

Procedimento de instalação do servidor IDP Eduroam

Objetivo

Este procedimento, tem como objetivo, auxiliar o usuário na execução do script de instalação do seu novo servidor IDP Eduroam



Este procedimento deve ser executado somente no Ubuntu versão 18.04 LTS 64bits

Entre em sua nova máquina Eduroam.

Utilizar o usuário root

```
sudo su -
```

Criar o diretório rnp dentro de /root

```
mkdir /root/rnp
```

Entrar no diretório /root/rnp

```
cd /root/rnp
```

IMPORTANTE:

Copiar o arquivo contendo o certificado que enviamos ao seu e-mail para dentro de seu novo servidor Eduroam, dentro do diretório /root/rnp
(Para copiar o arquivo de uma máquina Windows você pode utilizar por exemplo a ferramenta WinSCP <https://winscp.net/eng/download.php>)

Descompactar o arquivo recebido do certificado (ex. eduroam.ufcorrea.gov.br.tar.gz):

```
tar xzvf arquivo_recebido_em_seu_email.tar.gz
```

Baixar o script para instalar o Eduroam:

```
wget https://svn.rnp.br/repos/eduroam/atualiza_configura_idp_eduroam.bash
```

Mudar a permissão do arquivo para modo executável:

```
chmod +x atualiza_configura_idp_eduroam.bash
```

Executar o script:

```
./atualiza_configura_idp_eduroam.bash
```

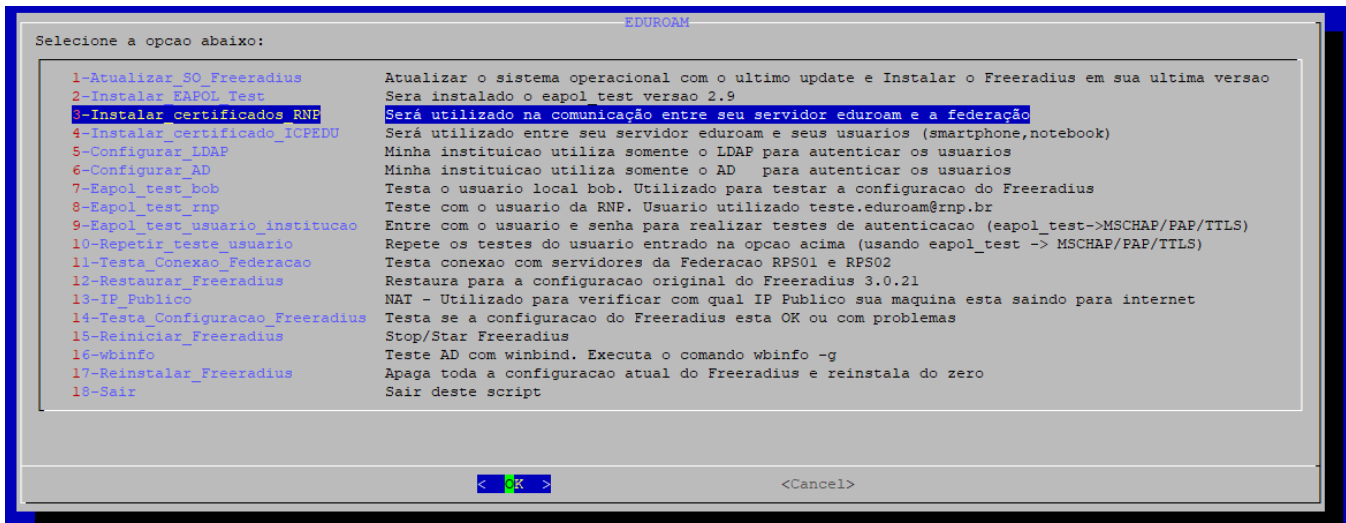
Após executar o comando `./atualiza_configura_idp_eduroam.bash` será mostrado uma janela com todas informações necessárias para dar início na configuração do **FREERADIUS**. Clique em [Yes](#) para seguir

```
root@diego: ~/mp
=====
= ATENÇÃO =
=====
Para dar continuidade ao processo de instalação favor ler cuidadosamente os itens abaixo:
Role a tela para baixo para ler até o final. Utilize as teclas "Page UP" ou "Page Down"
VOCÊ DEVE TER EM MÃOS AS SEGUINTE INFORMAÇÕES PARA A CONFIGURAÇÃO DO FREERADIUS:
=====
= Sobre sua nova máquina Eduroam =
=====
Tenha em mãos as seguintes informações:
Nome da máquina. Exemplo: eduroam
Domínio. Exemplo: instituicao.gov.br
FQDN (Nome da máquina mais domínio). Exemplo: eduroam.instituicao.gov.br
IP / Mascara / Gateway. Exemplo: 200.130.35.151 / 255.255.255.0 / 200.130.35.1
DNS direto. Exemplo: eduroam.instituicao.gov.br apontando para 200.130.35.91
DNS reverso. Exemplo: 91.35.130.200.in-addr.arpa apontando para eduroam.instituicao.gov.br
=====
= LDAP =
=====
Se sua instituição utiliza LDAP precisamos dos seguintes dados em mãos:
FQDN ou IP do servidor de LDAP. Exemplo: ldapi.instituicao.gov.br
Porta do servidor LDAP. Exemplo: 389 ou 636
Base DN. Exemplo: dc=instituicao,dc=local
Identity. Exemplo: uid=eduroam,ou=people,dc=instituicao,dc=local
Senha.
Favor solicitar a equipe de segurança a liberação no firewall para que este servidor eduroam consiga acessar o servidor LDAP.
=====
= AD - Microsoft Active Directory =
=====
Se sua instituição utiliza AD (Active Directory da Microsoft) precisamos das seguintes informações em mãos:
FQDN ou IP do servidor de AD. Exemplo: dc1.instituicao.local
Nome do domínio do AD. Exemplo: instituicao.local
Usuário com privilégios para inserir a máquina no domínio de seu AD.
Senha.
Favor solicitar a equipe de segurança a liberação no firewall para que este servidor eduroam consiga acessar o servidor do AD.
=====
= CERTIFICADO =
=====
Existem 4 certificados que podem ser utilizados
AD -> Certificado para o Samba se conectar com o AD, este certificado é gerado pela instituição e a responsabilidade pela instalação também é da Instituição.
LDAP -> Certificado para o Freeradius consultar a base LDAP, este certificado é gerado pela instituição e a responsabilidade pela instalação também é da Instituição.
EAP -> Certificado utilizado no Freeradius para conectar com segurança os seus usuários com Smartphone/Desktop via Wifi. Este certificado é auto assinado pela RNP mas a instituição deve gerar um certificado válido.
RADSEC -> Certificado auto gerado pela RNP para conectar com segurança a conexão da instituição à RNP
=====
= FIREWALL =
=====
Liberar a porta 2083 vindo das máquinas 200.130.35.98 e 200.143.193.92 para seu host eduroam (estes hosts são as máquinas rps01.eduroam.gov.br e rps02.eduroam.gov.br - são os hosts da Federação Brasileira do Eduroam)
Liberar temporariamente a saída do host eduroam para a internet pois nossos scripts dependem desta saída para testes a atualizações.
=====
= NAT =
=====
[1] Stopped ./atualiza_configura_idp_eduroam.bash < Yes > < No >
```

