



Cryptage du mot de passe



m:
<https://pandorafms.com/manual/!current/>
manent link:
https://pandorafms.com/manual/!current/fr/documentation/pandorafms/technical_annexes/08_password_encryption
24/06/10 14:36





Cryptage du mot de passe

Pandora FMS vous permet de crypter les mots de passe stockés 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 stockée 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 défini le mot de passe, le cryptage fonctionne de manière transparente pour l'utilisateur.

Si le mot de passe fourni par l'utilisateur est perdu, vous ne pourrez pas récupérer les mots de passe stockés dans la base de données de Pandora FMS. Sauvegardez dans un endroit sûr ou faites une sauvegarde (*backup*) des fichiers `config.php` et `pandora_server.conf`.

Détails techniques

Les mots de passe sont cryptés en utilisant le cryptage 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 défini par l'utilisateur.

Configuration dans une nouvelle installation du Pandora FMS

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

Les étapes du cryptage sont les suivantes:

- Arrêtez le serveur, à la fois dans le Command Center (Metaconsole) et dans les nodes.
- Mise à jour des champs `encryption_passphrase` dans `/etc/pandora/pandora_server.conf` et `/var/www/html/pandora_console/include/config.php`, à la fois dans Command Center (Metaconsole) et dans nodes.

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

- Lancez le cryptage *script* dans le Command Center (Metaconsole) et les nodes.

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

Le serveur Pandora FMS doit être redémarré une fois que les changements ont été effectués et que le *script* a été lancé.

Modification du mot de passe de cryptage

Il est possible de modifier le mot de passe de cryptage au cas où il aurait été compromis. Vous devez d'abord décrypter 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 cryptage (comme décrit dans la section [configuration sur une nouvelle installation](#)), vous pouvez le crypter à nouveau :

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

À partir de la version 7.0 NG 739, le [secure credential manager](#) est inclus. Veuillez vous référer à la section suivante pour mener à bien ce processus.

Gestionnaire de justificatifs:

Si vous avez une base de données cryptée, afin de continuer à utiliser le gestionnaire de justificatifs d'identité sans perdre de données *décrypter tout* sauf la table `tcredential_store`.

Pour ce faire, exécutez les commandes suivantes:

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

Le serveur Pandora FMS doit être redémarré une fois que les changements ont été effectués et que le *script* a été lancé.

Une fois décrypté, il sera recrypté à nouveau:

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

Si vous souhaitez uniquement crypter à partir de zéro, exécutez simplement la dernière commande.

Suppression du mot de passe de cryptage

Il est recommandé de crypter tous les mots de passe stockés dans Pandora FMS.

- Arrêtez le serveur, à la fois dans le Command Center (Metaconsole) et dans les nodes.
- Lancez le décryptage *script* dans le Command Center (Metaconsole) et les nodes.

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

- Commentaire `encryption_passphrase` dans `/etc/pandora/pandora_server.conf` et `/var/www/html/pandora_console/include/config.php` à la fois dans Command Center (Metaconsole) et dans nodes.

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

Le serveur Pandora FMS doit être redémarré une fois que les changements ont été effectués et que le *script* a été lancé.

[Retour à l'index de la documentation du Pandora FMS](#)