IdP eduroam FreeRadius v3 com AD

>> 1. Configuração da autenticação FreeRadius 3 com AD

Nota

- A instalação do AD e sua configuração foram suprimidas
- Esta tarefa permite a autenticação via NTML através do AD (Active Directory).
- Será necessário configurar o Kerberos, Samba e o Winbind no servidor.
- Ingressaremos o servidor FreeRADIUS no domínio <DOMINIO_AD> como um servidor Windows
- O nome do novo servidor eduroam não pode ultrapassar de 15 caracteres, o samba não aceita, e o mesmo deve estar inserido dentro do arquivo /etc/hosts com o IP e o domínio (do AD) completo.
  exemplo:
  200.100.10.10 eduroam.rnp.local
- Dentro do arquivo /etc/resolv.conf informe o dominio e o ip do seu servidor principal do AD, conforme exemplo abaixo:

  search rnp.local

  domain rnp.local

  nameserver 200.130.77.1

  nameserver 200.130.77.2

  nameserver 200.130.77.3

  nameserver 200.130.77.4

Variáveis a serem substituídas no tutorial por valores particulares de sua instituição:

Para este tutorial teremos as variáveis e seus respectivos valores para um domínio **ufjf.br** do Windows

- **<ENDERECO_AD> = IP DO SERVIDOR AD**
- **<dominio_ad> = ufjf.br (domínio em minúscula)**
- **<DOMINIO_AD> = UFJF.BR (domínio em maiúscula)**
- **<DOMINIO> = UFJF (apenas o valor antes do .br)**
- **<login.adm> = Administrador do AD no domínio**

Firewall

- Portas que devem estar abertas no seu servidor AD
- `TCP e UDP: 88, 389, 464`

1.1 Instalando pacotes necessários

```
apt-get  install krb5-user libpam-krb5 winbind samba cifs-utils smbclient krb5-config libkrb5-3 libkadm5clnt-mit9
```

1.2 Adicionando o grupo referente ao WINBIND para o usuário freerad do FreeRadius e alterando permissões de pasta

```
usermod -a -G winbindd_priv freerad
chown root:winbindd_priv /var/lib/samba/winbindd_privileged/
```

1.3 Teste sobre resposta à consulta DNS para o servidor AD

```
host -t SRV _kerberos._tcp.<DOMINIO_AD>
host -t SRV _ldap._tcp.<DOMINIO_AD>
 host -t SRV _kerberos._udp.<DOMINIO_AD>
```

1.3.1 Exemplo de comando para consulta DNS

```
host -t SRV _kerberos._tcp.unicamp.br
host -t A rnp.local
```

1.3.2 Exemplo de retorno **corretamente** configurado

```
_kerberos._tcp.unicamp.br has SRV record 0 0 88 andromeda.ccuec.unicamp.br.
```

1.3.1 Exemplo de retorno com **erro**

```
Host _kerberos._tcp.unicamp.br not found: 3(NXDOMAIN)
```

> Só avance do passo 1.3 para o passo 1.4 se os testes funcionarem.
>
> Caso tenha tido algum problema, verifique a configuração do seu DNS para consulta ao FQDN do servidor AD de sua instituição.

1.4 Configurando o NTP para sincronização de hora entre os servidores Linux e Windows AD

```
apt-get install ntpdate
ntpdate <DOMINIO_AD>
```

1.5 Editando o Kerberos para responder pelo domínio local

1.5.1 Editando o arquivo de realms

```
vim /etc/krb5.conf
```

1.5.2 Insira o conteúdo no bloco realms

```
[realms]
<DOMINIO_AD> = {
                kdc = <ENDERECO_AD>:88
                default_domain = <dominio_ad>
                kpasswd_server = <ENDERECO_AD>
                admin_server = <ENDERECO_AD>
        }
```

>>

Um exemplo de conteúdo do bloco em uma instituição real pode ser visto clicando aqui

```
[realms]
IFMT.EDU.BR = {
                kdc = cactus.ifmt.edu.br
                default_domain = IFMT.EDU.BR
                kpasswd_server = cactus.ifmt.edu.br
                admin_server = cactus.ifmt.edu.br
        }
```

1.5.3 Adicione, no mesmo arquivo /etc/krb5.conf o conteúdo do bloco domain_realm

```
[domain_realm]
.<dominio_ad> = <dominio_ad>
<dominio_ad> = <dominio_ad>
```

1.6 Realizando teste de autenticação

Informa um usuário válido para o teste

1.6.1 Inicializando autenticação com usuário válido no AD. Execute o comando

```
kinit login@<DOMINIO_AD>
```

1.6.2 Verificando o resultado. Execute o comando

```
klist
```

1.6.3 A saída esperada é

```
Ticket cache: FILE:/tmp/krb5cc_0

Default principal: Administrador@<DOMINIO_AD>


Valid        starting   Expires           Service principal
19/07/2017 15:32  20/07/2018 01:32  krbtgt/<DOMINIO_AD>@<DOMINIO_AD>


renew        until 20/07/2018 15:32
```

1.7 Editando os arquivos referentes ao SAMBA

1.7.1 editando o /etc/samba/smb.conf

```
vim /etc/samba/smb.conf
```

1.7.2 O conteúdo do arquivo smb.conf deve ser **exatamente**

```
[global]
        security = ads
        realm = <DOMINIO_AD>
        workgroup = <DOMINIO>
        winbind enum users = yes
        winbind enum groups = yes
        template homedir = /home/%D/%U
        template shell = /bin/bash
        client use spnego = yes
        client ntlmv2 auth = yes
        encrypt passwords = yes
        winbind use default domain = yes
        restrict anonymous = 2
        domain master = no
        local master = no
        preferred master = no
        os level = 0
```