Na imagem abaixo selecione a opção #1 Atualizar o SO Freeradius, esta opção atualizará o seu sistema operacional com o último update e instalará o Freeradius em sua última versão

```
EDUROAM
Selecione a opcao abaixo:
1-Atualizar SO Freeradius Atualizar o sistema operacional com o ultimo update e Instalar o Freeradius em sua ultima versao
2-Instalar_EAPOL_Test Sera instalado o eapol_test versao 2.9
3-Instalar_certificados_RNP Sera utilizado na comunicacao entre seu servidor eduroam e a federacao
4-Instalar_certificado_ICPFEDU Sera utilizado entre seu servidor eduroam e seus usuarios (smartphone,notebook)
5-Configurar_LDAP Minha instituicao utiliza somente o LDAP para autenticar os usuarios
6-Configurar_AD Minha instituicao utiliza somente o AD para autenticar os usuarios
7-Eapol_test_bob Testa o usuario local bob. Utilizado para testar a configuracao do Freeradius
8-Eapol_test_rnp Teste com o usuario da RNP. Usuario utilizado teste.eduroam@rnp.br
9-Eapol_test_usuario_instituicao Entre com o usuario e senha para realizar testes de autenticacao (eapol_test->MSCHAP/EAP/TTLS)
10-Repetir_teste_usuario Repete os testes do usuario entrado na opcao acima (usando eapol_test -> MSCHAP/EAP/TTLS)
11-Testa_Conexao_Federacao Testa conexao com servidores da Federacao RPS01 e RPS02
12-Restaurar_Freeradius Restaura para a configuracao original do Freeradius 3.0.21
13-IP_Publico NAT - Utilizado para verificar com qual IP Publico sua maquina esta saindo para internet
14-Testa_Configuracao_Freeradius Testa se a configuracao do Freeradius esta OK ou com problemas
15-Reiniciar_Freeradius Stop/Star Freeradius
16-wbinfo Teste AD com winbind. Executa o comando wbinfo -g
17-Reinstalar_Freeradius Apaga toda a configuracao atual do Freeradius e reinstala do zero
18-Sair Sair deste script
< OK > < Cancel >
```

Neste próximo passo, daremos início na etapa **3 - Instalar Certificados RNP**, ele é responsável pela comunicação entre o seu servidor Eduroam e a federação. **Selecione o item 3**, em seguida clique em OK



Após selecionar a etapa **3 - Instalação do certificado RNP** será feito um backup dos arquivos de configuração, assim que pronto, tecle **S (sim)** para confirmar que os arquivos FQDN são correspondentes ao seu servidor Eduroam. Observe a imagem abaixo

```
root@diego:~/mp
EDUROAM
Selecione a opcao abaixo:
1-Atualizar SO Freeradius          Atualizar o sistema operacional com o ultimo update e Instalar o Freeradius em sua ultima versao
2-Instalar EAPOL Test             Sera instalado o eapol test versao 2.9
3-Instalar certificados RNP       Será utilizado na comunicação entre seu servidor eduroam e a federação
4-Instalar certificado_ICPEDU     Será utilizado entre seu servidor eduroam e seus usuarios (smartphone,notebook)
5-Configurar LDAP                 Minha instituicao utiliza somente o LDAP para autenticar os usuarios
6-Configurar AD                   Minha instituicao utiliza somente o AD para autenticar os usuarios
7-Eapol_test_bob                  Testa o usuario local bob. Utilizado para testar a configuracao do Freeradius
8-Eapol_test_rnp                  Teste com o usuario da RNP. Usuario utilizado teste.eduroam@rnp.br
9-Eapol_test_usuario_instituicao  Entre com o usuario e senha para realizar testes de autenticacao (eapol_test->MSCHAP/PAP/TTLS)
10-Repetir teste_usuario          Repete os testes do usuario entrado na opcao acima (usando eapol_test -> MSCHAP/PAP/TTLS)
11-Testa_Conexao_Federacao       Testa conexao com servidores da Federacao RPS01 e RPS02
12-Restaurar_Freeradius           Restaura para a configuracao original do Freeradius 3.0.21
13-IP_Publico                     NAT - Utilizado para verificar com qual IP Publico sua maquina esta saindo para internet
14-Testa_Configuracao_Freeradius  Testa se a configuracao do Freeradius esta OK ou com problemas
15-Reinstalar_Freeradius         Stop/Star Freeradius
16-wbinfo                         Teste AD com winbind. Executa o comando wbinfo -g
17-Reinstalar_Freeradius         Apaga toda a configuracao atual do Freeradius e reinstala do zero
18-Sair                            Sair deste script
< OK > <Cancel>

Fazendo backup dos arquivos de configuracao .....
./clients.conf - encontrado - OK
./proxy.conf - encontrado - OK
./radsec - encontrado - OK
./inner-tunnel - encontrado - OK
./default - encontrado - OK
./rnp-ca.crt - encontrado - OK

Encontrado os arquivos:
eduroam.ufcorrea.gov.br.crt
eduroam.ufcorrea.gov.br.key

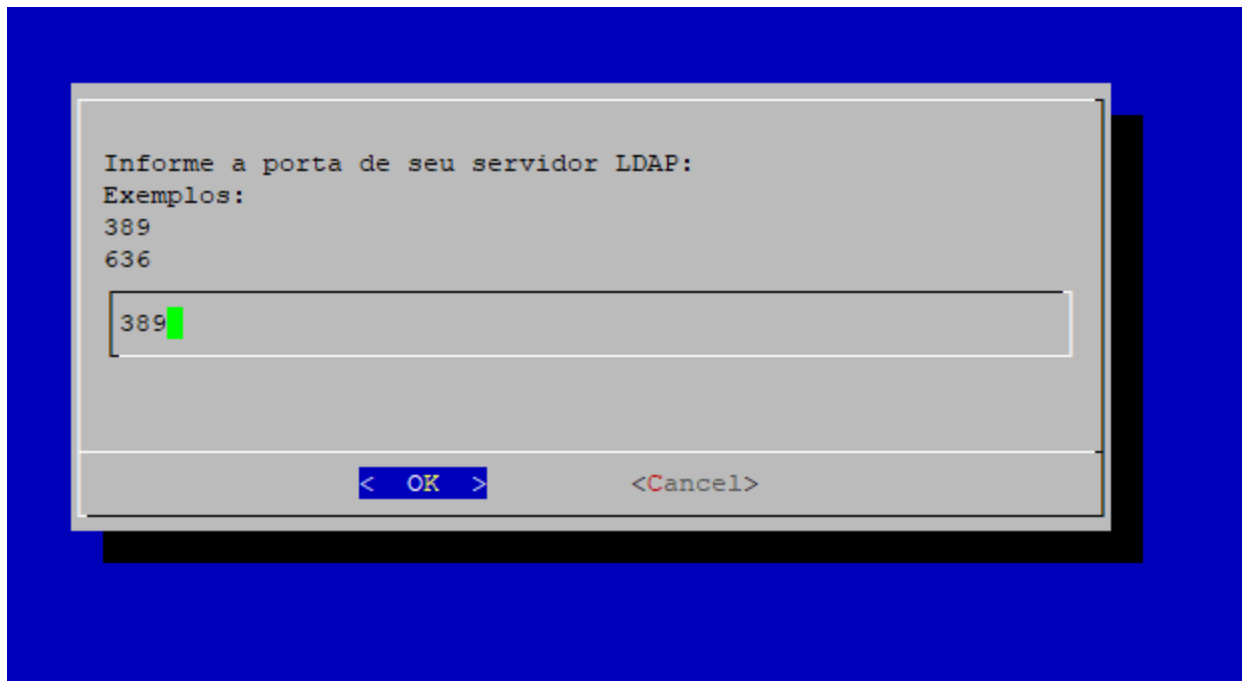
Estes arquivos correspondem ao FQDN de seu servidor Eduroam (S-sim ou N-nao) ? S
```

