

Radius

Autenticando sua equipe nos equipamentos de maneira simples, segura e barata.

MUM – Brasil – Novembro de 2012
Lacier Dias



Nome: Lacier Dias

- ✓ Formado em Segurança da Informação
- ✓ Pós-Graduado em Segurança de Rede de Computadores
- ✓ MBA em Gerenciamento de Projetos – FGV

- ✓ Treinamentos e Certificações:
 - IPV6
 - MikroTik Consultant, MTCNA, MTCWE, MTCUME, MTCRE e MTCINE,
 - Microsoft Certified Professional,
 - ITIL, Cobit,
 - BSC (Balanced Scorecard),
 - ISO 27001 e 27002,
 - Motorola, Proxim, Alvarion e Ubiquiti,
 - Allied Telesis, Cisco e Juniper,
 - Hughes Networks.





Publico Alvo e Objetivos da Apresentação

➤ **Publico Alvo**

- ✓ Administradores de redes de pequenos/médios provedores de serviço de acesso à Internet e Telecomunicações Wireless e/ou Cabeados.

➤ **Objetivos:**

- ✓ Apresentar uma solução simples e eficiente para administrar os acessos de suporte aos equipamentos que suportam Radius.



O que é Radius????

➤ RADIUS (Remote Authentication Dial In User Service) - É um protocolo criado para autenticação remota de usuários, onde um cliente, como por exemplo um Mikrotik, requer ao servidor RADIUS a validação de um usuário.

Os nomes de usuários e senhas, são mantidos guardados de maneira segura e centralizado.

O registrador RADIUS rastreia as transações de autorização e autenticação e captura as estatísticas de cada sessão.

Existem muitos servidores RADIUS gratuitos disponíveis na Web e vamos analisar um dos mais usuais: **FreeRadius**.





Instalando FreeRadius

➤ Com o Linux do seu sabor preferido instalado, atualizado, com acesso a internet e logado como root, vamos instalar o serviço Radius.

➤ Dependendo do seu Linux - Digite o comando:

```
# yum install freeradius – Família RedHat
```

```
# apt-get install freeradius – Família Debian
```

➤ Demais Sistemas:

```
# cd /usr/local/src
```

```
# wget ftp://ftp.freeradius.org/pub/radius/freeradius-x.x.x.tar.gz
```

```
# tar -xvzf freeradius-x.x.x.tar.gz
```

```
# cd freeradius-x.x.x/
```

```
# ./configure
```

```
# make
```

```
# make install
```

*free***RADIUS**



Configurando o FreeRadius:

➤ RADIUSD.CONF

Entre na pasta onde o radius está instalado, “ /etc/raddb”, vamos editar o arquivo “radiusd.conf”.

Editaremos as linhas conforme abaixo:

```
#
stripped_names = yes

# Log authentication requests to the log file.
#
# allowed values: {no, yes}
#
auth = yes

# Log passwords with the authentication requests.
# auth_badpass - logs password if it's rejected
# auth_goodpass - logs password if it's correct
#
# allowed values: {no, yes}
#
auth_badpass = yes
auth_goodpass = yes

# Log additional text at the end of the "Login OK" mess
```

- Desse modo o sistema vai gerar log para facilitar a auditoria de acesso nos equipamentos.



Configurando o FreeRadius:

➤ CLIENTS.CONF

Ainda na pasta onde o radius esta instalado “/etc/raddb” editaremos o arquivo “clients.conf”

Dentro do arquivo “clients.conf” vamos inserir as linhas com as redes que podem solicitar autenticação no radius.

➤ Detalhando a configuração:

client 192.168.0.0/24 { - # É o numero do ip ou da rede que pode solicitar autenticação.

secret = senha_da_rede - # É a chave do servidor, somente os hosts que possuem essa chave poderão solicitar usuário e senha para autenticação usando radius.

shortname = nome_da_rede - # É o nome do IP da rede ou do cliente. É muito importante esta configuração, pois é utilizado no log para analise.

```
#Rede do escritorio
client 192.168.0.0/24 {
    secret          = senha_da_rede
    shortname       = nome_da_rede
}
```



Configurando o FreeRadius:

➤ USERS

Vamos agora as configurações dos usuários dos técnicos:
Acessando o arquivo “users” no diretório onde o radius está instalado.

➤ **Tipo 1:** Configuração mais simples com a senha em texto plano no arquivo users.

➤ **Detalhando a configuração:**

“novousuario” # É o login de acesso.

Cleartext-Password := "novasenha" # Senha de acesso.

Reply-Message = "Hello, %{User-Name}" # Mensagem quando o usuário loga.

```
#
# "John Doe"      Cleartext-Password := "hello"
#                  Reply-Message = "Hello, %{User-Name}"
#
"novousuario"    Cleartext-Password := "novasenha"
                  Reply-Message = "Hello, %{User-Name}"
#
# Dial user back and telnet to the default host for that port
```




Configurando o FreeRadius:

➤ USERS

Tipo 2: Configuração mais elaborada com a senha criptografada.

➤ Detalhando a configuração:

"joaosilva" # Login de acesso.

Mikrotik-Group = "read", # Define qual nível de acesso do usuário. Read, Full ou Personalizado.

Reply-Message = "Hello, %{User-Name}" # Mensagem quando o usuário loga.

```
#
#"John Doe"      Cleartext-Password := "hello"
#                Reply-Message = "Hello, %{User-Name}"
#
#usuario com permissao para ler
"joaosilva"      Auth-Type := "Accept"
                 Mikrotik-Group = "read",
                 reply-Message = "Bem Vindo, %{User-Name}"
#Administrador
"walisson"       Auth-Type := "Accept"
                 Mikrotik-Group = "full",
                 reply-Message = "Bem Vindo, %{User-Name}"
#
```



Criando usuários para o Radius com senha criptografada pelo Linux

➤ Usuário no Linux.

➤ Como criar o usuário sem dar acesso ao servidor???????????

```
# adduser -M -s '/sbin/nologin' joaosilva  
# passwd joaosilva
```

➤ Digite a senha e confirme, pronto, criamos o usuários com a senha criptografada.

➤ Agora para inicie o serviço Radius no seu Linux preferido:

✓ Família RedHat:

```
# service radiusd start ou restart caso já esteja ativado.
```

✓ Família Debian:

Em outras distribuições o comando :

```
# /etc/init.d/radiusd start ou restart caso já esteja ativado.
```

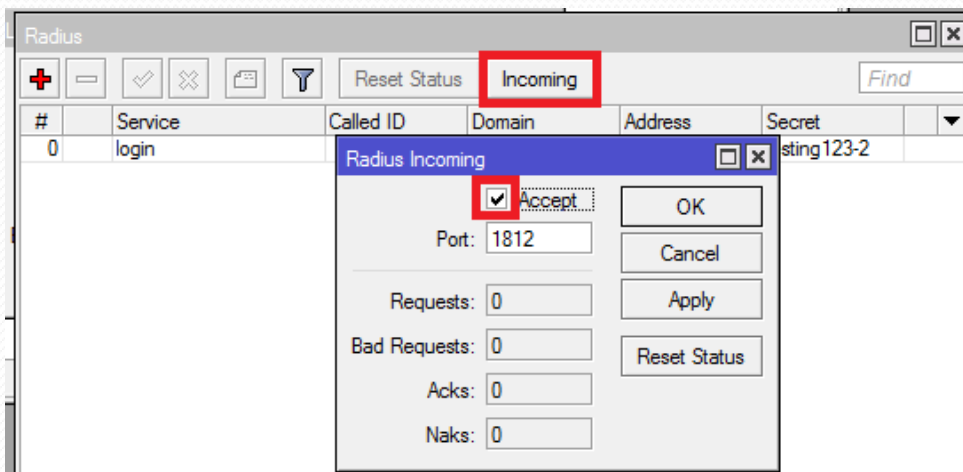
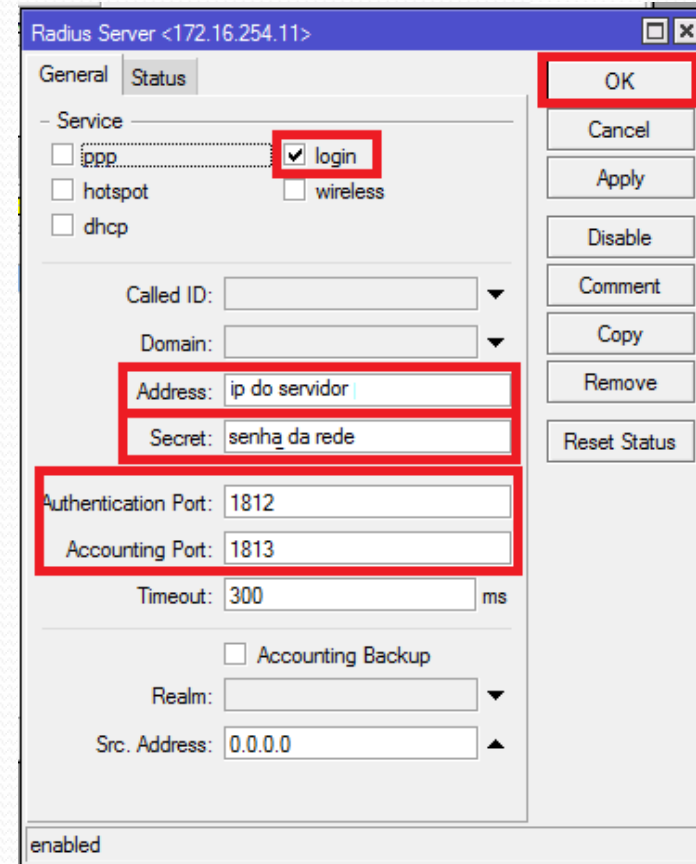
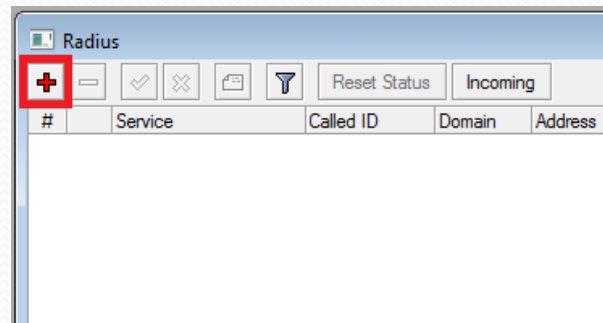




Configurando Radius no Mikrotik

- Acessando seus equipamentos pelo Winbox e tendo certeza que eles pingam o servidor radius, vamos as configurações.

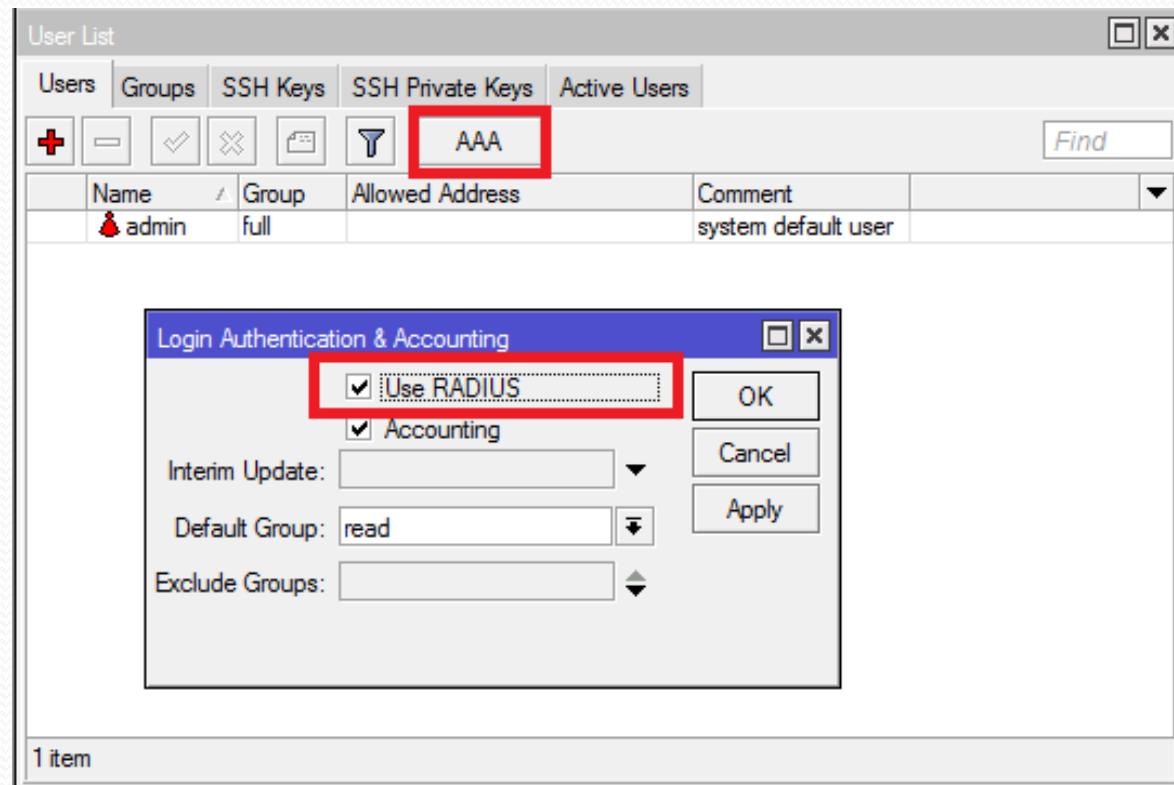
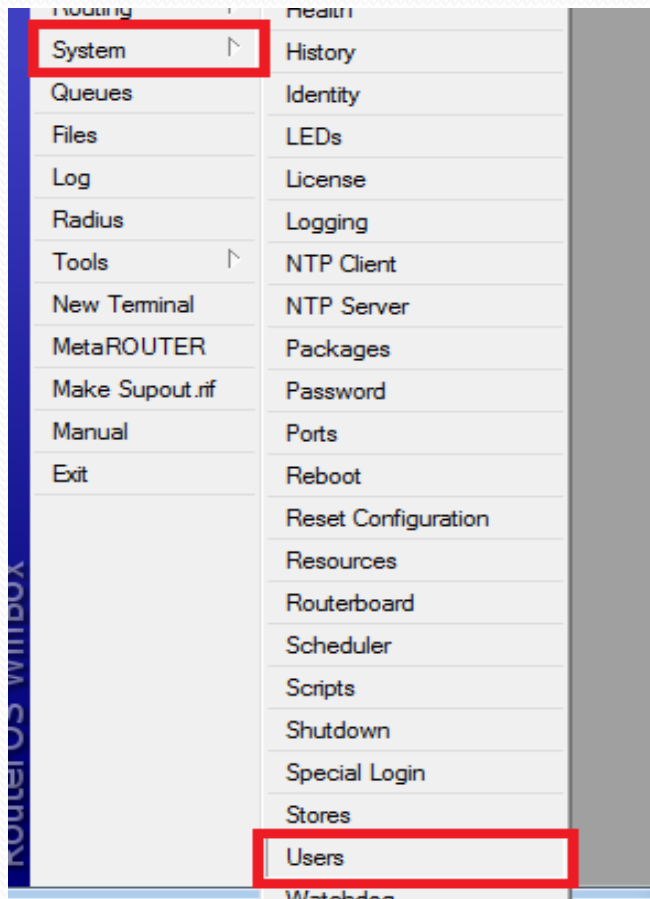
- **Passo 1:** Configurar o Mikrotik para consultar o Radius apenas nas solicitações de Login.





Configurando Radius no Mikrotik

- **Passo 2:** Configurar a função Users para usar o Radius e ter como opção default apenas acesso de Leitura.





Configurando Radius no Mikrotik

- **Passo 3:** Personalizando opções de login de acordo com a demanda.

Safe Mode

Interfaces
Bridge
PPP
Switch
Mesh
IP
IPv6
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
MetaROUTER
Make Supout.rif
Manual
Exit

User List

Users Groups SSH Keys SSH Private Keys Active Users

+ - [] [] Find

	Name	Policies	Skin
S	full	local telnet ssh ftp reboot read write policy test winbox passw...	default
	personalizado	local ssh reboot read test winbox password sniff sensitive	default
S	read	local telnet ssh reboot read test winbox password web sniff s...	default
S	write	local telnet ssh reboot read write test winbox password web ...	default

4 items

Group <personalizado>

Name: personalizado

OK Cancel

- Policies

local telnet
 ssh ftp
 reboot read
 write policy
 test winbox
 password web
 sniff sensitive
 api

Skin: default

System

Analizando logs do Radius



➤ Teste o login.

➤ Caso ocorra erro devemos analisar os logs no Linux com o comando:

```
# tail -f /var/log/radius/radius.log
```

➤ Tipos mais comuns de logs:

Log de um acesso correto:

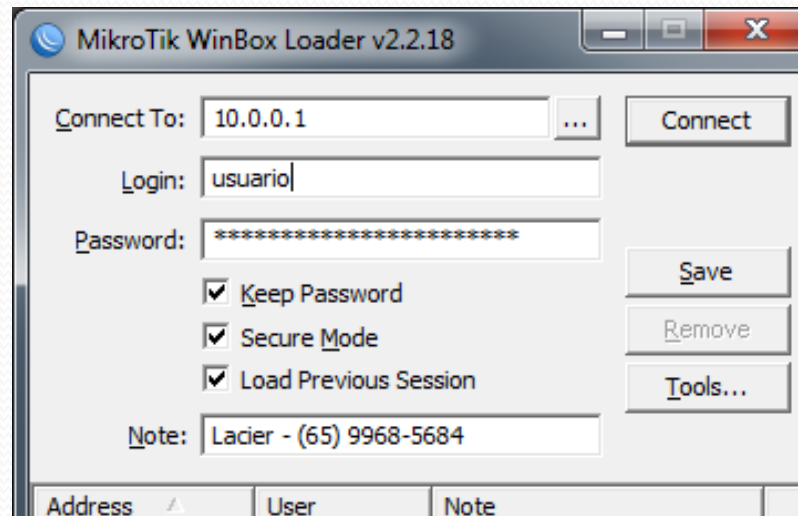
```
Sun Nov 04 03:33:27 2012 : Auth: Login OK: [walisson/<MD5-Password>] (from client POP-02 port 0 cli 10.172.192.1)
```

#Log por erro de senha:

```
Sun Nov 04 03:42:34 2012 : Auth: Login incorrect (rlm_chap: Clear text password not available): [joaopaulo/<MD5-Password>] (from client POP-07 port 0 cli 10.172.192.1)
```

#Log de rede não cadastrada no arquivo clientes.conf:

```
Sun Nov 04 03:54:23 2012 : Error: Ignoring request to authentication address * port 1812 from unknown client 10.99.123.1 port 60296
```





Conclusão

Simplifique. Fuja do complexo e diga não ao supérfluo.

Perguntas?????





Obrigado!!!

Lacier Dias

lacier@titania.com.br

Skype: lacier.dias

(65) 9968-5684

mum

Natal, November 26-27, 2012

MikroTik User Meeting