Trabalho Avaliação

Administração de Sistemas e Serviços II

Número: 46398

Nome: Redney Monteiro

Data de entrega: 30 / 06 / 2023

INDICE

INTRODUÇÃO

Neste projeto, realizamos a implementação e configuração de uma infraestrutura de tecnologias de informação para a empresa fictícia ProSysAdmin. Durante este processo, abordamos diversos serviços essenciais, tais como DNS, DHCP, servidor Web, diretoria (LDAP), serviço de correio eletrónico, mecanismos de análise de vírus e antispam, e servidor de VPN. A infraestrutura de TI implementada proporciona à empresa ProSysAdmin uma base sólida para as suas operações diárias, permitindo uma comunicação eficiente, conectividade segura e proteção dos ativos digitais. Com o serviço DNS, os colaboradores podem aceder de forma fácil e intuitiva a recursos internos e externos. O DHCP automatiza a atribuição de endereços IP, simplificando a administração e melhorando a conectividade.

O servidor Web oferece uma plataforma fiável para a hospedagem de websites e aplicações, possibilitando uma presença online eficaz. A diretoria (LDAP) centraliza a autenticação e autorização de utilizadores, facilitando a gestão de contas e garantindo a segurança dos dados. O serviço de correio eletrónico permite uma comunicação interna e externa eficiente, enquanto os mecanismos de análise de vírus e antispam protegem a rede contra ameaças cibernéticas.

Além disso, a implementação do servidor de VPN proporciona uma ligação segura para colaboradores e parceiros, independentemente da sua localização física, garantindo a confidencialidade das informações transmitidas.

TAREFAS EXECUTADAS

Tabela de endereçamento

Equipamento	Interface	Endereço/Mascara
Gateway		192.168.1.254
DNS-01		192.168.1.1
DNS-02		192.168.1.2
VPN		192.168.1.5
LDAP		192.168.1.9
EMAIL		192.168.1.10
WEB		192.168.1.250

Implementação do DNS

Configuração do hosts (/etc/hosts)

```
  GNU nano 5.4                                  /etc/hosts
127.0.0.1       localhost
127.0.1.1       DNS-01.dominio.pt       DNS-01
192.168.1.1     DNS.01.dominio.pt       DNS-01
```

Configuração do resolve (/etc/resolv.conf)

```
  GNU nano 5.4                                /etc/resolv.conf
domain dominio.pt
search dominio.pt
nameserver 192.168.1.1
nameserver 192.168.1.2
```

Configuração de IP

```
#placa da rede interna
auto enp0s3
iface enp0s3 inet static
        address 192.168.1.1
        netmask 255.255.255.0
        network 192.168.1.0
        broadcast 192.168.1.255
        gateway 192.168.1.254
```

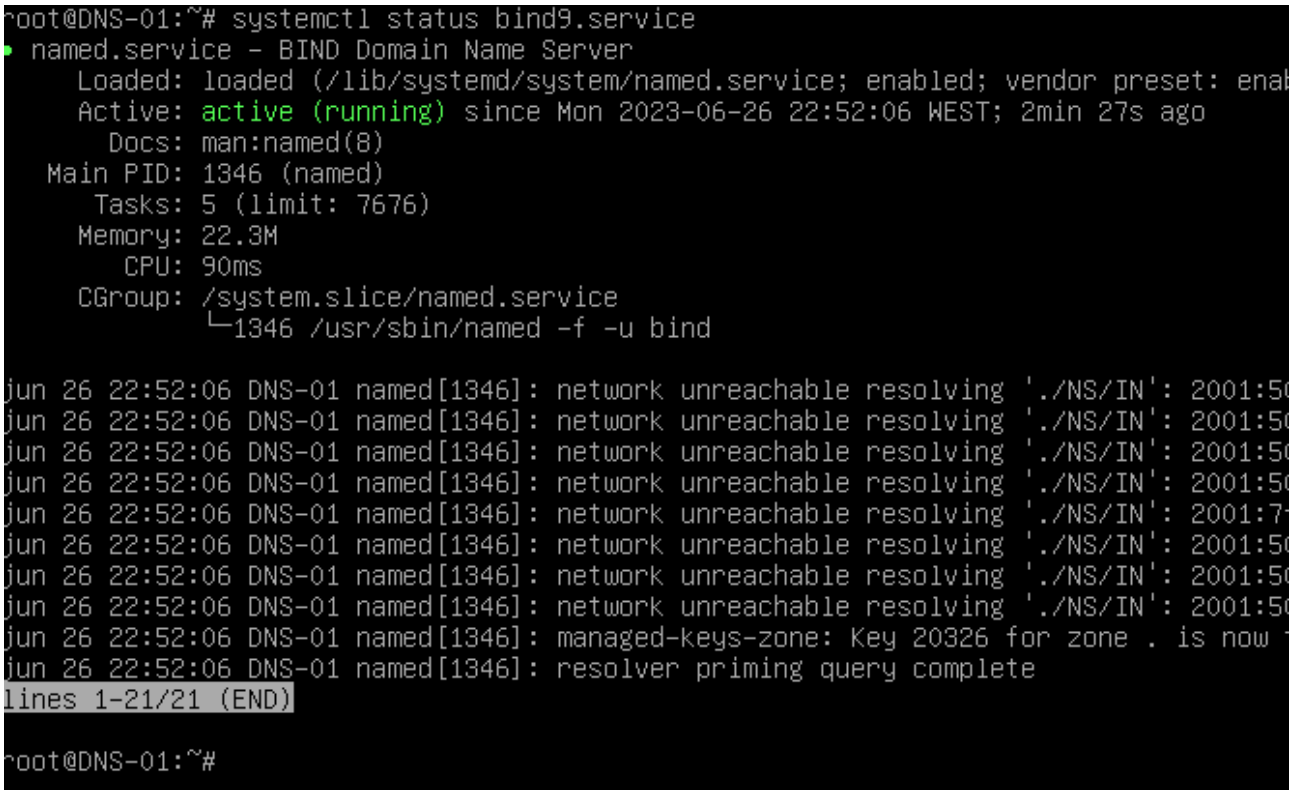
Instalação do BIND9

Antes de instalação do bind, fiz uma atualização do Sistema a fim de atualizar o meu servidor.

```
root@DNS-01:~# apt update_
```

Quando já estiver atualizado, segue para a instalação do serviço

```
root@DNS-01:~# apt install bind9
```



Ao instalar o serviço, os ficheiros de configuração estão localizados na pasta /etc/bind. Nesta pasta tem tres arquivos importante.
Além disso, existem os arquivos de zonas.
No arquivo arquivo name.conf.local, esta configurado a minha zona e a zona reserve

No arquivo db.dominio.pt, esta presente todos os meus registos para a conversão de nomes

```
  GNU nano 5.4                                    db.dominio.pt *
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     dns-01.dominio.pt. root.dominio.pt. (
                              8         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@               IN      NS      dns-01.dominio.pt.
@               IN      NS      dns-02.dominio.pt.
@               IN      A       192.168.1.1
dns-01          IN      A       192.168.1.1
dns-02          IN      A       192.168.1.2
webserver       IN      A       192.168.1.250
portal          IN      A       192.168.1.250
router          IN      A       192.168.1.254
dhcp            IN      A       192.168.1.1
vpn             IN      A       192.168.1.5
ldap            IN      A       192.168.1.9

@       MX      10      mail.dominio.pt.
mail    IN      A       192.168.1.10
@       txt     "v=spf1 a mx ~all"

mail.dominio.pt TXT     "spf1 a -all"
```

Depois configurei o arquivo db.1.168.192.rev, que contem os registo da zona reserve.

