**FACULDADE DE TECNOLOGIA SENAC GOIÁS**

**PROJETO DE REDES DE COMPUTADORES**

LogoSenac

Jefferson Medrado  
Desiron Gonçalves

Lucas Santos

**FreeRADIUS**

GOIÂNIA,

2018Jefferson Medrado  
Desiron Gonçalves

Lucas Santos

**FreeRADIUS**

Componente do Projeto Integrador 2018-1 apresentado como requisito parcial de avaliação na disciplina de Projeto de Redes de Computadores, no Curso de Gestão da Tecnologia da Informação, na Faculdade de Tecnologia Senac Goiás, ministrado pela professora Kelly Alves.

GOIÂNIA,

2018

**RESUMO**

FreeRADIUS é o servidor open source que suporta o maior número de tipos de autenticação e, atualmente, é o único servidor RADIUS de código livre que suporta o protocolo EAP - *Extensible Authentication Protocol*. Além disto, FreeRADIUS é o único que suporta virtualização, mantendo os custos de implantação e manutenção baixos. Seu desenho modular é fácil de entender, permitindo facilmente a inclusão ou remoção de módulos sem afetar o desempenho, os requisitos de hardware, de memória ou a segurança do sistema. Tem-se o com principal função o controle de acesso através de autenticações utilizando a rede WIFI.

Palavras-chave: FreeRADIUS, servidor, autenticação e controle de acesso.

**SUMÁRIO**

[INTRODUÇÃO 5](#_Toc516918912)

[CONHECENDO O FREERADIUS 6](#_Toc516918913)

[INSTALANDO O FREERADIUS 7](#_Toc516918914)

[CONFIGURANDO O FREERADIUS 9](#_Toc516918915)

[ADICIONANDO CLIENTES 11](#_Toc516918916)

[DEFINIR MÉTODOS EAP 12](#_Toc516918917)

[ADICIONAR USUÁRIOS 13](#_Toc516918918)

[AUTENTICAÇÃO DE TESTE 14](#_Toc516918919)

[INICIE O FREERADIUS 14](#_Toc516918920)

[CONCLUSÃO 15](#_Toc516918921)

[REFERENCIAS BIBLIOGRÁFICAS 16](#_Toc516918922)

# INTRODUÇÃO

Este trabalho tem o objetivo de apresentar a ferramenta FreeRADIUS ao leitor e a efetuar a capacitação de sua respectiva instalação. Esse software tem como função ser um servidor RADIUS de gerenciamento e controle de acesso através de autenticações utilizando a rede WIFI.

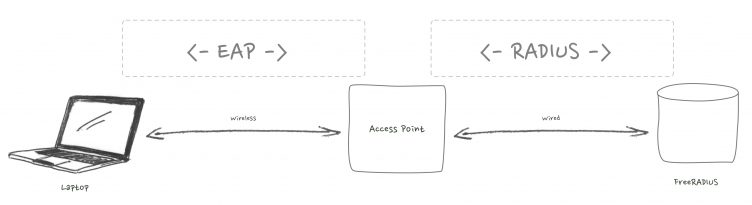
# CONHECENDO O FREERADIUS

O FreeRADIUS é um servidor RADIUS de código aberto utilizado por muitas organizações. Possui suporte a muitos protocolos de autenticação e é muito popular porque é modular e escalável tendo o papel de proteger credenciais de usuário via Wi-Fi através de autenticações direcionadas ao servidor do qual será realizado o controle e gerenciamento dessas autenticações. Em nosso laboratório de Wi-Fi, usaremos o FreeRADIUS para autenticar usuários de Wi-Fi com o 802.1X.

IEEE 802.1X é um padrão IEEE pertencente ao grupo do protocolo IEEE 802.1 para controle de acesso sendo um mecanismo de autenticação para dispositivos que desejam juntar-se a uma porta na WLAN, seja estabelecendo uma conexão ponto-a-ponto ou prevenindo acesso para esta porta se a autenticação falhar. No 802.1X e em nosso laboratório, o FreeRADIUS desempenhará o papel de servidor de autenticação.

O mecanismo de autenticação 802.1X possui três componentes:

* Suplicante (dispositivo móvel)
* Autenticador (AP)
* Servidor de Autenticação (FreeRADIUS)



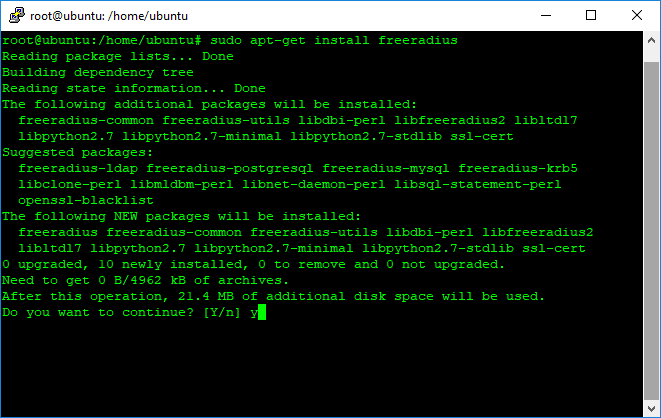
O suplicante solicitará a associação a um SSID, o autenticador solicitará uma identidade do dispositivo móvel, o autenticador encaminhará a identidade para o servidor de autenticação que responderá com êxito ou negação.

Este trabalho irá colocá-lo em funcionamento para isso implementaremos o FreeRADIUS no Ubuntu 16.04.1 LTS que eu temos rodando como uma VM.

# INSTALANDO O FREERADIUS

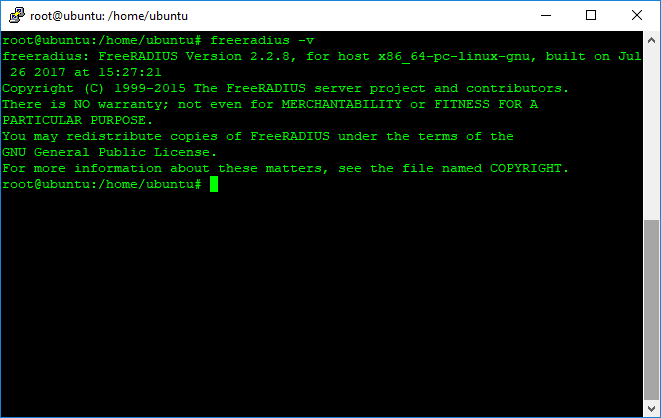
Para realizarmos a instalação, pressupomos que o leitor possua uma máquina VM com Ubuntu instalado e com todas as suas dependências em dia, sendo assim, seguiremos com a instalação. Para iniciarmos podemos começar com o apt-get. A instalação do FreeRADIUS também instalará dependências e pacotes adicionais necessários para a operação.

**$ sudo apt-get install freeradius**



* Verifique a versão do FreeRADIUS e se ele foi instalado, verificando a versão.

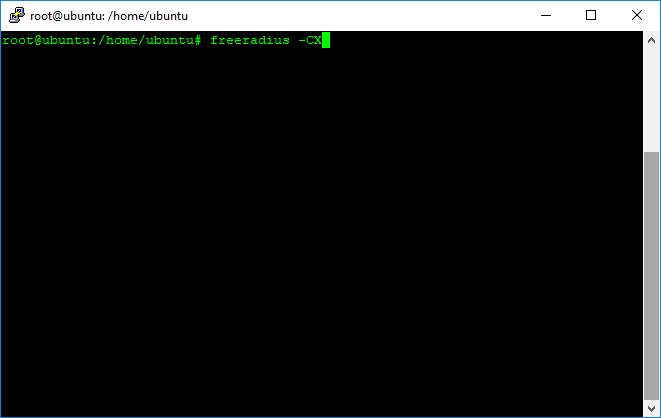
**$ freeradius –v**



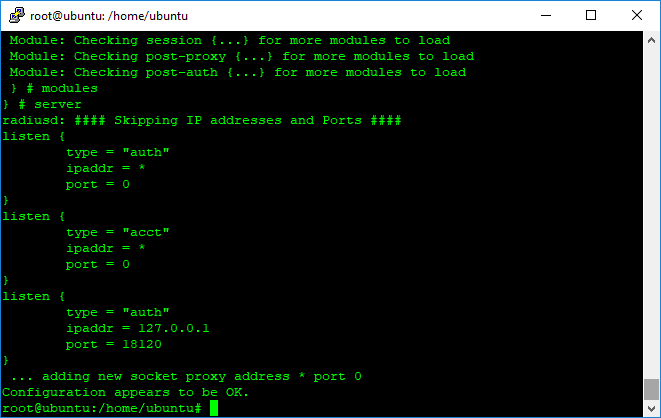
* Execute uma verificação rápida de configuração.

FreeRADIUS deve ser capaz de rodar com sucesso com todos os padrões.

**$ sudo freeradius -CX**



A saída na parte inferior exibirá:

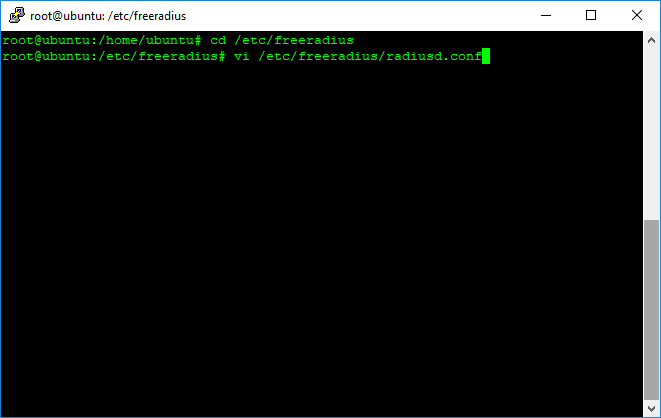


# CONFIGURANDO O FREERADIUS

* Os arquivos de configurações do FreeRADIUS estão localizados em / etc:

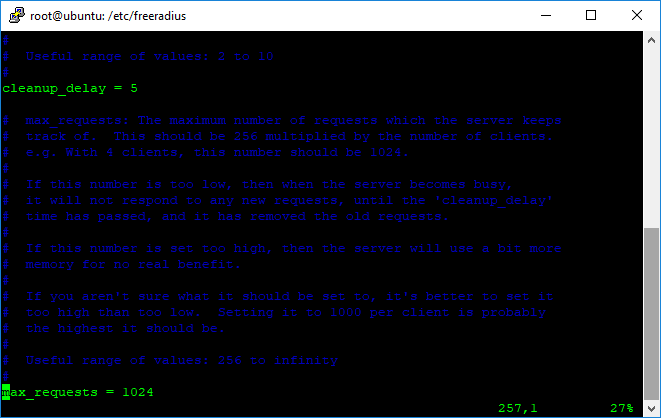
**cd /etc/freeradius**

**$ sudo vi /etc/freeradius/radiusd.conf**



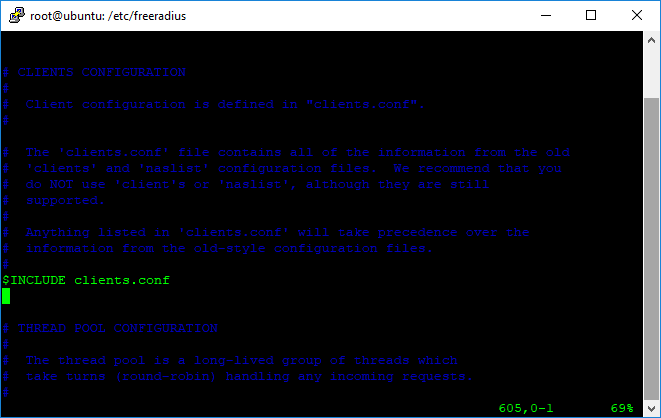
**Número máximo de pedidos:**

Aumente o valor padrão de 1024 se você planeja ter mais de 4 clientes autenticando por vez.

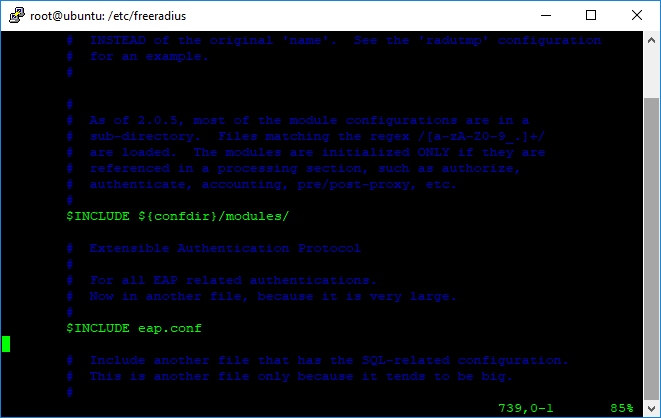


* Aqui é onde informamos ao FreeRADIUS para procurar por clientes autorizados (autenticadores).

Arquivo de configuração para seus **clientes** (pontos de acesso ou controladores)



Mais abaixo, no arquivo radiusd.conf, estão localizados os métodos EAP definidos, que é o arquivo eap.conf. Este arquivo de configuração é utilizado para definir métodos EAP usados:



# ADICIONANDO CLIENTES

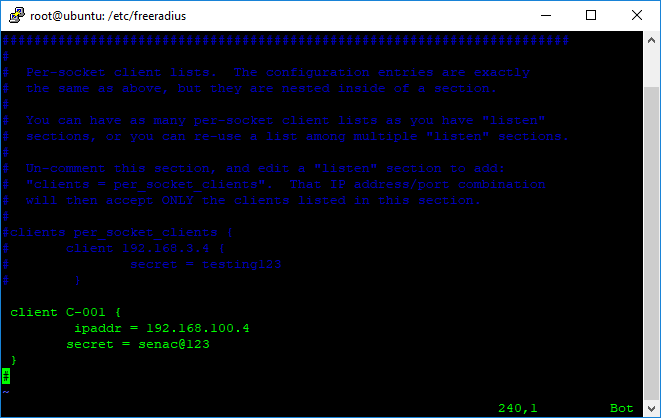
A palavra “clientes” pode ser enganosa, mas em termos de FreeRADIUS isso significa que os autenticadores, como os APs ou controladores de WLAN. Queremos verificar se apenas autenticadores autorizados são usados ​​em nossa rede. Os autenticadores e o servidor de autenticação usarão segredos compartilhados para verificar um ao outro.

* Abra o arquivo clients.conf para adicionar seu (s) autenticador (es).

**$ sudo vi clients.conf**

Se seus APs ou controladores estiverem em uma rede específica, você pode definir toda a rede ou especificar um segredo para clientes individuais.

Aqui é onde eu adiciono nosso ponto de acesso, que é um Cliente Networks C-001.

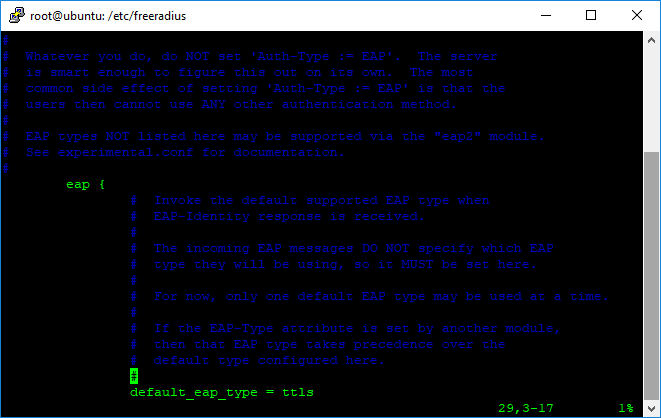


Em seguida, salve o arquivo e saia.

