# 在 Oracle® Solaris 11.2 中管理用户帐户和用户环境

文件号码 E53833-02
2014 年 9 月

ORACLE

# 目录

# 使用本文档

- **概述** – 介绍如何管理用户帐户和用户环境。
- **目标读者** – 使用 Oracle Solaris 11 发行版的系统管理员
- **必备知识** – 对 UNIX 系统具有管理经验

## 产品文档库

有关本产品的最新信息和已知问题均包含在文档库中，网址为：http://www.oracle.com/pls/topic/lookup?ctx=E56344。

## 获得 Oracle 支持。

Oracle 客户可通过 My Oracle Support 获得电子支持。有关信息，请访问 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info；如果您听力受损，请访问 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs。

## 反馈

可以在 http://www.oracle.com/goto/docfeedback 上提供有关本文档的反馈。

♦ ♦ ♦ 第 1 章

# 1 关于用户帐户和用户环境

本章介绍了管理用户帐户和用户环境的信息，包括以下主题：



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和第 3 章 使用用户管理器 GUI 管理用户帐户。

## Oracle Solaris 11.2 中管理用户帐户的新增功能

本节介绍此发行版中的新增功能或已更改的功能：



### 关机过程中扩展的登录选项

如果 `shutdown` 命令正在关闭系统，此过程将创建一个 `/etc/nologin` 文件。此文件显示一条消息，指示系统正在关闭，不允许登录。此外，超级用户可以分别创建和管理此 `/etc/nologin` 文件。

此类型的关闭不会阻止超级用户登录。从此发行版起，如果系统存在 `nologin` 文件，则不会阻止以下其他用户：

- 指定 root 角色的用户
- 指定 `solaris.system.maintenance` 授权的用户

有关详细信息，请参见 `nologin`(4) 和 `shutdown`(1M) 手册页。

## 影响用户帐户管理的安全更改

管理用户帐户的系统管理员应注意，此发行版中已更改以下安全功能：

- 可以将特定扩展特权应用于文件对象、端口号和用户 ID。这些扩展特权替代在其他情况下可以使用的特权集（基本特权集除外）。

  有关扩展用户特权的讨论，请参见《在 Oracle Solaris 11.2 中确保用户和进程的安全 》中的“扩展用户或角色的特权”。

  有关说明，请参见《在 Oracle Solaris 11.2 中确保用户和进程的安全 》中的第 4 章 “向应用程序、脚本和资源指定权限”。另请参见 `ppriv`(1) 或 `privileges`(5) 手册页。
- 您可以设置 `auth_profiles` 权限，从而使用户必须在执行通过权限配置文件指定的命令之前提供口令。口令在可配置的时间段内有效。

  `policy.conf` 文件中的 `AUTH_PROFS_GRANTED` 关键字为系统中的所有用户设置运行特权命令所需的口令。

  有关详细信息，请参见《在 Oracle Solaris 11.2 中确保用户和进程的安全 》中的“扩展用户权限”。另请参见 `useradd`(1M) 和 `usermod`(1M) 手册页。

# 什么是用户帐户和组？

本节介绍了以下信息：


- “用户帐户组件” [9]
- “用于指定用户名、用户 ID 和组 ID 的准则” [13]


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。“用户帐户组件” [9]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，其中包括参与 `topsecret` 项目的用户。此外，您可以为 `topsecret` 组设置对 `topsecret` 文件的 `read` 权限，从而只有 `topsecret` 组中的用户可以读取这些文件。

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。有关更多信息，请参见《在 Oracle Solaris 11.2 中确保用户和进程的安全 》中的第 1 章 “使用权限控制用户和进程”。

# 用户帐户组件

本节介绍了用户帐户的各种组件。

## 用户名（登录名）

用户名（也称为 *login names*）允许用户访问其各自的系统和具备相应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，John Smith 的用户名为 `jsmith`。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，`John Jay Smith` 的用户名为 `jjsmith`。

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：

- 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五个字母
- 添加数字 1、2 或 3，依此类推，直到用户名唯一

---

注 - 用户名都必须不同于系统或 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“用于指定用户名、用户 ID 和组 ID 的准则” [13]。

## 用户 ID 号

用户识别 (user identification, UID) 号与每个用户名关联。UID 号在任何用户尝试登录的系统中标识用户名。系统还可以使用 UID 来标识文件和目录的所有者。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 | 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 |

| UID 号 | 用户帐户或登录帐户 | 说明 |
| --- | --- | --- |
| 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“用于指定用户名、用户 ID 和组 ID 的准则” [13]。

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。如果您必须重新使用 UID，请彻底删除该帐户信息，以使新用户不受上一用户属性设置的影响。例如，先前的用户可能会包含在打印机拒绝列表中。但是，可能不应拒绝新用户访问该打印机。

## 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 cpio 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。归档中的 UID 和 GID 被设置为 nobody。 |
| 2097152 或更大 | 使用具有 -H odc 格式的 cpio 命令或者使用 pax -x cpio 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。归档中的 UID 和 GID 被设置为 nobody。 |
| 1000000 或更大 | 使用 ar 命令的用户，其归档中的 UID 和 GID 设置为 nobody。 |
| 2097152 或更大 | 使用 tar 命令、cpio -H ustar 命令或 pax -x tar 命令的用户，其 UID 和 GID 设置为 nobody。 |

## 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“用于指定用户名、用户 ID 和组 ID 的准则” [13]。

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 Oracle 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此用户所属的任何其他组。

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。未将用户名添加到主组中，因为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：

