Email Server - SELinux

SELinux

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

Warning
Fontos hogy a legújabb policy-t használjuk, különben a ClamAV futtatásához szükséges boolean-ek nem lesznek benne. Tehát ha nem az alábbi az SELInux-unk verziója, akkor a teljes rendszeren futtassunk egy update-t.

Legalább erre a policy-ra szükség van: **selinux-policy-3.7.19-292.el6.noarch**

```
# yum update
```

De legalább ezt:

```
# yum update selinux\* policycoreutils libsepol
```

Els?ként fel kell tenni a SELinux log modult:

```
# yum install setroubleshoot* setools
```

Itt az id?, hogy visszakapcsoljuk a SELinux-ot. A SELinux egyrészt nem fogja megengedni, hogy a Dovecot hozzáférjen a /var/spool/postfix/virtual mappákhoz, hogy ott fájlokat, mappákat hozzon létre, vagy töröljön. Másrészt a postfix_virtual_t kontextusú procesznek meg kell szintén engedjük, hogy írja a fent említett spool mappákat, vagyis a postfix_spool_t kontextusú mappákat és fájlokat.

A SELinuxban lehet?ség van a policy-ba egyedi modulokat betölteni, ezzel módosítani a gyári beállításokat. A audit2allow program az audit log alapján tud ajánlatokat tenni az egyes SELinux problémák megoldására, úgy hogy legyárt az adott problémára egy megfelel? modult. Egy .te kiterjesztés? fájlban legyártja a polocy fájlt, amiben leírja a szerinte alkalmazandó policy módosításokat.

A /var/log/messages fájlban megjelen? SELinux riasztások (For complete SELinux messages. run sealert -l 543e1f54-ddee-48ad-88a1-14854a9e887d) jobb híján az audit2allow program segítségével legyártható modul használatára tesznek ajánlatot. Pl. a dovecot által okozott riasztásokban leírt hozzáférések engedélyezésére az alábbi parancsot javasolja:

```
# grep doveconf /var/log/audit/audit.log | audit2allow -M dovecotMyPol
```

Ezt futtatva a jelenlegi mappában, ahol épp állunk, létrehoz egy .te fájlt, és generál bel?le egy .pp betölthet? modul fájlt.

A .pp kiterjesztés? modult így tölthetjük be:

```
# semodule -i dovecotMyPol.pp
```

Fontos, hogy amit a audit2allow -M után emgadunk, az lesz a modul neve. Egyszerre csak egy ilyen nev? modul lehet betöltve a policy-ba, tehát ha létrehozunk egy másik .pp modult ugyan ilyen névvel, és a semodul -i vel betöltjük, akkor a régit felül fogja írni, és ami abban volt, az elveszik. Tehát mindig egyedi modul neveket adjunk meg a audit2allow -M parancs használatakor.

A audit2allow -M nem tett bele mindent a virtuális mappát használó email rendszer m?ködéséhez szükséges engedélyekb?l. A audit2allow -M által legyártott .te fájl kiváló kiindulási alap. Én a három különböz? SELinux riasztásból generált .te fájl tartalmát másoltam össze egy .te fájlba:

```
module dovecotVirtualMailbox 1.0;

require {
        type dovecot_t;
       type postfix_virtual_t;
        type postfix_spool_t;
        type postfix_qmgr_t;
        type postfix_private_t;
        class file { rename read lock create write getattr link unlink open append };
        class dir { write read create add_name remove_name search };
}

#============= dovecot_t ==============
#!!!! The source type 'dovecot_t' can write to a 'dir' of the following types:
# user_home_dir_t, postfix_private_t, mail_spool_t, tmp_t, dovecot_tmp_t, user_home_t, var_run_t, var_log_t, dovecot_spool_t, mail_home_rw_t,
allow dovecot_t postfix_spool_t:dir { write add_name };
allow dovecot_t postfix_spool_t:dir { read remove_name create };
allow dovecot_t postfix_spool_t:file { rename read lock create write getattr link unlink open append };



#============= dovecot_t on httpd ==============
#allow dovecot_t httpd_config_t:dir search;
#allow dovecot_t httpd_config_t:file { read open };


#============= postfix_virtual_t ==============
#!!!! The source type 'postfix_virtual_t' can write to a 'dir' of the following types:
# user_home_dir_t, mail_spool_t, user_home_t, postfix_virtual_tmp_t, mail_home_rw_t, user_home_type, nfs_t

allow postfix_virtual_t postfix_spool_t:dir { write remove_name create add_name };
allow postfix_virtual_t postfix_spool_t:file { create unlink link };

#============= postfix_qmgr_t ==============
#!!!! The source type 'postfix_qmgr_t' can write to a 'dir' of the following types:
# var_run_t, postfix_spool_t, tmp_t, postfix_qmgr_tmp_t, var_spool_t, postfix_spool_maildrop_t

allow postfix_qmgr_t postfix_private_t:dir write;
```

Ebb?l els?ként készíteni kell egy .mod fájlt, majd a .mod fálból a .pp policy fájlt. Majd a semoudl -i vel betöltjük az új .pp fájlt.

```
# checkmodule -M -m -o virualMailPolicy.mod virualMailPolicy.te
```

```
# semodule_package -o virualMailPolicy.pp -m virualMailPolicy.mod
# semodule -i virualMailPolicy.pp
```

A modul betöltése boot perzisztens. A modult a -r kapcsolóval el lehet távolítani a policy-b?l, és a -d kapcsolóval ki lehet kapcsolni.