SELinux

Oscar Buse

25 januari 2017

ICT=Smart Nijmegen

Inhoudsopgave

Over mij

- Freelance Linux systeembeheer.
- Freelance Linux docent.

Meetup Linux Usergroup Nijmegen

- www.linuxnijmegen.nl (alle presentaties)
- Elke 2de dinsdag van de maand van 20:00 - 22:30. De klinker, van Broeckhuysenstraat 46, Nijmegen.

Overzicht

- Inleiding en terminologie (SELinux modes, SELinux policy en SELinux access control)
- Lastig?
- Configuratie
- Werkwijze en 2 voorbeelden
- Concluderend
- Referenties

Wat is SELinux?

- project van de NSA en de SELinux community voor extra beveiliging bovenop het standaard Linux permissie systeem.
- Mandators Access Control (MAC): het systeem bepaald de *policy*. Dit itt DAC (Discretionary Access Control: toegang gebasseerd op de *discretie* van de eigenaar).
- Betere scheiding van rechten, betere bescherming tegen bv. fouten in software (privilege escalation).
- SELinux data (de *security context*) is opgeslagen in de *extra attibutes* ruimte van de inode (sinds ext3, ook in xfs). Vaak zichtbaar met optie -Z bij bv. ls, id, ... Of -M bij ps.
- *policies* bepalen wat is toegestaan (straks meer over policies).

SELinux modes

Er zijn drie modes (toestanden) waarin SELinux zich kan bevinden:

- enforcing (aan). Tegenwoordig default op in elk geval Fedora, CentOS en RedHat.
- permissive (uit, wel logging)
- disabled (uit)

Commandos / config:

- sestatus: toont huidige mode
- setenforce: set mode (van/naar disabled: reboot)
- file: /etc/sysconfig/selinux

SELinux policy

SELinux kent meerdere **algemene** security policies, de bekendste:

- targeted - alléén van toepassing op specifieke targets (daemons). Denk aan httpd, named, mysqld, dhcpd, nscd, ...
  Users zijn niet beperkt (*unconfined*).
  Dit is de default.
- strict - Users ook aan policy onderhevig (confined). Is niet meer (sinds FC9) : opgenomen in de meer strict geworden targeted policy.
- minimum - alleen SELinux voor specifiek aangegeven processen (om te experimenteren).
- mls - zet Multi Level Security aan. Extra packages zijn nodig (o.a. selinux-policy-mls). Zet je niet "zomaar" aan.

SELinux access control

Als eerder vermeld: SELinux valt in de categorie MAC (itt DAC). Verder maakt SELinux in de **targeted policy** standaard gebruik van:

- Type Enforcement: security op basis van het type van "subjects" (processen), "access" (allow) en het type van "objects" (files, dirs, sockets, ...)".
  Dit is de default in de SELinux targeted policy.

