学习 Linux，302 （混合环境）: 管理用户帐号和组

规划用户和组帐号管理

关于本系列

本系列文章帮助您了解 Linux 系统管理任务相关知识。您可以使用本系列文章的资料准备 Linux Professional Institute Certification level 3 (LPIC-3) 考试 [1]。

参见我们的 学习 Linux, 302（混合环境）：LPI-302 路线图 [2]，查看本系列中各篇文章的介绍和链接。路线图目前仍在更新中，目前反映的最新内容是 LPIC-3 考试的最新目标（*2011* 年 *3* 月）。在我们完成每篇文章后，都会将其添加到路线图中。

在本文中，学习以下这些概念：

- UNIX 帐号
- 管理 Samba 帐号
- 对文件和目录强制执行帐号权限

本文帮助您准备 LPI 的 Mixed Environment 特性考试 (302) 的主题 313 中的目标 313.1。该目标的权重为 4。

先决条件

为了最有效地利用本系列中的文章，您应该具有高级 Linux 知识，并需要准备一个 Linux 系统，用于练习本文介绍的命令。特别是，本文假设您具有 Linux 命令行功能的工作知识且至少理解 “学习 Linux，302（混合环境）：概念 [3]” 中所涵盖的 Samba 目的。要执行本文描述的操作，您必须安装 Samba 软件。另外，您应该能够通过网络访问一个 Windows 客户机。

回页首

了解 UNIX 用户和组帐号

关于选择性 LPI-302 考试

与其他许多认证一样，Linux Professional Institute Certification (LPIC) 提供多个不同级别，每个级别都比前一个级别要求更多知识和经验。LPI-302 考试是 LPIC 层级的第三级中的一个可选特性考试，要求具有高级 Linux 系统管理知识。

要通过 LPIC 级别 3 (LPIC-3) 认证，您必须通过前两个一级考试（101 和 102），两个二级考试（201 和 202），以及 LPIC-3 核心考试 (301)。到达这个级别后，才能参加一些可选特性考试，比如 LPI-302。

您的 Samba 服务器可能没有位于一个接收器 (silo) 中。用户需要访问文件和目录，但事先需要验证身份。用户可能从 Linux 工作站或 Windows 桌面连接。无论采用哪种方式，他们都需要 Samba 服务器识别的帐号。

通过身份验证后，用户需要适当的权限以访问文件、目录和打印服务。组 是 Samba 的一个特性，能够帮助您更好地管理这些权限。

sam 后端数据库是本地 UNIX 帐号和远程用户帐号之间的中介。有几种方法允许您的用户验证到 Samba 服务器，但在深入了解 Samba 帐号之前，您应该深入了解 UNIX 用户和组帐号管理的基础知识。

用户帐号

使用 useradd 之类的工具在 Linux 计算机上创建本地用户帐号时，帐号信息被写入 /etc/passwd 文件。该文件存储用户的用户名、主目录、默认 shell 以及帐号注释等信息。这些帐号通常称为 *UNIX* 本地帐号。本文使用术语 *UNIX* 帐号 或本地帐号，它们可以互换使用。

清单 1 创建了一个本地帐号，用户名为 *monty* ，在注释区域中提供了一个 *Monty Python* (-c) 的描述，指定了一个主目录 (-m)，并向用户提供一个默认 shell：/bin/bash (-s)。

清单 1. 创建一个本地帐号

```
[tbost@samba ~]$ sudo useradd -c'Monty Python' -m -s /bin/bash monty
[tbost@samba ~]$ less /etc/passwd | grep monty
monty:x:504:504:Monty Python:/home/monty:/bin/bash
[tbost@samba ~]$
```

/etc/passwd 中的每一行都代表一条用户帐号记录。每条记录均有 7 个字段，并由

分隔符冒号 (:) 进行分隔。当您管理 Samba 帐号时，应该特别注意第一个字段中的用户名、第三个字段中的用户 ID (UID) 和第四个字段中的组 ID (GID)。

