项目14 配置与管理FTP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FTP服务的工作原理
- 学会配置vsftpd服务器

学习内容

LEARNING CONTENTS

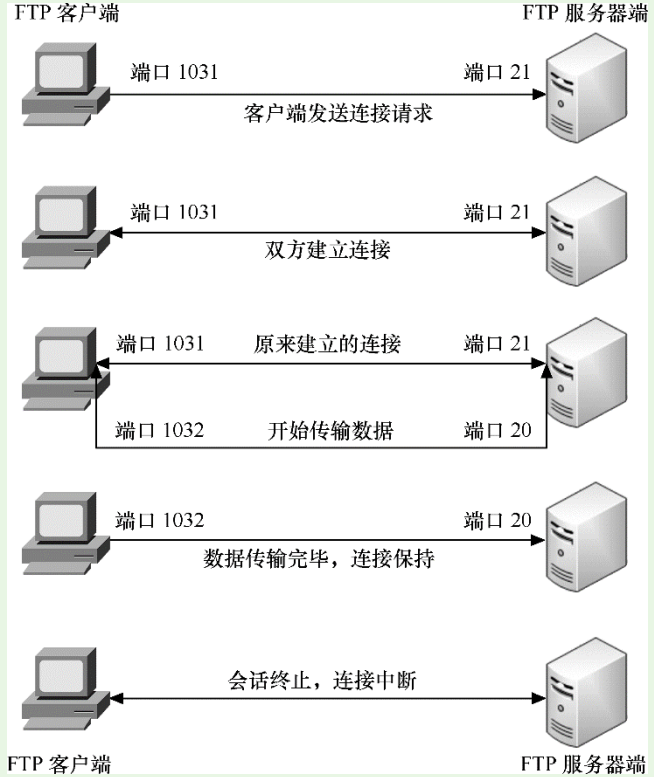
- 项目知识准备
- 项目设计与准备
- 项目实施
- 项目实录：配置与管理FTP服务器

FTP的工作原理

FTP大大简化了文件传输的复杂性，它能够使文件通过网络从一台主机传送到另外一台计算机上却不受计算机和操作系统类型的限制。

FTP服务的具体工作过程如图所示。

（1）客户端向服务器发出连接请求，同时客户端系统动态地打开一个大于1024的端口等候服务器连接（如1031端口）。



FTP的工作原理

（2）若FTP服务器在端口21侦听到该请求，则会在客户端1031端口和服务器的21端口之间建立起一个FTP会话连接。

（3）当需要传输数据时，FTP客户端再动态地打开一个大于1024的端口（如1032端口）连接到服务器的20端口，并在这两个端口之间进行数据的传输。当数据传输完毕，这两个端口会自动关闭。

（4）当FTP客户端断开与FTP服务器的连接时，客户端上动态分配的端口将自动释放。

FTP服务有两种工作模式：主动传输模式（Active FTP）和被动传输模式（Passive FTP）。

匿名用户

FTP服务不同于WWW，它首先要求登录到服务器上，然后再进行文件的传输。这对于很多公开提供软件下载的服务器来说十分不便，于是匿名用户访问就诞生了：通过使用一个共同的用户名anonymous，密码不限的管理策略（一般使用用户的邮箱作为密码即可）让任何用户都可以很方便地从FTP服务器上下载软件。

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FTP服务器

项目需求准备

两台安装了RHEL 8的计算机，连网方式都设为host only（VMnet1），一台作为服务器，一台作为客户端使用。宿主机使用Windows 10。计算机的配置信息如表所示（可以使用VM的克隆技术快速安装需要的Linux客户端）。

主机名称	操作系统	IP地址	角色及其他
FTP服务器：Server01	RHEL 8	192.168.10.1	FTP服务器，VMnet1
Linux客户端：Client1	RHEL 8	192.168.10.21	FTP客户端，VMnet1
Windows客户端：Client2	Windows 10	192.168.10.31	FTP客户端，VMnet1

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FTP服务器

任务14-1 安装、启动与停止vsftpd服务

1．安装vsftpd服务

```
[root@Server01 ~]# rpm -q vsftpd
[root@Server01 ~]# mount /dev/cdrom /media
[root@Server01 ~]# dnf clean all                    //安装前先清除缓存
[root@Server01 ~]# dnf install vsftpd -y
[root@Server01 ~]# dnf install ftp -y               //同时安装ftp软件包
[root@Server01 ~]# rpm -qa|grep vsftpd              //检查安装组件是否成功
```

