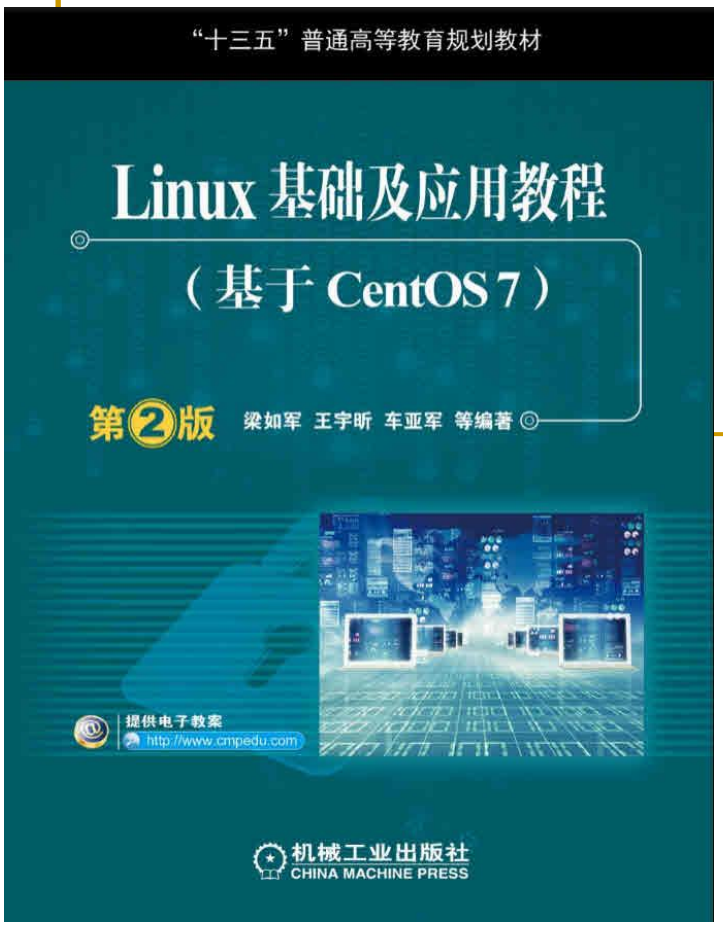


第13章 Samba服务

主讲人： 梁如军

2015-05-05

本章内容要点

- SMB/CIFS协议和Samba简介
- 安装和启动Samba
- 配置Samba文件共享
- 在Linux环境下访问Samba共享

梁如军（linuxbooks@126.com）

本章学习目标

- 熟悉 SMB/CIFS 协议
- 了解 Samba 的功能
- 熟悉 Samba 的工具使用
- 学会安装和启动 Samba 服务器
- 掌握 Samba 文件共享的配置
- 学会在 Linux 环境下访问 Samba 共享

梁如军（linuxbooks@126.com）

SMB/CIFS协议和SAMBA简介

梁如军（linuxbooks@126.com）

SMB协议

- SMB（Server Message Block，服务信息块）协议是一个高层协议， 它提供了在网络上的不同计算机之间共享文件、打印机和不同通信资料的手段。
- SMB使用 NetBIOS API实现面向连接的协议， 该协议为 Windows 客户程序和服务提供了一个通过虚电路按照请求—响应方式进行通信的机制。
- SMB的工作原理就是让 NetBIOS 与 SMB 协议运行在TCP/IP上， 并且使用NetBIOS的名字解释器让Linux机器可以在 Windows 的网上邻居中被看到， 从而和 Windows9X/NT/200X 进行相互沟通，共享文件和打印机。

梁如军（linuxbooks@126.com）

SMB与网络模型的关系

<table>
<tr><th>OSI</th><th colspan="4"></th><th>TCP/IP</th></tr>
<tr><td>Application
Presentation</td><td colspan="4">SMB</td><td rowspan="2">Application</td></tr>
<tr><td>Session</td><td>NetBIOS</td><td rowspan="3">NetBEUI</td><td>NetBIOS</td><td>NetBIOS</td></tr>
<tr><td>Transport</td><td rowspan="2">IPX[1]</td><td rowspan="2">DECnet</td><td>TCP&UDP</td><td>TCP/UDP</td></tr>
<tr><td>Network</td><td>IP</td><td>IP</td></tr>
<tr><td rowspan="2">Link</td><td rowspan="2">802.2,
802.3,802.5</td><td>802.2</td><td rowspan="2">Ethernet V2</td><td rowspan="2">Ethernet V2</td><td rowspan="2">Ethernet or
others</td></tr>
<tr><td>802.3,802.5</td></tr>
<tr><td>Physical</td><td colspan="4"></td></tr>
</table>