Caso a instituição utilize LDAP, selecionar a etapa 5 - **Configurar_LDAP**. Conforme imagem abaixo, informe o **IP ou FQDN** do seu servidor LDAP.

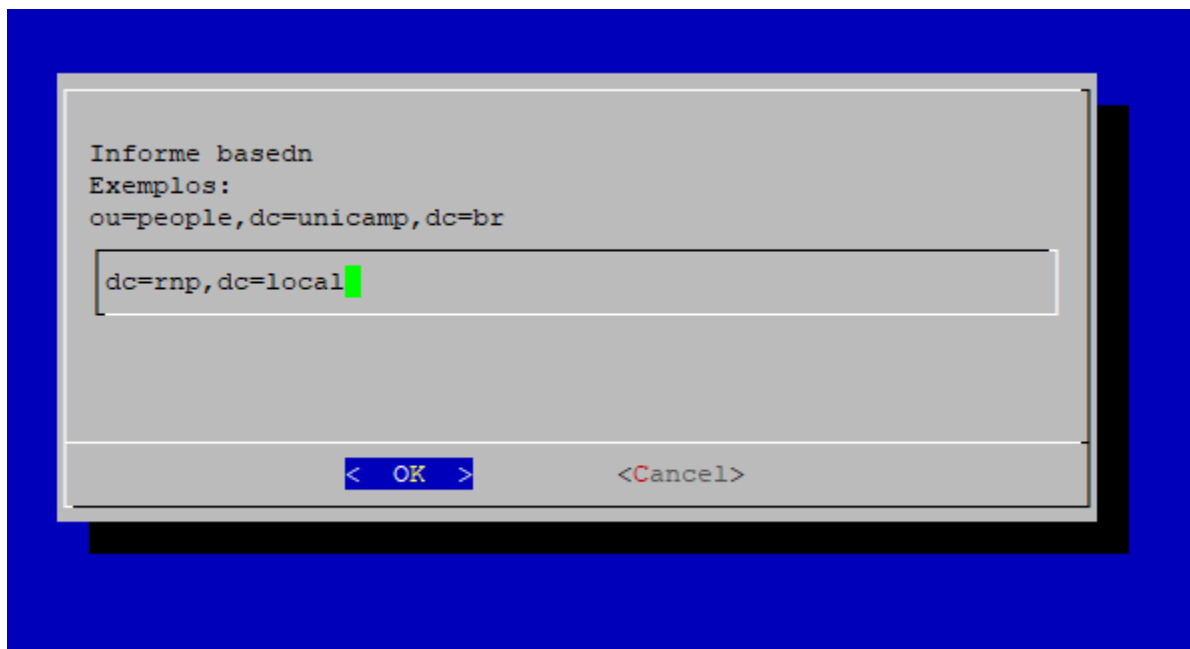
```
Informe o IP ou FQDN do seu servidor LDAP:
Exemplos:
200.130.115.18
ldap.unicamp.br

ldap.rnp.br
< OK > <Cancel>
```

Informe a porta de seu servidor LDAP, em seguida clique em **OK**



Informe o basedn, em seguida clique em **OK**



Informe o usuário com permissão de leitura em sua base LDAP, em seguida clique em **OK**

Informe usuario com permissao de leitura em sua base LDAP:

Exemplos:

uid=idpeduroam.r,ou=APLICACOES,dc=ufam,dc=edu,dc=br

uid=eduroam,ou=people,dc=rnp,dc=local

< OK >

<Cancel>

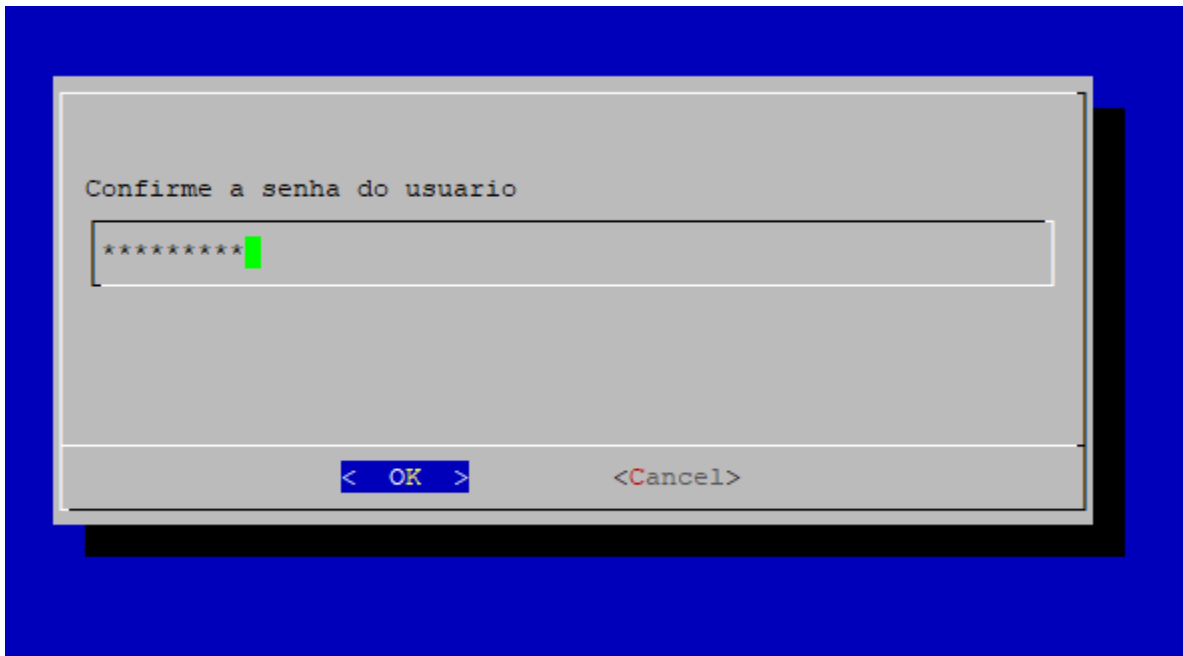
Informe a senha do usuário, em seguida clique em **OK**