- 口令长度是由 `/etc/default/password` 文件中的 `PASSLENGTH` 值定义的。

  缺省的口令散列算法为 `SHA256`。因此，用户口令不再像以前的 Oracle Solaris 发行版那样限制为 8 个字符。8 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。

  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。

- 新口令不得包含在名称服务的口令历史记录中。

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托管该目录的系统的大小以及用户所创建的文件的种类、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。为每个用户使用单独的文件系统，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 11.2 中管理网络文件系统 》中的“Autofs 管理”。

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。

有关使用命令行界面创建用户帐户时如何添加起始目录的更多信息，请参见“设置用户帐户的准则” [32]。

### 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“关于用户的工作环境” [21]。

## 用于指定用户名、用户 ID 和组 ID 的准则

组织中的用户名、UID 和 GID 应该是唯一的，当设置涉及多个域时尤为如此。

在创建用户名或角色名、UID 和 GID 时，请牢记以下准则：

- **用户名** – 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 “缺省 passwd 文件中的项” 和表 1-4 “缺省的 group 文件项”。

注意 - 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，包括当前锁定的系统帐户登录 shell。但是，为 `root` 帐户设置口令和口令生命期参数除外。

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

本节包括以下信息：



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，可以使用口令生命期。

对于 NIS，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）。

以下屏幕显示了示例 passwd 文件的内容。

注 - 如果在系统中添加或删除包，则会创建和删除其他用户和组。passwd 文件中反映了这些正在进行的更改。管理员无需清理此文件。

```
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
dladm: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:/:
gdm:x:50:50:GDM Reserved UID:/var/lib/gdm:
zfssnap: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:/:
webservd:x:80:80:WebServer Reserved UID:/:
postgres:x:90:90:PostgreSQL Reserved UID:/:/usr/bin/pfksh
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:/:
ikeuser:x:67:12:IKE Admin:/:
ftp:x:21:21:FTPD Reserved UID:/:
dhcpserv:x:18:65:DHCP Configuration Admin:/:
aiuser:x:60003:60001:AI User:/:
pkg5srv:x:97:97:pkg(5) server UID:/:
```

以上屏幕显示了示例 passwd 文件的内容，其中不包含任何说明。下表包含更多内容，提供了标准 passwd 文件中每个守护程序的描述和源包信息。

表 1-3 缺省 passwd 文件中的项

| 用户名 | 用户 ID | 说明 | 包 |
|---|---|---|---|
| root | 0 | 为超级用户帐户保留 | system/core-os |
| daemon | 1 | 与例行系统任务相关联的综合系统守护进程 | system/core-os |
| 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 | system/core-os |
| 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 | system/core-os |
| adm | 4 | 与系统日志记录相关联的管理守护进程 | system/core-os |
| lp | 71 | 为行式打印机守护进程保留 | system/core-os |
| uucp | 5 | 指定给与 uucp 函数关联的守护进程 | system/core-os |
| nuucp | 9 | 指定给与 uucp 函数关联的另一个守护进程 | system/core-os |
| dladm | 15 | 为数据链路管理保留 | system/core-os |
| netadm | 16 | 为网络管理保留 | system/core-os |
| netcfg | 17 | 为网络配置管理保留 | system/core-os |
| smmsp | 25 | 指定给 Sendmail 邮件提交程序守护进程 | system/core-os |
| gdm | 50 | 指定给 GNOME Display Manager 守护进程 | system/core-os |
| zfssnap | 51 | 为自动快照保留 | system/core-os |
| upnp | 52 | 为 UPnP 服务器保留 | system/core-os |
| xvm | 60 | 为 xVM 用户保留 | system/core-os |
| mysql | 70 | 为 MySQL 用户保留 | system/core-os |

| 用户名 | 用户 ID | 说明 | 包 |
|---|---|---|---|
| openldap | 75 | 为 OpenLDAP 用户保留 | library/ldap |
| webservd | 80 | 为 WebServer 访问保留 | system/core-os |
| postgres | 90 | 为 PostgresSQL 访问保留 | system/core-os |
| svctag | 95 | 为 Service Tag Registry（服务标签注册表）访问保留 | system/core-os |
| unknown | 96 | 为 NFSv4 ACL 中不可映射的远程用户保留 | system/core-os |
| nobody | 60001 | 为 NFS 匿名访问用户保留 | system/core-os |
| noaccess | 60002 | 为没有访问权限的用户保留 | system/core-os |
| nobody4 | 65534 | 为 SunOS 4.x NFS 匿名访问用户保留 | system/core-os |
| ikeuser | 67 | 为 Internet 密钥交换 (Internet Key Exchange, IKE) 访问保留 | system/network/ike |
| ftp | 21 | 为 FTP 访问保留 | service/network/ftp |
| dhcpserv | 18 | 为 DHCP 服务器用户保留 | service/network/dhcp/isc-dhcp |
| aiuser | 60003 | 为 AI 用户保留 | system/install/auto-install/auto-install-common |
| pkg5srv | 97 | 为 pkg(5) depot 服务器保留 | package/pkg |

## shadow 文件中的字段

/etc/shadow 文件存储用户的加密口令和相关信息。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

该组文件是组信息的本地源。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。

The following displays the contents of a sample group file.

```
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:
aiuser::61:
ftp::21
pkg5srv::97:
```