梁如军（linuxbooks@126.com）

CIFS协议

- 通用网际文件系统（CIFS）是微软服务器消息块协议（SMB）的增强版本
- 提供计算机用户在企业内部网和因特网上共享文件的标准方法
- CIFS 在 TCP/IP 上运行，利用因特网上的全球域名服务系统（DNS）增强其可扩展性，同时为因特网上普遍存在的慢速拨号连接优化

CIFS的特点

- 文件访问的完整性
- 为慢速链接优化
- 为文件或目录的访问提供安全性
- 高性能和可扩展性
- 使用统一码（Unicode）文件名
- 使用全局文件名

梁如军（linuxbooks@126.com）

微软的SMB协议及其版本

Windows版本	支持的SMB协议版本
Windows 95/98/XP、Windows Server NT 4.0/2000/2003	SMB/CIFS
Windows Vista SP1、Windows Server 2008	SMB 2.0.2
Windows 7、Windows Server 2008 R2	SMB 2.1, SMB 2.0.2
Windows 8、Windows Server 2012	SMB 3.0, SMB 2.1, SMB 2.0.2
Windows 8.1、Windows Server 2012 R2	SMB 3.0.2, SMB 3.0, SMB 2.1, SMB 2.0.2
Windows 10、Windows Server 2016	SMB 3.1.1, SMB 3.0.2, SMB 3.0, SMB 2.1, SMB 2.0.2

- [MS-CIFS] —— https://msdn.microsoft.com/en-us/library/ee442092.aspx
- [MS-SMB] —— https://msdn.microsoft.com/en-us/library/cc246231.aspx
- [MS-SMB2] —— https://msdn.microsoft.com/en-us/library/cc246482.aspx

Samba简介

- Samba 是一组软件包，使 Linux 支持 SMB/CIFS 协议
- Samba 可以在几乎所有的 类UNIX平台 上运行
- Samba 最初于1991年由澳大利亚人 Andrew Tridgell 研发
- Samba 基于 GPL发行，如今由 Samba小组（http://www.samba.org）维护
- Samba 更新速度很快，当前的最新版本是3.3.8版

Samba的版本

版本	发布时间	说明
3.0	2003/09/23	提供文件和打印共享服务，并整合Windows NT 4.0的域，既可是主域控制器（PDC）也可是域成员。
3.6	2011/08/09	支持 SMB2协议
4.1	2013/10/10	支持 SMB3协议，可以作为活动目录域控制器（Active Directory domain controller）或其成员。
4.3	2015/09/08	支持 SMB3.1.1协议

梁如军（linuxbooks@126.com）

Samba的主要功能

- 使Linux主机成为Windows网络中的一份子，与Windows系统相互分享资源。
- 使Linux主机可以使用 Windows系统共享的文件和打印机。
- 使Linux主机成为文件服务器或打印服务器，为Linux/Windows客户端提供文件共享服务和远程打印服务。
- 使Linux主机担任Windows域控制器和Windows成员服务器，管理 NT/200X 网络。
- 使Linux主机担任WINS名字服务器，提供 NetBIOS 名字解析服务。
- 提供用户身份认证功能。
- 支持SSL安全套接层协议。

