ADMINISTRACION DE SISTEMAS OPERATIVOS Y REDES DE COMPUTADORES

PRACTICA 2:

Instalación, puesta en marcha y evaluación de servicios básicos sobre los sistemas operativos

Xavier Siguero Mora 48787124F

Contenido

Introducción 4

Windows Server 2016 5

Particiones: 5

Seguridad: 5

SSH: 5

VNC Server: 5

RDP Server: 5

NX: 5

DNS: 6

DHCP: 6

NFS: 6

SAMBA: 6

FTP: 6

SENDMAIL: 7

CUPS: 7

LDAP 7

CentOS 8

Particiones: 8

Seguridad 8

SSH: 8

VNC Server: 9

RDP Server: 9

NX: 9

DNS: 10

DHCP: 10

NFS: 11

CUPS: 11

SAMBA: 11

FTP: 12

SENDMAIL: 12

LDAP 12

FreeBSD 13

Particiones: 13

Seguridad 13

SSH: 13

VNC Server: 14
RDP Server:..... 14
NX: 14
DNS:..... 14
DHCP:..... 14
NFS: 14
SAMBA:..... 15
FTP:..... 15
CUPS: 16
SENDMAIL: 16
LDAP 16

Introducción

En esta practica debemos familiarizarnos con varios programas muy comunes, todos enfocados al su uso en servidores, como utilizar un ordenador desde un escritorio remoto, compartir archivos, impresoras, servicios de email, DNS y DHSP. Además de la variedad en cuanto a servicios, también hemos de ser capaces de ejecutarlo en sistemas operativos con distintas bases: Windows, Linux y Unix.

En nuestro caso hemos usado Windows Server 2016, CentOS y FreeBSD virtualizados como servidores y como cliente hemos usado el sistema que los virtualizaba, Windows 10.

En todos los sistemas usamos la misma clave para las conexiones SSH. La clave se genera con con Puttygen, creamos una nueva clave privada y la guardamos tanto en el formato de Putty (.ppk) como en el de OpenSSH (La cual la usaremos en determinados servicios como NX). Esta clave privada habrá que referenciarla en Putty en ssh/autentification. La clave publica la guardaremos para introducirla cuando configuremos SSH.

Además, en todos hemos puesto la IP estática. Este proceso lo explico dentro del apartado de DHCP de cada sistema operativo, ya que es el único servicio que necesita obligatoriamente una IP estática para ejecutarse.

Windows Server 2016

Particiones:

Añadimos un disco de 20gb en VirtualBox. En este disco haremos 5 particiones, de 4GB cada una. Estas particiones serán usadas para los servicios que impliquen almacenar datos para evitar almacenarlos en la misma partición del sistema operativo. Es decir: NFS, SAMBA, FTP, SENDMAIL y LDAP.

En el buscador de Windows buscamos *Crea y formatea particiones de disco duro*, hacemos clic derecho en el nuevo disco que hemos insertado y pulsamos *Nuevo volumen*, le asignamos 4096mb y continuamos hasta finalizar la partición: Repetimos 5 veces este proceso para tener las particiones.

Seguridad:

Ya deberiamos tener el firewall desactivado de la practica anterior, en caso de no ser asi hay que desactivarlo desde Windows Defender.

SSH:

Descargamos Bitvise SSH Server (https://www.bitvise.com/ssh-server-download). Una vez instalado cambiamos el Puerto de ssh al 1234 y en windows accounts seleccionamos *allow all*. Después de la configuracion inicial reiniciamos el servidor para que el servicio sea completamente funcional. Una vez reiniciado el sistema volvemos a abrir el programa y pasamos por los siguientes menus: *Edit advanced settings -> Windows accounts -> add -> Autentification -> Public keys* e importamos nuestra clave publica .pub generada anteriormente con Putyygen.

En el cliente abrimos Putty, ponemos tanto la IP como el Puerto y en ssh/autentification seleccionamos el directorio donde se encuentra la clave privada.