Informe a senha do usuario

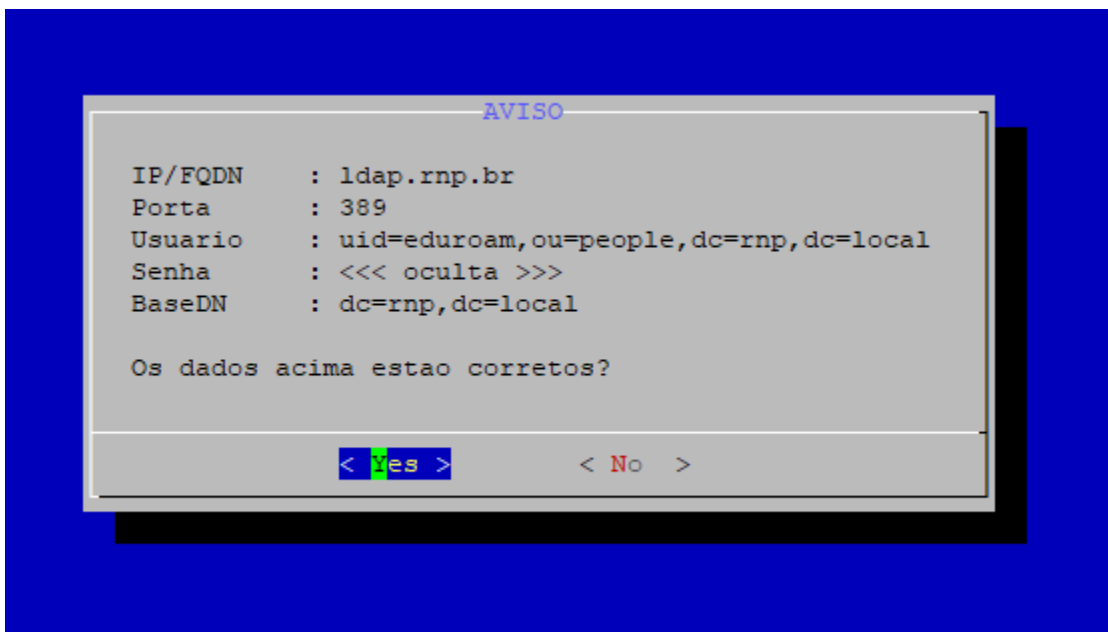
< OK >

<Cancel>

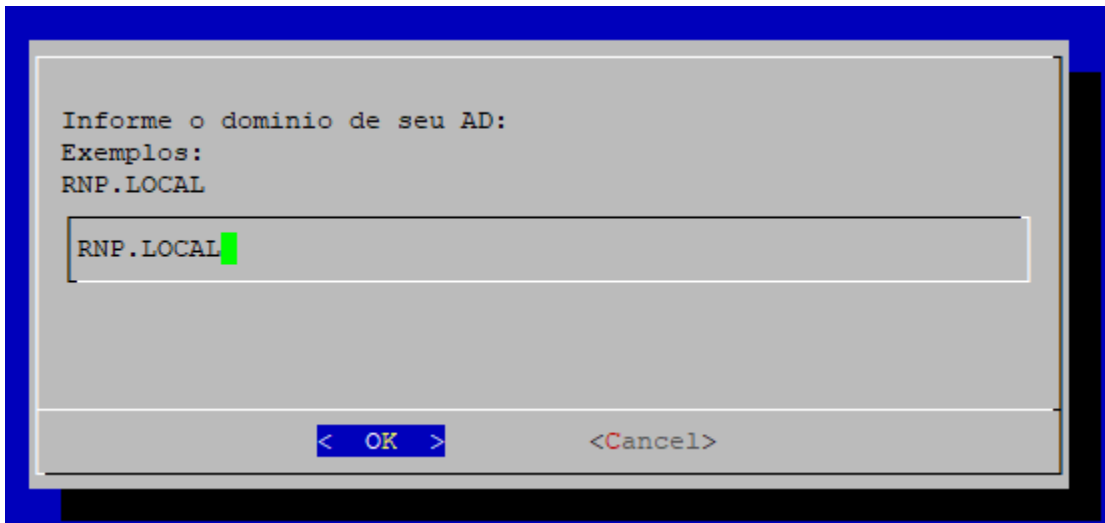
Conforme a senha do usuário e em seguida clique em **OK**



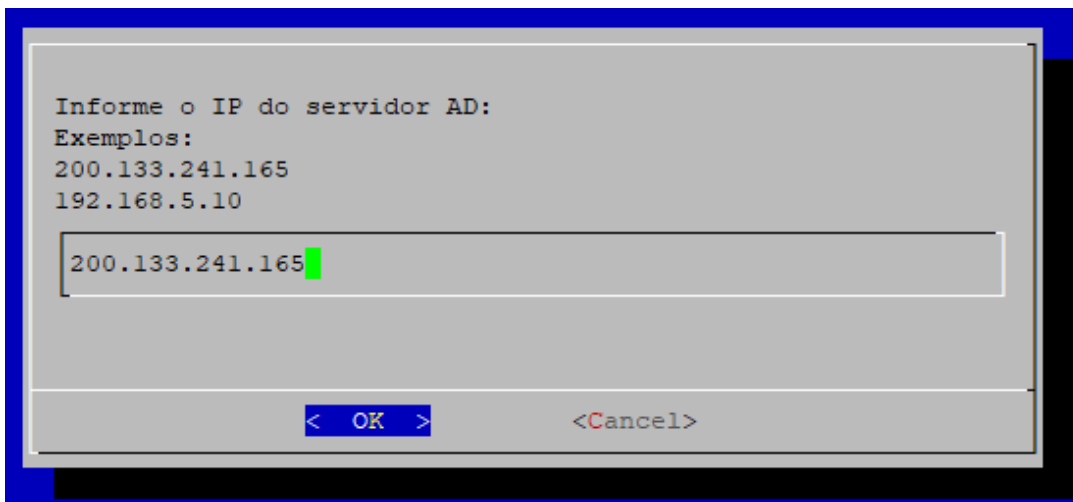
Por fim, confirme as informações e clique em **OK**



