S.I.G.D.

Sistemas Operativos III

ProgWare

ROL	APELLIDO	NOMBRE	C.I	E-MAIL	TEL/CEL
Coordinador	Gallas	Lucas	5.363.476-5	lucasgallas2003@gmail.com	093766017
Sub-coordinador	Gonzalo	Martinez	5.230.446-8	Gonzalom747@gmail.com	094663018
Integrante	Vidir	Kevin	5.646.391-3	kevinvidir@gmail.com	094230963
Integrante 2	Alvez	Mauricio	5.450.509-8	alvez.mauricio04@gmail.com	091240243
Integrante 3	Almeyra	Valentín	5.348.527-1	vaalca2017@gmail.com	092954187

Docente: Rodríguez, Carlos

Fecha de culminación

8/11/2022

TERCERA ENTREGA

I.S.B.O. **3°BC**

Índice

Usuarios necesarios para el Sistema Operativo

- **Administrador de Backups**
- **Administrador de Logs**
- **Operador**
- **Root**

Comandos:
groupadd Administradores
useradd -G Administradores Admin_Backups
useradd -G Operadores Operador

Configuración en Sudoers:

```
## Alias de Administrador y Operador

# Alias de Administrador de Backups
User_Alias ADM_B = Admin_Backups

## Alias de Operador
User_Alias OP = Operador

## Command Aliases
## These are groups of related commands...

%OP 192.168.1.3 = NOPASSWD:/usr/bin/mysql* , /usr/bin/gzip , /usr/bin/tar , /usr/bin/rsync , /usr/bin/less , /usr/bin/bash
 , /usr/bin/gunzip , /usr/bin/grep , /usr/bin/gzip , /usr/bin/ssh , /usr/bin/iptables , /usr/sbin/ifconfig/ , /etc/cryptta
b/ , /etc/libreport/events/ , /Scripts/ , /backups/ , /etc/my.cnf.d

## Alias de Comando - Crontabs
Cmnd_Alias CRON = /var/spool/cron/crontabs
OP ALL = CRON

## Alias de Comando - Backups
Cmnd_Alias BS = /Scripts/BackupCompleto.sh
ProgWare_Server ALL = BS
ADM_B ALL = BS
OP ALL = BS

## Alias de Comando - Logs
Cmnd_Alias LG = /var/log
OP ALL = LG
```

Estudio De Roles:

Usuarios del Sistema:

Invitado(Sin Login):

Tiene permiso de consulta y visualización (fixture, resultados, y gráficos, rendimiento, incidencias y anotaciones de un jugador)

Analista:

Se encargan del análisis de los datos y de su ingreso al sistema, registrando las incidencias, anotaciones y sanciones

Juez:

Los Usuarios con este Rol tienen los permisos de validar las incidencias registradas por los analistas.

Director Técnico (D.T.):

Se encarga de la gestión de su equipo, es decir tiene permisos de asignar jugadores al mismo, y de cargar las fichas de cada jugador

Administrativo:

Es el de mayor cargo y permisos dentro del sistema, este tiene permisos de cargar la ficha de jugadores,crea los equipos, y se ocupa de dar los roles a cada usuario del sitio

Administrador:

Super Usuario

Usuario de la Base de Datos:

Root:

Super Usuario

Administrativo:

Tiene permisos para crear perfiles, modificarlos, y de deshabilitarlos

Director Técnico(D.T):

Puede modificar su equipo, asignar y desasignar jugadores

Analista:

Ingresa los datos e incidencias

Usuarios del Servidor:

Root:

Super Usuario.

Administrador de Respaldos:

Se encarga de gestionar los respaldos, fecha y hora, datos a guardar.

Operador:

Tiene control sobre archivos, directorios, scripts y comandos.

Sistemas Operativos A Usar:

Para el uso del sistema se recomienda el uso de Windows 10, esté teniendo soporte aún vigente hasta el 14 de octubre de 2025 donde se dejará de dar soporte al Windows 10.
Se recomienda específicamente el uso de Windows 10 en su versión Pro, ya que esta ofrece una mayor seguridad, y opciones de accesibilidad, entre otras cosas, para más información se puede consultar en los anexos, que se incluirá más información

El Sistema Operativo de Windows 10 Pro tiene un coste de $U12.000, lo cual equivaldría a U$D292, en la cotización actual

(Revisar Anexo I para más información)

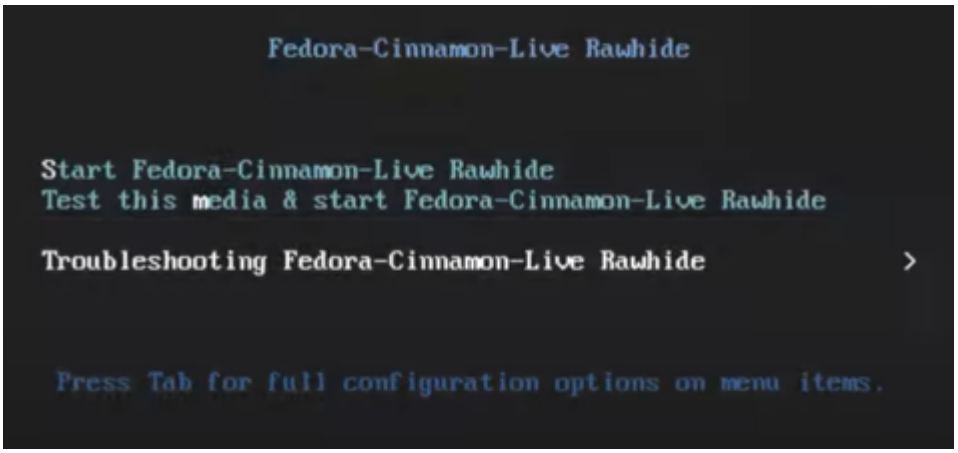
Para el servidor se recomienda Se recomienda usar un Servidor Fedora 36, esto debido a su fácil uso, y ser un sistema operativo de libre uso, con buena seguridad y estar respaldado por Red Hat, lo que incluye soporte comercial y actualizaciones constantes

(Revisar Anexo I para más información)

Manual de Instalación Fedora Server:

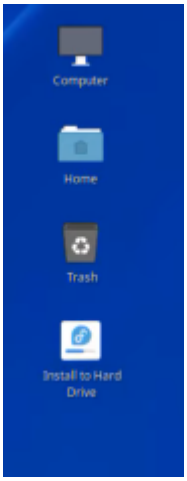
Se utilizará Cinnamon para la instalación.

