INSTITUTO POLITÉCNICO DE BEJA
Escola Superior de Tecnologia e Gestão
Licenciatura em Engenharia Informática

Administração de Sistemas
Relatório do laboratório n.º2

Elaborado por:
Ricardo Madeira, n.º 16147

Docentes:
Armando Ventura

01/05/2019

Introdução

Este relatório pretende descrever o trabalho realizado no decorrer do laboratório n.º1. Os objectivos principais desta avaliação prendiam-se com a instalação de duas máquina (servidor e cliente) e a configuração dos serviços named (DNS) e httpd (apache). Foi também necessário utilizar vários comandos e entender um pouco os mecanismos do sistema operativo LINUX e mais concretamente a distribuição CentOS.

Preparação das máquinas

O servidor foi preparado como pedido no enunciado, sendo a única alteração a colocação de duas placas de rede. A placa designada por eth0 foi em modo “Internal Network” e a placa designada eth1 foi colocada em modo “Bridged Adapter”. Esta alteração tem como objectivo manter a conexão à rede exterior (através da placa eth1) possibilitando também a ligação ao servidor por SSH, o que permite uma maior fluidez na realização das configurações.
A máquina cliente seguiu as mesmas alterações.

Em ambas as máquinas foram instalados os pacotes nano, setuptool e system-config-network-tui, sysem-config-securitylevel-tui e ntsysv.

Tarefa n.º1 – Crie 3 zonas masters para os domínios hotels.pt, insiste.org e teu.us

O primeiro passo é criar um servidor DHCP, de modo a poder atribuir um IP conhecido à máquina cliente.

```
# yum install dhcp

# chkconfig dhcpd on

# nano /etc/dhcp/dhcpd.conf
```

Neste ficheiro escrevemos a seguinte configuração.

```
subnet 192.168.0.0 netmask 255.255.255.0 {
    #Gama de endereços atribuídos dinânicamente pelo servidor de DHCP
    range 192.168.0.100 192.168.0.200;

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

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

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

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

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

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

Verificamos a existência de erros com o comando.

```
# /usr/sbin/dhcpd -f
```

Depois de corrigidos os erros, iniciamos o serviço DHCP

```
# /etc/init.d/dhcpd start
```

Na máquina reiniciamos o serviço network e o cliente deverá “apanhar” o IP 192.168.0.100 que pertence ao sub-range definido.

Passamos então à configuração do servidor DNS. Para tal instalamos o pacote bind e as suas dependências.

```
# yum install bind*

# chkconfig named on
```

Vamos então editar o ficheiro de configuração do serviço named.

```
# nano /etc/named.conf
```

```
(…)
options {
      listen-on port 53 { 127.0.0.1; any;};
      listen-on-v6 port 53 { ::1; any;};
            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";
            allow-query     { localhost; any;};
(…)
########################################
#               hotels.pt
########################################
zone "hotels.pt" IN {
        type master;
        file "/var/named/hotels.pt.hosts";
};

zone "2.3.8.in-addr.arpa" IN {
        type master;
        file "/var/named/2.3.8.in-addr.arpa.hosts";
};

########################################
#               insiste.org
########################################
zone "insiste.org" IN {
        type master;
        file "/var/named/insiste.org.hosts";
};

########################################
#               teu.us
########################################
zone "teu.us" IN {
        type master;
        file "/var/named/teu.us.hosts";
};
```

De seguida é necessário criar os ficheiros das zonas forward de cada um dos domínios.