VNC Server:

Descargamos Tightvnc (https://www.tightvnc.com/download.php), lo instalamos y elegimos las contraseñas(root). Abrimos Tightvnc Service que estara minimizado en la barra de tareas y ponemos el Puerto 5901 y las contraseñas.

En el cliente nos conectamos mediante VNC Viewer por la direccion 192.168.56.108:5901

RDP Server:

Administrador de servidor-> servidor local -> escritorio remoto -> permitir las conexiones remotas a este equipo -> actualizar servidor local.

En el cliente: *Conexión a escritorio remoto -> mas opciones*, metemos la ip y el usuario.

NX:

Descargamos nomachine (https://www.nomachine.com/es) tanto en el cliente como en el servidor

Ejecutamos el programa tanto en el cliente como en el servidor y nos aseguramos de que la conexión se hace por 192.1168.56.108 y no por 10.0.0.X

DNS:

DHCP:

Primero cambiamos la ip por una ip estatica. Para ello vamos al panel de control-> Redes e Internet -> Centro de redes y recursos compartidos -> Elegimos la red no identificada -> TCP/IPv4 -> propiedades -> Usar la siguiente dirección, 192.168.56.108

Abrimos el *Administrador del servidor -> Agregar roles y características* y pulsamos *Siguiente* hasta que aparecen las características, donde seleccionamos *Servidor DHCP* y pulsamos *Agregar*, después pulsamos *Siguiente* hasta llegar al final e instalamos el servicio.

Una vez instalado vamos al panel lateral del Administrador del servidor y seleccionamos DHCP, pulsamos en el aviso que nos dice que el servidor necesita configuración, *completar Configuración -> Confirmar -> Cerrar*.

En el Administrador del servidor vamos a *Herramientas -> DHCP*. Dentro de este menú hacemos click en el único desplegable de la izquierda y luego desplegamos IPv4, hacemos click derecho en IPv4 y pulsamos en *Ámbito nuevo…,* le ponemos un nombre (asorc) y ponemos las IP inicial y final (192.168.56.151 y 192.168.56.200) y pulsamos siguiente hasta finalizar.

Probaremos que el servidor esta bien configurado con DHCPtest, un programa que sirve para testear los servidores DHCP.

NFS:

Lo usaremos en la partición que hemos llamado particion1.

Administrador de servidor-> Administrar-> Agregar roles y características

Pulsamos *Siguiente* hasta *Roles de servidor*, seleccionamos *Servicios de archivos y almacenamiento/Servicios de iSCSI y archivos* y *Servicios de archivos y almacenamiento/Servidor para NFS*, *Agregar características*. *Siguiente* hasta *Instalar*

Panel lateral -> *Servicios de archivos y almacenamiento -> Recursos compartidos -> TAREAS -> Nuevo recurso -> NFS rápido -> Ubicación recurso compartido* -> Ruta personalizada (E:) -> Nombre del recurso compartido (particion1) -> *Autentificación* seleccionamos todas las casillas -> Agregar permisos 192.168.56.1, lectura y escritura. *Siguiente* hasta *crear.*

En el cliente ejecutamos `mount WIN-GAEINLKO0EO:/particion1 M:` en el CMD.

SAMBA:

Lo usaremos en la partición que hemos llamado particion2.

Se instala igual que NFS, pero en vez de elegir NFS rápido elegimos SMB rápido.

En el cliente usamos el programa Ejecutar (El cual Tambien se puede abrir con el atajo de teclado Win+R) y escribimos \\WIN-GAEINLKO0EO\particion2

FTP:

Lo usaremos en la partición que hemos llamado particion3.