1)



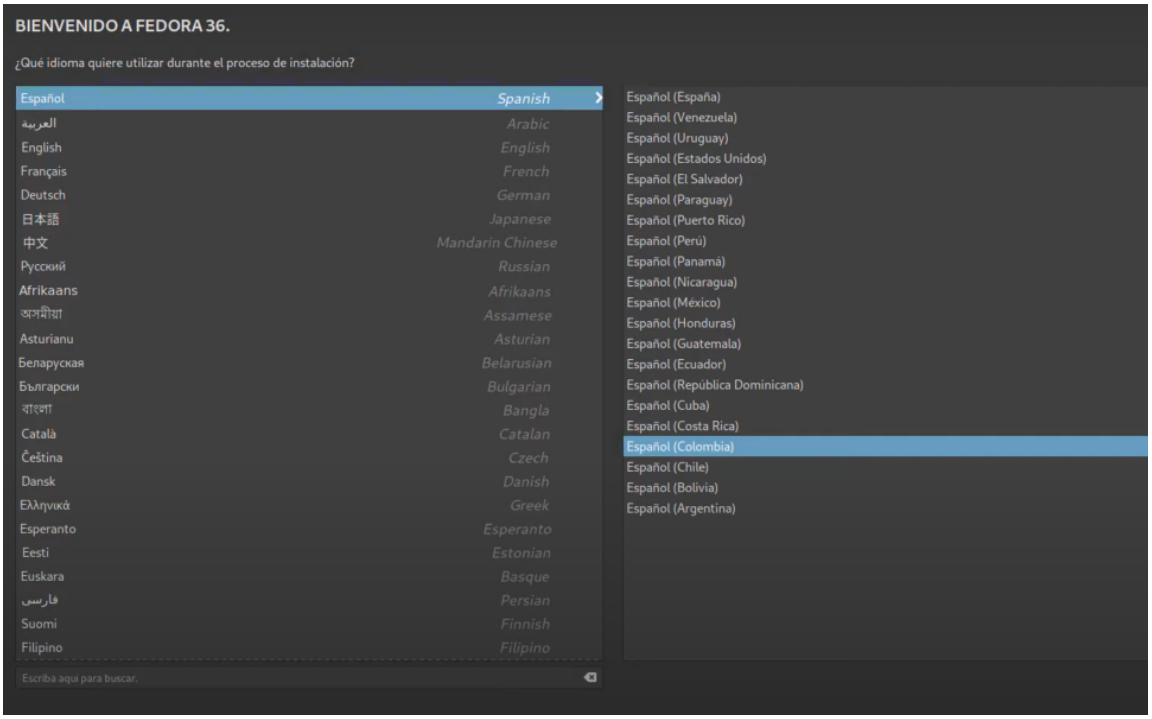
Le Damos Click en “Start Fedora-Cinnamon-Live Rawhide”

2)



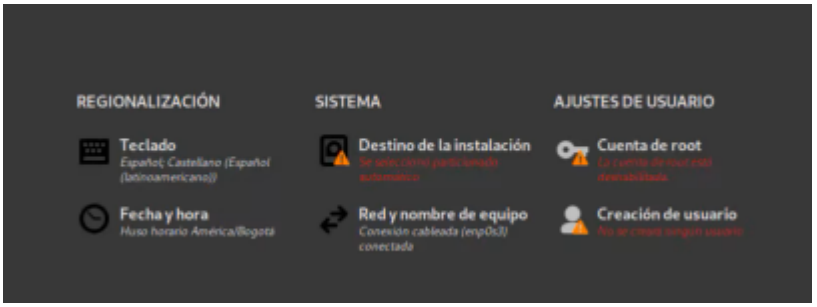
Se Abrirá el modo live de Fedora, le damos en “Install to Hard Drive”

3)



Seleccionamos el Idioma

4)



-En “Destino de la instalación” seleccionamos el disco duro.
-En “Cuenta de root” habilitamos la casilla de “activar cuenta root”, y le ingresamos la contraseña
-En “Creación de usuario” configuramos al usuario administrador
Después de terminar esto le damos a Instalar servidor, y con eso finalizamos la instalación

Instalar MariaDB en Fedora 36:

~$ sudo yum update
El paquete que necesitamos es mariadb-server, que instalaremos con yum:

~$ sudo yum install -y mariadb-server
Una vez descargado e instalado MariaDB Server junto a sus dependencias, se crea un nuevo servicio en Fedora 36 llamado mariadb.service que por defecto no queda en ejecución ni tampoco habilitado para su arranque automático.

~$ sudo systemctl start mariadb
Podemos comprobar el estado del servicio con el comando systemctl status mariadb:

El servicio de bases de datos se encuentra en ejecución y sólo falta habilitar el servicio para que arranque automáticamente con cada inicio de Fedora 36:

~$ sudo systemctl enable mariadb

Si sólo quieres instalar el cliente de MariaDB el paquete que necesitarías es mariadb:
~$ sudo yum install -y mariadb

