# 项目十 Samba服务部署

在Linux系统中想要实现文件共享比较简单的方式就是通过Samba服务。Samba可以让Windows系统的用户访问Linux系统的共享文件。通过本项目的学习了解Samba服务的基本原理，学会Samba的安装与配置，学会配置Samba服务的用户认证。

从本项目可以学习到：

* Samba服务的基本原理
* Samba服务的安装与配置
* Samba服务的基本指令
* 配置基于用户的Samba服务

本项目建议课时：6课时。

## 10.1 SMB服务概述

SMB（Server Messages Block，信息服务块）是一种在局域网上共享文件和打印机的通信协议。它为局域网内的不同操作系统的计算机之间提供文件及打印机等资源的共享服务。

SMB 协议是客户机/服务器型协议，客户机通过该协议可以访问服务器上的共享文件系统、打印机及其他资源。

#### 10.1.1 CIFS协议概述

随着 Internet 的流行，Microsoft 希望将SMB这个协议扩展到Internet上，成为Internet 上计算机之间相互共享数据的一种标准。因此它将原有的的SMB协议进行整理，重新命名为CIFS （Common Internet File System）。

CIFS协议使程序可以访问远程 Internet 计算机上的文件并要求此计算机提供服务。客户程序请求远在服务器上的服务器程序为它提供服务。服务器获得请求并返回响应。

CIFS 是公共的或开放的 SMB 协议版本，并由 Microsoft 使用。SMB 协议在局域网上用于服务器文件访问和打印的协议。

## 10.1.2 FTP服务与SMB服务的对比

1.FTP服务的优缺点

* 优点：文件传输、应用层协议、可跨平台。
* 缺点：只能实现文件传输，无法实现文件系统挂载；无法直接修改服务器端文件。

2.SMB服务的特性

* 使用cifs 协议、可跨平台、可实现文件系统挂载、可实现服务器端修改文件。

## 10.2 Samba服务的安装与配置

Samba服务是在Linux和Unix系统上实现SMB协议的一个免费软件由服务器及客户端程序构成。

Samba服务是在网络中实现文件共享的一种实现方式，Samba服务能够在任何支持SMB协议的主机之间共享文件的一种实现。

本节将主要介绍Samba服务的安装与配置。

#### 10.2.1 Samba相关进程

1.smbd

* 进程作用：smbd进程的作用是处理到来的SMB数据包，为使用该数据包的资源与Unix 进行协商
* 进程端口：smbd监听TCP的139号端口

2.nmbd

* 进程作用：nmbd进程使其他主机(或工作站)能浏览Unix/Linux的Samba服务器
* 进程端口：nmbd监听UDP的137和138号端口

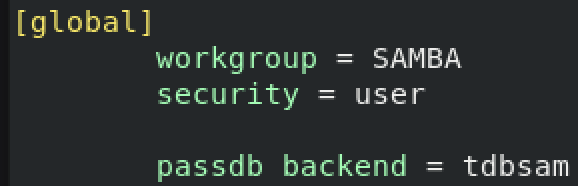
#### 10.2.2 Samba服务的配置文件说明

表10.2.1列出了Samba服务相关的目录和配置文件：

表10.2.1

|  |  |
| --- | --- |
| **配置文件的名称** | **存放位置** |
| 主配置文件路径 | /etc/Samba |
| 主配置文件 | /etc/Samba/smb.conf |

Samba中的所有配置文件区分大小写，在文件中以“＃”开始的行为注释行。指令的语法为“配置参数名称=参数值”。如图10.2.2列出了部分配置文件内容。



**配置文件参数**

图10.2.2

表10.2.3列出了/etc/Samba/smb.conf主配置文件中[global]全局配置的

一些主要参数的功能。

表10.2.3

|  |  |
| --- | --- |
| **参数** | **作用** |
| workgroup = name | 工作组名称 |
| netbios name = name | 主机名称 |
| serverstring = Samba server | 说明性文字，内容无关紧要 |
| log file = /var/log/log.%m | 日志文件的存储文件名，%m代表的是client端Internet主机名，就是hostname |
| max log size = 100 | 日志文件最大的大小为100Kb |
| security = share | 表示不需要密码，可设置的值为share、user和server |
| passdb backend = tdbsam | Samba用户认证方式，可设置值为smbpasswd、tdbsam和ldapsam |
| load printer = no | 不加载打印机 |

