



ANEP



UTU

DIRECCIÓN GENERAL
DE EDUCACIÓN
TÉCNICO PROFESIONAL



Instituto Tecnológico Superior
UTU



—B—I—N—D—E—V—

Solicitante:

I.T.S. – Instituto Tecnológico Superior Arias - Balparda

Nombre de Fantasía del Proyecto: BINDEV

Grupo de Clase: 3° IF

Turno: Nocturno

Materia: Sistemas Operativos III

**Nombre de los Integrantes del Grupo: Alvarez Nicolas,
Armand-ugon Ignacio, Estefan German, Rivera Fabricio.**

Fecha de entrega: 25/ 07 /2020

Instituto Tecnológico Superior Arias Balparda

Gral. Flores 3591 esq. Bvar. José Batlle y Ordoñez - Montevideo



Objetivo

Definir y especificar todo lo necesario para poder llevar a cabo el correcto funcionamiento del servidor, específicamente, definir sistemas operativos a utilizar, perfiles de usuarios, roles, configuraciones, entre otras cosas.

Alcance

Este documento está realizado con el fin de dejar una documentación estructurada para futuras personas que quieran hacer uso de la misma.



Índice

1. Sistemas Operativos a utilizar	4
1.1 Terminales	4
1.1.1 Licencias RTL	5
1.1.2 Licencias OEM	5
1.1.3 Licencia a utilizar	5
1.2 Servidores	6
1.2.1 Licencia a utilizar	7
1.2.2 Uso de CentOS en el mercado	7
1.2.3 Comparación con otra distribución de Linux (Ubuntu)	9
2. Roles de los usuarios	11
2.1 Roles de usuario para el servidor	11
2.2 Roles de usuario para las terminales	11
2.3 Roles de usuarios externos al cliente (Usuarios web)	12
3. Script de gestion de usuarios	13
5. Configuración del cliente	21
5.1 Cuentas de usuario	21
5.2 Servicio SSH	21
5.3 Software de monitoreo	22
5.4 Antivirus	23
5.5 Políticas de respaldo	24
5.5.1 Menú de respaldos de la base de datos	24
5.5.1 Respaldo de logs	26
Auditorias	26
5.5.2 Configuración de Rsyslog lado del cliente	27
6. Configuración del servidor de respaldo	28
6.1. Cuentas de usuario	28
6.2. Configuración ssh	28
6.3. Antivirus	28
6.4. Configuración de los respaldos	28
7. Vocabulario y Simbología	30
8. Bibliografía	32

1. Sistemas Operativos a utilizar

A continuación se detallarán los sistemas operativos que utilizarán todas las terminales que comprenden el sistema en cuestión.

1.1 Terminales



Para la utilización del sistema tanto como para los clientes y el personal que lleve a cabo la gestión del mismo no hay ninguna limitación en lo que comprende el sistema operativo, ya que la aplicación se ejecuta en un navegador web el cual existe en cualquier sistema operativo. Pero, por una cuestión de intuitividad exhortamos el uso de Windows, ya que la curva de aprendizaje para los RHH que utilicen las terminales se va a ver reducida debido a que es el sistema operativo más cotidiano para los usuarios. Independiente de eso, utilizando la última versión de Windows garantizamos el soporte y actualizaciones durante varios años, a diferencia de las demás versiones, que dentro de poco tiempo irán quedando obsoletas en cuanto a soporte y actualizaciones de seguridad.

Sobre el licenciamiento, existen varias tipologías, pero básicamente, las podemos dividir en dos grupos.

**ANEP****UTU**DIRECCIÓN GENERAL
DE EDUCACIÓN
TÉCNICO PROFESIONALInstituto Tecnológico Superior
UTU

1.1.1 Licencias RTL

Son aquellas licencias que se compran directamente en una tienda oficial. Quien las compra es el propio usuario final a través de un portal de Microsoft o una tienda física. Estas licencias se pueden usar en un solo equipo.

1.1.2 Licencias OEM

Son aquellas que vienen incluidas en un ordenador al momento de la compra del mismo.

1.1.3 Licencia a utilizar

Vamos a adquirir licencias RTL teniendo en cuenta que el cliente ya cuenta con 3 terminales. El costo de cada licencia es de 17,49 euros por lo tanto serían 52,47 euros en total para cubrir el licenciamiento de las terminales del cliente. La versión de Windows a utilizar es Windows 11 Pro ya que con respecto a la Home la diferencia en costo es mínima, y nos ofrece más seguridad.

1.2 Servidores



CentOS

Para los servidores utilizaremos CentOS 7 de Linux (Versión terminal) debido a que es una limitación impuesta por el cliente que solicita el proyecto. Además, debemos destacar los beneficios que nos brinda la utilización de este sistema para los servidores, entre ellas son:

- Bajos requisitos de hardware para el correcto funcionamiento del mismo. Esto nos beneficia ya que para todas las tareas que va a tener que realizar el servidor como almacenar archivos, realizar lecturas y servir contenido (entre otras) no vamos a tener problema de rendimiento.
- CentOS es de código abierto, por lo tanto hay mucho soporte por parte de la comunidad para la resolución de conflictos futuros que se puedan llegar a presentar.
- Altamente confiable y estable.
- Licencia GPL
- Liviano
- Actualizaciones de seguridad repetidamente

Y muchos beneficios más que estaremos comentando en el documento.