Menús Script para los Usuarios del Sistema

```
#!/bin/bash
function _menuPrincipal()
{
  echo "1) Operador"
  echo "2) Administrador"
  echo "10) Salir"
  echo
  echo "Elija una opción:"
 }

 function _menuOperador()
{
  echo "1) Hay Usuarios Conectados?"
  echo "2) Ip del Servidor"
  echo "3) Base de datos funcionando?"
  echo "4) Cambiar Password"
  echo "5) Respaldos y Recuperación del Sistema"
  echo "6) Respaldos y Recuperación de la Base de Datos"
  echo "7) Logs"
  echo "10) Salir"
  echo
  echo "Elija una opción:"
 }

  function _menuAdministrador()
{
  echo "1) Hay Usuarios Conectados?"
  echo "2) Ip del Servidor"
  echo "3) Base de datos funcionando?"
  echo "4) Cambiar Password"
  echo "5) Respaldos y Recuperación Sistema"
  echo "6) Respaldos y Recuperación de la Base de Datos"
  echo "7) Usuarios"
  echo "8) Grupos"
  echo "9) Logs"
  echo "10) Salir"
```

```
  echo
  echo "Elija una opción:"
 }
 function _submenuUsuarios()
{
  echo "1) Creación"
  echo "2) Modificacion - Nombre "
  echo "3) Modificación - Contraseña "
  echo "4) Borrado"
  echo "10) Salir"
  echo
  echo "Elija una opción:"
 }
 function _submenuGrupos()
{
  echo "1) Creación"
  echo "2) Modificación"
  echo "3) Borrado"
  echo "10) Salir"
  echo
  echo "Indica una opción:"
 }

 opc=0
 until [ $opc -eq 10 ]
     do
         case $opc in

           1)
              opc1=0
              until [ $opc1 -eq 9 ]
              do
              case $opc1 in
                    1)
                    echo "Operador - Hay Usuarios Conectados"
                    w
                    _menuOperador
             ;;
                    2)
```

```
        echo "Operador - IP Servidor"
        ifconfig
        _menuOperador
;;
        3)
        echo "Operador - Base de Datos Funcionando?"
        systemctl status mariadb
        _menuOperador
;;
        4)
        echo "Operador - Cambiar Password"
        sudo passwd
        _menuOperador
;;
        5)
        echo "Operador - Respaldos y Recuuperación del Sistema"
        sudo sh /Scripts/ScriptBackupRecovery.sh
        _menuOperador
;;

        6)
        echo "Operador - Respaldos y Recuperación de la Base de Datos"
        sudo sh /Scripts/ScriptBD.sh
        _menuOperador
;;
        7)
        echo "Logs"
      ;;
        *)
        _menuOperador
;;

      esac
      read opc1

 done
_menuPrincipal
  ;;
```

```
2)
  opc2=0
  until [ $opc2 -eq 10 ]
  do
        case $opc2 in
          1)
            echo "Administrador - Hay usuarios Conectados?"
            w
            _menuAdministrador
            ;;
          2)
            echo "Administrador - IP Servidor"
            ifconfig
            _menuAdministrador
            ;;
          3)
         echo "Operador - Base de Datos Funcionando?"
          systemctl status mariadb
          _menuAdministrador
            ;;
          4)
         echo "Operador - Cambiar Password"
            sudo passwd
            _menuAdministrador
            ;;
          5)
         echo "Operador - Respaldos y Recuperación del Sistema"
         sudo sh /Scripts/ScriptBackupRecovery.sh
         _menuOperador
            ;;
          6)
         echo "Operador - Respaldos y Recuperación de la Base de Datos"
         sudo sh /Scripts/ScriptBD.sh
         _menuOperador
            ;;
          7)
            echo "Administrador - Usuarios"
            opc3=0
            until [ $opc3 == 10 ]
```

```
do
case $opc3 in
    1) echo "Administrador - Usuarios - Creacion"
      echo "Insertar nombre"
      read user
      echo "Agregar Contraseña"
      read contra
       adduser $user -p $contra
    echo "usuario actualizado"
    echo
      _submenuUsuarios
      ;;

    2) echo "Administrador - Usuarios - Modificacion Nombre"
    echo "Ingresar usuario a modificar"
    read user
    echo "Ingresar nuevo nombre"
    read nuser
    usermod -l $nuser $user
    echo "usuario actualizado"
    echo
    _submenuUsuarios
      ;;

    3) echo "Administrador - Usuarios - Modificación Contraseña"
    echo "Ingrese usuario a modificar"
    read user
    passwd $user
    echo "usuario actualizado"
    echo
    _submenuUsuarios
      ;;

    4) echo "Administrador - Usuarios - Borrar"
    echo "usuario a eliminar"
    read user
    userdel -r $user
    echo "usuario actualizado"
    echo
```

```
        _submenuUsuarios

          ;;
        *)
          _submenuUsuarios
          ;;
  esac
  read opc3
  done
  _menuAdministrador

  ;;
 8)
  echo "Administrador - Grupos"
  opc4=0
  until [ $opc4 -eq 10 ]
  do
  case $opc4 in
      1) echo "Administrador - Grupos - Creación"
      echo "Ingrese Nombre del Grupo"
      read grupo
      groupadd $grupo
      echo "Grupo actualizado"
      echo
      _submenuGrupos
        ;;

      2) echo "Administrador - Grupos - Modificacion Nombre"
      echo "Grupo a modificar"
      read grupo
      echo "nuevo Nombre del grupo"
      read ngrupo
      groupmod -n $ngrupo $grupo

      echo "Grupo actualizado"
      echo
      _submenuGrupos
        ;;
```

```
                2) echo "Administrador - Grupos - Modificacion ID"
                echo "Grupo a modificar"
                read grupo
                echo "Nuevo GID"
                read gid
                groupmod -g $gid $grupo

                echo "Grupo actualizado"
                echo
                _submenuGrupos
                  ;;

                3) echo "Administrador - Grupos - Borrar"
                echo "Grupo a Modificar"
                read grupo
                groupdel $grupo
                echo "Grupo actualizado"
                echo
                _submenuGrupos
                  ;;
                *)
                  _submenuGrupos
                  ;;
            esac
            read opc4
            done
            _menuAdministrador

            ;;

           *)
            _menuAdministrador
            ;;
        esac
        read opc2
done
_menuPrincipal
        ;;
```

```
        *)
          _menuPrincipal
          ;;
        esac
        read opc
    done
```

Rutinas de Backup con Crontab

Scripts

Scripts de Backup y Recuperación del Sistema (Total e Incremental): Estos scripts crean el respaldo total e incremental comprimiendo los directorios del sistema, así como crean el respaldo de los logs. Además de eso se encargan de descomprimir los directorios respaldados, mediante este código (tanto menú como scripts individuales):

Script de Backup Total:

```
#!/bin/bash


cd /backups/Total && tar -cpvzf "Backup-Total-`date +%d-%b-%Y`.tgz" /home /etc /root
cd /backups/Total && tar -cpvzf "Backup-Total-Logs-`date +%d-%b-%Y`.tgz" /var/log

echo "Hecho!"
```

Script de Backup Incremental:

```
#!/bin/bash

cd /backups/Incremental && tar -cpvzf "Backup-Incremental-`date +%d-%b-%Y`.tgz" /home /etc /root /var/log
cd /backups/Incremental && tar -cpvzf "Backup.Incremental-Logs`date +%d-%b-%Y`.tgz" /var/logs

echo "Hecho!"
~
```

Script de Recovery Total:

```
#!/bin/bash


cd /backups/Total && tar -xpvzf Backup-Total-* -C /recovery/Total
cd /backups/Total && tar -xpvzf Backup-Total-Logs* -C /recovery/Total

echo "Hecho!"
~
```

Script de Recovery Incremental:

```
#!/bin/bash

cd /backups/Incremental && tar -xpvzf Backup-Incremental-* -C /recovery/Incremental
cd /backups/Incremental && tar -xpvzf Backup-Incremental-Logs* -C /recovery/Incremental

echo "Hecho!"
~
```

Script Menú de Backup:

```
echo "4) Recovery Incremental"
echo "5) Volver"
read opcion
case $opcion in
        1) clear
                echo "::Respaldo Total::"
                sudo sh /Scripts/BackupTotal.sh
                ;;
        2) clear
                echo "::Respaldo Incremental::"
                sudo sh /Scripts/BackupIncremental.sh
                ;;
        3) clear
                echo "::Recovery Total::"
                sudo sh /Scripts/RecoveryTotal.sh
                ;;
        4) clear
                echo "::Recovery Incremental::"
                sudo sh /Scripts/RecoveryIncremental.sh
                ;;
        5) clear
                exit
                ;;
        *) clear

esac
done
```

```
echo "4) Recovery Incremental"
echo "5) Volver"
read opcion
case $opcion in
        1) clear
                echo "::Respaldo Total::"
                sudo sh /Scripts/BackupTotal.sh
                ;;
        2) clear
                echo "::Respaldo Incremental::"
                sudo sh /Scripts/BackupIncremental.sh
                ;;
        3) clear
                echo "::Recovery Total::"
                sudo sh /Scripts/RecoveryTotal.sh
                ;;
        4) clear
                echo "::Recovery Incremental::"
                sudo sh /Scripts/RecoveryIncremental.sh
                ;;
        5) clear
                exit
                ;;
        *) clear
esac
done
```

Script de Respaldo y Restauración de Base de Datos: Estos scripts crean el respaldo total e incremental de la base de datos haciendo una copia de esta en formato .sql, mediante este código (tanto menú como scripts individuales):

Script de Respaldo:

```
#!/bin/bash

mysqldump -u root -h localhost 'ProgWare' > bd_pw-bck.sql -p

echo "El respaldo se realizó exitosamente."

sleep 2
```

Este respaldo se realiza tanto de forma manual como automática mediante el script y crontab, a través de estos códigos.

Script de Restauración:

```
#!/bin/bash

mysqldump -u root -h localhost 'ProgWare' < bd_pw-bck.sql -p

echo "La restauración se realizó exitosamente."

sleep 2
```

Script Menú de Base de Datos:

```
#!/bin/bash

clear

opcion=0
until ["$opcion" -eq "3"];
do



echo "::::Menu Base de Datos::::"
echo ""
echo ""
echo "1) Respaldar Base de Datos"
echo "2) Restaurar Base de Datos"
echo "3) Volver"
read opcion
case $opcion in
        1) clear
                sudo sh /Scripts/RespaldoBD.sh
                ;;
        2) clear
                sh /Scripts/RestaurarBD.sh
                ;;
        3) exit
                ;;
        *)
                ;;
esac
done
```

Crontab

Para que estos script se ejecuten de forma rutinaria se los ejecutó con crontab de forma total, incremental y manual mediante el archivo crontab, de esta forma:

```
#Total
30 18 * * * 6 cd /Scripts/ && ./BackupTotal.sh

#Incremental
00 19 * * * cd /Scripts/ && ./BackupIncremental.sh
00 18 * * * cd /Scripts/ && ./RespaldoBD.sh
```

Se accede a SSH mediante la IP fija del equipo y se escribe el comando **crontab -e** para editar el archivo. Se agregan ambas sentencias (total e incremental) y se guarda el archivo. Si salió bien nos tendría que aparecer un mensaje como este:

```
[ProgWare_Server@192 ~]$ ssh -p 3458 Operador@192.168.1.3
The authenticity of host '[192.168.1.3]:3458 ([192.168.1.3]:3458)' can't be established.
ED25519 key fingerprint is SHA256:jx3f4ATCPiiWyqwC1LJnwYVqE3rhsppmH0al2IO+/zA.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:1: 192.168.1.7
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[192.168.1.3]:3458' (ED25519) to the list of known hosts.
Operador@192.168.1.3's password:
Web console: https://192.168.1.3:9090/ or https://192.168.1.3:9090/

Last login: Mon Nov  7 23:26:53 2022
[Operador@192 ~]$ crontab -e
no crontab for Operador - using an empty one
crontab: installing new crontab
```

En el respaldo total la fecha y hora de este serán a las 18:30 de cada domingo de la semana y el mes.

Elegimos este método de backup porque nos garantiza que tengamos una copia total de los archivos del sistema ante cualquier eventualidad, y lo hacemos a la fecha y hora especificadas debido a que en estas no hay actividad en el sistema que interrumpa el respaldo, por tanto no se crean archivos nuevos a ser respaldados.

En el respaldo incremental la fecha y hora de este serán a las 19:00 todos los días de la semana y el mes.

De forma similar al respaldo incremental, elegimos esta fecha y hora debido a la nula actividad del sistema, así mismo, este tipo de respaldo nos permite ir guardando los nuevos datos que se crean en el sistema de forma automática para no depender de las copias más viejas que crea el respaldo total.

En el respaldo incremental la fecha y hora de este pueden ser cualquiera de las que el usuario del sistema requiera para poder respaldar el mismo.

Configuración de red en terminales y el servidor

Si no está configurada la IP fija tenemos que ejecutar el comando sudo vi /etc/networks.
Una vez dentro escribiremos lo siguiente:

 # Configuración de dirección IP fija para el interfaz enp0s3
auto enp0s3
iface enp0s3 inet static
address 192.168.56.101
netmask 255.255.255.0
network 192.168.1.3
broadcast 192.168.1.255
gateway 192.168.1.4

Una vez hecho esto es necesario reiniciar la interfaz de red. Para ello ejecutamos los siguientes códigos:

$ sudo ifconfig enp0s3 down
$ sudo if enp0s3 up

Una vez ya reiniciada la interfaz de red, procedemos a comprobar la conectividad a otros equipos de red y a internet mediante los comandos:

$ ping 192.168.1.4 (para comprobar conectividad con tu puerta de enlace)
$ ping google.com (para comprobar conexión a internet)

Para cortar la ejecución del ping tecleamos CTRL + C.

Para ingresar en el cliente solo debemos abrir **PuTTy** y en el campo **Host Name (or IP address)**, ingresar nuestra IP que la conseguimos también de ejecutar **ifconfig**.

Instalación y configuración de SSH

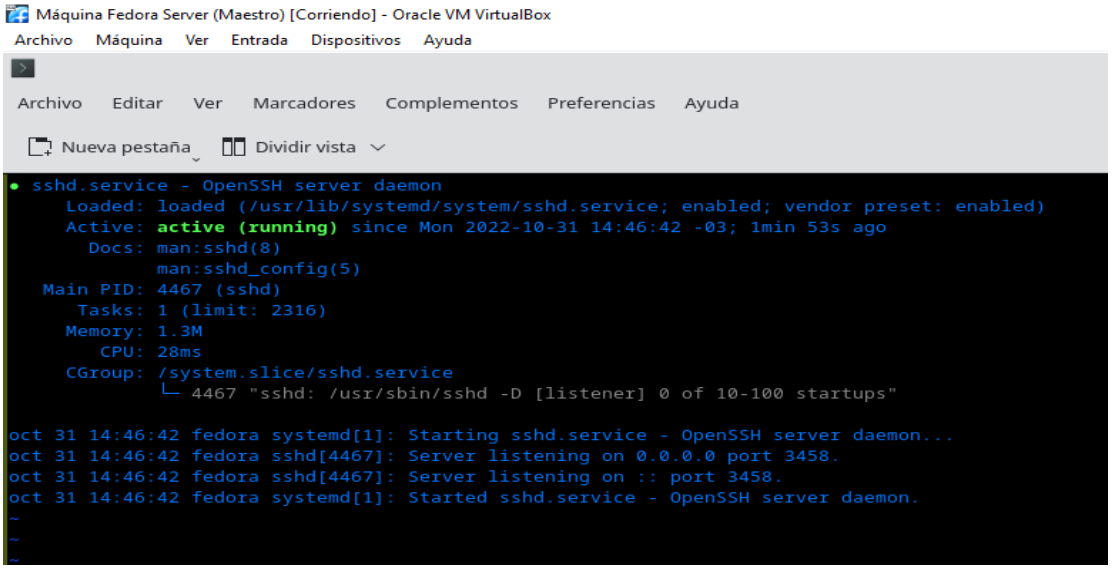
Comandos

(realizar los pasos como superusuario - se ingresa escribiendo “su -” en la terminal y escribiendo la contraseña)

