Procedimento de instalação do servidor IDP Eduroam

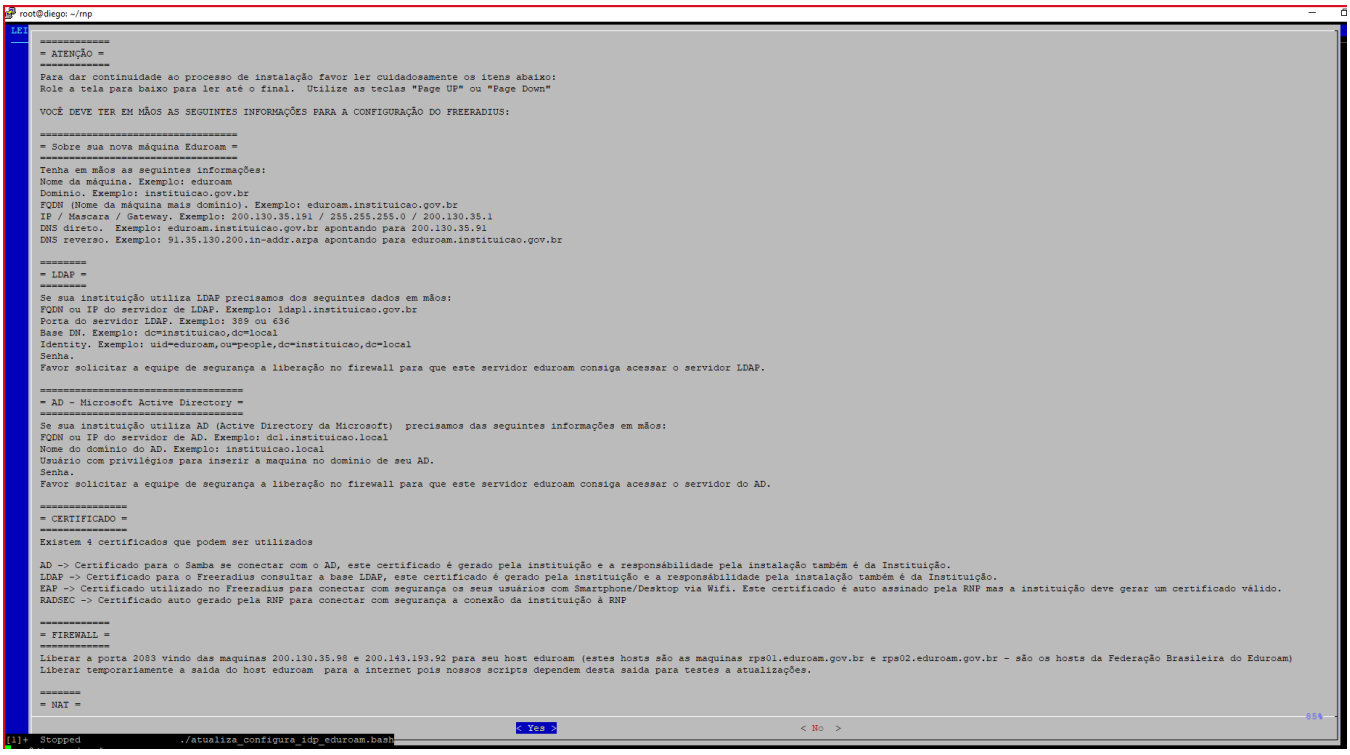
Objetivo

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

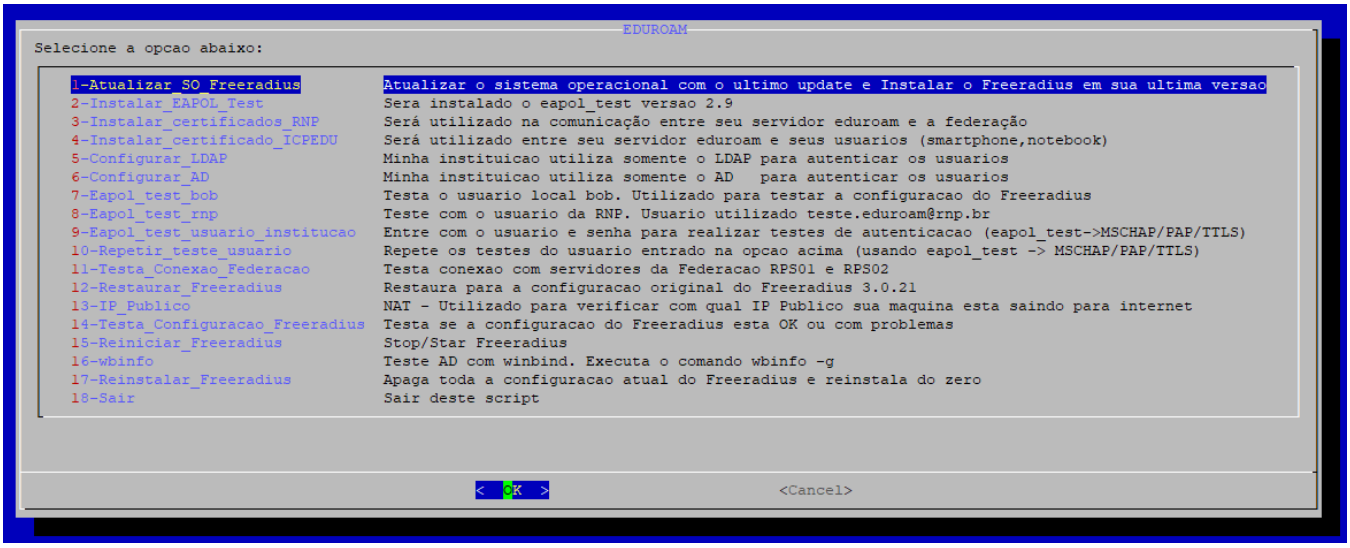
 **Este procedimento deve ser executado somente no Ubuntu versão 18.04 LTS 64bits**

```
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 )

Descompatar 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 scrippt:
./atualiza_configura_idp_eduroam.bash
```

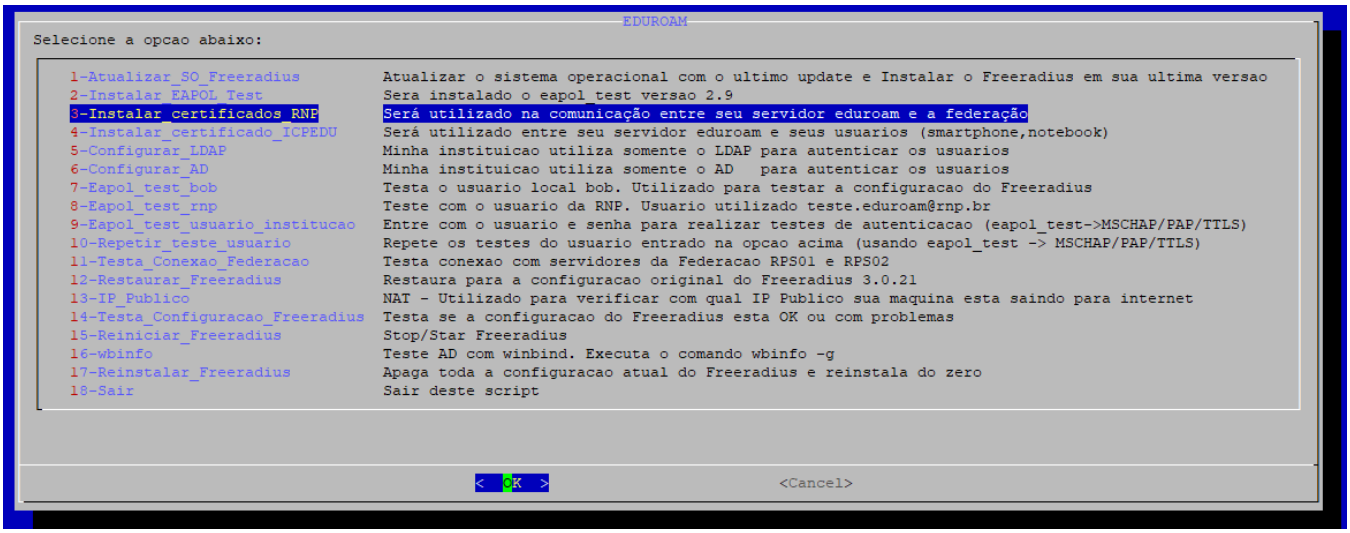
Após executar o comando `./atualiza_configura_idp_eduroam.bash` será mostrado uma janela com todas informações necessárias para dar inicio na configuração do FREERADIUS. Clique em Yes para seguir



