Ingeniería de Servidores (2023-2024)
Grado en Ingeniería Informática
Universidad de Granada

Bloque 1 : Instalación y Configuración de Sistema Operativo y Servicios

Índice

OBJETIVOS MÍNIMOS

1. Familiarizarse con el uso de Sistemas Operativos (SOs) en servidores.
2. Adquirir conceptos básicos de Virtualización y sobre su aplicación práctica.
3. Conocer las características de la gestión del espacio de almacenamiento empleando LVM y su aplicación práctica.
4. Conocer las características de RAID, al menos en sus niveles 0, 1 y 5, así como su aplicación práctica.
5. Virtual Box, características de las principales formas de networking virtual: Nat, Host-Only, Bridge.
6. Ser capaz de configurar una red local de máquinas virtuales.
7. Conocer los principales niveles de ejecución en Linux y saber utilizarlos en la administración práctica de sistemas.
8. Conocer las bases de la estructura estándar de directorio en Linux.
9. Entender el concepto de Cortafuegos y saber realizar configuraciones básicas.
10. Saber configurar el servicio de SSHD y acceder a un servidor de manera seguro empleando SSH.
11. Principios básicos de criptografía de llave simétrica y asimétrica. Aplicación en SSH para acceso remoto seguro.
12. Uso de Ansible para la configuración automática de servidores.

Lecciones

1. Instalación y configuración de un servidor base con Rocky.
2. Configuración de LVM + RAID.
3. Configuración de Firewall + SSH para administración remota.
4. Introducción a Ansible.

Competencias que se trabajarán

Competencias Básicas

1. CB2. Que los estudiantes sepan aplicar sus conocimientos a su trabajo o vocación de una forma profesional y posean las competencias que suelen demostrarse por medio de la elaboración y defensa de argumentos y la resolución de problemas dentro de su área de estudio.

Específicas de la Asignatura

1. R1. Capacidad para diseñar, desarrollar, seleccionar y evaluar aplicaciones y sis- temas informáticos, asegurando su fiabilidad, seguridad y calidad, conforme a prin- cipios éticos y a la legislación y normativa vigente.
2. R2. Capacidad para planificar, concebir, desplegar y dirigir proyectos, servicios y sistemas informáticos en todos los ámbitos, liderando su puesta en marcha y su mejora continua y valorando su impacto económico y social.
3. R5. Conocimiento, administración y mantenimiento de sistemas, servicios y aplica- ciones informáticas.

Competencias Específicas del Título:

1. E4. Capacidad para definir, evaluar y seleccionar plataformas hardware y software para el desarrollo y la ejecución de sistemas, servicios y aplicaciones informáticas.

Competencias Transversales o Generales:

1. T2. Capacidad de organización y planificación así como capacidad de gestión de la Información.

1.- Introducción

En esta práctica el alumno/a podrá realizar todos los pasos para la instalación de un servidor real. Para ello, una vez que se posee la máquina, es necesario instalar el Sistema Operativo (SO) que proporcionará y sobre el que se ejecutarán los servicios. Dado que no es posible tener la infraestructura necesaria para poder trabajar con servidores físicos, recurriremos a la virtualización de los servidores. Este método cada vez es más popular y se presenta como una gran alternativa a tener un servidor físico.

1.1.- Concepto de Virtualización y Máquina Virtual

Un software de máquinas virtuales es, esencialmente, aquel que permite crear una capa de abstracción sobre el HW en el que se ejecuta de modo que pueden ejecutarse simultánea- mente varias máquinas virtuales en el mismo servidor (o conjunto de servidores) físico. En los últimos años, hay una tecnología denominada contenedores, que está siendo adoptada en muchos entornos. Ésta permite compartir recursos entre los contenedores y el anfitrión. Una posible analogía es la diferencia entre proceso y hebra, dos máquinas virtualizadas completamente serían como dos procesos mientras que los contenedores serían como las hebras (que comparten "cosas") [1][2][3]. En este primer bloque emplearemos virtualización, mientras que en el segundo bloque haremos uso de contenedores.

1.1.1.- Software para virtualización: VirtualBox

Con objeto de reducir la complejidad del entorno de prácticas, homogeneizar preguntas y problemas, así como reducir incidencias, emplearemos únicamente VirtualBox.

A continuación, para evitar confusiones y por economía del lenguaje, el software de virtualización se notará como VMSW (*Virtual Machine SoftWare*).

Usted debe conocer qué tipo o modo de virtualización utiliza Virtual Box, entender las ventajas e inconvenientes de la tecnología de virtualización en la industria IT y su relación con las distintas formas de cloud-computing.

En la prácticas, debe ser capaz de crear y configurar máquinas virtuales adaptadas a los requerimientos de cada ejercicio y entender las características de los principales modos de visualización de red.

Al alumno/a le será de utilidad manejar con soltura la capacidad de clonar MV y de realizar Snapshots.

