Version : **2026.01**

Dernière mise-à-jour : 2025/12/09 10:23

LDF405 - System Hardening

Contenu du Module

- **LDF405 - System Hardening**
  - Contenu du Module
  - System Hardening Manuel
    - Les compilateurs
    - Les paquets
    - Les démons et services
    - Les fichiers .rhosts
    - Les fichiers et les répertoires sans propriétaire
    - Interdire les connexions de root via le réseau
    - Limiter le delai d’inactivité d'une session shell
    - Renforcer la sécurité 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 Lynis
    - 1.1 - Présentation
    - 1.2 - Installation
    - 1.3 - Utilisation
  - LAB #2 - System Hardening à l'aide de l'outil Bastille
    - 2.1 - Présentation
    - 2.2 - Installation
    - 2.3 - Utilisation

- LAB #3 - Mise en Place d'un Chroot pour isoler un utilisateur/une application
- LAB #4 - Mise en place d'AppArmor pour sécuriser le serveur
  - 4.1 - Présentation
  - 4.2 - Définitions
    - Les Profils d'AppArmor
    - Les Etats ou Modes d'AppArmor
  - 4.3 - Installation
    - Installation des Paquets
    - Modification de GRUB
    - Vérification de l'Activation d'AppArmor
- LAB #5 - Travailler avec AppArmor
  - 5.1 - Consulter la Liste des Profils Chargés
    - La Commande aa-status
  - 5.2 - Passer le Mode d'un Profil de Complain à Enforce
    - La Commande aa-complain
  - 5.3 - Passer le Mode d'un Profil d'Enforce à Complain
    - La Commande aa-enforce
  - 5.4 - Désactiver et Réactiver tous les Profils
  - 5.5 - Créer un Profil
    - La Commande aa-genprof
    - La Commande aa-logprof
  - 5.6 - Supprimer un Profil
    - La Commande apparmor_parser
    - La Commande aa-remove-unknown
- LAB #6 - Mise en place de SELinux pour sécuriser le serveur
  - 6.1 - Présentation
  - 6.2 - 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
- 6.3 - Commandes SELinux
- 6.4 - Les Etats de SELinux
- 6.5 - Booléens

- LAB #7 - Travailler avec SELinux
  - 7.1 - Copier et Déplacer des Fichiers
  - 7.2 - Vérifier les SC des Processus
  - 7.3 - Visualiser la SC d'un Utilisateur
  - 7.4 - Vérifier la SC d'un fichier
  - 7.5 - Troubleshooting SELinux
    - La commande chcon
    - La commande restorecon
  - 7.6 - Le fichier /.autorelabel
  - 7.7 - La commande semanage
  - 7.8 - 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 installés puis de supprimer ceux qui sont jugés être inutiles :

```
root@debian12:~# dpkg --get-selections | more
acl                                             install
adduser                                         install
adwaita-icon-theme                              install
afick                                           install
afick-gui                                       deinstall
alsa-topology-conf                              install
alsa-ucm-conf                                   install
alsa-utils                                      install
anacron                                         install
apache2                                         install
apache2-bin                                     install
apache2-data                                    install
apache2-utils                                   install
apparmor                                        install
apt                                             install
apt-listchanges                                 install
apt-utils                                       install
aspell                                          install
aspell-en                                       install
at-spi2-common                                  install
at-spi2-core                                    install
atril                                           install
atril-common                                    install
--More--
```

Important : Avec une distribution basée sur RedHat, utilisez la commande **rpm -qa | 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 jugés être inutiles;