Para testar utilize o comando abaixo:

```
testparm
```

O resultado deve ser:

```
rlimit_max: increasing rlimit_max (1024) to minimum Windows limit (16384)
Loaded services file OK.
Server role: ROLE_DOMAIN_MEMBER
Press enter to see a dump of your service definitions
```

Como vemos acima temos uma linha informando que precisamos alterar a variável rlimit_max de 1024 para 16384
execute o seguinte comando abaixo:

```
echo "root            soft    nofile          16384" >> /etc/security/limits.conf
echo "root            hard    nofile          32768" >> /etc/security/limits.conf
```

Para testar abra um novo terminal e volte a executar o comando abaixo e compare o resultado.

```
testparm -s
```

O resultado deve ser:

```
Load smb config files from /etc/samba/smb.conf
Loaded services file OK.
Server role: ROLE_DOMAIN_MEMBER
Press enter to see a dump of your service definitions
```

1.7.3 Reiniciando os serviços WINBIND e SAMBA

```
service smbd restart
service nmbd restart
service winbind restart
```

1.7.4 Editando o arquivo nsswitch.conf

1.7.4.1 Entre no arquivo

```
vim /etc/nsswitch.conf
```

1.7.4.2 Edite as linhas para que tenham o conteúdo

```
passwd: compat winbind
group:  compat winbind
shadow: compat
```

Salve e saia do arquivo acima

1.7.5.1 Insira a maquina em seu servidor de DNS de seu AD
execute o comando:

```
net ads dns register -I IP-de-seu-AD -U usuario-com-poder-administrativo-do-AD
ou
net ads dns register -P
```

1.7.5.2 Insira a conta do servidor no domínio, considerando **“<login.adm>”** como seu **Administrador de Domínio AD**

Importante: Preferencialmente crie um novo usuário no AD para associar com o samba. Este usuário não pode expirar, se a conta do usuário expirar o IDP Eduroam perde acesso ao seu servidor AD.
execute o comando:

```
net ads join osName=Ubuntu osVer="LTS-12" -U usuario-com-poder-administrativo-do-AD
```

1.8 Teste de ingresso no domínio

1.8.1 Execute o comando

```
net ads testjoin
```

1.8.2 Resultado esperado para o comando

```
Join is OK
```

1.8.3 Teste de login de usuário no domínio AD local. Onde, se deve ter a credencial no formato **"login%senha"**.

```
wbinfo -a login%senha
```

1.8.4 Resultado esperado para o comando

```
plaintext password authentication succeeded
challenge/response password authentication succeeded
```

1.8.5 Teste de autenticação usando a ferramenta ntlm_auth. Observe que novamente utiliza-se o usuário já cadastrado na base do AD, pertencente àquele domínio

1.8.5.1 Execute o comando

```
ntlm_auth --request-nt-key --domain=<DOMINIO> --username=login
```

1.8.5.2 Resultado esperado para o comando

```
NT_STATUS_OK: Success (0x0)
```

1.9 Configurando o FreeRadius 3.0

1.9.1 Edite o arquivo /etc/freeradius/mods-available/ntlm_auth para que ele tenha exatamente o conteúdo a seguir, respeitando o valor da variável **<DOMINIO>** seu ambiente.

```
exec ntlm_auth {
                wait = yes
                program = "/usr/bin/ntlm_auth --request-nt-key --domain=<DOMINIO> --username=%{mschap:User-
Name} --password=%{User-Password}"
        }
```

1.9.2 Edite também o arquivo /etc/freeradius/mods-available/mschap para que tenha exatamente o conteúdo a seguir, respeitando o valor da variável **<DOMINIO>** seu ambiente.

```
mschap {
        use_mppe = yes
        require_encryption = yes
        require_strong = yes
        with_ntdomain_hack = yes
        ntlm_auth = "/usr/bin/ntlm_auth --request-nt-key --username=%{%{Stripped-User-Name}:-%{%{User-Name}:-
None}} --challenge=%{%{mschap:Challenge}:-00} --nt-response=%{%{mschap:NT-Response}:-00}"
        # ntlm_auth = "/usr/bin/ntlm_auth --request-nt-key --username=%{%{Stripped-User-Name}:-%{User-Name:-
None}} --domain=%{%{mschap:NT-Domain}:-<DOMINIO>} --challenge=%{mschap:Challenge:-00} --nt-response=%{mschap:NT-
Response:-00}"
}
```

1.9.3 Edite os arquivos **/etc/freeradius/sites-enabled/default** e **/etc/freeradius/sites-enabled/inner-tunnel** para que tenham o módulo ntlm_auth carregado para autenticação

1.9.3.1 Editando o arquivo /etc/freeradius/sites-enabled/default

```
vim /etc/freeradius/sites-enabled/default
```

1.9.3.2 Adicionando o conteúdo no bloco authenticate

```
authenticate {
        ...
        ntlm_auth
        ...
}
```

1.9.3.4 Editando o arquivo /etc/freeradius/sites-enabled/inner-tunnel

```
vim /etc/freeradius/sites-enabled/inner-tunnel
```

1.9.3.5 Adicionando o conteúdo no bloco authenticate

```
authenticate {
        ...
        ntlm_auth
        ...
}
```

1.10 Reiniciando o serviço FreeRadius

```
service freeradius restart
```

1.11 Teste final. Realize a autenticação por radtest a partir de um usuário existe no AD.

```
radtest -t mschap login-usuario-AD senha-usuario-AD localhost ChaveSecretaClientLocalhost
```