任务14-1 安装、启动与停止vsftpd服务

2．vsftpd服务启动、重启、随系统启动、停止

安装完vsftpd服务后，下一步就是启动了。vsftpd服务可以以独立或被动方式启动。在Red Hat Enterprise Linux 8中，默认以独立方式启动。

重新启动vsftpd服务、随系统启动，开放防火墙，开放SELinux，输入下面的命令：

```
[root@Server01 ~]# systemctl restart vsftpd
[root@Server01 ~]# systemctl enable vsftpd
[root@Server01 ~]# firewall-cmd --permanent --add-service=ftp
[root@Server01 ~]# firewall-cmd --reload
[root@Server01 ~]# setsebool -P ftpd_full_access=on
```

任务14-2 认识vsftpd的配置文件

1．主配置文件

vsftpd服务程序的主配置文件（/etc/vsftpd/vsftpd.conf）的内容总长度达到127行，但其中大多数参数在开头都添加了井号（#），从而成为注释信息。

可以使用grep命令添加-v参数，过滤并反选出没有包含井号（#）的参数行（即过滤掉所有的注释信息），然后将过滤后的参数行通过输出重定向符写回原始的主配置文件中（为了安全起见，请先备份主配置文件）。

任务14-2 认识vsftpd的配置文件

```
[root@Server01 ~]# mv /etc/vsftpd/vsftpd.conf /etc/vsftpd/vsftpd.conf.bak
[root@Server01 ~]#  grep -v "#" /etc/vsftpd/vsftpd.conf.bak > /etc/vsftpd/vsftpd.conf
[root@Server01 ~]# cat /etc/vsftpd/vsftpd.conf -n
     1  anonymous_enable=YES
     2  local_enable=YES
     3  write_enable=YES
     4  local_umask=022
     5  dirmessage_enable=YES
     6  xferlog_enable=YES
     7  connect_from_port_20=YES
     8  xferlog_std_format=YES
     9  listen=NO
    10  listen_ipv6=YES
    11
    12  pam_service_name=vsftpd
    13  userlist_enable=YES
```

任务14-2 认识vsftpd的配置文件

表中列举了vsftpd服务程序主配置文件中常用的参数以及作用。

参 数	作 用
listen=[YES|NO]	是否以独立运行的方式监听服务
listen_address=IP地址	设置要监听的IP地址
listen_port=21	设置FTP服务的监听端口
download_enable = [YES|NO]	是否允许下载文件
userlist_enable=[YES|NO] userlist_deny=[YES|NO]	设置用户列表为“允许”还是“禁止”操作
max_clients=0	最大客户端连接数，0为不限制
max_per_ip=0	同一IP地址的最大连接数，0为不限制
anonymous_enable=[YES|NO]	是否允许匿名用户访问
anon_upload_enable=[YES|NO]	是否允许匿名用户上传文件
anon_umask=022	匿名用户上传文件的umask值
anon_root=/var/ftp	匿名用户的FTP根目录
anon_mkdir_write_enable=[YES|NO]	是否允许匿名用户创建目录
anon_other_write_enable=[YES|NO]	是否开放匿名用户的其他写入权限（包括重命名、删除等操作权限）
anon_max_rate=0	匿名用户的最大传输速率（字节/秒），0为不限制
local_enable=[YES|NO]	是否允许本地用户登录FTP
local_umask=022	本地用户上传文件的umask值
local_root=/var/ftp	本地用户的FTP根目录
chroot_local_user=[YES|NO]	是否将用户权限禁锢在FTP目录，以确保安全
local_max_rate=0	本地用户最大传输速率（字节/秒），0为不限制

任务14-2 认识vsftpd的配置文件

2．/etc/pam.d/vsftpd

vsftpd的Pluggable Authentication Modules（PAM）配置文件，主要用来加强vsftpd服务器的用户认证。

3．/etc/vsftpd/ftpusers

所有位于此文件内的用户都不能访问vsftpd服务。当然，为了安全起见，这个文件中默认已经包括了root、bin和daemon等系统账号。

任务14-2 认识vsftpd的配置文件

4．/etc/vsftpd/user_list

这个文件中包括的用户有可能是被拒绝访问vsftpd服务的，也可能是允许访问的，这主要取决于vsftpd的主配置文件/etc/vsftpd/vsftpd.conf中的“userlist_deny”参数是设置为“YES”（默认值）还是“NO”。

