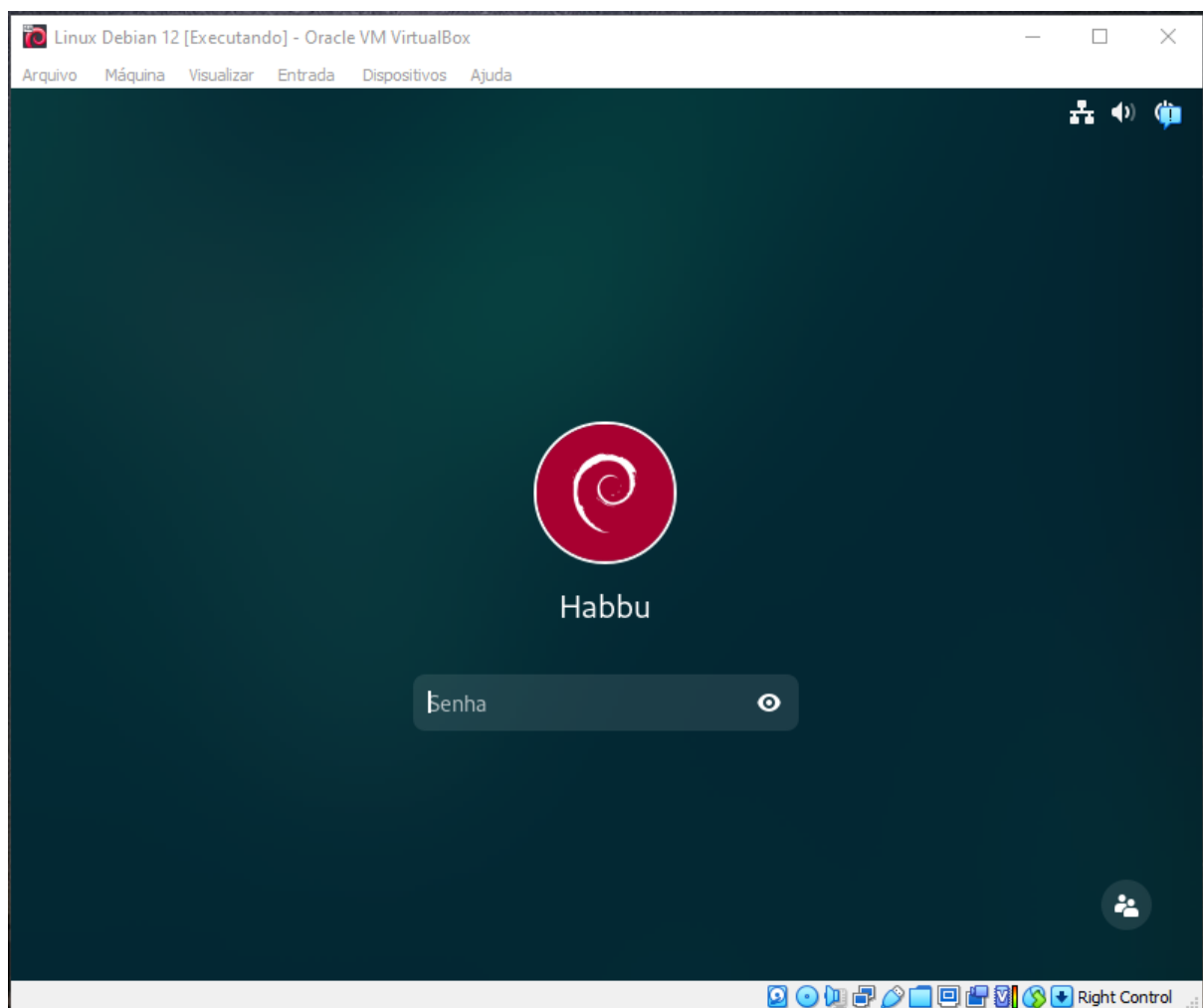


Criação das VMs do domain controller com rede de mais duas máquinas 1 windows e uma linux debian v12.

