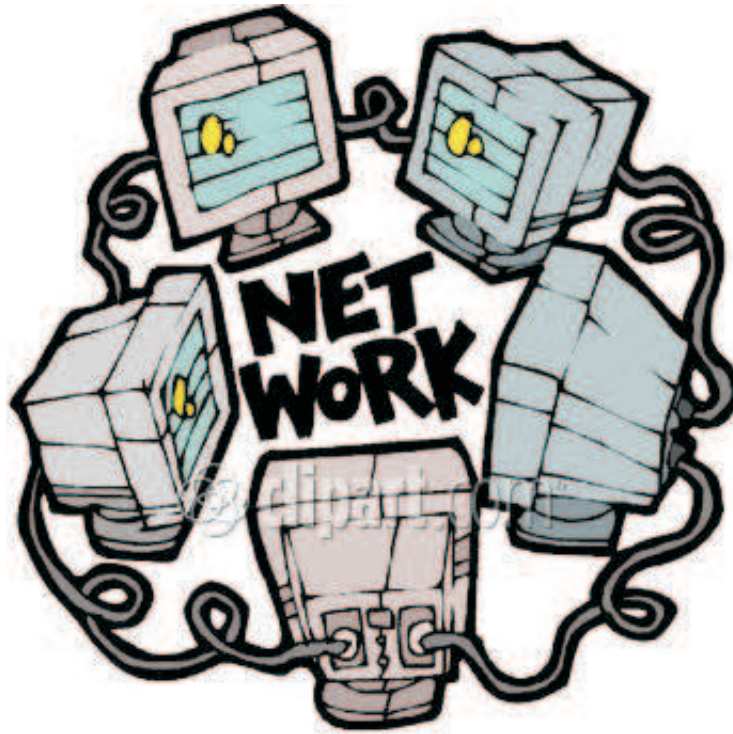

Trabalho de Arquitecturas de Redes e Serviços

Configuração de uma *Intranet*



Miguel Rentes	miguel.rentes@fe.up.pt
Nelson Rodrigues	nelson@fe.up.pt
Ricardo Veloso	ricardo.veloso@fe.up.pt
Rui Diogo	rui.diogo@fe.up.pt

Julho de 2004

Conteúdo

1	Introdução	5
1.1	Objectivo	5
1.2	Estrutura do Relatório	5
2	Arquitectura da Rede	6
3	Serviços de Suporte	7
3.1	DNS	7
3.1.1	Introdução	7
3.1.2	Configuração e instalação do Servidor	7
3.1.3	Configuração do Cliente	10
3.2	DHCP	12
3.2.1	Introdução	12
3.2.2	Configuração e instalação do Servidor	12
3.2.3	Configuração e instalação do Cliente	13
3.3	DHCP-DNS	14
3.3.1	Introdução	14
3.3.2	Configuração e instalação	14
3.4	Kerberos	15
3.4.1	Introdução	15
3.4.2	Configuração e instalação do Servidor	15
3.4.3	Configuração e instalação do Cliente UNIX	17
3.4.4	Configuração e instalação do Cliente Windows	17
3.5	LDAP	18
3.5.1	Introdução	18
3.5.2	Configuração e instalação do Servidor	18
3.5.3	Configuração e instalação do Cliente	25
4	Sistema de Ficheiros Distribuídos	27
4.1	<i>Andrew File System</i> (AFS)	27
4.1.1	Introdução	27
4.1.2	Configuração e instalação do Servidor	27
4.1.3	Configuração e instalação do Cliente UNIX	28
4.1.4	Configuração e instalação do Cliente Windows	29
4.2	SAMBA (SMB)	30
4.2.1	Introdução	30
4.2.2	Configuração e instalação do Servidor	30
4.2.3	Configuração e instalação do Cliente	33
5	Serviço de E-Mail	34
5.1	Serviço de E-Mail	34
5.1.1	Instalar o mini-qmail (servidor ns)	34
5.1.2	Instalar o qmail (servidor opio)	35
5.1.3	Instalar o IMAP e POP	38
5.1.4	Instalar o IMP	40

6	Serviços Web	43
6.1	Introdução	43
6.2	Servidor HTTP	43
6.2.1	Instalação	43
6.2.2	Acesso controlado por PAM	43
6.2.3	Configuração de domínios virtuais	44
6.2.4	Integração Apache, PHP e Base de dados	45
6.3	Proxy	46
6.3.1	Instalação	46
6.3.2	Acesso controlado por SMB	47
6.3.3	Controlo de débitos	47
6.4	Webalizer	48
7	Conclusão	50

Lista de Figuras

1	Rede da empresa tcsc.pt	6
---	--	---

1 Introdução

1.1 Objectivo

O objectivo deste trabalho prático é o de configurar alguns serviços de suporte a uma intranet.

Neste documento serão demonstradas as instalações e configurações dos seguintes serviços:

1. Serviços de Base ou de Suporte: DHCP, DNS, LDAP;
2. Serviços de Sistemas de Ficheiros: AFS, Samba;
3. Serviços de Mail: SMTP, IMAP, POP, IMP;
4. Serviços Web: HTTP, MySQL, PROXY.

O enunciado detalhado do trabalho pode ser encontrado em:
http://netlab.fe.up.pt/oliveira/sci/trabalho_intranet.pdf

1.2 Estrutura do Relatório

Para além desta Introdução e de uma Conclusão em que se explicam algumas das opções tomadas, este relatório contém um capítulo sobre a rede implementada e um capítulo por cada categoria de serviços instalada.

2 Arquitectura da Rede

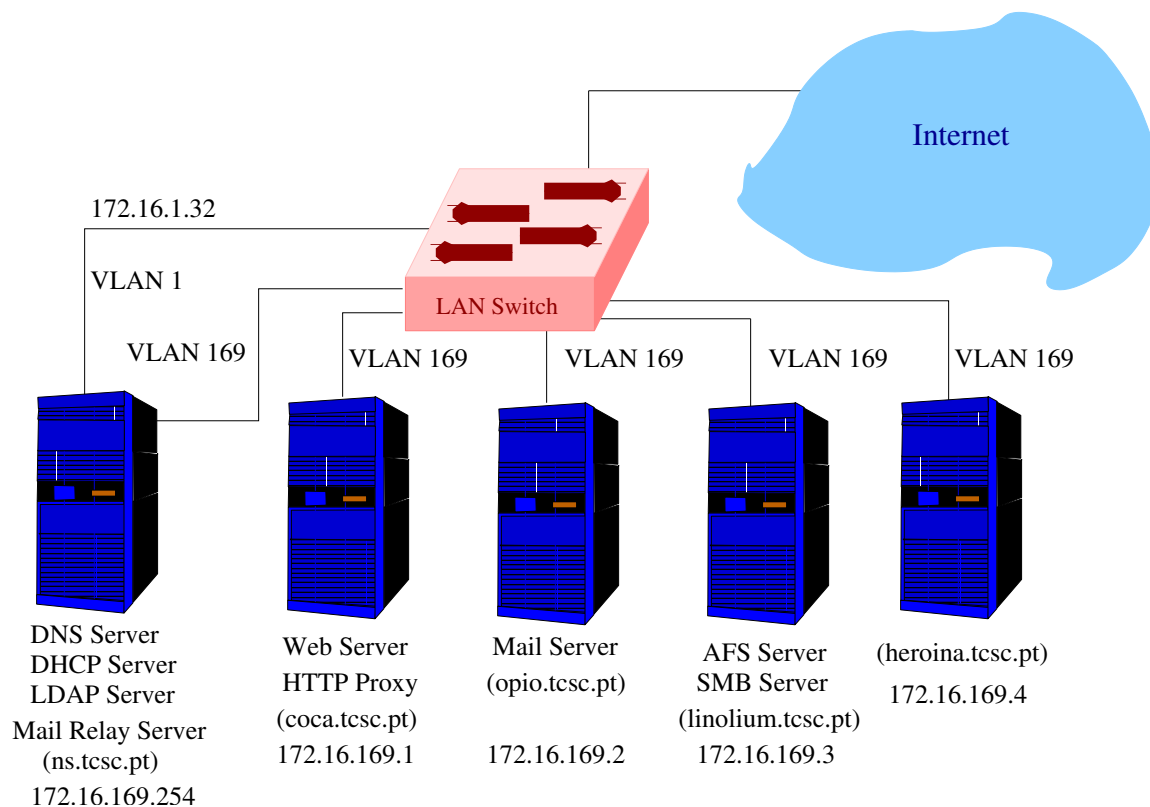


Figura 1: Rede da empresa tcsc.pt

Como se pode ver pela Figura 1, a nossa sub-rede é composta por quatro terminais com ip fixo e um último terminal com ip dinâmico. A rede comunica com o resto da internet através de um router, que no nosso caso é a máquina ns (máquina linux com duas interfaces de rede) que tem o NAT activo. O isolamento da nossa rede da rede do laboratório é conseguida utilizando uma VLAN exclusiva. Sendo assim todos os terminais se ligam ao switch numa porta da VLAN169. Apenas o nosso router, a máquina ns, liga a sua interface eth0 à VLAN do laboratório a VLAN1. Isto com o objectivo de permitir comunicação com o exterior.

A máquina ns tem instalados os servidores de DHCP, DNS, Kerberos e LDAP. A máquina coca disponibiliza o servidor web e o proxy. A máquina linolium tem os serviços de SMB e AFS. A máquina opio serve o mail.

3 Serviços de Suporte

3.1 DNS

3.1.1 Introdução

O DNS (*Domain Name Service*) é uma base de dados distribuída que contém informação sobre nomes de máquinas e seus respectivos IPs. Neste trabalho além de fazer o mapeamento já referido, iremos também utilizar o serviço de DNS para armazenar a localização dos serviços Kerberos e LDAP através da utilização de registos do tipo SRV.