以上屏幕提供示例 group 文件的内容，其中不包含任何说明。下表提供了有关典型 group 文件中列出的每个组的进一步信息。

表 1-4 缺省的 group 文件项

| 组名称 | 组 ID | 说明 | **pkg**(5) |
|---|---|---|---|
| root | 0 | 超级用户组 | system/core-os |
| other | 1 | 可选的组 | system/core-os |
| bin | 2 | 与正在运行的系统二进制文件相关联的管理组 | system/core-os |

| 组名称 | 组 ID | 说明 | **pkg**(5) |
|---|---|---|---|
| sys | 3 | 与系统日志记录或临时目录相关联的管理组 | system/core-os |
| adm | 4 | 与系统日志记录相关联的管理组 | system/core-os |
| uucp | 5 | 与 uucp 函数相关联的组 | system/core-os |
| mail | 6 | 电子邮件组 | system/core-os |
| tty | 7 | 与 tty 设备相关联的组 | system/core-os |
| lp | 8 | 行式打印机组 | system/core-os |
| nuucp | 9 | 与 uucp 函数相关联的组 | system/core-os |
| staff | 10 | 一般的管理组 | system/core-os |
| daemon | 12 | 与例行系统任务相关联的组 | system/core-os |
| sysadmin | 14 | 对系统管理员有用的管理组 | system/core-os |
| smmsp | 25 | Sendmail 邮件提交程序的守护进程 | system/core-os |
| gdm | 50 | 为 GNOME Display Manager 守护进程保留的组 | system/core-os |
| upnp | 52 | 为 UPnP 服务器保留的组 | system/core-os |
| xvm | 60 | 为 xVM 用户保留的组 | system/core-os |
| netadm | 65 | 为网络管理保留的组 | system/core-os |
| mysql | 70 | 为 MySQL 用户保留的组 | system/core-os |
| openldap | 75 | 为 OpenLDAP 用户保留 | library/ openldap |
| webservd | 80 | 为 WebServer 访问保留的组 | system/core-os |
| postgres | 90 | 为 PostgresSQL 访问保留的组 | system/core-os |
| slocate | 95 | 为 Secure Locate（安全定位）访问保留的组 | system/core-os |
| unknown | 96 | 为 NFSv4 ACL 中不可映射远程组保留的组 | system/core-os |
| nobody | 60001 | 为匿名 NFS 访问指定的组 | system/core-os |
| 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 | system/core-os |
| nogroup | 65534 | 为不是已知组中成员的用户指定的组 | system/core-os |
| aiuser | 61 | 为自动安装授权指定的组 | system/ install/auto-install/ auto-install-common |
| ftp | 21 | 为 FTP 访问指定的组 | system/core-os |
| pkg5srv | 97 | 指定给 pkg(5) depot 服务器的组 | package/pkg |

# 用于获取用户帐户信息的命令

下表介绍了系统管理员可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 获取用户相关信息的命令

| 命令 | 说明 | 手册页参考 |
| --- | --- | --- |
| auths | 列出和管理授权。 | auths(1) |
| getent | 显示来自管理数据库的项的列表。这些信息通常来自于为 /etc/nsswitch.conf 数据库指定的一个或多个源。 | getent(1M) |
| 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。 | logins(1M) |
| profiles | 列出和管理权限配置文件。 | profiles(1) |
| roles | 显示指定给用户的角色。 | roles(1) |
| userattr | 显示为 attribute_name 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 user_attr(4) 和 prof_attr(4) 手册页中定义的。<br>注 - 该命令是 Oracle Solaris 11 中新增的命令。 | Example 2–1 |

# 用于管理用户、角色和组的命令

注 - 不再支持 Solaris Management Console GUI 以及与 GUI 关联的命令行界面 (command-line interface, CLI)。

下表中说明的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 | 有关其他信息 |
| --- | --- | --- |
| useradd(1M) | 在本地或在 LDAP 系统信息库中创建用户。 | 如何添加用户 [35] |
| usermod(1M) | 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。 | 如何修改用户帐户 [36]<br>《在 Oracle Solaris 11.2 中确保用户和进程的安全 》中的“创建角色” |
| userdel(1M) | 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。 | 如何删除用户 [37] |
| roleadd(1M) | 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。 | 《在 Oracle Solaris 11.2 中确保用户和进程的安全 》中的“为用户指定权限” |

| 命令的手册页 | 说明 | 有关其他信息 |
| --- | --- | --- |
| rolemod(1M)<br>roledel(1M)<br>groupadd(1M)<br>groupmod(1M)<br>groupdel(1M) | 在本地或在 LDAP 系统信息库中管理组。 | 如何添加组 [38] |

# 关于用户的工作环境

本节介绍了以下信息：



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 都有各自的初始化文件，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 | 用途 |
| --- | --- | --- |
| bash | $HOME/.bash_profile<br>$HOME/.bash_login<br>$HOME/.profile | 定义用户登录时的用户环境 |
| ksh93 | /etc/profile<br>$HOME/.profile | 定义用户登录时的用户环境 |

| Shell | 用户初始化文件 | 用途 |
| --- | --- | --- |
| | `$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，请参见如何定制用户初始化文件 [34]。

