SELinux のツールや便利な機能の紹介

2019/2/18

藤原慎太郎
Shintaro Fujiwara

自己紹介

- **SELinux との関わり**
  - **2003年位から使っている。昔、C++（Qt)でSELinux用ツールを作っていた。ポリシパッチ採用されたことあり。SELinuxユーザ会のコアメンバーだった。**

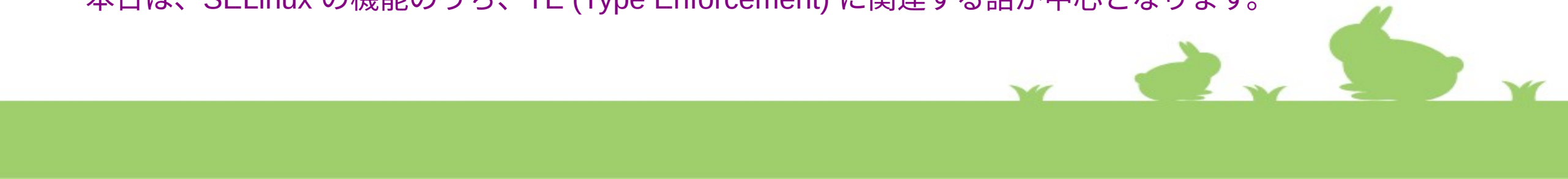
SELinux のツールや便利な機能の紹介

■こんな事が聞きたいという声

1. SELinux ポリシーの作り方や、コツ、便利ツールの紹介

2. Android や docker などで SELinux が使われていて、他にも SELinux の活用はもっとできる可能性があると思うので、最近の状況を知りたい。

本日は、SELinux の機能のうち、TE (Type Enforcement) に関連する話が中心となります。



内容

- 1. SELinux の概要とできてうれしいこと
- 2. SELinux ポリシーの作り方とコツ
  - 2-0. reference policy
  - 2-1. audit.log による確認
  - 2-2. audit2allow （昔からよく使われている）
  - 2-3. sepolgen （テンプレート的からポリシ作成）
- 3. 便利ツールの紹介
  - 3-1. Boolean （on/off による簡易設定）
  - 3-2. semanage （いわば詳細設定）
  - 3-3. その他

内容

- 4. 最近の状況

- なお、本日話さないこと、は以下となります。
  - 標準的でないと私が考えるシステム（組込系）でSELinuxが動くか
  - Linux Security Module の中で一番よいものはどれか
  - SELinux をどこからダウンロードしてどのように動かすのか
  - そもそも、セキュリティとは何か、どんな運用がよいのか
  - SELinux のカーネルコードや、ユーザーランドコードの詳細やその解説

1. SELinux の概要とできてうれしいこと（1/3）

- Security Enhanced Linux の概要
  - 元はNSAが作った2000~、Red Hat Enterprise Linuxデフォルト
  - Linux Security Module の一部（SELinux, Smack,AppArmor,TOMOYO等）
  - おおざっぱに言うと、システムコールが呼ばれる時にフックをかけてポリシと照合、拒否／許可する仕組み。また、ラベル方式である（AppArmor,TOMOYOは、パス方式）。
- できてうれしいこと
  - あるプロセスが乗っ取られても、別のプロセスに浸透されないので安心（ーにポリシによる）。

なので、「パッチを当てられなくても安心」（システム管理者的には）。実際、脆弱性が取れないために使っている場面もあるらしい。システムによっては、「ラベルを使わなければならない」というものも。[引用]SELinux 実行中のシステム上では、すべてのプロセスとファイルがセキュリティー関連の情報を表示する方法でラベル付けされます。この情報は、SELinux コンテキストと呼ばれます。ファイルに関しては、ls -Z コマンドでこれを表示できます。
SELinu ユーザーおよび管理者のガイド(RHEL6) 5.7. SELINUX コンテキスト - ファイルのラベル付け

1. SELinux の概要とできてうれしいこと（2/3）

◆ターゲットポリシ(selinux-policy-targeted)

