使用vsFTP服务实现大数据的远程灾备

目 录

[第一章] 安装VSFTPD

[第二章] 相关用户的创建，以及用户相关目录和文件的创建

[第三章] VSFTP客户端的使用

[第四章] 实施大数据文件的异地灾备

业务需求：对云主机的大数据做远程灾备（把云主机上的数据在其他的机器上做定期备份），以便云主机数据丢失后的恢复。

ftp客户端用户的权限：每个用户只能在自己的根目录执行ls、mkdir、put；不允许删除自己根目录下的文件，不允许删除其他目录下的文件，不允许查看或切换到其他目录(只能在自己根目录)。

[第一章] 安装VSFTPD

1.1 采用yum安装vsftpd

[root@backup\_host data6]# yum install -y vsftpd



默认的端口号21用于和client端进行指令传输；默认的20端口用于数据传输。

1.2 相关文件简介

[root@backup\_host data6]# rpm -qc vsftpd

/etc/logrotate.d/vsftpd

/etc/pam.d/vsftpd # Plugable Authentication可插拔的认证文件

/etc/vsftpd/ftpusers

/etc/vsftpd/user\_list

/etc/vsftpd/vsftpd.conf # VSFTP主配置文件，所有的配置选项必须顶格写

用户登录的安全级别高低顺序：虚拟用户 > 系统用户 > 匿名用户

由于是生产环境，建议使用安全性高的虚拟用户登陆。那么相应配置需要按照虚拟用户来实施。

下面开始实施虚拟用户方式的ftp登录。

[第二章] 系统用户、虚拟用户的创建，以及虚拟用户相关目录和文件的创建

2.1 创建vsftpd使用的系统用户vsftpd，主目录为/home/vsftpd，禁止ssh登录。

创建之后，所有虚拟用户将使用这个系统用户vsftpd访问文件，也就是说虚拟用户被映射为这个系统用户。

[root@backup\_host ~]# useradd -s /sbin/nologin vsftpd

[root@backup\_host ~]# mkdir /home/vsftpd # 无需为系统用户vsftpd建主目录，系统会自动为其创建家目录

mkdir: cannot create directory ‘/home/vsftpd’: File exists

[root@backup\_host ~]# ll /home/ | grep vsftpd

drwx------ 3 vsftpd vsftpd 78 5月 15 15:29 vsftpd

[root@backup\_host ~]# ll -ht /etc/vsftpd/

total 20K

-rw------- 1 root root 125 10月 31 2018 ftpusers

-rw------- 1 root root 361 10月 31 2018 user\_list

-rw------- 1 root root 5.0K 10月 31 2018 vsftpd.conf

-rwxr--r-- 1 root root 338 10月 31 2018 vsftpd\_conf\_migrate.sh

2.2 创建虚拟用户及其主目录

需创建的虚拟用户名叫testuser，那么先创建其主目录：

[root@backup\_host ~]# mkdir -p /home/vsftpd/testuser

[root@backup\_host ~]# ll /home/vsftpd/

total 0

drwxr-xr-x 2 root root 6 5月 15 15:50 testuser

[root@backup\_host ~]# chown -R vsftpd:vsftpd /home/vsftpd/testuser

[root@backup\_host ~]# ll /home/vsftpd/

total 0

drwxr-xr-x 2 vsftpd vsftpd 6 5月 15 15:50 testuser

# 在自定义的virtual\_users.conf文件中创建虚拟用户

[root@backup\_host ~]# vi /etc/vsftpd/virtual\_users.conf

[root@backup\_host ~]# ll /etc/vsftpd/virtual\_users.conf

-rw-r--r-- 1 root root 20 5月 15 16:04 /etc/vsftpd/virtual\_users.conf

# 文件中的奇数行号写虚拟用户名，偶数行号写密码

[root@backup\_host ~]# cat /etc/vsftpd/virtual\_users.conf

testuser

hi~tony^\_^

2.3 使用db\_load命令生成口令库文件，并启用该文件

口令库文件也叫认证文件，被用于vsftpd识别，需要由系统自带的db\_load生成

# 根据虚拟用户文件/etc/vsftpd/virtual\_users.conf创建数据库文件

[root@backup\_host ~]# db\_load -T -t hash -f /etc/vsftpd/virtual\_users.conf /etc/vsftpd/virtual\_users.db