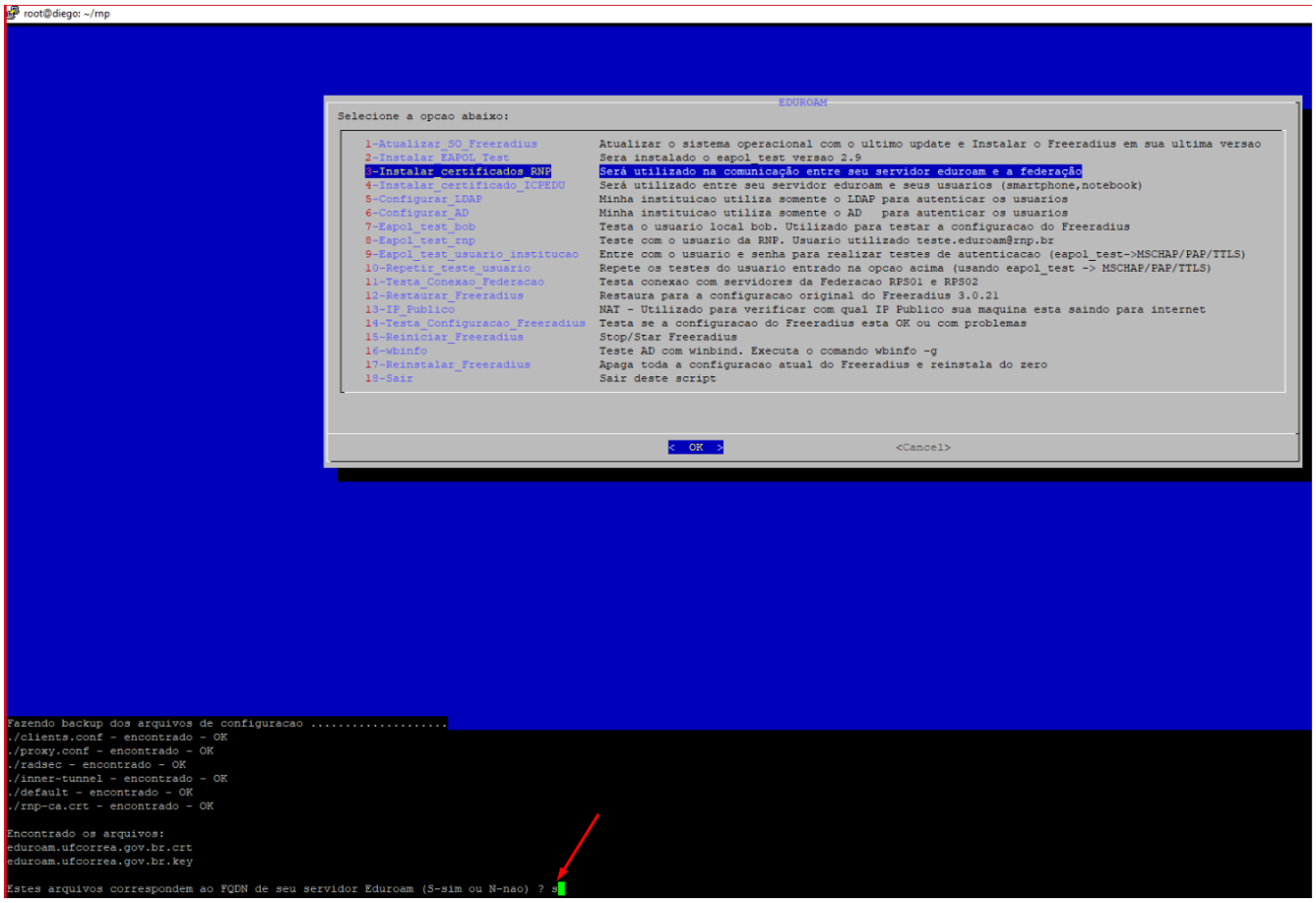
Na imagem abaixo selecione a opção #1 Atualizar o SO Freeradius, esta opção atualizará o seu sistema operacional com o ultimo update e instalará o Freeradius em sua ultima versão



Neste próximo passo, daremos inicio 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

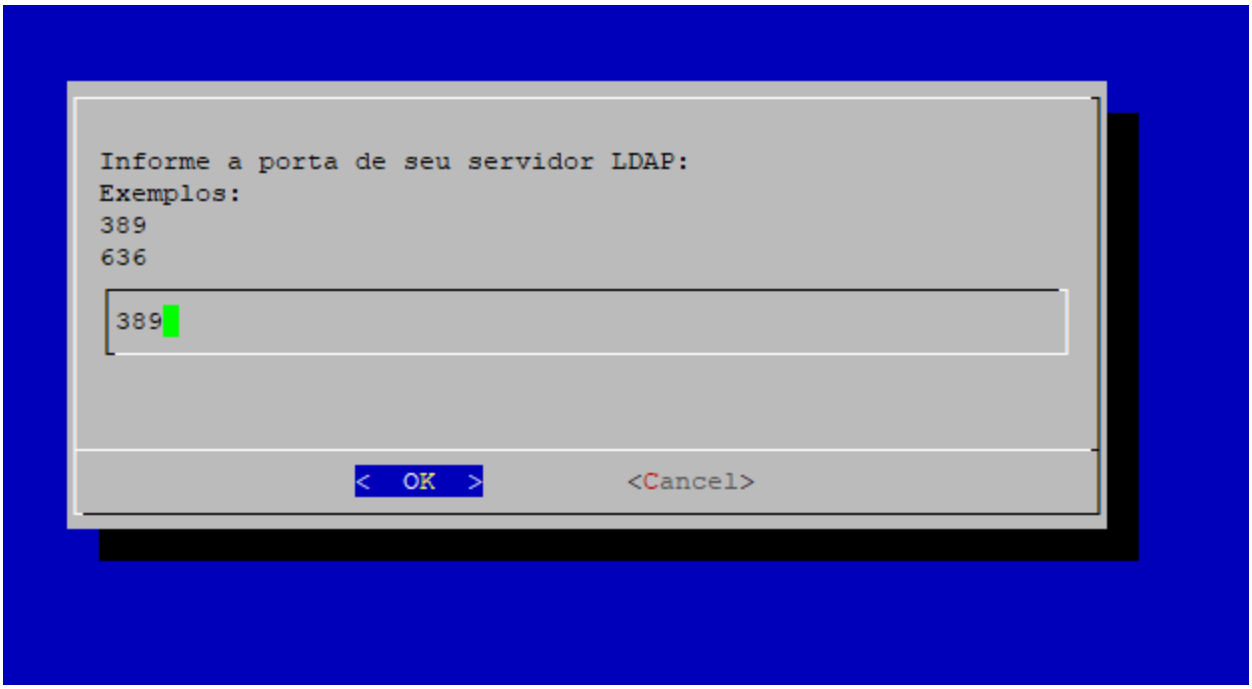


Após selecionar a etapa 3 - Instalação do certificado RNP será feito um backup dos arquivos de configuração, assim que pronto, tecle S (sim) para confirmar que os arquivos FQDN são correspondentes ao seu servidor Eduroam. Observe a imagem abaixo