1.2.1 Licencia a utilizar

Cuenta con licencia GPL lo cual nos permite la utilización del mismo sin la necesidad de abonar ninguna licencia, en efecto de reducir los gastos del proyecto.

Licencias GPL:

Es una licencia de derecho de autor ampliamente usada en el mundo del software libre y código abierto, garantiza a los usuarios finales (personas, organizaciones, compañías) la libertad de usar, estudiar, compartir (copiar) y modificar el software. Su propósito es doble: declarar que el software cubierto por esta licencia es libre, y protegerlo (mediante una práctica conocida como copyleft) de intentos de apropiación que restrinjan esas libertades a nuevos usuarios cada vez que la obra es distribuida, modificada o ampliada. Esta licencia fue creada originalmente por Richard Stallman fundador de la Free Software Foundation (FSF) para el proyecto GNU.

1.2.2 Uso de CentOS en el mercado

A continuación, este reporte muestra las estadísticas anuales del uso dado a las diferentes distribuciones de Linux desde enero del 2011 hasta el 2021. Como podemos apreciar tenemos a CentOS en tercer lugar como al más preferido por las empresas.

Historical yearly trends in the usage statistics of Linux subcategories for websites

This report shows the historical trends in the usage of Linux subcategories since January 2011.

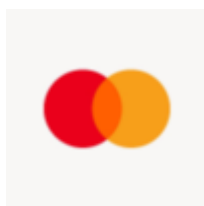
	2011 1 Jan	2012 1 Jan	2013 1 Jan	2014 1 Jan	2015 1 Jan	2016 1 Jan	2017 1 Jan	2018 1 Jan	2019 1 Jan	2020 1 Jan	2021 1 Jan	2022 1 Jan	2022 23 Jul
Ubuntu	11.9%	17.7%	22.0%	26.9%	24.5%	30.6%	34.9%	38.9%	38.1%	38.7%	48.1%	34.9%	33.7%
Debian	27.7%	29.4%	32.6%	32.8%	32.3%	32.5%	31.9%	30.7%	22.4%	19.4%	17.2%	15.5%	16.3%
CentOS	30.3%	29.3%	27.5%	25.1%	20.5%	20.3%	20.5%	20.6%	17.8%	16.9%	18.6%	9.9%	9.2%
Red Hat	15.7%	12.7%	9.8%	8.3%	4.7%	4.0%	3.5%	3.0%	2.3%	1.9%	1.8%	0.9%	0.8%
Gentoo	2.0%	1.2%	1.4%	2.4%	2.1%	2.6%	2.7%	2.7%	2.5%	1.8%	1.4%	0.6%	0.5%
Fedora	7.0%	5.2%	3.4%	2.4%	1.5%	1.2%	0.9%	0.7%	0.6%	0.4%	0.4%	0.2%	0.2%
SuSE	4.4%	3.1%	2.3%	1.5%	1.1%	1.0%	0.7%	0.6%	0.4%	0.3%	0.2%	0.1%	0.1%
Scientific Linux	<0.1%	0.1%	0.1%	0.1%	0.1%	0.1%	0.1%	0.1%	0.1%	0.1%	<0.1%	<0.1%	<0.1%
Turbolinux	0.1%	0.1%	0.1%	0.1%	0.1%	0.1%	0.1%	0.1%	<0.1%	<0.1%	<0.1%	<0.1%	<0.1%
CloudLinux		0.1%	0.1%	<0.1%	<0.1%	<0.1%	<0.1%	<0.1%	<0.1%	<0.1%		<0.1%	<0.1%
Mandriva	0.2%	0.1%	0.1%	0.1%	0.1%	0.1%	<0.1%	<0.1%	<0.1%	<0.1%	<0.1%	<0.1%	<0.1%

Estas son algunas de las empresas que reportaron el uso del mismo en varias charlas técnicas.

Booking.com



Ofrece servicios de reservas online, actuando como intermediarios entre los clientes que quieren reservar un alojamiento y el hotel, propiedad o alquiler temporal/vacacional. Este tipo de modelo de negocio también se conoce como modelo de agencia.



Mastercard

Es una multinacional de servicios financieros. Básicamente facilitan las transferencias electrónicas de fondos de todo el mundo, por lo general, a través de tarjetas de crédito, débito, etc.

ViaVarejo



Via Varejo S.A. es uno de los minoristas más grandes de Brasil, responsable de la gestión de las tiendas físicas y de comercio electrónico de grandes marcas como Casas Bahia, Pontofrio y Bartira.



Indeed.com

Es un motor de búsqueda de empleo concebido en los Estados Unidos en noviembre del 2004. Actualmente, Indeed se encuentra disponible en más de 50 países y en más de 28 idiomas.

1.2.3 Comparación con otra distribución de Linux (Ubuntu)

Al momento de elegir la mejor distribución de Linux para un servidor dedicado, en este caso, hay cientos de las mismas, pero a pesar de ello, hay dos distribuciones que se solicitan con mayor frecuencia : CentOS y Ubuntu.

