

**INSTITUTO POLITÉCNICO DE BEJA**  
**Escola Superior de Tecnologia e Gestão**  
**CTeSP em Redes e Sistemas Informáticos**

**Administração de Sistemas Linux**  
**Projeto**

**Guilherme Rodrigues Vieira**

**Beja**

**30/01/2022**

## Índice

1. Introdução.....	5
2. Ponto 1 – Execução de todas as configurações pedidas nos servidores .....	5
3. Ponto 2 – execução de todas as configurações pedidas .....	8
4. Ponto 3.1/3.2 – Configuração de 4 utilizadores no servidor FTP e jail (usera e userb) ...	10
5. Ponto 4 – Criação do Raid + Hotspare .....	14
6. Ponto 5 – Criação de users e configurações de Apache .....	16
6.1 Ponto 5.1 – Criação dois utilizadores .....	16
6.2 Ponto 5.2 – Criação da homepage para cada utilizador .....	17
6.3 Ponto 5.3 – Criação de página .html para cada utilizador .....	18
6.4 Ponto 5.4 – Criação ed uma diretoria com o nome private .....	19
6.5 Ponto 5.5 – Criação de 2 utilizadores para acederem á diretoria privada .....	20
7. Ponto 6 – Criação dos domínios no servidor DNS .....	21
7.1 Ponto 6.1 – Definir no servidor DNS a possibilidade de receber os backups de ficheiros e configurações cruciais a ambos os servidores .....	21
8. Ponto 7 – Configurar o Servidor de DNS .....	24
8.1 Ponto 7.1 – Criação de 3 zonas master (gules.org, 300emfrente.eu e then.com) .....	24
8.2 Ponto 7.2 – Configurar o as-smtp.300emfrente.eu para ficar responsável pelos emails dos 3 domínios .....	26
8.3 Ponto 7.3 – Criação das zonas reverse do domínio then.com .....	29
9. Ponto 8.1/8.2 – Criação 3 domínios no Servidor DNS e aplicação das configurações pedidas.....	32
10. Conclusão .....	39

## Lista de Figuras

Figura 1 – Configuração do utilizador de administração .....	5
Figura 2 – Configuração do utilizador de guilhermevieira .....	5
Figura 3 – Login com o utilizador guilhermevieira .....	6
Figura 4 – Interface de cada servidor.....	6
Figura 5 – Ping entre máquinas servidor.....	7
Figura 6 – Instalação do SSH .....	7
Figura 7 – Configuração do SSH .....	7
Figura 8 – Acesso negado aos utilizadores via SSH .....	7
Figura 9 – Acesso confirmado ao utilizador root via SSH.....	8
Figura 10 – Login no PC utilizador .....	8
Figura 11 – Pings aos servidores e google.....	8
Figura 12 – Acesso negado ao utilizador usera por SSH .....	9
Figura 13 – Acesso negado ao utilizador userc por SSH.....	9

Figura 14 – Acesso autorizado ao utilizador root por SSH .....	9
Figura 15 – Instalação do pacote VSFTPD .....	10
Figura 16 – Configuração do serviço vsftpd .....	10
Figura 17 – Impedir o acesso via utilizador anónimo e modo autónomo.....	11
Figura 18 – Criação dos utilizadores nas pastas.....	11
Figura 19 – Configuração do ficheiro vsftpd.userlist .....	12
Figura 20 – Utilizadores não enjaulados .....	12
Figura 21 – Configuração na pasta vsftpd.conf.....	13
Figura 22 – Utilizadores FTP em funcionamento .....	13
Figura 23 – Atribuição de 4 discos á máquina servidor.....	14
Figura 24 – Atribuição de 4 discos para o RAID 1 + Hotspare .....	14
Figura 25 – Blkid .....	15
Figura 26 – Configuração do diretório /etc/fstab .....	15
Figura 27 – RAID 1 + Hotspare feito com sucesso.....	16
Figura 28 – Criação dos utilizadores para o serviço de FTP .....	16
Figura 29 – Instalação dos pacotes Apache .....	17
Figura 30 – Alteração do ficheiro userdir.conf.....	17
Figura 31 – Criação e atribuição de permissões a cada utilizador .....	18
Figura 32 – Criação das páginas .html para cada utilizador .....	18
Figura 33 – Mudar o Index para inicio.html .....	19
Figura 34 – Colocar autenticação .....	19
Figura 35 – Criação das diretorias private e o inicio.html.....	20
Figura 36 – Criação do ficheiro .htaccess.....	20
Figura 37 – Criação do utilizador “private” e do “privado” .....	20
Figura 38 – Aceder ao asuser1 .....	20
Figura 39 – Aceder ao asuser2 .....	21
Figura 40 – Aceder ao asuser1 na pasta private .....	21
Figura 41 – Editar o ficheiro tftp-server.service.....	22
Figura 42 – Editar o ficheiro tftp-server.socket .....	22
Figura 43 – Visualizar o estado do TFTP Server o sudo systemctl status tftp-server.....	23
Figura 44 – Parar a firewall .....	23
Figura 45 – Criar o ficheiro hello.txt.....	23
Figura 46 – Regras de firewall serviço TFTP .....	23
Figura 47 – Upload do ficheiro hello.txt para a máquina servidor TFTP.....	24
Figura 48 – Confirmação do upload do ficheiro hello.txt para o servidor TFTP .....	24
Figura 49 – Instalação do DNS.....	24
Figura 50 – Regras da firewall .....	24
Figura 51 – Configuração do ficheiro named .....	25
Figura 52 – Criação das zonas para o exercício 7.1 e 7.2 .....	25
Figura 53 – Configuração do gules.org.db.....	26
Figura 54 – Configuração do 300enfrente.eu.db .....	26
Figura 55 – Configuração do then.com.db.....	27
Figura 56 – Dig 300enfrente.eu MX .....	27
Figura 57 – Dig then.com MX.....	28
Figura 58 – Dig gules.org MX.....	28
Figura 59 – Criação das zonas para o exercício 7.3.....	29
Figura 60 – Configuração do 14.22.200.191.db .....	29
Figura 61 – Configuração do 1.45.147.92.db .....	30

Figura 62 – Configuração do 16.22.168.194.db .....	30
Figura 63 – Dig -x 191.200.22.14.....	30
Figura 64 – Dig -x 92.147.45.1.....	31
Figura 65 – Dig -x 194.168.22.16.....	31
Figura 66 – Instalação dos pacotes httpd no servidor DNS .....	32
Figura 67 – Comandos para iniciar os serviços Apache.....	32
Figura 68 – Criação das zonas para o exercício 8.....	33
Figura 69 – Ficheiro httpd.conf .....	33
Figura 71 – Criação do ficheiro html para o domínio allow.org.....	33
Figura 72 – Configuração do ficheiro html para o domínio allow.org .....	34
Figura 73 – Dar permissões ao domínio allow.org.....	34
Figura 74 – Configuração do VirtualHost do domínio allow.org .....	34
Figura 75 – Configuração do allow.org.....	34
Figura 76 – Criação do ficheiro html para o domínio circle360.pt.....	35
Figura 77 – Configuração do ficheiro html para o domínio circle.pt.....	35
Figura 78 – Dar permissões ao domínio circle360.pt.....	35
Figura 79 – Configuração do VirtualHost do domínio circle360.pt .....	35
Figura 80 – Configuração do circle360.pt.....	36
Figura 81 – Criação do ficheiro html para o domínio festas.pt.....	36
Figura 82 – Configuração do ficheiro html para o domínio festas.pt.....	36
Figura 83 – Dar permissões ao domínio festas.pt.....	36
Figura 84 – Configuração do VirtualHost do domínio festas.pt .....	37
Figura 85 – Configuração do festas.pt.....	37
Figura 86 – Configuração para a porta tcp 25000 e 28000 – parte 1.....	37
Figura 87 – Configuração para a porta tcp 25000 e 28000 – parte 2.....	37
Figura 88 – Acesso ao domínio festas.pt pela porta 25000 .....	38
Figura 89 – Acesso ao domínio circle360.pt pela porta 28000 .....	38
Figura 90 – Acesso ao domínio allow.org pela porta 28000 .....	39

## 1. Introdução

Antes da implementação dos serviços e comandos pedidos pelo professor foram instalados diferentes pacotes para ajudar na configuração dos comandos ou a visualizar outras características, com isto refiro-me á instalação do nano e da net-tools.

Usei 2 máquinas CentOS 7 e como servidor uma máquina cliente com 1 interface controlado pelo GNS3, e usei o PuTTY algo que facilitou na transposição de comandos.

No projeto não foi implementado o script relativo á pergunta 6.1.

## 2. Ponto 1 – Execução de todas as configurações pedidas nos servidores

Nesta figura 1 foi configurado o utilizador de administração para ambos os servidores.

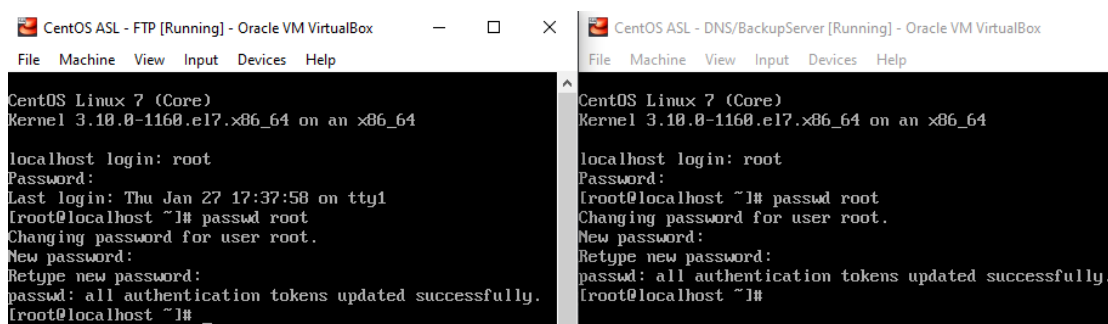


Figura 1 – Configuração do utilizador de administração

Nesta etapa foi criado o utilizador guilhermevieira com a password ASL2022 como pedido no enunciado, é possível ver o utilizador a ser utilizado na figura 3.

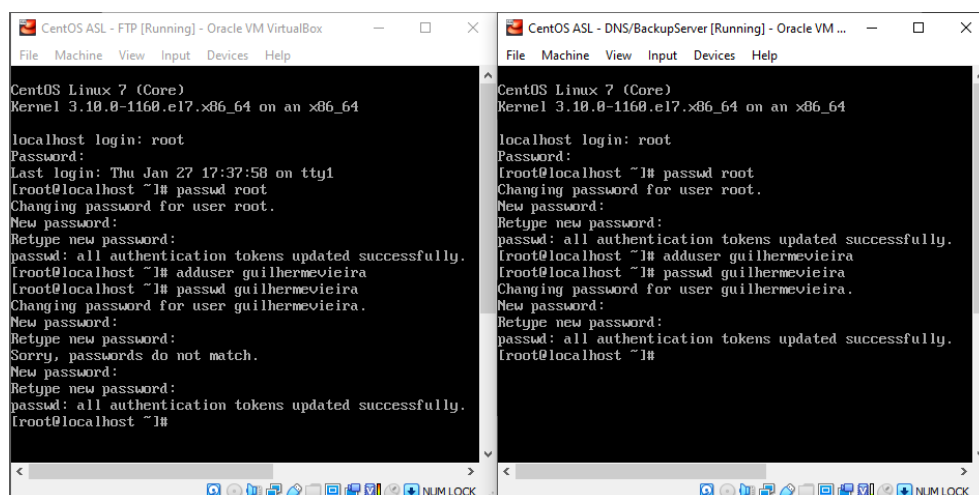


Figura 2 – Configuração do utilizador de guilhermevieira

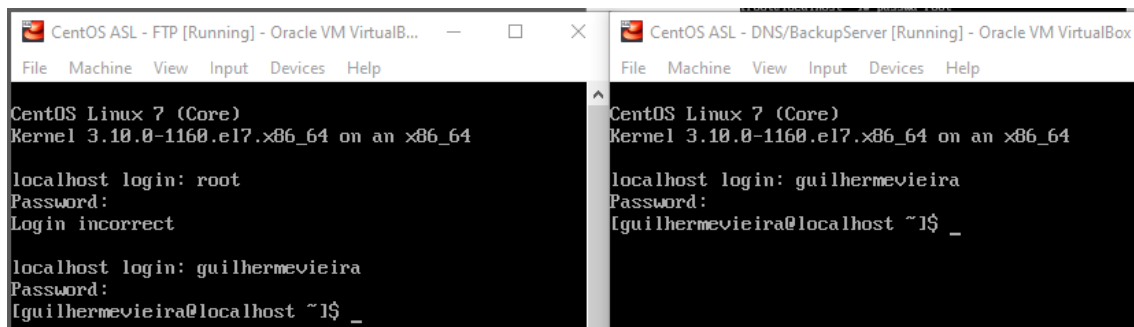


Figura 3 – Login com o utilizador guilhermevieira

Na figura 4 é possível ver na esquerda o endereço da interface do servidor FTP e na direita o endereço da interface do servidor de DNS, os endereços podem variar porque quando desligo as máquinas e encerro o PC e volto a ligar por vezes a interface loopback não é reconhecida fazendo com que eu tenha de desligar a partilha na minha interface Ethernet e voltar a partilhar para assim conseguir voltar a ter um endereço atribuído nas minhas máquinas.

Cada máquina seja a máquina utilizador ou servidor apenas têm 1 interface que é controlada pelo próprio GNS3 “Generic Driver”, poderia também estabelecer comunicação entre as máquinas caso usa-se uma interface de rede interna em cada máquina e depois usa-se uma interface bridge para cada máquina conseguir ter acesso á internet para assim baixar os recursos que fossem necessário, porém como o projeto pede foi feito apenas com o controlo do GNS3.

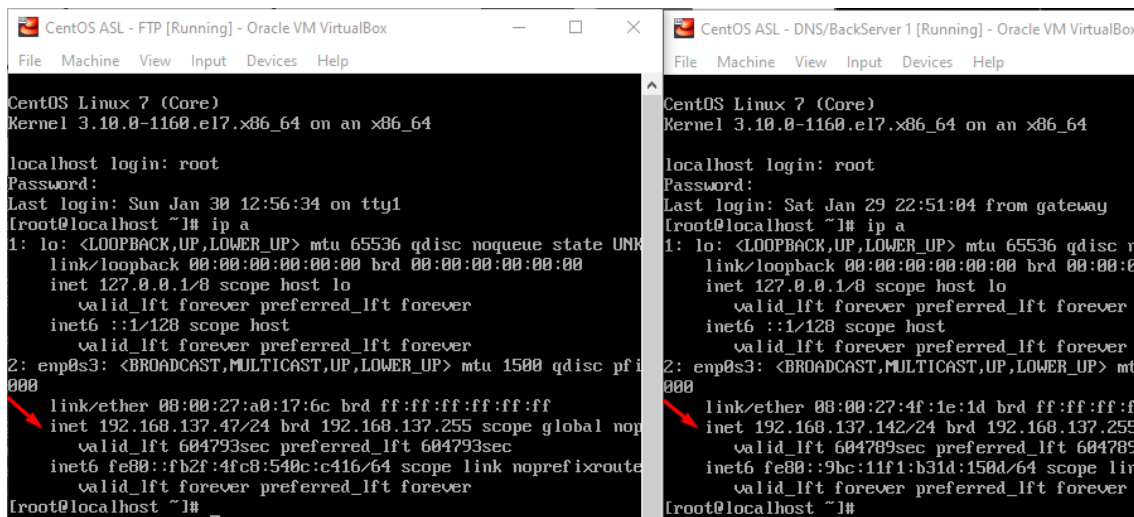


Figura 4 – Interface de cada servidor

Como é possível visualizar ambas as máquinas servidor conseguem comunicar entre si.

```
root@localhost ~]# ping 192.168.137.142
PING 192.168.137.142 (192.168.137.142) 56(84) bytes of data:
64 bytes from 192.168.137.142: icmp_seq=1 ttl=64 time=0.967 ms
64 bytes from 192.168.137.142: icmp_seq=2 ttl=64 time=0.976 ms
64 bytes from 192.168.137.142: icmp_seq=3 ttl=64 time=1.00 ms
^C
--- 192.168.137.142 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 0.967/0.983/1.008/0.040 ms

root@localhost ~]# ping 192.168.137.47
PING 192.168.137.47 (192.168.137.47) 56(84) bytes of data:
64 bytes from 192.168.137.47: icmp_seq=1 ttl=64 time=0.734 ms
64 bytes from 192.168.137.47: icmp_seq=2 ttl=64 time=1.50 ms
64 bytes from 192.168.137.47: icmp_seq=3 ttl=64 time=1.16 ms
^C
--- 192.168.137.47 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 0.734/1.134/1.508/0.316 ms
```

Figura 5 – Ping entre máquinas servidor

Instalação do serviço de SSH para assim as máquinas comunicarem entre si por de forma segura.

```
root@localhost ~]# yum install openssh-server
```

Figura 6 – Instalação do SSH

Na diretoria /etc/ssh/sshd\_config das 2 máquinas servidor foi negado o utilizador guilhermevieira e todos os outros utilizadores “utilizadores que foram criados no ponto 3” como é possível visualizar, permitindo assim que apenas o utilizador root seja o único a conseguir comunicar via SSH.

Depois das alterações aplicadas na figura 7 foi feito o restart aos serviços de ssh “systemctl restart sshd”.

```
# Authentication:
#LoginGraceTime 2m
PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
DenyUsers      guilhermevieira usera userb userc userd
```

Figura 7 – Configuração do SSH

Na figura 8 é possível ver que o ssh não permite o acesso aos utilizadores criados no ponto 3 e na figura 9 temos as máquinas servidor a conseguiram entrar uma dentro da outra com recurso ao utilizador root via SSH.

```
root@localhost:~
[root@localhost ~]# sudo ssh userc@192.168.137.47
userc@192.168.137.47's password:
Permission denied, please try again.
userc@192.168.137.47's password:

root@localhost:~
[root@localhost ~]# sudo ssh userc@192.168.137.142
userc@192.168.137.142's password:
Permission denied, please try again.
userc@192.168.137.142's password:
```

Figura 8 – Acesso negado aos utilizadores via SSH

```
[root@localhost ~]# sudo ssh 192.168.137.142
root@192.168.137.142's password:
Last login: Sun Jan 30 13:01:40 2022 from desktop-jclv956.mshome.net
[root@localhost ~]#

[root@localhost ~]# sudo ssh 192.168.137.47
root@192.168.137.47's password:
Last login: Sun Jan 30 13:04:36 2022 from desktop-jclv956.mshome.net
[root@localhost ~]#
```

Figura 9 – Acesso confirmado ao utilizador root via SSH

### 3. Ponto 2 – execução de todas as configurações pedidas

Durante a instalação da máquina Ubuntu com interface gráfica foi criado o utilizador guilhermevieira com a respetiva password ASL2022.

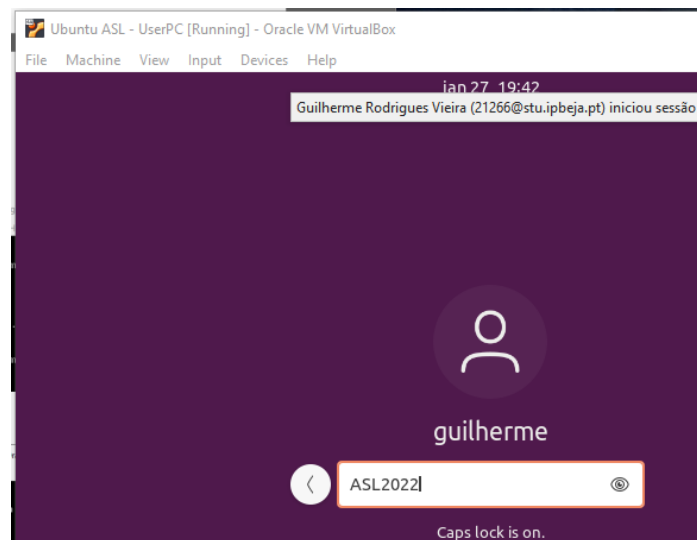


Figura 10 – Login no PC utilizador

Com a figura 11 verifica-se que a máquina cliente consegue tanto pingar as interfaces das máquinas servidor o google.

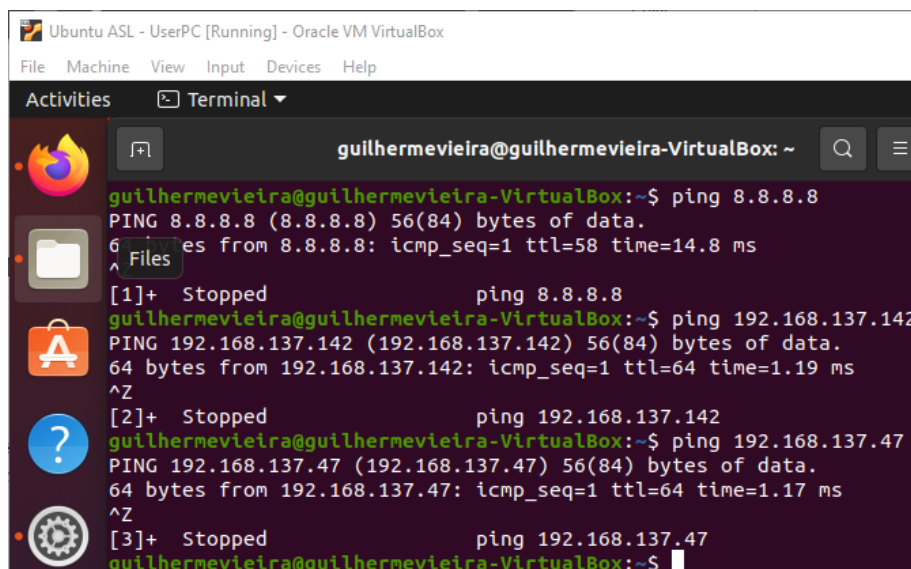


Figura 11 – Pings aos servidores e google



Como é possível visualizar na figura 12 o utilizador usera da máquina cliente está a tentar aceder por SSH ao servidor 192.168.137.142, é possível verificar que o acesso é negado, o mesmo acontece quando o utilizador userc tenta aceder ao endereço da outra máquina servidor 192.168.137.47 na figura 13 porém na figura 14 ao usar o utilizador root e a sua respetiva password é possível aceder aos servidores via ssh pela máquina cliente.

```
guilhermevieira@guilhermevieira-VirtualBox:~$ sudo ssh usera@192.168.137.142
[sudo] password for guilhermevieira:
usera@192.168.137.142's password:
Permission denied, please try again.
usera@192.168.137.142's password:
```

Figura 12 – Acesso negado ao utilizador usera por SSH

```
guilhermevieira@guilhermevieira-VirtualBox:~$ sudo ssh userc@192.168.137.47
userc@192.168.137.47's password:
Permission denied, please try again.
userc@192.168.137.47's password:
Permission denied, please try again.
userc@192.168.137.47's password:
userc@192.168.137.47: Permission denied (publickey,gssapi-keyex,gssapi-with-
```

Figura 13 – Acesso negado ao utilizador userc por SSH

```
guilhermevieira@guilhermevieira-VirtualBox:~$ sudo ssh 192.168.137.142
[sudo] password for guilhermevieira:
root@192.168.137.142's password:
Last login: Sun Jan 30 15:44:34 2022 from 192.168.137.123
[root@localhost ~]#

guilhermevieira@guilhermevieira-VirtualBox:~$ sudo ssh 192.168.137.47
[sudo] password for guilhermevieira:
root@192.168.137.47's password:
Last login: Sun Jan 30 15:30:55 2022 from 192.168.137.142
[root@localhost ~]#
```

Figura 14 – Acesso autorizado ao utilizador root por SSH

#### 4. Ponto 3.1/3.2 – Configuração de 4 utilizadores no servidor FTP e jail (usera e userb)

Antes de começar a configuração do FTP foi necessário instalar os pacotes necessários ao funcionamento do serviço FTP para isso foi instalado o pacote vsftpd como está demonstrado na figura 15 e foi instalado o pacote ftp usando o comando “yum -y install ftp”.

```
Installing:
vsftpd                                x86_64                3.0.2-29.el7_9

Transaction Summary
=====
Install 1 Package

Total download size: 173 k
Installed size: 353 k
Downloading packages:
vsftpd-3.0.2-29.el7_9.x86_64.rpm
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : vsftpd-3.0.2-29.el7_9.x86_64
  Verifying  : vsftpd-3.0.2-29.el7_9.x86_64

Installed:
vsftpd.x86_64 0:3.0.2-29.el7_9

Complete!
[root@localhost ~]#
```

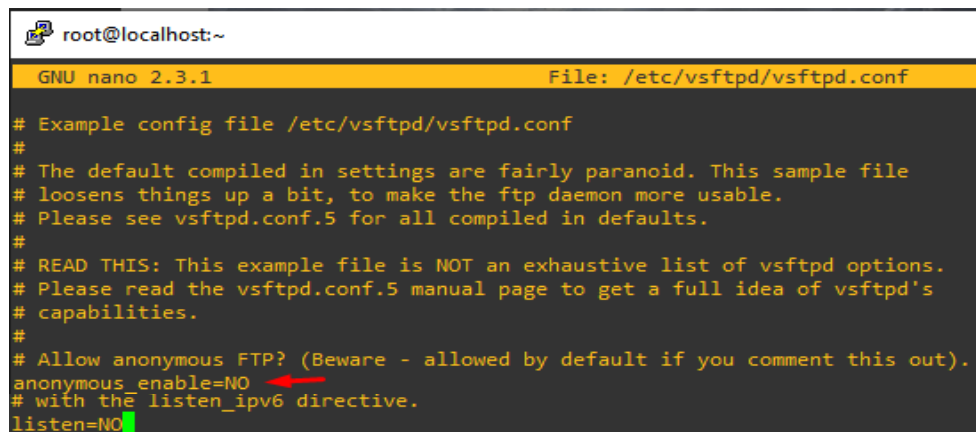
Figura 15 – Instalação do pacote VSFTPD

Os comandos seguintes do systemctl foram aplicados para que nas próximas sessões o sistema inicie automaticamente o serviço FTP e foram aplicados os comandos de firewall para permitir que outras máquinas conseguissem aceder ao serviço de FTP.

```
[root@localhost ~]# systemctl start vsftpd
[root@localhost ~]# systemctl enable vsftpd
Created symlink from /etc/systemd/system/multi-user.target.wants/vsftpd.service to /usr/lib/systemd/system/vsftpd.service.
[root@localhost ~]# firewall-cmd --zone=public --permanent --add-port=21/tcp
success
[root@localhost ~]# firewall-cmd --zone=public --permanent --add-service=ftp
success
[root@localhost ~]# firewall-cmd --reload
success
[root@localhost ~]# cp /etc/vsftpd/vsftpd.conf /etc/vsftpd/vsftpd.conf.orig
[root@localhost ~]#
```

Figura 16 – Configuração do serviço vsftpd

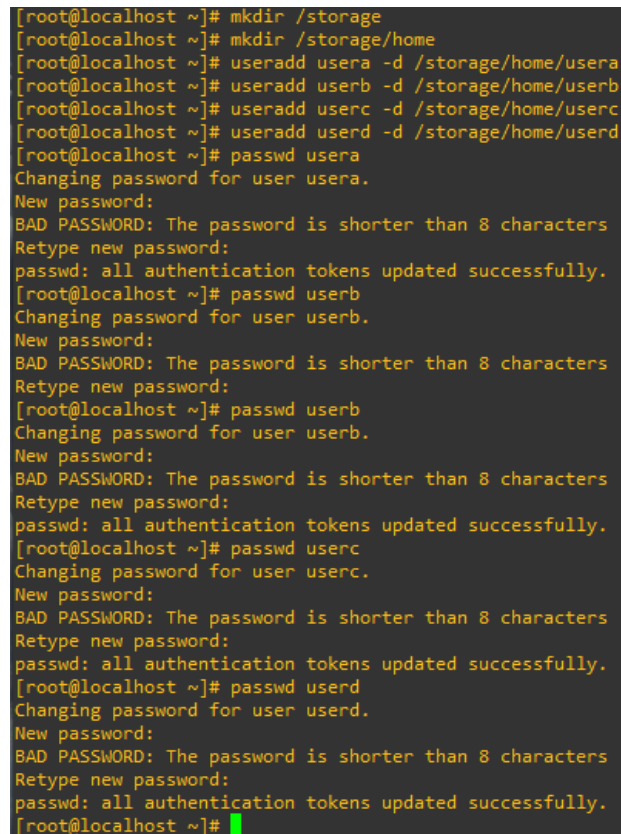
Dentro do ficheiro vsftpd.conf foi necessário alterar a linha anonymous=yes para anonymous=no assim desabilitando o acesso anónimo ao FTP e configurado o listen=NO para impedir que o vsftpd fosse executado no modo autónomo.



```
root@localhost:~
GNU nano 2.3.1 File: /etc/vsftpd/vsftpd.conf
# Example config file /etc/vsftpd/vsftpd.conf
#
# The default compiled in settings are fairly paranoid. This sample file
# loosens things up a bit, to make the ftp daemon more usable.
# Please see vsftpd.conf.5 for all compiled in defaults.
#
# READ THIS: This example file is NOT an exhaustive list of vsftpd options.
# Please read the vsftpd.conf.5 manual page to get a full idea of vsftpd's
# capabilities.
#
# Allow anonymous FTP? (Beware - allowed by default if you comment this out).
anonymous_enable=NO
# with the listen_ipv6 directive.
listen=NO
```

Figura 17 – Impedir o acesso via utilizador anónimo e modo autónomo

Na figura 18 foram criados os utilizadores dentro do diretório /storage/home e dadas as suas respetivas passwords.



```
[root@localhost ~]# mkdir /storage
[root@localhost ~]# mkdir /storage/home
[root@localhost ~]# useradd usera -d /storage/home/usera
[root@localhost ~]# useradd userb -d /storage/home/userb
[root@localhost ~]# useradd userc -d /storage/home/userc
[root@localhost ~]# useradd userd -d /storage/home/userd
[root@localhost ~]# passwd usera
Changing password for user usera.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
[root@localhost ~]# passwd userb
Changing password for user userb.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
[root@localhost ~]# passwd userb
Changing password for user userb.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
[root@localhost ~]# passwd userc
Changing password for user userc.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
[root@localhost ~]# passwd userd
Changing password for user userd.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
[root@localhost ~]#
```

Figura 18 – Criação dos utilizadores nas pastas

Depois de criados os utilizadores estes foram inseridos dentro da diretoria /vsftpd.userlist.

Foram ainda permito o chroot\_list\_enable=yes para assim conseguir permitir a configuração do enjaulamento.

```
root@localhost:/etc/httpd/conf.d
GNU nano 2.3.1 File: /etc/vsftpd.userlist
userlist_enable=YES # vsftpd will load a list of usernames, from the filename given by userlist_file
userlist_file=/etc/vsftpd.userlist # stores usernames.
userlist_deny=NO
chroot_local_user=YES
allow_writeable_chroot=YES
chroot_list_enable=YES
usera
userb
userc
userd
```

Figura 19 – Configuração do ficheiro vsftpd.userlist

Durante a criação da Jail que supostamente deveria ter inserido os utilizadores usera e userb, por alguma razão estes conseguiam sair das suas pastas /home e ir para as dos outros utilizadores, para contrariar essa “anormalidade” inseri o userc e userd dentro da jail, alteração essa que veio a demonstrar o funcionamento do pretendido no enunciado e como tal deixei assim mesmo, o funcionamento do mesmo vai ser visto nas próximas figuras.

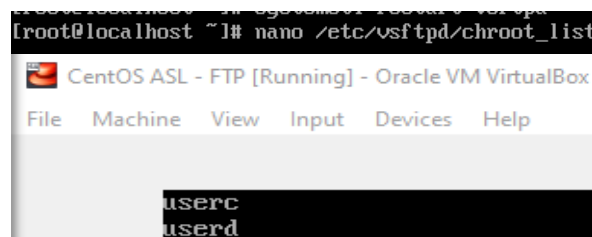


Figura 20 – Utilizadores não enjaulados

Na figura 21 foram aplicados os comandos necessários para conseguir que os utilizadores dentro da lista /chroot\_list tivessem acesso às pastas dos outros utilizadores.

```
GNU nano 2.3.1 File: /etc/vsftpd/vsftpd.conf
# predicted this attack and has always been safe, reporting the size of the
# raw file.
# ASCII mangling is a horrible feature of the protocol.
#ascii_upload_enable=YES
#ascii_download_enable=YES
#
# You may fully customise the login banner string:
#ftpd_banner=Welcome to blah FTP service.
#
# You may specify a file of disallowed anonymous e-mail addresses. Apparently
# useful for combatting certain DoS attacks.
#deny_email_enable=YES
# (default follows)
#banned_email_file=/etc/vsftpd/banned_emails
#
# You may specify an explicit list of local users to chroot() to their home
# directory. If chroot_local_user is YES, then this list becomes a list of
# users to NOT chroot().
# (Warning! chroot'ing can be very dangerous. If using chroot, make sure that
# the user does not have write access to the top level directory within the
# chroot)
chroot_local_user=YES
chroot_list_enable=YES
# (default follows)
chroot_list_file=/etc/vsftpd/chroot_list
```

Figura 21 – Configuração na pasta vsftpd.conf

É possível aceder ao serviço de FTP com o usera, este não consegue aceder às áreas dos outros utilizadores porém como podemos ver mais abaixo na figura 22 o userc consegue aceder às pastas /home dos outros utilizadores. Apesar de não estar demonstrado em imagens tanto o usera e userb não conseguem aceder aos outros porém os userc e userd conseguem aceder a qualquer outro user sem problema.

```
guilhermevieira@guilhermevieira-VirtualBox:~$ ftp 192.168.137.38
Connected to 192.168.137.38.
220 (vsFTPd 3.0.2)
Name (192.168.137.38:guilhermevieira): usera
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pwd
257 "/"
ftp> cd /storage/home/userc
550 Failed to change directory.
ftp> cd /storage/home/userb
550 Failed to change directory.
ftp> ^Z
[18]+  Stopped                  ftp 192.168.137.38
guilhermevieira@guilhermevieira-VirtualBox:~$ ftp 192.168.137.38
Connected to 192.168.137.38.
220 (vsFTPd 3.0.2)
Name (192.168.137.38:guilhermevieira): userc
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pwd
257 "/storage/home/userc"
ftp> cd /storage/home/usera
250 Directory successfully changed.
```

Figura 22 – Utilizadores FTP em funcionamento

## 5. Ponto 4 – Criação do Raid + Hotspare

Foram inseridos 4 discos dentro da máquina DNS, onde 2 desses serviram para criar o raid 1, 1 para o Hotspare e 1 para o Sistema Operativo.

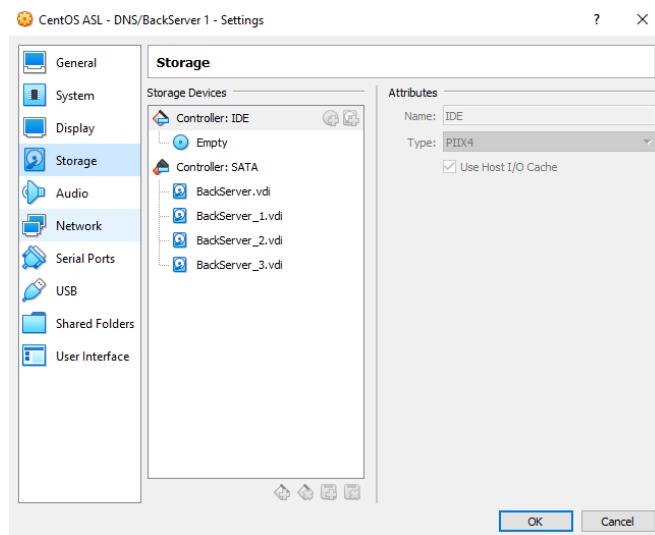


Figura 23 – Atribuição de 4 discos á máquina servidor

Antes de fazer as configurações que se encontram na figura 24 foi instalado o pacote mdadm “yum install mdadm -y”, depois foi inserido o comando “mdadm –create ....” para assim criar o Raid de nível 1, onde foram usados 2 discos de 10GB como pedido no enunciado e deixado 1 disco de parte disco esse que é o Spare. O disco Spare tem como função entrar em funcionamento caso algum dos discos do Raid 1 fique inoperacional.

```
[root@localhost ~]# mdadm --create --verbose --level=1 --metadata=1.2 --raid-devices=2 /dev/md/backup
p /dev/sdb /dev/sdc --spare-devices=1 /dev/sdd
mdadm: partition table exists on /dev/sdb
mdadm: partition table exists on /dev/sdb but will be lost or
meaningless after creating array
mdadm: size set to 10476544K
Continue creating array?
Continue creating array? (y/n) y
mdadm: array /dev/md/backup started.
[root@localhost ~]# lsblk
```

NAME	MAJ:MIN	RM	SIZE	RO	TYPE	MOUNTPOINT
sda	8:0	0	10G	0	disk	
└─sda1	8:1	0	1G	0	part	/boot
└─sda2	8:2	0	9G	0	part	
└─centos-root	253:0	0	8G	0	lvm	/
└─centos-swap	253:1	0	1G	0	lvm	[SWAP]
sdb	8:16	0	10G	0	disk	
└─sdb1	8:17	0	10G	0	part	
└─md127	9:127	0	10G	0	raid1	
sdc	8:32	0	10G	0	disk	
└─md127	9:127	0	10G	0	raid1	
sdd	8:48	0	10G	0	disk	
└─md127	9:127	0	10G	0	raid1	
sr0	11:0	1	1024M	0	rom	

```
[root@localhost ~]#
```

Figura 24 – Atribuição de 4 discos para o RAID 1 + Hotspare

Depois de aplicado os comandos acima mostrados é necessário fazer reboot para ter certeza que as alterações efetuadas foram aplicadas, depois de reiniciada a máquina é feito o blkid para ver as todas as partições e verificar se a m127 se encontra entre as mesmas.

```
[root@localhost ~]# blkid
/dev/sda1: UUID="cc12f67a-bb73-4585-b293-fd784d298e43" TYPE="xfs"
/dev/sda2: UUID="DIIiB1f-EJuf-Sz1t-EZUm-7xwt-QDbn-kIRrzA" TYPE="LVM2_member"
/dev/sdb: UUID="bb895144-ed0c-f686-a195-fdc8043d483" UUID_SUB="06ec84f3-578d-aedb-0179-00186c553841" LABEL="localhost.localdomain:backup" TYPE="linux_raid_member"
/dev/sdc: UUID="bb895144-ed0c-f686-a195-fdc8043d483" UUID_SUB="7f4863b0-ab8e-0b02-18bf-f4b1de5a110c" LABEL="localhost.localdomain:backup" TYPE="linux_raid_member"
/dev/sdd: UUID="bb895144-ed0c-f686-a195-fdc8043d483" UUID_SUB="30dd9f4c-63b0-bd05-3bad-02acb9d74887" LABEL="localhost.localdomain:backup" TYPE="linux_raid_member"
/dev/mapper/centos-root: UUID="0b2d24b7-9443-40fe-8b16-97de1c3f7942" TYPE="xfs"
/dev/mapper/centos-swap: UUID="73d7cbe3-bf6c-4375-8630-5732958b0103" TYPE="swap"
/dev/md127: UUID="fd2c62f8-0e7f-4bf5-819d-a0d305b29fad" TYPE="ext4"
[root@localhost ~]#
```

Figura 25 – Blkid

Depois de verificar se a m127 estava na blk, inseri a última linha de comando da figura 26, esta serviu para montar a partição dentro do array, array esse que foi criado na configuração do no mdadm.conf e depois de aplicado o comando a máquina foi reiniciada.

```
##
## /etc/fstab
## Created by anaconda on Fri Jan 28 13:24:21 2022
##
## Accessible filesystems, by reference, are maintained under '/dev/disk'
## See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
##
/dev/mapper/centos-root / xfs defaults 0 0
/dev/mapper/centos-root /boot xfs defaults 0 0
/dev/mapper/centos-swap swap swap defaults 0 0
/dev/md127 /disk1 ext4 defaults 0 0
```

Figura 26 – Configuração do diretório /etc/fstab

Depois de iniciada a máquina é possível verificar se tudo ficou bem configurado partir do comando “mdadm –detail /dev/md127”, ao executar o comando é possível ver as características da criação do RAID 1, o qual ficou com 2 discos atribuídos e o Spare com 1 disco, disco esse que entra em funcionamento caso algum dos discos do RAID 1 falhe.

```
[root@localhost ~]# mdadm /dev/md127
/dev/md127: 9.99GiB raid1 2 devices, 1 spare. Use mdadm --detail for more detail.
[root@localhost ~]# mdadm --detail /dev/md127
/dev/md127:
    Version : 1.2
    Creation Time : Fri Jan 28 19:13:32 2022
    Raid Level : raid1
    Array Size : 10476544 (9.99 GiB 10.73 GB)
    Used Dev Size : 10476544 (9.99 GiB 10.73 GB)
    Raid Devices : 2
    Total Devices : 3
    Persistence : Superblock is persistent

    Update Time : Fri Jan 28 19:30:24 2022
    State : clean
    Active Devices : 2
    Working Devices : 3
    Failed Devices : 0
    Spare Devices : 1

    Consistency Policy : resync

    Name : localhost.localdomain:backup (local to host localhost.localdomain)
    UUID : bb895144:ed0cf686:a195fcd4:8043d483
    Events : 18

    Number Major Minor RaidDevice State
    0      8      16        0 active sync /dev/sdb
    1      8      32        1 active sync /dev/sdc
    2      8      48        - spare   /dev/sdd

[root@localhost ~]#
```

Figura 27 – RAID 1 + Hotspare feito com sucesso

## 6. Ponto 5 – Criação de users e configurações de Apache

### 6.1 Ponto 5.1 – Criação dois utilizadores

Criação dos respetivos utilizadores “asuser1, asuser2” no grupo “users.

```
[root@localhost ~]# useradd asuser1 -G users
[root@localhost ~]# useradd asuser2 -G users
[root@localhost ~]# passwd asuser1
Changing password for user asuser1.
New password:
BAD PASSWORD: The password contains the user name in some form
Retype new password:
passwd: all authentication tokens updated successfully.
[root@localhost ~]# passwd asuser2
Changing password for user asuser2.
New password:
BAD PASSWORD: The password contains the user name in some form
Retype new password:
passwd: all authentication tokens updated successfully.
[root@localhost ~]#
```

Figura 28 – Criação dos utilizadores para o serviço de FTP



## 6.2 Ponto 5.2 – Criação da homepage para cada utilizador

Instalação de todos os pacotes necessários ao bom funcionamento dos serviços Apache.

```
[root@localhost ~]# yum install httpd*
```

Figura 29 – Instalação dos pacotes Apache

Para configurar o servidor Apache de modo que cada utilizador tenha uma diretoria com o nome “homepage” na sua diretoria home, para isso primeiro foi necessário ir ao ficheiro `userdir.conf` e editar a `UserDir` para homepage como é possível ver na figura.

```
#
# UserDir: The name of the directory that is appended onto a user's home
# directory if a ~user request is received.
#
# The path to the end user account 'public_html' directory must be
# accessible to the webserver userid. This usually means that ~userid
# must have permissions of 711, ~userid/public_html must have permissions
# of 755, and documents contained therein must be world-readable.
# Otherwise, the client will only receive a "403 Forbidden" message.
#
<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 enable homepage

#
# 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 homepage
</IfModule>

#
# Control access to UserDir directories. The following is an example
# for a site where these directories are restricted to read-only.
#
<Directory "/home/*/homepage">
    AllowOverride FileInfo AuthConfig Limit Indexes
    Options MultiViews Indexes SymLinksIfOwnerMatch IncludesNoExec
    Require method GET POST OPTIONS
</Directory>
```

Figura 30 – Alteração do ficheiro `userdir.conf`

Depois de aplicar as alterações ao ficheiro `userdir.conf` é necessário reiniciar os serviços e entrar dentro da pasta “asuser” e criar a respetiva homepage para cada utilizador dando depois as permissões que se encontram no final a cada utilizador.


```
[asuser1@localhost root]$ cd /home/asuser1
[asuser1@localhost ~]$ pwd
/home/asuser1
[asuser1@localhost ~]$ mkdir homepage
[asuser1@localhost ~]$ ls
homepage
[root@localhost ~]# su asuser2
[asuser2@localhost root]$ cd /home/asuser2
[asuser2@localhost ~]$ mkdir homepage
[asuser2@localhost ~]$ ls
homepage
[root@localhost home]# chmod 755 asuser1 -R
[root@localhost home]# chmod 755 asuser2 -R
```

Figura 31 – Criação e atribuição de permissões a cada utilizador

### 6.3 Ponto 5.3 – Criação de página .html para cada utilizador

Nesta etapa foi criado uma pequena página html como o nome de `inicio.html` tanto para o `asuser1` como para o `asuser2` para depois ser possível visualizar o conteúdo da página quando fosse aceder à página no browser.

```
[asuser1@localhost ~]$ cd /home/asuser1/homepage
[asuser1@localhost homepage]$ nano inicio.html
```



```
[asuser2@localhost home]$ cd /home/asuser2/homepage
[asuser2@localhost homepage]$ nano inicio.html
```

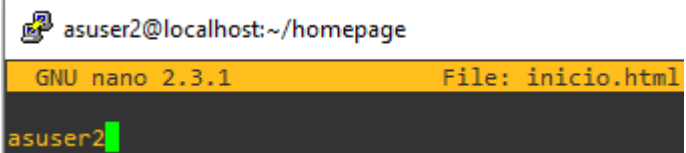


Figura 32 – Criação das páginas .html para cada utilizador

Para ser possível mudar o nome do ficheiro `index.html` para o pedido tive de aceder ao ficheiro de configuração `httpd` apagar o `index.html` e substituir pelo nome `inicio.html`.

```
asuser2@localhost:~/homepage
GNU nano 2.3.1 File: /etc/httpd/conf/httpd.conf

#
Options Indexes FollowSymLinks

#
# 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

#
# Controls who can get stuff from this server.
#
Require all granted
</Directory>

#
# DirectoryIndex: sets the file that Apache will serve if a directory
# is requested.
#
<IfModule dir_module>
    DirectoryIndex inicio.html
</IfModule>
```

Figura 33 – Mudar o Index para inicio.html

## 6.4 Ponto 5.4 – Criação ed uma diretoria com o nome private

Foi necessário alterar o ficheiro httpd.conf nomeadamente a autenticação.

```
root@localhost:~
GNU nano 2.3.1 File: /etc/httpd/conf/httpd.conf

#
ServerAdmin root@localhost

#
# ServerName gives the name and port that the server uses to identify itself.
# This can often be determined automatically, but we recommend you specify
# it explicitly to prevent problems during startup.
#
# If your host doesn't have a registered DNS name, enter its IP address here.
#
#ServerName www.example.com:80

#
# Deny access to the entirety of your server's filesystem. You must
# explicitly permit access to web content directories in other
# <Directory> blocks below.
#
<Directory />
    AllowOverride AuthConfig
    Require all denied
</Directory>
```

Figura 34 – Colocar autenticação

Na figura 35 foi criada as diretorias “private” e por sua vez o ficheiro inicio.html dentro das pastas “private” para cada utilizador.

```
[root@localhost ~]# cd /home/asuser1/homepage/  
[root@localhost homepage]# mkdir private  
[root@localhost homepage]# cd /home/asuser2/homepage/  
[root@localhost homepage]# mkdir private  
[root@localhost homepage]# cd /home/asuser1/homepage/private/  
[root@localhost private]# nano inicio.html  
[root@localhost private]# cd /home/asuser2/homepage/private/  
[root@localhost private]# nano inicio.html
```

Figura 35 – Criação das diretorias private e o inicio.html

Por fim foi criado o ficheiro .htaccess que é um ficheiro oculto no diretório private /home/asuser2/homepage/private.

```
[root@localhost private]# vi .htaccess  
AuthName "Diretorio Privado - Nome Utilizador"  
AuthType Basic  
AuthUserFile /home/asuser1/homepage/private/.user_passwd  
require valid-user
```

Figura 36 – Criação do ficheiro .htaccess

## 6.5 Ponto 5.5 – Criação de 2 utilizadores para acederem á diretoria privada

Nesta etapa do projeto houve a criação dos utilizadores “private” e “privado” de forma oculta.

```
[root@localhost private]# htpasswd -c /home/asuser1/homepage/private/.user_passwd private  
New password:  
Re-type new password:  
Adding password for user private  
[root@localhost private]# htpasswd /home/asuser1/homepage/private/.user_passwd privado  
New password:  
Re-type new password:  
Adding password for user privado  
[root@localhost private]# cat .user_passwd  
private:$apr1$qs9NVpfJ$gn3k4JHqrVVeZVqAVZCUA0  
privado:$apr1$xuPgNebo$GuWBQ1Z7mpjD09aA1Br7M/  
[root@localhost private]#
```

Figura 37 – Criação do utilizador “private” e do “privado”

Como é possível visualizar os domínios criados para cada user estão a funcionar.

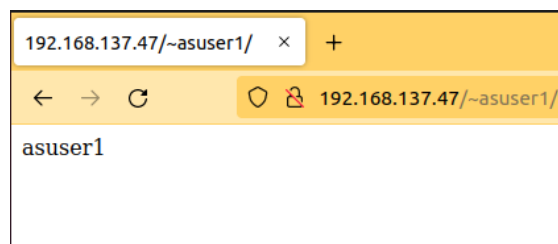


Figura 38 – Aceder ao asuser1

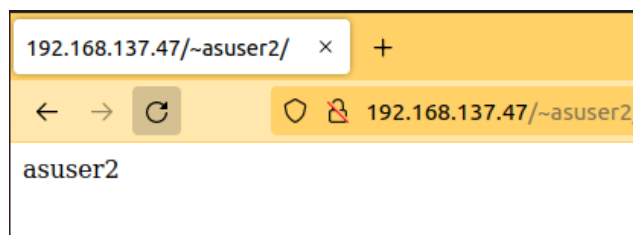


Figura 39 – Aceder ao asuser2

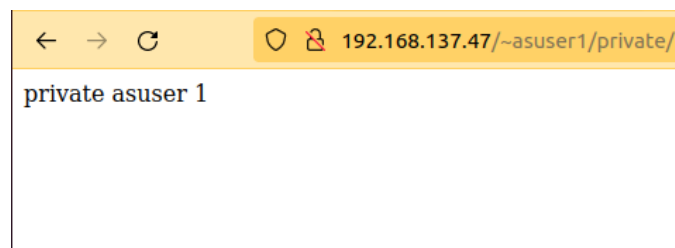


Figura 40 – Aceder ao asuser1 na pasta private

## 7. Ponto 6 – Criação dos domínios no servidor DNS

### 7.1 Ponto 6.1 – Definir no servidor DNS a possibilidade de receber os backups de ficheiros e configurações cruciais a ambos os servidores

Nos comandos e figuras abaixo mostrados estão todas as configurações e implementações necessárias para possibilitar a receção de backups ao servidor DNS.

Como tal essas configurações efetuadas estão explicadas passo a passo como é possível visualizar, os comandos/figuras foram alternadamente implementados na máquina servidor e na máquina cliente, vale lembrar que para permitir que mais máquinas consigam transferir ficheiros para o servidor de Backup é apenas necessário fazer as configurações da máquina FTP abaixo mostradas:

Os 2 comandos abaixo mostrados foram executados em ambas as máquinas, o primeiro comando faz o update à cache do repositório de pacotes YUM e o segundo instala os pacotes necessários para instalar os serviços de tftp.

```
sudo yum makecache
```

```
sudo yum install tftp tftp-server
```

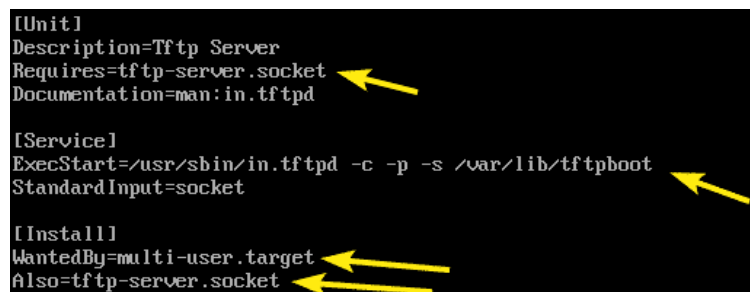
Comandos executados na máquina DNS/Backup copiei os arquivos do serviço systemd do servidor tftp para o diretório /etc/systemd/system apenas por segurança e copiei o arquivo tftp.service para o diretório /etc/systemd/system, executando os seguintes comandos:

```
sudo cp -v /usr/lib/systemd/system/tftp.service /etc/systemd/system/tftp-server.service
```

```
sudo cp -v /usr/lib/systemd/system/tftp.socket /etc/systemd/system/tftp-server.socket
```

```
sudo vi /etc/systemd/system/tftp-server.service
```

Inserir o comando acima mostrado e editei o ficheiro tal e qual como é demonstrado na figura 41:



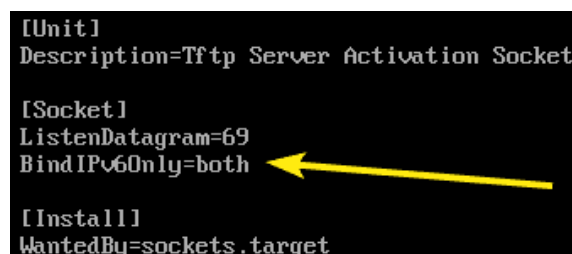
```
[Unit]
Description=Tftp Server
Requires=tftp-server.socket
Documentation=man:in.tftpd

[Service]
ExecStart=/usr/sbin/in.tftpd -c -p -s /var/lib/tftpboot
StandardInput=socket

[Install]
WantedBy=multi-user.target
Also=tftp-server.socket
```

Figura 41 – Editar o ficheiro tftp-server.service

```
sudo vi /etc/systemd/system/tftp-server.socket
```



```
[Unit]
Description=Tftp Server Activation Socket

[Socket]
ListenDatagram=69
BindIPv6Only=both

[Install]
WantedBy=sockets.target
```

Figura 42 – Editar o ficheiro tftp-server.socket

`sudo yum install polycoreutils-python` → Instalação do pacote, esse mesmo irá permitir com que qualquer máquina consiga fazer upload de ficheiros para dentro do servidor de Backups

`sudo setsebool -P tftp_anon_write 1` → Permissão de escrita ao utilizador anónimo

`sudo chmod 777 /var/lib/tftpboot` → São dadas todas as permissões para assim tornar possível que todas as máquinas consigam fazer download e upload de ficheiros

`sudo systemctl start tftp-server` → Inicialização do serviço TFTP

`sudo systemctl status tftp-server` → Comando que permite ver o estado do servidor TFTP, figura 43.

```
• tftp-server.service - Tftp Server
  Loaded: loaded (/etc/systemd/system/tftp-server.service; enabled; vendor preset: disabled)
  Active: active (running) since Sat 2022-01-29 16:22:49 WET; 14min ago
  Docs: man:in.tftpd
  Main PID: 1771 (in.tftpd)
  CGroup: /system.slice/tftp-server.service
          └─1771 /usr/sbin/in.tftpd -c -p -s /var/lib/tftpboot

Jan 29 16:22:49 localhost.localdomain systemd[1]: Started Tftp Server.
[root@localhost ~]#
```

Figura 43 – Visualizar o estado do TFTP Server o `sudo systemctl status tftp-server`

Para permitir o envio de ficheiros da máquina servidor FTP para a máquina DNS foi necessário fazer stop na firewall e depois criar os ficheiros como está na figura 45.

```
[shovon@linuxhint ~]$ sudo systemctl stop firewalld
```

Figura 44 – Parar a firewall

```
[root@localhost ~]# touch hello.txt
[root@localhost ~]# nano hello.txt
```

Figura 45 – Criar o ficheiro hello.txt

Foram aplicados os comandos da figura 46 á máquina DNS, sendo que o primeiro comando serve para inicializar o serviço TFTP sempre que a máquina iniciar, os outros comandos serviram para programar a firewall para deixar passar os pedidos ao servidor TFTP/Backups.

```
[root@localhost ~]# sudo systemctl enable tftp-server
Created symlink from /etc/systemd/system/multi-user.target.wants/tftp-server.service to /etc/systemd/system/tftp-server.service.
Created symlink from /etc/systemd/system/sockets.target.wants/tftp-server.socket to /etc/systemd/system/tftp-server.socket.
[root@localhost ~]# sudo firewall-cmd --zone=public --add-service=tftp --permanent
success
[root@localhost ~]# sudo firewall-cmd --reload
success
```

Figura 46 – Regras de firewall serviço TFTP

Depois de aplicadas todas as permissões na firewall, apenas tive de aceder á máquina FTP, aceder ao serviço TFTP, ligar o verbose e enviar o ficheiro que havia criado antes, enviando o mesmo para a máquina servidor Backup.

```
[root@localhost ~]# tftp 192.168.137.142
tftp> verbose
Verbose mode on.
tftp> put hello.txt
putting hello.txt to 192.168.137.142:hello.txt [netascii]
Sent 57 bytes in 0.0 seconds [109901 bit/s]
tftp>
```

Figura 47 – Upload do ficheiro hello.txt para a máquina servidor TFTP

Como é possível visualizar a figura 48, dá a confirmação que o ficheiro hello.txt se encontra armazenado dentro da mesma, confirmando o suceso do funcionamento do serviço TFTP.

```
[root@localhost ~]# ls /var/lib/tftpboot
hello.txt
```

Figura 48 – Confirmação do upload do ficheiro hello.txt para o servidor TFTP

## 8. Ponto 7 – Configurar o Servidor de DNS

### 8.1 Ponto 7.1 – Criação de 3 zonas master (gules.org, 300emfrente.eu e then.com)

No ponto 7 em geral apenas foram criadas as zonas e editados os ficheiros e depois foram feitos os digs para verificar o funcionamento das zonas forward no ponto 7.2 e zonas reverse no ponto 7.3. Não foi configurado nada em apache nem nenhuns virtualhosts pois tal não era pedido pelo enunciado.

Instalação do DNS (Bind) na máquina CentOS.

```
[root@localhost ~]# yum -y install bind bind-utils
```

Figura 49 – Instalação do DNS

Adicionar uma regra firewall para permitir que os clientes possam se conectar ao servidor DNS para resolução de nomes.

```
[root@localhost ~]# firewall-cmd --permanent --add-port=53/udp
success
[root@localhost ~]# firewall-cmd --reload
success
```

Figura 50 – Regras da firewall



Para configurar o DNS é necessário aceder à pasta /etc/named.conf e alterar tanto o listen-on port 53 { 127.0.0.1; any; }; e o allow-query { localhost; any; };. Deste modo estou a configurar o BIND para ficar à escuta em todos os endereços, e no allow-query é configurado todos os endereços. Ao colocar “any” no allow-query e listen-on permite que todos os endereços de todos os domínios criados nas zonas consigam ter endereços diferentes consoante aquilo que é pedido no enunciado.

```
root@localhost:~  
//  
// named.conf  
//  
// Provided by Red Hat bind package to configure the ISC BIND named(8) DNS  
// server as a caching only nameserver (as a localhost DNS resolver only).  
//  
// See /usr/share/doc/bind*/sample/ for example named configuration files.  
//  
// See the BIND Administrator's Reference Manual (ARM) for details about the  
// configuration located in /usr/share/doc/bind-{version}/Bv9ARM.html  
  
options {  
    listen-on port 53 { 127.0.0.1; any; };  
    listen-on-v6 port 53 { ::1; };  
    directory "/var/named";  
    dump-file "/var/named/data/cache_dump.db";  
    statistics-file "/var/named/data/named_stats.txt";  
    memstatistics-file "/var/named/data/named_mem_stats.txt";  
    recursing-file "/var/named/data/named.recursing";  
    secroots-file "/var/named/data/named.secroots";  
    allow-query { localhost; any; };  
  
    /*  
    - If you are building an AUTHORITATIVE DNS server, do NOT enable recursion.  
    - If you are building a RECURSIVE (caching) DNS server, you need to enable  
    recursion.  
    - If your recursive DNS server has a public IP address, you MUST enable access  
    control to limit queries to your legitimate users. Failing to do so will  
    cause your server to become part of large scale DNS amplification  
    attacks. Implementing BCP38 within your network would greatly  
    reduce such attack surface  
    */  
    recursion no;  
};
```

Figura 51 – Configuração do ficheiro named

```
zone "gules.org" IN {  
    type master;  
    file "/var/named/gules.org.db";  
    allow-update { none; };  
};  
  
zone "300emfrente.eu" IN {  
    type master;  
    file "/var/named/300emfrente.eu.db";  
    allow-update { none; };  
};  
  
zone "then.com" IN {  
    type master;  
    file "/var/named/then.com.db";  
    allow-update { none; };  
};
```

Figura 52 – Criação das zonas para o exercício 7.1 e 7.2

Depois de criadas as zonas é necessário dar restart “systemctl restart named” e enable “systemctl enable named” ao named para assim reiniciar e permitir que nas próximas sessões da máquina o serviço seja logo iniciado.

## 8.2 Ponto 7.2 – Configurar o as-smtp.300emfrente.eu para ficar responsável pelos emails dos 3 domínios

Como é possível ver na figura 53 foi necessário configurar o mail do gules.org para ser o as-smtp.300emfrente.eu e depois foram configurados os subdomínios do domínio principal gules.org “ftp, webmail”. O mesmo procedimento foi aplicado na configuração do 300emfrente.eu e no then.com como é possível ver nas figuras 54 e 55.

```
[root@localhost ~]# vi /var/named/gules.org.db
;
IN SOA      ns1.gules.org. root.gules.org. (
                                1001 ;Serial
                                3H   ;Refresh
                                15M  ;Retry
                                1W   ;Expire
                                1D   ;Minimum TTL
                                )

;Name Server Information
@      IN  NS      ns1.gules.org.

;IP address of Name Server
ns1 IN  A      192.168.137.142

;Mail exchanger
gules.org.      IN  MX 10  as-smtp.300emfrente.eu.

;A - Record HostName To IP Address
gules.org.      IN  A      8.3.2.14
ftp      IN  A      8.3.2.15
webmail  IN  A      8.3.2.16
```

Figura 53 – Configuração do gules.org.db

```
[root@localhost ~]# vi /var/named/300emfrente.eu.db
;
IN SOA      ns1.300emfrente.eu. root.300emfrente.eu. (
                                1001 ;Serial
                                3H   ;Refresh
                                15M  ;Retry
                                1W   ;Expire
                                1D   ;Minimum TTL
                                )

;Name Server Information
@      IN  NS      ns1.300emfrente.eu.

;IP address of Name Server
ns1 IN  A      192.168.137.142

;Mail exchanger
300emfrente.eu. IN  MX 10  as-smtp.300emfrente.eu.

;A - Record HostName To IP Address
300emfrente.eu. IN  A      14.21.1.14
www      IN  A      77.8.90.1
webmail  IN  A      11.21.1.16
as-smtp  IN  A      11.0.0.1
```

Figura 54 – Configuração do 300emfrente.eu.db

```

[root@localhost ~]# vi /var/named/then.com.db
;
IN SOA      ns1.then.com. root.then.com. (
                                1001    ;Serial
                                3H      ;Refresh
                                15M     ;Retry
                                1W      ;Expire
                                1D      ;Minimum TTL
                                )

;Name Server Information
@          IN  NS      ns1.then.com.

;IP address of Name Server
ns1 IN  A      192.168.137.142

;Mail exchanger
then.com. IN  MX 10    as-smtp.300emfrente.eu.

;A - Record HostName To IP Address
webmail    IN  A      194.168.22.16

@          IN  A      191.200.22.14

ftp        IN  A      92.147.45.1

```

Figura 55 – Configuração do then.com.db

Nas figuras 56, 57 e 58 foram feitos os digs aos domínios + MX, o mx faz referência ao domínio de emails, domínio esse que tem de resultar no domínio as-smtp.300emfrente.eu pois foi este que ficou responsável por receber mails dos 3 domínios.

```

[root@localhost ~]# dig 300emfrente.eu MX

; <<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.8 <<>> 300emfrente.eu MX
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 53727
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;300emfrente.eu.                IN      MX

;; ANSWER SECTION:
300emfrente.eu.                86400   IN      MX      10 as-smtp.300emfrente.eu.

;; AUTHORITY SECTION:
300emfrente.eu.                86400   IN      NS      ns1.300emfrente.eu.

;; ADDITIONAL SECTION:
as-smtp.300emfrente.eu.        86400   IN      A       11.0.0.1
ns1.300emfrente.eu.            86400   IN      A       192.168.137.142

;; Query time: 0 msec
;; SERVER: 192.168.137.142#53(192.168.137.142)
;; WHEN: Sat Jan 29 22:17:42 WET 2022
;; MSG SIZE rcvd: 117

[root@localhost ~]#

```

Figura 56 – Dig 300emfrente.eu MX

```
[root@localhost ~]# dig then.com MX

; <<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.8 <<>> then.com MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53237
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 3
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;then.com.                IN      MX

;; ANSWER SECTION:
then.com.                86400   IN      MX      10 as-smtp.300emfrente.eu.

;; AUTHORITY SECTION:
then.com.                86400   IN      NS      ns1.then.com.

;; ADDITIONAL SECTION:
as-smtp.300emfrente.eu. 86400   IN      A       11.0.0.1
ns1.then.com.            86400   IN      A       192.168.137.142

;; Query time: 0 msec
;; SERVER: 192.168.137.142#53(192.168.137.142)
;; WHEN: Sun Jan 30 13:22:35 WET 2022
;; MSG SIZE rcvd: 125
```

Figura 57 – Dig then.com MX

```
[root@localhost ~]# dig gules.org MX

; <<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.8 <<>> gules.org MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 39233
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 3
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;gules.org.                IN      MX

;; ANSWER SECTION:
gules.org.                86400   IN      MX      10 as-smtp.300emfrente.eu.

;; AUTHORITY SECTION:
gules.org.                86400   IN      NS      ns1.gules.org.

;; ADDITIONAL SECTION:
as-smtp.300emfrente.eu. 86400   IN      A       11.0.0.1
ns1.gules.org.            86400   IN      A       192.168.137.142

;; Query time: 0 msec
;; SERVER: 192.168.137.142#53(192.168.137.142)
;; WHEN: Sun Jan 30 13:31:45 WET 2022
;; MSG SIZE rcvd: 126
```

Figura 58 – Dig gules.org MX

### 8.3 Ponto 7.3 – Criação das zonas reverse do domínio then.com

Como é possível visualizar foram criadas as zonas reverse respetivamente para o then.com “14.22.200.191” , ftp.then.com “1.45.147.92” e webmail.then.com “16.22.168.194”.

```
zone "14.22.200.191.in-addr.arpa" IN {
    type master;
    file "/var/named/14.22.200.191.db";
    allow-update { none; };
};

zone "1.45.147.92.in-addr.arpa" IN {
    type master;
    file "/var/named/1.45.147.92.db";
    allow-update { none; };
};

zone "16.22.168.194.in-addr.arpa" IN {
    type master;
    file "/var/named/16.22.168.194.db";
    allow-update { none; };
};
```

Figura 59 – Criação das zonas para o exercício 7.3

Nas figuras 60, 61 e 62 foram respetivamente configuradas as zonas reverse para o domínio then.com, ftp.then.com e para o webmail.then.com.

```
[root@localhost ~]# vi /var/named/14.22.200.191.db
@ IN SOA      ns1.then.com. root.then.com. (
                                1001    ;Serial
                                3H      ;Refresh
                                15M     ;Retry
                                1W      ;Expire
                                1D      ;Minimum TTL
                                )

;Name Server Information
@ IN NS       ns1.then.com.

;PTR Record IP address to HostName
@ IN PTR      then.com.
```

Figura 60 – Configuração do 14.22.200.191.db

```
[root@localhost ~]# vi /var/named/1.45.147.92.db
;
      IN      SOA      ns1.ftp.then.com. root.ftp.then.com. (
                                1001      ;Serial
                                3H        ;Refresh
                                15M       ;Retry
                                1W        ;Expire
                                1D        ;Minimum TTL
                                )

;Name Server Information
@ IN NS      ns1.then.com.

;PTR Record IP address to HostName
@ IN PTR     ftp.then.com.
```

Figura 61 – Configuração do 1.45.147.92.db

```
[root@localhost ~]# vi /var/named/16.22.168.194.db
;
      IN      SOA      ns1.webmail.then.com. root.webmail.then.com. (
                                1001      ;Serial
                                3H        ;Refresh
                                15M       ;Retry
                                1W        ;Expire
                                1D        ;Minimum TTL
                                )

;Name Server Information
@ IN NS      ns1.then.com.

;PTR Record IP address to HostName
@ IN PTR     webmail.then.com.
```

Figura 62 – Configuração do 16.22.168.194.db

Nas figuras 63 ,64, 65 foram respetivamente feitos os digs aos endereços 191.200.22.14 “then.com”, 92.147.45.1 “ftp.then.com” e 194.168.22.16 “webmail.then.com”, dando o resultado esperado.

```
[root@localhost ~]# dig -x 191.200.22.14

; <<>> Dig 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.8 <<>> -x 191.200.22.14
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19285
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;14.22.200.191.in-addr.arpa.      IN      PTR

;; ANSWER SECTION:
14.22.200.191.in-addr.arpa. 86400 IN    PTR    then.com.

;; AUTHORITY SECTION:
14.22.200.191.in-addr.arpa. 86400 IN    NS     ns1.then.com.

;; ADDITIONAL SECTION:
ns1.then.com.               86400 IN    A      192.168.137.142

;; Query time: 0 msec
;; SERVER: 192.168.137.142#53(192.168.137.142)
;; WHEN: Sat Jan 29 22:29:11 WET 2022
;; MSG SIZE rcvd: 111
```

Figura 63 – Dig -x 191.200.22.14

```
[root@localhost ~]# dig -x 92.147.45.1

; <<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.8 <<>> -x 92.147.45.1
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29997
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;1.45.147.92.in-addr.arpa.      IN      PTR

;; ANSWER SECTION:
1.45.147.92.in-addr.arpa. 86400 IN      PTR      ftp.then.com.

;; AUTHORITY SECTION:
1.45.147.92.in-addr.arpa. 86400 IN      NS       ns1.then.com.

;; ADDITIONAL SECTION:
ns1.then.com.             86400 IN      A        192.168.137.142

;; Query time: 0 msec
;; SERVER: 192.168.137.142#53(192.168.137.142)
;; WHEN: Sat Jan 29 22:28:31 WET 2022
;; MSG SIZE rcvd: 113
```

Figura 64 – Dig -x 92.147.45.1

```
[root@localhost ~]# dig -x 194.168.22.16

; <<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.8 <<>> -x 194.168.22.16
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 37077
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;16.22.168.194.in-addr.arpa.    IN      PTR

;; ANSWER SECTION:
16.22.168.194.in-addr.arpa. 86400 IN      PTR      webmail.then.com.

;; AUTHORITY SECTION:
16.22.168.194.in-addr.arpa. 86400 IN      NS       ns1.then.com.

;; ADDITIONAL SECTION:
ns1.then.com.             86400 IN      A        192.168.137.142

;; Query time: 0 msec
;; SERVER: 192.168.137.142#53(192.168.137.142)
;; WHEN: Sun Jan 30 19:04:38 WET 2022
;; MSG SIZE rcvd: 119

[root@localhost ~]#
```

Figura 65 – Dig -x 194.168.22.16

## 9. Ponto 8.1/8.2 – Criação 3 domínios no Servidor DNS e aplicação das configurações pedidas

No ponto 8 foram criados 3 domínios allow.org, circle360.pt, festas.pt e respetivos VirtualHosts nas portas tcp 25000 e 28000, assim como as suas respetivas páginas .html.

Instalação dos pacotes do Apache mais precisamente do serviço de httpd, como é possível verificar foi aplicado o comando `sudo yum install httpd`.

```
[root@localhost ~]# sudo yum install httpd
```

Figura 66 – Instalação dos pacotes httpd no servidor DNS

Depois da instalação concluída o comando `sudo systemctl enable/start httpd` é aplicado para habilitar e iniciar o serviço apache, depois foram inseridos os devidos comandos para abrir as portas necessárias dos serviços http e https e por fim foram aplicados os comandos necessários para inicializar o Apache.

```
[root@localhost ~]# sudo systemctl enable httpd
Created symlink from /etc/systemd/system/multi-user.target.wants/httpd.service to /usr/lib/systemd/system/httpd.service.
[root@localhost ~]# sudo systemctl start httpd
[root@localhost ~]# sudo firewall-cmd --permanent --zone=public --add-service=http
success
[root@localhost ~]# sudo firewall-cmd --permanent --zone=public --add-service=https
success
[root@localhost ~]# sudo firewall-cmd --reload
success
[root@localhost ~]# sudo systemctl stop httpd
[root@localhost ~]# sudo systemctl start httpd
[root@localhost ~]# sudo systemctl restart httpd
[root@localhost ~]# sudo systemctl reload httpd
[root@localhost ~]# sudo systemctl disable httpd
Removed symlink /etc/systemd/system/multi-user.target.wants/httpd.service.
[root@localhost ~]# sudo systemctl enable httpd
-bash: sudo: command not found
[root@localhost ~]# sudo systemctl enable httpd
Created symlink from /etc/systemd/system/multi-user.target.wants/httpd.service to /usr/lib/systemd/system/httpd.service.
[root@localhost ~]#
```

Figura 67 – Comandos para iniciar os serviços Apache



Na figura está representado a criação de todas as zonas necessárias para o exercício 8.

```
zone "allow.org" IN {  
    type master;  
    file "/var/named/allow.org.db";  
    allow-update { none; };  
};  
zone "circle360.pt" IN {  
    type master;  
    file "/var/named/circle360.pt.db";  
    allow-update { none; };  
};  
zone "festas.pt" IN {  
    type master;  
    file "/var/named/festas.pt.db";  
    allow-update { none; };  
};
```

Figura 68 – Criação das zonas para o exercício 8

É necessário ir ao ficheiro que aparece na figura 69 e mudar o Listen que está comentado para os que estão apresentados na figura 70.

```
[root@localhost ~]# vi /etc/httpd/conf/httpd.conf
```

Figura 69 – Ficheiro httpd.conf

```
Listen 192.168.137.142:25000  
Listen 192.168.137.142:28000
```

Figura 70 – Adicionar os portes pedidos no enunciado 25000 e 28000

Nas seguintes figuras irá estar demonstrado todo o passo a passo que foi necessário fazer para configurar completamente o domínio allow.org.

```
[root@localhost ~]# sudo mkdir -p /var/www/allow.org/public_html/  
[root@localhost ~]# touch /var/www/allow.org/public_html/index.html
```

Figura 71 – Criação do ficheiro html para o domínio allow.org

```
[root@localhost ~]# vi /var/www/allow.org/public_html/index.html
<!DOCTYPE html>
<html lang="en" dir="ltr">
  <head>
    <meta charset="utf-8">
    <title>Welcome to allow.org</title>
  </head>
  <body>
    <h1>Success! allow.org home page!</h1>
  </body>
</html>
```

Figura 72 – Configuração do ficheiro html para o domínio allow.org

```
[root@localhost ~]# sudo chown -R apache: /var/www/allow.org/
```

Figura 73 – Dar permissões ao domínio allow.org

```
[root@localhost ~]# vi /etc/httpd/conf.d/allow.org.conf
<VirtualHost *:25000 *:28000>
  ServerName allow.org
  ServerAlias www.allow.org
  ServerAdmin webmaster@allow.org
  DocumentRoot /var/www/allow.org/public_html

  <Directory /var/www/allow.org/public_html>
    Options -Indexes +FollowSymLinks
    AllowOverride All
  </Directory>

  ErrorLog /var/log/httpd/allow.org-error.log
  CustomLog /var/log/httpd/allow.org-access.log combined
</VirtualHost>
```

Figura 74 – Configuração do VirtualHost do domínio allow.org

```
[root@localhost ~]# vi /var/named/allow.org.db
IN SOA      ns1.allow.org. root.allow.org. (
                                1001      ;Serial
                                3H         ;Refresh
                                15M        ;Retry
                                1W         ;Expire
                                1D         ;Minimum TTL
                                )

;Name Server Information
@      IN  NS      ns1.allow.org.

;IP address of Name Server
ns1 IN  A      192.168.137.142

;A - Record HostName To IP Address
allow.org.      IN      A      192.168.137.142
```

Figura 75 – Configuração do allow.org.

Nas seguintes figuras irá estar demonstrado todo o passo a passo que foi necessário fazer para configurar completamente o domínio circle360.pt.

```
[root@localhost ~]# sudo mkdir -p /var/www/circle360.pt/public_html/  
[root@localhost ~]# touch /var/www/circle360.pt/public_html/index.html
```

Figura 76 – Criação do ficheiro html para o domínio circle360.pt

```
<!DOCTYPE html>  
<html lang="en" dir="ltr">  
  <head>  
    <meta charset="utf-8">  
    <title>Welcome to circle360.pt</title>  
  </head>  
  <body>  
    <h1>Success! circle360.pt home page!</h1>  
  </body>  
</html>
```

Figura 77 – Configuração do ficheiro html para o domínio circle360.pt

```
[root@localhost ~]# sudo chown -R apache: /var/www/circle360.pt/
```

Figura 78 – Dar permissões ao domínio circle360.pt

```
<VirtualHost *:25000 *:28000>  
  ServerName circle360.pt  
  ServerAlias www.circle360.pt  
  ServerAdmin webmaster@circle360.pt  
  DocumentRoot /var/www/circle360.pt/public_html  
  
  <Directory /var/www/circle360.pt/public_html>  
    Options -Indexes +FollowSymLinks  
    AllowOverride All  
  </Directory>  
  
  ErrorLog /var/log/httpd/circle360.pt-error.log  
  CustomLog /var/log/httpd/circle360.pt-access.log combined  
</VirtualHost>
```

Figura 79 – Configuração do VirtualHost do domínio circle360.pt

```
[root@localhost ~]# vi /var/named/circle360.pt
@ IN SOA ns1.circle360.pt. root.circle360.pt. (
                                1001 ;Serial
                                3H   ;Refresh
                                15M   ;Retry
                                1W    ;Expire
                                1D    ;Minimum TTL
                                )

;Name Server Information
@ IN NS ns1.circle360.pt.

;IP address of Name Server
ns1 IN A 192.168.137.142

;A - Record HostName To IP Address
circle360.pt. IN A 192.168.137.142
```

Figura 80 – Configuração do circle360.pt.

Nas seguintes figuras irá estar demonstrado todo o passo a passo que foi necessário fazer para configurar completamente o domínio festas.pt.

```
[root@localhost ~]# sudo mkdir -p /var/www/festas.pt/public_html/
[root@localhost ~]# touch /var/www/festas.pt/public_html/index.html
```

Figura 81 – Criação do ficheiro html para o domínio festas.pt

```
[root@localhost ~]# vi /var/www/festas.pt/public_html/index.html
<!DOCTYPE html>
<html lang="en" dir="ltr">
  <head>
    <meta charset="utf-8">
    <title>Welcome to festas.pt</title>
  </head>
  <body>
    <h1>Success! festas.pt home page!</h1>
  </body>
</html>
```

Figura 82 – Configuração do ficheiro html para o domínio festas.pt

```
[root@localhost ~]# sudo chown -R apache: /var/www/festas.pt/
```

Figura 83 – Dar permissões ao domínio festas.pt

```
[root@localhost ~]# vi /etc/httpd/conf.d/festas.pt.conf
<VirtualHost *:25000 *:28000>
    ServerName festas.pt
    ServerAlias www.festas.pt
    ServerAdmin webmaster@festas.pt
    DocumentRoot /var/www/festas.pt/public_html

    <Directory /var/www/festas.pt/public_html>
        Options -Indexes +FollowSymLinks
        AllowOverride All
    </Directory>

    ErrorLog /var/log/httpd/festas.pt-error.log
    CustomLog /var/log/httpd/festas.pt-access.log combined
</VirtualHost>
```

Figura 84 – Configuração do VirtualHost do domínio festas.pt

```
[root@localhost ~]# vi /var/named/festas.pt
@ IN SOA ns1.festas.pt. root.festas.pt. (
    1001 ;Serial
    3H ;Refresh
    15M ;Retry
    1W ;Expire
    1D ;Minimum TTL
)

;Name Server Information
@ IN NS ns1.festas.pt.

;IP address of Name Server
ns1 IN A 192.168.137.142

;A - Record HostName To IP Address
festas.pt. IN A 192.168.137.142
```

Figura 85 – Configuração do festas.pt.

Depois de efetuadas todas as configurações nos 3 domínios foi necessário fazer os comandos que aparecem na figura 86 e 87 para assim permitir a comunicação da porta 25000 e 28000 nos Virtualhosts e ativar os serviços do apache.

```
[root@localhost ~]# semanage port -m -t http_port_t -p tcp 25000
[root@localhost ~]# semanage port -m -t http_port_t -p tcp 28000
```

Figura 86 – Configuração para a porta tcp 25000 e 28000 – parte 1

```
[root@localhost ~]# sudo firewall-cmd --zone=public --add-port=25000/tcp --permanent
success
[root@localhost ~]# sudo firewall-cmd --zone=public --add-port=28000/tcp --permanent
success
[root@localhost ~]# sudo firewall-cmd --reload
[root@localhost ~]# sudo systemctl restart httpd
[root@localhost ~]# sudo systemctl start httpd
[root@localhost ~]# sudo systemctl enable httpd
```

Figura 87 – Configuração para a porta tcp 25000 e 28000 – parte 2

Depois de todos os comandos apresentados serem aplicados apenas foi necessário ir à máquina cliente e experimentar os domínios, como é possível visualizar nas figuras 88, 89e 90 todos os domínios permitem o acesso via porta TCP 25000 e 28000.

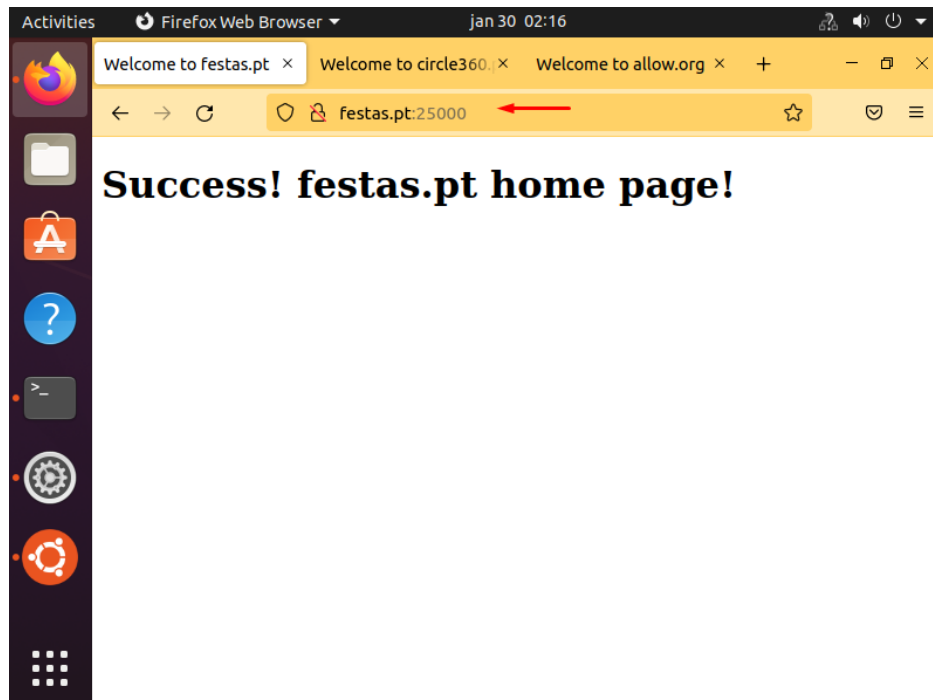


Figura 88 – Acesso ao domínio festas.pt pela porta 25000

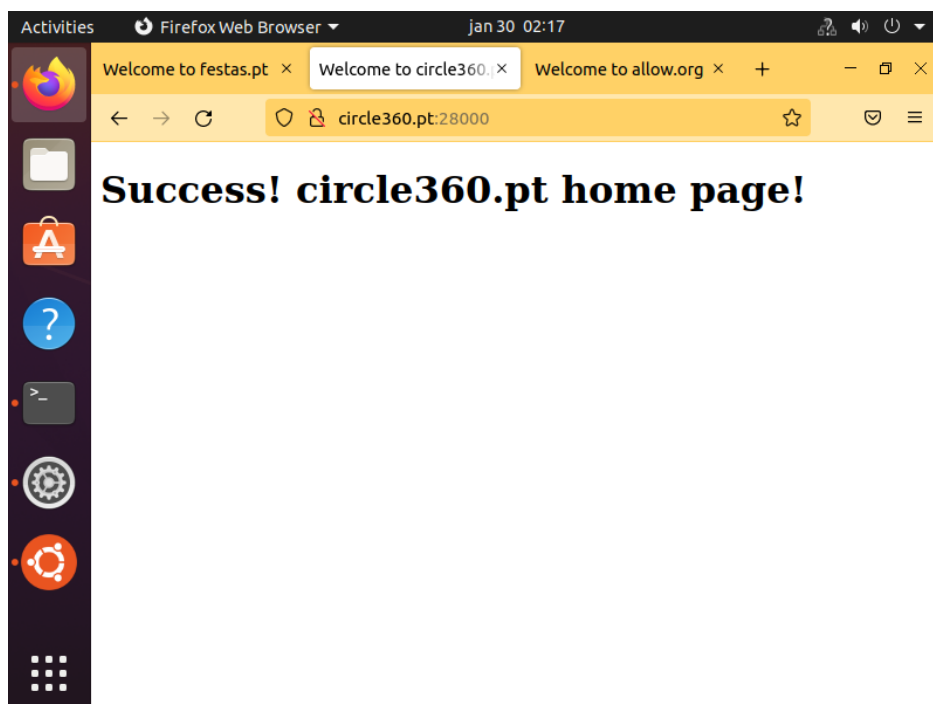


Figura 89 – Acesso ao domínio circle360.pt pela porta 28000

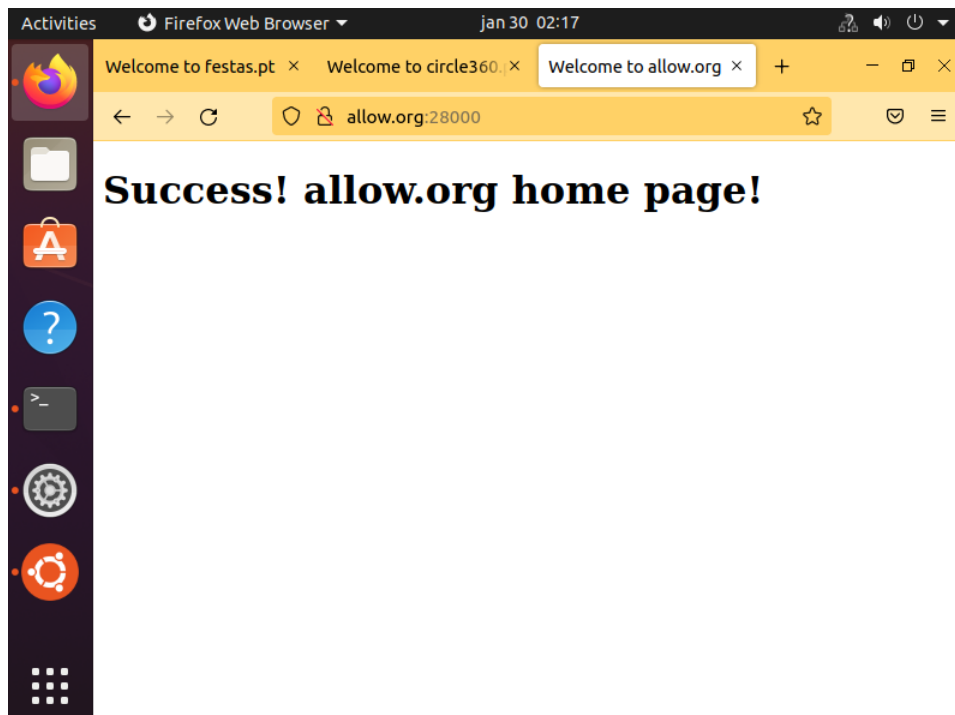


Figura 90 – Acesso ao domínio allow.org pela porta 28000

## 10. Conclusão

Inicialmente tive alguma dificuldade em configurar nomeadamente com a criação das zonas no servidor FTP no ponto 5 do trabalho, algo que consegui resolver com alguma pesquisa e tive também alguma dificuldade nomeadamente com a pergunta 7 mas felizmente foi algo que consegui ultrapassar.

Neste projeto criei uma rede com apenas 3 máquinas, 2 máquinas servidor e uma máquina cliente, numa das máquinas servidor foi configurado o FTP com vários utilizadores e o Apache, e na outra foi criado inicialmente o RAID 1 + Hotspare, configurado o DNS para a criação de vários domínios instalado o TFTP para permitir armazenar ficheiros e fazer download dos mesmo. A máquina cliente serviu para ir testando todos os serviços que eram aplicados.

Com todos estes pontos que acabei de referir quero deixar claro que este projeto foi bastante importante para desenvolver de maneira mais aprofundada o meu conhecimento, adquirir novas ferramentas de trabalho e desenvolver as minhas capacidades de resolução de problemas.