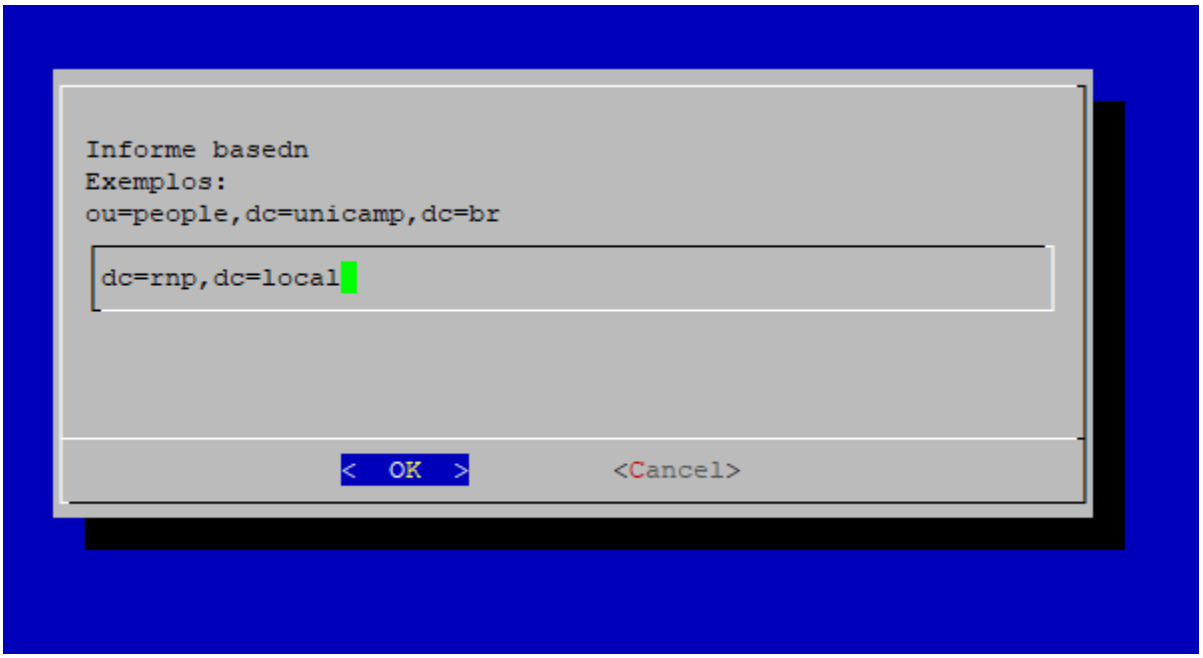


Caso a instituição utilize LDAP, selecionar a etapa 5 - Configurar_LDAP. Conforme imagem abaixo, informe o IP ou FQDN do seu servidor LDAP.

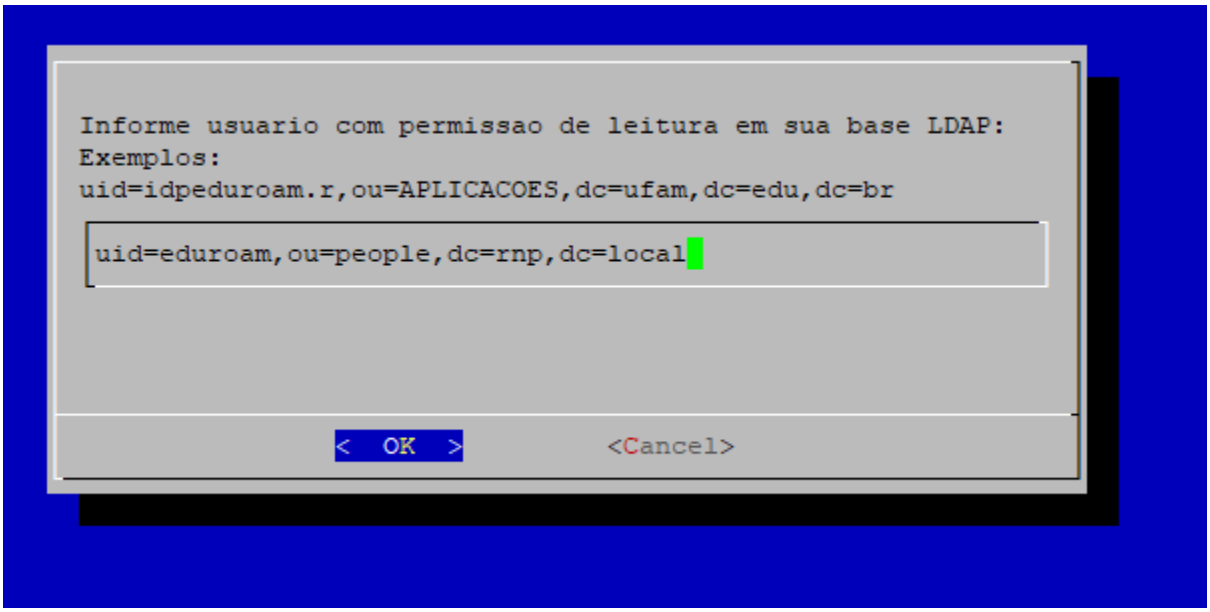
Informe a porta de seu servidor LDAP, em seguida clique em OK



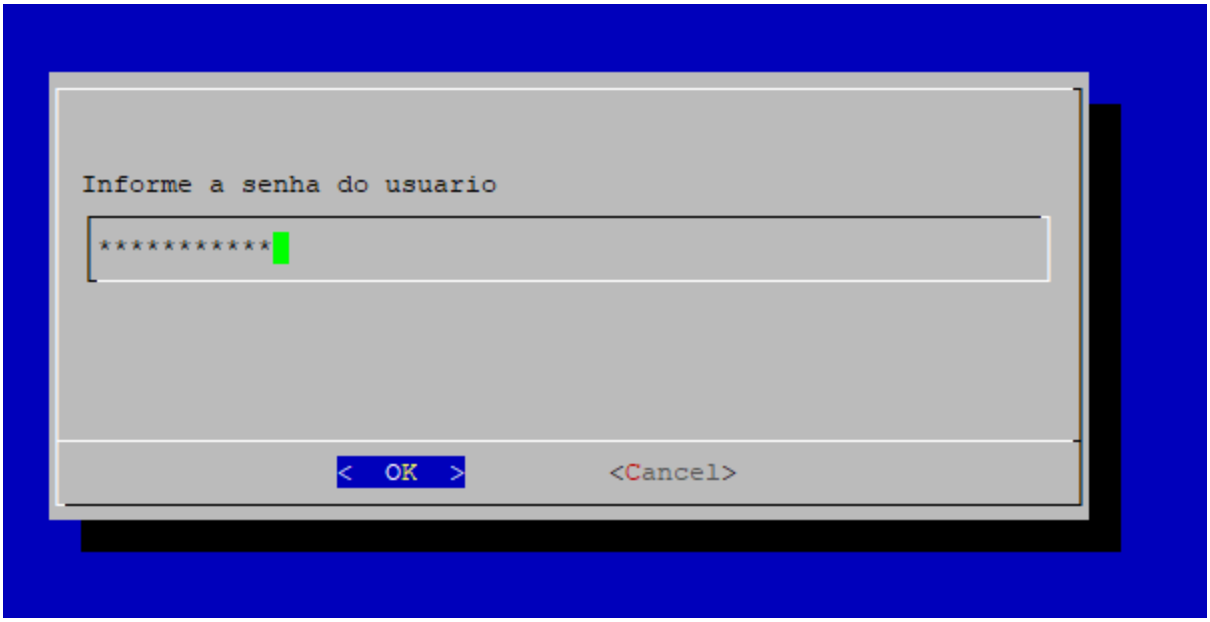
Informe o basedn, em seguida clique em OK



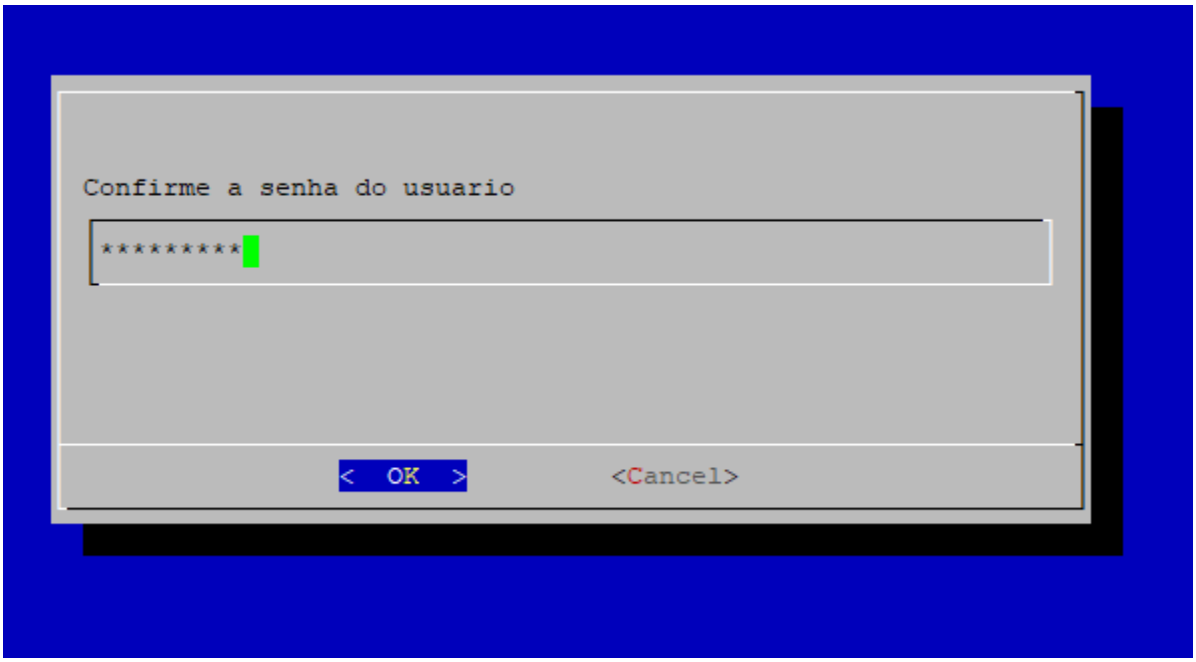
Informe o usuário com permissão de leitura em sua base LDAP, em seguida clique em OK