组帐号

组帐号在减轻多用户计算机的管理负担方面至关重要。如果您正在管理一个 Samba 服务器，那么允许对特定目录、文件和打印服务进行指定访问是典型配置的一部分。

与用户帐号一样，如果您正在处理一个本地 Samba 帐号配置，那么在大多数 Samba 配置中，您需要在本地 Samba 服务器上创建 UNIX 组帐号。您可以在 /etc/group 文件中找到 UNIX 组帐号信息。有些 Linux 发行版为每个新用户创建一个本地私有 组。这里的情况也一样，只是添加了用户 *monty*：

```
[tbost@samba ~]$ less /etc/group | grep monty
monty:x:504:
[tbost@samba ~]$
```

这里的代码展示为用户 monty 创建的私有组帐号。如果您在包含 Windows 计算机的混合环境中工作，那么应记住，Windows 不允许用户帐号和组帐号拥有相同的名称。

与用户帐号非常相似，组帐号只有位于本地 UNIX 服务器上，Samba 才能使用它们。要创建一个组，可以使用 groupadd 之类的工具（见清单 2），也可以使用 vim 之类的编辑器直接编辑 /etc/group 文件。

清单 2. 创建一个组帐号并向其添加一个用户

```
[tbost@samba ~]$ sudo groupadd accounting
[tbost@samba ~]$ sudo usermod -G accounting monty
[tbost@samba ~]$ less /etc/group | grep accounting
accounting:x:506:monty
[tbost@samba ~]$
```

清单 2 使用 /sbin/groupadd 和 /sbin/usermod 工具创建一个组并向其添加一个用户。如果您要向一个组添加多个用户，可以创建一个脚本来执行添加任务，也可以直接将用户添加到 /etc/group 文件。组成员应该位于最后一个字段中并以逗号 (,) 分隔。如果您手动创建组，那么应记住，每个组都应该拥有一个惟一的 GID。

回页首

管理 Samba 帐号

对于典型的 Samba 配置，帐号信息存储在下面三个密码数据库中的一个：

- smbpasswd
- tdbsam
- ldapsam

使用 smbpasswd 和 tdbsam

在版本 3.4 之前，Samba 使用的默认后端数据库是 smbpasswd 数据库。在 Samba 3.4 中，smbpasswd 已被淘汰，现在使用的默认后端数据库是 tdbsam，它也是推荐使用在用户数量低于 250 个的环境的后端数据库。

据说 tdbsam 数据库的伸缩性比 smbpasswd 更好。如果您使用的 Samba 版本采用 smbpasswd 作为默认后端数据库，可以在 smb.conf 文件中更改后端数据库：在 global 区域中指定参数 passdb = tdbsam。

但 smbpasswd 不仅仅是一个数据库：它是 Samba 套件包含的一个工具，支持通过简单的 Samba 配置管理 Samba 帐号。创建 Samba 帐号需要根权限。在尝试创建 Samba 帐号之前，该帐号应该已存在于本地 Linux 服务器上。清单 3 展示了使用 smbpasswd 创建一个 Samba 用户帐号的代码。

清单 3. 使用 smbpasswd 创建一个 Samba 用户帐号

```
[tbost@samba ~]$ sudo smbpasswd -a monty
New SMB password:
Retype new SMB password:
Added user monty.
```

用户拥有访问 smbpasswd 的权限，以便更改他们的密码，如清单 4 所示。

清单 4. 本地用户使用 smbpasswd 更改密码

```
[monty@samba ~]$ smbpasswd
Old SMB password:
New SMB password:
Retype new SMB password:
Password changed for user monty
[monty@samba ~]$
```

或者，您可以配置 Samba 密码同步，以便在用户更改本地帐号密码时，更新 Samba 密码。

```
[global]
unix password sync = yes
```

如果用户在较长的时间内不需要访问 Samba 服务器，那么您可以临时禁用帐号，在稍后需要时再启用它。如果用户不再需要访问服务器，则可以删此除帐号。清单 5 展示了相关命令。