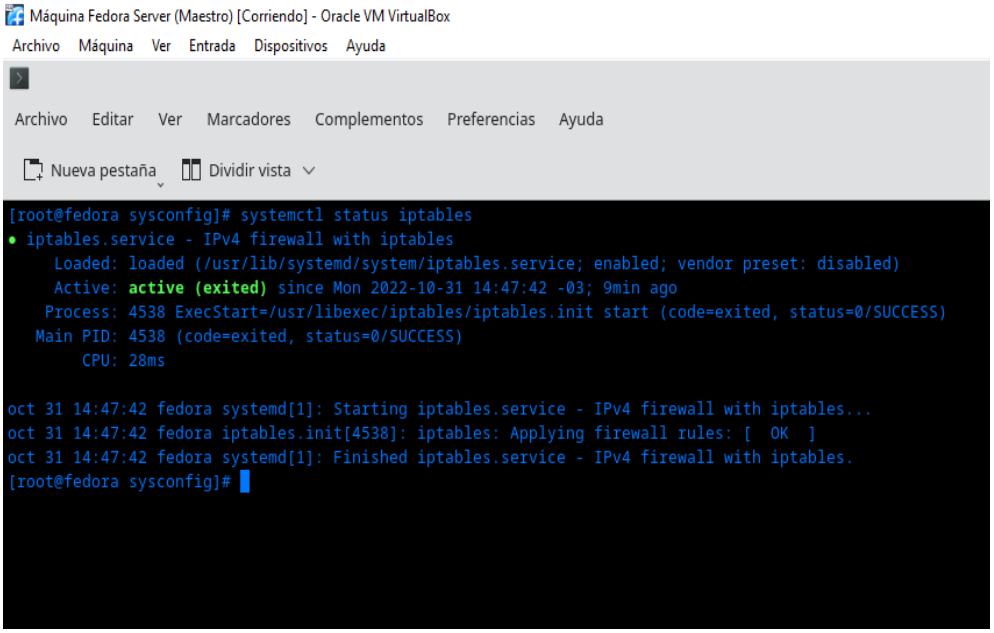
1. **Instalación:** dnf -y install openssh-server openssh-clients
   dnf -y install iptables-services
2. **Creación del servicio:** systemctl enable sshd
3. **Ejecución del servicio:**
   SSH: systemctl start sshd
   Iptables: systemctl start iptables
4. **Entrar al directorio:** cd /etc/ssh
5. **Escribir el comando:** netstat -ptona (aquí podremos ver en el apartado “Local Address”, a continuación de “:” el puerto utilizado por el servicio en específico, hemos de tener en cuenta esto para poder establecer un puerto nuevo para el servicio SSH que no esté siendo utilizado por otro servicio.).
6. **Configuración del archivo de configuración de SSH:** Una vez en el directorio “/etc/ssh” escribir “vi sshd_config” y dar enter.
   Una vez dentro del archivo pulsar shift+i para poder editarlo. A continuación, borramos el “#” del inicio del texto que dice “Port 22”, borramos el número de puerto y escribimos uno nuevo, en este caso se eligió el puerto 3458. Más abajo se encuentra “PermitRootLogin yes” que debemos cambiar por “PermitRootLogin no”, que deshabilita el inicio de sesión como superusuario, evitando así posibles ataques de fuerza bruta al sistema. Luego editamos la opción “SyslogFacility AUTH” borrando el “#” y cambiándola por “SyslogFacility AUTHPRIV”. Una vez editadas ambas partes guardar el archivo (ctrl+o → :x → enter).
7. **Configuración de SELinux:** En Fedora 36 el módulo de seguridad SELinux está habilitado por defecto, lo que significa que debemos agregar una regla para admitir el puerto establecido para SSH. Agregaremos la regla escribiendo el comando “semanage port -a -t ssh_port_t -p tcp 3458” donde 3458 es el puerto anteriormente establecido para el servicio SSH.
   Reiniciar SSH para aplicar cambios (systemctl restart sshd).
8. **Dirigirse a:** /etc/sysconfig (estando en “/etc/ssh” escribir “cd ..” y luego “cd sysconfig/”).
   Abrir el archivo iptables escribiendo “vi iptables” y pulsando “enter”.

Hemos de añadir una regla a iptables que habilite el nuevo puerto para SSH, para ello cambiaremos la línea que dice “-A INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT” por “-A INPUT -p tcp -m state --state NEW -m tcp --dport 3458 -j ACCEPT” donde 3456 es el puerto establecido para el servicio SSH.
Guardar el archivo.