No nosso trabalho foi utilizado o servidor *bind* (*Berkeley Internet Name Daemon*).

3.1.2 Configuração e instalação do Servidor

Para instalar o *bind* corremos o seguinte comando:

```
apt-get install bind
```

De forma a configurar o servidor DNS para o nosso domínio, *tcsc.pt*, foi necessário editar o ficheiro */etc/bind/named.conf* e criar os ficheiros *db.tcsc* e *db.tcsc.rev*.

Ficheiro */etc/bind/named.conf* Este é o principal ficheiro de configuração do *bind* e é aqui que criamos o nosso domínio, nas secções destinadas a *tcsc.pt* e *169.16.172.in-addr.arpa*.

```
// This is the primary configuration file for the BIND DNS server named.
//
// Please read /usr/share/doc/bind/README.Debian for information on the
// structure of BIND configuration files in Debian for BIND versions 8.2.1
// and later, *BEFORE* you customize this configuration file.
//
options {
    directory "/var/cache/bind";

    // If there is a firewall between you and nameservers you want
    // to talk to, you might need to uncomment the query-source
    // directive below. Previous versions of BIND always asked
    // questions using port 53, but BIND 8.1 and later use an unprivileged
    // port by default.

    // query-source address * port 53;

    // If your ISP provided one or more IP addresses for stable
    // nameservers, you probably want to use them as forwarders.
    // Uncomment the following block, and insert the addresses replacing
```

```
        // the all-0's placeholder.

        // forwarders {
        //     0.0.0.0;
        // };
};

// reduce log verbosity on issues outside our control
logging {
    category lame-servers { null; };
    category cname { null; };
};

// prime the server with knowledge of the root servers
zone "." {
    type hint;
    file "/etc/bind/db.root";
};

// be authoritative for the localhost forward and reverse zones, and for
// broadcast zones as per RFC 1912

zone "localhost" {
    type master;
    file "/etc/bind/db.local";
};

zone "127.in-addr.arpa" {
    type master;
    file "/etc/bind/db.127";
};

zone "0.in-addr.arpa" {
    type master;
    file "/etc/bind/db.0";
};

zone "255.in-addr.arpa" {
    type master;
    file "/etc/bind/db.255";
};

// add entries for other zones below here

zone "tcsc.pt" {
```

```

        type master;
        file "/etc/bind/db.tcsc";
        allow-update {
            172.16.169.254;
        };
};

zone "169.16.172.in-addr.arpa" {
    notify no;
    type master;
    file "/etc/bind/db.tcsc.rev";
    allow-update {
        172.16.169.254;
    };
};

```

Ficheiro *db.tcsc* Neste ficheiro definimos os mapeamentos nome de máquina, IP correspondentes às máquinas presentes na nossa rede. Estão também definidas as localizações dos serviços Kerberos e LDAP através de registos do tipo SRV.

```

;
; BIND data file for local loopback interface
;
$TTL      604800
@         IN      SOA      ns.tcsc.pt. operador.tcsc.pt. (
                        2000031600      ; Serial
                        604800           ; Refresh
                        86400            ; Retry
                        2419200          ; Expire
                        604800 )         ; Negative Cache TTL
;
@         IN      NS       ns.tcsc.pt.
@         IN      A        172.16.169.254
@         IN      MX       10 mail

ns        IN      A        172.16.169.254

coca      IN      A        172.16.169.1
opio      IN      A        172.16.169.2
linolium  IN      A        172.16.169.3
heroína   IN      A        172.16.169.4

mail      CNAME   opio

www       CNAME   coca
droga     CNAME   coca

```

```

proxy          CNAME   coca
webmail        CNAME   coca

kerberos       CNAME   ns

_kerberos      IN       TXT     "TCSC.PT"
_kerberos-master._udp.TCSC.PT.  IN       SRV     0 0 88  kerberos
_kerberos-adm._tcp.TCSC.PT.     IN       SRV     0 0 749 kerberos
_kpasswd._udp.TCSC.PT.          IN       SRV     0 0 464 kerberos
_kerberos._udp.TCSC.PT         IN       SRV     0 0 88  kerberos

_ldap._tcp.tcsc.pt.            IN       SRV     0 0 389 ns

```

Ficheiro *db.tcsc.rev* Este ficheiro define os mapeamentos reversos aos do ficheiro anterior, isto é, define o mapeamento IP, nome de máquina.

```

;
; BIND data file for local loopback interface
;
$TTL      604800
@         IN      SOA      ns.tcsc.pt.  operador.tcsc.pt. (
                        2000031600      ; Serial
                        604800           ; Refresh
                        86400            ; Retry
                        2419200          ; Expire
                        604800 )         ; Negative Cache TTL
;

         IN      NS       ns.tcsc.pt.

1        IN      PTR      coca.tcsc.pt.
2        IN      PTR      opio.tcsc.pt.
3        IN      PTR      linolium.tcsc.pt.
4        IN      PTR      heroína.tcsc.pt.
254     IN      PTR      ns.tcsc.pt.

```

3.1.3 Configuração do Cliente

No cliente apenas é necessário alterar os ficheiros *resolv.conf* e *nsswitch.conf* da seguinte forma:

***resolv.conf*:**

```

search tcsc.pt
nameserver 172.16.169.254

```

nsswitch.conf, neste ficheiro apenas é necessário garantir que a seguinte linha existe:

```
hosts: files dns
```

Como se poderá verificar na secção seguinte esta configuração está automatizada utilizando o serviço DHCP.

3.2 DHCP

3.2.1 Introdução

O serviço DHCP (*Dinamic Host Configuration Protocol*) consiste num protocolo de configuração automático de estações IP. Neste trabalho optou-se pela atribuição manual de endereços a máquinas conhecidas.

A grande vantagem do uso de um serviço deste tipo é permitir a configuração automática das estações de trabalho presentes numa rede.

3.2.2 Configuração e instalação do Servidor

O servidor *dhcpcd* é instalado com o seguinte comando:

```
apt-get install dhcp
```

Ficheiro *dhcpcd.conf* Neste ficheiro estão presentes as configurações correspondentes à nossa rede. Os IPs atribuídos de forma dinâmica ficam na subrede 172.16.169.128/25, com excepção do endereço 172.16.169.254 já atribuído ao router.

```
default-lease-time 36000;
max-lease-time 36000;
option subnet-mask 255.255.255.0;
option broadcast-address 172.16.169.255;
option routers 172.16.169.254;
option domain-name "tcsc.pt";
option domain-name-servers 172.16.169.254;

subnet 172.16.1.0 netmask 255.255.255.0 {
}

subnet 172.16.169.0 netmask 255.255.255.0 {
    range 172.16.169.128 172.16.169.253;
    default-lease-time 1800;
}

# TUX32
#host ns {
#    hardware ethernet 00:80:C8:27:1D:99;
#    fixed-address 172.16.169.254;
#    option host-name "ns"
#}

#TUX61
host coca {
    hardware ethernet 00:C0:DF:08:D5:B0;
    fixed-address 172.16.169.1;
```

```
        option host-name "coca";
    }

#TUX63
host opio {
    hardware ethernet 00:C0:DF:08:D5:AF;
    fixed-address 172.16.169.2;
    option host-name "opio";
}

#TUX33
host linolium {
    hardware ethernet 00:C0:DF:08:D5:B6;
    fixed-address 172.16.169.3;
    option host-name "linolium";
}

#TUX62
host heroína {
    hardware ethernet 00:80:C8:7F:B2:E7;
    fixed-address 172.16.169.4;
    option host-name "heroína";
}
```

3.2.3 Configuração e instalação do Cliente

O cliente de DHCP vem instalado por omissão, mas pode ser instalado, se necessário, utilizando o seguinte comando:

```
apt-get install dhcp-client
```

Ficheiro */etc/network/interfaces*

```
# The loopback interface
# Interfaces that comes with Debian Potato does not like to see
# "auto" option before "iface" for the first device specified.
iface lo inet loopback
auto lo

# Device eth0 configured by System Configurator

auto eth0
iface eth0 inet dhcp
```

3.3 DHCP-DNS

3.3.1 Introdução

Nos casos em que o servidor DHCP faz atribuição dinâmica de endereços, é conveniente que a máquina seja registada no serviço de DNS por forma a poder ser acedida pelo seu nome. Isto é conseguido através da instalação de software (*dhcp-dns*) que monitoriza o ficheiro de *leases* do servidor DHCP. Para que este software tenha permissão para alterar a base de dados DNS foram inseridas as seguintes linhas na configuração do domínio *tcsc.pt*:

```
allow-update {
    172.16.169.254;
};
```

3.3.2 Configuração e instalação

Para instalar o *dhcp-dns* deverá ser utilizado o seguinte comando:

```
apt-get install dhcp-dns
```

Ficheiro *dhcp-dns.conf* Neste ficheiro apenas é necessário indicar o domínio que é necessário actualizar, bem como a localização do ficheiro de *leases*.

```
# edit these for your own system

# this conf file is 'required()' into perl scripts so
# perl syntax applies.

$DDNSHOME="/usr/sbin";
$DHCPD="/var/lib/dhcp/dhcpd.leases";
$DOMAIN="tcsc.pt";
$NSUPDATE="/usr/sbin/nsupdate";
```

Ficheiro *crontab* Neste ficheiro é necessário acrescentar as seguintes entradas para que o domínio seja actualizado de 5 em 5 minutos.

```
# sincronizacao dhcp-dns
*/5 * * * * root /usr/sbin/ddns.cron.pl
0 */4 * * * root /usr/sbin/ndc.cron.pl
```

3.4 Kerberos

3.4.1 Introdução

Kerberos é um serviços de autenticação distribuída que permite a um cliente provar a sua identidade a um servidor sem enviar dados confidenciais através da rede. Em Kerberos um cliente tanto pode ser um utilizador como um serviço, e este envia um pedido por um *ticket* ao *Key Distribution Center (KDC)*. O KDC gera um *ticket-granting-ticket (TGT)* para o cliente, encripta-o utilizando a password armazenada localmente como chave privada, e envia o TGT encriptado de volta ao cliente. O cliente só conseguirá desencriptar o TGT se este usar a password correcta. O TGT desencriptado é então guardado pelo cliente como prova da sua identidade.

