Configuration de SELinux pour Pandora FMS

Configuration de SELinux pour Pandora FMS

Introduction

Dans Pandora FMS, l'installation doit toujours être effectuée avec Security-Enhanced Linux (SELinux) désactivé. Après l'installation et compte tenu de la nécessité de l'activer dans certains environnements, détaillez les paramètres de configuration dans CentOS 7.

CentOS 7

Installation d'Audit2allow

CentOS 7 atteindra bientôt sa fin de vie (EOL). *Cette documentation est conservée à des fins historiques.*

Pour créer ce type de règles utilisezAudit2allow, qui sera chargé de permettre les actions nécessaires.

Avant de commencer à créer des règles pour les stratégies, vous devrez peut-être installer un certain nombre de paquets pour pouvoir utiliser Audit2allow. Entrez dans le terminal de commande avec la clé root ou des droits équivalents (précédez la commande sudo) :

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

Localisation du répertoire journal de SELinux

Les erreurs renvoyées par SELinux peuvent être trouvées dans les chemins suivants :

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

IMPORTANT :

Dans les versions précédentes à la version 747, le fichier audit.log se trouve dans/var/log/audit/audit.log.

Dans le cas d'une mise à jour par OUM, le fichier logrotate correspondant doit être modifié.

Pour vérifier plus proprement ce qui bloque SELinux, nous vous recommandons de supprimer les journaux précédents et d'attendre qu'ils soient générés à nouveau avec de nouveaux

enregistrements. Pour cela :

Arrêtez syslog (Ce service pourrait également être appelé rsyslog) :

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

Supprimez l'audit.log et le fichier journal des messages système :

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

Redémarrez syslog :

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

Configuration de SELinux

CentOS 7 atteindra bientôt sa fin de vie (EOL). *Cette documentation est conservée à des fins historiques.*

Pour configurer SELinux avec la valeur souhaitée, modifiez votre fichier de configuration :

```
# 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
```

Si vous voulez que SELinux s'exécute en mode restrictif en ne laissant exécuter que ce qui apparaît dans les règles des modules, configurerez-le en mode “enforcing”, en obtenant les exécutions refusées par SELinux par audit.log. Si, au contraire, vous voulez que les warnings soient imprimés au lieu de bloquer les actions, laissez “permissive”, vous pourrez vérifier ces warnings dans le fichier audit.log.

Localiser les entrées pour la création des règles de politiques

CentOS 7 atteindra bientôt sa fin de vie (EOL). *Cette documentation est conservée à des fins historiques.*

Pour visualiser les dernières entrées des journaux, exécutez :

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

Vous verrez qu'il y aura des erreurs comme par exemple :

```
# 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
```

Pour transformer ces erreurs en règles que SELinux peut interpréter, exécutez :

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

Cela créera 2 fichiers dans le répertoire actuel :

```

- pandora.pp
- pandora.te
```

Pour activer la nouvelle règle, exécutez :

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

Répétez le processus pour ajouter les règles manquantes. Après avoir ajouté toutes les règles, SELinux cessera de signaler des erreurs.

Règles nécessaires au bon fonctionnement de Pandora FMS

CentOS 7 atteindra bientôt sa fin de vie (EOL). *Cette documentation est conservée à des fins historiques.*

Pour que Pandora FMS puisse exécuter tous les services correctement, des règles doivent être créées pour les fonctionnalités suivantes :

- Créer, mettre à jour et supprimer des collections.
- Envoyer des e-mails en utilisant les tâches planifiées (Cronjob).
- Configuration à distance des agents.

Sinon, SELinux bloquera toute action associée à ces fonctionnalités.

Une façon de combiner toutes ces règles en une seule pour pouvoir utiliser Pandora FMS à 100% serait :

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

Répétez ensuite l'étape décrite ci-dessus pour activer la règle. Cela couvrirait tous les conflits possibles entre Pandora FMS et SELinux.

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

Retour à l'index de documentation Pandora FMS.