SELinux nekouše!

SELinux troubleshooting

Prezentuje
Lukáš Vrabec

8.11.2015 OpenAlt Brno

SELinux?

SELinux is labelling system!

Použitie?

Izolácia procesov!

Type Enforcement

- Deklaratívny popis služby = SELinux Politika
  - Pravidlá *policy.te*
  - Rozhrania *policy.if*
  - Štítky policy.fc
- SELinux pravidlá
  - Povolovacie pravidlá
  - Čo nie je povolené, je implicitne zakázané!

fedora

SELinux pravidlo

```
allow Rule | source_domain | target_type  : class    | permission
-----------▼---------------▼-------------------------▼------------
allow        unconfined_t    ext_gateway_t : process    transition;
```

```
allow ext_gateway_t in_file_t : file { write create getattr };
```

fedora™

Booleany

- Dočasné prispôsobovanie politiky
- #semanage boolean -l
- #setsebool / #semanage boolean -m

AVC správa

- # ausearch -m AVC -ts recent
- # cat /var/log/audit/audit.log | grep AVC

Troubleshooting Apache služby

Permissive mode

- #setenforce 0
- #getenforce

fedora

Popis problému

- Httpd služba
  - Httpd-2.4.17-3
- Index.html v domovskom adresári
- Port 8989
- Logovacie súbory v /var/log/openalt

audit2allow

- #cat avc_file | audit2allow -M mymodule
- #semodule -i mymodule.pp

!!NIE!!!

fedora

1.Krok

- #mv ~/index.html /var/www/html/
- #systemctl start httpd
  - ???
- # ls -Z
  - ???
- # restorecon -v index.html
- # ls -Z
  - ???

2. Krok

- Port pre bindovanie: 8989
- #systemctl restart httpd
- #semanage port -a -t http_port_t -p tcp 8989
- #semanage port -l | grep 8989

3. Krok

- Vlastná cesta ukladania logov
- #systemctl restart httpd
- Logy: /var/log/openalt/access_log
- #chcon -R -t httpd_log_t /var/log/openalt/

4. krok

- Chýbajúce pravidlo
  - AVC sprava (ausearch)
  - Je pripadné pravidlo zmysluplné?
- Pridanie pravidla
  - #audit2allow
  - #semodule

Enforcing mode

- # setenforce 1
- # getenforce

Príkazy

- #ausearch -m AVC -ts recent
- #audit2allow -i avc_file (-R)
- #semodule -i mymodule.pp
- #sesearch
- # ls -Z
- #semanage
- #restorecon

SELinux vs. Sudo CVE

Seriously, stop disabling SELinux.
Learn how to use it before you blindly shut it off.

Every time you run setenforce 0, you make Dan Walsh weep.
Dan is a nice guy and he certainly doesn't deserve that.

“http://stopdisablingselinux.com/”

Otázky?

Kontakt:
lvrabec@redhat.com