Windows Server

Usuário linux debian v12

Depois da VM com debian instalado comecei as instalações dos pacotes necessários para a inclusão no domain controller.



vm-debian

Instalando o editor de texto VIM

instalação.

Digite, no terminal

```
$ sudo apt install vim
```

- \$ indica que você deve usar o usuário comum para fazer essa operação.
- sudo serve para pedir permissões de administrador temporariamente.
- apt do inglês, *Advanced Package Tool*, em português, *Ferramenta de Empacotamento Avançada*; é a ferramenta que nos ajuda na instalação, atualização e desinstalação de programas, entre outras funções.
- install é o comando de instalar, indicando ao apt o que fazer.

ou

```
$ sudo apt install neovim
```

para instalar o NeoVIM.

Eu vou optar por usar o NeoVIM, então algumas configurações podem ser um pouco diferentes, mas os comandos são os mesmos. Fiquem tranquilos quanto a isso.

No Debian e derivados (Ubuntu, por exemplo) existem algumas versões diferentes do vim no repositório, que podem ser instalados pelo apt:

- [vim-tiny](#) que é uma versão reduzida do vim.
- [vim](#) que é a versão padrão do vim.
- [vim-nox](#) que é a versão padrão do vim compilado com suporte interno a Lua, Perl, Python 3, Ruby e Tcl (usado pelos plugins, e não por quem estiver desenvolvendo).
- [vim-gtk](#) que é o vim-nox junto com uma interface gráfica GTK2.
- [vim-gtk3](#) que é o vim-nox junto com uma interface gráfica GTK3.
- [vim-athena](#) que é o vim-nox junto com uma interface gráfica Athena.

Assim, se for utilizar o vim, recomendo o vim-nox caso queira apenas a linha de comando, ou o vim-gtk3 se for utilizar tanto na linha de comando quanto na interface gráfica (conhecida também como gvim).

Colocando Linux no Domínio – Debian



Este Artigo tem como objetivo realizar o ingresso de uma máquina Linux em um domínio. Diferente do Windows, o Linux requer uma atenção especial quanto trata-se de integração em um ambiente corporativo. Isso porque ele exige alguns fatores que devem ser levados em consideração na hora de integrá-lo. Aqui tentaremos abordar todos os aspectos necessários para realizarmos este procedimento de forma profissional, trazendo ao final do artigo uma integração correta.

Para que este procedimento seja possível, iremos utilizar três serviços essenciais, os quais são:

Kerberos: É um protocolo de rede usado para autenticação de usuários e/ou serviços de rede, como o Active Directory. utilizando um sistema criptografado, permitindo comunicações seguras e identificadas em redes, fazendo uso de tickets (chaves criptografadas).

Winbind: O Winbind é um daemon usado pelo PAM, NSSWITCH, Samba e podendo ser usado por outros serviços de rede e/ou sistema, fazendo a interface entre o PDC e o computador cliente rodando o serviço Winbindd, permitindo que máquinas com o sistema GNU/Linux comuniquem-se com DC Active Directory.

Samba: É um serviço cuja principal função é disponibilizar recursos compartilhados em uma rede, tais como arquivos e impressoras, além de também ser utilizado como controlador de domínio.

CONSIDERAÇÕES

Vamos levar em consideração que você já possui um ambiente com um servidor de domínio Windows Server / Samba com o Active Directory, DNS e DHCP instalados e funcionando. Neste exemplo estaremos utilizando o Debian 12

Veja a disposição dos servidores na rede para explicação do artigo:

Floresta Domínio → COMPANYPERICIAX.COM.BR

Servidor controlador de domínio → 192.168.2.1

Servidor DHCP → 192.168.2.1

Servidor DNS primário → 192.168.2.1

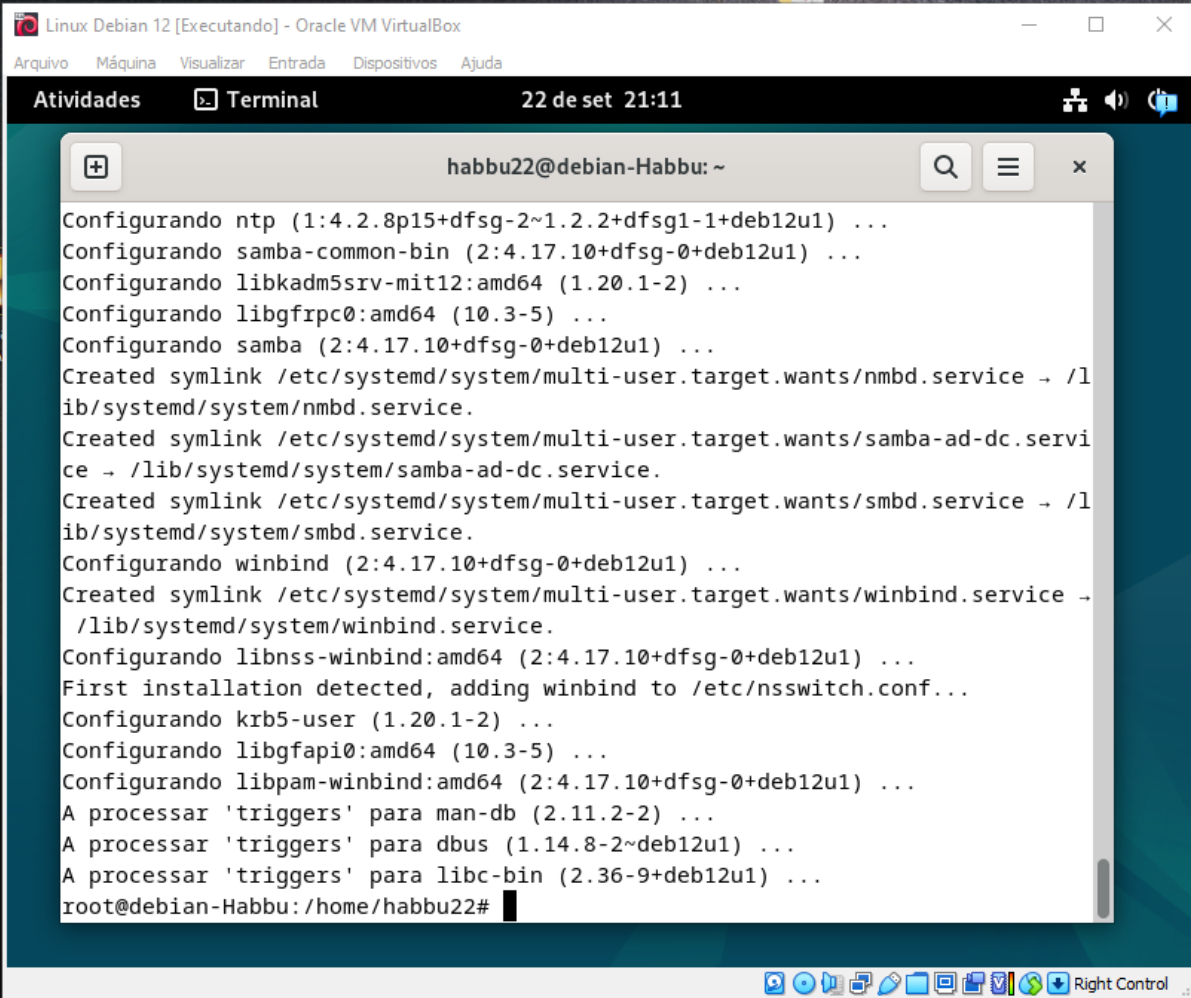
Desktop client → Habbu (Distribuição: Debian 12 “BookWorm”)

Nota: Para editar os arquivos de configuração você pode escolher qual editor padrão deseja usar. Neste artigo iremos utilizar o editor “vi” como padrão.