- ps aux
- systemctl list-unit-files
- chkconfig –list (pour les systèmes n'utilisant pas systemd)

```
root@debian12:~# ps aux | more
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.0  0.0 168564 13040 ?        Ss   Nov26   0:09 /sbin/init
root           2  0.0  0.0      0     0 ?        S    Nov26   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        I<   Nov26   0:00 [rcu_gp]
root           4  0.0  0.0      0     0 ?        I<   Nov26   0:00 [rcu_par_gp]
root           5  0.0  0.0      0     0 ?        I<   Nov26   0:00 [slub_flushwq]
root           6  0.0  0.0      0     0 ?        I<   Nov26   0:00 [netns]
root           8  0.0  0.0      0     0 ?        I<   Nov26   0:00 [kworker/0:0H-events_highpri]
root          10  0.0  0.0      0     0 ?        I<   Nov26   0:00 [mm_percpu_wq]
root          11  0.0  0.0      0     0 ?        I    Nov26   0:00 [rcu_tasks_kthread]
root          12  0.0  0.0      0     0 ?        I    Nov26   0:00 [rcu_tasks_rude_kthread]
root          13  0.0  0.0      0     0 ?        I    Nov26   0:00 [rcu_tasks_trace_kthread]
root          14  0.0  0.0      0     0 ?        S    Nov26   0:00 [ksoftirqd/0]
root          15  0.0  0.0      0     0 ?        I    Nov26   0:01 [rcu_preempt]
root          16  0.0  0.0      0     0 ?        S    Nov26   0:01 [migration/0]
root          18  0.0  0.0      0     0 ?        S    Nov26   0:00 [cpuhp/0]
root          19  0.0  0.0      0     0 ?        S    Nov26   0:00 [cpuhp/1]
root          20  0.0  0.0      0     0 ?        S    Nov26   0:02 [migration/1]
root          21  0.0  0.0      0     0 ?        S    Nov26   0:00 [ksoftirqd/1]
root          23  0.0  0.0      0     0 ?        I<   Nov26   0:00 [kworker/1:0H-events_highpri]
root          24  0.0  0.0      0     0 ?        S    Nov26   0:00 [cpuhp/2]
root          25  0.0  0.0      0     0 ?        S    Nov26   0:02 [migration/2]
root          26  0.0  0.0      0     0 ?        S    Nov26   0:00 [ksoftirqd/2]
root          28  0.0  0.0      0     0 ?        I<   Nov26   0:00 [kworker/2:0H-events_highpri]
root          29  0.0  0.0      0     0 ?        S    Nov26   0:00 [cpuhp/3]
```

```
root          30  0.0  0.0      0     0 ?        S    Nov26   0:02 [migration/3]
root          31  0.0  0.0      0     0 ?        S    Nov26   0:00 [ksoftirqd/3]
root          33  0.0  0.0      0     0 ?        I<   Nov26   0:00 [kworker/3:0H-events_highpri]
root          34  0.0  0.0      0     0 ?        S    Nov26   0:00 [cpuhp/4]
root          35  0.0  0.0      0     0 ?        S    Nov26   0:02 [migration/4]
root          36  0.0  0.0      0     0 ?        S    Nov26   0:00 [ksoftirqd/4]
root          38  0.0  0.0      0     0 ?        I<   Nov26   0:00 [kworker/4:0H-events_highpri]
root          39  0.0  0.0      0     0 ?        S    Nov26   0:00 [cpuhp/5]
root          40  0.0  0.0      0     0 ?        S    Nov26   0:02 [migration/5]
root          41  0.0  0.0      0     0 ?        S    Nov26   0:00 [ksoftirqd/5]
root          43  0.0  0.0      0     0 ?        I<   Nov26   0:00 [kworker/5:0H-events_highpri]
root          44  0.0  0.0      0     0 ?        S    Nov26   0:00 [cpuhp/6]
root          45  0.0  0.0      0     0 ?        S    Nov26   0:02 [migration/6]
root          46  0.0  0.0      0     0 ?        S    Nov26   0:00 [ksoftirqd/6]
root          48  0.0  0.0      0     0 ?        I<   Nov26   0:00 [kworker/6:0H-events_highpri]
root          49  0.0  0.0      0     0 ?        S    Nov26   0:00 [cpuhp/7]
root          50  0.0  0.0      0     0 ?        S    Nov26   0:02 [migration/7]
root          51  0.0  0.0      0     0 ?        S    Nov26   0:00 [ksoftirqd/7]
root          53  0.0  0.0      0     0 ?        I<   Nov26   0:00 [kworker/7:0H-events_highpri]
root          62  0.0  0.0      0     0 ?        S    Nov26   0:00 [kdevtmpfs]
root          63  0.0  0.0      0     0 ?        I<   Nov26   0:00 [inet_frag_wq]
root          64  0.0  0.0      0     0 ?        S    Nov26   0:00 [kauditd]
root          65  0.0  0.0      0     0 ?        S    Nov26   0:00 [khungtaskd]
root          66  0.0  0.0      0     0 ?        S    Nov26   0:00 [oom_reaper]
root          67  0.0  0.0      0     0 ?        I<   Nov26   0:00 [writeback]
root          68  0.0  0.0      0     0 ?        S    Nov26   0:12 [kcompactd0]
root          69  0.0  0.0      0     0 ?        SN   Nov26   0:00 [ksmd]
root          70  0.0  0.0      0     0 ?        SN   Nov26   0:02 [khugepaged]
root          71  0.0  0.0      0     0 ?        I<   Nov26   0:00 [kintegrityd]
root          72  0.0  0.0      0     0 ?        I<   Nov26   0:00 [kblockd]
--More--
```

```
root@debian12:~# systemctl list-unit-files | more
UNIT FILE                                                                  STATE           PRESET
```

```
proc-sys-fs-binfmt_misc.automount                                static          -
-.mount                                                          generated       -
dev-hugepages.mount                                              static          -
dev-mqueue.mount                                                 static          -
media-cdrom0.mount                                               generated       -
proc-sys-fs-binfmt_misc.mount                                    disabled        disabled
snap-core-17247.mount                                            enabled         enabled
snap-core24-1225.mount                                           enabled         enabled
snap-john\x2dthe\x2dripper-706.mount                             enabled         enabled
snap-snapd-25577.mount                                           enabled         enabled
sys-fs-fuse-connections.mount                                    static          -
sys-kernel-config.mount                                          static          -
sys-kernel-debug.mount                                           static          -
sys-kernel-tracing.mount                                         static          -
cups.path                                                        enabled         enabled
systemd-ask-password-console.path                                static          -
systemd-ask-password-plymouth.path                               static          -
systemd-ask-password-wall.path                                   static          -
session-100.scope                                                transient       -
session-11.scope                                                 transient       -
session-112.scope                                                transient       -
session-18.scope                                                 transient       -
session-c1.scope                                                 transient       -
alsa-restore.service                                             static          -
alsa-state.service                                               static          -
alsa-utils.service                                               masked          enabled
anacron.service                                                  enabled         enabled
apache-htcacheclean.service                                      disabled        enabled
apache-htcacheclean@.service                                     disabled        enabled
apache2.service                                                  enabled         enabled
apache2@.service                                                 disabled        enabled
apparmor.service                                                 enabled         enabled
apt-daily-upgrade.service                                        static          -
apt-daily.service                                                static          -
```

```
autovt@.service                                                 alias           -
avahi-daemon.service                                            enabled         enabled
colord.service                                                  static          -
configure-printer@.service                                      static          -
console-getty.service                                           disabled        disabled
console-setup.service                                           enabled         enabled
container-getty@.service                                        static          -
cron.service                                                    enabled         enabled
cryptdisks-early.service                                        masked          enabled
cryptdisks.service                                              masked          enabled
cups-browsed.service                                            enabled         enabled
cups.service                                                    enabled         enabled
dbus-fi.w1.wpa_supplicant1.service                              alias           -
dbus-org.fedoraproject.FirewallD1.service                       alias           -
dbus-org.freedesktop.Avahi.service                              alias           -
dbus-org.freedesktop.hostname1.service                          alias           -
dbus-org.freedesktop.locale1.service                            alias           -
dbus-org.freedesktop.login1.service                             alias           -
dbus-org.freedesktop.ModemManager1.service                      alias           -
dbus-org.freedesktop.nm-dispatcher.service                      alias           -
--More--
```

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@debian12:~# vi /etc/securetty

root@debian12:~# cat /etc/securetty
# Virtual Consoles (local access)
tty1
tty2
tty3
tty4
tty5
tty6