Ubuntu:

Está basado en la arquitectura Debian, Ubuntu se usó desde un principio para P.C, pero se ha convertido familiar en entornos de cloud y servidores. Ubuntu se ejecuta en las arquitecturas más populares, incluidas como máquinas basadas en Intel, AMD y ARM.

Pros y contras:

Pros: Actualizaciones frecuentes, gran cantidad de funciones, vanguardia, fácil de usar para desarrolladores, estable, soporte durante cinco años para versiones principales.

Desventajas: Mayor consumo de recursos, menos seguridad desde el primer momento, requiere más soporte para mantenerse actualizado.



CentOS:

Una variante gratuita de Red Hat Enterprise Linux, CentOS es conocido por su estabilidad y soporte de su amplia comunidad. Esta distribución de Linux se ajusta a las necesidades de clase empresarial y brinda a los usuarios de TI una forma confiable de entregar sus aplicaciones y servicios.

Pros y contras:

Pros: Altamente confiable y estable para cargas de trabajo empresariales, una variante gratuita del muy confiable Red Hat Enterprise Linux (RHEL), cada versión principal sirve o hasta 10 años con actualizaciones de seguridad gratuitas durante 7-10 años, requiere menos soporte, liviano .

Contras : actualizaciones menos frecuentes, carece de riqueza de funciones en comparación con otros sistemas operativos.

Features	CentOS	Ubuntu
		
Package Command	RPM and YUM	APT-GET
Variant	Based on Red Hat Enterprise Linux (RHEL)	Based on Debian
Percentages of websites using (as per this site)	20.4%	34.8%
Release Cycle	Long period	Short period
Security	Secure out of the box	Less secure (out of the box) compare to CentOS
Download Link	Download CentOS	Download Ubuntu

En conclusión:

Ubuntu es una distribución con una gran cantidad de funciones y actualizaciones, lo cual lo hace poco performante hablando sobre los recursos, tenemos menos seguridad desde un principio y requiere mucho más soporte para mantenerse actualizado. En cambio, CentOS recibe las actualizaciones justas y necesarias para mantenerse al tanto de las nuevas vulnerabilidades y no sobrecargar tanto el sistema, además, tiene una comunidad enorme de desarrolladores dispuesta a brindar ayuda a cualquier situación y cuenta con licencia GPL.

2. Roles de los usuarios

A continuación definiremos los roles de usuarios que interactuaron con el sistema tanto como los recursos humanos del cliente y los clientes del cliente valga la redundancia.

2.1 Roles de usuario para el servidor

1. **Administrador:** Este rol de usuario tendrá la totalidad de los permisos dentro del servidor. Podrá gestionar usuarios, inicializar servicios, instalar dependencias, realizar configuraciones a nivel sistema entre otras muchas cosas más. Por motivos de seguridad, se decidió, no utilizar el usuario Root como administrador del sistema ya que es una vulnerabilidad en el mismo y estaríamos más expuestos a recibir ataques maliciosos como por ejemplo una escalada de privilegios.
2. **DBA(Database administrator):** Este rol tendrá total control sobre las bases de datos que impliquen al sistema realizado, así como los servicios que requieran las bases de datos y todo lo relacionado a ellas.
3. **Soporte:** Será el encargado de solucionar e investigar cualquier error inesperado o falla que surja en el servidor, así como mantener actualizado los paquetes y cuestiones de hardware.

2.2 Roles de usuario para las terminales

1. **Vendedores:** Es el encargado de gestionar los envíos de las compras confirmadas, una vez confirmada la misma, este usuario se encargará de gestionar el estado.
2. **Compradores:** El rol de este usuario va a ser de aprovisionamiento para la empresa, es decir, se va a encargar de verificar el stock disponible y contactar con los proveedores para realizar la compra a conciencia. Para luego dar de alta los productos al sistema.
3. **Jefe:** El jefe tendrá todos los permisos que tienen los usuarios mencionados anteriormente, y además podrá crear y eliminar R.H.H en la aplicación.



2.3 Roles de usuarios externos al cliente (Usuarios web)

- **Usuarios Web**

Se considera usuario web a cualquier tipo de navegante en el sitio que no esté claramente identificado como Cliente. Este rol de usuario únicamente podrá visualizar los productos que ofrece la empresa, pero no podría realizar compras hasta que se autentique como un cliente(empresa, particular)

- **Clientes Empresa**

Se considera cliente empresa al usuario claramente identificado en la base de datos con Documento RUT. Este rol de usuario podrá efectuar compras(Siempre y cuando haya stock) y visualizar todos los productos que ofrece la empresa.

- **Clientes Particulares**

Se considera cliente particular al usuario claramente identificado en la base de datos con Documento CI. Este rol podrá realizar compras y visualizar los productos que ofrece la empresa.



