

# Samba 大型文件服务器创建实例

深圳市靖邦科技 File Server 服务搭建记录

## 搭建 Samba 用途

满足公司计算机员工在使用过程中的重要资料备份和离职员工资料的归档。并顺便提供无纸化的工作内容汇报和出厂登记等。在100M 的全双工局域网中，将文件服务器映射为网络硬盘，可直接读取写入。减少数据丢失和数据安全烦恼。

## 创建目录列表

公共临时交换区	方便员工在传递文件资料时在双方计算机上插拔移动设备的麻烦。
部门公共文件	公司各部门对外公开的制度性或服务性文件
部门内部文件	公司部门内部重要文件资料的备份，或同部门资料的共享
每日工作内容登记	为计算机员工下班前 5 分钟将当日所做工作内容以 Excel 文件汇报。负责人可在此目录下随时查看。
办公时间出厂登记	为计算机员工在出厂时将出厂信息以 Excel 文件汇报。负责人可在此目录下随时查看。
离职员工资料归档	由负责人将离职员工使用的计算机资料上传至此处。方便业务手人随时查看。

## 权限大致规划

计算机员工每人分配帐号和密码，以部门为单位归属为同一用户组。	
公共临时交换区	每个用户均有权文件和目录。但创建完的文件和目录只允许该用户更改、删除，其它人只可读取。
部门公共文件	以每个部门为一目录。只能由部门的主管级别的用户在所属部门目录下创建、更改、删除文件和目录。所有用户均可读取任意部门目录下的任意文件，不能进行其它操作。
部门内部文件	以每个部门为一目录。只能由部门的主管级别的用户在所属部门目录下创建、更改、删除文件和目录。同一部门的用户只可读取自己部门下的任意文件，不能进行其它操作。对于其下以个人姓名命名的目录，只允许该姓名的用户进行一切操作。
每日工作内容登记	每个用户均可创建、修改、删除自己的文件，其它人无权读取其内容。但负责人用户可读取和删除文件。负责人可创建以当天日期为目录名的目录。
办公时间出厂登记	权限同“每日工作内容登记”类似
离职员工资料归档	只允许归档负责人创建、修改、删除文件。对于业务接手人用户，可查看某一特定员工的目录内容。

## 初步搭建方案

首先，修改 Samba 配置文件“/etc/samba/smb.conf”。主要配置内容为采用密码登陆方式，对共享目录进行允许读写的权限。

其次，创建本地网络登陆用户，并创建用户的 Samba 密码。

最后，在本地操作系统上根据权限内容，对文件和目录的权限属性进行细致地更改。

## 修改配置文件

打开配置文件命令：`sudo gedit /etc/samba/smb.conf`

注意：修改此文件前最好是备份一份，以免在以后配置彻底错误后提供初始示范样本。命令为：`sudo cp /etc/samba/smb.conf /etc/samba/smb.conf.back`

配置文件修改内容大致如下：

- 1、修改 `workgroup = XX` //Xx 为公司局域网统一工作组名
- 2、再添加三行以下代码，防止编码乱码问题：  
`display charset = UTF-8`  
`unix charset = UTF-8`  
`dos charset = cp950`
- 3、自定义 `server string = XX` //Xx 为网上邻居看到的计算机名
- 4、去掉 `wins support = no` 前的注释符号，使其生效
- 5、修改 `security = user` //user 表示不提供匿名用户登陆，访问需提供帐号密码
- 6、`map to guest = bad user` 前一定有注释符号，否则上面的第 5 步设置失效，即可以直接以匿名用户登陆
- 7、在“Share Definitions”创建需要共享的目录，如下示范：

[部门公共文件]

`comment = public`

`path = /home/szyzln/JBFileServer/部门公共文件/`

`writable = yes`

`public = yes`

`force use = szyzln` //无论是哪个帐户在此共享目录下创建文件或目录，被创建的文件和目录所属者和所属组均强制改变为 `szyzln` 和 `szyzln` 用户组。

`create mask = 0600` // 对应 -rw----- 文件权限

`directory mask = 0700` //对应 -rwx----- 目录权限

**技巧：**这里 0600 和 0700 与文件权限的对应关系

0600，第一个 0 可以忽略，似乎没有意义

第二个 6，转换为二进制为 110，表示该文件目录权限此处是 rw-

第三个 0 和第四个 0，转换为二进制为 000000，表示权限为-----

## 创建 Samba 用户和密码

这里不讨论创建虚拟用户,而是实实在在的系统用户。只不过这些用户不允许在本地系统上登陆,只可以在本机提供的服务里登陆。密码也并非系统用户的登陆密码。因为这些用户一开始就被设置为不允许本地登录,所以没必要设置它的系统密码。这里的密码只是指登陆 Samba 服务时所用的密码,被称为 Samba 密码。

### 1、创建用户组(以公司部门名为准)

示范命令: `sudo groupadd WL` //这里用户组为大写字母, WL 表示公司的网络部

其它命令: `groupdel` `groupmod`

### 2、创建用户(以公司计算机用户名为准)

示范命令: `sudo useradd -g WLXX -s /bin/false`

参数说明: -g 表示初始用户组 -s 表示使用的 base 权限,这里为禁止本地登录

其它命令: `userdel` `usermod`

### 3、设置 Samba 密码

示范命令: `smbpasswd XX` //XX 为帐号

参数说明: -d 表示暂时禁用帐号 -e 表示启动帐号

## 修改本地权限

前面的配置文件已经将共享目录配置为可以读写执行。但是具体该共享目录允许哪些用户读写执行,是需要以本地系统中的文件权限为基准的。下面举一个实例。以上面的配置文件中配置的共享目录“部门公共文件”为例。

