XL2TP+ daloradius详细部署

现场环境：

OS：centos6.5 x86\_64

Xl2tp：xl2tpd-1.3.8-1.el6.x86\_64.rpm

Freeradius：freeradius-server-2.2.9.tar.gz

Mysql：mysql-community-server-5.6.35-2.el6.x86\_64

Daloradius：daloradius-0.9-9.tar.gz

HH：daloradius-0.9-8-hh.tar.gz

修改hosts文件 把主机名添加进去

Vi /etc/hosts



# 安装freeradius2.2.9+mysql

## 安装源并更新

rpm -Uvh <http://dl.fedoraproject.org/pub/epel/6/x86_64/epel-release-6-8.noarch.rpm>

yum update -y

## 安装相关库

yum -y install wget expat-devel gcc make gmp-devel gmp pkgconfig perl libpcap gcc-c++ logrotate tar cpio gawk flex bison bison-devel lsof libpcap-devel patch openssl openssl-devel libgcrypt\* crypt\* autoconf automake libtasn1-devel zlib zlib-devel trousers trousers-devel texinfo libnl-devel libnl dbus dbus-devel ncurses-devel readline-devel libtool-ltdl libtalloc\* hiredis\* redhat-lsb python

## 安装Mysql

rpm -Uvh <http://dev.mysql.com/get/mysql-community-release-el6-5.noarch.rpm>

yum install -y mysql-community-server mysql-devel

chkconfig mysqld on

service mysqld start

mysql\_secure\_installation设置root密码、移除test数据库

## 编译安装freeradius

wget <ftp://ftp.freeradius.org/pub/freeradius/freeradius-server-2.2.9.tar.gz>

tar zxvf freeradius-server-2.2.9.tar.gz

cd freeradius-server-2.2.9

./configure && make && make install

## 测试

vi /usr/local/etc/raddb/users

找到这一行

#steve Cleartext-Password:="testing"

将前面的#去掉

steve Cleartext-Password := "testing"

Service-Type = Framed-User,

Framed-Protocol = PPP,

Framed-IP-Address = 172.16.3.33,

Framed-IP-Netmask = 255.255.255.0,

Framed-Routing = Broadcast-Listen,

Framed-Filter-Id = "std.ppp",

Framed-MTU = 1500,

Framed-Compression = Van-Jacobsen-TCP-IP

调试模式命令：

radiusd –X

提示Refusing to start with libssl version OpenSSL 1.0.1e-fips

vi /usr/local/etc/raddb/radiusd.conf

找到allow\_vulnerable\_openssl = no,修改成allow\_vulnerable\_openssl = yes

再次启动radiusd -X 最后显示Ready to process requests.说明服务成功启动

新打开一个终端

终端输入命令：radtest steve testing localhost 0 testing123

获得结果：

Sent Access-Request Id 50 from 0.0.0.0:34461 to 127.0.0.1:1812 length 75

User-Name = "steve"

User-Password = "testing"

NAS-IP-Address = 106.186.116.69

NAS-Port = 0

Message-Authenticator = 0x00

Cleartext-Password = "testing"

Received Access-Accept Id 50 from 127.0.0.1:1812 to 0.0.0.0:0 length 71

Service-Type = Framed-User

Framed-Protocol = PPP

Framed-IP-Address = 172.16.3.33

Framed-IP-Netmask = 255.255.255.0

Framed-Routing = Broadcast-Listen

Filter-Id = "std.ppp"

Framed-MTU = 1500

Framed-Compression = Van-Jacobson-TCP-IP

accept！貌似成了

## 让radius和mysql融合

vi /usr/local/etc/raddb/radiusd.conf

$INCLUDE sql.conf 去掉该行注释

vi /usr/local/etc/raddb/sql.conf 定义连接数据库用户名和密码

database = "mysql"

login = "radius"

password = "radpass"

vi /usr/local/etc/raddb/sites-available/default

将authorize，accounting，session，post\_auth段的sql关键字前的注释去掉，如：

post-auth {

....

sql

....

