# 项目八 FTP服务部署

我们在企业内部经常会需要共享文件，FTP服务可以很好的满足这个需求。FTP服务基于TCP/IP协议，大多数系统都支持FTP协议。通过本项目的学习了解FTP的工作原理，学会安装和配置vsftp服务。

从本项目可以学习到：

* FTP服务的工作原理
* vsftp服务的安装与配置
* vsftp本地用户隔离配置
* vsftp虚拟用户配置

本项目建议课时：6课时。

## 8.1 FTP服务器概述

FTP（File Transfer Protocol）服务能够使文件通过网络从一台主机传送到另外一台主机。且不受计算机和操作系统类型的限制。无论是PC、服务器、大型机，还是IOS、Linux、Windows操作系统，只要通信双方都支持协议FTP，就可以进行文件的传送。

#### 8.1.1 FTP服务的工作工程

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（比如1031端口）。

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。

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（比如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。当数据传输完毕后，这两个端口会自动关闭。

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。

整个过程如图8.1.1所示。

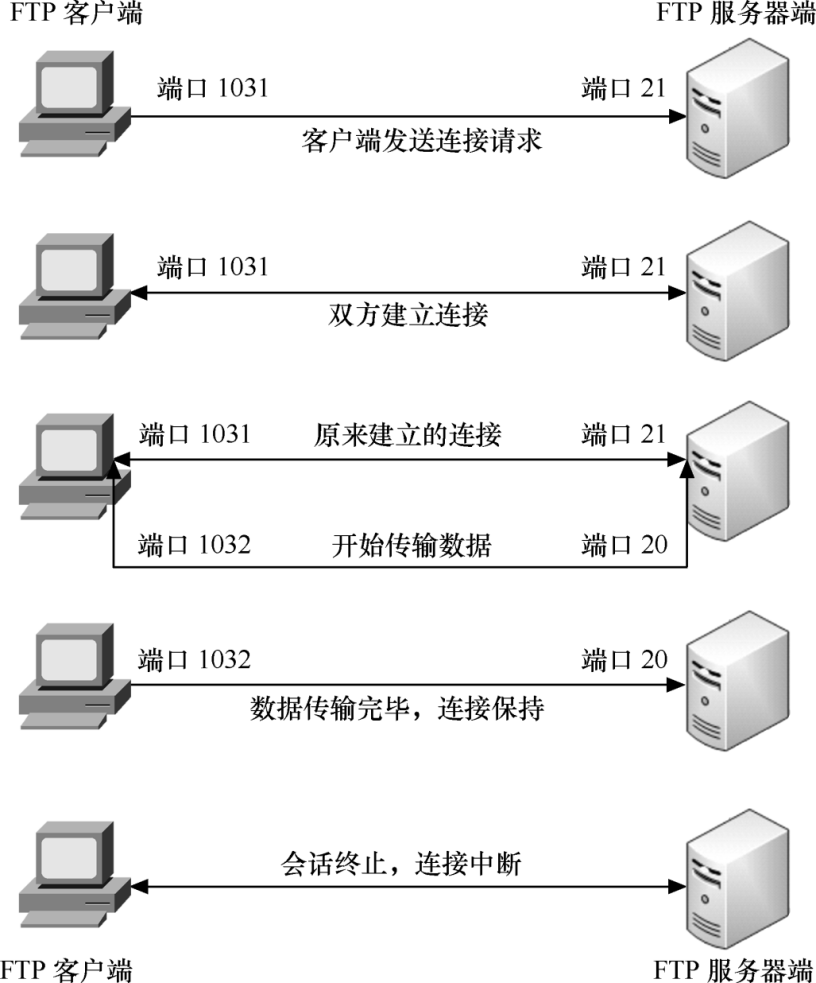


图8.1.1

#### 8.1.2 FTP服务三类用户

* 匿名用户：匿名用户在登录FTP服务器时不需要账号密码就能访问服务器。一般匿名用户的用户名为ftp 或者anonymous。
* 本地用户：本地用户是指具有本地登录权限的用户。这类用户在登录FTP服务器时，所用的登录名为本地用户名，采用的密码为本地用户的口令。登录成功之后进入本地用户的家目录。
* 虚拟用户：虚拟用户只具有从远程登录FTP服务器的权限。虚拟用户不具有本地登录权限。虚拟用户的用户名和口令都是由用户口令库指定。一般采用PAM进行认证。

## 8.2 vsftp服务的安装与配置

vsftp（Very Secure FTP）是一个基于GPL发布的类Unix系统上使用的FTP服务器软件。安全性是编写vsftp的初衷，除了这与生俱来的安全特性以外，高速与高稳定性也是vsftp的两个重要特点。本节主要介绍vsftp服务的安装与配置。

