Configuración de Fail2ban

Fail2ban es un servicio que hace un sondeo en la carpeta /var/logs y analiza el contenido de los archivos para ver la cantidad de autenticaciones erróneas y proceder a banear IPs teniendo en cuenta como lo configuremos.

La principal finalidad de Fail2ban es evitar ataques que traten de conseguir nuestra contraseña por fuerza bruta.

Instalación y arranque

Fail2ban no tiene su propio paquete, se encuentra dentro del conjunto de paquetes extendidos epel-release, así que este es el paquete que tenemos que instalar.

sudo dnf install epel-release

ahora sí podríamos hacer la búsqueda de fail2ban

dnf search fail2ban

y efectivamente lo encuentra, asía ue podemos instalarlo

sudo dnf install fail2ban

El servicio comienza inactivo y deshabilitado, (podemos comprobarlo com un systemctl status fail2ban), así que lo habilitamos e iniciamos respectivamente:

sudo systemctl enable fail2ban

sudo systemctl start fail2ban

Configuración

Para configurar los jails de fail2ban se hará desde un archivo de copia local igual al archivo de configuración /etc/fail2an/jail.config (no se hace en este archivo directamente ya que fail2ban lo desaconseja pues en sus actualizaciones sobreescribe el fichero).

Para ello haremos la copia:

(ubicados en la carpeta /etc/fail2ban) sudo cp -a jail.conf jail.local

Y modificaremos el fichero jail.local:

En la zona [sshd], debajo de port pondremos un enabled=true, y en port tendremos que poner el puerto que estamos utilizando.

También podemos modificar las distintas variables para modificar la configuración, por ejemplo maxretry tiene en cuenta el máximo número de intentos de conexión.

Para desbanear ip utilizaremos el siguiente comando:

fail2ban-client set <servicio> unbanip <ip>

y para ver la lista de IPs baneadas, sudo fail2ban-client status <servicio>

Nota ejemplo: en nuestro caso que estamos comprobando con el servicio sshd, servicio sería sshd.