FAZER BACKUP DE TODOS OS FICHEIROS DE CONFIG!!!

FAZER apt update

CONFIRMAR QUE ESTÁ EM BRIDGED ADAPTER PRIMEIRO

Comandos Básicos em Linux:

ls (listar) - serve para listar o conteúdo de pastas

ls -l (listagem detalhada) - serve para listar o conteúdo das pastas em formato de detalhe

cd (change directory) - serve para entrar dentro das pastas

cd .. - Serve para voltar para a pasta anterior

mkdir (make directory) - serve para criar pastas

touch - serve para criar ficheiros em branco

xed (editor de texto) - serve para criar ou editar ficheiros

nano (editor de texto de linhade comandos) - cria ou edita ficheiros

cp (copy) - serve para copiar ficheiros

cp -r (copy) - serve para copiar pastas

mv (move) - serve para mover ou renomear ficheiros ou pastas

rm (remove) - serve para apagar ficheiros

rm -r (remove) - serve para apagar pastas

cat - serve para listar o conteúdo de um ficheiro

tree - estrutura em árvore

man – serve para mostrar todas as opções de um determinado comando

***** - zero ou mais caracteres

? – um caracter (sempre 1 caracter)

> - redireciona o output do comando para um ficheiro de texto, eliminando o conteúdo do ficheiro de destino se existir

>> - redireciona o output do comando para um ficheiro de texto, acrescentando o output ao conteúdo que poderá já existir no ficheiro

head -10 – mostra as primeiras n linhas do ficheiro, neste caso 10 linhas

tail -15 – mostra as últimas n linhas do ficheiro, neste caso 15 linhas

sort – mostra como output o conteúdo do ficheiro ordenado

wget URL -O file.txt – Faz o download do conteúdo do URL e guarda diretamente no ficheiro file.txt

Qualquer comando tem várias opções que podemos descobrir usando o comando man nome_do_comando, por exemplo: man sort

/ - raiz do sistema, apenas o root pode escrever por defeito

~ - homefolder de cada utilizador (utilizador com que estamos logados no momento)

/home – local onde estão as homefolders de todos os utilizadores excepto o root

/root – homefolder do root

/home/ciber – homefolder do utilizador ciber

nano – editor de texto para ambientes em linha de comandos, tal como o xed, cria ou edita ficheiros – para sair do editor ctrl + x

su - - Serve para passar de um utilizador normal para root

init 0 - desliga a máquina

init 6 - reinicia a máquina

/etc/passwd – Ficheiro que contém todos os utilizadores do sistema (um por linha)

/etc/group – Ficheiro que contém todos os grupos de utilizadores do sistema e os utilizadores que pertencem a cada grupo (um por linha)

/etc/shadow – Ficheiro que contém as passwords (encriptadas) dos utilizadores

passwd *utilizador* – comando para alterar a password de um utilizador. O root pode alterar a password de qualquer utilizador. Cada utilizador para alterar a sua própria password usa apenas o comando passwd

adduser *utilizador* – comando para criar utilizadores

deluser *utilizador* – comando para eliminar utilizadores

deluser *utilizador* --remove-home – comando para eliminar utilizadores e a sua homefolder ao mesmo tempo

addgroup *grupo* – comando para adicionar grupos de utilizadores

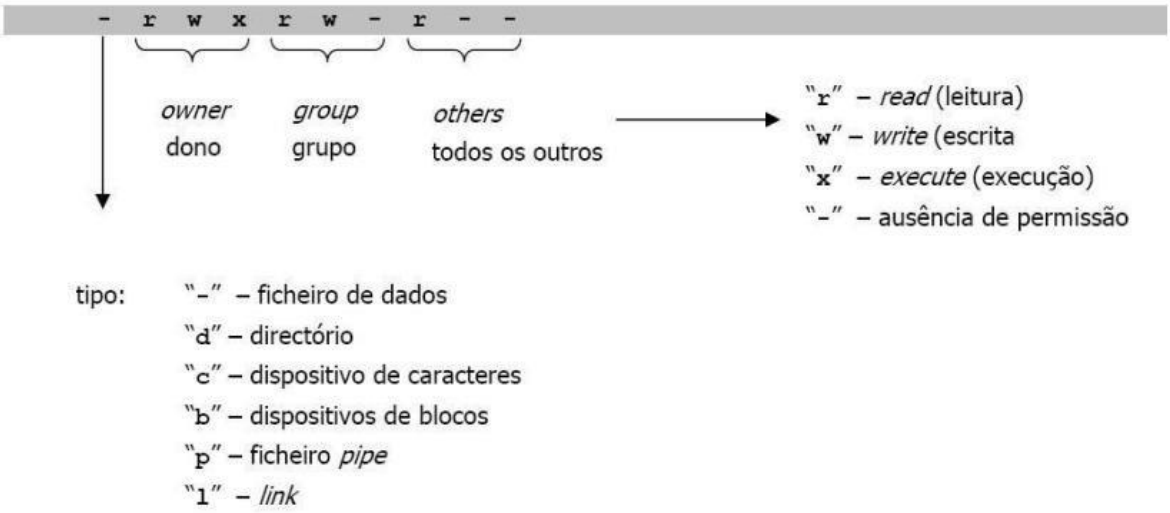
adduser *utilizador grupo* – comando para adicionar utilizadores a grupos

deluser *utilizador grupo* – comando para retirar um utilizador de um grupo de utilizadores

delgroup *grupo* – comando para eliminar grupos de utilizadores

usermod –g *grupo utilizador* – comando para alterar o grupo primário de um utilizador

id – mostra os grupos a que o utilizador pertence



chown – comando para alterar ownership de ficheiros e pastas. Exemplos:

- **chown *utilizador* pasta/ficheiro** – Altera o dono da pasta ou ficheiro para o novo utilizador
- **chown –R *utilizador* pasta** – Altera o dono da pasta e todo o seu conteúdo para o novo utilizador
- **chown *utilizador*:*grupo* pasta/ficheiro** – Altera o dono e grupo dono da pasta ou ficheiro para o novo utilizador e grupo

chgrp – comando para alterar o grupo dono de ficheiros e pastas. Exemplos:

- **chgrp *grupo* pasta/ficheiro** – Altera o grupo dono da pasta ou ficheiro para o novo grupo dono
- **chgrp –R *grupo* pasta** – Altera o grupo dono da pasta e de todo o seu conteúdo para o novo grupo dono

Octal	Tipo de Permissão	Representação Linux
0	nenhuma	-
1	execute	x
2	write	w
3	write e execute	wx
4	read	r
5	read e execute	rx
6	read e write	rw
7	read, write e execute	rwx

chmod – comando para alterar as permissões a ficheiros ou pastas. Exemplos:

- chmod 754 pasta/ficheiro – Altera as permissões da pasta ou ficheiro para as novas permissões (7 para o dono, 5 para o grupo dono e 4 para os restantes utilizadores)
- chmod –R 754 pasta - Altera as permissões da pasta e todo o seu conteúdo para as novas permissões

SSH

O que é? Ferramenta para possibilitar o acesso remoto ao servidor Linux. SSH (Secure SHell) permite que de qualquer lugar da rede, estando nós numa máquina com Linux ou Windows, consiga comunicar-se com o servidor a fim de realizar rotinas administrativas como se estivesse diante do próprio servidor.

Uma observação interessante é que para utilizar o Windows para administrar o Linux é necessário utilizar uma aplicação leve e gratuita chamada Putty, que deve ser instalada no Windows. Antigamente tínhamos o telnet, ferramenta que era utilizada para administração remota e hoje temos o SSH, que é uma ferramenta muito mais segura e eficiente.

Instalar e configurar o SSH no servidor

Para instalarmos o SSH no Debian é muito simples. Basta, estando na shell como root, escrever um dos comandos:

apt install ssh

apt install openssh-server (usado em distribuições mais antigas)

O SSH, após instalado, gera alguns arquivos de configuração e o principal deles é o /etc/ssh/sshd_config - arquivo de configuração do servidor SSH.

Primeiro passo: vamos começar editando o principal arquivo de configuração, o sshd_config encontrado em: /etc/ssh/sshd_config. Para tal, estando na shell como root, digite:

nano /etc/ssh/sshd_config

E realize as seguintes alterações dentro do arquivo:

Em **port** coloque o padrão 22 ou uma de sua escolha. Esse campo diz ao SSH que ele estará à escuta das requisições vindas de outros computadores por esta porta ficando assim: port 22

Na linha **AllowUsers**, que pode existir ou não (se não existir pode criar), serve para especificar quais utilizadores pode aceder ao servidor via SSH. Caso deseje especificar apenas um utilizador para poder dar acesso ao servidor remotamente, a linha poderá ficar assim:

AllowUsers ciber

Para além da linha AllowUsers também podemos usar a linha DenyUsers para negar o acesso a um ou vários utilizadores:

DenyUsers xpto testes

Com esta linha de código os utilizadores xpto e testes não poderão fazer login remotamente usando o serviço de SSH.

Existe ainda a possibilidade de efectuar o controlo de acessos por grupos de utilizadores, devendo para isso usar os comandos **AllowGroups** e **DenyGroups**.

NOTA: Não deve utilizar em simultâneo as linhas AllowUsers e AllowGroups. Apenas deve utilizar uma de cada vez

Por defeito o utilizador root não pode aceder ao servidor, via ssh. Para tornar isso possível deve alterar a linha **PermitRootLogin prohibit-password** para **PermitRootLogin yes**

Segundo passo: agora precisamos reiniciar o serviço para que as nossas configurações entrem em vigor. Para isso, ainda estando como root, fazemos:

systemctl restart ssh

Para obter o estado do service podemos executar o comando **systemctl status ssh**

Quando obtemos o erro, a maneira mais fácil de detector um erro é usar o comando **journalctl -xe**

Serviço de FTP

O serviço de FTP (File Transfer Protocol) é um dos protocolos mais usados para transferência de ficheiros de e para servidores. Existem diversos serviços disponíveis, mas um dos mais seguros, completos e robustos é sem dúvida o vsftpd

O pacote de software a instalar é o vsftpd (sempre após apt update). O ficheiro de configuração está em /etc/vsftpd.conf

Devemos fazer um backup do ficheiro de configuração para o caso de ser necessário repor as definições:

cp /etc/vsftpd.conf /etc/vsftpd.conf.orig

Para reiniciar o serviço o comando a usar deve ser **systemctl restart vsftpd** e para consultar o estado do serviço o comando a usar é **systemctl status vsftpd**

Pode usar directamente na linha de comandos o comando **vsftpd** para verificar se o ficheiro tem erros de configuração ou então o comando journalctl -xe.

Uma das primeiras coisas que devemos fazer no serviço é alterar a porta por defeito (a porta por defeito é a 21, devemos alterar uma à nossa escolha que esteja livre), adicionando no ficheiro de configuração:

listen_port=933

Por defeito o serviço deixa todos os utilizadores do sistema (existentes no ficheiro /etc/passwd) ligarem-se ao servidor, porém não permite upload, apenas download. Para activar essa funcionalidade devemos descomentar/adicionar a seguinte linha no ficheiro de configuração:

write_enable=YES

Quando os utilizadores se ligam ao servidor através de um cliente de ftp, conseguem navegar em todo o sistema ao qual estão aceder mas só podem listar conteúdos e nunca escrever. Existe uma forma de bloquear o acesso para que os utilizadores apenas consigam listar o conteúdo da sua própria homefolder, basta para isso descomentar/adicionar ao ficheiro de configuração as seguintes linhas:

chroot_local_user=YES

allow_writeable_chroot=YES

Podemos ainda permitir a alguns utilizadores a possibilidade de navegar em todo o sistema. Para isso temos de adicionar um ficheiro com os utilizadores a permitir e definir qual o ficheiro onde vamos colocar os utilizadores (um por linha):

chroot_list_enable=YES

chroot_list_file=/etc/vsftpd.chroot_list

VSFTPD com SSL/TLS

Por defeito o FTP é um protocolo inseguro, para o tornar seguro pode ser criado um certificado selfsigned (válido por 365 dias), com recurso aos comandos:

cd /etc/ssl/private

openssl req -x509 -nodes -newkey rsa:2048 -keyout vsftpd.pem -out vsftpd.pem -days 365

Segue um exemplo com as definições:

```
root@dbserver:~# cd /etc/ssl/private/
root@dbserver:/etc/ssl/private# openssl req -x509 -nodes -newkey rsa:2048 -keyou
t vsftpd.pem -out vsftpd.pem -days 365
Generating a 2048 bit RSA private key
.....................................................................
.....................................+++
.........+++
writing new private key to 'vsftpd.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:PT
State or Province Name (full name) [Some-State]:Porto
Locality Name (eg, city) []:Porto
Organization Name (eg, company) [Internet Widgits Pty Ltd]:PERR
Organizational Unit Name (eg, section) []:PERR Linux
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:
root@dbserver:/etc/ssl/private# _
```

De seguida devemos alterar as permissões do certificado:

(dentro da pasta /etc/ssl/private)**# chmod 600 vsftpd.pem**

Faltam apenas as configurações no ficheiro /etc/vsftpd.conf (linha 150 +-):

```
# This option specifies the location of the RSA certificate to use for SSL
# encrypted connections.
rsa_cert_file=/etc/ssl/private/vsftpd.pem
rsa_private_key_file=/etc/ssl/private/vsftpd.pem
ssl_enable=YES
ssl_ciphers=HIGH
ssl_tlsv1=YES
ssl_sslv2=NO
ssl_sslv3=NO
force_local_data_ssl=YES
force_local_logins_ssl=YES
```

Agora já podemos efectuar uma ligação segura via FTP com SSL/TLS.

Editor de texto vim

Para utilizar o editor vim na versão completa, temos de instalar o pacote de software vim:

apt install vim

Após a instalação, já podemos utilizar o editor usando o comando vi ou vim, que edita ou cria os ficheiros caso não existam.

Comandos vi:

i ou tecla Insert - permite escrever no ficheiro; tecla ESC - para sair do modo de inserção; :wq - write and quit para guardar e sair do ficheiro;

:q! - para sair do ficheiro mesmo tendo feito alterações;

:q - para sair do ficheiro sem guardar;

Quando obtemos o erro de ficheiros temporários (normalmente ficheiros swap com extensão .swp), devemos eliminar os ficheiros que começam por . e terminam em .swp (ou similares), por exemplo:

rm /etc/ssh/.sshd_config.swp ou rm /etc/ssh/.sshd_config.s*

Network Configuration

As placas de rede são identificadas pelo sistema com o nome enpXsY (Predictable network interface device names), sendo que:

- en significa ethernet
- p significa que é uma placa pci. Outros tipos de placa podem ser o (onboard) ou s (pci express) ficando a designação da placa eno ou ens, respectivamente.
- X indica o número do barramento (bus)
- Y indica a slot ocupada

Nomes de placas de rede comuns são por exemplo enp0s3 ou enp0s8 e os nomes são atribuídos conforme a identificação que a BIOS de cada computador atribui aos seus dispositivos.

Para rapidamente identificar todas as placas de rede disponíveis, usamos o comando **ip address** ou **ip addr** ou **ip a**:

```
root@dbserver:~# ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
group default qlen 1000
    link/ether 08:00:27:c7:7f:87 brd ff:ff:ff:ff:ff:ff
    inet 10.4.69.146/16 brd 10.4.255.255 scope global enp0s3
       valid_lft forever preferred_lft forever
    inet6 fd1e:2bae:c6fd:1004:a00:27ff:fec7:7f87/64 scope global mngtmpaddr dyna
mic
       valid_lft 2592000sec preferred_lft 604800sec
    inet6 fe80::a00:27ff:fec7:7f87/64 scope link
       valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
group default qlen 1000
    link/ether 08:00:27:89:b8:6b brd ff:ff:ff:ff:ff:ff
    inet 10.4.69.147/16 brd 10.4.255.255 scope global enp0s8
       valid_lft forever preferred_lft forever
```

Ou através do comando **ls /sys/class/net/**:

```
root@dbserver:~# ls /sys/class/net/
enp0s10  enp0s3  enp0s8  enp0s9  lo
root@dbserver:~# _
```

Podemos ainda usar o comando **ifconfig**, mas apenas após a instalação do package net-tools (apt install nettools):

```
root@dbserver:~# ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.4.70.110  netmask 255.255.0.0  broadcast 10.4.255.255
        inet6 fd1e:2bae:c6fd:1004:a00:27ff:fee4:8861  prefixlen 64  scopeid 0x0<
global>
        inet6 fe80::a00:27ff:fee4:8861  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:e4:88:61  txqueuelen 1000  (Ethernet)
        RX packets 10751  bytes 1509872 (1.4 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2777  bytes 219701 (214.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.4.70.112  netmask 255.255.0.0  broadcast 10.4.255.255
        inet6 fe80::a00:27ff:fe3b:79c7  prefixlen 64  scopeid 0x20<link>
        inet6 fd1e:2bae:c6fd:1004:a00:27ff:fe3b:79c7  prefixlen 64  scopeid 0x0<
global>
        ether 08:00:27:3b:79:c7  txqueuelen 1000  (Ethernet)
        RX packets 11104  bytes 1796473 (1.7 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2952  bytes 232002 (226.5 KiB)
```

IP dinâmico (DHCP)

Por defeito as placas de rede adquirem ip dinâmico, fazendo o pedido de ip aos servidores de DHCP, mas se quisermos garantir que é desse modo que as nossas placas estão a funcionar, editamos o ficheiro **/etc/network/interfaces**

O ficheiro deve ter a seguinte configuração:

```
# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug enp0s3
iface enp0s3 inet dhcp
```

Para desactivar a placa de rede usamos o comando **ifdown enp0s3**

Para activar a placa de rede usamos o comando **ifup enp0s3**

Podemos forçar ainda a nossa placa a libertar o ip actual através do comando **dhclient –r enp0s3** e fazer um novo pedido de ip aos servidores de dhcp com o comando **dhclient enp0s3**

IP Estático ou Fixo

Para configurar um ip fixo ou estático precisamos de:

- Ip para a máquina;
- Máscara de rede;
- Gateway;
- Dns

Para consultar o endereço de gateway é usado o comando ip route ou ip r

```
root@dbserver:~# ip route
default via 10.4.0.1 dev enp0s3
10.4.0.0/16 dev enp0s3 proto kernel scope link src 10.4.70.110
10.4.0.0/16 dev enp0s8 proto kernel scope link src 10.4.70.112
169.254.0.0/16 dev enp0s3 scope link metric 1000
192.168.0.0/24 dev enp0s8 proto kernel scope link src 192.168.0.3
```

Para consultar os endereços de DNS usamos comando cat /etc/resolv.conf

```
root@dbserver:~# cat /etc/resolv.conf
nameserver 62.28.40.173
nameserver 62.28.116.41
```

Fixar IP temporariamente

Para fixar ip temporariamente (até ao reboot) usamos o comando ip address ou ip addr da seguinte forma:

```
root@dbserver:~# ip address add 192.168.0.3/24 dev enp0s8
```

Precisamos ainda de configurar o default gateway:

```
root@dbserver:~# ip route add default via 192.168.27.223
```

Estas definições são voláteis, ou seja, assim que reiniciar a máquina ficamos sem estas definições. Se quisermos limpar as definições sem desligar ou reiniciar a máquina usamos o comando: **ip addr flush enp0s3**

Nota: limpando as configurações com o comando flush apenas não são eliminados os dns, precisamos de limpar os ficheiros manualmente.

Fixar IP em definitivo

Antes de configurar o ip fixo devemos instalar o programa resolvconf para ser possível indicar os dns manualmente:

apt install resolvconf

Para fixar definitivamente um ip na máquina, devemos editar o ficheiro

vi **/etc/network/interfaces**

e alterar a configuração de dhcp para static e adicionar o endereço de rede, máscara de rede, gateway, dns:

```
allow-hotplug enp0s3
iface enp0s3 inet static
address 192.168.27.249
netmask 255.255.255.0
gateway 192.168.27.222
dns-nameservers 8.8.8.8 8.8.4.4
```

Para que a placa de rede adquira o ip pretendido devem ser executados os comandos:

ifdown enp0s3 e **ifup enp0s3**

Fixar IP em definitivo numa placa adicional

Para adicionar uma placa de rede adicional ao nosso sistema em Linux, temos de adicionar uma nova placa através do VirtualBox e reiniciar a máquina. Quando a máquina arrancar devemos executar o comando ip addr para descobrir o nome que foi dado à nossa placa de rede. No caso do VirtualBox a placa terá o nome enp0s8. De seguida temos de adicionar uma nova configuração no ficheiro /etc/network/interfaces de forma a que o sistema reconheça essa placa e atribua um ip por dhcp ou estático. Para configurar um ip estático adicionamos no final do ficheiro:

```
allow-hotplug enp0s8
iface enp0s8 inet static
address 192.168.27.253
netmask 255.255.255.0
```

Compressão de ficheiros

Comando tar – Agrupar (sem comprimir)

Para agrupar ficheiros ou pastas (sem comprimir) na pasta onde estamos posicionados, usamos o comando: **tar cvf arquivo.tar arquivos.txt pastas**

A extensão de um ficheiro agrupado deve ser sempre do tipo .tar

Se quisermos podemos indicar uma outra localização onde criar o ficheiro, usando:

tar cvf /home/atec/arquivo.tar arquivos.txt pastas

Para extrair um arquivo .tar para a pasta onde estamos posicionados, usamos o comando:

tar xvf arquivo.tar

Se quisermos extrair o conteúdo do ficheiro para outra localização, acrescentamos a opção –C:

tar xvf arquivo.tar -C /home/atec/

Para acrescentar um ficheiro ou pasta a um ficheiro já agrupado usamos o comando:

tar rvf arquivo.tar outros_ficheiros_ou_pastas_a_adicionar

Comando tar – Comprimir

Apenas temos de acrescentar a opção z nos comandos, ou seja, para comprimir: **tar zcvf arquivo.tar.gz arquivos.txt pastas**

Em ficheiros comprimidos devemos usar sempre a extensão .tar.gz

Para extrair na pasta actual: tar zxvf arquivo.tar.gz

Ou para extrair para outra pasta: **tar zxvf arquivo.tar.gz –C /home/xpto/**

Seja o ficheiro agrupado ou comprimido, podemos sempre usar o comando tar tvf para listar o conteúdo:

tar tvf arquivo.tar ou tar tvf arquivo.tar.gz

Comando gzip

O comando gzip comprime ficheiros individualmente e a sua utilização é bastante simples: **gzip arquivos_a_comprimir**

Podemos indicar vários ficheiros (apenas ficheiro e não pastas) para comprimir ao mesmo tempo.

Para descomprimir devemos usar o comando gzip com o argumento –d:

gzip –d arquivos.tar.gz

O gzip por defeito transforma os ficheiros originais, para manter uma cópia dos ficheiros originais podemos usar a opção –k, ou seja: **gzip –k arquivos_a_comprimir**

Comando zip

A sintaxe é a seguinte:

zip files.zip arquivos_a_comprimir

Para descompactar usamos o comando unzip:

unzip files.zip

Para listar o conteúdo de um ficheiro "zipado" usamos a opção –sf, tal como: **zip –sf files.zip**

Para comprimir uma pasta e todo o seu conteúdo com o comando zip temos de usar a opção –r:

zip –r /home/xpto/file_destino.zip /home/

NOTA: Caso um ficheiro tenha a extensão errada, podemos usar o comando file para saber qual é o tipo de ficheiro: file files.zip

Comando Find

O comando find serve para procurar, no sistema Linux, ficheiros ou pastas baseados em condições que são colocadas nas opções dos comandos. Podem ser pocurados ficheiros ou pastas através de nomes, permissões, utilizadores, tipo de ficheiro, data, tamanho e outras.

Procurar ficheiros e pastas por nome a partir da pasta actual:

find . –name ficheiro.txt

Procurar ficheiros por nome em toda a pasta /home:

find /home –name ficheiro.txt

Procurar apenas ficheiros por nome ignorando minusculas e maiusculas:

find /home –iname ficheiro.txt

Procurar pastas por nome: **find / -type d –name Formacao**

Procurar ficheiros por nome: **find . -type f –name ficheiro.txt**

Procurar os ficheiros de uma extensão: **find / -type f –name "*.txt"**

Procurar ficheiros através de permissões: **find . -type f -perm 0777**

Procurar ficheiros por utilizador dono:

find / -user root -name "*.txt"

Procurar todos os ficheiros que pertencem a um utilizador:

find /home –user grsi

Procurar ficheiros por grupo de utilizadores: **find /home -group developer**

Procurar ficheiros modificados na última hora: **find / -mmin -60**

Procurar ficheiros por tamanho (maiores que 50 MB): **find / -size +50M**

Procurar ficheiros por tamanho (entre 50 MB e 100MB):

find / -size +50M -size -100M

Procurar ficheiros por determinada extensão mas apenas até ao 4º nível de profundidade:

find / -maxdepth 4 –iname "*.php"

Exemplos de utilização: https://tecadmin.net/delete-files-older-x-days/

Comando GREP

O grep é um comando em Linux que permite procurar palavras ou expressões dentro de um ficheiro. Desta forma, se quisermos encontrar uma palavra específica dentro de ficheiros, não precisamos de abrir o ficheiro para verificar se existe essa mesma palavra no seu conteúdo. Também podemos usar este comando para nos mostrar apenas linhas de um comando que contenham determinada palavra. O comando grep quando executado, devolve-nos a linha completa onde encontra a palavra ou expressão indicada.

Procurar a palavra grsi num ficheiro:

grep ciber /etc/passwd

Procurar apenas a palavra completa grsi num ficheiro:

grep –w ciber /etc/group

Procurar a expressão Network Management num ficheiro:

grep "Network Management" /etc/passwd

Procurar uma palavra num ficheiro ignorando minusculas e maiusculas:

grep –i root /etc/group

Procurar uma palavra em todos os ficheiros de uma pasta (pasta e subpastas):

grep –r root /etc

Procurar todas as linhas em que não exista determinada palavra:

grep –v nologin /etc/passwd

Procurar todas as linhas que começam por um caracter ou palavra:

grep ^system /etc/passwd

Procurar todas as linhas que terminam por um determinado caracter ou palavra:

grep nologin$ /etc/passwd

Comando history

Com o comando history podemos visualizar os últimos comandos inseridos na Shell do Linux pelo utilizador no qual estamos a usar o comando.

Usando um número como argumento do comando history, um número inteiro (history 50) temos acesso aos últimos 50 comandos executados pelo utilizador actual. Podemos repetir um comando utilizado anteriormente sabendo o número de execução do comando que nos é mostrado quando visualizamos o histórico. Para isso basta usar o numero de execução do comando com o simbolo ! antes:

!310

Este comando executa o comando número 310 que foi executado anteriormente.

Os comandos são gravados na homefolder de cada utilizador, no ficheiro **.bash_history** (um ficheiro escondido). Se editarmos este ficheiro, estão lá apenas os comandos executados em sessões anteriores. Sempre que um utilizador faz logoff no sistema (ou reboot, ou init 6 ou init 0), os comandos da sessão actual, são adicionados a esse ficheiro.

Crontab

Linux Crontab Format

```
MIN HOUR DOM MON DOW CMD
```

Table: Crontab Fields and Allowed Ranges (Linux Crontab Syntax)

Field	Description	Allowed Value
MIN	Minute field	0 to 59
HOUR	Hour field	0 to 23
DOM	Day of Month	1-31
MON	Month field	1-12
DOW	Day Of Week	0-6
CMD	Command	Any command to be executed.

```
*     *     *   *    *        command to be executed
-     -     -   -    -
|     |     |   |    |
|     |     |   |    +----- day of week (0 - 6) (Sunday=0)
|     |     |   +------- month (1 - 12)
|     |     +--------- day of        month (1 - 31)
|     +------------ hour (0 - 23)
+-------------- min (0 - 59)
```

O crontab é um serviço que permite que tarefas sejam executadas em modo “background” em intervalos regulares pelo deamon da cron. Estas tarefas são normalmente designadas por “cron jobs”.

crontab -e - Edita o ficheiro crontab ou cria um novo caso não exista.

crontab -l - Mostra o conteúdo do ficheiro crontab.

crontab -r - Remove o ficheiro crontab.

Para seleccionar novamente o editor de texto a utilizar, podemos usar o comando select-editor, directamente na linha de comandos.

Por defeito todos os utilizadores podem usar o crontab para executar tarefas, até ao user root criar um dos ficheiros **/etc/cron.allow** ou **/etc/cron.deny**. O user root tem sempre acesso ao crontab, não precisando sequer de ser colocado no ficheiro /etc/cron.allow caso exista.

Nestes ficheiros apenas devem constar os nomes dos utilizadores (um por cada linha) que podem aceder ao serviço de crontab (/etc/cron.allow) ou os que queremos impedir que tenham acesso (/etc/cron.deny). Apenas deve existir um ficheiro no sistema, caso existam os dois, o sistema só vai interpretar o ficheiro cron.allow, ignorando o cron.deny.

Cada utilizador que consiga executar tarefas com o crontab tem o seu próprio ficheiro com as suas tarefas (um ficheiro para cada utilizador), que o root pode consultar em **/var/spool/cron/crontabs**. Se o user root quiser eliminar todo o crontab de um determinado utilizador, pode eliminar o ficheiro com o nome do utilizador que consta naquela pasta.

Todas as operaçoes executadas ficam guardadas no ficheiro de logs da máquina (**/var/log/syslog**).

O root pode filtar apenas as linhas que dizem respeito ao crontab usando o comando **grep –i cron /var/log/syslog**

RSYNC

Rsync é um utilitário de cópia e sincronização de directórios e ficheiros, tanto no mesmo computador como em máquinas distintas. Com a ajuda do comando rsync podemos copiar e sincronizar os nossos dados remotamente e localmente entre directórios, entre discos externos ou rede.

Algumas vantagens e funcionalidades do comando RSYNC

- Copia e sincroniza ficheiros de e para sistemas remotos;
- Suporta a cópia de links, dispositivos, donos, grupos e permissões;
- É mais rápido do que o comando SCP (Secure Copy) porque o rsync usa um protocolo de update remoto que permite transferir apenas as diferenças entre os dois blocos de ficheiros (origem e destino). Na primeira vez copia todos o conteúdo de um ficheiro ou directório mas nas próximas vezes apenas copia os blocos e bytes alterados para o destino;
- O rsync consome menos largura de banda porque usa o método de compressão e descompressão enquanto envia e recebe os dados.

A sintaxe do comando é:

rsync opções origem destino

Argumentos mais usados com o rsync:

- **-v** : Verbose - Descritivo
- **-r** : copia dados recursivamente (mas não preserva data/hora e permissões)
- **-a** : archive mode - modos de arquivo permite copiar ficheiros recursivamente e também preserva links simbólicos, permissões de ficheiros, data/hora e utilizador e grupos.
- **-z** : compress file data – Comprime os dados
- **-h** : human-readable - mostra o tamanho dos ficheiros no formato facilmente reconhecido (KB,MB, GB)

Exemplos:

Copiar/sincronizar um ficheiro na mesma máquina:

rsync -zvh backup.tar /tmp/backups/

Copiar/sincronizar um directório na mesma máquina:

rsync -avzh /root/rpmpkgs /tmp/backups/

Copiar/sincronizar um directório local para uma máquina remota:

rsync -avz rpmpkgs/ root@192.168.27.101:/home/

Copiar/sincronizar um directório local numa máquina remota para uma pasta local:

rsync -avz root@192.168.27.101:/home/rpmpkgs /tmp/rpmpkgs/

Copiar/sincronizar um directório local para uma máquina remota, indicando a porta do SSH aberta:

rsync -avz -e "ssh –p901" rpmpkgs/ root@192.168.27.101:/home/

Mostrar o progresso enquanto transfere os dados:

rsync -avzhe "ssh –p901" --progress /home/rpmpkgs root@192.168.0.100:/root/rpmpkgs

Usar as opções de –include e –exclude para incluir ou excluir ficheiros ou pastas(neste exemplo só são copiados ficheiros ou pastas que começam por R):

rsync -avze ssh --include 'R*' --exclude '*' /mnt/teste/ root@192.168.0.101:/var/lib/rpm/

Mais exemplos em : http://www.tecmint.com/rsync-local-remote-file-synchronization-commands/

Login SSH sem password – p crontab

Necessário para adicionar comandos no crontab em que haja ligações por ssh.

Problema: efectuar login por ssh do servidor ub_server (user pedro) para o servidor ub_client(user root) Passos necessários:

pedro@ub_server ~ $ ssh-keygen –t rsa

Após inserir este comando deixe a password em branco e não é necessário especificar o ficheiro. pedro@ub_server ~ $ ssh-copy-id -i .ssh/id_rsa.pub root@192.168.28.XXX

Para testar:

pedro@ub_server ~ $ssh root@192.168.28.XXX Deverá aceder por SSH sem precisar de inserir password.

Instalação de um servidor DHCP

A instalação de um servidor DHCP em Debian Server é relativamente simples, resumindo-se à instalação do pacote de software e posterior edição dos parâmetros do servidor por edição de um ficheiro de configuração. Todos os passos são realizados na linha de comandos e devem ser realizados como root.

Vamos primeiro instalar o servidor:

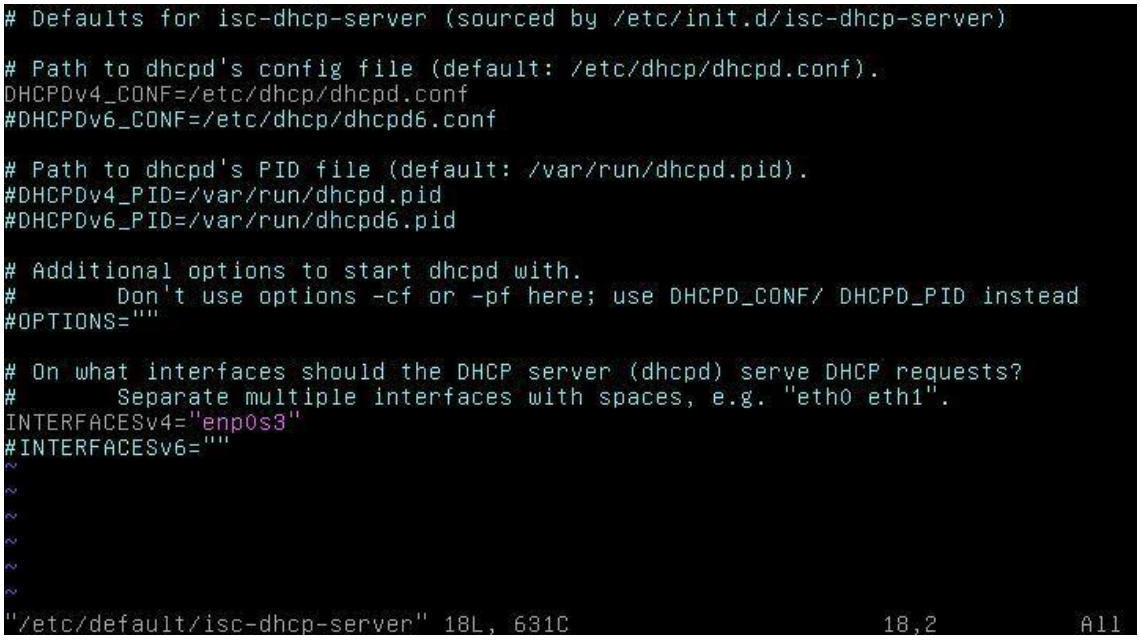
apt-get install isc-dhcp-server

Este pacote de software coloca os ficheiros de configuração do serviço de dhcp na pasta /etc/dhcp/

Antes de iniciar as configurações do serviço de dhcp, precisamos de indicar qual a rede à qual fazemos parte vamos partilhar ip's.

Para isso temos de indicar qual a placa de rede cuja rede vamos partilhar e qual a localização do ficheiro de configuração, acedendo ao ficheiro **/etc/default/isc-dhcp-server**

Neste ficheiro devemos descomentar a linha de configuração correspondente ao ipv4 ou ipv6 (por defeito usamos o ipv4, na linha 4). Devemos também indicar qual a placa de rede do nosso servidor que vamos usar para configurar o serviço de DHCP. Por defeito vamos usar o ipv4 também e a placa enp0s3 (linha 17). Se não necessitarmos de usar o ipv6 devemos comentar a linha correspondente (linha 18). Exemplo:



De seguida vamos efectuar as configurações no ficheiro de configuração indicado anteriormente, **/etc/dhcp/dhcpd.conf**, por isso vamos primeiro efectuar um backup de segurança do ficheiro para depois partirmos de um novo:

– mv /etc/dhcp/dhcpd.conf /etc/dhcp/dhcpd.conf.old

– vi /etc/dhcp/dhcpd.conf

O ficheiro original já possuía várias configurações de exemplo, mas vamos começar com um ficheiro vazio onde vamos criar uma pequena sub-rede, e dentro dessa rede definir uma máquina com IP atribuído dinamicamente. Para isso preenchemos o ficheiro da seguinte forma:

Começamos pela definição da rede que queremos configurar:

subnet 10.4.0.0 netmask 255.255.0.0 {

– Não nos podemos esquecer de abrir chavetas no final da linha, e que irão ser fechadas mais à frente.

– A seguir indica-se qual a gama de endereços dentro desta rede, que irão ser atribuídos por DHCP:

range 10.4.100.100 10.4.100.200;

– Adicionamos alguns parâmetros, como o servidor DNS e o nome de domínio:

option domain-name-servers 8.8.8.8, 8.8.4.4;

option domain-name "linux.dhcp";

– E, de seguida alguns parâmetros específicos da rede, como o gateway **option routers 10.4.0.1**;

Podemos também definir os limites de tempo de reserva do ip através dos comandos default-lease-time e max-lease-time (tempo definido em segundos)

default-lease-time 86400: max-lease-time 172800;

}

– Tudo junto, ficamos com a seguinte configuração:

```
subnet 10.4.0.0 netmask 255.255.0.0
{
        range 10.4.100.100 10.4.100.200;
        option domain-name-servers 8.8.8.8, 8.8.4.4;
        option domain-name "linux.dhcp";
        option routers 10.4.0.1;
        default-lease-time 86400;
        max-lease-time 172800;
}
```

Resta iniciar o servidor DHCP, com o seguinte comando:

systemctl restart isc-dhcp-server e systemctl status isc-dhcp-server para reiniciar e verificar o estado do serviço respectivamente.

A partir deste momento passamos a ter um servidor DHCP funcional. Caso o servidor não arranque, há dois motivos mais frequentes para isso acontecer.

1. Em primeiro lugar, a configuração do ficheiro dhcpd.conf pode ter erros e nesse caso o próprio serviço ao tentar iniciar, devolve mensagens de erro indicando as linhas onde a configuração está errada. Um erro comum é a falta de um ; no final de cada linha.

2. Outro problema que pode surgir, é estarmos a configurar o serviço DHCP para operar numa rede, quando o servidor onde ele está instalado não possui um endereço válido dentro dessa mesma rede. É fundamental que o servidor possua um endereço IP válido (e definido manualmente, já que será ele a atribuir os endereços aos restantes) em cada uma das subredes definidas no ficheiro dhcpd.conf.

Se der erro ao reiniciar o serviço devemos usar o comando **journalctl –xe** de forma a facilitar a detecção de erros.

Agora vamos poder testar com vários sistemas operativos:

- Debian Server;

• Debian Desktop usando o ambiente gráfico ou a linha de comandos; • Windows usando o comando ipconfig.

No Linux conseguimos ver o IP usando o comando **ip addr**;

Para saber o nosso gateway devemos usar o comando **ip route**;

Para ver os nossos DNS usamos o comando **cat /etc/resolv.conf**

Fixar IP's através do MAC Address

Para que um determinado computador receba sempre o mesmo ip baseado no Mac Address so temos que adicionar umas linhas no final do ficheiro **dhcpd.conf**:

Neste caso, iniciamos a declaração desta forma:

host webserver {

– Isto indica que vamos iniciar a configuração de um único host dentro da rede.

Mais uma vez abrimos chavetas, e será dentro desse espaço que irá ser efectuada a definição dos parâmetros. Nunca podemos esquecer de fechar as chavetas no final.

– Vamos agora especificar os dois endereços da máquina, ou seja, o endereço físico que a máquina possui, e o lógico que irá receber:

hardware ethernet 08:00:27:89:A2:D8;

fixed-address 10.4.100.30;

– Como anteriormente, terminamos com o fecho das chavetas:

}

Tudo junto fica da seguinte forma:

```
host webserver
{
        hardware ethernet 08:00:27:89:A2:D8;
        fixed-address 10.4.100.30;
}
```

Resta reiniciar o serviço de DHCP e testar para verificar que a atribuição de IP baseada no endereço físico (Mac Address) funciona.

systemctl restart isc-dhcp-server

LOGS do serviço DHCP

cat /var/lib/dhcp/dhcpd.leases

DHCP client lease database. É neste arquivo onde se monitora, em tempo real, o que o DHCP

Server está a fazer em relação a entrega dos IPs

cat /var/lib/dhcp/dhcpd.leases~

backup dos dados mais antigos do "/var/lib/dhcp/dhcpd.leases"

Todos os logs estão guardados em **/var/log/syslog**

Para filtrar apenas os logs relativos ao dhcp deve ser usado o comando:

grep dhcp /var/log/syslog

Para visualizar apenas os últimos 20 logs do dhcp deve usar o comando:

grep dhcp /var/log/syslog | tail -20

LOCAL Network

De forma a permitir a ligação à internet de uma rede local, precisamos de ter um servidor de DHCP a funcionar e precisamos de configurar o servidor Linux para reencaminhar todo o tráfego desconhecido para a placa que tem ligação à internet (normalmente enp0s3) através das ip tables:

1. Use um Linux com duas interfaces de rede:

   a. a primeira placa configurada com ip válido da rede da sala de formação (fixo ou dinâmico) e com acesso à internet (**bridge adapter**).

   b. a segunda por ip estático com uma rede doméstica (**internal network**). Para essa rede use uma gama de ip's completamente diferente da rede principal, como por exemplo:

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug enp0s3
iface enp0s3 inet static
address 10.4.88.198
netmask 255.255.255.0
gateway 10.4.0.1
dns-nameservers 8.8.8.8 8.8.4.4


# The secondary network interface
allow-hotplug enp0s8
iface enp0s8 inet static
address 192.168.0.1
netmask 255.255.255.0
~
"/etc/network/interfaces" 23L, 534C                           16,31         All
```

2. Configure um servidor DHCP para partilhar a rede da 2ªplaca com outras máquinas:

```
subnet 192.168.0.0 netmask 255.255.255.0
{
        range dynamic-bootp 192.168.0.100 192.168.0.200;
        option domain-name-servers 8.8.8.8, 8.8.4.4;
        option domain-name "linux.dhcp";
        option routers 192.168.0.1;
}
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"/etc/dhcp/dhcpd.conf" 7L, 204C                               7,1           All
```

3. Use outra máquina virtual em Linux ou Windows para receber um ip da gama que indicou anteriormente.

4. Use os comandos que achar necessários para ter a certeza que fica com um ip do seu servidor DHCP.

5. Para que consiga aceder à internet no seu cliente dhcp tem de efectuar as seguintes configurações no servidor DHCP:

a. Editar o ficheiro **/etc/sysctl.conf** e retirar o # do início da linha "net.ipv4.ip_forward=1" para o Linux ser capaz de encaminhar pacotes de uma placa para outra. Deve **reiniciar** o servidor para que as alterações sejam assumidas.

b. Instalar o pacote das iptables com o comando **apt install iptables**

c. Executar o comando: **iptables --table nat --append POSTROUTING --out-interface enp0s3 -j MASQUERADE**

6. Agora já deverá conseguir aceder à internet através da máquina cujo ip não pertence à rede principal.

7. Um dos problemas é que os comandos inseridos na alínea **5b** são eliminados assim que reiniciar a máquina, por isso devemos criar um script e colocá-lo no nosso servidor de forma a ser executado sempre que a máquina é reiniciada:

a. Criar um ficheiro em /root com o nome "script.sh" e escrever o seguinte:

b. Devemos dar a permissão de execução ao ficheiro (chmod +x /root/script.sh) Para verificarmos se o script executa sem problemas podemos testar escrevendo directamente na linha de comandos: /root/script.sh

Se não der erros, quer dizer que o script está livre de erros e com permissões de execução.

c. Criar o ficheiro /etc/rc.local e colocar o nome do script de forma a ser executado sempre que o sistema arranca, e dar permissão de execução ao ficheiro (chmod +x /etc/rc.local). Devemos testar o script para verificar se executa: /etc/rc.local

Verifique se depois de reiniciar o seu servidor, consegue aceder à internet com o seu sistema cujo ip não pertence à rede oficial da sua sala de formação.

Samba SEM Autenticação

Para instalar o samba deve ser usado o comando:

apt install samba

O ficheiro de configuração do samba é **/etc/samba/smb.conf**

NOTA: sempre que alterar este ficheiro deve reiniciar os serviços do samba:

systemctl restart smbd

Antes de fazer alguma alteração ao ficheiro smb.conf, deve fazer um backup desse ficheiro.

Edite o ficheiro smb.conf e verifique a sua estrutura.

O ficheiro smb.conf está dividido em diversas secções:

Global Settings

Debugging/Accounting

Authentication

Printing

File sharing

Misc

Share Definitions

As definições do smb.conf podem ser consultadas em pormenor em http://www.samba.org/samba/docs/using_samba/ch06.html

As pastas a partilhar devem ser configuradas na parte final do ficheiro em Share Definitions:

no final do ficheiro deve adicionar as seguintes linhas:

[shared_folder] comment = partilha de ficheiros em Debian

path = /srv/samba/share

browsable = yes

guest ok = yes

read only = no

Tente explicar o significado de cada uma das linhas acima adicionadas ao ficheiro.

Crie a estrutura de directórios /srv/samba/share e depois devemos atribuir permissões totais à pasta com o comando chmod:

Chmod –R 777 /srv/samba/share/

Reinicie os serviços do samba (smbd). systemctl restart smbd

Através do windows tente aceder a esta pasta partilhada através da vizinhança de rede.

Consegue vizualizar a pasta? Crie um ficheiro dentro da pasta através do windows e feche a janela. Altere o ficheiro smb.conf: altere a linha browsable = yes para browsable = no

Reinicie o serviço do samba.

Tente aceder novamente ao sistema através da vizinhança de rede. O que verifica?

Na barra de procura de Windows escreva \\ip_pc_destino\shared_folder

Altere novamente o ficheiro smb.conf: altere a linha browsable = no para browsable = yes e reinicie os serviços de samba.

Verifique os resultados.

Crie uma nova pasta em /srv/samba/nova_pasta onde todos os utilizadores podem ver o conteúdo da pasta, mas apenas podem ler a informação contida na pasta.

Verifique se consegue aceder a essa pasta através do Windows.

Samba COM autenticação

Adicione as seguintes linhas no final do ficheiro:

[private]

comment = partilha de ficheiros com acesso autenticado

path = /srv/samba/docs_privados

browsable = yes

guest ok = no

read only = no

Podemos definir as permissões para os ficheiros e pastas que forem criados através do samba com os comando create mask (permissões de ficheiros) e directory mask (permissões de pastas):

create mask = 0750

directory mask = 0770

Também podemos definir que todos os ficheiros e pastas que sejam criados através das partilhas herdem as permissões da pasta superior. As pastas criadas ficam exatamente com as permissões da pasta superior, os ficheiros herdam apenas as permissões de leitura e escrita:

inherit permissions = yes

O comando inherit permissions sobrepoe-se ao create mask e directory mask.

Para aceder temos de adicionar utilizadores ao samba. O comando a usar é o smbpasswd:

- smbpasswd –a "utilizador" --adiciona um utilizador
- smbpasswd –d "utilizador" --desabilita um utilizador
- smbpasswd –e "utilizador" --habilita um utilizador
- smbpasswd –x "utilizador" --remove um utilizador

Adicione um utilizador e tente fazer aceder novamente à partilha.

Para verificar os utilizadores samba existentes no sistema deverá usar o comando

pdbedit –L

Algumas linhas que poderão ser usadas no ficheiro smb.conf #linha para dar acesso de leitura ao grupo editores

read list = @editores

#linha para dar acesso de escrita ao grupo editores e ao utilizador alex

write list = @editores,alex

#linha para dar acesso à partilha ao grupo pvsw # only members of group pvsw will have access

valid users = @pvsw

#linha para dar negar o acesso à partilha a utilizador xpto

invalid users = xpto

Option	Parameters	Function
admin users	string (list of usernames)	Specifies a list of users who can perform operations as root.
valid users	string (list of usernames)	Specifies a list of users that can connect to a share.
invalid users	string (list of usernames)	Specifies a list of users that will be denied access to a share.
read list	string (list of usernames)	Specifies a list of users that have read-only access to a writable share.
write list	string (list of usernames)	Specifies a list of users that have read-write access to a read-only share.
max connections	numerical	Indicates the maximum number of connections for a share at a given time.
guest only (only guest)	boolean	Specifies that this share allows only guest access.
guest account	string (name of account)	Names the Unix account that will be used for guest access.

Por defeito a homefolder do utilizador que utilizamos para aceder às partilhas é disponibilizada automaticamente. A pasta é partilhada com o mesmo nome do utilizador. Para cancelar a partilha temos de comentar a partilha no ficheiro configuração:

```
#======================= Share Definitions =======================

[homes]
   comment = Home Directories
   browseable = no

# By default, the home directories are exported read-only. Change the
# next parameter to 'no' if you want to be able to write to them.
   read only = yes

# File creation mask is set to 0700 for security reasons. If you want to
# create files with group=rw permissions, set next parameter to 0775.
   create mask = 0700

# Directory creation mask is set to 0700 for security reasons. If you want to
# create dirs. with group=rw permissions, set next parameter to 0775.
   directory mask = 0700

# By default, \\server\username shares can be connected to by anyone
# with access to the samba server.
# The following parameter makes sure that only "username" can connect
# to \\server\username
# This might need tweaking when using external authentication schemes
   valid users = %S
```

Podemos também utilizar os comandos hosts allow e hosts deny para permitir ou restringir o acesso às partilhas.

Ex: hosts allow = 192.168.2.0/24 192.168.3.0/24 ou hosts deny = 10.0.0.0/24

Se houver erros no ficheiro de configuração, podemos verificar os erros com o comando testparm:

```
root@debian:~# testparm
Load smb config files from /etc/samba/smb.conf
set_variable_helper(ys): value is not boolean!
Error loading services.
```

Limpar Cache Windows 7 / 8

Na linha de comandos (cmd):

- Para limpar a cache do Windows deve usar o comando net use * /DELETE
- klist purge

Limpar Cache Windows 10

Na linha de comandos (cmd):

- klist purge