3. Script de gestion de usuarios

```
opt=0
while [ "$opt" != "10" ]
do
echo "Selecciona una opcion"
echo "-----"
echo "-----USUARIOS-----"
echo "-----"
echo "1- Agregar un usuario"
echo "2- Eliminar un usuario"
echo "3- Modificar un usuario"
echo "4- Listar usuarios"
echo "5- Verificar existencia de usuario"
echo "-----"
echo "-----GRUPOS-----"
echo "-----"
echo "6- Agregar un nuevo grupo"
echo "7- Eliminar un grupo"
echo "8- Modificar un grupo"
echo "9- Listar grupos"
echo "10- Salir"
read opt
case $opt in

    1)
        clear
        read -p "Nombre de usuario: " userName
        if [ -z "$userName" ]
        then
            clear
            echo "No se admiten valores vacios!"
            continue
        fi
        if [ $(cat /etc/passwd | cut -f1 -d':' | grep -c -w $userName)
!= 0 ]
        then
            clear
            echo "El usuario $userName ya existe"
```



```
        continue
    else
        clear
        sudo useradd $userName
        echo "Usuario $userName creado"
    fi
    read -p "¿Desea asignarle una contraseña? y | n " asignPasswd
    if [ $asignPasswd = "y" ]
    then
        clear
        sudo passwd $userName
        echo "Contraseña creada"
    elif [ $asignPasswd = "n" ]
    then
        clear
        continue
    else
        clear
        echo "Opcion incorrecta"
        continue
    fi
;;

2)
clear
read -p "Ingrese el nombre del usuario: " userName
if [ -z "$userName" ]
then
    echo "No se admiten valores vacios!"
    continue
fi
if [ $(cat /etc/passwd | cut -f1 -d':' | grep -c -w $userName)
!= 0 ]
then
    clear
    sudo deluser $userName
else
    clear
    echo "El usuario $userName no existe"
fi
;;
```



```
3)
clear
read -p "Nombre de usuario a modificar: " userName
if [ -z "$userName" ]
then
echo "No se admiten valores vacios!"
continue
fi
if [ $(cat /etc/passwd | cut -f1 -d':' | grep -c -w $userName)
!= 0 ]
then
while [ "$opt" != "z" ]
do
echo "Seleccione una opcion"
echo "A- Bloquear contraseña de $userName"
echo "B- Desbloquear contraseña de $userName"
echo "C- Modificar contraseña de $userName"
echo "D- Agregar $userName a un grupo"
echo "E- Eliminar $userName de un grupo"
echo "Z- Volver"
read opt
case $opt in
a)
clear
sudo usermod -L $userName
echo "Contraseña bloqueada correctamente: "
sudo cat /etc/shadow | grep -w $userName
;;
b)
clear
sudo usermod -U $userName
echo "Contraseña desbloqueada correctamente: "
sudo cat /etc/shadow | grep -w $userName
;;
c)
clear
sudo passwd $userName
;;
d)
clear
```



```
read -p "Ingrese nombre de grupo: " groupName
if [ -z "$groupName" ]
then
echo "No se admiten valores vacios!"
continue
fi
if [ $(cat /etc/group | cut -f1 -d':' | grep -c -w
$groupName) != 0 ]
then
sudo usermod -a -G $groupName $userName
echo "Usuario $userName agregado al grupo
$groupName"

sudo cat /etc/group | grep -w $groupName
else
echo "El grupo no existe"
fi
;;
e)
clear
read -p "Ingrese nombre de grupo: " groupName
if [ -z "$groupName" ]
then
echo "No se admiten valores vacios!"
continue
fi
if [ $(cat /etc/group | cut -f1 -d':' | grep -c -w
$groupName) != 0 ]
then
sudo gpasswd -d $userName $groupName
echo "Usuario $userName eliminado de $groupName
correctamente"

sudo cat /etc/group | grep -w $groupName
else
echo "El grupo no existe"
fi
;;
z)
clear
opt=z
;;
*)
```




```
clear
echo "Opcion invalida"
;;
esac
done
else
echo "El Usuario $userName no existe"
continue
fi
;;

4)
clear
sudo cat /etc/passwd | cut -f1 -d':'
sleep 2
;;

5)
clear
read -p "Nombre del usuario: " userName
if [ -z "$userName" ]
then
echo "No se admiten valores vacios!"
continue
fi
if [ $(cat /etc/passwd | cut -f1 -d':' | grep -c -w $userName)
!= 0 ]
then
echo "El usuario $userName existe"
else
echo "El usuario $userName no existe"
fi
;;

6)
clear
read -p "Ingrese el nombre del grupo: " groupName
if [ -z "$groupName" ]
then
echo "No se admiten valores vacios!"
continue
```



```
fi
    if [ $(cat /etc/group | cut -f1 -d':' | grep -c -w $groupName)
!= 0 ]
then
    echo "El grupo $groupName ya existe"
else
    sudo groupadd $groupName
    echo "Grupo $groupName creado"
    sudo cat /etc/group | grep -w $groupName
fi
;;

7)
clear
read -p "Ingrese nombre del grupo: " groupName
if [ -z "$groupName" ]
then
    echo "No se admiten valores vacios!"
    continue
fi
    if [ $(cat /etc/group | cut -f1 -d':' | grep -c -w $groupName)
!= 0 ]
then
    sudo delgroup $groupName
    echo "El grupo $groupName fue eliminado correctamente"
else
    echo "El grupo $groupName no existe"
fi
;;

8)
clear
read -p "Ingrese nombre de grupo: " groupName
if [ -z "$groupName" ]
then
    echo "No se admiten valores vacios!"
    continue
fi
    if [ $(cat /etc/group | cut -f1 -d':' | grep -c -w $groupName)
!= 0 ]
then
```



```
while [ "$opt" != "z" ]
do
clear
echo "Seleccione una opcion"
echo "A - Cambiar GID del grupo $groupName"
echo "B - Cambiar nombre del grupo $groupName"
echo "Z- Volver"
read opt
case $opt in
a)
clear
read -p "Ingrese el nuevo GID del grupo " gid
if [ -z "$gid" ]
then
echo "No se admiten valores vacios"
sleep 2
continue
fi
re='^[0-9]+$'
if ! [[ $gid =~ $re ]] ; then
echo "Solo se admiten valores numericos"
sleep 2
continue
fi
if [ $(cat /etc/group | cut -f3 -d':' | grep -c -w
$gid) != 0 ]
then
echo "El GID $gid ya se encuentra en uso"
sleep 2
continue
fi
sudo groupmod -g $gid $groupName
echo "El GID se cambio con exito"
sudo cat /etc/group | grep -w $groupName
sleep 3
;;
b)
read -p "Ingrese el nuevo nombre " newName
if [ -z "$newName" ]
then
echo "No se admiten valores vacios"
```



```
        sleep 2
        continue
    fi
    sudo groupmod -n $newName $groupName
    echo "Nombre de grupo cambiado con exito"
    sleep 2
    ;;
    z)
    clear
    opt=z
    ;;
    *)
    echo "Opcion invalida"
    ;;
esac
done
else
    echo "El grupo no existe"
fi
;;
9)
clear
sudo cat /etc/group | cut -f1 -d':'
sleep 2
;;

10)
clear
exit
;;

*)
clear
echo "Opcion incorrecta"
;;

esac

done
```

