6.8 Ingressar cliente Linux no domínio

Diferente do Windows, o Linux requer uma atenção especial quanto trata-se de inserção em um determinado domínio. Isso porque ele exige alguns fatores que devem ser levados em consideração na hora de integrá-lo. Neste laboratório será abordado os aspectos necessários para realizarmos este procedimento de forma correta.

Para que este procedimento seja possível, iremos utilizar três serviços essenciais, são eles: Kerberos (protocolo de rede usado para autenticação de usuários), Winbind: (daemon usado pelo PAM, NSSWITCH e Samba, permitindo que máquinas com o sistema GNU/Linux comuniquem-se com DC Active Directory) e o Samba.

ATENÇÃO, OS PASSOS A SEGUIR DEVEM SER EXECUTADOS NA ESTAÇÃO DE TRABALHO LINUX!

6.8.1 Ajustes iniciais

Antes de iniciar realize os seguintes ajustes no arquivo hosts:

```
root@ws-linux:/# vim /etc/hosts
```

E verifique se a linha a seguir esta configurada corretamente:

```
127.0.1.1 ws-linux.empresax.com.br ws-linux
```

Instale as seguintes dependências:

```
root@ws-linux:/# apt install krb5-user krb5-config winbind samba samba-common smbclient
cifs-utils libpam-krb5 libpam-winbind libnss-winbind ntp
```

Durante a instalação do “kerberos“, pode ser perguntado algo relacionado ao KDC, mas ignore e pressione ENTER. Trataremos deste assunto no decorrer do artigo.

Sincronize a Data/Hora da estação com a do Controlador de Domínio:

```
root@ws-linux:/# nano /etc/ntp.conf
```

Onde o conteúdo começa com a palavra “pool“, comente estas linhas com uma cerquilha “#“, e adicione o conteúdo conforme segue:

```
# pool 0.debian.pool.ntp.org iburst
# pool 1.debian.pool.ntp.org iburst
# pool 2.debian.pool.ntp.org iburst
# pool 3.debian.pool.ntp.org iburst
#Controlador de Dominio
server 172.16.1.5
restrict 172.16.1.5
```

Reinicie o serviço NTP:

```
root@ws-linux:/# systemctl restart ntp
root@ws-linux:/# systemctl status ntp
```

Ajuste o arquivo resolv.conf apontando a resolução de nomes para o servidor Samba:

```
root@ws-linux:/# vim /etc/resolv.conf
```

E adicione as seguintes linhas:

search empresax.com.br
nameserver 172.16.1.5

6.8.2 Configuração do Kerberos

Para que o usuário consiga autenticar-se no controlador de domínio iremos utilizar um protocolo de autenticação de redes chamado kerberos. O controlador de domínio com o serviço de Active Directory instalado já possui por default um KDC (Controlador de domínio Kerberos) apto para autenticar este tipo de protocolo. Iremos então editar o arquivo "/etc/krb5.conf":

```
root@ws-linux:/# mv /etc/krb5.conf /etc/krb5.conf.bkp
root@ws-linux:/# vim /etc/krb5.conf
```

E realizar as configurações conforme ilustrado abaixo:

```
[logging]
        Default = FILE:/var/log/krb5.log

[libdefaults]
        ticket_lifetime = 24000
        clock-skew = 300
        default_realm = EMPRESAX.COM.BR
        dns_lookup_realm = true
        dns_lookup_kdc = true
[realms]
        EMPRESAX.COM.BR = {
                kdc = samba4.empresax.com.br
                admin_server = samba4.empresax.com.br
                default_domain = samba4.empresax.com.br
        }
[domain_realm]
        .empresax.com.br = EMPRESAX.COM.BR
        empresax.com.br = EMPRESAX.COM.BR
[login]
        krb4_convert = true
        krb4_get_tickets = true
```

Depois de configurado o kerberos, precisamos testar a comunicação com o controlador de domínio. Para isto, utilizaremos o comando "kinit" seguido pelo parâmetro "Nome de usuário que esteja cadastrado no domínio":

> ***root@ws-linux:/# kinit administrator***

Será gerado um ticket kerberos e o retorno do comando será similar ao da figura abaixo:

```
root@ws-linux:~# kinit administrator
Password for administrator@EMPRESAX.COM.BR:
Warning: Your password will expire in 36 days on dom 04 jul 2021 22:31:28 -03
```

Após realizar o comando e o mesmo não retornar nenhuma mensagem de erro, é possível verificar o "ticket kerberos" gerado através do comando "klist":

> ***root@ws-linux:/# klist***

O retorno do comando será similar ao da figura abaixo:

```
root@ws-linux:~# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: administrator@EMPRESAX.COM.BR

Valid starting       Expires              Service principal
28/05/2021 23:18:49  29/05/2021 05:58:46  krbtgt/EMPRESAX.COM.BR@EMPRESAX.COM.BR
```