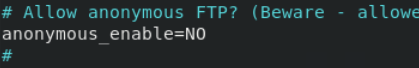
#### 8.2.1 vsftp服务的配置文件说明

表8.2.1列出了vsftp服务相关的目录和配置文件：

表8.2.1

|  |  |
| --- | --- |
| **配置文件的名称** | **存放位置** |
| 服务目录 | /etc/vsftpd |
| 主配置文件 | /etc/vsftpd/vsftpd.conf |
| 默认vsftp主目录路径 | /var/ftp |
| 默认vsftp匿名用户路径 | /var/ftp/pub |
| 在该文件中列出的用户清单将不能访问vsftp服务器 | /etc/vsftpd/ftpusers |
| 用于vsftp的访问控制 | /etc/vstpd/user\_list |

/etc/vsftpd/vsftpd.conf主配置文件不区分大小写，在该文件中以“＃”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8.2.2列出了部分配置文件内容。



**配置文件参数**

**注释行**

图8.2.2

表8.2.3列出/etc/vsftpd/vsftpd.conf主配置文件中各项参数的功能。

表8.2.3

|  |  |
| --- | --- |
| **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] | 是否将用户权限锁定在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 |

当/etc/vsftpd/vsftpd.conf文件中的“userlist\_enable”和“userlist\_deny”的值都为 “YES时”，在/etc/vstpd/user\_list文件中列出的用户不能访问FTP服务器。

当/etc/vsftpd/vsftpd.conf文件中的“userlist\_enable”的取值为YES而“userlist\_deny”的取值为NO时，只有/etc/vstpd/user\_list文件中列出的用户才能访问vsftp服务器。

#### 8.2.2安装vsftp服务

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

查询系统是否已经安装了vsftp服务。输入命令后没有任何输出表示没有安装。

rpm -qa | grep vsftpd

安装vsftpd服务

yum install -y vsftpd

使用命令“rpm -qa | grep vsftp”检查vsftp安装是否成功，如图8.2.4所示。

Screenshot 2022-08-02 at 12.23.41

图8.2.4

启动vsftpd服务

systemctl start vsftpd

设置vsftpd服务为开机自动启动

systemctl enable vsftpd

添加防火墙条目放行vsftpd服务

firewall-cmd --permanent --add-service=ftp

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

#### 8.2.3 配置简单的vsftp服务

1.实例说明

现在有一台FTP服务器，要求服务器能满足上传文件、创建目录等功能。允许匿名用户上传和下载文件，将匿名用户的根目录设置为/var/ftp。允许本地用户user1、user2和user3登录FTP服务器，本地用户更目录为/var/ftp/users。

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

2.实验环境

表8.2.5列出了实验需要用到的虚拟机

表8.2.5

|  |  |  |
| --- | --- | --- |
| **角色** | **操作系统** | **IP地址** |
| vsftp服务器 | Centos8.3 | 192.168.107.95 |
| 访问客户端 | Centos8.3 | 192.168.107.96 |

3.具体步骤

建立user1 、user2和user3本地用户作为FTP账号，并将三个用户的密码设置为和用户名相同。操作如同8.2.6所示。

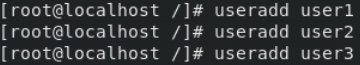


图8.2.6

按照表8.2.7所示，修改主配置文件/etc/vsftpd/vsftpd.conf中的参数。

|  |  |
| --- | --- |
| **配置文件参数** | **作用** |
| 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 |
| local\_enable=YES | 允许本地用户登录 |
| local\_root=/opt/ftp/users | 设置本地用户的ftp根目录为/opt/ftp/users |
| write\_enable=YES | 对登录用户开启写权限 |
| local\_umask=022 | 本地用户的文件生成掩码为022 |

表8.2.7

创建本地用户user1、user2、user3的根目录/opt/ftp/users。修改/opt/ftp/users的目录的权限，为“其他人”添加写入权限。并在/opt/ftp/users目录下新建文件testfile文件用于测试。操作如图8.2.8所示。

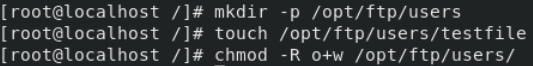


图8.2.8

在/var/ftp/pub目录下为匿名用户建立测试文件testfile2文件,并修改/var/ftp/pub目录的权限，为“其他人”添加写权限。操作如图8.2.9所示。

