Cryptage des mots de passe

Cryptage des mots de passe

Cryptage des mots de passe dans Pandora FMS

Pandora FMS permet de chiffrer les mots de passe que vous stockez dans la base de données. La clé de chiffrement est générée à partir d'un mot de passe fourni par l'utilisateur et n'est pas enregistrée dans la base de données (*ni le mot de passe ni la clé*), de sorte que les mots de passe ne peuvent pas être récupérés à partir d'un vidage de la base de données. Une fois que l'utilisateur a configuré le mot de passe, le cryptage fonctionne de manière transparente pour l'utilisateur.

Si vous perdez le mot de passe fourni par l'utilisateur, vous ne pourrez pas récupérer les mots de passe stockés dans la base de données Pandora FMS. Enregistrez-le dans un endroit sûr ou sauvegardez les fichiers `config.php` et `pandora_server.conf`.

Détails techniques

Les mots de passe sont chiffrés à l'aide du chiffrement Rijndael avec des blocs de 128 bits en mode ECB. Une clé de 256 bits est générée au démarrage à partir du MD5 du mot de passe configuré par l'utilisateur.

Configuration d'une nouvelle installation Pandora FMS

Pour activer le chiffrement des clés, le mot de passe doit être configuré à la fois sur le serveur Pandora FMS et sur la console.

Les étapes à suivre pour le chiffrement sont les suivantes :

- Arrêter le serveur, à la fois sur la Métaconsole et sur le nœud.
- Mettre à jour les encryption_passphrase dans`/etc/pandora/pandora_server.conf` et `/var/www/html/pandora_console/include/config.php` à la fois sur le nœud et sur la Métaconsole.

```
$config["encryption_passphrase"]="your encryption passphrase";
```

- Lancer le *script* de chiffrement à la fois sur le nœud et sur la Métaconsole.

```
/usr/bin/pandora_encrypt_db /etc/pandora/pandora_server.conf
```

```
N'oubliez pas de redémarrer le serveur Pandora FMS après avoir effectué les
modifications et lancé le //script//.
```

Configuration dans une installation existante de Pandora FMS

Cette section ne doit être prise en compte que si vous souhaitez passer de la version 743 à la version 744. Si ce n'est pas le cas, le chiffrement doit être effectué comme s'il s'agissait d'un nouveau chiffrement.

Configurez le chiffrement des mots de passe en suivant les étapes décrites pour une nouvelle installation. Les nouveaux mots de passe entrés dans la console Pandora FMS seront désormais stockés dans la base de données. Cependant, vous devrez chiffrer les mots de passe existants. Pour ce faire, procédez comme suit :

- Arrêter le serveur, à la fois sur la Métaconsole et sur le nœud.
- Lancer le *script* de décryptage à la fois sur le nœud et sur la Métaconsole :

```
/usr/bin/pandora_encrypt_db -d -m /etc/pandora/pandora_server.conf
```

- Lancer le *script* de chiffrement à la fois sur le nœud et sur la Métaconsole.

```
/usr/bin/pandora_encrypt_db /etc/pandora/pandora_server.conf
```

- Redémarrer le serveur de la Métaconsole et du nœud.

Le *script* ne permettra pas de s'exécuter une deuxième fois, sinon les mots de passe seraient corrompus.

Il est important de noter que le paramètre -m sera obligatoire pour l'ajouter afin de déchiffrer uniquement les anciens mots de passe. Si vous n'ajoutez pas ce paramètre aux bases de données cryptées ci-dessus, les mots de passe seront perdus.

Changer le mot de passe de chiffrement

Il est possible de changer le mot de passe de chiffrement si celui-ci a été compromis. Vous devez d'abord déchiffrer les mots de passe stockés dans la base de données :

```
/usr/bin/pandora_encrypt_db -d /etc/pandora/pandora_server.conf
```

Ensuite, après avoir changé le mot de passe de chiffrement (comme décrit dans la section Configuration dans une nouvelle installation), vous pouvez le chiffrer à nouveau :

```
/usr/bin/pandora_encrypt_db /etc/pandora/pandora_server.conf
```

À partir de 7.0 NG 739, le magasin_d_informations_d_identification. Reportez-vous à la section suivante pour terminer correctement ce processus.

Gestionnaire d'identifiants :

Si vous disposez d'une base de données chiffrée, pour pouvoir continuer à utiliser le gestionnaire d'informations d'identification sans perdre de données, vous *devrez tout décrypter* sauf la table tcredential_store

Pour ce faire, exécutez les commandes suivantes :

```
/usr/bin/pandora_encrypt_db -d -c /etc/pandora/pandora_server.conf
```

Ce qui le rendra déchiffré.

Une fois déchiffré, il sera à nouveau chiffré :

```
/usr/bin/pandora_encrypt_db /etc/pandora/pandora_server.conf
```

Si vous souhaitez simplement chiffrer à partir de zéro, il vous suffit d'exécuter la dernière commande.

Changer le mot de passe de chiffrement

Il est recommandé de garder chiffré tout mot de passe stocké dans Pandora FMS.

- Arrêtez le serveur, à la fois sur la Métaconsole et sur le nœud.
- Commenter encryption_passphrase dans`/etc/pandora/pandora_server.conf` et `/var/www/html/pandora_console/include/config.php` à la fois sur le nœud et sur la Métaconsole.

```
# $config["encryption_passphrase"]="your encryption passphrase";
```

- Lancer le *script* de décryptage à la fois sur le nœud et sur la Métaconsole.

```
/usr/bin/pandora_encrypt_db -d -e /etc/pandora/pandora_server.conf
```

```
N'oubliez pas de redémarrer le serveur Pandora FMS après avoir effectué les
modifications et lancé le //script//.
```

Retour à l'index de documentation Pandora FMS.