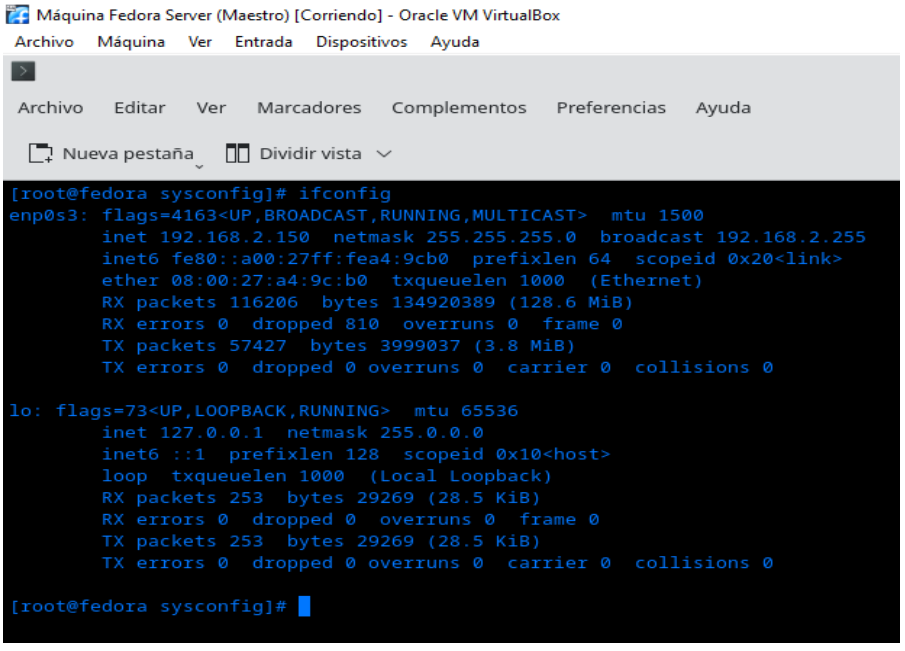
9. **Ejecutar la siguiente serie de comandos:**
systemctl disable firewalld (Deshabilita firewalld, para evitar conflictos con iptables).
systemctl enable iptables (Habilita el inicio del servicio iptables junto con el sistema).
systemctl enable sshd (Habilita el inicio del servicio SSH junto con el sistema).
Reiniciar los servicios para aplicar cambios (“systemctl restart sshd” → “systemctl restart iptables”).
Escribir el comando “systemctl status sshd” para ver el estado del servicio, en el apartado “Active” debe decir “active” en color verde y más abajo debe decir “Server listening on port 3458” o el puerto antes establecido.



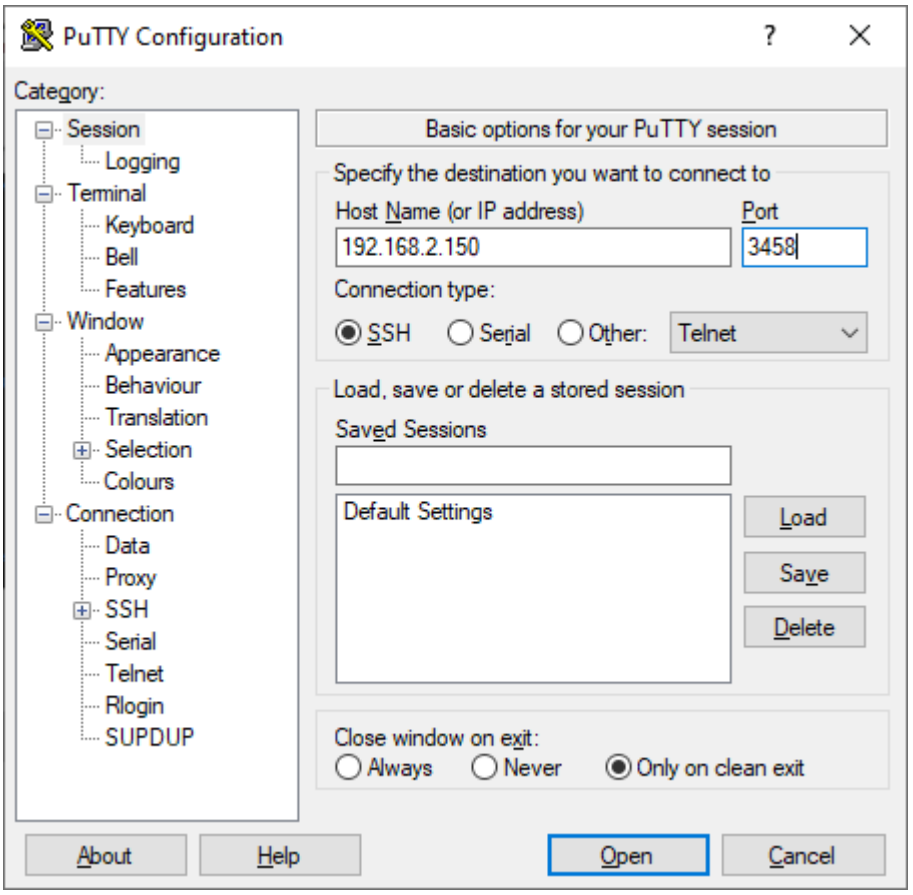
Escribir el comando “systemctl status iptables” para ver el estado del servicio, en el apartado “Active” debe decir “active” en color verde.



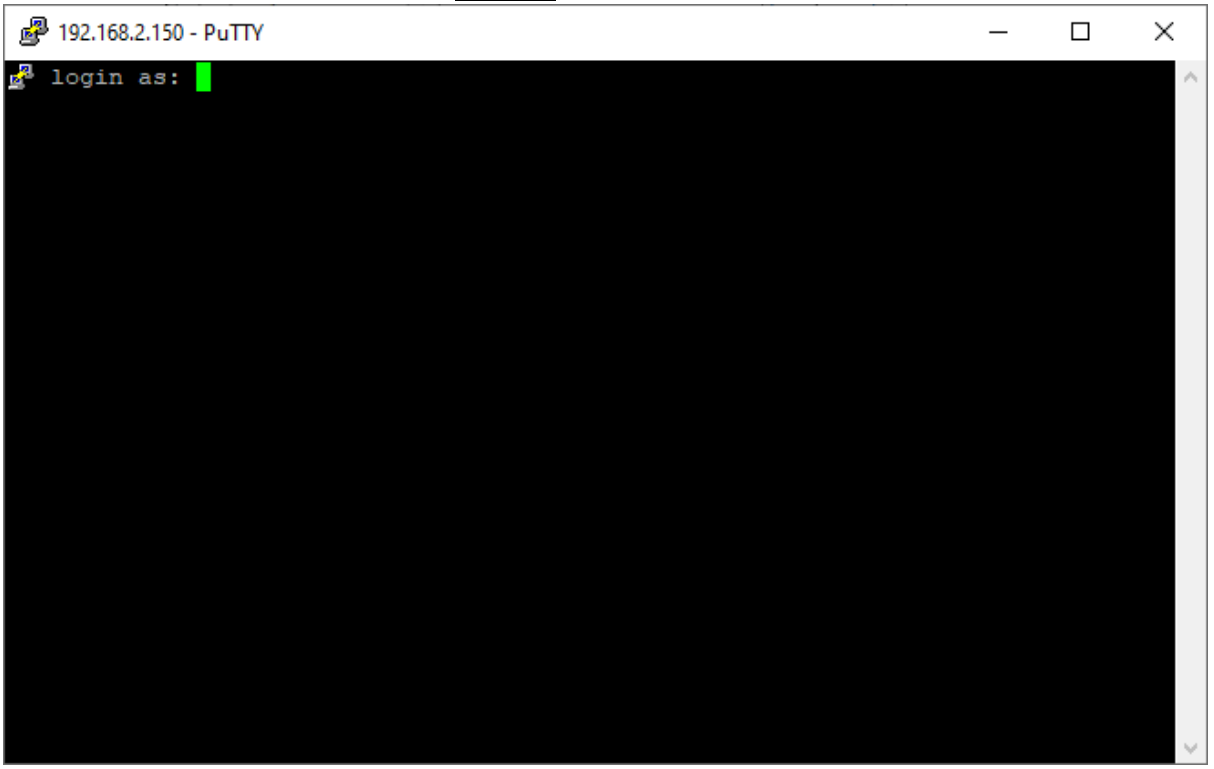
10. **Configuración del acceso remoto:** Escribir el comando “ifconfig” que nos mostrará diferentes datos de las distintas interfaces de red en el sistema. En este caso en los datos de la interfaz “enp0s3” se debe copiar la IP que aparece a continuación del campo “inet” que es 192.168.2.150 (o cualquier otra).