# 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。站点初始化文件可用于将系统范围的更改分发到您在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。
- 您可以通过几种不同方式显示缺省 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) | `/usr/bin/bash` | 为安装程序创建的用户以及 `root` 角色使用的缺省 shell。<br><br>为通过 `useradd` 命令创建的用户以及 `root` 角色使用的缺省（交互式）shell 为 `/usr/bin/bash`。缺省路径为 `/usr/bin:/usr/sbin`。 |
| Korn Shell | `/usr/bin/ksh` | `ksh93` 是该 Oracle Solaris 发行版中的缺省 shell |

| Shell | 路径 | 注释 |
| --- | --- | --- |
| C Shell 和增强的 C Shell | `/usr/bin/csh` 和 `/usr/bin/tcsh` | C Shell 和增强的 C Shell |
| 符合 POSIX 的 Shell | `/usr/xpg4/bin/sh` | 符合 POSIX 的 Shell |
| Z Shell | `/usr/bin/zsh` | Z Shell |

注 - 缺省情况下，Z Shell (`zsh`) 和增强的 C Shell (`tsch`) 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。

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 1-9 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#` |

# 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 和 Korn 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_LINEND=()
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 - 环境变量在会话之间不会持续。要设置持久性环境变量值，请在 .bashrc 文件中设置值。

---

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 1-10 shell 变量和环境变量的说明

| 变量 | 说明 |
| --- | --- |
| CDPATH | 设置由 cd 命令使用的变量。如果将 cd 命令的目标目录指定为相对路径名，cd 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 CDPATH 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，假设 CDPATH 变量设置为 /home/jean，/home/jean 下面有两个目录：bin 和 doc。如果当前的目录是 /home/jean/bin 目录，那么，当您键入 cd doc 时，即使您未指定全路径名，目录也将切换到 /home/jean/doc。 |
| 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 LOGNAME 的缺省值自动设置为在 passwd 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。<br>注 - 从 Oracle Solaris 11 开始，不再需要 MANPATH 环境变量。man 命令根据 PATH 环境变量设置来确定合适的 MANPATH。 |
| 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。<br><br>在登录过程中，系统会自动定义缺省的 PATH，并将其设置为 .profile 中指定的路径。<br><br>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 PATH 定义为 PATH=/usr/bin:/usr/sbin:$HOME/bin，且 /usr/bin 和 /home/jean/bin 中均有名为 sample 的文件。如果用户键入 sample 命令而未指定其全路径名，则将使用在 /usr/bin 中找到的版本。 |
| PS1 | 为 bash shell 或 ksh93 shell 定义 shell 提示符。 |
| SHELL | 设置由 make、vi 和其他工具使用的缺省 shell。 |
| TERMINFO | 指定存储备用 terminfo 数据库的目录。可使用 /etc/profile 或 /etc/.login 文件中的 TERMINFO 变量。有关更多信息，请参见 terminfo(4) 手册页。<br><br>如果设置了 TERMINFO 环境变量，系统将首先检查由用户定义的 TERMINFO 路径。如果系统在用户定义的 TERMINFO 目录中找不到终端的定义，它将在缺省目录 (/usr/ |

| 变量 | 说明 |
| --- | --- |
| | share/lib/terminfo) 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 /etc/profile 或 /etc/.login 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 TERMINFO 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 ls -l 命令中显示日期。如果没有在用户的环境中设置 TZ，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，请在位于起始目录的 .bashrc 文件中添加或更改信息。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。

缺省路径由系统设置。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

设置 PATH 变量时，请注意以下准则：

- 如果您的路径中必须包括当前目录（.），请将其放置在最后。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，以降低 NFS 服务器不响应时系统无响应的概率。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 1-11 语言环境变量的值

| 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) |
| 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) |

例 1-1 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
```

# 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。

下表提供了 umask 值。它显示了为 umask 的每个八进制值创建的文件权限和目录权限。

表 1-12 umask 权限的值

| umask 八进制值 | 文件权限 | 目录权限 |
|---|---|---|
| 0 | rw- | rwx |
| 1 | rw- | rw- |
| 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

以下示例显示了 .profile 用户初始化文件的示例。您可以将此示例文件用作模板，以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。

例 1-2 .profile 文件

```
PATH=$PATH:$HOME/bin:/usr/local/bin:/usr/gnu/bin:       User's shell serach path
MAIL=/var/mail/$LOGNAME       Path to user's mail file
NNTPSERVER=server1       User's time/clock server
MANPATH=/usr/share/man:/usr/local/man       User's search path for man pages
PRINTER=printer1       User's default printer
umask 022       User's default file creation permissions
export PATH MAIL NNTPSERVER MANPATH PRINTER       Sets the listed environment variables
```

# 使用 Oracle Enterprise Manager Ops Center 管理用户

如果您在数据中心中管理物理和虚拟操作系统、服务器和存储设备，而不是仅管理单个系统，则可以使用 Oracle Enterprise Manager Ops Center 中提供的管理解决方案。

通过 Enterprise Manager Ops Center，您可以管理整个数据中心的用户和角色。您可以将来自各个系统的现有本地用户添加为 Ops Center 中的用户，并可以控制向这些用户授权使用的资产和功能。

有关信息，请参见 http://www.oracle.com/pls/topic/lookup?ctx=oc122。

♦ ♦ ♦ 第 2 章

# 使用命令行界面管理用户帐户

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 关于用户帐户和用户环境。

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。

## 使用 CLI 设置和管理用户帐户的任务列表

以下任务介绍了如何使用命令行界面 (Command-Line Interface, CLI) 设置和管理用户帐户。

| 任务 | 说明 | 相关说明 |
| --- | --- | --- |
| 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。 | “收集用户信息” [33] |
| 定制用户初始化文件。 | 设置用户初始化文件，以便为新用户提供一致的环境。 | 如何定制用户初始化文件 [34] |
| 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。 | 如何更改所有角色的帐户缺省值 [34] |
| 创建一个用户帐户。 | 使用您设置的帐户缺省值，通过 `useradd` 命令创建一个本地用户。 | 如何添加用户 [35] |
| 修改用户帐户。 | 修改系统上的用户登录信息。 | 如何修改用户帐户 [36] |
| 删除用户帐户。 | 使用 `userdel` 命令删除用户帐户。 | 如何删除用户 [37] |
| 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。 | 《在 Oracle Solaris 11.2 中确保用户和进程的安全 》中的“创建角色” |
| 创建组。 | 使用 `groupadd` 命令创建新组。 | 如何添加组 [38] |
| 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。 | 《在 Oracle Solaris 11.2 中确保用户和进程的安全 》中的“创建角色” |
| 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。 | 如何共享作为 ZFS 文件系统创建的起始目录 [39] |

| 任务 | 说明 | 相关说明 |
| --- | --- | --- |
| 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。 | “手动挂载用户的起始目录” [40] |

# 使用 CLI 设置用户帐户

本部分包括以下内容：



## 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会将用户的起始目录作为单独的 ZFS 文件系统放置在 `/export/home` 文件系统上。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《在 Oracle Solaris 11.2 中确保用户和进程的安全 》中的“使用所指定的管理权限”。
- 使用 `useradd` 命令创建用户帐户时，您必须指定 `-m` 选项，为该用户创建起始目录。

  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 - 如果您希望通过 `pam_zfs_key` 模块为用户创建加密的起始目录，请勿为 `useradd` 命令指定 `-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` 映射中创建项。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 映射项。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
```