使用 smbpasswd 禁用、启用和删除一个 Samba 帐号

```
[tbost@samba ~]$ sudo smbpasswd -d monty
Disabled user monty.
[tbost@samba ~]$ sudo smbpasswd -e monty
Enabled user monty.
[tbost@samba ~]$ sudo smbpasswd -x monty
Deleted user monty.
[tbost@samba ~]$
```

使用 pdbedit

Samba 套件中包含一个功能丰富的工具：pdbedit。这个工具能够处理三个后端数据库中任何一个数据库的帐号。除了创建、修改和移除用户外，还可以使用 pdbedit 执行以下操作：

- 列示用户帐号
- 指定主目录
- 导入用户帐号
- 设置帐号策略

您可以在 tdbsam 数据库上互换使用 pdbedit 和 sambapasswd（见清单 6）。但是，使用 pdbedit 执行的命令需要根权限。

清单 6. 使用 smbpasswd 和 pdbedit 与后端数据库交互

```
[tbost@samba ~]$ sudo smbpasswd -a monty
New SMB password:
Retype new SMB password:
Added user monty.
[tbost@samba ~]$ sudo pdbedit -L
```

```
monty:504:Monty Python
[tbost@samba ~]# sudo pdbedit -L --verbose
Unix username:        monty
NT username:
Account Flags:        [U          ]
User SID:             S-1-5-21-2247757331-3676616310-3820305120-1001
Primary Group SID:    S-1-5-21-2247757331-3676616310-3820305120-513
Full Name:            Monty Python
Home Directory:       \\samba\monty
HomeDir Drive:
Logon Script:
Profile Path:         \\samba\monty\profile
Domain:               SAMBA
Account desc:
Workstations:
Munged dial:
Logon time:           0
Logoff time:          never
Kickoff time:         never
Password last set:    Tue, 24 May 2011 14:19:46 CDT
Password can change:  Tue, 24 May 2011 14:20:16 CDT
Password must change: Tue, 24 May 2011 14:20:16 CDT
Last bad password   : 0
Bad password count  : 0
Logon hours         : FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
```

清单 6 展示如何使用 smbpassd 创建一个用户，并使用 pdbedit 列示 Samba 用户。要在 pdbedit 中获取更详细的用户信息，可以包含 --verbose 开关。

构建您自己的提要

您可以构建自定义 RSS、Atom 或 HTML 提要，以便在我们添加新文章或者更新内容时收到通知。访问 developerWork RSS 提要 [4]。选择 Linux 作为专区，Articles 作为类型，输入 Linux Professional Institute 作为关键字。然后选择您的首选提要类型。

还可以使用 pdbedit 设置帐号策略。可管理的帐号策略名称如下：

- min password length
- password history
- user must logon to change password

- maximum password age
- minimum password age
- lockout duration
- reset count minutes
- bad lockout attempt
- disconnect time
- refuse machine password change

清单 7 将最小密码长度更改为 8 个字符，然后将最大密码有效期更改为 30 天。-P 开关接受一个字符串参数，该参数应该精确匹配预定义的策略名称；-c 开关接受的参数的值为策略设置。

清单 7. 使用 pdbedit 管理帐号

```
[tbost@samba ~]$ sudo pdbedit -P 'min password length' -C 8
account policy "min password length" description: Minimal password length (default: 5)
account policy "min password length" value was: 5
account policy "min password length" value is now: 8
[tbost@samba ~]$ sudo pdbedit -P 'maximum password age' -C 30
...
account policy "maximum password age" value was: 4294967295
account policy "maximum password age" value is now: 30
```

