LAMP Stack en Fedora

Despliegue de Aplicaciones Web

José Juan Sánchez Hernández

Curso 2023/2024

Índice

Índice de figuras

Índice de cuadros

1 LAMP Stack en Fedora

LAMP es el acrónimo usado para describir un sistema de infraestructura de Internet que usa las siguientes herramientas:

- Linux (Sistema Operativo)
- Apache (Servidor Web)
- MySQL/MariaDB (Sistema Gestor de Bases de Datos)
- PHP (Lenguaje de programación)

2 Linux

En esta prática vamos a utilizar el sistema operativo Fedora.

Fedora es una sistema operativo de código abierto basado en Linux, que es mantenido por la comunidad y que está patrocinado por Red Hat.

2.1 Gestor de paquetes dnf

`dnf` (*Dandified Yum*) es un gestor de paquetes para distribuciones GNU/Linux badadas en RPM (*Red Hat Package Manager*). `dnf` es la evolución de `yum` *Yellowdog Updater, Modified*.

2.1.1 Actualizar los paquetes del sistema

Para actualizar los paquetes del sistema podemos utilizar cualquiera de estos comandos:

```
1  sudo dnf update
```

```
1  sudo dnf upgrade
```

En en gestor de paquetes `dnf`, las opciones `update` y `upgrade` realizan la misma acción.

Podemos utilizar una versión abreviada.

```
1  sudo dnf up
```

Si sólo queremos actualizar un paquete del sistema podemos utilizar:

```
1  sudo dnf update <nombre_paquete>
```

2.1.2 Buscar paquetes

```
1  sudo dnf search <nombre_paquete>
```

2.2 Instalar un paquete

```
1  sudo dnf install <nombre_paquete>
```

2.2.1 Eliminar un paquete

```
sudo dnf autoremove <nombre_paquete>
```

Para limpiar los archivos temporales de un repositorio que haya sido eliminado o deshabilitado podemos utilizar la opción `clean`.

```
sudo dnf clean all
```

2.2.2 Obtener un listado de todos los paquetes (instalados y disponibles)

Para obtener un listado de los paquetes que están instalados en el sistema y los paquetes que están disponibles en los repositorios para instalar, podemos utilizar cualquiera de estos dos comandos:

```
sudo dnf list all
```

```
sudo dnf list
```

2.2.3 Obtener un listado de los paquetes instalados

```
sudo dnf list installed
```

2.2.4 Obtener información de un paquete

```
sudo dnf info <nombre_paquete>
```

Ejemplo:

```
sudo dnf info mysql-server
```

3 Apache

3.1 Instalación del servidor web Apache

Instalamos el paquete del servidor web Apache.

```
1  sudo dnf install httpd -y
```

Después de la instalación del servidor hay que iniciar el servicio.

```
1  sudo systemctl start httpd
```

Y habilitar el servicio para que se inicie automáticamente después de cada reinicio.

```
1  sudo systemctl enable httpd
```

Ahora podemos comprobar el estado del servicio para verificar que se está ejecutando.

```
1  sudo systemctl status httpd
```

4 MySQL Server

4.1 Instalación del sistema gestor de bases de datos MySQL Server

Instalamos el paquete de MySQL Server.

```
sudo dnf install mysql-server -y
```

Después de la instalación del servidor hay que iniciar el servicio.

```
sudo systemctl start mysqld
```

Y habilitar el servicio para que se inicie automáticamente después de cada reinicio.

```
sudo systemctl enable mysqld
```

Ahora podemos comprobar el estado del servicio para verificar que se está ejecutando.

```
sudo systemctl status httpd
```

5 PHP

5.1 Instalación de PHP

Instalamos el intérprete de PHP con el comando:

```
sudo dnf install php -y
```

Podemos comprobar que PHP se ha instalado correctamente ejecutando el siguiente comando:

```
php -v
```

Instalamos la extensión de PHP para conectar con MySQL.

```
sudo dnf install php-mysqlnd -y
```

Después de la instalación es necesario reiniciar el servicio de Apache para que se apliquen los cambios.

```
sudo systemctl restart httpd
```

6 Security Enhanced Linux (SELinux)

SELinux (Security-Enhanced Linux) es un módulo de seguridad que está integrado en el kernel de Linux. Actualmente, se incluye en muchas distribuciones Linux como Fedora, Red Hat Enterprise Linux (RHEL) y CentOS entre otras.

Control de Acceso Discrecional

La política de acceso estándar en los sistemas UNIX es conocida como el Control de Acceso Discrecional o DAC (*Discretionary Access Control*), y se basa en restringir el acceso a los objetos del sistema (archivos, directorios, procesos, etc.) en función del usurio, el grupo y los permisos de acceso (lectura, escritura y ejecución).

El Control de Acceso Discrecional o DAC tiene el inconveniente de que no permite crear políticas de seguridad más específicas.

Control de Acceso Obligatorio y Control de Acceso Basado en Roles

SELinux, incluye políticas de Control de Acceso Obligatorio o MAC (*Mandatory Access Control*) y Control de Acceso Basado en Roles o RBAC (*Role-Based Access Control*).

En SELinux, cada objeto (archivos, directorios, procesos, etc.) tiene un **contexto de seguridad** (*SELinux context*) que se utiliza para aplicar políticas de seguridad y definir reglas de acceso.

El contexto de seguridad está formado por los campos: usuario, rol, tipo y nivel de seguridad, y siguen la siguiente estructura `usuario_u:rol_r:tipo_t:nivel`. Donde:

- `usuario_u`: Indica el usuario al que pertenece el objeto. **Ejemplo:** `unconfined_u` se utliza para un usuario que no está restringido por políticas de seguridad más estrictas.
- `rol_r`: Indica el rol del usuario, que define el conjunto de permisos y acciones que el usuario o el proceso pueden realizar. **Ejemplo:** `object_r` se utiliza para archivos y directorios.
- `tipo_t`: Define el tipo del objeto, lo que determina las políticas de seguridad aplicables a ese objeto. **Ejemplo:** `httpd_sys_content_t` será el tipo de contexto que necesitamos configurar en el directorio `/var/www/html`.
- `nivel`: Indica el nivel de seguridad, que se utiliza en sistemas con múltiples niveles de seguridad. **Ejemplo:** `s0` será el nivel de seguridad más bajo.

Para seguir profundizando en este tema se recomienda la lectura del documento Uso de SELinux de la página oficial de Red Hat.

6.1 Comprobar el estado de SELinux

El comando `sestatus` nos permite conocer cuál es el estado de SELinux.

```
$ sestatus

SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             targeted
Current mode:                   enforcing
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Memory protection checking:     actual (secure)
Max kernel policy version:      33
```

6.2 Configuración del tipo de contexto al contenido del directorio `/var/www/html`

En Fedora es necesario cambiar recursivamente el tipo de contexto de seguridad SELinux de todos los archivos y directorios que hay dentro del directorio `/var/www/html/` y configurarlo como `httpd_sys_content_t`, para que el servidor web Apache pueda acceder a ellos de forma segura.

```
sudo chcon -R --type=httpd_sys_content_t /var/www/html/
```

Una vez que hemos modificado el tipo de contexto podemos comprobar que se ha realizado de forma correcta utilizando el parámetro `-Z` del comando `ls`.

```
ls -Z /var/www/html/
```

7 Errores que pueden aparecer durante la instalación

7.1 Error `Cannot allocate memory`

Si durante la instalación obtiene el siguiente mensaje de error:

```
[Errno 12] Cannot allocate memory
The downloaded packages were saved in cache until the next successful
    transaction.
You can remove cached packages by executing 'dnf clean packages'.
```

Es posible que necesite incrementar la cantidad de memoria de RAM de la instancia.

Una posible solución es detener de forma temporal los servicios que estén haciendo un uso intensivo de memoria RAM. Una vez que detenga los servicios puede volver a intentar realizar la instalación y si la operación termina con éxito, puede volver a iniciar los servicios que había detenido.

7.2 Error `Access denied`

Revisa la configuración del tipo contexto de seguridad de SELinux del contenido que hay en el directorio `/var/www/html`. Recuerda que tiene que estar configurado como `httpd_sys_content_t`.

8 Referencias

- How to Install Apache, MySQL, and PHP (LAMP) Stack on Fedora 34. Francis Ndungu.
- Fedora
- DNF (Dandified Yum). Wikipedia
- SELinux. Wikipedia
- Uso de SELinx. Red Hat
- Control de acceso discrecional o DAC (*Discretionary access control*)
- Control de acceso obligatorio o MAC (*Mandatory access control*). Wikipedia
- Control de acceso basado en roles o RBAC (*Role-based access control*)

9 Licencia