

df -k para ver espacio en disco

defensa

Qué es una máquina virtual ?

Es un software que simula un sistema de computación y puede ejecutar programas como si fuese una computadora real. Permite crear múltiples entornos simulados o recursos dedicados desde un solo sistema de hardware físico.

¿Cual es el propósito de las máquinas virtuales? Proporcionar un entorno de ejecución independiente del hardware y del sistema operativo que garantiza la independencia entre ambos.

Porque has escogido Debian ?

Porque es más sencillo

Diferencias entre Debian y Rocky ?

- **debian**

Orientación: Ideal para servidores, estaciones de trabajo y cualquier sistema donde la estabilidad sea prioritaria.

Ventajas:

Estabilidad: Menos propensa a fallos o errores.

Amplia variedad de software: Gracias a su repositorio de paquetes.

Gran comunidad: Facilita la resolución de problemas y el aprendizaje.

- **rocky**

Ventajas: Tb prioriza la estabilidad como Debian

Dirigida a entornos empresariales y servidores

Tiene una comunidad más pequeña y menos variedad de software

App y Aptitude ?

Son herramientas de gestión de paquetes en sistemas basados en Debian, como Ubuntu, que se utilizan para instalar, actualizar y eliminar software. Aunque ambas cumplen la misma función principal, existen algunas diferencias clave entre ellas:

Diferencias entre apt y aptitude. Aptitude es una versión mejorada de apt, Apt es un administrador de paquetes de nivel inferior y aptitude es de alto nivel. Aptitude tiene una mejor funcionalidad.

- **apt:** Ofrece una interfaz de línea de comandos más sencilla y directa. Es ideal para usuarios que prefieren una experiencia más minimalista y están familiarizados con los comandos básicos.
- **aptitude:** Proporciona una interfaz de usuario más interactiva, con un menú que facilita la selección de paquetes y la resolución de dependencias. Es una excelente opción para usuarios que buscan una experiencia más visual y desean tener un mayor control sobre las acciones que se realizan.

Qué es Apparmor ?

Es un módulo de seguridad del kernel Linux que permite al administrador del sistema restringir las capacidades de un programa.

AppArmor es el sistema de seguridad predeterminado de Debian que proporciona seguridad MAC (control de acceso obligatorio). Restringe el acceso de las aplicaciones únicamente a los archivos esenciales que necesitan para funcionar.

Qué es LVM ?

Es un gestor de volúmenes lógicos. Proporciona un método para asignar espacio en dispositivos de almacenamiento más flexible.

Qué es SELinux ?

SELinux (Security-Enhanced Linux) es una arquitectura de seguridad para sistemas operativos Linux que proporciona una capa adicional de protección más allá de los mecanismos de control de acceso tradicionales. Su objetivo principal es reforzar la seguridad del sistema al limitar las acciones que los procesos pueden realizar, incluso si un atacante logra comprometer uno de ellos.

Es una capa de seguridad extra

Cómo funciona SELinux?

SELinux funciona mediante la implementación de políticas de seguridad que definen qué procesos pueden acceder a qué recursos del sistema. Estas políticas se basan en un modelo de seguridad llamado *Control de Acceso Obligatorio* (MAC), que establece reglas más estrictas que el tradicional *Control de Acceso Discrecional* (DAC).

Ver las particiones `lsblk`

The hostname is cagomez-42 Deberás modificar este hostname durante tu evaluación.

`sudo nano -i /etc/hostname`

Password root: Myproyectborn1

Password de encriptacion Myproyectborn1

Password cagomez- XXXXXXXX Este usuario debe pertenecer a los grupos user42 y sudo.

Go to your root user su

[apt install sudo](#)

La forma más sencilla de comprobar la ausencia de un entorno gráfico es comprobar si puede ver el cursor. Si desaparece cuando pasa el cursor sobre la máquina virtual, no hay interfaz gráfica. También puede utilizar el comando `echo $DISPLAY`. Si devuelve algo que no sea una línea vacía, está utilizando una interfaz gráfica.

Check OS (Debian or Rocky) ?

[head -v 2 /etc/os-release](#)

Check is sudo is installed ?

[sudo -V](#)

Check for Password on Start ?

[sudo reboot](#)

Connect with a user (Mustn't be root) ?

You can check this at the beginning of the command line. If your user isn't root, you should see something like: `user@hostname:~$`

If your user is root, you will see "root" in front: `root@hostname:~#`

To set up our password policy, we will be using:

[nano -l](#)

Check if UFW is installed: ?

[sudo apt install ufw](#)

Instalación de sudo y configuración de usuarios y grupos ?

Configuración de la máquina `apt install sudo` "me instala los paquetes necesarios
`sudo reboot` reinicia la máquina
para entrar con el usuario root ponemos

`su Myprojectborn1`

Creamos cagomez-

`sudo` un usuario con nuestro login, como lo hemos creado en la instalación nos debe aparecer que ya existe

`sudo adduser cagomez-` Nos indica que ya existe

`sudo addgroup user42` Creamos el grupo user42

con `ctrl + D` salgo de `cat`

`sudo adduser cagomez- user42` añado mi usuario al grupo

con `getent group user42` compruebo que mi usuario pertenece al grupo
al crear el grupo `sudo` me dice que ya existe

`sudo adduser cagomez- sudo` añado mi usuario al grupo `sudo`

Instalación y configuración SSH ?

Hacemos `sudo apt update` para actualizar los repositorios que definimos en el archivo `etc/apt/sources.list`

Necesitamos instalar `openssh` para el inicio de sesión remoto con el protocolo `ssh`

`sudo apt install openssh-server`

Hacemos `sudo service ssh status` y nos debe aparecer `active`

Tenemos que modificar el fichero `sudo nano /etc/ssh/sshd_config` hacerlo con este otro
cdon la `-l` `sudo nano -l /etc/ssh/sshd_config`

Cambiamos el port 22 por port 4242

`PermitRootlogin` no

`sudo service ssh restart`

`sudo service ssh status` confirmamos que se han realizado los cambios y aparece el puerto 4242

No se debe conectar por `ssh` con `root`, el uso de `SSH` será comprobado durante la defensa creando un nuevo usuario. Por lo tanto, debes entender cómo funciona.

Instalación y configuración de UFW ?

```
sudo apt install ufw
sudo ufw enable
sudo ufw allow 4242
sudo ufw status
```

Configurar contraseña fuerte para sudo ?

Creamos el fichero de conf de contraseña

```
sudo touch /etc/sudoers.d/sudo_config
```

```
sudo mkdir /var/log/sudo
```

 Creamos el directorio sudo en esa ruta

Editamos el fichero creado: `nano /etc/sudoers.d/sudo_config`

Introducimos los siguientes comandos:

```
Defaults passwd_tries=3
Defaults badpass_message="Mensaje de error personalizado"
Defaults logfile="/var/log/sudo/sudo_config"
Defaults log_input, log_output
Defaults iolog_dir="/var/log/sudo"
Defaults requiretty
```

Defaults

```
secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"
```

- Número de intentos de poner contraseña erróneo
- Mensaje personalizado
- Archivo donde quedan registrados los comandos sudo
- Para que cada comando ejecutado con sudo quede archivado en el directorio especificado
- Activar modo TTY
- Restringir los directorios utilizados por sudo

Configuración de política de contraseñas fuerte ?

Hay que editar fichero login.defs

```
nano etc/login.defs
```

```
> PASS_MAX_DAYS 99999 -> PASS_MAX_DAYS 30
```

```
> PASS_MIN_DAYS 0 -> PASS_MIN_DAYS 2
```

debemos instalar los siguientes paquetes con este comando `sudo apt install`

```
libpam-pwquality
```

 Editamos el siguiente fichero:

```
nano /etc/pam.d/common-password
```

minlen=10 ➤ La cantidad mínima de caracteres que debe contener la contraseña.

ucredit=-1 ➤ Como mínimo debe contener una letra mayúscula. Ponemos el - ya que debe contener como mínimo un carácter, si ponemos + nos referimos a como máximo esos caracteres.

dcredit=-1 ➤ Como mínimo debe contener un dígito.

lcredit=-1 ➤ Como mínimo debe contener una letra minúscula.

maxrepeat=3 ➤ No puede tener más de 3 veces seguidas el mismo carácter.

reject_username ➤ No puede contener el nombre del usuario.

difok=7 ➤ Debe tener al menos 7 caracteres que no sean parte de la antigua contraseña.

enforce_for_root ➤ Implementaremos esta política para el usuario root.

Para comprobar si el usuario no cumple con la política haremos uso del comando `sudo chage -l username`

Como no cumple pq aplica a los nuevos usuarios tenemos que aplicar el cambio a los usuarios

`sudo chage -m <time> <username>` y `sudo chage -M <time> <username>`.

`sudo chage -m 2 root`

`sudo chage -M 30 root`

Configuración de ssh en virtual vox ?

Conexión ssh Para ssh he puesto el puerto 4243 en el host al estar cogido el 4242 se pone

`ssh cagomez-@127.0.0.1 -p 4243`. Si me sale el nombre en verde significa que he conectado

para mandar un mensaje pongo `sudo wall` y el mensaje que quiero enviar

SSH (Secure Shell) es un protocolo de red criptográfico que permite la comunicación segura entre un cliente y un servidor a través de una red no segura.

Proporciona una forma segura de acceder y administrar sistemas remotos, lo que permite a los usuarios ejecutar comandos y transferir archivos.

El uso de SSH es esencial para proteger la información confidencial de escuchas no autorizadas durante la administración remota

Chequear que solo use puerto 4242

`sudo nano -l /etc/ssh/sshd_config`

Confirmar que no puedo conectar con el usuario root, lo definimos en el fichero al poner `PermitRootlogin no`

Script ?

Para poder ver la arquitectura del SO y su versión de kernel utilizaremos el comando `uname -a` `grep "physical id" /proc/cpuinfo | wc -l` Nos indica los núcleos físicos 2 `grep processor /proc/cpuinfo | wc -l` núcleos virtuales 2

MEMORIA

`free --mega` memoria ram

`free --mega | awk '$1 == "Mem:" {print $3}'` **memoria usada**

`free --mega | awk '$1 == "Mem:" {print $2}'` **memoria total**

`free --mega | awk '$1 == "Mem:" {printf("%.2f%%)\n", $3/$2*100)}'` **% de memoria usada**

`df -m | grep "/dev/" | grep -v "/boot" | awk '{memory_use += $3} END {print memory_use}'` **memoria de disco ocupada**

`df -m | grep "/dev/" | grep -v "/boot" | awk '{memory_result += $2} END {printf("%.0fGb\n"), memory_result/1024}'` **espacio total en Gb me da como resultado 26 así que parece espacio en disco en Gb**

`df -m | grep "/dev/" | grep -v "/boot" | awk '{use += $3} {total += $2} END {printf("(%d%%)\n"), use/total*100}'` **porcentaje de la memoria usada**

PORCENTAJE USO CPU

`vmstat 1 3 | tail -1 | awk '{print $15}'100`

ULTIMO REINICIO

`who -b | awk '$1 == "system" {print $3 " " $4}'`

USO LVM

`if [$(lsblk | grep "lvm" | wc -l) -gt 0]; then echo yes; else echo no; fi`

`devuelve yes`

`CONEXIONES TCP ss -ta | grep ESTAB | wc -l`

`NÚMERO DE USUARIOS users | wc -w` devuelve 2

Dirección IP y MAC ?

`hostname -I`

`ip link | grep "link/ether" | awk '{print $2}'`

Número de comandos ejecutados con sudo

`journalctl _COMM=sudo | grep COMMAND | wc -l`

Crontab ?

`sudo crontab -u root -e`


Signature.txt ?

Lo primero es apagar la máquina, en cuanto se encienda o modifique algo la firma cambiará
`shasum nombremaquina.vdi`


No volver a abrir la máquina ya que la firma cambiará, tengo que clonar la máquina


Qué es Lighttpd ? Es un servidor web diseñado para ser rápido, seguro, flexible, y fiel a los estándares. Está optimizado para entornos donde la velocidad es muy importante. Esto se debe a que consume menos CPU y memoria RAM que otros servidores.

WordPress

 **Qué es WordPress ?** Es un sistema de gestión de contenidos enfocado a la creación de cualquier tipo de página web.

1 ° Para instalar la última versión de WordPress primero debemos instalar wget y zip. Para ello haremos uso del siguiente comando `sudo apt install wget zip`.

 **Qué es wget ?** Es una herramienta de línea de comandos que se utiliza para descargar archivos de la web.

 **Qué es zip ?** Es una utilidad de línea de comandos para comprimir y descomprimir archivos en formato ZIP.

voy a la carpeta `cd /var/www`

`sudo wget https://es.wordpress.org/latest-es_ES.zip`

descargamos la última versión de wordpress

Renombraremos la carpeta html y la llamaremos html_old. `sudo mv html/ html_old/`

Ahora renombraremos la carpeta wordpress y la llamaremos html. `sudo mv wordpress/ html`


Descomprimos el archivo que acabamos de descargar con el comando `sudo unzip latest-es_ES.zip`

Renombraremos la carpeta html y la llamaremos html_old. `sudo mv html/ html_old/`

Ahora renombraremos la carpeta wordpress y la llamaremos html. `sudo mv wordpress/ html`

Por último, estableceremos estos permisos en la carpeta html. Daremos uso del comando `sudo chmod -R 755 html`


Mariadb

 Qué es MariaDB ? Es una base de datos. Se utiliza para diversos fines, como el almacenamiento de datos, el comercio electrónico, funciones a nivel empresarial y las aplicaciones de registro.

para acceder a mariadb `sudo mariadb`

```
CREATE DATABASE wp_database;  
CREATE USER 'cagomez'@'localhost' IDENTIFIED BY '12345';  
GRANT ALL PRIVILEGES ON wp_database.* TO 'cagomez'@'localhost';  
FLUSH PRIVILEGES;
```

PHP

 Qué es PHP ? Es un lenguaje de programación. Se utiliza principalmente para desarrollar aplicaciones web dinámicas y sitios web interactivos. PHP se ejecuta en el lado del servidor.

1. Instalamos los paquetes necesarios para poder ejecutar aplicaciones web escritas en lenguaje PHP y que necesiten conectarse a una base de datos MySQL. Ejecutaremos el siguiente comando

```
sudo apt install php-cgi php-mysql
```

Configuración WordPress

Accedemos al directorio `/var/www/html` con el comando: `cd /var/www/html`

Copiamos el fichero `wp-config-sample.php` y lo renombraremos `wp-config.php` se hace con comando `cp`

lo editamos

```
nano wp-config.php
```

◦ Habilitamos el módulo `fastcgi-php` en `Lighttpd` para mejorar el rendimiento y la velocidad de las aplicaciones web en el servidor. `sudo lighty-enable-mod fastcgi`

Actualizamos y aplicamos los cambios en la configuración con el comando `sudo service lighttpd force-reload`

COMANDOS

1. Comprobar que no hay interfaz gráfica **`ls /usr/bin/*session`**

2. El servicio `ufw` está en uso

```
sudo ufw status
```

```
sudo service ufw status
```

3. El servicio `SSH` en uso

```
sudo service ssh status
```

4. Comprobar si utilizo `Debian` o `Centos`

```
uname -v o uname --kernel-version
```

5.- Comprobar que mi usuario está dentro de los grupos `"sudo"` y `"user42"`

getent group sudo

getent group user42

6.- Crear nuevo usuario y comprobar que sigue políticas de contraseñas que hemos creado

sudo adduser userprueba Myproyectborn1

```
$ su root Password:
# nano /etc/sudoers
# User privilege specification root ALL=(ALL:ALL) ALL francis
ALL=(ALL:ALL) ALL
```