实例 97　linux 下远程认证拨号用户服务的实现



实现目的

远程认证拨号用户服务（Remote Authentication Dial In User Service，RADIUS）是在网络访问服务器（Network Access Server，NAS）和集中存放认证信息的 Radius 服务器之间传输认证、授权和配置信息的协议。其协议的标准定义在 IETF 的 RFC 2865 和 RFC 2866 文件中。对于中小型网络 NAS 应用来说，以 Linux 为平台建立 RADIUS 服务器是非常好的选择。使用共享软件完全可以建立简洁、高效的 RADIUS 服务器。本例介绍 linux 下远程认证拨号用户服务（RADIUS）的实现方法。



实现技术

RADIUS 以 Client/Server 方式工作，实现了对远程电话拨号用户的身份认证、授权和计费功能。其 Client 端多为通过拨号方式实现的 NAS，主要用来将用户信息传递给服务器；RADIUS 服务器则对用户进行认证，并返回用户的配置信息。为了保证传输的安全性，在 Client 和 Server 之间传送的数据均以 MD5 方式加密。在 RADIUS 的 Server 端和 Client 端之间的通信主要有两种情况：一种是接入认证；另一种是计费请求。

使用 RADIUS 可以实现集中化的认证和记费功能，可以减少管理的负担和费用，同时还可以实现很多扩展的功能，如用户拨号时间的限定、用户拨号时间的配额、根据用户分配特定 IP 地址等等。RADIUS 是一种基于 UDP 协议的上层协议，认证服务的监听端口号为 1812，记费服务的监听端口号为 1813。

RADIUS 的工作流程是：

（1）用户拨入 NAS；

（2）NAS 向 RADIUS 服务器发送一系列加密的“属性/值”；

（3）RADIUS 服务器检查用户是否存在、属性/值是否匹配；

（4）RADIUS 服务器发送回“接受”或“拒绝”给 NAS。

RADIUS 服务器通常是基于数据库来实现的。对于大型 ISP，通常会使用大型后台数据库。而对于中小型应用使用小型数据库就足够了。RADIUS 的身份验证也可以通过 LDAP 来实现，但其应用不如数据库那么广泛。

本例介绍一种使用 IC-RADIUS 与 mySQL 配合建立 RADIUS 服务器的方案。并介绍如何使用 Cisco2610+Modem Pool 作为 NAS 和如何配置 Linux 作为 NAS 的实例。



实现方法

1、RADIUS 服务器的建立

先安装配置好 Linux 的基本系统，注意同时安装开发工具、Perl、Perl DBI 和 mySQL DBD 模块，当然还必须安装 mySQL 数据库。本例中把数据库和 RADIUS 服务放在同一台服务器

上。现在的 Linux 发行版本里都包含 mySQL，可以直接安装到系统里。安装步骤如下：

（1）安装和配置 ICRADIUS

1）输入命令：

#tar xvfz icradius-0.18.1.tar.gz

#cd icradius-0.18.1/src

然后拷贝针对 Linux 的 Make 文件 Makefile.lnx 为 Makefile，命令为：

cp Makefile.lnx Makefile

这里有可能需要修改 Makefile 文件，把 mySQL 库、头文件的位置根据实际安装的情况加以修改。对于可执行文件的安装位置也可以修改。

2）运行命令：

#make

#make install

（2）创建 RADIUS 数据库

1）连接 mysql 数据库，命令为：

#mysql -u root –pyourpassword

>create database radius; ### 创建 radius 数据库

然后需要创建 RADIUS 数据库需要的各个表格，这里要使用 icradius-0.18.1 目录下 script 子目录中的 radius.db 文件，该文件已经定义了所需要的各个表格，这里只需使用以下命令：

#mysql -u root -pyourpassword radius < radius.db

这时就创建了 Radius 认证和计费所需要的各个表格，如表 97-1 所示。

表 97-1　创建 Radius 认证和计费所需的表

名　称	作　用
dictionary	定义了在 RADIUS 消息中的属性及属性值和其数字 ID 的对应关系，还定义了每个属性值允许的数据类型
nas	定义了该 radius 管理的访问服务器的信息，如其 IP 地址和设备名等等
radacct	保存记帐信息
radacct_summary	保存记帐信息
radcheck	定义了当用户拨入时需要检查的属性、加密码和时间限制等等
radgroupcheck	定义了某个组的成员在拨入时，需要检查的公共属性
radgroupreply	定义了该组成员在拨入验证通过以后，在应答信息内需要定义的属性及其对应的属性值
radreply	定义了成员在拨入验证通过以后，在应答信息内需要定义的属性及其对应的属性值
realmgroup	定义了用户和组的对应关系