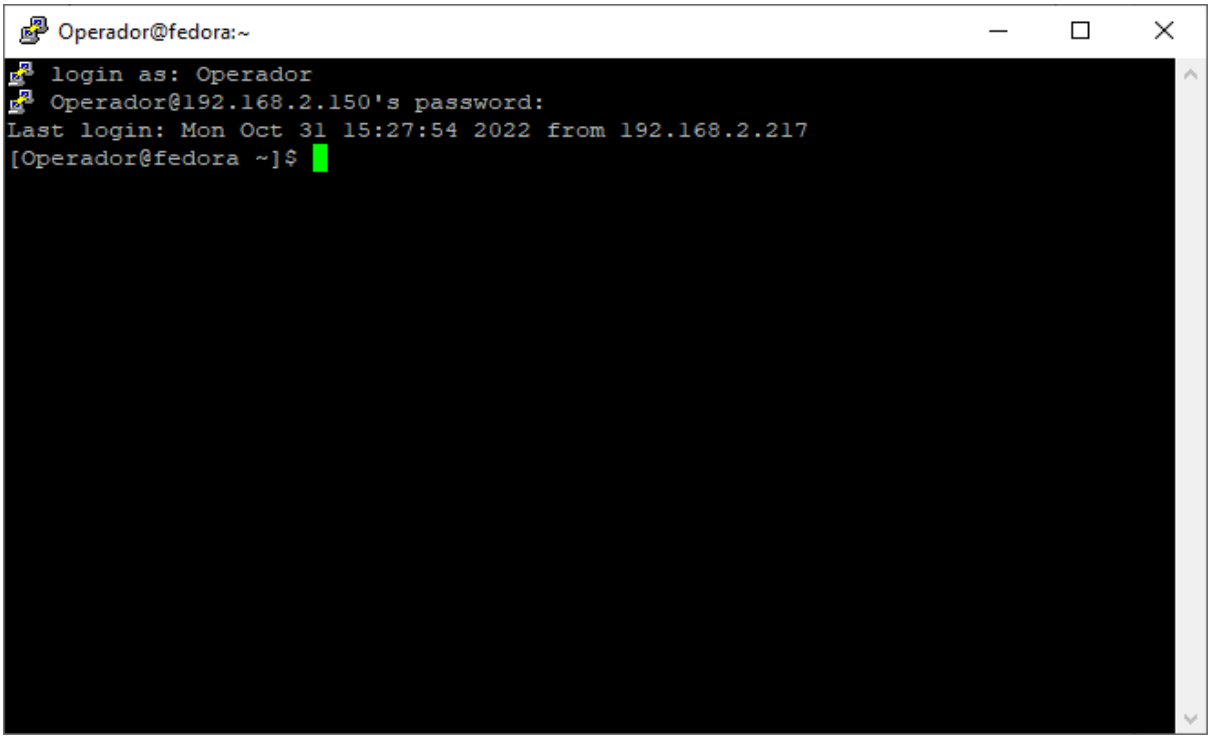
Desde el equipo con el que se piensa acceder remotamente, debemos instalar un cliente SSH, en este caso se descargó e instaló PuTTY, en el sistema Windows 10.



En el apartado “Category” de la izquierda, seleccionamos “Sessions”, en el campo “Host Name (or IP address)” ingresamos la IP antes copiada, en el campo “Port” ingresamos el puerto que establecimos para SSH y hacemos click en el botón “Open”.



En “login as” debemos ingresar el nombre de un usuario registrado en el sistema del servidor, a continuación su contraseña.



Con esto ya tenemos instalado y configurado el acceso remoto al sistema.

Instalación y Configuración de Firewall

1. **Instalación:** sudo dnf -y install Firewalld
2. **Inicialización del servicio:** sudo systemctl start firewalld

```
[root@fedora ProgWare_Server]# systemctl start firewalld
[root@fedora ProgWare_Server]#
```

3. **Comprobación de estado:** sudo firewalld-cmd --state

```
[root@fedora ProgWare_Server]# firewall-cmd --state
running
[root@fedora ProgWare_Server]#
```

4. **Visualización de la zona actual del sistema:**
   firewall-cmd --get-default-zone

```
[root@fedora ProgWare_Server]# firewall-cmd --get-default-zone
FedoraServer
[root@fedora ProgWare_Server]#
```

5. **Visualización de reglas asociadas a dicha zona:**
   firewall-cmd --list-all

```
[root@fedora ProgWare_Server]# firewall-cmd --list-all
FedoraServer (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpv6-client ssh
  ports:
  protocols:
  forward: no
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
[root@fedora ProgWare_Server]#
```

6. **Obtener zonas:** firewall-cmd --get-zones

```
[root@fedora ProgWare_Server]# firewall-cmd --get-zones
FedoraServer FedoraWorkstation block dmz drop external home internal nm-shared public trusted work
[root@fedora ProgWare_Server]#
```

7. **Establecer por defecto la zona interna:**
   firewall-cmd --set-default-zone=internal

```
[root@fedora ~]# firewall-cmd --set-default-zone=internal
success
[root@fedora ~]#
```

8. **Verificación de zona en la que está limitada la interfaz:**
   firewall-cmd --get-zone-of-interface=enp0s3

```
[root@fedora ~]# firewall-cmd --get-zone-of-interface=enp0s3
internal
[root@fedora ~]#
```

9. **Obtener tipos de icmp:**
   firewall-cmd --get-icmptypes

```
[root@fedora ~]# firewall-cmd --get-zone-of-interface=enp0s3
internal
[root@fedora ~]# firewall-cmd --get-icmptypes
address-unreachable bad-header beyond-scope communication-prohibited destination-unreachable echo-reply echo-request
 failed-policy fragmentation-needed host-precedence-violation host-prohibited host-redirect host-unknown host-unreac
hable ip-header-bad neighbour-advertisement neighbour-solicitation network-prohibited network-redirect network-unkno
wn network-unreachable no-route packet-too-big parameter-problem port-unreachable precedence-cutoff protocol-unreach
able redirect reject-route required-option-missing router-advertisement router-solicitation source-quench source-rou
te-failed time-exceeded timestamp-reply timestamp-request tos-host-redirect tos-host-unreachable tos-network-redirec
t tos-network-unreachable ttl-zero-during-reassembly ttl-zero-during-transit unknown-header-type unknown-option
[root@fedora ~]#
```