# System Console (rarely needed for direct root login)
console
```

Important : 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. Un fichier /etc/securetty **vide** empechera toute connexion directe de l'utilisateur root. Notez que le fichier /etc/securetty n'a aucune incidence sur les connexions SSH.

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@debian12:~# cat /etc/profile
# /etc/profile: system-wide .profile file for the Bourne shell (sh(1))
# and Bourne compatible shells (bash(1), ksh(1), ash(1), ...).

if [ "$(id -u)" -eq 0 ]; then
  PATH="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"
else
  PATH="/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games"
fi
export PATH

if [ "${PS1-}" ]; then
  if [ "${BASH-}" ] && [ "$BASH" != "/bin/sh" ]; then
    # The file bash.bashrc already sets the default PS1.
    # PS1='\h:\w\$ '
    if [ -f /etc/bash.bashrc ]; then
      . /etc/bash.bashrc
```

```
    fi
  else
    if [ "$(id -u)" -eq 0 ]; then
      PS1='# '
    else
      PS1='$ '
    fi
  fi
fi

if [ -d /etc/profile.d ]; then
  for i in /etc/profile.d/*.sh; do
    if [ -r $i ]; then
      . $i
    fi
  done
  unset i
fi
```

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/login.defs**.

Renforcer la securite d'init

Les Distributions SysVInit

Le fichier **/etc/inittab** est utilisé 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 un 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"
```

Les Distributions Systemd

Afin d'empêcher une personne à redémarrer le serveur à l'aide des touches **ctrl+alt+supp**, saisissez la commande suivante :

```
# systemctl mask ctrl-alt-del.target
```

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 consignées dans le fichier **/etc/sysctl.conf** au démarrage de la machine.

Saisissez la commande :

```
root@debian12:~# cat /etc/sysctl.conf
#
# /etc/sysctl.conf - Configuration file for setting system variables
# See /etc/sysctl.d/ for additional system variables.
# See sysctl.conf (5) for information.
#

#kernel.domainname = example.com

# Uncomment the following to stop low-level messages on console
#kernel.printk = 3 4 1 3

###################################################################
```

```
# Functions previously found in netbase
#

# Uncomment the next two lines to enable Spoof protection (reverse-path filter)
# Turn on Source Address Verification in all interfaces to
# prevent some spoofing attacks
#net.ipv4.conf.default.rp_filter=1
#net.ipv4.conf.all.rp_filter=1

# Uncomment the next line to enable TCP/IP SYN cookies
# See http://lwn.net/Articles/277146/
# Note: This may impact IPv6 TCP sessions too
#net.ipv4.tcp_syncookies=1

# Uncomment the next line to enable packet forwarding for IPv4
#net.ipv4.ip_forward=1

# Uncomment the next line to enable packet forwarding for IPv6
#  Enabling this option disables Stateless Address Autoconfiguration
#  based on Router Advertisements for this host
#net.ipv6.conf.all.forwarding=1


###################################################################
# Additional settings - these settings can improve the network
# security of the host and prevent against some network attacks
# including spoofing attacks and man in the middle attacks through
# redirection. Some network environments, however, require that these
# settings are disabled so review and enable them as needed.
#
# Do not accept ICMP redirects (prevent MITM attacks)
#net.ipv4.conf.all.accept_redirects = 0
#net.ipv6.conf.all.accept_redirects = 0
# _or_
```

```
# Accept ICMP redirects only for gateways listed in our default
# gateway list (enabled by default)
# net.ipv4.conf.all.secure_redirects = 1
#
# Do not send ICMP redirects (we are not a router)
#net.ipv4.conf.all.send_redirects = 0
#
# Do not accept IP source route packets (we are not a router)
#net.ipv4.conf.all.accept_source_route = 0
#net.ipv6.conf.all.accept_source_route = 0
#
# Log Martian Packets
#net.ipv4.conf.all.log_martians = 1
#

###################################################################
# Magic system request Key
# 0=disable, 1=enable all, >1 bitmask of sysrq functions
# See https://www.kernel.org/doc/html/latest/admin-guide/sysrq.html
# for what other values do
#kernel.sysrq=438
```

Options de la commande

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

```
root@debian12:~# 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
      --dry-run         Print the key and values but do not write
  -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 the given variable(s)
  -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 Lynis

1.1 - Présentation

Lynis est un outil de renforcement de la sécurité pour certaines distributions de Linux dont RHEL, CentOS et Debian.

