

ftp服务

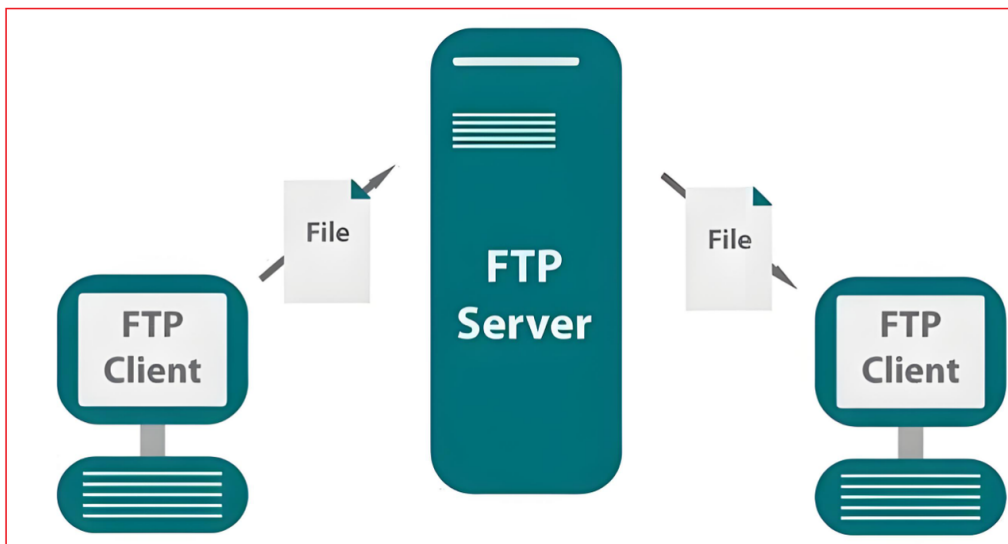
作者：牟建波 (1353429820@qq.com)

时间：2025-05-31

描述：日常自学笔记

1 文件传输协议FTP

FTP (File Transfer Protocol)：是一种用于在网络上进行文件传输的协议，允许用户通过客户端和服务端之间上传、下载文件

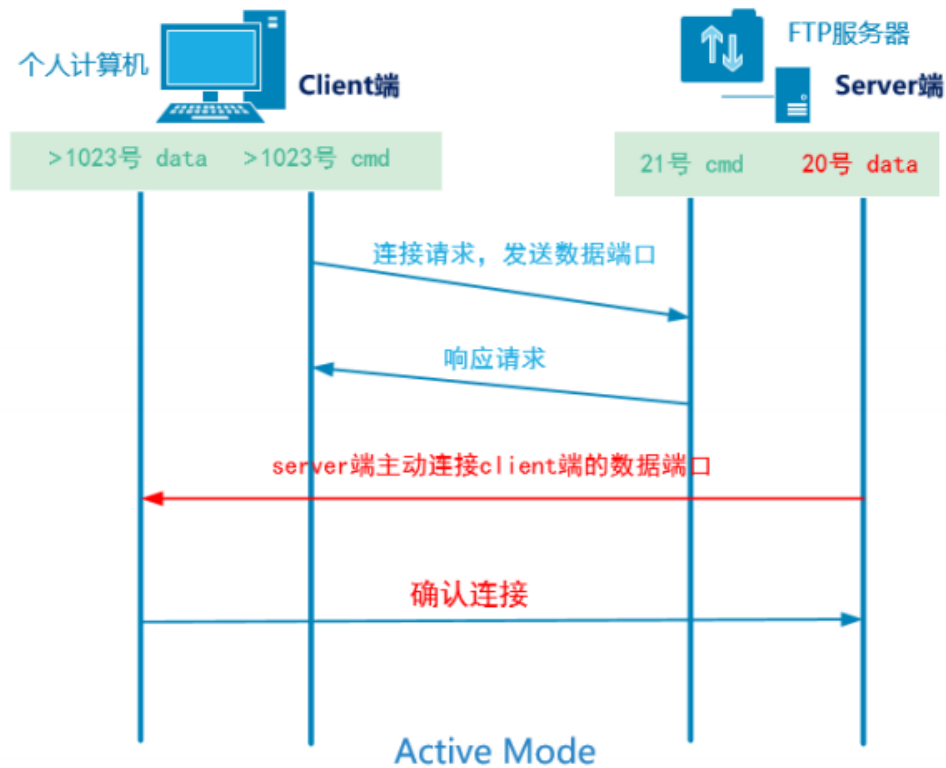


2.FTP两种工作模式

主动模式 (Active Mode)：在主动模式下，**客户端** 发起控制连接到服务器，而服务器用来传输数据的端口是由 **服务器** 发起的连接到客户端

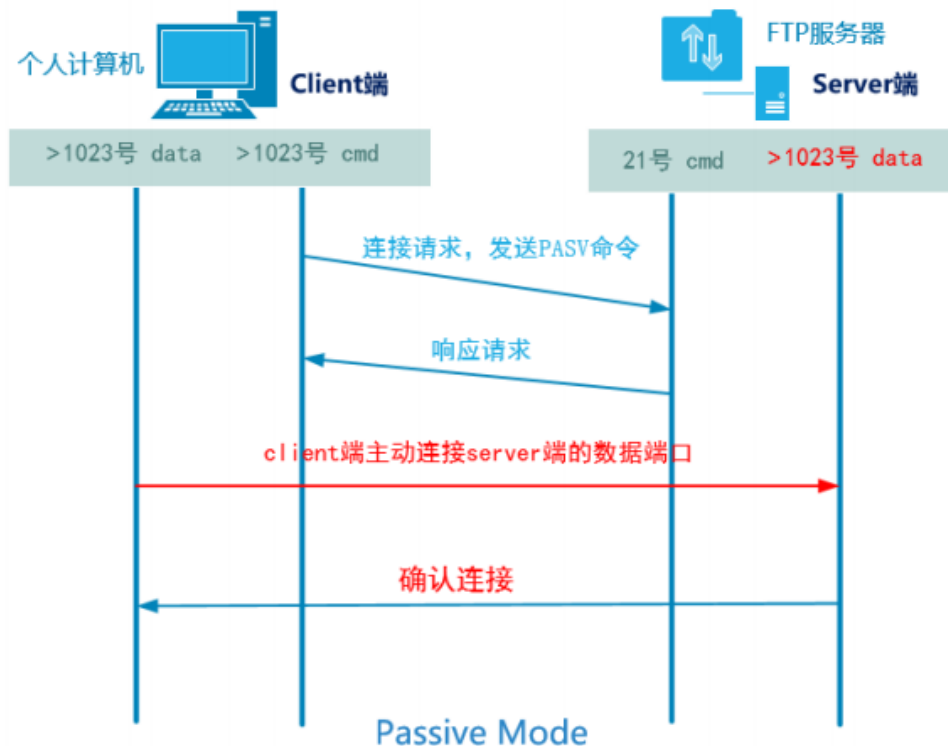
- 客户端与服务器建立连接，使用 21端口
- 客户端准备接收数据，使用随机端口（通常是20以外端口）

- 服务器连接到客户端端口后，从 20端口 发起一个连接到客户端指定的端口，用于数据传输



☁ **被动模式 (Passive Mode)**：在被动模式下，**客户端** 仍然发起控制连接，但在传输数据时，**客户端** 会请求服务器开放一个随机的端口来进行数据传输，服务器只负责监听数据连接，客户端主动发起连接。**FTP主要使用被动模式**

- 客户端与服务器建立连接，使用 21端口
- 客户端请求服务器在随机端口上等待数据连接
- 服务器响应并告知客户端该数据端口号
- 客户端随后向该端口发起连接进行数据传输



特性	主动模式 (Active Mode)	被动模式 (Passive Mode)
控制连接	客户端连接服务器的端口 21	客户端连接服务器的端口 21
数据连接	服务器从端口 20 发起连接到客户端的随机端口	客户端连接服务器提供的随机端口
适用网络环境	客户端需要有公网 IP 或不在防火墙后	客户端位于 NAT 或防火墙后时较为适用
防火墙问题	可能无法穿越客户端防火墙或 NAT	由于客户端发起数据连接, 较易穿越防火墙

3.FTP服务器搭建

☁ 环境准备：两台服务器，一台用于客户端(node1)、一台用于服务端(node2)

☁ 服务端node2配置

代码块


```
1 # 1.在node2上安装vsftpd服务 (FTP服务器)
2 [node2]
```

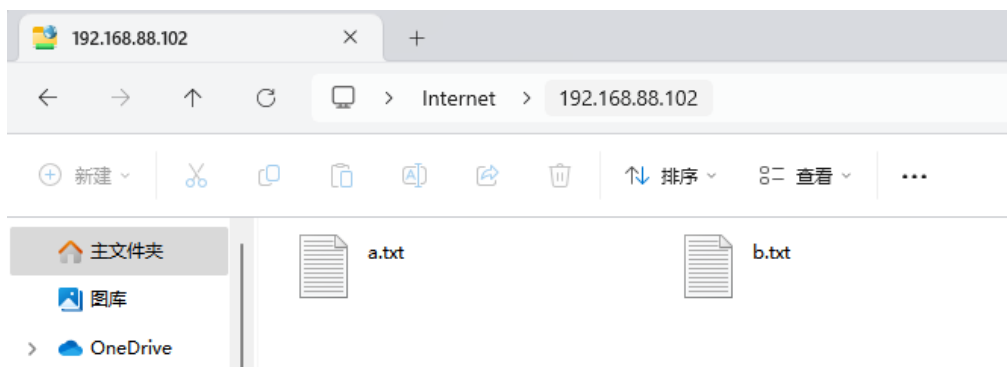
```
3  dnf install -y vsftpd
4
5  # 2.启动并配置vsftpd服务
6  systemctl start vsftpd
7  systemctl enable --now vsftpd
8  systemctl status vsftpd
9
10 # 3.配置防火墙
11 firewall-cmd --zone=public --add-service=ftp --permanent
12 firewall-cmd --reload
13
14 # 4.基本访问配置
15 # 环境：创建一个用于共享的目录并创建几个文件
16 mkdir -p /anon
17 echo 'hello' >> /anon/a.txt
18 echo 'hi' >> /anon/b.txt
19 # 修改配置
20 vim /etc/vsftpd/vsftpd.conf
21 # 设置以下几个配置项：
22 anonymous_enable=YES          # 允许匿名用户访问
23 anon_root=/anon              # 设置匿名用户默认的根目录
24 anon_upload_enable=YES       # 允许匿名用户上传文件
25 anon_mkdir_write_enable=YES  # 运行匿名用户创建文件夹
26 anon_other_write_enable=YES  # 允许匿名用户删除和重命名文件
27 # 注意：修改配置文件，记得重启下FTP服务
28 systemctl restart vsftpd
29 # 校验：
30 systemctl status vsftpd
```

客户端node1配置

代码块

```
1  # 1.在node1上安装FTP服务器
2  dnf install -y lftp
3  # 说明：lftp是命令行FTP客户端，FileZilla是图形化客户端
4
5  # 2.连接FTP服务器
6  lftp ftp://192.168.88.102    # 连接node2
```

 windows浏览器访问：FTP被建立后，都可以用 `ftp://服务器IP地址` 进行访问



4.禁止匿名用户访问

代码块

```
1 # 1.在node2修改FTP相关配置
2 vim /etc/vsftpd/vsftpd.conf
3 # 修改以下配置
4 anonymous_enable=NO # 禁用匿名用户访问
5 local_enable=YES # 运行本地用户登录
6 write_enable=YES # 运行写入操作（上传文件）
7 # 保存文件并退出，重启服务
8 systemctl restart vsftpd
9
10 # 2.创建一个普通用户用于后续访问FTP
11 # 由于开启了允许本地用户访问，但系统仅一个root超级用户，权限过大，FTP无法直接使用root访问，所以需要创建普通用户来访问
12 useradd smartgouser
13 echo 123 | passwd --stdin smartgouser
14
15 # 3.node1客户端访问查看
16 lftp ftp://smartgouser:123@192.168.88.102
```

```
[rsync@node1 ~]$ lftp ftp://smartgouser:123@192.168.88.102
lftp smartgouser@192.168.88.102:~> ls
lftp smartgouser@192.168.88.102:~> pwd
ftp://smartgouser:123@192.168.88.102/%2Fhome/smartgouser
lftp smartgouser@192.168.88.102:~>
```

```
lftp smartgouser@192.168.88.102:/> cd /tmp
cd ok, cwd=/tmp
lftp smartgouser@192.168.88.102:/tmp> ls
drwx----- 3 0 0 17 Nov 08 10:07 systemd-private-d58857b694ef4876af8171f11fb62255-chronyd.service-0bthys
drwx----- 3 0 0 17 Nov 08 10:07 systemd-private-d58857b694ef4876af8171f11fb62255-dbus-broker.service-u0qC5g
drwx----- 3 0 0 17 Nov 08 10:07 systemd-private-d58857b694ef4876af8171f11fb62255-irqbalance.service-8F0t0o
drwx----- 3 0 0 17 Nov 08 10:07 systemd-private-d58857b694ef4876af8171f11fb62255-kdump.service-fsyDWE
drwx----- 2 0 0 6 Nov 08 10:01 vmware-root_765-4248156194
drwx----- 2 0 0 6 Nov 08 10:07 vmware-root_769-4248090657
drwx----- 2 0 0 6 Nov 08 07:27 vmware-root_771-4256545187
```

5.禁锢在指定的文件数据目录中

```

1  # 1.在node2中创建一个本地用户的数据目录
2  [node2]
3  mkdir -p /data/kefu          # 该目录将作为共享上下传目录
4
5  # 2.修改配置文件
6  vim /etc/vsftpd/vsftpd.conf
7  # 添加以下内容
8  local_root=/data/kefu      # 设置默认访问的路径地址 ,如果不指定,默认访问的是该用户的家目录
9  # 修改以下内容: 前面的#去除即可
10 chroot_local_user=YES      # 限制所有本地用户(即服务器上的普通用户)只能访问他们的 home 目录
11 # 保持退出后,重启vsftpd服务
12 systemctl restart vsftpd
13
14 # 3.创建用户,指定用户的家目录为禁锢的数据目录下
15 useradd -m ftpuser
16 echo 123 | passwd --stdin ftpuser
17
18 # 4.客户端访问测试
19 lftp ftp://ftpuser:123@192.168.88.102

```

```

local_root=/data/kefu
chroot_local_user=YES
#chroot_list_enable=YES
# (default follows)
#chroot_list_file=/etc/vsftpd/chroot_list
#

```

```

rsync[node1 ~]$ lftp ftp://ftpuser:123@192.168.88.102
ftp ftpuser@192.168.88.102:~> ls
-rw-r--r--  1 0      0              6 Nov 11 05:29 a.txt
ftp ftpuser@192.168.88.102:/>
ftp ftpuser@192.168.88.102:/> pwd
ftp://ftpuser:123@192.168.88.102/
ftp ftpuser@192.168.88.102:/> cd /tmp
d: Access failed: 550 Failed to change directory. (/tmp)
ftp ftpuser@192.168.88.102:/>

```

☁ 某些特殊的用户需要具备访问其他目录的权限, 如何解决?

代码块

```

1  # 1.修改配置文件
2  vim /etc/vsftpd/vsftpd.conf
3
4  # 2.修改以下配置(打开对应行注释即可)
5  chroot_list_enable=YES      # 开启允许访问其他目录的功能
6  chroot_list_file=/etc/vsftpd/chroot_list  # 设置哪些用户可以例外

```

```
7
8 # 3.编辑/etc/vsftpd/chroot_list文件
9 vim /etc/vsftpd/chroot_list # 直接添加额外的用户名即可
10 zhangsan
11 lisi
12
13 # 4.重启vsftpd, 重新测试
14 systemctl restart vsftpd
```

6.用户名列表使用

☁ 环境：先把禁锢用户数据目录功能关闭（把禁锢操作相关配置前全部加#）

☁ 在 node2 中的 /etc/vsftpd 目录下，有两个文件： ftpusers (黑名单)、 user_list (黑白名单)

- ftpusers 文件： ftpusers 文件用于列出不允许访问 FTP 服务的用户。任何列在这个文件中的用户都将被拒绝登录到 FTP 服务器，即使这些用户的用户名和密码是正确的

```
total 20
-rw----- 1 root root 125 Aug 20 16:47 ftpusers
-rw----- 1 root root 361 Aug 20 16:47 user_list
-rw----- 1 root root 5097 Nov 14 16:20 vsftpd.conf
-rwxr--r-- 1 root root 352 Aug 20 16:47 vsftpd_conf_migrate.sh
[root@node2 vsftpd]# cat ftpusers
# Users that are not allowed to login via ftp
root
bin
daemon
adm
lp
sync
shutdown
halt
mail
news
uucp
operator
games
nobody
[root@node2 vsftpd]#
```

- **user_list文件：** `user_list` 文件的作用和 `ftpusers` 文件相似，但有一些区别。`user_list` 文件控制哪些用户可以访问 FTP 服务，具体取决于配置文件中 `userlist_enable` 和 `userlist_deny` 的设置
 - **userlist_enable=YES** 启用或禁用 `vsftpd` 服务的系统用户列表功能。
 - **userlist_deny=YES** 默认情况下，列在 `user_list` 文件中的用户会被拒绝访问。
 - **userlist_deny=NO** 列在 `user_list` 文件中的用户将被允许访问，除非在 `ftpusers` 中显式禁止。

```

# vsftpd userlist
# If userlist_deny=NO, only allow users in this file
# If userlist_deny=YES (default), never allow users in this file, and
# do not even prompt for a password.
# Note that the default vsftpd pam config also checks /etc/vsftpd/ftpusers
# for users that are denied.
root
bin
daemon
adm
lp
sync
shutdown
halt
mail
news
uucp
operator
games
nobody

```

应用场景：通过这两个文件，可以为FTP服务器设置黑名单和白名单用户

代码块

```

1  # 1.关闭禁锢用户数据目录功能
2  # local_root=/data/kefu
3  # chroot_local_user=YES
4
5  # 2.测试用root直接访问ftp服务：报错，因为FTP默认不允许root访问
6  lftp ftp://root:123456@192.168.99.102 # 输入ls，提醒Login failed: 530
   Permission denied.
7
8  # 3.开启白名单功能
9  vim /etc/vsftpd/vsftpd.conf
10 # 修改以下内容
11 userlist_enable=YES # 开启user_list权限设置功能
12 # 添加以下内容
13 userlist_deny=NO # 开启白名单，运行文件中的用户
14 # 保存以下，重启FTP服务
15 systemctl restart vsftpd
16
17 # 4.在ftpusers(黑名单)文件中去除root用户
18 vim /etc/vsftpd/vsftpd.conf
19
20 # 5.访问FTP服务器
21 lftp ftp://root:123456@192.168.88.102

```



```

[root@node1 ~]# curl http://root.123456@192.168.88.102
lftp root@192.168.88.102:~> ls /
-rw-r--r--    1 0      0          6 Nov 11 04:23 a.txt
drwxr-xr-x    2 0      0          6 Nov 11 04:22 aaa
dr-xr-xr-x    2 0      0          6 Jun 25 14:23 afs
drwxr-xr-x    3 0      0         46 Nov 11 04:32 anon
-rw-r--r--    1 0      0          6 Nov 11 04:23 anona.txt
-rw-r--r--    1 0      0          3 Nov 11 04:23 anonb.txt
-rw-r--r--    1 0      0          3 Nov 11 04:23 b.txt
lrwxrwxrwx    1 0      0          7 Jun 25 14:23 bin -> usr/bin
dr-xr-xr-x   5 0      0        4096 Oct 12 08:44 boot
drwxr-xr-x    3 0      0         18 Nov 14 08:08 data
drwxr-xr-x   20 0      0        3320 Nov 14 12:57 dev
drwxr-xr-x  105 0      0        8192 Nov 14 12:57 etc
drwxr-xr-x    3 0      0         18 Nov 09 05:07 export
drwxr-xr-x    7 0      0         84 Nov 14 07:58 home
lrwxrwxrwx    1 0      0          7 Jun 25 14:23 lib -> usr/lib
lrwxrwxrwx    1 0      0          9 Jun 25 14:23 lib64 -> usr/lib64
drwxr-xr-x    2 0      0          6 Jun 25 14:23 media
drwxr-xr-x    3 0      0         18 Oct 12 08:29 mnt
drwxr-xr-x    2 0      0          6 Jun 25 14:23 opt
dr-xr-xr-x  239 0      0          0 Nov 14 12:57 proc
dr-xr-x---    3 0      0        163 Nov 14 07:35 root
drwxr-xr-x   28 0      0        800 Nov 14 12:57 run
lrwxrwxrwx    1 0      0          8 Jun 25 14:23 sbin -> usr/sbin
drwxr-xr-x    2 0      0          6 Jun 25 14:23 srv
dr-xr-xr-x   13 0      0          0 Nov 14 12:57 sys
drwxrwxrwt   16 0      0        4096 Nov 14 12:58 tmp
drwxr-xr-x   12 0      0        144 Oct 12 08:27 usr
drwxr-xr-x   19 0      0        4096 Oct 12 08:44 var
lftp root@192.168.88.102:~>

```

7.删除FTP服务

代码块

```

1  node1:
2      dnf -y remove lftp
3      dnf clean all
4
5  node2:
6      dnf -y remove vsftpd
7      dnf clean all
8      rm -rf /etc/vsftpd/
9
10     firewall-cmd --permanent --remove-service ftp
11     firewall-cmd --reload
12     firewall-cmd --list-all
13
14     rm -rf /anon
15     userdel -rf smartgouser
16     userdel -rf ftpuser

```

8.常见错误

vsftpd: refusing to run with writable root inside chroot()

```
lftp 192.168.88.102:~> ls
ls: 登录失败: 500 OOPS: vsftpd: refusing to run with writable root inside chroot()
lftp 192.168.88.102:~>
```

代码块

- 1 **说明:** 此错误表示的当前FTP文件系统的根目录的权限过大, 存在写权限, 一般就会爆出如上错误, 因为FTP默认情况下, 不允许文件系统根目录存在写权限, 以保证根目录的文件安全(根目录下可能会放置一些系统文件信息, 担心出现破坏)

```
lftp itheima@192.168.88.102:/anon> rm a.txt
rm: 访问失败: 550 Delete operation failed. (a.txt)
lftp itheima@192.168.88.102:/anon>
```

代码块

- 1 当在ftp中看到550错误的时候, 一般就是当前这个用户没有权限操作这个文件或目录, 如果想要操作, 请赋予相应权限