```
# nano /var/named/hotels.pt.hosts
```

```
$ttl  38400
@           IN    SOA   serverlab2.asistemas.pt. mail.asistemas.pt. (
                        1165190726
```

```
                        10800
                        3600
                        604800
                        38400
                        )
            IN    NS    serverlab2.asistemas.pt.
            IN    A     8.3.2.14
ftp         IN    A     8.3.2.15
webmail     IN    A     8.3.2.16
            MX    10    as-smtp.insiste.org.
```

```
# nano /var/named/insiste.org.hosts
```

```
$ttl  38400
@           IN    SOA   serverlab2.asistemas.pt. mail.asistemas.pt. (
                        1165190726
                        10800
                        3600
                        604800
                        38400
                        )
            IN    NS    serverlab2.asistemas.pt.
            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
            MX    10    as-smtp.insiste.org.
```

```
# nano /var/named/teu.us.hosts
```

```
$ttl  38400
@           IN    SOA   serverlab2.asistemas.pt. mail.asistemas.pt. (
                        1165190726
                        10800
                        3600
                        604800
                        38400
                        )
            IN    NS    serverlab2.asistemas.pt.
            IN    A     191.200.22.14
ftp         IN    A     92.147.45.1
webmail     IN    A     191.168.22.16
            MX    10    as-smtp.insiste.org.
```

Vamos agora criar o ficheiro da zona reverse do domínio hotels.pt.

```
# nano /var/named/2.3.8.in-addr.arpa.hosts
```

```
$ttl  38400
@           IN    SOA   serverlab2.asistemas.pt. mail.asistemas.pt. (
                        1165192116
                        10800
                        3600
                        604800
                        38400
```

```
                        )
            IN    NS    serverlab2.asistemas.pt.
14          IN    PTR   hotels.pt.
15          IN    PTR   ftp.hotels.pt.
16          IN    PTR   webmail.hotels.pt.
```

De seguida iniciamos o serviço named. Caso sejam detectados erros os mesmo devem ser corrigidos. Neste momento o servidor está configurado, passamos então ao cliente.

O primeiro passo é instalar as ferramentas nslookup.
```
#yum install bind-utils
```

Podemos agora desligar a segunda placa de rede que comunica com a rede exterior.
```
# ifdown eth1
```

Através da ferramenta setup verificamos se a placa de rede eth0 está utilizar o servidor DHCP para "apanhar" IP. Depois é necessário confirmar que o cliente consegue comunicar com o servidor.
```
# ping 192.168.0.1
```

Por fim editamos o ficheiro resolv.conf, para adicionar em primeiro lugar o IP do nosso servidor DNS.
```
# nano /etc/resolv.conf
```

```
; generated by /sbin/dhclient-script
search Home asistemas.pt
nameserver 192.168.0.1 ; DNS do nosso servidor
nameserver 192.168.1.254 ; DNS da ligação exterior
```

Passamos então a testar a resolução de nomes e de IP's através da ferramenta nslookup.
```
# nslookup
```
> hotels.pt Address: 8.3.2.14
> ftp.hotels.pt Address: 8.3.2.15
> webmail.hotels.pt Address: 8.3.2.16
> insiste.org Address: 14.21.1.14
> www.insiste.org Address: 77.8.90.1
> webmail.insiste.org Address: 11.21.1.16
> as-smtp.insiste.org Address: 11.0.0.1
> teu.us Address: 191.200.22.14
> ftp.teu.us Address: 92.147.45.1
> webmail.teu.us Address: 191.168.22.16
> 8.3.2.14 name = hotels.pt.
> 8.3.2.15 name = ftp.hotels.pt.
> 8.3.2.16 name = webmail.hotels.pt.

Todos os testes devolveram os nomes e IP correctos.

Tarefa n.º2 – Crie 2 utilizadores e configure o servidor Apache de modo a que cada um possua uma página inicial numa directória "homepage"

Vamos criar um esqueleto para as directórias home dos utilizadores pedidos. Para tal utilizamos o directório /etc/skel.

```
# mkdir -p /etc/skel/homepage
```

De seguida vamos crioar os dois utilizadores:

```
# useradd subuser1 -g users
# passwd subuser1
# useradd subuser2 -g users
# passwd subuser2
```

Para confirmar que os utilizadores foram adicionados ao grupo "users" podemos verificar o output do comando:

```
# id -gn subuser1 && id -gn subsuser2
```

Para que o servidor apache leia os ficheiros no directório homepagel, temos que dar as permissões necessárias. Podemos fazê-lo com os seguintes comandos.