1.1.2.- Sistema Operativo: Rocky Linux

De nuevo, con el objeto de reducir la complejidad del entorno, todos los alumnos/as emplearán la misma versión de Rocky Linux 9, disponible en forma de imagen ISO en

facilitar la realización del ejercicio, la imagen http://atcproyectos.ugr.es/esriie/Rocky-9.0-20220805.0-x86_64-minimal.iso

Para tomar decisiones antes de configurar un servidor, es importante conocer quién está detrás de cada distribución, su relación con otras distribuciones así como qué empresas dan soporte y apoyo ante posibles problemas [4]

2.- Instalación y configuración de un servidor básico Rocky Linux

2.1.- Instalación del SO

La instalación se realizará empleando las opciones "por defecto" con las únicas personalizaciones relativas a la localización (idioma y zona horaria) [5][17]. Aunque forma parte de la instalación por defecto, el alumno/a deberá asegurarse de que **no** se instale un entorno gráfico y de que **si** se instale un servicio de SSHD [6].

En caso de no haberlo hecho durante el proceso de instalación, debe asegurarse de disponer de una cuenta de usuario (distinta de root) con privilegios de administración. Puede crear un usuario nuevo con `useradd` o modificar uno existente con `usermod` [7][8].

si es la última versión se configura en el menú gráfico.

Otro de los aspectos importantes en la administración de puestos de trabajo y configuración de servidores es la configuración de la red [47]. Por tanto se espera que usted sepa configurar las interfaces de red a nivel de aplicación de VMSW así como a nivel del SO.

La MV debe disponer de dos tarjeta de red [9][10]:

- NAT con capacidad de acceso a Internet Pública.
- Host-Only configurada con IP estática, que permita la comunicación con el equipo Anfitrión (Host) y otras posibles máquinas virtuales (Guests).

El servidor dispondrá de un `hostname` [13]significativo formado por las iniciales del alumno/a seguido por una secuencia que facilite su identificación. Por ejemplo: `dpsMV01`.

sudo hostnamectl set-hostname <nombre>

El `prompt` de la shell se configurará para mostrar el usuario actual, el `hostname` y hora, junto con el directorio actual de trabajo [11][12]. Por ejemplo:

```
[admin@dpsMV-17:30:25 etc]$
```

La hora del equipo debe estar correctamente configurada para reflejar la hora actual en España.

Este `prompt` debe estar visible en toda captura de pantalla que el alumno/a entregue como parte de la evaluación. **Las capturas que no lo contengan o no sigan este diseño de prompt se considerarán inválidas**.

Para ello, añadimos al archivo .bashrc (se ejecuta automáticamente en cada login por lo que guarda información permanentemente):

PS1="[\u@\h-\t \W]$ "

Usuario · Máquina · Hora · Directorio actual de trabajo

Llegado a este punto, el alumno/a dispondrá de una MV básica cuya configuración podrá ser reutilizada en el futuro. Se recomienda almacenar la MV así configurada para esta y futuras prácticas empleando VirtualBox snapshots [14] y clone [15].

2.2.- Ejercicio evaluable:

El alumno/a debe ser capaz de presentar un MV con la configuración descrita en este apartado. La configuración debe ser permanente, es decir, en todo caso, tras reiniciar el equipo, la configuración será la esperada.

Para **validar la configuración de red**, el alumno/a debe ser capaz de:

- Hacer `ping` desde el equipo anfitrión a la MV y viceversa.
- Hacer ping desde la MV a cualquier equipo accesible públicamente en Internet por FQHN o IP.
- Conectar por `ssh` desde el equipo anfitrión a la MV [16].

Para ver configuración de red usamos: ip a (equivalente a ifconfig pero + moderno).

3.- Configuración de LVM y RAID

Cuando estamos preparando una máquina para su uso como servidor, se nos plantean tomas de decisiones cruciales tanto a nivel hardware como a nivel software desde el inicio del diseño de la solución. La instalación de un SO en una máquina implica a una serie de elementos que deben ser configurados desde el comienzo, cuya modificación implica la detención del servicio y un esfuerzo adicional, además de incrementar la posibilidad de cometer errores.

Uno de los elementos más importantes es el almacenamiento ya que el número de parámetros que se pueden configurar es elevadísimo y su impacto en el rendimiento, fiabilidad, tolerancia a fallos, etc. es enorme.

Por tanto, usted debe ser capaz de tomar una decisión de a tener que elegir un sistema de archivos concreto así como tener nociones sobre cómo gestionar el almacenamiento. Dada la importancia del almacenamiento, en servidores es normal aplicar soluciones RAID para que el acceso sea más eficiente y para preservar la información en caso de que haya roturas o problemas de disco.

3.1 .- Configuración de un servidor con LVM + Raid

3.1.1.- LVM

Logical Volume Manager (LVM) es una tecnología que facilita la gestión de los volúmenes de almacenamiento de un sistema Linux [18].

LVM organiza el almacenamiento empleando tres componentes: Physical Volumes, Volume

lsblk: muestra un árbol cuyos nodos son los dispositivos.

Groups y Lógical Volumes [19]. Durante la instalación del SO , realizada en el apartado anterior, el asistente de Rocky Linux configuró LVM por nosotros. En este apartado el alumno/a debe ser capaz de modificar esta configuración "por defecto" adaptándola al caso descrito en el ejercicio evaluable.

Para ello, es importante que se familiarice con los siguientes aspectos de LVM:

- Rol de cada componente en la arquitectura de almacenamiento: Phisical Volume, Volume Group & Logical Volume.
- Gestión de almacenamiento con distintas características físicas (HDD, SSD, Raid, ..).
- El *etiquetado/naming* de componentes y su correspondencia con los ficheros de dispositivo.
- Uso de los comandos propios de LVM para gestionar componentes.

3.1.2.- RAID

Redundant Array of Independent/Inexpensive Disks (RAID) es un tecnología que permite agrupar varios dispositivos de almacenamiento (en nuestro caso, discos duros), creando un nuevo dispositivo virtual con capacidades extendidas [20].

A efectos de estas prácticas, los niveles de RAID relevantes son: 0, 1 y 5. Debe entender las ventajas e inconvenientes de cada nivel, su aplicación a la implementación de requerimientos de almacenamiento, así como su administración empleando las herramientas de CLI proporcionadas por Linux [21][27]

Raid no es ampliable como LVM, la estructura definida es fija.

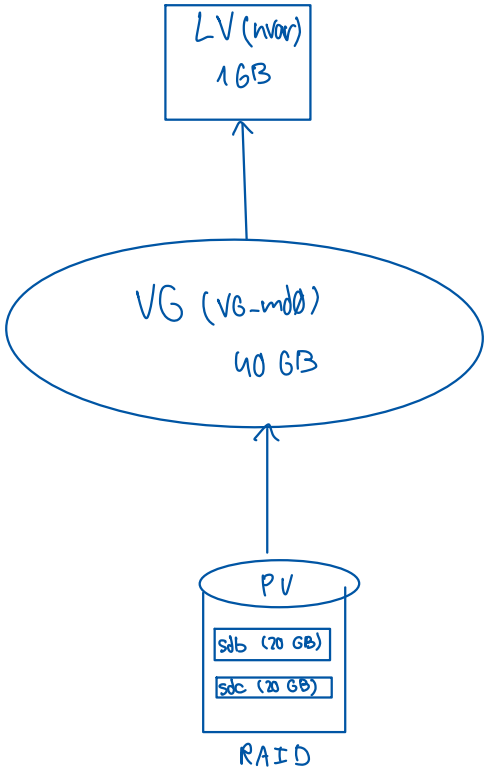
3.1.3.- Administración del Sistema de Ficheros Linux

Independientemente del diseño realice para solucionar el caso práctico de este apartado, su implementación efectiva requiere de conocimientos adicionales sobre el sistema de ficheros y las prácticas de administración de servidores. Entre otros aspectos a considerar:

- Modos de ejecución y, en especial, el modo mantenimiento de un servidor linux [22].
- Estructura estándar del sistema de fichero Linux [23].
- Sistemas de ficheros comunes en linux. [24][25]
- Montaje y desmontaje de volúmenes [26].
- Comandos básicos de copia, renombrado, borrado, edición y consulta de ficheros.

3.2)

Esquema:



1º) Añadir discos a MV (en la parte SATA).

2º) Crear raid con mdadm.

sudo mdadm --create --verbose <nombre> --level=1 --raid-devices=2 <disco1> <disco2>
(/dev/md0) Raid 1: necesita mín 2 discos. (/dev/sdb) (/dev/sdc)

Para ver el estado de la creación: cat /proc/mdstat

3º) Crear PV con /dev/md0

sudo pvcreate <dispositivo físico>
(/dev/md0)

Ver otras opciones como pvremove.

Para ver el resultado: pvdisplay o pvs

4º) Crear VG con /dev/md0

sudo vgcreate <nombre> <PV>
(VG_md0) (/dev/md0)

Ver otras opciones como vgremove, vgrename.

Para ver el resultado: vgdisplay o vgs

5º) Crear LV nvar

sudo lvcreate -L 1G -n <directorio> <VG>
(nvar) (VG_md0)

Para ver el resultado: lvdisplay o lvs

6º) Dar formato de sist. de archivos (XFS, ext4)

sudo mkfs -t ext4 <LV>
(/dev/VG_md0/nvar o /dev/mapper/VG_md0-nvar)

7º) Montar /dev/VG_md0/nvar o /dev/mapper/VG_md0-nvar en /mnt/nvar

sudo mkdir /mnt/nvar; mount /dev/VG_md0/nvar /mnt/nvar

8º) Pasar a modo mantenimiento.

sudo systemctl isolate runlevel1.target

Niveles de ejecución (runlevels):

0: Hace shutdown sobre el sistema.
1: Modo mantenimiento de usuario.
2: Multiusuario sin acceso a red.
3: Multiusuario sin GUI, solo terminal + red.
4: Configuración personal, pues está indefinido.
5: Igual que 3 pero con GUI.
6: Reboot del sistema.

9º) Copiar /var en /mnt/nvar

cp -a /var /mnt/nvar

-a respeta todos los formatos de los archivos y es necesario

Comprobar: ls -lZ /mnt/nvar

10º) (opcional): Renombrar /var a /oldvar con

mv /var /oldvar

11º) Crear /var

mkdir /var

12º) Montar /dev/VG-md0/nvar en /var

mount /dev/VG-md0/nvar /var

13) Añadir a /etc/fstab para hacer los cambios permanentes.

/dev/VG-md0/nvar /var ext4 defaults 0 0

- /dev/VG-md0/nvar → Dispositivo
- /var → Pto. montaje
- ext4 → Formato (tipo de dispositivo)
- defaults → Opciones
- 0 → Backup (0 = no backup)
- 0 → Chequeo de sist archivos de boot. (0 = no chequeo). Para root debe estar a 1 y para otras particiones a 2.

Anticuado: no usar

3.2.- Ejercicio Evaluable:

Partiendo de un servidor básico configurado de acuerdo al apartado 2, el alumno/a deberá afrontar el caso práctico descrito a continuación:

Se desea instalar un servicio de gestión documental en el servidor. Se espera que este servicio precise de una cantidad espacio de almacenamiento creciente con el tiempo, pudiendo llegar a ser considerable. Por otro lado, el contenido será crítico, por lo que se desea proporcionar algún mecanismo de respaldo ante fallos en el dispositivo de almacenamiento.

El alumno/a debe diseñar los cambios en el sistema de almacenamiento e implementarlo empleando prácticas adecuadas de administración que garanticen la conservación de la información en el sistema y procuren la máxima disponibilidad del servicio.

4.- Acceso seguro al servidor: Firewall + SSHD

4.1.- Gestionando el cortafuegos

Rocky Linux dispone de un front-end para el cortafuegos que permite definir cómodamente las reglas para `iptables` [28].

Independientemente de que estudie o no el uso de `iptables` en otra asignatura, es muy útil conocer el uso adecuado del front-end `firewall-cmd` en Rocky Linux [29]. Se espera que usted sea capaz de abrir y cerrar puertos así como de comprobar y modificar el estado del servicio de firewall con `systemctl` [30].

Para ello, no solo usará las opciones disponibles por los comandos anteriores, sino que debe ser capaz de verificar su configuración empleando el comando `nmap` [31].

4.1.1.- Ejercicio Evaluable:

Como caso práctico, partiendo de una MV con la configuración base descrita en el apartado 2, el alumno/a deberá ser capaz de instalar un servidor de HTTP, Apache[32] [33] o Nginx [34][35] , y habilitar/deshabilitar su acceso por Firewall.

Para ello, instalará el servidor web de su elección y modificará la home page para mostrar un mensaje: “Bienvenidos a la web de <Nombre y Apellidos del alumno/a> en Prácticas ISE”.

El servicio web debe estar accesible en la servidor (MV) en el puerto por defecto (80) usando un navegador web convencional corriendo en el anfitrión (Host).

Un escaneo de puertos sobre el servidor solo debe mostrar como accesibles los puerto web y ssh.

Habilitar servicio por nombre y no por nº. Tener únicamente abiertos los puertos HTTP (80) y SSH (22), no todos.

4.1.1) Es necesario ejecutar en super usuario.

- Apache:

1º) Instalar httpd: Daemon encargado de la configuración del servidor y renombrar welcome page.

dnf (-y) install httpd

↳ contestar sí a todo.

sudo mv /etc/httpd/conf.d/welcome.conf /etc/httpd/conf.d/welcome.conf.org

2º) Configurar httpd:

nano /etc/httpd/conf/httpd.conf

ServerAdmin : root@fjvISE	(línea 89)
ServerName : www.fjvISE.world:80	(línea 98)
Options FollowSymLinks (borrar Indexes)	(línea 147)
AllowOverride All	(línea 154)
DyrectoryIndex index.html index.php index.cgi	(línea 167)
ServerTokens Prod	(al final)

systemctl enable --now httpd

3º) Configurar firewall:

sudo systemctl enable --now firewalld

Otros:

Ver si está corriendo: systemctl status firewalld

Pararlo/reiniciarlo: systemctl stop/restart firewalld

Ver configuraciones: firewall-cmd --list-all

Las zonas permiten definir conjuntos independientes de reglas. Deben estar ligadas a una interfaz de red o a un rango de ip's.

```
firewall-cmd --zone=public --add-service=http
firewall-cmd --zone=public --add-service=ssh
firewall-cmd --runtime-to-permanent
firewall-cmd --reload
```

Otros:

Servicios disponibles: `firewall-cmd --get-services`

Servicios corriendo: `firewall-cmd --list-services`

Eliminar servicio: `firewall-cmd --zone=public --remove-service=http`

Ver zonas: `firewall-cmd --get-zones`

Ver zonas activas: `firewall-cmd --get-active-zones`

Ver zona por defecto: `firewall-cmd --get-default-zone`

Añadir zona: `firewall-cmd --new-zone=<nueva-zona>`

Añadir interfaz a zona: `firewall-cmd --zone=<zona> --add-interface=<interfaz>`

Establecer zona por defecto: `firewall-cmd --set-default-zone <zona>`

Ver puertos: `firewall-cmd --list-ports`

Añadir puerto: `firewall-cmd --zone=public --add-port=<n°>/tcp`

Eliminar puerto: `firewall-cmd --zone=public --remove-port=<n°>/tcp`

4°) Crear y editar index.html

`nano /var/www/html/index.html`

`<html><body>texto</body></html>`

5°) Comprobar con nmap que solo están abiertos los puertos de http y ssh.

`dnf -y install nmap` Ver ip's de cada interfaz: `hostname -I`

`nmap <ip>`

- Nginx:

1º) Instalar Nginx: dnf -y install nginx.

2º) Activar Nginx: systemctl enable --now nginx

3º) Configurar firewall: systemctl enable --now firewalld

4º) Añadir servicio http:

firewall-cmd --add-service=http; firewall-cmd --runtime-to-permanent;

firewall-cmd --reload

5º) Crear index.html (hay uno creado por defecto):

nano /usr/share/nginx/html/index.html

4.2.- SSH

Una vez que ya se disponen de las herramientas para instalar servicios y abrir la puerta para que presten servicio, vamos a trabajar con la administración remota.

Es importante ser conscientes de la ambigüedad de que ssh es tanto un cliente como un servicio. En algunos sistemas es sencillo ya que para denotar al servicio, se utiliza una `d` (de daemon) al final. Debe prestar especial atención cuando edite los archivos de configuración.

Se espera que usted sea capaz de instalar, configurar y "asegurar" el servicio SSH[36], limitando el acceso por contraseña al root (configuración por defecto) o activándolo y cambiando el puerto por defecto. Debe tener en cuenta, que en caso de cambio de puerto, deberá modificar la configuración de firewalld, empleando los conocimientos adquiridos en el apartado anterior.

Un aspecto fundamental en la administración de servidores es la automatización de la ejecución de comandos remotos empleando SSH. Para ello, es necesario identificar al usuario sin contraseña, empleando herramientas de llave asimétrica. El alumno/a debe entender los conceptos de criptografía simétrica y asimétrica[37] implicados en garantizar la confidencialidad y la autenticación en una conexión de ssh.

4.2.1.- Ejercicio Evaluable.

Partiendo de un servidor base configurado siguiendo las indicaciones del apartado 2, el alumno/a modificará servicio SSHD para que, en lugar del puerto por defecto (22), se ejecute en un puerto alternativo de un valor mayor a 1024. Se recomienda que consulte la lista de puertos reconocidos por el sistema en `/etc/ports` para evitar emplear un puerto que ya tenga una aplicación predefinida.

Se concederá acceso remoto por llave pública a un usuario de su elección.

El ejercicio se validará ejecutando un comando de forma remota sobre el servidor SSH con la nueva configuración. El comando presentará el contenido completo (incluido ficheros y directorios ocultos) con del directorio home del usuario remoto empleado en la conexión. Para ello, desde el ordenador anfitrión (o una MV distinta a la que se va a acceder) se empleará ssh sin terminal remoto y sin contraseña, pasando como único como parámetro el comando a ejecutar.

5.- Automatización de la configuración con Ansible.

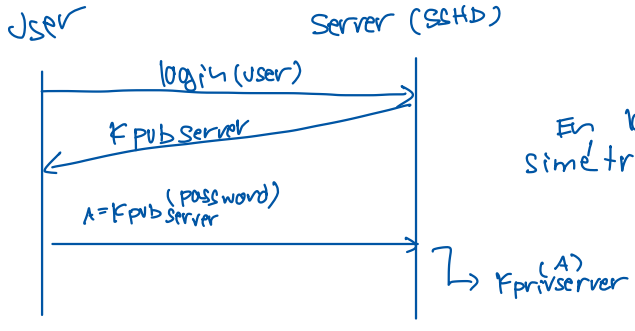
RedHat Ansible [41] es una de las referencias más habituales en la industria IT para la automatización de la configuración de servidores. Otras referencias populares son: Hasicorp Terraform, Chef o Puppet [39].

Su instalación es sencilla y sus dependencias mínimas. Ansible se basa en el uso de SSH para la ejecución remota de comandos y Python como lenguaje de scripting. Siendo estas dos herramientas de amplia difusión e instalación estandarizada en la mayor parte de las

4.2.1)

Intercambio SSH:

Aclaraciones previas:



En la práctica, la llave es simétrica de sesión.

`ssh -V(V(V))` `user@server` : Proporciona paso a paso el proceso ssh.

Es posible comunicarse con SSH sin contraseña, sólo con llave pública.

Las llaves privadas siempre deben ir cifradas por contraseña.
Para no introducirla todo el rato : `ssh-agent`

Se da por hecho que todo es ejecutado en superuser.

1º) Ver estado del daemon sshd y comprobar que está corriendo.

```
systemctl status sshd
```

2º) Prohibir conexión remota a root. Es lo mínimo que debe tener un servidor.

```
nano /etc/ssh/sshd_config
```

Descomentar #PermitRootLogin... y escribir no. Por defecto la conexión remota a root no está permitida.

```
systemctl restart sshd
```

3º) Ver qué puertos hay disponibles, aquellos no asignados a un servicio. Normalmente tomamos un > 1024, como por ejemplo 22022.

```
cat /etc/services
```

4º) Para cambiar el puerto debemos informar a SELinux.

Para ello instalamos:

```
dnf provides semanage
dnf -y install policycoreutils-python...
```

Ejecutamos:

```
semanage port -a -t ssh_port_t -p tcp 22022
```

5º) Descomentar #Port 22 y escribir Port 22022.

Si no hubiéramos ejecutado semanage daría un error al hacer restart|reload.

```
systemctl reload sshd.
```

6º) Configurar firewall. Si probamos a hacer ssh no encontrará la ruta al host.

- Ver que está corriendo:

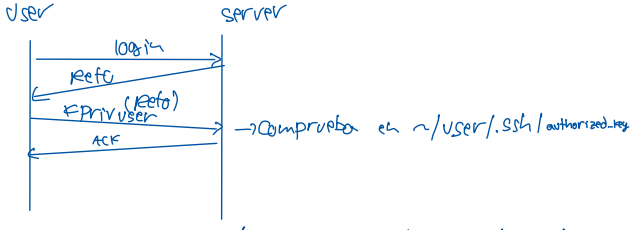
```
firewall-cmd --state  o' systemctl status firewalld
```

- Añadir puerto 22022 a los permitidos:

```
firewall-cmd --add-port 22022/tcp; firewall-cmd --runtime-to-permanent
systemctl reload firewalld
```

Ahora iniciamos la conexión por SSH sin contraseña.

SSH toma un 1º login con usuario-contraseña. Por tanto, al usar una clave pública únicamente en las siguientes conexiones, el servidor ya puede autenticar al usuario.



7º) Generamos llave pública y privada en el sistema usuario (Ubuntu).

`ssh-keygen`: se crea directorio ~/.ssh/ que contiene las llaves, id_rsa, id_rsa.pub

8º) Transferimos llave pública al servidor.

`ssh-copy-id -p 22022` <usuario_servidor>@<ip>

↓ Como lo hemos cambiado hay que indicarlo.

Ahora nos pedirá la contraseña para finalizar la autenticación.

En el servidor: Se crea ~/.ssh/ authorized_keys

En el cliente: Se crea ~/.ssh/ known_hosts y know_hosts.old

Ahora podemos ejecutar cualquier comando en el servidor de forma remota: `ssh -p <puerto> <usuario_servidor>@<ip> <comando>`

9º) También podemos deshabilitar el acceso por contraseña para que se haga únicamente por cifrado asimetrico. En el servidor:

nano /etc/ssh/sshd_config

Descomentamos # PasswordAuthentication yes, y escribimimos PasswordAuthentication no

Si ahora un usuario quiere acceder por ssh y no ha gestionado el cifrado asimétrico con el servidor, en el servidor se deberá volver a editar PasswordAuthentication yes. A continuación, el usuario hará la gestión del cifrado asimétrico, y finalmente cambiamos de nuevo PasswordAuthentication no en el server.

10º) Se pueden gestionar los usuarios a los que se puede conectar remotamente

En /etc/ssh/sshd-config añadimos AllowUsers <nombre>.

Solo se permitirá la conexión remota a los usuarios del servidor ahí listados.

distribuciones Linux .

El alumno/a debe entender cómo funciona Ansible [38], entender las diferencias entre los tipos de nodo, saber administrar el inventario [40], ejecutar comandos ad-hoc por CLI [42][43]y realizar configuraciones de servidores empleando Playbooks [44][45].

Es una práctica de seguridad habitual no emplear el usuario "`root`" para el acceso a los nodos controlados por Ansible. En su lugar, se prefiere crear un usuario, por ejemplo "`admin`", con acceso SSH únicamente con llave pública y que puede ejecutar comandos privilegiados sin contraseña adicional. Para ello, el comando `sudo` debe configurarse correctamente en servidor controlado empleando el archivo `/etc/sudoers [46]`.

5.1.- Ejercicio Evaluable.

El ejercicio versa sobre la configuración de servidores empleando Ansible playbooks. Se valorará, la estructuración y claridad del código, el uso de parámetros para facilitar la reutilización de los playbooks, el uso de comentarios, el uso de variables, la organización de los artefactos, el uso de convenciones de nombrado de Ansible y de Yaml y, aunque escapa al objetivo de este ejercicio, el posible uso de recursos para reutilización de artefactos, como los Ansible Roles.

Partiendo de dos servidores, configurados de acuerdo a los requerimientos del apartado 2, debe modificarlos para que sea posible el acceso remoto del usuario root empleando contraseña (el acceso con contraseña está desactivado por defecto en la instalación de Rocky).

A continuación, realizará la siguiente configuración en los dos servidores empleando un playbook:

1. Crear un nuevo usuario llamado "`admin`" que pueda ejecutar comandos privilegiados sin contraseña.
2. Dar acceso por SSH al usuario "`admin`" con llave pública.
3. Crear el grupo "`wheel`" (si no existe) y permitir a sus miembros ejecutar sudo.
4. Añadir una lista de usuarios (al menos dos), añadiéndolos al grupo "`wheel`" y concediéndoles acceso por SSH con llave pública.
5. Deshabilitar el acceso por contraseña sobre SSH para el usuario root.

Los servidores anteriormente configurados son ahora administrables mediante Ansible empleando el usuario "`admin`". Ponga a prueba esta configuración con los siguientes cambios/playbooks:

1. Modifique conveniente el inventario para el uso del nuevo usuario "`admin`".
2. Uno de los servidores se empleará para correr Apache Httpd y el otro Nginx. Modifique el inventario de forma conveniente para realizar correctamente su administración.
3. Desarrolle un playbook para implementar los requerimientos del ejercicio 4.1.1 en los dos servidores, instalando en cada caso Apache Httpd o Nginx según la configuración del inventario.

Principales comandos/servicios empleados en prácticas:

A continuación se presenta una serie de comandos con las que el alumno/a debe familiarizarse durante la realización de las prácticas. No pretende ser un listado completo de las herramientas a utilizar, pero si orientar al alumno/a sobre las opciones disponibles más relevantes para la resolución de los ejercicios prácticos.

El alumno/a puede emplear las referencias proporcionadas, recurrir a referencias propias o a las páginas de manual.

`ansible`
`ansible-*`
`bashrc`
`cp`
`echo`
`find`
`firewall-cmd`
`firewalld`
`fstab`
`grep`
	`history`
	`hostname`
	`hostnamectl`
	`hosts`
	`httpd`
	`less`
	`lsblk`
	`lvm`
	`man`
	`mdadm`
	`mkfs`
	`more`
		`mount`
		`mv`
		`nano`
		`nginx`
		`nmap`
		`nmcli`
		`nmtui`
		`ping`
		`poweroff`
		`reboot`
		`resize2fs`
		`rm`
			`ssh`
			`ssh-*`
			`sudoers`
			`systemctl`
			`tail`
			`umount`
			`useradd`
			`usermod`
			`vi`
			`visudo`

5.1)

Lo recomendable es usar una interfaz gráfica (Ubuntu) en el anfitrión para editar los archivos, y después transferirlos al server. Para la edición se usará vscode. Trabajaremos con 1 anfitrión (Ubuntu) y 2 servers (Rocky), de IP's 192.168.56.114 y 192.168.56.115

Es recomendable gestionar el acceso a cada server con llave pública, pues Ansible se basa en ssh y no queremos que nos pida la contraseña cada vez que ejecutamos un comando.

1º) Instalar Ansible y crear directorio de trabajo.

```
sudo apt install ansible
mkdir <nombre> ; cd <nombre>
```

2º) Creamos inventario: fichero que indica la IP's de los servers a configurar.

El inventario podrá tener extensión .ini o' .yaml. Las sintaxis cambian.

```
touch inventory.yml   y editamos:

myhosts:   → metagrupo
    hosts:   → palabra reservada para indicar hosts.

        server1:
            ansible_host: 192.168.56.114

        server2:
            ansible_host: 192.168.56.115
```

Para comprobar sintaxis:

```
ansible-inventory -i inventory.yml --list
```

Para probar ejecutar un comando remotamente:

```
ansible <server(s)> -i inventory.yml -m <comando> (-u) <server_user>
```

(-u) → Cuando la configuración se hace en ≠ sitio que el server configurado hay que dar el nombre del usuario del server.

Cuando queremos ejecutar en otro usuario, añadimos:

- Para root: --become --ask-become-pass
- Otro: --become --become-user <user> --ask-become-pass

Cuando el acceso sin contraseña no está configurado, para que nos la pida.

Para ejecutar comando de shell:

ansible <server(s)> -i inventory.yml -m shell -a '<comando>'

-u <server_user>

3º) Creamos playbook.

Los playbooks son ficheros que indican a Ansible que instrucciones seguir.

Comprobación: ansible-playbook --check <playbook> -i <inventory>

Ejecución: ansible-playbook <playbook> -i <inventory>

Referencias

1: VMWare," Tipos de virtualización.", https://www.vmware.com/es/solutions/%20virtualization.html,
2: Oracle," Tipos de virtualización.", https://www.virtualbox.org/wiki/%20Virtualization,
3: Docker," What is a container.", https://www.docker.com/what-container,
4: Rocky Linux," About Rocky Linux", https://rockylinux.org/about/, Explicación del contexto del Proyecto Rocky Linux y su relación con CentOS
5: Rocky Linux," Rocky Install Guide", https://docs.rockylinux.org/guides/installation/, Guía de instalación de Rocky
17: CentOS," Installing in text mode", https://docs.centos.org/en-US/centos/install-guide/Text_Installation_Intro-x86/, Procedimiento de instalación de CentOS/Rocky en modo texto (útil en caso de incompatibilidad con modo gráfico).
6: Rocky Linux," Rocky Guides", https://docs.rockylinux.org/, Guías de procedimientos habituales de administración en Rocky Linux
7: NixCraft," How to create a new user account in CentOS", https://www.cyberciti.biz/faq/create-a-new-user-account-in-centos-7-8-linux/, Guía para la creación de usuarios empleando utilidades de comandos.
8: Fedora," Adding a user to sudoers", https://docs.fedoraproject.org/en-US/quick-docs/adding_user_to_sudoers_file/, Guía para conceder privilegios de administración a un usuario.
47: T. A. Limoncelli, C. J. Hogan, and S. R. Chalup, Practice of System and Network Administration, The (2Nd Edition), 2007
9: Virtual Box," Virtual Networking", https://www.virtualbox.org/manual/UserManual.html#networkingdetails, Documentación de referencia de Virtual Box para la gestión de redes virtuales.
10: RedHat," Ip Networking", https://access.redhat.com/documentation/es-es/red_hat_enterprise_linux/7/html/networking_guide/ch-configuring_ip_networking, Guía para la configuración de interfaces de red IP
13: RedHat," How to configure a hostname on a Linux system", https://www.redhat.com/sysadmin/configure-hostname-linux, Guía para la configuración de forma permanente del hostname de un servidor.
11: Linux Hint," Bash PS1 customization examples", https://linuxhint.com/bash-ps1-customization/, Ejemplos de configuración del prompt de la shell, de forma temporal y permanente..
12: Baeldung," Customizing Bash Prompt", https://www.baeldung.com/linux/customize-bash-prompt, Ejemplos avanzados de configuración del prompt
14: VirtualBox," Snapshots", https://docs.oracle.com/en/virtualization/virtualbox/6.0/user/snapshots.html, Documentación sobre la gestión de Snapshots en VirtualBox
15: ," ", https://docs.oracle.com/en/virtualization/virtualbox/6.0/user/clone.html, Guía para el clonado de MV en VirtualBox
16: PuTTy," Home Page", https://www.putty.org/, Cliente de SSH portable para windows
18: RedHat," Logical Volumes", https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/

logical_volume_manager_administration/logical_volumes, Características/Beneficios del uso de LVM para la administración de los volúmenes de almacenamiento.
19: Red Hat," LVM Components", https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/logical_volume_manager_administration/lvm_components#doc-wrapper, División en components de LVM, responsabilidades y uso de cada nivel.
20: Kernel.org," What is RAID and why should you want it?", https://raid.wiki.kernel.org/index.php/What_is_RAID_and_why_should_you_want_it%3F, Niveles de Raid y aplicaciones.
21: ," ", https://wiki.archlinux.org/title/RAID, Introducción a tipos de raid y su administración mediante comandos en Linux
27: Digital Ocean," How To Create RAID Arrays with mdadm on Ubuntu 22.04", https://www.digitalocean.com/community/tutorials/how-to-create-raid-arrays-with-mdadm-on-ubuntu-22-04, Uso de mdadm para la administración de RAID
22: Alibaba Cloud," Understanding and changing runlevels", https://alibaba-cloud.medium.com/understanding-and-changing-runlevels-in-systemd-ccc30065c53d, Niveles de ejecución, aplicaciones y gestión.
23: Rusty Russell," Filesystem Hierachy Standard in Linux", https://www.pathname.com/fhs/pub/fhs-2.3.html, Principales componentes del sistema estándar de ficheros linux.
24: Baeldung," Guide to Linux Filesystems", https://www.baeldung.com/linux/filesystems, Principales sistemas de ficheros, características y comandos. FS avanzados.
25: Opensource.com," An introduction to Linux filesystems", https://opensource.com/life/16/10/introduction-linux-filesystems, FS en Fedora, estructura de directorios, y montaje.
26: Red Hat," An introduction to the Linux /etc/fstab file", https://www.redhat.com/sysadmin/etc-fstab, fstab + mount
28: Arch Linux," IPTables", https://wiki.archlinux.org/title/Iptables, Introducción a IPTables
29: Rocky Linux," Firewalld for Beginners", https://docs.rockylinux.org/guides/security/firewalld-beginners/, Introducción a la gestión del firewall en Rocky Linux
30: Digital Ocean," How To Use Systemctl to Manage Systemd Services and Units", https://www.digitalocean.com/community/tutorials/how-to-use-systemctl-to-manage-systemd-services-and-units, Gestion de servicios con systemctl
31: Nmap," Home Page", https://nmap.org/, Nmap herramienta de escaneo de puertos.
32: Apache Fundation," Httpd Home Page", https://httpd.apache.org/, Servdor Httpd Apache
33: Rocky Linux," How to install Apache Httpd on Rocky Linux", https://www.server-world.info/en/note?os=Rocky_Linux_8&p=httpd&f=1, Instalación de Apache en Rocky Linux
34: Nginx," Home Page", https://www.nginx.com/, Nginx Home Page
35: Digital Ocean," How to install Nginx on Rocky Linux", https://www.digitalocean.com/community/tutorials/how-to-install-nginx-on-rocky-linux-8, Guia de instalación de Nginx en Rocky Linux
36: Open SSH," Home Page", https://www.openssh.com/, Pagina Home de OpenSSH
37: Wikipedia," Public Key criptography", https://en.wikipedia.org/wiki/Public-key_cryptography, Critpografía de Llave Pública
41: Ansible Red Hat," Home Page", https://www.ansible.com/, Ansible Home Page
39: 6sense," Ansible Market Share", https://6sense.com/tech/configuration-management/ansible-market-share#:~:text=Ansible%20has%20market%20share%20of,Chef%20with%208.77%25%20market%20share., Market Share de las principales soluciones de Configuration Automation

38: Ansible," Getting started with Ansible", https://docs.ansible.com/ansible/latest/getting_started/index.html%20Configuring, Introducción a Ansible
40: Ansible," How to build your inventory", https://docs.ansible.com/ansible/latest/inventory_guide/intro_inventory.html, Guía para administrar el inventario de Ansible.
42: Ansible," Introduction to Ad-Hoc Commands", https://docs.ansible.com/ansible/2.7/user_guide/intro_adhoc.html#id7, Guía general sobre funcionamiento y uso de comandos ad-hoc por línea de comandos.
43: Ansible," All Modules", https://docs.ansible.com/ansible/2.7/modules/list_of_all_modules.html, Listado completo de módulos de Ansible
44: Ansible," Ansible Playbooks", https://docs.ansible.com/ansible/latest/playbook_guide/playbooks_intro.html, Introducción al uso de Playbooks
45: Ansible," Working with Playbooks", https://docs.ansible.com/ansible/latest/playbook_guide/playbooks.html, Playbooks avanzado.
46: Nix Craft," How to edit sudoers", https://www.cyberciti.biz/faq/linux-unix-running-sudo-command-without-a-password/, Guía para otorgar privilegios sudo a un usuario sin contraseña.