



Enigma Engineers

Solicitante:

I.T.S. – Instituto Tecnológico Superior Arias - Balparda
Nombre de Fantasía del Proyecto: Enigma Engineers

Grupo de Clase: 3°BR

Turno: Nocturno

Materia: Sistemas Operativos III

Nombre de los Integrantes del Grupo:

Dominguez Maximiliano, Hernandez Leandro, Labora Mathias, Schiavoni Lucio

Fecha de entrega: 11/09/2023



ANEP



UTU

DIRECCIÓN GENERAL
DE EDUCACIÓN
TÉCNICO PROFESIONAL



Instituto Tecnológico Superior
UTU

Objetivo

El objetivo principal de este documento es proporcionar una guía clara y concisa para el desarrollo de un proyecto de una página web utilizando un sistema operativo versión Server, establecer los lineamientos y las mejores prácticas para el equipo de desarrollo, con el fin de asegurar la estabilidad, seguridad y eficiencia del sistema operativo en el entorno de desarrollo y producción y asegurar la compatibilidad adecuada entre el sistema operativo y las tecnologías utilizadas.

Alcance

El documento abarca todas las etapas del proyecto referidas a el Sistema operativo, desde la instalación y configuración inicial del sistema operativo, su elección y fundamentación, hasta la puesta en producción y el soporte. También incluirá la selección y configuración de las herramientas y tecnologías necesarias para el desarrollo de la página, tales como servicios, programas, bases de datos entre otros.

Índice

1. Argumentación Técnica sobre la elección del sistema operativo para las terminales de la red.....	5
1.1 Licenciamiento a utilizar.....	5
1.2 Soporte.....	7
1.3 Beneficios.....	7
2 Argumentación Técnica sobre la elección del sistema operativo para los servidores de la red.....	8
2.1 Licenciamiento.....	9
2.3 Soporte.....	10
3 Roles de usuarios que utilizarán el servidor y las terminales.....	11
3.1 Terminales:.....	11
3.2 Servidor.....	12
4 Configuraciones básicas en los sistemas operativos de los servidores, y de las terminales (hostname, red, etc.).....	13
4.1 Cambio de Hostname.....	13
4.2 Configuración SSH.....	14
4.3 Configuración clave pública-privada.....	15
4.5 Instalación php 8.2:.....	16
4.6 Instalación de W11 para las terminales:.....	18
5 Configuraciones de las cuentas y su perfilamiento a través de privilegios y restricciones Cuentas por perfil.....	27
5.1 Creación de los Roles(grupos) de usuarios:.....	27
5.2 Configuración SUDOERS.....	28
6 Licenciamiento, soporte, instalaciones y configuraciones.....	29
6.1 Servidor de base de datos MySQL(MariaDB).....	29
6.1.1 Licenciamiento.....	29
6.1.2 Soporte:.....	31
6.1.3 Instalación y configuración.....	33
6.2 Software de monitoreo.....	37
6.2.1 Licenciamiento grafana:.....	37
6.2.2 Soporte grafana:.....	38
6.2.3 Instalación grafana:.....	40
6.3 Antivirus ClamAV.....	47
6.3.1 Soporte.....	48
6.3.2 Licenciamiento.....	49
6.3.3 Instalación.....	50

7 Procedimientos de respaldo y recuperación de datos.....	58
Bibliografía.....	62

1. Argumentación Técnica sobre la elección del sistema operativo para las terminales de la red

Para las terminales de red decidimos que se va a utilizar el sistema operativo, Windows 11, ya que el mismo cuenta con ciertas ventajas a la hora de comenzar a utilizarlo, mantenerlo y personalizarlo. También cuenta con un abanico de aplicaciones adaptadas a Windows, que funcionan con fluidez, y utilizando eficientemente los recursos del sistema. Esto conlleva también a una puerta a la entrada de malwares, virus, ataques DDoS, etc por eso la utilización de Windows 11 frente al antecesor (Windows 10) nos brinda mayor seguridad con protecciones contra la suplantación de identidad (phishing), seguridad sin contraseña y control de apps. Además los clientes de Windows 11 indican una reducción de hasta un 58 % en incidentes de seguridad, así como 2,8 veces menos instancias de robo de identidad.

1.1 Licenciamiento a utilizar

La licencia que se utilizará por parte de los terminales de red, es Windows 11 Enterprise E3.

La misma incluye características de seguridad avanzadas, herramientas de administración y actualizaciones regulares de seguridad. Además, ofrece compatibilidad con aplicaciones heredadas y mejoras en la productividad.

E3 Ofrece lo que Windows 11 Pro nos brinda y a demás agrega:

- Una amplia gama de opciones para la implementación del sistema operativo y el control de actualizaciones
- Gestión integral de dispositivos y aplicaciones.
- Gestión de impresión sin servidor con Universal Print.
- Protección avanzada contra amenazas de seguridad modernas.

-Actualizaciones automáticas de Windows y Office 365 con Windows Autopatch.

La decisión por licencias E3 para ofrecerle al cliente, surge por la poca distancia económica entre E3 y W11 pro y también las ventajas que ofrece W11 E3 entre las que integra el Soporte.

Solicitamos una cotización para 4 licencias W11 pro, y W11 E3.

La cotización de precios fue hecha por el Partner:
Prisma Soluciones Tecnológicas.



1. Audiencia y confidencialidad

Se define como audiencia del presente proyecto al personal de **Enigma** que el equipo de trabajo considere necesario, a los usuarios internos de los servicios desplegados en la presente solución y al personal de Prisma Soluciones Tecnológicas o de socios de negocios que participan del proyecto.

Los materiales contenidos en este documento representan información propietaria de **Enigma** y Prisma Soluciones Tecnológicas. Incluye información que no debe ser discutida fuera de **Enigma** y no debe ser duplicada, usada, o discutida por ningún propósito más que el del presente proceso de implementación. Se asume un compromiso bilateral en honrar la discrecionalidad de la información.

2. Objetivo

A partir de las necesidades planteadas por el cliente y posterior análisis por parte de Prisma, se brindará una propuesta económica para Licencias Microsoft.

3. Propuesta comercial

Cantidad	SKU	Descripción	P.U.	Subtotal
4	DG7GMGF0L4TL	Windows GGWA - Windows 11 Pro - Legalization Get Genuine - Perpetuo	\$222,25	\$222,25
4	CFQ7TTC0LGTX	Windows 10/11 Enterprise E3 - Anual	\$83,10	\$332,40
Propuesta expresada en dólares y sin 21% IVA				

La operación se realiza por cuenta y orden de **Nexsys Uruguay**.

Los precios están expresados en dólares y sin IVA.

1.2 Soporte

Nuestro equipo dará soporte técnico inicial, para apoyar y acompañar en el comienzo del despliegue, tanto como la instalación y configuración.

Para proseguir con el soporte, nuestra elección para el cliente, basada en Windows 11 E3, cuenta con el soporte de la plataforma 365, que le brinda al cliente la opción de cargar tickets a Microsoft para que te contacten desde el soporte.

Según información proporcionada por el partner, siempre contestan dentro de las 24/48 los tickets normales, siendo esto un punto que juega a favor para que nuestro cliente esté satisfecho.

1.3 Beneficios

Algunos de los beneficios de utilizar Windows 11 (Para empresas) son:

Biometría: Windows 11 usa tecnología de las características avanzadas de datos biométricos de los dispositivos modernos, como lectores de huellas digitales y cámaras IR especiales para el reconocimiento facial.

Cifrado: Ayuda a proteger tus datos mediante el cifrado, solo las personas autorizadas podrán acceder al dispositivo y datos.

Firewall: Windows incluye características completas de seguridad integradas, como firewall y protecciones para Internet, que ayudan a proteger contra virus, malware y ransomware.

Autenticación doble factor: A través de llamada telefónica, mensaje de texto o la app Microsoft Authenticator para teléfonos celulares y tabletas.

Actualizaciones y soporte: Windows 11 ofrece actualizaciones de seguridad regulares y soporte extendido de Microsoft. Esto garantiza que los dispositivos estén protegidos con las últimas actualizaciones de seguridad y que los usuarios reciban asistencia técnica en caso de problemas.

2 Argumentación Técnica sobre la elección del sistema operativo para los servidores de la red

Luego de investigar algunos sistemas operativos, analizamos más a fondo la posibilidad de utilizar Windows Server, Ubuntu o AlmaLinux.

Windows Server nos presentaba algunas ventajas llamativas como la facilidad para ser administrado, la gran cantidad de documentación que se puede encontrar en Internet, la curva de aprendizaje es bastante accesible y otro punto a favor es el soporte a ASP.NET pero nosotros no utilizamos esa tecnología. Además tiene como desventaja que es de pago y a demás cuenta con muchas vulnerabilidades, es bastante inseguro, consume una gran cantidad de recursos en comparación con otros sistemas operativos y cada vez que se instala una actualización hay que reiniciar el servidor, por esas razones descartamos la opción de utilizar Windows Server.

Por su lado Ubuntu se basa en Debian, tiene una comunidad muy amplia y activa, ofrece estabilidad, rendimiento y una amplia gama de servicios y aplicaciones, como servidores web, bases de datos, servicios de correo electrónico, servidores de archivos y mucho más.

Aunque Ubuntu Server es generalmente estable, en algunas ocasiones las actualizaciones pueden causar problemas de compatibilidad con hardware o software específico, lo que podría requerir solución de problemas adicionales o caídas de servidores o servicios. Eso sumado a que Almalinux tiene un enfoque más orientado a empresas también Almalinux goza de una buena reputación por ser una opción confiable y estable para empresas tradicionales por eso el sistema operativo para nuestros servidores será AlmaLinux.

AlmaLinux es una distribución que es de código abierto, también cuenta con gran compatibilidad y estabilidad. Como distribución de Linux, AlmaLinux tiene el respaldo de una comunidad de desarrolladores y expertos en seguridad, lo cual nos asegura que el sistema operativo reciba actualizaciones de seguridad y parches de manera continua, ayudando a proteger nuestros servidores de red contra posibles vulnerabilidades y ataques de software malicioso.

Esta distribución de Linux nos garantiza un soporte a largo plazo para sus versiones, por lo tanto estará actualizado. Esto trae

cierta tranquilidad ya que nos ayuda a garantizar estabilidad y confiabilidad a lo largo del ciclo de vida del proyecto.

Es importante destacar que AlmaLinux se basa en las mismas fuentes de CentOS y RHEL (Red Hat Enterprise Linux), lo que nos asegura una muy buena compatibilidad con muchas aplicaciones y herramientas empresariales, esto facilita la gestión del mismo.

Además está diseñado para ofrecer un rendimiento óptimo en cuanto al entorno de servidores. Su núcleo y administración de recursos permite utilizar el hardware eficientemente, brindando una respuesta rápida y predecible para las aplicaciones de la red.

Una característica sumamente importante es que AlmaLinux es gratuito para su utilización, esto representa un ahorro en licencias significativo para la empresa y hace mucho más rentable la aplicación del proyecto en su totalidad.

2.1 Licenciamiento

AlmaLinux es una distribución de Linux de código abierto y se distribuye bajo la Licencia Pública General de GNU (GPL) y otras licencias de código abierto que permiten a los usuarios acceder al código fuente, modificarlo y redistribuirlo de acuerdo con los términos de esas licencias.

La Licencia Pública General de GNU (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.

2.3 Soporte

El soporte que tendrá el cliente para el servidor con Almalinux será brindado por el servicio técnico comercial Openlogic, recomendado por el mismo equipo de Almalinux y utilizado por IBM, Toyota, Microsoft, entre otros.

OpenLogic by Perforce brinda el soporte técnico experto necesario para tener éxito con el código abierto, lo que brindará a el cliente la libertad de concentrarse en impulsar su negocio.

Con soporte técnico respaldado por SLA para más de 400 paquetes de código abierto y acceso directo a arquitectos empresariales experimentados, el cliente recibirá soporte técnico integral y servicios profesionales creados para la empresa, todo en un solo lugar.

3 Roles de usuarios que utilizarán el servidor y las terminales

A continuación detallaremos los roles de usuario que interactúan con el servidor y que utilizaran las terminales.

3.1 Terminales:

Administrador:

Descripción: Este usuario tiene privilegio para administrar, configurar el sistema operativo, crear nuevos usuarios realizar instalaciones etc, Este rol será utilizados por los cargos de más confianza por parte de el cliente, así como los jefes y gerentes, y estos deberán contar con conocimientos para realizar las tareas ya que la utilización del rol Administrador puede llevar a realizar rupturas o desconfiguraciones importantes si no se cuenta con los conocimientos necesarios.

Administrativo:

Descripción: Este usuario tiene privilegio para la utilización del sistema operativo, utilizará las terminales para sus tareas como administrador del sitio web WhereWeEat, así como para realizar otras tareas administrativas inherentes a su trabajo.

3.2 Servidor

Administradores (wheel):

Descripción: Serán los encargados de administrar el servidor, realizar instalaciones, correcciones e instalaciones en él, podrán crear nuevos roles y nuevos usuarios y también serán encargados de el monitoreo del servidor. Estos usuarios, por su responsabilidad, deberán ser jefes o personal de confianza de ellos y deberán contar con conocimientos para manipular el servidor.

Administrador Base de Datos(ABD):

Descripción: Este usuario tiene privilegios de administración en la base de datos integrada en el sistema operativo AlmaLinux y accede a ella utilizando herramientas específicas de gestión de bases de datos.

Tareas, respaldos, redes y servicios (Users):

Estos usuarios realizan tareas cotidianas que no requieren privilegios administrativos. Este usuario puede acceder a su directorio personal y ejecutar comandos básicos. Tambien tiene permisos para gestionar redes y servicios.

Web(Web):

Para la utilización de servicios web (como Apache, etc.), este usuario se utiliza para ejecutar el proceso del servidor web. Este usuario tendrá acceso limitado para aumentar la seguridad, para proteger la integridad del sistema.

4 Configuraciones básicas en los sistemas operativos de los servidores, y de las terminales (hostname, red, etc.)

4.1 Cambio de Hostname

```
[mlabora@www-server etc]$ sudo nano hosts
[sudo] password for mlabora: _

127.0.0.1    localhost localhost.localdomain localhost4 localhost4.localdomain4
::1          localhost localhost.localdomain localhost6 localhost6.localdomain6
127.0.0.1    wwwat.com
```

Anfitrión establecido a «wwwat.com»

Aceptar

4.2 Configuración SSH

Cambio de puerto ssh

```
Port 50000
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
```

Impedimos el logueo con usuario Root, limitamos el máximos número de intentos al ingresar password y el tiempo de gracia que pasa para que introduzca la contraseña

```
LoginGraceTime 30
PermitRootLogin no
#StrictModes yes
MaxAuthTries 2
```

Impedimos que se puedan loguear con contraseña para que solo permita mediante clave pública:

```
#RSAAuthentication no
#PubkeyAuthentication yes
```

Habilitamos el registro de eventos subiendo el nivel del Log:

```
LogLevel VERBOSE
```

Utilizamos Protocol 2 de ssg:

```
Protocol 2
```

Limitar el número de pantallas de login:

```
#Failure /var/run/
MaxStartups 1
#PermitTunnel no
```

4.3 Configuración clave pública-privada

```
C:\Users\mathi>ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (C:\Users\mathi/.ssh/id_rsa): wweat-mlabora
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in wweat-mlabora
Your public key has been saved in wweat-mlabora.pub
The key fingerprint is:
SHA256:7e0i+P+21XQvEeMgcESFi/OJSUj0V3kHdKgHn1DHdaQ mathi@LAPTOP-TMDH2S2N
The key's randomart image is:
+---[RSA 3072]---+
|   .o+oo++=B|
|   ..o..+ o++|
|   . . .o...*Eo|
|   . +o...o+o|
|   .S=... .+ .|
|   o.o  o o.|
|   o . o .|
|   . . .o .|
|   ..oo.++.|
+---[SHA256]---+
```

La transferimos al servidor:

```
C:\Users\mathi>scp -P 50000 C:\Users\mathi/.ssh/id_rsa.pub mlabora@192.168.56.103:/tmp/id_rsa.pub
mlabora@192.168.56.103's password:
id_rsa.pub                                         100%  576    102.9KB/s   00:00
```

```
[mlabora@wweat ~]$ sudo cat id_rsa.pub >> ~/.ssh/authorized_keys
```

```
[mlabora@wweat .ssh]$ ls -la
total 20
drwx----- 2 mlabora mlabora 80 set  3 02:59 .
drwx----- 8 mlabora mlabora 4096 set  3 02:56 ..
-rw----- 1 mlabora mlabora 576 set  3 02:59 authorized_keys
-rw----- 1 mlabora mlabora 3434 ago 26 01:08 id_rsa
-rw-r--r-- 1 mlabora mlabora 744 ago 26 01:08 id_rsa.pub
-rw-r--r-- 1 mlabora mlabora 183 ago 27 19:12 known_hosts
```

```
C:\Users\mathi>ssh -p 50000 mlabora@192.168.56.103
Enter passphrase for key 'C:\Users\mathi/.ssh/id_rsa':
Last login: Sun Sep 3 02:56:08 2023
[mlabora@wheat ~]$ |
```

4.5 Instalación php 8.2:

Instalación epel-release

```
[mlabora@wwe-server httpd]$ sudo dnf install -y epel-release
[sudo] password for mlabora:
Última comprobación de caducidad de metadatos hecha hace 0:25:10, el dom 27 ago 2023 17:5
1:43 -03.
El paquete epel-release-8-19.el8.noarch ya está instalado.
Dependencias resueltas.
Nada por hacer.
¡Listo!
[mlabora@wwe-server httpd]$ sudo dnf install -y http://rpms.remirepo.net/enterprise/remi
-release-8.rpm
Última comprobación de caducidad de metadatos hecha hace 0:25:22, el dom 27 ago 2023 17:5
1:43 -03.
remi-release-8.rpm                                         35 kB/s | 32 kB     00:00
Dependencias resueltas.
=====
 Paquete          Arquitectura  Versión           Repositorio      Tam.
=====
Instalando:
 remi-release      noarch       8.8-1.el8.remi    @commandline     32 k

Resumen de la transacción
=====
Instalar 1 Paquete

Tamaño total: 32 k
Tamaño instalado: 27 k
Descargando paquetes:
Ejecutando verificación de operación
Verificación de operación exitosa.
Ejecutando prueba de operaciones
```

Instalamos dnf-utils

```
[mlabora@wwe-server httpd]$ sudo dnf install -y dnf-utils
Remi's Modular repository for Enterprise Linux 8 - x86_6 411 B/s | 833 B 00:02
Remi's Modular repository for Enterprise Linux 8 - x86_6 3.0 MB/s | 3.1 kB 00:00
Importando llave GPG 0xF11735A:
ID usuario: "Remi's RPM repository <remi@remirepo.net>"
Huella : 6B38 FEA7 231F 87F5 2B9C A9D8 5550 9759 5F11 735A
Desde : /etc/pki/rpm-gpg/RPM-GPG-KEY-remi.el8
Remi's Modular repository for Enterprise Linux 8 - x86_6 204 kB/s | 1.3 MB 00:06
Safe Remi's RPM repository for Enterprise Linux 8 - x86_6 553 B/s | 833 B 00:01
Safe Remi's RPM repository for Enterprise Linux 8 - x86_6 3.0 MB/s | 3.1 kB 00:00
Importando llave GPG 0xF11735A:
ID usuario: "Remi's RPM repository <remi@remirepo.net>"
Huella : 6B38 FEA7 231F 87F5 2B9C A9D8 5550 9759 5F11 735A
Desde : /etc/pki/rpm-gpg/RPM-GPG-KEY-remi.el8
Safe Remi's RPM repository for Enterprise Linux 8 - x86_6 705 kB/s | 2.5 MB 00:03
Última comprobación de caducidad de metadatos hecha hace 0:00:01, el dom 27 ago 2023 18:1
7:36 -03.
Dependencias resueltas.
=====
Paquete Arquitectura Versión Repositorio Tam.
=====
Instalando:
yum-utils noarch 4.0.21-19.el8_8 baseos 74 k

Resumen de la transacción
=====
```

Instalamos PHP 8.2

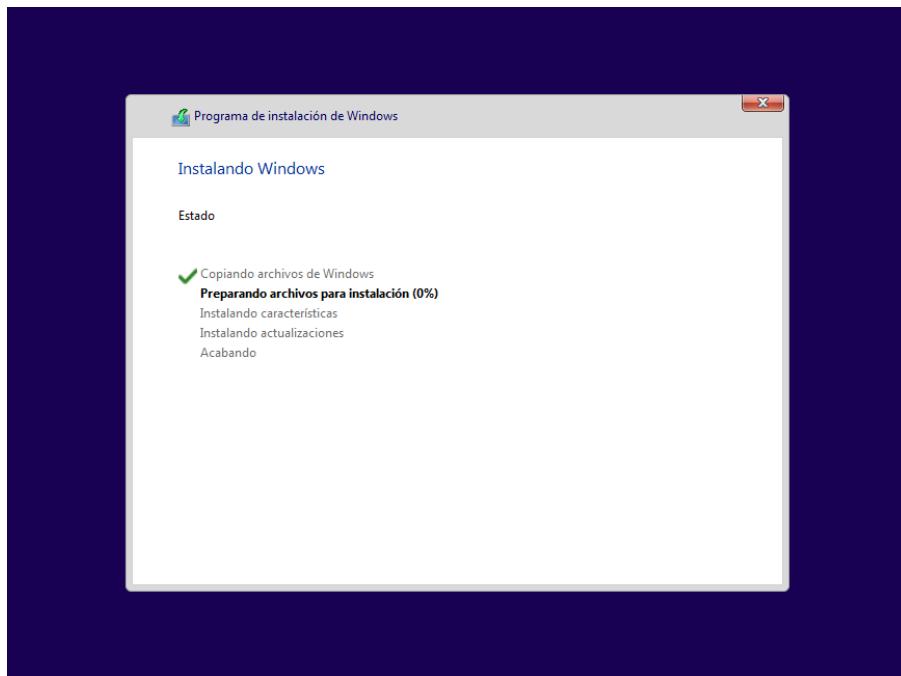
```
[mlabora@wwe-server httpd]$ sudo dnf module install -y php:remi-8.2
Última comprobación de caducidad de metadatos hecha hace 0:00:28, el dom 27 ago 2023 18:1
7:36 -03.
Dependencias resueltas.
=====
Paquete Arq. Versión Repositorio Tam.
=====
Instalando los paquetes del grupo/módulo:
php-cli x86_6 8.2.9-2.el8.remi remi-modular 5.4 M
php-common x86_6 8.2.9-2.el8.remi remi-modular 1.3 M
php-fpm x86_6 8.2.9-2.el8.remi remi-modular 1.9 M
php-mbstring x86_6 8.2.9-2.el8.remi remi-modular 580 k
php-xml x86_6 8.2.9-2.el8.remi remi-modular 260 k
Instalando dependencias:
libxslt x86_6 1.1.32-6.el8 baseos 248 k
oniguruma5php x86_6 6.9.8-1.el8.remi remi-safe 212 k
Instalando dependencias débiles:
nginx-filesystem noarch 1:1.14.1-9.module_el8.3.0+2165+af250afe.alma appstream 23 k
Instalando perfiles de módulos:
php/common
Activando flujos de módulos:
nginx 1.14
php remi-8.2

Resumen de la transacción
=====
Instalar 8 Paquetes

Tamaño total de la descarga: 9.9 M
```

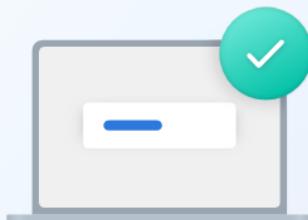
```
[mlabora@wwe-server httpd]$ php --version
PHP 8.2.9 (cli) (built: Aug 3 2023 11:39:08) (NTS gcc x86_64)
Copyright (c) The PHP Group
Zend Engine v4.2.9, Copyright (c) Zend Technologies
```

4.6 Instalación de W11 para las terminales:



Asignemos un nombre al dispositivo

Personalícelo con un nombre único que sea fácil de reconocer cuando se conecte a través de otros dispositivos. Su dispositivo se reiniciará después de que le asigne el nombre.



terminalWWE

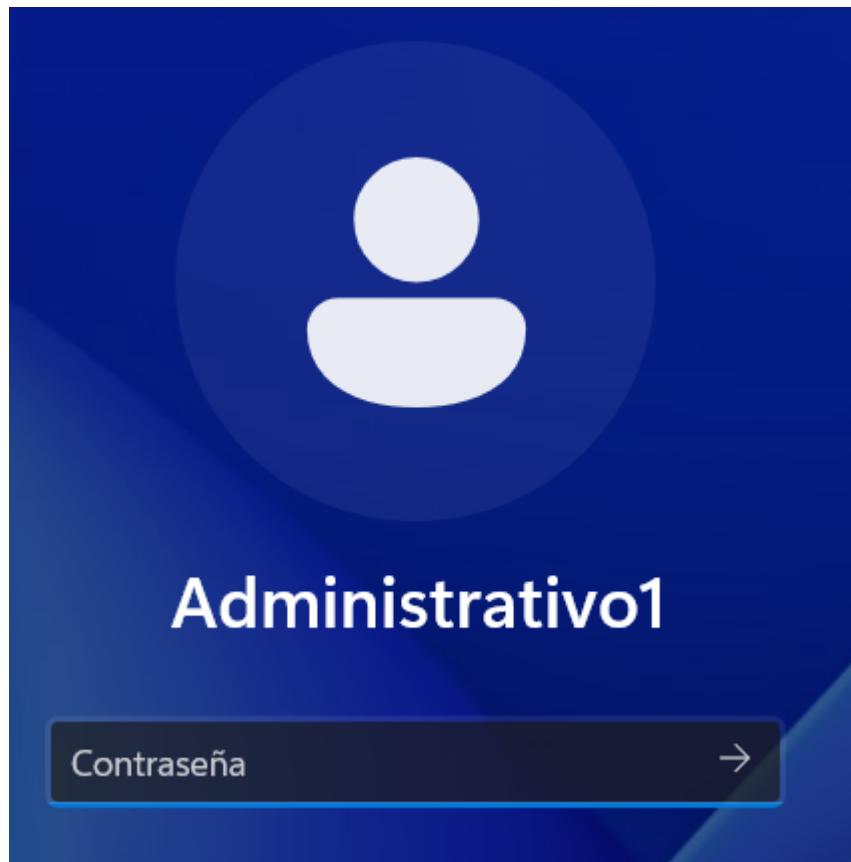
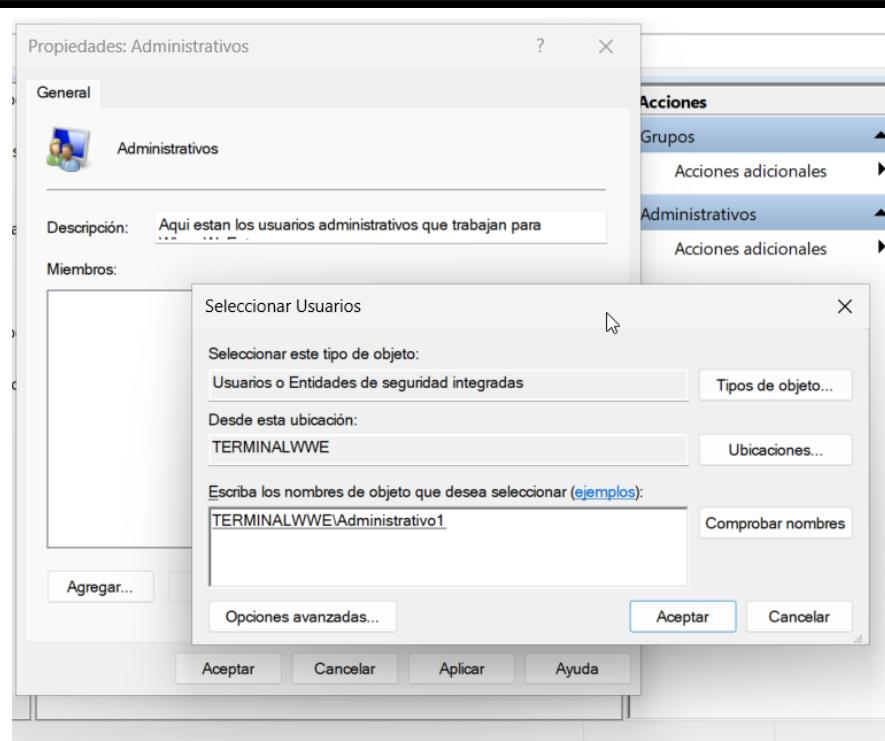
X

No puede contener solo números
No más de 15 caracteres
No hay espacios ni caracteres especiales que no sean guiones (-), guiones (— y –) ni caracteres de subrayado (_).

[Omitir por ahora](#)[Siguiente](#)

Configuración usuarios W11

Nombre	Nombre completo
Administrador	
Administrativo1	Administrativo1

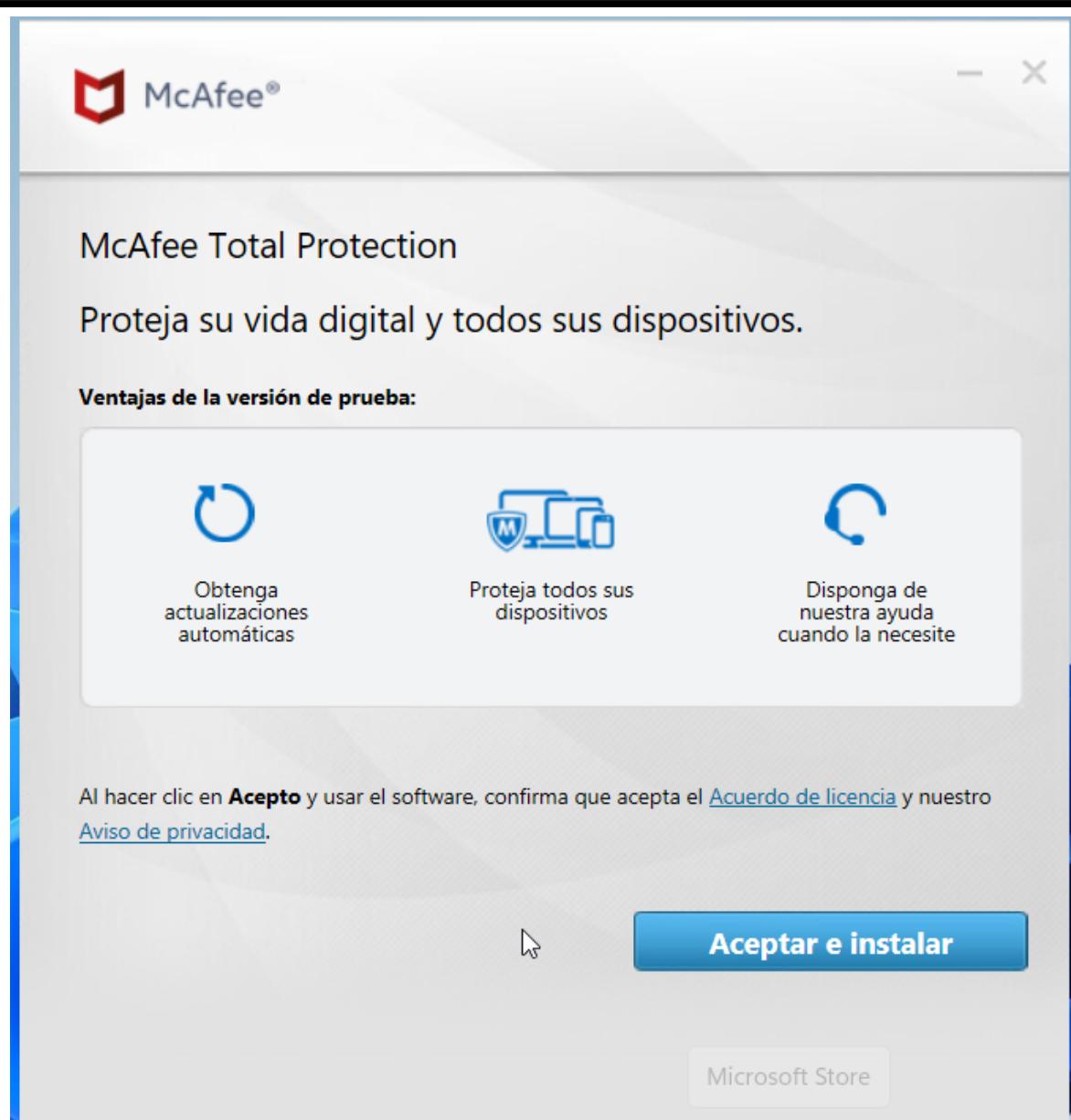


Proporcionamos la instalación de McAfee

En esencia, McAfee Total Protection proporciona nuestro antivirus galardonado para defenderlo contra virus, amenazas en línea y ransomware con protección fuera de línea y en línea basada en la nube. Más allá de sus PC con Windows, McAfee Total Protection brinda una protección entre dispositivos que extiende su tranquilidad a sus Mac y dispositivos móviles iOS/Android para que pueda disfrutar de la seguridad en el hogar y en cualquier lugar, en todos sus dispositivos compatibles.

La protección web de McAfee® WebAdvisor le permite evitar los ataques antes de que sucedan con advertencias claras sobre sitios web, enlaces y archivos peligrosos para que pueda navegar, hacer compras y realizar transacciones bancarias con confianza.

Las funciones de Optimización de PC ayudan a que su PC vaya más rápido, al tiempo que garantiza que usted tenga una seguridad de primer nivel. La optimización web ayuda a salvar tanto su batería como el ancho de banda al detener automáticamente los videos de reproducción automática que intentan desviar su atención. Y con el Potenciador de aplicaciones, las aplicaciones en las que está trabajando activamente recibirán automáticamente una optimización en los recursos para que pueda hacer el trabajo más rápido.



Como herramientas de ofimática al usuario se le brindará Microsoft Office, suministrado por el paquete que nos brinda Office 365.



Te damos la bienvenida a Microsoft 365.

Cree, organice y colabore **gratis** en un solo lugar con **Microsoft 365**



ANEP



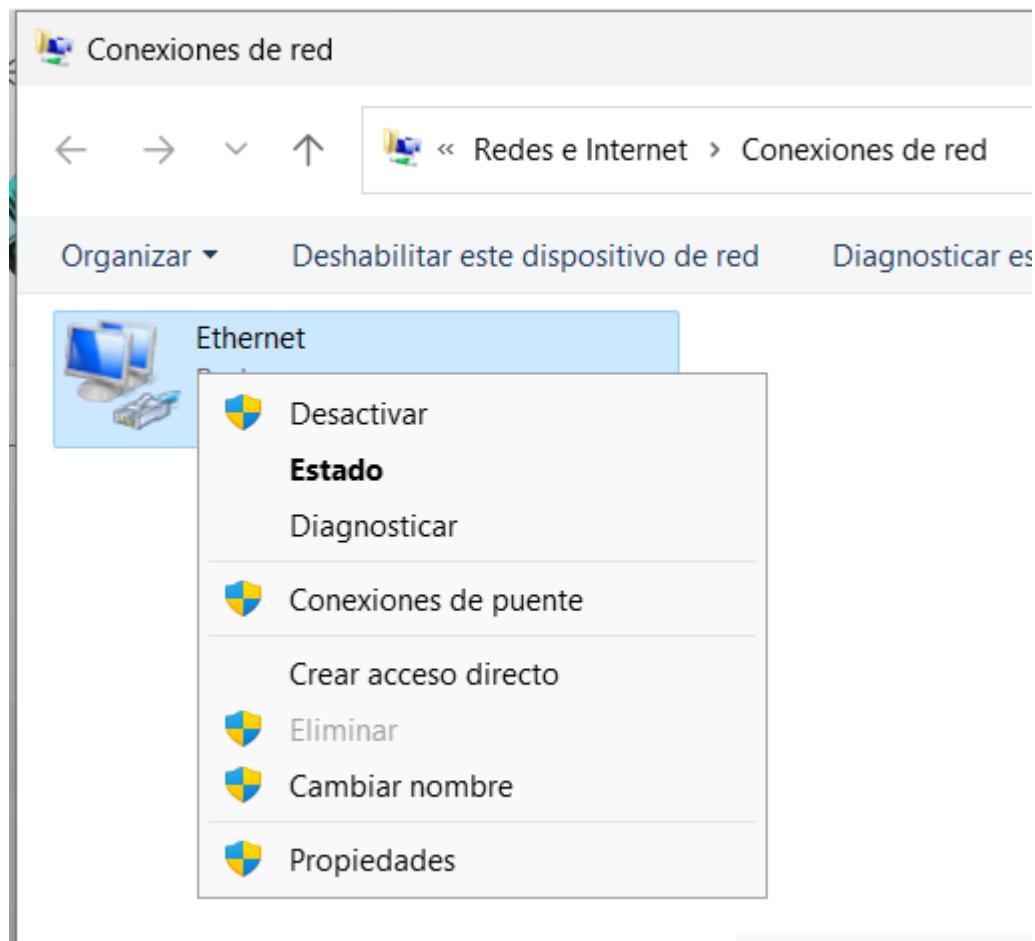
UTU

DIRECCIÓN GENERAL
DE EDUCACIÓN
TÉCNICO PROFESIONAL



Instituto Tecnológico Superior
UTU

Configuración de red:





ANEP

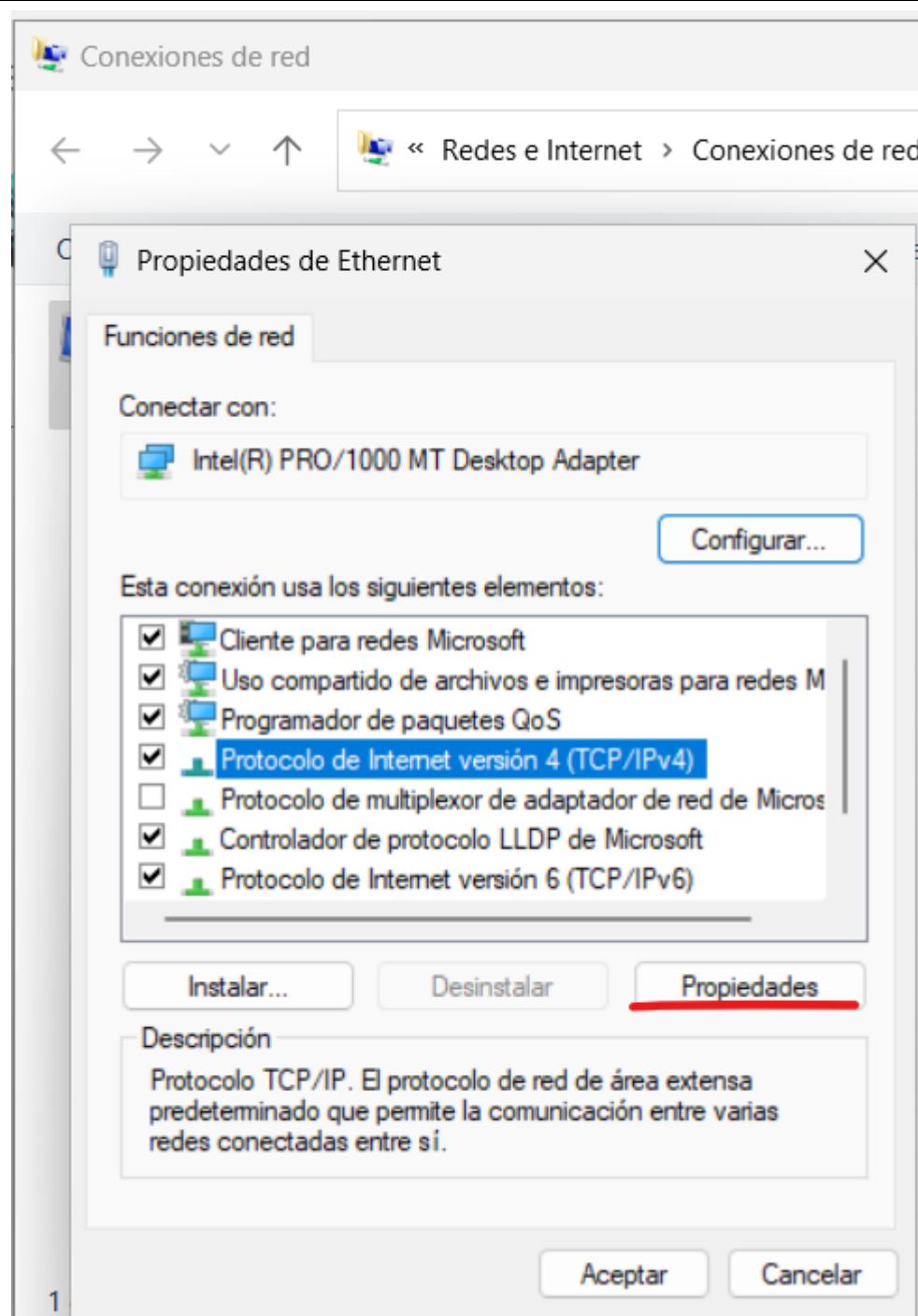


UTU

DIRECCIÓN GENERAL
DE EDUCACIÓN
TÉCNICO PROFESIONAL



Instituto Tecnológico Superior
UTU

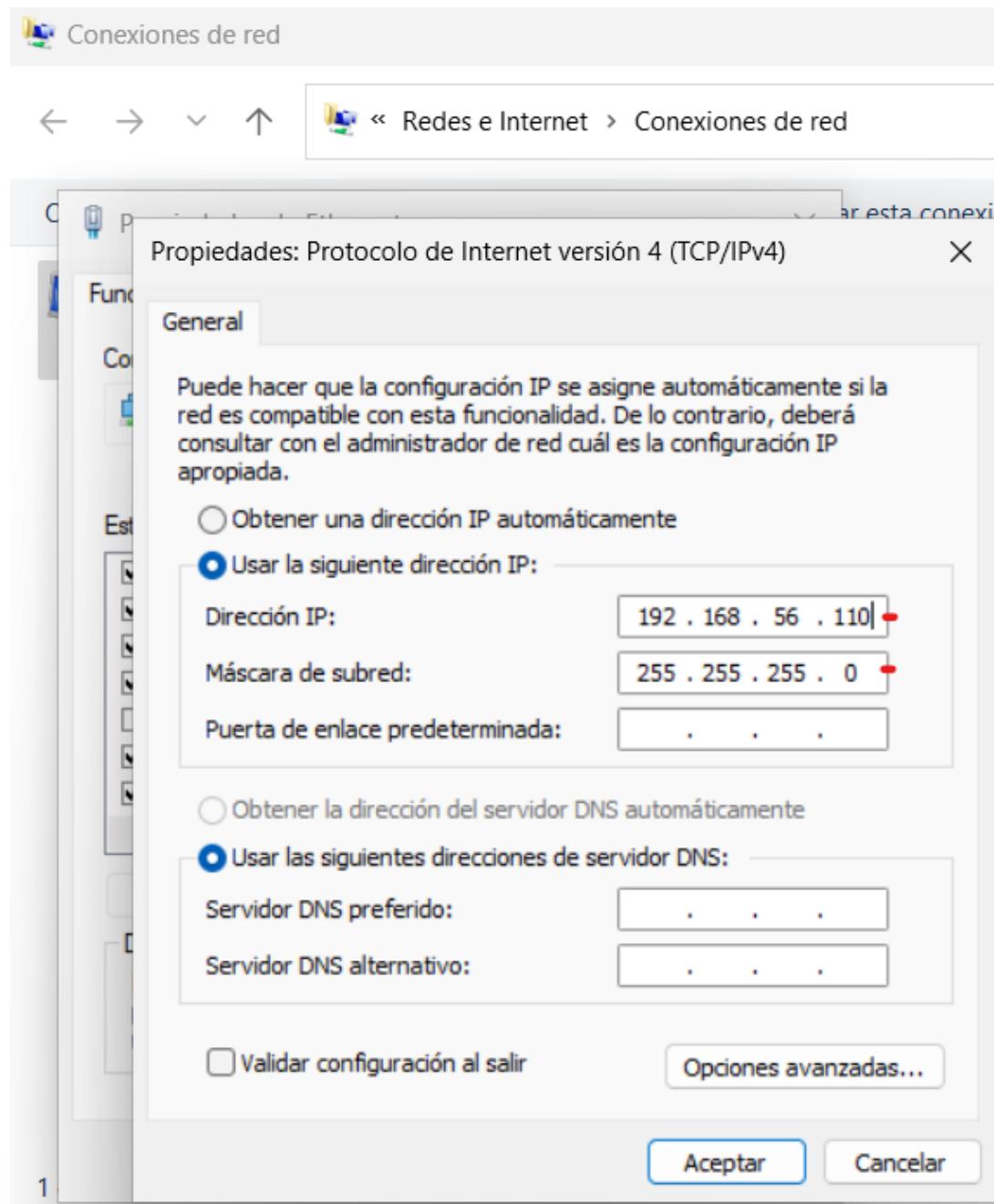


Siguiendo la configuración del servidor Almalinux:

```
inet 192.168.56.103/24
```

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

Configuramos ip y máscara de subred de la terminal:



5 Configuraciones de las cuentas y su perfilamiento a través de privilegios y restricciones Cuentas por perfil

5.1 Creación de los Roles(grupos) de usuarios:

También creamos los usuarios que se encargaran de configuraciones apache y de herramientas de red (network), asignamos al grupo Web

```
[mlabora@wwe-server scripts_adm]$ sudo groupadd ABD
```

```
[mlabora@wwe-server scripts_adm]$ sudo groupadd Users
[mlabora@wwe-server scripts_adm]$ sudo groupadd Web
[mlabora@wwe-server scripts_adm]$ sudo useradd conTurista
[mlabora@wwe-server scripts_adm]$ sudo useradd conAdmin
[mlabora@wwe-server scripts_adm]$ sudo useradd conRest
```

```
[mlabora@wwe-server scripts_adm]$ sudo usermod -aG Web conTurista
[mlabora@wwe-server scripts_adm]$ sudo usermod -aG Web conAdmin
[mlabora@wwe-server scripts_adm]$ sudo usermod -aG Web conRest
```

5.2 Configuración SUDOERS

```
%ABD      ALL=(ALL) NOPASSWD: /usr/bin/mysql
%ABD      ALL=(ALL) NOPASSWD: /usr/bin/mysqldump

%Users    ALL=NETWORKING
%Users    ALL=SERVICES

Cmnd_Alias APACHE_CMDS = /var/www, /etc/httpd

%Web      ALL=APACHE_CMDS
%Web      ALL=NETWORKING
```

6 Licenciamiento, soporte, instalaciones y configuraciones

6.1 Servidor de base de datos MySQL(MariaDB)

6.1.1 Licenciamiento

Para WhereWeEat hemos decidido utilizar MariaDB para gestionar, almacenar y respaldar su base de datos, mas específicamente: MARIADB COMMUNITY SERVER, los motivos los pasamos a detallar a continuación junto al soporte y las alternativas a la misma.

MariaDB utiliza la Licencia GNU: GPLv2

Las licencias para la mayoría del software están diseñadas para quitarle su libertad

para compartirlo y cambiarlo. Por el contrario, la Licencia Pública General GNU es

destinado a garantizar su libertad para compartir y cambiar libremente

software: para asegurarse de que el software sea gratuito para todos sus usuarios. Este

La Licencia Pública General se aplica a la mayor parte del Software Libre

Algunas de las empresas que utilizan MariaDB:



Los planes de licencia que tiene mariaDB son:

MariaDB Community Server (MariaDB Community Server License):

La Licencia de MariaDB Community Server es una licencia de código abierto bajo la cual se distribuye el servidor de base de datos MariaDB. Esta licencia es similar a la Licencia Pública General de GNU (GPL), pero incluye una excepción de almacenamiento, lo que significa que puedes usar la biblioteca MariaDB Connector/C para desarrollar aplicaciones sin que estas aplicaciones sean consideradas como software derivado de MariaDB.

MariaDB Enterprise:

MariaDB Enterprise se destaca como una destacada base de datos de código abierto para entornos de producción, ofreciendo un conjunto de características que sobrepasan significativamente lo disponible en MySQL Enterprise o EnterpriseDB Postgres Platform. Siguiendo los pasos de su predecesora, MySQL, MariaDB Enterprise sigue avanzando con innovaciones notables, como capacidades de SQL distribuido y almacenamiento en columnas. Por otro lado, EnterpriseDB aún carece de características críticas como la agrupación en clústeres multimaestro y el cifrado de datos transparente, lo que pone a MariaDB Enterprise en una posición ventajosa en términos de funcionalidad y soluciones avanzadas.

La siguiente tabla destaca algunas de las diferencias entre MariaDB Enterprise y sus competidores de código abierto:

	ENTERPRISEDB	MYSQL	MARIADB
NoSQL compatible con MongoDB	No	No	Sí
SQL distribuido	No	No	Sí
almacenamiento columnar	No	No	Sí
Tablas temporales	No	No	Sí
Compatibilidad con bases de datos Oracle	Sí	No	Sí
Copias de seguridad sin bloqueo	Sí	producto de terceros	Sí
Agrupación de escritura en cualquier lugar	No	Sí	Sí
Reproducción de transacciones	No	No	Sí
Seguro por defecto	No	Sí	Sí

MariaDB SKYSQL:

SkySQL es un servicio de base de datos en la nube de segunda generación que automatiza la implementación, la administración y el escalado para que pueda concentrarse en iniciativas estratégicas que hagan avanzar el negocio, es el más completo de MariaDB y abarca muchos otros productos los cuales no vamos a incluir al cliente.

6.1.2 Soporte:

El soporte de MariaDB se encuentra disponible mediante la adquisición de una suscripción a MariaDB. Existen diversas alternativas de suscripción diseñadas para cubrir las necesidades individuales. Entre las opciones disponibles se incluyen planes que abarcan desde asistencia destinada a desarrolladores hasta soporte ininterrumpido las 24 horas del día, los 7 días de la semana, durante todo el año, especialmente dirigido a sistemas de producción de suma importancia.

Los planes antes detallados en el Licenciamiento son 3, MariaDB Enterprise y MariaDB SKYSQL incluyen soporte, el plan SKYSQL abarca más productos

El soporte gratuito MARIADB COMMUNITY SERVER solo abarca base de conocimientos y comunidad.

Conclusión:

Hemos optado por recomendarle a nuestro cliente utilizar en principio MARIADB COMMUNITY SERVER que es la versión y soporte básico gratuito y en base a documentaciones. Y más avanzado en el tiempo le recomendamos la utilización de MARIADB ENTERPRISE (por la módica suma de 7500 USD por nodo), ya que abarca todo lo que necesitamos para la base de datos y también incluye el soporte necesario para la base de datos MariaDB.

PRODUCT FEATURESCommunity
Server

Enterprise

- Knowledge Base
- Technical Support
- Consultative Support
- Product Notifications
- Security Alerts
- Indemnification



6.1.3 Instalación y configuración

-sudo dnf install mariadb-server

```
[mlabora@192 ~]$ sudo dnf install mariadb-server
^[[SAlmaLinux 8 - BaseOS           [
^[[SAlmaLinux 8 - BaseOS           [ ===
^[[SAlmaLinux 8 - BaseOS           [ ===
^[[SAlmaLinux 8 - BaseOS           [   ===
AlmaLinux 8 - BaseOS             [ ===
```

Iniciamos y habilitamos el servicio para que inicie siempre con el sistema.

-sudo systemctl start mariadb
-sudo systemctl enable mariadb

Configuración de seguridad inicial:

- mysql_secure_installation
yes para el password (por defecto en mariadb es sin clave el root)
Pass: Mariadb123**

```
[mlabora@wwe ~]$ sudo systemctl start mariadb
[mlabora@wwe ~]$ sudo systemctl enable mariadb
[mlabora@wwe ~]$ mysql_secure_installation
```

NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB
SERVERS IN PRODUCTION USE! PLEASE READ EACH STEP CAREFULLY!

In order to log into MariaDB to secure it, we'll need the current
password for the root user. If you've just installed MariaDB, and
you haven't set the root password yet, the password will be blank,
so you should just press enter here.

Enter current password for root (enter for none):
OK, successfully used password, moving on...

Setting the root password ensures that nobody can log into the MariaDB
root user without the proper authorisation.

You already have a root password set, so you can safely answer 'n'.

Change the root password? [Y/n] Y

New password:

Re-enter new password:

Password updated successfully!

Reloading privilege tables..

... Success!

By default, a MariaDB installation has an anonymous user, allowing anyone
to log into MariaDB without having to have a user account created for
them. This is intended only for testing, and to make the installation
go a bit smoother. You should remove them before moving into a
production environment.

Remove anonymous users? [Y/n]

```
Remove anonymous users? [Y/n] y
... Success!

Normally, root should only be allowed to connect from 'localhost'. This
ensures that someone cannot guess at the root password from the network.

Disallow root login remotely? [Y/n] y
... Success!

By default, MariaDB comes with a database named 'test' that anyone can
access. This is also intended only for testing, and should be removed
before moving into a production environment.

Remove test database and access to it? [Y/n] y
- Dropping test database...
... Success!
- Removing privileges on test database...
... Success!

Reloading the privilege tables will ensure that all changes made so far
will take effect immediately.

Reload privilege tables now? [Y/n] y
... Success!

Cleaning up...

All done! If you've completed all of the above steps, your MariaDB
installation should now be secure.

Thanks for using MariaDB!
```

Agregamos al Firewall el puerto 3306 para poder conectarnos
sudo firewall-cmd --add-port=3306/tcp --permanent

```
[mlabora@wherewe eat ~]$ sudo firewall-cmd --add-port=3306/tcp --permanent
[sudo] password for mlabora:
success
[mlabora@wherewe eat ~]$ _
```

```
[mlabora@whereweet ~]$ sudo firewall-cmd --reload
success
[mlabora@whereweet ~]$ sudo firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3 enp0s8 enp0s9
  sources:
  services: cockpit dhcpv6-client http https ssh
  ports: 3000/tcp 3306/tcp
  protocols:
  forward: no
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
[mlabora@whereweet ~]$
```

6.2 Software de monitoreo

6.2.1 Licenciamiento grafana:

Para realizar el monitoreo del servidor y los recursos del mismo, hemos decidido utilizar Grafana, es un software libre, en plena expansión y mantenido a su vez cuenta con gran cantidad de configuraciones de dashboards prediseñados o creados por la comunidad que agregan un valor importante a la herramienta.

Grafana Labs fue fundada en 2014 con el propósito de establecer un modelo de negocio sostenible en torno al proyecto de código abierto Grafana. La intención era que los ingresos generados por sus ofertas comerciales pudieran ser reinvertidos en el desarrollo de la tecnología y en beneficio de la comunidad. Desde entonces, la compañía ha ampliado su alcance en el ecosistema de código abierto, dando origen a proyectos adicionales como Grafana Loki y Grafana Tempo. Además, ha tenido una destacada participación en iniciativas como Graphite, Prometheus y Cortex. Al mismo tiempo, ha creado productos orientados a sus clientes, como Grafana Cloud y Grafana Enterprise Stack.

La empresa ha priorizado equilibrar la creación de valor a través del código abierto y la comunidad, mientras busca una estrategia de monetización. La elección de la licencia ha sido fundamental y ha sido discutida desde los inicios de la compañía.

En los últimos años, Grafana Labs ha observado de cerca las decisiones de otras empresas importantes en el ámbito del código abierto, como Elastic, Redis Labs, MongoDB, Timescale y Cockroach Labs. La mayoría de estas empresas han optado por cambiar sus licencias a modelos de fuente disponible no aprobados por la Iniciativa de Código Abierto (OSI).

Después de debates internos a principios de 2021, la compañía anunció un cambio en su enfoque de licenciamiento. Los proyectos

principales de código abierto de Grafana Labs (Grafana, Grafana Loki y Grafana Tempo) cambiarán su licencia de Apache 2.0 a la Licencia Pública General Afferro (AGPL) versión 3. Sin embargo, los complementos, agentes y algunas bibliotecas seguirán bajo la Licencia Apache. La licencia AGPLv3 es aprobada por la OSI y garantiza las libertades de la comunidad, lo que sigue siendo esencial para la empresa. Este cambio no restringe la capacidad de los usuarios para utilizar, modificar o compartir el software, pero requiere que compartan el código fuente si realizan modificaciones y ofrecen el software a otros. Además, se actualiza el Acuerdo de Licencia de Colaborador (CLA) de la compañía para equilibrar los intereses de los contribuyentes y los derechos de la compañía.

6.2.2 Soporte grafana:

Para grafana se utilizará el soporte básico(Soporte de la comunidad) y el Soporte Cloud gratuito. A continuación detallamos los tipos de soporte con los que cuenta grafana.

Soporte basico

Grafana ofrece varios tipos de soporte para facilitar su uso y maximizar su eficacia.

Soporte de la comunidad: Grafana cuenta con una comunidad activa de usuarios y desarrolladores que brindan soporte y comparten recursos. Puede acceder a la documentación oficial, foros de discusión y otros recursos en línea para obtener ayuda y aprender de otros usuarios de Grafana.

Soporte Cloud

Tipos de cuenta y soporte disponibles para usuarios de Grafana Cloud

Hay tres tipos de cuentas de Grafana Cloud:

Gratis: una cuenta gratuita está destinada a equipos pequeños y aficionados para comenzar. Las funciones son limitadas, pero proporcionan una buena combinación de lo que se necesita para comenzar con la observabilidad. Esta también es una buena manera de familiarizarse con Grafana Cloud. Consulte los precios para obtener detalles sobre las funciones incluidas. El soporte se limita a este conjunto de documentación y consultas en los foros públicos de la comunidad , excepto por problemas como cuentas rotas. Para problemas relacionados con la cuenta que no están relacionados con "¿Cómo hago que Grafana Cloud haga algo?", haga clic en Abrir un ticket de soporte desde el portal de la nube.

Pro: Pro está diseñado para casos de uso en crecimiento, para equipos y cargas de trabajo que requieren escala, seguridad y colaboración. Se espera que los usuarios aquí comienzan con la documentación y las consultas en los foros públicos de la comunidad sin embargo, el soporte por correo electrónico está disponible durante el horario comercial.

Avanzado: el nivel Avanzado está diseñado para casos de uso de métricas y registros a gran escala, equipos con cargas de trabajo de misión crítica y equipos con muchos usuarios. Puede registrarse en línea o ponerse en contacto con nuestro equipo para obtener ayuda para determinar la configuración y el entorno adecuados. El soporte completo, que se ofrece las 24 horas del día, los 7 días de la semana a los clientes de nuestro plan Avanzado, se proporciona a través del botón Abrir un ticket de soporte en el Portal de la nube o desde su equipo de cuenta. Para más información, contacta con Grafana .

6.2.3 Instalación grafana:

->Paso 1

Agregar el repositorio de Grafana, Grafana no se encuentra en los repositorios predeterminados de AlmaLinux, por eso agregamos el repositorio de Grafana para facilitar la instalación. Ejecuta los siguientes comandos para agregar el repositorio y habilitar Grafana:

```
sudo tee /etc/yum.repos.d/grafana.repo << EOF
#Todo lo que se encuentra entre "<<EOF" y "EOF" precedido del comando "tee" se copiara
en el archivo especificado "grafana.repo"
[grafana]
name=grafana
baseurl=https://packages.grafana.com/oss/rpm
repo_gpgcheck=1
enabled=1
gpgcheck=1
gpgkey=https://packages.grafana.com/gpg.key
EOF #End Of File
```

->Paso 2

sudo dnf install grafana

datos que nos brinda la instalación:

ID usuario: "Grafana Labs <engineering@grafana.com>"
Huella : 0E22 EB88 E39E 1227 7A77 60AE 9E43 9B10 2CF3 C0C6
Desde : <https://packages.grafana.com/gpg.key>

```

Total                                         6.5 MB/s | 79 MB   00:12
Ejecutando verificación de operación
Verificación de operación exitosa.
Ejecutando prueba de operaciones
Prueba de operación exitosa.
Ejecutando operación
Preparando          : 1/
Instalando         : urw-base35-standard-symbols-ps-fonts-20170801-10.el8.noarch 1/
Ejecutando scriptlet: urw-base35-standard-symbols-ps-fonts-20170801-10.el8.noarch 1/
Instalando         : urw-base35-fonts-20170801-10.el8.noarch                2/
Instalando         : grafana-10.0.3-1.x86_64                            3/
Ejecutando scriptlet: grafana-10.0.3-1.x86_64                          3/
### NOT starting on installation, please execute the following statements to configure grafana to
start automatically using systemctl
sudo /bin/systemctl daemon-reload
sudo /bin/systemctl enable grafana-server.service
### You can start grafana-server by executing
sudo /bin/systemctl start grafana-server.service

Ejecutando scriptlet: urw-base35-standard-symbols-ps-fonts-20170801-10.el8.noarch 3/
Ejecutando scriptlet: grafana-10.0.3-1.x86_64                          3/
POSTTRANS: Running script

Verificando        : urw-base35-fonts-20170801-10.el8.noarch      1/
Verificando        : urw-base35-standard-symbols-ps-fonts-20170801-10.el8.noarch 2/
Verificando        : grafana-10.0.3-1.x86_64                            3/

Instalado:
grafana-10.0.3-1.x86_64
urw-base35-fonts-20170801-10.el8.noarch
urw-base35-standard-symbols-ps-fonts-20170801-10.el8.noarch

¡Listo!
[mlabora@www ~]$ _

```

->Paso 3

Habilitamos grafana para que inicie al iniciar el sistema:

-sudo systemctl enable grafana-server

-sudo systemctl start grafana-server

Agregamos al firewall:

-sudo firewall-cmd --add-port=3000/tcp --permanent

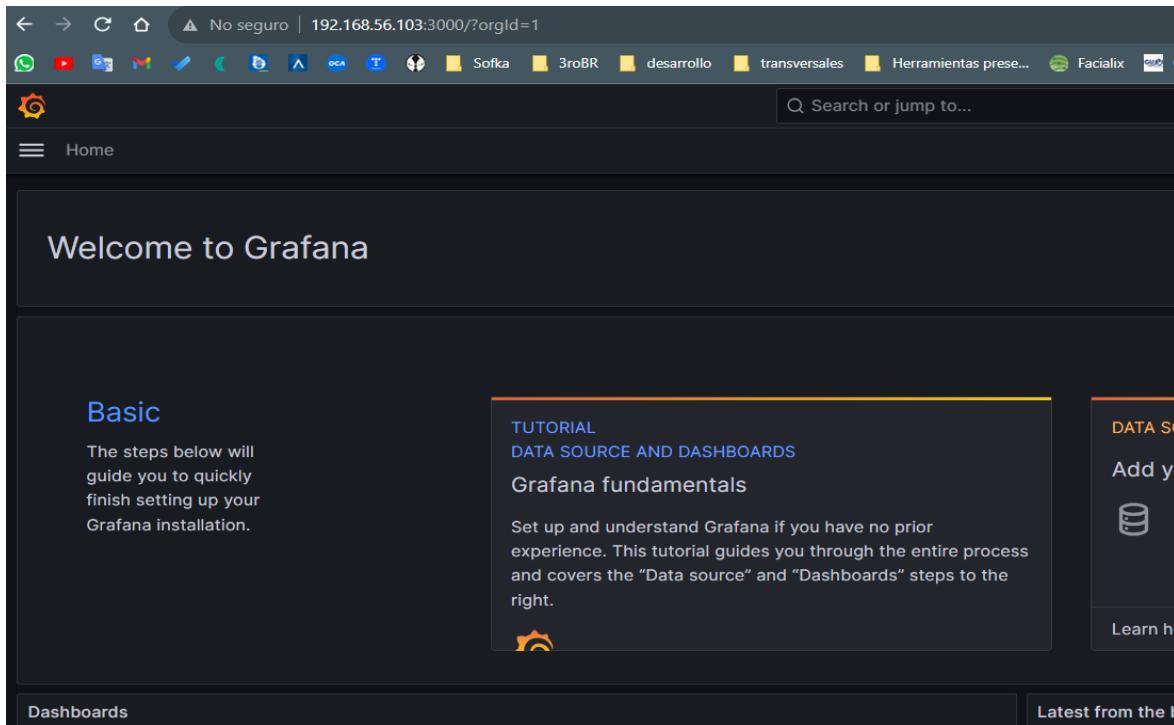
-sudo firewall-cmd --reload

```
[mlabora@wwe ~]$ sudo systemctl enable grafana-server
[sudo] password for mlabora:
Sorry, try again.
[sudo] password for mlabora:
Synchronizing state of grafana-server.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable grafana-server
[mlabora@wwe ~]$ sudo systemctl start grafana-server
[mlabora@wwe ~]$ sudo firewall-cmd --add-port=3000/tcp --permanent
Warning: ALREADY_ENABLED: 3000:tcp
success
[mlabora@wwe ~]$ sudo firewall-cmd --reload
success
[mlabora@wwe ~]$ _
```

Interfaz:

Usuario: admin

Pass: Admin123**



The screenshot shows the Grafana home page. At the top, there's a navigation bar with icons for back, forward, search, and other system links. Below the bar, a header says "Welcome to Grafana". On the left, there's a sidebar with a "Basic" section containing a brief guide for new users. To the right, there are several links: "TUTORIAL", "DATA SOURCE AND DASHBOARDS", "Grafana fundamentals", and a "Set up and understand Grafana if you have no prior experience. This tutorial guides you through the entire process and covers the "Data source" and "Dashboards" steps to the right." link. Further down, there are sections for "Dashboards" and "Latest from the blog".

Instalacion Prometheus + node_exporter

```
[mlabora@whereweet ~]$ sudo useradd --no-create-home --shell /bin/false prometheus
[sudo] password for mlabora:
[mlabora@whereweet ~]$ sudo mkdir /etc/prometheus
[mlabora@whereweet ~]$ sudo mkdir /var/lib/prometheus
[mlabora@whereweet ~]$ sudo chown prometheus:prometheus /etc/prometheus
[mlabora@whereweet ~]$ sudo chown prometheus:prometheus /var/lib/prometheus
[mlabora@whereweet ~]$ cd ~
[mlabora@whereweet ~]$ curl -L0 https://github.com/prometheus/prometheus/releases/download/v2.0.0/prometheus-2.0.0.linux-amd64.tar.gz_
```

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

```
[mlabora@whereweet ~]$ tar xvf prometheus-2.0.0.linux-amd64.tar.gz
prometheus-2.0.0.linux-amd64/
prometheus-2.0.0.linux-amd64/consoles/
prometheus-2.0.0.linux-amd64/consoles/index.html.example
prometheus-2.0.0.linux-amd64/consoles/node-cpu.html
prometheus-2.0.0.linux-amd64/consoles/node-disk.html
prometheus-2.0.0.linux-amd64/consoles/node-overview.html
prometheus-2.0.0.linux-amd64/consoles/node.html
prometheus-2.0.0.linux-amd64/consoles/prometheus-overview.html
prometheus-2.0.0.linux-amd64/consoles/prometheus.html
prometheus-2.0.0.linux-amd64/console_libraries/
prometheus-2.0.0.linux-amd64/console_libraries/menu.lib
prometheus-2.0.0.linux-amd64/console_libraries/prom.lib
prometheus-2.0.0.linux-amd64/prometheus.yml
prometheus-2.0.0.linux-amd64/LICENSE
prometheus-2.0.0.linux-amd64/NOTICE
prometheus-2.0.0.linux-amd64/prometheus
prometheus-2.0.0.linux-amd64/promtool
[mlabora@whereweet ~]$ _
```

```
[mlabora@whereweet ~]$ sudo cp prometheus-2.0.0.linux-amd64/prometheus /usr/local/bin/
[mlabora@whereweet ~]$ sudo cp prometheus-2.0.0.linux-amd64/promtool /usr/local/bin/
[mlabora@whereweet ~]$ sudo chown prometheus:prometheus /usr/local/bin/prometheus
[mlabora@whereweet ~]$ sudo chown prometheus:prometheus /usr/local/bin/promtool
[mlabora@whereweet ~]$ sudo cp -r prometheus-2.0.0.linux-amd64/consoles /etc/prometheus/
[mlabora@whereweet ~]$ sudo cp -r prometheus-2.0.0.linux-amd64/console_libraries /etc/prometheus/
[mlabora@whereweet ~]$ sudo chown -R prometheus:prometheus /etc/prometheus/consoles
[mlabora@whereweet ~]$ sudo chown -R prometheus:prometheus /etc/prometheus/console_libraries/
[mlabora@whereweet ~]$ rm -rf prometheus-2.0.0.linux-amd64.tar.gz prometheus-2.0.0.linux-amd64
[mlabora@whereweet ~]$ sudo touch /etc/prometheus/prometheus.yml
[mlabora@whereweet ~]$ sudo chown prometheus:prometheus /etc/prometheus/prometheus.yml
```

```
[mlabora@whereweet ~]$ sudo systemctl start node_exporter
[mlabora@whereweet ~]$ sudo systemctl daemon-reload
[mlabora@whereweet ~]$ sudo systemctl start prometheus
[mlabora@whereweet ~]$ sudo systemctl start node_exporter
```



ANEP



UTU

DIRECCIÓN GENERAL
DE EDUCACIÓN
TÉCNICO PROFESIONAL



Instituto Tecnológico Superior
UTU

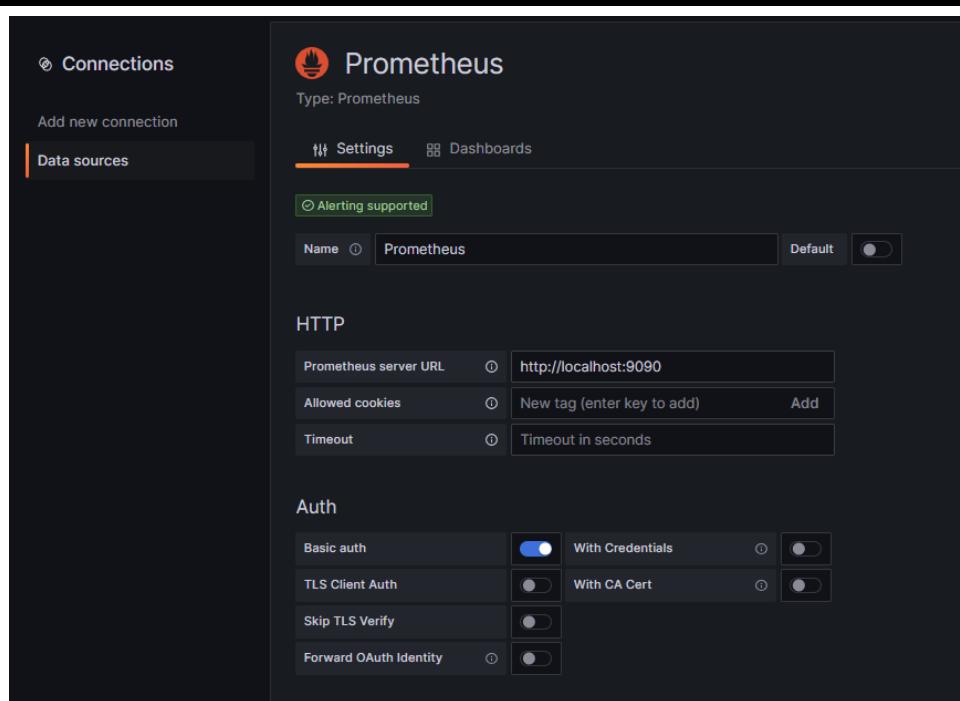
Ya instalado node_exporter y prometheus, aqui la configuracion de prometheus.yml:

```
mabora@whereweate:~/etc/prometheus$ cat prometheus.yml
# Attach these labels to any time series or alerts when co
# external systems (federation, remote storage, Alertmanag
# external_labels:
# monitor: 'codelab-monitor'

# A scrape configuration containing exactly one endpoint to
# Here it's Prometheus itself.
scrape_configs:
  # The job name is added as a label 'job=<job_name>' to any
  - job_name: 'prometheus'
    # Override the global default and scrape targets from thi
    scrape_interval: 5s
    static_configs:
      - targets: ['localhost:9090']
  - job_name: 'node_exporter'
    scrape_interval: 5s
    static_configs:
      - targets: ['localhost:9100']

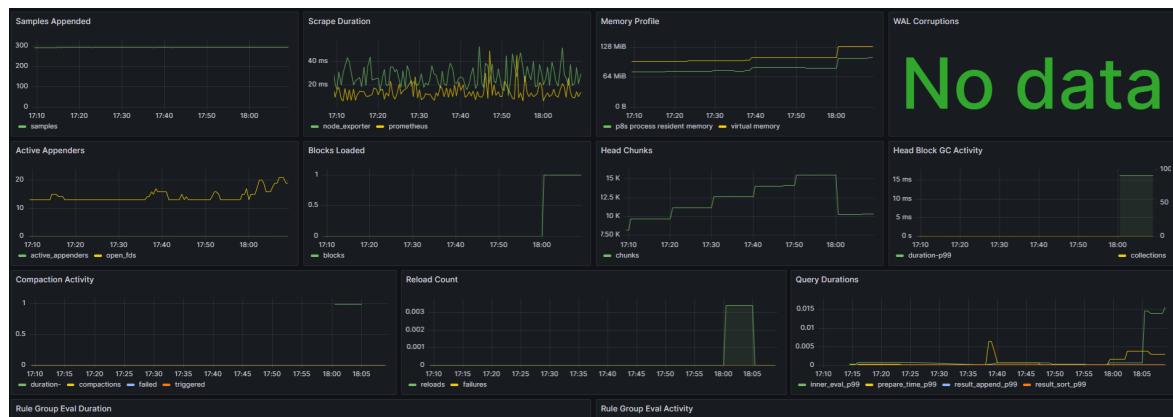
mabora@whereweate:~/etc/prometheus$
```

configuramos en grafana Prometheus, con la url y usuario y password (prometheus pass: Grafana123**):



The screenshot shows the Prometheus configuration interface. On the left, there's a sidebar with 'Connections' and 'Data sources' tabs. The 'Data sources' tab is selected. The main area is titled 'Prometheus' with the sub-type 'Prometheus'. It has two tabs: 'Settings' (which is active) and 'Dashboards'. A green button labeled 'Alerting supported' is visible. Below it, there's a 'Name' input field set to 'Prometheus', a 'Default' toggle switch, and a 'Timeout' input field set to 'Timeout in seconds'. The 'HTTP' section contains fields for 'Prometheus server URL' (set to 'http://localhost:9090'), 'Allowed cookies' (with a 'New tag (enter key to add)' input and an 'Add' button), and 'Timeout' (set to 'Timeout in seconds'). The 'Auth' section includes toggles for 'Basic auth' (on), 'With Credentials' (off), 'TLS Client Auth' (off), 'With CA Cert' (off), 'Skip TLS Verify' (off), and 'Forward OAuth Identity' (off).

Y aqui tenemos la monitorización del sistema obteniendo dashboards preconfigurados:





6.3 Antivirus ClamAV

ClamAV

En la realización del proyecto para *Where We Eat* nos decidimos por utilizar ClamAv en el servidor AlmaLinux 8.7, algunos de los motivos son:

Código Abierto y Gratuito: ClamAV es un software de código abierto, lo que significa que puedes utilizarlo y modificarlo sin costo alguno. Esto es beneficioso para reducir los costos de licencia en comparación con las soluciones antivirus de pago.

Amplia Base de Datos de Firmas: ClamAV cuenta con una extensa base de datos de firmas de virus.

Detecta Diferentes Tipos de Amenazas: ClamAV no solo detecta virus, sino también otros tipos de malware como troyanos, gusanos y spyware.

Ligero y Eficiente: ClamAV está diseñado para ser ligero en recursos, lo que significa que no consumirá una gran cantidad de recursos del sistema mientras realiza escaneos o actualizaciones.

Soporte Activo de la Comunidad: ClamAV cuenta con una comunidad activa de usuarios y desarrolladores que trabajan en mejoras continuas y proporcionan soporte a través de foros y recursos en línea.

Actualizaciones Regulares: La base de datos de firmas de ClamAV se actualiza regularmente para incluir las últimas amenazas conocidas.

6.3.1 Soporte

Optamos por comenzar a utilizar el soporte de la Comunidad de usuarios sumado a la documentación oficial y al canal de Discord que brinda ClamAV para soporte

ClamAV es un proyecto de código abierto y, aunque no hay un soporte oficial directo, la comunidad de usuarios y los recursos en línea pueden proporcionarnos la ayuda que necesitamos para utilizar y solucionar problemas con ClamAV

Algunas opciones de soporte:

Documentación oficial: El sitio web oficial de ClamAV proporciona documentación completa sobre el uso y la configuración de ClamAV. Podemos encontrar guías, tutoriales y otros recursos útiles en la sección de documentación.

Comunidad de usuarios: ClamAV cuenta con una comunidad activa de usuarios que comparten sus experiencias y conocimientos en foros y grupos de discusión. Podemos buscar en línea grupos de usuarios de ClamAV donde poder hacer preguntas y obtener ayuda de otros usuarios.

Soporte comercial: Es un soporte más avanzado y personalizado, se puede considerar contratar servicios de soporte comercial para ClamAV. Algunas empresas ofrecen servicios de soporte técnico especializados en ClamAV y pueden brindar asistencia y soluciones específicas para las necesidades que nos surjan.

Sourcefire y Cyren son empresas que nos pueden brindar soporte para ClamAv entre otras tantas

6.3.2 Licenciamiento

ClamAV es un software antivirus de código abierto y se distribuye bajo la Licencia Pública General de GNU (GPL). La licencia GPL es una licencia de software libre que garantiza la libertad de usar, estudiar, modificar y distribuir el software. Esto significa que ClamAV se puede utilizar de forma gratuita y se permite su modificación y distribución, siempre que se cumplan los términos de la licencia GPL.

Es importante tener en cuenta que, aunque ClamAV se distribuye bajo la licencia GPL, algunas empresas o servicios pueden ofrecer soporte y asistencia técnica adicional como mencionamos en el apartado de soporte.

6.3.3 Instalación

```
[mlabora@wwe ~]$ sudo dnf install -y clamav clamd clamav-update
[sudo] password for mlabora:
Última comprobación de caducidad de metadatos hecha hace 2:08:51, el jue 10 ago 2023 21:12:32 EDT.
Dependencias resueltas.
=====
Paquete           Arquitectura     Versión       Repositorio   Tam.
=====
Instalando:
clamav           x86_64          0.103.8-3.el8    epel          339 k
clamav-update    x86_64          0.103.8-3.el8    epel          131 k
clamd            x86_64          0.103.8-3.el8    epel          126 k
Instalando dependencias:
clamav-filesystem noarch        0.103.8-3.el8    epel          47 k
clamav-lib       x86_64          0.103.8-3.el8    epel          863 k
libprelude       x86_64          5.2.0-1.el8      epel          326 k
libtool-ltdl     x86_64          2.4.6-25.el8     baseos        58 k
Resumen de la transacción
=====
Instalar 7 Paquetes

Tamaño total de la descarga: 1.8 M
Tamaño instalado: 169 M
Descargando paquetes:
(1/?): libtool-ltdl-2.4.6-25.el8.x86_64.rpm          106 kB/s | 58 kB  00:00
(2/?): clamav-filesystem-0.103.8-3.el8.noarch.rpm    23 kB/s | 47 kB  00:02
(3-4/?): clamav-lib-0.103.8-3. 15% [=====          ] 419 kB/s | 296 kB  00:03 ETA
```

```

Total                                         295 kB/s | 1.8 MB   00:06
Ejecutando verificación de operación
Verificación de operación exitosa.
Ejecutando prueba de operaciones
Prueba de operación exitosa.
Ejecutando operación
  Preparando :                                         1/1
  Ejecutando scriptlet: clamav-filesystem-0.103.8-3.el8.noarch 1/7
  Instalando  : clamav-filesystem-0.103.8-3.el8.noarch
  Instalando  : libtool-ltdl-2.4.6-25.el8.x86_64           2/7
  Ejecutando scriptlet: libtool-ltdl-2.4.6-25.el8.x86_64
  Instalando  : libprelude-5.2.0-1.el8.x86_64             3/7
  Ejecutando scriptlet: libprelude-5.2.0-1.el8.x86_64
  Instalando  : clamav-lib-0.103.8-3.el8.x86_64           4/7
  Instalando  : clamav-update-0.103.8-3.el8.x86_64          5/7
  Ejecutando scriptlet: clamav-update-0.103.8-3.el8.x86_64
  Instalando  : clamav-0.103.8-3.el8.x86_64              6/7
  Ejecutando scriptlet: clamav-0.103.8-3.el8.x86_64
  Ejecutando scriptlet: clamd-0.103.8-3.el8.x86_64
  Instalando  : clamd-0.103.8-3.el8.x86_64               7/7
  Ejecutando scriptlet: clamd-0.103.8-3.el8.x86_64
  Verificando  : libtool-ltdl-2.4.6-25.el8.x86_64           1/7
  Verificando  : clamav-0.103.8-3.el8.x86_64              2/7
  Verificando  : clamav-filesystem-0.103.8-3.el8.noarch
  Verificando  : clamav-lib-0.103.8-3.el8.x86_64           4/7
  Verificando  : clamav-update-0.103.8-3.el8.x86_64          5/7
  Verificando  : clamd-0.103.8-3.el8.x86_64              6/7
  Verificando  : libprelude-5.2.0-1.el8.x86_64             7/7

Instalado:
  clamav-0.103.8-3.el8.x86_64                      clamav-filesystem-0.103.8-3.el8.noarch
  clamav-lib-0.103.8-3.el8.x86_64                   clamav-update-0.103.8-3.el8.x86_64
  clamd-0.103.8-3.el8.x86_64                        libprelude-5.2.0-1.el8.x86_64
  libtool-ltdl-2.4.6-25.el8.x86_64

¡Listo!
[milabora@wwe ~]$ _

```

Configuración:

Actualizamos las firmas:

-sudo freshclam

```
[mlabora@wwe ~]$ sudo freshclam
ClamAV update process started at Thu Aug 10 23:25:07 2023
daily database available for download (remote version: 26996)
Time: 4.7s, ETA: 0.0s [=====>] 58.82MiB/58.82MiB
Testing database: '/var/lib/clamav/tmp.9df8e3db09/clamav-959974bdc538c0682acdea8c508946f8.tmp-daily.cvd' ...
Database test passed.
daily.cvd updated (version: 26996, sigs: 2039824, f-level: 90, builder: raynman)
main database available for download (remote version: 62)
Time: 12.5s, ETA: 0.0s [=====>] 162.58MiB/162.58MiB
Testing database: '/var/lib/clamav/tmp.9df8e3db09/clamav-e0db0d25f4f0af0c5ac6b3ed33c88b1b.tmp-main.cvd' ...
Database test passed.
main.cvd updated (version: 62, sigs: 6647427, f-level: 90, builder: sigmgr)
bytecode database available for download (remote version: 334)
Time: 0.1s, ETA: 0.0s [=====>] 285.12KiB/285.12KiB
Testing database: '/var/lib/clamav/tmp.9df8e3db09/clamav-a7047dfcdeb1c6cf626863156e7f5343.tmp-bytecode.cvd' ...
Database test passed.
bytecode.cvd updated (version: 334, sigs: 91, f-level: 90, builder: anvilleg)
[mlabora@wwe ~]$
```

```
[mlabora@wwe ~]$ sudo freshclam
ClamAV update process started at Fri Aug 11 00:11:54 2023
daily.cvd database is up-to-date (version: 26996, sigs: 2039824, f-level: 90, builder: raynman)
main database available for download (remote version: 62)
Time: 10.5s, ETA: 0.0s [=====>] 162.58MiB/162.58MiB
Testing database: '/var/lib/clamav/tmp.f82ff37e81/clamav-26a7a4e64b0632b916682987ae34889c.tmp-main.cvd' ...
Database test passed.
main.cvd updated (version: 62, sigs: 6647427, f-level: 90, builder: sigmgr)
bytecode.cvd database is up-to-date (version: 334, sigs: 91, f-level: 90, builder: anvilleg)
[mlabora@wwe ~]$
```

Configuración de escaneos:

```
sudo touch /var/log/freshclam.log
sudo chmod 600 /var/log/freshclam.log
sudo chown clamav /var/log/freshclam.log
```

```
[mlabora@wwe ~]$: sudo chown clamav /var/log/freshclam.log
[mlabora@wwe ~]$: sudo freshclam -d
[mlabora@wwe ~]$: ls
administracion clamd.conf freshclam.conf
[mlabora@wwe ~]$: sudo systemctl status clamav-freshclam.service
● clamav-freshclam.service - ClamAV virus database updater
  Loaded: loaded (/usr/lib/systemd/system/clamav-freshclam.service; disabled; vendor preset: disabled)
  Active: inactive (dead)
    Docs: man:freshclam(1)
          man:freshclam.conf(5)
          https://docs.clamav.net/
[mlabora@wwe ~]$: sudo systemctl start clamav-freshclam.service
[mlabora@wwe ~]$: sudo systemctl status clamav-freshclam.service
● clamav-freshclam.service - ClamAV virus database updater
  Loaded: loaded (/usr/lib/systemd/system/clamav-freshclam.service; disabled; vendor preset: disabled)
  Active: active (running) since Fri 2023-08-11 19:55:11 EDT; 3s ago
    Docs: man:freshclam(1)
          man:freshclam.conf(5)
          https://docs.clamav.net/
  Main PID: 2026 (freshclam)
    Tasks: 1 (limit: 13620)
   Memory: 2.1M
      CGroup: /system.slice/clamav-freshclam.service
              └─2026 /usr/bin/freshclam -d --foreground=true

ago 11 19:55:11 wwe.com.uy systemd[1]: Started ClamAV virus database updater.
ago 11 19:55:11 wwe.com.uy freshclam[2026]: ClamAV update process started at Fri Aug 11 19:55:11 2023
ago 11 19:55:11 wwe.com.uy freshclam[2026]: WARNING: Can't query current.cvd.clamav.net
ago 11 19:55:11 wwe.com.uy freshclam[2026]: WARNING: Invalid DNS reply. Falling back to HTTP mode.
ago 11 19:55:11 wwe.com.uy freshclam[2026]: Trying to retrieve CVD header from https://database.clamav.net
ago 11 19:55:11 wwe.com.uy freshclam[2026]: WARNING: remote_cvthead: Download failed (6) WARNING: >
ago 11 19:55:11 wwe.com.uy freshclam[2026]: WARNING: Failed to get daily database version information
ago 11 19:55:11 wwe.com.uy freshclam[2026]: ERROR: check_for_new_database_version: Failed to find download URL
ago 11 19:55:11 wwe.com.uy freshclam[2026]: Trying again in 5 secs...
Lines: 1-21/21 (END)
```

Habilitamos:

```
[mlabora@wwe ~]$: sudo systemctl enable clamav-freshclam.service
Created symlink /etc/systemd/system/multi-user.target.wants/clamav-freshclam.service → /usr/lib/systemd/system/clamav-freshclam.service.
[mlabora@wwe ~]$: 
```

en el archivo freshclam.conf

Debemos descomentar las líneas

- LogTime - *Controla si se incluye la marca de tiempo en las entradas de registro*
- LogRotate - Rotación de registros, es recomendable para asegurarse de que los archivos de registro no crezcan indefinidamente y no consuman todo el espacio en disco.
- NotifyClamd - freshclam notificará a clamd(demonio) después de actualizar las definiciones de virus. Esto permitirá que clamd recargue la base de datos automáticamente después de una actualización.
- DatabaseOwner - Para establecer el usuario y el grupo propietario de los archivos y directorios relacionados con la base de datos de definiciones de virus y actualizaciones.
- UpdateLogFile - Aquí va la ruta completa al archivo de registro donde deseas que freshclam registre sus acciones y eventos relacionados con las actualizaciones de las bases de datos.

```
# Log time with each message.  
# Default: no  
LogTime yes
```

```
LogVerbose yes
```

```
# Rotate log file. Requires LogFileMaxSize  
# Default: no  
LogRotate yes
```

```
# Send the RELOAD command to clamd after a successful scan.  
# Default: /etc/clamd.d/scan.conf  
NotifyClamd yes
```

```
# defined in this option.  
# Default: clamupdate  
DatabaseOwner clamupdate
```

```
# Save all reports to a log file.  
#Default: enabled  
UpdateLogFile /var/log/freshclam.log
```

Creamos grupo y agregamos el usuario clamav al grupo clamav:

```
[mlabora@wwe etc]$ sudo gpasswd -a clamav clamav  
[sudo] password for mlabora:  
Sorry, try again.  
[sudo] password for mlabora:  
Añadiendo al usuario clamav al grupo clamav  
[mlabora@wwe etc]$ _
```

Agregamos a crontab la siguiente linea para buscar una nueva base de datos cada Domingo a las 2am => 0 02 * * 0

```
0 02 * * 0 /usr/local/bin/freshclam --quiet
```

```
~  
~  
~  
~
```

Realizamos un escaneo:

```
[mlabora@wwe log]$ sudo clamscan -r /home/mlabora/  
/home/mlabora/.bash_logout: OK  
/home/mlabora/.bash_profile: OK  
/home/mlabora/.bashrc: OK  
/home/mlabora/.zshrc: OK  
/home/mlabora/.bash_history: OK  
/home/mlabora/.vim/.netrwhist: OK  
/home/mlabora/administracion/administracion_usuarios.sh: OK  
/home/mlabora/administracion/.administracion_usuarios.sh.swp: OK  
/home/mlabora/.mysql_history: Empty file  
/home/mlabora/.lesshst: OK  
/home/mlabora/.config/htop/htoprc: OK  
/home/mlabora/freshclam.conf: OK  
/home/mlabora/clamd.conf: OK  
/home/mlabora/.viminfo: OK  
  
----- SCAN SUMMARY -----  
Known viruses: 8671679  
Engine version: 0.103.8  
Scanned directories: 5  
Scanned files: 13  
Infected files: 0  
Data scanned: 0.04 MB  
Data read: 0.02 MB (ratio 2.00:1)  
Time: 21.117 sec (0 m 21 s)  
Start Date: 2023:08:11 23:54:18  
End Date: 2023:08:11 23:54:39  
[mlabora@wwe log]$ _
```

Prueba con una detección de amenaza usando 2 archivos con características para que lo califique como sospechoso:

```
/home/mlabora/.viminfo: OK
/home/mlabora/a.sh: Eicar-Signature FOUND
/home/mlabora/a.txt: Eicar-Signature FOUND
/home/mdominguez: Can't open directory.
/home/lsciavoni: Can't open directory.
/home/lhernandez: Can't open directory.
/home/Administrador: Can't open directory.
/home/baseddedatos: Can't open directory.
/home/mathias: Can't open directory.
/home/clamav: Can't open directory.

----- SCAN SUMMARY -----
Known viruses: 8671679
Engine version: 0.103.8
Scanned directories: 6
Scanned files: 16
Infected files: 2
Total errors: 7
Data scanned: 0.04 MB
Data read: 0.02 MB (ratio 2.00:1)
Time: 19.342 sec (0 m 19 s)
Start Date: 2023:08:12 00:16:53
End Date: 2023:08:12 00:17:12
[mlabora@wwe ~]$ |
```

7 Procedimientos de respaldo y recuperación de datos

Para el servidor de Where we eat Realizaremos los respaldos del mismo, en un Fedora Server 36.

Fedora es conocido por adoptar tecnologías y software más nuevos antes que muchas otras distribuciones, es mantenido por la comunidad y respaldado por Red Hat.

Fedora se enfoca en la seguridad y adopta tecnologías como SELinux para fortalecer la protección del sistema, se adhiere a un estricto compromiso con el software libre y de código abierto y también cuenta con una sólida base de documentación y una comunidad amplia y activa.

```
[root@respaldo-enigma ssh]# cat /etc/fedora-release
Fedora release 36 (Thirty Six)
[root@respaldo-enigma ssh]#
```

-Creacion grupo ‘respaldos’ por si creamos en un futuro mas usuarios

y le agregamos usuario ‘respaldo’.

-Asignamos permisos de escritura y lectura al grupo ‘respaldos’

```
[root@respaldo-enigma ssh]# sudo groupadd respaldos
[root@respaldo-enigma ssh]# sudo usermod -aG respaldos respaldo
[root@respaldo-enigma ssh]# groups respaldo
respaldo : respaldo respaldos
```

```
[root@respaldo-enigma ssh]# ls -la ~/home/
total 0
drwxr-xr-x. 3 root      root      22 ago 27 11:34 .
dr-xr-xr-x. 18 root     root     235 oct 18 2022 ..
drwxrwx---. 2 respaldo respaldo  62 ago 27 11:34 respaldo
[root@respaldo-enigma ssh]# _
```

-Tenemos la ip 192.168.100.5 y configurado el puerto 50000 en ssh.

Prueba de transferencia para respaldo.

```
[mlabora@wwe-server ~]$ touch a.txt
[mlabora@wwe-server ~]$ holaquetal > a.txt
-bash: holaquetal: no se encontró la orden
[mlabora@wwe-server ~]$ echo holaquetal > a.txt
[mlabora@wwe-server ~]$ cat a
administracion/ a.txt
[mlabora@wwe-server ~]$ cat a.txt
holaquetal
[mlabora@wwe-server ~]$ scp -P 50000 a.txt respaldo@192.168.100.5:/home/respaldo
The authenticity of host '[192.168.100.5]:50000 ([192.168.100.5]:50000)' can't be established.
ECDSA key fingerprint is SHA256:QR71FCKGNXmmPUzboBcyDbeliT5R0upX9xJl0ESbnQc.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[192.168.100.5]:50000' (ECDSA) to the list of known hosts.
respaldo@192.168.100.5's password:
a.txt                                              100%   11      1.8KB/s   00:00
[mlabora@wwe-server ~]$ |
```

Resultado:

```
[respaldo@respaldo-enigma ~]$ cd /home/respaldo/
[respaldo@respaldo-enigma ~]$ ls
a.txt
[respaldo@respaldo-enigma ~]$ cat a.txt
holaquetal
[respaldo@respaldo-enigma ~]$ _
```

Con las configuraciones anteriores realizadas, procedemos a detallar cómo se realizarán los respaldos y la frecuencia de los mismos:

Utilizaremos RSYNC para realizar la transferencia de archivos-

Ejemplo de cómo se realizará un respaldo:

```
rsync -avzh -e ssh -p 50000 archivorespaldo.gz
respaldo@192.168.100.5:/home/respaldo/respaldosWWeat
```

Utilizaremos CRON que es un programador de tareas para agendar y ejecutar respaldos mensuales, semanales y diarios.

Respaldo Mensual (Realizaremos este respaldo todos los comienzos de mes –5 de cada mes–):

Configuración de MySQL (MariaDB):

/etc/my.cnf
/etc/my.cnf.d/
/var/lib/mysql/

Configuración de ClamAV:

/etc/clamd.conf
/etc/freshclam.conf
/var/lib/clamav/

Configuración de Grafana:

/etc/grafana/
/var/lib/grafana/

Configuración de PHP:

/etc/php.ini
/etc/php.d/
/var/lib/php/

Configuración de Apache:

/etc/httpd/
/var/www/html/

Logs:

/var/log/messages
/var/log/syslog

Respaldo Semanal (Lo realizaremos semanalmente los días domingo):

Configuración de SSH (sshd):

/etc/ssh/
/var/log/secure

Scripts personalizados en /etc/skel/administración:
/etc/skel/administracion/

Respaldo Diario (Lo realizaremos todos los días en horas de la madrugada 3am):

Configuraciones de red:
/etc/sysconfig/network-scripts/
/etc/sysconfig/network/
/etc/hosts
/etc/resolv.conf

Configuraciones de usuarios, grupos, etc.:
/etc/passwd
/etc/shadow
/etc/group
/etc/sudoers

Logs:
/var/log/mysql/error.log
/var/log/mysql/mysql.log
/var/log/clamav/clamav.log
/var/log/clamav/freshclam.log
/var/log/httpd/error_log
/var/log/httpd/access_log
/var/log/secure
/var/log/grafana/grafana.log
/var/log/lastlog

Bibliografía

- Razones Por Las Que AlmaLinux Es La Mejor Alternativa A CentOS (07 de mayo de 2023)
Recuperado de:
<https://www.dz-techs.com/es/reasons-choose-almalinux-over-centos>
- ¿Qué es AlmaLinux? (s.f)
Recuperado de: <https://www.k2webhost.com/blog/que-es-almalinux/>
- (s.f)
Recuperado de:
<https://www.microsoft.com/es-xl/windows/business/compare-windows-11>
- windows-11-enterprise (s.f)
Recuperado de:
<https://www.microsoft.com/en-us/microsoft-365/windows/windows-11-enterprise>
- OpenLogic Support (s.f)
Recuperado de: <https://www.openlogic.com/>
- Recuperación para MySQL, (s.f)
Recuperado de: <https://www.officerecovery.com/es/mysql/licensing.htm>
- Gestión de licencias, (s.f)
Recuperado de:
<https://docs.oracle.com/es-ww/iaas/Content/LicenseManager/Concepts/licensemanageroverview.htm>
- ¿Qué es Grafana? 13 de Mayo de 2022, Redhat
Recuperado de: <https://www.redhat.com/es/topics/data-services/what-is-grafana>
- Licencias | Laboratorios Grafana, (s.f.). Grafana.
Recuperado de: <https://grafana.com/licensing/>
- Opciones de soporte de Grafana Cloud | Documentación de Grafana Cloud (s.f.). Grafana.
Recuperado de:
<https://grafana.com/docs/grafana-cloud/account-management/support/>
- Canal discord ClamAV (s.f)
Recuperado de: <https://discord.com/invite/6vNAqWnVgw>
- Antivirus ClamAV para linux (s.f)
Recuperado de: <https://weblinus.com/antivirus-clamav-para-linux/>
- Configuración, (s.f)
Recuperado de: <https://docs.clamav.net/manual/Usage/Configuration.html>
- Como Instalar php 8, (s.f)
Recuperado de:<https://redessy.com/como-instalar-php-8-en-centos-8-rhel-8/>



ANEP



UTU

DIRECCIÓN GENERAL
DE EDUCACIÓN
TÉCNICO PROFESIONAL



Instituto Tecnológico Superior
UTU

HOJA TESTIGO

MATERIA: Sistemas Operativos 3

Nombre del Profesor: Christian Barrios

Nota Final