```
# chmod -R 755 /home/subuser1
# chmod -R 755 /home/subuser2
```

Passamos então a ter as seguintes permissões, que permitem que o user apache leia os ficheiros:

```
#ls -la /home

drw-r--r--   3 subuser1 users 4096 Apr 30 22:17 subuser1
drw-r--r--   3 subuser2 users 4096 Apr 30 22:18 subuser2
```

Com os utilizadores criados, passamos agora à instalção e configuração do servidor apache.

```
# yum install httpd
# chkconfig httpd on
```

Vamos agora configurar o serviço.

```
# nano /etc/httpd/conf/httpd.conf
```

```
(…)
    # UserDir is disabled by default since it can confirm the presence
    # of a username on the system (depending on home directory
    # permissions).
    #
    #UserDir disabled

    #
    # 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
    Options MultiViews Indexes SymLinksIfOwnerMatch IncludesNoExec
    <Limit GET POST OPTIONS>
        Order allow,deny
        Allow from all
    </Limit>
    <LimitExcept GET POST OPTIONS>
        Order deny,allow
        Deny from all
   </LimitExcept>
</Directory>

#
# DirectoryIndex: sets the file that Apache will serve if a directory
# is requested.
#
# The index.html.var file (a type-map) is used to deliver content-
# negotiated documents.  The MultiViews Option can be used for the
# same purpose, but it is much slower.
#
DirectoryIndex inicio.html index.html index.html.var
(...)
```

Depois de guardar a configuração iniciamos o serviço httpd.

```
# /etc/init.d/httpd start
```

Caso haja erros os mesmos devem ser corrigidos.

Passamos então à máquina cliente, onde poderemos aceder ao servidor através da rede externa (graças à placa de rede eth1) através do IP 192.168.1.84 (Ip designado pelo meu router à placa eth1 da máquina virtual). Podemos ver de seguida screenshots do browser na máquina cliente.

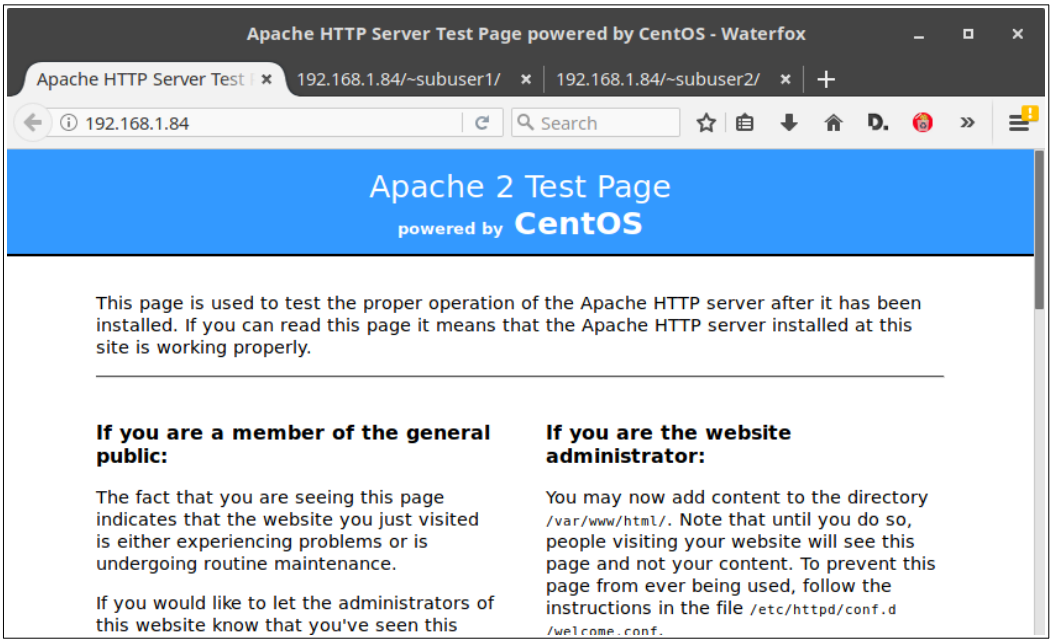

Figure 1: Página de teste do servidor Apache

Figure 2: Página inicicial do utilizador subuser1

Figure 3: Página inicicial do utilizador subuser2

Tarefa n.º3 – Criar uma directória “private” onde será necessária autenticação através do apache para aceder.

Devemos criar as directórias “private” nas directórias home de cada um dos utilizadores

```
# mkdir /home/subuser1/homepage/private && mkdir /home/subuser2/homepage/private
```

Verificar que ambas possuem permissões de escrita e execução para o utilizador apache

```
# ls -la /home/subuser*/homepage
(…)
-rwxr-xr-x 1 subuser1 users   54 Apr 30 23:04 inicio.html
drwxr-xr-x 2 root     root  4096 May  1 00:01 private
(…)
-rwxr-xr-x 1 subuser2 users   54 Apr 30 23:03 inicio.html
drwxr-xr-x 2 root     root  4096 Apr 30 23:58 private
```

Vamos agora configurar o serviço para que peça autenticação.

```
# nano /etc/httpd/conf/httpd.conf
```

```
(…)
# First, we configure the "default" to be a very restrictive
set of
# features.
#
<Directory />
    Options FollowSymLinks
    AllowOverride AuthConfig
</Directory>
(…)
#  AllowOverride  controls  what  directives  may  be  placed
in .htaccess files.
# It can be "All", "None", or any combination of the keywords:
#   Options FileInfo AuthConfig Limit
#
    AllowOverride AuthConfig
(…)
```

Criamos o ficheiro que contêm os dados de autenticação para o directório “private” do subuser1.

```
# htpasswd -c /home/.apache_private_subuser1 private
# htpasswd /home/.apache_private_subuser1 privado
```

De seguida criamos o ficheiro .htaccess no directório “private” do subuser1

```
# nano /home/subuser2/private/.htaccess
```

```
AuthName "private directory for subuser1"
AuthType Basic
AuthUserFile /home/.apache_private_subuser1
require valid-user
```

Criamos o ficheiro que contêm os dados de autenticação para o directório “private” do subuser2.

```
# htpasswd -c /home/.apache_private_subuser2 rdis
```

De seguida criamos o ficheiro .htaccess no directório “private” do subuser2
```
# nano /home/subuser2/private/.htaccess
```