梁如军（linuxbooks@126.com）

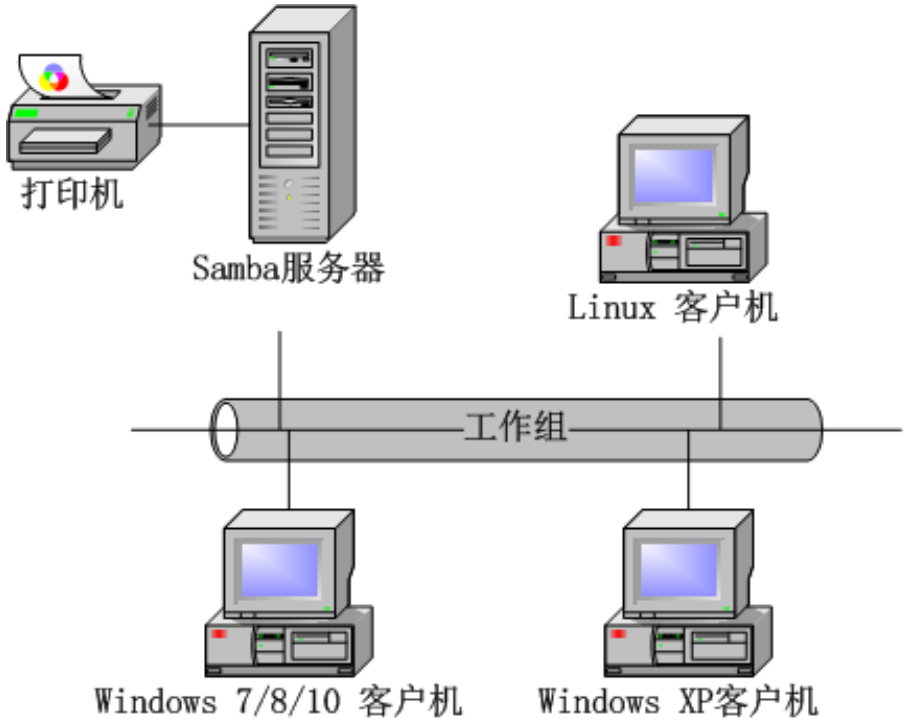
Samba 提供的服务

- Samba 提供了四种主要服务
  - 文件和打印机共享
  - 用户验证和授权
  - 名子解析
  - 浏览（服务通告）
- Samba 的守护进程
  - Smbd：实现共享和验证授权服务
  - Nmbd：实现名字解析和浏览服务