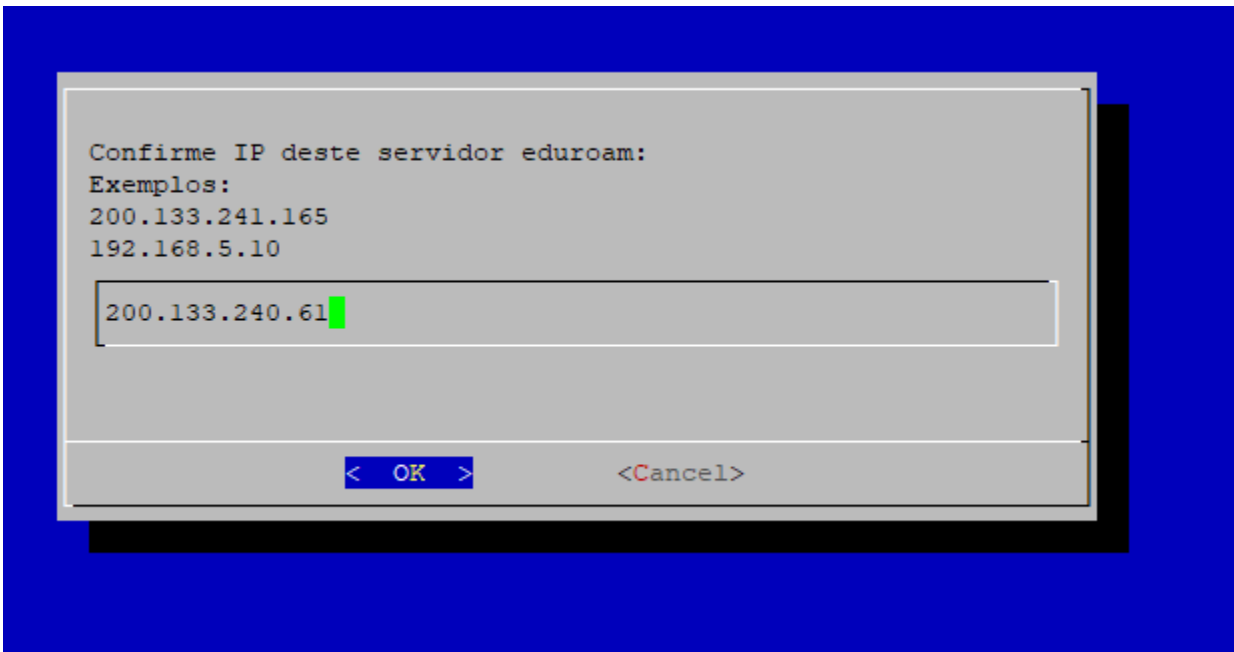
Caso sua instituição utilize o AD, selecione a etapa **6 - Configurar_AD**. Conforme a imagem abaixo, informe o domínio de seu AD, em seguida clique em **OK**



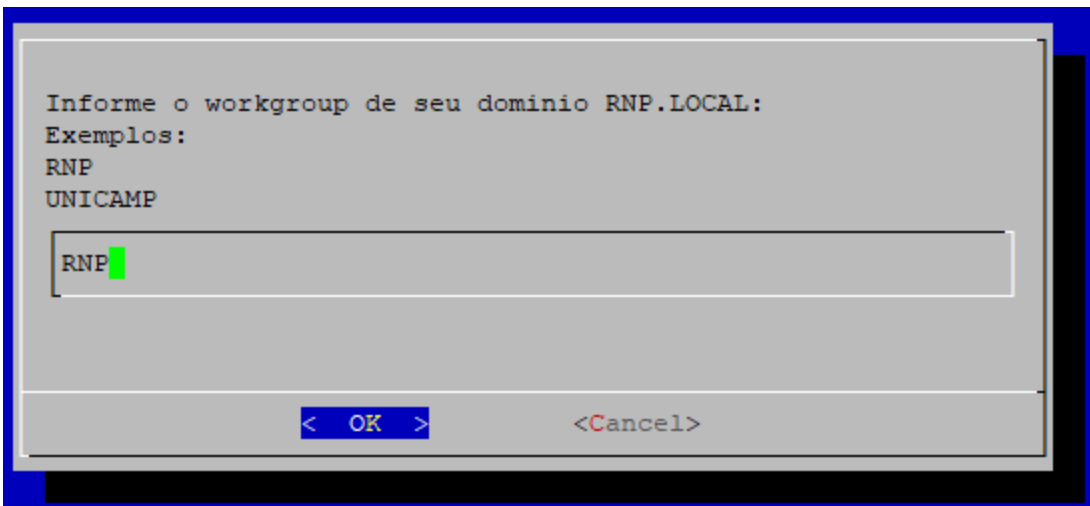
Informe o IP do servidores AD, em seguida clique em **OK**



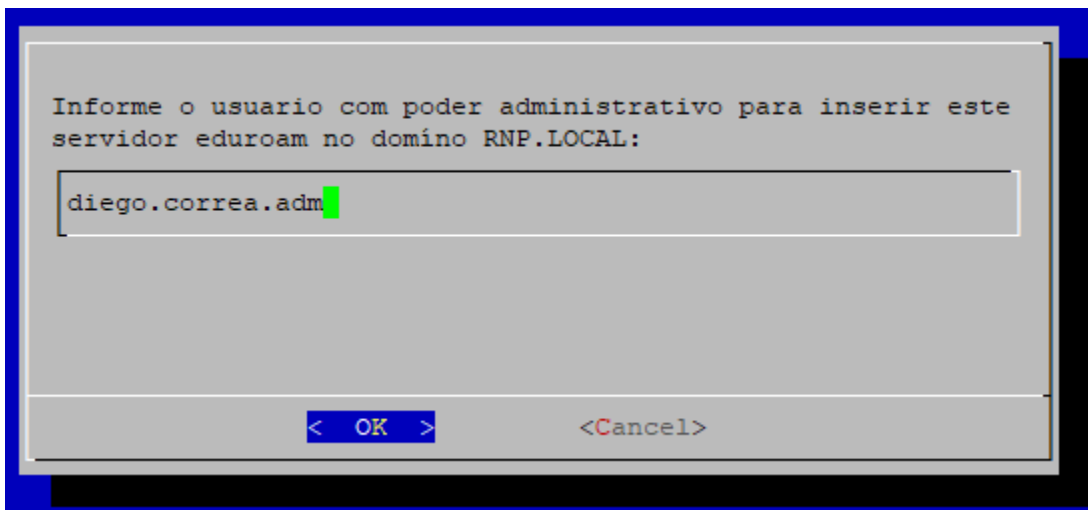
Confirme o IP deste servidor eduroam, em seguida clique em **OK**



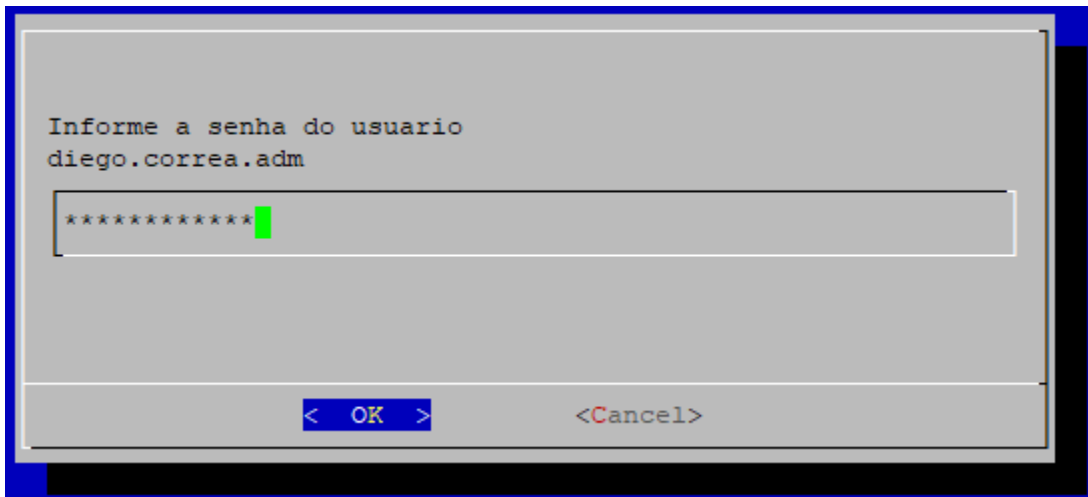
Informe o WorkGroup do seu domínio, em seguida clique em **OK**



