KB / 10 mars 2014

Comparatif SELinux F16 et F19

Vue d'ensemble

Fedora 19

```
[root@F19 labotd]# seinfo

Statistics for policy file: /sys/fs/selinux/policy
Policy Version & Type: v.28 (binary, mls)

   Classes:            83    Permissions:       253
   Sensitivities:       1    Categories:       1024
   Types:            4202    Attributes:        350
   Users:               8    Roles:              14
   Booleans:          259    Cond. Expr.:       308
   Allow:           87481    Neverallow:          0
   Auditallow:        132    Dontaudit:        7802
   Type_trans:      14729    Type_change:        74
   Type_member:        33    Role allow:         33
   Role_trans:        712    Range_trans:      4690
   Constraints:        97    Validatetrans:       0
   Initial SIDs:       27    Fs_use:             25
   Genfscon:           91    Portcon:           522
   Netifcon:            0    Nodecon:             0
   Permissives:        10    Polcap:              2
```

Fedora 16

```
[root@F16 ~]# seinfo

Statistics for policy file: /etc/selinux/targeted/policy/policy.26
Policy Version & Type: v.26 (binary, mls)

   Classes:            82    Permissions:       241
   Sensitivities:       1    Categories:       1024
   Types:            3602    Attributes:        290
   Users:               9    Roles:              13
   Booleans:          204    Cond. Expr.:       241
   Allow:           90266    Neverallow:          0
   Auditallow:         97    Dontaudit:        6944
   Type_trans:      13374    Type_change:        62
   Type_member:        46    Role allow:         23
   Role_trans:        290    Range_trans:      2970
   Constraints:        81    Validatetrans:       0
   Initial SIDs:       27    Fs_use:             22
   Genfscon:           85    Portcon:           432
   Netifcon:            0    Nodecon:             0
   Permissives:        49    Polcap:              2
```

F19 par rapport à F16

Classes : 83 ↗ +1

Types : 4202 ↗ +600

Users : 8 ↘ -1

Booleans : 259 ↗ +55

Allow : 87481 ↘ -2785

Attributes : 350 ↗ +60

Permissions : 253 ↗ +12

Roles : ↗ +1

Classe :

```
[root@F19 labotd]# seinfo -c > /tmp/class19.se
[root@F19 labotd]# scp root@10.2.3.182:/tmp/class.se /tmp
root@10.2.3.182's password:
class.se                                      100% 1178     1.2KB/s   00:00
[root@F19 labotd]# diff /tmp/class.se /tmp/class19.se
1c1
< Object classes: 82
---
> Object classes: 83
69a70
>     proxy
```

Dans F19, il y a une nouvelle classe « proxy »

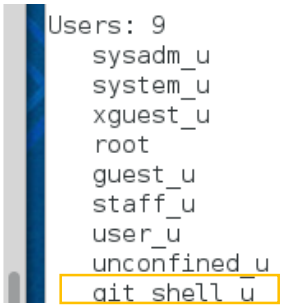
KB / 10 mars 2014 Comparatif SELinux F16 et F19

Users

Fedora 19

```
Users: 8
   sysadm_u
   system_u
   xguest_u
   root
   guest_u
   staff_u
   user_u
   unconfined_u
```

Fedora 16



Dans F19, il y a l'utilisateur git_shell_u en moins. Cette utilisateur permettait de créer un contexte non privilégié pour le serveur de versioning git

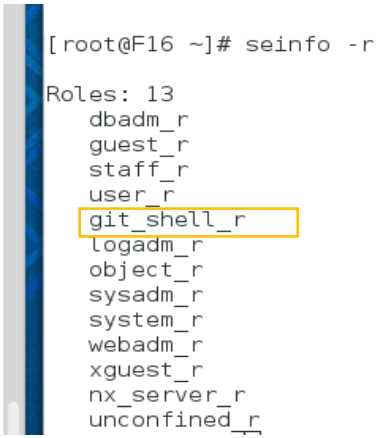
Roles

Fedora 19

```
[root@F19 labotd]# seinfo -r

Roles: 14
   auditadm_r
   dbadm_r
   guest_r
   staff_r
   user_r
   logadm_r
   object_r
   secadm_r
   sysadm_r
   system_r
   webadm_r
   xguest_r
   nx_server_r
   unconfined_r
```

Fedora 16



Dans F19, il y a le role git_shell_r en moins aussi.

Les développeurs de policy SELinux ont pris une décision de mettre le minimum de role et d'utilisateurs SELinux dans la distribution de base. Des rôles et des utilisateurs SELinux sont installés en même temps que l'installation de nouveau service tel que FreeIPA.

Allow Rules

Contrairement au chiffre attendu, il y a 2800 règles allow en moins défini dans F19 qu'en F16. L'explication de cette baisse étonnante se trouve dans l'augmentation du nombre d'attributs. Voici un aperçu de quelques attributs sous F19 :

```
[root@F19 ~]# seinfo -a -x | head -n 50

Attributes: 350
   cert_type
      dovecot_cert_t
      home_cert_t
      cert_t
      slapd_cert_t
   direct_init
   privfd
      sysadm_su_t
      auditadm_su_t
      secadm_t
      getty_t
      rpm_t
      sysadm_ssh_agent_t
      usernetctl_t
      auditadm_t
```

Attribut cert_type

Type qui sont dans l'ensemble cert_type

En effet, une règle allow est composée d'un type source et d'un type de destination. Mais une règle allow peut être définie aussi à l'aide d'un attribut source à la place d'un type source et la même chose pour le champ destination. Un attribut est nom donnée à un ensemble de types. Celui-ci permet de définir avec une règle allow l'équivalent de plusieurs règles allow défini uniquement avec des types spécifiques.

Exemple :

1) Règle allow défini avec 2 types spécifiques :

```
allow passwd_t var_log_t : dir {ioctl read write getattr … search open}

allow httpd_t var_log_t : dir {ioctl read write getattr … search open}
```

2) Déclaration équivalente faite à l'aide d'un attribut :

Définition d'un attribut nommé groupe_log_type qui regroupe les types suivant : passwd_t et httpd_t

```
attribute groupe_log_type;

type passwd_t, groupe_log_type;

type httpd_t, groupe_log_type;
```

Règle allow équivalente aux 2 règles allow précédente :

```
allow groupe_log_type var_log_t : dir {ioctl read write getattr … search open}
```

Avec une règle défini à l'aide d'attribut, celle-ci peux remplacer plus d'une centaine de règles allow faite avec des types spécifique. Ceci dépend du nombre de types regroupés dans l'attribut utilisé.

Fedora 19

```
[root@F19 ~]# seinfo -a -x | wc --line
22426
```

Fedora 16

```
[root@F16 ~]# seinfo -a -x | wc --line
14210
```

Ici j'ai demandé à afficher les attributs avec l'option –a et l'option –x permet de lister pour chaque attribut les types définis dans celui-ci. Après le pipe je demande a compter le nombre de lignes affichées dans F16 et F19. Ici nous pouvons relever qu'il y a beaucoup plus de types contenu dans les attributs sous F19 en comparaison avec F16. Ceci explique la diminution du nombre de règles allow.