6.8.3 Configuração do Samba

Antes de ingressarmos a Estação de Trabalho Linux no domínio é necessário realizar algumas configurações preliminares no Samba4. Para isso, edite o arquivo de configuração /etc/samba/smb.conf:

> ***root@ws-linux:/# mv /etc/samba/smb.conf /etc/samba/smb.conf.bkp***
> ***root@ws-linux:/# vim /etc/samba/smb.conf***

Insira as seguintes linhas:

```
[global]
        workgroup = EMPRESAX
        server string = ws-linux
        netbios name = ws-linux
        realm = EMPRESAX.COM.BR

        log file = /var/log/samba/log.%m
        os level = 2
        preferred master = no
        max log size = 50
        debug level = 1

##### Authentication #####

        security = user
        encrypt passwords = yes
        allow trusted domains = yes
```

```
        winbind uid = 10000-20000
        winbind gid = 10000-20000
        winbind enum users = yes
        winbind enum groups = yes
        winbind use default domain = yes
        winbind refresh tickets = yes
        template shell = /bin/bash
        template homedir = /home/%D/%U
        client use spnego = yes
        domain master = no
```

Após configurado o arquivo “smb.conf“, reinicie o serviço do Samba e do Winbind.

```
root@ws-linux:/# systemctl restart winbind
root@ws-linux:/# systemctl restart smbd
```

Edite novamente o arquivo smb.conf e altere a seguinte linha conforme segue:

security = user

Para

security = ads

Salve e feche a edição do arquivo, porém desta vez, reinicie somente o Samba:

```
root@ws-linux:/# systemctl restart smbd
```

6.8.4 Ingressando o Debian 10 no domínio

Feito isso já podemos passar para o próximo passo e ingressar nossa máquina cliente no domínio.

Se todas configurações foram feitas de forma correta, podemos ingressar a máquina no domínio executando o seguinte comando:

```
root@ws-linux:/# net ads join -U administrator
```

Se a máquina ingressar no domínio, serão exibidas as seguintes informações:

```
root@ws-linux:~# net ads join -U administrator
Enter administrator's password:
Using short domain name -- EMPRESAX
Joined 'WS-LINUX'_to dns domain 'empresax.com.br'
```

Agora serão realizados os testes para certificar se o controlador de domínio está respondendo. Para isso, utilize os seguintes comandos:

```
root@ws-linux:/# net ads testjoin
```

Se tudo correr bem, o sistema responderá: “Join is OK”

Agora será testado o Winbind. Para isso, reinicie o serviço:

```
root@ws-linux:/# systemctl restart winbind
```

Agora execute o comando wbind com a opção -t:

```
root@ws-linux:/# wbinfo -t
```

Se tudo correr bem o sistema responderá:

checking the trust secret for domain EMPRESAX via RPC calls succeeded

Agora verifique se já o sistema já consegue buscar os grupos e usuários do controlador de domínio com os seguintes comandos:

```
root@ws-linux:/# wbinfo -u
```

(Serão listados os usuários criados no AD)

```
root@ws-linux:/# wbinfo -g
```

(Serão listados os grupos criados no AD)

6.8.5 Ajustes finais

Como agora estamos trabalhando com usuários e grupos do domínio, precisamos informar ao sistema que desejamos trabalhar com o “winbind” para procurar nossas informações de login. Para isso, é necessário editar duas linhas no arquivo “/etc/nsswitch.conf“, como segue:

```
root@ws-linux:/# vim /etc/nsswitch.conf
```

Insira a palava "winbind" após a palavra "systemd", nas linhas "passwd" e "group", como apresentado na figura abaixo:

```
# `info libc "Name Service Switch"' for information

passwd:         files systemd winbind
group:          files systemd winbind
shadow:         files
gshadow:        files
```

Após editar o arquivo, realize o restart do serviço “Winbind” e “Samba”

```
root@ws-linux:/# systemctl restart winbind
root@ws-linux:/# systemctl restart smbd
```

Para as distribuições Debian é necessário realizar uma alteração no arquivo “/etc/pam.d/common-session“. Esta alteração faz o diretório home de cada usuário ser criado automaticamente no inicio

de cada sessão após a autenticação do usuário, setando as permissões para os arquivos e diretórios com a “umask 0022” e obtendo do diretório “/etc/skel” seus sub-diretórios e arquivos padrões.

> ***root@ws-linux:/# vim /etc/pam.d/common-session***

Após o linha que contém:

session required pam_unix.so

Inclua:

session required pam_mkhomedir.so umask=0022 skel=/etc/skel

Seu sistema já esta no domínio e apto para uso, reinicia o sistema e tente acessar com um usuário do domínio:

> ***root@client:/# reboot***