Pandora FMS のための SELinux 設定

Pandora FMS のための SELinux 設定

Pandora FMS ドキュメント一覧に戻る

概要

Pandora FMS では、インストールは常に Security-Enhanced Linux (SELinux) を無効にして行う必要があります。 インストール後、環境によって有効にする必要がある場合の CentOS 7 での設定について詳しく説明します。

CentOS 7

Audit2allow のインストール

CentOS 7 はまもなくサポート終了(EOL)になります。 *このドキュメントは過去の記録のために保持しています.*

Audit2allow を利用したルールを作成します。これは必要なアクションを許可する役割を持ちます。

ポリシーのルール作成を開始する前に、Audit2allow を使用できるようにいくつかのパッケージをインストールする必要がある場合があります root または同等の権限でコマンドラインから入力します (コマンドの先頭に sudo を付けます):

```
yum install selinux-policy-devel -y
yum install policycoreutils-python -y
```

SELinux ディレクトリの場所

CentOS 7 はまもなくサポート終了(EOL)になります。 *このドキュメントは過去の記録のために保持しています.*

SELinux が返すエラーは、以下にあります。

- /var/log/audit/audit.log
- /var/log/messages

重要:

バージョン 747 までは、監査ログのパスは /var/log/audit/audit.log です。

OUM からアップデートした場合は、logrotate ファイルを修正する必要があります。

確認をしやすくするために、すでに出ているログを削除し新たなログが出るまで待つことを強くお勧めします。

syslog を停止します (rsyslog の場合もあります)

```
# /etc/init.d/syslog stop
```

audit.log とシステムのメッセージログファイルを削除します。

```
# rm /var/www/html/pandora_console/log/audit.log /var/log/messages
```

syslog を再開します。

```
# /etc/init.d/syslog start
```

SELinux 設定

CentOS 7 はまもなくサポート終了(EOL)になります。 *このドキュメントは過去の記録のために保持しています.*

SELinux を希望の内容で設定するには、設定ファイルを編集します。

```
# This file controls the state of SELinux on the system.
# SELinux= can take one of these three values:
#     enforcing - SELinux security policy is enforced.
#     permissive - SELinux prints warnings instead of enforcing.
#     disabled - No SELinux policy is loaded.
SELinux=enforcing
# SELinuxTYPE= can take one of these two values:
#     targeted - Targeted processes are protected,
#     mls - Multi Level Security protection.
SELinuxTYPE=targeted
```

プログラムの実行に制限を付けるには SELinux を “enforcing” に設定します(SELinux での実行制限は audit.log で確認します)。別のオプションとしては SELinux を “permissive” に設定します。この場合、実行は制限されませんが audit.log ファイルにエラーが記録されます。

ポリシールールを作成するためのエントリーの検索

CentOS 7 はまもなくサポート終了(EOL)になります。 *このドキュメントは過去の記録のために保持しています.*

最新のログを見るにはつぎのようにします。

```
# tail -f /var/www/html/pandora_console/log/audit.log /var/log/messages
```

次のようないくつかのエラーがみつかります。

```
 # type=AVC msg=audit(1431437562.755:437): avc:  denied  { write } for  pid=1835
comm="httpd" name="collections" dev=dm-0 ino=266621
scontext=unconfined_u:system_r:httpd_t:s0
tcontext=system_u:object_r:var_spool_t:s0 tclass=dir
```

これらのエラーを SELinux ルールに変換します。

```
 # grep collections /var/www/html/pandora_console/log/audit.log | audit2allow -M
pandora
```

実行すると 2つの新たなファイルが作成されます。

```
- pandora.pp
- pandora.te
```

新たなルールを有効化するには、次のようにします。

```
# sudo semodule -i pandora.pp
```

エラーが出たものをルールに追加する対応を繰り返します。その後、SELinux からエラーの出力がなくなります。

Pandora FMS の適切な動作に必要なルール

CentOS 7 はまもなくサポート終了(EOL)になります。 *このドキュメントは過去の記録のために保持しています.*

Pandora FMS が実行するすべてのサービスが正しく動作するようにしたい場合は、次の操作を許可するいくつかのルールを作成する必要があります。

- コレクションの作成、更新、削除

- プログラムタスクによるメール送信 (cronジョブ)

- エージェントのリモート設定

逆にいうとSELinux はこれらの操作に関連するアクションをブロックします。

SELinux が有効化された状態で Pandora FMS を利用するためのルールを追加するには、次のように

します。

```
# grep -e data_in -e collections -e var_spool_t -e zip -e md5 -e denied
/var/log/audit/audit.log | audit2allow -M pandora
```

その後、ルールを有効化するための前述の対応を行う必要があります。

```
# sudo semodule -i pandora.pp
```