1.2 - Installation

Installez Lynis en utilisant APT :

```
root@debian12:~# apt install lynis
```

1.3 - Utilisation

Pour démarrez Lynis, saisissez la commande suivante :

```
root@debian12:~# lynis audit system

[ Lynis 3.0.8 ]

################################################################################
  Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
  welcome to redistribute it under the terms of the GNU General Public License.
  See the LICENSE file for details about using this software.

  2007-2021, CISOfy - https://cisofy.com/lynis/
  Enterprise support available (compliance, plugins, interface and tools)
################################################################################


[+] Initializing program
------------------------------------
  - Detecting OS...                                           [ DONE ]
```

```
  - Checking profiles...                                      [ DONE ]

  ---------------------------------------------------
  Program version:           3.0.8
  Operating system:          Linux
  Operating system name:     Debian
  Operating system version:  12
  Kernel version:            6.1.0
  Hardware platform:         x86_64
  Hostname:                  debian12
  ---------------------------------------------------
  Profiles:                  /etc/lynis/default.prf
  Log file:                  /var/log/lynis.log
  Report file:               /var/log/lynis-report.dat
  Report version:            1.0
  Plugin directory:          /etc/lynis/plugins
  ---------------------------------------------------
  Auditor:                   [Not Specified]
  Language:                  en
  Test category:             all
  Test group:                all
  ---------------------------------------------------
  - Program update status...                                  [ NO UPDATE ]

[+] System tools
------------------------------------
  - Scanning available tools...
  - Checking system binaries...

[+] Plugins (phase 1)
------------------------------------
 Note: plugins have more extensive tests and may take several minutes to complete
  - Plugin: debian
    [
```

```
[+] Debian Tests
------------------------------------
  - Checking for system binaries that are required by Debian Tests...
    - Checking /bin...                                          [ FOUND ]
    - Checking /sbin...                                         [ FOUND ]
    - Checking /usr/bin...                                      [ FOUND ]
    - Checking /usr/sbin...                                     [ FOUND ]
    - Checking /usr/local/bin...                                [ FOUND ]
    - Checking /usr/local/sbin...                               [ FOUND ]
  - Authentication:
    - PAM (Pluggable Authentication Modules):
      - libpam-tmpdir                                           [ Not Installed ]
  - File System Checks:
    - DM-Crypt, Cryptsetup & Cryptmount:
  - Software:
    - apt-listbugs                                              [ Not Installed ]
    - apt-listchanges                                           [ Installed and enabled for apt ]
    - needrestart                                               [ Not Installed ]
    - fail2ban                                                  [ Installed with jail.local ]
]

[+] Boot and services
------------------------------------
  - Service Manager                                             [ systemd ]
  - Checking UEFI boot                                          [ DISABLED ]
  - Checking presence GRUB2                                     [ FOUND ]
    - Checking for password protection                          [ NONE ]
  - Check running services (systemctl)                          [ DONE ]
        Result: found 27 running services
  - Check enabled services at boot (systemctl)                  [ DONE ]
        Result: found 36 enabled services
  - Check startup files (permissions)                           [ OK ]
  - Running 'systemd-analyze security'
        - ModemManager.service:                                 [ MEDIUM ]
```

```
        - NetworkManager.service:                                   [ EXPOSED ]
        - anacron.service:                                          [ UNSAFE ]
        - apache-htcacheclean.service:                              [ UNSAFE ]
        - apache2.service:                                          [ UNSAFE ]
        - avahi-daemon.service:                                     [ UNSAFE ]
        - cron.service:                                             [ UNSAFE ]
        - cups-browsed.service:                                     [ UNSAFE ]
        - cups.service:                                             [ UNSAFE ]
        - dbus.service:                                             [ UNSAFE ]
        - emergency.service:                                        [ UNSAFE ]
        - fail2ban.service:                                         [ UNSAFE ]
        - firewalld.service:                                        [ UNSAFE ]
        - getty@tty1.service:                                       [ UNSAFE ]
        - lightdm.service:                                          [ UNSAFE ]
        - lynis.service:                                            [ UNSAFE ]
        - plymouth-start.service:                                   [ UNSAFE ]
...
================================================================================

  Lynis security scan details:

  Hardening index : 64 [#############        ]
  Tests performed : 259
  Plugins enabled : 1

  Components:
  - Firewall               [V]
  - Malware scanner        [X]

  Scan mode:
  Normal [V]  Forensics [ ]  Integration [ ]  Pentest [ ]

  Lynis modules:
  - Compliance status      [?]
```

```
  - Security audit         [V]
  - Vulnerability scan     [V]

  Files:
  - Test and debug information      : /var/log/lynis.log
  - Report data                     : /var/log/lynis-report.dat

================================================================================

  Lynis 3.0.8

  Auditing, system hardening, and compliance for UNIX-based systems
  (Linux, macOS, BSD, and others)

  2007-2021, CISOfy - https://cisofy.com/lynis/
  Enterprise support available (compliance, plugins, interface and tools)

================================================================================

  [TIP]: Enhance Lynis audits by adding your settings to custom.prf (see /etc/lynis/default.prf for all settings)
```

Le comportement de Lynis est configuré dans le fichier **/etc/lynis/default.prf** :

```
root@debian12:~# more /etc/lynis/default.prf
################################################################################
#
#
# Lynis - Default scan profile
#
#
################################################################################
#
#
# This profile provides Lynis with most of its initial values to perform a
```

```
# system audit.
#
#
# WARNINGS
# ----------
#
# Do NOT make changes to this file. Instead, copy only your changes into
# the file custom.prf and put it in the same directory as default.prf
#
# To discover where your profiles are located: lynis show profiles
#
#
# Lynis performs a strict check on profiles to avoid the inclusion of
# possibly harmful injections. See include/profiles for details.
#
#
################################################################################
#
# All empty lines or with the # prefix will be skipped
#
################################################################################

# Use colored output
colors=yes

# Compressed uploads (set to zero when errors with uploading occur)
compressed-uploads=yes

# Amount of connections in WAIT state before reporting it as a suggestion
#connections-max-wait-state=5000

# Debug mode (for debugging purposes, extra data logged to screen)
#debug=yes
```

```
# Show non-zero exit code when warnings are found
error-on-warnings=no

# Use Lynis in your own language (by default auto-detected)
language=

# Log tests from another guest operating system (default: yes)
#log-tests-incorrect-os=yes

# Define if available NTP daemon is configured as a server or client on the network
# values: server or client (default: client)
--More--(7%)
```

Lynis journalise sa sortie dans le fichier **/var/log/lynis.log** :

```
root@debian12:~# more /var/log/lynis.log
2025-11-30 07:51:41 Starting Lynis 3.0.8 with PID 10764, build date 2022-05-17
2025-11-30 07:51:41 ====
2025-11-30 07:51:41 ### 2007-2021, CISOfy - https://cisofy.com/lynis/ ###
2025-11-30 07:51:41 Checking permissions of /usr/share/lynis/include/profiles
2025-11-30 07:51:41 File permissions are OK
2025-11-30 07:51:41 Reading profile/configuration /etc/lynis/default.prf
2025-11-30 07:51:41 Action: created temporary file /tmp/lynis.BQ3mIliUFT
2025-11-30 07:51:41 Language set via profile to ''
2025-11-30 07:51:41 Plugin 'authentication' enabled according profile (/etc/lynis/default.prf)
2025-11-30 07:51:41 Plugin 'compliance' enabled according profile (/etc/lynis/default.prf)
2025-11-30 07:51:41 Plugin 'configuration' enabled according profile (/etc/lynis/default.prf)
2025-11-30 07:51:41 Plugin 'control-panels' enabled according profile (/etc/lynis/default.prf)
2025-11-30 07:51:41 Plugin 'crypto' enabled according profile (/etc/lynis/default.prf)
2025-11-30 07:51:41 Plugin 'dns' enabled according profile (/etc/lynis/default.prf)
2025-11-30 07:51:41 Plugin 'docker' enabled according profile (/etc/lynis/default.prf)
2025-11-30 07:51:41 Plugin 'file-integrity' enabled according profile (/etc/lynis/default.prf)
2025-11-30 07:51:41 Plugin 'file-systems' enabled according profile (/etc/lynis/default.prf)
2025-11-30 07:51:41 Plugin 'firewalls' enabled according profile (/etc/lynis/default.prf)
```

```
2025-11-30 07:51:41 Plugin 'forensics' enabled according profile (/etc/lynis/default.prf)
2025-11-30 07:51:41 Plugin 'hardware' enabled according profile (/etc/lynis/default.prf)
2025-11-30 07:51:41 Plugin 'intrusion-detection' enabled according profile (/etc/lynis/default.prf)
2025-11-30 07:51:41 Plugin 'intrusion-prevention' enabled according profile (/etc/lynis/default.prf)
2025-11-30 07:51:41 Plugin 'kernel' enabled according profile (/etc/lynis/default.prf)
2025-11-30 07:51:41 Plugin 'malware' enabled according profile (/etc/lynis/default.prf)
2025-11-30 07:51:41 Plugin 'memory' enabled according profile (/etc/lynis/default.prf)
2025-11-30 07:51:41 Plugin 'nginx' enabled according profile (/etc/lynis/default.prf)
2025-11-30 07:51:41 Plugin 'pam' enabled according profile (/etc/lynis/default.prf)
2025-11-30 07:51:41 Plugin 'processes' enabled according profile (/etc/lynis/default.prf)
2025-11-30 07:51:41 Plugin 'security-modules' enabled according profile (/etc/lynis/default.prf)
2025-11-30 07:51:41 Plugin 'software' enabled according profile (/etc/lynis/default.prf)
2025-11-30 07:51:41 Plugin 'system-integrity' enabled according profile (/etc/lynis/default.prf)
2025-11-30 07:51:41 Plugin 'systemd' enabled according profile (/etc/lynis/default.prf)
2025-11-30 07:51:41 Plugin 'users' enabled according profile (/etc/lynis/default.prf)
2025-11-30 07:51:42 Plugin 'debian' enabled according profile (/etc/lynis/default.prf)
2025-11-30 07:51:42 Set option to default value: NTPD_ROLE --> client
2025-11-30 07:51:42 ====
2025-11-30 07:51:42 EOL check: 255
2025-11-30 07:51:42 Note: the end-of-life of 'Debian GNU/Linux 12 (bookworm)' could not be checked. Entry missing
in software-eol.db?
2025-11-30 07:51:42 Program version:           3.0.8
2025-11-30 07:51:42 Operating system:          Linux
2025-11-30 07:51:42 Operating system name:     Debian
2025-11-30 07:51:42 Operating system version:  12
2025-11-30 07:51:42 Kernel version:            6.1.0
2025-11-30 07:51:42 Kernel version (full):     6.1.0-41-amd64
2025-11-30 07:51:42 Hardware platform:         x86_64
2025-11-30 07:51:42 ----------------------------------------------------
2025-11-30 07:51:42 Hostname:                  debian12
2025-11-30 07:51:42 Auditor:                   [Not Specified]
2025-11-30 07:51:42 Profiles:                  /etc/lynis/default.prf
2025-11-30 07:51:42 Work directory:            /root
2025-11-30 07:51:42 Include directory:         /usr/share/lynis/include
```

```
2025-11-30 07:51:42 Plugin directory:          /etc/lynis/plugins
2025-11-30 07:51:42 ------------------------------------------------------
2025-11-30 07:51:42 Log file:                  /var/log/lynis.log
2025-11-30 07:51:42 Report file:               /var/log/lynis-report.dat
--More--(0%)
```

Dans le journal se trouve des suggestions pour durcir le système, par exemple :

```
root@debian12:~# cat /var/log/lynis.log | grep BANN-7126
2025-11-30 07:52:25 Performing test ID BANN-7126 (Check issue banner file contents)
2025-11-30 07:52:25 Suggestion: Add a legal banner to /etc/issue, to warn unauthorized users [test:BANN-7126]
[details:-] [solution:-]
```

```
root@debian12:~# cat /var/log/lynis.log | grep FILE-7524
2025-11-30 07:52:47 Performing test ID FILE-7524 (Perform file permissions check)
2025-11-30 07:52:48 Suggestion: Consider restricting file permissions [test:FILE-7524] [details:See screen output
or log file] [solution:text:Use chmod to change file permissions]
```

Sections clefs de la sortie :

- Indice de Renforcement (Hardening Index) : C'est un score qui indique le niveau de sécurité global de votre système. Un nombre plus élevé est meilleur, et votre objectif est d'augmenter ce score en abordant les suggestions.
- Avertissements (Warnings) : Problèmes qui présentent un risque de sécurité potentiel et doivent être traités immédiatement (par exemple, logiciels obsolètes, mots de passe faibles).
- Suggestions : Recommandations pour améliorer la configuration de sécurité de votre système (par exemple, meilleure rotation des journaux, renforcement du noyau). Chaque suggestion inclut un ID de test unique (par exemple, BANN-7126) et une URL pour plus d'informations.

A l'issue de l'implémentation des suggestions, il convient d'exécuter de nouveau la commande **lynis audit system**.

A Faire - Passez en revue et implémentez les suggestions de Lynis.

LAB #2 - System Hardening à l'aide de l'outil Bastille

Connectez-vous à votre VM **CentOS7_10.0.2.51_SSH**.

2.1 - Présentation

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

2.2 - Installation

Installez le dépôt EPEL :

```
[root@centos7 ~]# wget
https://www.dropbox.com/scl/fi/1o0byl5fqdup3l8nj0nmy/epel-release-7-14.noarch.rpm?rlkey=4hikdmn27y1yjdg9tyeplagk3
&st=g1vbyij5&dl=0

[root@centos7 ~]# mv epel-release-7-14.noarch.rpm?rlkey=4hikdmn27y1yjdg9tyeplagk3&st=g1vbyij5&dl=0 epel-
release-7-14.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/scl/fi/6n5h843od2n9nczhrybre/Bastille-3.0.9-1.0.noarch.rpm?rlkey=4r0pbn50yu6ltosfju24b16r
```

```
x&st=qf42127o&dl=0

[root@centos7 ~]# mv Bastille-3.0.9-1.0.noarch.rpm?rlkey=4r0pbn50yu6ltosfju24b16rx&st=qf42127o&dl=0
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/
```

2.3 - 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 #3 - Mise en Place d'un Chroot pour isoler un utilisateur/une application

Reconnectez-vous à votre VM **Debian12_10.0.2.46_SSH**.

Le chrootage permet de séparer un utilisateur ou un utilisateur système (et donc un serveur) du système.

Sous Debian 12 le binaire chroot est installé par défaut :

```
root@debian12:~# which chroot
/usr/sbin/chroot
```

Commencez par créer un répertoire pour l'utilisateur qui sera emprisonné :

```
root@debian12:~# mkdir /home/prison
```

Le binaire **/usr/sbin/chroot** doit prendre le SUID bit :

```
root@debian12:~# mkdir /home/prison

root@debian12:~# ls -l /usr/sbin/chroot
-rwxr-xr-x. 1 root root 48112 Sep 20  2022 /usr/sbin/chroot

root@debian12:~# chmod +s /usr/sbin/chroot

root@debian12:~# ls -l /usr/sbin/chroot
-rwsr-sr-x. 1 root root 48112 Sep 20  2022 /usr/sbin/chroot
```

Créez maintenant un script de connexion générique pour que l'utilisateur **prison** puisse se connecter :

```
root@debian12:~# vi /bin/chroot

root@debian12:~# cat /bin/chroot
#!/bin/bash
exec -c /usr/sbin/chroot /home/$USER /bin/bash
```

Rendez ce script exécutable :

```
root@debian12:~# chmod +x /bin/chroot
```

Il est maintenant nécessaire de copier toutes les commandes dont l'utilisateur **prison** aura besoin. Dans cet exemple, nous allons nous contenter de copier **/bin/bash** et **/bin/ls** ainsi que les bibliothèques associées :

```
root@debian12:~# mkdir /home/prison/bin

root@debian12:~# cp /bin/bash /home/prison/bin/

root@debian12:~# ldd /bin/bash
        linux-vdso.so.1 (0x00007ffd39fcf000)
        libtinfo.so.6 => /lib/x86_64-linux-gnu/libtinfo.so.6 (0x00007fef082e8000)
        libc.so.6 => /lib/x86_64-linux-gnu/libc.so.6 (0x00007fef08106000)
        /lib64/ld-linux-x86-64.so.2 (0x00007fef08471000)
root@debian12:~# mkdir /home/prison/lib64

root@debian12:~# mkdir -p /home/prison/lib/x86_64-linux-gnu/

root@debian12:~# cp /lib/x86_64-linux-gnu/libtinfo.so.6 /home/prison/lib/x86_64-linux-gnu/

root@debian12:~# cp /lib/x86_64-linux-gnu/libc.so.6 /home/prison/lib/x86_64-linux-gnu/

root@debian12:~# cp /lib64/ld-linux-x86-64.so.2 /home/prison/lib64

root@debian12:~# cp /bin/ls /home/prison/bin/

root@debian12:~# ldd /bin/ls
        linux-vdso.so.1 (0x00007fff3db26000)
        libselinux.so.1 => /lib/x86_64-linux-gnu/libselinux.so.1 (0x00007f8afb9a0000)
        libc.so.6 => /lib/x86_64-linux-gnu/libc.so.6 (0x00007f8afb7be000)
        libpcre2-8.so.0 => /lib/x86_64-linux-gnu/libpcre2-8.so.0 (0x00007f8afb724000)
        /lib64/ld-linux-x86-64.so.2 (0x00007f8afba0a000)

root@debian12:~# cp /lib/x86_64-linux-gnu/libselinux.so.1 /home/prison/lib/x86_64-linux-gnu/
```

```
root@debian12:~# cp /lib/x86_64-linux-gnu/libpcre2-8.so.0 /home/prison/lib/x86_64-linux-gnu/
```

Créez maintenant le groupe chroot :

```
root@debian12:~# groupadd chroot

root@debian12:~# cat /etc/group | grep chroot
chroot:x:1001:
```

Créez maintenant l'utilisateur **prison** :

```
root@debian12:~# useradd prison -c chroot_user -d /home/prison -g chroot -s /bin/chroot
```

Dernièrement, modifiez le propriétaire et le groupe du répertoire **/home/prison** :

```
root@debian12:~# chown -R prison:chroot /home/prison
```

Essayez maintenant de vous connecter en tant que l'utilisateur prison :

```
root@debian12:~# su - prison

bash-5.2$ pwd
/

bash-5.2$ ls
bin  lib  lib64

bash-5.2$ ls -la
total 20
drwxr-xr-x. 5 1001 1001 4096 Dec  1 13:59 .
drwxr-xr-x. 5 1001 1001 4096 Dec  1 13:59 ..
drwxr-xr-x. 2 1001 1001 4096 Dec  1 13:56 bin
drwxr-xr-x. 3 1001 1001 4096 Dec  1 13:59 lib
drwxr-xr-x. 2 1001 1001 4096 Dec  1 13:56 lib64
```

```
bash-5.2$ exit
exit

root@debian12:~#
```

Notez que l'utilisateur **prison** est *chrooté*.

LAB #4 - Mise en place d'AppArmor pour sécuriser le serveur

4.1 - Présentation

AppArmor, abréviation d'Application Armor (Armure d'Application), est un module de sécurité du noyau pour les distributions Linux basées sur Debian qui vous permet de définir des profils de sécurité par application. Ces profils restreignent les ressources système auxquelles une application peut accéder, créant ainsi efficacement un bac à sable (sandbox) autour de chaque application. Ce mécanisme de sécurité permet de prévenir l'accès non autorisé aux données sensibles et réduit le risque de failles de sécurité. AppArmor s'appuie sur l'interface **LSM** (Linux Security Modules) fournie par le noyau Linux.

L'approche AppArmor à la sécurité est une approche de type **MAC** :

Type de Sécurité	**Nom**	**Description**
DAC	*Discretional Access Control*	L'accès aux objets est en fonction de l'identité (utilisateur,groupe). Un utilisateur peut rendre accessibles aux autres ses propres objets.
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.

Les avantages clés de l'utilisation d'AppArmor sont :

- **Isolation** : AppArmor aide à contenir les menaces de sécurité en isolant les applications les unes des autres et du reste du système.
- **Contrôle précis** (Fine-grained control) : Vous pouvez spécifier exactement quels fichiers, répertoires et capacités une application peut accéder.
- **Conformité en matière de sécurité** : De nombreuses distributions Linux, notamment Debian et Ubuntu, utilisent AppArmor par défaut pour appliquer des politiques de sécurité.

4.2 - Définitions

Les Profils d'AppArmor

AppArmor utilise des **profils** pour définir les règles de sécurité pour les applications. Ces profils sont stockés dans le répertoire **/etc/apparmor.d/** :

```
root@debian12:~# ls -l /etc/apparmor.d/
total 220
drwxr-xr-x 2 root root  4096 Nov 24 17:22 abi
drwxr-xr-x 4 root root 12288 Dec  3 12:40 abstractions
drwxr-xr-x 2 root root  4096 Dec  3 12:40 apache2.d
-rw-r--r-- 1 root root   879 Feb 14  2023 bin.ping
drwxr-xr-x 2 root root  4096 Apr  3  2021 disable
drwxr-xr-x 2 root root  4096 Apr  3  2021 force-complain
-rw-r--r-- 1 root root   819 Feb  3  2020 lightdm-guest-session
drwxr-xr-x 2 root root  4096 Dec  3 12:40 local
-rw-r--r-- 1 root root  1379 Feb 14  2023 lsb_release
-rw-r--r-- 1 root root  1189 Feb 14  2023 nvidia_modprobe
-rw-r--r-- 1 root root  1713 Feb 14  2023 php-fpm
-rw-r--r-- 1 root root   623 Feb 14  2023 samba-bgqd
-rw-r--r-- 1 root root  1061 Feb 14  2023 samba-dcerpcd
-rw-r--r-- 1 root root   817 Feb 14  2023 samba-rpcd
-rw-r--r-- 1 root root   755 Feb 14  2023 samba-rpcd-classic
-rw-r--r-- 1 root root   964 Feb 14  2023 samba-rpcd-spoolss
-rw-r--r-- 1 root root  3461 Mar 30  2023 sbin.dhclient
-rw-r--r-- 1 root root  1017 Feb 14  2023 sbin.klogd
-rw-r--r-- 1 root root  1458 Feb 14  2023 sbin.syslogd
```

```
-rw-r--r-- 1 root root  2076 Feb 14  2023 sbin.syslog-ng
drwxr-xr-x 5 root root  4096 Nov 24 17:22 tunables
-rw-r--r-- 1 root root  1446 Dec 10  2022 usr.bin.irssi
-rw-r--r-- 1 root root  3448 Feb 19  2021 usr.bin.man
-rw-r--r-- 1 root root  2561 Dec 10  2022 usr.bin.pidgin
-rw-r--r-- 1 root root  2038 Dec 10  2022 usr.bin.totem
-rw-r--r-- 1 root root  1400 Dec 10  2022 usr.bin.totem-previewers
-rw-r--r-- 1 root root  1519 Aug 13 17:35 usr.lib.libreoffice.program.oosplash
-rw-r--r-- 1 root root  1227 Oct 10  2021 usr.lib.libreoffice.program.senddoc
-rw-r--r-- 1 root root 10694 Aug 13 17:35 usr.lib.libreoffice.program.soffice.bin
-rw-r--r-- 1 root root  1046 Oct 10  2021 usr.lib.libreoffice.program.xpdfimport
-rw-r--r-- 1 root root 28486 Jun  6 16:53 usr.lib.snapd.snap-confine.real
-rw-r--r-- 1 root root  1060 Dec 10  2022 usr.sbin.apt-cacher-ng
-rw-r--r-- 1 root root  1027 Feb 14  2023 usr.sbin.avahi-daemon
-rw-r--r-- 1 root root   761 May 19  2023 usr.sbin.cups-browsed
-rw-r--r-- 1 root root  6027 Sep  7 19:45 usr.sbin.cupsd
-rw-r--r-- 1 root root  4291 Feb 14  2023 usr.sbin.dnsmasq
-rw-r--r-- 1 root root  1071 Feb 14  2023 usr.sbin.identd
-rw-r--r-- 1 root root  1001 Feb 14  2023 usr.sbin.mdnsd
-rw-r--r-- 1 root root   987 Feb 14  2023 usr.sbin.nmbd
-rw-r--r-- 1 root root  1381 Feb 14  2023 usr.sbin.nscd
-rw-r--r-- 1 root root  2164 Feb 14  2023 usr.sbin.smbd
-rw-r--r-- 1 root root   981 Feb 14  2023 usr.sbin.smbldap-useradd
-rw-r--r-- 1 root root  1091 Feb 14  2023 usr.sbin.traceroute
```

