

# 项目10 配置与管理samba服务器

---

深圳职业技术大学  
人工智能学院  
孔畅

# 学习目标

LEARNING OBJECTIVES

掌握samba的工作原理

掌握主配置文件samba.conf的配置方法

掌握samba服务密码文件的配置方法

掌握samba文件和打印共享的设置方法

# 学习内容

LEARNING CONTENTS

- **项目知识准备**

- **项目设计与准备**

- **项目实施**

- **项目实录：配置与管理Samba服务器**

## 了解samba应用环境

- 文件和打印机共享：文件和打印机共享是samba的主要功能，通过SMB进程实现资源共享，将文件和打印机发布到网络之中，以供用户访问。
- 身份验证和权限设置：smbd服务支持user mode和domain mode等身份验证和权限设置模式，通过加密方式可以保护共享的文件和打印机。
- 名称解析：samba通过nmbd服务可以搭建NBNS（NetBIOS Name Service）服务器，提供名称解析，将计算机的NetBIOS名解析为IP地址。
- 浏览服务：局域网中，samba服务器可以成为本地主浏览服务器（LMB），保存可用资源列表，当使用客户端访问Windows网上邻居时，会提供浏览列表，显示共享目录、打印机等资源。



## 了解SMB协议

---

SMB (Server Message Block) 通信协议可以看作是局域网上共享文件和打印机的一种协议。

samba则是将SMB协议搬到UNIX系统上来使用，通过“NetBIOS over TCP/IP”，使用samba不但能与局域网络主机共享资源，而且能与全世界的计算机共享资源。



# 学习内容

LEARNING CONTENTS

- 项目知识准备

- 项目设计与准备

- 项目实施

- 项目实录：配置与管理Samba服务器

## 了解samba服务器配置的工作流程

---

- 1.基本的samba服务器的搭建流程主要分为5个步骤。
  - (1) 编辑主配置文件smb.conf，指定需要共享的目录，并为共享目录设置共享权限。
  - (2) 在smb.conf文件中指定日志文件名称和存放路径。
  - (3) 设置共享目录的本地系统权限。
  - (4) 重新加载配置文件或重新启动SMB服务，使配置生效。
  - (5) 关闭防火墙，同时设置SELinux为允许。

## 了解samba服务器配置的工作流程

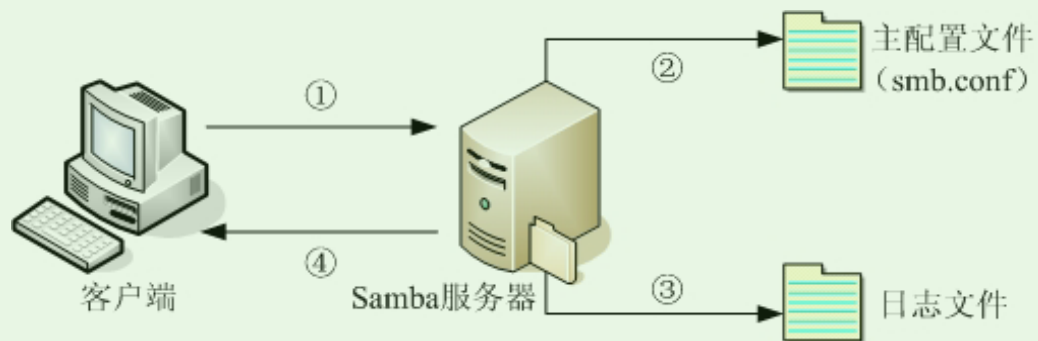
2. samba的工作流程如图所示。

(1) 客户端请求访问samba服务器上的共享目录。

(2) samba服务器接收到请求后，会查询主配置文件smb.conf，看是否共享了目录，如果共享了目录则查看客户端是否有权限访问。

(3) samba服务器会将本次访问信息记录在日志文件之中，日志文件的名称和路径都需要我们设置。

(4) 如果客户端满足访问权限设置，则允许客户端进行访问。





## 设备准备

本项目要用到Server01、Client2和Client1，设备情况如表所示:

主机名称	操作系统	IP地址	网络连接方式
samba共享服务器: Server01	RHEL 8	192.168.10.1/24	VMnet1 (仅主机模式)
Windows客户端: Client2	Windows 10	192.168.10.31/24	VMnet1 (仅主机模式)
Linux客户端: Client1	RHEL 8	192.168.10.21/24	VMnet1 (仅主机模式)

# 学习内容

LEARNING CONTENTS

- 项目知识准备

- 项目设计与准备

- 项目实施

- 项目实录：配置与管理Samba服务器

## 任务10-1 安装并启动samba服务

使用rpm -qa |grep samba命令检测系统是否安装了samba相关性软件包：

```
[root@Server01 ~]# rpm -qa |grep samba
```

(1) 挂载ISO安装映像。

```
[root@Server01 ~]# mount /dev/cdrom /media
```

(2) 制作yum源文件/etc/yum.repos.d/dvd.repo（略）。

(3) 使用dnf命令查看samba软件包的信息。

```
[root@Server01 ~]# dnf info samba
```

(4) 使用yum命令安装samba服务。

```
[root@Server01 ~]# dnf clean all
```

//安装前先清除缓存

```
[root@Server01 ~]# dnf install samba -y
```

## 任务10-1 安装并启动samba服务

(5) 所有软件包安装完毕，可以使用rpm命令再一次进行查询：

```
[root@Server01 ~]# rpm -qa | grep samba
```

```
.....
```

```
samba-4.11.2-13.el8.x86_64
```

(6) 启动smb服务，设置开机启动该服务，重启服务。

```
[root@Server01 ~]# systemctl start smb ; systemctl enable smb
```

注意：在服务器配置中，更改了配置文件后，一定要记得重启服务，让服务重新加载配置文件，这样新配置才生效。重启的命令是：systemctl restart smb或systemctl reload smb

## 任务10-2 主要配置文件smb.conf

### 1. samba服务程序中的参数以及作用

samba的配置文件一般就放在/etc/samba目录中，主配置文件名为smb.conf。

RHEL 8的smb.conf配置文件已经简化，只有37行左右。

为了方便配置，建议先备份smb.conf，一旦发现错误可以随时从备份文件中恢复主配置文件。

操作如下：

```
[root@Server01 ~]# cd /etc/samba
```

```
[root@Server01 samba]# ls
```

```
[root@Server01 samba]# cp smb.conf smb.conf.bak
```

```
[root@Server01 samba]# cd
```

## 任务10-2 主要配置文件smb.conf

### 2. Share Definitions共享服务的定义

Share Definitions设置对象为共享目录和打印机，如果想发布共享资源，需要对Share Definitions部分进行配置。

(1) 设置共享名。

共享名的设置非常简单，格式为：

[共享名]

(2) 共享资源描述。

格式：comment = 备注信息

(3) 共享路径。

格式：path = 绝对地址路径

## 任务10-2 主要配置文件smb.conf

(4) 设置匿名访问。

设置是否允许对共享资源进行匿名访问，可以更改public字段。

格式：

```
public = yes    #允许匿名访问
```

```
public = no     #禁止匿名访问
```

## 任务10-2 主要配置文件smb.conf

【例10-1】samba服务器中有一个目录为/share，需要发布该目录成为共享目录，定义共享名为public，要求：允许浏览、允许只读、允许匿名访问。设置如下所示。

```
[public]

    comment = public

    path = /share

    browseable = yes

    read only = yes

    public = yes
```



## 任务10-2 主要配置文件smb.conf

(5) 设置访问用户。

如果共享资源存在重要数据的话，需要对访问用户进行审核，我们可以使用valid users字段进行设置。

格式：

```
valid users = 用户名
```

```
valid users = @组名
```

【例10-2】samba服务器/share/tech目录中存放了公司技术部数据，只允许技术部员工和经理访问，技术部组为tech，经理账号为manager。

```
[tech]
```

```
comment=tech
```

```
path=/share/tech
```

```
valid users=@tech,manager
```

## 任务10-2 主要配置文件smb.conf

(6) 设置目录只读。

共享目录如果需要限制用户的读写操作，我们可以通过read only实现。

格式：

```
read only = yes    #只读  
read only = no     #读写
```

(7) 设置过滤主机。

```
hosts allow = 192.168.10.  server.abc.com
```

上述程序表示允许来自192.168.10.0或server.abc.com的访问者访问samba服务器资源。

```
hosts deny = 192.168.2.
```

上述程序表示不允许来自192.168.2.0网络的主机访问当前samba服务器资源。

## 任务10-2 主要配置文件smb.conf

【例10-3】 samba服务器公共目录/public存放大量共享数据，为保证目录安全，仅允许192.168.10.0网络的主机访问，并且只允许读取，禁止写入。

```
[public]

comment=public

path=/public

public=yes

read only=yes

hosts allow = 192.168.10.
```

## 任务10-2 主要配置文件smb.conf

(8) 设置目录可写。

如果共享目录允许用户写操作，可以使用writable或write list两个字段进行设置。

writable格式：

```
writable = yes    #读写
```

```
writable = no     #只读
```

write list格式：

```
write list = 用户名
```

```
write list = @组名
```

## 任务10-3 samba服务的日志文件和密码文件

日志文件对于samba非常重要，它存储着客户端访问samba服务器的信息，以及samba服务的错误提示信息等，可以通过分析日志，帮助解决客户端访问和服务器维护等问题。

在/etc/samba/smb.conf文件中，log file为设置samba日志的字段。如下所示：

```
log file = /var/log/samba/log.%m
```

samba服务的日志文件默认存放在/var/log/samba/中，其中samba会为每个连接到samba服务器的计算机分别建立日志文件。使用ls -a /var/log/samba命令可以查看日志的所有文件。

## **任务10-3 samba服务的日志文件和密码文件**

### 2. samba服务密码文件

samba服务器发布共享资源后，客户端访问samba服务器，需要提交用户名和密码进行身份验证，验证合格后才可以登录。samba服务为了实现客户身份验证功能，将用户名和密码信息存放在/etc/samba/smbpasswd中，在客户端访问时，将用户提交的资料与smbpasswd中存放的信息进行比对，如果相同，并且samba服务器其他安全设置允许，客户端与samba服务器的连接才能建立成功。

## 任务10-3 samba服务的日志文件和密码文件

那如何建立samba账号呢？首先，samba账号并不能直接建立，需要先建立Linux同名的系统账号。例如，如果要建立一个名为yy的samba账号，那么Linux系统中必须提前存在一个同名的yy系统账号。

samba中添加账号的命令为smbpasswd，格式为：

```
smbpasswd -a 用户名
```

## 任务10-3 samba服务的日志文件和密码文件

【例10-4】在samba服务器中添加samba账号reading。

(1) 建立Linux系统账号reading。

```
[root@Server01 ~]# useradd reading
```

```
[root@Server01 ~]# passwd reading
```

(2) 添加reading用户的samba账号。

```
[root@Server01 ~]# smbpasswd -a reading
```



## 任务10-4 user服务器实例解析

在RHEL 8系统中，samba服务程序默认使用的是用户口令认证模式（user）。这种认证模式可以确保仅让有密码且受信任的用户访问共享资源，而且验证过程也十分简单。

【例10-5】如果公司有多个部门，因工作需要，就必须分门别类地建立相应部门的目录。要求将销售部的资料存放在samba服务器的/companydata/sales/目录下集中管理，以便销售人员浏览，并且该目录只允许销售部员工访问。

需求分析：在/companydata/sales/目录中存放有销售部的重要数据，为了保证其他部门无法查看其内容，我们需要将全局配置中security设置为user安全级别。这样就启用了samba服务器的身份验证机制。然后在共享目录/companydata/sales下设置valid users字段，配置只允许销售部员工访问这个共享目录。

## **任务10-4 user服务器实例解析**

(1) 建立共享目录，并在其下建立测试文件。

```
[root@Server01 ~]# mkdir /companydata
```

```
[root@Server01 ~]# mkdir /companydata/sales
```

```
[root@Server01 ~]# touch /companydata/sales/test_share.tar
```

## 任务10-4 user服务器实例解析

(2) 添加销售部用户和组并添加相应的samba账号。

① 使用groupadd命令添加sales组，然后执行useradd命令和passwd命令，以添加销售部员工的账号及密码。此处单独增加一个test\_user1账号，不属于sales组，供测试用。

```
[root@Server01 ~]# groupadd sales #建立销售组sales
[root@Server01 ~]# useradd -g sales sale1 #建立用户sale1，添加到sales组
[root@Server01 ~]# useradd -g sales sale2 #建立用户sale2，添加到sales组
[root@Server01 ~]# useradd test_user1 #供测试用
[root@Server01 ~]# passwd sale1 #设置用户sale1密码
[root@Server01 ~]# passwd sale2 #设置用户sale2密码
[root@Server01 ~]# passwd test_user1 #设置用户test_user1密码
```

## 任务10-4 user服务器实例解析

② 为销售部成员添加相应samba账号。

```
[root@Server01 ~]# smbpasswd -a sale1
```

```
[root@Server01 ~]# smbpasswd -a sale2
```

## 任务10-4 user服务器实例解析

(3) 修改samba主配置文件：vim /etc/samba/smb.conf。直接在原文件末尾添加，但要注意将原文件的[global]删除或用“#”注释掉，文件中不能有两个同名的[global]。当然也可直接在原来的[global]上进行修改。

```
39 [global]
40   workgroup = Workgroup
41   server string = File Server
42   security = user
43   #设置user安全级别模式，取默认值
44   passdb backend = tdbsam
45   printing = cups
46   printcap name = cups
47   load printers = yes
48   cups options = raw
```

```
49 [sales]
50   #设置共享目录的共享名为sales
51   comment=sales
52   path=/companydata/sales
53   #设置共享目录的绝对路径
54   writable = yes
55   browseable = yes
56   valid users = @sales
57   #设置可以访问的用户为sales组
```

## 任务10-4 user服务器实例解析

(4) 设置共享目录的本地系统权限和属组。

```
[root@Server01 ~]# chmod 770 /companydata/sales -R
```

```
[root@Server01 ~]# chown :sales /companydata/sales -R
```

-R参数是递归用的，一定要加上。

## 任务10-4 user服务器实例解析

(5) 更改共享目录和用户家目录的context值，或者禁掉SELinux。

```
[root@Server01 ~]# chcon -t samba_share_t /companydata/sales -R
```

```
[root@Server01 ~]# chcon -t samba_share_t /home/sale1 -R
```

```
[root@Server01 ~]# chcon -t samba_share_t /home/sale2 -R
```

或者：

```
[root@Server01 ~]# getenforce
```

```
Enforcing
```

```
[root@Server01 ~]# setenforce Permissive
```

或者：

```
[root@Server01 ~]# setenforce 0
```

## 任务10-4 user服务器实例解析

(6) 让防火墙放行，这一步很重要。

```
[root@Server01 ~]# firewall-cmd --permanent --add-service=samba
```

```
[root@Server01 ~]# firewall-cmd --reload //重新加载防火墙
```

```
[root@Server01 ~]# firewall-cmd --list-all
```

```
public (active)
```

```
.....
```

```
services: ssh dhcpv6-client samba //已经加入防火墙的允许服务
```

```
ports:
```

```
.....
```



## 任务10-4 user服务器实例解析

(7) 重新加载samba服务并设置开机时自动启动。

```
[root@Server01 ~]# systemctl restart smb
```

```
[root@Server01 ~]# systemctl enable smb
```