```
AuthName "private directory for subuser2"
AuthType Basic
AuthUserFile /home/.apache_private_subuser2
require valid-user
```

Depois de guardar todos os ficheiros re-iniciamos o serviço httpd.
```
# /etc/init.d/httpd start
```

Caso haja erros os mesmos devem ser corrigidos.
Ao acedermos ao endereço 192.168.1.84/~subuser1/private, é nos pedido uma autenticação.

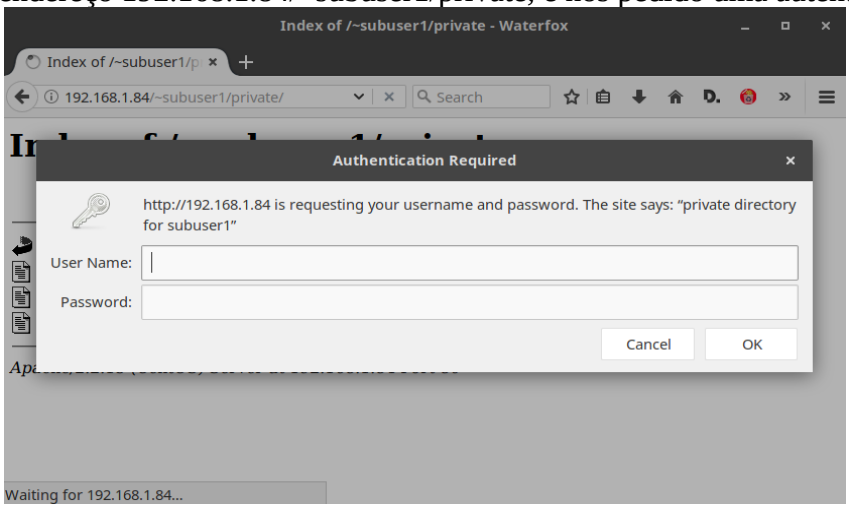

Figure 4: Pedido de autenticação para a página private do subuser1

Do mesmo modo é pedido uma autenticação ao acedermos a 192.168.1.84/~subuser2/private

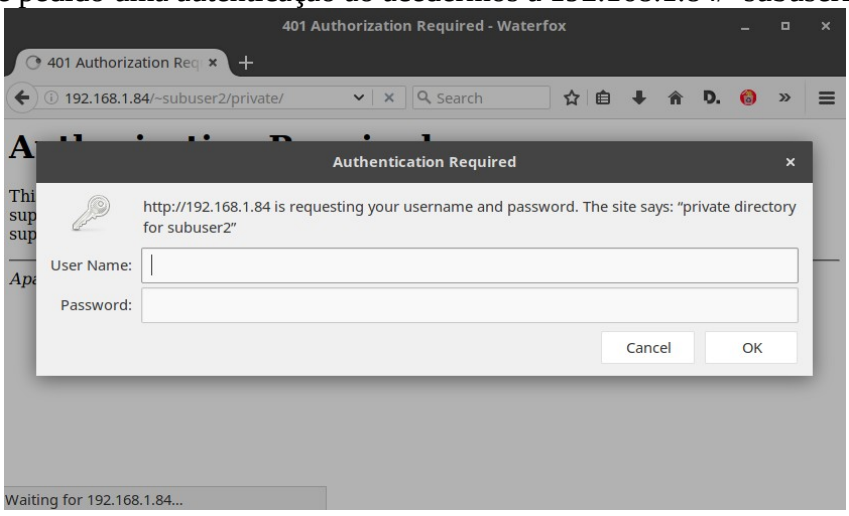

Figure 5: Pedido de autenticação para a página private do subuser2

Tarefa n.º4 – Criar virtualhosts que permitam alojar 3 domínios.

Criar os directórios que vão alojar os documentos dos domínios.

```
# mkdir -p /domains/castro.org
# mkdir -p /domains/circuito.pt
# mkdir -p /domains/festa-as.arco
```

Dentro de cada uma das directórias criamos um ficheiro inicio.html com o nome do domínio.

De seguida procedemos à criação das zonas master dos domínos que desejamos criar.

nano /etc/named.conf

```
(…)
########################################
#               castro.org
########################################
zone "castro.org" IN {
        type master;
        file "/var/named/castro.org.hosts";
};

########################################
#               circuito.pt
########################################
zone "circuito.pt" IN {
        type master;
        file "/var/named/circuito.pt.hosts";
};

########################################
#               festa-as.arco
########################################
zone "festa-as.arco" IN {
        type master;
        file "/var/named/festa-as.arco.hosts";
};
(…)
```

Vamos então criar os ficheiros das zonas forward de cada um dos domínios. Optei por colocar dois ip's de resolução de nome para que pudesse aceder ao endereço quer do cliente virtual e do cliente físico.