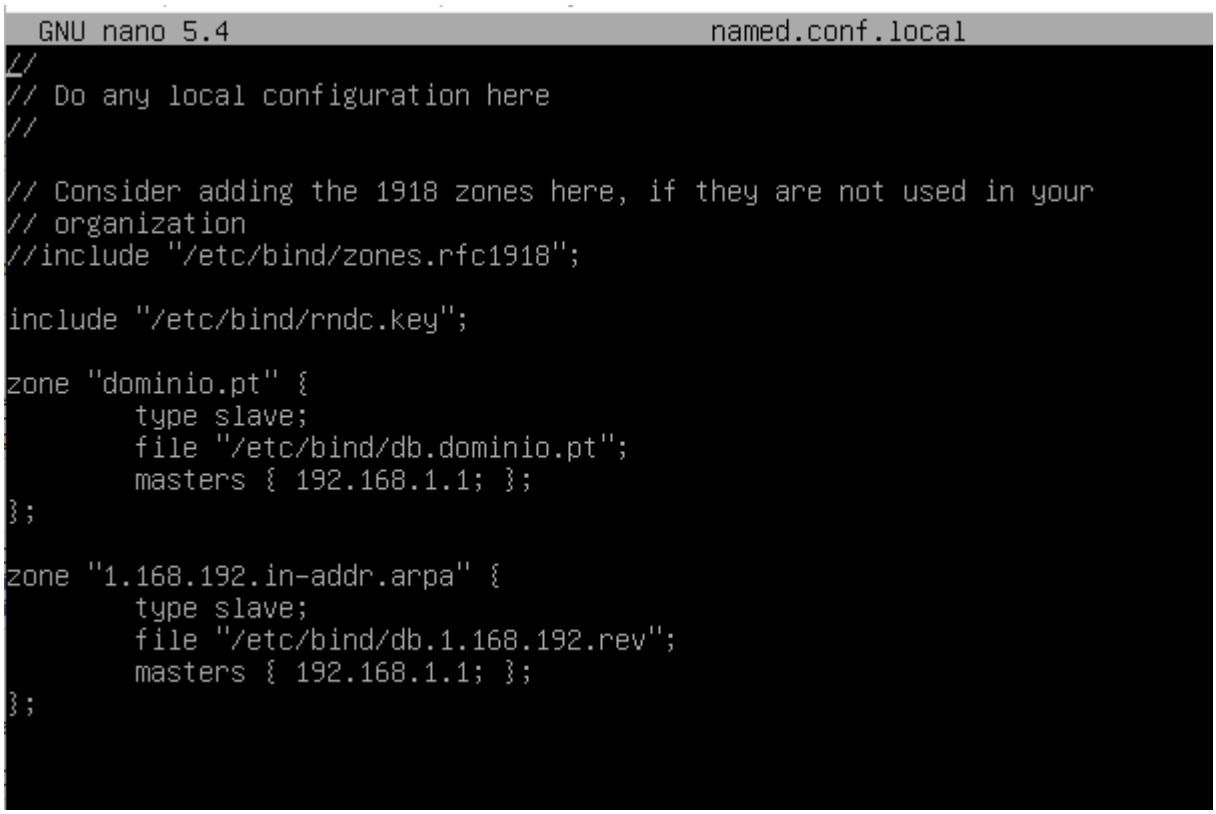
DNS secundario

Implementação

Para instalar o servidor DNS secundario, antes necessitarei de efetuar as configuraçõesbasicas, como ip, hostname, hosts e o resolve. Com isso já configurado, atualizei o servidor e instalei o BIND9:

apt update
apt install bind9

Como este servidor será destinado para backup, não se coloca nenhum registo preciso informar ao serviço que esse é o secundario (slave), logo necessita de indifcar que é o servidor primeiro a quem deve ir buscar as configuração.
Alterie o ficheiro name.conf.local, indicando quem é o master (primario) e onde vai buscar as configurações:



SERVIDOR WEB

Instalação

Antes de instalação é necessario novamente efetuar as configurações basicos, tanto o ip, o host-name, o hosts e o resolve.

Após isso, atualiza o Sistema e instala o apache. O apache é que vai ser utilizado como servidor web.

```
apt update && apt upgrade
```

Instalar o serviço de HTTP:

```
apt install apache2
```

Após isso a servidor já esta ativo e ao utlizar algum navegador podera ver uma pagina que é carregada por defeito. E esse arquivo html se encontra em /var/www. Nessa pasta criei uma outra pasta chamada dominio.pt:

E Nessa pasta criei um arquivo html, que será a pasta que vou carregar.

Para informar ao apache que vai carregar meu arquivo que criei, navegei até a pasta /etc/apache2/sites-avaliable.

Listando todos os arquivos (ls) iremos encontrar um arquivo que se chama 000-default.conf. E nesse arquivo iremos configurar.

Edita esse ficheiro de forma a ficar assim:

```
  GNU nano 5.4                                 000-default.conf
<VirtualHost *:80>
        # The ServerName directive sets the request scheme, hostname and port that
        # the server uses to identify itself. This is used when creating
        # redirection URLs. In the context of virtual hosts, the ServerName
        # specifies what hostname must appear in the request's Host: header to
        # match this virtual host. For the default virtual host (this file) this
        # value is not decisive as it is used as a last resort host regardless.
        # However, you must set it for any further virtual host explicitly.
        #ServerName www.example.com

        ServerAdmin webmaster@dominio.pt
        Servername www.dominio.pt
        ServerAlias dominio.pt  www.domain.pt


        DocumentRoot /var/www/dominio.pt

        # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
        # error, crit, alert, emerg.
        # It is also possible to configure the loglevel for particular
        # modules, e.g.
        #LogLevel info ssl:warn

        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined

        # For most configuration files from conf-available/, which are
        # enabled or disabled at a global level, it is possible to
        # include a line for only one particular virtual host. For example the
        # following line enables the CGI configuration for this host only
        # after it has been globally disabled with "a2disconf".
        #Include conf-available/serve-cgi-bin.conf
</VirtualHost>
```

Ativa/carrega o novo site:

```
a2ensite 000-default.conf_
```

Recarrega o serviço

```
systemctl reload apache2
```

Testa a configuração do site acendo ao http://www.dominio.pt

Para que seja reconhecido as pagina tilizando o nome inicial.html

```
  GNU nano 5.4                                    dir.conf *
<IfModule mod_dir.c>
        DirectoryIndex inicial.html principal.html_index.htm
</IfModule>
```

Confgração para o SSL, para conseguir responder ao HTTPS. Começa por ativar o modulo de SSL do apache:

```
root@webserver:/etc/apache2/sites-available# a2enmod ssl
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create self-signed certifica
tes.
To activate the new configuration, you need to run:
  systemctl restart apache2
```

Posiciona no diretório /etc/apache2/sites-avaliable, faz uma copia de segurança do arquivo domain.pt-ssl.conf. E edita esse arquiva, adicioando essas informações

```
  GNU nano 5.4                                  default-ssl.conf *
<IfModule mod_ssl.c>
        <VirtualHost _default_:443>
                ServerAdmin webmaster@localhost
                ServerName www.dominio.pt_
                DocumentRoot /var/www/dominio.pt
```

Criando o certificado auto assinado SSL

```
root@webserver:/etc/apache2/sites-available# openssl req -x509 -nodes -days 365 -newkey rsa:2048 -ke
yout /etc/ssl/private/dominio_crt.key -out /etc/ssl/certs/dominio_pt.crt
Generating a RSA private key
....+++++
.........+++++
writing new private key to '/etc/ssl/private/dominio_crt.key'
-----
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]:Bragança
Locality Name (eg, city) []:Mirandela
Organization Name (eg, company) [Internet Widgits Pty Ltd]:IPB-ESACT
Organizational Unit Name (eg, section) []:Trabalho
Common Name (e.g. server FQDN or YOUR name) []:www.dominio.pt
Email Address []:webmaster@dominio.pt_
```

Edita o ficheoro novamente e adiciona essas informações:

Agora é capaz de responder pedidos HTTPS

```
root@webserver:/etc/apache2/sites-available# systemctl restart apache2.service
root@webserver:/etc/apache2/sites-available# systemctl status apache2.service
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
     Active: active (running) since Tue 2023-06-27 22:11:55 WEST; 8s ago
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 1055 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 1059 (apache2)
      Tasks: 6 (limit: 7661)
     Memory: 11.7M
        CPU: 507ms
     CGroup: /system.slice/apache2.service
             ├─1059 /usr/sbin/apache2 -k start
             ├─1060 /usr/sbin/apache2 -k start
             ├─1061 /usr/sbin/apache2 -k start
             ├─1062 /usr/sbin/apache2 -k start
             ├─1063 /usr/sbin/apache2 -k start
             └─1064 /usr/sbin/apache2 -k start

jun 27 22:11:54 webserver systemd[1]: Starting The Apache HTTP Server...
jun 27 22:11:55 webserver systemd[1]: Started The Apache HTTP Server.
root@webserver:/etc/apache2/sites-available#
```

Criando um outro web site (portal.dominio.pt)

Para criar um outro web site (portal.dominio.pt) é feita utilizando a mesma forma do site dominio.pt. Faz uma copia do copia 000-default.conf e edita com as informações do seu site
Para criar um novo site com base em acesso através do nome (name-based) e configurar um novo VirtualHost, siga as seguintes etapas:

Posicione-se no diretório `/var/www/` e crie um novo diretório chamado `portal.dominio.pt`. Cria um ficeiro index.php e escreve algum codig PHP

```
*cd /var/www/*
*mkdir portal.domain.pt*
*cp www.domain.pt/index.html portal.domain.pt/*
*nano portal.domain.pt/index.html*
```

Faça uma cópia do arquivo `000-default.conf` com o nome `portal.domain.pt.conf`: Edite o arquivo `portal.domain.pt.conf` com as seguintes configurações:

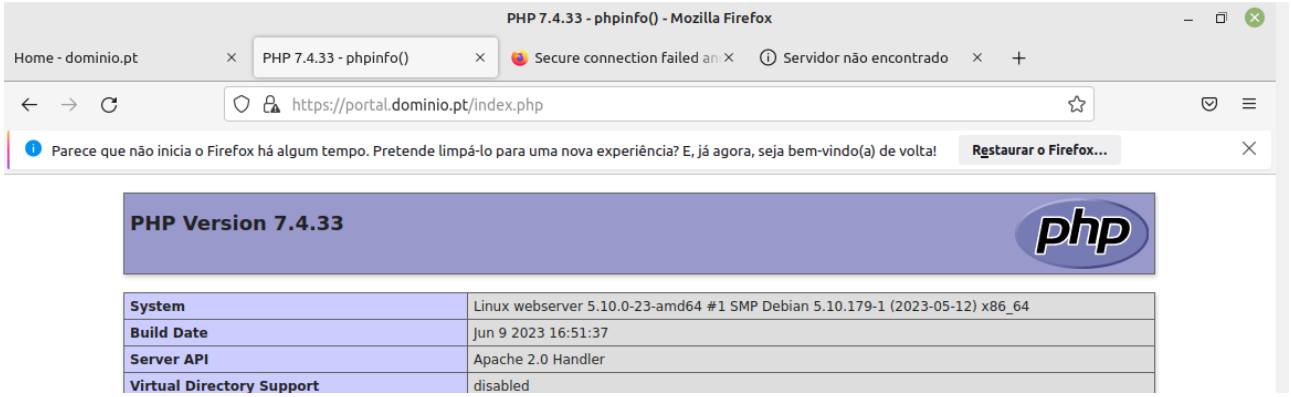
```
*<VirtualHost *:80>*
   *ServerAdmin webmaster@dominio.pt*
   *Servername portal.dominio.pt*
   *DocumentRoot /var/www/portal.dominio.pt*
   *ErrorLog ${APACHE_LOG_DIR}/error-portal.domain.pt.log*
   *LogLevel warn*
   *CustomLog ${APACHE_LOG_DIR}/access-portal.dominio.pt.log combined*
*</VirtualHost>*
```

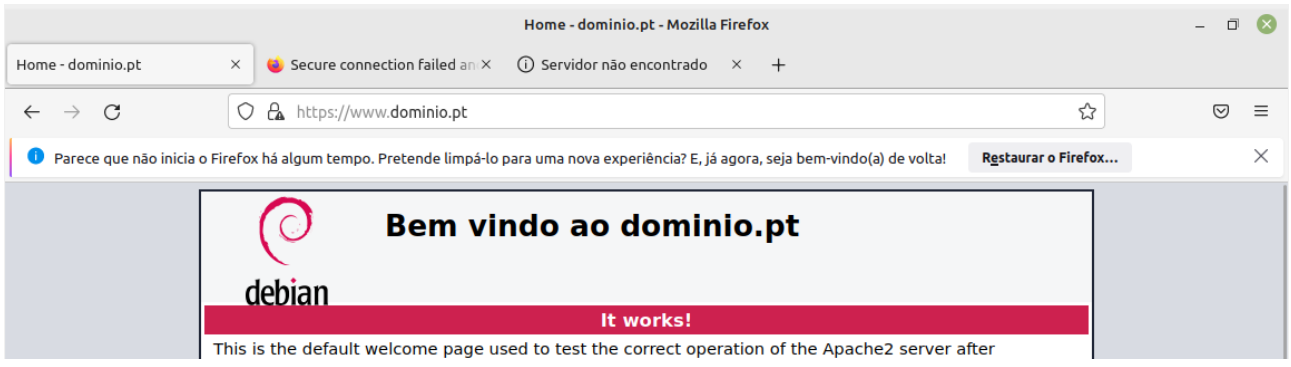
Ative o site utilizando o comando `a2ensite` e, em seguida, faça o reload do serviço Apache

Para habilitar o ssl faz o mesmo processo. Criando um novo certificado para esse website

```
Jun 28 12:19:17 webserver systemd[1]: Started The Apache HTTP Server.
root@webserver:/etc/apache2/sites-available# openssl req -x509 -nodes -days 365 -newkey rsa:2048 -ke
yout /etc/ssl/private/portal_dominio_crt.key -out /etc/ssl/certs/portal_dominio_pt.crt
Generating a RSA private key
.................................+++++
...................+++++
writing new private key to '/etc/ssl/private/portal_dominio_crt.key'
-----
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]:Bragança
Locality Name (eg, city) []:Mirandela
Organization Name (eg, company) [Internet Widgits Pty Ltd]:IPB-ESACT
Organizational Unit Name (eg, section) []:Trabalho
Common Name (e.g. server FQDN or YOUR name) []:portal.dominio.pt
Email Address []:webmaster@dominio.pt
root@webserver:/etc/apache2/sites-available#
```

Acedendo ao website





PAGINA PARA UTILIZADOR

Adicionar user

```
root@webserver:/etc/apache2/sites-available# adduser carlos
A adicionar o utilizador `carlos' ...
A adicionar o novo grupo `carlos' (1001) ...
A adicionar o novo utilizador `carlos' (1001) com grupo `carlos' ...
A criar directório home `/home/carlos' ...
A copiar ficheiros de `/etc/skel' ...
Nova palavra-passe:
Digite novamente a nova palavra-passe:
passwd: a palavra-passe foi actualizada com sucesso
A alterar a informação de utilizador de carlos
Introduza o novo valor, ou carregue em ENTER para o valor pré-definido
        Nome Completo []: Carlos
        Número da Sala []:
        Telefone do Emprego []:
        Telefone de Casa []:
        Outra Informação []:
Esta informação é correcta? [Y/n] s
root@webserver:/etc/apache2/sites-available# _
```

Posicione-se na pasta pessoal do utilizador recém-criado e crie o diretório "public_html":

```
root@webserver:/etc/apache2/sites-available# cd /home/carlos/
root@webserver:/home/carlos# mkdir public_html
```

Configure as permissões do utilizador sobre o diretório/pasta "public_html":

```
root@webserver:/home/carlos# chown carlos. -R public_html/
root@webserver:/home/carlos# _
```

Verifique se o módulo "userdir" está disponível e carregue-o:

```
root@webserver:/home/carlos# ls /etc/apache2/mods-available/userdir.*
/etc/apache2/mods-available/userdir.conf  /etc/apache2/mods-available/userdir.load
root@webserver:/home/carlos# _
```

Certifique-se de que aparecem dois ficheiros: "userdir.conf" e "userdir.load". Caso não estejam habilitados, execute o seguinte comando para ativá-los:

```
root@webserver:/home/carlos# a2enmod userdir
Enabling module userdir.
To activate the new configuration, you need to run:
  systemctl restart apache2
root@webserver:/home/carlos#
```

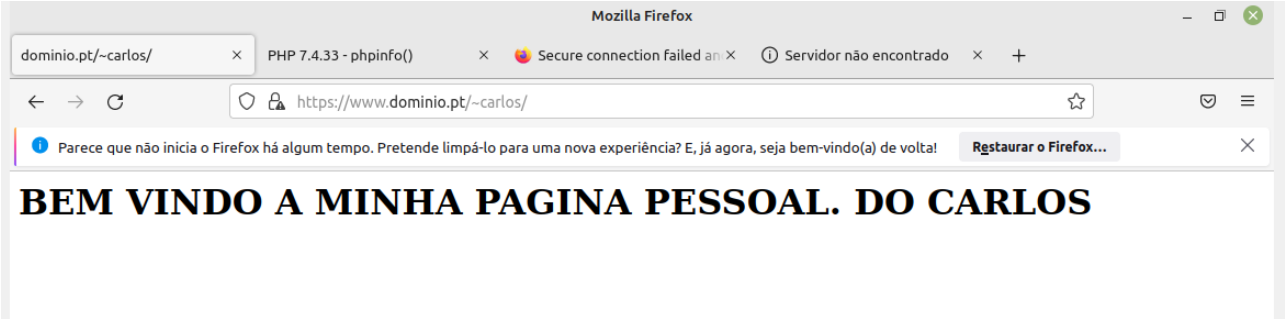
Opcionalmente, se pretender habilitar o PHP nas páginas pessoais dos utilizadores, execute os seguintes passos: Abra o ficheiro de configuração do PHP:

```
root@webserver:/home/carlos# nano /etc/apache2/mods-available/php7.4.conf
```

Comente as seguintes linhas, adicionando o caractere "#" no início de cada linha:

```
# (from <IfModule ...> to </IfModule>.) Do NOT set it to On
# prevents .htaccess files from disabling it.
#<IfModule mod_userdir.c>
#    <Directory /home/*/public_html>
#        php_admin_flag engine Off
#    </Directory>
#</IfModule>
```

Acedendo a pasta personalizado do utilizador

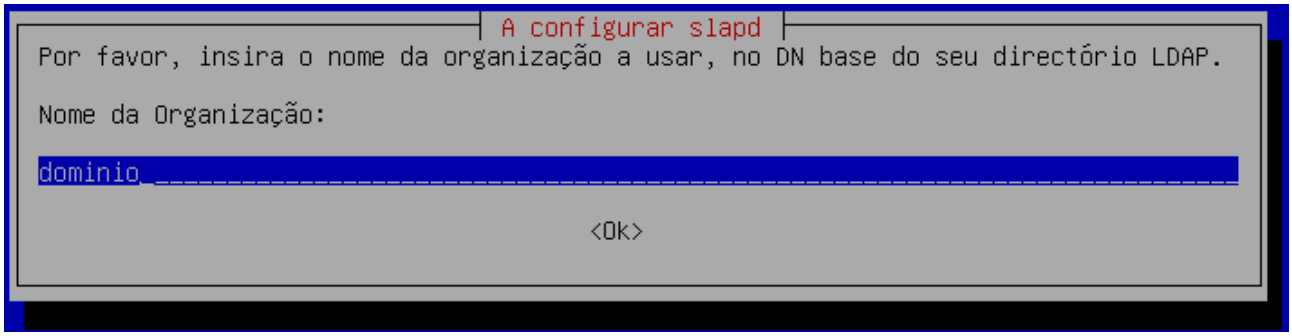


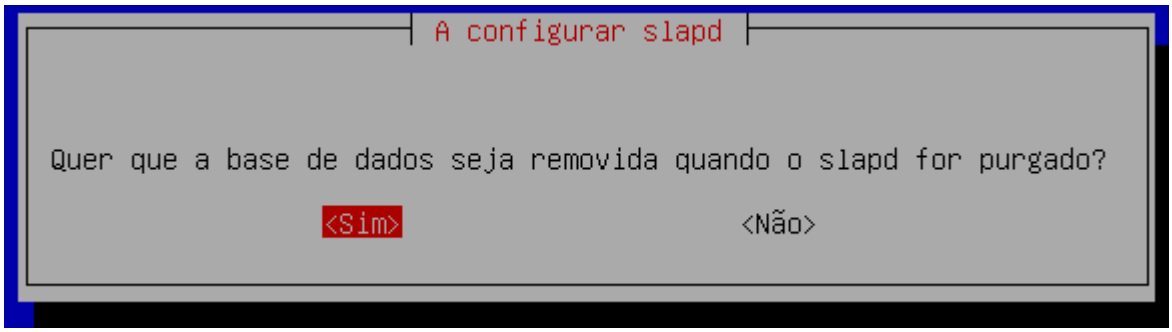

```
root@webserver:/# mkdir /srv/ftp/download
root@webserver:/# mkdir /srv/ftp/upload
root@webserver:/#
```

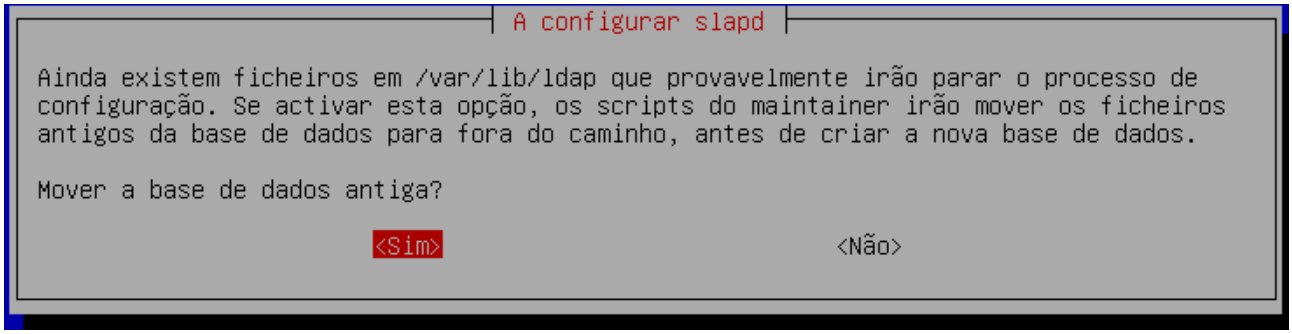
Servidor LDAP

Instalação do LDAP

```
apt-get install slapd ldap-utils
```







No final para verificar os dados execute o comando:

```
root@ldap:~# slapcat
dn: dc=dominio,dc=pt
objectClass: top
objectClass: dcObject
objectClass: organization
o: dominio
dc: dominio
structuralObjectClass: organization
entryUUID: 94f9c458-aa0d-103d-87e4-9f8ab61a9e55
creatorsName: cn=admin,dc=dominio,dc=pt
createTimestamp: 20230628144116Z
entryCSN: 20230628144116.503912Z#000000#000#000000
modifiersName: cn=admin,dc=dominio,dc=pt
modifyTimestamp: 20230628144116Z

root@ldap:~# _
```

Cria um ficeiro backend.dominio.pt.ldif e adicionar o seguinte codigo

para adicionarmos o ficheiro LDIF à diretoria:

```
root@ldap:/etc/ldap# ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/ldap/schema/backend.dominio.pt.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
ldapadd: attributeDescription "dn": (possible missing newline after line 7, entry "cn=module,cn=conf
ig"?)
adding new entry "cn=module,cn=config"
ldap_add: Undefined attribute type (17)
        additional info: objectClpt: attribute type undefined

root@ldap:/etc/ldap# _
```

Para criar uma senha encriptada para o utilizador "admin" utilizando o utilitário slappasswd, você pode seguir as instruções a seguir:

```
root@ldap:/etc/ldap# slappasswd -h {SSHA}
New password:
Re-enter new password:
{SSHA}wPEPRicEWLhEhDOHEpXI7eNUPF8SVeou
root@ldap:/etc/ldap# _
```

Depois criar os ficheiros e adiciona a diretoria

- unidadesOrg.ldif

```
root@ldap:/etc/ldap/schema# ldapadd -x -D cn=admin,dc=dominio,dc=pt -W -f unidade-sOrg.ldif
Enter LDAP Password:
adding new entry "ou=utilizadores,dc=dominio,dc=pt"

adding new entry "ou=grupos,dc=dominio,dc=pt"

adding new entry "ou=computadores,dc=dominio,dc=pt"
```

- computadores

```
root@ldap:/etc/ldap/schema# ldapadd -x -D cn=admin,dc=dominio,dc=pt -W -f computadores.ldif
Enter LDAP Password:
adding new entry "cn=desktops,ou=computadores,dc=dominio,dc=pt"
ldap_add: Undefined attribute type (17)
        additional info: objectClpt: attribute type undefined

root@ldap:/etc/ldap/schema#
```

- grupos.ldif

- user.ldif

Efetuando alguns de testes. Pesquisando e outras operações

```
root@ldap:/etc/ldap/schema# ldapsearch -x LLL -b "dc=dominio,dc=pt" "out=*"
# extended LDIF
#
# LDAPv3
# base <dc=dominio,dc=pt> with scope subtree
# filter: (objectclass=*)
# requesting: LLL out=*
#

# dominio.pt
dn: dc=dominio,dc=pt

# utilizadores, dominio.pt
dn: ou=utilizadores,dc=dominio,dc=pt

# grupos, dominio.pt
dn: ou=grupos,dc=dominio,dc=pt

# computadores, dominio.pt
dn: ou=computadores,dc=dominio,dc=pt

# search result
search: 2
result: 0 Success

# numResponses: 5
# numEntries: 4
```

```
root@ldap:/etc/ldap/schema# ldapsearch -xLLL -b 'dc=dominio,dc=pt' user.ldif
dn: dc=dominio,dc=pt

dn: ou=utilizadores,dc=dominio,dc=pt

dn: ou=grupos,dc=dominio,dc=pt

dn: ou=computadores,dc=dominio,dc=pt

dn: cn=alunos,ou=grupos,dc=dominio,dc=pt

dn: cn=professores,ou=grupos,dc=dominio,dc=pt

dn: uid=luis,ou=utilizadores,dc=dominio,dc=pt

dn: uid=ana,ou=utilizadores,dc=dominio,dc=pt

dn: uid=mariana,ou=utilizadores,dc=dominio,dc=pt

dn: uid=redney,ou=utilizadores,dc=dominio,dc=pt

root@ldap:/etc/ldap/schema#
```

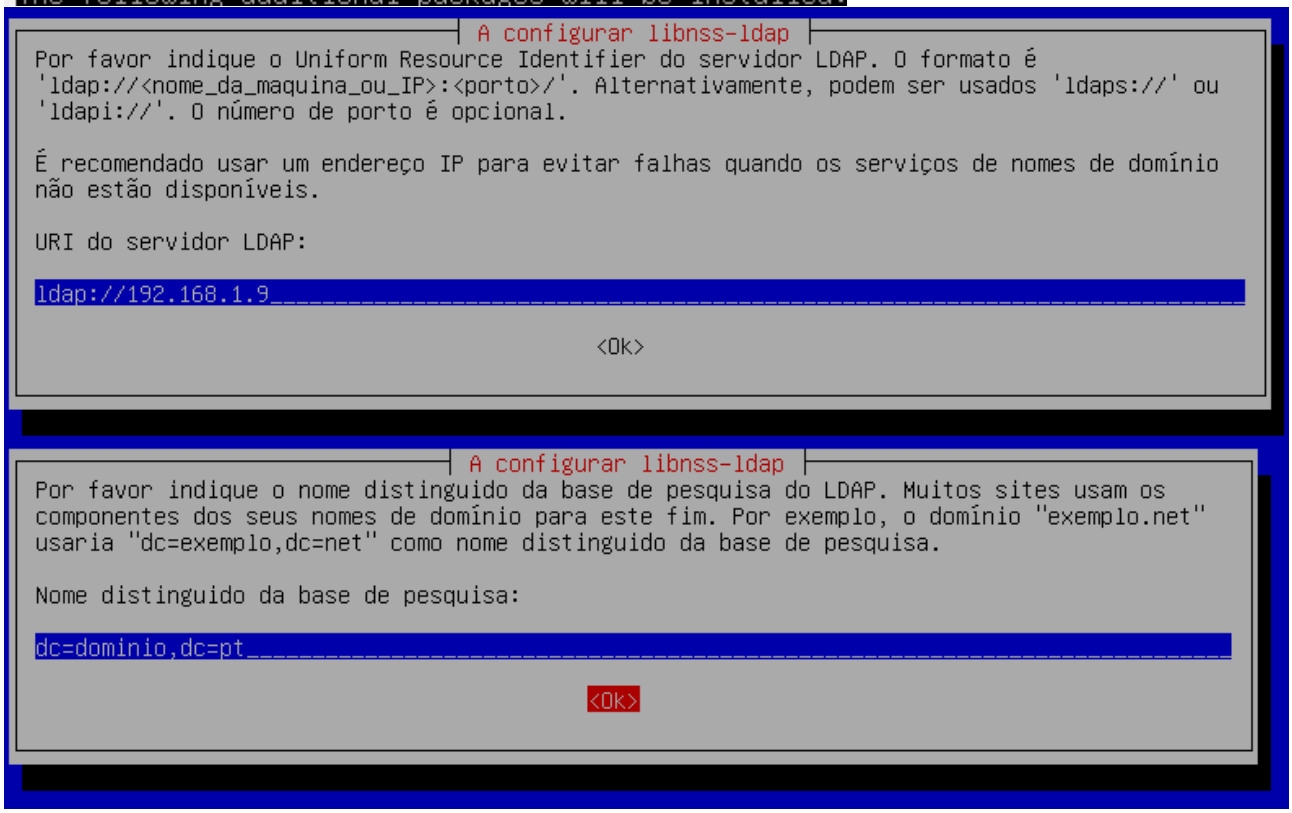
```
root@ldap:/etc/ldap/schema# ldapsearch -xLLL -b 'dc=dominio,dc=pt' uid=redney sn givenName cn
dn: uid=redney,ou=utilizadores,dc=dominio,dc=pt
sn: Monteiro
givenName: Redney
cn: Redney

root@ldap:/etc/ldap/schema# _
```

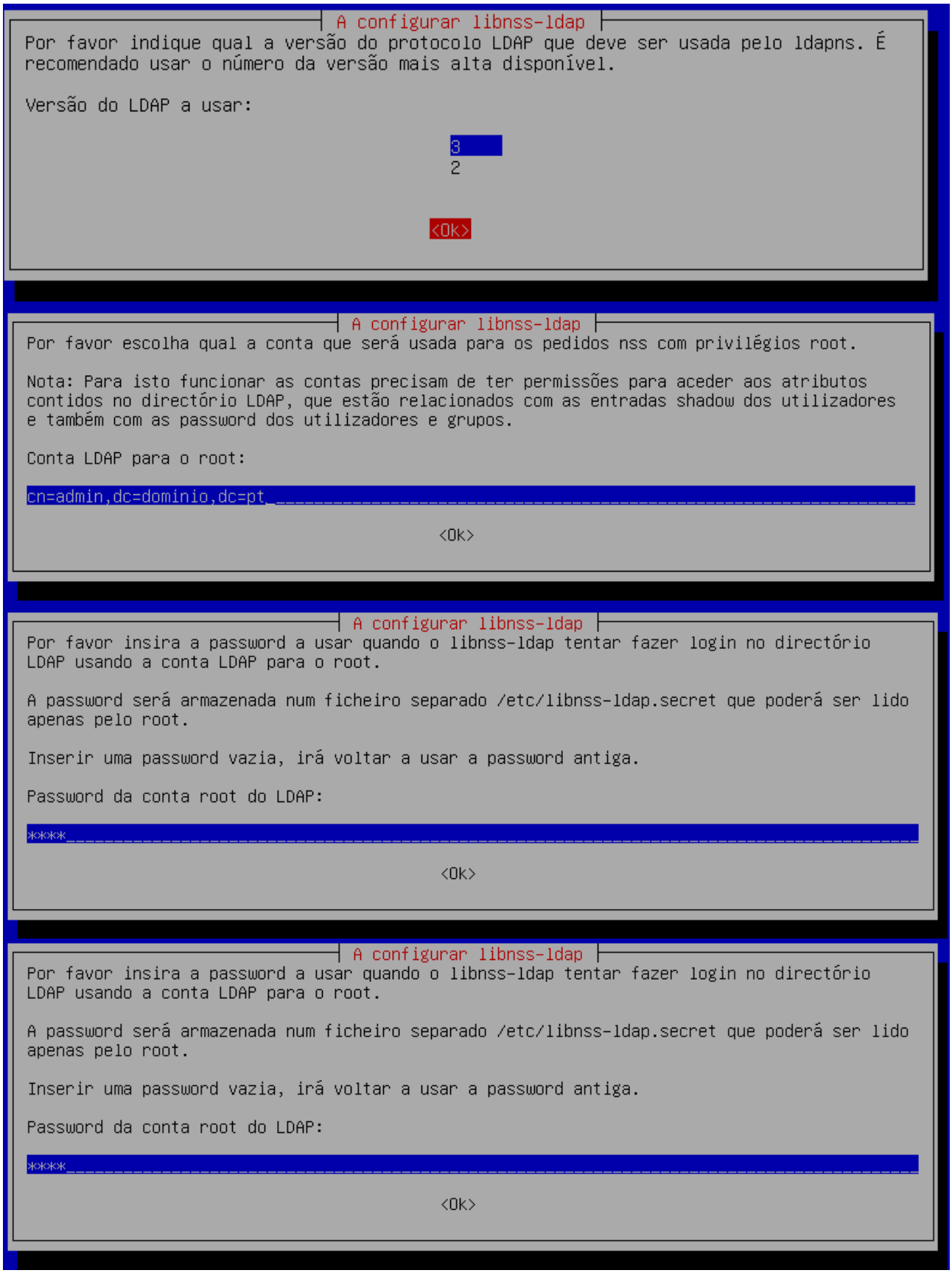
```
root@ldap:/etc/ldap/schema# ldapdelete -x -v -W uid=luis,ou=utilizadores,dc=dominio,dc=pt -D  cn=adm
in,dc=dominio,dc=pt
ldap_initialize( <DEFAULT> )
Enter LDAP Password:
deleting entry "uid=luis,ou=utilizadores,dc=dominio,dc=pt"
root@ldap:/etc/ldap/schema#
```

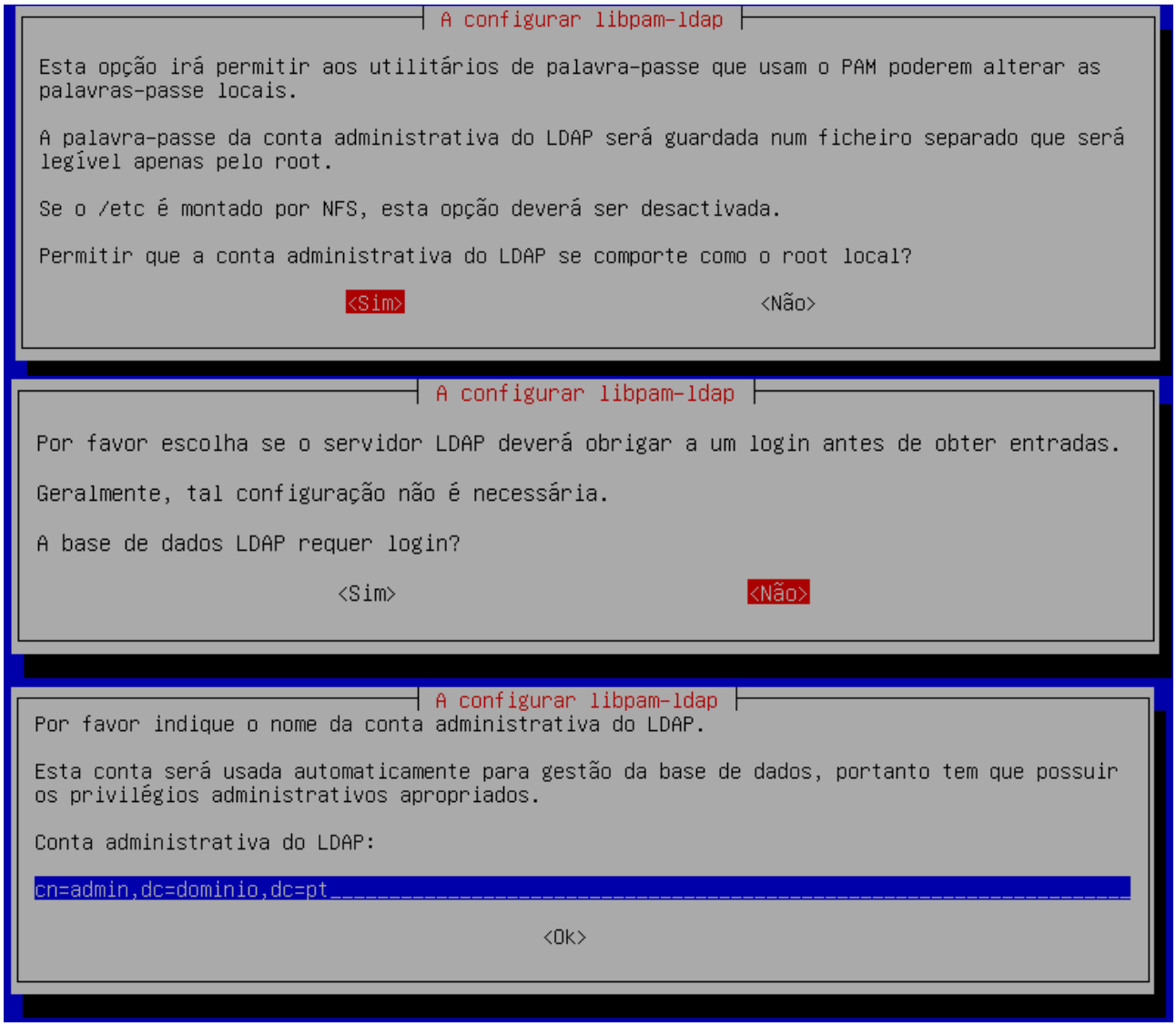
No cliente ldap instala o serviço.
Instalar o ldap cliente

```
root@clente:~# apt install ldap-client
A ler as listas de pacotes... Pronto
A construir árvore de dependências... Pronto
A ler a informação de estado... Pronto
Note, a seleccionar 'ldap-utils' em vez de 'ldap-client'
Pacotes sugeridos:
```

```
root@clente:~# apt install libpam-ldap libnss-ldap
A ler as listas de pacotes... Pronto
A construir árvore de dependências... Pronto
A ler a informação de estado... Pronto
The following additional packages will be installed:
```




A configurar libnss-ldap
Por favor indique qual a versão do protocolo LDAP que deve ser usada pelo ldapns. É recomendado usar o número da versão mais alta disponível.
Versão do LDAP a usar:
3
2
<Ok>
A configurar libnss-ldap
Por favor escolha qual a conta que será usada para os pedidos nss com privilégios root.
Nota: Para isto funcionar as contas precisam de ter permissões para aceder aos atributos contidos no directório LDAP, que estão relacionados com as entradas shadow dos utilizadores e também com as password dos utilizadores e grupos.
Conta LDAP para o root:
cn=admin,dc=dominio,dc=pt
<Ok>
A configurar libnss-ldap
Por favor insira a password a usar quando o libnss-ldap tentar fazer login no directório LDAP usando a conta LDAP para o root.
A password será armazenada num ficheiro separado /etc/libnss-ldap.secret que poderá ser lido apenas pelo root.
Inserir uma password vazia, irá voltar a usar a password antiga.
Password da conta root do LDAP:
****
<Ok>
A configurar libnss-ldap
Por favor insira a password a usar quando o libnss-ldap tentar fazer login no directório LDAP usando a conta LDAP para o root.
A password será armazenada num ficheiro separado /etc/libnss-ldap.secret que poderá ser lido apenas pelo root.
Inserir uma password vazia, irá voltar a usar a password antiga.
Password da conta root do LDAP:
****
<Ok>



Navega até nano /etc/nsswitch.conf e edita esse feicheiro.

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

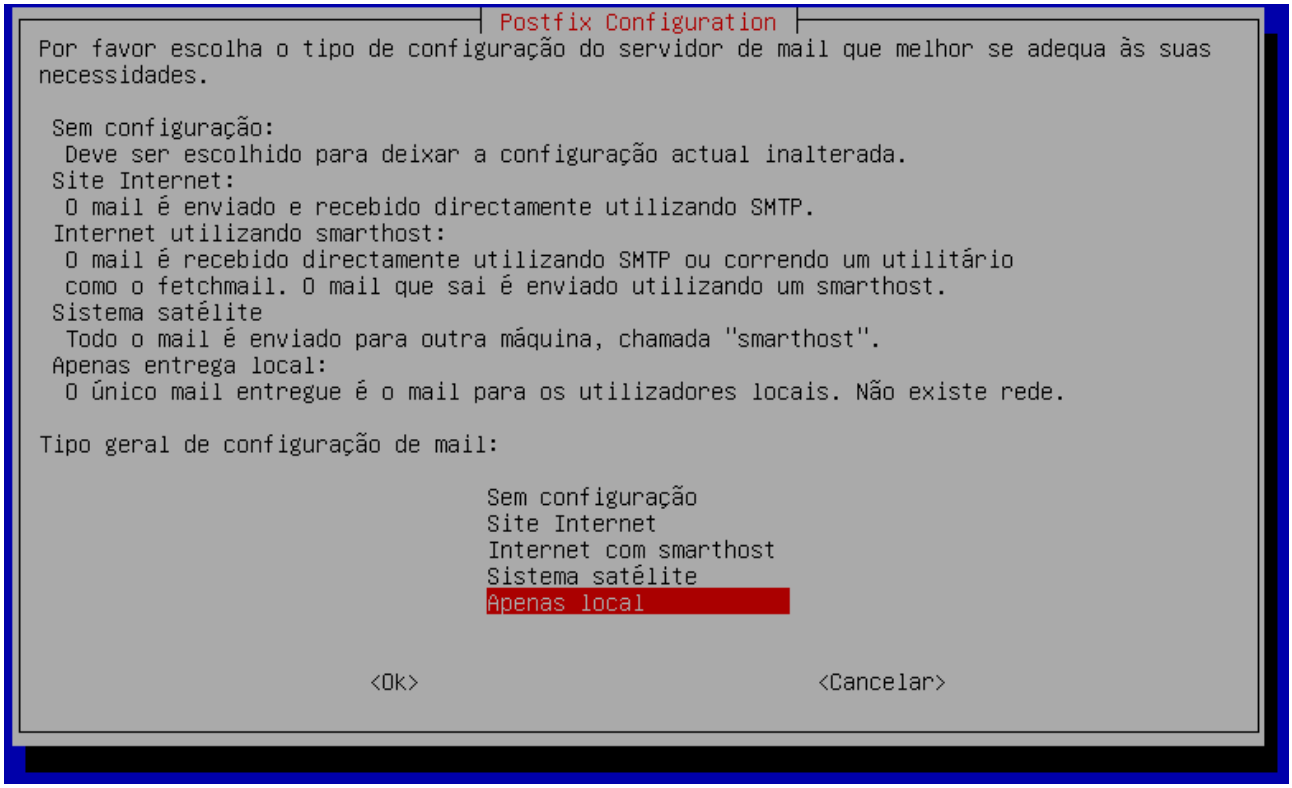
```
Last login: Tue Feb 28 10:39:50 WET 2023 on tty1
redney@clente:~$ getent passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-network:x:101:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:102:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:109::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:104:110:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
avahi-autoipd:x:105:113:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
sshd:x:106:65534::/run/sshd:/usr/sbin/nologin
redney:x:1000:1000:redney,,,:/home/redney:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
bind:x:107:114::/var/cache/bind:/usr/sbin/nologin
carlos:x:2001:10001:Carlos Silva[LDAP]:/home/carlos:/bin/bash
mariana:x:1001:10001:Redney Monteiro[LDAP]:/home/mariana:/bin/bash
redney:x:10001:10001:Redney Monteiro[LDAP]:/home/redney:/bin/bash
redney@clente:~$ _
```

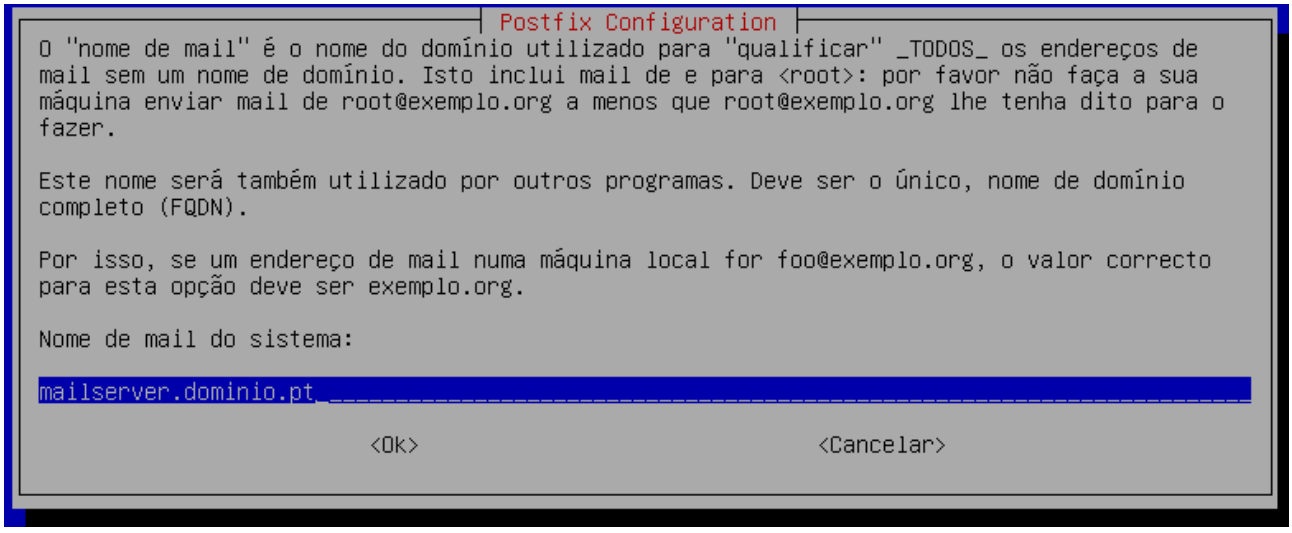
Testando

```
root@clente:~# ldapsearch -h 192.168.1.9 -x ou=utilizadores -b dc=dominio,dc=pt
# extended LDIF
#
# LDAPv3
# base <dc=dominio,dc=pt> with scope subtree
# filter: ou=utilizadores
# requesting: ALL
#

# utilizadores, dominio.pt
dn: ou=utilizadores,dc=dominio,dc=pt
objectClass: organizationalUnit
ou: utilizadores

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
root@clente:~# _
```

Instalação

```
# apt-get install postfix ssl-cert
```





Navega para o ficheiro /etc/postfix. Lá tem dois ficheiros de configuração, o main.cf e o master.cf. No arquivo main.cf deve estar assim, caso forneca as informação no ato da instalação.

```
smtpd_relay_restrictions = permit_mynetworks permit_sasl_authenticated defer_unauth_destination
myhostname = mail.dominio.pt
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
myorigin = /etc/mailname
mydestination =
relayhost =
mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1] 192.168.1.10
mailbox_size_limit = 10000000
inet_interfaces = all
inet_protocols = all
inet_protocols = all
home_mailbox = Maildir/
```

Verifica se existe erro

```
postconf -n
```

Reinicia o serviço do postfix

Testa o serviço na porta 25

```
telnet localhost 25
```

Instalação do dovecot (IMAP, POP3 e LMTP)

```
apt install dovecot-core dovecot-imapd dovecot-pop3d dovecot-lmtpd
```

Testa o serviço na porta 110 (POP3) ou na 143 (IMAP)

```
telnet localhost 110
```

Na diretoria /etc/dovecot/conf.d/10-master.conf, edita o ficheiro e adiciona essas informações:

```
  # Postfix smtp-auth
  unix_listener /var/spool/postfix/private/auth {
    mode = 0666
    user = postfix
    group = postfix
  }
```

```
service lmtp {
        unix_listener /var/spool/postfix/private/dovecot-lmtp {
                mode = 0600
                user = postfix
                group = postfix
        }
}
```

NA mesma diretoria /etc/dovecot/conf.d/. Tem um ficheiro de configuraçã 10-mail.conf, adiicona essas informações

```
mail_location = maildir:~/Maildir
  (...)
mail_privileged_group = mail
```

Adiciona o user dovecot ap grupo mail

```
adduser dovecot mail
```

Para a autenticação no dovecot adiciona essas informações:

```
disable_plaintext_auth = yes

auth_mechanisms = plain login

auth_username_format = %n
```

Para ofecer mais segurança utilizamos o mecanismo de SSL.
Criar certificados
Cria uma pasta em /etc/postfix/ssl e entra nesse diretorio. E gere os certificados

```
openssl genrsa -des3 -out smtpd.key 2048
openssl rsa -in smtpd.key -out smtpd.key.insecure
chmod 600 smtpd.key.insecure
mv smtpd.key smptd.key.secure
mv smtpd.key.insecure smtpd.key
openssl req -new -key smtpd.key -out smtpd.csr
openssl x509 -req -days 365 -in smtpd.csr -signkey smtpd.key
-out smtpd.crt


mv smtpd.key /etc/ssl/private/
mv smtpd.crt /etc/ssl/certs/
```

Ao gerar os certificados, entra no arquivo localizado em /etc/dovecot/conf.d/10-ssl.conf e adiciona essas informações:

```
# SSL/TLS support: yes, no, required. <doc/wiki/SSL.txt>
ssl = required

# PEM encoded X.509 SSL/TLS certificate and private key. They're opened before
# dropping root privileges, so keep the key file unreadable by anyone but
# root. Included doc/mkcert.sh can be used to easily generate self-signed
# certificate, just make sure to update the domains in dovecot-openssl.cnf
ssl_cert = </etc/ssl/certs/smtpd.crt
ssl_key = </etc/ssl/private/smtpd.key
```

Para habilitar a porta 587 e o SASL
Entra no ficheiros main.cf

```
nano /etc/postfix/main.cf
```

edita o ficheiro

```
### Configuração TLS ###
### Ativar Encriptação TLS Encryption quando Postfix recebe emails (entrada) #
smtpd_tls_cert_file=/etc/ssl/certs/smtpd.crt
smtpd_tls_key_file=/etc/ssl/private/smtpd.key
smtpd_tls_security_level=may
smtpd_tls_loglevel = 1
smtpd_tls_session_cache_database = btree:${data_directory}/smtpd_scache
###Ativa Encriptação TLS Encryption quando Postfix envia email(de saída) ###
smtp_tls_security_level = may
smtp_tls_loglevel = 1
smtp_tls_session_cache_database = btree:${data_directory}/smtp_scache
```

```
smtpd_sasl_type = dovecot
smtpd_sasl_path = private/auth
smtpd_sasl_local_domain =
smtpd_sasl_security_options = noanonymous,noplaintext
smtpd_sasl_tls_security_options = noanonymous
broken_sasl_auth_clients = yes
smtpd_sasl_auth_enable = yes
smtpd_recipient_restrictions = permit_sasl_authenticated,
permit_mynetworks,
reject_unauth_destination
```

Descomenta essas linhas do ficheiro /etc/postfix/master.cf

```
# ==========================================================================
smtp      inet  n       -       y       -       -       smtpd
#smtp      inet  n       -       y       -       1       postscreen
#smtpd     pass  -       -       y       -       -       smtpd
#dnsblog   unix  -       -       y       -       0       dnsblog
#tlsproxy  unix  -       -       y       -       0       tlsproxy
submission inet n       -       y       -       -       smtpd
  -o syslog_name=postfix/submission
  -o smtpd_tls_security_level=encrypt
  -o smtpd_sasl_auth_enable=yes
  -o smtpd_tls_auth_only=yes
  -o content_filter=smtp-amavis:[127.0.0.1]:10026
#  -o smtpd_reject_unlisted_recipient=no
```

Com as alterações feitas, faz um restart ou um reload do serviço e testa o correio eletronico.

Para ver mensagens enviadas aos logs em termpo real

```
tail -f /var/log/mail.log
```

Mecanismo de scan virus e antispam

No servidor de mail instala o serviço

```
apt-get install amavisd-new clamav-daemon

 apt-get install pyzor razor

 apt install arc arj bzip2 cabextract cpio lhasa lzop no-
 march p7zip-full pax rpm tnef unrar-free rar unzip zip
```

Adicione o utilizador "clamav" ao grupo "amavis" para garantir as permissões adequadas:

```
adduser clamav amavis
adduser amavis clamav
```

Reinicie o serviço ClamAV para utilizar a versão mais recente:

```
systemctl restart clamav-daemon
```

Configure o Postfix para direcionar os emails para o Amavisd. Abra o ficheiro /etc/postfix/master.cf e adicione as seguintes configurações no final do ficheiro:

```
  GNU nano 5.4                          /etc/postfix/master.cf
smtp-amavis   unix   -   -   n   -   2   smtp
    -o syslog_name=postfix/amavis
    -o smtp_data_done_timeout=1200
    -o smtp_send_xforward_command=yes
    -o disable_dns_lookups=yes
    -o max_use=20
    -o smtp_tls_security_level=none


127.0.0.1:10025   inet   n    -     n     -     -    smtpd
    -o syslog_name=postfix/10025
    -o content_filter=
    -o mynetworks_style=host
    -o mynetworks=127.0.0.0/8
    -o local_recipient_maps=
    -o relay_recipient_maps=
    -o strict_rfc821_envelopes=yes
    -o smtp_tls_security_level=none
    -o smtpd_tls_security_level=none
    -o smtpd_restriction_classes=
    -o smtpd_delay_reject=no
    -o smtpd_client_restrictions=permit_mynetworks,reject
    -o smtpd_helo_restrictions=
    -o smtpd_sender_restrictions=
    -o smtpd_recipient_restrictions=permit_mynetworks,reject
    -o smtpd_end_of_data_restrictions=
    -o smtpd_error_sleep_time=0
    -o smtpd_soft_error_limit=1001
    -o smtpd_hard_error_limit=1000
    -o smtpd_client_connection_count_limit=0
    -o smtpd_client_connection_rate_limit=0
    -o receive_override_options=no_header_body_checks,no_unknown_recipient_checks,no_address_mappin>
```

Adicione as seguintes linhas no final do ficheiro /etc/postfix/main.cf para ativar o filtro do Amavisd:

```
smtpd_milters = local:(....),local:spamass/spamass.sock
non_smtpd_milters = $smtpd_milters



content_filter = smtp-amavis:[127.0.0.1]:10024
smtpd_proxy_options = speed_adjust
```

Reinicie o serviço Postfix

Instalação do SpamAssasim

Instale o SpamAssassin executando o seguinte comando:

```
apt install spamassassin
```

2. Edite o arquivo `/etc/default/spamassassin` e altere as opções `ENABLED` e `CRON` da seguinte maneira:

```
ENABLED=1 (está opção no Debian 10 já não é necessária)

CRON=1
```

Reinicie o serviço SpamAssassin:

Ative a filtragem de spam e antivírus no Amavisd-new. Edite o arquivo `/etc/amavis/conf.d/15-content_filter_mode` e faça as seguintes alterações:

Descomente as linhas abaixo para ativar a verificação de antivírus:
```
@bypass_virus_checks_maps = (
  \%bypass_virus_checks, \@bypass_virus_checks_acl, \$bypass_virus_checks_re);
```

Descomente as linhas abaixo para ativar a verificação de spam:
```
@bypass_spam_checks_maps = (
  \%bypass_spam_checks, \@bypass_spam_checks_acl, \$bypass_spam_checks_re);
```

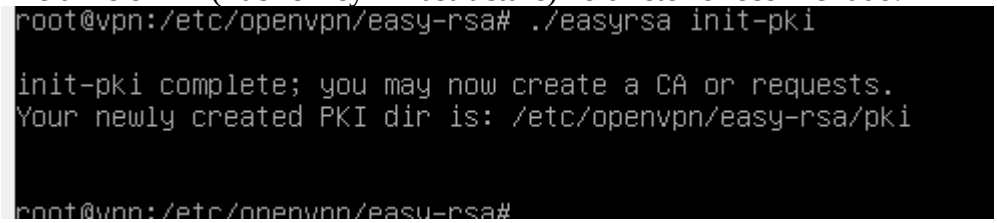
Configure a ação a ser tomada com as mensagens marcadas como spam. Edite o arquivo `/etc/amavis/conf.d/20-debian_defaults` e altere a seguinte linha para descartar a mensagem:
```
$final_spam_destiny = D_DISCARD;
```

Ajuste as opções de marcação de mensagens spam, se necessário. No mesmo arquivo `/etc/amavis/conf.d/20-debian_defaults`, você pode alterar as seguintes variáveis de acordo com suas preferências:
```
$sa_tag_level_deflt = -999;  # adiciona cabeçalhos de informações de spam
$sa_tag2_level_deflt = 6.0;  # adiciona cabeçalhos de "spam detectado"
$sa_kill_level_deflt = 21.0; # aciona ações evasivas contra spam
$sa_dsn_cutoff_level = 4;    # nível de spam além do qual um DSN não é enviado
```

7. Se o nome do servidor for diferente do registro MX ou se o servidor receber emails para vários domínios, você precisará configurar a opção `$myhostname`. Edite o arquivo `/etc/amavis/conf.d/50-user` e faça as alterações necessárias. Por exemplo:
```
$myhostname = 'mail.dominio.pt;
@local_domains_acl = ("dominio.pt");
```

8. Reinicie o serviço Amavisd-new para aplicar as alterações:

```
```

systemctl restart amavis
```

Funcionamento:


Servidor VPN

**Instalação do OPENVPN**

```
apt-get install openvpn easy-rsa
```

Extrai o ficheiro server.conf e edita-o.

```
gunzip -c /usr/share/doc/openvpn/examples/sample-config-fi-
les/server.conf.gz > /etc/openvpn/server.conf
```

Configuração dos certificados

Copie o diretório Easy-RSA para a pasta do OpenVPN:

```
cp -r /usr/share/easy-rsa/ /etc/openvpn/
```

Crie um link simbólico para os arquivos do Easy-RSA:

```
ln -s /usr/share/easy-rsa/* /etc/openvpn/easy-rsa/
```

Inicialize o PKI (Public Key Infrastructure) no diretório recém-criado:



Criação da Autoridade Certificadora (CA):
```

```
root@vpn:/etc/openvpn/easy-rsa# ./easyrsa build-ca nopass
Using SSL: openssl OpenSSL 1.1.1n  15 Mar 2022
Generating RSA private key, 2048 bit long modulus (2 primes)
.....................+++++
.........................................+++++
e is 65537 (0x010001)
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.
-----
Common Name (eg: your user, host, or server name) [Easy-RSA CA]:PT

CA creation complete and you may now import and sign cert requests.
Your new CA certificate file for publishing is at:
/etc/openvpn/easy-rsa/pki/ca.crt


root@vpn:/etc/openvpn/easy-rsa# _
```

Verifique a criação dos arquivos:

```
root@vpn:/etc/openvpn/easy-rsa# cd pki/
root@vpn:/etc/openvpn/easy-rsa/pki# ls private/
ca.key
root@vpn:/etc/openvpn/easy-rsa/pki# _
```

Criação da chave do servidor OpenVPN:

```
root@vpn:/etc/openvpn/easy-rsa#
root@vpn:/etc/openvpn/easy-rsa# ./easyrsa build-server-full vpn_server nopass
Using SSL: openssl OpenSSL 1.1.1n  15 Mar 2022
Generating a RSA private key
.........+++++
.................................+++++
writing new private key to '/etc/openvpn/easy-rsa/pki/easy-rsa-14878.9n8TjV/tmp.4u5i7F'
-----
Using configuration from /etc/openvpn/easy-rsa/pki/easy-rsa-14878.9n8TjV/tmp.u3N4mm
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName            :ASN.1 12:'vpn_server'
Certificate is to be certified until Oct  1 16:28:57 2025 GMT (825 days)

Write out database with 1 new entries
Data Base Updated

root@vpn:/etc/openvpn/easy-rsa# _
```

Criando um TLS crypt v2:

```
root@vpn:/etc/openvpn/easy-rsa/pki# openvpn --tls-crypt-v2 private/vpn_server.pem --genkey tls-crypt
-v2-client private/redney.pem
root@vpn:/etc/openvpn/easy-rsa/pki# _
```

Verifique se o arquivo vpn_server.key foi criado:

```
root@vpn:/etc/openvpn/easy-rsa# ls pki/private/
ca.key  vpn_server.key
root@vpn:/etc/openvpn/easy-rsa#
```

Verifique também que foi criado um certificado para o servidor (vpn_server.crt):

```
root@vpn:/etc/openvpn/easy-rsa# ls pki/issued/
vpn_server.crt
root@vpn:/etc/openvpn/easy-rsa#
```

Assinatura do certificado do servidor OpenVPN:

```
root@vpn:/etc/openvpn/easy-rsa# ./easyrsa sign-req server vpn_server
Using SSL: openssl OpenSSL 1.1.1n  15 Mar 2022


You are about to sign the following certificate.
Please check over the details shown below for accuracy. Note that this request
has not been cryptographically verified. Please be sure it came from a trusted
source or that you have verified the request checksum with the sender.

Request subject, to be signed as a server certificate for 825 days:

subject=
    commonName                = vpn_server


Type the word 'yes' to continue, or any other input to abort.
  Confirm request details: yes
Using configuration from /etc/openvpn/easy-rsa/pki/easy-rsa-14969.OnOkxi/tmp.jPHZLY
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName            :ASN.1 12:'vpn_server'
Certificate is to be certified until Oct  1 16:32:04 2025 GMT (825 days)

Write out database with 1 new entries
Data Base Updated

Certificate created at: /etc/openvpn/easy-rsa/pki/issued/vpn_server.crt


root@vpn:/etc/openvpn/easy-rsa# _
```

Geração dos parâmetros Diffie-Hellman (DH):

```
cd /etc/openvpn/easy-rsa/
./easyrsa gen-dh
```

Criação do TLS Crypt v2 para o OpenVPN:

```
root@vpn:/etc/openvpn/easy-rsa# cd pki/
root@vpn:/etc/openvpn/easy-rsa/pki# openvpn --genkey tls-crypt-v2-server private/vpn_server.pem
root@vpn:/etc/openvpn/easy-rsa/pki# ls /private/
root@vpn:/etc/openvpn/easy-rsa/pki# ls private/
ca.key  vpn_server.key  vpn_server.pem
root@vpn:/etc/openvpn/easy-rsa/pki#
```

Criar o ficheiro /etc/openvpn/server.conf e edita-o
Copiando os arquivos para a pasta /etc/openvpn/server:

```
root@vpn:/etc/openvpn/easy-rsa# cp pki/ca.crt /etc/openvpn/
root@vpn:/etc/openvpn/easy-rsa# cp pki/private/vpn_server.key /etc/openvpn/
root@vpn:/etc/openvpn/easy-rsa# cp pki/issued/vpn_server.crt /etc/openvpn/
root@vpn:/etc/openvpn/easy-rsa# cp pki/private/vpn_server.pem /etc/openvpn/
root@vpn:/etc/openvpn/easy-rsa# cp pki/dh.pem /etc/openvpn/
```

Criar um diretria paraguardar as chaves do cliente (/etc/openvpn/client/redeny/)
Copia os certificados do cliente redeny

```
root@vpn:/etc/openvpn/easy-rsa/pki# cp ca.crt /etc/openvpn/client/redney/
root@vpn:/etc/openvpn/easy-rsa/pki# cp issued/redney.crt /etc/openvpn/client/redney/
root@vpn:/etc/openvpn/easy-rsa/pki# cp private/redney.key /etc/openvpn/client/redney/
root@vpn:/etc/openvpn/easy-rsa/pki# cp private/redney.pem /etc/openvpn/client/redney/
root@vpn:/etc/openvpn/easy-rsa/pki# _
```

Cria um ficheiro em /etc/openvpn/client/redeny e edita-o:

```
#VPN port
port 1194

#VPN over UDP
proto udp

# "dev tun" will create a routed IP tunnel
dev tun

ca ca.crt
cert vpn_server.crt
key vpn_server.key
tls-crypt-v2 vpn_server.pem
dh dh.pem

#network for the VPN
server 10.8.0.0 255.255.255.0

push "redirect-gateway autolocal"

# Maintain a record of client <-> virtual IP address

# associations in this file.
ifconfig-pool-persist /var/log/openvpn/ipp.txt

# Ping every 10 seconds and assume client is down if
# it receives no response in 120 seconds.
keepalive 10 120

#cryptographic cipher
cipher AES-256-GCM

#avoid accessing certain resources on restart
persist-key
persist-tun

#log of current connections
status /var/log/openvpn/openvpn-status.log

#log verbose level (0-9)
verb 4

# Notify the client when the server restarts
explicit-exit-notify 1
```

Altera as permisões e executa esse ficheiro

Usar o arquivo preconfigurado
cp /usr/share/doc/openvpn/examples/sample-config-files/client.conf /etc/openvpn/clientes_vpn/redney/cliente.ovpn

Dentro do arquivo cliente.ovpn, edite a linha remote 192.168.1.1 1194 para refletir o DNS correto.

No Cliente
Instala o openvpn e habilita o ssh na porta 22

Transferir arquivos para o cliente

```
scp /etc/openvpn/clientes_vpn/redney/redney.* utilizador@
192.168.1.120:/etc/openvpn/client/
```

Ligar ao openvpn:

```
openvpn --config redney.ovpn
```

CONCLUSÃO

Durante este projeto, tive a oportunidade de implementar e configurar diversos serviços de tecnologia da informação para a empresa fictícia ProSysAdmin. Através dessa experiência, pude compreender melhor o funcionamento e a importância de cada um desses serviços.

A implementação do DNS permitiu a tradução de nomes de domínio em endereços IP, facilitando o acesso aos recursos da rede. O serviço DHCP automatizou a atribuição de endereços IP, simplificando a gestão da rede.

O servidor Web possibilitou a disponibilização de páginas e aplicações web, enquanto a diretoria (LDAP) centralizou as informações de utilizadores e recursos. O serviço de correio eletrónico melhorou a comunicação interna e externa da empresa, enquanto os mecanismos de scan de vírus e antispam protegeram a infraestrutura contra ameaças cibernéticas.

Por fim, a implementação do servidor de VPN estabeleceu uma conexão segura entre a empresa e utilizadores remotos, garantindo o acesso confidencial a recursos internos.

Este projeto proporcionou um maior entendimento sobre a implementação e o funcionamento desses serviços, sendo uma experiência enriquecedora para o meu desenvolvimento profissional. Estou confiante de que as habilidades adquiridas serão valiosas para enfrentar desafios futuros na área de tecnologia da informação.

BIBLIOGRAFIA/WEBGRAFIA