(8) 测试。

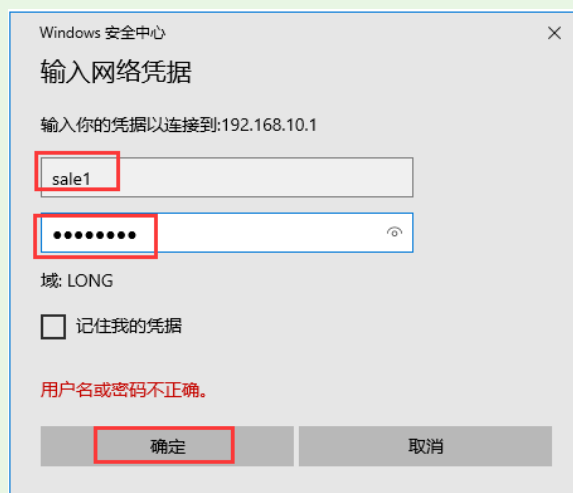
一是在Windows 10中利用资源管理器进行测试，二是利用Linux客户端。

## 任务10-4 user服务器实例解析

以下的操作在Client2上进行。

### (1) 使用UNC路径直接进行访问

依次选择“开始”→“运行”命令，使用UNC路径直接进行访问，例如\\192.168.10.1。打开“Windows安全”对话框，如图所示。输入sale1或sale2及其密码，登录后可以正常访问。



## 任务10-4 user服务器实例解析

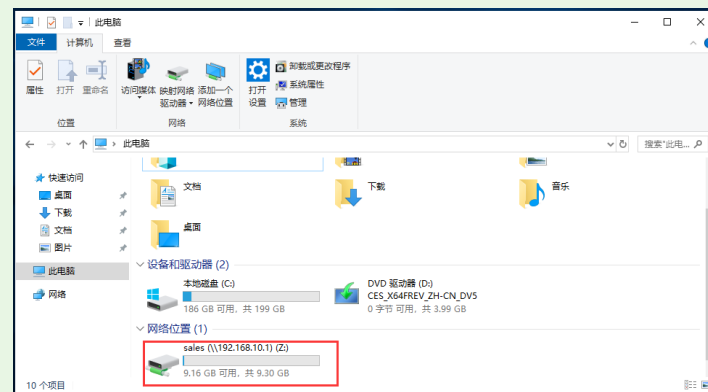
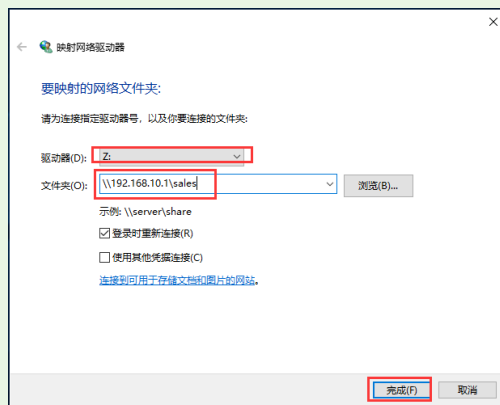
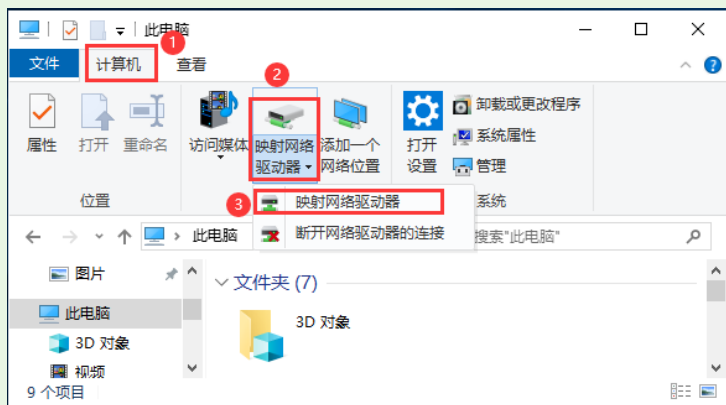
### (2) 使用映射网络驱动器访问samba服务器共享目录

① 在桌面双击“此电脑”图标，再依次选择“计算机”→“映射网络驱动器”命令，如图所示。

②单击“映射网络驱动器”命令，在弹出的“映射网络驱动器”对话框中选择Z驱动器，并输入sales共享目录的地址，如\\192.168.10.1\sales，如图所示。

③单击“完成”按钮，在接下来的对话框中输入可以访问sales共享目录的samba账号和密码。

④再次双击“此电脑”图标，如图所示。驱动器Z就是共享目录sales，就可以很方便地访问了。



## 任务10-5 配置可匿名访问的samba服务器

【例10-6】 公司需要添加samba服务器作为文件服务器，工作组名为Workgroup，共享目录为/share，共享名为public，这个共享目录允许公司所有员工下载文件，但不允许上传文件。

step1：在Server01上建立share目录，并在其下建立测试文件，设置共享文件夹本地系统权限。

```
[root@Server01 ~]# mkdir /share ; touch /share/test_share.tar
```

```
[root@Server01 ~]# chmod 645 /share -R
```

## 任务10-5 配置可匿名访问的samba服务器

step2: 修改samba主配置文件smb.conf。

```
[root@Server01 ~]# vim /etc/samba/smb.conf
```

在任务10-4的基础上修改配置文件，与任务10-4配置文件内容一样的不再显示出来。

```
39          [global]
          .....
44          map to guest = bad user
          .....
50          [public]
51          comment=public
52          path=/share
53          guest ok=yes
54          #允许匿名用户访问
55          browseable=yes
56          #在客户端显示共享的目录
57          public=yes
58          #最后设置允许匿名访问
59          read only = yes
```

## 任务10-5 配置可匿名访问的samba服务器

step3: 让防火墙放行samba服务。在任务10-4中已详细设置，这里不再赘述。。

step4: 更改共享目录的context值。

```
[root@Server01 ~]# chcon -t samba_share_t /share
```

step5: 重新加载配置。

可以使用restart重新启动服务或者使用reload重新加载配置。

```
[root@Server01 ~]# systemctl restart smb
```

//或者

```
[root@Server01 ~]# systemctl reload smb
```

## 任务10-5 配置可匿名访问的samba服务器

(2) 解决Windows 10默认不允许匿名访问的问题

- ① 在Client2的命令提示符下输入命令 “gpedit.msc” ，并单击 “确定” 按钮。
- ② 待本地组策略编辑器弹出后，依次选取 “计算机管理” → “管理模板” → “网络” → “lanman工作站” 命令。
- ③ 在右侧窗口找到 “启用不安全的来宾登录” 选项，将之调整为 “已启用” ，单击 “应用” → “确定” 按钮。
- ④ 重启设备再次测试。

## 任务10-6 配置samba客户端

### 1. Linux客户端访问samba共享

(1) 在Clients上安装samba-client和cifs-utils。

```
[root@@Client1 ~]# mount /dev/cdrom /media
```

```
mount: /media: WARNING: device write-protected, mounted read-only.
```

```
[root@@Client1 ~]# vim /etc/yum.repos.d/dvd.repo
```

```
[root@@Client1 ~]# dnf install samba-client -y
```

```
[root@@Client1 ~]# dnf install cifs-utils -y
```



## 任务10-6 配置samba客户端

### 1. Linux客户端访问samba共享

(2) Linux客户端使用smbclient命令访问服务器。

① smbclient可以列出目标主机共享目录列表。Smbclient的命令格式为：

smbclient -L 目标IP地址或主机名 -U 登录用户名%密码

当查看Server01（192.168.10.1）主机的共享目录列表时，提示输入密码，这时候可以不输入密码，而直接按“Enter”键，这样表示匿名登录，然后就会显示匿名用户可以看到的共享目录列表。

```
[root@@Client1 ~]# smbclient -L 192.168.10.1
```

## 任务10-6 配置samba客户端

### 1. Linux客户端访问samba共享

想使用samba账号查看samba服务器端共享的目录，可以加上-U参数，后面跟上用户名%密码。下面的命令显示只有sale2账号（其密码为12345678）才有权限浏览和访问的sales共享目录：

```
[root@@Client1 ~]# smbclient -L 192.168.10.1 -U sale2%12345678
```

注意：不同用户使用smbclient浏览的结果可能是不一样的，这要根据服务器设置的访问控制权限而定。

## 任务10-6 配置samba客户端

下面命令运行后，将进入交互式界面。

```
[root@@Client1 ~]# smbclient //192.168.10.1/sales -U sale2%12345678
Try "help" to get a list of possible commands.
smb: \> ls

.                D      0 Mon Jul 16 21:14:52 2018
..               D      0 Mon Jul 16 18:38:40 2018
test_share.tar   A      0 Mon Jul 16 18:39:03 2018

                                9754624 blocks of size 1024. 9647416 blocks available

smb: \> mkdir testdir                                //新建一个目录进行测试
smb: \> ls

.                D      0 Mon Jul 16 21:15:13 2018
..               D      0 Mon Jul 16 18:38:40 2018
test_share.tar   A      0 Mon Jul 16 18:39:03 2018
testdir          D      0 Mon Jul 16 21:15:13 2018

                                9754624 blocks of size 1024. 9647416 blocks available

smb: \> exit
[root@@Client1 ~]#
```

## 任务10-6 配置samba客户端

(3) Linux客户端使用mount命令挂载共享目录。

mount命令挂载共享目录的格式为：

```
mount -t cifs //目标IP地址或主机名/共享目录名称 挂载点 -o username=用户名
```

下面的命令结果为挂载192.168.10.1主机上的共享目录sales到/mnt/sambadata目录下，cifs是samba所使用的文件系统。

```
[root@@Client1 ~]# mkdir -p /mnt/sambadata
[root@@Client1 ~]# mount -t cifs //192.168.10.1/sales /mnt/sambadata/ -o username=sale1
Password for sale1@//192.168.10.1/sales: *****
//输入sale1的samba用户密码，不是系统用户密码
[root@@Client1 ~]# cd /mnt/sambadata
[root@@Client1 sambadata]# ls
testdir test_share.tar
```

## 任务10-6 配置samba客户端

### 2. Linux客户端访问Windows共享

在客户端Client1上直接使用命令smbclient可以访问Windows共享。

```
[root@Server01 ~]# smbclient -L //192.168.10.31 -U administrator
```

```
Enter SAMBA\administrator's password:
```

Sharename	Type	Comment
-----------	------	---------

-----	----	-----
-------	------	-------

ADMIN\$	Disk	远程管理
---------	------	------

C\$	Disk	默认共享
-----	------	------

IPC\$	IPC	远程 IPC
-------	-----	--------

```
SMB1 disabled -- no workgroup available
```

```
[root@Server01 ~]#
```

# 学习内容

LEARNING CONTENTS

- 项目知识准备

- 项目设计与准备

- 项目实施

- 项目实录：配置与管理Samba服务器

## 配置与管理Samba服务器

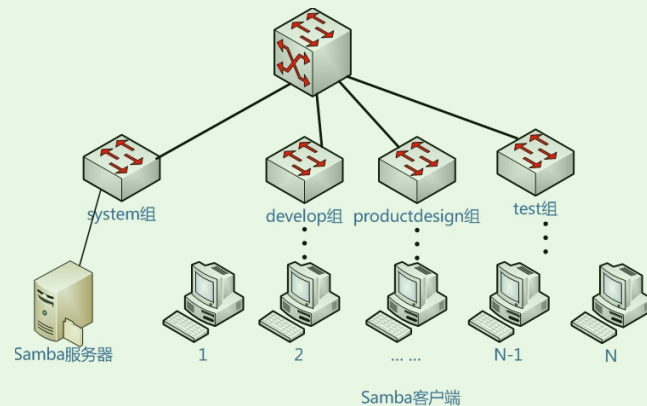
### 1.视频学习



## 配置与管理Samba服务器

### 2. 项目背景

某公司有system、develop、productdesign和test 4个小组，个人办公机操作系统为Windows 7/8，少数开发人员采用Linux操作系统，服务器操作系统为RHEL 8，需要设计一套建立在RHEL 8之上的安全文件共享方案。每个用户都有自己的网络磁盘，develop组到test组有共用的网络硬盘，所有用户（包括匿名用户）有一个只读共享资料库；所有用户（包括匿名用户）要有一个存放临时文件的文件夹。网络拓扑如图所示。





## 配置与管理Samba服务器

---

### 3. 项目要求

- (1) System组具有管理所有samba空间的权限。
- (2) 各部门的私有空间：各小组拥有自己的空间，除了小组成员及system组有权限以外，其他用户不可访问（包括列表、读和写）。
- (3) 资料库：所有用户（包括匿名用户）都具有读取权限而不具有写入数据的权限。
- (4) develop组与test组之外的用户不能访问develop组与test组的共享空间。
- (5) 公共临时空间：让所有用户可以读取、写入、删除。

---

# THANKS

---