1) INSTALAÇÃO DE PACOTES NECESSÁRIOS.

```
apt-get 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.



```
Linux Debian 12 [Executando] - Oracle VM VirtualBox
Arquivo  Máquina  Visualizar  Entrada  Dispositivos  Ajuda
Atividades  Terminal  22 de set 21:11

habbu22@debian-Habbu: ~
Configurando ntp (1:4.2.8p15+dfsg-2~1.2.2+dfsg1-1+deb12u1) ...
Configurando samba-common-bin (2:4.17.10+dfsg-0+deb12u1) ...
Configurando libkadm5srv-mit12:amd64 (1.20.1-2) ...
Configurando libgfrpc0:amd64 (10.3-5) ...
Configurando samba (2:4.17.10+dfsg-0+deb12u1) ...
Created symlink /etc/systemd/system/multi-user.target.wants/nmbd.service → /lib/systemd/system/nmbd.service.
Created symlink /etc/systemd/system/multi-user.target.wants/samba-ad-dc.service → /lib/systemd/system/samba-ad-dc.service.
Created symlink /etc/systemd/system/multi-user.target.wants/smbd.service → /lib/systemd/system/smbd.service.
Configurando winbind (2:4.17.10+dfsg-0+deb12u1) ...
Created symlink /etc/systemd/system/multi-user.target.wants/winbind.service → /lib/systemd/system/winbind.service.
Configurando libnss-winbind:amd64 (2:4.17.10+dfsg-0+deb12u1) ...
First installation detected, adding winbind to /etc/nsswitch.conf...
Configurando krb5-user (1.20.1-2) ...
Configurando libgfapi0:amd64 (10.3-5) ...
Configurando libpam-winbind:amd64 (2:4.17.10+dfsg-0+deb12u1) ...
A processar 'triggers' para man-db (2.11.2-2) ...
A processar 'triggers' para dbus (1.14.8-2~deb12u1) ...
A processar 'triggers' para libc-bin (2.36-9+deb12u1) ...
root@debian-Habbu: /home/habbu22#
```

2) EDIÇÃO DO ARQUIVO `/etc/hosts`.

Em nossa máquina “Habbu” que pretendemos colocar no domínio, entre no arquivo “`sudo vim /etc/hosts`” e adicione o complemento do domínio junto ao host da máquina cliente.

Opcional: Também adicione o endereço de ip do servidor controlador de domínio, este procedimento ajuda na resolução de nomes, pois já estamos setando diretamente quem será o controlador.

Linux Debian 12 [Executando] - Oracle VM VirtualBox

Arquivo Máquina Visualizar Entrada Dispositivos Ajuda

Atividades Terminal 22 de set 21:24

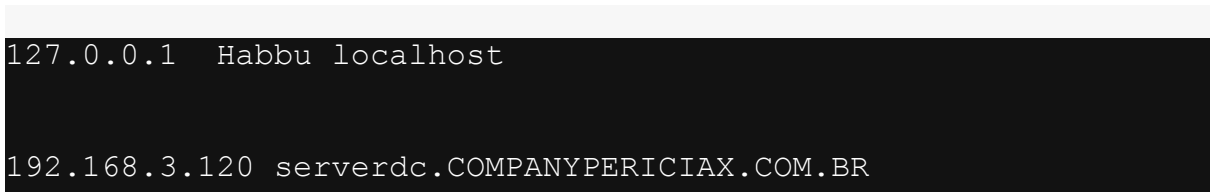
habbu22@debian-Habbu: ~

```
E325: ATENÇÃO
Foi encontrado um arquivo de troca de nome "/etc/.hosts.swp"
    pertence a: root    com data: sex set 22 21:17:11 2023
    nome do arquivo: /etc/hosts
    modificado: SIM
    nome de usuário: root    nome do host: debian-Habbu
    ID do processo: 5779
Ao abrir o arquivo "/etc/hosts"
    com data de: sex set 22 17:14:27 2023

(1) Outro programa pode estar editando o mesmo arquivo. Se for esse
    o caso, cuidado para não acabar com duas versões do mesmo arquivo
    ao fazer alterações. Saia, ou continue com cuidado.
(2) Uma sessão de edição para esse arquivo travou.
    Se for esse o caso, use ":recover" ou "vim -r /etc/hosts"
    para recuperar as alterações (veja ":help recovery").
    Se você já fez isso, exclua o arquivo de troca "/etc/.hosts.swp"
    para evitar esta mensagem.

O arquivo de troca "/etc/.hosts.swp" já existe!
[A]brir somente-leitura, (E)ditar mesmo assim, (R)ecuperar, E(x)cluí-lo, (S)air, (C)ancelar: █
```

Right Control



3) SINCRONIZANDO DATA/HORA COM O CONTROLADOR DE DOMÍNIO.

Para que possamos ser autenticados pelo controlador de domínio é de primordial importância que estejamos sincronizados com a data e a hora do mesmo. No Linux é possível realizar este procedimento de forma automática, configurando um serviço de “NTP”.

Acesse o arquivo de configuração “*/etc/ntp.conf*” e nas linhas do arquivo onde o conteúdo começa com a palavra “pool”, comente estas linhas com uma *cerquilha* “#”, e adicione o conteúdo conforme ilustrado abaixo, salve e saia do arquivo.

```
# 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 192.168.3.120

restrict 192.168.3.120
```

Realizar o restart do serviço “NTP”. Como estamos utilizando Debian 8, o mesmo já possui um novo sysinit chamado “systemD”, para que possamos restartar um serviço devemos utilizar o seguinte comando:

(Restarta o serviço)

```
systemctl restart ntp.service
```

ou (Para e inicia o serviço)


```
systemctl stop ntp.service
```

```
systemctl start ntp.service
```

(Verifica status do serviço)

```
systemctl status ntp.service
```

Caso esteja utilizando versões anteriores do Debian, ou uma outra distribuição que esteja baseada em outro sysinit como por exemplo o “systemV” antecessor do “systemD”, utilize o seguinte comando:

(Reinicia o serviço)

```
/etc/init.d/ntp restart
```

ou (Para e inicia o serviço)

```
/etc/init.d/ntp stop
```

```
/etc/init.d/ntp start
```

Nota: Para sistemas que possuem outros sysinit's como o Ubuntu que possui o “upstart”, consulte a página da distribuição para maiores esclarecimentos.

4) EDIÇÃO DO ARQUIVO “/etc/resolv.conf”.

No ambiente apresentado estamos considerando que a máquina cliente “Habbu” esta recebendo IP através de um serviço DHCP startado no servidor controlador de domínio “serverdc”. Caso não esteja utilizando o serviço DHCP, é possível setar os servidores de nomes “DNS” no arquivo “/etc/resolv.conf” conforme ilustrado abaixo.

```
# Generated by NetworkManager

search COMPANYPERICIAX.COM.BR

nameserver 192.168.3.120
```

5) CONFIGURAÇÃO 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” e realizar as configurações conforme ilustrado abaixo. Salve e saia do arquivo.

```
0  [logging]
1
2  Default = FILE:/var/log/krb5.log
3
4
5  [libdefaults]
6
7  ticket_lifetime = 24000
8
9  clock-skew = 300
10
11 default_realm = COMPANYPERICIAX.COM.BR
12
13 dns_lookup_realm = true
```

```
0 dns_lookup_kdc = true
7
0
8
[realms]
0
9 COMPANYPERICIAX.COM.BR = {
1 kdc = serverdc.COMPANYPERICIAX.COM.BR
0
default_domain = COMPANYPERICIAX.COM.BR
1
1 admin_server = serverdc.COMPANYPERICIAX.COM.BR
1
2 }
1
2
1
3
[domain_realm]
1
4 .COMPANYPERICIAX.COM.BR = COMPANYPERICIAX.COM.BR
1
5 COMPANYPERICIAX.COM.BR = COMPANYPERICIAX.COM.BR
1
6
[login]
1
7 krb4_convert = true
1
8 krb4_get_tickets = false
```

```
1
9
2
0
2
1
2
2
2
3
2
4
```

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*”, conforma ilustrado abaixo.

```
kinit rafael
```

Será solicitado a senha de usuário, digite a senha e pressione “ENTER”.

Após realizar o comando e o mesmo não retornar nenhuma mensagem de erro, é possível verificar o “ticket kerberos” gerado através do comando “*klist*” conforme ilustrado abaixo.

```
klist
```

Mostrando como resultado:

```
Ticket cache: FILE:/tmp/krb5cc_10001_j3SWTA

Default principal: AMAURI@AFAGAH.COM.BR

Valid starting Expires Service principal
31-01-2017 18:15:56 01-02-2017 00:55:49
krbtgt/COMPANYPERICIAX.COM.BR@COMPANYPERICIAX.COM.BR
```

6) CONFIGURANDO O SAMBA.

Também antes de ingressarmos na máquina cliente “Habbu” no domínio é necessário realizar algumas configurações preliminares no Samba. Neste artigo já estamos utilizando o Samba 4, alguns parâmetros estão sendo disponibilizados, mesmo que não sejam necessários para o artigo em questão. Estes padrões são úteis caso deseje compartilhar informações de sua máquina cliente, ou transformá-la em um servidor de arquivos. Faça uma cópia de segurança do arquivo “*/etc/samba/smb.conf*” de sua máquina e crie um novo arquivo conforme conteúdo ilustrado abaixo.

```
01 [global]
02
03 workgroup = Habbu
04
05 server string = Maquina Cliente
06
07
08 netbios name = DCSR VH1
09
10 VIRTUALrealm = COMPANYPERICIAX.COM.BR
11
12 #veto files = /*.exe/*.bat/*.inf/*.pif/
13
14
15
16 #===== Log do Samba
17 =====.
18
19 log file = /var/log/samba/samba.log
20
21
22 os level = 2
23
24 preferred master = no
25
26
27 max log size = 50
28
29
30 debug level = 1
31
32
33
34
35
36 #===== Autenticação
37 =====.
```

```
17 security = ads

18 encrypt passwords = yes

19 # password server = 192.168.2.1

20 allow trusted domains = yes

21

22 #===== Configuração WINBIND
=====
23
24 winbind uid = 10000-20000
25
26 winbind gid = 10000-20000
27
28 winbind enum users = yes
29
30 winbind enum groups = yes
31
32 winbind use default domain = yes
33
34 winbind refresh tickets = yes
35
36 template shell = /bin/bash
37
38 template homedir = /home/%D/%U
39
40 client use spnego = yes
41
42 domain master = no
```

```
33
34 #===== Configuração LINKSIMBOLICO
=====
35
unix extensions = no

wide links = yes
```

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

OBS: Iremos utilizar o padrão “systemD” conforme ilustrado no item 3 deste artigo.

(Restarta o serviço)

```
systemctl restart winbind.service

systemctl restart smbd.service
```

ou (Para e inicia o serviço)

```
systemctl stop winbind.service

systemctl start winbind.service

systemctl stop smbd.service

systemctl start smbd.service
```

(Verifica status do serviço)


```
systemctl status winbind.service
```

```
systemctl status smbd.service
```

7) CORRIGINDO ERRO WINBIND.

Diferentemente do Debian 8 – Jessie, no Debian 9 – Stretch, vamos precisar realizar um procedimento diferenciado, você deve ter reparado que ao reiniciar os serviços, o Winbind não iniciou. Para corrigir o problema precisamos realizar uma pequena alteração em nosso `/etc/samba/smb.conf`.

Acesse novamente o arquivo `smb.conf` e altere a seguinte linha conforme ilustrado abaixo.

```
security = ads
```

Para

```
security = user
```

Salve, saia do arquivo e reinicie os serviços Samba e Winbind.

```
systemctl restart winbind.service
```

```
systemctl restart smbd.service
```

Repare que agora os dois serviços foram iniciados com sucesso. Feito isso, volte nas configurações do arquivo `smb.conf` e retorne a configuração conforme ilustrado abaixo.

```
security = user
```

Para

```
security = ads
```

Salve e sai do arquivo, porém desta vez, reinicie somente o Samba conforme ilustrado abaixo.

```
systemctl restart smbd.service
```

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

8) INGRESSANDO A MÁQUINA CLIENTE NO DOMÍNIO.

Agora que nossas configurações estão corretas, podemos ingressar a máquina no domínio conforme comando ilustrado abaixo.

```
net ads join -U administrador
```

Nota: A conta passada para este comando precisa ter poderes de ingressar máquinas no domínio. Em nosso exemplo, foi utilizado a conta “administrador” do domínio.

Após executar o arquivo será retornada uma informação parecida com a ilustrada abaixo.

```
Using short domain name - Habbu
```

```
Joined 'DCSRVH1' to realm 'COMPANYPERICIAX.COM.BR'
```

Agora vamos testar se o controlador de domínio está respondendo. Utilizando os seguintes comandos:

```
net ads testjoin
```

Se tudo correr bem o sistema responderá:

```
Join is OK
```

Também vamos testar utilizando o seguinte comando:

```
wbinfo -t
```

Se tudo correr bem o sistema responderá:

```
checking the trust secret for domain Habbu via RPC calls  
succeeded
```

Feito isto, precisamos testar e verificar se já conseguimos buscar os grupos e usuários do controlador de domínio conforme o seguinte comando a seguir:

(Lista de usuários do domínio)

```
wbinfo -u
```

(Lista de grupos do domínio)

```
wbinfo -g
```

Nota: Caso não seja possível trazer alguma das duas listas informadas, reinicie o “winbind” novamente. Se mesmo assim não conseguir executar os comandos com sucesso, volte o artigo e analise os passos anteriores refazendo a configuração, provavelmente algo passou despercebido.

Também é possível utilizar outros dois comandos para realizar a verificação, mas a diferença é que trazem a informação dos usuários e grupos locais, seguidos dos usuários e grupos do domínio.

(Lista usuários Local/Domínio)

```
getent passwd
```

(Lista grupos Local/Domínio)

```
getent group
```

Caso queira retirar a máquina do domínio utilize o seguinte comando:

```
net ads leave -U administrador
```

Nota: Após a integração da máquina cliente ao domínio, os serviços Samba e Winbind poderão ser reiniciados sem nenhum problema.

9) EDIÇÃO DO ARQUIVO “/etc/nsswitch.conf”.

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”, conforme ilustrado abaixo.

```
7 passwd:          compat winbind
```

```
8 group:           compat winbind
```

Após editar o arquivo, realize o restart do serviço “*Winbind*” e “*Samba*” conforme demonstrado no item “6” deste artigo.

Seu sistema já esta no domínio e apto para uso.

10) DETALHES DEBIAN.

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.

Após o linha que contém:

```
session required pam_unix.so
```

Inclua:

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

CONCLUSÃO

Neste artigo foi demonstrado como colocar uma máquina baseada na distribuição Debian 9 – Stretch no domínio de forma correta.

Se você gostou deste post e através dele pude lhe ajudar, o que acha de aproximarmos nosso contato? Siga meu blog e me adicione no [Linkedin](#), aproveite para classificar algumas das minhas competências/recomendações, este simples gesto faz toda a diferença.

Fontes:

<https://rafaelit.com.br/colocando-linux-no-dominio-debian-9/>