Screenshot 2022-08-03 at 10.32.42

图8.2.9

**注意：使用匿名登入时, 所登入的目录默认为/var/ftp。vsftp服务不能将根目录的权限设置为777。所以将/var/ftp目录下的共享目录pub权限放开，用来存放匿名用户的文件。**

配置完成后使用如下命令重启vsftp服务。

systemctl restart vsftpd

在客户端上使用ftp工具登陆vsftp服务器测试。通过YUM来安装ftp工具。操作如图8.2.10所示。

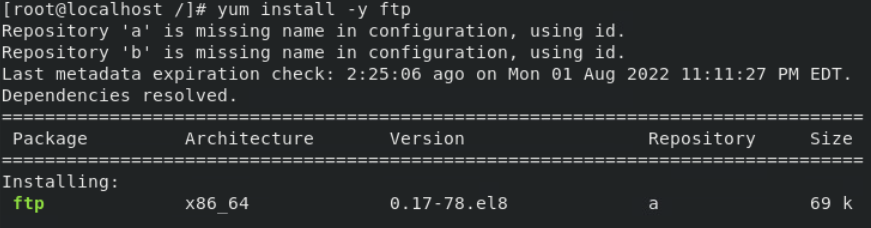
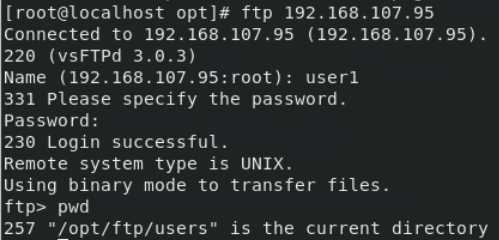


图8.2.10

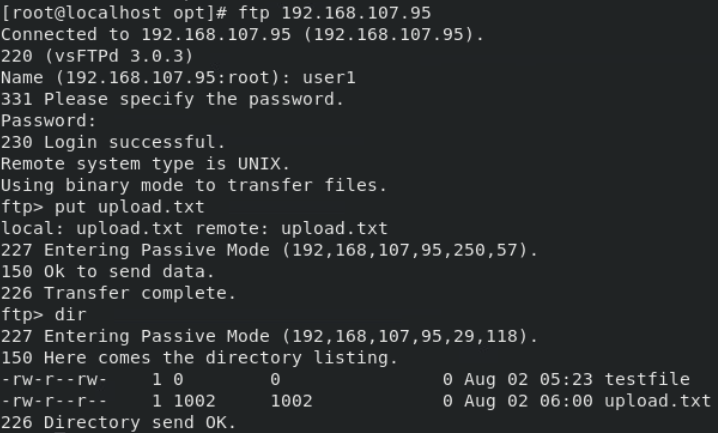
使用命令“ftp 服务器地址”访问vsftp服务器。本例中访问vsftp服务器的命令为“ftp 192.168.107.95”。输入user1的用户名和密码后就可以登陆vsftp服务器。操作如图8.2.11所示。



**使用pwd命令查看当前登陆的目录为/opt/ftp/users**

图8.2.11

在/opt目录下新建一个upload.txt文件。 测试本地用户user1的上传权限，将/opt/upload.txt上传到vsftp服务器。操作如图8.2.12所示。



**upload.txt文件上传成功**

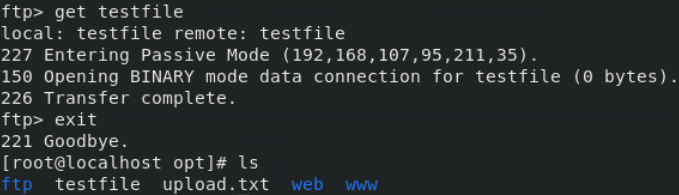
**dir命令用于查看当前**

**目录下的所有文件**

**使用put命令上传文件**

图8.2.12

使用user1用户登陆，下载文件testfile到/opt目录下。操作如图8.2.13所示。



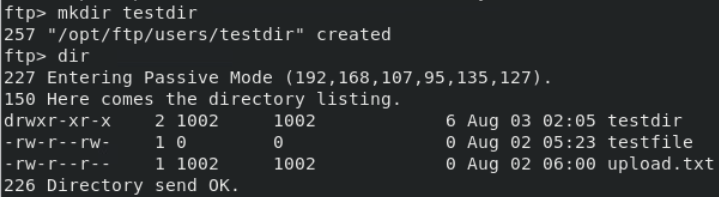
**使用exit命令退出ftp工具**

**使用get命令下载文件**

图8.2.13

**testfile文件下载成功**

使用user1用户登陆，建立一个名为testdir的目录，用于测试新建目录功能是否可用。操作如图8.2.14所示.