Red Hat Enterprise Linux では、sshd や httpd といったネットワーク上でリッスンするサービスは、ほとんどすべて制限があります。...プロセスに制限があると、プロセス自体のドメイン内で実行されます。例えば、httpd_t ドメイン内で httpd プロセスが実行される、といったようにです。制限のあるプロセスが攻撃者によって危険にさらされても、SELinux ポリシーの設定によって、攻撃者のリソースへのアクセスや攻撃による損害は限定されます。

制限のないプロセスは、制限のないドメインで実行されます。例えば、init で実行される制限のないサービスは unconfined_service_t ドメインで、カーネルで実行される制限のないサービスは kernel_t ドメインで、制限のない Linux ユーザーによって実行される制限のないサービスは unconfined_t ドメインで実行されることになります。制限のないプロセスでは SELinux ポリシールールが適用されますが、既存のポリシールールは制限のないドメイン内で実行中のプロセスにほとんどすべてのアクセスを許可します。制限のないドメイン内で実行中のプロセスは、ほとんど DAC ルールにフォールバックします。制限のないプロセスが危険にさらされても、SELinux は攻撃者によるシステムリソースやデータへのアクセス獲得を阻止しません。しかし、もちろん DAC ルールは常に使われます。SELinux は DAC ルールの上に加わるもので、DAC ルールに取って代わるものではありません。

[出典]第3章 ターゲットポリシー 3.1. 制限のあるプロセス
https://access.redhat.com/documentation/ja_jp/red_hat_enterprise_linux/7/html/selinux_users_and_administrators_guide/chap-security-enhanced_linux-targeted_policy#sect-Security-Enhanced_Linux-Targeted_Policy-Confined_Processes

1. SELinux の概要とできてうれしいこと（3/3）

- ターゲットポリシには、どれくらいの数があるの？

Fedora29 で以下のコマンドを実行しました。

```
$ rpm -ql selinux-policy-targeted | grep 100 | grep cil | wc -l
834
```

上記以外は、unconfined_t ドメインとなり、SELinux の制御をほとんど受けません。

[出典]第3章 ターゲットポリシー 3.1. 制限のあるプロセス
https://access.redhat.com/documentation/ja_jp/red_hat_enterprise_linux/7/html/selinux_users_and_administrators_guide/chap-security-enhanced_linux-targeted_policy#sect-Security-Enhanced_Linux-Targeted_Policy-Confined_Processes

2. SELinux ポリシーの作り方とコツ(1/6)

- reference policy（targeted）

  モジュール方式で、ロード／アンロードできる
  タイプ(.te)、ファイルコンテキスト(.fc)、インターフェース(.if)
  上記をまとめて、.pp とする。(/usr/share/selinux/targeted/default/active/modules/100/apache/cil)
  解凍する bunzip2 -d cil
  ...(snip)...
  (type httpd_exec_t)
  ...(snip)…
  (typeattributeset entry_type (httpd_exec_t httpd_helper_exec_t httpd_initrc_exec_t httpd_php_exec_t
  httpd_rotatelogs_exec_t httpd_suexec_exec_t httpd_sys_content_t httpd_sys_script_exec_t
  httpd_user_script_exec_t httpd_passwd_exec_t shell_exec_t nfs_t cifs_t))
  ...(snip)…
  (allow httpd_t httpd_exec_t (file (entrypoint)))
  (allow httpd_t httpd_exec_t (file (ioctl read getattr lock map execute open)))
  (typetransition initrc_domain httpd_exec_t process httpd_t)
  ...(snip)...
  (filecon "/usr/sbin/apache(2)?" file (system_u object_r httpd_exec_t ((s0) (s0))))

2. SELinux ポリシーの作り方とコツ(2/6)

- audit.log による確認
-

  SELinux が拒否したログが出力されます
  （一例）
  type=AVC msg=audit(1546555311.530:97): avc: denied { create } for pid=1000 comm="vboxdrv.sh"
  name="vbox-setup.log" scontext=system_u:system_r:init_t:s0 tcontext=system_u:object_r:var_log_t:s0
  tclass=file permissive=0

そういえば、カーネルアップデート後に、virtualbox の初期化に失敗していたんです。。

/sbin/vboxconfig
Failed…..

上記のように、audit.log を調べてみると、SELinux のせいでした。ログを書き出せないだけなのかな？よくわからないな。。「なんだよーSELinux つかえねー」、と、大声で叫びたい瞬間ですね。でも、ちょっと待って。。

2. SELinux ポリシーの作り方とコツ(3/6)

- audit2allow （拒否したログからポリシを作成）

```
# audit2allow -a (全ての拒否ログを許可するコマンド：以下、実行の一例の一部)
#============= init_t ==============
#!!!! This avc can be allowed using the boolean 'use_virtualbox'
allow init_t var_log_t:file create;

# audit2allow -i <file_name> -M <module_name>
module test 1.0;
require {
        type var_log_t;
        type init_t;
        class file create;
}
#============= init_t ==============
#!!!! This avc can be allowed using the boolean 'use_virtualbox'
allow init_t var_log_t:file create;
```

2. SELinux ポリシーの作り方とコツ(4/6)

- audit2allow :表示の続き（拒否したログからポリシを作成）

  ********** 重要 **********

  このポリシーパッケージを有効にするには、以下を実行して下さい:

  semodule -i test.pp

- semodule （モジュールのロード／アンロード／確認等）

  # semodule -l （モジュールのリスト表示）

  # semodule -i test.pp （モジュールのロード）

  # semodule -r test （モジュールのアンロード）

- .te ファイル（最低限これは必要）、.fc ファイル、.if ファイルから.pp ファイルを作成する方法

  # make -f /usr/share/selinux/devel/Makefile （ファイルが存在するディレクトリ上で実施）

2. SELinux ポリシーの作り方とコツ(5/6)

- sepolgen （テンプレートを利用してポリシ作成）
  sepolgen は、sepolicy generate へのシンボリックリンクとなっている。

```
# sepolicy generate -n myprogram --application /usr/local/bin/myprogram
（表示例）
Failed to retrieve rpm info for selinux-policy
Created the following files:
myprogram.te # 強制ファイルの記入
myprogram.if # インターフェイスファイル
myprogram.fc # ファイルコンテキストファイル
myprogram.spec # スペックファイル
myprogram.sh # セットアップスクリプト
```

2. SELinux ポリシーの作り方とコツ(6/6)

- # ./myprogram.sh
  Building and Loading Policy
  + make -f /usr/share/selinux/devel/Makefile myprogram.pp
  make: 'sosreport-analyzer.pp' は更新済みです.
  + /usr/sbin/semodule -i myprogram.pp
  + sepolicy manpage -p . -d myprogram_t
  ./myprogram_selinux.8
  + /sbin/restorecon -F -R -v /usr/local/bin/myprogram
  ...(snip)...
  # ls noarch
  myprogram_selinux-1.0-1.fc29.noarch.rpm

と、モジュールインストールや、ポリシパッケージの作成をやってくれます（るようです）。

3. 便利な機能(1/2)

- Boolean

  覚えてますか？ audit2allow -a コマンドにより出力されていたんです。
  #!!!! This avc can be allowed using the boolean 'use_virtualbox'

特定のポリシにつて、boolean というので、オン/オフをランタイムおよび永久に切り換えられます。avc(access vector cache)　SELinux が使用する、ポリシ照合キャッシュ

現在の設定の確認
$ getsebool -a | grep virtualbox あるいは、$ getsebool use_virtualbox
use_virtualbox --> off
では、オンにしてみる。
setsebool virtualbox on
再度確認。
use_virtualbox --> on

Boolean でオンにした後、もう一度
コマンド実行
/sbin/vboxconfig
今度はうまくいったようです。

3. 便利な機能(2/2)

- semanage(モジュールの作成を除き、ほとんどの設定が可能なコマンド)
  先程の例で言えば、

  # semanage boolean –list | grep virtualbox
  (表示)
  state default
  use_virtualbox (オフ , オフ) Allow create vbox modules during startup new kernel.

  有効にする方法
  # semanage boolean --modify --on use_virtualbox

  その他、semanage で可能な設定
  # semanage [tab]押下
  (表示)
  boolean dontaudit export fcontext import interface login module node permissive port user
  と、ほとんどの設定が可能（説明省略）

4. 最近の状況

- Linux 5.1 では、複数のセキュリティモジュールを同時選択できるようになるかもしれない(メーリングリストで議論中のようです)。

内容は以上です。

5. まとめ

日本で、「まずSELinux を disabled にする」、ということになってしまったのは、targeted policy が生まれる前の、strict policy （全て拒否）の時代の名残と思われます。
現在は、ポリシのあるものだけを守る、というスタンスなので、enabled にしても、何ら不都合はないはずです(プログラムが正しい動きをするなら)。
また、reference policy が生まれてからは、モジュール方式でポリシを管理しやすくなりました。

- Linus に会った時に、「君はSELinux 好きじゃないよね」って言ったら、”Understandable. Some system will need it.” と言ってくれたので、決して嫌いなわけではなく、デフォルトで必ず使えとかこれが正しいから使え、というのがイヤなだけみたいだと思ったので、LSM の種類や選択肢が増えていくでしょう。

ご静聴、ありがとうございましたm__m

参考サイトおよび質問等

（参考サイト）
1.SELinuxの概要とできてうれしいこと
[1]SELinuxで組み込み機器のセキュリティを高める（前編） —— SELinuxの概要
http://www.kumikomi.net/archives/2008/09/18selin1.php?page=7
[2] Tresys
http://userspace.selinuxproject.org/
[3]【図解/初心者向け】SELinuxとは？～仕組みやメリット・効果の基礎入門解説～
https://milestone-of-se.nesuke.com/sv-advanced/selinux/selinux-summary/
[4] SELinu ユーザーおよび管理者のガイド 5.7. SELINUX コンテキスト – ファイルのラベル付け
https://access.redhat.com/documentation/ja-jp/red_hat_enterprise_linux/6/html/security-enhanced_linux/sect-security-enhanced_linux-working_with_selinux-selinux_contexts_labeling_files
2.SELinuxポリシーの作り方とコツ
[5] 【SELinuxポリシー追加】audit2allowの使い方/ .teの書き方, make方法, .ppの内容確認方法
https://milestone-of-se.nesuke.com/sv-advanced/selinux/add-av-rules-module/
[6] Linux セキュリティ標準教科書(Ver1.0.0)
[フォルダに入れました]
[7] SELinu ユーザーおよび管理者のガイド 10.3. 問題の修正
https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/selinux_users_and_administrators_guide/sect-security-enhanced_linux-troubleshooting-fixing_problems
[8] SELinu ユーザーおよび管理者のガイド 5.2. SELINUX ポリシーモジュールの生成: SEPOLICY GENERATE
https://access.redhat.com/documentation/ja_jp/red_hat_enterprise_linux/7/html/selinux_users_and_administrators_guide/security-enhanced_linux-the-sepolicy-suite-sepolicy_generate
3.便利な機能
[9]SELinu ユーザーおよび管理者のガイド 4.5. ブール値
https://access.redhat.com/documentation/ja-jp/red_hat_enterprise_linux/7/html/selinux_users_and_administrators_guide/sect-security-enhanced_linux-working_with_selinux-booleans
[10]SELinu ユーザーおよび管理者のガイド 5.7.2. 永続的な変更: SEMANAGE FCONTEXT
https://access.redhat.com/documentation/ja-jp/red_hat_enterprise_linux/6/html/security-enhanced_linux/sect-security-enhanced_linux-selinux_contexts_labeling_files-persistent_changes_semanage_fcontext
[11] CTJブログ Linux OS のセキュリティ-2 (RBACの話です)
https://www.miraclelinux.com/tech-blog/7byu5i
[12] メーリングリスト
selinux@vger.kernel.org