Como instalar o FreeRADIUS no servidor Ubuntu

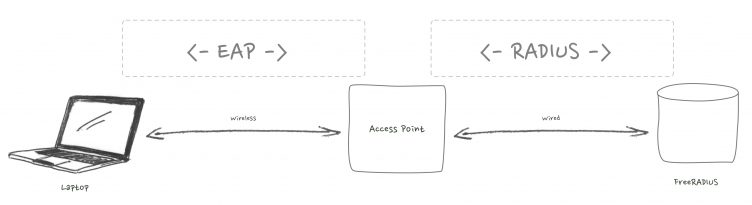
Não deixe o Wi-Fi ser o elo mais fraco da segurança. Protegendo credenciais de usuário via Wi-Fi não deve ser tomada de ânimo leve. No meu laboratório de Wi-Fi, uso o FreeRADIUS para autenticar usuários de Wi-Fi com o 802.1X.

O FreeRADIUS é um servidor RADIUS de código aberto usado por muitas organizações. Ele executa funções AAA, suportando muitos protocolos de autenticação e é muito popular porque é modular e escalável.

No 802.1X e no meu laboratório, o FreeRADIUS desempenhará o papel de servidor de autenticação. O FreeRADIUS pode ser o proxy para outro servidor de autenticação, como o Active Directory.

Sem entrar em muitos detalhes, o 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.

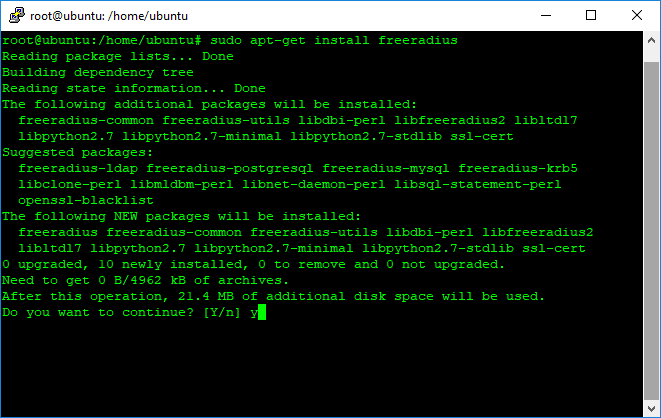
Este guia irá colocá-lo em funcionamento rapidamente com o FreeRADIUS no servidor Ubuntu usando o EAP-TTLS.

Minha implementação do FreeRADIUS foi feita no Ubuntu 16.04.1 LTS que eu tenho rodando como uma VM no meu notebook.

## **1. Instale o FreeRADIUS**

A instalação do FreeRADIUS é a parte mais fácil deste guia. Isso pode ser feito com o apt-get. A instalação do FreeRADIUS também instalará dependências e pacotes adicionais necessários para a operação.

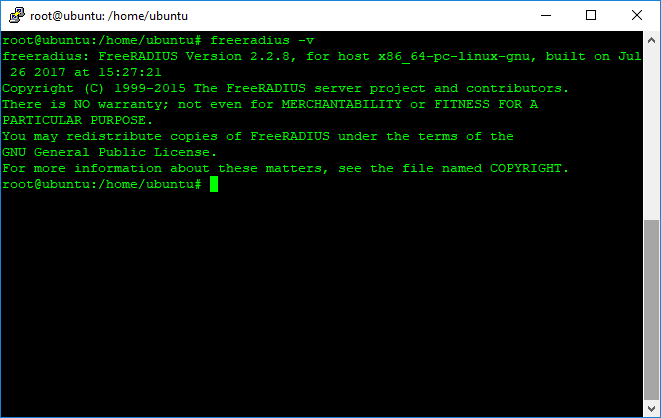
**$ sudo apt-get install freeradius**



## **2. Verifique a versão do FreeRADIUS**

Verifique se ele foi instalado, verificando a versão.