参阅 man pdbedit 文档或键入 pdbedit -h，了解关于可用命令的详细信息。

使用 ldapsam

如果您正在使用一个现有目录服务，比如 Lightweight Directory Access Control (LDAP)，或者正在一个大环境（即超过 250 个用户）中工作，那么您可以使用 ldapsam 后端。在三个后端数据库中，ldapsam 是惟一支持组帐号存储的数据库。通过将所有用户和组存储在 ldap 后端中，您的所有服务器就能拥有统一的 UID 和 GID。配置 LDAP 超出了本文的范围，但 smb.conf 中的 idmap backend 参数会指定您的 LDAP 服务器的位置。

下面设置的参数指示 Samba 将名为 directory-services.example.org 的主机的 LDAP 目录服务用作其后端存储。您首先应该拥有一个配置为与 Samba 交互的工作 LDAP 服务器。（下一节将详细讨论 idmap。）

```
[global]
idmap backend = ldap:ldap://directory-services.example.org:636
```

回页首

映射帐号

如果您的 Samba 服务器是一个域中的独立服务器，那么您可能只需要使用映射文件。但是，如果您的环境包含从另一个域连接到 Samba 服务器的用户，那么 idmap 工具可以帮助您正确映射这些 UID 和 GID。

使用 sampasswd 和 TDB 文件进行用户映射

如果连接到 Samba 服务器的 Windows 用户与 Samba 服务器上创建的用户拥有相同的用户名，那么就不需要使用映射文件。但是，如果您的 Windows 用户的用户名不完全匹配，那么您可以创建一个映射文件来链接用户名。记住，尽管 Linux 会区分大小写，但 Windows 用户名不区分大小写。因此，Windows 用户名 *TBost* 与 *tbost* 不是相同的本地帐号。表 1 展示了从 Windows 到 UNIX 帐号名称的映射。

表 1. 将用于映射的 Windows 和 UNIX 帐号名称

Windows	UNIX
Monty	monty
bostt	tbost
sue.george	sue

创建 Samba 帐号时，使用 Windows 帐号名称。这样，您可以在 smb.conf 文件中指定一个文件位置，将帐号映射到适当的 UNIX 帐号。清单 8 展示了 UNIX 中的帐号映射。

清单 8. UNIX 中的简单帐号映射

```
[tbost@samba ~]$ sudo vi /etc/samba/smb.conf
[global]
username map = /etc/samba/smbusers
...
...
...
[tbost@samba ~]$ sudo vi /etc/samba/smbusers
# Unix_name = SMB_name1 SMB_name2 ...
root = administrator admin
nobody = guest pcguest smbguest
monty = Monty
tbost = bostt
```

```
sue = sue.george
```

清单 8 中的代码命令将 username map 参数配置为使用 /etc/samba/smbusers 作为映射文件。映射帐号时，操作很简单：将 UNIX 帐号名称放在左边，Samba 帐号名称放在右边，中间用等号 (=) 连接。当用户连接时，Samba 映射到相应的帐号。

映射组

对于典型的 Samba 服务器环境，可以使用 Samba 套件的 net groupmap 命令配置组映射。假设 Windows 用户帐号 Monty、bostt 和 sue.george 分别是 Domain Admins、Domain Users 和 Domain Guests 组帐号的成员。如果您想要这些用户拥有 Samba 服务器上的类似 UNIX 组的组帐号权限，那么可以将 UNIX 帐号用户名添加到每个组：

```
adm:x:4:root,adm,daemon,monty,tbost,sue
users:x:100:monty,tbost,sue
guests:x:507:monty,tbost,sue
```

这只是 Samba 服务器上的完整组列表的一部分。在 Linux 操作系统安装时会创建 adm 和 users 组，您需要将每个用户添加到相应的组（见表 2）。

表 2. 将用于映射的 Windows 和 UNIX 帐号组

Windows	UNIX	Windows relative ID (RID)	UNIX GID
Domain Admins	adm	512	4
Domain Users	users	513	100
Domain Guests	guests	514	507

net groupmap 命令能够映射您的域组（见清单 9），net groupmap list 会列示域组映射。从 Samba 3.x 开始，可以使用新的组映射功能在 Windows 组 RID 和 UNIX GID 之间创建关联。

