パスワード暗号化

パスワード暗号化

Pandora FMS ドキュメント一覧に戻る

Pandora FMS でのパスワード暗号化

Pandora FMS はデータベース上のパスワードの暗号化に対応しています。暗号化キーは、ユーザが用意するパスフレーズから生成され、(キーやパスフレーズも含め)データベースには保存されません。これにより、データベースのダンプからパスワードを再現することはできません。パスフレーズを設定すると、暗号化がユーザに透過的に動作します。

パスフレーズを無くすとPandora FMS データベースに保存されたパスワードは利用できなくなります。安全な場所に置くか、config.php および pandora_server.conf をバックアップしてください。

技術詳細

パスワードは、128bit の Rijndael cipher の ECB モードを使って暗号化しています。パスフレーズの MD5 から、最初に 256bit のキーが生成されます。

新規インストールの Pandora FMS での設定

パスワード暗号化を有効化するには、Pandora FMS サーバと Pandora FMS コンソール双方でパスフレーズを設定する必要があります。

暗号化の手順は次の通りです。

- メタコンソールとノードサーバの両方を停止します。
- /etc/pandora/pandora_server.conf 内の encryption_passphrase および、ノード および メタコンソール 双方の /var/www/html/pandora_console/include/config.php を更新します。

```
$config["encryption_passphrase"]="あなたの暗号化パスフレーズ";
```

- ノード および メタコンソール 両方の暗号化スクリプトを起動します。

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

設定変更後は、Pandora FMS サーバを忘れずに再起動して

ください。

すでにインストール済の Pandora FMS での設定

この章は、バージョン 743 からバージョン 744 に更新する
場合にのみです。それ以外の場合は、新規の暗号化です。

新規インストールの Pandora FMS の手順に従って暗号化パスワード設定をします。ここでPandora FMS コンソールで任意の新たなパスワードが設定され、データベースに暗号化したものが保存されます。ただし、既存のパスワードも暗号化する必要があります。そのためには、次の手順を実行します。

- メタコンソール と ノード 双方を停止します。
- メタコンソール および ノード の復号化スクリプトを実行します。

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

- ノード および メタコンソール 双方の暗号化スクリプトを実行します。

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

- メタコンソールおよびノードサーバを再起動します。

スクリプトは 2回実行できません。2回実行するとパスワードが破損します。

古いパスワードを復号化するときのみ、-m パラメータを追
加する必要があることに注意してください。暗号化された
データベースにこのパラメータが追加されない場合、パス
ワードが失われます

暗号化パスワードの変更

暗号化パスワードは、漏えいしてしまった場合などは変更することができます。最初に、データベース内のパスワードを復号化する必要があります。

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

そして、(新規 Pandora FMS インストール時の設定で説明した方法で)パスワードを変更後、再度暗号化します。

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

7.0NG 739 以降には、安全な認証管理が含まれています。

認証情報管理:

暗号化データベースがある場合、データを失うことなく認証情報管理を使い続けることができるようにするには、tcredential_store テーブルを除いてすべての暗号を解除します。

そのためには、以下のコマンドを実行します。

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

全ての暗号化が解除されます。

暗号化を解除したら、再度暗号化を行います。

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

初回の暗号化では、最後のコマンドを実行します。

暗号化パスワードの削除

Pandora FMS に保存されているパスワードは、全体を暗号化しておくことをお勧めします。

- メタコンソール と ノード 双方のサーバを停止します。
- メタコンソール と ノード 双方の /etc/pandora/pandora_server.conf および /var/www/html/pandora_console/include/config.php の encryption_passphrase をコメントアウトします。

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

- ノード および メタコンソール で復号化スクリプトを実行します。

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

変更を加えてスクリプトを実行した後は、Pandora FMS サーバを再起動することを忘れないでください。

Pandora FMS ドキュメント一覧に戻る