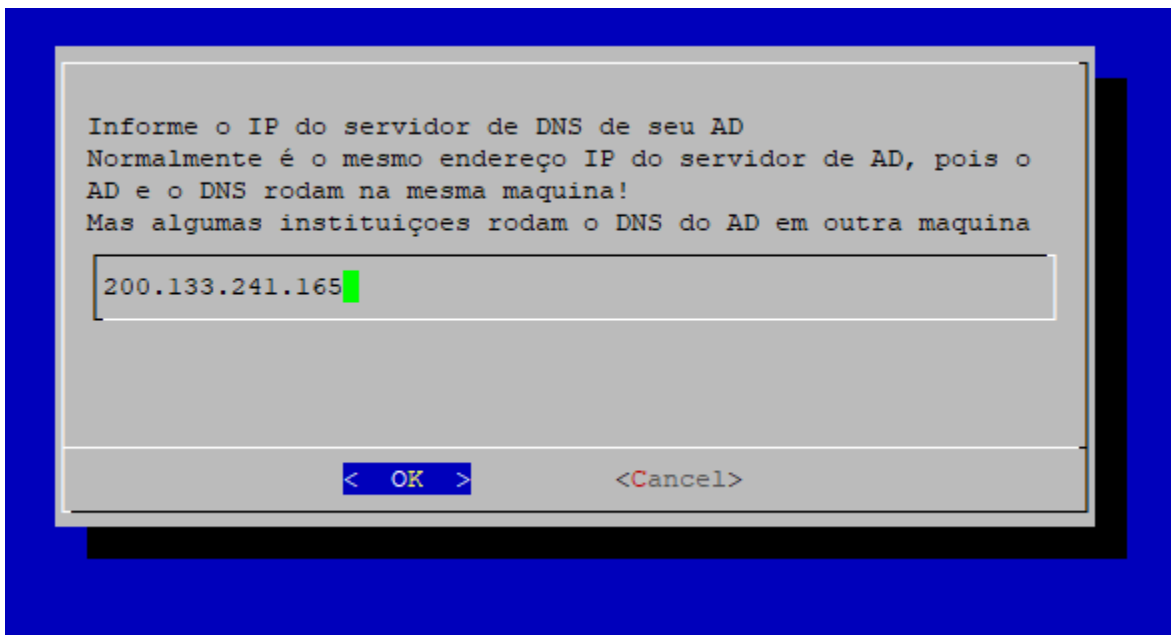
Informe o usuário com privilégio de Administrador para inserir seu servidor Eduroam ao domínio, em seguida clique em **OK**



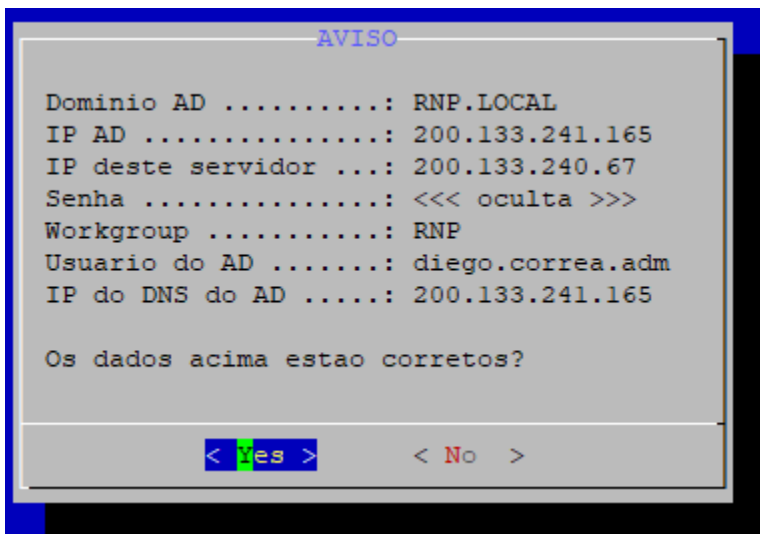
Em seguida informe a senha do usuário administrador, em seguida clique em **OK**



Informe o IP do servidor de DNS de seu AD. Geralmente é o mesmo endereço do IP do servidor de AD. Em alguns casos, são utilizados servidores distintos. Em seguida, clique em **OK**




Se os dados estiverem corretos, confirme clicando em **Yes**



Aguarde a verificação dos pacotes instalados, em seguida tecle **ENTER** para continuar

=====
Verificando pacotes instalados
=====

```
Pacote krb5-user = OK  
Pacote libpam-krb5 = OK  
Pacote krb5-config = OK  
Pacote libkrb5-3 = OK  
Pacote libkadm5clnt-mitll = OK  
Pacote winbind = OK  
Pacote ntp = OK  
Pacote ntpdate = OK  
Pacote samba = OK  
Pacote samba-common = OK  
Pacote samba-common-bin = OK  
Pacote samba-dsdb-modules = OK  
Pacote samba-libs = OK  
Pacote samba-vfs-modules = OK  
Pacote cifs-utils = OK  
Pacote smbclient = OK  
Pressione ENTER para continuar █
```



Conforme imagem abaixo, aguarde finalizar a configuração do SAMBA e tecle em **ENTER** para continuar

```
=====
SAMBA - Configurando o arquivo smb.conf
=====
```

```
Encontrado o arquivo /etc/samba/smb.conf - Realizando backup
Gerando um novo arquivo /etc/samba/smb.conf
```

```
=====
Verificando a configuracao do arquivo /etc/samba/smb.conf
=====
```

```
testparm -s
Load smb config files from /etc/samba/smb.conf
rlimit_max: increasing rlimit_max (1024) to minimum Windows limit (16384)
Loaded services file OK.
Server role: ROLE_DOMAIN_MEMBER
```

```
# Global parameters
```

```
[global]
```

```
domain master = No
local master = No
log file = /var/log/samba/%m.log
logging = syslog@1 file
os level = 0
preferred master = No
realm = RNP.LOCAL
restrict anonymous = 2
security = ADS
smbd profiling level = on
template shell = /bin/bash
winbind enum groups = Yes
winbind enum users = Yes
winbind use default domain = Yes
workgroup = RNP
idmap config * : range = 1000000-19999999
idmap config * : rangesize = 1000000
idmap config * : backend = autorid
```

```
Pressione ENTER para continuar █
```

Aguarde o término da configuração WINBIND em seguida tecle **ENTER** para continuar

```
=====
WINBIND - Configurando o arquivo /etc/nsswitch.conf
=====
```

```
Encontrado o arquivo /etc/nsswitch.conf - Realizando backup
Gerando um novo arquivo /etc/nsswitch.conf
Pressione ENTER para continuar
```

```
Ativando permanentemente os servicos SMBD NMBD WINBIND com os seguintes comandos:
```

```
systemctl enable smb 2>/dev/null
systemctl enable nmbd 2>/dev/null
```

```
Pressione ENTER para continuar
```

```
Pressione ENTER para continuar █
```