# DEFINIR MÉTODOS EAP

Agora, a parte divertida é saber quais métodos EAP você deseja usar. Eu não vou fazer um tutorial EAP aprofundado sobre este segmento. Em nosso laboratório estamos usando o EAP-TTLS porque requer o uso de um certificado do lado do servidor, mas os certificados do cliente são opcionais.

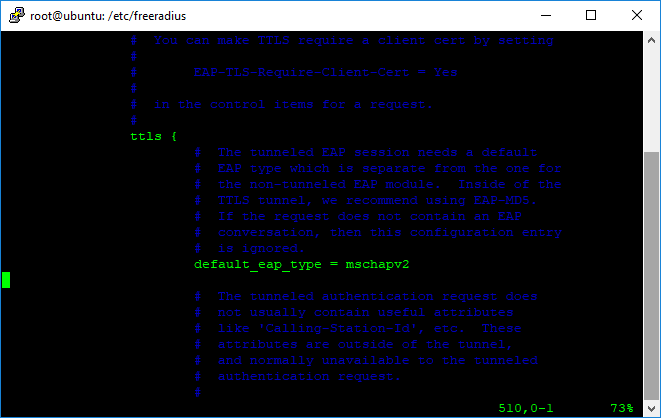
Por padrão, o FreeRadius usará o MD5, que não é muito forte.



Comente a de default\_eap\_type = md5 e altere para: **default\_eap\_type = ttls**

O FreeRadius vem com um certificado de servidor por padrão que usaremos para testes iniciais.Comente os tipos de EAP suportados de MD5, LEAP, GTC

* Em ttls, altere **default\_eap\_type** para **mschapv2**

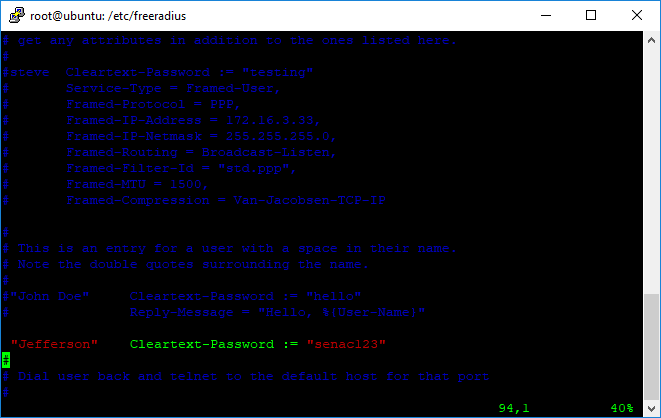


# ADICIONAR USUÁRIOS

Vamos adicionar usuários que serão autenticados neste servidor RADIUS. Edite o arquivo de usuários com este comando:

**$ sudo vi users**

Adicione uma conta ao arquivo:



* Jefferson = meu nome de usuário.

Cleartext-Password = declaração indicando que vamos atribuir uma senha de texto claro a esse nome de usuário. Observe que “: =“ é usado para atribuição.

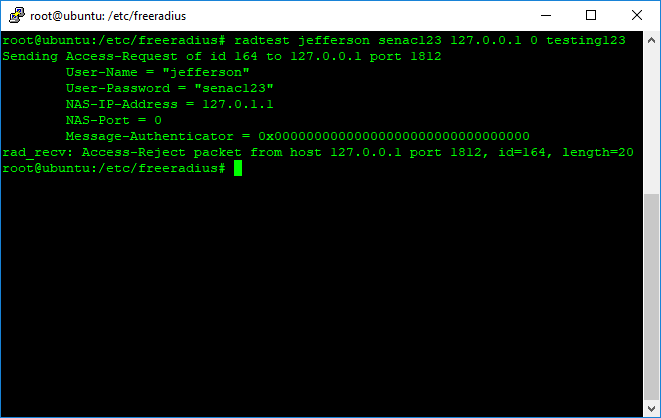
* senac123 = Minha senha super forte entre aspas.

Nesse cenário, os usuários são definidos em um arquivo usando senhas de texto não criptografado. Não é a coisa mais inteligente a se fazer na produção. Se você seguir esse caminho, você deve proteger este servidor muito bem.

# AUTENTICAÇÃO DE TESTE

Execute um teste rápido para ver se o FreeRADIUS aceitará o nome de usuário e a senha recém-criados. Executar isto a partir do servidor significa que você terá que usar o segredo configurado para o host local que é definido no arquivo clients.conf:

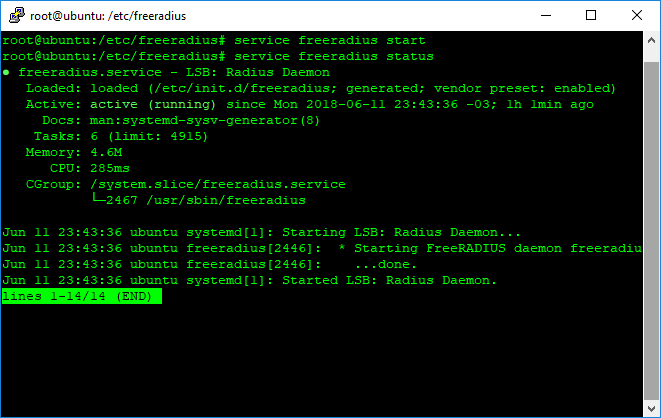
**$ radtest jefferson senac123 127.0.0.1 0 testing123**



# INICIE O FREERADIUS

**$ serviço freeradius start**

**$ status de serviço freeradius**



Agora você tem um servidor FreeRADIUS pronto para autenticar usuários em sua rede Wi-Fi. O próximo passo é configurar um ponto de acesso ou controlador para apontar para o seu servidor RADIUS. Tenha em mente que esses autenticadores estão listados no arquivo clients.conf com suas senhas. A senha será configurada no AP ou no controlador.

# CONCLUSÃO

A utilização de um sistema de autenticação como o FreeRdius é em uma opção extremamente interessante para empresas que desejam constituir uma rede WIFI com segurança e divisão de categorias de autenticação.

Este trabalho apresentou o conceito de segurança do FreeRADIUS, sua importância e um passo a passo de como realizar sua instalação e configuração básica, sendo assim, concluímos que o leitor está completamente apito a realizar todos os procedimentos desse trabalho conseguindo obter sucesso em sua instalação e uso da ferramenta.

# REFERENCIAS BIBLIOGRÁFICAS

INSTALAÇÃO E CONFIGURAÇÃO DO FREERADIUS. GIT HUB. Disponível em: < https://github.com/RafaelFazzolino/ServicoRadiusLdap/wiki/Instala%C3%A7%C3%A3o-e-configura%C3%A7%C3%A3o-do-FreeRadius>. Acesso em: 10 de Junho de 2018.

FREERADIUS – NOCÕES PARTE I. Disponível em: <https://www.vivaolinux.com.br/artigo/FreeRADIUS-Nocoes-basicas-Parte-I>. Acesso em: 12 Junho de 2018.

ENTENDENDO O FREERADIUS. Disponível em: < https://medium.com/@m0blabs/entendendo-o-freeradius-cfd788b47753>. Acesso em: 11 Junho de 2018.

FREERADIUS - UM SERVIDOR DE AUTENTICAÇÃO GRATUITO. Disponível em: < https://pplware.sapo.pt/linux/freeradius-um-servidor-de-autenticao-gratuito/>. Acesso em: 15 Junho de 2018.