如果按如下所示使用 -d 选项创建用户，则用户将具有 auto_home 项，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。

# 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 | |
| 角色名称 | |
| 配置文件或授权 | |
| UID | |
| 主要组 | |
| 辅助组 | |
| 注释 | |
| 缺省 Shell | |
| 口令状态和更新 | |
| 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

以下任务介绍了如何为您的系统上的用户设置定制的初始化文件。

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《在 Oracle Solaris 11.2 中确保用户和进程的安全 》中的“使用所指定的管理权限”。

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. 为每个用户类型定制用户初始化文件。
有关用户初始化文件定制方法的详细说明，请参见“关于用户的工作环境” [21]。

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《在 Oracle Solaris 11.2 中确保用户和进程的安全 》中的“使用所指定的管理权限”。

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。

# 使用 CLI 管理用户帐户

本部分包括以下内容：



## ▼ 如何添加用户

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《在 Oracle Solaris 11.2 中确保用户和进程的安全 》中的“使用所指定的管理权限”。

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。<br>使用 -d localhost:/export/home/*username* 而不是 -d /export/home/*username* 强制将项写入 auto_home 中。 |
| -m | 在系统上为用户创建本地起始目录。 |

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
```

有关更多命令选项的信息，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，以及显示和更改用户的权限配置文件。有关更多信息，请参见《在 Oracle Solaris 11.2 中确保用户和进程的安全 》中的“创建角色”。

## ▼ 如何修改用户帐户

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《在 Oracle Solaris 11.2 中确保用户和进程的安全 》中的“使用所指定的管理权限”。

2. 根据需要修改用户帐户。

   有关可以使用 usermod 命令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
```

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 `jdoe`。有关更多信息，请参见 `pam_user_policy(5)` 手册页。

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

另请参见 有关更多信息，请参见《在 Oracle Solaris 11.2 中确保用户和进程的安全 》中的“创建角色”。

## ▼ 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. 删除用户。

```
# userdel -r username
```

```
The -r option removes the account from the system.
```

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。

4. 如果用户的起始目录位于远程服务器上，请手动删除该目录。

```
# userdel username
```

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）或该用户在非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《在 Oracle Solaris 11.2 中确保用户和进程的安全 》中的“使用所指定的管理权限”。

2. **列出现有组。**

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

3. **创建新组。**

   ```
   $ groupadd -g group-id group-name
   ```

   | | |
   |---|---|
   | `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。

例 2-2 使用 `groupadd` 和 `useradd` 命令设置组和用户

以下示例显示如何使用 `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。

# 共享 ZFS 文件系统

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。

有关共享和取消共享文件系统的更多信息，请参见《在 Oracle Solaris 11.2 中管理网络文件系统 》中的“Autofs 管理”。

## ▼ 如何共享作为 ZFS 文件系统创建的起始目录

1. **承担 root 角色。**

   请参见《在 Oracle Solaris 11.2 中确保用户和进程的安全 》中的“使用所指定的管理权限”。

2. **为用户起始目录创建一个独立的池。**

   ```
   # zpool create pool mirror disk 1 disk 2 mirror disk 3 disk 4
   ```

   例如：

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

3. **为起始目录创建一个容器。**

   ```
   # zfs create filesystem
   ```

   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 11.2 中管理网络文件系统 》中的“Autofs 管理”。

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/jdoe
```

---

注 - 确保用户的起始目录已共享。有关详细信息，请参阅如何共享作为 ZFS 文件系统创建的起始目录 [39]。

---

♦ ♦ ♦ 第 3 章

# 3 使用用户管理器 GUI 管理用户帐户

本章提供了有关使用 Oracle Solaris 用户管理器图形用户界面 (GUI) 设置和管理用户的概述和任务相关信息。可以使用用户管理器 GUI 执行等效命令（例如，`useradd`、`usermod` 和 `userdel`）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 GUI 中的联机帮助。

本章包含以下主题：



有关管理用户帐户的概述信息，请参见第 1 章 关于用户帐户和用户环境。

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。

## 用户管理器 GUI 简介

本节提供以下信息：



用户管理器 GUI 基于 Visual Panels 框架并作为 Visual Panels 界面提供。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）GUI。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。

---

注 - 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。

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

## ▼ 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《在 Oracle Solaris 11.2 中确保用户和进程的安全 》中的“使用所指定的管理权限”。

2. 启动用户管理器 GUI。

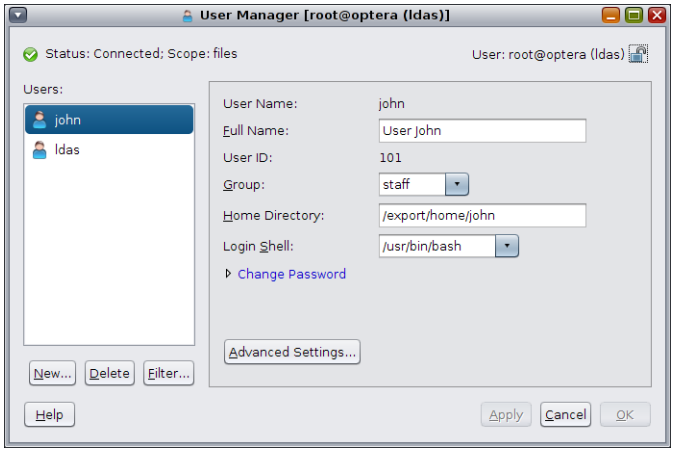
   - 桌面：选择 "System"（系统）-> "Administration"（管理）-> "User Manager"（用户管理器）。
   - 命令行：

     ```
     # vp usermgr &
     ```

## "User Manager"（用户管理器）对话框布局

启动用户管理器 GUI 时，将显示 "User Manager"（用户管理器）主对话框。"User Manager"（用户管理器）对话框用于管理用户和角色。对话框的左上角是 "Status"（状态）字段，该字段显示当前在本地主机上运行的服务的状态。在对话框的右上角是 "User"（用户）字段，其中显示用户管理器 GUI 当前正在使用的凭证。要了解如何更改凭证，请参见“承担角色” [44]。

下图显示了 "User Manager"（用户管理器）主对话框，其中选择了用户 john。




"User Manager"（用户管理器）对话框包括以下两个组成部分：

- 用户和角色列表 – 您可以从中选择要管理的用户的列表
- 基本设置 – 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。选择一位用户后，该用户的信息将显示在对话框的右侧。

您可以在 "User Manager"（用户管理器）对话框中执行以下操作：

- 创建新用户或角色 – 请参见如何使用用户管理器 GUI 添加用户或角色 [45]。
- 删除现有用户或角色 – 请参见如何使用用户管理器 GUI 删除用户或角色 [47]。
- 过滤用户信息 – 请参见“过滤 GUI 中显示的信息” [43]。
- 管理现有用户的高级设置 – 请参见如何使用用户管理器 GUI 修改用户或角色 [47]。

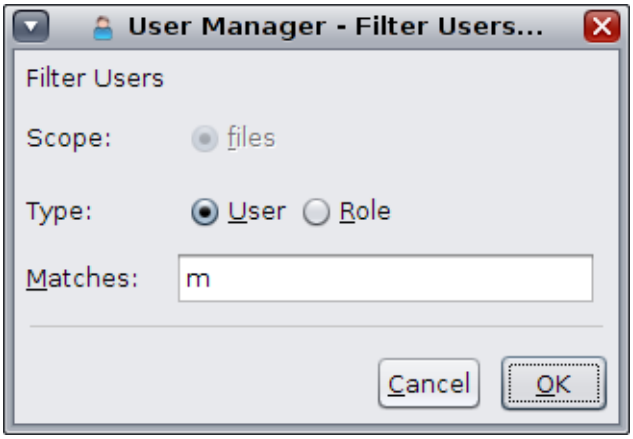
# 过滤 GUI 中显示的信息

您可以过滤用户管理器 GUI 中显示的信息。可以选择仅显示用户，也可以选择仅显示角色。并且，如果将系统配置为 LDAP 客户机，您可以将范围限制为显示文件信息或 LDAP 信息。

缺省设置为 "User"（用户）和 "Files"（文件）。这些设置显示用户（而不是角色）和用户的文件信息（而不是用户的 LDAP 规范）。

在过滤器对话框中，还提供了选项以用于搜索与您输入的任何搜索条件匹配的用户名或角色名称。

在以下对话框中，系统没有针对 LDAP 进行配置，因此未提供范围选项。对类型进行了过滤，以便显示用户（而不是角色）。而且指定了一个搜索来来查找以 "m" 开头的用户名。




### ▼ 如何为缺省名称服务类型和范围设置过滤器

1. 启动用户管理器 GUI。
   请参见如何启动用户管理器 GUI [42]。
2. 单击“筛选”按钮。