- 当userlist_deny=NO时，仅允许文件列表中的用户访问FTP服务器。
- 当userlist_deny=YES时，这也是默认值，拒绝文件列表中的用户访问FTP服务器。

5．/var/ftp文件夹

该文件夹是vsftpd提供服务的文件集散地，它包括一个pub子目录。在默认配置下，所有的目录都是只读的，不过只有root用户有写权限。

任务14-3 配置匿名用户FTP实例

1．vsftpd的认证模式

vsftpd允许用户以3种认证模式登录到FTP服务器上。

（1）匿名开放模式：是一种最不安全的认证模式，任何人都无须密码验证而直接登录FTP服务器。

（2）本地用户模式：是通过Linux系统本地的账户密码信息进行认证的模式，相较于匿名开放模式，该模式更安全，而且配置起来也很简单。

（3）虚拟用户模式：是这3种模式中最安全的一种认证模式，它需要为FTP服务单独建立用户数据库文件，虚拟映射用来进行口令验证的账户信息，而这些账户信息在服务器系统中实际上是不存在的，仅供FTP服务程序进行认证使用。

任务14-3 配置匿名用户FTP实例

2．匿名用户登录的参数说明

参　数	作　用
anonymous_enable=YES	允许匿名访问模式
anon_umask=022	匿名用户上传文件的umask值
anon_upload_enable=YES	允许匿名用户上传文件
anon_mkdir_write_enable=YES	允许匿名用户创建目录
anon_other_write_enable=YES	允许匿名用户修改目录名称或删除目录

任务14-3 配置匿名用户FTP实例

3．配置匿名用户登录FTP服务器实例

【例14-1】搭建一台FTP服务器，允许匿名用户上传和下载文件，匿名用户的根目录设置为/var/ftp。

（1）新建测试文件，编辑/etc/vsftpd/vsftpd.conf。

```
[root@Server01 ~]# touch /var/ftp/pub/sample.tar
[root@Server01 ~]# vim  /etc/vsftpd/vsftpd.conf
```

任务14-3 配置匿名用户FTP实例

3．配置匿名用户登录FTP服务器实例

（2）在文件后面添加如下4行（语句前后一定不要带空格，若有重复的语句请删除或直接在其上更改，“#”及后面的内容不要写到文件里）。

```
anonymous_enable=YES
#允许匿名用户登录
anon_root=/var/ftp
#设置匿名用户的根目录为/var/ftp
anon_upload_enable=YES
#允许匿名用户上传文件
anon_mkdir_write_enable=YES
#允许匿名用户创建文件夹
```

任务14-3 配置匿名用户FTP实例

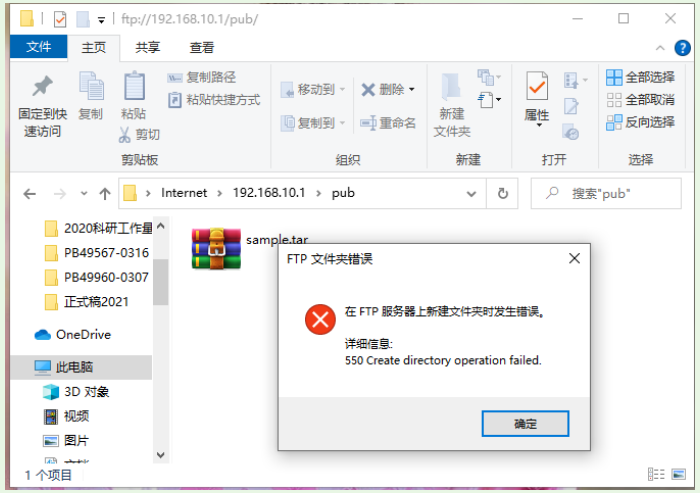
3．配置匿名用户登录FTP服务器实例

（3）允许SELinux，让防火墙放行ftp服务，重启vsftpd服务。

```
[root@Server01 ~]# setenforce 0
[root@Server01 ~]# firewall-cmd --permanent --add-service=ftp
[root@Server01 ~]# firewall-cmd --reload
[root@Server01 ~]# firewall-cmd --list-all
[root@Server01 ~]# systemctl restart vsftpd
```

任务14-3 配置匿名用户FTP实例

在Windows 10客户端的资源管理器中输入ftp://192.168.10.1，打开pub目录，新建一个文件夹，结果出错了，如图所示。



任务14-3 配置匿名用户FTP实例

什么原因呢？系统的本地权限没有设置！

（4）设置本地系统权限，将属主设为ftp，或者对pub目录赋予其他用户写的权限。

```
[root@Server01 ~]# ll -ld /var/ftp/pub
drwxr-xr-x. 2 root root 6 Mar 23  2017 /var/ftp/pub //其他用户没有写入权限
[root@Server01 ~]#  chown ftp /var/ftp/pub          //将属主改为匿名用户ftp
```

（5）在Windows 10客户端再次测试，在pub目录下能够建立新文件夹。

任务14-4 配置本地模式的常规FTP服务器案例

1．FTP服务器配置要求

公司内部现在有一台FTP服务器和Web服务器，FTP主要用于维护公司的网站内容，包括上传文件、创建目录、更新网页等。公司现有两个部门负责维护任务，两者分别适用team1和team2账号进行管理。先要求仅允许team1和team2账号登录FTP服务器，但不能登录本地系统，并将这两个账号的根目录限制为/web/www/html，不能进入该目录以外的任何目录。

2．需求分析

将FTP服务器和Web服务器放在一起是企业经常采用的方法，这样方便实现对网站的维护。为了增强安全性，首先需要仅允许本地用户访问，并禁止匿名用户登录。其次，使用chroot功能将team1和team2锁定在/web/www/html目录下。如果需要删除文件，则还需要注意本地权限。

任务14-4 配置本地模式的常规FTP服务器案例

3．解决方案

（1）建立维护网站内容的FTP账号team1、team2，并为其设置密码。

```
[root@Server01 ~]# useradd  team1; useradd team2; useradd  user1
[root@Server01 ~]# passwd  team1
[root@Server01 ~]# passwd  team2
[root@Server01 ~]# passwd  user1
```

任务14-4 配置本地模式的常规FTP服务器案例

（2）配置vsftpd.conf主配置文件并做相应修改写入配置文件时，下面的注释一定去掉，语句前后不要加空格。

```
[root@Server01 ~]# vim  /etc/vsftpd/vsftpd.conf
anonymous_enable=NO
#禁止匿名用户登录
local_enable=YES
#允许本地用户登录
local_root=/web/www/html
#设置本地用户的根目录为/web/www/html
chroot_local_user=NO
#是否限制本地用户，这也是默认值，可以省略
chroot_list_enable=YES
#激活chroot功能
chroot_list_file=/etc/vsftpd/chroot_list
#设置锁定用户在根目录中的列表文件
allow_writeable_chroot=YES
#只要启用chroot就一定加入这条：允许chroot限制，否则出现连接错误。
```

任务14-4 配置本地模式的常规FTP服务器案例

注意：chroot是靠例外列表来实现的，列表内用户即是例外的用户。所以根据是否启用本地用户转换，可设置不同目的的例外列表，从而实现chroot功能。因此实现锁定目录有两种实现方法。第一种是除列表内的用户外，其他用户都被限定在固定目录内，即列表内用户自由，列表外用户受限制。这时启用chroot_local_user=YES。

① 第一种表示。

```
chroot_local_user=YES
chroot_list_enable=YES
chroot_list_file=/etc/vsftpd/chroot_list
allow_writeable_chroot=YES
```

任务14-4 配置本地模式的常规FTP服务器案例

② 第二种是除列表内的用户外，其他用户都可自由转换目录。即列表内用户受限制，列表外用户自由。这时启用chroot_local_user=NO。本例使用第二种。

```
chroot_local_user=NO
chroot_list_enable=YES
chroot_list_file=/etc/vsftpd/chroot_list
allow_writeable_chroot=YES
```

任务14-4 配置本地模式的常规FTP服务器案例

（3）建立/etc/vsftpd/chroot_list文件，添加team1和team2账号。

```
[root@Server01 ~]# vim  /etc/vsftpd/chroot_list
team1
team2
```

