# 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設定について詳しく説明します。

## Rocky Linux 8

### Audit2allow のインストール

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):

```
dnf install selinux-policy-devel -y
dnf install policycoreutils-python-utils -y
```

### SELinux ログディレクトリの場所

SELinux が返すエラーは、以下にあります。

- `/var/www/html/pandora_console/log/audit.log`
- `/var/log/messages`

OUM によって Pandora FMS を更新する場合は、対応するlogrotate ファイルを変更する必要があります。

SELinux がブロックするものをより明確に確認するには、以前の *logs* を削除し、新しいレコードで再度生成されるまで待つことをお勧めします。

syslog を停止する必要があります (このサービスは rsyslog とも呼ばれます)。root または同等の権限でコマンドターミナルに入力します (コマンドの前に sudo を付けます)。

```
systemctl stop syslog
```

audit.log および *log* システムメッセージファイルを削除する必要があります。

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

syslog を再起動します (このサービスは rsyslog とも呼ばれます)。

```
systemctl start syslog
```

### SELinux 設定

SELinux を設定するには、設定ファイル /etc/selinux/config を変更します。

```
# 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
```

- SELinux を制限モードで実行し、モジュールルール内に表示されているものだけを実行できるようにする必要がある場合は、これを enforcing に設定して、SELinux によって拒否された実行を (audit.log を通じて) 削除する必要があります。
- アクションをブロックするのではなく、警告 (*warnings*) を表示する必要がある場合は、それらを permissive のままにして、audit.log ファイルでこれらの *warnings* を確認します。

### ポリシールールを作成するためのエントリーの検索

最新の *ログ* エントリを表示するには、root または同等の権限でコマンドターミナルを入力します (コマンドの前に sudo を付けます)。

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

次のようなエラーが表示される場合があります。

```
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 が解釈できるルールに変換するには、以下を実行する必要があります。

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

これにより、現在のディレクトリに 2 つのファイルが作成されます。

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

新しいルールを有効にするには、以下を実行する必要があります。

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

不足しているルールを追加するには、このプロセスを繰り返します。すべてのルールを追加すると、SELinux はエラーの報告をしなくなります。

### Pandora FMS の適切な動作に必要なルール

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
- 計画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
- snmptrapd 監視
- NetFlow 監視

そうでないと、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。

これらすべてのルールを 1 つに統合して Pandora FMS を完全に使用できるようにする方法は次のとおりです。

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

次に、上記の手順を繰り返してルールを有効にします。これにより Pandora FMS と SELinux 間のすべての競合が解消されます。root または同等の権限 (コマンドの前に sudo を付けます) を使用してコマンドターミナルに入力します。

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

**実践的なまとめ**

Pandora FMS で SELinux を使用するためのルールがまとめられています。特定のケースごとに、値とパラメータを dev=sdaX や pid=XXX などのカスタマイズされた方法で変更する必要があることに注意してください。

setsebool コマンドは、SELinux の *booleans* を設定するためのツールです。-P オプションは、再起動後も設定された値を維持することを示し、命令の末尾の 1 は true 値を示し、アプリケーションを有効化します。root または同等の権限でコマンドターミナルに入力します (コマンドの前に sudo を付けます)。

```
setsebool -P httpd_unified 1
setsebool -P httpd_read_user_content 1
setsebool -P httpd_can_network_connect 1
setsebool -P httpd_execmem 1
setsebool -P httpd_can_network_connect_db 1
setsebool -P httpd_can_connect_ldap 1
setsebool -P authlogin_nsswitch_use_ldap 1
setsebool -P nis_enabled 1
setsebool -P httpd_setrlimit 1
```

chcon コマンドは、ファイルの SELinux コンテキストを変更します。-t オプションは SELinux ファイルタイプを示し、-R オプションはそれをディレクトリとそのすべての内容に再帰的に適用します。root または同等の権限でコマンドターミナルに入力します (コマンドの前に sudo を付けます)。

```
chcon -R -t httpd_sys_content_rw_t /var/www/html/pandora
chcon -R -t httpd_sys_content_rw_t /var/spool/pandora/
chcon -R -t httpd_sys_content_rw_t /tmp/
```

以下のルールが追加され、それぞれのケースで必要なカスタマイズが常に適用されます。root または同等の権限でコマンドターミナルに入力します (コマンドの前に sudo を付けます)。

```
echo 'type=AVC msg=audit(1709637797.944:2074063): avc:  denied  { write } for
pid=176072 comm="php-fpm" name="collections" dev="sda5" ino=142704842
scontext=system_u:system_r:httpd_t:s0 tcontext=system_u:object_r:var_spool_t:s0
tclass=dir permissive=1' | audit2allow -a
echo 'type=AVC msg=audit(1709639101.328:2100929): avc:  denied  { unlink } for
pid=152354 comm="php-fpm" name="gotty_cron_tmp.log" dev="sda5" ino=134725871
scontext=system_u:system_r:httpd_t:s0 tcontext=system_u:object_r:user_home_t:s0
tclass=file permissive=1'  | audit2allow -a
echo 'type=AVC msg=audit(1710850539.491:32359350): avc:  denied  { write } for
pid=3895348 comm="connection" name="tmp" dev="sda5" ino=8398230
scontext=system_u:system_r:mysqld_t:s0
tcontext=system_u:object_r:httpd_sys_rw_content_t:s0 tclass=dir permissive=1' |
audit2allow -a
```

次のコマンドは、ru□□les_apply.pp という名前のファイルにルールを作成するために使用され

ます。

```
audit2allow -a -M rules_apply
```

前の手順で semodule コマンドを使用して作成されたルールが適用されます。

```
semodule -i rules_apply.pp
```

Pandora FMS ドキュメント一覧に戻る