Post-Auth-Type REJECT {

# Login failed: log to SQL database.

sql

}

}

输入mysql -u root -p，输入密码

1. 建立数据库并导入radius数据结构

mysql>create database radius;

mysql>grant all on radius.\* to 'radius'@'localhost' identified by 'radpass';

mysql>flush privileges;

# mysql -u root -p radius < /usr/local/etc/raddb/sql/mysql/schema.sql

# mysql -u root -p radius < /usr/local/etc/raddb/sql/mysql/nas.sql

# mysql -u root -p radius < /usr/local/etc/raddb/sql/mysql/ippool.sql

# mysql -u root -p radius < /usr/local/etc/raddb/sql/mysql/wimax.sql

1. 建立组（在此新建组名称为user）

mysql>use radius;

mysql>insert into radgroupreply (groupname,attribute,op,value) values ('user','Auth-Type',':=','Local');

mysql>insert into radgroupreply (groupname,attribute,op,value) values ('user','Service-Type',':=','Framed-User');

mysql>insert into radgroupreply (groupname,attribute,op,value) values ('user','Framed-IP-Address',':=','255.255.255.255');

mysql>insert into radgroupreply (groupname,attribute,op,value) values ('user','Framed-IP-Netmask',':=','255.255.255.0');

1. 建立用户（在此新建用户名为test，密码为testpwd）

mysql>insert into radcheck (username,attribute,op,value) values ('test','Cleartext-Password',':=','testpwd');

1. 将用户加入组中

mysql>insert into radusergroup (username,groupname) values ('test','user');

测试：radiusd -X，在另一终端执行radtest test testpwd localhost 1812 testing123

获得结果

Sending Access-Request of id 247 to 127.0.0.1 port 1812

User-Name = "test"

User-Password = "testpwd"

NAS-IP-Address = 127.0.0.1

NAS-Port = 1812

Message-Authenticator = 0x00000000000000000000000000000000

rad\_recv: Access-Accept packet from host 127.0.0.1 port 1812, id=247, length=38

Service-Type = Framed-User

Framed-IP-Address = 255.255.255.255

Framed-IP-Netmask = 255.255.255.0

Accept！说明成了。

接下来加需要认证的服务器

vi /usr/local/etc/raddb/clients.conf

在最后一行 添加 下面的IP是公司的网关

client 192.168.0.1 {

secret = testing123

shortname = private-network-1

}

# 安装 freeradius管理程序daloradius

## web环境搭建

yum groupinstall ‘web server’ //安装web服务程序

yum groupinstall ‘php support’ ///安装php

yum groupinstall ‘mysql database server’ ///这个在配置freeradius时就安装过的

yum install php-mysql //这个如果不安装，打开php+mysql的程序会出错的

1. 下载daloradius

官方下载地址：

wget <http://nchc.dl.sourceforge.net/project/daloradius/daloradius/daloradius0.9-9/daloradius-0.9-9.tar.gz>

## 配置daloradius

将程序解压到/var/www/html目录下面

tar -zxvf daloradius-0.9-9.tar.gz -C /var/www/html/daloradius

修改daloradius目录所有者

Chown –R apache:apache daloradius

## 配置mysql数据库

导入/contrib/db目录下的数据库表

Myslq –u root –p radius < mysql-daloradius.sql

Mysql –u root –p radius < fr2-mysql-daloradius-and-freeradius.sql

修改数据库连接

vim /var/www/html/daloradius/daloradius-0.9-9/library/daloradius.conf.php



这里只需要把数据库的密码写上就可以关联了

## 测试

配置好后在浏览器中打开，下面是默认登录用户名和密码

启动apache服务

Service httpd start

http://yourIP/daloradius

login：administrator

password：radius

## 问题：点击登录页面出错

查看http错误日志信息/var/log/httpd/error\_log

[Mon Oct 14 15:44:51 2013] [error] [client 172.16.1.55] PHP Warning: include\_once(): Failed opening 'DB.php' for inclusion (include\_path='.:/usr/share/pear:/usr/share/php') in /var/www/html/daloradius/library/opendb.php on line 84, referer: http://172.16.1.50/daloradius/login.php