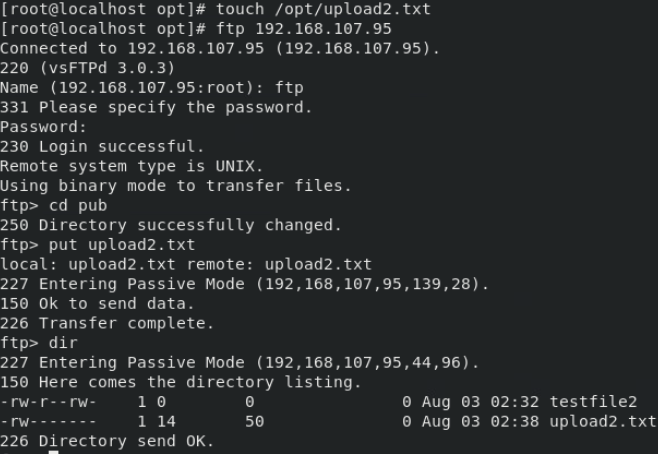


**testdir目录创建成功**

**使用mkdir命令创建目录testdir**

图8.2.14

在客户机的/opt目录下创建文件upload2.txt文件，使用匿名用户ftp登陆vsftpD服务器，密码为空，上传/opt/upload2.txt文件，测试匿名用户上传功能。操作如图8.2.15所示。

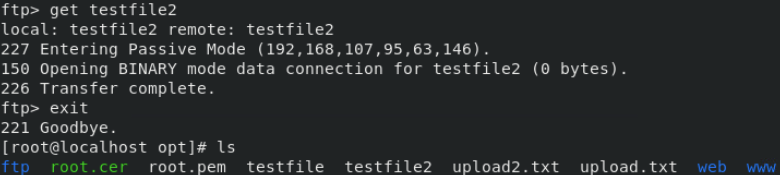


**upload2.txt文件上传成功**

**使用cd命令进入你用户的共享目录**

图8.2.15

使用匿名用户ftp登陆vsftpD服务器，下载文件testfile2到客户机的/opt目录下，测试匿名用户下载功能。操作如图8.2.16所示。

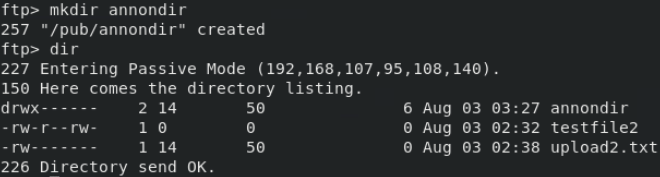


**testfile2文件下载成功**

**使用get命令下载testfile2文件**

图8.2.16

使用匿名用户ftp登陆vsftpD服务器，新建目录annondir。操作如图8.2.17所示。



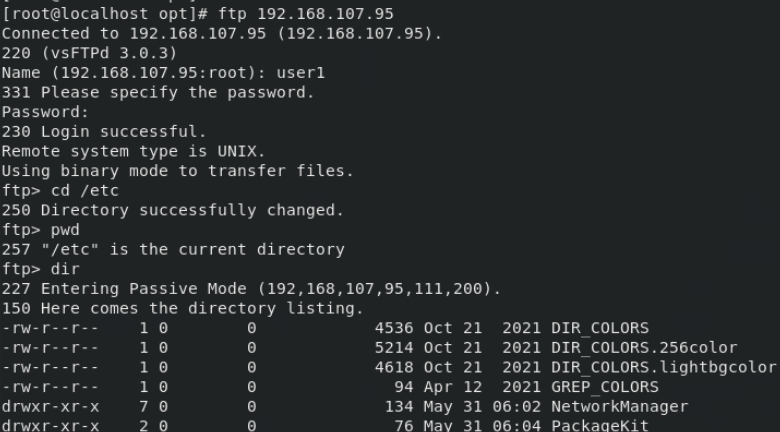
**创建annondir目录成功**

图8.2.17

#### 8.2.5 配置vsftp服务家目录锁定

1.目录锁定概述

在vsftp服务的配置中，如果不做目录锁定，默认登陆的用户可以随意切换有权限访问的目录。让vsftp用户随意的切换目录是非常不安全的操作。在前面的例子中，我么可以使用cd命令切换到/etc目录下。操作如图8.2.18。



**成功切换到/etc目录下**

图8.2.18

表8.2.19列出了vsftp服务家目录锁定的参数选项。

表8.2.19

|  |  |
| --- | --- |
| **参数** | **作用** |
| chroot\_local\_user=[YES|NO] | 是否将所有用户限制在主目录,YES为启用,NO禁用 |
| chroot\_list\_enable＝[YES|NO] | 是否启动限制用户的名单,YES为启用 ,NO禁用 |
| chroot\_list\_file=/etc/vsftpd/chroot\_list | 限制用户名单路径 |
| allow\_writeable\_chroot=[YES|NO] | 所有的用户都将拥有chroot权限 |