Após a validação do usuário com KINIT, tecle **ENTER** para continuar

```
=====
KERBEROS - Validando o usuario com kinit
=====
kinit diego.correa.adm@RNP.LOCAL
Password for diego.correa.adm@RNP.LOCAL:
OK - Autenticacao via Kerberos realizado com sucesso. Arquivo /etc/krb5.conf
Pressione ENTER para continuar
=====

net ads leave -U diego.correa.adm%senha
=====

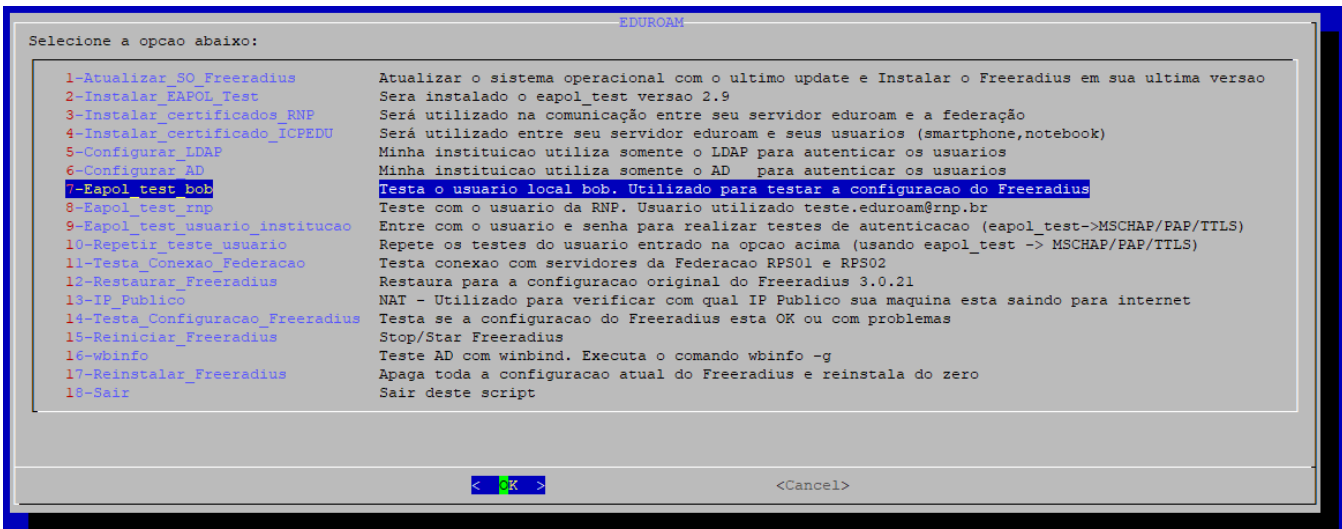
net ads dns unregister diego.RNP.LOCAL
=====

Successfully un-registered hostname from DNS
=====

Inserindo a maquina no dominio
=====

net ads join --no-dns-updates osName=Ubuntu osVer=LTS-18 -U diego.correa.adm%senha
Using short domain name -- RNP
Joined 'DIEGO' to dns domain 'rnp.local'
Maquina adicionada com sucesso ao dominio !!!
Pressione ENTER para continuar
```

Vamos executar a opção **7 - Eapol test bob**, nesta opção existe um usuário local chamado **BOB**, utilizado pra testar a configuração do Freeradius



Observe na imagem abaixo, deu tudo **OK**.

```
Verificacao da configuracao do Freeradius
=====
User: bob
Pass: <<< oculto >>>
=====
PAP= OK
MSCHAP=OK

--- WPA-EAP ---
PEAP MSCHAPv2=OK
TTLS MSCHAPv2=OK
TTLS MSCHAPv2=OK key_mgmt=WPA-EAP eap=TTLS phase2="autheap=MSCHAPv2"
TTLS PAP=OK

=====
< OK >
```

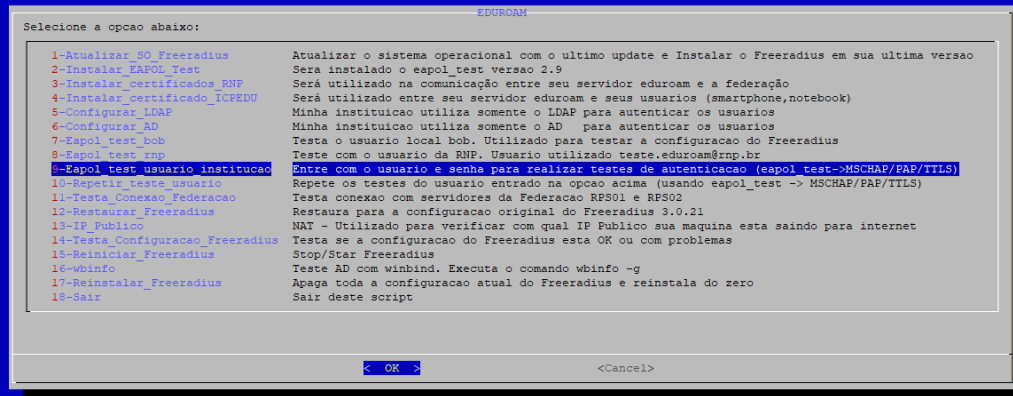
Agora execute a opção 8 - Eapol teste rnp esta opção executa um teste com o usuário teste.eduroam@rnp.br

```
Verificacao da configuracao do Freeradius
=====
User: teste.eduroam@rnp.br
Pass: <<< oculto >>>
=====
PAP= OK
MSCHAP=OK

--- WPA-EAP ---
PEAP MSCHAPv2=OK
TTLS MSCHAPv2=OK
TTLS MSCHAPv2= erro key_mgmt=WPA-EAP eap=TTLS phase2="autheap=MSCHAPv2"
TTLS PAP=OK

=====
< OK >
```

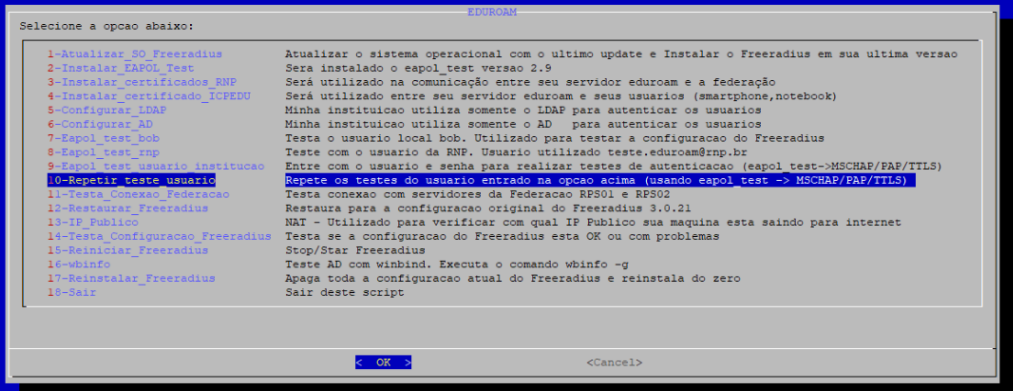
Em seguida executar a opção 9 - Eapol test usuario instituicao, entre com seu usuário e senha para realizar teste de autenticação, observe a imagem abaixo