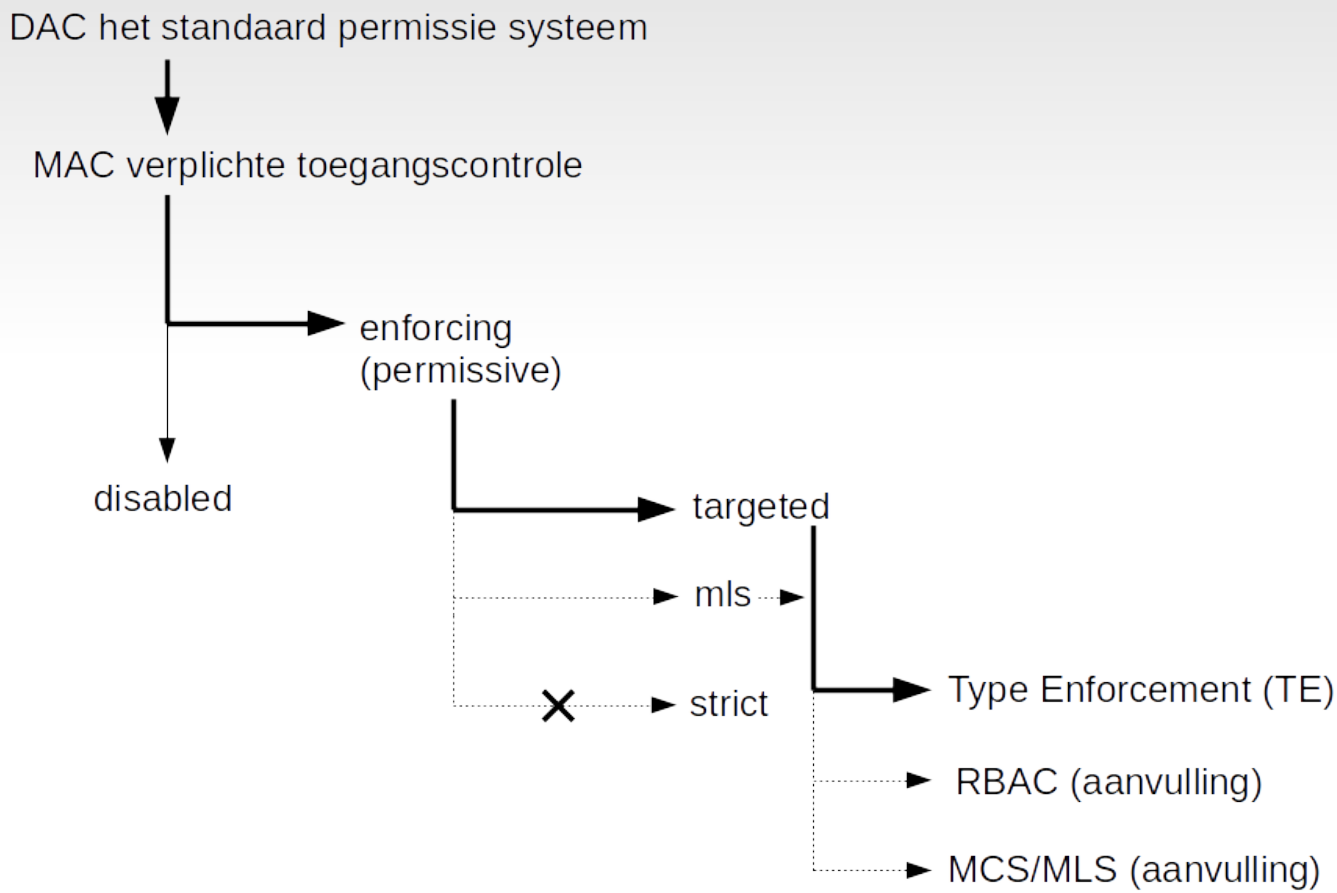
Andere typen access control die mogelijk zijn met SELinux maar niet standaard enabled (en geconfigureerd) zijn:

- RBAC - Role based access control.
- MCS/MLS - Multi Category (Sales, Tech, Staff) / Multi Level Security (Topsecret, Secret, Classified). Vooral MLS is meer voor militaire doeleinden en minder geschikt voor Linux servers..

Lastig?

- In theorie is SELinux best complex: er kan veel met SELinux (denk ook aan RBAC, MCS/MLS)
- Valt mee in de praktijk:
  - Alléén *Type Enforcement* (TE), als onderdeel van MAC: "mag proces van type naam_t iets (lezen, schrijven, executen, ...) met object van type naam_t?"
  - Default een *targeted* policy: alléén voor bepaalde daemons (httpd, dhcpd, ncsd, ...) geldt Type Enforcement.
  - Daemons komen standaard met gangbare default policy modules: zelf veelal geen policies te wijzigen/maken.
  - Users runnen standaard "unconfined" (SELinux niet van toepassing).
  - Voor het geval je wel zelf policies moet verzinnen zijn er veel hulpmiddelen (straks meer).

in een plaatje



Configuratie

- /etc/sysconfig/selinux (mode, type algemene policy)
- file labeling configuratie (*security contexts*): /etc/selinux/targeted/contexts/files/
- pre-compiled policy modules voor veelvoorkomende toepassingen (.pp files): /etc/selinux/targeted/modules
  Bv.: apache.pp, lvm.pp, ...

Werkwijze en tooling

- Hoe weet je nu of een policy-rule bestaat voor bepaalde types?

```
# sesearch -Ad -s httpd_t -t httpd_sys_content_t -c file
```

- Wat als je de policy wilt aanpassen of toevoegen?
  - `semodule_unpackage`: maar niet de bedoeling dat je de default policies wijzigt...wordt ontmoedigd
  - `booleans`: verander policy runtime (en ook permanent) met logische variabelen (on/off).
    - getsebool -a : toont alle logische variabelen
    - setsebool : set een logische variabele (-P : maak de setting permanent)
  - `semanage`: config policies zonder de default policy te wijzigen.
  - Maak een module (pas op)

Voorbeeld scenario 1: een apart upload-dir

Stel je hebt een boel ruimte gecreëerd onder `/opt/upload/` waar de apache daemon mag schrijven:

```
drwx----.  apache apache unconfined_u:object_r:usr_t:s0 upload
```

Gebruik `/var/log/audit/audit.log` om te kijken wat er mis gaat:
`tail -f /var/log/audit/audit.log | grep denied`
Let op: niet alles wordt standaard gelogt..! Zie waarde `Dontaudit` met het commando `seinfo`.
SELinux **alles** laten loggen met: `semodule -BD`
Wel weer terugzetten (`semodule -B`) na troubleshooten.

De dir is van type **usr_t** maar voor apache moet deze van type **httpd_sys_rw_content_t** zijn:

```
semanage fcontext -m -t httpd_sys_rw_content_t '/opt/upload(/.*)?'

restorecon -Rv /opt/upload
```

Voorbeeld scenario 2: maak een module

BackupPC is een handige grafische schil om rsync voor het maken van backups.

Er is geen standaard policy voor dus die moeten we zelf maken. De stappen:

- definieer de type-labeling (file context):
  - files onder /vol/grote_patitie/BackupPC moeten benaderbaar zijn voor de webserver. Daartoe moeten ze van type httpd_sys_content_t zijn:

```
# semanage fcontext -a -t httpd_sys_content_t
  '/vol/grote_patitie/BackupPC(/.*)?'
# restorecon -Rv /vol/grote_partitie/BackupPC
```

  - onder /var/log/BackupPC moet de webserver kunnen loggen. Daartoe moeten de files van type httpd_log_t zijn:

```
# semanage fcontext -a -t httpd_log_t
  '/var/log/BackupPC(/.*)?'
# restorecon -Rv /var/log/BackupPC/
```

Voorbeeld scenario 2: BackupPC

Vaak nog niet genoeg..

- Kijk naar denied regels in `/var/log/audit/audit.log` en stop in file `backuppc.txt`
- Maak van opgespaarde denied regels policy rules (met audit2allow):
  `cat backuppc.txt | audit2allow -M backuppc`
  Dit geeft:
  - De Type Enforcement rules (ascii): `backuppc.te`
  - Het binaire policy file met de type enforcement allow rules: `backuppc.pp`
- De nieuwe policy rules installeren: `# semodule -i backuppc.pp`

Let wederom op: niet alles wordt standaard gelogt..! Zie waarde `Dontaudit` met het commando `seinfo` en run evt. `semodule -BD`.

Pas voor introduceren ruime of anderszins ongebruikelijke policies..

Voorbeeld scenario 2 - extra

Het .te file is ook te gebruiken om een policy handmatig te maken/onderhouden. Bv. als je later toch nog een "denied" regel in de audit.log tegenkomt. De stappen:

- voeg bv. een extra allow regel toe (lastig! `audit2allow` is er niet voor niets..)
- denk ook aan de "required" items en verhoog het versie nummer van je module
- Genereer een binary module:

```
# checkmodule -o backuppc.mod backuppc.te -m
```

- Genereer een module package:

```
# semodule_package -o backuppc.pp -m backuppc.mod
```

- `# semodule -i backuppc.pp`

Concluderend

- SELinux geeft meer fijnmazige controle.
- Introduceert complexiteit. In veel (standaard) gevallen opgevangen door klant-en-klare policies en alléén Type Enforcement.
- Minder kans op *privilege escalation*.
- Door systeem geforceerd (niet gebasseerd op de *discretie* van de eigenaar zoals bij het normale Linux permissiesysteem).
- Kan nog veel meer mee (RBAC, MCS/MLS (wordt dan al snel complexer)).
- Geen vervanging van andere security maatregelen, alleen iets extra's
- Bij ondeskundig gebruik (makkelijk met audit2allow!) kans op afzwakken security model (er is natuurlijk nog wel altijd nog het normale permissiesysteem).

Referenties

Enkele url's met informatie:

http://docs.fedoraproject.org/en-US/Fedora/25/html/SELinux_Users_and_Administrators_Guide/

http://wiki.centos.org/HowTos/SELinux

https://debian-handbook.info/browse/stable/sect.selinux.html

http://stopdisablingselinux.com/