Version : **2021.01**

Dernière mise-à-jour : 2023/02/15 16:08

LCF308 - Gestion du System Hardening

Contenu du Module

- **LCF308 - Gestion du System Hardening**
  - Contenu du Module
  - System Hardening Manuel
    - Les compilateurs
    - Les paquets
    - Les démons et services
    - Les fichiers .rhosts
    - Les fichiers et les repertoires sans proprietaire
    - Interdire les connexions de root via le réseau
    - Limiter le delai d'inactivite d'une session shell
    - Renforcer la securite d'init
      - Les Distributions SysVInit
      - Les Distributions Upstart
    - Renforcer la sécurité du Noyau
    - La commande sysctl
  - LAB #1 - System Hardening à l'aide de l'outil Bastille
    - Présentation
    - Installation
    - Utilisation
  - LAB #2 - Mise en place de SELinux pour sécuriser le serveur
    - Introducton
    - Définitions
      - Security Context

        - Domains et Types
        - Roles
        - Politiques de Sécurité
        - Langage de Politiques
            - allow
            - type
        - type_transition
        - Décisions de SELinux
            - Décisions d'Accès
            - Décisions de Transition
        - Commandes SELinux
        - Les Etats de SELinux
        - Booléens
    - LAB #3 - Travailler avec SELinux
        - Copier et Déplacer des Fichiers
        - Vérifier les SC des Processus
        - Visualiser la SC d'un Utilisateur
        - Vérifier la SC d'un fichier
        - Troubleshooting SELinux
            - La commande chcon
        - La commande restorecon
        - Le fichier /.autorelabel
        - La commande semanage
        - La commande audit2allow

System Hardening Manuel

Les compilateurs

Afin d'empêcher un pirate de créer des exécutables sur le serveur vous devez modifier les permissions sur les compilateurs éventuellement présents afin que seulement root puisse les exécuter.

Les paquets

Il convient dans ce cas de passer en revue la liste des paquets installes puis de supprimer ceux qui sont juges être inutiles :

```
[root@centos7 ~]# rpm -qa | more
libtalloc-2.1.9-1.el7.x86_64
gnome-contacts-3.22.1-1.el7.x86_64
lrzsz-0.12.20-36.el7.x86_64
NetworkManager-team-1.8.0-11.el7_4.x86_64
opus-1.0.2-6.el7.x86_64
libsss_certmap-1.15.2-50.el7_4.11.x86_64
m17n-db-1.6.4-3.el7.noarch
expat-2.1.0-10.el7_3.x86_64
gvfs-mtp-1.30.4-3.el7.x86_64
hypervfcopyd-0-0.30.20161211git.el7.x86_64
perl-parent-0.225-244.el7.noarch
libreport-centos-2.1.11-38.el7.centos.x86_64
pixman-0.34.0-1.el7.x86_64
alsa-plugins-pulseaudio-1.1.1-1.el7.x86_64
libreoffice-graphicfilter-5.0.6.2-15.el7_4.x86_64
libreport-rhel-anaconda-bugzilla-2.1.11-38.el7.centos.x86_64
libXext-1.3.3-3.el7.x86_64
libtool-ltdl-2.4.2-22.el7_3.x86_64
NetworkManager-ppp-1.8.0-11.el7_4.x86_64
osinfo-db-20170423-2.el7.noarch
fftw-libs-double-3.3.3-8.el7.x86_64
kernel-tools-libs-3.10.0-693.21.1.el7.x86_64
e2fsprogs-libs-1.42.9-10.el7.x86_64
--More--
```

Les démons et services

Il convient dans ce cas de passer en revue la liste des démons et services actives puis de supprimer ceux qui sont juges être inutiles;

- ps aux
- chkconfig –list
- systemctl list-unit-files

```
[root@centos7 ~]# ps aux | more
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  0.9 128172  4768 ?        Ss   14:58   0:11 /usr/lib/systemd/systemd --swit
ched-root --system --deserialize 21
root         2  0.0  0.0      0     0 ?        S    14:58   0:00 [kthreadd]
root         3  0.0  0.0      0     0 ?        S    14:58   0:13 [ksoftirqd/0]
root         5  0.0  0.0      0     0 ?        S<   14:58   0:00 [kworker/0:0H]
root         6  0.0  0.0      0     0 ?        S    14:58   0:00 [kworker/u2:0]
root         7  0.0  0.0      0     0 ?        S    14:58   0:00 [migration/0]
root         8  0.0  0.0      0     0 ?        S    14:58   0:00 [rcu_bh]
root         9  0.0  0.0      0     0 ?        S    14:58   0:09 [rcu_sched]
root        10  0.0  0.0      0     0 ?        S    14:58   0:00 [watchdog/0]
root        12  0.0  0.0      0     0 ?        S    14:58   0:00 [kdevtmpfs]
root        13  0.0  0.0      0     0 ?        S<   14:58   0:00 [netns]
root        14  0.0  0.0      0     0 ?        S    14:58   0:00 [khungtaskd]
root        15  0.0  0.0      0     0 ?        S<   14:58   0:00 [writeback]
root        16  0.0  0.0      0     0 ?        S<   14:58   0:00 [kintegrityd]
root        17  0.0  0.0      0     0 ?        S<   14:58   0:00 [bioset]
root        18  0.0  0.0      0     0 ?        S<   14:58   0:00 [kblockd]
root        19  0.0  0.0      0     0 ?        S<   14:58   0:00 [md]
root        25  0.0  0.0      0     0 ?        S    14:58   0:03 [kswapd0]
root        26  0.0  0.0      0     0 ?        SN   14:58   0:00 [ksmd]
root        27  0.0  0.0      0     0 ?        S<   14:58   0:00 [crypto]
root        35  0.0  0.0      0     0 ?        S<   14:58   0:00 [kthrotld]
--More--
```

```
[root@centos7 ~]# chkconfig --list
```

```
Note: This output shows SysV services only and does not include native
      systemd services. SysV configuration data might be overridden by native
      systemd configuration.

      If you want to list systemd services use 'systemctl list-unit-files'.
      To see services enabled on particular target use
      'systemctl list-dependencies [target]'.

livesys         0:off    1:off    2:off    3:on    4:on    5:on    6:off
livesys-late    0:off    1:off    2:off    3:on    4:on    5:on    6:off
netconsole      0:off    1:off    2:off    3:off    4:off    5:off    6:off
network         0:off    1:off    2:off    3:off    4:off    5:off    6:off
snortd          0:off    1:off    2:on    3:on    4:on    5:on    6:off
```

```
[root@centos7 ~]# systemctl list-unit-files
UNIT FILE                                   STATE
proc-sys-fs-binfmt_misc.automount           static
dev-hugepages.mount                         static
dev-mqueue.mount                            static
proc-fs-nfsd.mount                          static
proc-sys-fs-binfmt_misc.mount               static
sys-fs-fuse-connections.mount               static
sys-kernel-config.mount                     static
sys-kernel-debug.mount                      static
tmp.mount                                   enabled
var-lib-nfs-rpc_pipefs.mount                static
brandbot.path                               disabled
cups.path                                   enabled
systemd-ask-password-console.path           static
systemd-ask-password-plymouth.path          static
systemd-ask-password-wall.path              static
session-33.scope                            static
abrt-ccpp.service                           enabled
abrt-oops.service                           enabled
```

```
abrt-pstoreoops.service                         disabled
abrt-vmcore.service                             enabled
abrt-xorg.service                               enabled
abrtd.service                                   enabled
lines 1-23
```

Les fichiers .rhosts

Le systeme rhosts presente une faille de securite importante pour un serveur Linux. Pour cette raison, il convient de supprimer les fichiers **.rhosts** des utilisateurs. Utilisez la commande suivante:

```
# find / -name "\.rhosts" -exec rm -f \{\} \; [Entree]
```

Les fichiers et les repertoires sans proprietaire

Afin de dresser la liste des fichiers et des groupes sans proprietaires sur le serveur, il convient d'utiliser les deux commandes suivantes:

```
# find / -nouser -exec ls -l \{\} \; 2> sans_pro.txt [Entree]
```

```
# find / -nogroup -exec ls -l \{\} \; 2>> sans_pro.txt[Entree]
```

Ces commandes produiront une liste éventuelle dans le fichier **sans_pro.txt**.

L'examen de cette liste pourrait dévoiler des anomalies au quel cas il conviendrait de:

- modifier le propriétaire a root
- modifier le groupe a root
- modifier les permissions a 700

Interdire les connexions de root via le reseau

Le fichier de configuration des connexions de root est **/etc/securetty** :

```
[root@centos7 ~]# cat /etc/securetty
console
vc/1
vc/2
vc/3
vc/4
vc/5
vc/6
vc/7
vc/8
vc/9
vc/10
vc/11
tty1
tty2
tty3
tty4
tty5
tty6
tty7
tty8
tty9
tty10
tty11
ttyS0
ttysclp0
sclp_line0
3270/tty1
hvc0
```

```
hvc1
hvc2
hvc3
hvc4
hvc5
hvc6
hvc7
hvsi0
hvsi1
hvsi2
xvc0
```

Afin d'empêcher une connexion de root *directement* via le réseau et donc d'obliger une connexion en utilisant un compte d'utilisateur normal avant de passer en root grâce à la commande **su**, ce fichier ne doit **pas** contenir des entrees du type **ttysX** ou X = 0,1,2 etc.