（4）防火墙放行和SELinux允许！重启FTP服务。

```
[root@Server01 ~]# firewall-cmd --permanent --add-service=ftp
[root@Server01 ~]# firewall-cmd --reload
[root@Server01 ~]# setenforce 0
[root@Server01 ~]# systemctl restart vsftpd
```

任务14-4 配置本地模式的常规FTP服务器案例

（5）修改本地权限。

```
[root@Server01 ~]# mkdir  /web/www/html -p
[root@Server01 ~]# touch  /web/www/html/test.sample
[root@Server01 ~]# ll   -d   /web/www/html
[root@Server01 ~]# chmod   -R   o+w   /web/www/html                    //其他用户可以写入！
[root@Server01 ~]# ll   -d   /web/www/html
```

（6）在Linux客户端client1上先安装ftp工具，然后测试。

```
[root@client1 ~]# mount /dev/cdrom /so
[root@client1 ~]# dnf clean all
[root@client1 ~]# dnf install ftp –y
```

（7）最后，在Server01上把该任务的配置文件新增语句前面加上“#”注释掉。

任务14-5 设置vsftp虚拟账号

为了FTP服务器的安全，可以使用虚拟用户验证方式，也就是将虚拟的账号映射为服务器的实体账号，客户端使用虚拟账号访问FTP服务器。

要求：使用虚拟用户user2、user3登录FTP服务器，访问主目录是/var/ftp/vuser，用户只允许查看文件，不允许上传、修改等操作。

任务14-5 设置vsftp虚拟账号

对于vsftp虚拟账号的配置主要有以下几个步骤。

1．创建用户数据库

（1）创建用户文本文件。

首先，建立保存虚拟账号和密码的文本文件，格式如下。

```
虚拟账号1
密码
虚拟账号2
密码
```

任务14-5 设置vsftp虚拟账号

（2）生成数据库。

保存虚拟账号及密码的文本文件无法被系统账号直接调用，需要使用db_load命令生成db数据库文件。

```
[root@Server01 ~]# db_load  -T  -t  hash  -f  /vftp/vuser.txt  /vftp/vuser.db
[root@Server01 ~]# ls   /vftp
vuser.db   vuser.txt
```

任务14-5 设置vsftp虚拟账号

（3）修改数据库文件访问权限。

数据库文件中保存着虚拟账号和密码信息，为了防止非法用户盗取，可以修改该文件的访问权限。

```
[root@Server01 ~]# chmod  700  /vftp/vuser.db; ll  /vftp
```

任务14-5 设置vsftp虚拟账号

2．配置PAM文件

为了使服务器能够使用数据库文件，对客户端进行身份验证，需要调用系统的PAM模块。下面修改vsftp对应的PAM配置文件/etc/pam.d/vsftpd，将默认配置使用“#”全部注释，添加相应字段，如下所示。

```
[root@Server01 ~]# vim   /etc/pam.d/vsftpd
#%PAM-1.0
#session    optional     pam_keyinit.so    force revoke
#auth required pam_listfile.so item=user sense=deny file=/etc/vsftpd/ftpusers onerr=succeed
#auth       required    pam_shells.so
#auth       include     password-auth
#account    include     password-auth
#session    required     pam_loginuid.so
#session    include     password-auth
auth                                    required                        pam_userdb.so   db=/vftp/vuser
account                                 required                        pam_userdb.so   db=/vftp/vuser
```

任务14-5 设置vsftp虚拟账号

3．创建虚拟账户对应系统用户，并建立测试文件和目录。

```
[root@Server01 ~]# useradd -d /var/ftp/vuser vuser                    ①
[root@Server01 ~]# chown vuser.vuser /var/ftp/vuser                   ②
[root@Server01 ~]# chmod 555 /var/ftp/vuser                           ③
[root@Server01 ~]# touch /var/ftp/vuser/file1; mkdir /var/ftp/vuser/dir1
[root@Server01 ~]# ls -ld /var/ftp/vuser                              ④
dr-xr-xr-x. 6 vuser vuser 127 Jul 21 14:28 /var/ftp/vuser
```

任务14-5 设置vsftp虚拟账号

4．修改/etc/vsftpd/vsftpd.conf

```
anonymous_enable=NO                    ①
anon_upload_enable=NO
anon_mkdir_write_enable=NO
anon_other_write_enable=NO
local_enable=YES                       ②
chroot_local_user=YES                  ③
allow_writeable_chroot=YES
write_enable=NO                        ④
guest_enable=YES                       ⑤
guest_username=vuser                   ⑥
listen=YES                             ⑦
Listen_ipv6=NO                         ⑧
pam_service_name=vsftpd                9
```