清单 9. 使用 groupmap 命令映射组

```
[tbost@samba ~]$sudo net groupmap add ntgroup="Domain Admins" unixgroup=adm \
rid=512 type=d
Successfully added group Domain Admins to the mapping db as a domain group
[tbost@samba ~]$ sudo net groupmap add ntgroup="Domain Users" unixgroup=users \
```

```
rid=513 type=d
Successfully added group Domain Users to the mapping db as a domain group
[tbost@samba ~]$sudo net groupmap add ntgroup="Domain Guests" unixgroup=guests \
rid=514 type=d
Successfully added group Domain Guests to the mapping db as a domain group
[tbost@samba ~]$sudo net groupmap list
Domain Users (S-1-5-21-2247757331-3676616310-3820305120-513) -> users
Domain Guests (S-1-5-21-2247757331-3676616310-3820305120-514) -> guests
Domain Admins (S-1-5-21-2247757331-3676616310-3820305120-512) -> adm
```

清单 9 中映射组操作的步骤顺序如下：

1. 通过根权限，使用 net groupmap add 命令指定要映射到 UNIX 组 *unixgroup=adm* 的 Windows 组 *ntgroup='Domain Admin"*。对每个组映射执行这个步骤。
2. 清单 9 中的最后一条命令显示了组映射。

使用身份映射

对于大多数环境，上述映射就足够了。但是，如果您管理更复杂的环境，比如包含从多个不同的域连接到您的 Samba 服务器的多个 Samba 服务器或工作站的环境，那么您应该熟悉一下身份映射 (IDMAP) 和 Winbind。IDMAP 能够帮助克服安全 ID (SID) 和本地 UNIX UID 或 GID 之间的互操作性问题。

如果您的 Samba 服务器是 Windows 域成员，那么您可以使用 Winbind 将 SID 映射到 UID 或 GID。 您可以设置 idmap 参数的范围，指定 Winbind 在 smb.conf 文件中缓存帐号信息的时间 ：

```
[global]
idmap uid = 20000-50000
idmap gid = 20000-50000
winbind cache time = 300
```

上述代码中的参数指示 Winbind 使用本地 UID 范围为 20000-50000，GID 范围为 20000-50000。对于不大可能拥有数千本地用户或组帐号的 Samba 服务器而言，这个配置是一个相对安全的范围。winbind cache time = 300 参数指示 Winbind 缓存帐号信息 300 秒。在默认情况下，Winbind 在 inbind_idmap.tdb 文件中存储映射。

回页首

使用默认帐号强制所有权

您可能会发现，向一个组添加每个用户比较麻烦，更简单的方法是使用 force user 和 force group 参数。这些参数指示 Samba 连接到一个授权用户，该用户拥有指定用户和组的权限。这在配置由多个用户访问的共享时尤其有用，只需配置一些公共权限就足够了：

```
[global]
username map = /etc/samba/smbusers
force user = guest
force group = +employees
```

在上面的代码中，force user 参数在处理文件时会将所有已连接用户视为用户 *guest*。用户必须仍然使用一个有效用户帐号进行连接。 这个配置将一些用户帐号强制为 *guest*，其组帐号为 *employees*。

参考资料

学习

- 参阅 Samba 3.x 手册第 11 章，详细了解 Samba 帐号信息数据库 [5]。
- 参阅 Samba 3.x 手册第 12 章，详细了解 组映射 [6]。
- 参阅 pdbedit 手册文档，了解 pdbedit 工具 [7] 的详细说明。
- 参阅 Samba 手册第 14 章，详细了解独立和主域控制器服务器的 Identity Mapping (IDMAP) [8]。
- 在 LPIC Program [9] 网站查找 LPI 的 Linux 系统管理认证的三个级别的具体目标、任务列表和例题。特别是要查看 LPI-302 具体目标 [10] 和 任务和例题 [11]。
- 复习 developerWorks 上的整个 LPI 考试备考系列 [12]，学习 Linux 基础知识，根据 2009 年 4 月以前的 Linux 考试目标准备系统管理员认证考试。
- 适用于修订版 LPIC 考试的考试准备资源 [13] 提供了一系列由 LPI 维护的其他认证培训资源。
- 观看 developerWorks 演示中心 [14]，包括面向初学者的产品安装和设置演示，以及为经验丰富的开发人员提供的高级功能。
- 在 developerWorks Linux 专区 [15] 寻找为 Linux 开发人员（包括 Linux 新手入门 [16]）准备的更多参考资料，查阅我们 最受欢迎的文章和教程 [17]。
- 在 developerWorks 上查阅所有 Linux 技巧 [18] 和 Linux 教程 [19]。