Samba服务有三种访问模式，可以通过[global]全局配置中的“security”参数进行配置：

* share：用户访问Samba不需要提供用户名和口令，安全性低
* user：本地用户验证Samba服务器默认的安全级别，用户在访问共享资源之前必须提供用户名和密码进行验
* domian：域安全级别认证，使用域控制器来完成验证

Samba服务中的用户认证方式有三种，可以通过[global]全局配置中的“passdb backend”参数进行配置：

* smbpasswd：使用SMB服务的smbpasswd命令为系统用户设置密码；客户端使用此密码来访问Samba的资源smbpasswd文件默认保存在/etc/Samba目录下，如果不存在需要手动创建
* tdbsam：使用数据库来建立用户权限，默认保存在/etc/Samba/passdb.tdb文件中，使用命令smbpasswd -a来建立Samba账户，也可以使用pdbedit来建立Samba账户:
* 新建用户：pdbedit username
* 删除用户：pdbedit -x username
* ldapsam：基于LDAP服务进行帐户验证。

表10.2.4列出了/etc/Samba/smb.conf主配置文件中[Share]共享资源的一些主要参数的功能。

表10.2.4

|  |  |
| --- | --- |
| **参数** | **作用** |
| [Share] | 共享资源名称 |
| comment = smb warehouse | 共享资源名称注释 |
| path = /tmp | 实际的共享目录 |
| writable = yes | 设置为可写入 |
| browseable = yes | 可以被所有用户浏览 |
| guest ok = yes | 可以让用户随意登录 |
| valid users = 用户名 | 设置访问用户 |
| valid users = @组名 | 设置访问组 |
| readonly = yes | 只读 |
| readonly = no | 读写 |
| hosts deny = 192.168.0.0 | 表示禁止所有来自192.168.0.0/24 网段的IP 地址访问 |
| hosts allow = 192.168.0.24 | 表示允许192.168.0.24 这个IP 地址访问 |
| public = yes | 允许匿名访问 |

#### 10.2.3 安装Samba服务

使用YUM应用程序管理器安装Samba服务。首先利用Centos8安装光盘搭建本地YUM仓库。下面开始安装Samba服务。

查询系统是否已经安装了Samba服务。输入命令后没有任何输出表示没有安装。

rpm -qa | grep Samba

安装Samba服务

yum install -y Samba

使用命令“rpm -qa | grep Samba”检查Samba安装是否成功，如图10.2.5所示。

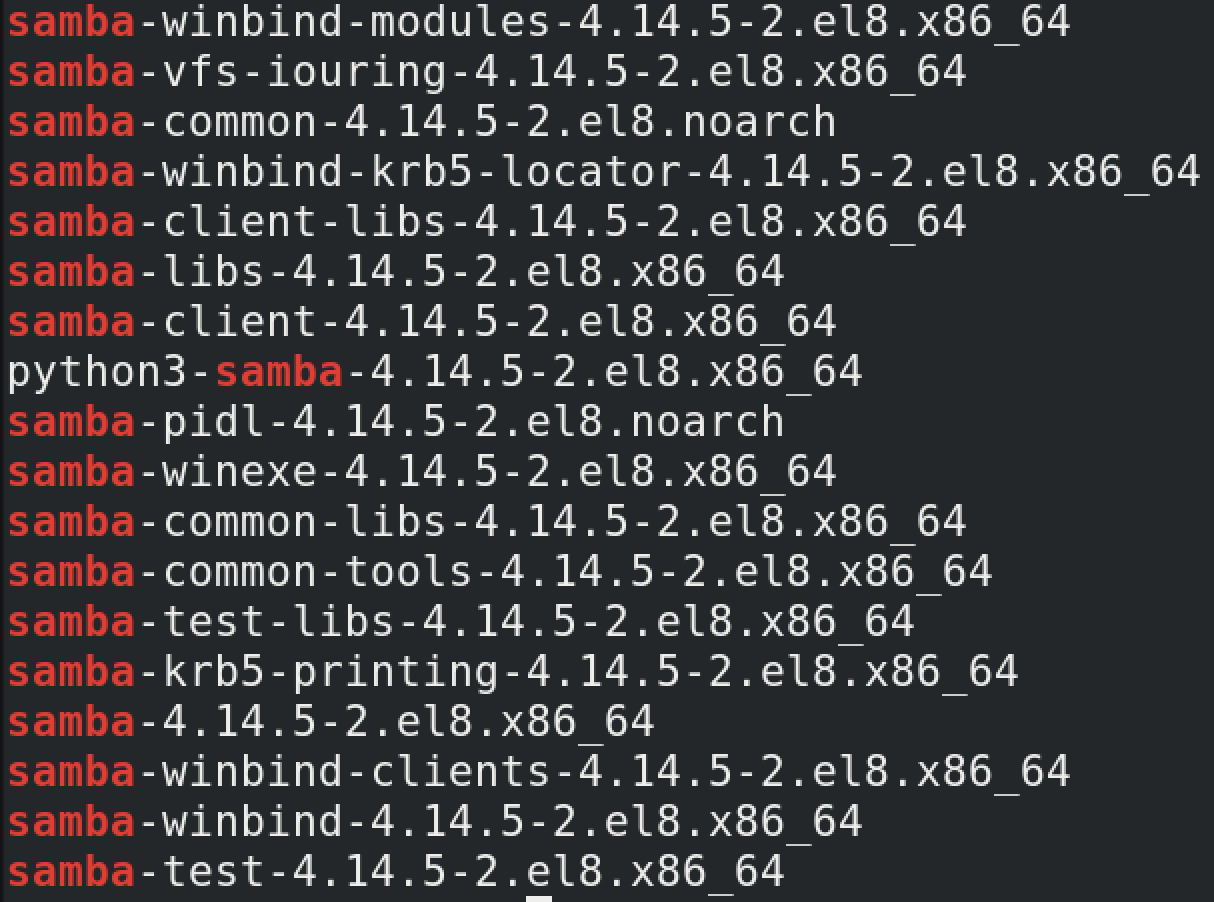


图10.2.5

启动Samba服务

systemctl start smb

设置Samba服务为开机自动启动

systemctl enable smb

添加防火墙条目放行Samba服务

firewall-cmd --add-port=139/tcp --permanent

firewall-cmd --add-port=445/tcp --permanent

firewall-cmd --add-port=137/tcp --permanent

firewall-cmd --add-port=138/tcp --permanent

重启防火墙生效步骤添加的条目

firewall-cmd --reload

使用如下命令临时关闭Selinux

setenforce 0

#### 10.2.4 配置简单的Samba服务

1.实例说明

创建匿名Samba共享资源，资源名为public。所有用户都可以对共享资源进行读写。

开始配置之前需要预先配置好Linux虚拟机的IP地址，安装好Samba服务并在防火墙放行相应服务和关闭Selinux。

2.实验环境

表10.2.6列出了实验需要用到的虚拟机

表10.2.6

|  |  |  |
| --- | --- | --- |
| **角色** | **操作系统** | **IP地址** |
| Samba服务器 | Centos8.3 | 192.168.107.165 |
| 访问客户端 | Centos8.3 | 192.168.107.166 |

3.具体步骤

在Samba服务器的/opt目录下创建abc目录，配置目录权限并在目录下创建testfile目录作为测试文件。将这个目录作为Samba服务匿名共享目录。操作如图10.2.7所示。

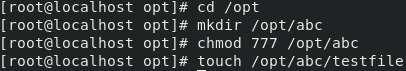
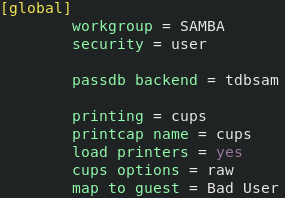


图10.2.7

编辑Samba服务主配置文件/etc/Samba/smb.conf，在[global]全局配置中添加开启匿名参数。操作如图10.2.8所示。



**添加“map to guest”参数开启匿名访问**

】

图10.2.8

编辑Samba服务主配置文件/etc/Samba/smb.conf，添加一个名为[public]的匿名共享资源。操作如图10.2.9所示。

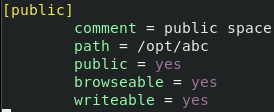


图10.2.9

表10.2.10列出了[public]的匿名共享资源配置的含义。

表10.2.10

|  |  |
| --- | --- |
| **参数** | **作用** |
| [public] | 共享资源名称 |
| comment = ... | 对资源文件的说明 |
| path = /opt/abc | 指定资源的物理路径 |
| public = yes | 开启共享 |
| browseable = yes | 开启目录访问 |
| writeable = yes | 允许目录写入功能 |

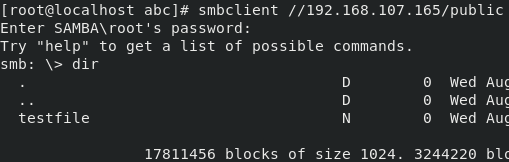
配置完成后使用如下命令重启Samba服务。

systemctl restart smb

在客户机上安装使用下面的命令安装Samba服务的登陆客户端。

yum install Samba-client

在客户机上使用smbclient命令登陆Samba服务器。操作如图10.2.11所示。



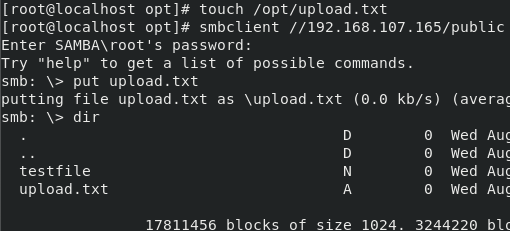
**使用dir命令查看当前目录下的文件**

**“//”参数表示Samba服务器的IP地址以及共享资源名称**

图10.2.11

匿名用户登陆不需要密码，在提示要密码的时直接按下”回车键”即可跳过。

在客户机的/opt目录下创建文件upload.txt文件。将文件上传到Samba服务器中。操作如图10.2.12所示。

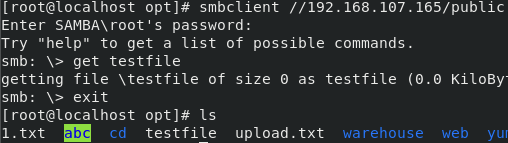


**使用put命令上传upload.txt文件**

**upload.txt文件上传成功**

图10.2.12

将Samba服务器上的“testfile”文件下载到客户机的“/opt”目录下。操作如图10.2.13所示。



**testfile文件下载成功**

**使用get命令下载testfile文件**

=；；

图10.2.13

## 10.3 Samba共享服务身份验证

本节主要介绍Samba共享服务身份验证的配置。

#### 10.3.1 配置Samba共享服务身份验证

1.实例说明

某公司需要创建一个公共存储空间名称为share，要求如下：

1. 存储路径为/opt/abc。
2. 要求公司员工都能对存储空间进行读写。
3. 公司员工在存储空间中新建的文件权限为644，新建的目录权限为755。
4. 创建smbclient公司员工帐户进行测试访问。

2.实验环境

表10.3.1列出了实验需要用到的虚拟机

表10.3.1

|  |  |  |
| --- | --- | --- |
| **角色** | **操作系统** | **IP地址** |
| Samba服务器 | Centos8.3 | 192.168.107.165 |
| 访问客户端 | Centos8.3 | 192.168.107.166 |

3.具体步骤

在Samba服务器的/opt目录下创建abc目录，配置目录权限并在目录下创建testfile目录作为测试文件。将这个目录作为Samba服务匿名共享目录。操作如图10.3.2所示。

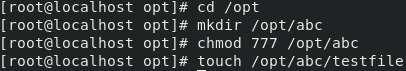


图10.3.2

编辑Samba服务主配置文件/etc/Samba/smb.conf，添加一个名为[share]的共享资源。操作如图10.3.3所示。

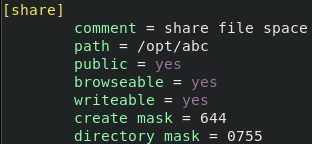


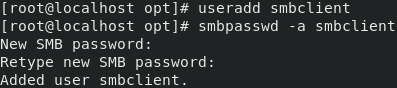
图10.3.3

表10.3.4列出了[share]的匿名共享资源配置的含义。

表10.3.4

|  |  |
| --- | --- |
| **参数** | **作用** |
| [share] | 共享资源名称 |
| comment = ... | 对资源文件的说明 |
| path = /opt/abc | 指定资源的物理路径 |
| public = yes | 开启共享 |
| browseable = yes | 开启目录访问 |
| writeable = yes | 允许目录写入功能 |
| create mask = 0644 | smb用户新建文件权限都是644 |
| directory mask = 0755 | smb用户新建子目录权限为755 |

创建Samba用户smbclient，密码和用户名相同。操作如图10.3.5所示。



**使用smbpasswd命令创建Samba用户**

】

图10.3.5

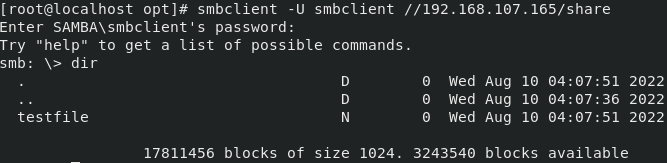
配置完成后使用如下命令重启Samba服务。

systemctl restart smb

在客户机上安装使用下面的命令安装Samba服务的登陆客户端。

yum install Samba-client

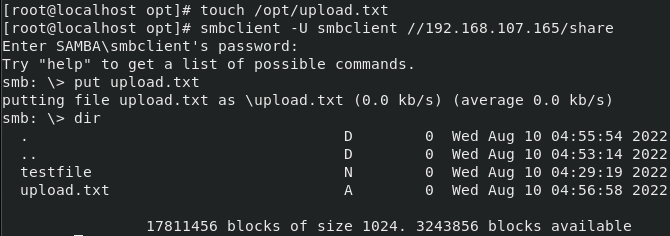
在客户机上使用smbclient命令登陆Samba服务器。操作如图10.3.6所示。



**“-U”参数表示要登陆的用户名**

图10.3.6

在客户机的/opt目录下创建文件upload.txt文件。将文件上传到Samba服务器中。操作如图10.3.7所示。

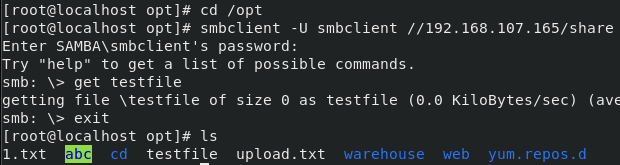


**上传upload.txt文件**

**upload.txt文件上传成功**

图10.3.7

将Samba服务器上的testfile文件下载到客户机的/opt目录下。操作如图10.3.8所示。



**testfile文件下载成功**

**下载testfile文件**

图10.3.8

#### 10.3.2 配置Samba服务实例

1.实例说明

配置一台Samba服务器要求如下：

1. 用户身份模式为user,采用tdbsam验证机制。
2. 创建三个账号作为Samba登陆帐户：user1、user2、user3,密码和用户名相同。

3） 建立Samba共享目录/opt/sharesmb，共享名为smbdir。

4） 要求user1、user2和user3用户都具有上传权限。

5） user1用户能下载和删除所有用户的文件，user2和user3用户能下载所有用户文件但不能删除其他用户文件。

2.实验环境

表10.3.9列出了实验需要用到的虚拟机

表10.3.9

|  |  |  |
| --- | --- | --- |
| **角色** | **操作系统** | **IP地址** |
| Samba服务器 | Centos8.3 | 192.168.107.165 |
| 访问客户端 | Centos8.3 | 192.168.107.166 |

3.具体步骤

在/opt目录下创建sharesmb目录，并配置权限。操作如图10.3.10。

Screenshot 2022-08-10 at 15.10.45

图10.3.10

实例说明中要求user2和user3用户不能删除其他用户创建的文件。这就涉及到了父目录的写权限问题，但是在配置时不能直接关闭父目录的写权限，这会导致不能向父目录上传文件。

解决的方法是在创建父目录时为父目录设置t标识位。这样用户就不能删除父目录下不属于自己的文件了,图10.3.10中的“-m”参数就是用来设置t标记位的。

通过下面的命令，修改sharesmb目录的的所有者为user1用户，满足user1用户能上传和删除的权限。

chwon user1:user1 /opt/sharesmb

创建user1,user2,user3用户，使用“smbpasswd -a”指令将所有用户都转换为Samba用户。操作如图10.3.11所示。

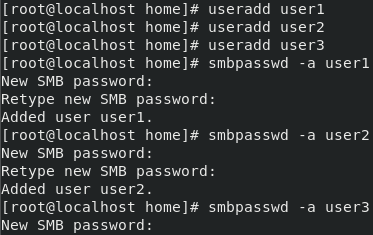


图10.3.11

编辑Samba服务主配置文件/etc/Samba/smb.conf，添加一个名为[smbdir]的共享资源。操作如图10.3.12所示。

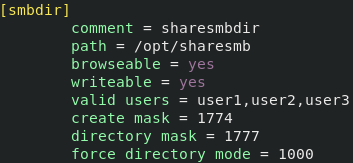


图10.3.12

表10.3.13列出了[smbdir]共享资源配置的含义。

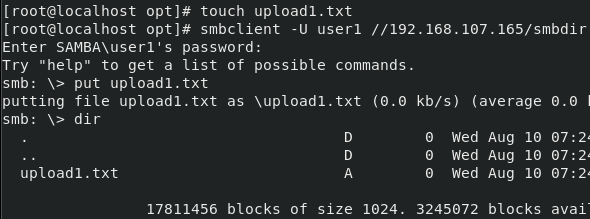
表10.3.13

|  |  |
| --- | --- |
| **参数** | **作用** |
| [smbdir] | 共享资源名称 |
| comment = ... | 对资源文件的说明 |
| path = /opt/abc | 指定资源的物理路径 |
| browseable = yes | 开启目录访问 |
| writeable = yes | 允许目录写入功能 |
| create mask = 1774 | 配置新建或者上传的文件没有写权限 |
| directory mask = 1777 | 配置新建或者上传的目录具有所有的权限 |
| valid users = user1,user2,user3 | 允许user1、user2和user3用户访问该共享资源 |
| force directory mode = 1000 | 为父目录设置标识位 |

配置完成后使用如下命令重启Samba服务。

systemctl restart smb

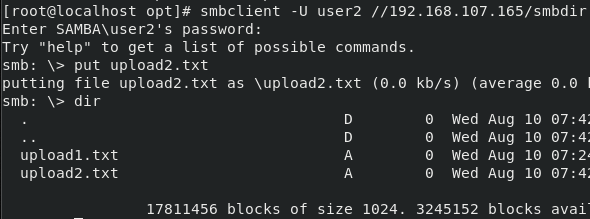
在客户端机的/opt目录下新建文件upload1.txt文件并使用smbclient命令登陆Samba服务器，测试user1用户上传权限。操作如图10.3.14所示。



**user1用户上传upload1.txt文件成功**

图10.3.14

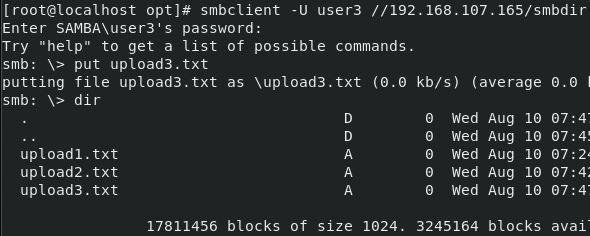
在客户端的/opt目录下新建文件upload2.txt文件并使用smbclient命令登陆Samba服务器，测试user2用户上传权限。操作如图10.3.15所示。



**user2用户上传upload2.txt文件成功**

图10.3.15

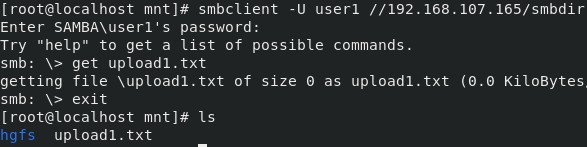
在客户端的/opt目录下新建文件upload3.txt文件并使用smbclient命令登陆Samba服务器，测试user3用户上传权限。操作如图10.3.16所示。



**user3用户上传upload3.txt文件成功**

图10.3.16

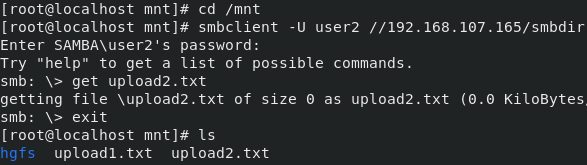
在客户端使用smbclient命令登陆Samba服务器，测试user1用户下载权限。将步骤上传的upload1.txt文件下载到客户机的/mnt目录下。操作如图10.3.17所示。



**user1用户下载upload1.txt文件成功**

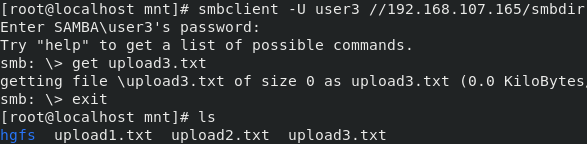
图10.3.17

在客户端使用smbclient命令登陆Samba服务器，测试user2用户下载权限。将步骤上传的upload2.txt文件下载到客户机的/mnt目录下。操作如图10.3.18所示。

图10.3.18

**user2用户下载upload2.txt文件成功**

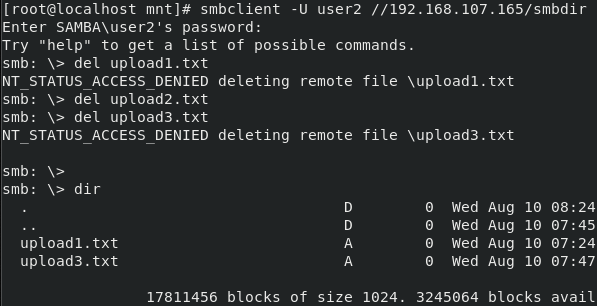
在客户端使用smbclient命令登陆Samba服务器，测试user3用户下载权限。将步骤上传的upload3.txt文件下载到客户机的/mnt目录下。操作如图10.3.19所示。



**user3用户下载upload3.txt文件成功**

图10.3.19

在客户端使用smbclient命令登陆Samba服务器，测试user2用户的删除权限。删除上面实验中上传的文件验证效果。操作如图10.3.20所示。

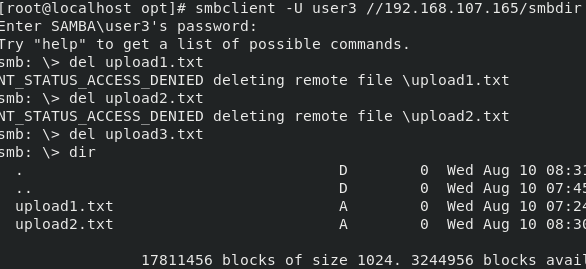


**user2用户可以删除自己上传的文件但不能删除user1和user3用户上传的文件user2用户权限正确**

**使用del命令分别删除3个已经上传的文件**

图10.3.20

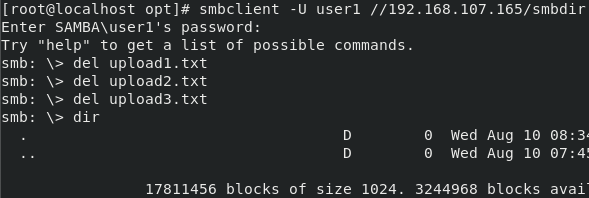
在客户端使用smbclient命令登陆Samba服务器，测试user3用户的删除权限。删除上面实验中上传的文件验证效果。操作如图10.3.21所示。



**user3用户可以删除自己上传的文件但不能删除user1和user2用户上传的文件user2用户权限正确**

图10.3.21

在客户端使用smbclient命令登陆Samba服务器，测试user1用户的删除权限。删除上面实验中上传的文件验证效果。操作如图10.3.22所示。



**user1可以删除所有用户上传的文件。**

图10.3.22

#### 章节测试

1.操作题

1）某比赛组委会需要需搭建一台Samba服务器，具体要求如下：

（1）Samba服务器中有六个用户，分别是竞赛秘书：jnjsms，企业网项目负责人：jnqyw，园区网项目负责人：jnyqw，江苏代表队联系人：jnjs，上海代表队联系人：jnsh，浙江代表队联系人：jnzj。

（2）所有用户的统一登目录是linuxjn目录，下设：竞赛组委会、新闻发布、公共文档、参赛代表队、上传可写等七个目录。

（3）其中竞赛组委会目录下设三个子目录，分别是竞赛秘书处、企业网项目和园区网项目，对应的目录提供给竞赛秘书jnjsms、企业网项目负责人jnqyw和园区网项目负责人jnyqw私人所有，其他用户不得查看和修改。

（4）新闻发布目录供竞赛秘书和项目负责人向参赛代表队联系人发布自己职权范围内的新闻和通知，供参赛单位查看。

（5）公共文档目录供竞赛秘书和项目负责人向参赛单位提供政策性文件、指导纲要、竞赛大纲、评分细则、竞赛政策解读等文件，仅供参赛单位下载。

（6）参赛单位目录下设三个子目录，分别是江苏代表队、上海代表队、浙江代表队，目录提供给相应联系人私人所有，其他用户不得查看；

（7）上传可写目录供各代表队联系人向竞赛组委会提交参赛选手资料，各代表队负责本队选手资料的维护，不得删除友队的选手资料，竞赛组委会秘书和项目负责人可复制选手的资料。