Limiter le delai d'inactivite d'une session shell

Une session de shell laissee ouverte inutilement et d'une maniere sans surveillance est un risque de securite. Verifiez donc le contenu du fichier **/etc/profile** :

```
[root@centos7 ~]# cat /etc/profile
# /etc/profile

# System wide environment and startup programs, for login setup
# Functions and aliases go in /etc/bashrc

# It's NOT a good idea to change this file unless you know what you
# are doing. It's much better to create a custom.sh shell script in
# /etc/profile.d/ to make custom changes to your environment, as this
# will prevent the need for merging in future updates.

pathmunge () {
    case ":${PATH}:" in
```

```
        *:"$1":*)
            ;;
        *)
            if [ "$2" = "after" ] ; then
                PATH=$PATH:$1
            else
                PATH=$1:$PATH
            fi
    esac
}


if [ -x /usr/bin/id ]; then
    if [ -z "$EUID" ]; then
        # ksh workaround
        EUID=`/usr/bin/id -u`
        UID=`/usr/bin/id -ru`
    fi
    USER="`/usr/bin/id -un`"
    LOGNAME=$USER
    MAIL="/var/spool/mail/$USER"
fi

# Path manipulation
if [ "$EUID" = "0" ]; then
    pathmunge /usr/sbin
    pathmunge /usr/local/sbin
else
    pathmunge /usr/local/sbin after
    pathmunge /usr/sbin after
fi

HOSTNAME=`/usr/bin/hostname 2>/dev/null`
HISTSIZE=1000
```

```
if [ "$HISTCONTROL" = "ignorespace" ] ; then
    export HISTCONTROL=ignoreboth
else
    export HISTCONTROL=ignoredups
fi

export PATH USER LOGNAME MAIL HOSTNAME HISTSIZE HISTCONTROL

# By default, we want umask to get set. This sets it for login shell
# Current threshold for system reserved uid/gids is 200
# You could check uidgid reservation validity in
# /usr/share/doc/setup-*/uidgid file
if [ $UID -gt 199 ] && [ "`/usr/bin/id -gn`" = "`/usr/bin/id -un`" ]; then
    umask 002
else
    umask 022
fi

for i in /etc/profile.d/*.sh ; do
    if [ -r "$i" ]; then
        if [ "${-#*i}" != "$-" ]; then
            . "$i"
        else
            . "$i" >/dev/null
        fi
    fi
done

unset i
unset -f pathmunge
```

A ce fichier doivent etre ajoutées les deux lignes suivantes:

```
Readonly TMOUT=300
```

```
Export TMOUT
```

Par cette action, vous définissez le délai d’inactivité d'une session shell a une durée de 5 minutes.

Dernièrement, afin de se protéger contre des permissions trop permissives lors de la création de fichiers et de répertoires, il convient de passer la valeur d'**umask** à **077** dans le fichier **/etc/profile**.

Renforcer la securite d'init

Les Distributions SysVInit

Le fichier **/etc/inittab** est utilise pour configurer le démarrage de votre serveur.

La première modification à effectuer est de spécifier le niveau d’exécution par défaut a 3 au lieu de 5. Ceci permet de ne pas lancer les sessions graphiques sur une serveur de production. Cherchez donc la ligne suivante:

```
id:5:initdefault:
```

Modifiez-la en:

```
id:3:initdefault:
```

Le mode **single user** de démarrage de Linux n'est pas habituellement protégé par un mot de passe. Afin de remédier a cela, ajoutez les lignes suivantes:

```
# Single user mode
~~:S:wait:/sbin/sulogin
```

Dernièrement, afin d'empêcher une personne a redémarrer le serveur à l'aide des touches **ctrl+alt+supp**, il convient de mettre en commentaire la ligne correspondante:

```
# ca::ctrlaltdel:/sbin/shutdown -t3 -r now
```

Les Distributions Upstart

Afin d'empêcher une personne à redémarrer le serveur à l'aide des touches **ctrl+alt+supp**, éditez le fichier **/etc/init/control-alt-delete.conf** en modifiant la ligne suivante :

```
exec /sbin/shutdown -r now "Control-Alt-Delete pressed"
```

en

```
#exec /sbin/shutdown -k now "Control-Alt-Delete pressed"
```

Renforcer la sécurité du Noyau

La commande sysctl

Les fichiers dans le répertoire **/proc/sys** peuvent être administrés par la commande **sysctl** en temps réel.

La commande **sysctl** applique les règles consignés dans le fichier **/etc/sysctl.conf** au démarrage de la machine.

Saisissez la commande :

```
[root@centos7 ~]# cat /etc/sysctl.conf
# System default settings live in /usr/lib/sysctl.d/00-system.conf.
# To override those settings, enter new settings here, or in an /etc/sysctl.d/<name>.conf file
#
# For more information, see sysctl.conf(5) and sysctl.d(5).

[root@centos7 ~]# cat /usr/lib/sysctl.d/00-system.conf
# Kernel sysctl configuration file
#
# For binary values, 0 is disabled, 1 is enabled.  See sysctl(8) and
```

```
# sysctl.conf(5) for more details.

# Disable netfilter on bridges.
net.bridge.bridge-nf-call-ip6tables = 0
net.bridge.bridge-nf-call-iptables = 0
net.bridge.bridge-nf-call-arptables = 0

# Controls the maximum shared segment size, in bytes
kernel.shmmax = 4294967295

# Controls the maximum number of shared memory segments, in pages

[root@centos7 ~]# ls -l /etc/sysctl.d/
total 0
lrwxrwxrwx. 1 root root 14 Jun  4 09:54 99-sysctl.conf -> ../sysctl.conf

[root@centos7 ~]# cat /etc/sysctl.d/99-sysctl.conf
# System default settings live in /usr/lib/sysctl.d/00-system.conf.
# To override those settings, enter new settings here, or in an /etc/sysctl.d/<name>.conf file
#
# For more information, see sysctl.conf(5) and sysctl.d(5).
```

Options de la commande

Les options de la commande **sysctl** sont :

```
[root@centos7 ~]# sysctl --help

Usage:
 sysctl [options] [variable[=value] ...]

Options:
  -a, --all            display all variables
```

```
  -A                    alias of -a
  -X                    alias of -a
      --deprecated      include deprecated parameters to listing
  -b, --binary          print value without new line
  -e, --ignore          ignore unknown variables errors
  -N, --names           print variable names without values
  -n, --values          print only values of a variables
  -p, --load[=<file>]   read values from file
  -f                    alias of -p
      --system          read values from all system directories
  -r, --pattern <expression>
                        select setting that match expression
  -q, --quiet           do not echo variable set
  -w, --write           enable writing a value to variable
  -o                    does nothing
  -x                    does nothing
  -d                    alias of -h

 -h, --help     display this help and exit
 -V, --version  output version information and exit

For more details see sysctl(8).
```

Important : Consultez la page de la traduction du manuel de **sysctl ici** pour comprendre la commande.

LAB #1 - System Hardening à l'aide de l'outil Bastille

Présentation

Bastille Linux est un script interactif de renforcement de la sécurité pour certaines distributions de Linux dont RHEL, CentOS et Debian.

Installation

Installez le dépôt EPEL :

```
[root@centos7 ~]# wget http://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
[root@centos7 ~]# rpm -ivh epel-release-latest-7.noarch.rpm
```

Commencez par installer la dépendance de Bastille :

```
[root@centos7 ~]# yum install perl-Curses
```

Téléchargez et installez Bastille :

```
[root@centos7 ~]# wget https://www.dropbox.com/s/sz0ggexdkkduumb/Bastille-3.0.9-1.0.noarch.rpm
```

```
[root@centos7 ~]# yum localinstall Bastille-3.0.9-1.0.noarch.rpm --nogpgcheck
```

Dernièrement créez un lien symbolique :

```
[root@centos7 /]# ln -s /usr/lib/Bastille /usr/lib64/
```

Utilisation

Pour démarrez bastille en mode texte, saisissez la commande suivante :

```
# /usr/sbin/bastille -c [Entrée]
```

Pour démarrez bastille en mode graphique, saisissez la commande suivante :

```
# /usr/sbin/bastille -x [Entrée]
```

> **A Faire** - Lancez Bastille et répondez aux questions posées. Ré-amorcez votre machine virtuelle et testez le résultat.

LAB #2 - Mise en place de SELinux pour sécuriser le serveur

Introducton

L'approche SELinux (*Security Enhanced Linux*) à la sécurité est une approche de type **TE**. Elle essaie aussi d'intégrer les notions des approches de type **RBAC**, **MAC** et **MLS** sous la forme de **MCS** : ur

Type de Sécurité	Nom	Description
TE	*Type enforcement*	Chaque objet a une étiquette appelé *type* pour un fichier et *domaine* pour un processus. La politique de sécurité définit l'interaction entre les types et les domaines.
RBAC	*Role Based Access Control*	Un utilisateur a un ou plusieurs rôles. Les droits sont attribués aux rôles.
MAC	*Mandatory Access Control*	L'accès aux objets est en fonction de la classification de l'objet (Très secret, Secret, Confidentiel, Public). L'administrateur définit la politique de sécurité et les utilisateurs s'y conforment.
MLS	*Multi-Level Security*	Les politiques de sécurité imposent que qu'un sujet doit dominer un objet pour pouvoir le lire tandis que l'objet doit dominer le sujet pour que ce dernier puisse y écrire.

