Aceder por SSH ao servidor:
ssh <IP_DO_SERVIDOR> -l <USERNAME>

NANO:
CTRL + SHIFT + A – selecciona texto
ALT + 6 - Copia texto
CTRL + U – Cola texto
CTRL + G - Documentação

| [encadeia comandos]

&& [Executa comandos sequencialmente]

> [envia output para um ficheiro, apagando o conteudo do mesmo]

>> [faz append do output para o ficheiro]

touch [FILENAME] [“toca” um ficheiro já existente, ou cria-o caso não exista]

cat [FILENAME] [mostra todo o conteudo de um ficheiro]

less [FILENAME] [mostra por ecrans o conteudo de um ficheiro]

/etc/rc.local [scripts que são corridos ao iniciar o sistema]
/etc/init.d/ [local onde estão os serviços do sistema]

chkconfig –list [NOME DE SERVIÇO] [Lista os serviços e os níveis de permissão]

yum install [NOME DO SERVIÇO] [Instala um serviço em falta]

service [NOME DO SERVIÇO] restart [Reinicia um serviço]
etc/init.d/[NOME DO SERVIÇO] restart

service [NOME DO SERVIÇO] start [Inicia um serviço]
etc/init.d/[NOME DO SERVIÇO] start

service [NOME DO SERVIÇO] stop [Pára um serviço]
etc/init.d/[NOME DO SERVIÇO] stop

/etc/passwd [Ficheiro que contêm a lista de users do sistema]
useradd [NOME DE UTILIZADOR] [Adicona utilizador ao sistema e cria a pasta home]
passwd [NOME DE UTILIZADOR] [Adiciona ou alteria a password do utilizador]

chage -E [DIA/MÊS/ANO] [USER] [Marca a data de expiração da password do user]
chage –list [USER] [Verifica as informações da conta do user]

/etc/groups [Ficheiro que contêm os grupos e os seus membros]

etc/gshadow [Ficheiro que contêm a informação de segurança do grupos e os administradores]

groupadd [NOME DO GRUPO] [Cria um novo grupo de utilizadores]
gpasswd -a [USER] [GROUP] [Adiciona um utilizador a uma grupo]
gpasswd -M [USER1], [USER2] [GROUP] [Adiciona n users a uma grupo]
gpasswd -A [USER] [GROUP] [Define o user como administrador do grupo]

chgrp [GROUP] [DIRECTORY] [Atribui a um grupo a posse de uma pasta]

ls -la [Mostra a listagem extendida do conteudo da directoria]

- (rootfile) d (directory) l (link)	Owner permissions	Group permissions	Others permissions	Nº de links ou directories	User that owns the file	Group that owns the file	Tamanho em bytes	Data da ultima modificação	Nome
-	rw-	r--	r--	1	root	root	763	Mar 30 12:59	Teste.txt
d	rwx	rwx	r--	2	user1	test_user	4096	Mar 30 19:45	test_files

Permissões:

#	**Permissão**	**rwx**	**Binário**
7	leitura, escrita e execução	rwx	111
6	leitura e escrita	rw-	110
5	leitura e execução	r-x	101
4	apenas leitura	r--	100
3	escrita e execução	-wx	011
2	apenas escrita	-w-	010
1	apenas execução	--x	001
0	nenhum	---	000

chmod -c ### [FILENAME] [Muda as permissões de um ficheiro]
chmod -cR ### [FILENAME] [Muda as permissões da directoria e os ficheiros no seu interior]

chmod [u ou g ou o] [+ ou – ou =] [rwx, s para sticky bit] [FILENAME]

crontab -u [USER] -e [SET_UP] [COMANDO A EXECUTAR]
CADA USER POSSUI O SEU PRÓPRIO CRONTAB

minutos	horas	dia do mês	mês	dia da semana
mm	hh	dd	MM	ss
0-59	0-23	1-31	1-12	0-7 (domingo a domingo)

Todo dia de hora em hora (hora cheia)

00 * * * * /bin/script

De cinco em cinco minutos todos os dias (note a divisão por 5 do intervalo 00-59)

00-59/5 * * * * /bin/script

Nas seguintes horas: 10, 12, 16, 18, 22 aos 15 minutos dhora

15 10,12,16,18,22 * * * /bin/script

Nos primeiros cinco dias do mês às 19:25

25 19 01-05 * * /bin/script

De segunda a sexta ao meio-dia e a meia-noite

00 00,12 * * 1-5 /bin/script

Script rodar Segunda,Quarta,Sexta às 2 horas

0 2 * * mon,wed,fri /bin/script

Script para rodar Terça,Quinta às 3 horas

0 3 * * tue,thu /bin/script

Script para ser executado minuto a minuto

*/1 * * * * /bin/script

/ect/sysconfig/network-scripts/ifcfg-eth0 [contêm as configurações da placa de rede]
/etc/resolv.conf [contem os servidores de DNS]

Adicionar uma segunda placa de rede:
Criá-la no VirtualBox, a placa deve ficar em NAT?
Entrar no SETUP e ir a network configurations, device configuration e selecionar <NEW DEVICE>
Name: eth1
Device: eh1
use DHCP: [*]
TODOS OS IP'S FICAM EM BRANCO
Peer DNS: [*]
On boot: [*]
Controlled by NetworkManager: [*]

Sair
ip link show (para ter a certeza que foi criada e que está down)
ifup eth1 (para a ligar)

Configurar o DHCP:

Colocar ambas as máquinas em NAT

No servidor	yum install `setuptool` yum install system-config-network-tui

	yum install dhcp
No cliente	yum install `setuptool` yum install system-config-network-tui

Passar ambas as máquinas para uma rede interna

No server editar o ficheiro **/etc/dhcp/dhcp.conf** (ATENÇÃO AOS ESPAÇOS E CARACTERES)

```
Subnet 192.168.0.0 netmask 255.255.255.0 {

#Gama de endereços atribuídos dinânicamente pelo servidor de DHCP
range 192.168.0.100 192.168.0.200;

#Tempo em segundos que um IP fica atribuído a um dado cliente
default-lease-time 86400;
max-lease-time 86400;

#Indicar a Gateway a ser utilizada pelos clientes
option routers 192.168.0.254;

#Indica o endereço de broadcast e a mascara da sub-rede a ser utilizada pelos clientes
option broadcast-address 192.168.0.255;
option subnet-mask 255.255.255.0;

#Indica a lista de servidores DNS a serem utilizados pelos clientes;
option domain-name-servers 192.168.0.10,192.168.0.11;

#Indica o servidor de WINS utilizado pelos clientes
option netbios-name-servers 192.168.0.12;

#Indica, aos clientes, qual o sufixo DNS a ser utilizado
option domain-name “estig.pt";

“ Atribui um IP especifico a um cliente (as partir do endereço MAC)
host serverAS
{
hardware ethernet 00:00:27:5B:23:F6;      # As letras do MAC Address devem ser MAISCULAS
fixed-address 192.168.0.111;                #este IP não deve estar no range definido acima
}

}
```

Passar o servido para um IP for a do range definido , por exemplo 192.168.0.1

Reiniciar a interface de rede:
chkconfig dhcpd on

/etc/inti.d/network restart

Usar o seguinte comando para verifica se há erros:
/usr/sbin/dhcpd -f

iniciar o serviço DHCP deamon:
/etc/init.d/dhcpd start

No cliente:

reiniciar o interface de rede:
/etc/init.d/network restart [DEMORA A APANHAR IP]
cat /etc/resolv.conf [MOSTRA OS IP DOS DNS's]

Confirmar os IP com ifconfig
pingar entre eles

Desligar as firewalls do linux em ambas as máquinas:
chkconfig iptables off
/etc/init.d/iptables stop

nano /etc/selinux/config
passar SELINUX=enforcing para SELINUX=disabled

Configurar o NFS:

Ambas as máquinas	yum install nfs-utils chkconfig nfs on /etc/init.d/nfs start

no servidor:
definir as directórias que vão ser partilhadas:
nano /etc/exports
exemplo, atenção que as opções estão "coladas" à especificação da rede:
/home/test_users 192.168.0.0/24(ro, nohide,sync)
/home/user1 192.168.0.0/24(rw,hide,async)

Mudar as pastas para permissões totais:
chmod -R 777 /home/test_users
chmod -R 777 /home/user1

reiniciar o serviço nfs:
chkconfig –levels 23 ntf on
/etc/init.d/nfs restart

no cliente, montar as directorias:
mkdir /home/dump
mount -t nfs 192.168.0.1:/home/user1 /home/dump

mkdir /home/user1
mount -t nfs 192.168.0.1:/home/user1 /home/user1

para ver os mountpoints:
df -h

Para tornar automático:
nano /etc/fstab

adicionar:

192.168.0.1:/home/test_users	/*home/*dump	nfs	ro,nohide,sync	0 0
192.168.0.1:/home/user1	/home/user1	nfs	rw,hide,async	0 0

ATENÇÃO:
Usar o ntsysv para garantir que dhcpd, dhcpd6, ntfs
O mount dos sistemas de ficheiros nfs demora muitos minutos a realizar

Configurar NIS:

No servidor	yum install ypserv ntsysv inciar yupserv e yppasswdd */etc/*init.d/ypserv start /etc/init.d/yppasswdd start
No cliente	yum install ypbind chkconfig ypbind on

No servidor:
touch /etc/gshadow
touch /etc/netgroup
nisdomainname estig.pt **[O serviço só funciona se houver um domainname]**

Ir para directoria /var/yp e fazer make [**DEVE SER FEITO CADA VEZ QUE SE ADICIONA UM UTILIZADOR]**

Reiniciar os serviços do yellow pages:
/etc/init.d/ypserv restart
/etc/init.d/yppasswdd restart [**PODE SER NECESSÀRIO REINICIAR MAIS QUE UMA VEZ**]

No cliente:
verificar as comunicações com o server
Setup – Authentication – Use NIS

domain: estig.pt
server: 192.168.0.1

/etc/init.d/ypbind start

PARA QUE OS USER ENTREM PARA A SUA DIRECTORIA /HOME DEVEMOS ADICIONAR A:

nano /etc/exports

A LINHA:

/home 192.168.0.0/24(rw,hide,sync)

REINICIAR O NFS
NO CLIENTE:
mount -t nfs 192.168.0.1:/home /home

AS DIRECTORIAS DOS USERS DEVER ESTAR EM 777

chmod -R 777 /home

Configurar Quotas:

no servidor:
yum install quota
yum install quota-devel

Editar o ficheiro fstab do SERVIDOR

nano /etc/fstab

e no filesystem onde se pretende activar as quotas adicionar:

defaults**,grpquota,usrquota**

de seguida correr os comandos
mount -o -remount [NOME_DO_FILESYSTEM]

#quotacheck -cugm [NOME_DO_FILESYSTEM]

não devem retornar output

Usar o comando para ligar as quotas
quotaon [NOME_DO_FILESYSTEM]

Atribuir quotas a um utilizador:
edquota -u [USERNAME]

Preencher os campos soft com o valor de aviso e o hard com o valor limite

Pode criar dummy fiules com o comando:
fallocate -l [TAMANHO_K/M/G] [FILENAME]

Configurar server Ftp:

yum install vsftpd

chkconfig vsftpd on
/etc/init.d/vsftpd start

nano /etc/vsftpd/vsftpd.conf
Máscara = 777-[PERMISSÃO_DESEJADA]

ex:
para ter 751 - 777-751=026
para ter 550 – 777-551= 0226
ATENÇÃO - A LOCAL_UMASK TEM COMEÇAR SEMPRE COM UM 0

# Código para enjaular os utilizadores do FTP
chroot_local_user=YES
chroot_list_enable=YES
# (default follow)
# chroot_list_file=/etc/vsftpd/chroot_list
chroot_list_file=/etc/vsftpd/ftp_list

No ficheiro ftp_list devem constar em cada linha os utilizadores que **não** queremos que sejam enjaulados

Configurar o serviço DNS (bind):

/etc/hosts – tabela com ip's e nomes. Primórdios antes do serviço DNS
/etc/resolv.conf – guarda os ip's dos servidores de DNS
/etc/nsswitch.conf - Ficheiro que diz qual a ordem de procura entre ficheiro hosts e DNS

Tipo	Significado	Conteúdo
A	IPv4 host	Endereço IP de 32-bit
AAAA	IPv6 host	Endereço IP de 64-bit
CNAME	Canonical Name	Nome canónico para um alias
MX	Mail Exchanger	Host que actua como mail exchanger do domínio
NS	Name Server	Nome do server autorizador do

		domínio
PTR	Pointer	Nome do Dominio (um tipo de link simbólico)
SOA	Start of Authority	

yum install bind* (instala todos os pacotes relacionados com o bind)

O serviço chama-se named
chkconfig named on
/etc/init.d/named start

nano /etc/named.conf

Para este exemplo vamos usar:
Domain name – as.com
IP – 10.2.0.0/24

Adicionar as zonas master

```
ATENÇÃO:
options {
        listen-on port 53 {127.0.0.1; any;}; ADICIONAR ANY NESTA LINHA
…
        allow-query {localhost; any;}; ADICIONAR ANY NESTA LINHA
...

zone “as.com” IN {
        type master;
        file “/var/named/as.com.hosts”;
};
Zone “0.2.10.in-addr.arpa” IN {
        type master;
        file “/var/named/0.2.10.in-addr.arpa.hosts”;
};
```

Para saber nome do nosso servidor de DNS:
hostname

Criar as zonas forward
nano /var/named/as.com.hosts

```
$ttl 38400 ; time to live em segundos, pode ser 24h ou 1d
@       IN      SOA    dns.estig.pt. mail.as.com. (  # ESTE ENDEREÇO ESTÀ NO SETUP
```

```
                        1165190726 ;serial do dominio
                        10800 ;refresh em segundos
                        3600; retry em segundos
                        604800 ;expire em segundos
                        38400; minimum de propagação do DNS
                        )
        IN      NS      dns.estig.pt. ;
www     IN      A       10.2.0.1
ftp     IN      A       10.2.0.2
abc     IN      CNAME   www.google.com. #O ENDEREÇO abc.as.com VAI APONTAR google
        MX      10      mail.outrodominio.com. # este é o servido que recebe o mail
        MX      20      mail2.outrodominio.com.
```

ATENÇÃO:
dns.estig.pt. Corresponde ao nome do nosso DNS
mail.as.com. Corresponde ao mail de contacto do dominio, é usado para notificações

nano /var/named/0.2.10.in-addr.arpa.hosts

```
$ttl 38400 ; time to live em segundos, pode ser 24h ou 1d
@       IN      SOA     dns.estig.pt. mail.as.com. (  # ESTE ENDEREÇO ESTÀ NO SETUP
                        1165192116 ;serial
                        10800 ;refresh
                        3600; retry
                        604800 ;expire
                        38400; minimum
                        )
        IN      NS      dns.estig.pt.
1       IN      PTR     www.as.com.
2       IN      PTR     ftp.as.com.
```

Para atribuir o nosso servidor DNS ao cliente

yum install bind-utils
yum install jwhois

nano /etc/resolv.conf

e adicionar a linha em primeiro lugar:
nameserver <IP_DO_SERVIDOR>

Configurar o serviço HTTP (servidor web):

yum install httpd
chkconfig httpd on
/etc/init.d/httpd start

Ficheiro principal de configuração do serviço:
nano /etc/httpd/conf/httpd.conf

O DocumentRoot pré-definido é:
“ cd /var/www/html ; está definido no httpd.conf

Ficheiros de configaração de módulos específicos:
nano /etc/httpd/conf.d/<NOME_MODULO>.conf

Ver as directivas de configuração do servidor Apache na documentação do ficheiro httpd.conf, em especial:
- listen <PORT> – define o porto em que o servidor recebe os comendos HTTP
- listen <IP:PORT> - define o IP e o porto em que o servidor recebe os comendos HTTP
- user – define o user que corre o serviço HTTPD
- group – define o grupo que corre o serviço HTTPD
- DocumentRoot “<PATH>” - define a raiz das pastas públicas
- DirectoryIndex <FILENAME> - define qual o ficheiro html que é devolvido ao carregar o URL
- userDir <DIRECTORY_NAME> - directória da página dos utilizadores
- AddDefaultCharset ISO-8859-1 – para que os acentos e caracteres especiais (ç) sejam reconhecidos

Cada directória pode ter um ficheiro de regras (.htaccess) local, para não haver falhas de segurança vamos

nano /etc/httpd/conf/httpd.conf

```
#
# The following lines prevent .htaccess and .htpasswd files from being
# viewed by Web clients.
#
<Files ~ "^\.ht">
    Order allow,deny
    Deny from all
    Satisfy All APAGAMOS ESTA LINHA??
</Files>
```

Definir utilizadores e password para o servidor http:
htpasswd -c .filepasswd <USERNAME_1> ; com -c criamos o ficheiro novo
htpasswd .filepasswd <USERNAME_2> ; para adicionar um novo utilizador

Autenticação através de Apache para directórias:
nano /etc/httpd/conf/httpd.conf

```
#
# First, we configure the "default" to be a very restrictive set of
# features.
#
```

```
<Directory />
    Options FollowSymLinks
    AllowOverride None ; alterar de None para AuthConfig
</Directory>

(…)

#
# AllowOverride controls what directives may be placed in .htaccess files.
# It can be "All", "None", or any combination of the keywords:
#   Options FileInfo AuthConfig Limit
#
    AllowOverride None ; alterar de None para AuthConfig
```

Em cada uma das directórias a que o servidor apache tem acesso criar um ficheiro .htaccess

nano .htaccess

```
AuthName "Diretorio Privado – Nome Utilizador"
AuthType Basic
AuthUserFile /home/user/.user_passwd ;caminho até ao ficheiro que contêm os users do apache
require valid-user
```

Criar espaços pessoais:

cd /etc/skel/ ; cria um esqueleto de directórios

A estrutura de directórios criado aqui dentro será replicado no directório HOME que será criado para cada utilizador novo.

Para permitir que os utilizadores do

nano /etc/httpd/conf/httpd.conf

```
#
# See also: http://httpd.apache.org/docs/misc/FAQ.html#forbidden
#
<IfModule mod_userdir.c>
    #
    # UserDir is disabled by default since it can confirm the presence
    # of a username on the system (depending on home directory
    # permissions).
    #
    # UserDir disabled ; Comentamos esta linha
```

```
    #
    # To enable requests to /~user/ to serve the user's public_html
    # directory, remove the "UserDir disabled" line above, and uncomment
    # the following line instead:
    #
     UserDir public_html ; Descomentamos esta linha, ESTA DIRECTÓRIA DEVE SER ALTERADA PARA O QUE FOR PEDIDO

</IfModule>
#
# Control access to UserDir directories.  The following is an example
# for a site where these directories are restricted to read-only.
#
<Directory  /home/*/public_html> ; Descomentar daqui para baixo, DEVE SER IGUAL AO QUE ESTÁ EMCIMA
    AllowOverride FileInfo AuthConfig Limit
    Options MultiViews Indexes SymLinksIfOwnerMatch IncludesNoExec
    <Limit GET POST OPTIONS>
        Order allow,deny
        Allow from all
    </Limit>
    <LimitExcept GET POST OPTIONS>
        Order deny,allow
        Deny from all
    </LimitExcept>
</Directory>
```

Antes de conseguirmos entrar nas páginas dos utilizadores temos que mudar as permissões das pastas dos USERS de modo a que o user apache consiga ler e executar os ficheiros 644 (rw-;r--;r--) ou 755 (rwx;r-x;r-x).

chmod -R 644 /home/<USER> ou # chmod -R 755 /home/<USER>

Adicionar caminhos na página (ALIAS):
nano /etc/httpd/conf/httpd.conf

```
# We include the /icons/ alias for FancyIndexed directory listings.  If you
# do not use FancyIndexing, you may comment this out.
#
Alias /icons/ "/var/www/icons/"
Alias /teste/ "/trabalhos/" ; endereço da página (ATENÇÃO AOS /) – caminho no disco
```

Criar um virtualhost:

```
NameVirtualHost 192.168.0.1:80 ; definimos o IP do servidor
```

```
# Dominio de dominio.com
```

```
<VirtualHost 192.168.0.1:80>
        DocumentRoot "/home/dominio.com/" ; Caminho para o directório do utilizador do dominio
        ServerName www.dominio.com
        ServerAlias dominio.com
        <Directory "/home/dominio.com">
                Options Indexes FollowSymLinks
                AllowOverride All
                Order allow,deny
                Allow from all
        </Directory>
</VirtualHost>
```

Configurar SAMBA:

```
# yum install samba

# chkconf smb on
# /etc/init.d/smb start

# nano /etc/samba/smb.conf
```

```
[global]
   workgroup = sistemas
   server string = Samba Server
   security = user ; controlado por dupla user/password
   # security = share ; semsegurança
   #passdb backend = tdbsam ; isto está mais a baixo

[web]
   path = /www
   commment = Ficheiros privados
   # valid users = root,ricardo
   # invalid users = dalia,neusa
   browseable = yes
   # hide dot files =yes
   public = yes
   read only = yes
   # writable = yes
```

testparm ; para testar se a configuração está correcta

#smbadduser
smbpasswd -a <USERNAME> ; adiciona um user à autenticação SAMBA

mount -t cifs -o username=<USERNAME>,pasword=<PASSWORD> //IP/<SHARE_NAME> /<MOUNTING_POINT>