5. Configuración del cliente

5.1 Cuentas de usuario

Se creará la cuenta “**master**” como usuario administrador del sistema. Al mismo se le darán permisos de super usuario para que este sea capaz de instalar/actualizar/desinstalar dependencias, paquetes y servicios, también administrar nuevos usuarios de ser requerido.

Dentro de la carpeta /home/master/ se crearán las carpetas de Scripts para todos los scripts que se usen en el proyecto. Además se creará una carpeta de respaldos para los respaldos temporales que se realicen cuando se hace una exportación de la base de datos.

Además se creará una cuenta de usuario para el servicio de monitoreo, llamada “**prometheus**”, la cual tendrá en su /home/ el software de monitoreo instalado así como los agregados de Node Exporter.

5.2 Servicio SSH

Configuración:

- Allow root remote login: no
- port: 2244

```
GNU nano 2.3.1          Fichero: /etc/ssh/sshd_config
# $OpenBSD: sshd_config,v 1.100 2016/08/15 12:32:04 naddy Exp $
# This is the sshd server system-wide configuration file. See
# sshd_config(5) for more information.
# This sshd was compiled with PATH=/usr/local/bin:/usr/bin
# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.
# If you want to change the port on a SELinux system, you have to tell
# SELinux about this change.
# semanage port -a -t ssh_port_t -p tcp #PORTNUMBER
#
Port 2244
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
```

```
GNU nano 2.3.1          Fichero: /etc/ssh/sshd_config

#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_dsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
SyslogFacility AUTHPRIV
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
```

Para crear la conexión usamos la dirección ip del servidor de respaldos por defecto: respaldo@192.168.1.2

5.3 Software de monitoreo



Prometheus

Utilizaremos Prometheus como software de monitoreo para nuestro sistema, el mismo es un software de monitorización y alertas de código abierto, está programado en Go y fue desarrollado en el año 2012. Estaremos utilizando también la herramienta “node exporter” para poder ver métricas de los nodos del sistema.



Además agregamos Grafana el cual es también un software de código abierto y escrito en Go. Gracias a Grafana podemos ver los paneles de monitoreo de una manera más fácil de leer y también tiene la característica de poder crear paneles personalizados de monitoreo utilizando Prometheus.

5.4 Antivirus



Utilizaremos el antivirus ClamAV el cual puede identificar y bloquear el malware proveniente del correo electrónico. Una de las características principales en este tipo de software es la rápida localización e inclusión en su base de nuevos virus encontrados y escaneados. Esto se logra gracias a la colaboración de los miles de usuarios que usan ClamAv y a múltiples sitios que proporcionan registros de virus escaneados.

5.5 Políticas de respaldo

5.5.1 Menú de respaldos de la base de datos

```
#!/bin/bash

#variables
DATABASE="bindev"
USER="master"
PASSWORD="1234"
RESPALDOS="/home/master/respaldos"
SERVIDOR="respaldo@192.168.1.2:/home/respaldo/respaldos"
logger -p local1.info "Ingreso al menu de respaldos de la Base de datos"

#Menu principal
opt=1
while [ "$opt" != 0 ]
do
    echo "Bienvenido al sistema de respaldos de la base de datos"
    echo "Para continuar elija una opcion"
    echo "-----"
    echo "1) Crear un respaldo de la Base de datos"
    echo "2) Importar respaldo a la Base de datos"
    echo "3) ver el estado del servicio mariaDB"
    echo "4) Probar conexion al servidor de respaldos"
    echo "0) Salir"
    read opt
    case $opt in
        1)
            clear
            logger -p local1.info "Comenzo intento de realizar un respaldo de la BD"
            echo "Base de datos: "$DATABASE
            echo "-----"
            mysqldump -u $USER -p$PASSWORD $DATABASE > $RESPALDOS/$DATABASE".sql"
            if [ $? -eq 0 ]
            then
                logger -p local1.info "Se ha exportado la DB con exito"
                tar -zcvf ./"${date +%d-%m-%y}"_hora_${date +%R'}_respaldo.tar.gz" $RESPALDOS/$DATABASE".sql"
                if [ $? -eq 0 ]
                then
                    mysqldump -u $USER -p$PASSWORD $DATABASE > $RESPALDOS/$DATABASE".sql"
                    if [ $? -eq 0 ]
                    then
                        logger -p local1.info "Se ha llevado a cabo la compresion del archivo"
                        mv $(find . -name "*.tar.gz") $RESPALDOS
                        rm $RESPALDOS/$DATABASE".sql"
                        rsync --remove-source-files -avhzP -e "ssh -p 2244" $RESPALDOS/ $SERVIDOR
                        if [ $? -eq 0 ]
                        then
                            echo "Respaldo completado..."
                            logger -p local1.info "Respaldo de la base de datos creado"
                            sleep 2s
                        else
                            echo "##### Algo salio MUY mal #####"
                            echo "No se completo el respaldo"
                            logger -p local1.info "No se pudo completar el respaldo. Sucedio un fallo en la conexion hacia el servidor"
                            sleep 2s
                        fi
                    else
                        echo "Fallo en la compresion"
                        logger -p local1.info "Fallo en la compresion"
                    fi
                else
                    echo "Error al exportar desde la base de datos"
                    logger -p local1.info "No se pudo hacer el respaldo, sucedio un error en la BD"
                fi
            fi
        ;;
```




```
;;
2)
clear
echo "Importando ultimo registro disponible..."
resp=$(rsync -avhz --dry-run -e "ssh -p 2244" $SERVIDOR $RESPALDOS | grep respaldo.tar.gz | tail -1 | cut -f2 -d"/")
echo "Ultimo registro disponible -> "$resp
sleep 1s
rsync -avhZP --include=${resp} --exclude '*' -e "ssh -p 2244" $SERVIDOR/ $RESPALDOS
if [ $? -eq 0 ]
then
    echo "Respaldo importado desde el servidor.."
    logger -p local1.info "Respaldo $resp importado desde el servidor"
    sleep 1s
    tar -zxvf $RESPALDOS/$resp -C $RESPALDOS/
    if [ $? -eq 0 ]
    then
        echo "Descomprimiendo archivos..."
        logger -p local1.info "Descomprimiendo archivos para importar a la base de datos, $resp"
        ls $RESPALDOS
        echo "Importando a la base de datos.."
        mysql -u $USER -p$PASSWORD $DATABASE < $RESPALDOS/home/master/respaldos/$DATABASE.sql
        if [ $? -eq 0 ]
        then
            rm -r $RESPALDOS/*
            echo "Exit!"
            logger -p local1.info "Respaldo importado desde el servidor"
            echo "#####"
        else
            "Ocurrio un error al importar el respaldo a la BD"
            logger -p local1.info "Error al importar hacia la BD"
        fi
    else
        echo "No se pudo descomprimir el archivo"
        logger -p local1.info "No se pudo descomprimir el archivo"
    fi
fi
else
    else
        echo "No se pudo descomprimir el archivo"
        logger -p local1.info "No se pudo descomprimir el archivo"
    fi
else
    echo "Algo salio mal al importar desde el servidor"
    logger -p local1.info "Ocurrio un error al importar el respaldo desde el servidor externo"
fi
;;
3)
systemctl status mariadb | grep active
logger -p local1.info "Info del estado del servicio mariadb"
sleep 2s
clear
;;
4)
clear
echo "Sincronizando con el servidor de respaldo"
echo "-----"
rsync -ahzP --dry-run -e "ssh -p 2244" $SERVIDOR $RESPALDOS | grep respaldo.tar.gz
if [ $? -eq 0 ]
then
    sleep 1s
    echo "#####"
    echo "Conexion establecida con exito, Presione enter para volver al menu principal"
    logger -p local1.info "Probando conexion al servidor de respaldo, EXITO"
    read cosa
    clear
else
    sleep 1s
    echo "#####"
    echo "El servidor esta OFFLINE o no se puede acceder al mismo, Presione enter para volver al menu principal"
    logger -p local1.info "Probando conexion al servidor de respaldos, No se puede conectar con el servidor"
    read cosa
    clear
fi
```

```
0)
echo "Bye"
logger -p local1.info "Salida del menu de respaldos de la base de datos"
;;
*)
clear
echo "Opcion invalida"
;;
esac
done
```

5.5.1 Respaldo de logs

- Configuraciones, usuarios, grupos, paquetes instalados, actualizaciones

```
GNU nano 2.3.1          Fichero: Scripts/config_logs.sh

#!/bin/bash

#archivos de configuracion
cat /etc/my.cnf > /var/log/customlogs/mariadb.config.log
cat /etc/httpd/conf/httpd.conf > /var/log/customlogs/apache.config.log
cat /etc/rsyslog.conf > /var/log/customlogs/rsyslog.conf.log
cat /etc/php.ini > /var/log/customlogs/php.conf.log
cat /etc/rsyncd.conf > /var/log/customlogs/rsync.conf.log

#paquetes instalados
rpm -qa > /var/log/customlogs/paquetesInstalados.log

#actualizaciones
yum history > /var/log/customlogs/yumHistorial.log

#usuarios y grupos
cat /etc/passwd > /var/log/customlogs/usuarios.log
cat /etc/group > /var/log/customlogs/grupos.log
```

- Auditorias

```
#!/bin/bash

"${last}" > /var/log/customlogs/last.log
"${lastlog | grep -v "Nunca ha accedido"}" > /var/log/customlogs/last_log.log
```

- Logs de Servicios (systemd)

```
GNU nano 2.3.1          Fichero: Scripts/systemdLogs.sh
#!/bin/bash
journalctl -o cat -u httpd > /var/log/customlogs/apacheSystemDLogs.log
journalctl -o cat -u mariadb > /var/log/customlogs/MariadbSystemDLogs.log
journalctl -o cat -u prometheus.service > /var/log/customlogs/PromethuesSystemDLogs.log
journalctl -o cat -u grafana-server > /var/log/customlogs/GrafanaSystemDLogs.log
journalctl -o cat -u clamd@scan > /var/log/customlogs/clamdSystemDLogs.log
```

5.5.2 Configuración de Rsyslog lado del cliente

```
# Save news errors of level crit and higher in a special file.
uucp,news.crit                               /var/log/spooler

# Save boot messages also to boot.log
local7.*                                     /var/log/boot.log
local11.info                                /var/log/customlogs/menu_backup.log

### begin forwarding rule ###
# The statement between the begin ... end define a SINGLE forwarding
# rule. They belong together, do NOT split them. If you create multiple
# forwarding rules, duplicate the whole block!
# Remote Logging (we use TCP for reliable delivery)
#
# An on-disk queue is created for this action. If the remote host is
# down, messages are spooled to disk and sent when it is up again.
#$ActionQueueFileName fwdRule1 # unique name prefix for spool files
#$ActionQueueMaxDiskSpace 1g    # 1gb space limit (use as much as possible)
#$ActionQueueSaveOnShutdown on  # save messages to disk on shutdown
#$ActionQueueType LinkedList    # run asynchronously
#$ActionResumeRetryCount -1     # infinite retries if host is down
# remote host is: name/ip:port, e.g. 192.168.0.1:514, port optional
*. * @192.168.1.2:514
### end of the forwarding rule ###
```

6. Configuración del servidor de respaldo

6.1. Cuentas de usuario

En el servidor de respaldo tendremos el usuario “respaldo” actuando como el administrador del sistema.

6.2. Configuración ssh

Configurado en el puerto 2244, y con el root remoto desactivado.

6.3. Antivirus

Se utilizará el mismo antivirus que en el cliente.

6.4. Configuración de los respaldos

Los respaldos de la base de datos se encuentran en la carpeta respaldos, en el home del usuario “respaldo”. /home/respaldo/respaldos.

Los Logs de la máquina cliente se encuentran en la carpeta /var/log/remote/

Los respaldos están configurados para ser llevados 1 vez al día a las 23:00 horas. Los logs de usuarios logueados (last, lastlog) están configurados para ser ejecutados cada 20 minutos.

Configuración de Rsyslog lado del servidor

- puertos

```
# Provides UDP syslog reception
$ModLoad imudp
$UDPServerRun 514

# Provides TCP syslog reception
$ModLoad imtcp
$InputTCPServerRun 514
```

- Template de los logs remotos

```
#### GLOBAL DIRECTIVES ####

# Where to place auxiliary files
$WorkDirectory /var/lib/rsyslog

# Use default timestamp format
$ActionFileDefaultTemplate RSYSLOG_TraditionalFileFormat

$template Remotelogs, "/var/log/remote/%HOSTNAME%/%PROGRAMNAME%.log"

# File syncing capability is disabled by default. This feature is usually not required,
# not useful and an extreme performance hit
#$ActionFileEnableSync on

# Include all config files in /etc/rsyslog.d/
$IncludeConfig /etc/rsyslog.d/*.conf

# Turn off message reception via local log socket;
# local messages are retrieved through imjournal now.
$OmitLocalLogging on

# File to store the position in the journal
$IMJournalStateFile imjournal.state
```

- Todos los logs se guardan en el template de los logs remotos

```
#### RULES ####

# Log all kernel messages to the console.
# Logging much else clutters up the screen.
kern.*                                          /dev/console

# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
*.info;mail.none;authpriv.none;cron.none    /var/log/messages

# The authpriv file has restricted access.
authpriv.*                                   /var/log/secure

# Log all the mail messages in one place.
mail.*                                        -/var/log/maillog

# Log cron stuff
cron.*                                       /var/log/cron

# Everybody gets emergency messages
*.emerg                                       :omusrmsg:*

# Save news errors of level crit and higher in a special file.
uucp,news.crit                              /var/log/spooler

# Save boot messages also to boot.log
local7.*                                     /var/log/boot.log
local11.info                                /var/log/BACKUPLOGS/DBbackup.log

*,*                                          ?Remotelogs
```


7. Vocabulario y Simbología

OEM

Las siglas OEM vienen de Original Equipment Manufacturer, que significa Fabricante de Equipo Original.

CentOS

CentOS (Community ENTERprise Operating System) es una distribución Linux que consiste en una bifurcación a nivel binario de la distribución GNU/Linux Red Hat Enterprise Linux RHEL, compilado por voluntarios a partir del código fuente publicado por Red Hat, siendo la principal diferencia con este la eliminación de todas las referencias a las marcas y logos propiedad de Red Hat.

Linux

Linux es un sistema operativo (o una familia de sistemas operativos) tipo Unix compuesto por software libre y de código abierto.¹ GNU/Linux surge de las contribuciones de varios proyectos de software, entre los cuales destacan GNU (iniciado por Richard Stallman en 1983) y el kernel «Linux» (iniciado por Linus Torvalds en 1991).

Sistemas Operativos

Un sistema operativo (SO) es el conjunto de programas de un sistema informático que gestiona los recursos de hardware y provee servicios a los programas de aplicación de software. Estos programas se ejecutan en modo privilegiado respecto de los restantes.

Terminales

En informática, se denomina terminal o consola (hardware) a un dispositivo electrónico o electromecánico que se utiliza para interactuar con un computador.

GPL

La Licencia Pública General de GNU o más conocida por su nombre en inglés GNU General Public License es una licencia de derecho de autor ampliamente usada en el mundo del software libre y código abierto, y garantiza a los usuarios finales la libertad de usar, estudiar, compartir y modificar el software

P.C

Una computadora personal, computador personal u ordenador, conocida como PC (siglas en inglés de Personal Computer), es un tipo de microcomputadora diseñada en principio para ser utilizada por una sola persona.

INTEL

Intel Corporation es el mayor fabricante de circuitos integrados del mundo según su cifra de negocio anual. La compañía estadounidense es la creadora de la serie de procesadores x86, los procesadores más comúnmente encontrados en la mayoría de las computadoras personales. Intel fue fundada el 18 de julio de 1968 como Integrated Electronics Corporation (aunque un error común es el de que "Intel" viene de la palabra intelligence) por los pioneros en semiconductores Robert Noyce y Gordon Moore, y muchas veces asociados con la dirección ejecutiva y la visión de Andrew Grove.

AMD

(AMD) es una compañía estadounidense de semiconductores con sede en Santa Clara, California, que desarrolla procesadores de computación y productos tecnológicos similares de consumo.

Script

En informática, un script, secuencia de comandos o guión (traduciendo desde inglés) es un término informal que se usa para designar a un programa relativamente simple. Los scripts regularmente no se compilan con anticipación a código máquina, sino que son ejecutados por un intérprete que lee el archivo de código fuente al momento; o incluso por una consola interactiva donde el usuario suministra el programa al intérprete paso a paso.

Rsync

Rsync, que significa “sincronización remota”, es una herramienta de sincronización de archivos remotos y locales. Utiliza un algoritmo que minimiza la cantidad de datos copiados, moviendo solo las partes de los archivos que cambiaron.

Rsyslog

Rsyslog es una utilidad englobada dentro de la filosofía de desarrollo de código abierto y que utiliza una licencia de software libre. Es muy utilizada en sistemas UNIX y similares, como GNU/Linux. Esta se encarga de reenviar mensajes de registro dentro de una red.

Prometheus

Un sistema de recolección métrica de aplicaciones y servicios para el almacenamiento en un banco de datos de serie temporal resultando muy eficiente.

Clamav

Es un antivirus open source para detectar troyanos, virus, malware y otras amenazas.



ANEP



UTU

DIRECCIÓN GENERAL
DE EDUCACIÓN
TÉCNICO PROFESIONAL



Instituto Tecnológico Superior
UTU

8. Bibliografía

https://w3techs.com/technologies/history_details/os-linux

<https://stackshare.io/centos>

<https://www.inap.com/blog/centos-vs-ubuntu-linux-server/>

<https://www.softzone.es/windows/como-se-hace/diferencias-licencias-oem-retail-volumen/>

<https://www.digitalocean.com/community/tutorials/how-to-use-rsync-to-sync-local-and-remote-directories-es>

<https://www.ochobitshacenunbyte.com/2018/10/29/registros-centralizados-en-linux-con-rsyslog/>

<https://es.sensedia.com/post/monitoring-with-prometheus-grafana-alertmanager-and-victoriametrics>

<https://github.com/Cisco-Talos/clamav>