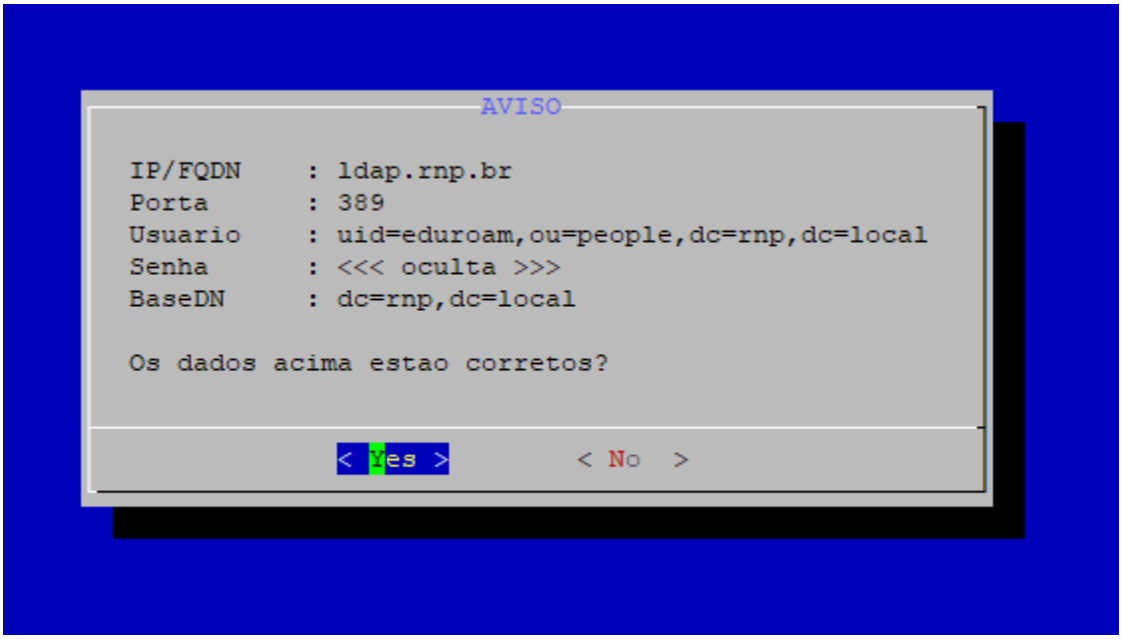
Informe a senha do usuário, em seguida clique em OK



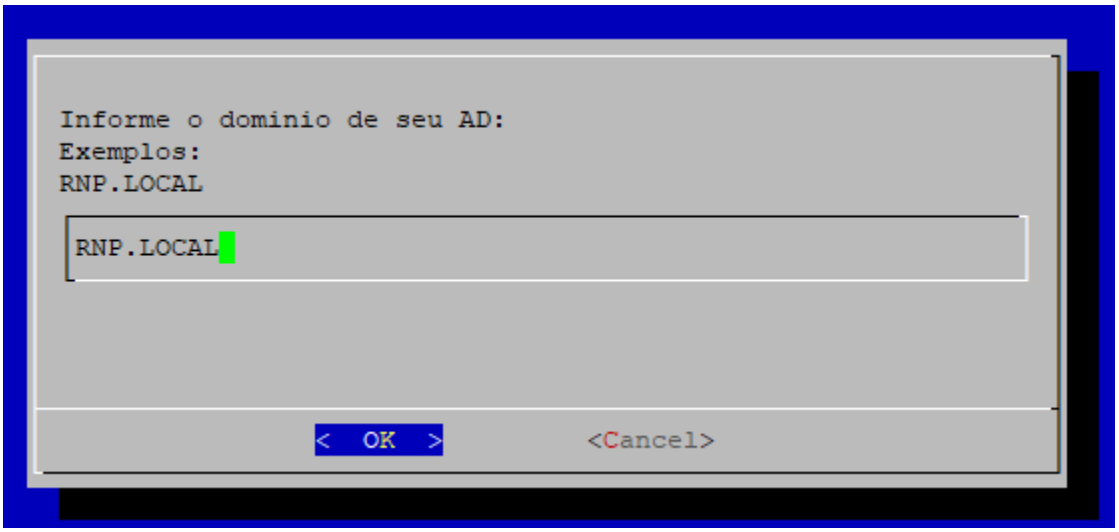
Conforme a senha do usuário e em seguida clique em OK



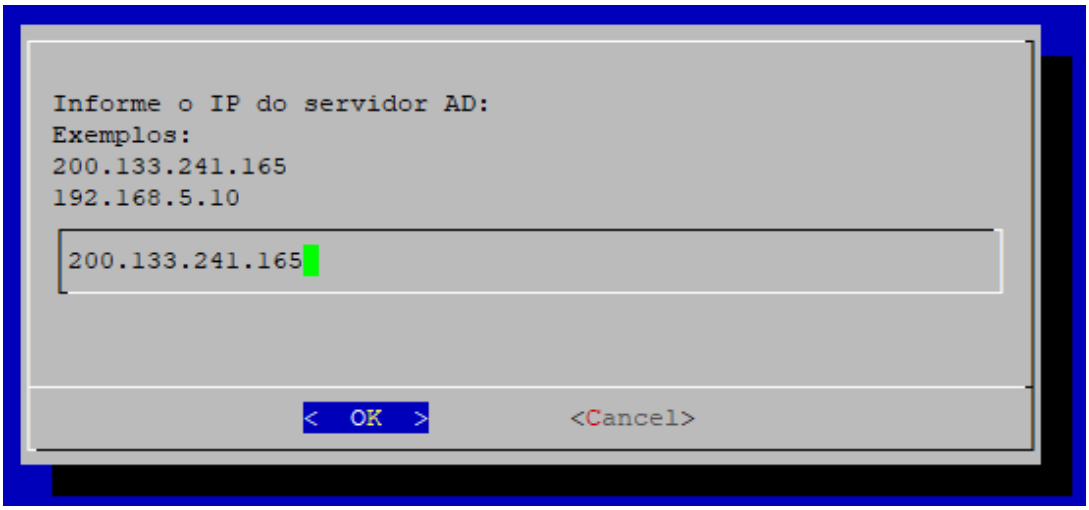
Por fim, confirme as informações e clique em OK



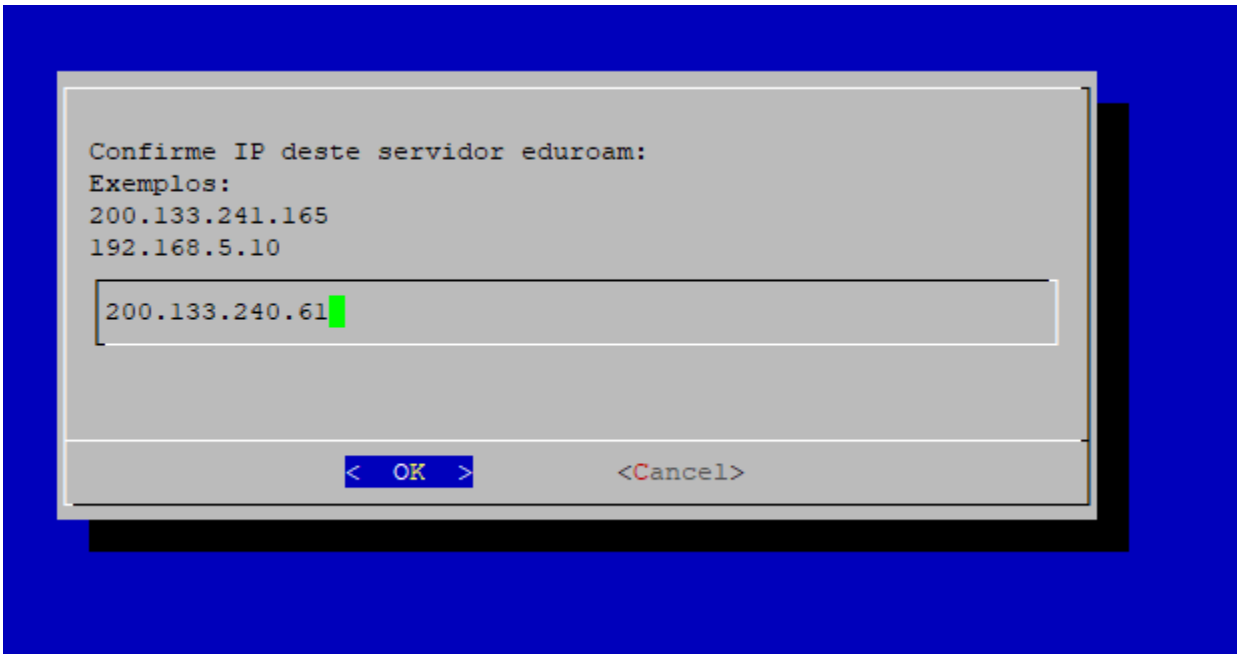
Caso sua instituição utilize o AD, selecione a etapa 6 - Configurar_AD. Conforme a imagem abaixo, informe o domínio de seu AD, em seguida clique em OK



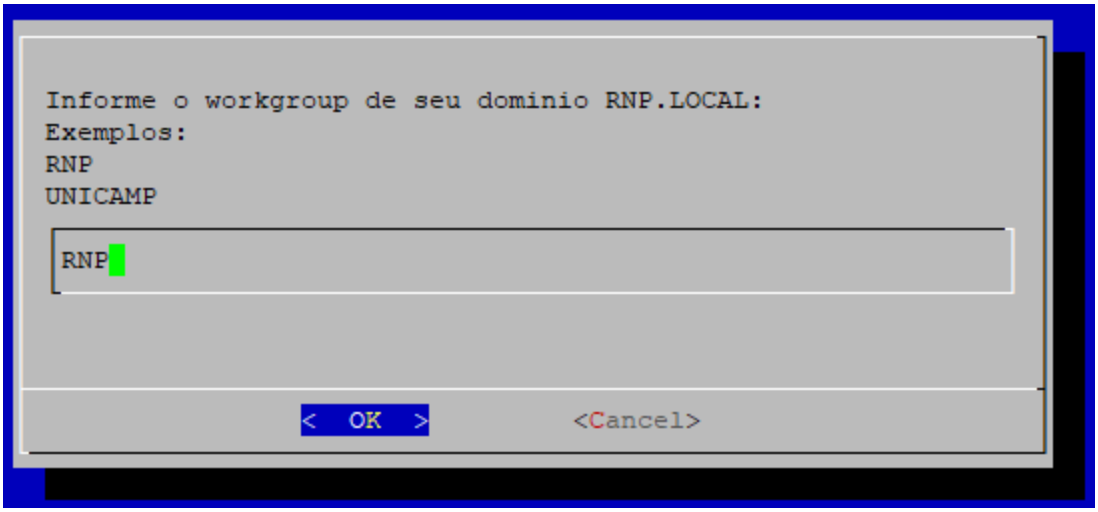
Informe o IP do servidos AD, em seguida clique em OK



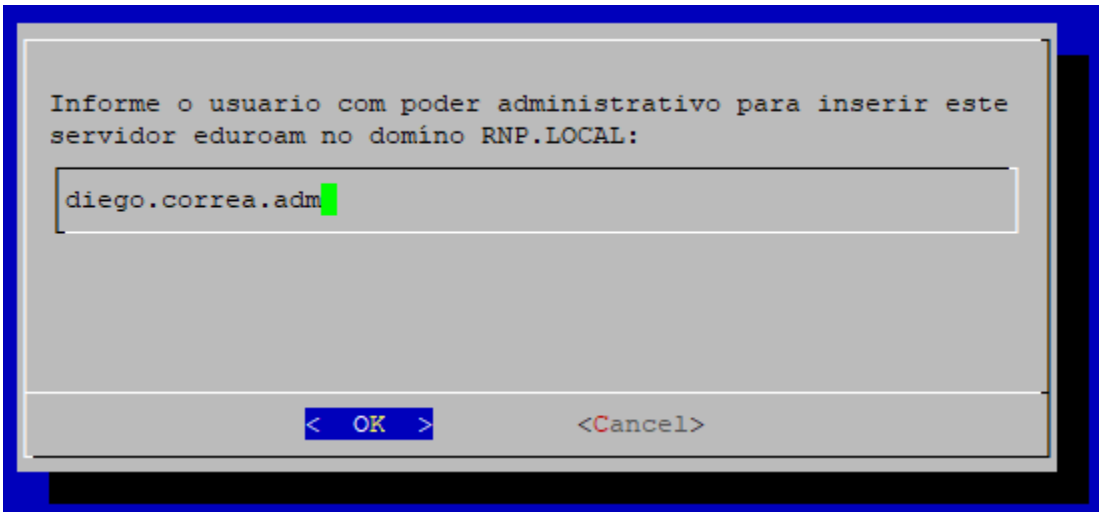
Confirme o IP deste servidor eduroam, em seguida clique em OK



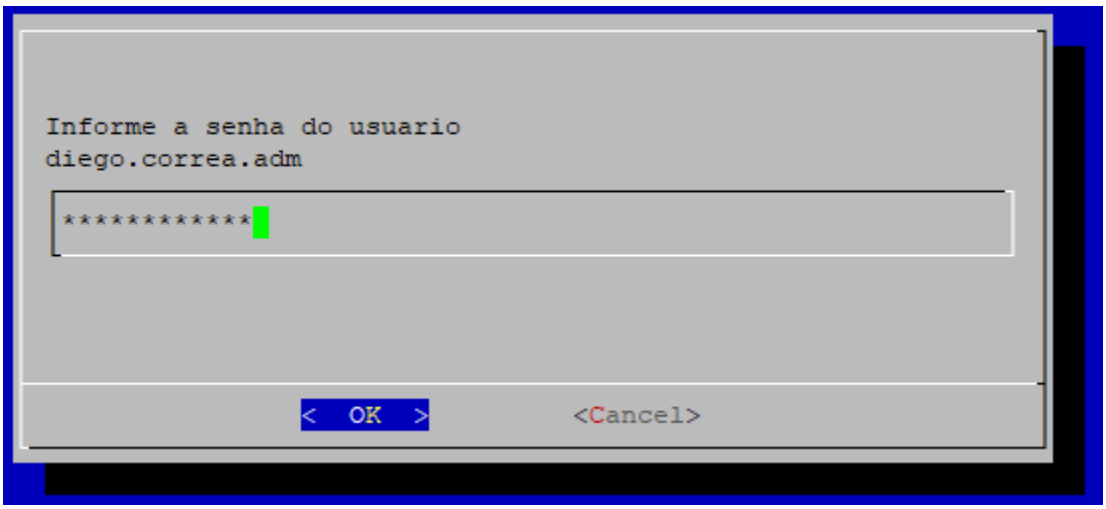
Informe o <u>WorkGroup</u> do seu domínio, em seguida clique em OK



