SELinux problémák

A SELinux érdekes állatfaj, a használatával biztonságosabb lehet a szerverünk, de néha bele tudunk futni fura hibákba, amelyeknek nem feltétlen értjük a forrását. Ilyen hiba lehet az, ha egy saját magunk által írt *Munin* plugin nem tud lefutni, s az alábbi hibát írja a logba:

/var/log/munin/munin-node.log

```
2012/06/22-13:20:05 [13773] Error output from jstat_confluence:
2012/06/22-13:20:05 [13773]     Can't exec "/etc/munin/plugins/jstat_confluence": Permission denied at /usr
/share/perl5/vendor_perl/Munin/Node/Service.pm line 215, <STDIN> line 37.
2012/06/22-13:20:05 [13773]     # ERROR: Failed to exec.
2012/06/22-13:20:05 [13773] Service 'jstat_confluence' exited with status 42/0.
2012/06/22-13:20:05 [13773] Error output from jstat_confluence:
2012/06/22-13:20:05 [13773]     Can't exec "/etc/munin/plugins/jstat_confluence": Permission denied at /usr
/share/perl5/vendor_perl/Munin/Node/Service.pm line 215, <STDIN> line 38.
2012/06/22-13:20:05 [13773]     # ERROR: Failed to exec.
2012/06/22-13:20:05 [13773] Service 'jstat_confluence' exited with status 42/0.
```

Ránézésre semmi ok nincs arra, hogy ne tudná lefuttatni az adott szkriptet, kézzel indítva remekül lefut, az adott felhasználó nevében is lefut, mindenféle variációban lefut, de a *Munin* nem futtatja le. Ilyenkor ersen gyanakodjunk arra, hogy a SELinux nem engedi az adott hívást... 🙂

Persze nem egyszer erre rájönni, mert a SELinux alapból nem írja az *audit.log* állományba azt, hogy valamit megtagadott, ehhez át kell kapcsolnunk a *-D* paraméter használatával egyfajta *hibakeres* módba:

```
# semodule -DB
```

Majd ersen figyeljük a *munin*-releváns eseményeket az *aud it.log* állományban:

```
# tail -f /var/log/audit/audit.log | grep munin
type=AVC msg=audit(1340364509.760:42854): avc:  denied  { execute } for  pid=14980 comm="munin-node" name="
jstat" dev=xvda1 ino=135170 scontext=unconfined_u:system_r:munin_t:s0 tcontext=unconfined_u:object_r:
munin_etc_t:s0 tclass=file
type=SYSCALL msg=audit(1340364509.760:42854): arch=c000003e syscall=59 success=no exit=-13 a0=160b4a0
a1=160b400 a2=15f1c10 a3=7fff0de26710 items=0 ppid=14979 pid=14980 auid=0 uid=99 gid=498 euid=99 suid=0
fsuid=99 egid=498 sgid=0 fsgid=498 tty=(none) ses=4247 comm="munin-node" exe="/usr/bin/perl" subj=unconfined_u:
system_r:munin_t:s0 key=(null)
```

Meg is van a bnös, már csak létre kell hoznunk a fenti tartalom alapján egy egyedi policy fájlt:

```
# cat /tmp/munin_jstat_policy | audit2allow -M munin_jstat_policy
******************* IMPORTANT ***********************
To make this policy package active, execute:
semodule -i munin_jstat_policy.pp
# semodule -i munin_jstat_policy.pp
# semodule -l | grep munin_jstat
munin_jstat_policy      1.0
```

Lezárásképp állítsuk vissza az *audit.log* naplózását az eredeti állapotra:

```
# semodule -B
```

Majd ellenrizzük le az eredményt, s ha továbbra is hibás mködést találunk, akkor ismételjük meg (az elz policy sértés mögé hozzáírva az újabbakat), amíg kapunk elutasító *audit.log* kimenetet az adott hivással kapcsolatban.