PAM

Linux PAM(Pluggable Authentication Modules) 提供了一个框架，用于进行系统级的用户认证。PAM起一个在应用程序和底层不同认证模块的连接作用即API。用户可以方便灵活的使用不同模块，甚至替换之前的模块。在CentOS中，默认下没有基于MariaDB的PAM认证模块，所以需要自行安装第三方模块，以实现基于MariaDB的认证机制。

下载pam_mysql模块rpm包

> 说明：实践中将用户账号信息由MariaDB存放管理，数据库服务器IP-192.168.1.151，vsftpd服务器ip-192.168.1.150

MariaDB配置

安装MariaDB

```
yum install mariadb mariadb-server mariadb-devel
systemctl enable mariadb
systemctl start mariadb
```

绑定IP以远程连接

> 如果将MariaDB和vsftpd部署到一台服务器，则不需要绑定IP，通过本地连接数据库即可。

```
vim /etc/my.cnf
bind-address=192.168.1.151
```

设定数据库密码及删除匿名用户

```
#使用交互式的设定工具
mysql_secure_installation
```

创建数据库及授权

```
#创建存储用户账号信息的数据库 ftpdb
CREATE DATABASE ftpdb;
#选择操作数据库
use ftpdb;
#授权 ftpuser 用户可以通过 IP 连接 访问ftpdb数据库
##授予所有权限给vsftpd用户本地登录和远程登录访问ftpdb数据库
GRANT ALL PRIVILEGES ON ftpdb.* TO 'ftpuser'@'localhost' IDENTIFIED BY 'xxxxxx';
GRANT ALL PRIVILEGES ON ftpdb.* TO 'ftpuser'@'192.168.1.150' IDENTIFIED BY 'xxxxxx';
#或者只授予查询权限
GRANT SELECT ON ftpdb.* to 'ftpuser'@'localhost' IDENTIFIED BY 'xxxxxx';
GRANT SELECT ON ftpdb.* to 'ftpuser'@'192.168.1.150' IDENTIFIED BY 'xxxxxx';
#让数据库服务器重读权限表
FLUSH PRIVILEGES;
```

创建表及添加虚拟用户信息

```
#创建表 vsuser
CREATE TABLE vsuser (
    Id int AUTO_INCREMENT NOT NULL,
    Name char(20) binary NOT NULL,
    Password char(48) binary NOT NULL,
    primary key(id)
);
```

```
#查看
SHOW TABLES;
##查看表结构
DESC vsuser;
```

```
#给表中插入数据(虚拟用户账号信息)
INSERT INTO vsuser(Name,Password)
VALUES('test1',Password('xxxxxx'));
INSERT INTO vsuser(Name,Password)
VALUES('test2',Password('xxxxxx'));
```

```
#使用远程主机验证ftpuser用户是否可以连接MariaDB数据库
mysql -u ftpuser -h localhost -pxxxxxx
```

vsftpd配置

安装pam_mysql模块

```
#下载
wget ftp://ftp.icm.edu.pl/vol/rzm5/linux
fedora/linux/releases/25/Everything/x86_64/os/Package
s/p/pam_mysql-0.7-0.21.rc1.fc24.x86_64.rpm
#安装
yum localinstall pam_mysql-0.7-
0.21.rc1.fc24.x86_64.rpm
```

> /lib64/security/pam_mysql.so--->认证模块
>
> /usr/share/doc/pam_mysql/README--->帮助文档，可阅读查看如何配置以及如何结合MySQL使用。

提供pam认证配置文件

```
vim /etc/pam.d/vsftpd.mysql
auth required /lib64/security/pam_mysql.so
user=ftpuser passwd=xjw,./qwe host=192.168.1.151
db=ftpdb table=vsuser usercolumn=Name
passwdcolumn=Password crypt=2
account required /lib64/security/pam_mysql.so
user=ftpuser passwd=xjw,./qwe host=192.168.1.151
db=ftpftp table=vsuser usercolumn=Name
passwdcolumn=Password crypt=0
```

建立虚拟用户所映射的用户

> 所有的虚拟用户都映射为一个本地用户，这些虚拟用户登录的家目录就是这个本地用户的家目录。

```
#创建用户
useradd -s /sbin/nologin -d /var/ftpmore ftpmore
#添加权限。注意：此目录不能拥有执行写权限，否则登录失败
chmod go+r /var/ftpmore
#家目录下创建目录
mkdir /var/ftpmore/pub
chown ftpmore:ftpmore pub
```

vsftpd配置

```
guest_enable=YES
#虚拟用户映射的本地用户名名称
guest_username=vsuser
#修改认证配置文件
pam_service_name=vsftpd.mysql
```

对虚拟用户分别进行权限控制

> 虚拟用户默认映射为匿名用户的权限，虚拟用户对vsftpd服务的访问权限是通过匿名用户相关的指令进行配置的。

```
#指定配置目录，dir以映射本地用户的用名称命名
user_config_dir=/path/to/dir
```

> 在这个目录下创建以虚拟用户用户名为文件名的文件，然后在文件内定义不同用户的访问权限。