3. 将 "Scope"（范围）选项设置为 "file"（文件）件或 "LDAP"（如果提供）。
4. 将 "Type"（类型）选项设置为 "User"（用户）或 "Role"（角色）。
5. 或者，要针对特定角色名称或用户名进行过滤，请输入要作为搜索条件的文本。
6. 单击 "OK"（确定）。

## 承担角色

如果您具有 "User Management"（用户管理）权限配置文件，则可以创建新用户和新角色，但前提是要创建的用户或角色的高级属性属于您自己的颁发机构的属性。如果您没有足够的授权，但是拥有具备足够授权的管理角色，则您可以承担该角色，通过单击 "User Manager"（用户管理器）主对话框中的 "Lock"（锁定）按钮来执行必要的管理操作（如此过程中所述）。

### ▼ 如何承担角色

1. 启动用户管理器 GUI。

请参见如何启动用户管理器 GUI [42]。

2. 在 "User Manager"（用户管理器）主对话框中，单击对话框右上部的用户名旁边的 "Lock"（锁定）图标。
   显示一个子菜单，其中包含下列选项：
   - 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，其中列出了您可以获得的角色。
4. 选择相应的角色。
5. 单击 "Log In"（登录）以承担该角色。
   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。

本节介绍了以下信息：

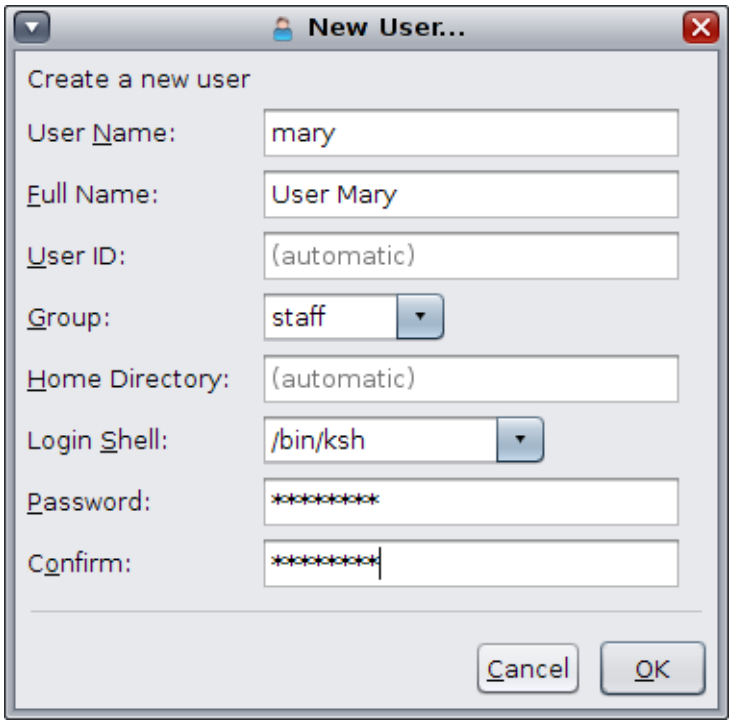


## ▼ 如何使用用户管理器 GUI 添加用户或角色

此过程在 GUI 当前正在使用的过滤器范围内添加新用户或角色。

1. 启动用户管理器 GUI。
   请参见如何启动用户管理器 GUI [42]。
2. 单击 "User Manager"（用户管理器）主对话框中的 "New"（新建）按钮。

将显示 "New User"（新建用户）对话框。




3. 提供用户帐户信息。
   - User Name（用户名）
   - Full Name（全名）
   - User ID（用户 ID） – 此信息是可选的。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） – 此信息是可选的。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） – 为用户指定临时口令。
   - Confirm（确认） – 确认为用户指定的临时口令。
4. 单击 "OK"（确定）。

该用户或角色将添加到 "User Manager"（用户管理器）主对话框中显示的用户列表中，单击 "OK"（确定）。

## ▼ 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。
   请参见如何启动用户管理器 GUI [42]。
2. 从所显示的列表中选择要修改的用户或角色。
   选择用户后，对话框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，则在该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“使用用户管理器 GUI 指定高级属性” [47]。
6. 单击 "OK"（确定）保存更改并关闭对话框。

## ▼ 如何使用用户管理器 GUI 删除用户或角色

此过程在 GUI 当前正在使用的过滤器范围内删除用户或角色。

1. 在 "User Manager"（用户管理器）主对话框中选择该用户或角色。
2. 单击 "Delete"（删除）按钮。
3. 在确认对话框中单击 "OK"（确定）。

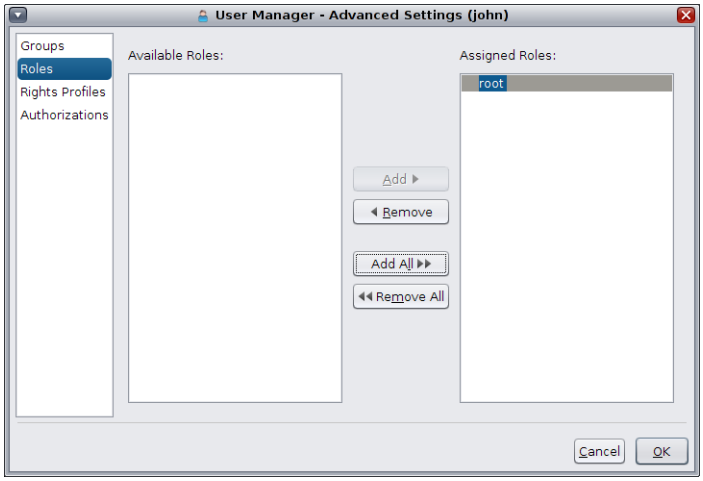
# 使用用户管理器 GUI 指定高级属性

本节介绍了以下信息：

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。

有关概述的信息，请参见《在 Oracle Solaris 11.2 中确保用户和进程的安全 》中的第 1 章 “使用权限控制用户和进程”。

下图显示了 "Advanced Settings"（高级设置）对话框，其中选择了用户 john 的 "Roles"（角色）安全属性。所选用户的名称将显示在该对话框标题栏中的括号内。




"Advanced Settings"（高级设置）对话框可用于指定以下安全属性：

- Groups（组）
- Roles（角色）
- Rights Profiles（权限配置文件）
- Authorizations（授权）

# 使用用户管理器 GUI 指定组

通过用户管理器 GUI 的 "Advanced Settings"（高级设置）指定组。

## ▼ 如何指定组

1. 启动用户管理器 GUI。