Descargar serv-u (https://www.serv-u.com/) e instalarlo. Agregar, deseleccionamos la casilla. Cuando acabe cerramos el programa y lo volvemos a abrir para acceder al asistente de configuración. Pulsamos sobre *Agregar dominio*, cuando nos pidan un nombre se lo daremos,

en nuestro caso este nombre es asorc. Solo seleccionamos *File transfer domain* y pulsamos *Siguiente*. Crear usuarios y seleccionamos nuestro disco G:.

Desde el cliente nos conectamos desde Filezilla poniendo la IP, el usuario y la contraseña.

SENDMAIL:

CUPS:

Como CUPS no tiene una version para windows en su lugar instalaremos PDF Creator (https://www.pdfforge.org/pdfcreator)

Una vez instalado vamos a dispositivos e impresoras hacemos click derecho en PDFCreator y seleccionamos propiedades de la impresora, entramos en la pestaña compartir y tickamos en las cajas

En el cliente vamos a dispositivos e impresoras , añadir nueva impresora, no se encuentra aqui, direccion, \\192.168.56.108\PDF Architect 6

LDAP:

CentOS

Particiones:

Añadimos un disco de 20gb. Ejecutamos `fdisk /dev/sdb y` creamos 3 particiones primarias de 4GB. La 4 partición será extended y tendrá el resto del espacio del disco, una vez creada, creamos las otras dos particiones restantes de 4gb cada una. Formateamos todas las particiones menos la extended (la 4): `mkfs.ext4 /dev/sdb1` y los montamos `mkdir /particion1,mount /dev/sdb1 /particion1/.`

Podemos comprobar que hemos montado bien las particiones con el siguiente comando: `df -h | grep /dev/sdb.`

Por último editamos /etc/fstab para que las particiones se monten automáticamente en el arranque:

```
/dev/sdb1 /particion1                    ext4    defaults  0 1
/dev/sdb2 /particion2                    ext4    defaults  0 1
/dev/sdb3 /particion3                    ext4    defaults  0 1
/dev/sdb5 /particion4                    ext4    defaults  0 1
/dev/sdb6 /particion5                    ext4    defaults  0 1
```

Seguridad

Desactivaremos tanto SELinux como el Firewalld:

Para desactivar SELinux editamos `/etc/sysconfig/selinux` y cambiamos `enforcing` por `disabled`.

Para desactivar el firewalld:

```
Systemctl stop firewalld
Systemctl disable firewalld
```

Y reiniciamos para que todos los cambios se realicen correctamente.

SSH:

Editamos /etc/ssh/sshd_config y cambiamos/añadimos las siguientes lineas:

```
Port 1234
Protocol 2
AllowUsers programador
PermitRootLogin no
PubkeyAuthentication yes
PasswordAuthentication no
```

Con estos parametros cambiamos el Puerto por defecto por temas de seguridad, del 22 al 1234, habilitamos la autentificación con clave publica y evitamos que se pueda conectar desde root.

Para añadir la clave publica primero deberemos generar los directorios y los archivos necesarios. Eso lo haremos generando una clave privada desde CentOS con `ssh-keygen -t rsa` y la copiamos en el fichero authorized_keys, el cual tiene las claves autorizadas para conectarse al servidor: `mv ~/.ssh/id_rsa.pub ~/.ssh/authorized_keys`

Abrimos este fichero y guardamos la clave publica generada con Puttygen en el.

Reiniciamos el servicio `systemctl restart sshd.service`

El Port maping o Port forwarding implica la redirección de puertos. En nuestro caso redirigiremos el puerto 9000 al 1234:

```
ssh -p 1234 -L 0.0.0.0:9000:localhost:1234 programador@localhost
```

Y comprobamos que lo hemos realizado correctamente con:

```
netstat -lnp | grep 9000
```

Ejecutamos el servicio en el server con:

```
ssh -p 1234 programador@192.168.56.104
```

Nos conectamos en el cliente con Putty exactamente igual que en el resto de sistemas.