下面介绍两种目录锁定的操作：

* “chroot\_local\_user=YES”，其他用户都被限定在固定目录内。即列表（/etc/vsftpd/chroot\_list）内用户自由，列表（/etc/vsftpd/chroot\_list）外用户受限制。
* “chroot\_local\_user=NO”，其他用户都可自由转换目录。即列表（/etc/vsftpd/chroot\_list）内用户受限制，列表（/etc/vsftpd/chroot\_list）外用户自由。

2.配置实例

1）实例说明

将8.2.4实验中的user1和user2用户的根目录限制为/opt/ftp/users，不能进入该目录以外的任何目录。user3用户账号不做限制。

开始配置之前需要预先配置好Linux虚拟机的IP地址，安装好、vsftp服务、在防火墙放行vsftp服务并且关闭Selinux。

出于安全性考虑，本例使用第一种锁定方式完成下面的配置。

2）具体步骤

修改主配置文件/etc/vsftpd/vsftpd.conf中目录锁定的配置。操作如图8.2.20所示。

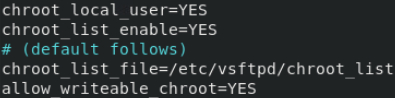


图8.2.20

在/etc/vsftpd/目录中创建文件chroot\_list并在文件中添加用户user3。操作如图8.2.21所示。

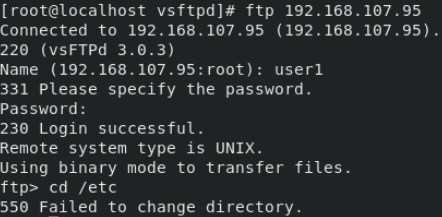
Screenshot 2022-08-03 at 11.07.26

图8.2.21

配置完成后使用如下命令重启vsftp服务。

systemctl restart vsftpd

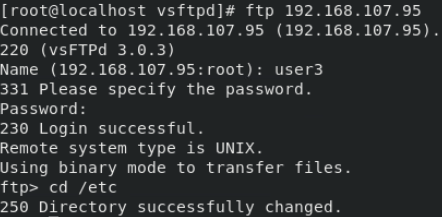
使用user1用户测试目录锁定，操作如图8.2.22。



**user1用户切换目录失败**

图8.2.22

使用“user3”用户测试目录锁定，操作如图8.2.23。



**user3用户切换目录成功**

图8.2.23

## 8.3 本地用户隔离

FTP用户隔离通过将用户限制在自己的目录中，来防止用户查看或修改其他用户的文件内容。因为顶层目录就是FTP服务的根目录，用户无法浏览目录树的上一层。在特定的站点内，用户能创建、修改或删除文件和文件夹。FTP用户隔离是站点属性，而不是服务器属性，无法为每个FTP站点启动或关闭该属性。本节主要介绍vsftp服务本地用户隔离配置。

#### 8.3.1 配置vsftp本地用户隔离

1.实例说明

创建user1和user2两个本地用户，两个用户的主目录分别为/opt/ftp/user1和/opt/ftp/user2。要求user1和user2用户可以在自己的目录中实现上传和下载，其他目录没有权限。

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

2.实验环境

表8.3.1列出了实验需要用到的虚拟机

表8.3.1

|  |  |  |
| --- | --- | --- |
| **角色** | **操作系统** | **IP地址** |
| vsftp服务器 | Centos8.3 | 192.168.107.95 |
| 访问客户端 | Centos8.3 | 192.168.107.96 |

3.具体步骤

创建user1和user2用户作为FTP的账号，密码与用户名相同。操作如图8.3.2所示。

Screenshot 2022-08-03 at 11.56.21

图8.3.2

分别建立user1和user2对应的用户主目录/opt/ftp/user1和/opt/ftp/user2。操作如图8.3.3所示。

Screenshot 2022-08-03 at 14.10.22

图8.3.3

分别修改user1和user2对应的用户主目录的所有者和属组分别为user1和user2。操作如图8.3.4所示。

Screenshot 2022-08-03 at 14.14.13

图8.3.4

在user1和user2对应的用户主目录中分别创建test1和test2测试文件。操作如图8.3.5所示。

Screenshot 2022-08-03 at 14.16.23

图8.3.5

创建用户配置文目录为/etc/vsftpd/vsftpd\_user\_conf/，并且在目录中分别创建user1和user2用户配置文件。操作如图8.3.6所示。

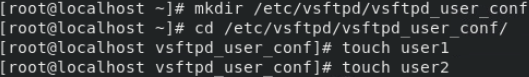


图8.3.6

在user1和user2的用户配置中添加主目录参数。操作如图8.3.7所示。

Screenshot 2022-08-03 at 14.28.08

图8.3.7

**local\_root参数用于指定用户的根目录路径**

修改主配置文件/etc/vsftpd/vsftpd.conf。添加参数如表8.3.8所示。

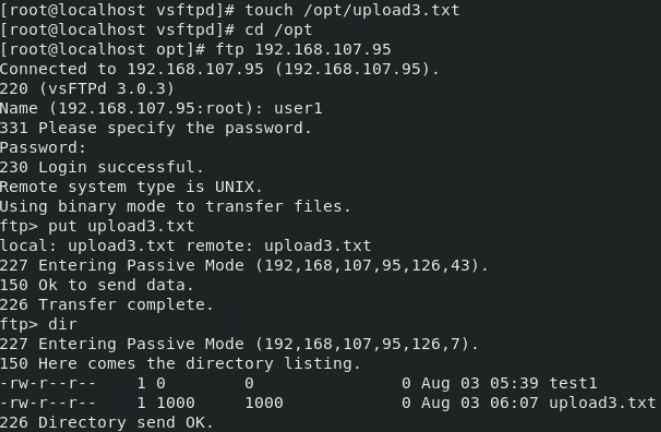
表8.3.8

|  |  |
| --- | --- |
| **参数** | **作用** |
| userlist\_enalbe=YES | 开启用户列表 |
| userlist\_deny=YES | 如果为NO，则只能是user\_list中存在的用户才可以登陆FTP |
| userlist\_file=/etc/vsftpd/user\_list | 用户列表文件路径 |
| user\_config\_dir=/etc/vsftpd/vsftpd\_user\_conf | 用户配置文件路径 |
| allow\_writeable\_chroot=YES | 所有的用户都将拥有chroot权限 |

配置完成后使用如下命令重启vsftp服务。

systemctl restart vsftpd

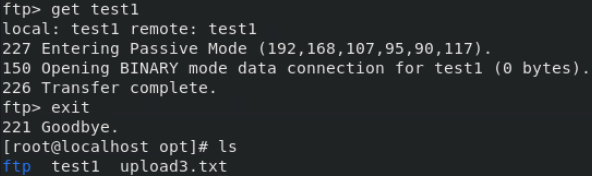
在/opt目录下新建一个upload3.txt文件。将/opt/upload3.txt上传到vsftp服务器，测试本地用户user1的上传权限。操作如图8.3.9所示。



**上传upload3.txt文件成功**

图8.3.9

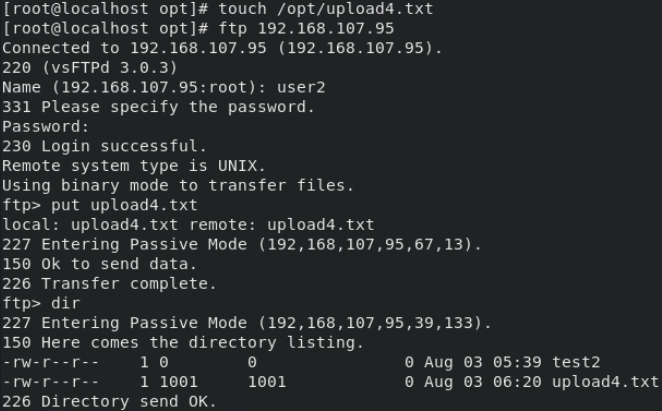
使用user1用户登陆，下载文件test1到/opt目录下。操作如图8.3.10所示。



**下载test1文件成功。**

图8.3.10

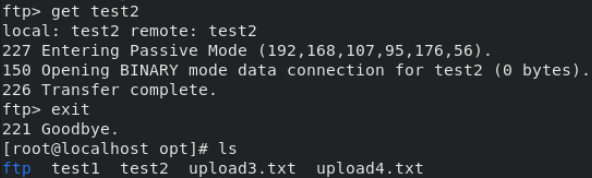
在/opt目录下新建一个upload4.txt文件。将/opt/upload4.txt上传到vsftp服务器，测试本地用户user2的上传权限。操作如图8.3.11所示。



**上传upload4.txt文件成功**

图8.3.11

使用user2用户登陆，下载文件test2到/opt目录下。操作如图8.2.12所示。



**下载test2文件成功。**

图8.2.12

## 8.4 虚拟用户

如果想实现多个用户同时访问某一个目录，同时又要对同一目录下的文件拥有不同的权限，如部分用户只能看，不修改，或者部分用户只能下载不能上传这些权限。

普通用户是无法达到这样的效果，这些设定只能通过vsftp服务中的虚拟用户来进行配置。虚拟用户无需建立本地用户，用户数据全部存在数据库中。由于虚拟用户本身不存在系统中，需要将虚拟用户映射到一个本地用户。

本节主要介绍vsftp服务虚拟用户配置。

#### 8.4.1 配置虚拟用户

1.实例说明

创建虚拟用户vftp1和vftp2，密码均为“123456”。分别对应根目录/opt/ftp/vftp1和/opt/ftp/vftp2。要求vftp1用户可上传可下载，vftp2用户只能下载，不能上传。

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

2.实验环境

表8.4.1列出了实验需要用到的虚拟机

表8.4.1

|  |  |  |
| --- | --- | --- |
| **角色** | **操作系统** | **IP地址** |
| vsftp服务器 | Centos8.3 | 192.168.107.95 |
| 访问客户端 | Centos8.3 | 192.168.107.96 |

3.具体步骤

分别建立vftp1和vftp2对应的用户主目录/opt/ftp/vftp1和/opt/ftp/vftp2。并在目录中分别创建test1和test2测试文件。操作如图8.4.2所示。

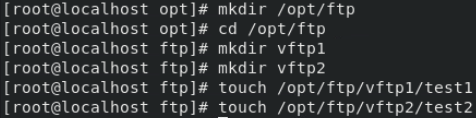


图8.4.2

修改vftp1和vftp2对应根目录的权限为777。操作如图8.4.3所示。

Screenshot 2022-08-03 at 19.01.32

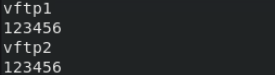
图8.4.3

在/etc/vsftpd目录下建立虚拟用户账号文件vuser.list,操作如图8.4.4所示。

Screenshot 2022-08-03 at 15.43.02

图8.4.4

使用vi工具编辑/etc/vsftpd/vuser.list，添加虚拟用户vftp1和vftp2的帐户信息进入文件。操作如图8.4.5所示。



**vftp2的用户名和密码**

**vftp1的用户名和密码**

图8.4.5

使用命令db\_load在/etc/vsftpd目录下，生成虚拟vsftp用户账号数据库vuser.db。操作如下命令所示。

db load -T -t hash -f /etc/vsftpd/vuser.list /etc/vsftpd/vuserdb.db

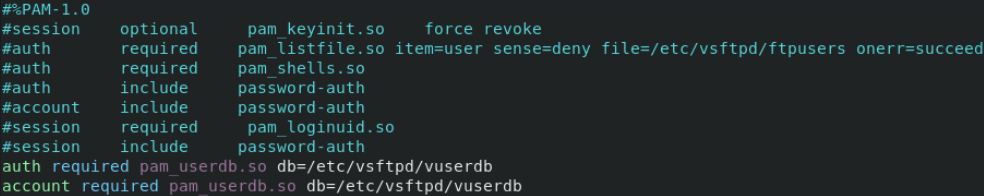
创建一个本地用户vftpuser，用于建立家目录将所有的虚拟用户映射到对应的普通系统用户家目录中对各虚拟用户进行权限控制。操作如下命令所示。

useradd -d /var/ftproot -s /sbin/nologin vftpuser

-d /var/ftproot：用于指定vftpuser用户的家目录为“/var/ftproot”

-s /sbin/nologin：让vftpuser用户不能登陆系统

配置PAM认证让其支持vsftp服务的虚拟用户登陆认证。使用vi工具编辑/etc/pam.d/vsftpd。操作如图8.4.6所示。



**注释掉原来的认证内容，添加2行对应虚拟用户的帐户认证**

**注意：vuserdb文件不需要后缀名**

图8.4.6

修改主配置文件/etc/vsftpd/vsftpd.conf。添加参数如表8.4.7所示。

表8.4.7

|  |  |
| --- | --- |
| **参数** | **作用** |
| pam\_service\_name=vsftpd | 开启pam认证支持 |
| anonymous\_enable=no | 禁止匿名用户登陆 |
| guest\_enable=yes | 启用虚拟账号 |
| guest\_username=vftpuser | 配置虚拟账号映射的本地账号 |
| user\_config\_dir=/etc/vsftpd/vuser\_dir | 用户配置文件路径 |
| allow\_writeable\_chroot=YES | 所有的用户都将拥有chroot权限 |

在/etc/vsftpd/vuser\_dir目录下，为vftp1和vftp2虚拟用户建立独立的配置文件。操作如图8.4.8所示。

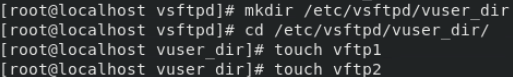


图8.4.8

在/etc/vsftpd/vuser\_dir/vftp1中添加对虚拟用户vftp1的配置。如表8.4.9列出了配置虚拟用户配置文件中的参数。

表8.4.9

|  |  |
| --- | --- |
| **参数** | **作用** |
| write\_enable=[YES|NO] | 开启虚拟账号写入权限 |
| anon\_world\_readable\_only=[YES|NO] | 当为YES时，文件夹的“o”权限必须有只读权限才能下载，若设置为NO,则只要所有者有读权限即可下载 |
| anon\_upload\_enable=[YES|NO] | 开启虚拟账号上传权限 |
| anon\_mkdir\_write\_enable=[YES|NO] | 开启虚拟账号建立目录权限 |
| anon\_other\_write\_enable=[YES|NO] | 开启虚拟账号删除权限 |
| local\_root=目录 | 虚拟用户对应的ftp根目录路径，如果没有这项则默认指向映射的本地用户目录 |