Insira o usuário e senha de sua instituição

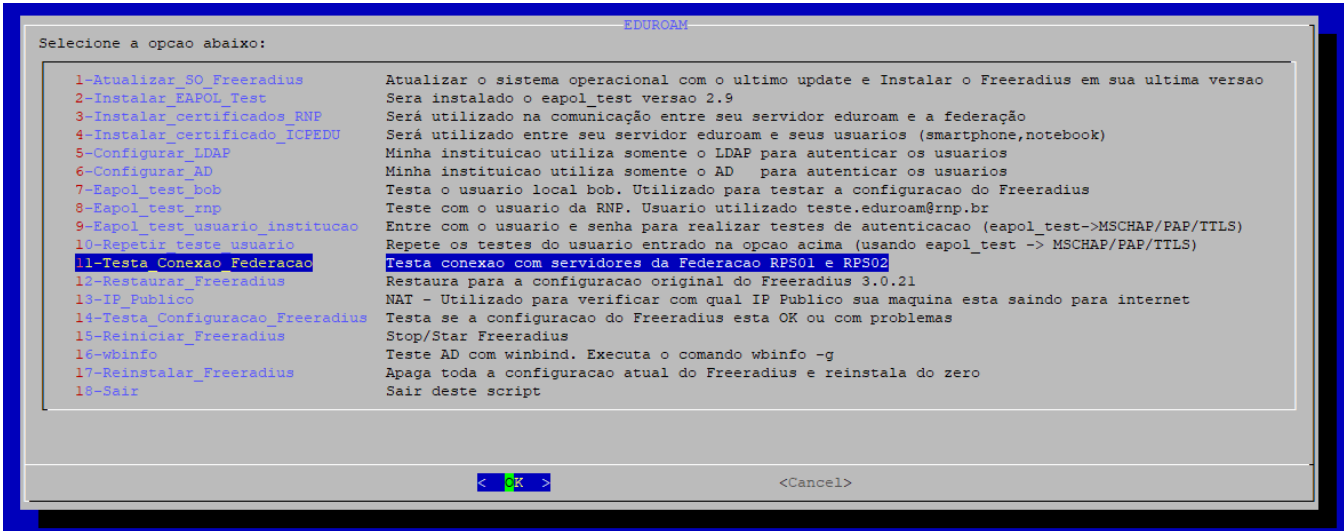
Entre com o email:diego.correa@ufcorrea.gov.br
Entre com a senha: *****

Repita o teste executando a opção 10 para confirmar a autenticação, conforme a imagem abaixo, pressione ENTER para continuar

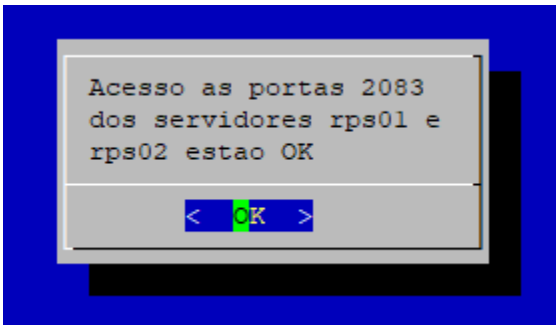


```
=====  
User: diego.correa@ufcorrea.gov.br  
Pass: <<< oculto >>>  
=====  
PAP= OK  
MSCHAP=OK  
--- WPA-EAP ---  
PEAP MSCHAPv2=OK  
TTLS MSCHAPv2=OK  
TTLS MSCHAPv2= erro key_mgmt=WPA-EAP eap=TTLS phase2="authcap=MSCHAPv2"  
TTLS PAP=OK  
=====  
Pressione ENTER para continuar
```

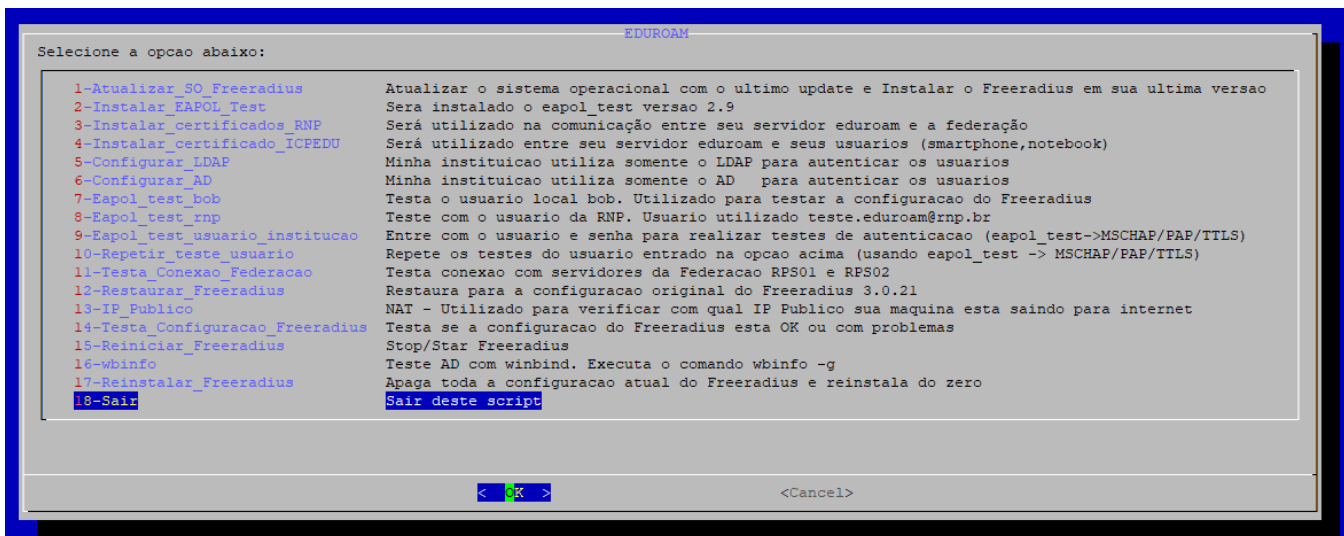

Execute a opção **11 - Testa Conexão Federação**, esta opção irá testar a conexão dos servidores da Federação **RPS01** e **RPS02**



Observe que a conexão foi bem sucedida teste OK na porta **2083** dos servidores **RPS01** e **RPS02**



Execute a opção **18 - Sair**, para sair do Script



Procedimentos finais

Após ter saído do Script Incluir o IP de sua controladora/AP e sua chave secreta dentro do arquivo **/etc/freeradius/clients.conf**

Segue exemplo de configuração:

```
### Campus Sede

client 200.137.193.131 {
    ipaddr = 200.137.193.131
    shortname = campus_sede
    secret = qplmkdfjgszvqru
    require_message_authenticator = no
    nastype = other
}
```

Após as alterações reiniciar o Freeradius

```
/etc/init.d/freeradius restart
```

Configurar a controladora para se conectar no servidor eduroam.

E por fim, executar testes em seu smartphone usando o SSID eduroam.