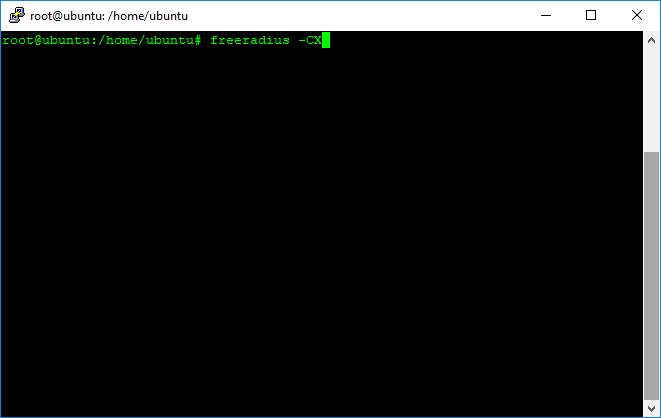
**$ freeradius -v**



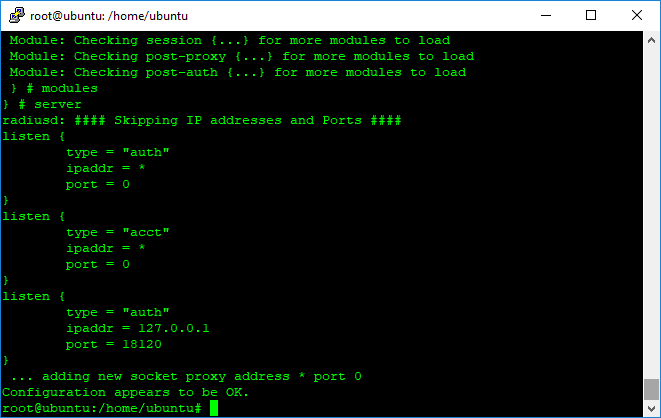
## **3. Execute uma verificação rápida de configuração.**

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

**$ sudo freeradius -CX**



A saída na parte inferior exibirá:

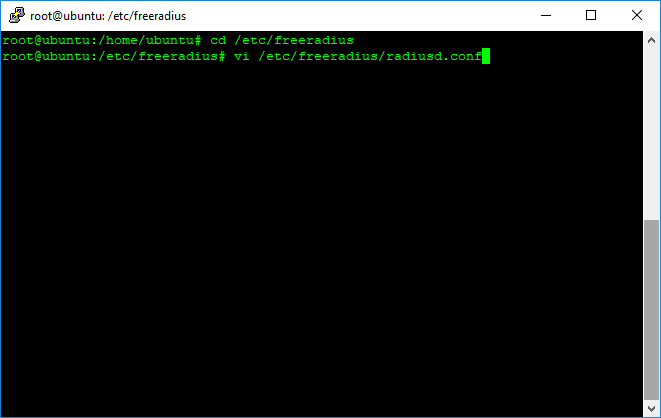


## **4. Revise os arquivos de configuração**

Os arquivos do FreeRADIUS estão localizados em / etc:

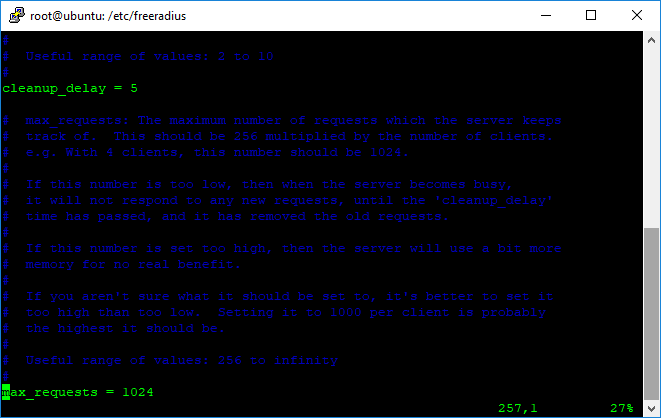
**cd /etc/freeradius**

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



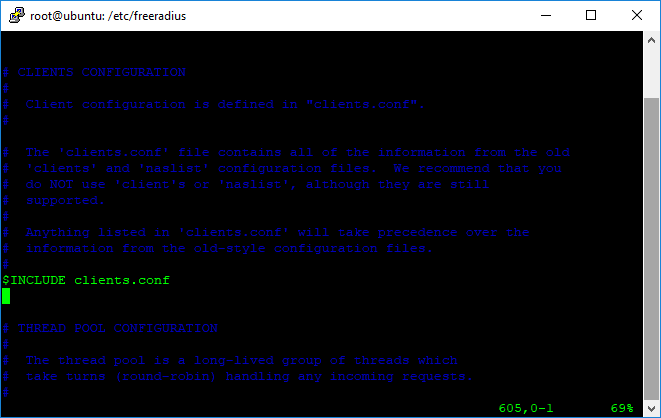
**Número máximo de pedidos:**

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



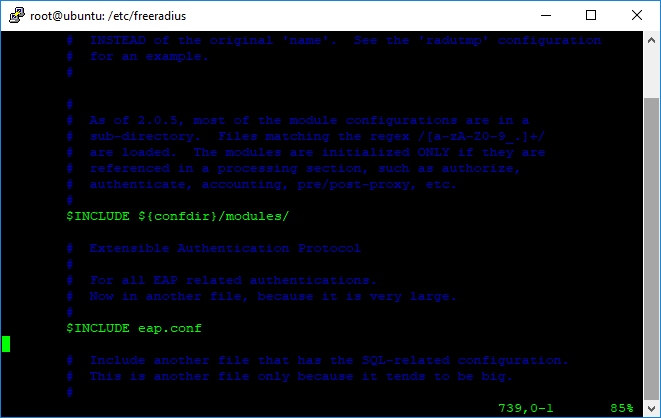
Aqui é onde dizemos ao FreeRADIUS para procurar por clientes autorizados (autenticadores).

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.

Arquivo de configuração EAP para definir métodos EAP usados:



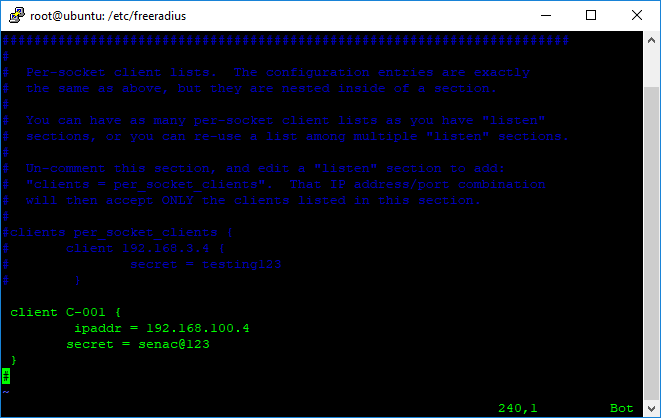
## **5. Adicionar Clientes**

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).

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 meu ponto de acesso, que é um Cliente Networks C-001.

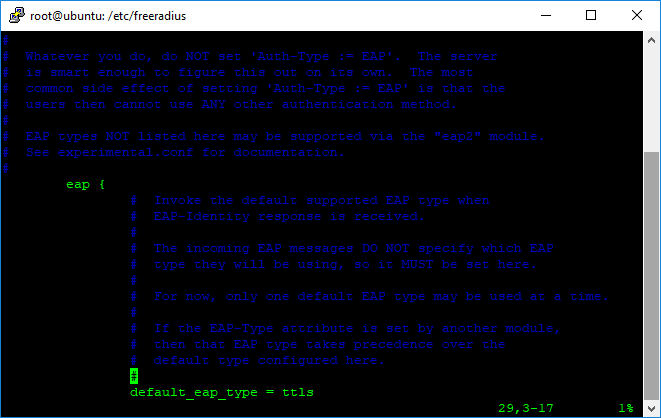


Em seguida, salve o arquivo e saia.

## **6. 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. Só sei que neste laboratório estou 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.



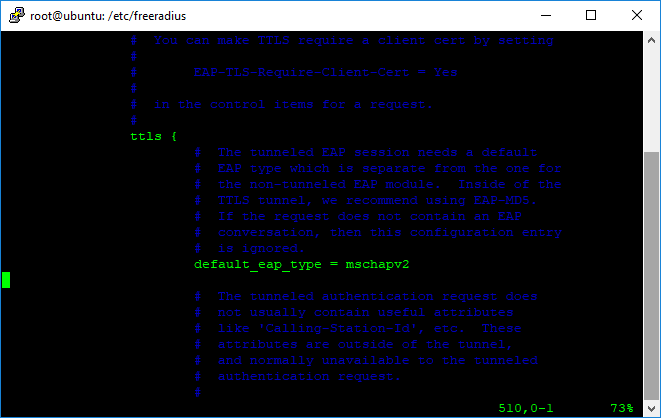
Comente a default\_eap\_type = md5 string e adicione:

**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**

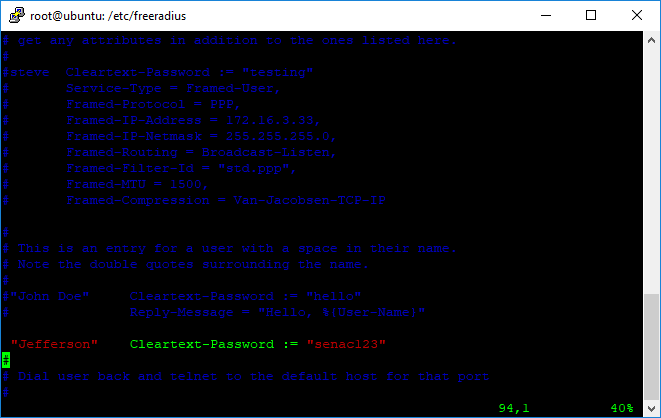


## **7. Adicionar usuários**

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:



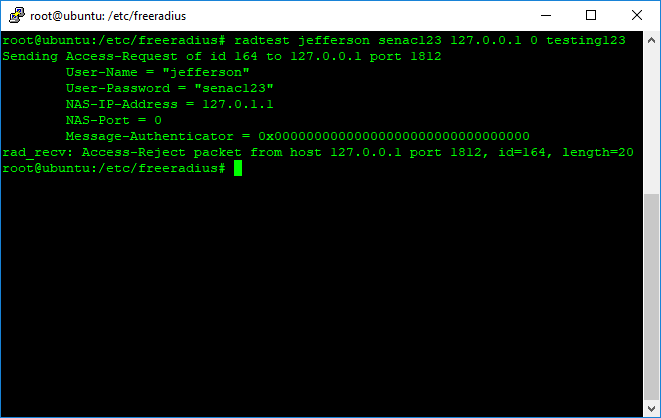
Jefferson = meu nome de usuário.   
Cleartext-Password = declaração indicando que vamos atribuir uma senha de texto claro a esse nome de usuário. Observe que “: =“ é usado para atribuição.   
Senac123 = Minha senha super forte entre aspas.

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.

## **8. 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:

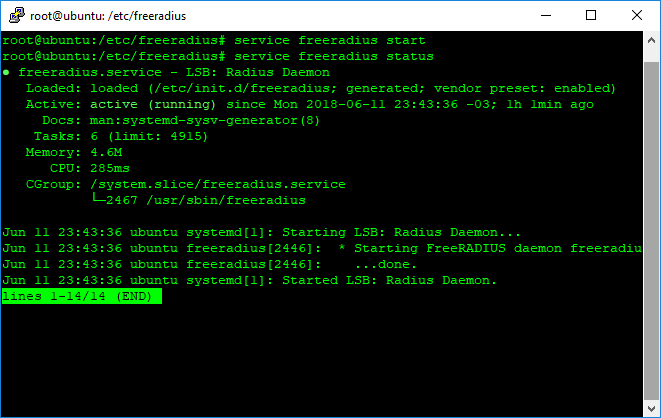
**$ radtest jefferson senac123 127.0.0.1 0 testing123**



## **9. 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.