   请参见如何启动用户管理器 GUI [42]。

2. 在 "User Manager"（用户管理器）主对话框中选择一个用户，然后单击 "Advanced Settings"（高级设置）按钮。
   此时将显示 "Advanced Settings"（高级设置）对话框。

3. 单击对话框左侧的 "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）列表中选择一个或多个组，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，请从该列表中选择一个或多个组，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）主对话框中单击 "Apply"（应用）或 "OK"（确定）之后，才会应用更改。

# 使用用户管理器 GUI 指定角色

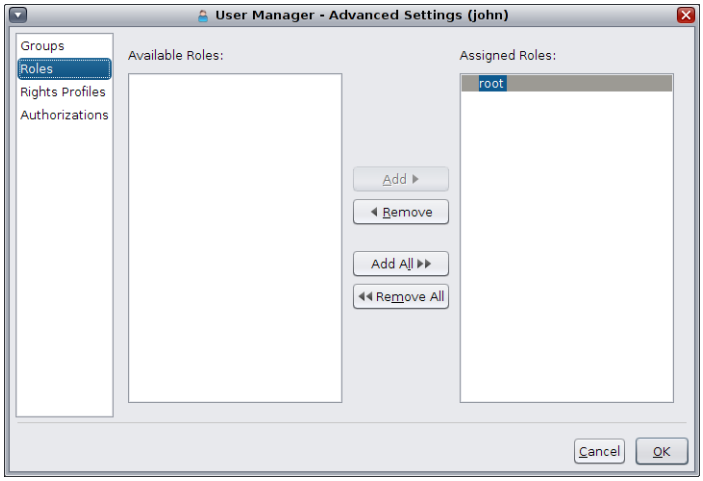
通过用户管理器 GUI 的 "Advanced Settings"（高级设置）指定角色。

---

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）对话框，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 指定角色

1. 启动用户管理器 GUI。
   请参见如何启动用户管理器 GUI [42]。

2. 在 "User Manager"（用户管理器）主对话框中选择一个用户，然后单击 "Advanced Settings"（高级设置）按钮。
   此时将显示 "Advanced Settings"（高级设置）对话框。

3. 单击对话框左侧的 "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）列表中选择一个或多个角色，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个或多个角色，然后单击 "Remove"（删除）。

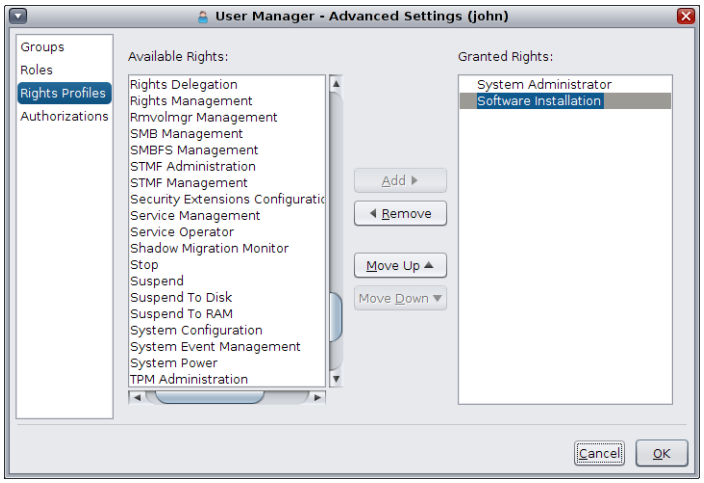
   - 要添加或删除当前用户的所有角色，请单击 "Add All"（全部添加）或 "Remove All"（全部删除）按钮。

4. 单击 "OK"（确定）保存设置。
   只有在 "User Manager"（用户管理器）主对话框中单击 "Apply"（应用）或 "OK"（确定）之后，才会应用更改。

# 使用用户管理器 GUI 指定权限配置文件

通过用户管理器 GUI 的 "Advanced Settings"（高级设置）指定权限配置文件。

下图显示了 "Advanced Settings"（高级设置）对话框，其中选择了用户 john 的 "Rights Profile"（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。
   请参见如何启动用户管理器 GUI [42]。

2. 在 "User Manager"（用户管理器）主对话框中选择一个用户，然后单击 "Advanced Settings"（高级设置）按钮。
   此时将显示 "Advanced Settings"（高级设置）对话框。

3. 单击对话框左侧的 "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）配置文件列表中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，请从该列表中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）主对话框中单击 "Apply"（应用）或 "OK"（确定）之后，才会应用更改。

# 使用用户管理器 GUI 指定授权

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 指定授权

1. 启动用户管理器 GUI。

   请参见如何启动用户管理器 GUI [42]。

2. 在 "User Manager"（用户管理器）主对话框中选择一个用户，然后单击 "Advanced Settings"（高级设置）按钮。

   此时将显示 "Advanced Settings"（高级设置）对话框。

3. 单击对话框左侧的 "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）列表中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，请从该列表中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）主对话框中单击 "Apply"（应用）或 "OK"（确定）之后，才会应用更改。

# 索引

## Z