[Mon Oct 14 15:44:51 2013] [error] [client 172.16.1.55] PHP Fatal error: Class 'DB' not found in /var/www/html/daloradius/library/opendb.php on line 86, referer: http://172.16.1.50/daloradius/login.php

提示数据库连接失败。再次检查连接数据库文件，没有问题。

解决：新版本的daloradius连接数据库，需要安装数据库连接模块。php-pear-DB

没办法安装吧！ yum install php-pear-DB

再次打开web，如果还有出错，安装一下php扩展程序。

下载 ：wget http://pear.php.net/go-pear.phar

安装：php go-gear.phar

OK！一切问题解决完毕。

######\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*搭建完网页你刚才创建的radius库就没了 需要重新创建

## 建立数据库并导入radius数据结构

mysql>create database radius;

mysql>grant all on radius.\* to 'radius'@'localhost' identified by 'radpass';

mysql>flush privileges;

# mysql -u root -p radius < /usr/local/etc/raddb/sql/mysql/schema.sql

# mysql -u root -p radius < /usr/local/etc/raddb/sql/mysql/nas.sql

# mysql -u root -p radius < /usr/local/etc/raddb/sql/mysql/ippool.sql

# mysql -u root -p radius < /usr/local/etc/raddb/sql/mysql/wimax.sql

## Daloradius汉化

daloradius汉化包下载：下载地址 <http://pan.baidu.com/share/link?shareid=2500086958&uk=3843037427>

下载之后解压，然后把解压出来的lang 中的china.php 放到 /var/www/html/daloradius/daloradius-0.9-9/lang目录下

mv china.php /var/www/html/daloradius/daloradius-0.9-9/lang/zh.php

vim /var/www/html/daloradius/daloradius-0.9-9/lang/main.php



添加以上信息

vim /var/www/html/daloradius/daloradius-0.9-9/config-lang.php



添加以上信息

最后就可以在登录到web程序里设置语言了。

# 配置ppp和 xl2tpd

## 安装

rpm -ivh ppp-2.4.5-10.el6.x86\_64.rpm

rpm -ivh xl2tpd-1.3.8-1.el6.x86\_64.rpm

## 修改配置xl2tpd

vim /etc/xl2tpd/xl2tpd.conf



修改成想分配给vpn客户机地址池

## 修改配置ppp

vim /etc/ppp/options.xl2tpd



添加两个dns服务器地址

启动 xl2tpd 服务

service xl2tpd start

## 设置拨号的账号密码

vim /etc/ppp/chap-secrets



用户名是mmm 密码是123456

此时可以用以上用户建立连接拨号了。

# Xl2tp和freeradius整合

## 安装freeradius客户端

tar zxvf freeradius-client-1.1.7.tar.gz

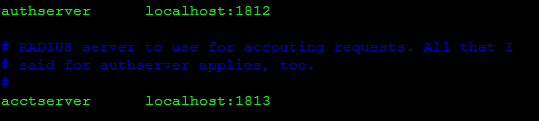
cd freeradius-client-1.1.7

./configure

make && make install

## 添加2个认证和计费端口

vim /usr/local/etc/radiusclient/radiusclient.conf



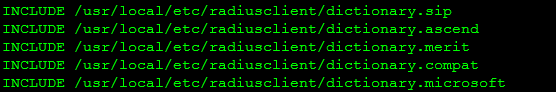
## 添加服务器的认证信息

vim /usr/local/etc/radiusclient/servers



## 添加字典文件到配置文件中

vim /usr/local/etc/radiusclient/dictionary



文件最后添加以上信息

在网上下载dictionary.microsoft文件，放到/usr/local/etc/radiusclient目录下。

## 添加配置ppp

vim /etc/ppp/options.xl2tpd



文件最后添加以上信息

## 重启动radiusd服务

cp /usr/local/sbin/rc.radiusd /etc/init.d/radius





至此整个xl2tp和freeradius搭建完成。