VNC Server:

Lo instalamos con `yum -y install tigervnc-server`

Creamos y modificamos el archivo de configuración del display 1:

```
cp /lib/systemd/system/vncserver@.service \
/etc/systemd/system/vncserver@:1.service
```

Modificamos <USER> por nuestro usuario usuario:

```
nano /etc/systemd/system/vncserver@\:1.service
```

Configuramos el servicio:

```
su - usuario
vncserver
```

Ejecutar server:

```
systemctl start vncserver@:1.service
```

Ejecutar cliente con VNC viewer: ip:1, contraseña -> root12

RDP Server:

Lo instalamos con `yum install xrdp --enablerepo=cr`

Ejecutar el servicio:

```
systemctl start xrdp
```

En el cliente ejecutar Conexión a Escritorio Remoto, y nos conectamos con la IP.

Este servicio funciona perfectamente, pero como implica actualizar XORG, el sistema pierde el escritorio al reiniciarlo, por lo que no es utilizable.

NX:

Lo instalamos con `yum -y install x2goserver x2goserver-xsession`

En el cliente elegimos Conexión al escritorio local y en la configuración seleccionamos la clave de OpenSSH.

DNS:

Lo instalamos con `yum install bind`

Lo configuramos con `nano /etc/named.conf`

```
#listen-on port
allow-query { localhost; 192.168.56.222; };
forwarders { 8.8.8.8; 1.1.1.1; };

zone "asorc.local" IN {
        type master;
        file "asorc.local";
};
zone "56.168.192.in-addre.arpa" IN {
        type master;
        file "reverse.local";
};

nano /var/named/asorc.local
$TTL 86400
@ IN SOA asorc.local root.asorc.local.
(150115 28800 7200 604800 86400)
IN NS servidor.asorc.local.
asorc.local. IN A 216.58.211.35

nano /var/named/reverse.local

$TTL 86400
@ IN SOA asorc.local root.asorc.local.
(150115 28800 7200 604800 86400)
IN NS servidor.asorc.local.
35.211.58.216.in-addr.arp in PTR asorc.local
```

DHCP:

Para establecer una IP estática ejecutamos `nmtui`, modificar una conexión, seleccionamos Conexión cableada 1, cambiamos IPv4 *automático* por *manual.*

IPv4 -> `Mostrar` -> `Direcciones` -> `Añadir`, 192.168.56.104/24

```
service network restart
```

Después de esto procedemos con DCHP: `yum install dhcp`

```
nano /etc/dhcp/dhcpd.conf
subnet 192.168.56.0 netmask 255.255.255.0 {
      range 192.168.56.51 192.168.56.100;
      option domain-name-servers 8.8.8.8;
      option routers 192.168.56.100;
      option broadcast-address 192.168.56.255;
      default-lease-time 600;
      max-lease-time 7200;
}
```

```
systemctl restart dhcpd
```

En el cliente ejecutamos dhcptest-0.7 para comprobar si el servicio funciona.

NFS:

Lo usaremos en la partición que hemos llamado particion1.

Lo instalamos con `yum -y install nfs-utils`

Cambiamos los privilegios de las carpetas: `chmod -R 755 /particion1`

```
chown nfsnobody:nfsnobody /particion1
```

Y configuramos para que solo acceda al directorio que queremos:

```
nano /etc/exports
/particion1        *(rw,sync,no_root_squash,no_all_squash)

systemctl start nfs-server.service
```

En el cliente ejecutamos `mount 192.168.56.104:/particion1 M:` en el CMD.

CUPS:

Lo instalamos con `yum -y install cups cups-pdf`

En CentOS he dado el acceso a la impresora mediante SAMBA, asi que deberemos instalar SAMBA primero.

SAMBA:

Lo usaremos en la partición que hemos llamado particion2.

Lo instalamos con `yum -y install samba samba-client samba-common`

Editamos la configuracion con `nano /etc/samba/smb.conf`

```
workgroup = WORKGROUP
map to guest = Bad User
hosts allow = 192.168.56.1
rpc_server:spoolss = external
rpc_daemon:spoolssd = fork
[Share]
        path = /particion2
        writable = yes
        guest ok = yes
        guest only = yes
        create mode = 0777
        directory mode = 0777
        browseable = Yes
```

Ejecutamos los siguientes comandos:

```
cupsaddsmb -a
systemctl restart smb.service nmb.service
```

En el cliente *Ejecutar* -> \\192.168.56.104, desde ahi podemos acceder tanto a la carpeta compartida como a la impresora. En la impresora hay que escoger el driver MS Color Printer.

FTP:

Lo usaremos en la partición que hemos llamado particion3.

Lo instalamos con `yum -y install vsftpd`

Lo editamos con `nano /etc/vsftpd/vsftpd.conf`

```
anonymus enable no
chroot_local_user=YES
chroot_list_enable=YES
chroot_list_file=/etc/vsftpd/chroot_list
local_root=/particion3

touch /etc/vsftpd/chroot_list
systemctl start vsftpd.service
```

SENDMAIL:

LDAP:

Instalamos con `yum -y install openldap-clients openldap-servers authconfig authconfig-gtk migrationtools`

```
cd /etc/openldap/cacerts
echo "01" > ca.srl
openssl genrsa -aes128 2048 > cacert.key
openssl req -utf8 -new -key cacert.key -out cacert.csr
openssl x509 -req -in cacert.csr -out cacert.pem -signkey
cacert.key -days 3650

openssl genrsa -aes128 2048 > key.pem
openssl req -utf8 -new -key key.pem -out slapd.csr


nano /etc/openldap/slapd.conf
SLAPD_LDAPS=yes
```

FreeBSD

Particiones:

Añadimos un disco de 20gb. En la raíz creamos las 5 carpetas en las cuales montaremos las particiones con `mkdir.` Usamos `sade` para particionar. Elegimos `ada1, Create y` ponemos GPT como tabla. Volvemos a darle a créate y tabulamos para movernos, elegimos 4GB, /particion1/, particion1 y repetimos para las 5 particiones. Finalizamos y ya estaría todo listo.

Seguridad

Desabilitamos el firewall:

```
nano /etc/rc.conf
firewall_enable="NO"
```

Y reiniciamos.

SSH:

Editamos /etc/ssh/sshd_config y cambiamos/añadimos las siguientes lineas:

```
Port 1234
Protocol 2
AllowUsers programador
PermitRootLogin no
PubkeyAuthentication yes
PasswordAuthentication no
```

Con estos parametros cambiamos el Puerto por defecto por temas de seguridad, del 22 al 1234, habilitamos la autentificación con clave publica y evitamos que se pueda conectar desde root.

Para añadir la clave publica primero deberemos generar los directorios y los archivos necesarios. Eso lo haremos generando una clave privada desde CentOS con `ssh-keygen -t rsa` y la copiamos en el fichero authorized_keys, el cual tiene las claves autorizadas para conectarse al servidor: `mv ~/.ssh/id_rsa.pub ~/.ssh/authorized_keys`
Abrimos este fichero y guardamos la clave publica generada con Puttygen en el.

Reiniciamos el servicio `service sshd restart`

El Port maping o Port forwarding implica la redirección de puertos. En nuestro caso redirigiremos el puerto 9000 al 1234:

```
ssh -p 1234 -L 0.0.0.0:9000:localhost:1234 programador@localhost
```

Y comprobamos que lo hemos realizado correctamente con:

```
netstat -lnp | grep 9000
```

Ejecutamos el servicio en el server con:

```
ssh -p 1234 programador@192.168.56.102
```

Ejecutamos Putty en el cliente para conectarnos.

VNC Server:

Instalamos con `pkg install x11vnc`

`x11vnc -storepasswd` para poner la contraseña

contraseña: root

Ejecutamos con `x11vnc -rfbauth ~/.vnc/passwd -forever -display :0 &`

Nos conectamos con VNC Viewer.

RDP Server:

Instalamos con `pkg install xrdp`

```
nano /etc/rc.conf
xrdp_enable="YES"
xrdp_sesman_enable="YES"
service xrdp start
```

NX:

DNS:

DHCP:

Configuramos la IP estatica en `nano /etc/rc.conf`

```
ifconfig_em1="inet 192.168.56.102 netmask 255.255.255.0"
```

Instalamos DHCP con `pkg install isc-dhcp44-server`

Lo habilitamos con `nano /etc/rc.conf`

```
dhcpd_enable="YES"
dhcpd_ifaces="em1"
```

Lo configuramos con `nano /usr/local/etc/dhcpd.conf`

```
subnet 192.168.56.0 netmask 255.255.255.0 {
      range 192.168.56.101 192.168.56.150;
      option domain-name-servers 8.8.8.8;
      option routers 192.168.56.100;
      option broadcast-address 192.168.56.255;
      default-lease-time 600;
      max-lease-time 7200;
}
service isc-dhcpd restart
```

NFS:

Lo usaremos en la partición que hemos llamado particion1.

Editamos las carpetas a compartir con `nano /etc/exports`

```
/particion1 192.168.56.1
```

De manera que se comparta la particion1 y solo pueda acceder a él el host.

Lo habilitamos en `nano /etc/rc.conf`

```
rpcbind_enable="YES"
nfs_server_enable="YES"
mountd_flags="-r"
```

En el cliente ejecutamos `mount 192.168.56.102:/particion1 M:` en el CMD

SAMBA:

Lo usaremos en la partición que hemos llamado particion2.

Lo instalamos con `pkg install samba48`

```
nano /usr/local/etc/smb4.conf
[global]
        workgroup = WORKGROUP
        security = user
        map to guest = Bad User
        hosts allow = 192.168.56.1
        passdb backend = tdbsam
        valid users = programador
[Share]
            path = /particion2
        writable = yes
        guest ok = yes
        guest only = yes
        create mode = 0777
        directory mode = 0777
        browseable = Yes
nano /etc/rc.conf
samba_server_enable="YES"

pdbedit -a -u programador
```

contraseña: root

```
service samba_server start
```

En el cliente *Ejecutar* -> \\192.168.56.102

FTP:

Lo usaremos en la partición que hemos llamado particion2.

Lo configuramos con `nano /etc/ftpchroot`

```
@     /particion3
```

Con esta linea compartimos la particion3 de manera que todos los usuarios puedan acceder a el(a excepcion de los que se encuentran en el fichero ftpusers, el el cual se encuentra root por defecto).

```
nano /etc/rc.conf
ftpd_enable="YES"
```

CUPS:

Lo instalamos con `pkg install cups cups-pdf cups-filters`

Lo configuramos con `nano /etc/devfs.rules`

```
[system=10]
add path 'unlpt*' mode 0660 group cups
add path 'ulpt*' mode 0660 group cups
add path 'lpt*' mode 0660 group cups

nano /etc/rc.conf
cupsd_enable="YES"
devfs_system_ruleset="system"

service devfs restart
service cupsd restart

cupsctl --remote-admin
```

Desde el navegador accedemos a localhost:631 desde el navegador y añadimos una nueva impresora:

Administration -> Add printer -> CUPS-PDF

Name: Cups-PDF, Tick share, Generic, Generic CUPS-PDF Printer (en), Add printer

Cambiamos los permisos de las carpetas en las que se guardan los pdf para poder acceder a ellas desde cualquier usuario:

```
chmod -R 755 /var/spool/cups-pdf
```

En el cliente vamos a Dispositivos e impresoras y Agregar impresoras, no se encuentra, poner la siguente ruta: http://192.168.56.102:631/printers/Virtual_PDF_Printer

SENDMAIL:

LDAP: