Cheat Sheet de Comandos Utilizados

Creación de Particiones y Montaje de Volumenes con LVM

Crear una partición

- *lsblk*: Muestra las particiones que tenemos y los puntos de montaje utilizados
- *fdisk*: Se utilizaba antes para hacer particiones.
- *parted*: Permite hacer particiones
  - *help*: Muestra los comandos permitidos dentro de parted
  - *print*: Muestra las particiones actuales y el espacio disponible
  - *mkpart*: Crea una nueva partición:
    - File System Type: xfs
    - Start?: X GB
    - End?: X GB
  - *quit*: Sale de parted

Comandos para que el sistema operativo reconozca la partición:

- *udevadm settle*: Espera a que udev procese los eventos de creación de dispositivos para todos los dispositivos de hardware, garantizando que todos los nodos se hayan creado correctamente antes de continuar.
- *findmnt --verify*: Encuentra un sistema de archivos y comprueba el contenido de la tabla de montaje.
- *lsblk -fp*: Muestra información del sistema de archivos y muestra las rutas de los dispositivos completas.

Crear logical volumes en lvm

- *pvcreate /dev/sda4*: Indica que sda4 será un physical volume de udlvm.
- *vgcreate VG_TSIC2 /dev/sda4*: Dentro del physical volume se crea un volume group llamado VG_TSIC2 y que proviene de la partición física /dev/sda4.
- *vgs*: Muestra información de los volume group existentes.
- *lvcreate -L 1GB -n lv_oso VG_TSIC2*: Dentro del volume group se crean logical volumes.
- *lvs*: Muestra información de los volume group existentes.
- *mkfs.xfs /dev/VG_TSIC2/lv_oso*: Da formato xfs a las particiones lógicas creadas (logical volume).
- *mkdir /oso*: Crea el directorio oso.

- *mount /dev/VG_TSIC2/lv_oso /oso*: Monta sistema de archivos o dispositivos extraíbles en un punto de montaje particular en el árbol de directorios.

Crear una partición con disco duro externo

- *parted /dev/sdb*
- *mklabel msdos*
- *print*
- *mkpart primary xfs 1MB 2047MB*

Incrementar el tamaño de un logical volume

- *lvextend -L 1.5G /dev/VG_TSIC_2/lv_oso*: Incrementa el tamaño de un logical volume. Para ello debe tener espacio el volume group.
- *df -h*: Muestra información sobre el espacio total y el espacio disponible en cada disco montado en múltiples de 1024 (human readable).
- *xfs_growfs /dev/VG_TSIC_2/lv_oso*: Aumenta el tamaño de un sistema de archivos xfs (le avisa al SO que ya creció la partición).

Configuración de Redes

- *nmcli*: network manager command line interface.
  - nmcli connection show: Vemos las interfaces que tenemos y si ya está configurada.
  - nmcli connection add type ethernet ip4 172.16.51.137/25 gw4 172.16.51.129: Configura una interfaz.
- nmtui: network manager text user interface.
  - Edit a Connection>Add>Ethernet
    - Profile name: ens192
    - Device name: ens192
    - ipv4 configuration: Automatic (para que sea por DHCP) o Manual (o especificar direccion y gateway)
  - Activate a Connection: Comprobar que la interfaz esta activada.
    Comprobar la configuración de red:
- ip addr: Vemos las interfaces que hay con su respectiva IP.
- ifup ens192: Vemos si la interfaz está activada.

Creación de Usuarios/Grupos/Permisos

- *ls -lrt*: Enlista el contenido de un directorio con formato extendido (con usuarios y permisios) viendo el archivo mas antiguo primero

Creación de Usuarios/Grupos

Creación de Usuarios/Grupos y Modificarlos

- *useradd -u 1001 -c "miprimerusuario Peru" peru*: Crea un usuario con un userid específico y con comentario (visible en etc/passwd). Es lo mismo que adduser. Un usuario puede pertenecer a uno o más grupos.
- *useradd -u 2001 -g [europa|3000] francia*: Crea un usuario con un userid y un grupo específico (al especificar el grupo no crea por defecto su grupo idéntico).
- *groupadd america*: Crea un grupo.
- *groupmod -g 2000 america*: Modifica el groupid de un grupo.
- *usermod -g america peru*: Modifica el grupo al que pertenece un usuario.
- *userdel Italia*: Elimina un usuario.
- *chown francia /paris*: Cambia el usuario propietario de un archivo.
- *chgrp europa /paris*: Cambia el grupo de un archivo.

Verificación de los usuarios/grupos creados

- *cat /etc/passwd*: Se obtienen todos los usuarios creados en el sistema.
- *cat /etc/group*: Se obtienen todos los grupos creados en el sistema.
- *cat /etc/login.dfs*: En este archivo de configuración se puede observar que el uid/gid minimo es 1000 y uid/gid maximo es 60000 y que umask es 0022

Permisos

Para poder entrar a un directorio, es necesario tener permisos de lectura y ejecución (write es opcional). En Archivos creados el número máximo en permisos creados es 666, mientras que en directorios es 777. Por regla de seguridad, OS no da permiso de ejecucion a archivos pero sí a directorios para brincar entre subdirectorios

- *umask*: Permisos que se van a estar restando para crear los archivos y directorios. Dependiendo de este numero es el numero de los permisos que van a tener en la creacion de archivos y directorios.
- *chmod 744 iffel; chmod g+wx iffel; chmod o-r*: Cambiar los permisos de u n archivo
- *id*: Ver uid y gid del usuario actual.

Instalación de Paquetes y Repositorios

Instalación de paquetes desde el disco de instalación

1. Insertar el archivo .iso desde virtualbox
    - *lsblk*: Se comprueba que el disco está en sr0
2. Montar el disco en un directorio

- *mkdir /disk*: Crear directorio donde se montara
- *mount /dev/sr0 /disk/*: Monta el disco en el directorio
- *ls */disk/*: Comprueba que se pueden leer los archivos del disco
- *umount*: Desmonta el disco (no utilizarlo a menos que haya fallas al montar)

3. Se crean los archivos de repositorio
   - *cd /etc/yum.repos.d*: Se cambia al directorio de repos
   - *vi mirepo.repo*: Se crea la estructura del archivo
     [BaseOS]
     name=BaseOS
     baseurl=file:///disk/BaseOS
     enabled=1
     gpgcheck=0
     [AppStream]
     name=App Stream
     baseurl=file:///disk/AppStream
     enabled=1
     gpgcheck=0
   - *dnf*: Manejador de paquetes para distribuciones de Linux basadas en RPM.
   - *dnf clean all*: Limpia los archivos temporales guardados para los repositorios (incluyendo repositorios deshabilitados o eliminados, lo usamos porque cambiamos el nombre del paquete mirepo).
   - *dnf repolist*: Enlista todos los repositorios habilitados (encuentra el repositorio creado).
   - *dnf list*: Imprime listas de paquetes dependiendo de la relación de los paquetes con el sistema (encuentra todos los paquetes que puede instalar yescarga los repositorios).
   - *dnf install httpd*: Instala la herramienta httpd, el cual permite configurar un linux como un servidor web.

- systemctl start httpd
- firewall-cmd --permanent --add-service=http
- firewall-cmd --reload

Instalación de paquetes desde internet

1. Eliminar las configuraciones anteriores:
   - *unmount /disk/*
   - *mv /etc/yum.repos.d/mirepo.repo /root/*:
2. Registro a la suscripción de Redhat
   - *sucription-manager register*:

        - Username:
        - Password:

3. Asociarlo a un contrato
    - *subscrption-manager list --available*: Ver los contratos disponibles en nuestra cuenta.
    - *subscription-manager attach --pool=[InserteAqui]*: Realiza la asociación.
4. Habilitar los paquetes que se desean agregar.
    - *subscription-manager repos --list*: Enlista todos los repositorios disponibles para este contrato.
    - *subscription-manager repos --enable=rhel-8-for-x86_64-appstream-rpms*:
    - *subscription-manager repos --enable=rhel-8-for-x86_64-baseos-rpms*
5. Limpiamos todos los repositorios del sistema y verificamos los paquetes en nuestro sistema:
    - *dnf clean all*: Limpia los archivos temporales guardados para los repositorios.
    - *dnf repolist*: Enlista todos los repositorios habilitados (encuentra el repositorio agregado).
    - *dnf list*: Imprime listas de paquetes dependiendo de la relación de los paquetes con el sistema (encuentra todos los paquetes que puede instalar y descarga los repositorios).
    - *yum upgrade httpd*: Actualiza la herramienta con los paquetes actualizados.
    - *dnf whatprovides netstat*: Checa que paqueteria contiene cierta herramienta

Administración de un Firewall (Firewall-CMD)

- *firwall-cmd --list-all-zones:* Revisar la política que tienen todas las zonas (block, dmz, drop, external, internal, work, trusted, etc)
- *firwall-cmd --get-default-zones*: Obtener las zonas activas.
- *firwall-cmd --info-zone=public* Obtiene información de una zona como su interfaz, los servicios configurados (cockpit, dhcp, etc), puertos definidos, protocolos, origen
- *firewall-cmd --permanent --add-port=80/tcp --zone=public*: Agregar como regla admitir http por puerto (permament para que se mantengan los cambios)
- *firewall-cmd --reload*: Necesario recargar cada que se realiza un cambio.

- *ls /lib/firewalld/services*: Se pueden observar todos los servicios con los que se puede trabajar (y asi revisar los puertos que se utilizan)
- *firewall-cmd --permanent --add-service=high-availability*:
- *firewall-cmd --permanent --remove-service=ssh --zone=public*: (no elimina la sesión actual de ssh porque la conexión ya está establecida)
- *netstat -putona*: Muestra el estado de las conexiones existentes, t (tcp),u(udp),p(procesos)
- *firewall-cmd --permanent --add-source=10.77.5.143 --zone=public*: Se agrega la dirección ip para la zona interna

- *firewall-cmd --permanent --add-source=172.16.51./24 --zone=public*: Se agrega todo el segmento de red
- *systemctl status firewalld*: Observar que el servicio de firewall esta activo.
- *systemctl stop firewalld*: Detener el servicio de firewall
- *systemctl enable firewalld*: Para que inicie firewall y se quede disponible aunque se reinicie el equipo
-
    - *systemctl start firewalld*: Para levantar el servicio de firewall

---

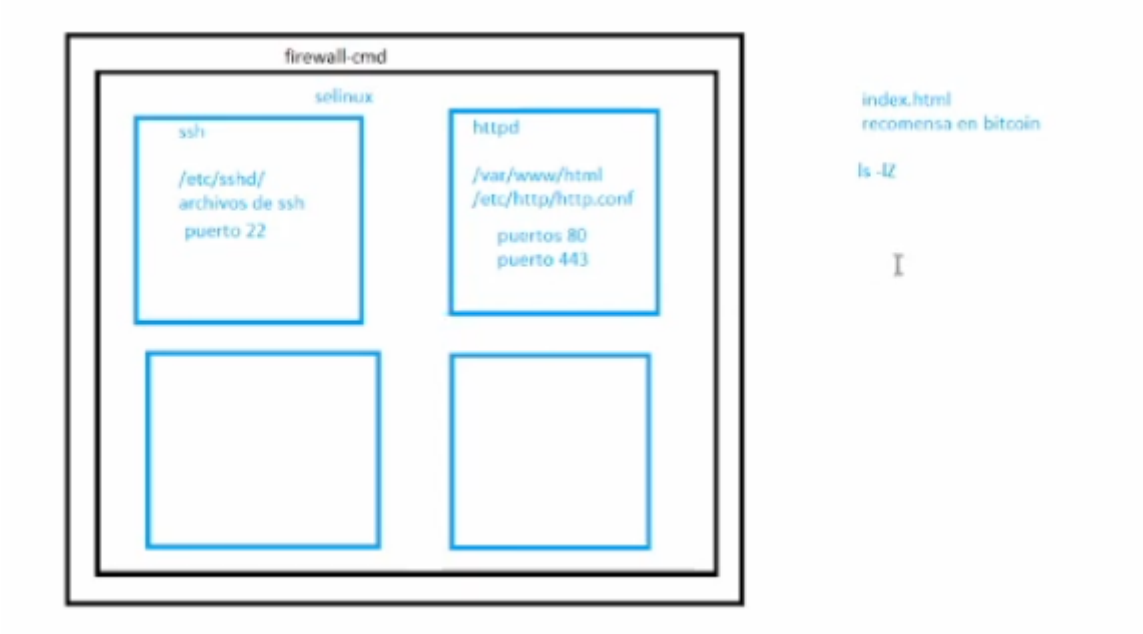
Selinux

Selinux nos sirve para darle formalidad a los archivos y directorios y les demos un propósito. Selinux se compone de contextos, se define el contexto que va a tener cada archivo y directorio. Si el contexto no funciona o no es el correcto el servicio no levanta
Ej. Archivo 1, para qué vas a servir y te pongo en el lugar que corrrespondes. Si no te tengo identificado o no te autorice no pasas y no te levanto

- *ls -lZ*: Enlista el contenido de un directorio, imprimiendo el contexto de seguridad y permisos de cada archivo. Se pueden ver roles como httpd_sys_content, log,httpd_config_t

Escenario 1

Como buena práctica se ha cambiado el puerto de http al 85. Linux dice que le ha avisado de este cambio y no tiene declarado ese puerto para ese servicio, por lo que no levantará hasta que se declare. Esto porque http es un well known port y se intenta cambiar por otro well known port.



- *systemctl status httpd*: Muestra que el servicio no funciona y hubo un permission denied.
- *cat /etc/sysconfig/selinux*: Muestra los estados de selinux.

    - Enforcing: Toda política se aplica
    - Permissive: Imprime warnings pero deja trabajar
    - Disabled: No se utiliza selinux

- *getenforce*: Vemos en qué estado de selinux se encuentra
- *setenforce 0*: Se cambia a modo permisivo. Con 1 cambia a enforcing
- *ausearch -c 'httpd' --raw*: Muestra que en httpd el src es 85
  Se buscará cambiar el puerto en el que escucha el servidor web.
- *dnf whatprovides policy*: Comando que saber que paquete contiene determinado comando.
- *dnf install policycoreutils:* Se instala el servicio que contiene el comando semanage
- *semanage*: Comando que permite configurar contextos, habilitar puertos, etc.
- *semanage port -a -t http_port_t -p tcp 85*: Cambia de puerto y el tipo para escuchar el servicio web en 85.
- *systemctl restart httpd*: Reiniciamos el servicio http
- *systemctl status httpd*: Vemos el estado del servicio y vemos que se corrigió

Escenario 2

Se quiere cambiar que, en lugar de utilizar /var/www, se utilice /web.

- *ls -laZ /web*: No tiene contexto de contenido, por lo que hay que configurarlo para que levante la página
- *ls -laZ /var/www/*: Si no nos acordamos del contexto web , ahí lo podemos encontrar (httpd_sys_content)
- semanage fcontext -a -t httpd_sys_content "/web(/*)?": A todo el contenido de /web se le asigna ese contexto
- *restorecon -Rv /web*: Con eso ya podemos levantar nuestro servicio

---

- *semanage login -l:* Muestra que hay un servicio de login para root
- *seinfo -u:* Muestra que existen 8 usuarios para configurar el contexto.
- *seinfo -t*: Muestra todos los tipos de contexto que podemos configurar

---

Escenario 3

Se quiere cambiar el puerto que utiliza ssh

- *vi /etc/ssh/sshd_config*: Se modifica el archivo de configuración de ssh (PORT=2222)
- *systemctl restart sshd*: Se observa que no se puede reiniciar el servicio.
- *systemctl status sshd*: Vemos que hay error en la ejecución del servicio
- *sealert:*: Nos dice que debemos de hacer para realizar una configuración de selinux. Comando que nos debemos aprender

- *journalctl -xe*: Comando que aparecio como sugerencia cuando tratamos de reiniciar ssh.
    - sealert nos pone las banderas donde nos dice el problema (veo que ocupas el puerto tal, por lo que hay que configurarlo. Te recomiendo ejecutar este comando)
- *semanage port -a -t ssh_port_t -p tcp 2222*: Cambia de puerto de escucha para ssh.
    - Cuando reinicia el servicio (systemctl restart sshd) y le ponemos status, vemos que ya está activo

      SEMANA #6

Administración y gestión de contraseñas

Se configura en:
/etc/security/pwquality.conf

CONFIGURACIONES EN PWQUALITY.CONF
difok: numero de caracteres que no deben estar presentes de la pw anterior
minlen: longitud minima
minclass: minimo de tipos de cada caracter
maxrepeat: maximo numero de repeticion de caracteres
maxclassrepeat: maximo numero seguido de caracteres del mismo tipo
dictcheck: que no este en un diccionario existente
usercheck: que no contenga alguna forma del username
retry: numero de intentos

CONTRASEÑAS BANEADAS
/usr/share/dict/linux.words

Agregar archivo de PWs prohibidas a la lista
#create-cracklib-dict /usr/share/dict/linux.words

CONFIGURACION DEL PASSWORD
/etc/login.defs
PASS_MAX_DAYS: Duracion Maxima de Password (expiracion en dias)
PASS_MIN_DAYS: Duracion minima de Password
PASS_MIN_LEN: Longitud minima de password
PASS_WARN_AGE: Dias de aviso de caducacion de password

UID_MIN/MAX: Minimo/Maximo de UID

Gestión de sesiones de acceso

Se configura sobre la sesiones SSH:
/etc/ssh/sshd_config

Port

SyslogFacility AUTH
SyslogFacility AUTHPRIV
LogLevel INFO Obtener mas logs

LoginGraceTime: Tiempo para ingresar
PermitRootLogin: Acceso directo a root

MaxAuthTries: Maximo numero de intentos

MaxSessions: Maximo numero de sesiones

ClientAliveInterval: Cuanto tiempo estara inactiva la sesion

ClientAliveCountMax: Cuanto tiempo maximo estara activa la sesion

Banner : Mostrar como banner al iniciar la sesión

Configurar puerto de ssh:

#semanage port -a -t ssh_port -p tcp 2222

Reiniciar sshd

#system restart sshd.service

Status

#systen status sshd.service