（3）填充各个表格

向创建的各个数据库的表中添加内容。对于 dictionary 表的内容，icradius 软件提供了一个脚本文件 script/dictimport.pl 来创建，具体步骤为：

1）编辑该文件，修改

my $dbusername =root;

my $dbpassword = yourpassword;

为对应的数据库管理员的用户名和密码。

2）运行该脚本，命令为：

#./dictimport.pl ../raddb/dictionary

如果使用 Cisco 路由器，还需要加载 Cisco 的 dictionary 文件，命令如下：

./dictimport.pl ../raddb/dictionary.cisco

3）向 nas 表格中添加内容，先进入 mysql：

mysql -u root -pyourpassword radius

执行 SQL 语言命令如下：

insert into nas

values （0,"cisco nas","nas","202.197.89.250","cisco",32,"cisco","public","on"）;

其中各字段的意义如表 97-2 所示。

表 97-2　nas 表格各字段的意义

字段号	字　段　意　义
1	该 nas 设备的 ID 号，为数字类型
2	设备名
3	设备的简称
4	设备的 IP 地址
5	设备类型
6	设备的端口总数
7	Radius 服务器和 nas 之间共享的密码
8	Snmp 协议的共同体名
9	对 snmp 协议是否开放

4）srcipts 目录下的 radius.cgi 是一个实现 Web 界面管理用户及记费信息的 CGI 程序，但是要在使用该脚本程序以前，首先要在 radcheck 表格中添加如下内容：

INSERT INTO radcheck VALUES （"","admin","Password","adminpassword"）;

INSERT INTO radcheck VALUES （"","admin","Radius-Operator","Yes"）;

其中，admin 为 RADIUS 管理员的用户名，adminpassword 为管理员的密码。

5）将 radius.cgi 和 usage.cgi 拷贝到 Web 服务器的 cgi-bin 目录下，再编辑这两个文件，正确的设定数据库管理员的用户名和密码。最后指定两个文件中的$cookiedomain 及$radhost 为空。两个文件中的$radsecret 指定为 NAS 和 RADIUS 共享的密码。

（4）配置启动 radiusd

1）在/etc/目录下创建子目录 raddb

mkdir /etc/raddb

2）在该目录下创建文件 client，并设定其访问权限：

touch clients

chmod 664 clients

3）把 icradius-0.18.1/raddb /目录下的 radiusd.conf 拷贝到/etc/raddb 目录下：

#cp ~/icradius-0.18.1/raddb/radius.conf /etc/raddb/

4）把~/icradius-0.18.1/raddb/中的所有文件拷贝到/etc/raddb 目录中。

其中在~/icradius-0.18.1/redhat/目录下有一个名为 rc.radiusd-redhat 的文件，它是 redhat 环境下 radiusd 的启动文件，将其拷贝到/etc/rc.d/init.d 目录下：

cp ~/icradius-0.18.1/redhat/rc.radiusd-redhat /etc/rc.d/init.d/rc.radiusd

5）编辑文件/etc/raddb/radius.conf 文件，password 后面修改为 mysql 的管理员密码。

6）编辑文件/etc/rc.d/init.d/rc.radius 成如下内容：

RADIUSD=/usr/sbin/radiusd

WATCHER=/usr/sbin/radwatch 修改为（缺省安装时）

RADIUSD=/usr/local/sbin/radiusd

WATCHER=/usr/local/sbin/radwatch

7）拷贝~/icradius-0.18.1/scripts 目录下的 radwatch 到/usr/local/sbin 目录下。拷贝~/icradius-0.18.1/scripts 目录下的 radiusd.cron.daily 到 /etc/cron.daily/ 目录下。拷贝~/icradius-0.18.1/scripts 目录下的 radiusd.cron.monthly 到/etc/cron.daily/目录下。

8）启动 radiusd，命令为：

/etc/rc.d/init/rc.radiusd start

（5）添加用户

在浏览器里输入 http://radiusserver/cgi-bin/radius.cgi 进入管理界面，在这里输入 RADIUS 管理员的用户名和密码。

1）创建一个组，该组具有所有用户都应该具有的特性，为该组起一个名字。

2）进入组属性设置界面，在“reply item”中设置最基本的属性，命令为：

Framed-Protocol PPP

Service-Type Framed-User

3）添加用户，为该用户组起一个名字：dfd，并设定该用户的密码。

4）进入了用户属性设置界面，选择“add to group”→“all_user 组”→“确定”，就可以看到，该用户如下“reply item”：

Framed-Protocol PPP

Service-Type Framed-User

5）如果需要设置该用户的时间限制，则需要输入时间限制的数字，时间单位为秒。

6）如果需要是设置回拨，在“reply item”中选择“Cisco-AVPair lcp:callback-dialstring=8765432（回拨的电话号码）”。

2、拨号服务器的设置

经过上述步骤，RADIUS 服务器基本建立完毕了。为了让拨号服务器使用 RADIUS 作为拨号用户的身份验证方式，必须在拨号服务器上作相应的设置。本例中以 Cisco 2610 路由器作为拨号服务器，在配备了 16 端口的异步串口模块后，可以允许 16 个用户同时拨入。在 Cisco 2610 上完成拨号基本配置可以正常工作后，需要加入如下语句来使用 RADIUS 作身份认证和记账。

```
…
dfd new-model
dfd authentication login default line enable
dfd authentication ppp default radius local
dfd authorization exec default radius none
dfd authorization network default radius local
dfd accounting network default start-stop radius
…
radius-server host 202.197.89.19 auth-port 1812 acct-port 1813
radius-server key cisco
…
!
```

使用 Linux 作拨号服务器的同时，也可以使用 RADIUS 作身份认证和记费，但需要安装 radiusclient-0.2.7.tar.gz。具体步骤为：

（1）必须已经配置好拨号服务器 PPP Server，使其能够正常工作，修改/etc/mgetty+sendfax/login.config 文件，去掉下面一行的注释符号：

/AutoPPP/ - a_ppp /usr/sbin/pppd-radius

目的是实现基于 RADIUS 的 PAP 验证，使通过 Windows 95/98 的拨号用户不需弹出终端窗口，直接在拨号窗口中输入用户 ID 和口令即可进入。

（2）修改/etc/options 文件，需要去掉 idle 600 等配置项，因为 pppd-radius 这个脚本不支持这些参数。在配置文件中添加参数 radius 和 radacct，这两项是告诉 pppd-radius 要用 RADIUS 进行验证。

（3）修改/etc/radiusclient/radiusclient.conf 文件，具体为：

auth_order radius，local #验证顺序
login_tries 4
login_timeout 60
nologin /etc/nologin

issue /etc/radiusclient/issue
authserver 202.197.89.19 #RADIUS Server 的地址，可以是 localhost
acctserver 202.197.89.19 clients/etc/raddb/clients #作为 client 的一些配置
login_radius /usr/sbin/login.radius
seqfile /var/run/radius.seq
mapfile /etc/radiusclient/port-id-map
default_realm
radius_timeout 10
radius_retries 3
login_local /bin/login
port_pool /etc/radiusclient/modem-pool

（4）修改/etc/raddb/clients 文件。并在对应 Client Name 处写入 Radius Server 的 IP 地址，也就是在/etc/radiusclient/radiusclient.conf 文件中定义的 authserver 和 acctserver 的地址，在对应 Key 处应加上保密字。

至此，linux 下远程认证拨号用户服务就完成了。



Q & A

问：查看系统信息的命令有哪些？

答：查看系统信息的命令主要有：

show version	查看系统软硬件配置信息
show configuration	查看保存在闪存中的配置信息
show running-config	查看交换机正在执行中的配置信息
show interface brief	查看交换机端口的主要信息
show vlan	查看 VLAN 信息
show ip ospf config	查看 OSPF 相关的配置信息
show ip interface	查看已经配置了 IP 地址的端口的状态信息
show ip route	查看交换机的路由信息