在 Samba 配置文件里,这个共享目录已经被配置为“writable = yes”可写。我们再在本地系统上使用“ls -l”看一下这个目录的具体系统权限是什么。结果如下:

```
drwxr-xr-x 12 szyzln szyzln 4096 2009-08-28 16:25 部门公共文件
```

我们看到,这个目录的所有者和所属组均是 szyzln。对所有者的权限为 rwx,对所属组的权限为 r-x,对其它用户和其它组的权限为 r-x。

那么,如果我们通过网上邻居,不是以 szyzln 用户登陆的话,对这个共享出来的目录就只有 r-x 权限,即可读可执行,不可写。

**说明:** 文件的读权限和目录的读权限的区别。

如果对于一个文件,我们设置为 r,那么这个目录就可以被读出来。

如果对于一个目录,我们也只设置为 r,则这个目录下的文件或者二级目录是无法打开的。

比如我们将上面的“部公共文件”权限修改为以下:

```
drwxr-xr-- 12 szyzln szyzln 4096 2009-08-28 16:25 部门公共文件
```

那么,当我们以非 szyzln 帐户登陆后,双击该共享目录是无法进入的。原因就是进入该目录,实际上要执行一个“cd 部门公共文件”命令。所以,我们还设置加上一个 X 权限,即执行权限。

继续以上面的“部门公共文件”为例进行本地权限修改的说明。我们看一下这个共享目录下一级目录的本地权限。如下:

```
drwxr-xr-x 3 ch GC 4096 2009-08-28 16:11 PCB 工程部
```

```
drwxr-xr-x 2 zyq CW 4096 2009-08-14 13:22 财务部
```

```
drwxr-xr-x 2 wm CG 4096 2009-08-17 19:21 采购部
```

```
drwxr-xr-x 2 zx1 GJYW 4096 2009-08-17 19:28 国际业务部
```

```
drwxr-xr-x 2 gjj GNYW 4096 2009-08-17 19:24 国内业务部
```

```
drwxr-xr-x 2 hcp HC    4096 2009-08-14 13:23 货仓部
drwxr-xr-x 2 lff RS    4096 2009-08-14 13:22 人力资源部
drwxr-xr-x 2 cj  SC    4096 2009-08-17 16:12 生产部
drwxr-xr-x 6 ln  WL    4096 2009-09-02 10:47 网络技术部
drwxr-xr-x 2 yy  ZJB   4096 2009-08-17 19:48 总经理办公室
```

我们按照刚才的权限说明，就可以看出。上面的设置已经完全符合我们当初规划的“部门公共文件由部门管理级别的帐户来创建、修改、删除文件和目录，其它任何帐户只能读取文件内容”的目的。

同时，我们还需要考虑到一个问题。那就是：上面的这些目录以及目录的权限都是我们事先设置好的。如果在 Samba 使用过程中，某个部门主管帐户真的在它的部门目录下创建了一个文件或目录，那么这个后来创建的文件或目录权限是多少呢？这就要看这个该共享目录在 Samba 配置文件里的参数值。比如此处的实例，在配置参数中有两处，分别为“create mask = 0600”和“directory mask = 0700”。我们看懂了这个 0600 和 0700 所对应的权限，就会知道接下来发生的后果现象就是：部门主管在这个“部门公共文件目录”下的自己部门下创建的文件和目录都不会被其它用户读取到。

## 最后扩展

如果我们在 Samba 共享目录里没有加上“force use = szylzn”这个参数，表示是哪个 Samba 帐户创建的文件或目录，那么这个文件或目录的所有者和所属组就是这个帐号和这个帐号的所属组。下面我们假设这样一个规划：

某个目录，和这个目录下的所有文件(包括后来创建的二级 N 级文件和目录)，为某个部门主管级别帐户所创建。这个目录下的所有文件主要是用来让公司领导查看的，其它 Samba 用户均无法访问。

我们需要这样做：

第一：这个目录及其下的所有文件，权限全部设置为“-rwx--r-x”。

第二：在 Samba 配置文件中在该共享目录中再加上“valid users = XX,XXX,XXXX”。

上面的作法就是：先让这个目录和其下的所有文件对所有者(即创建者)有读写执行的权限，对其它用户和用户组有读执行的权限。然后再加上一个“valid users”，表示只允许指定的帐号登陆。这样就完全把除创建者和指定外的帐号全部排除在外。

说明：public 和 valid users

在 Samba 配置文件中的共享目录参数中，这两个参数最好只选择其中一个。我个人比较讨厌简单的问题复杂化。“Public”表示这个共享目录能所有能成功登陆 Samba 帐号都可见。

而“valid users”则只对指定的 Samba 帐号可见，包括它的创建者。

我想，这种共享目录特殊权限的帐号添加应该不多吧，建议也不要过多。

## 最后说明

本实例说明教程不包括“创建虚拟用户”、“挂载其它格式的共享目录”等。