梁如军（linuxbooks@126.com）

Samba的应用

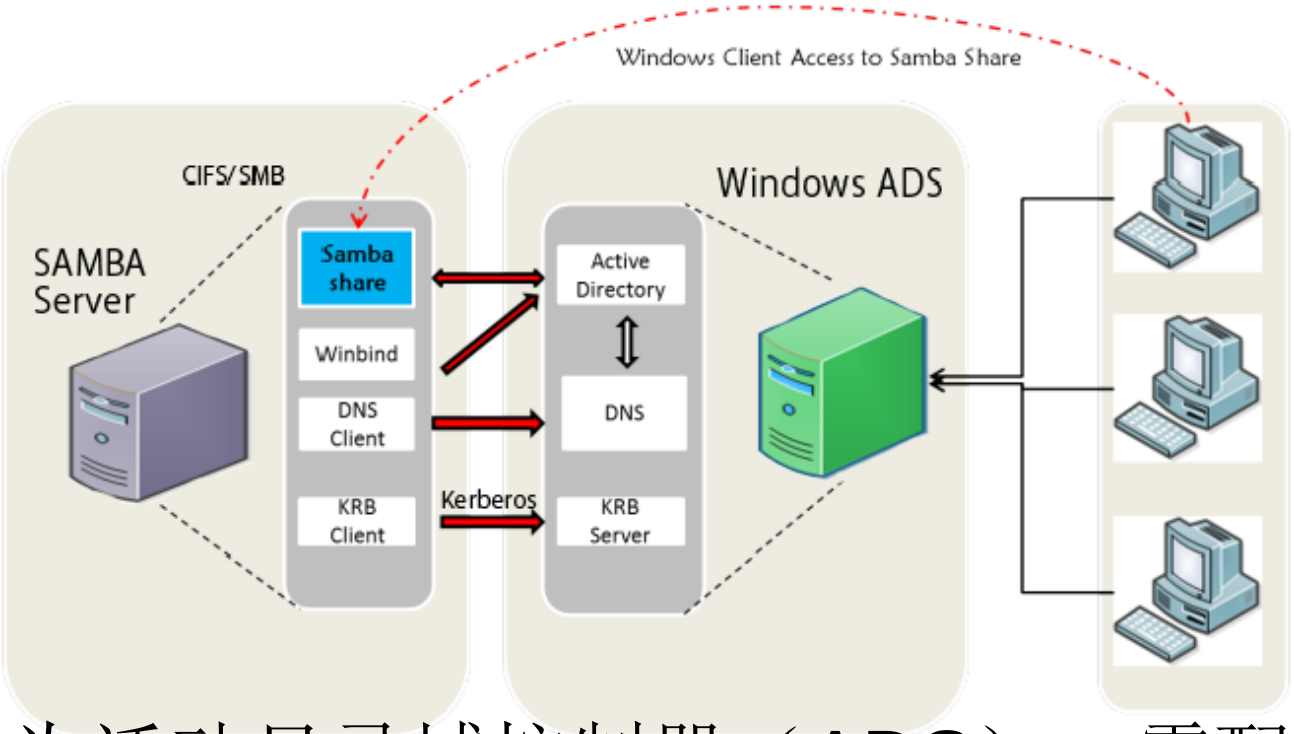
- 运行在Windows工作组网络并提供文件和打印共享服务。



梁如军（linuxbooks@126.com）

Samba的应用（续）

- 加入Windows活动目录并成为其成员。



- 作为活动目录域控制器（ADS），需配合Kerberos服务和LDAP服务。

梁如军（linuxbooks@126.com）

CentOS 7中的Samba

- CentOS 7中提供了Samba的RPM包
  - **samba-common**：包括Samba服务器和客户均需要的文件。
  - **samba**：Samba服务端软件。
  - **samba-winbind**：可选的winbind服务。
  - **samba-client**：Samba客户端软件。
  - **samba-swat**：Samba的Web配置工具。
- 安装
  - **# yum install samba**

梁如军（linuxbooks@126.com）

SMB服务概览

- 软件包：samba, samba-common
- 服务类型：由Systemd启动的守护进程
- 配置单元：
  - /usr/lib/systemd/system/{smb,nmb}d.service
- 守护进程：/usr/sbin/nmbd, /usr/sbin/smbd
- 监听端口：
  - [NetBIOS] **UDP:137**(-ns), **UDP:138**(-dgm), **TCP:139**(-ssn)
  - [SMB over TCP] **TCP:445**(-ds)
- 配置文件：/etc/samba/*
- 相关软件包：
  - samba-swat, samba-client , testparm，cifs-utils

梁如军（linuxbooks@126.com）

Samba的相关工具

- 服务器端工具
  - **/usr/bin/smbpasswd**：用于设置Samba用户账号及口令。
  - **/usr/bin/testparm**：用于检测配置文件的正确性。
  - **/usr/bin/smbstatus**：用于显示Samba的连接状态。
- 客户端工具
  - **/usr/bin/findsmb**：用于查找网络中的Samba服务器。
  - **/usr/bin/smbclient**：Linux下的Samba客户端。
  - **/usr/bin/smbget**：基于SMB/CIFS的类似于wget的下载工具。
  - **/usr/bin/smbtar**：类似于tar的归档工具，用于将SMB/CIFS的共享打包备份到Linux主机。

梁如军（linuxbooks@126.com）

Samba相关的配置文件

- **/etc/sysconfig/samba**：用于设置守护进程的启动参数。
- **/etc/samba/smb.conf**：主配置文件。
- **/etc/samba/smbusers**：用于映射Linux用户和Windows用户。
- **/etc/samba/lmhosts**：用于设置NetBIOS名字与IP地址的对应关系表。
- **/etc/pam.d/samba**：Samba的PAM配置文件。
- **/etc/rc.d/init.d/smb**：Samba的INIT启动脚本。

梁如军（linuxbooks@126.com）

CentOS 7中Samba —/etc/samba/smb.conf的默认配置

- 工作组：MYGROUP
- 安全等级：user
- 设置用户密码加密：Yes
- 口令数据库的后台：tdbsam（TDB数据库）
- 口令数据库：**/etc/samba/{passdb,secrets}.tdb**
- 认证用户时服从PAM的管理限制：Yes
- 设置了每个用户的主目录的共享
- 设置了全部打印机（/etc/cups/printers.conf中定义的）的共享

梁如军（linuxbooks@126.com）

Samba服务器角色

- standalone：独立服务器模式。
  - 用户验证由本机负责，登录用户的口令数据库存储在本机
- member server：成员服务器模式。
  - 用户验证由Windows或Samba域控制器负责
- domain controller：域控制器模式。
  - 本机为Windows和Samba客户提供登录验证服务

梁如军（linuxbooks@126.com）

Samba 的安全等级

- **User**：由本地Samba服务器负责账户验证
  - 使用smbpasswd 设置账号（默认的安全等级）
- **Domain**：账户验证账户及口令的工作由其他的Windows 或Samba域控制器负责
  - 需要使用“password server”指令指定验证服务器
- **Ads**：验证账户及口令的工作由支持Kerberos验证的Windows活动目录服务器负责。
  - 需要使用“realm”指令指定Kerberos领域

梁如军（linuxbooks@126.com）

SAMBA 账户及口令数据库

梁如军（linuxbooks@126.com）

Samba账户

- Samba使用的账户文件/数据库是与系统账户文件分离的。
- 当设置了user的安全等级后（此为默认设置），将由本地系统对访问Samba共享资源的用户进行认证。
- 用户认证需要Samba的口令文件，CentOS 7 默认使用.tdb格式的口令数据库，初始情况下口令数据库文件并不存在。
- 为了创建Samba的口令数据库文件，管理员可以在添加Samba账户的同时创建它。
- 管理员可以使用 **smbpasswd** 命令配置Samba账号并设置其口令。

梁如军（linuxbooks@126.com）

smbpasswd 命令

CentOS
The Community ENTerprise Operating System

smbpasswd [options] [username]

- username：为 username 设置Samba口令，仅超级用户可用。
- 选项 -a：添加Samba用户。
- 选项 -d：冻结Samba用户，就是这个用户不能在登录了。
- 选项 -e：解冻Samba用户，让冻结的用户可以再登录。
- 选项 -x：删除Samba用户。
- 选项 -s：非交互模式，从标准输入读取口令。
- 选项 -r MACHINE：指定远程Samba服务器的主机名或IP。
- 选项 -U USER：指定Samba用户名，省略时默认为当前登录用户。

梁如军（linuxbooks@126.com）

成批添加 samba 账户

```
#!/bin/bash
## filename: /root/bin/set-users-smb-init-passwd.sh
for username in $(awk -F ':'  '$3 >= 1000 {print $1}'  /etc/passwd) ;do
    (echo "centos"; echo "centos" ) | smbpasswd -s -a $username
done
```

- # chmod +x /root/bin/set-users-smb-init-passwd.sh
- # set-users-smb-init-passwd.sh

梁如军（linuxbooks@126.com）

smbpasswd 命令举例

CentOS
The Community ENTerprise Operating System

```
$ smbpasswd
$ smbpasswd -r 192.168.0.252 -U osmond

# smbpasswd -a jasonxie
# smbpasswd -x nfsnobody
# smbpasswd -a
```


梁如军（linuxbooks@126.com）

smbpasswd命令注意事项

- 使用smbpasswd命令添加Samba用户口令之前同名的系统用户账号必须已经存在。
- 同名的本地系统用户账号不存在时应使用useradd命令添加。
- 用户使用smbpasswd命令修改自己的口令时，smb服务必须已经启动。
- 可以使用pdbedit -Lv 命令查看Samba口令数据库的内容。

梁如军（linuxbooks@126.com）

CentOS
The Community ENTerprise Operating System

SAMBA 的测试和启动

梁如军（linuxbooks@126.com）

正确性检查和启动

- 使用testparm检查/etc/samba/smb.conf的语法

  # testparm

  # testparm --show-all-parameters

  # testparm -v

- 启动 Samba 服务

  # systemctl start smb nmb

  # systemctl enable smb nmb

- 查看Samba监听的端口

  # netstat -lunt|egrep '137|138|139|445'

梁如军（linuxbooks@126.com）

在Windows环境下访问Samba共享

- 使用网上邻居
- 通过映射网络驱动器
- 使用UNC路径
  - **\\192.168.0.252**
  - **\\centos1\osmond**
- 使用命令行（Windows的cmd窗口）
  - **C:\>net use Y: \\192.168.0.252\osmond**
  - **C:\>net use**
  - **C:\>net use Y: /delete**

梁如军（linuxbooks@126.com）

在Linux下访问Samba共享

- 检查Samba服务器所共享的资源
  - 使用匿名用户检查Samba服务器所共享的资源

$ smbclient -L //192.168.0.252

  - 使用Samba用户查看Samba服务器所共享的资源

$ smbclient -L //192.168.0.252 -U Osmond

- 列出Samba的资源使用情况
  - 查看详细的使用信息（包括进程、共享服务和锁文件等）

$ smbstatus

  - 查看简要的使用信息

$ smbstatus -b

梁如军（linuxbooks@126.com）

SAMBA 的主配置文件

梁如军（linuxbooks@126.com）

Samba 配置基础

- smb.conf 文件的分节结构
  - **[Global]**：用于定义全局参数和缺省值
  - **[Homes]**：用于定义用户的Home目录共享
  - **[Printers]**：用于定义打印机共享
  - **[Userdefined_ShareName]**：用户自定义共享（可有多个）

梁如军（linuxbooks@126.com）

Samba的全局参数（1）

- 基本全局参数
  - **netbios name**：设置Samba的NetBIOS名字
  - **workgroup**：设置Samba要加入的工作组
  - **server string**：指定浏览列表里的机器描述
  - **unix charset**：指定服务器使用的字符集
- 安全全局参数
  - **interfaces**：指定Samba监听的网络端口
  - **security**：定义Samba的安全级别
  - **passdb backend**：指定口令数据库的后台
  - **hosts allow**：指定可以访问Samba的主机列表
  - **hosts deny**：指定不可以访问Samba的主机列表

梁如军（linuxbooks@126.com）

Samba的全局参数（2）

- 日志全局参数
  - **log file**：指定日志文件的名称
  - **log level**：指定日志等级（0-10，数值越大越详细）
  - **max log size**：指定日志文件的最大尺寸（KB）
- 效率全局参数
  - **change notify timeout**：设置服务器周期性异常通知
  - **deadtime**：客户端无操作多少分钟后服务器端中断连接
  - **max connections**：设置同时访问Samba服务器及其共享资源的客户数量（0表示不限制）
  - **max open files**：同一个客户端最多能打开的文件数目
  - **socket options**：设置服务器和客户会话的Socket选项

梁如军（linuxbooks@126.com）

Samba的共享资源参数（1）

- 基本共享参数
  - **comment**：指定对共享的描述
  - **path**：指定共享服务的路径
- 文件系统控制参数
  - **dont descend**：指定内容不可见的子目录列表
  - **hide files**：指定含有特定关键字的文件的可见性
  - **veto files**：指定含有特定关键字的文件的可见性和可访问性
  - **hide dot files**：指定是否将Linux的隐藏文件对Windows也隐藏
  - **follow symlinks**：是否跟随符号链接

梁如军（linuxbooks@126.com）

Samba的共享资源参数（2）

- 访问控制参数
  - **available**：指定共享资源是否可用
  - **browseable**：指定共享的路径是否可浏览（默认为可以）
  - **read only**：指定共享的路径是否为只读
  - **writable**：指定共享的路径是否可写
  - **read list**：设置只读访问用户列表
  - **write list**：设置读写访问用户列表
  - **valid users**：指定允许使用服务的用户列表
  - **invalid users**：指定不允许使用服务的用户列表

梁如军（linuxbooks@126.com）

Samba的共享资源参数（3）

- 访问控制参数
  - **public**：指定是否可以允许guest账户访问
  - **guest ok**：指定是否可以允许guest账户访问
  - **guest only**：指定是否只允许guest账户访问
  - **guest account**：指定一般性客户的账号
  - **admin users**：为指定的共享设置管理员
  - **force user**：强制写入的文件具有指定的属主
  - **force group**：强制写入的文件具有指定的组
  - **hosts allow**：指定可以访问共享资源的主机列表
  - **hosts deny**：指定不可以访问共享资源的主机列表

SAMBA共享配置举例

梁如军（linuxbooks@126.com）

Samba 共享的基本配置

- 修改RHEL/CentOS 7默认的全局配置参数
- 使用符号链接组织本地共享资源
- 配置ftp用户的上传共享

参见教材的配置步骤

梁如军（linuxbooks@126.com）

文件系统权限和Samba共享权限

- Samba 服务器要将本地文件系统共享给 Samba 用户，涉及本机文件系统和 Samba 两种权限
- 本机文件系统权限
  - 使用**chmod**和**chown**命令设置
  - 使用**setfacl**命令设置FACL权限
- Samba 权限
  - 在主配置文件中使用Samba的**访问控制参数设置**
- **当Samba用户访问共享时，最终的权限将是这两种权限中最严格的权限（交集）。**