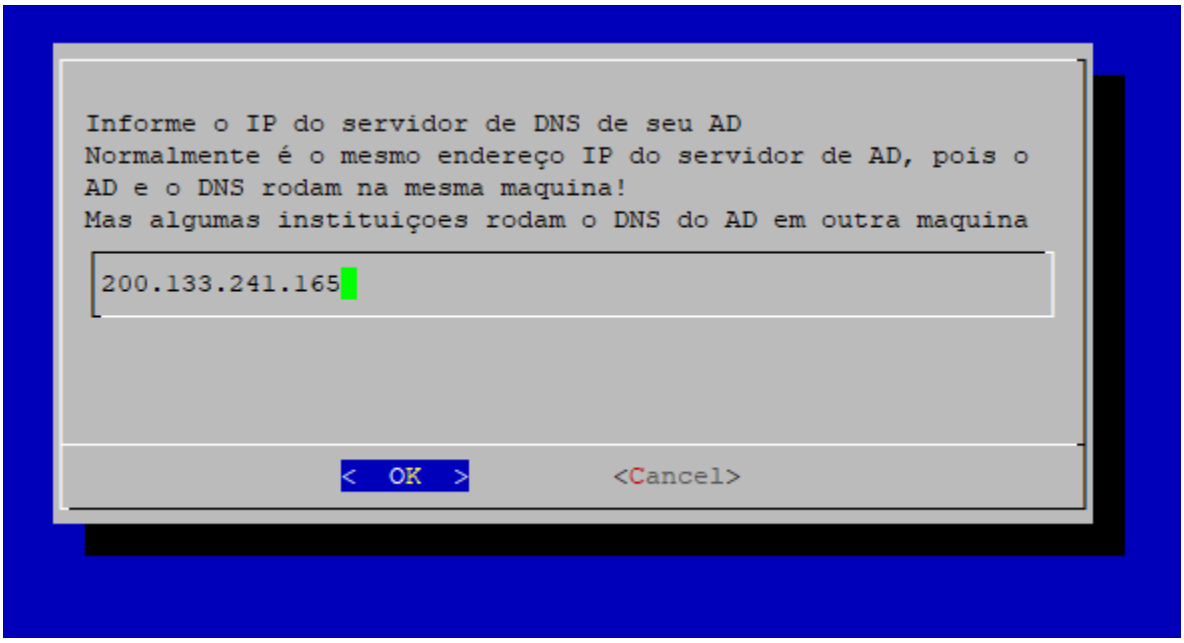
Informe o usuário com privilégio de Administrador para inserir seu servidor Eduroam ao domínio, em seguida clique em OK



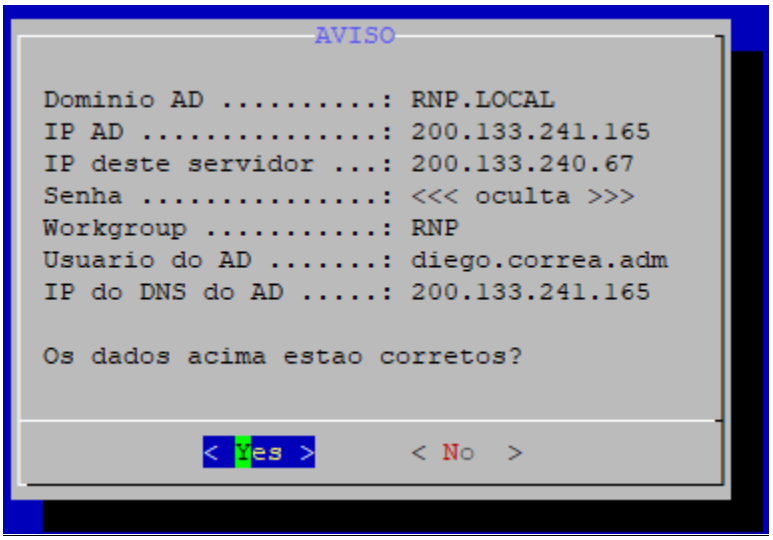
Em seguida informe a senha do usuário administrador, em seguida clique em OK



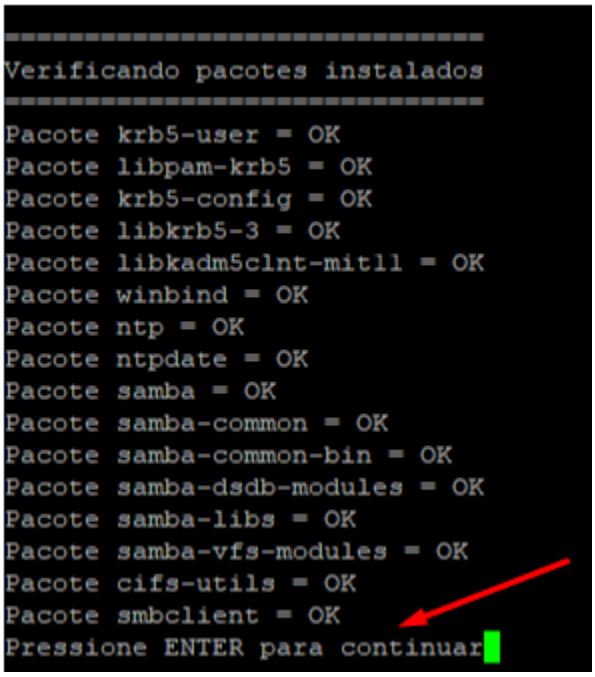
Informe o IP do servidor de DNS de seu AD. Geralmente é o mesmo endereço do IP do servidor de AD. Em alguns casos, são utilizados servidores destintos. Em seguida, clique em OK



Se os dados estiverem corretos, confirme clicando em Yes



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



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
```

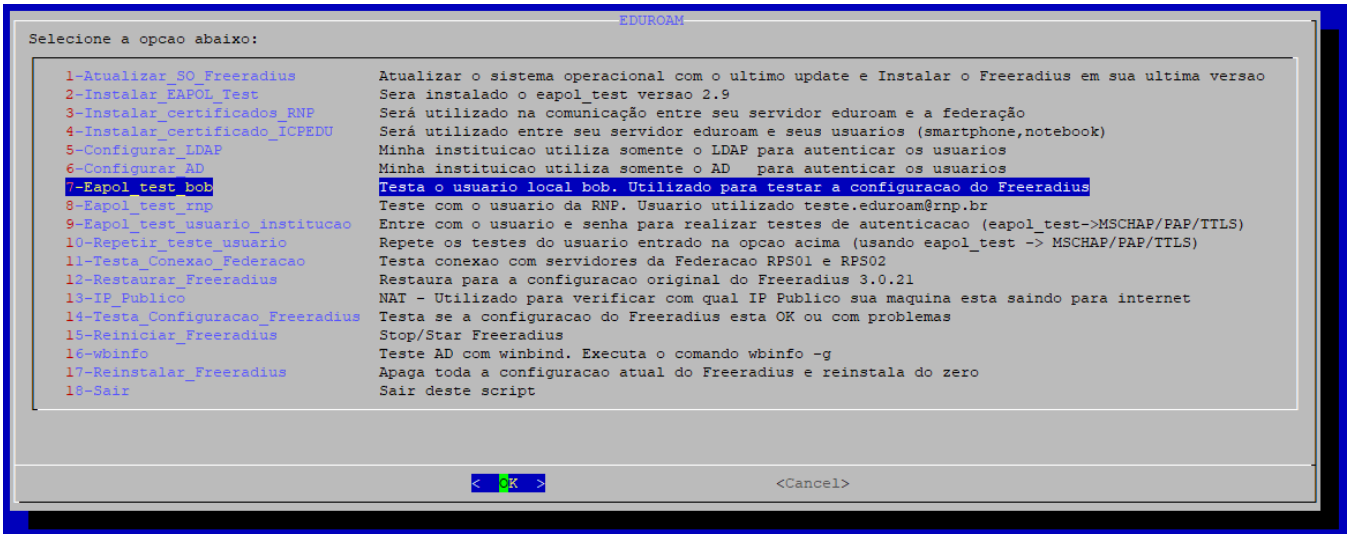
Aguarde o término da configuração <u>WINBIND</u> em seguida tecle ENTER para continuar

```
============================================================
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 smbd 2>/dev/null
systemctl enable nmbd 2>/dev/null
Pressione ENTER para continuar
Pressione ENTER para continuar
```

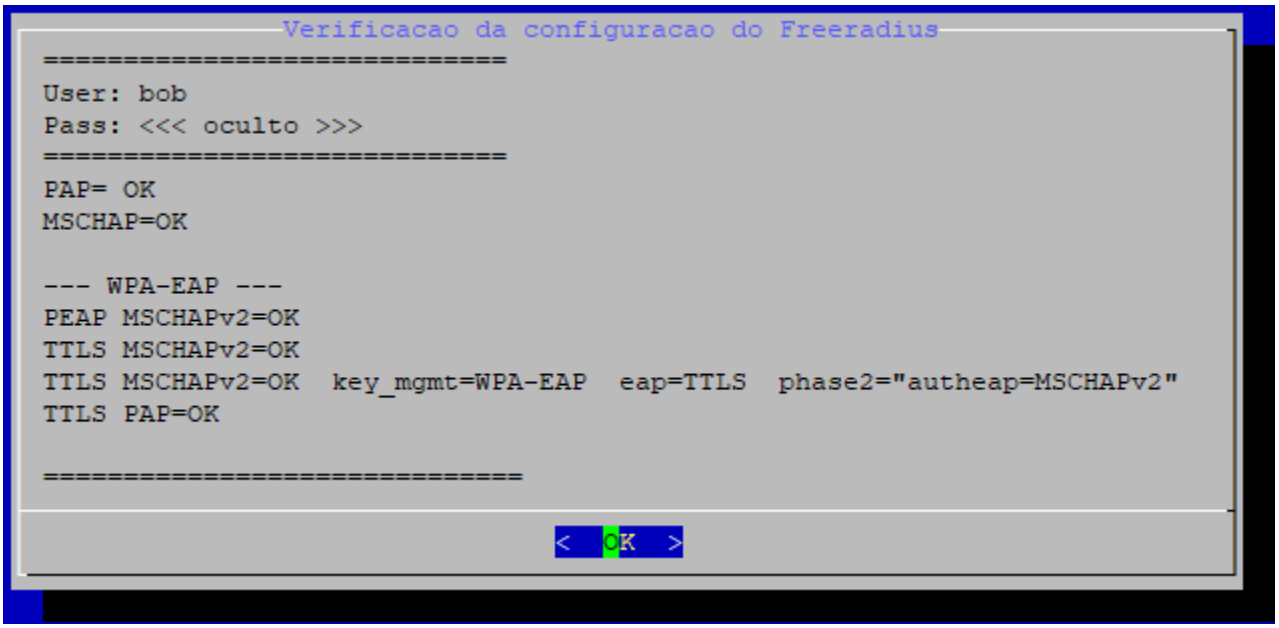
Após a validação do usuário com KINIT, tecle ENTER para continuar

```
=======================================
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
```

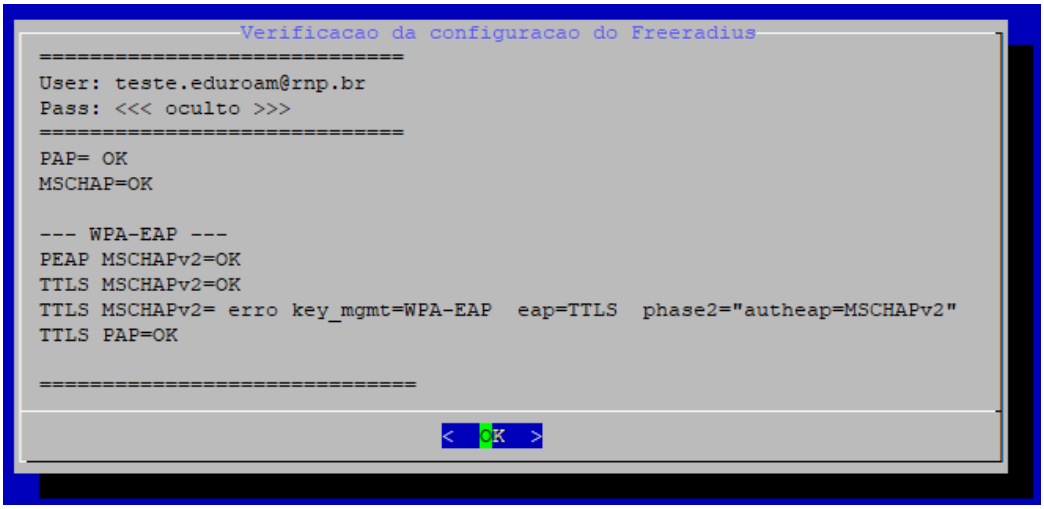
Vamos executar a opção 7 - Eapol test bob, nesta opção existe um usuário local chamado BOB, utilizado pra testar a configuração do Freeradius



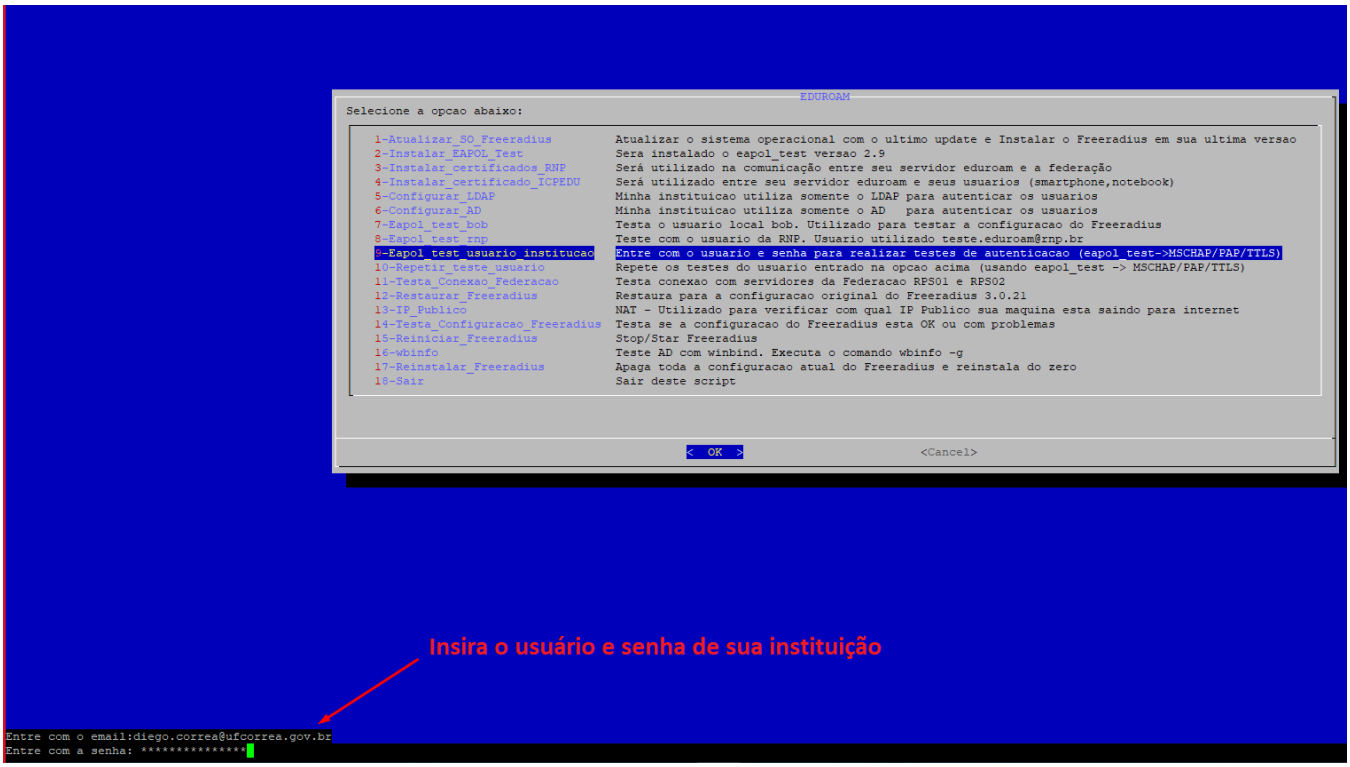
Observe na imagem abaixo, deu tudo OK.



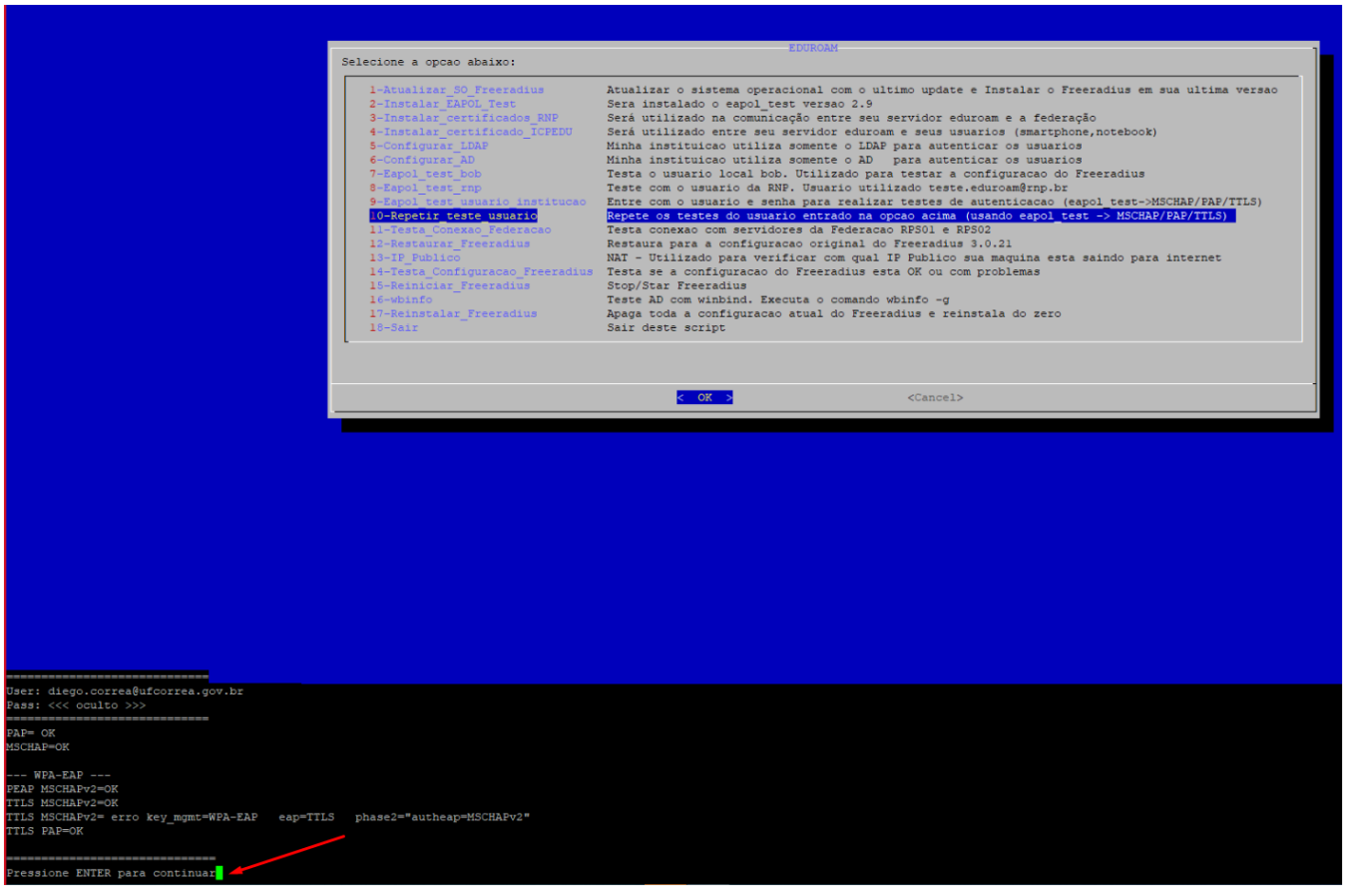
Agora execute a opção 8 - Eapol teste rnp esta opção executa um teste com o usuário teste.eduroam@rnp.br



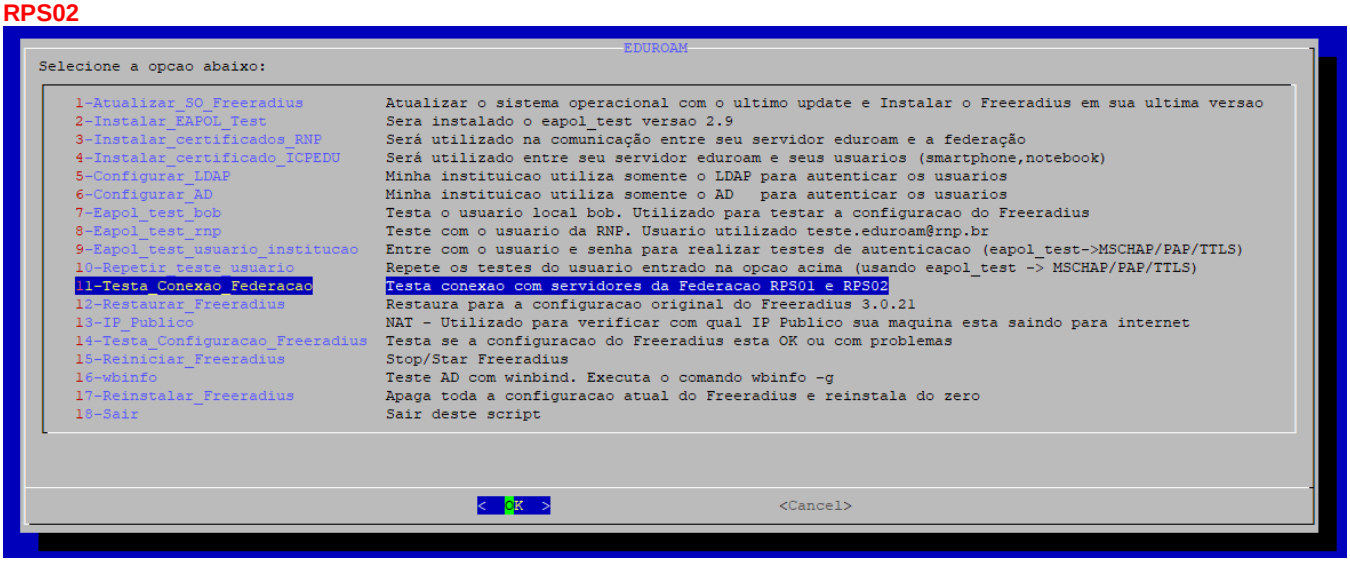
Em seguida executar a opção 9 - Eapol test usuario instituicao, entre com seu usuário e senha para realizar teste de autenticação, observe a imagem abaixo



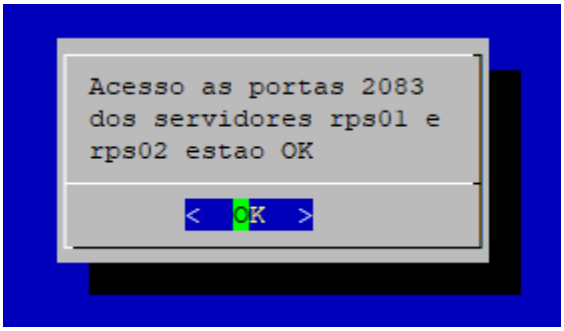
Repita o teste executando a opção 10 para confirmar a autenticação, conforme a imagem abaixo, pressione ENTER para continuar



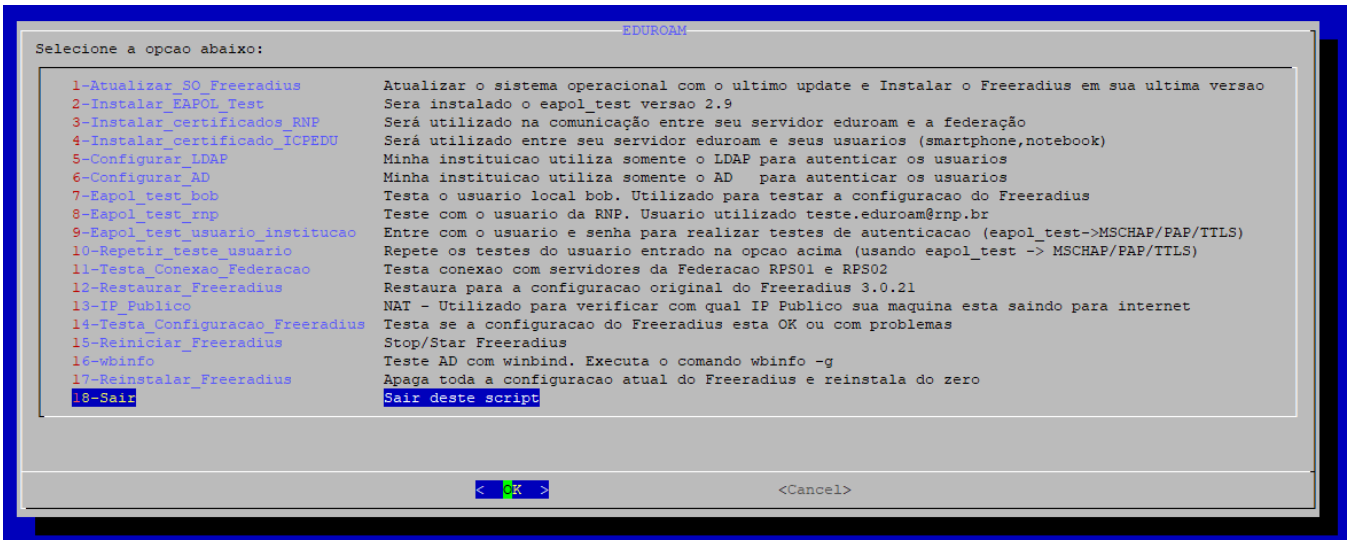
Execute a opção 11 - Testa Conexao Federacao, esta opção irá testar a conexão dos servidores da Federação RPS01 e RPS02



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.