



Universidad de Palermo - Facultad de
Ingeniería
Computación Aplicada

TRABAJO PRÁCTICO I

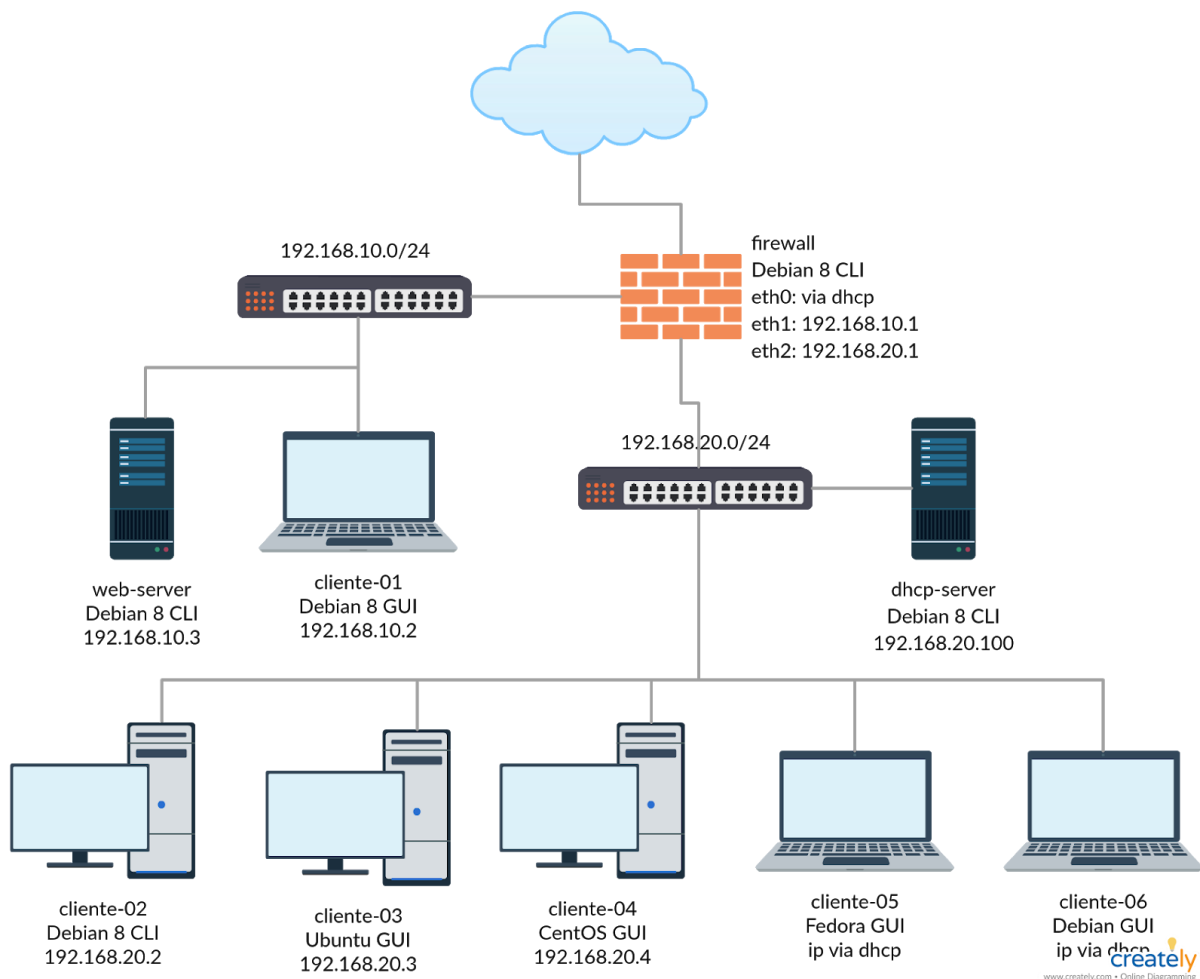
Miguel Calzadilla
Legajo : 0113192

Introducción

En el siguiente documento podrán ver los pasos realizados para la implementación del trabajo práctico solicitado, se detalla los pasos para la configuración de las 9 máquinas virtuales, capturas de pantallas de los archivos de configuración y estados de las máquinas, y al final podrán observar como se previsualiza el VirtualBox con las configuraciones generales.

Parte I - Topología fisica y logica de la red

A continuación veremos la imagen de la topología de red utilizada como base para la implementación de este trabajo práctico.



Parte II - Configuración de las Máquinas Virtuales

Firewall

Lo primero que realice fue configurar la máquina virtual, con 3 adaptadores de red, desde el virtualbox, quedando de la siguiente manera

Network

Adapter 1: Intel PRO/1000 MT Desktop (Bridged Adapter, wlp2s0)
Adapter 2: Intel PRO/1000 MT Desktop (Internal Network, '192.168.10.0_24')
Adapter 3: Intel PRO/1000 MT Desktop (Internal Network, '192.168.20.0_24')

Luego pase a la modificación del archivo de configuración de las interfaces de red, de manera tal que cumpliera con la topología de red propuesta, el archivo de configuración se encuentra en `/etc/network/interfaces`, quedando el archivo de interfaces de la siguiente manera.

```
root@firewall:~# cat /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug eth0
iface eth0 inet dhcp

# .10 network interface
allow-hotplug eth1
iface eth1 inet static
    address    192.168.10.1
    netmask    255.255.255.0
    broadcast  192.168.10.255

# .20 network interface
allow-hotplug eth2
iface eth2 inet static
    address    192.168.20.1
    netmask    255.255.255.0
    broadcast  192.168.20.255
root@firewall:~#
```

Luego pase a realizar la configuración de las reglas del firewall a través de iptables

según las siguientes consignas:

1- El firewall deberá cargar la configuración de iptables al inicio.

Para este paso cree el archivo *iptables* en la siguiente ubicación */etc/network/if-up.d/*, con la siguiente información:

```
# script para cargar reglas de configuracion de iptables en el boot
#!/bin/sh
iptables-restore < /etc/rules.ipv4.conf
```

Paso siguiente ejecute el comando *chmod +x iptables* para hacerlo ejecutable, quedando de la siguiente manera

```
root@firewall:/etc/network/if-up.d# ls -l iptables
-rwxr-xr-x 1 root root 50 Jun 10 22:37 iptables
```

2- Las políticas por defecto de las 3 cadenas de la tabla FILTER sea DROP.

Implemente los siguientes comandos

```
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
```

3 - El tráfico desde/hacia la interfaz loopback sea posible.

Implemente los siguientes comandos

```
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT
```

4- La única VM que pueda administrar el firewall vía ssh (puerto tcp 22) sea cliente-02.

Implemente los siguientes comandos

```
iptables -A INPUT -i eth2 -s 192.168.20.2 -p tcp --dport 22 -j ACCEPT
iptables -A OUTPUT -o eth2 -d 192.168.20.2 -p tcp --sport 22 -j ACCEPT
```

5- La única VM que pueda navegar por internet sea cliente-03.

```
iptables -A INPUT -i eth0 -j ACCEPT
iptables -A OUTPUT -o eth0 -j ACCEPT
```

```
iptables -A FORWARD -i eth2 -s 192.168.20.3 -o eth0 -j ACCEPT
iptables -A FORWARD -i eth0 -d 192.168.20.3 -o eth2 -j ACCEPT
iptables -t nat -A POSTROUTING -s 192.168.20.3 -o eth0 -j MASQUERADE
```

6- La única VM de la red 192.168.20.0/24 que pueda ingresar al web server de la red 10.0 sea cliente-04.

```
Iptables -A FORWARD -i eth2 -s 192.168.20.4 -o eth1 -d 192.168.10.3 -j ACCEPT
Iptables -A FORWARD -i eth1 -s 192.168.10.3 -o eth2 -d 192.168.20.4 -j ACCEPT
```

Quedando la configuración de la tabla de la siguiente manera.

```
root@firewall:~# iptables -L -n -v
Chain INPUT (policy DROP 0 packets, 0 bytes)
  pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     all  --  lo      *        0.0.0.0/0            0.0.0.0/0
    0     0 ACCEPT     tcp  --  eth2    *      192.168.20.2         0.0.0.0/0            tcp dpt:22
 2152 114K ACCEPT     all  --  eth0    *        0.0.0.0/0            0.0.0.0/0

Chain FORWARD (policy DROP 0 packets, 0 bytes)
  pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     all  --  eth2    eth0    192.168.20.3         0.0.0.0/0
    0     0 ACCEPT     all  --  eth0    eth2    0.0.0.0/0            192.168.20.3
    0     0 ACCEPT     all  --  eth2    eth1    192.168.20.4         192.168.10.3
    0     0 ACCEPT     all  --  eth1    eth2    192.168.10.3         192.168.20.4

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
  pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     all  --  *       lo      0.0.0.0/0            0.0.0.0/0
    0     0 ACCEPT     tcp  --  *       eth2    0.0.0.0/0            192.168.20.2            tcp spt:22
   42 3668 ACCEPT     all  --  *       eth0    0.0.0.0/0            0.0.0.0/0
```

Y la tabla NAT de la siguiente manera.

```
root@firewall:~# iptables -t nat -L -n -v
Chain PREROUTING (policy ACCEPT 2 packets, 98 bytes)
  pkts bytes target     prot opt in     out     source               destination

Chain INPUT (policy ACCEPT 2 packets, 98 bytes)
  pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 22 packets, 1364 bytes)
  pkts bytes target     prot opt in     out     source               destination

Chain POSTROUTING (policy ACCEPT 22 packets, 1364 bytes)
  pkts bytes target     prot opt in     out     source               destination
    0     0 MASQUERADE all  --  *       eth0    192.168.20.3         0.0.0.0/0
```

Servidor-Web

El servidor web tiene que tener una dirección de IP fija, es por eso que configure el archivo interfaces, mencionado anteriormente, de la siguiente manera

```
# The primary network interface
auto eth0
iface eth0 inet static
    address    192.168.10.3
    netmask    255.255.255.0
    broadcast  192.168.10.255
    network    192.168.10.0
    gateway    192.168.10.1
```

Para configurar el servidor web son necesarios dos elementos, el Java Development Kit (JDK) y el Apache Tomcat. como primero descargue en mi máquina local, desde la página de Oracle, el JDK 8u202 y a través de scp copie el archivo de mi máquina local al servidor-web

\$ scp jdk-8u202-linux-x64.tar.gz root@<dirección de red> :

El mismo procedimiento lo realice con el paquete de apache

\$ scp apache-tomcat-8.5.55.tar.gz root@<dirección de red> :

Una vez teniendo ambos archivos de forma local en el servidor y estando posicionado en el directorio donde se encontraban, los descomprimi en el directorio /opt/ con los siguientes comandos

\$ tar xzvf jdk-8u202-linux-x64.tar.gz -C /opt/
\$ tar xzvf apache-tomcat-8.5.55.tar.gz -C /opt/

Ahora para que el sistema pueda saber dónde están los archivos de configuración y binarios del JDK tuve que crear la variable JAVA_HOME en el archivo ~/.bashrc

Implemente las siguientes líneas al final del archivo .bashrc

```
#JDK
JAVA_HOME=/opt/jdk1.8.0_202
export PATH=$PATH:$JAVA_HOME/bin
```

Para corroborar que funciona de manera correcta corremos el comando
\$ java -version

```
root@web-server:~# java -version
java version "1.8.0_202"
Java(TM) SE Runtime Environment (build 1.8.0_202-b08)
Java HotSpot(TM) 64-Bit Server VM (build 25.202-b08, mixed mode)
```

Ahora para iniciar el servicio de apache, se tiene que ir a la siguiente ubicación

cd /opt/apache-tomcat-8.5.55/bin

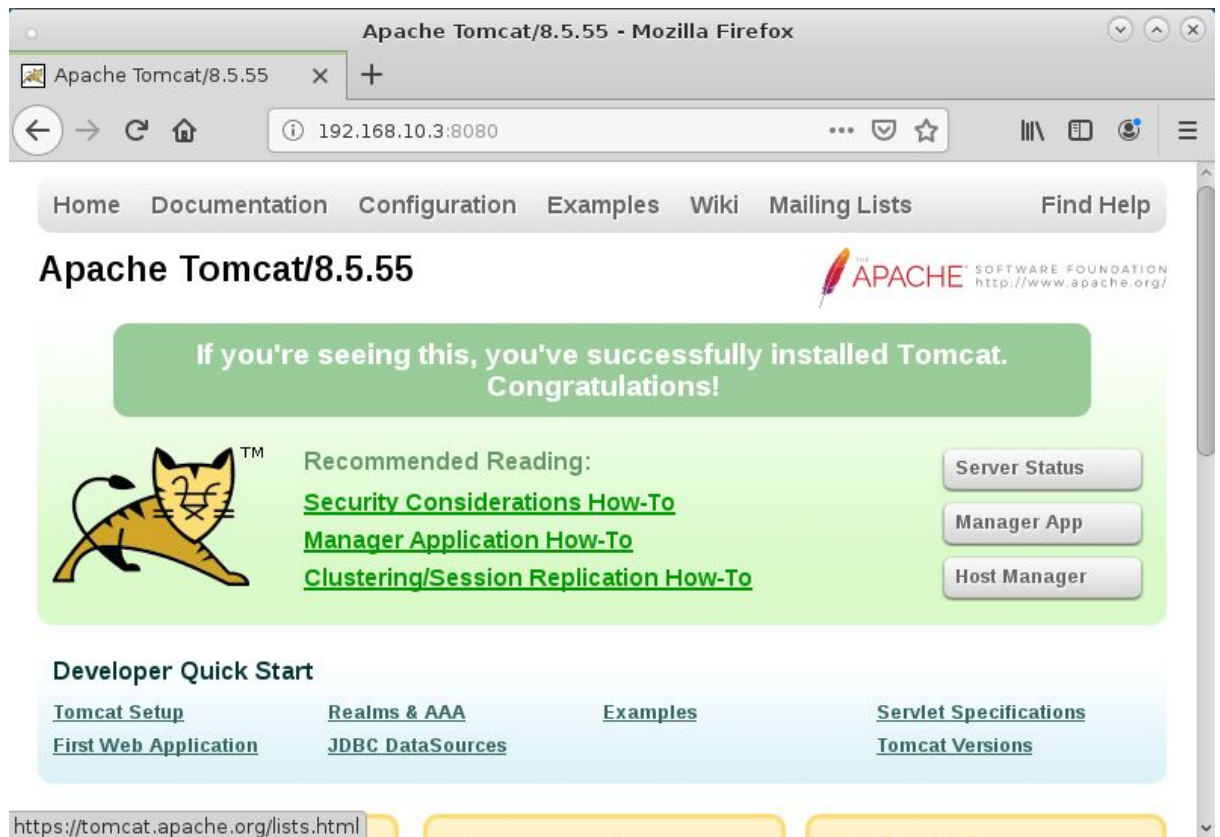
Y ejecutamos el comando **./startup.sh** y nos debera salir la siguiente pantalla

```
root@web-server:/opt/apache-tomcat-8.5.55/bin# ./startup.sh
Using CATALINA_BASE:   /opt/apache-tomcat-8.5.55
Using CATALINA_HOME:   /opt/apache-tomcat-8.5.55
Using CATALINA_TMPDIR: /opt/apache-tomcat-8.5.55/temp
Using JRE_HOME:        /opt/jdk1.8.0_202
Using CLASSPATH:        /opt/apache-tomcat-8.5.55/bin/bootstrap.jar:/opt/apache-tomcat-8.5.55/bin/tomcat-juli.jar
Tomcat started.
```

También con el siguiente comando podemos verificar que el servicio está corriendo

\$ systemctl status tomcat.service

Si accedemos desde un cliente con GUI a la direccion 192.168.10.3:8080/ podremos ver que el servicio está corriendo correctamente



Como paso final nos pedían cargar una aplicación de prueba en el servidor, la misma fue obtenida a través de una máquina con GUI, con el siguiente comando.

```
$ wget https://tomcat.apache.org/tomcat-7.0-doc/appdev/sample/sample.war
```

Y como se mostró en los pasos anteriores copie el archivo sample.war con scp al servidor web, luego con el siguiente comando moví el archivo al directorio de webapps

```
$ mv sample.war /opt/apache-tomcat-8.5.55/webapps/
```


La aplicaciom descargada la visualizamos ingresando a traves de 192.168.10.3:8080/sample/



Servidor DHCP

Como primer paso para que nuestro servidor DHCP funcione debemos asignarle una dirección IP estática, configure el archivo interfaces mencionado antes de la siguiente manera

```
# The primary network interface
auto eth0
iface eth0 inet static
    address    192.168.20.100
    netmask    255.255.255.0
    broadcast  192.168.20.255
    network    192.168.20.0
    gateway    192.168.20.1
```

Luego procedi a instalar el ISC DHCP con el siguiente comando

\$ apt-get install isc-dhcp-server

Luego pase a configurar el archivo que indica porque interfaz de red el servidor va a ofrecer las direcciones IP, en este caso es la interfaz eth0, el archivo se encuentra en la siguiente ubicación */etc/defaults/isc-dhcp-server*

```

GNU nano 2.2.6                               File: /etc/default/isc-dhcp-server

# Defaults for isc-dhcp-server initscript
# sourced by /etc/init.d/isc-dhcp-server
# installed at /etc/default/isc-dhcp-server by the maintainer scripts
#
# This is a POSIX shell fragment
#
# Path to dhcpd's config file (default: /etc/dhcp/dhcpd.conf).
#DHCPD_CONF=/etc/dhcp/dhcpd.conf
#
# Path to dhcpd's PID file (default: /var/run/dhcpd.pid).
#DHCPD_PID=/var/run/dhcpd.pid
#
# Additional options to start dhcpd with.
# Don't use options -cf or -pf here; use DHCPD_CONF/ DHCPD_PID instead
#OPTIONS=""
#
# On what interfaces should the DHCP server (dhcpd) serve DHCP requests?
# Separate multiple interfaces with spaces, e.g. "eth0 eth1".
INTERFACES="eth0"

```

Paso siguiente configure el archivo donde está contenida la mayor parte de la configuración del DHCP, */etc/dhcp/dhcpd.conf*, como este archivo trae por defecto información y ejemplos de como configurarlo, mostraré la primera parte y la última parte, que son las que nos interesa para la configuración que se solicitó.

```

# The ddns-updates-style parameter controls whether or not the server will
# attempt to do a DNS update when a lease is confirmed. We default to the
# behavior of the version 2 packages ('none', since DHCP v2 didn't
# have support for DDNS.)
ddns-update-style none;

# option definitions common to all supported networks...
option domain-name "homenet";
option domain-name-servers 8.8.8.8;

default-lease-time 600;
max-lease-time 7200;

# If this DHCP server is the official DHCP server for the local
# network, the authoritative directive should be uncommented.
authoritative;

# Use this to send dhcp log messages to a different log file (you also
# have to hack syslog.conf to complete the redirection).
log-facility local7;

```

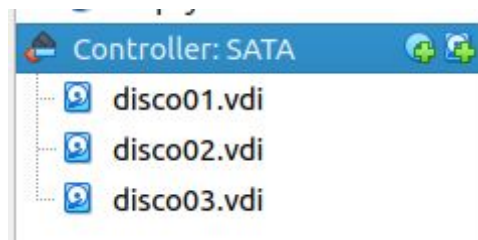
```
# Subnet homenet

subnet 192.168.20.0 netmask 255.255.255.0 {
    range 192.168.20.101 192.168.20.110;
    option routers 192.168.20.1;
    option broadcast-address 192.168.20.255;
}
```

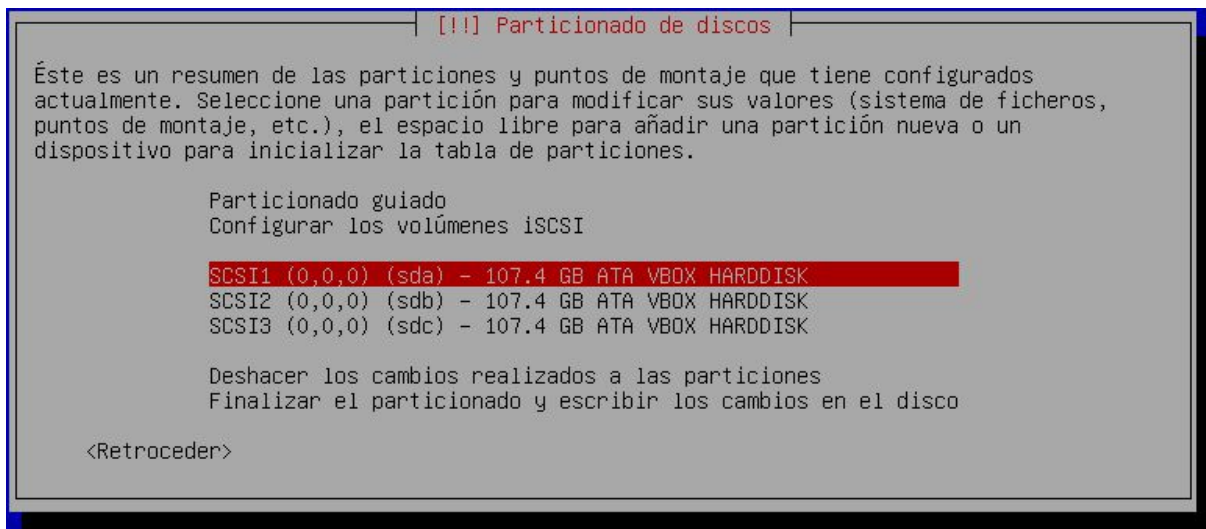
Como podemos ver el servidor DHCP ofrece direcciones IP del rango 192.168.20.101 al 192.168.20.110

Logical Volume Manager

Para poder llevar a cabo la implementación del LVM en el cliente-02 primero cree una maquina virtual en el Virtual Box con el debian-8.10.0-amd64-CD-1.iso, con un disco duro de 100GB, posteriormente cree dos discos duros de 100GB cada uno y se los asigne a la VM cliente-02 quedando de la siguiente manera

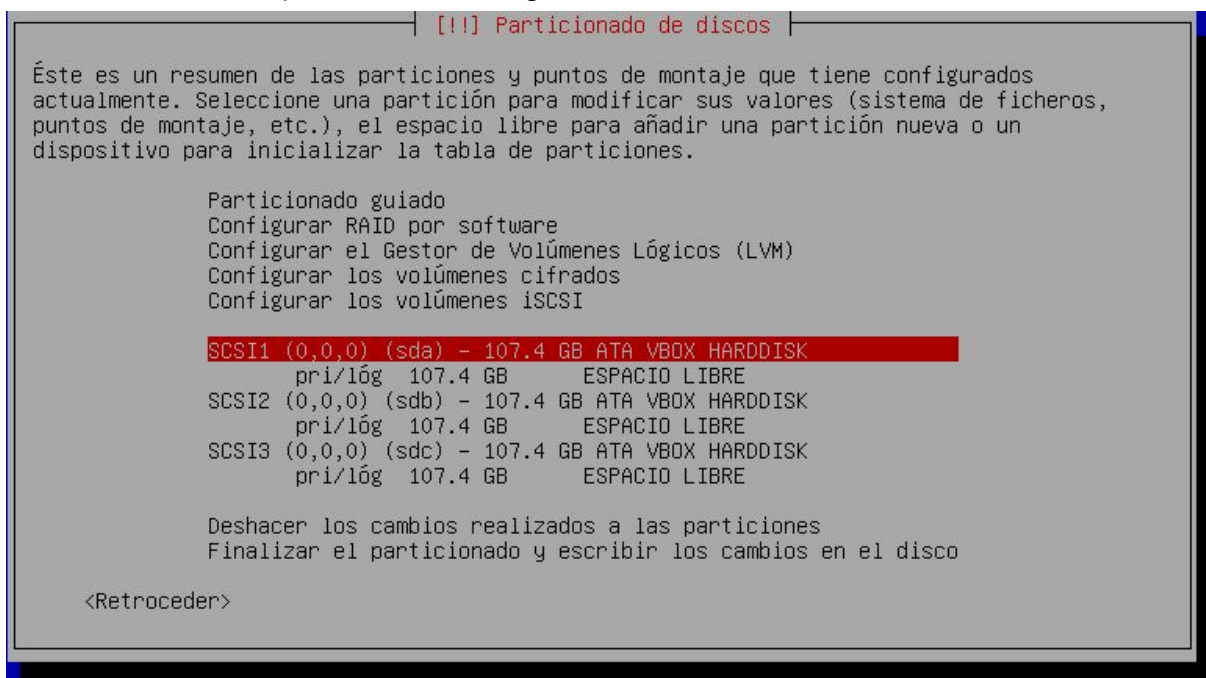


Una vez iniciada la VM y siguiendo los pasos de la configuración inicial, llegamos a la sección del particionado de discos, aquí fue donde implemente los cambios necesarios para poder hacer el LVM,



antes de implementar los cambios

Primero seleccione los 3 discos disponibles para crear una tabla de partición en cada uno de ellos, quedando de la siguiente manera



Antes de implementar LVM, opte por implementar RAID por software, decidí implementar un RAID 5 ya que si alguno de los discos falla, con los bloques de paridad se podría recuperar la información.

En la opción de configurar RAID por software, seleccione crear un dispositivo md de RAID 5, con un array de 3 dispositivos activos y 0 dispositivos libre, si bien entiendo que para que en caso de que falle se debe contar con un dispositivo libre, por esta oportunidad lo dejaré configurado de esa manera.

Quedando la sección de particionado de discos de la siguiente manera

```
[!!!] Particionado de discos

Éste es un resumen de las particiones y puntos de montaje que tiene configurados
actualmente. Seleccione una partición para modificar sus valores (sistema de ficheros,
puntos de montaje, etc.), el espacio libre para añadir una partición nueva o un
dispositivo para inicializar la tabla de particiones.

Particionado guiado
Configurar RAID por software
Configurar el Gestor de Volúmenes Lógicos (LVM)
Configurar los volúmenes cifrados
Configurar los volúmenes iSCSI

Dispositivo RAID5 #0 - 214.6 GB Dispositivo RAID por software
#1 214.6 GB
SCSI1 (0,0,0) (sda) - 107.4 GB ATA VBOX HARDDISK
#1 primaria 107.4 GB K raid
SCSI2 (0,0,0) (sdb) - 107.4 GB ATA VBOX HARDDISK
#1 primaria 107.4 GB K raid
SCSI3 (0,0,0) (sdc) - 107.4 GB ATA VBOX HARDDISK
#1 primaria 107.4 GB K raid

Deshacer los cambios realizados a las particiones
Finalizar el particionado y escribir los cambios en el disco

<Retroceder>
```

Luego procedí a configurar el Volumen Lógico para nuestros 3 discos, en el apartado de configurar el gestor de volúmenes lógicos, cree el Volumen Lógico *vg01* y seleccione el dispositivo */dev/md* que es el conjunto de nuestros 3 discos por RAID, luego procedi a crear los volúmenes lógicos, *lv-swap*, *lv-home* y *lv-root* quedando de la siguiente manera

```
[!!!] Particionado de discos

Configuración actual LVM:
Volúmenes físicos no asignados:
* ninguno

Grupo de volúmenes:
* vg01 (214605MB)
- Utiliza el volumen físico: /dev/md0 (214605MB)
- Provee el volumen lógico: lv-home (99996MB)
- Provee el volumen lógico: lv-root (114097MB)
- Provee el volumen lógico: lv-swap (511MB)

<Continuar>
```

Luego en el menú principal de particionado de discos, procedi a asignarle a cada volumen lógico el tipo de formato de archivos y el punto de montaje para cada uno

Configurandolo de la siguiente manera

lv-swap ; utilizar como área de intercambio

lv-home; utilizar como sistema de ficheros ext4 ; punto de montaje /home

lv-root; utilizar como sistema de ficheros ext4 ; punto de montaje / sistema de ficheros raíz

Quedando todo configurado de la siguiente manera

```
[!!] Particionado de discos

Éste es un resumen de las particiones y puntos de montaje que tiene configurados actualmente. Seleccione una partición para modificar sus valores (sistema de ficheros, puntos de montaje, etc.), el espacio libre para añadir una partición nueva o un dispositivo para inicializar la tabla de particiones.

Particionado guiado
Configurar RAID por software
Configurar el Gestor de Volúmenes Lógicos (LVM)
Configurar los volúmenes cifrados
Configurar los volúmenes iSCSI

LVM VG vg01, LV lv-home - 100.0 GB Linux device-mapper (linear)
#1          100.0 GB   f  ext4          /home
LVM VG vg01, LV lv-root - 114.1 GB Linux device-mapper (linear)
#1          114.1 GB   f  ext4          /
LVM VG vg01, LV lv-swap - 511.7 MB Linux device-mapper (linear)
#1          511.7 MB   f  intercambio   intercambio
Dispositivo RAID5 #0 - 214.6 GB Dispositivo RAID por software
#1          214.6 GB   K  lvm
SCSI1 (0,0,0) (sda) - 107.4 GB ATA VBOX HARDDISK
#1 primaria 107.4 GB   K  raid
SCSI2 (0,0,0) (sdb) - 107.4 GB ATA VBOX HARDDISK
#1 primaria 107.4 GB   K  raid
SCSI3 (0,0,0) (sdc) - 107.4 GB ATA VBOX HARDDISK
#1 primaria 107.4 GB   K  raid

Deshacer los cambios realizados a las particiones
Finalizar el particionado y escribir los cambios en el disco

<Retroceder>
```

Finalizamos el proceso de instalación y una vez nuestra máquina andando con el comando `lvmdiskscan` podremos ver el detalle de nuestro LVM PV y los LV.

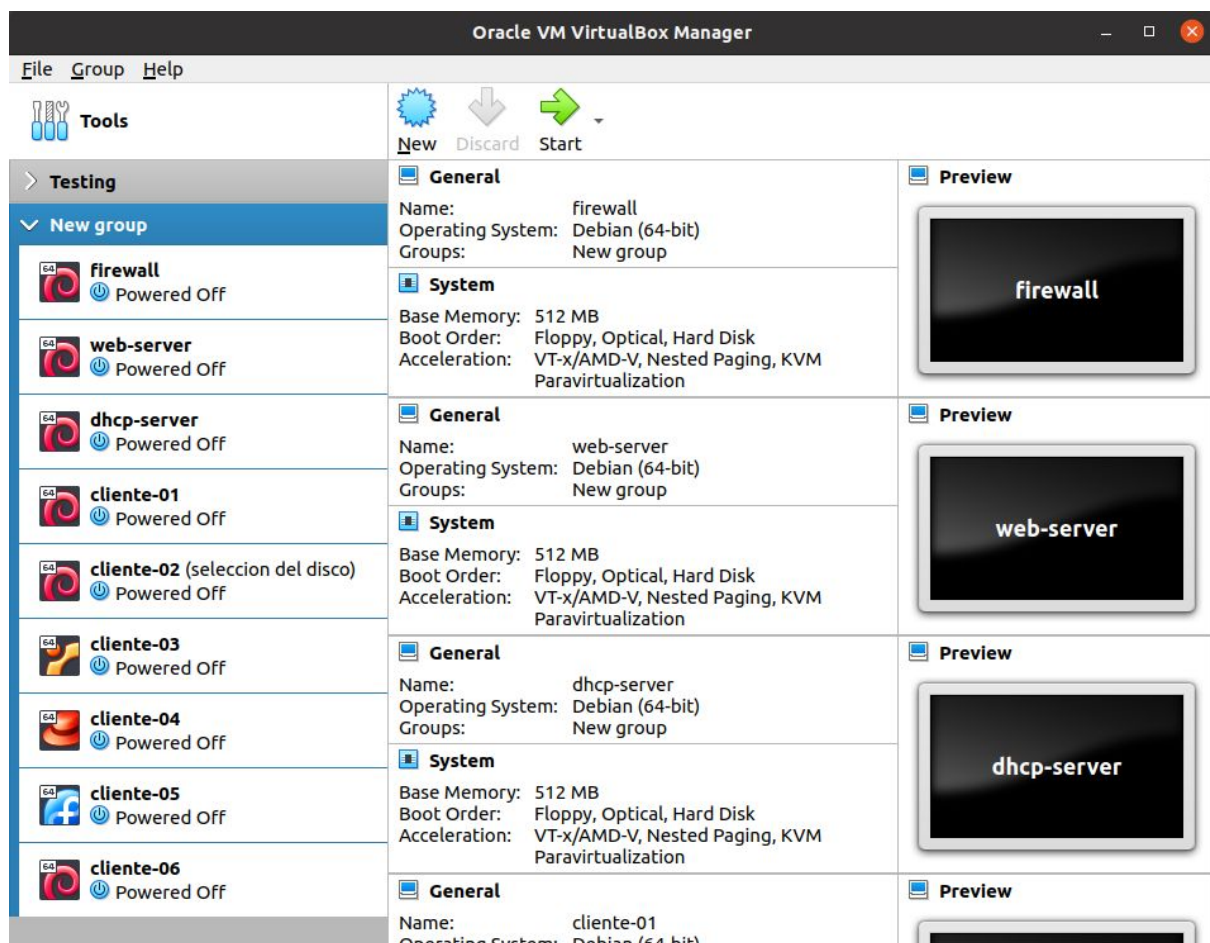

```

root@cliente-02:~# lvm diskscan
/dev/md0          [    199,87 GiB] LVM physical volume
/dev/vg01/lv-home [    93,13 GiB]
/dev/vg01/lv-swap [    488,00 MiB]
/dev/vg01/lv-root [    106,26 GiB]
3 disks
0 partitions
0 LVM physical volume whole disks
1 LVM physical volume

```

Máquinas Virtuales

Este es un pantallazo de como se ve el trabajo práctico en el Virtual Box



Cabe destacar que para poder cumplir con la topología de red solicitada en este tp cree dos redes virtuales internas en el virtualbox y las configure a cada máquina según lo solicitado en la topología de red.

Las máquinas con distribuciones debian fueron instaladas con la imagen debian-8.10.0-amd64-netinst.iso obtenida del siguiente link:

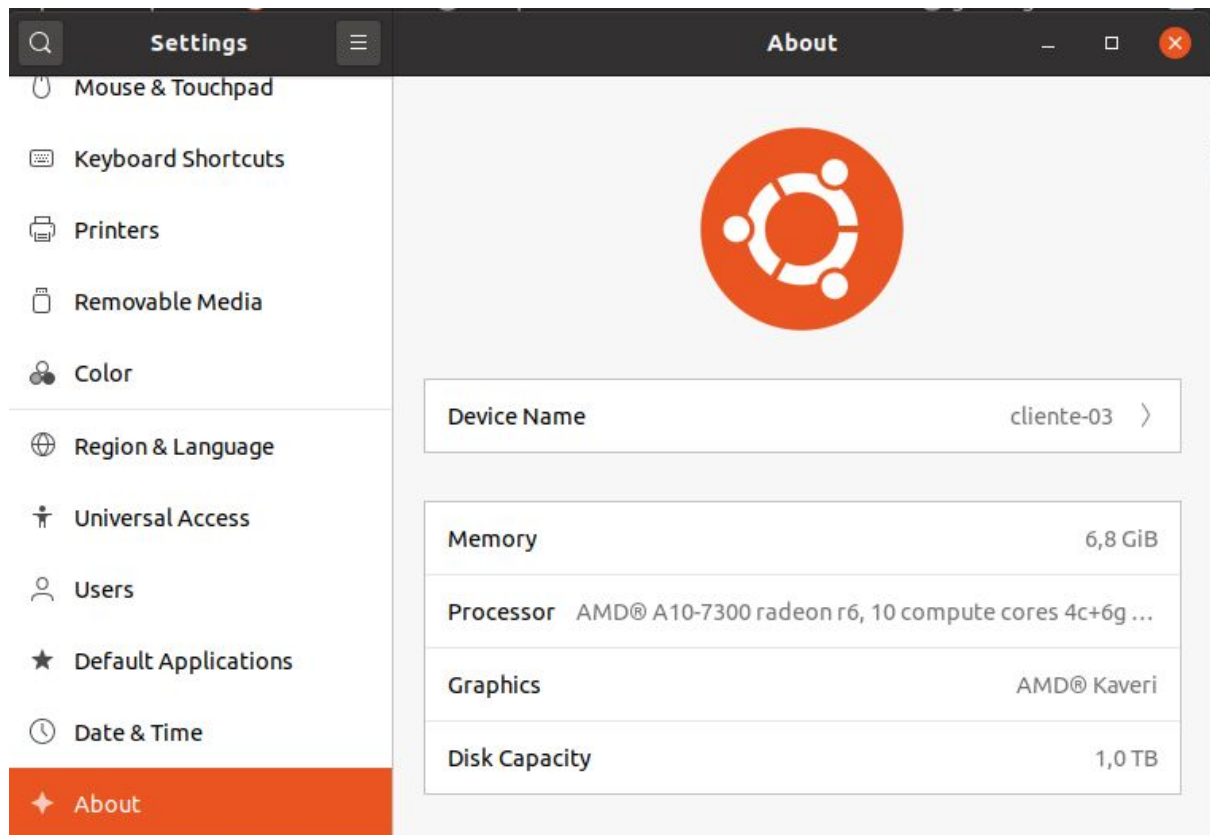
<https://cdimage.debian.org/cdimage/archive/8.10.0/amd64/iso-cd/>

Los clientes 1 y 6 tienen un (GUI) entorno gráfico MATE



El cliente-03 tiene una distribución de Ubuntu 20.4 cuya imagen fue obtenida a través del siguiente link siguiente link

<https://ubuntu.com/#download>



El cliente-04 tiene una distribución CentOS, cuya imagen fue obtenida a través del siguiente link

<https://wiki.centos.org/Download>

Jun 15 17:53



Miguel Calzadilla

Not listed?



CentOS



El cliente-05 tiene una distribución Fedora, cuya imagen de instalación fue obtenida a través del siguiente link

<https://getfedora.org/es/workstation/download/>



En cada cliente se configuró una dirección IP estática o por DHCP según la topología de red, las configuraciones se hicieron en el archivo interfaces ubicado en etc/network/.