梁如军（linuxbooks@126.com）

为用户和组设置Samba 共享

- 为所有用户配置Samba的只读共享和读写共享
- 为指定用户配置Samba读写共享
  - 为指定的单个用户配置读写共享
  - 为指定的多个用户配置读写共享
- 为指定组配置读写共享
  - 组中的所有成员均具有读写权限
  - 组中仅一个成员具有读写权限，其他成员具有只读权限
  - 组中有部分成员具有读写权限，其他成员具有只读权限

参见教材的配置步骤

梁如军（linuxbooks@126.com）

Samba的其他配置

CentOS
The Community ENTerprise Operating System

- 配置 Windows 和 Linux 的用户映射
- 配置 Samba 的隐藏共享
- 限制文件共享类型
- 主机访问控制
- 用户访问控制
- 对不同主机或用户的访问实施不同的配置

参见教材的配置步骤

梁如军（linuxbooks@126.com）

CentOS
The Community ENTerprise Operating System

在LINUX环境下使用SAMBA共享

梁如军（linuxbooks@126.com）

smbclient

- Samba提供了一个类似FTP客户程序的Samba客户程序smbclient
- 可以使用smbclient查看并访问共享

smbclient //NetBIOS名或IP地址/共享名 -U 用户名

- **-U用户名**参数表示以指定用户的身份访问共享
  - 当访问Windows共享时，用户名是所访问的Windows计算机中的用户账户，验证口令是Windows计算机中的用户账户的口令
  - 当访问Linux提供的Samba共享时，用户名是所访问的Linux计算机中的Samba用户账户，验证口令是Samba用户账户的口令

挂装Samba共享

- 手动挂装 Windows/Samba 共享

```
# mkdir –p /mnt/smb/win01/tools
  /mnt/smb/centos1/public
# mount –t cifs //win01/tools
  /mnt/smb/win01/tools  -o user=osmond
# mount.cifs //192.168.0.252/pulic
  /mnt/smb/centos1/public  -o user=smbuser1
```

- 手动卸装 Windows/Samba 共享

```
# umount  /mnt/smb/win01/tools
# umount  /mnt/smb/centos1/public
```


梁如军（linuxbooks@126.com）

启动挂装Samba共享

- /etc/fstab

```
//win01/tools /mnt/smb/win01/tools  cifs
credentials=/etc/samba/cred1.txt  0  0
//192.168.0.252/pulic /mnt/smb/centos1/public cifs
credentials=/etc/samba/cred2.txt 0 0
```

```
# cat <<_END_> /etc/samba/cred1.txt
username=osmond
password=osmond-s-passwd
_END_
# cat <<_END_> /etc/samba/cred2.txt
username=smbuser1
password=smbuser1-s-passwd
_END_
# chmod 0600 /etc/samba/cred{1,2}.txt
```


梁如军（linuxbooks@126.com）

本章思考题

- 什么是SMB/CIFS？什么是Samba？
- Samba有几种认证方式？
- 如何设置Samba用户口令？
- 如何检验Samba配置文件参数的正确性？
- 如何在Linux下访问Windows的共享资源？

梁如军（linuxbooks@126.com）

本章实验

- 学会设置Samba用户口令。
- 学会配置Samba的各种文件共享。
- 学会使用smbclient命令访问Windows/Linux共享。
- 学会使用mount.cifs命令挂装远程CIFS文件系统。

进一步学习

- 学习Christopher R. Hertel所著的《Implementing CIFS: The Common Internet File System》（http://www.ubiqx.org/cifs/）。

- 学习 Timothy D Evans所著的《NetBIOS, NetBEUI, NBF, NBT, NBIPX, SMB, CIFS Networking》（http://timothydevans.me.uk/nbf2cifs/nbf2cifs.pdf）了解与SMB/CIFS相关的协议。

进一步学习

- 学习使用SWAT或Webmin等Web工具配置Samba。

- 学习配置Linux下的CUPS本地打印机。
- 学习配置Samba的打印共享。

- 学习将Samba 4服务器配置为Windows活动目录成员的方法。
- 学习将Samba 4服务器配置为活动目录域控制器的方法。

梁如军（linuxbooks@126.com）

进一步学习

- 学习NAS发行版的安装和使用
  - **FreeNAS** —— http://www.freenas.org
  - **Openfiler** —— http://www.openfiler.com
  - **Rockstor** —— http://rockstor.com
  - **OpenMediaVault** —— http://www.openmediavault.org

梁如军（linuxbooks@126.com）