Même quand le modèle SELinux de sécurité est actif, la sécurité type DAC est toujours active. Cependant dans le cas où la sécurité du type DAC autorise une action, SELinux va évaluer cette action par rapport à ses propres règles avant de l'autoriser.

SELinux évalue toujours des ***actions*** tentées par des ***sujets*** sur des ***objets***.

Dans le contexte de SELinux :

- un ***sujet*** est toujours un **processus**,
- un ***objet*** peut être un fichier, un répertoire, un autre processus ou une ressource système,
- une ***action*** est une **permission**.

Chaque ***classe d'objet*** possède un jeu de permissions possibles ou ***actions*** qui peuvent être uniques à la classe ou bien **héritées** d'autres classes.

Définitions

Security Context

SELinux associe un *Security Context* (SC) à chaque ***objet*** et ***sujet*** du système.

Un SC prend la forme **identité:rôle:type:niveau** :

Nom	**Descriptions**
Identité	Le nom du propriétaire de l'objet. Une identité est associée à des rôles. Par défaut l'utilisateur à une identité de **user_u**.
Rôle	Essentiellement appliqué aux processus, le rôle est appelé une domaine. Dans le cas d'un rôle de fichier, celui-ci est toujours **object_r**. Un rôle se termine généralement par **_r**.
Type	Définit la classification de sécurité de l'objet. Un type se termine généralement par **_t**.
Niveau	Un niveau est un attribut de MLS et MCS. Une plage MLS est une paire de niveaux exprimée en utilisant la syntaxe *niveaubas-niveauhaut*. Chaque niveau est une paire exprimée en tant que sensibilitéhaut-sensibilitébas:catégoriehaut:catégoriebas par exemple s0-s0:c0.c1023. Il est important de noter que s0-s0 s'exprime aussi s0 et c0, c1, c2, c3 est exprimé c0.c3.

Sous RHEL/CentOS 7, le fichier **/etc/selinux/targeted/setrans.conf** contient la correspondance entre les niveaux et leurs valeurs compréhensibles par l'utilisateur :

```
[root@centos7 /]# cat /etc/selinux/targeted/setrans.conf
#
# Multi-Category Security translation table for SELinux
#
```

```
# Uncomment the following to disable translation libary
# disable=1
#
# Objects can be categorized with 0-1023 categories defined by the admin.
# Objects can be in more than one category at a time.
# Categories are stored in the system as c0-c1023.  Users can use this
# table to translate the categories into a more meaningful output.
# Examples:
# s0:c0=CompanyConfidential
# s0:c1=PatientRecord
# s0:c2=Unclassified
# s0:c3=TopSecret
# s0:c1,c3=CompanyConfidentialRedHat
s0=SystemLow
s0-s0:c0.c1023=SystemLow-SystemHigh
s0:c0.c1023=SystemHigh
```

Dans le contexte d'un SC pour un ***sujet***, le champ **identité** indique les privilèges de l'utilisateur SELinux utilisés par le ***sujet***.

Dans le contexte d'un SC pour un ***objet***, le champ **identité** indique à quel utilisateur SELinux appartient l'***objet***.

SELinux maintient sa propre liste d'utilisateurs, différente de la liste DAC de Linux. Il existe cependant une correspondance entre les deux listes de façon à ce que les utilisateurs MAC puissent être soumissent aux restrictions de SELinux :

```
[root@centos7 /]# /usr/sbin/semanage login -l

Login Name           SELinux User         MLS/MCS Range        Service

__default__          unconfined_u         s0-s0:c0.c1023       *
root                 unconfined_u         s0-s0:c0.c1023       *
system_u             system_u             s0-s0:c0.c1023       *
```

Domains et Types

Le **Domain** est l'endroit d'exécution d'un processus. Chaque processus a un **Domain**. Le **Domain** détermine les accès du processus.

Le **Domain** contient des ***objets*** et des ***sujets*** qui interagissent ensemble. Ce modèle, où chaque ***sujet*** se voit attribué à un **Domain** et où uniquement certaines opérations sont permises, est appelé ***Type Enforcement***.

Dans SELinux on utilise le mot :

- **Domain** pour un processus,
- **Type** pour un fichier.

Roles

Un **Rôle** est comme un utilisateur dans le système de sécurité DAC de Linux. Chaque utilisateur autorisé peut assumer l'identité du **Rôle** afin d'exécuter les commandes liées au **Rôle**.

Politiques de Sécurité

Une politique de sécurité définit les SC de chaque application. Elle définit des droits d'accès des domaines aux types. Il y a deux types de politique possible :

Politique	**Description**
targeted	Les politiques de sécurité ne s'appliquent qu'à certaines applications
mls	Multi Level Security protection

Les politiques de sécurité se trouvent dans le répertoire **/etc/selinux** :

```
[root@centos7 /]# ls -lR /etc/selinux/ | more
/etc/selinux/:
total 12
```

```
-rw-r--r--. 1 root root  547 Dec 10  2015 config
drwx------. 2 root root    6 Apr 23 16:24 final
-rw-r--r--. 1 root root 2321 Aug  4  2017 semanage.conf
drwxr-xr-x. 7 root root 4096 Apr 23 16:24 targeted
drwxr-xr-x. 2 root root    6 Aug  4  2017 tmp

/etc/selinux/final:
total 0

/etc/selinux/targeted:
total 24
drwx------. 3 root root 4096 Apr 23 16:24 active
-rw-r--r--. 1 root root 2623 Mar  7 15:19 booleans.subs_dist
drwxr-xr-x. 4 root root 4096 Apr 23 16:20 contexts
drwxr-xr-x. 2 root root    6 Mar  7 15:19 logins
drwxr-xr-x. 3 root root   19 Apr 23 16:41 modules
drwxr-xr-x. 2 root root   22 Apr 23 16:41 policy
-rw-------. 1 root root    0 Mar  7 14:52 semanage.read.LOCK
-rw-------. 1 root root    0 Mar  7 14:52 semanage.trans.LOCK
-rw-r--r--. 1 root root  607 Mar  7 15:19 setrans.conf
-rw-r--r--. 1 root root  176 Apr 23 16:24 seusers
--More--
```

Afin d'utiliser SELinux en ligne de commande sous RHEL/CentOS 7, il est nécessaire d'installer le paquet **setools-console** :

```
[root@centos7 ~]# yum install setools-console
```

Pour consulter les statistiques de la politique, il convient d'utiliser la commande **seinfo** :

```
[root@centos7 ~]# seinfo

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

```
   Classes:            94    Permissions:       262
   Sensitivities:       1    Categories:       1024
   Types:            4747    Attributes:        251
   Users:               8    Roles:              14
   Booleans:          307    Cond. Expr.:       356
   Allow:          101746    Neverallow:          0
   Auditallow:        155    Dontaudit:        8846
   Type_trans:      17759    Type_change:        74
   Type_member:        35    Role allow:         39
   Role_trans:        416    Range_trans:      5697
   Constraints:       109    Validatetrans:       0
   Initial SIDs:       27    Fs_use:             29
   Genfscon:          105    Portcon:           602
   Netifcon:            0    Nodecon:             0
   Permissives:         6    Polcap:              2
```

Important : Notez ici le grand nombre de la catégorie **Dontaudit**.

Langage de Politiques

Un politique est composé de centaines de directives. Les principales directives sont :

allow

allow autorise l'accès d'un processus d'un domaine à des fichiers appartenant à un type donné. Le format de la directive est :

```
allow user_t domaine_t : file (read execute getattr) ;
```

Dans cette directive :

- user_t est le type de fichier,
- domaine_t est le domaine des processus qui sont autorisés par allow,
- file (droit1 droit2 etc) est la liste des permissions accordées.

Les permissions possibles sont :

- read
- write
- append
- execute
- getattr
- setattr
- lock
- link
- unlink
- rename
- ioctl

type

La directive **type** définit un type SELinux. Le type se termine généralement par **_t**.

auditallow, dontaudit

La directive **auditallow** demande l'écriture d'un message de type **avc** dans les journaux. Elle n'est associée à aucune restriction.

L'inverse peut être obtenue avec **dontaudit**, à savoir, cette directive demande à ce qu'il n'y ait pas de journalisation après une interdiction.

type_transition

Normalement quand un fichier est créé, il hérite du SC du répertoire parent. De même quand un processus SELinux active un nouveau processus, ce dernier s'exécute dans le même domaine que son parent. La directive type_transition permet de modifier ce comportement.

Décisions de SELinux

Il existe deux types de décisions auxquelles SELinux doit faire face :

- **Décisions d'Accès**
- **Décisions de Transition**

Décisions d'Accès

Dans ce type de décision SELinux doit décider d'accorder ou non la permission à :

- un ***sujet*** de faire quelque chose à un ***objet*** existant,
- un ***sujet*** de créer de nouvelles choses dans le **Domain**.

Décisions de Transition

Dans ce type de décision SELinux doit décider d'accorder ou non la permission :

- d'invoquer un processus dans un **Domain** différent du **Domain** courant du ***sujet***,
- de créer des ***objets*** dans différents **Types** que le répertoire parent de l'***objet***.

Commandes SELinux

Commande	**Description**
chcon	Changer le SC d'un fichier
audit2allow	Générer la source de la règle de sécurité à l'origine d'une erreur
restorecon	Restaurer le SC par défaut à un ou plusieurs fichiers

Commande	Description
setfiles -n	Vérifier si les SC sont corrects
semodule	Gèrer les modules de politiques
semodule -i	Installer un module de politiques
checkmodule	Compiler un module
semodule_package	Créer un module installable par semodule
semanage	Administrer une politique
audit2allow -M	Créer un module à partir d'un message d'audit
sesearch	Recherche des règles SELinux
seinfo	Effectuer des recherches dans la politique
getsebool	Affiche l'état d'un booléen
getsebool -a	Affiche l'état de l'ensemble des booléens
sestatus -b	Affiche l'état de l'ensemble des booléens
setsebool	Modifie l'état d'un booléen
togglesebool	Bascule la valeur d'un booléen

Les Etats de SELinux

SELinux connait trois états :

Etat	Description
disabled	SELinux est inactif.
permissive	SELinux est actif mais tout est permis. Des interdictions ne font que de générer des messages d'erreurs dans les logs.
enforcing	SELinux est actif.

L'examen du contenu du fichier **/selinux/enforce** révèle une de deux valeurs qui correspondent à l'**état** de SELinux :

Valeur	Description
0	SELinux est en mode *permissive*
1	SELinux est en mode *enforcing*

La configuration de l'activation de SELinux ainsi que son état est effectuée grâce au fichier **/etc/selinux/config** :