[root@backup\_host ~]# ll /etc/vsftpd/virtual\_users.\*

-rw-r--r-- 1 root root 20 5月 15 16:04 /etc/vsftpd/virtual\_users.conf

-rw-r--r-- 1 root root 12288 5月 15 16:14 /etc/vsftpd/virtual\_users.db

[root@backup\_host ~]# chmod 600 /etc/vsftpd/virtual\_users.db

[root@backup\_host ~]# ll /etc/vsftpd/virtual\_users.db

-rw------- 1 root root 12288 5月 15 16:14 /etc/vsftpd/virtual\_users.db

# 通过修改pam配置来启用这个数据库文件

[root@backup\_host ~]# vim /etc/pam.d/vsftpd # 在前面增加这两行

auth sufficient /lib64/security/pam\_userdb.so db=/etc/vsftpd/virtual\_users

account sufficient /lib64/security/pam\_userdb.so db=/etc/vsftpd/virtual\_users

2.4创建虚拟用户个人配置文件（每个虚户各自有一个配置文件）

# 虚拟用户配置文件目录下创建一个和虚拟用户同名的文件

[root@backup\_host userconf]# pwd

/etc/vsftpd/userconf

[root@backup\_host userconf]# cat /etc/vsftpd/virtual\_users.conf | head -n 1

testuser

[root@backup\_host userconf]# vim testuser

[root@backup\_host userconf]# cat testuser

local\_root=/home/vsftpd/testuser/

write\_enable=YES

2.5 修改主配置文件

[root@backup\_host ~]# grep --color "=" /etc/vsftpd/vsftpd.conf | grep -v "^#"

anonymous\_enable=NO # 禁止匿名用户登录

ascii\_upload\_enable=YES #支持ASCII模式的上传功能

local\_enable=YES # 虚拟用户需要映射到本地系统用户，故开此选项

guest\_enable=YES # 启用虚拟用户

guest\_username=vsftpd # 指定虚拟用户映射到哪个系统用户名

user\_config\_dir=/etc/vsftpd/userconf # 所有虚拟用户(其中一个虚户是testuser)使用的配置文件目录

allow\_writeable\_chroot=YES

virtual\_use\_local\_privs=NO # 虚拟用户只能上传文件，不能删除、不能对已上传的文件改名

anon\_world\_readable\_only=NO

local\_enable=YES

write\_enable=YES

local\_umask=022

anon\_upload\_enable=YES # 必须YES，虚拟用户才能上传

anon\_mkdir\_write\_enable=YES # 必须YES，虚拟用户才能新建目录

anon\_other\_write\_enable=NO

dirmessage\_enable=YES

xferlog\_enable=YES

connect\_from\_port\_20=YES

xferlog\_std\_format=YES

listen=NO

listen\_ipv6=YES

pam\_service\_name=vsftpd

tcp\_wrappers=YES

重启vsftpd服务即可。

[第三章] VSFTP客户端的使用

3.1安装lftp

[appadmin@elcndc5dsj01 ~]$ sudo yum -y install lftp

服务端启动vsftpd后会监听默认21端口，那么要确保客户端能和21端口通信。

3.2 未开启虚拟用户认证时，(使用匿名用户)登录vsftp客户端操作

[root@backup\_host ~]# ls -lh /tmp/derby.log

-rw-rw-r-- 1 appadmin appadmin 890K 5月 13 11:40 /tmp/derby.log

[appadmin@elcndc5dsj01 ~]$ lftp 10.4.106.133

lftp 10.4.106.133:~> pwd

ftp://10.4.106.133

lftp 10.4.106.133:~> !ls -lh

total 892K

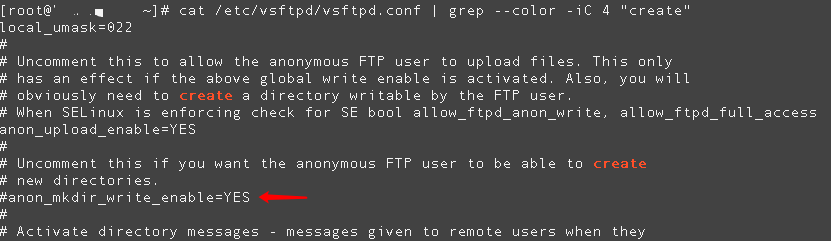
-rw-rw-r-- 1 appadmin appadmin 890K 2019-05-06 14:29 derby.log

3.3 未开启虚拟用户认证时，使用匿名用户上传文件

可发现，匿名用户可登陆但无法上传：



原因是未放开匿名用户的写权限



如截图，放开后，重试：

[root@backup\_host ~]# systemctl restart vsftpd

重试put上传仍然失败。检查一下默认ftp公共目录的权限发现：



配置有关匿名的选项：

[root@backup\_host ~]# grep --color "=" /etc/vsftpd/vsftpd.conf | grep -v "^#"

anonymous\_enable=YES # 启用匿名访问

local\_enable=YES

write\_enable=YES

local\_umask=022

anon\_upload\_enable=YES # 允许匿名用户上传

anon\_mkdir\_write\_enable=YES # 允许匿名用户创建目录

anon\_other\_write\_enable=YES # 向匿名用户开放其他写入权限

dirmessage\_enable=YES

xferlog\_enable=YES

connect\_from\_port\_20=YES

xferlog\_std\_format=YES

listen=NO

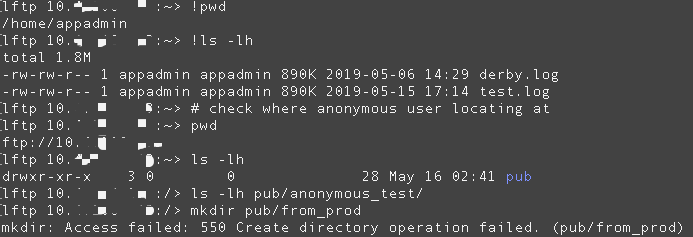
listen\_ipv6=YES

pam\_service\_name=vsftpd

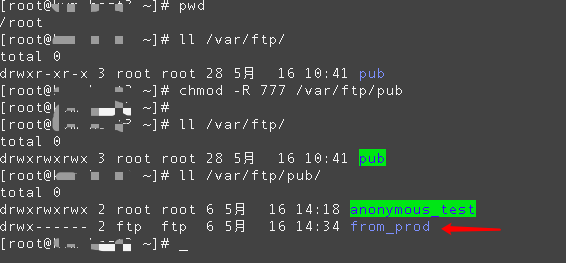
userlist\_enable=YES

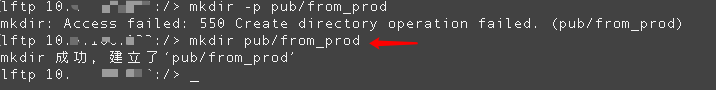
tcp\_wrappers=YES

重启服务后重试，可以上传，但是无法在匿名用户的根目录(默认为/var/ftp/pub)下新建目录：



修改匿名用户的根目录权限后，重试新建目录，成功：

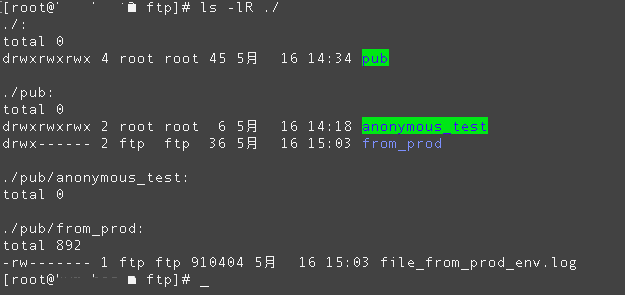




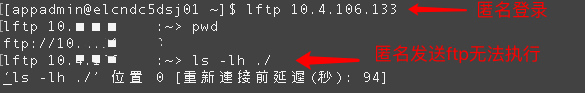
继续往该目录上传文件并对文件改名：



到vsFTP查看结果，客户端成功上传：



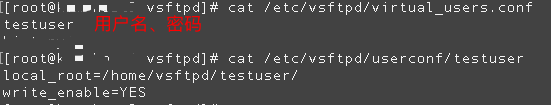
3.4 开启安全性高的虚拟用户登录方式后，尝试匿名登录后发送指令：



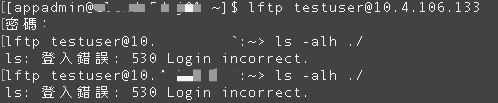
匿名用户也无法执行mkdir。

采用虚拟用户登录操作——

先从虚拟用户配置文件所在目录 /etc/vsftpd/virtual\_users.conf 查找到虚拟用户testuser的登录信息



再用虚户testuser登录操作,首先尝试输错密码，此时能登录：



但是无法执行命令，说明身份认证生效了，必须输入正确密码才能继续操作：

可以上传到指定虚拟用户所在的根目录 /home/vsftpd/testuser

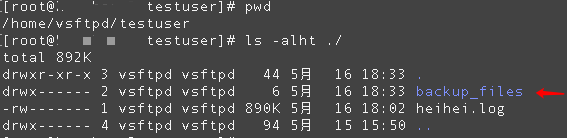


虚拟用户testuser既无法看其他目录也不允许切换到其他目录，只能在/home/vsftpd/testuser操作

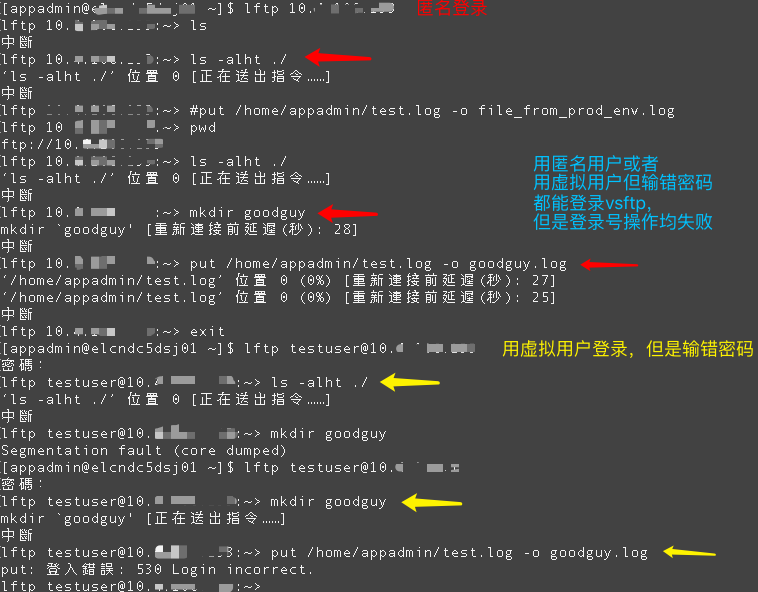


只能在testuser的主目录下创建目录





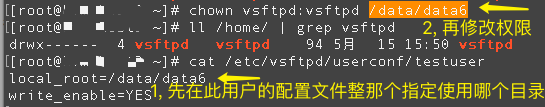
分别测试匿名用户登录后的操作、虚拟用户用错误密码登录后操作：



结果达到预期：禁止匿名用户操作，只允许虚拟用户成功登录后操作。

----

另外的问题：虚户testuser的主目录挂载盘容量太小，只有几十Gb，那么如何为其分配专用盘？



修改指定专用盘挂载的目录(/data/data6)权限后，重试上传，成功：



----

[第四章] 实施大数据文件的异地灾备

4.1 操作流程

将hdfs待备份路径下的文件下载到hadoop集群所在的linux本地目录 🡺 对该目录下的所有文件打包压缩 🡺 在vsftp服务端主机预先创建存放灾备数据的目录 🡺 在vsftp客户端把压缩包通过虚拟用户上传到vsftp服务端主机 🡺 在vsftp客户端验证服务端是否已收到。

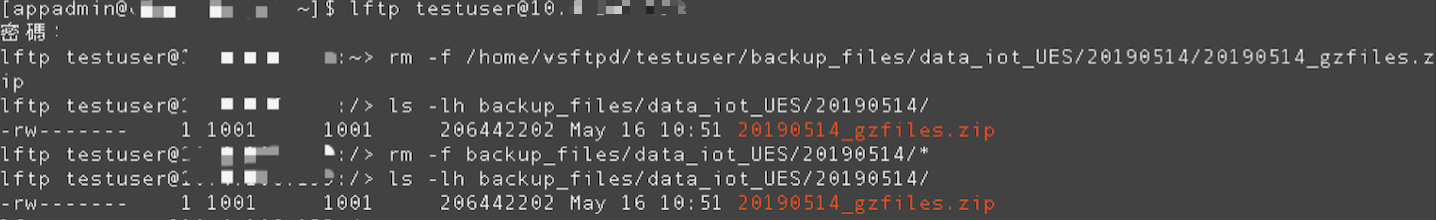
4.2 vsftp服务端数据的安全性保障

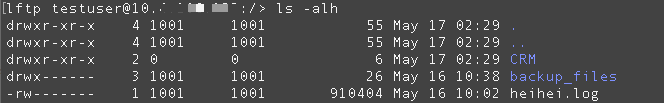
请参考本文开头的“ftp客户端用户的权限”。

搞破坏的黑客即使攻破了数据源所在的云主机，想通过ssh方式登录到FTP服务端是不可能的，因为我们已关闭ssh的22端口。

如果黑客想从云主机上用虚拟用户testuser通过lftp登录到FTP服务端，也无法删除文件或重命名文件，只能上传和查看文件。

如截图的验证：





从截图可看出，虚拟用户testuser尝试删除文件，结果失败。

【结论】大数据的异地灾备及其数据安全需求，已成功实现