如图8.4.10列出了虚拟用户vftp1的配置文件配置。

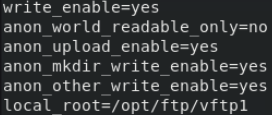
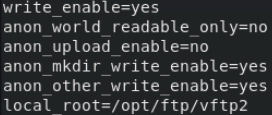


图8.4.10

在/etc/vsftpd/vuser\_dir/vftp2中添加对虚拟用户vftp2的配置。操作如图8.4.11所示。



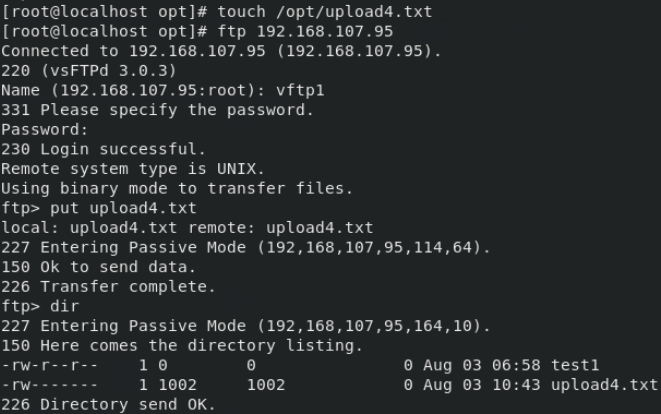
**本例要求vftp2用户无上传权限，所以将上传参数改为“no”。**

图8.4.11

配置完成后使用如下命令重启vsftp服务。

systemctl restart vsftpd

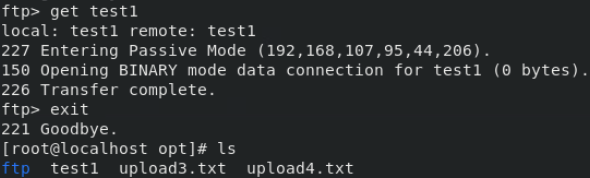
在/opt目录下新建一个upload4.txt文件。 将/opt/upload4.txt上传到vsftp服务器,测试虚拟用户vftp1的上传权限。操作如图8.4.12所示。



**上传upload4.txt文件成功**

图8.4.12

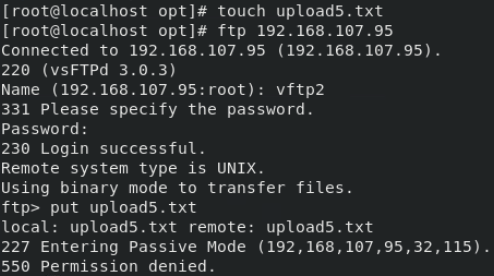
使用vftp1用户登陆，下载文件test1到/opt目录下。操作如图8.4.13所示。



**下载test1文件成功**

图8.4.13

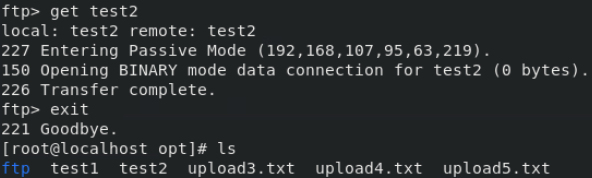
在/opt目录下新建一个upload5.txt文件，将/opt/upload4.txt上传到vsftp服务器，测试虚拟用户vftp2的上传权限。操作如图8.4.14所示。



**上传upload5.txt文件失败**

图8.4.14

使用vftp2用户登陆，下载文件“test2”到/opt目录下。操作如图8.4.15所示。



**下载test2文件成功**

图8.4.15

#### 章节测试

1.操作题

1）公司内部现在有一台FTP服务器，FTP主要用于存放公司的内部文件。要求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。本地用户允许team1、team2和user1账号登录FTP服务器，但不能登录本地系统，并将这team1和team2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。本地用户user1账号不做目录限制。根据需求完成如下配置：

（1）请配置FTP服务器。

（2）本地用户测试：使用team1用户不能转换目录，可以上传和下载，能建立新文件夹。

（3）本地用户测试：使用user1用户能转换目录。

（4）匿名用户测试：使用匿名用户能上传和下载文件，建立新文件夹。