任务14-5 设置vsftp虚拟账号

以上代码中其后带序号的各行功能说明如下。

① 为了保证服务器的安全，关闭匿名访问，以及其他匿名相关设置。

② 虚拟账号会映射为服务器的系统账号，所以需要开启本地账号的支持。

③ 锁定账户的根目录。

④ 关闭用户的写权限。

⑤ 开启虚拟账号访问功能。

⑥ 设置虚拟账号对应的系统账号为vuser。

⑦ 设置FTP服务器为独立运行。

⑧ 配置vsftp使用的PAM模块为vsftpd。

任务14-5 设置vsftp虚拟账号

5．设置防火墙放行和SELinux允许，重启vsftpd服务

6．在Client1上测试

使用虚拟账号user2、user3登录FTP服务器，进行测试，会发现虚拟账号登录成功，并显示FTP服务器目录信息。

```
[root@Client1 ~]# ftp 192.168.10.1
Connected to 192.168.10.1 (192.168.10.1).
220 (vsFTPd 3.0.2)
Name (192.168.10.1:root): user2
……
```

任务14-5 设置vsftp虚拟账号

7．补充服务器端vsftp的主被动模式配置

（1）主动模式配置

```
Port_enable=YES //开启主动模式
Connect_from_port_20=YES //指定当主动模式开启的时候，是否启用默认的20端口监听
Ftp_date_port=%portnumber% //上一选项使用NO参数时指定数据传输端口
```

（2）被动模式配置

```
connect_from_port_20=NO
PASV_enable=YES //开启被动模式
PASV_min_port=%number% //被动模式最低端口
PASV_max_port=%number% //被动模式最高端口
```

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FTP服务器

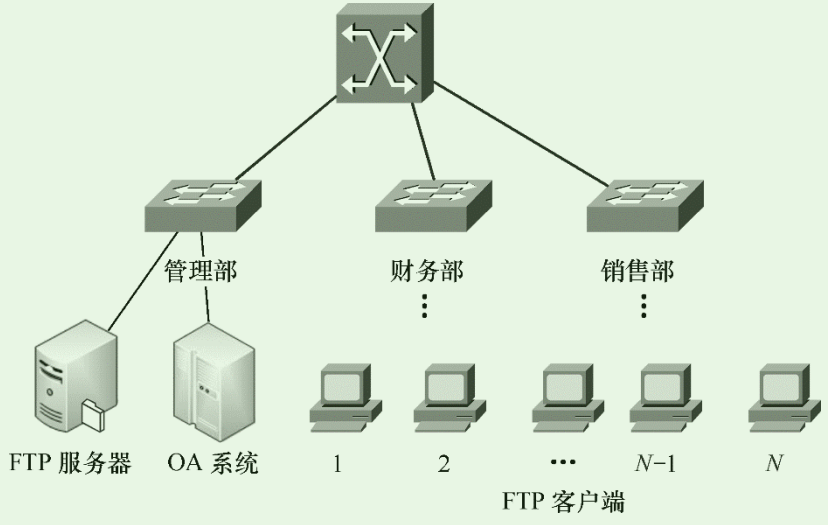
配置与管理FTP服务器

1.视频学习

配置与管理FTP服务器

2．项目背景

某企业的网络拓扑图如图14-3所示。该企业想构建一台FTP服务器，为企业局域网中的计算机提供文件传送任务，为财务部门、销售部门和OA系统提供异地数据备份。要求能够对FTP服务器设置连接限制、日志记录、消息、验证客户端身份等属性，并能创建用户隔离的FTP站点。



配置与管理FTP服务器

3．深度思考

在观看视频时思考以下几个问题。

（1）如何使用service vsftpd status命令检查vsftp的安装状态?

（2）FTP权限和文件系统权限有何不同？如何进行设置?

（3）为何不建议对根目录设置写权限?

（4）如何设置进入目录后的欢迎信息?

（5）如何锁定FTP用户在其宿主目录中?

（6）user_list和ftpusers文件都存有用户名列表，如果一个用户同时存在两个文件中，最终的执行结果是怎样的?

THANKS