# 安装ftp服务器

安装vsftpd

# yum install -y vsftpd

===============================================================================

添加用户名，用作ftp匿名访问用户

# useradd ftpuser

给用户名设置密码

# passwd ftpuser

# 配置文件

# cd /etc/vsftpd/

# vim vsftpd.conf

# 允许匿名访问

anonymous\_enable=YES

# 不允许本地用户，如root用户登陆。默认允许

local\_enable=NO

#设置本地用户登录所在的目录。默认配置文件中没有该配置项，本地用户登录FTP服务器后所在的目录为所登录用户的主目录，如：对于root用户，则为/root目录

# local\_root=/home/ftpuser

# 本地用户上传文件权限

local\_umask=022

# 匿名用户上传文件权限

anon\_umask=022

# 允许写入操作，否则不能上传文件

write\_enable=YES

# 允许匿名用户上传文件，需要配合write\_enable=yes

anon\_upload\_enable=YES

# 控制匿名用户对文件和文件夹的删除和重命名(自己添加，没有该配置)

anon\_other\_write\_enable=YES

# 允许匿名用户创建目录

anon\_mkdir\_write\_enable=YES

# ftp工具连接成功提示

ftpd\_banner=Welcome to blah FTP service.

# 所有用户均不能切换到上级目录

chroot\_local\_user=YES

# 是否启动限制用户的名单。YES为启用，NO禁用。默认禁用

chroot\_list\_enable=NO

# /etc/vsftpd/user\_list文件不生效

userlist\_enable=NO

#坑，添加以下配置。不添加此项，文件无法上传。报错：550 Permission denied。新版本vsftpd加入了安全需求，切根不允许写，要添加这个配置并设置为YES才可以

allow\_writeable\_chroot=YES

#匿名用户的根目录。这个非常重要

anon\_root=/usr/local/ftpdir

#匿名用户不要密码就靠这个

no\_anon\_password=YES

# 匿名登录后的使用者

ftp\_username=ftpuser

===============================================================================

# 启动ftp服务器

**注：我这里是把所有防火墙都给关了的**

端口是21(有的人线下装Linux服务器系统时候会安装一个ftp服务器：pure-ftpd，而且默认是开机自启，而且端口也是21端口)

启动之前可以查询是否有ftp服务在跑着，或者查看21端口是否有程序占用

Linux查询某个端口是否被占用：netstat -anp | grep 端口号

通过pid查看对应端口使用者：netstat -antup | grep pid

或者查询管道过滤：ps -ef | grep ftp

===============================================================================

最后ftp服务器启动命令

# systemctl start vsftpd

# 附（坑）

## ftp客户端

下载ftp工具测试连接：

# yum install -y ftp

# ftp localhost

或者cmd连接：

ftp 192.168.163.4

或者客户端工具filezilla连接。火狐浏览器访问链接(其它浏览器不支持访问，不建立资源目录，我不知道为啥)：

ftp://192.168.163.4

如果需要输入密码，但是不想输入密码，就这样访问（重点）

ftp://ftpuser:ftpuser@192.168.163.4/

## 不需要输入用户名、密码访问ftp服务器终极解决方案

#匿名用户的根目录。这个非常重要**(注：这个目录不可以是Linux已有账号的家目录)**

anon\_root=/usr/local/ftpdir

## 不能上传文件问题

首先保证匿名用户登录根目录为755权限，例上述：/usr/local/ftpdir

再一个，在/usr/local/ftpdir创建目录files，权限给777，客户端就可以在/usr/local/ftpdir/files上传文件进来了

## 上传上来的文件权限太低，浏览器下载不了



这个上传文件的权限不是ftp服务器决定的，决定权限的是上传的客户端。我在给设备配置ftp服务器的时候(此时设备就相当于客户端)，上传上去的文件权限大都够用的

但是上图这种情况是确实存在的，我在测试的时候遇到了。这时候如果匿名访问不了，就这样：ftp://ftpuser:ftpuser@192.168.163.4/。**注：这样使用ftpuser用户登录的话就必须在配置文件中打开local\_enable=YES，并且设置本地用户登录根目录local\_root=/usr/local/ftpdir(跟匿名登陆根目录必须一样的啊)**

注：我已经在配置文件中设置了匿名用户登录为ftpuser，即ftp\_username=ftpuser。为什么匿名用户下载不了那个软件，必须使用用户名和密码登录了之后才行呢？不去纠结了，不钻牛角尖，不过这确是一个可行的解决方案。猜想可能是因为匿名用户不询问密码那个配置，即no\_anon\_password=YES，但是ftpuser这个系统用户是有密码的，所有就出现了这样的情况，当然我也只是猜想罢了，这个问题就先研究到这…



## 阿里云服务器搭建ftp服务器的坑

参考博客：https://blog.csdn.net/newborn2012/article/details/15812821/

按找上述步骤在局域网内是没有问题的，但是在云服务器上就有坑要填。因为云服务器有一个安全组的机制，然后从这个突破口去寻找解决方案。首先将局域网的配置步骤照搬到服务器上，启动发现无论是浏览器还是filezilla客户端都访问不了

**在解决这个问题之前要了解ftp的两个工作模式：**Port和Pasv。FTP连接一般会有两个连接，也就是会需要用到两个端口。一个服务器与客户端跟进行命令交互的，一个是进行数据传送的。那两种工作模式跟两个连接是怎么搭配起来工作的呢？

假设客户端为C，服务器端为S(以下简称C和S)：

* Port模式：当客户端C和服务端S连接起来后，C会发送一条命令告诉S：“我在本地打开了一个端口N等你进行数据连接”，当S收到这个Port命令后就会向C打开的那个端口N进行数据连接。S主动向C的某个端口进行数据连接，此乃主动模式
* Pasv模式：当客户端C和服务端S连接起来后，S会发送一条命令告诉C：“我再本地打开了一个端口M你来连接我吧”，当C收到这个消息后就会向S的M端口发起数据连接。S打开端口被C主动连接，此乃被动模式

**那我们应该使用哪种工作模式呢？**答案是被动（默认工作模式就是被动）。为什么？很简单，你是在局域网内，你可以连接到云服务器的某个端口（前提是这个端口放开了），但是云服务器连接不到你的

**FTP模式与数据端口：**无论是哪一种工作模式，首先在建立控制连接时候操作是一样的，都是由客户端（首先随机选取一个大于1024以上的端口）和FTP服务器的控制端口21建立连接，并通过该连接传输操作指令。**两种工作模式的区别是什么呢？**在于使用数据传输端口（ftp-data）方式。port mode由FTP服务器指定数据传输所使用的端口，默认值为20。pasv mode由FTP客户端决定数据传输端口，客户端向服务端发出连接请求包含了数据传输端口

**（重要）**

主动模式相关配置（了解）：

port\_enable=YES|NO：数据连接时取消PORT模式，默认为YES

connetc\_from\_port\_20=YES|NO：控制以PORT模式进行数据传输时是否使用20端口，默认是NO（但实际上我用的RHL-CentOS7.6，vsftpd.conf文件中该配置设为YES，该配置生效前提是工作模式为主动的）

ftp\_data\_port=端口号：设置FTP数据传输端口（ftp-data）值，默认值为20。此参数也用于主动模式

port\_promiscuous=YES|NO：取消PORT安全检查，该检查确保外出的数据只能连接到客户端上，默认为NO。小心打开此选项（**Don't care**）

被动模式相关配置：

pasv\_enable=YES|NO：允许数据传输使用PASV模式，默认为YES，且配置文件中没有该配置

pasv\_min\_port=端口号、pasv\_max\_port=端口号：设置在PASV模式下建立数据传输所用端口范围上界和下界，0表示任意，默认为0。把端口范围设在比较高的一段范围内，比如50000-60000，将有助于安全性的提高，我设置的是30000-50000，这个看你自己的啦

pasv\_promiscuous=YES|NO：此选项激活时，将关闭PASV模式的安全检查。该检查确保数据连接和控制连接是来自同一个IP地址。小心打开此选项。此选项唯一合理的用法是存在于由安全隧道方案构成的组织中，默认值为NO（**Don't care**）

pasv\_address=ip地址：此选项为一个数字IP地址，作为PASV命令的响应，默认值为none，地址是从呼入的连接套接字(incoming connectd socket)中获取（**Don't care**）

命令通道端口配置，默认为21

listen\_port=21

**最后一步，修改配置，使云服务器上搭建的FTP服务器可以正常使用：**

也没啥要修改的，主要就是加两个配置（为明确工作模式，我给加上pasv\_enable=YES）：

pasv\_enable=YES

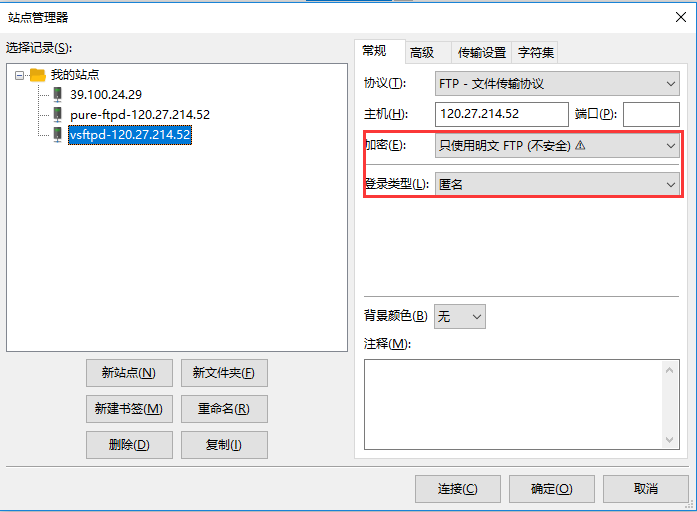
pasv\_min\_port=30000

pasv\_max\_port=50000

打开阿里云服务器30000-50000范围端口

（完）

## 客户端filezilla在连接vsftpd时候要明确加密类型为：只使用明文FTP（不安全）



## 扩展：pure-ftpd

这个跟vsftpd性质一样的啊，ftp是个什么玩意，你能看到这里心里就应该很清楚了，我也不再去解释他的概念、协议一些乱七八糟的东西了

直接进入安装：

按需安装pure-ftpd其它依赖，如ep el扩展：yum install -y epel-release

# yum install -y pure-ftpd

在启动pure-ftpd之前，需要先修改配置文件/etc/pure-ftpd/pure-ftpd.conf

# cd /etc/pure-ftpd

# vim pure-ftp.conf

打开PureDB配置，删除该行“#”号

PureDB /etc/pure-ftpd/pureftpd.pdb

然后跟vsftpd一样，设置被动模式数据端口范围：



**passive（被动模式）连接的端口范围-保持尽可能宽。（我vsftpd也是这么设置的，俩都是30000到50000，方便，而且我没记错的话这儿本来就是这个范围，只不过注释默认没打开）**

PassivePortRange 30000 50000

建立账号和文件使用目录。注意：为了安全，pure-ftpd使用的账号并非Linux的系统账号，而是虚拟账号，然后和Linux系统用户进行绑定

# mkdir /data/ftp

如果没有ftpuser账号的话

# useradd ftpuser

# passwd ftpuser

存储目录所有者切换为ftpuser

# chown -R pure-ftp:pure-ftp /data/ftp

创建虚拟账户，-u是将虚拟用户admin与系统用户ftpuser关联在一起，也就是说使用admin账号登录ftp后，会以ftpuser的身份来读取和下载文件，-d是指定admin账户的家目录，这样可以使用户admin登陆进来就可以也只能访问其家目录/data/ftp/

# pure-pw useradd admin -u ftpuser -d /data/ftp

Password：

Enter it again：

创建用户信息数据库文件，这一步很关键

# pure-pw mkdb

列出当前账号

pure-pw list

删除账号

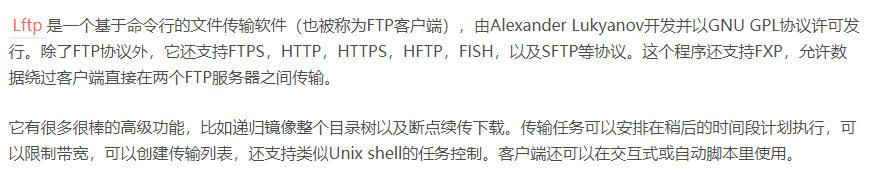
pure-pw userdel admin….

添加一个测试文件

# touch /data/ftp/123.txt

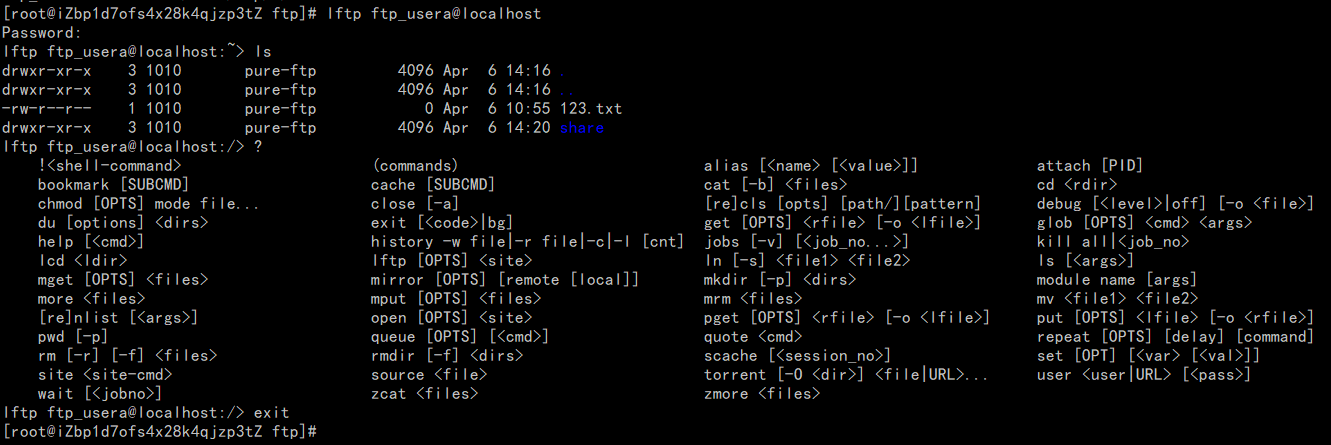
安装lftp客户端软件，跟ftp一样，可以理解为也是一个工具

简介：



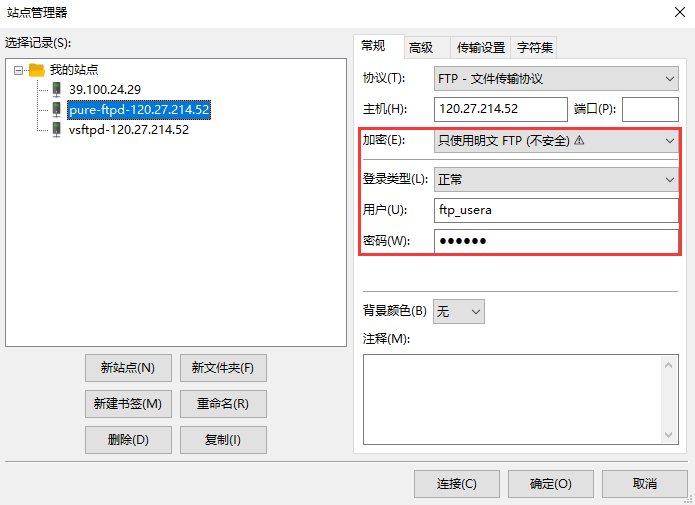
# yum install -y lftp

# lftp admin@127.0.0.1



**注：这个软件会在ftp的工作目录生成两个隐藏文件：“.”和“..”**

## 客户端filezilla连接pure-ftpd



# Java连接ftp服务器