- 随时关注 developerWorks 技术活动 [20]和网络广播 [21]。

讨论

- 加入 developerWorks 中文社区 [22]，developerWorks 社区是一个面向全球 IT 专业人员，可以提供博客、书签、wiki、群组、联系、共享和协作等社区功能的专业社交网络社区。

关于作者

Tracy Bost 是一名经验丰富的软件开发人员和系统工程师。他的专长是企业应用程序集成。他过去曾担任过抵押行业标准维护组织 (Mortgage Industry Standards Maintenance Organization, MISMO) 业务规则工作组的联合主席和 RuleML2010 行业标准的委员会联合主席。他曾在多个行业任职，这些行业包括抵押贷款、房地产和非营利行业。

为本文评分

平均分 (0个评分)

1 星 1 星
2 星 2 星
3 星 3 星
4 星 4 星
5 星 5 星

评论

添加评论:

请 登录 或 注册 [23] 后发表评论。

注意：评论中不支持 HTML 语法

有新评论时提醒我剩余 1000 字符

快来添加第一条评论

回页首

1. http://www.lpi.org/
2. http://www.ibm.com/developerworks/cn/linux/l-lpic3-map/
3. http://www.ibm.com/developerworks/cn/linux/l-lpic3-310-1/
4. http://www.ibm.com/developerworks/cn/views/rss/customfeed.jsp
5. http://www.samba.org/samba/docs/man/Samba-HOWTO-Collection/passdb.html
6. http://www.samba.org/samba/docs/man/Samba-HOWTO-Collection/groupmapping.html
7. http://linuxcommand.org/man_pages/pdbedit8.html
8. http://www.samba.org/samba/docs/man/Samba-HOWTO-Collection/idmapper.html
9. http://www.lpi.org/eng/certification/the_lpic_program
10. http://www.lpi.org/eng/certification/the_lpic_program/lpic_3/exam_302_detailed_objectives
11. http://www.lpi.org/eng/certification/the_lpic_program/lpic_3/exam_302_tasks_and_sample_questions
12. http://www.ibm.com/developerworks/cn/linux/lpi/index.html
13. http://www.lpi.org/eng/training__1/new_exam_preparation_resources_for_revised_lpic_exams
14. http://www.ibm.com/developerworks/cn/offers/lp/demos/
15. http://www.ibm.com/developerworks/cn/linux/
16. http://www.ibm.com/developerworks/cn/linux/newto/
17. http://www.ibm.com/developerworks/cn/linux/best2009/index.html
18. http://www.ibm.com/developerworks/cn/views/linux/libraryview.jsp?search_by=Linux+%E6%8A%80%E5%B7%A7
19. http://www.ibm.com/developerworks/cn/views/linux/libraryview.jsp?type_by=%E6%95%99%E7%A8%8B
20. http://www.ibm.com/developerworks/cn/offers/techbriefings/
21. http://www.ibm.com/developerworks/cn/swi/
22. http://www.ibm.com/developerworks/cn/community/
23. http://www.ibm.com/developerworks/dwwi/DWAuthRouter?m=register&lang=zh_CN&d=http%3A%2F%2Fwww.ibm.com%2Fdeveloperworks%2Fcn%2Flinux%2Fl-lpic3-313-1%2F%23icomments