```
# nano /var/named/castro.org.hosts
```

```
$ttl  38400
@           IN    SOA   serverlab2.asistemas.pt. mail.asistemas.pt. (
                        1165190726
                        10800
                        3600
                        604800
                        38400
                        )
            IN    NS    serverlab2.asistemas.pt.
```

```
            IN    A     192.168.0.1
www         IN    A     192.168.0.1
            IN    A     192.168.1.84
www         IN    A     192.168.1.84
```

```
# nano /var/named/circuito.pt.hosts
```

```
$ttl  38400
@           IN    SOA   serverlab2.asistemas.pt. mail.asistemas.pt. (
                        1165190726
                        10800
                        3600
                        604800
                        38400
                        )
            IN    NS    serverlab2.asistemas.pt.
            IN    A     192.168.0.1
www         IN    A     192.168.0.1
            IN    A     192.168.1.84
www         IN    A     192.168.1.84
```

```
# nano /var/named/festa-as.arco.hosts
```

```
$ttl  38400
@           IN    SOA   serverlab2.asistemas.pt. mail.asistemas.pt. (
                        1165190726
                        10800
                        3600
                        604800
                        38400
                        )
            IN    NS    serverlab2.asistemas.pt.
            IN    A     192.168.0.1
www         IN    A     192.168.0.1
            IN    A     192.168.1.84
www         IN    A     192.168.1.84
```

Reiniciámos o serviço named. Caso sejam detectados erros os mesmo devem ser corrigidos.
Colocamos o endereço do servidor nos ficheiros resolv.conf do cliente virtual (nameserver 192.168.0.1) e fazemos o mesmo para o cliente físico (nameserver 192.168.1.84). Os endereços são diferentes pois correspondem a diferentes interfaces de rede, que possuem endereços diferentes.
E finalmente efectuamos teste para verificar que a resolução de nomes está correcta.

Passamos então à configuração dos ‘VirtualHosts’ no servido apache.
nano /etc/http/conf/httpd.conf

```
(…)
# Change this to Listen on specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses (0.0.0.0)
#
#Listen 12.34.56.78:80
Listen 0.0.0.0:15000
Listen 0.0.0.0:18000
Listen 0.0.0.0:80
(…)
```

```
# Use name-based virtual hosting.
#
NameVirtualHost *:15000
NameVirtualHost *:18000
[redacted]
(…)
##########################################
#     castro.org
##########################################
<VirtualHost [redacted] *:15000 *:18000>
        DocumentRoot "/domains/castro.org/"
        ServerName www.castro.org
        ServerAlias castro.org
        <Directory "/domains/castro.org">
                Options Indexes FollowSymLinks
                AllowOverride All
                Order allow,deny
                Allow from all
        </Directory>
</VirtualHost>

##########################################
#     circuito.pt
##########################################
<VirtualHost [redacted] *:15000 *:18000>
        DocumentRoot "/domains/circuito.pt/"
        ServerName www.circuito.pt
        ServerAlias circuito.pt
        <Directory "/domains/circuito.pt">
                Options Indexes FollowSymLinks
                AllowOverride All
                Order allow,deny
                Allow from all
        </Directory>
</VirtualHost>

##########################################
#     festa-as.arco
##########################################
<VirtualHost [redacted] *:15000 *:18000>
        DocumentRoot "/domains/festa-as.arco/"
        ServerName www.festa-as.arco
        ServerAlias festa-as.arco
        <Directory "/domains/festa-as.arco">
                Options Indexes FollowSymLinks
                AllowOverride All
                Order allow,deny
                Allow from all
        </Directory>
</VirtualHost>
(…)
```

Finalmente reiniciei o serviço httpd

```
# /etc/init.d/httpd restart
```

Mantive a escuta na porta 80, esta é necessária para que os utilizadores criados na tarefa 2 acedam às suas áreas privadas, bem como que seja exibida a sua homepage. Para garantir que os endereços sem especificação de porta são encaminhados para os VirtualHosts adicionei o *:80 a cada configuração.
No cliente virtual instalei o browser lynx para poder aceder às paginas html criadas. No cliente físico utilizei o waterfox. Todos os endereços testados apresentaram as páginas dos domínios.

Conclusão

Depois de realizar todas as tarefas pedidas, posso concluir que estas não eram de uma dificuldade apreciável, sendo até tarefas bastante simples em relação ao que se espera de um administrador de sistemas.