10. **Obtener servicios de Firewall:** firewall-cmd --get-services

```
[root@fedora ~]# firewall-cmd --get-services
RH-Satellite-6 RH-Satellite-6-capsule amanda-client amanda-k5-client amqp amqps apcupsd audit bacula bacula-client b
b bgp bitcoin bitcoin-rpc bitcoin-testnet bitcoin-testnet-rpc bittorrent-lsd ceph ceph-mon cfengine cockpit collectd
 condor-collector ctdb dhcp dhcpv6 dhcpv6-client distcc dns dns-over-tls docker-registry docker-swarm dropbox-lansyn
c elasticsearch etcd-client etcd-server finger foreman foreman-proxy freeipa-4 freeipa-ldap freeipa-ldaps freeipa-re
plication freeipa-trust ftp galera ganglia-client ganglia-master git grafana gre high-availability http https imap i
maps ipp ipp-client ipsec irc ircs iscsi-target isns jenkins kadmin kdeconnect kerberos kibana klogin kpasswd kprop
kshell kube-api kube-apiserver kube-control-plane kube-controller-manager kube-scheduler kubelet-worker ldap ldaps l
ibvirt libvirt-tls lightning-network llmnr managesieve matrix mdns memcache minidlna mongodb mosh mountd mqtt mqtt-t
ls ms-wbt mssql murmur mysql nbd netbios-ns nfs nfs3 nmea-0183 nrpe ntp nut openvpn ovirt-imageio ovirt-storageconso
le ovirt-vmconsole plex pmcd pmproxy pmwebapi pmwebapis pop3 pop3s postgresql privoxy prometheus proxy-dhcp ptp puls
eaudio puppetmaster quassel radius rdp redis redis-sentinel rpc-bind rquotad rsh rsyncd rtsp salt-master samba samba
-client samba-dc sane sip sips slp smtp smtp-submission smtps snmp snmptrap spideroak-lansync spotify-sync squid ssd
p ssh steam-streaming svdrp svn syncthing syncthing-gui synergy syslog syslog-tls telnet tentacle tftp tile38 tinc t
or-socks transmission-client upnp-client vdsm vnc-server wbem-http wbem-https wireguard wsman wsmans xdmcp xmpp-bosh
 xmpp-client xmpp-local xmpp-server zabbix-agent zabbix-server
[root@fedora ~]#
```

11. **Ver reglas de Iptables:**
    iptables -L
12. **Configuración para que el hardware rechace el acceso a internet de cualquier red:**
    iptables -A OUTPUT -o -eth0 -j DROP

13. **Configuración para que la red principal pueda tener acceso a internet:**
    iptables -A OUTPUT -s 192.168.1.3/24 -j DROP
14. **Configuración de firewall para permitir el servicio mysql:**
    # firewall-cmd --add-service=mysql
    # firewall-cmd --add-service=mysql --permanent
    # firewall-cmd --reload

Replicación de MySQL de Maestro a Esclavo

1. **Edite el archivo /etc/my.cnf.** Debajo de la sección [mysqld], agregue las siguientes cuatro líneas:

   log-bin
   server_id=1
   replicate-do-db=ProgWare
   bind-address=192.168.1.3
   Reiniciar el servicio: systemctl restart mariadb

2. **Iniciar sesión en el servidor MariaDB como root, crear el esclavo del usuario y asignar las subvenciones necesarias:**

   MariaDB [(none)]> CREATE USER 'slave'@'localhost' IDENTIFIED BY 'SlavePassword';
   MariaDB [(none)]> GRANT REPLICATION SLAVE ON *.* TO slave IDENTIFIED BY 'SlavePassword' WITH GRANT OPTION;
   MariaDB [(none)]> FLUSH PRIVILEGES;
   MariaDB [(none)]> FLUSH TABLES WITH READ LOCK;
   MariaDB [(none)]> SHOW MASTER STATUS;

3. **Configurar MySQL Master para la replicación:**
   Salga del indicador MariaDB (con exit;) y use el siguiente comando para tomar una instantánea de la base de datos de los empleados. Cuando presione enter se le pedirá que escriba la contraseña para la raíz que configuró anteriormente a través de mysql_secure_installation:
   # mysqldump -u root -p elmundo > elmundo-dump.sql

   Una vez completado el volcado, conéctese nuevamente al servidor de la base de datos para desbloquear las tablas y luego salga:

   MariaDB [(none)]> UNLOCK TABLES;
   MariaDB [(none)]> exit;

Anexos:

I. Comprar y mas Información sobre Windows 10 Pro: https://www.microsoft.com/es-es/d/windows-10-pro/df77x4d43rkt?activetab=pivot:informacióngeneraltab

II. Descargar Fedora 36 Server: https://getfedora.org/en/server/download/

Bibliografía

1. iptables(8)-Linux man page. Recuperado 27 de Julio de 2020, de https://linux.die.net/man/8/iptables

2. iptables (Español), (2019). Recuperado 27 de Julio de 2020, de https://wiki.archlinux.org/index.php/Iptables_(Espa%C3%Bol)

3. IPTABLES manual practico, tutorial de iptables con ejemplos. Recuperado 28 de Julio de 2020, de https://www.fing.edu.my/tecnoint/maldonado/cursos/admin/materiales/doc-iptables-firewall.pdf

4. sshd config-SSH Server Configuration. Recuperado 26 de Julio de 2020, de https://www.ssh.com/ssh/sshd_config/

5. semanage-port(8)-Linux manual page. Recuperado 26 de Julio de 2020, de https://man7.org/linux/man-pages/man8/semanage-port.8.html

6. SELinux. (2020). Recuperado 26 de Julio de 2020, de https://es.wikipedia.org/wiki/SELinux#:~:text=Security%2DEnhanced%20Linux%20(SELinux).de%20Defensa%20de%20Estados%20Unidos.

7. Configuración de red en la terminal y el servidor, de https://pc-solucion.es/linux/configurar-una-ip-estatica-en-ubuntu/

8. Scripts y crontabs, de 2da entrega de SO III de SOFTCOMM

9. Firewall y replicación de MySQL, extraído de https://www.linuxparty.es/89-basesdedatos/10507-como-configurar-la-replicacion-mariadb-maestro-esclavo-en-centos-rhel-y-debian.html https://www.solvetic.com/tutoriales/article/3467-firewall-centos-7-configurar-habilitar-deshabilitar-crear-reglas/

Hoja Testigo: