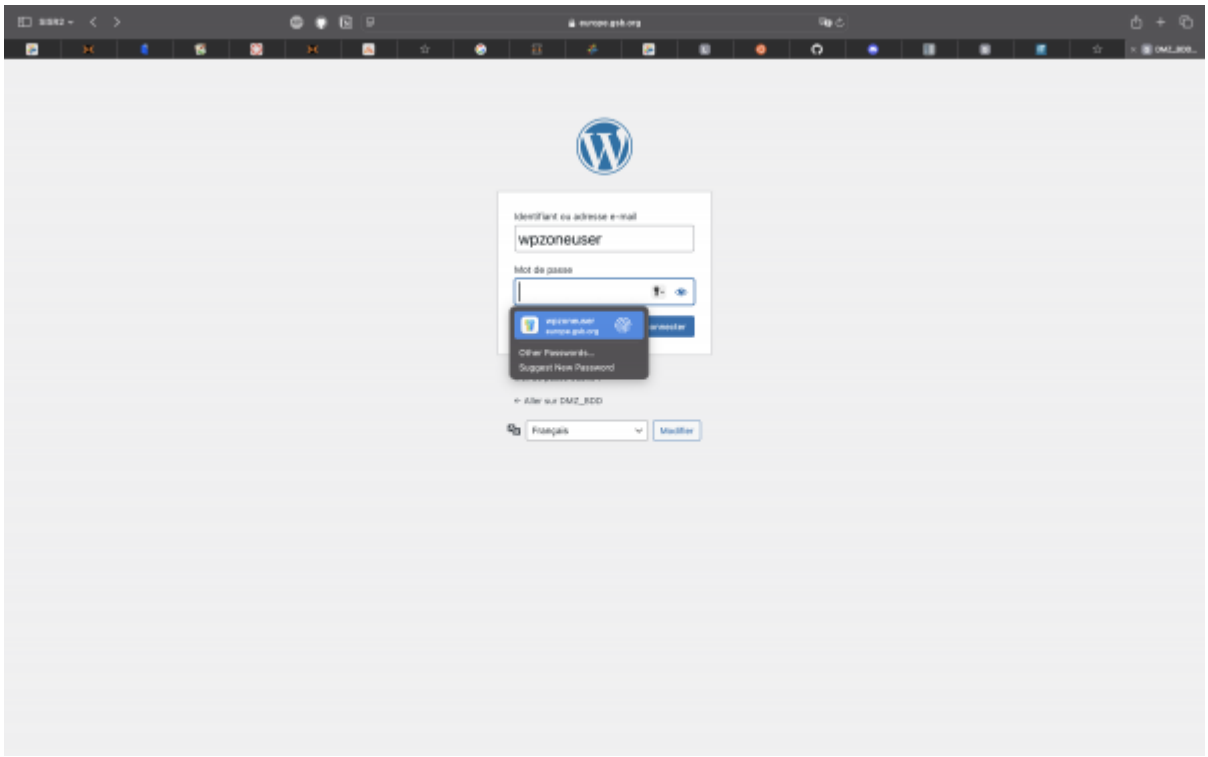
Installation Fail2ban pour wordpress

Wordpress

Pour configurer Fail2ban pour wordpress, on se connecte en ssh depuis notre conteneur ou se trouve nos sites wordpress dans notre cas ce sera 10.31.200.80 puis on installe Fail2ban.

```
apt update
apt install fail2ban
```

Ensuite on installe un plugin sur le site de wordpress pour que wordpress génère des fichiers de logs fail2ban. Pour se faire nous devons nous connecter avec le compte admin de notre site wordpress.



Modifiez le fichier **wp-config.php** pour votre installation Wordpress le chemin sera **/home/htdocs/gsb/wordpress/wp-config.php**

```
// Make sure we're not using the short ("wp") tag
```

```
define('WP_FAIL2BAN_SYSLOG_SHORT_TAG', false);

// Don't include the HTTP host in the tag
define('WP_FAIL2BAN_SYSLOG_TAG_HOST', false);

/* That's all, stop editing! Happy blogging. */
```

Maintenant on retourne dans le conteneur de l'adresse 10.31.200.80. Nous passons du côté de la configuration Fail2ban, le plugin WordPress WP-Fail2ban comporte un nouveau filtre pour notre Fail2ban, on va le trouver dans le répertoire du plugin dans WordPress chemin_wordpress/wp-content/plugins/wp-fail2ban:

```
root@Europe-web:/home/htdocs/gsb/wordpress/wp-content/plugins/wp-fail2ban/filters.d# ls
wordpress-extra.conf  wordpress-hard.conf  wordpress-soft.conf
root@Europe-web:/home/htdocs/gsb/wordpress/wp-content/plugins/wp-fail2ban/filters.d#
```

Puis on copie les fichiers wordpress-hard.conf et wordpress-soft.conf dans le /etc/fail2ban/filter.d

```
cp home/htdocs/gsb/wordpress/wp-content/plugins/wp-
fail2ban/filters.d/wordpress-hard.conf /etc/fail2ban/filter.d

cp home/htdocs/gsb/wordpress/wp-content/plugins/wp-
fail2ban/filters.d/wordpress-soft.conf /etc/fail2ban/filter.d
```

Une fois que nous avons le filtre permettant de surveiller ce qui nous intéresse, à savoir les erreurs d'authentifications dans WordPress, il nous faut maintenant créer une nouvelle jail (prison) dans Fail2ban. On commence par se rendre dans le fichier de configuration des jails Fail2ban, **/etc/fail2ban/jail.d**

```
nano wordpress.conf

[wordpress-soft]
enabled = true
filter = wordpress-soft
backend = systemd
journalmatch = SYSLOG_IDENTIFIER=wordpress
logpath = /var/log/auth.log
maxretry = 3
port = http,https
```

Redémarrer le logiciel: **systemctl fail2ban**

Pour vérifier qu'une adresse IP à bien été banni on utilise cette commande :

```
fail2ban-client status wordpress-soft
```

Pour se faire débannir notre adresse IP on utilise cette commande:

```
fail2ban-client set wordpress unbanip 10.187.20.???
```

nextcloud fail2ban

fail2ban-client set wordpress-soft unbanip 10.187.20.196