Em Kerberos, a chave de encriptação do cliente é derivada da password. Kerberos utiliza o *Data Encryption Standard (DES)* como o método de encriptação. Este método assegura que os dados encriptados apenas podem ser desencriptados utilizando a mesma chave que foi utilizada para encriptar.

3.4.2 Configuração e instalação do Servidor

Para instalar o serviço na máquina servidor deverá ser utilizado o seguinte comando:

```
apt-get install krb5-kdc krb5-admin-server
```

De seguida deverão ser corridos os seguintes comandos para inicializar a base de dados, optou-se por criar já nesta altura um principal para administração da base de dados Kerberos.

```
krb5_newrealm
```

```
kadmin.local -q \"addprinc krbadm@TCSC.PT\"
```

De seguida apresentam-se os ficheiros de configuração.

Ficheiro *krb5.conf* Neste ficheiro está definido o reino por defeito, TCSC.PT, bem como a localização dos servidores Kerberos, informação redundante uma vez que já está presente no DNS.

```
[libdefaults]
    default_realm = TCSC.PT
# The following krb5.conf variables are only for MIT Kerberos.
    default_tgs_enctypes = des3-hmac-sha1 des-cbc-crc des-cbc-md5
    default_tkt_enctypes = des3-hmac-sha1 des-cbc-crc des-cbc-md5
    permitted_enctypes = des3-hmac-sha1 des-cbc-crc des-cbc-md5
    krb4_config = /etc/krb.conf
    krb4_realms = /etc/krb.realms
    kdc_timesync = 1
    ccache_type = 4
    forwardable = true
```

```
    proxiabile = true
# The following libdefaults parameters are only for Heimdal Kerberos.
    v4_instance_resolve = false
    v4_name_convert = {
        host = {
            rcmd = host
            ftp = ftp
        }
        plain = {
            something = something-else
        }
    }

[realms]
    TCSC.PT = {
        kdc = kerberos
        admin_server = kerberos
    }

[domain_realm]
    .tcsc.pt = TCSC.PT

[login]
    krb4_convert = true
    krb4_get_tickets = true
```

Ficheiro *kadm.acl* Neste ficheiro são definidas as listas de controlo de acesso à base de dados Kerberos. O principal *krbadm* possui acesso total, o principal *samba* possui privilégios de mudança de passwords e consulta, para permitir a sincronização entre passwords Windows e UNIX e qualquer outro principal possui apenas acesso de consulta.

```
# This file Is the access control list for krb5 administration.
# When this file is edited run /etc/init.d/krb5-admin-server restart to activate
# One common way to set up Kerberos administration is to allow any principal
# ending in /admin is given full administrative rights.
# To enable this, uncomment the following line:
# */admin *

kadmin/admin@TCSC.PT    *
krbadm@TCSC.PT         *
samba@TCSC.PT          ci
*/*@TCSC.PT            i
```

Finalmente podemos reiniciar os servidores utilizando os seguintes comandos:

```
/etc/init.d/krb5-kdc restart
/etc/init.d/krb5-admin-server restart
```

3.4.3 Configuração e instalação do Cliente UNIX

Para instalar o cliente Kerberos deverão ser executados os seguintes comandos:

```
apt-get install libsasl7 libsasl-modules-plain libsasl-gssapi-mit
apt-get install krb5-user krb5-clients libpam-krb5
```

O ficheiro *krb5.conf*, já apresentado, também deverá estar presente no cliente.

Ficheiro */etc/pam.d/login* Segue-se um exemplo dos ficheiros presentes na directoria */etc/pam.d*:

```
##%PAM-1.0
auth      required      /lib/security/pam_securetty.so
auth      required      /lib/security/pam_nologin.so
auth      sufficient    /lib/security/pam_krb5.so
auth      sufficient    /lib/security/pam_ldap.so
auth      required      /lib/security/pam_unix_auth.so try_first_pass
account   sufficient    /lib/security/pam_krb5.so
account   sufficient    /lib/security/pam_ldap.so
account   required      /lib/security/pam_unix_acct.so
password  required      /lib/security/pam_cracklib.so
password  required      /lib/security/pam_krb5.so
password  required      /lib/security/pam_ldap.so
password  required      /lib/security/pam_unix.so use_first_pass
session   required      /lib/security/pam_unix_session.so
```

3.4.4 Configuração e instalação do Cliente Windows

A instalação do cliente Kerberos em Windows resume-se a correr o pacote de instalação disponível em:

<http://web.mit.edu/kerberos/dist/kfw/2.6/kfw-2.6/MITKerberosForWindows-2.6.exe>

Durante a instalação é perguntada a localização do ficheiro de configuração, este encontra-se em:

<http://deec.fe.up.pt/~ei00070/ARS/krb5.ini>

Este ficheiro é uma cópia do ficheiro *krb5.conf* já apresentado apenas com a extensão modificada.

3.5 LDAP

3.5.1 Introdução

3.5.2 Configuração e instalação do Servidor

Compilar o pacote a partir da source Devido ao uso de autenticação usando o serviço Kerberos houve necessidade de compilar o servidor *slapd* por forma a incluir esta hipótese. Já que iríamos compilar o pacote decidimos também activar o uso de TLS como uma medida adicional de segurança. Para efectuar a compilação procedemos da seguinte forma:

Actualizar */etc/apt/sources.list*:

```
deb http://deec.fe.up.pt/debian/ woody main contrib non-free
deb-src http://debian.ua.pt/debian/ woody main contrib non-free
```

Instalar pacote source OpenLDAP:

```
apt-get update
apt-get source openldap2
```

Actualizar o ficheiro *debian/rules* para conter as opções necessárias:

```
--with-kpasswd
--with-tls
```

Instalar pacotes adicionais necessários à compilação:

```
apt-get install libssl-dev libkrb5-dev libsasl-dev
apt-get install devscripts
```

Compilar o pacote:

```
debuild
```

Instalar o servidor *slapd* Tendo os pacotes do *slapd* podemos prosseguir com a sua instalação:

```
apt-get install libsasl7 libsasl-modules-plain libsasl-gssapi-mit
apt-get install libgl1.2 libgtk1.2 libgtk1.2-common libiodbc2
dpkg -i libldap2_2.0.23-6.3_i386.deb
dpkg -i slapd_2.0.23-6.3_i386.deb
dpkg -i ldap-utils_2.0.23-6.3_i386.deb
apt-get install migrationtools
```

Criar certificado SSL Para criar o certificado SSL necessário ao uso de comunicações seguras entre cliente e servidor executamos o seguinte comando:

```
openssl req -new -x509 -nodes -out server.pem \
-keyout server.pem -days 36
```

É necessário responder à pergunta Common Name com o FQDN da máquina servidora, tendo o cuidado de ser o nome devolvido fazendo um lookup reverso no DNS com o ip da máquina. O ficheiro gerado deverá ser colocado em */etc/ldap*.

Integração Kerberos Por forma a que a autenticação seja feita utilizando o serviço Kerberos é necessário que o *schema* apropriado esteja referenciado no ficheiro de configuração e que seja criado uma *service key* para o servidor LDAP, mais uma vez é necessário que seja introduzido o FQDN da máquina servidora, tendo o cuidado de ser o nome devolvido fazendo um lookup reverso no DNS com o ip da máquina. Criamos também um principal dedicado à administração do servidor LDAP. Para efectuar estas duas operações é necessário correr os seguintes comandos:

```
kadmin -p krbadm -q \  
    "addprinc -pw bill9gates ldapadm@TCSC.PT"  
kadmin -p krbadm -q \  
    "addprinc -randkey ldap/ns.tcsc.pt@TCSC.PT"  
kadmin -p krbadm -q \  
    "ktadd -k /etc/ldap/krb5.keytab.ldap ldap/ns.tcsc.pt"
```

Ficheiro */etc/init.d/slapd* É necessário alterar a linha 8 do ficheiro */etc/init.d/slapd* para que o servidor escute também na porta dedicada a LDAPS:

```
start-stop-daemon --start --quiet --pidfile "/var/run/slapd.pid" \  
    --exec /usr/sbin/slapd \  
    -- -h "ldap://0.0.0.0/ ldaps://0.0.0.0/"
```

Ficheiro */etc/ldap/slapd.conf* As alterações introduzidas relativamente ao ficheiro de configuração *default* foram:

- Introdução dos schemas necessários à operação de Kerberos, QMail, Courier, Horde e Samba
- Introdução da configuração SASL
- Introdução da configuração SSL
- Modificação do sufixo
- Mover as ACLs para um ficheiro à parte

```
# This is the main ldapd configuration file. See slapd.conf(5) for more  
# info on the configuration options.
```

```
# Schema and objectClass definitions  
include      /etc/ldap/schema/core.schema  
include      /etc/ldap/schema/cosine.schema  
include      /etc/ldap/schema/nis.schema  
include      /etc/ldap/schema/inetorgperson.schema  
  
include      /etc/ldap/schema/krb5-kdc.schema  
include      /etc/ldap/schema/authldap.schema  
include      /etc/ldap/schema/samba.schema
```

```
# Schema check allows for forcing entries to
# match schemas for their objectClasses's
schemacheck      on

# Where the pid file is put. The init.d script
# will not stop the server if you change this.
pidfile          /var/run/slapd.pid

# List of arguments that were passed to the server
argsfile         /var/run/slapd.args

# Where to store the replica logs
repllogfile      /var/lib/ldap/repllog

# Read slapd.conf(5) for possible values
loglevel        0

sasl-realm       TCSC.PT
sasl-host       ns.tcsc.pt

TLSCertificateFile    /etc/ldap/server.pem
TLSCertificateKeyFile /etc/ldap/server.pem
TLSCACertificateFile /etc/ldap/server.pem

#####
# ldbm database definitions
#####

# The backend type, ldbm, is the default standard
database         ldbm

# The base of your directory
suffix           "dc=tcsc,dc=pt"

# Where the database file are physically stored
directory        "/var/lib/ldap"

# Indexing options
index objectClass eq

# Save the time that the entry gets modified
lastmod on
```

```
include          /etc/ldap/slapd.access
```

Ficheiro */etc/ldap/slapd.access* Neste ficheiro são definidas as ACLs de acesso à base de dados LDAP.

```
# For Netscape Roaming support, each user gets a roaming profile for
# which they have write access to
access to dn=".*,ou=Roaming,dc=*"
    by dn="cn=admin,dc=tcsc,dc=pt" write
    by dn="uid=LDAPADM" write
    by dnattr=owner write
    by * none

# Some things should be editable by the owner, and viewable by anyone...
access to attr=cn,givenName,sn,krbName,krb5PrincipalName,gecos
    by dn="cn=admin,dc=tcsc,dc=pt" write
    by dn="uid=LDAPADM" write
    by self write
    by users read

access to attr=loginShell,gecos
    by dn="cn=admin,dc=tcsc,dc=pt" write
    by dn="uid=LDAPADM" write
    by self write
    by * read

# Since we're using {KERBEROS}<PRINCIPAL>, we can't allow the user
# to change the password. They have to use the Kerberos 'kpasswd' to
# do this... But the admin can change (if need be).
# Please see krb5 userPassword attribute

access to attr=userPassword
    by dn="cn=admin,dc=tcsc,dc=pt" write
    by dn="uid=LDAPADM" write
    by anonymous auth
    by * none

# The mail and mailAlternateAddress should only be readable if you
# authenticate!
access to attr=mail,mailAlternateAddress,mailHost
    by dn="cn=admin,dc=tcsc,dc=pt" write
    by dn="uid=LDAPADM" write
    by users read
    by * none

# Should not be readable to anyone, and only editable by admin...
```

```
access to attr=mailQuota,trustModel,accessTo
    by dn="cn=admin,dc=tcsc,dc=pt" write
    by dn="uid=LDAPADM" write
    by self read
    by * none

# The admin dn has full write access
access to *
    by dn="cn=admin,dc=tcsc,dc=pt" write
    by dn="uid=LDAPADM" write
    by dn="uid=SAMBA" write
    by * read
```

Migração de utilizadores Para efectuar a migração dos utilizadores existentes no sistema foram utilizadas as *migrationtools* já previamente instaladas. Estes utilizadores não vão poder ser autenticados utilizando Kerberos uma vez que não possuímos acesso às suas passwords, sendo assim continuarão a ser autenticados utilizando o sistema LDAP. Antes de iniciar o processo de migração foi necessário alterar as linhas 72 e 75 do ficheiro */usr/share/migrationtools/migration_common.ph* para conterem as definições da nossa rede:

```
$DEFAULT_MAIL_DOMAIN = "tcsc.pt";
$DEFAULT_BASE = "dc=tcsc,dc=pt";
```

Os ficheiros de migração podem ser criados com os seguintes comandos:

```
cd /usr/share/migrationtools
./migrate_base.pl > base.ldif
./migrate_group.pl /etc/group > groups.ldif
./migrate_passwd.pl /etc/passwd > users.ldif
```

Para inserir os dados no servidor LDAP é necessário executar os seguintes comandos:

```
kinit ldapadm
ldapadd -f base.ldif
ldapadd -f groups.ldif
ldapadd -f users.ldif
kdestroy
```

Criação de utilizadores Para inserir um novo utilizador na nossa rede é necessário que ele esteja presente em 3 bases de dados diferentes: LDAP, Kerberos e, como veremos mais adiante, AFS. Para automatizar o processo foi criado um script de criação de utilizadores que mostramos a seguir:

```
#!/bin/bash
```

```
if test $# -lt 3
then
    echo "Uso; $0 username 'Nome do Utilizador' password"
    exit 1
fi

contas="/afs/tcsc.pt/user"
profiles="/var/samba/profiles"
afs_server="linolium"
afs_quota=5000

userid=$1
nome=$2
password=$3
home_dir=$contas/$userid
profiles_dir=$profiles/$userid

templdif='tempfile'

#procurar o prox UID livre, ignorar user nobody=>uidNumber=65534
let UID1='ldapsearch -x '(& (objectClass=posixAccount) (! (uidNumber=65534)))'\
    | grep uidNumber | cut -b 12- | sort -g | tail -n 1 '+1

GID1=100

echo "dn: uid=$userid,ou=People,dc=tcsc,dc=pt" > $templdif
echo "uid: $userid" >> $templdif
echo "cn: $nome" >> $templdif
echo "mail: $userid@tcsc.pt" >> $templdif
echo "uidNumber: $UID1" >> $templdif
echo "gidNumber: $GID1" >> $templdif
echo "homeDirectory: $home_dir" >> $templdif
echo "krb5PrincipalName: $userid@TCSC.PT" >> $templdif
echo "loginShell: /bin/bash" >> $templdif
echo "sn: $userid" >> $templdif
echo "objectClass: top" >> $templdif
echo "objectClass: account" >> $templdif
echo "objectClass: organizationalPerson" >> $templdif
echo "objectClass: inetOrgPerson" >> $templdif
echo "objectClass: posixAccount" >> $templdif
echo "objectClass: krb5Principal" >> $templdif
echo >> $templdif

echo "A inserir $userid na base de dados LDAP..."
echo "bill9gates" | kinit ldapadm
```

```
ldapadd -f $templdif || exit 1

/usr/local/samba3/bin/smbpasswd -a $userid $password

echo "A inserir $userid na base de dados Kerberos..."
kadmin -p krbadm -q "addprinc -pw $password $userid@TCSC.PT" || exit 1

echo "A inserir $userid na base de dados AFS"
echo "bill9gates" | kinit krbadm
aklog || exit 1

#inserir utilizador
pts createuser $userid $UID1

#criar o volume
vos create -server $afs_server -partition /vicepa \
          -name user.$userid -maxquota $afs_quota

#criar o mountpoint
fs mkm $home_dir user.$userid
chmod 755 $home_dir

#copiar o skel para a home
cd /etc/skel && find | cpio -p $home_dir
chown -R $userid:users $home_dir

#colocar as ACL's no volume
fs setacl -dir 'find $home_dir -type d' \
          -acl $userid all system:administrators all \
          system:anyuser none -clear
fs setacl $home_dir/public_html $userid all \
          system:administrators all system:anyuser read -clear

mkdir $profiles_dir
chown $userid:users $profiles_dir
chmod 700 $profiles_dir

unlog
kdestroy
rm -f $templdif
echo "Pronto..."
```

3.5.3 Configuração e instalação do Cliente

Todas as máquinas existentes na rede são clientes LDAP. Para instalar o cliente devem-se executar os seguintes comandos:

```
apt-get install libglib1.2 libgtk1.2-common libgtk1.2 libiodbc2
dpkg -i libldap2_2.0.23-6.3_i386.deb
dpkg -i ldap-utils_2.0.23-6.3_i386.deb
apt-get install libpam-ldap libnss-ldap
apt-get install libpam-cracklib libnet-ldap-perl libpam-modules
```

É necessário alterar os seguintes ficheiros por forma a que fiquem a apontar para a localização correcta do nosso servidor LDAP:

Ficheiro */etc/ldap/ldap.conf*

```
# See ldap.conf(5) for details
# This file should be world readable but not world writable.

BASE    dc=tcsc,dc=pt
URI     ldaps://ns.tcsc.pt
```

Ficheiro */etc/libnss-ldap.conf*

```
# The distinguished name of the search base.
base dc=tcsc,dc=pt

# Another way to specify your LDAP server is to provide an
# uri with the server name. This allows to use
# Unix Domain Sockets to connect to a local LDAP Server.
uri ldaps://ns.tcsc.pt

# The LDAP version to use (defaults to 3
# if supported by client library)
ldap_version 3

# The distinguished name to bind to the server with.
# Optional: default is to bind anonymously.
binddn cn=admin,dc=tcsc,dc=pt

# The credentials to bind with.
# Optional: default is no credential.
bindpw bill9gates
```

Ficheiro *pam_ldap.conf*

```
# The distinguished name of the search base.
base dc=tcsc,dc=pt

# Another way to specify your LDAP server is to provide an
# uri with the server name. This allows to use
# Unix Domain Sockets to connect to a local LDAP Server.
uri ldaps://ns.tcsc.pt

# The LDAP version to use (defaults to 3
# if supported by client library)
ldap_version 3

# The distinguished name to bind to the server with.
# Optional: default is to bind anonymously.
binddn cn=admin,dc=tcsc,dc=pt

# The credentials to bind with.
# Optional: default is no credential.
bindpw bill9gates
```

Ficheiro *nsswitch.conf*

```
# /etc/nsswitch.conf
#
# Example configuration of GNU Name Service Switch functionality.
# If you have the 'glibc-doc' and 'info' packages installed, try:
# 'info libc "Name Service Switch"' for information about this file.

passwd:          compat ldap
group:           compat ldap
shadow:         compat ldap

hosts:           files dns
networks:        files

protocols:       db files
services:        db files
ethers:          db files
rpc:             db files

netgroup:        nis
```

Ficheiros em */etc/pam.d* Nesta directoria encontram-se os ficheiros de configuração do PAM já referidos na secção sobre Kerberos.

4 Sistema de Ficheiros Distribuídos

4.1 *Andrew File System* (AFS)

4.1.1 Introdução

O AFS é um sistema de ficheiros distribuído originalmente desenvolvido pela IBM sendo que actualmente o seu desenvolvimento é assegurado pela comunidade *open-source*. É um sistema de ficheiros caracterizado pela elevada independência do cliente em relação ao servidor e também pela elevada tolerância a falhas, inclusivé a falhas de rede. Um dos pontos fortes deste sistema de ficheiros é a segurança que impõe sendo necessário ter um reino Kerberos funcional. Esta elevada segurança trás também alguns problemas ao nível do acesso de certos programas ao sistema de ficheiros, ex: qmail, uma vez que o user root deixa de ter acesso a todos os ficheiros existentes, apenas users com tickets Kerberos válidos podem aceder ao sistema de ficheiros, e mesmo estes estão sujeitos ás ACLs definidas no espaço AFS. Outro aspecto digno de ser referido é que não é possível aceder directamente a ficheiros contidos no espaço AFS sem ser através do servidor, isto é, não é possível aceder aos ficheiros localmente.

4.1.2 Configuração e instalação do Servidor

Para instalar o servidor AFS foi necessário compilar o módulo AFS para o kernel. A seguir é mostrado o procedimento para proceder à sua compilação bem como instalação.

```
apt-get install kernel-headers-2.4.18-bf2.4
echo "deb http://www.openafs.org/dl/openafs/1.2.11 debian-3.0/" \
    >> /etc/apt/sources.list
apt-get update
apt-get install openafs-modules-source
cd /usr/src
tar -zxvf openafs.tar.gz
cd kernel-source-2.4.18
cp /boot/config-2.4.18-bf2.4 .config
make-kpkg configure
make-kpkg modules-install
```

Após terminado o procedimento será criado em */usr/src* o pacote *openafs-modules-2.4.18_1.2.11-0.woody1+10.00.Custom.i386.deb* que deverá ser instalado em todas as máquinas.

Seguidamente apresenatam-se os comandos que instalam o servidor AFS propriamente dito.

```
echo "deb http://www.openafs.org/dl/openafs/1.2.11 debian-3.0/" \
    >> /etc/apt/sources.list
```

```
apt-get update

echo "instalar modulos..."
dpkg -i openafs-modules-2.4.18_1.2.11-0.woody1+10.00.Custom_i386.deb

echo "instalar pacotes servidor..."
apt-get install openafs-client
apt-get install openafs-dbserver openafs-fileserver openafs-krb5
apt-get install libpam-openafs-session

echo "a criar afs service keys..."
kadmin -p krbadm -s kerberos -q "ank -randkey afs"
kadmin -p krbadm -s kerberos -q "ktadd -k krb5.keytab.afs afs"

asetkey add 3 krb5.keytab.afs afs

rm -f krb5.keytab.afs

echo "a criar volumes afs..."
dd if=/dev/zero of=/var/lib/openafs/vicepa bs=1024k count=100
mke2fs /var/lib/openafs/vicepa
mkdir /vicepa
mount -o loop /var/lib/openafs/vicepa /vicepa

echo "a criar cell..."
afs-newcell

echo "a criar root volume..."
kinit krbadm
aklog
afs-rootvol
```

No final da execução dos comandos executados o servidor AFS estará a correr.

4.1.3 Configuração e instalação do Cliente UNIX

Para instalar o cliente de AFS é apenas necessário executar os seguintes comandos:

```
echo "deb http://www.openafs.org/dl/openafs/1.2.11 debian-3.0/" \  
>> /etc/apt/sources.list

apt-get update

dpkg -i openafs-modules-2.4.18_1.2.11-0.woody1+10.00.Custom_i386.deb
apt-get install openafs-client
apt-get install libpam-openafs-session
```

Posteriormente todos os serviços que façam uso do PAM e necessitem obter acesso a ficheiros existentes no espaço AFS devem de conter a seguinte linha:

```
session optional /lib/security/pam_openafs_session.so
```

Isto assegura que o serviço obtenha o token necessário ao acesso a ficheiros no espaço AFS.

4.1.4 Configuração e instalação do Cliente Windows

Para instalar o cliente Windows basta correr o pacote de instalação disponível em:

```
http://www.openafs.org/dl/openafs/1.3.64/winnt/OpenAFSforWindows-1-3-6400.exe
```

Durante a instalação é perguntada a localização do ficheiro de configuração que pode ser obtido em:

```
http://deec.fe.up.pt/~ei00070/ARS/CellServDB
```

Este ficheiro apenas contém o endereço do servidor de localização de volumes AFS da nossa rede.

4.2 SAMBA (SMB)

4.2.1 Introdução

O serviço Samba foi utilizado para permitir que máquinas Windows coexistissem ao lado de máquinas UNIX de forma transparente. Desta maneira um utilizador da rede apenas tem de possuir um único username/password que lhe permita obter acesso a todos os recursos disponibilizados. No nosso trabalho apenas vamos utilizar o serviço para efectuar *netlogon* e obter acesso aos perfis de utilizador. O acesso às respectivas áreas de trabalho é efectuado através do uso do cliente AFS.

4.2.2 Configuração e instalação do Servidor

Para instalar o servidor Samba com suporte para LDAP tivemos de compilar o pacote a partir da *source*. Seguem-se os passos necessários para efectuar a compilação e posterior instalação:

Instalar pacote com a source:

```
wget http://us1.samba.org/samba/ftp/samba-3.0.4.tar.gz
tar -zxvf samba-3.0.4.tar.gz
```

Instalar pacotes adicionais necessários à compilação:

```
apt-get install libldap2-dev
```

Compilar o pacote:

```
./configure --prefix=/usr/local/samba3 --with-ldapsam
```

Para que o Samba possa fazer pesquisas e inserir novas máquinas no LDAP é necessário introduzir a password de administração LDAP e a password de root:

```
/usr/local/samba3/bin/smbpasswd -w bill9gates
/usr/local/samba3/bin/smbpasswd -a root bill9gates
```

Após estes passos falta só criar o principal `samba@TCSC.PT` bem como inserir o utilizador `samba` na base de dados AFS:

```
#Inserir principal samba em Kerberos
kadmin -p krbadm -q "ank -randkey samba"
kadmin -p krbadm -q "ktadd -keytab /etc/samba/krb5.keytab.samba samba"

#Inserir user samba em AFS
kinit krbadm
aklog
pts createuser samba 100
pts adduser samba system:administrators
unlog
kdestroy
```

Foram criados vários ficheiros para configurar e controlar a actuação do servidor Samba. Estes ficheiros são:

- smb.conf - Ficheiro principal de configuração.
- passwd.sh - Script para manter sincronizadas as passwords Windows e UNIX.
- netlogin-init.sh - Script para criar o logon.bat personalizado a cada utilizador.

Ficheiro `/usr/local/samba3/lib/smb.conf`

```
[global]
#identificacao
    netbios name = LINOLIUM
    workgroup = TCSC
    server string = Samba Server

#config LDAP
    passdb backend = ldapsam:ldaps://ns.tcsc.pt/
    ldap suffix = dc=tcsc,dc=pt
    ldap machine suffix = ou=Hosts
    ldap user suffix = ou=People
    ldap admin dn = "cn=admin,dc=tcsc,dc=pt"

    # smbpasswd -x delete the entire dn-entry
    ldap delete dn = no

#sincronizacao das pass's
    ldap passwd sync = yes

    unix password sync = yes
    passwd program = /usr/local/sbin/passwd.sh %u
    passwd chat = *Nova*password* %n\n *sucesso*

#config seguranca
    security = user
    null passwords = Yes
    encrypt passwords = yes

#config pdc
    domain master = yes
    domain logons = yes
    wins support = yes
    wins proxy = no
    time server = yes
    preferred master = yes
    os level = 255

#logon script && profiles
    logon path = \\linolium\profiles\%U
```

```
logon script = \\linolium\netlogon\logon.bat

# necessary share for domain controller
[netlogon]
    path = /var/samba/netlogon
    locking = no
    read only = yes
    locking = no
    read only = yes
    root preexec = /usr/local/sbin/netlogon-init.sh %m %u

#share for storing user profiles
[profiles]
    path = /var/samba/profiles/
    read only = no
    writeable = yes
    create mask = 0600
    directory mask = 0700
```

Ficheiro */usr/local/sbin/passwd.sh*

```
#!/bin/bash

if test $# -lt 1
then
    echo "Uso: $0 username"
    exit 1
fi

echo -n "Nova password: "
read password

kadmin -p samba -k -t /etc/samba/krb5.keytab.samba \
    -q "cpw -pw $password $userid" || exit 1

echo "Password mudada com sucesso."
```

Ficheiro */usr/local/sbin/netlogon-init.sh*

```
#!/bin/bash
if test $# -lt 2
then
    echo "Uso: $0 hostname username"
    exit 1
```

```
fi
```

```
hostname=$1  
username=$2
```

```
#queremos passar dois \'s ao echo para ele mandar 1 para o output  
#mas para cada um que vai para o echo temos de mandar 2 por causa da shell  
#logo para cada \ no output precisamos de 4 \'s ;)
```

```
echo -n -e "net use Z: \  
          \\\\\\\\\\\\$hostname-afs\\\\\\\\all\\\\\\\\tcsc.pt\\\\\\\\user\\\\\\\\$username \  
          /PERSISTENT:NO \\r\\n" \  
          > /var/samba/netlogon/logon.bat  
echo -n -e "net time \\\\\\\\\\\\\\\$linolium /SET /YES \\r\\n" \  
          >> /var/samba/netlogon/logon.bat
```

Finalmente reiniciamos os servidores SAMBA:

```
/usr/local/samba3/sbin/nmbd -D  
/usr/local/samba3/sbin/smbd -D
```

4.2.3 Configuração e instalação do Cliente

Antes de configurar as máquinas Windows para fazerem parte do domínio é necessário criar contas de máquina no LDAP. Para isso pode-se recorrer aos seguintes comandos:

```
useradd nome_de_maquina$  
/usr/local/samba3/bin/smbpasswd -a -m nome_de_maquina
```

Para configurar o cliente Windows basta ir às propriedades do 'Meu Computador' e na tab 'Identificação' inserir o domínio TCSC. Após a introdução do username e password de root o processo está finalizado.

5 Serviço de E-Mail

5.1 Serviço de E-Mail

Neste presente trabalho pretende-se instalar e configurar um servidor de mail com os seguintes serviços:

- SMTP (qmail);
- IMAP (courier-imap);
- POP (courier-pop);
- Webmail (imp).

O sistema deverá guardar uma cópia dos emails de entrada e de saída, de modo a que posteriormente possam ser consultados por IMAP.

O serviço de e-mail é baseado num servidor interno de correio electrónico e num servidor *relay* visível na Internet. Todo o correio electrónico recebido passa pelo *relay*, que o reencaminha para o servidor interno. Os utilizadores podem aceder ao seu correio electrónico via IMAP, POP3 ou Webmail.

Para as funções de *mail relay* escolhemos o `mini-qmail` por ser mais simples de configurar que o `qmail` e ser o mais indicado para o nosso caso. Como servidor de mail interno, usamos o `qmail`. Finalmente, para os serviços de interface com o utilizador, instalamos o Courier (IMAP e POP3) e a interface de Webmail da Horde (o IMP).

5.1.1 Instalar o `mini-qmail` (servidor ns)

Para instalar o `mini-qmail` no servidor ns, procedemos do seguinte modo:

```
# passar para root
su -

# remover possíveis servidores de email
apt-get remove --purge exim

apt-get install qmail-src ucspi-tcp-src daemontools-installer
build-daemontools
build-ucspi-tcp
build-qmail
```

Neste caso, não é preciso alterar nada nas sources destes pacotes, por isso pode-se responder afirmativamente a todas as perguntas que vão sendo colocadas durante o *build* destes pacotes.

Relativamente aos ficheiros de configuração, será necessário proceder às seguintes alterações (alterar os conteúdos dos seguintes ficheiros de controlo):

1. `/var/qmail/control/defaultdomain : tcsc.pt;`
2. `/var/qmail/control/locals : deverá estar vazio;`
3. `/var/qmail/control/me : ns;`
4. `/var/qmail/control/plusdomain : tcsc.pt;`
5. `/var/qmail/control/rcpthosts : tcsc.pt;`
6. `/var/qmail/control/smtproutes : tcsc.pt:172.16.169.2.`

Resta apenas permitir a todos os utilizadores da rede fazerem relay, criando o ficheiro `/etc/tcp.smtp` com o seguinte conteúdo:

```
172.16.169.:allow, RELAYCLIENT=""  
:allow
```

e fazendo

```
cat /etc/tcp.smtp | tcprules /etc/tcp.smtp.cdb rules.temp
```

5.1.2 Instalar o qmail (servidor opio)

Esta instalação do qmail é muito semelhante à da secção anterior, mas serão necessários algumas configurações antes da compilação. Assim, depois de termos executado:

```
apt-get install qmail-src ucspi-tcp-src daemontools-installer  
build-daemontools  
build-ucspi-tcp
```

Executamos o `build-qmail` só até ao ponto em que a *source* é descompactada. Nesta altura, abrimos outra consola, alteramos o ficheiro que se encontra na pasta do qmail para onde descompactamos a *source*, do seguinte modo:

```
#define QUEUE_EXTRA "Tlogs"  
#define QUEUE_EXTRALEN 6
```

Este ficheiro define o *user* (logs) para onde será sempre enviada uma cópia de todas as mensagens enviadas e recebidas pelo servidor. Posteriormente à instalação do qmail, será necessário criar uma conta para o *user* logs para que esta alteração tome efeito.

Neste ponto, voltamos à consola originale continuamos com o processo de compilação do qmail, pressionado enter. O script de instalação vai auto-detectar uma parte das configurações do servidor opio, mas é necessário modificar os ficheiros de controlo como vimos na secção anterior.

Para que o correio seja depositado nas contas dos *users* e sob o formato Maildir, é preciso que todos os *users* tenham uma pasta Maildir criada e um ficheiro `$HOME/.qmail` que aponte para lá. Para que as contas de todos os novos *users* sejam criadas já com estas configurações de forma automática, basta fazer (no servidor de LDAP, no nosso caso, no servidor ns):

```
# cd /etc/skel
# mailldirmake Maildir
# echo './Maildir/' > .qmail
```

Para que o correio enviado e recebido possa ser monitorado via IMAP, na conta do *user logs*, coloca-se um filtro *procmail*, para separar as mensagens recebidas das enviadas. O filtro deve estar em */home/logs/.procmailrc* e ter a seguinte configuração:

```
SHELL = /bin/sh
LINEBUF = 4096
HOME = /home/logs
PATH = $HOME/bin:/bin:/usr/bin:/usr/local/bin:/sbin:/usr/sbin:
VERBOSE = off
MAILDIR = $HOME/Maildir/
DEFAULT = $MAILDIR
LOGFILE = $HOME/logfile
FORMAIL = /usr/bin/formail
SENDMAIL = /usr/sbin/sendmail

# separar o mail proveniente do exterior do mail interno
:0
* ^TO_tcsc.pt
$HOME/Maildir/.inbound/

:0
* !^TO_tcsc.pt
$HOME/Maildir/.outbound/
```

As subdirectorias *.inbound* e *.outbound* devem ser criadas com o comando *mailldirmake* como foi exemplificado em cima.

Após ter sido criado o *user logs*, com o comando *adduser logs*, edita-se o ficheiro */etc/passwd*, comenta-se a linha que se inicia por *smb*, e alteramos a linha referente ao *logs* (deverá ser a última linha deste ficheiro) para:

```
logs:x:64009:1000:logs,,,:/home/bssi/bin/bash.
```

Finalmente, altera-se o dono e o grupo do *logs* fazendo *chown -R logs:users .*

De seguida, dever-se-á proceder à integração do *qmail* com o *AFS* e o *Kerberos*, sendo preciso para tal, proceder do seguinte modo numa linha de comandos:

```
# kadmin -p krbadm -q "ank -randkey qmail"
# kadmin -p krbadm -q "ktadd -k /etc/qmail/krb5.keytab.qmail qmail"
# chmod 666 /etc/qmail/krb5.keytab.qmail
# kinit krbadm
# aklog
# pts createuser qmail 200
# pts adduser qmail system:administrators
# mv /var/qmail/bin/qmail-local /var/qmail/bin/qmail-local.real
```

Neste ponto, edita-se o ficheiro `/var/qmail/bin/qmail-local` e coloca-se o seguinte conteúdo:

```
#!/bin/bash

set -eu
kinit -k -t /etc/qmail/krb5.keytab.qmail qmail
aklog -setpag
exec /var/qmail/bin/qmail-local.real $2 $3 $4 "" "" $7 $8 $9
```

Em seguida, alterar as permissões deste ficheiro fazendo:

```
# chmod 755 /var/qmail/bin/qmail-local
# chown root:qmail /var/qmail/bin/qmail-local
```

Relativamente aos ficheiros de configuração, será necessário proceder às seguintes alterações (alterar os conteúdos dos seguintes ficheiros de controlo):

1. `/var/qmail/control/defaultdomain` : tcsc.pt;
2. `/var/qmail/control/locals` : tcsc.pt;
3. `/var/qmail/control/me` : tcsc.pt;
4. `/var/qmail/control/plusdomain` : tcsc.pt;
5. `/var/qmail/control/rcpthosts` : tcsc.pt;
6. `/var/qmail/control/smtproutes` : :172.16.169.254.

Resta apenas permitir a todos os utilizadores da rede fazerem relay, criando o ficheiro `/etc/tcp.smtp` com o seguinte conteúdo:

```
172.16.169.:allow, RELAYCLIENT=""
:allow
```

e fazendo

```
cat /etc/tcp.smtp | tcprules /etc/tcp.smtp.cdb rules.temp
```

A instalação do qmail com integração com AFS e Kerberos fica assim concluída. A partir deste momento (com a nossa configuração), já é possível enviar emails para dentro da rede, e para fora da rede, usando para isso o servidor de relay.

Para testar o SMTP podem-se executar os testes que se encontram descritos em: `/usr/local/src/qmail-1.03/TEST.deliver` e `TEST.receive`.

5.1.3 Instalar o IMAP e POP

Os servidores de IMAP e POP escolhidos para este trabalho foram o uw-imapd e o ipopd. Para instalar estes servidores basta executar os seguintes comandos:

```
apt-get install uw-imapd ipopd
```

(seleccionar Y nas duas questões que o programa instalador apresenta)

De seguida, editar o ficheiro `/etc/apt/sources.list` e adicionar a linha

```
deb-src http://debian.ua.pt/debian woody main contrib non-free
```

e fazer

```
apt-get update
apt-get source uw-imapd
apt-get build-dep uw-imapd
```

```
cd uw-imap-2001adebian/
tar -zxvf imap-2001a.tar.gz
cd imap-2001a/
```

```
for f in debian/patches/*; do patch -p0 < $f; done
```

```
cd imap-2001a/src/osdep/unix
```

Agora, edita-se o ficheiro `ckp-pam.c` e altera-se a linha que tem a primeira ocorrência da string `#if 0` para `#if 1`. Editamos igualmente o ficheiro `maildir.c` e alteramos todas as ocorrências da função `link` para `rename`.

Continuamos com a instalação,

```
cd ../../..
```

```
make lnp
```

```
cd imapd
cp imapd /usr/sbin/imapd
cd ../ipopd
cp ipop2d /usr/sbin/ipop2d
cp ipop3d /usr/sbin/ipop3d
```

```
cd /etc/pam.d
```

Editamos agora o ficheiro `imap` para

```
auth sufficient /lib/security/pam_krb5.so
auth required /lib/security/pam_unix_auth.so try_first_pass
account sufficient /lib/security/pam_krb5.so
account required /lib/security/pam_unix_acct.so try_first_pass
password sufficient /lib/security/pam_krb5.so
password required /lib/security/pam_unix_passwd.so try_first_pass
session optional /lib/security/pam_krb5.so
session optional /lib/security/pam_openafs_session.so
session required /lib/security/pam_unix_session.so
```

Resta agora copiar o conteúdo deste ficheiro para o ficheiro `pop` que se encontra na mesma pasta:

```
cp imap pop
```

Após esta configuração, os servidores de IMAP e POP já se encontram disponíveis para uso.

Para testar se o servidor de IMAP está realmente a funcionar realizou-se o seguinte teste:

- Fez-se telnet à porta 143 do servidor de IMAP (porta por defeito)

```
# telnet localhost 143
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
* OK Courier-IMAP ready. Copyright 1998-2002 Double Precision, Inc.
See COPYING for distribution information.
```

O servidor de IMAP respondeu, o que indica que poderia estar a funcionar correctamente;

Para testar se o servidor de POP está realmente a funcionar realizou-se o seguinte teste:

- Fez-se telnet à porta 110 do servidor de POP (porta por defeito)

```
# telnet localhost 110
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
+OK Hello there.
```

O servidor respondeu com uma mensagem positiva, indicando que o servidor está disponível;

5.1.4 Instalar o IMP

Das várias soluções possíveis para implementar o serviço de Webmail, escolhemos a combinação do horde com o imp.

Para instalar o sistema foi necessário fazer (optou-se por instalar o Webmail no servidor de HTTP por facilidade de uso de algumas funcionalidades do apache já instaladas neste servidor):

```
apt-get install php4-pear

wget ftp://ftp.horde.org/pub/horde/horde-2.2.3.tar.gz
tar -xzf horde-2.2.3.tar.gz
mv horde-2.2.3 /var/www/webmail/horde/

wget ftp://ftp.horde.org/pub/imp/imp-3.2.1.tar.gz
tar -xzf imp-3.2.1.tar.gz
mv imp-3.2.1 /var/www/webmail/horde/imp/
```

Após a instalação do horde e do imp, é necessário editar alguns ficheiros de modo a configurar o Webmail para o nosso servidor de email, e alterar algumas preferências.

Em seguida serão apresentados os ficheiros alterados:

(ir para a directoria dos ficheiros de configuração do horde)

```
cd /var/www/webmail/horde/config/
```

(copiar os ficheiros originais de configuração)

```
for foo in *.dist; do cp -v $foo 'basename $foo .dist'; done
```

(editar ficheiro /var/www/horde/config/horde.php)

```
$conf['auth']['params']['dsn'] = '{tcsc.pt:143/imap/notls}INBOX';
```

```
$conf['log']['enable'] = 'true';
```

```
$conf['log']['type'] = 'syslog';
```

```
$conf['auth']['driver'] = 'none';
```

```
$conf['prefs']['driver'] = 'none';
```

```
$conf['mailer']['type'] = 'smtp';
```

```
$conf['mailer']['params'] = array('host' => 'opio.tcsc.pt');
```

```
(editar ficheiro registry.php)

$this->registry['auth']['login'] = 'imp';

$this->registry['auth']['logout'] = 'imp';

$this->applications['imp'] = array(

...

'status' => 'active');
```

Para se testar o horde pode-se aceder à seguinte página:

```
http://webmail.tcsc.pt/horde/test.php
```

Estando o horde configurado é necessário alterar ficheiros de configuração do imp.

Novamente são apresentados os ficheiros de configuração alterados:

(ir para a directoria dos ficheiros de configuração do imp)

```
cd /var/www/webmail/horde/imp/config/
```

(copiar os ficheiros originais de configuração)

```
for foo in *.dist; do cp -v $foo 'basename $foo .dist'; done
```

(editar ficheiro /var/www/webmail/horde/imp/config/servers.php)

```
$servers['imap'] = array(
'name' => 'IMAP server',
'server' => 'tcsc.pt',
'protocol' => 'imap/notls',
'port' => '143',
'folders' => 'INBOX',
'namespace' => '',
'maildomain' => 'tcsc.pt',
'smtp host' => 'opio.tcsc.pt',
'realm' => 'tcsc.pt',
'preferred' => ''
);
```

O imp também tem um ficheiro de teste em:

<http://webmail.tcsc.pt/horde/imp/test.php>

Deve-se começar a testar todas as funcionalidades do sistema e a verificar se há alguma falha ou algum requisito do sistema de mail que não está a ser devidamente cumprido.

6 Serviços Web

6.1 Introdução

Em seguida são apresentados os procedimentos necessários para a instalação do servidor Web e Proxy. O servidor Web bem como o Proxy foram configurados na máquina coca (172.16.169.1). Nesta mesma máquina foi também criada uma pequena base de dados em MySQL, cujo conteúdo pode ser acedido por um dos domínios virtuais criados para o efeito. Para a configuração do servidor Web e Proxy foram utilizadas três aplicações: o Apache para servidor de HTTP, o Squid para servidor de Proxy e o Webalizer como módulo estatístico.

6.2 Servidor HTTP

6.2.1 Instalação

Para instalar o Apache é utilizado o seguinte comando:

```
# apt-get install apache
```

6.2.2 Acesso controlado por PAM

Para se configurar o Apache para que o acesso às páginas seja feito mediante autenticação, optou-se por usar o PAM. Para isso foi necessário instalar o seguinte módulo:

```
# apt-get install libapache-mod-auth-pam  
# /etc/init.d/apache restart
```

No ficheiro `httpd.conf` é necessário carregar o módulo de autenticação do pam. Isso é feito inserido a seguinte linha:

```
LoadModule pam_auth_module /usr/lib/apache/1.3/mod_auth.pam.so
```

Para usar autenticação num determinado directório, basta apenas criar um ficheiro `.htaccess` dentro do mesmo. Isso é particularmente necessário para se poder aceder às páginas web (montadas pelo AFS) dos utilizadores, usando autenticação. A informação que este deve conter deve ser a seguinte:

```
AuthName "Área Reservada"  
AuthType Basic  
require group users
```

Isto permite apenas o acesso a utilizadores dentro do grupo `users`.

É ainda necessário, após colocar o ficheiro `.htaccess` dentro das pastas `public.html` das contas dos utilizadores, inserir as seguintes linhas no ficheiro `httpd.conf`, para que se possa aceder a essas mesmas páginas:

```
<Directory /afs/tcsc.pt/*/public_html>
  AllowOverride All
  Options MultiViews Indexes SymLinksIfOwnerMatch IncludesNoExec
</Directory>
```

Após isto, deve-se inserir no directório `/etc/pam.d` um ficheiro `httpd`, cujo conteúdo deve ser:

```
##%PAM-1.0
auth sufficient /lib/security/pam_krb5.so
auth required pam_unix.so

account sufficient /lib/security/pam_krb5.so
account required pam_unix.so

password sufficient /lib/security/pam_krb5.so
password required pam_unix.so

session sufficient /lib/security/pam_krb5.so
session required pam_unix.so

session optional /lib/security/pam_openafs_session.so
```

Em seguida dever-se-á restaurar o Apache para as alterações fazerem efeito:

```
/etc/init.d/apache restart
```

Para se aceder à página web de por exemplo do user xyz basta executar o link:

```
www.tcsc.pt/~xyz
```

6.2.3 Configuração de domínios virtuais

Para criar domínios virtuais basta apenas editar o ficheiro `httpd.conf`. Foram criados 4 domínios virtuais. Um para o site base da empresa (foi necessário criar um ficheiro `index.html` e colocá-lo no directório `/var/www/`), um outro para aceder à página em PHP (colocado no directório `/var/www/droga/`), um terceiro para aceder à página gerada pelo Webalizer com as estatísticas de uso do Proxy (colocado em `/var/www/proxy/`) e um quarto para acesso ao webmail. As alterações efectuadas para este efeito foram as seguintes:

```
#Domínio virtual que representa o site base
<VirtualHost 172.16.169.1>
DocumentRoot /var/www
ServerName coca.tcsc.pt
ServerAlias www
CustomLog /var/log/apache/coca-access.log common
</VirtualHost>
```

```
#Domínio virtual para a página criada em PHP
<VirtualHost 172.16.169.1>
DocumentRoot /var/www/droga/
ServerName droga.tcsc.pt
CustomLog /var/log/apache/droga-access.log common
</VirtualHost>

#Domínio virtual para a página com estatísticas do Proxy
<VirtualHost 172.16.169.1>
DocumentRoot /var/www/proxy
ServerName proxy.tcsc.pt
ServerAlias proxy
</VirtualHost>

#Domínio virtual para o Webmail
<VirtualHost 172.16.169.1>
DocumentRoot /var/www/webmail
ServerName webmail.tcsc.pt
ServerAlias webmail
</VirtualHost>
```

De referir que deverão para isso ser criados os directórios `/var/www/droga/`, `/var/www/proxy/` e `/var/www/webmail/`.

6.2.4 Integração Apache, PHP e Base de dados

Para se criar uma base de dados e permitir o seu acesso a partir de páginas web dinâmicas é necessário instalar os seguintes pacotes:

```
# apt-get install php4 php4-ldap php4-imap php4-mysql
# apt-get install mysql-server
```

O pacote `php4` activa o suporte por parte do `apache` a `php`. O `mysql-server` é o servidor de `mysql` (base de dados) e `php4-mysql` faz a ponte entre o `php4` e o `mysql`.

Em seguida, foi especificada a seguinte base de dados em SQL exemplificativa:

```
CREATE DATABASE tcsc;
USE tcsc;
CREATE TABLE alunos (nome VARCHAR(50), morada VARCHAR(50));
INSERT INTO alunos VALUES ("Miguel Rentes", "Ermesinde");
INSERT INTO alunos VALUES ("Nelson Rodrigues", "Porto");
INSERT INTO alunos VALUES ("Ricardo Veloso", "Porto");
INSERT INTO alunos VALUES ("Rui Diogo", "Felgueiras");
```

Após isto dever-se-á iniciar o MySQL e criar a base de dados, fazendo:

```
# /etc/init.d/mysql start
# mysql -u root < bd.sql
```

O ficheiro PHP para acesso à base de dados tem o seguinte código:

```
<?

$ligacao = mysql_connect("localhost", "root")
    or die("Erro ao tentar ligar ao mysql: " . mysql_error());
echo "Efetuada ligacao ao mysql<br>";
mysql_select_db("tcsc")
    or die("Erro ao selecciona BD: " . mysql_error());
echo "Efetuada ligacao à BD<br>";

$string_sql = "SELECT * FROM alunos";
echo "<br>Listagem do conteudo da tabela alunos:<br>";
$resultado = mysql_query($string_sql)
    or die ("Erro na query<br>");
$num_linhas = mysql_num_rows($resultado);

if ($num_linhas > 0)
{
    $i = 0;
    while ($linha[$i] = mysql_fetch_array($resultado))
    {
        echo "<br> - <br>Nome:" . $linha[$i] ['nome'] .
            "<br>Morada:" . $linha[$i] ['morada'];
        $i++;
    }
}

mysql_close($ligacao);

?>
```

Este ficheiro, criado com o nome `index.php`, deverá ser colocado em `/var/www/droga`. Para se aceder a ele poder-se-á usar o endereço `http://droga.tcsc.pt`, ao passo que para aceder ao ficheiro `index.html` com o site base da empresa, `http://coca.tcsc.pt`.

6.3 Proxy

6.3.1 Instalação

Para a implementação do Proxy foi usada a aplicação Squid:

```
# apt-get install squid
```

O Proxy pode ser testado no próprio servidor bastando para isso fazer:

```
# export http_proxy=http://localhost:3128
```

o que indica que se irá usar a porta padrão do Squid, 3128. Para os clientes usarem o Proxy instalado na máquina coca, deverão proceder de forma análoga:

```
# export http_proxy=http://coca:3128
```

Para testar o funcionamento do proxy bastará usar por exemplo um browser bastante prático, o Lynx. Os acessos que se vão fazendo através do proxy podem ser visualizados recorrendo ao ficheiro fazendo na máquina servidora:

```
# more /var/log/squid/access.log
```

6.3.2 Acesso controlado por SMB

Para efectuar a autenticação do proxy, optou-se por usar SMB. Para isso foi necessário alterar a seguinte linha ao ficheiro `/etc/squid.conf`, na tag `authenticate_program`:

```
authenticate_program /usr/lib/squid/smb_auth -W TCSC
```

Em seguida, é necessário instalar o pacote `samba-client`:

```
# apt-get install samba-client
```

Em seguida, na máquina servidora de Samba (linolium) dever-se-á, no directório `/var/samba/netlogon` criar um ficheiro com a designação `proxy_auth`, devendo o seu conteúdo ser `allow`.

6.3.3 Controlo de débitos

Para se controlar o débito dos clientes do Proxy, é preciso configurar o ficheiro `/etc/squid.conf`.

Primeiro, começa-se por configurar as listas de controlo de acesso (ACL's). Estas permitem especificar endereços de origem ou destino, domínios, horários, utilizadores, portas ou métodos de conexão ao Proxy, que servirão de base para permitir ou negar o acesso baseando-se em conjuntos dessas ACL's. Assim, na tag `acl` foram inseridas as seguintes linhas:

```
acl all src 0.0.0.0/0.0.0.0
acl internos proxy_auth REQUIRED src
    172.16.169.0-172.16.169.127/24
acl dhcp_internos proxy_auth REQUIRED src
    172.16.169.128-172.16.169.253/24
```

O grupo `internos` diz respeito aos computadores da nossa rede. Estes estão sujeitos a uma autenticação. O acesso ao proxy é controlado pela tag `http_access`. Nesta foram inseridas as seguintes linhas:

```
http_access allow internos
http_access allow dhcp_internos
http_access deny all
```

Para a realização do controlo de débitos é necessário introduzir as seguintes linhas, nas tags `delay_access`, `delay_pools`, `delay_class` e `delay_parameters` respectivamente:

```
delay_access 1 allow internos
delay_access 2 allow dhcp_internos
```

```
delay_pools 2
```

```
delay_class 1 1
delay_class 2 1
```

```
delay_parameters 1 20000/20000
delay_parameters 2 2000/2000
```

Segundo esta configuração está-se a definir que os utilizadores da gama de endereços descrita na ACL `internos` terão um acesso restrito de 20000 bytes por segundo ao passo que os utilizadores da acl `dhcp_internos` respeitante aos utilizadores de DHCP, têm acesso restrito de 2000 bytes por segundo.

Finalmente, dever-se-á reiniciar o Squid para as alterações anteriores fazerem efeito:

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

6.4 Webalizer

Este módulo foi instalado para que fosse possível obter uma série de estatísticas de forma amigável, relativamente aos acessos aos serviços web. A sua instalação poderá ser feita fazendo:

```
# apt-get install webalizer
```

Para que este analise o log gerado pelo Squid (`/var/log/squid/access.log`) deverá configurar-se o webalizer. Isso deverá ser feito alterando o ficheiro `webalizer.conf` e colocando-o de seguida no directório `/var/www/proxy/` onde irá ser colocado também a página html de estatística gerada pelo webalizer. As alterações a fazer no ficheiro `webalizer.conf` são as seguintes:

```
LogFile /var/log/squid/access.log
OutputDir /var/www/proxy
ReportTitle Usage Statistics for
```

Deste modo, quando se pretender gerar as estatísticas de acesso ao proxy, ao fazer-se

```
# webalizer -F squid -c /var/www/proxy/webalizer.conf
```

estas irão parar ao directório /var/www/proxy, onde ficarão acessíveis a qualquer cliente da rede, que as poderão visualizar bastando para isso usar um browser e escrever: `http://proxy.tcsc.pt`.

Para se gerarem as estatísticas dos domínios coca (do site principal) e droga, o procedimento a seguir é o mesmo. Assim, os ficheiros webalizer.conf desses domínios teriam o seguinte aspecto respectivamente:

```
LogFile /var/log/apache/coca-access.log
OutputDir /var/www/webalizer
ReportTitle Usage Statistics for
HostName www.tcsc.pt
```

```
LogFile /var/log/apache/droga-access.log
OutputDir /var/www/droga/webalizer
ReportTitle Usage Statistics for
HostName droga.tcsc.pt
```

Adicionalmente poderiam ser criados dois domínios virtuais, um para cada página de estatísticas de domínio (coca e droga), bastando para isso alterar o ficheiro `httpd.conf`.

Foi ainda necessário configurar o `crontab` para que as estatísticas sejam geradas automaticamente. Optou-se por colocar o sistema a analisar os ficheiros log às 12 horas e 24 horas do dia, obtendo-se assim estatísticas actualizadas de 12 em 12 horas. As alterações no `crontab` foram as seguintes:

```
01 12,00 * * * root webalizer -c \
    /var/www/webalizer/webalizer.conf
01 12,00 * * * root webalizer -F squid -c \
    /var/www/proxy/webalizer.conf
01 12,00 * * * root webalizer -c \
    /var/www/droga/webalizer/webalizer.conf
```

7 Conclusão

A elaboração deste trabalho representou uma experiência bastante enriquecedora para o grupo, e permitiu-nos obter um conhecimento do sistema operativo linux muito mais alargado e coeso do que aquele que tínhamos antes de realizar este trabalho prático. Simultaneamente, percebemos a complexidade e a prática requerida para implementar redes, quer a nível da configuração, quer a nível da própria topologia interna da rede.

Relativamente ao trabalho prático em si, o que se revelou mais difícil foi a integração de todos os serviços implementados, nomeadamente da integração dos serviços com o AFS, que representa uma tecnologia radicalmente diferente da do NFS, o que nos colocou alguns problemas de configuração pois estávamos a lidar com algo de novo e muito diferente pela primeira vez.

Em jeito de conclusão, e tendo em conta todos os aspectos que envolveram a elaboração deste trabalho prático, podemos concluir que este trabalho foi uma experiência bastante valiosa para o nosso conhecimento de redes e para uma eventual experiência prática na concepção de redes num futuro próximo.