

Aula 13



Servidor RADIUS

Prof. Roitier Campos Gonçalves

Protocolo RADIUS

O RADIUS foi criado para ser utilizado em serviços de acesso por telefone, pela sua simplicidade, eficiência e facilidade de implementação. Actualmente suporta VPNs (Virtual Private Network), norma 802.1x que é a usada na autenticação de clientes em ambientes de rede.

O RADIUS (Remote Authentication Dial In User Service - Serviço de Autenticação Remota de Utilizadores por Acesso Telefónico), é um protocolo normalmente usado em ISPs e em empresas que façam controlo de acesso à rede.

Este protocolo pode ser usado em vários tipos de tecnologia como por exemplo, a tecnologia DSL , Wireless e VPN, permitindo efetuar a autenticação, autorização e registo (AAA) do cliente que acessa aos serviços. Inicialmente

Características

- Protocolo aberto, assim qualquer fabricante/utilizador pode utilizá-lo sem custos;
- É independente do sistema operacional;
- É considerado um protocolo seguro;
- É escalável e expansível, sendo capaz de acompanhar a evolução/necessidades futuras;
- Simples de implementar, tanto no lado do servidor RADIUS como no cliente;

Funcionamento

O RADIUS utiliza protocolo UDP e normalmente utiliza as portas 1812 ou 1645 para autenticação e 1813 ou 1646 para registro.

O servidor RADIUS é responsável por:

- Receber os pedidos de ligação dos clientes RADIUS (ex. Pontos de acessos);
- Autenticar os clientes remotos (utilizadores móveis, cliente);
- Ceder informação de clientes RADIUS (AP) para que este permita ou negue o acesso aos clientes remotos.
- Autorizar os clientes de modo a que estes possam acessar a determinados recursos.

AAA

Authentication

Who are you?



Authorization

How much can you spend?

Statement of Personal Credit Card Account

Cardmember Name: JOE EMPLOYEE Account Number: 1234-456-890 Statement Closing Date: 01-31-01

Statement Date: 02-01-01 Payment Due Date: 03-01-01

Closing Date: 01-31-01

Credit Limit: \$1,500.00 Credit Available: \$1,021.50

New Balance: \$278.50 Minimum Payment Due: \$20.00

Account Summary

Previous Balance:	+74.24	Transaction Fees:	+3.00
Purchases:	+250.50	Annual Fees:	+25.00
Cash Advances:	+0	Current Amount Due:	+250.50
Payments:	-74.25	Amount Past Due:	+0
Finance Charge:	+0	Amount Over Credit Line:	+0
Late Charge:	+0	NEW BALANCE:	\$278.50

Reference Number	Bill	Posted	Activity Since Last Statement	Amount
4329097	01-03	01-13	Payment, Thank You	-\$74.25
01234567	01-12	01-13	Wings 'N' Things Anytown, USA	\$25.25
78901234	01-14	01-17	Record Release Anytown, USA	\$40.00
45678901	01-14	01-17	Sports Stadium Anytown, USA	\$75.25
3210987	01-22	01-23	Tie Tack Anytown, USA	\$20.75
76543210	01-26	01-30	Electronic World Anytown, USA	\$89.25
23456789		01-30	Transaction Fees	\$3.00
34567890		01-01	Annual Fee	\$25.00

PAGE 1 OF 1

Accounting

What did you spend it on?



FreeRADIUS

O desenvolvimento do projeto FreeRADIUS iniciou-se em Agosto 1999 por Alan DeKok e por Miquel Smoorenburg.

Este servidor ganhou muita popularidade devido à integração de módulos para o suporte de LDAP, SQL entre outros. Foi também adicionado o suporte para EAP pelos meados de 2001, assim como PEAP e EAP-TTLS em 2003, o suporte EAP é muito importante, pois é utilizado pelos APs Cisco.

Atualmente o FreeRADIUS suporta um sistema de proxying, load-balance e fail-over .

FreeRadius é um dos servidores de autenticação mais usados pelas Universidades e Politécnicos portugueses, para autenticação, autorização e gestão de utilizadores na rede eduroam.

Principais funcionalidades

Métodos de autorização

- Local
- LDAP
- Bases de dados
MySQL/PostgreSQL/Oracle

Métodos de Accounting (Regostro)

- local (ficheiros com informação detalhada)
- suporte para SQL (Oracle, MySQL, PostgreSQL, Sybase, ODBC, etc)

Métodos de autenticação

- PAP
- CHAP
- MS-CHAP
- MS-CHAPv2
- Kerberos
- EAP
 - EAP-MD5
 - Cisco LEAP
 - EAP-MSCHAP-v2
 - EAP-GTC
 - EAP-SIM
 - EAP-TLS

Instalação do FreeRADIUS

Instalação do FreeRADIUS

```
# apt-get install freeradius-mysql mysql-server -y
```

Instalação do Mysql

```
#apt-get install mysql-server
```

```
# apt-get install freeradius-mysql
```

Verificando a instalação

```
# freeradius -X
```

```
read_config_files: reading clients
```

```
read_config_files: reading realms
```

```
There appears to be another RADIUS server running on the authentication port 1812
```


Configuração do radius.conf.

Por padrão do *Debian* ele fica em `/etc/freeradius/`.

```
# nano /etc/freeradius/radius.conf
```

Dentro de "authorize", tirar o comentário "#" da linha sql.

Dentro do "accounting", tirar o comentário "#" da linha sql.

```
# nano /etc/freeradius/sql.conf
```

Nas linhas:

```
server = "localhost"  
login = "root"  
password = "rootpass"
```

coloque os dados correspondentes do banco de dados

Configuração do `clients.conf`

Editando o arquivo `clients.conf`, que pode e será o nosso "NAS".

Obs: Em produção, pode ser qualquer aparelho que pode enviar o pedido de autenticação ao Radius.

```
# vi /etc/freeradius/clients.conf
```

Vamos ao final do arquivo, nele poderemos verificar vários exemplos de configuração. Colocaremos assim:

```
client 10.1.1.200 {  
    secret = senhateste  
    shortname = testesamente  
    nastype = other  
}
```

Configurações do BD

Baixar em:

<http://roitier.pro.br/wp-content/uploads/2016/02/Configura%C3%A7%C3%A3o-de-Banco-de-Dados-do-FreeRADIUS.odt>

Testando o FreeRADIUS

```
# freeradius -X
```

Se estiver, aparecerá mensagem semelhante a essa:

```
read_config_files: reading clients
read_config_files: reading realms
There appears to be another RADIUS server running on the authentication port 1812
```

Agora vamos efetuar o teste de autenticação. Para isso vamos usar o programa *radtest*, que vem junto com o *Freeradius*:

```
# radtest <usuárioi> <password> <ip NAS> <porta NAS> senhateste
```

aparecerá a seguinte resposta:

```
Sending Access-Request of id 74 to 10.1.1.200:1812
  User-Name = "usuário03"
  User-Password = "user03"
  NAS-IP-Address = tdebian
  NAS-Port = 0
rad_recv: Access-Accept packet from host 10.1.1.200:1812, id=74, length=20
```

Aqui finalizamos os testes.