```
[root@centos7 /]# cat /etc/selinux/config

# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#     enforcing - SELinux security policy is enforced.
#     permissive - SELinux prints warnings instead of enforcing.
#     disabled - No SELinux policy is loaded.
SELINUX=enforcing
# SELINUXTYPE= can take one of three two values:
#     targeted - Targeted processes are protected,
#     minimum - Modification of targeted policy. Only selected processes are protected.
#     mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

Afin de connaître l'état de SELinux, il convient d'utiliser la commande **getenforce** :

```
[root@centos7 /]# getenforce
Enforcing
```

Pour modifier l'état de SELinux, il convient d'utiliser la commande **setenforce** :

```
[root@centos7 /]# setenforce permissive
[root@centos7 /]# getenforce
Permissive
```

La commande **sestatus** vous informe sur la configuration de SELinux et notamment sur la version de la politique utilisée :

```
[root@centos7 /]# sestatus
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             targeted
Current mode:                   permissive
```

```
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Max kernel policy version:      28
```

Les différentes versions de politiques évolue en même temps que le noyau Linux.

La commande sestatus peut aussi prendre l'option -v :

```
[root@centos7 /]# sestatus -v
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             targeted
Current mode:                   permissive
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Max kernel policy version:      28

Process contexts:
Current context:                unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
Init context:                   system_u:system_r:init_t:s0
/usr/sbin/sshd                  system_u:system_r:sshd_t:s0-s0:c0.c1023

File contexts:
Controlling terminal:           unconfined_u:object_r:user_devpts_t:s0
/etc/passwd                     system_u:object_r:passwd_file_t:s0
/etc/shadow                     system_u:object_r:shadow_t:s0
/bin/bash                       system_u:object_r:shell_exec_t:s0
/bin/login                      system_u:object_r:login_exec_t:s0
/bin/sh                         system_u:object_r:bin_t:s0 -> system_u:object_r:shell_exec_t:s0
/sbin/agetty                    system_u:object_r:getty_exec_t:s0
/sbin/init                      system_u:object_r:bin_t:s0 -> system_u:object_r:init_exec_t:s0
```

```
/usr/sbin/sshd                  system_u:object_r:sshd_exec_t:s0
/lib/libc.so.6                  system_u:object_r:lib_t:s0 -> system_u:object_r:lib_t:s0
/lib/ld-linux.so.2              system_u:object_r:lib_t:s0 -> system_u:object_r:ld_so_t:s0
```

Booléens

Les booléens permettent à des ensembles de règles d'être utilisées d'une manière alternative.

Pour visualiser l'état l'ensemble des booléens, il convient d'utiliser la commande **getsebool -a** :

```
[root@centos7 /]# getsebool -a | more
abrt_anon_write --> off
abrt_handle_event --> off
abrt_upload_watch_anon_write --> on
antivirus_can_scan_system --> off
antivirus_use_jit --> off
auditadm_exec_content --> on
authlogin_nsswitch_use_ldap --> off
authlogin_radius --> off
authlogin_yubikey --> off
awstats_purge_apache_log_files --> off
boinc_execmem --> on
cdrecord_read_content --> off
cluster_can_network_connect --> off
cluster_manage_all_files --> off
cluster_use_execmem --> off
cobbler_anon_write --> off
cobbler_can_network_connect --> off
cobbler_use_cifs --> off
cobbler_use_nfs --> off
collectd_tcp_network_connect --> off
condor_tcp_network_connect --> off
conman_can_network --> off
```

```
container_connect_any --> off
--More--
```

ou la commande **sestatus -b** :

```
[root@centos7 /]# sestatus -b | more
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             targeted
Current mode:                   permissive
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Max kernel policy version:      28

Policy booleans:
abrt_anon_write                             off
abrt_handle_event                           off
abrt_upload_watch_anon_write                on
antivirus_can_scan_system                   off
antivirus_use_jit                           off
auditadm_exec_content                       on
authlogin_nsswitch_use_ldap                 off
authlogin_radius                            off
authlogin_yubikey                           off
awstats_purge_apache_log_files              off
boinc_execmem                               on
cdrecord_read_content                       off
--More--
```

Pour fixer l'état d'un booléen, il convient d'utiliser la commande setsebool :

```
[root@centos7 /]# setsebool antivirus_can_scan_system 1
```

```
[root@centos7 /]# getsebool antivirus_can_scan_system
antivirus_can_scan_system --> on
[root@centos7 /]# setsebool antivirus_can_scan_system 0
[root@centos7 /]# getsebool antivirus_can_scan_system
antivirus_can_scan_system --> off
```

LAB #3 - Travailler avec SELinux

Afin reconstruire la politique actuelle **sans** les règles **dontaudit**, utilisez la commande **semodule** :

```
[root@centos7 ~]# semodule -DB
```

Vérifiez qu'il ne reste aucune règle de type **dontaudit** :

```
[root@centos7 ~]# seinfo

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

   Classes:            94    Permissions:       262
   Sensitivities:       1    Categories:       1024
   Types:            4747    Attributes:        251
   Users:               8    Roles:              14
   Booleans:          307    Cond. Expr.:       356
   Allow:          101746    Neverallow:          0
   Auditallow:        155    Dontaudit:           0
   Type_trans:      17759    Type_change:        74
   Type_member:        35    Role allow:         39
   Role_trans:        416    Range_trans:      5697
   Constraints:       109    Validatetrans:       0
   Initial SIDs:       27    Fs_use:             29
   Genfscon:          105    Portcon:           602
```

```
   Netifcon:            0    Nodecon:             0
   Permissives:         6    Polcap:              2
```

Copier et Déplacer des Fichiers

Créez deux fichiers **file1** et **file2** en tant que l'utilisateur **trainee** puis visualisez les SC des fichiers :

```
[root@centos7 /]# exit
logout
[trainee@centos7 ~]$ touch file1 file2
[trainee@centos7 ~]$ ls -Z file*
-rw-rw-r--. trainee trainee unconfined_u:object_r:user_home_t:s0 file1
-rw-rw-r--. trainee trainee unconfined_u:object_r:user_home_t:s0 file2
```

Notez que le type des deux fichiers est **user_home_t**.

Copiez maintenant le fichier **file1** vers **/tmp** en utilisant la commande **cp** et visualiser son SC :

```
[trainee@centos7 ~]$ cp file1 /tmp
[trainee@centos7 ~]$ ls -Z /tmp/file1
-rw-rw-r--. trainee trainee unconfined_u:object_r:user_tmp_t:s0 /tmp/file1
```

Notez que le fichier ainsi copié a hérité du **type** du répertoire parent, à savoir **tmp_t**.

Déplacez maintenant le fichier **file2** dans le répertoire **/tmp** et contrôlez son SC :

```
[trainee@centos7 ~]$ mv file2 /tmp
[trainee@centos7 ~]$ ls -Z /tmp/file2
-rw-rw-r--. trainee trainee unconfined_u:object_r:user_home_t:s0 /tmp/file2
```

Notez que la commande **mv** maintient le **type** d'origine.

Vérifier les SC des Processus

Il convient d'utiliser l'option **Z** avec la commande **ps** :

```
[trainee@centos7 ~]$ ps auxZ | more
LABEL                             USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
system_u:system_r:init_t:s0       root         1  0.0  1.2  46140  6456 ?        Ss   juin17   0:27
/usr/lib/systemd/systemd --system --
deserialize 24
system_u:system_r:kernel_t:s0     root         2  0.0  0.0      0     0 ?        S    juin17   0:00 [kthreadd]
system_u:system_r:kernel_t:s0     root         3  0.0  0.0      0     0 ?        S    juin17   0:25 [ksoftirqd/0]
system_u:system_r:kernel_t:s0     root         5  0.0  0.0      0     0 ?        S<   juin17   0:00 [kworker/0:0H]
system_u:system_r:kernel_t:s0     root         6  0.0  0.0      0     0 ?        S    juin17   0:00 [kworker/u2:0]
system_u:system_r:kernel_t:s0     root         7  0.0  0.0      0     0 ?        S    juin17   0:00 [migration/0]
system_u:system_r:kernel_t:s0     root         8  0.0  0.0      0     0 ?        S    juin17   0:00 [rcu_bh]
system_u:system_r:kernel_t:s0     root         9  0.0  0.0      0     0 ?        S    juin17   0:17 [rcu_sched]
system_u:system_r:kernel_t:s0     root        10  0.0  0.0      0     0 ?        S    juin17   0:01 [watchdog/0]
system_u:system_r:kernel_t:s0     root        12  0.0  0.0      0     0 ?        S    juin17   0:00 [kdevtmpfs]
system_u:system_r:kernel_t:s0     root        13  0.0  0.0      0     0 ?        S<   juin17   0:00 [netns]
system_u:system_r:kernel_t:s0     root        14  0.0  0.0      0     0 ?        S    juin17   0:00 [khungtaskd]
system_u:system_r:kernel_t:s0     root        15  0.0  0.0      0     0 ?        S<   juin17   0:00 [writeback]
system_u:system_r:kernel_t:s0     root        16  0.0  0.0      0     0 ?        S<   juin17   0:00 [kintegrityd]
system_u:system_r:kernel_t:s0     root        17  0.0  0.0      0     0 ?        S<   juin17   0:00 [bioset]
system_u:system_r:kernel_t:s0     root        18  0.0  0.0      0     0 ?        S<   juin17   0:00 [kblockd]
system_u:system_r:kernel_t:s0     root        19  0.0  0.0      0     0 ?        S<   juin17   0:00 [md]
system_u:system_r:kernel_t:s0     root        25  0.0  0.0      0     0 ?        S    juin17   0:05 [kswapd0]
system_u:system_r:kernel_t:s0     root        26  0.0  0.0      0     0 ?        SN   juin17   0:00 [ksmd]
system_u:system_r:kernel_t:s0     root        27  0.0  0.0      0     0 ?        S<   juin17   0:00 [crypto]
system_u:system_r:kernel_t:s0     root        35  0.0  0.0      0     0 ?        S<   juin17   0:00 [kthrotld]
system_u:system_r:kernel_t:s0     root        37  0.0  0.0      0     0 ?        S<   juin17   0:00 [kmpath_rdacd]
system_u:system_r:kernel_t:s0     root        38  0.0  0.0      0     0 ?        S<   juin17   0:00 [kpsmoused]
system_u:system_r:kernel_t:s0     root        39  0.0  0.0      0     0 ?        S<   juin17   0:00 [ipv6_addrconf]
system_u:system_r:kernel_t:s0     root        59  0.0  0.0      0     0 ?        S<   juin17   0:00 [deferwq]
```

```
system_u:system_r:kernel_t:s0   root        94  0.0  0.0      0     0 ?        S    juin17   0:00 [kauditd]
system_u:system_r:kernel_t:s0   root       226  0.0  0.0      0     0 ?        S<   juin17   0:00 [ata_sff]
system_u:system_r:kernel_t:s0   root       238  0.0  0.0      0     0 ?        S    juin17   0:00 [scsi_eh_0]
system_u:system_r:kernel_t:s0   root       240  0.0  0.0      0     0 ?        S<   juin17   0:00 [scsi_tmf_0]
system_u:system_r:kernel_t:s0   root       241  0.0  0.0      0     0 ?        S    juin17   0:00 [scsi_eh_1]
system_u:system_r:kernel_t:s0   root       242  0.0  0.0      0     0 ?        S    juin17   0:02 [kworker/u2:2]
system_u:system_r:kernel_t:s0   root       243  0.0  0.0      0     0 ?        S<   juin17   0:00 [scsi_tmf_1]
system_u:system_r:kernel_t:s0   root       244  0.0  0.0      0     0 ?        S    juin17   0:00 [scsi_eh_2]
--Plus--
```

Visualiser la SC d'un Utilisateur

Utilisez l'option **-Z** avec la commande **id** :

```
[trainee@centos7 ~]$ id -Z
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

Notez que vous ne pouvez pas consulter le SC d'un autre utilisateur :

```
[trainee@centos7 ~]$ id root
uid=0(root) gid=0(root) groupes=0(root)
[trainee@centos7 ~]$ id -Z root
id: impossible d'afficher le contexte de sécurité quand un utilisateur est indiqué
```

Vérifier la SC d'un fichier

Il convient d'utiliser la commande ls avec l'option **-Z** :

```
[trainee@centos7 ~]$ cd /etc
[trainee@centos7 etc]$ ls -Z l* -d
-rw-r--r--. root root unconfined_u:object_r:ld_so_cache_t:s0 ld.so.cache
```

```
-rw-r--r--. root root system_u:object_r:etc_t:s0       ld.so.conf
drwxr-xr-x. root root system_u:object_r:etc_t:s0       ld.so.conf.d
-rw-r-----. root root system_u:object_r:etc_t:s0       libaudit.conf
drwxr-xr-x. root root system_u:object_r:etc_t:s0       libnl
drwxr-xr-x. root root system_u:object_r:etc_t:s0       libreport
-rw-r--r--. root root unconfined_u:object_r:etc_t:s0   libuser.conf
-rw-r--r--. root root unconfined_u:object_r:locale_t:s0 locale.conf
lrwxrwxrwx. root root unconfined_u:object_r:locale_t:s0 localtime -> ../usr/share/zoneinfo/Europe/Paris
-rw-r--r--. root root unconfined_u:object_r:etc_t:s0   login.defs
-rw-r--r--. root root system_u:object_r:etc_t:s0       logrotate.conf
drwxr-xr-x. root root system_u:object_r:etc_t:s0       logrotate.d
drwxr-xr-x. root root system_u:object_r:etc_t:s0       lsm
drwxr-xr-x. root root system_u:object_r:lvm_etc_t:s0   lvm
```

Troubleshooting SELinux

L'interprétation des messages journalisés de SELinux est souvent la clef d'un dépannage efficace et rapide.

Si le démon **auditd** est démarré, les messages de SELinux sont consignés dans le fichier **/var/log/audit/audit.log**. Dans le cas contraire, les mêmes messages sont consignés dans le fichier **/var/log/messages**. Dans les deux cas, chaque message de SELinux contient le mot clef **AVC** :

La commande chcon

La commande **chcon** permet de modifier *temporairement* une SC.

```
[trainee@centos7 etc]$ cd ~
[trainee@centos7 ~]$ chcon --help
Utilisation : chcon [OPTION]... CONTEXT FILE...
         ou : chcon [OPTION]... [-u USER] [-r ROLE] [-l RANGE] [-t TYPE] FILE...
         ou : chcon [OPTION]... --reference=RFILE FILE...
Modifier le contexte de sécurité SELinux de chaque FILE en CONTEXT.
```

```
Avec --reference, modifier le contexte de sécurité de chaque FILE à
celui de RFILE.

Les arguments obligatoires pour les options longues le sont aussi pour les
options courtes.
      --dereference      affecter le référent de chaque lien symbolique (par
                           défaut), au lieu du lien symbolique lui-même
  -h, --no-dereference   affecter les liens symboliques au lieu des fichiers
                           référencés
  -u, --user=USER        définir l'utilisateur USER dans le contexte de
                           sécurité cible
  -r, --role=ROLE        définir le rôle ROLE dans le contexte de sécurité cible
  -t, --type=TYPE        définir le type TYPE dans le contexte de sécurité cible
  -l, --range=RANGE      définir l'intervalle RANGE dans le contexte de
                         sécurité cible
      --no-preserve-root ne pas traiter « / » de manière spéciale (par défaut)
      --preserve-root    bloquer le traitement récursif sur « / »
      --reference=RFILE  utiliser le contexte de sécurité de RFILE au lieu
                           d'indiquer une valeur CONTEXT
  -R, --recursive        opérer récursivement sur les fichiers et répertoires
  -v, --verbose          afficher un diagnostic pour chaque fichier traité

Les options suivantes modifient la façon de parcourir la hiérarchie lorsque
l'option -R est aussi indiquée. Si plusieurs options sont indiquées, seule la
dernière sera prise en compte.

  -H                     si l'argument en ligne de commande est un lien
                           symbolique vers un répertoire, le parcourir
  -L                     parcourir tous les liens symboliques menant à un
                           répertoire
  -P                     ne parcourir aucun lien symbolique (par défaut)

      --help     afficher l'aide et quitter
      --version  afficher des informations de version et quitter
```

```
Aide en ligne de GNU coreutils : <http://www.gnu.org/software/coreutils/>
Signalez les problèmes de traduction de « chcon » à : <traduc@traduc.org>
Utilisez « info coreutils 'chcon invocation' » pour toute la documentation
```

Prenons le cas de la création d'un répertoire à la racine du système de fichiers afin d'y stocker les pages web du serveur apache :

```
[trainee@centos7 ~]$ su -
Mot de passe :
Dernière connexion : dimanche 17 juin 2018 à 20:21:42 CEST sur pts/1
[root@centos7 ~]# mkdir /www
[root@centos7 ~]# touch /www/index.html
```

Installez maintenant le serveur Apache :

```
[root@centos7 ~]# yum install httpd
```

Modifiez ensuite la directive **DocumentRoot** dans le fichier **/etc/httpd/conf/httpd.conf** :

```
[...]
#DocumentRoot "/var/www/html"
DocumentRoot "/www"
[...]
```

Ajoutez les section **<Directory “/www”>**:

```
...
<Directory "/var/www">
    AllowOverride None
    # Allow open access:
    Require all granted
</Directory>

<Directory "/www">
    Options Indexes FollowSymLinks
```

```
    AllowOverride None
    Require all granted
</Directory>

# Further relax access to the default document root:
<Directory "/var/www/html">
...
```

Créez le fichier **/www/index.html** :

```
[root@centos7 ~]# vi /www/index.html
[root@centos7 ~]# cat /www/index.html
<html>
<title>
This is a test
</title>
<body>
www test page
</body>
</html>
```

Modifiez ensuite le propriétaire et le groupe du répertoire **/www** et son contenu :

```
[root@centos7 ~]# chown -R apache:apache /www
```

Dernièrement, créez un fichier index.html **vide** dans le répertoire **/var/www/html/** :

```
[root@centos7 ~]# touch /var/www/html/index.html
```

Redémarrez maintenant le service httpd :

```
[root@centos7 ~]# systemctl restart httpd.service
```

Consultez le site localhost en utilisant **lynx** :

```
[root@centos7 ~]# lynx localhost
```

Pour consulter les messages d'alerte de SELinux, vous disposez de la commande **sealert** du paquet **setroubleshoot-server**.

Installez donc ce paquet :

```
[root@centos7 ~]# yum install setroubleshoot-server
```

La commande **sealert** possède à la fois une interface graphique **et** un mode en ligne de commande :

```
[root@centos7 ~]# sealert -a /var/log/audit/audit.log > /root/mylogfile.txt
type=AVC msg=audit(1524491216.546:616): avc:  denied  { getattr } for  pid=15389 comm="gssproxy" name="/"
dev="sda2" ino=128 scontext=system_u:system_r:gssproxy_t:s0 tcontext=system_u:object_r:fs_t:s0 tclass=filesystem

**** Invalid AVC allowed in current policy ***

type=AVC msg=audit(1524491220.766:622): avc:  denied  { getattr } for  pid=15459 comm="gssproxy" name="/"
dev="sda2" ino=128 scontext=system_u:system_r:gssproxy_t:s0 tcontext=system_u:object_r:fs_t:s0 tclass=filesystem

**** Invalid AVC allowed in current policy ***
```

Consultez le fichier **/root/mylogfile.txt** :

```
[root@centos7 ~]# more /root/mylogfile.txt

found 3 alerts in /var/log/audit/audit.log
--------------------------------------------------------------------------------

SELinux is preventing /usr/libexec/dbus-1/dbus-daemon-launch-helper from using the rlimitinh access on a process.

*****  Plugin catchall (100. confidence) suggests   **************************
```

```
you believe that dbus-daemon-launch-helper should be allowed rlimitinh access on processes labeled
unconfined_service_t by default.
Then you should report this as a bug.
You can generate a local policy module to allow this access.
Do
allow this access for now by executing:
# ausearch -c 'dbus-daemon-lau' --raw | audit2allow -M my-dbusdaemonlau
# semodule -i my-dbusdaemonlau.pp


Additional Information:
Source Context                system_u:system_r:system_dbusd_t:s0-s0:c0.c1023
Target Context                system_u:system_r:unconfined_service_t:s0-s0:c0.c1
                              023
Target Objects                Unknown [ process ]
Source                        dbus-daemon-lau
Source Path                   /usr/libexec/dbus-1/dbus-daemon-launch-helper
Port                          <Unknown>
Host                          <Unknown>
Source RPM Packages           dbus-1.10.24-13.el7_6.x86_64
Target RPM Packages
Policy RPM                    selinux-policy-3.13.1-166.el7_4.9.noarch
Selinux Enabled               True
Policy Type                   targeted
Enforcing Mode                Permissive
Host Name                     centos7.fenestros.loc
Platform                      Linux centos7.fenestros.loc
                              3.10.0-693.21.1.el7.x86_64 #1 SMP Wed Mar 7
                              19:03:37 UTC 2018 x86_64 x86_64
Alert Count                   1
First Seen                    2020-01-23 16:04:33 CET
Last Seen                     2020-01-23 16:04:33 CET
--More--(4%)
```

Cherchez dans le fichier la chaine **Plugin catchall** de la section concernant apache :

```
*****  Plugin catchall (17.1 confidence) suggests   **************************

you believe that httpd should be allowed getattr access on the index.html file by default.
Then you should report this as a bug.
You can generate a local policy module to allow this access.
Do
allow this access for now by executing:
# ausearch -c 'httpd' --raw | audit2allow -M my-httpd
# semodule -i my-httpd.pp


Additional Information:
Source Context                system_u:system_r:httpd_t:s0
Target Context                unconfined_u:object_r:default_t:s0
Target Objects                /www/index.html [ file ]
Source                        httpd
Source Path                   /usr/sbin/httpd
Port                          <Unknown>
Host                          <Unknown>
Source RPM Packages           httpd-2.4.6-90.el7.centos.x86_64
Target RPM Packages
Policy RPM                    selinux-policy-3.13.1-166.el7_4.9.noarch
Selinux Enabled               True
Policy Type                   targeted
Enforcing Mode                Permissive
Host Name                     centos7.fenestros.loc
Platform                      Linux centos7.fenestros.loc
                              3.10.0-693.21.1.el7.x86_64 #1 SMP Wed Mar 7
                              19:03:37 UTC 2018 x86_64 x86_64
Alert Count                   1
First Seen                    2020-01-23 16:04:30 CET
Last Seen                     2020-01-23 16:04:30 CET
```

```
Local ID                      096941d6-1c72-49bd-862b-9bfc3aad32e5

Raw Audit Messages
type=AVC msg=audit(1579791870.276:244): avc:  denied  { getattr } for  pid=1728 comm="httpd"
path="/www/index.html" dev="sda2" ino=2240172 scontext=system_u:system_r:httpd_t:s0
tcontext=unconfined_u:object_r:default_t:s0 tclass=file


type=SYSCALL msg=audit(1579791870.276:244): arch=x86_64 syscall=stat success=yes exit=0 a0=56255c9727b8
a1=7ffd44466030 a2=7ffd44466030 a3=7f3a4d9ab712 items=0 ppid=1722 pid=1728 auid=4294967295 uid=48 gid=48 euid=48
suid=48 fsuid=48 egid=48 sgid=48 fsgid=48 tty=(none) ses=4294967295 comm=httpd exe=/usr/sbin/httpd
subj=system_u:system_r:httpd_t:s0 key=(null)

Hash: httpd,httpd_t,default_t,file,getattr
```

Ce message a été généré parce que le repertoire /www ainsi que le fichier index.html ne possèdent pas le **type** nécessaire pour que le service apache puisse les utiliser :

```
[root@centos6 ~]# ls -Z /www/index.html
-rw-r--r--. root root unconfined_u:object_r:default_t:s0 /www/index.html
```

```
[root@centos7 ~]# ls -Z /var/www/html/index.html
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/index.html
```

L'exemple ci-dessus nous montre clairement que le type pour **/www/index.html** est **default_t** or apache a besoin du type **httpd_sys_content_t** pour pouvoir accéder au fichier.

Modifiez donc la SC de /www et /www/index.html en utilisant la commande **chcon** :

```
[root@centos7 ~]# chcon -Rv --type=httpd_sys_content_t /www
changing security context of ‘/www/index.html’
changing security context of ‘/www’

[root@centos7 ~]# ls -Z /www/index.html
```

```
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 /www/index.html
```

Afin de maintenir ces SC lors d'une **restauration des SC par défaut**, il convient d'utiliser la commande **semanage** afin d'appliquer la modification d'une manière définitive :

```
[root@centos7 ~]# semanage fcontext -a -t httpd_sys_content_t "/www(/.*)?"
```

La commande restorecon

```
usage:  restorecon [-iFnrRv] [-e excludedir ] [-o filename ] [-f filename | pathname... ]
```

Pour illustrer l'utilisation de cette commande, créez les fichiers copy.html et move.html dans le répertoire /tmp :

```
[root@centos7 ~]# cd /tmp ; touch copy.html move.html
[root@centos7 tmp]# ls -Z | grep html
-rw-r--r--. root root unconfined_u:object_r:user_tmp_t:s0 copy.html
-rw-r--r--. root root unconfined_u:object_r:user_tmp_t:s0 move.html
```

Copiez le fichier copy.html vers /var/www/html et **déplacez** le fichier move.html vers la même cible :

```
[root@centos7 tmp]# cp copy.html /var/www/html/
[root@centos7 tmp]# mv move.html /var/www/html/
[root@centos7 tmp]# ls -Z /var/www/html
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 copy.html
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 index.html
-rw-r--r--. root root unconfined_u:object_r:user_tmp_t:s0 move.html
```

Important : Notez ici que copy.html a pris le type du répertoire de destination tandis que move.html retient le type obtenu lors de la création.

Restaurez maintenant la SC par défaut de move.html compte tenu de son emplacement en utilisant la commande **restorecon** :

```
[root@centos7 tmp]# restorecon -v /var/www/html/move.html
restorecon reset /var/www/html/move.html context
unconfined_u:object_r:user_tmp_t:s0->unconfined_u:object_r:httpd_sys_content_t:s0

[root@centos7 tmp]# ls -Z /var/www/html
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 copy.html
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 index.html
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 move.html
```

Le fichier /.autorelabel

En cas de besoin il est intéressant de pouvoir restaurer les SC par défaut sur l'ensemble des objets du système. Cette procédure est très simple à mettre en oeuvre. Il convient de créer le fichier **.autorelabel** à la racine et de redémarrer le système :

```
[root@centos7 tmp]# touch /.autorelabel
[root@centos7 tmp]# shutdown -r now
```

La commande semanage

La commande **semanage** peut prendre plusieurs options :

```
[root@centos7 tmp]# semanage --help
usage: semanage [-h]
                {import,export,login,user,port,interface,module,node,fcontext,boolean,permissive,dontaudit}
                ...

semanage is used to configure certain elements of SELinux policy with-out
requiring modification to or recompilation from policy source.
```

```
positional arguments:
  {import,export,login,user,port,interface,module,node,fcontext,boolean,permissive,dontaudit}
    import              Import local customizations
    export              Output local customizations
    login               Manage login mappings between linux users and SELinux
                        confined users
    user                Manage SELinux confined users (Roles and levels for an
                        SELinux user)
    port                Manage network port type definitions
    interface           Manage network interface type definitions
    module              Manage SELinux policy modules
    node                Manage network node type definitions
    fcontext            Manage file context mapping definitions
    boolean             Manage booleans to selectively enable functionality
    permissive          Manage process type enforcement mode
    dontaudit           Disable/Enable dontaudit rules in policy

optional arguments:
  -h, --help            show this help message and exit
```

Pour illustrer l'utilisation de cette commande, considérez le besoin de mettre le service apache à l'écoute du port **8090** au lieu du port standard.

SELinux gère aussi l'accès aux ports par les différents serveurs. La liste complète des ports autorisés par serveur puet être visualiser à l'aide de la commande **semanage** :

```
[root@centos7 tmp]# semanage port -l
SELinux Port Type              Proto    Port Number

afs3_callback_port_t           tcp      7001
afs3_callback_port_t           udp      7001
afs_bos_port_t                 udp      7007
afs_fs_port_t                  tcp      2040
afs_fs_port_t                  udp      7000, 7005
afs_ka_port_t                  udp      7004
```

```
afs_pt_port_t                  tcp      7002
afs_pt_port_t                  udp      7002
afs_vl_port_t                  udp      7003
agentx_port_t                  tcp      705
agentx_port_t                  udp      705
amanda_port_t                  tcp      10080-10083
amanda_port_t                  udp      10080-10082
amavisd_recv_port_t            tcp      10024
amavisd_send_port_t            tcp      10025
amqp_port_t                    tcp      15672, 5671-5672
amqp_port_t                    udp      5671-5672
aol_port_t                     tcp      5190-5193
aol_port_t                     udp      5190-5193
apc_port_t                     tcp      3052
apc_port_t                     udp      3052
apcupsd_port_t                 tcp      3551
apcupsd_port_t                 udp      3551
apertus_ldp_port_t             tcp      539
apertus_ldp_port_t             udp      539
asterisk_port_t                tcp      1720
asterisk_port_t                udp      2427, 2727, 4569
audit_port_t                   tcp      60
auth_port_t                    tcp      113
bacula_port_t                  tcp      9103
bacula_port_t                  udp      9103
bctp_port_t                    tcp      8999
bctp_port_t                    udp      8999
bgp_port_t                     tcp      179, 2605
bgp_port_t                     udp      179, 2605
boinc_client_port_t            tcp      1043
boinc_client_port_t            udp      1034
boinc_port_t                   tcp      31416
brlp_port_t                    tcp      4101
certmaster_port_t              tcp      51235
```

```
chronyd_port_t                 udp      323
clamd_port_t                   tcp      3310
clockspeed_port_t              udp      4041
cluster_port_t                 tcp      5149, 40040, 50006-50008
cluster_port_t                 udp      5149, 50006-50008
cma_port_t                     tcp      1050
cma_port_t                     udp      1050
cobbler_port_t                 tcp      25151
collectd_port_t                udp      25826
commplex_link_port_t           tcp      4331, 5001
commplex_link_port_t           udp      5001
commplex_main_port_t           tcp      5000
commplex_main_port_t           udp      5000
comsat_port_t                  udp      512
condor_port_t                  tcp      9618
condor_port_t                  udp      9618
conman_port_t                  tcp      7890
conman_port_t                  udp      7890
connlcli_port_t                tcp      1358
connlcli_port_t                udp      1358
couchdb_port_t                 tcp      5984, 6984
couchdb_port_t                 udp      5984, 6984
ctdb_port_t                    tcp      4379
ctdb_port_t                    udp      4379
cvs_port_t                     tcp      2401
cvs_port_t                     udp      2401
cyphesis_port_t                tcp      6767, 6769, 6780-6799
cyphesis_port_t                udp      32771
cyrus_imapd_port_t             tcp      2005
daap_port_t                    tcp      3689
daap_port_t                    udp      3689
dbskkd_port_t                  tcp      1178
dcc_port_t                     udp      6276, 6277
dccm_port_t                    tcp      5679
```

```
dccm_port_t                    udp      5679
dey_keyneg_port_t              tcp      8750
dey_keyneg_port_t              udp      8750
dey_sapi_port_t                tcp      4330
dhcpc_port_t                   tcp      68, 546, 5546
dhcpc_port_t                   udp      68, 546, 5546
dhcpd_port_t                   tcp      547, 548, 647, 847, 7911
dhcpd_port_t                   udp      67, 547, 548, 647, 847
dict_port_t                    tcp      2628
distccd_port_t                 tcp      3632
dns_port_t                     tcp      53
dns_port_t                     udp      53
dnssec_port_t                  tcp      8955
dogtag_port_t                  tcp      7390
echo_port_t                    tcp      7
echo_port_t                    udp      7
efs_port_t                     tcp      520
embrace_dp_c_port_t            tcp      3198
embrace_dp_c_port_t            udp      3198
ephemeral_port_t               tcp      32768-61000
ephemeral_port_t               udp      32768-61000
epmap_port_t                   tcp      135
epmap_port_t                   udp      135
epmd_port_t                    tcp      4369
epmd_port_t                    udp      4369
fac_restore_port_t             tcp      5582
fac_restore_port_t             udp      5582
fingerd_port_t                 tcp      79
flash_port_t                   tcp      843, 1935
flash_port_t                   udp      1935
fmpro_internal_port_t          tcp      5003
fmpro_internal_port_t          udp      5003
freeipmi_port_t                tcp      9225
freeipmi_port_t                udp      9225
```

```
ftp_data_port_t                tcp      20
ftp_port_t                     tcp      21, 989, 990
ftp_port_t                     udp      989, 990
gatekeeper_port_t              tcp      1721, 7000
gatekeeper_port_t              udp      1718, 1719
gdomap_port_t                  tcp      538
gdomap_port_t                  udp      538
gds_db_port_t                  tcp      3050
gds_db_port_t                  udp      3050
gear_port_t                    tcp      43273
gear_port_t                    udp      43273
geneve_port_t                  tcp      6080
giftd_port_t                   tcp      1213
git_port_t                     tcp      9418
git_port_t                     udp      9418
glance_port_t                  tcp      9292
glance_port_t                  udp      9292
glance_registry_port_t         tcp      9191
glance_registry_port_t         udp      9191
gluster_port_t                 tcp      38465-38469, 24007-24027
gluster_port_t                 udp      24007-24027
gopher_port_t                  tcp      70
gopher_port_t                  udp      70
gpsd_port_t                    tcp      2947
hadoop_datanode_port_t         tcp      50010
hadoop_namenode_port_t         tcp      8020
hddtemp_port_t                 tcp      7634
hi_reserved_port_t             tcp      512-1023
hi_reserved_port_t             udp      512-1023
howl_port_t                    tcp      5335
howl_port_t                    udp      5353
hplip_port_t                   tcp      1782, 2207, 2208, 8290, 8292, 9100, 9101, 9102, 9220, 9221, 9222, 9280,
9281, 9282, 9290, 9291, 50000, 50002
http_cache_port_t              tcp      8080, 8118, 8123, 10001-10010
```

```
http_cache_port_t              udp      3130
http_port_t                    tcp      80, 81, 443, 488, 8008, 8009, 8443, 9000
...
```

Notez par exemple que le serveur apache est autorisé d'utiliser les ports suivants :

```
http_port_t                    tcp      80, 81, 443, 488, 8008, 8009, 8443, 9000
```

Dans le cas où on souhaite qu'apache utilise le port **8090** par exemple, il est nécessaire de créer la règle adéquate avec la commande semanage :

```
[root@centos7 ~]# semanage port -a -t http_port_t -p tcp 8090
```

Vous noterez que le port 8090 a été ajouté à la liste des ports reconnus comme valides par SELinux :

```
[root@centos7 tmp]# semanage port -l | grep http
http_cache_port_t              tcp      8080, 8118, 8123, 10001-10010
http_cache_port_t              udp      3130
http_port_t                    tcp      8090, 80, 81, 443, 488, 8008, 8009, 8443, 9000
pegasus_http_port_t            tcp      5988
pegasus_https_port_t           tcp      5989
```

La commande audit2allow

```
[root@centos7 tmp]# audit2allow --help
Usage: audit2allow [options]

Options:
  --version             show program's version number and exit
  -h, --help            show this help message and exit
  -b, --boot            audit messages since last boot conflicts with -i
  -a, --all             read input from audit log - conflicts with -i
  -p POLICY, --policy=POLICY
```

```
                        Policy file to use for analysis
  -d, --dmesg           read input from dmesg - conflicts with --all and
                        --input
  -i INPUT, --input=INPUT
                        read input from <input> - conflicts with -a
  -l, --lastreload      read input only after the last reload
  -r, --requires        generate require statements for rules
  -m MODULE, --module=MODULE
                        set the module name - implies --requires
  -M MODULE_PACKAGE, --module-package=MODULE_PACKAGE
                        generate a module package - conflicts with -o and -m
  -o OUTPUT, --output=OUTPUT
                        append output to <filename>, conflicts with -M
  -D, --dontaudit       generate policy with dontaudit rules
  -R, --reference       generate refpolicy style output
  -N, --noreference     do not generate refpolicy style output
  -v, --verbose         explain generated output
  -e, --explain         fully explain generated output
  -t TYPE, --type=TYPE  only process messages with a type that matches this
                        regex
  --perm-map=PERM_MAP   file name of perm map
  --interface-info=INTERFACE_INFO
                        file name of interface information
  --debug               leave generated modules for -M
  -w, --why             Translates SELinux audit messages into a description
                        of why the access was denied
```

La création d'un module de politique personnalisé se fait en utilisant la commande **audit2allow**. L'administrateur de sécurité à recours à la création de modules quand, et uniquement quand :

- la résolution du problème n'est pas possible en utilisant une des commandes précédemment citées,
- il n'existe pas de booléen capable de régler le problème.

Pour illustrer l'utilisation de cette commande, créez un nouveau répertoire pour les documents d'apache ainsi que la page d'accueil :

```
[root@centos7 tmp]# mkdir /www1
[root@centos7 tmp]# touch /www1/index.html
```

Éditez le fichier **/etc/httpd/conf/httpd.conf** :

```
[...]
#DocumentRoot "/var/www/html"
DocumentRoot "/www1"
[...]
```

Ajoutez les section **<Directory “/www”>**:

```
...
<Directory "/var/www">
    AllowOverride None
    # Allow open access:
    Require all granted
</Directory>

<Directory "/www1">
    Options Indexes FollowSymLinks
    AllowOverride None
    Require all granted
</Directory>

# Further relax access to the default document root:
<Directory "/var/www/html">
...
```

Créez le fichier **/www1/index.html** :

```
[root@centos7 ~]# cd ~
[root@centos7 ~]# vi /www1/index.html
```

```
[root@centos7 ~]# cat /www1/index.html
<html>
<title>
This is a test
</title>
<body>
www test page
</body>
</html>
```

Modifiez ensuite le propriétaire et le groupe du répertoire **/www1** et son contenu :

```
[root@centos7 ~]# chown -R apache:apache /www1
```

Redémarrez le service httpd :

```
[root@centos7 ~]# systemctl restart httpd.service
```

Consultez le site localhost en utilisant **lynx** :

```
[root@centos7 ~]# lynx localhost
```

Le fichier **/var/log/audit/audit.log** contient maintenant des notifications de type **AVC** :

```
[root@centos7 ~]# cat /var/log/audit/audit.log | grep AVC
type=USER_AVC msg=audit(1462020229.957:425): pid=1 uid=0 auid=4294967295 ses=4294967295
subj=system_u:system_r:init_t:s0 msg='avc:  received policyload notice (seqno=2)  exe="/usr/lib/systemd/systemd"
sauid=0 hostname=? addr=? terminal=?'
type=AVC msg=audit(1524491216.546:616): avc:  denied  { getattr } for  pid=15389 comm="gssproxy" name="/"
dev="sda2" ino=128 scontext=system_u:system_r:gssproxy_t:s0 tcontext=system_u:object_r:fs_t:s0 tclass=filesystem
type=AVC msg=audit(1524491220.766:622): avc:  denied  { getattr } for  pid=15459 comm="gssproxy" name="/"
dev="sda2" ino=128 scontext=system_u:system_r:gssproxy_t:s0 tcontext=system_u:object_r:fs_t:s0 tclass=filesystem
type=AVC msg=audit(1529418883.052:818): avc:  denied  { getattr } for  pid=10071 comm="httpd"
path="/www/index.html" dev="sda2" ino=35670335 scontext=system_u:system_r:httpd_t:s0
```

```
tcontext=unconfined_u:object_r:default_t:s0 tclass=file
type=AVC msg=audit(1529418883.052:819): avc:  denied  { getattr } for  pid=10071 comm="httpd"
path="/www/index.html" dev="sda2" ino=35670335 scontext=system_u:system_r:httpd_t:s0
tcontext=unconfined_u:object_r:default_t:s0 tclass=file
type=AVC msg=audit(1529418919.091:822): avc:  denied  { getattr } for  pid=10385 comm="httpd"
path="/www/index.html" dev="sda2" ino=35670335 scontext=system_u:system_r:httpd_t:s0
tcontext=unconfined_u:object_r:default_t:s0 tclass=file
type=AVC msg=audit(1529418919.092:823): avc:  denied  { getattr } for  pid=10385 comm="httpd"
path="/www/index.html" dev="sda2" ino=35670335 scontext=system_u:system_r:httpd_t:s0
tcontext=unconfined_u:object_r:default_t:s0 tclass=file
type=AVC msg=audit(1529418954.500:826): avc:  denied  { getattr } for  pid=10669 comm="httpd"
path="/www/index.html" dev="sda2" ino=35670335 scontext=system_u:system_r:httpd_t:s0
tcontext=unconfined_u:object_r:default_t:s0 tclass=file
type=AVC msg=audit(1529418954.500:827): avc:  denied  { getattr } for  pid=10669 comm="httpd"
path="/www/index.html" dev="sda2" ino=35670335 scontext=system_u:system_r:httpd_t:s0
tcontext=unconfined_u:object_r:default_t:s0 tclass=file
type=AVC msg=audit(1529419054.949:865): avc:  denied  { getattr } for  pid=10670 comm="httpd"
path="/www/index.html" dev="sda2" ino=35670335 scontext=system_u:system_r:httpd_t:s0
tcontext=unconfined_u:object_r:default_t:s0 tclass=file
type=AVC msg=audit(1529419054.949:866): avc:  denied  { getattr } for  pid=10670 comm="httpd"
path="/www/index.html" dev="sda2" ino=35670335 scontext=system_u:system_r:httpd_t:s0
tcontext=unconfined_u:object_r:default_t:s0 tclass=file
type=USER_AVC msg=audit(1529421001.608:919): pid=1 uid=0 auid=4294967295 ses=4294967295
subj=system_u:system_r:init_t:s0 msg='avc:  received policyload notice (seqno=2)  exe="/usr/lib/systemd/systemd"
sauid=0 hostname=? addr=? terminal=?'
type=USER_AVC msg=audit(1529421602.007:946): pid=1 uid=0 auid=4294967295 ses=4294967295
subj=system_u:system_r:init_t:s0 msg='avc:  received policyload notice (seqno=3)  exe="/usr/lib/systemd/systemd"
sauid=0 hostname=? addr=? terminal=?'
type=AVC msg=audit(1529422368.058:1019): avc:  denied  { getattr } for  pid=1755 comm="httpd"
path="/www1/index.html" dev="sda2" ino=53579496 scontext=system_u:system_r:httpd_t:s0
tcontext=unconfined_u:object_r:default_t:s0 tclass=file
type=AVC msg=audit(1529422368.058:1020): avc:  denied  { getattr } for  pid=1755 comm="httpd"
path="/www1/index.html" dev="sda2" ino=53579496 scontext=system_u:system_r:httpd_t:s0
tcontext=unconfined_u:object_r:default_t:s0 tclass=file
```

A l'aide de la commande grep, il convient maintenant d'envoyer les messages d'erreurs en provenance du fichier **/var/log/audit/audit.log** sur l'entrée standard de la commande **audit2allow** afin de permettre celle-ci de créer des règles permettant l'autorisation de ce qui a été précédemment interdit par SELinux :

```
[root@centos7 ~]# grep httpd_t /var/log/audit/audit.log | audit2allow -m httpdlocal > httpdlocal.te
```

L'examen du fichier **httpdlocal.te** révèle la création de ces règles :

```
[root@centos7 ~]# cat httpdlocal.te

module httpdlocal 1.0;

require {
    type httpd_t;
    type default_t;
    class file getattr;
}

#============= httpd_t ==============

#!!!! WARNING: 'default_t' is a base type.
#!!!! The file '/www/index.html' is mislabeled on your system.
#!!!! Fix with $ restorecon -R -v /www/index.html
allow httpd_t default_t:file getattr;
```

L'audit du fichier terminé, il faut maintenant utiliser audit2allow pour fabriquer un module de politique :

```
[root@centos7 ~]# grep httpd_t /var/log/audit/audit.log | audit2allow -M httpdlocal
******************** IMPORTANT ***********************
To make this policy package active, execute:

semodule -i httpdlocal.pp
```

Chargez maintenant le module dans la politique SELinux :

```
[root@centos7 ~]# semodule -i httpdlocal.pp
```

Vérifiez que le module est chargé :

```
[root@centos7 ~]# semodule -l | grep httpd
httpdlocal  1.0
```

Redémarrez le service httpd :

```
[root@centos7 ~]# systemctl restart httpd.service
```

Videz le fichier **/var/log/audit/audit.log** :

```
[root@centos7 ~]# vi /var/log/audit/audit.log
```

Consultez le site localhost :

```
[root@centos7 ~]# lynx localhost
```

Constatez que la consultation ne génère plus de messages de type **AVC** :

```
[root@centos7 ~]# cat /var/log/audit/audit.log
[root@centos7 ~]#
```
