映射条目在 LDAP 服务器上更新，而非在本地 `auto_home` 映射上更新。

## ▼ 如何添加用户

在此发行版中，用户帐户将创建为 Oracle Solaris ZFS 文件系统。使用 `useradd` 和 `roleadd` 命令创建的每个起始目录将作为单个 ZFS 文件系统放置在 `/export/home` 文件系统中，形成该用户的起始目录。

仅当随 `-d` 选项一起指定了 `hostname:/pathname` 时，`useradd` 命令才会在 `auto_home` 映射中创建条目。否则，指定的路径名会更新为 `passwd` 数据库中用户的起始目录，而不会创建 `auto_home` 映射条目。仅当启用了 `autofs` 服务时，才会挂载 `auto_home` 自动挂载程序映射中指定的起始目录。

- 1 承担 `root` 角色或拥有 "User Management"（用户管理）权限配置文件的角色。  
请参见《Oracle Solaris 11.1 管理：安全服务》中的“如何使用指定给您的管理权限”。

## 2 创建一个本地用户。

缺省情况下，用户是在本地创建的。如果包含 `-s ldap` 选项，可以在现有的 LDAP 系统信息库中创建用户。

```
# useradd -d dir -m username
```

`useradd` 为指定的用户创建帐户。

`-d` 指定用户的起始目录的位置。

使用 `-d localhost:/export/home/username` 而不是 `-d /export/home/username` 强制将条目写入 `auto_home` 中。

`-m` 在系统上为用户创建本地起始目录。

如果按如下所示指定 `-d dir` 选项，创建的用户将不包含 `auto_home` 条目，且 `passwd` 条目将指定 `/export/home/user1` 作为用户的起始目录：

```
# useradd -d /export/home/user1 user1
```

如果按如下所示指定 `-d dir` 选项，用户将包含 `auto_home` 条目，且 `passwd` 数据库将包含 `/home/user1`，指示依赖于 `autofs` 服务：

```
# useradd -d localhost:/export/home/user1 user1
```

---

注 – 如果您希望用 `pam_zfs_key` 模块为用户创建加密的起始目录。在这种情况下，请不要在 `useradd` 命令中指定 `-m` 选项。请参见第 38 页中的“设置用户帐户的准则”。

有关可以与 `useradd` 命令一起指定的所有选项和参数的详细说明，请参见 [useradd\(1M\)](#) 手册页。

---

注 – 帐户将被锁定，直到您为用户指定口令。

## 3 为用户指定口令。

```
# passwd username
```

```
New password:      Type user password
```

```
Re-enter new password:      Retype password
```

有关更多命令选项，请参见 [useradd\(1M\)](#) 和 [passwd\(1\)](#) 手册页。

**另请参见** 创建用户后，您可能需要执行一些其他任务，包括向用户添加和指定角色、列出和更改用户的权限配置文件以及更改用户的 RBAC 属性。有关更多信息，请参见下列参考信息：

- 《Oracle Solaris 11.1 管理：安全服务》中的“如何创建角色”和《Oracle Solaris 11.1 管理：安全服务》中的“如何指定角色”
- 《Oracle Solaris 11.1 管理：安全服务》中的“如何查看所有已定义的安全属性”
- 《Oracle Solaris 11.1 管理：安全服务》中的“如何创建权限配置文件”
- 《Oracle Solaris 11.1 管理：安全服务》中的“如何更改用户的安全属性”

## ▼ 如何修改用户

使用 `usermod` 命令更改用户登录定义以及为用户作出相应的与登录相关的文件系统更改。

### 1 承担 root 角色或拥有 "User Management" ( 用户管理 ) 权限配置文件的角色。

请参见《Oracle Solaris 11.1 管理：安全服务》中的“如何使用指定给您的管理权限”。

### 2 根据需要修改用户帐户。

有关可以与 `usermod` 命令一起指定的参数和选项的详细信息，请参见 `usermod(1M)` 手册页。

例如，向用户添加角色，应键入：

```
# usermod -R role username
```

### 示例 2-1 通过修改用户帐户设置每个用户的 PAM 策略

以下示例显示了如何修改用户以设置 PAM 策略。该特定修改指定对于所有 PAM 服务，只应使用 Kerberos V5 协议验证用户 `jdoue`。有关更多信息，请参见 `pam_user_policy(5)`。

```
# usermod -K pam_policy=krb5_only jdoue
```

**另请参见** 有关修改用户的其他示例，请参见以下参考资料：

- 《Oracle Solaris 11.1 管理：安全服务》中的“如何指定角色”
- 《Oracle Solaris 11.1 管理：安全服务》中的“如何更改用户的安全属性”

## ▼ 如何删除用户

### 1 承担 root 角色

```
$ su -
Password:
#
```

---

注 – 无论 root 是用户帐户还是角色，此方法都是可行的。

---

### 2 归档用户的起始目录。

### 3 运行以下命令之一：

- 如果用户有一个本地起始目录，请删除此用户和起始目录。

```
# userdel -r username
userdel    删除指定用户的帐户。
-r         从系统中删除帐户。
```

因为用户起始目录现在是 ZFS 数据集，所以，要为已删除的用户移除本地起始目录，首选方法是随 `userdel` 命令指定 `-r` 选项。

- 否则，只能删除用户。

```
# userdel username
```

在远程服务器上，您必须手动删除用户的起始目录。

有关命令选项的完整列表，请参见 [userdel\(1M\)](#) 手册页。

**接下来的步骤** 如果您删除的用户具有管理职责（例如创建 cron 作业）或该用户在全局区域中具有其他帐户，则可能需要执行额外的清除操作。

## ▼ 如何添加组

管理员创建组时，系统会将 `solaris.group.assign/groupname` 指定给此管理员，并向管理员赋予对该组的完全控制权。如果其他拥有相同授权的管理员创建了组，则该管理员可以控制此组。对其中一组具有控制权的管理员无法管理其他管理员的组。有关更多信息，请参见 [groupadd\(1M\)](#) 和 [groupmod\(1M\)](#) 手册页。

### 1 承担 root 角色或拥有 `solaris.group.manage` 授权的管理员。

请参见《Oracle Solaris 11.1 管理：安全服务》中的“如何使用指定给您的管理权限”。

## 2 列出现有组。

```
# cat /etc/group
```

## 3 创建新组。

```
$ groupadd -g 18 exadata
```

groupadd 通过向 /etc/group 文件中添加相应的条目，在系统上创建新的组定义。

-g 为新组指定组 ID。

有关更多信息，请参见 [groupadd\(1M\)](#) 手册页。

### 示例 2-2 用 groupadd 和 useradd 命令设置组和用户

下面的示例说明如何使用 groupadd 和 useradd 命令向本地系统上的文件中添加 scutters 组和 scutter1 用户。

```
# groupadd -g 102 scutters
# useradd -u 1003 -g 102 -d /export/home/scutter1 -s /bin/csh \
-c "Scutter 1" -m -k /etc/skel scutter1
64 blocks
```

有关更多信息，请参见 [groupadd\(1M\)](#) 和 [useradd\(1M\)](#) 手册页。

## ▼ 如何共享作为 ZFS 文件系统创建的起始目录

在此 Oracle Solaris 发行版中，您可以通过设置 share.nfs 属性或 share.smb 属性来共享 ZFS 文件系统。或者，您可以通过使用 zfs share 命令来创建文件系统共享。缺省情况下，所有文件系统都不共享。

缺省情况下，pool/export/home 数据集已挂载在 /export/home 中。useradd 命令自动将每个用户的数据集创建为该数据集的子项。作为管理员，您可以选择为用户起始目录创建一个新池。以下过程说明了各个步骤。

有关共享和取消共享文件系统的更多信息，请参见《[Oracle Solaris 11.1 管理：ZFS 文件系统](#)》中的“共享和取消共享 ZFS 文件系统”。

### 1 承担 root 角色。

请参见《[Oracle Solaris 11.1 管理：安全服务](#)》中的“如何使用指定给您的管理权限”。

### 2 为用户起始目录创建一个独立的池。例如：

```
# zpool create users mirror c1t1d0 c1t2d0 mirror c2t1d0 c2t2d0
```

### 3 为起始目录创建一个容器。例如：

```
# zfs create users/home
```

- 4 为起始目录设置共享属性。例如，要创建 NFS 共享以及为 `users/home` 设置 `share.nfs` 属性，应键入：

```
# zfs set share.nfs=on users/home
```

使用此新语法时，每个文件系统将包含一个“自动共享”，此共享是在将该文件系统的 `share.nfs` 属性（或 `share.smb` 属性）设置为 `on` 后立即创建的。前一命令将共享名为 `users/home` 的文件系统及其所有子系统。

- 5 确认后代文件系统共享也已发布。例如：

```
# zfs get -r share.nfs users/home
```

`-r` 选项可显示所有的后代文件系统。

## 手动挂载用户的起始目录

作为 ZFS 文件系统创建的用户帐户通常不需要进行手动挂载。通过 ZFS，文件系统在创建时自动挂载，然后在引导时通过 SMF 本地文件系统服务进行挂载。

在创建用户帐户时，请确保起始目录的设置与名称服务（位于 `/home/username`）中的设置相同。然后，确保 `auto_home` 映射表示用户起始目录的 NFS 路径。有关与任务相关的信息，请参见《在 Oracle Solaris 11.1 中管理网络文件系统》中的“Autofs 管理的任务概述”。

如果需要手动挂载用户的起始目录，请使用 `zfsmount` 命令。例如：

```
# zfs mount users/home/alice
```

---

注 - 确保用户的起始目录已共享。有关更多信息，请参见第 43 页中的“如何共享作为 ZFS 文件系统创建的起始目录”。

---

## 使用用户管理器 GUI 管理用户帐户（任务）

---

本章提供了有关使用 Oracle Solaris 用户管理器 GUI 设置和管理用户的概述和任务相关信息。使用用户管理器 GUI 可执行等效 CLI（`useradd`、`usermod`、`userdel` 等）可执行的大部分任务。有关用户管理器 GUI 的更多信息，请参阅联机帮助。

以下是本章中信息的列表：

- 第 45 页中的“用户管理器 GUI 简介”
- 第 49 页中的“使用用户管理器 GUI 添加、修改和删除用户和角色”
- 第 52 页中的“使用用户管理器 GUI 管理高级设置”

有关管理用户帐户的概述信息，请参见第 1 章，管理用户帐户和用户环境（概述）。

有关使用 CLI 管理用户帐户的信息，请参见第 2 章，使用命令行界面管理用户帐户（任务）。

### 用户管理器 GUI 简介

本节介绍了以下信息：

- 第 46 页中的“启动用户管理器 GUI”
- 第 46 页中的““User Manager”（用户管理器）面板布局”
- 第 47 页中的“选择缺省名称服务范围 and 类型”
- 第 48 页中的“承担角色或更改用户凭证”

用户管理器 GUI 基于 Visual Panels 框架并作为 Visual Panels 界面提供。可以通过远程管理守护进程 (Remote Administration Daemon, RAD) 远程管理用户和角色。此 GUI 依靠用户/角色管理器 RAD 模块执行所有操作。RAD 模块的工作原理是：调用执行所有 GUI 管理功能的基于角色的访问控制 (role-based access control, RBAC) CLI。

Visual Panels 框架自身提供用户验证和角色承担功能，这些功能可供所有面板使用，包括“User Manager”（用户管理器）面板。用户管理器 GUI 取代了 Oracle Solaris 10 中支持的 Solaris 管理控制台的用户和角色工具。尽管与 Solaris 管理控制台不同，但此 GUI 具有一些相同功能。请注意，本发行版不支持 Solaris 管理控制台。

用户管理器 GUI 提供的界面既简洁又易用。为将出错的可能性降到最低，此 GUI 将根据已验证的用户或角色的授权和权限配置文件，仅显示有效的选项。可使用 GUI 执行的任务与可使用 CLI（例如 `useradd`、`usermod`、`userdel`、`roleadd`、`groupadd` 等）执行的任务相同。有关使用 CLI 管理用户和角色的信息，请参见第 2 章，[使用命令行界面管理用户帐户（任务）](#)。

用户管理器 GUI 由 `pkg:/system/management/visual-panels/panel-usermgr` IPS 软件包提供。

## 启动用户管理器 GUI

### ▼ 如何启动用户管理器 GUI

- 1 承担 `root` 角色或以指定有 "User Management"（用户管理）权限配置文件的用户身份登录。

请参见 [《Oracle Solaris 11.1 管理：安全服务》](#) 中的“如何使用指定给您的管理权限”。

- 2 选择以下方法之一启动用户管理器 GUI：

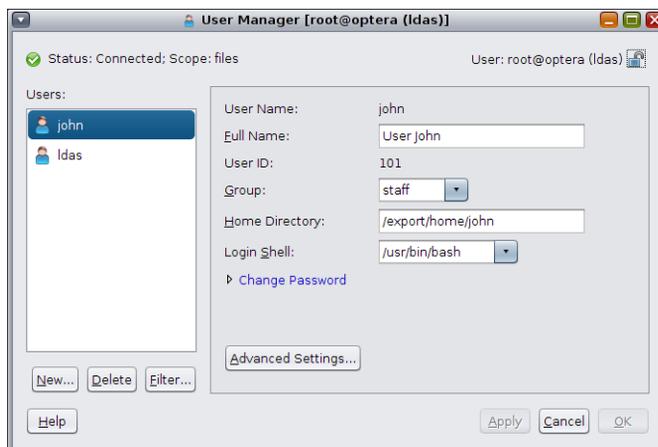
- 选择 "System"（系统）→ "Administration"（管理）→ "User Manager"（用户管理器），从桌面启动用户管理器 GUI。
- 从命令行启动用户管理器 GUI，如下所示：

```
# vp usermgr &
```

## "User Manager"（用户管理器）面板布局

启动用户管理器 GUI 时，将显示 "User Manager"（用户管理器）主面板。"User Manager"（用户管理器）面板用于管理用户和角色。该面板的左侧是 "Status"（状态）字段，显示当前在本地主机上运行的服务的状态。该面板的右侧是 "User"（用户）字段。"User"（用户）字段显示用户管理器 GUI 当前正在使用的凭证。要更改凭证，请单击面板最右侧的 "Lock"（锁定）按钮。请参见第 48 页中的 [“承担角色或更改用户凭证”](#)。

下图中显示了 "User Manager"（用户管理器）主面板。



"User Manager"（用户管理器）面板包括以下两个组成部分：

- 用户和角色列表—包含您可以从中选择要管理的用户的列表
- 基本设置—显示用户的基本设置，例如用户名和全名

要查看或修改现有用户的信息，请从显示的用户列表中选择用户。选择用户后，该用户的信息将显示在面板右侧。

您可以在 "User Manager"（用户管理器）面板中执行以下操作：

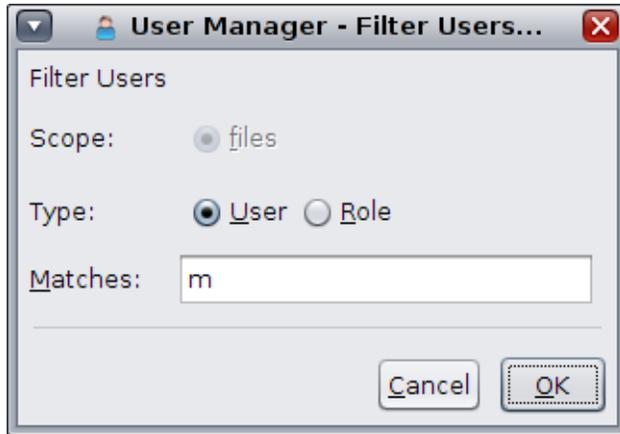
- 创建一个新用户或角色。请参见第 49 页中的“如何使用用户管理器 GUI 添加用户或角色”。
- 删除现有用户或角色。请参见第 51 页中的“使用用户管理器 GUI 删除用户或角色”。
- 过滤用户信息。请参见第 47 页中的“选择缺省名称服务范围 and 类型”。
- 管理现有用户的高级设置。请参见第 51 页中的“如何使用用户管理器 GUI 修改用户或角色”。

## 选择缺省名称服务范围 and 类型

用户管理器 GUI 的缺省名称服务范围 and 类型分别为 `files` 和 `User`。要管理不同范围（例如 `ldap` 和 `roles`）内的用户管理器 GUI，请单击 "Filter"（过滤器）按钮。单击 "Filter"（过滤器）按钮将启动一个对话框，在此对话框中，您可以更改缺省范围和/或类型。

- 对于 "Scope"（范围）选项，可选择 `files` 和 `ldap`。
- 对于 "Type"（类型）选项，可选择 `User` 和 `Role`。单击 "OK"（确定）保存更改。

单击 "Cancel"（取消）取消操作。



注 - 如果系统未配置为 ldap 客户机，则只有 files 范围可用。

## 承担角色或更改用户凭证

具有 "User Management"（用户管理）权限配置文件的用户可以创建新用户，只要即将创建的用户或角色的高级属性属于正在执行管理的用户的属性即可。如果正在执行管理的用户没有足够授权但拥有具备足够授权的管理角色，则用户可以承担该角色，通过单击 "User Manager"（用户管理器）主面板中的 "Lock"（锁定）按钮来执行必要的管理操作。

### ▼ 如何更改用户的凭证

#### 1 启动用户管理器 GUI。

请参见第 46 页中的“如何启动用户管理器 GUI”。

#### 2 在 "User Manager"（用户管理器）主面板中，单击 "Lock"（锁定）图标打开包含以下选项的子菜单：

- Change Role（更改角色）
- Change User（更改用户）
- Administer New Host（管理新主机）
- Clear History（清除历史记录）

#### 3 选择 "Change Role"（更改角色）选项。

将显示验证对话框。此验证对话框包含一个下拉菜单，其中列出了可用于指定用户的角色。

- 4 选择相应角色，然后单击 "Log In"（登录）以更改角色。  
承担角色后，可以执行必需的管理任务。

## 使用用户管理器 GUI 添加、修改和删除用户和角色

使用用户管理器 GUI 添加、修改和删除用户的作用效果与分别使用 `useradd`、`usermod` 和 `userdel` 命令的作用效果一样。有关从命令行添加用户的更多信息，请参见第 2 章，使用命令行界面管理用户帐户（任务）。

本节介绍了以下信息：

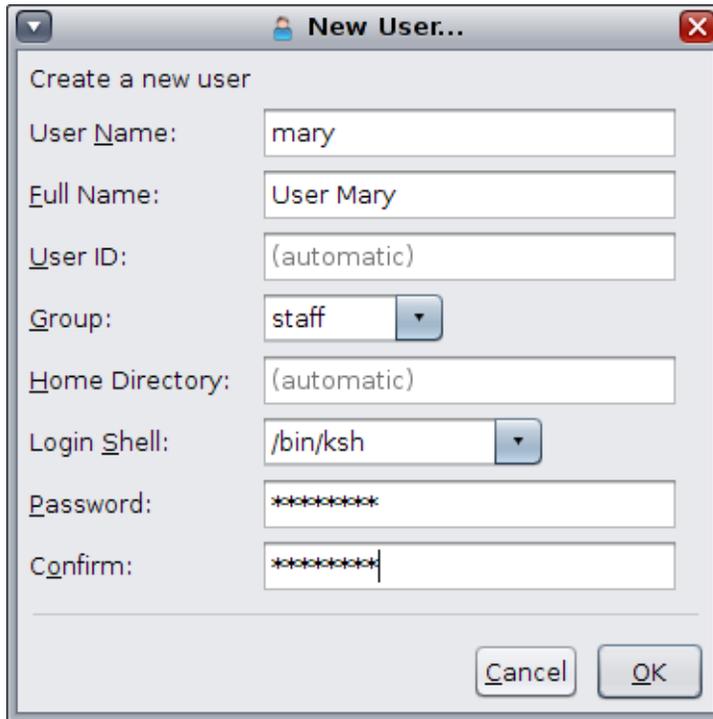
- 第 49 页中的“如何使用用户管理器 GUI 添加用户或角色”
- 第 51 页中的“如何使用用户管理器 GUI 修改用户或角色”
- 第 51 页中的“使用用户管理器 GUI 删除用户或角色”

### ▼ 如何使用用户管理器 GUI 添加用户或角色

- 1 启动用户管理器 GUI。  
请参见第 46 页中的“如何启动用户管理器 GUI”。

- 2 要在 GUI 当前正在使用的过滤器范围内添加新用户或角色，请单击 "User Manager"（用户管理器）主面板中的 "New"（新建）按钮。

将显示 "New User"（新建用户）对话框。



The screenshot shows a "New User..." dialog box with the following fields and values:

- User Name: mary
- Full Name: User Mary
- User ID: (automatic)
- Group: staff
- Home Directory: (automatic)
- Login Shell: /bin/ksh
- Password: \*\*\*\*\*
- Confirm: \*\*\*\*\*

- 3 在 "New User"（新建用户）对话框中，填写以下字段：

- User Name（用户名）
- Full Name（全名）
- User ID（用户 ID）  
此字段是可选的。如果您不提供任何信息，系统将自动指定缺省值。
- Group（组）  
"Group"（组）字段的可用选项因系统配置而异。
- Home Directory（起始目录）  
此字段是可选的。如果您不提供任何信息，系统将自动指定缺省值。  
如果要自动挂载用户的起始目录，请在路径名前面添加主机名或本地主机。例如，localhost:/export/home/test1。
- Login Shell（登录 shell）  
"Login Shell"（登录 Shell）字段的选项因系统配置而异。

- Password (口令)  
为用户指定一个临时口令。
- Confirm (确认)  
确认指定给用户的临时口令。

---

注 - 除了可选字段外，必须填写其他所有字段。

---

- 4 要创建新用户或角色并将其添加到 "User Manager" (用户管理器) 主面板中显示的用户列表中，请单击 "OK" (确定)。  
要取消操作，请单击 "Cancel" (取消)。

## ▼ 如何使用用户管理器 GUI 修改用户或角色

- 1 启动用户管理器 GUI。  
请参见第 46 页中的“如何启动用户管理器 GUI”。
- 2 要修改现有用户或角色，请在 "User Manager" (用户管理器) 主面板中，从显示的列表中选择要修改的用户或角色。  
选择用户后，面板右侧将填充关于当前用户的信息。
- 3 修改当前用户或角色的任何信息或所有信息。

---

注 - 如果某个字段发生修改，则在已修改字段的旁边将显示一个指示符。

---

- 4 单击 "Apply" (应用) 保存更改。
- 5 可选单击 "Advanced Settings" (高级设置) 按钮修改用户或角色的其他安全属性。请参见第 52 页中的“使用用户管理器 GUI 管理高级设置”。
- 6 单击 "OK" (确定) 保存更改并关闭 "User Manager" (用户管理器) 面板。  
单击 "Cancel" (取消) 放弃所有未保存的更改并关闭面板。

## 使用用户管理器 GUI 删除用户或角色

要删除用户管理器 GUI 当前正在使用的过滤器范围内的用户或角色，请在 "User Manager" (用户管理器) 主面板中选择该用户或角色，然后单击 "Delete" (删除) 按钮。要保存更改，请在显示确认对话框后单击 "OK" (确定)。要取消操作，请单击 "Cancel" (取消)。

## 使用用户管理器 GUI 管理高级设置

本节介绍了以下信息：

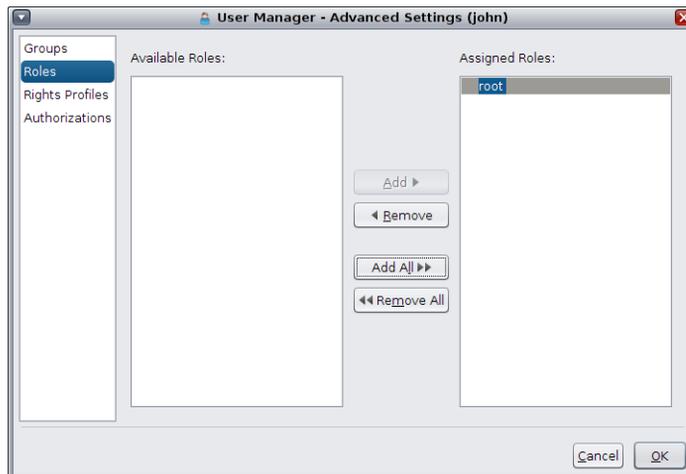
- 第 53 页中的“使用用户管理器 GUI 管理组”
- 第 53 页中的“使用用户管理器 GUI 管理角色”
- 第 55 页中的“使用用户管理器 GUI 管理权限配置文件”
- 第 56 页中的“使用用户管理器 GUI 管理授权”

使用用户管理器 GUI 的 "Advanced Settings"（高级设置）对话框可为用户指定其他安全属性，例如权限配置文件、角色和授权。

有关 Oracle Solaris 支持的安全功能的概述，请参见《Oracle Solaris 11.1 管理：安全服务》中的第 I 部分，“安全性概述”。有关此发行版中基于角色的访问控制 (role-based access control, RBAC) 工作原理的详细说明，请参见《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”。

要管理用户或角色的高级属性，请在 "User Manager"（用户管理器）主面板中选择用户或角色，然后单击 "Advanced Settings"（高级设置）按钮。将显示当前用户或角色的 "Advanced Settings"（高级设置）面板。当前用户的名称显示在面板顶部，位于括号内。

下图显示了 "Advanced Settings"（高级设置）面板，其中选择了用户 john 的 "Roles"（角色）安全属性。



在 "Advanced Settings"（高级设置）面板中可以管理以下安全属性：

- Groups（组）
- Roles（角色）

- Rights Profiles（权限配置文件）
- Authorizations（授权）

## 使用用户管理器 GUI 管理组

通过单击用户管理器 GUI 的 "User Manager"（用户管理器）主对话框中的 "Advanced Settings"（高级设置）按钮可以管理组。

### ▼ 如何管理组

#### 1 启动用户管理器 GUI。

请参见第 46 页中的“如何启动用户管理器 GUI”。

#### 2 在 "User Manager"（用户管理器）主面板中选择一个用户，然后单击 "Advanced Settings"（高级设置）按钮。

将显示 "Advanced Settings"（高级设置）面板。

#### 3 单击面板左侧的 "Groups"（组）属性。

将显示可用组列表以及当前用户所属的组列表。

- 要将一个或多个组分配给用户，请从 "Available Groups"（可用组）列表选择一个或多个组，然后单击 "Add"（添加）。

添加的组将显示在 "Assigned Groups"（已分配组）列表中。

- 要从 "Assigned Groups"（已分配组）列表中删除组，请从该列表选择一个或多个组，然后单击 "Remove"（删除）。

- 要添加或删除当前用户的所有组，请单击 "Add All"（全部添加）或 "Remove All"（全部删除）按钮。

#### 4 单击 "OK"（确定）保存设置。

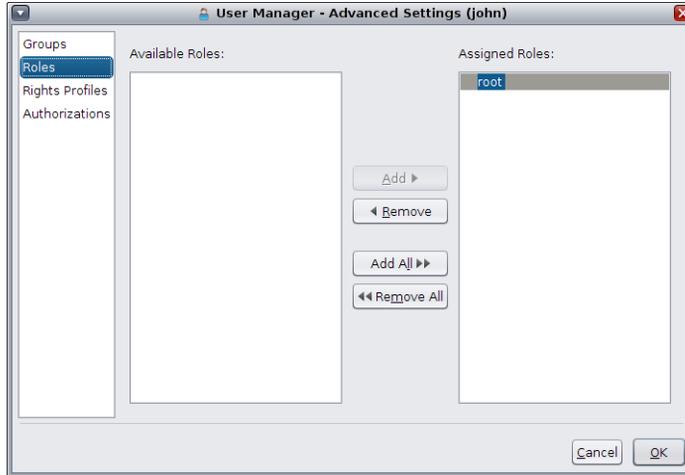
只有在 "User Manager"（用户管理器）主面板中单击 "Apply"（应用）或 "OK"（确定）之后，才会应用更改。

## 使用用户管理器 GUI 管理角色

通过单击用户管理器 GUI 的 "User Manager"（用户管理器）主对话框中的 "Advanced Settings"（高级设置）按钮可以管理角色。

注 - "Roles" (角色) 属性只能用于用户, 不能用于角色, 因为角色只能分配给用户。

下图显示了 "Advanced Settings" (高级设置) 面板, 其中选择了用户 john 的 "Roles" (角色) 安全属性。



## ▼ 如何使用用户管理器 GUI 管理角色

### 1 启动用户管理器 GUI。

请参见第 46 页中的“如何启动用户管理器 GUI”。

### 2 在 "User Manager" (用户管理器) 主面板中选择一个用户, 然后单击 "Advanced Settings" (高级设置) 按钮。

将显示 "Advanced Settings" (高级设置) 面板。

### 3 单击面板左侧的 "Roles" (角色) 属性。

将显示可用角色列表以及分配给当前用户的角色列表。

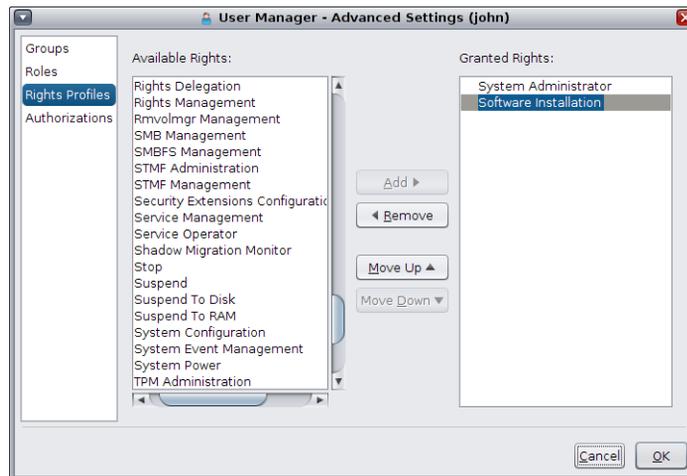
- 要将一个或多个角色分配给用户, 请从 "Available Roles" (可用角色) 列表中选择一或多个角色, 然后单击 "Add" (添加)。  
添加的角色将显示在 "Assigned Roles" (已分配角色) 列表中。
- 要从 "Assigned Roles" (已分配角色) 列表中删除角色, 请从该列表中选择一或多个角色, 然后单击 "Remove" (删除)。

- 要添加或删除当前用户的所有角色，请单击 "Add All"（全部添加）或 "Remove All"（全部删除）按钮。
- 4 单击 "OK"（确定）保存设置。
- 只有在 "User Manager"（用户管理器）主面板中单击 "Apply"（应用）或 "OK"（确定）之后，才会应用更改。

## 使用用户管理器 GUI 管理权限配置文件

通过单击用户管理器 GUI 的 "User Manager"（用户管理器）主对话框中的 "Advanced Settings"（高级设置）按钮可以管理权限配置文件。

下图显示了 "Advanced Settings"（高级设置）面板，其中选择了用户 john 的 "Rights Profiles"（权限配置文件）安全属性。



注 - 权限配置文件须按顺序优先级进行分配。使用 "Move Up"（上移）和 "Move Down"（下移）按钮可根据需要更改为当前用户授予的权限配置文件的顺序。

### ▼ 如何使用用户管理器 GUI 管理权限配置文件

- 1 启动用户管理器 GUI。  
请参见第 46 页中的“如何启动用户管理器 GUI”。

- 2 在 "User Manager" (用户管理器) 主面板中选择一个用户, 然后单击 "Advanced Settings" (高级设置) 按钮。  
将显示 "Advanced Settings" (高级设置) 面板。
- 3 单击面板左侧的 "Rights Profiles" (权限配置文件) 属性。  
将显示可用权限配置文件列表以及授予给当前用户的权限配置文件列表。
  - 要将一个或多个权限配置文件分配给用户, 请从 "Available Rights" (可用权限) 配置文件列表选择一个或多个权限配置文件, 然后单击 "Add" (添加)。  
添加的权限配置文件将显示在 "Granted Rights" (已授予权限) 配置文件列表中。
  - 要从 "Granted Rights" (已授予权限) 配置文件列表中删除权限配置文件, 请从该列表选择一个或多个权限配置文件, 然后单击 "Remove" (删除)。
  - 要添加或删除当前用户的所有权限配置文件, 请单击 "Add All" (全部添加) 或 "Remove All" (全部删除) 按钮。
- 4 单击 "OK" (确定) 保存设置。  
只有在 "User Manager" (用户管理器) 主面板中单击 "Apply" (应用) 或 "OK" (确定) 之后, 才会应用更改。

## 使用用户管理器 GUI 管理授权

通常, 用户都是通过权限配置文件间接授予授权。授权设置可用于为用户或角色授予特定授权。一些授权可能具有其他属性, 例如对象名称。例如, 管理员创建组 `games` 时, 将授予该管理员隐式授权: `solaris.group.manage/games`。对象名称随后将显示在 "Granted Authorizations" (已授予授权) 列表中。

### ▼ 如何使用用户管理器 GUI 管理授权

- 1 启动用户管理器 GUI。  
请参见第 46 页中的“如何启动用户管理器 GUI”。
- 2 在 "User Manager" (用户管理器) 主面板中选择一个用户, 然后单击 "Advanced Settings" (高级设置) 按钮。  
将显示 "Advanced Settings" (高级设置) 面板。

### 3 单击面板左侧的 "Authorizations" ( 授权 ) 属性。

将显示可用授权列表以及授予当前用户的授权列表。

- 要将一个或多个授权分配给用户，请从 "Available Authorizations" ( 可用授权 ) 列表选择一个或多个授权，然后单击 "Add" ( 添加 )。  
添加的授权将显示在 "Granted Authorizations" ( 已授予授权 ) 列表中。
- 要从 "Granted Authorizations" ( 已授予授权 ) 列表中删除授权，请从该列表选择一个或多个授权，然后单击 "Remove" ( 删除 )。
- 要添加或删除当前用户的所有授权，请单击 "Add All" ( 全部添加 ) 或 "Remove All" ( 全部删除 ) 按钮。

### 4 单击 "OK" ( 确定 ) 保存设置。

只有在 "User Manager" ( 用户管理器 ) 主面板中单击 "Apply" ( 应用 ) 或 "OK" ( 确定 ) 之后，才会应用更改。



# 索引

---

## 数字和符号

"User Manager" (用户管理器) 面板, 组件, 46-47

## B

bin 组, 13

## C

C shell, 用户初始化文件和, 34

CDPATH 环境变量, 30

.cshrc 文件, 定制, 34

## D

daemon 组, 13

## E

/etc/passwd 文件

说明, 19

用户 ID 号指定和, 13

字段, 19

/etc/shadow 文件, 说明, 19

/etc 文件

用户帐户信息和, 17

/export/home 文件系统, 16

## G

GID, 13

定义, 14

较大, 14

指定, 15

group 文件

说明, 19

字段, 21

groupadd 命令, 25

添加组, 42-43

groupdel 命令, 25

groupmod 命令, 25

groups 命令, 15

## H

HOME 环境变量, 30

/home 文件系统, 用户起始目录和, 16

## I

ID 号

用户, 13, 14

组, 13, 14, 15

## K

ksh93 shell, 用户初始化文件和, 26

## L

LANG 环境变量, 30, 32  
LC 环境变量, 32  
locale 环境变量, 30  
.login 文件, 定制, 34  
LOGNAME 环境变量, 30

## M

MAIL 环境变量, 30  
MANPATH 环境变量, 30

## N

newgrp 命令, 15  
NIS  
    用户帐户和, 17, 19  
noaccess 用户/组, 13  
nobody 用户/组, 13

## P

passwd 命令, 指定用户口令, 39–41  
passwd 文件, 19  
    用户 ID 号指定和, 13  
    字段, 19  
PATH 环境变量  
    说明, 30, 31  
.profile 文件, 定制, 34  
PS1 环境变量, 30  
pseudo-ttys, 13

## R

roleadd 命令, 25  
    设置帐户缺省值, 37–38  
roledel 命令, 25  
rolemod 命令, 25

## S

shadow 文件  
    说明, 19  
    字段, 21  
shell, 用户初始化文件和, 34  
SHELL 环境变量, 30  
staff 组, 15  
stty 命令, 32

## T

TERM 环境变量, 31  
TERMINFO 环境变量, 31  
ttys (伪), 13  
ttytype 伪用户登录, 13  
TZ 环境变量, 31

## U

UID  
    定义, 13  
    较大, 14  
    指定, 14  
umask 命令, 33  
UNIX 组, 14  
useradd 命令, 24  
    设置帐户缺省值, 37–38  
    添加用户, 39–41  
userdel 命令, 25  
    删除用户, 42  
usermod 命令, 24  
uucp 组, 13

## V

Visual Panels, 用户管理器 GUI, 45

## 安

安全, 用户 ID 号重新使用和, 14

## 别

别名, 用户登录名与, 13

## 初

初始化文件, 系统, 17

## 登

登录名 (用户), 说明, 12

## 辅

辅助组, 14, 15

## 高

高级设置, 使用用户管理器 GUI 管理, 52-57

## 更

更改

用户口令

按用户, 15

频率, 15

帐户缺省值, 37-38

更改凭证

用户管理器 GUI

如何, 48-49

## 挂

挂载

用户起始目录

自动挂载, 17

用户起始目录 (如何), 44

## 管

管理

用户, 39-41, 42

帐户, 37-38

组, 42-43

管理角色, 使用用户管理器 GUI, 53-55

管理权限配置文件, 使用用户管理器 GUI, 55-56

管理授权, 使用用户管理器 GUI, 56-57

管理组, 使用用户管理器 GUI, 53

## 环

环境变量

LOGNAME, 30

PATH, 30

SHELL, 30

TZ, 31

## 加

加密, 19

## 角

角色, 使用用户管理器 GUI 管理, 53-55

## 控

控制文件和目录访问权限, 33

## 口

口令, 指定给用户, 39-41

口令 (用户)

更改

按用户, 15

频率, 15

加密, 19

生命期, 19

选择, 15

## 口令（用户）（续）

预防措施, 16

## 框

框架目录 (/etc/skel), 26

## 名

名称

用户登录

说明, 12

组

说明, 14

名称服务范围和类型, 用户管理器 GUI, 47-48

## 命

命名服务

用户帐户和, 17, 19

组和, 15

## 目

目录

PATH 环境变量和, 30, 31

控制访问权限, 33

框架, 26

起始, 16

## 启

启动用户管理器 GUI, 46

## 起

起始目录, 删除, 42

## 权

权限, 33

权限配置文件, 使用用户管理器 GUI 管理, 55-56

## 缺

缺省值, 用户和角色的设置, 37-38

## 确

确定用户口令生命期, 19

## 删

删除, 用户, 42

删除用户或角色, 使用用户管理器 GUI, 51

## 设

设置, 使用用户管理器 GUI 管理, 52-57

## 时

时区环境变量, 31

## 授

授权, 使用用户管理器 GUI 管理, 56-57

## 添

添加

用户, 39-41

用户初始化文件, 26

组, 42-43

添加用户

使用用户管理器 GUI

如何, 49-51

添加用户或角色,使用用户管理器 GUI, 51

## 伪

伪用户登录, 13

## 文

文件,控制访问权限, 33

## 系

系统初始化文件, 17

系统帐户, 13

## 显

显示,用户掩码, 33

## 用

用户

删除起始目录, 42

设置, 37-38

添加, 39-41, 42

用户 ID 号, 13, 14

用户初始化文件

shell 和, 34

定制, 25, 34

shell 变量, 31

避免引用本地系统, 26

概述, 26

添加定制文件, 26

用户掩码设置, 33

站点初始化文件, 26

说明, 17

用户登录(伪), 13

用户登录名,说明, 12

用户管理器 GUI

Visual Panels, 45

用户管理器 GUI (续)

更改凭证, 48-49

管理高级设置, 52-57

管理角色, 53-55

管理权限配置文件, 55-56

管理授权, 56-57

管理组, 53

缺省的名称服务范围 and 类型, 47-48

如何启动, 46

删除用户或角色, 51

添加用户, 49-51

修改用户或角色, 51

用户起始目录

定制初始化文件, 26

对(\$HOME)的非本地引用, 16, 26

挂载

自动挂载, 17

挂载(如何), 44

说明, 16

用户掩码, 33

用户帐户, 12

ID 号, 13, 14

登录名, 12

命名服务和, 17, 19

设置

信息表单, 36

说明, 12

信息存储, 17

准则, 17

## 邮

邮件别名,用户登录名与, 13

## 站

站点初始化文件, 26

## 主

主面板,用户管理器 GUI, 46-47

主组, 14, 15

## 自

自动挂载, 用户起始目录, 17

## 组

### 组

ID 号, 13, 14, 15

UNIX, 14

辅助, 14, 15

更改主, 15

管理指南, 14

名称

说明, 14

名称说明, 14

命名服务和, 15

缺省值, 15

使用用户管理器 GUI 管理, 53

说明, 14

添加, 42-43

显示用户所属的组, 15

信息存储, 19, 21

用于管理的准则, 15

主, 14, 15

组 ID 号, 13, 14, 15

## 最

### 最大值

辅助组用户可以属于, 14

用户 ID 号, 13

用户登录名长度, 17

最小值, 用户登录名长度, 17