Le profil est un fichier texte qui fournit la liste complète des autorisations (et des interdictions) pour un programme particulier :

```
root@debian12:~# cat /etc/apparmor.d/usr.sbin.smbd
abi <abi/3.0>,

include <tunables/global>

profile smbd /usr/{bin,sbin}/smbd flags=(complain) {
  include <abstractions/authentication>
```

```
  include <abstractions/base>
  include <abstractions/consoles>
  include <abstractions/cups-client>
  include <abstractions/nameservice>
  include <abstractions/openssl>
  include <abstractions/samba>
  include <abstractions/user-tmp>
  include <abstractions/wutmp>

  capability audit_write,
  capability dac_override,
  capability dac_read_search,
  capability fowner,
  capability lease,
  capability net_bind_service,
  capability setgid,
  capability setuid,
  capability sys_admin,
  capability sys_resource,
  capability sys_tty_config,

  signal send set=term peer=samba-bgqd,

  /etc/mtab r,
  /etc/netgroup r,
  /etc/printcap r,
  /etc/samba/* rwk,
  @{PROC}/@{pid}/mounts r,
  @{PROC}/sys/kernel/core_pattern r,
  /usr/lib*/samba/vfs/*.so mr,
  /usr/lib*/samba/auth/*.so mr,
  /usr/lib*/samba/charset/*.so mr,
  /usr/lib*/samba/gensec/*.so mr,
  /usr/lib*/samba/pdb/*.so mr,
```

```
  /usr/lib*/samba/{,samba/}samba-bgqd Px -> samba-bgqd,
  /usr/lib*/samba/{,samba/}samba-dcerpcd Px -> samba-dcerpcd,
  /usr/lib*/samba/{lowcase,upcase,valid}.dat r,
  /usr/lib/@{multiarch}/samba/*.so{,.[0-9]*} mr,
  /usr/lib/@{multiarch}/samba/**/ r,
  /usr/lib/@{multiarch}/samba/**/*.so{,.[0-9]*} mr,
  /usr/share/samba/** r,
  /usr/{bin,sbin}/smbd mr,
  /usr/{bin,sbin}/smbldap-useradd Px,
  /var/cache/samba/** rwk,
  /var/{cache,lib}/samba/printing/printers.tdb mrw,
  /var/lib/samba/** rwk,
  /var/lib/sss/pubconf/kdcinfo.* r,
  @{run}/dbus/system_bus_socket rw,
  @{run}/smbd.pid rwk,
  @{run}/samba/** rk,
  @{run}/samba/ncalrpc/ rw,
  @{run}/samba/ncalrpc/** rw,
  @{run}/samba/smbd.pid rw,
  /var/spool/samba/** rw,

  @{HOMEDIRS}/** lrwk,
  /var/lib/samba/usershares/{,**} lrwk,

  # Permissions for all configured shares (file autogenerated by
  # update-apparmor-samba-profile on service startup on Debian and openSUSE)
  include if exists <samba/smbd-shares>
  include if exists <local/usr.sbin.smbd-shares>

  # Site-specific additions and overrides. See local/README for details.
  include if exists <local/usr.sbin.smbd>
}
```

Ce que le profil définit :

- **Accès aux fichiers** : Le profil spécifie quels fichiers et répertoires l'application peut lire, écrire, modifier ou exécuter.
- **Accès au réseau** : Il détermine si l'application peut établir des connexions réseau (sortantes ou entrantes).
- **Capacités du noyau** : Il restreint certaines fonctions puissantes du noyau Linux que l'application pourrait essayer d'utiliser.

Le rôle principal du profil est de créer un bac à sable (sandbox) autour de l'application. Si l'application est compromise (par exemple, par un virus ou une faille de sécurité), elle ne peut pas sortir de son bac à sable pour nuire au reste du système, car AppArmor l'empêche d'accéder aux ressources non autorisées par son profil.

Les Modes d'AppArmor

AppArmor connait trois états ou modes pour chaque profil :

Mode	Description
unconfined	AppArmor est inactif.
complain	AppArmor autorise l'action, mais enregistre un message d'avertissement (log) indiquant que l'application a essayé de faire quelque chose d'interdit. Ce mode est utile pour créer ou affiner un nouveau profil, car il montre toutes les actions réelles que l'application tente d'effectuer.. C'est un mode d'apprentissage pour régler le profile. Ceci est l'état par défaut lors qu'un paquet installe un profile AppArmor.
enforce	C'est le mode par défaut. AppArmor bloque toute tentative de l'application de faire quelque chose qui n'est pas explicitement autorisé par son profil.

4.3 - Installation

Installation des Paquets

AppArmor peut être installé en utilisant **APT** :

```
root@debian12:~# apt install apparmor apparmor-utils apparmor-profiles apparmor-profiles-extra apparmor-notify
apparmor-easyprof auditd -y
```

*

Modification de GRUB

Editez la ligne **GRUB_CMDLINE_LINUX_DEFAULT** dans le fichier **/etc/default/grub** :

```
root@debian12:~# vi /etc/default/grub

root@debian12:~# cat /etc/default/grub
# If you change this file, run 'update-grub' afterwards to update
# /boot/grub/grub.cfg.
# For full documentation of the options in this file, see:
#   info -f grub -n 'Simple configuration'

GRUB_DEFAULT=0
GRUB_TIMEOUT=5
GRUB_DISTRIBUTOR=`lsb_release -i -s 2> /dev/null || echo Debian`
GRUB_CMDLINE_LINUX_DEFAULT="quiet splash apparmor=1 security=apparmor"
GRUB_CMDLINE_LINUX=""

# If your computer has multiple operating systems installed, then you
# probably want to run os-prober. However, if your computer is a host
# for guest OSes installed via LVM or raw disk devices, running
# os-prober can cause damage to those guest OSes as it mounts
# filesystems to look for things.
#GRUB_DISABLE_OS_PROBER=false

# Uncomment to enable BadRAM filtering, modify to suit your needs
# This works with Linux (no patch required) and with any kernel that obtains
# the memory map information from GRUB (GNU Mach, kernel of FreeBSD ...)
#GRUB_BADRAM="0x01234567,0xfefefefe,0x89abcdef,0xefefefef"

# Uncomment to disable graphical terminal
#GRUB_TERMINAL=console
```

```
# The resolution used on graphical terminal
# note that you can use only modes which your graphic card supports via VBE
# you can see them in real GRUB with the command `vbeinfo'
#GRUB_GFXMODE=640x480

# Uncomment if you don't want GRUB to pass "root=UUID=xxx" parameter to Linux
#GRUB_DISABLE_LINUX_UUID=true

# Uncomment to disable generation of recovery mode menu entries
#GRUB_DISABLE_RECOVERY="true"

# Uncomment to get a beep at grub start
#GRUB_INIT_TUNE="480 440 1"
```

Mettez à jour GRUB :

```
root@debian12:~# update-grub
Generating grub configuration file ...
Found background image: /usr/share/images/desktop-base/desktop-grub.png
Found linux image: /boot/vmlinuz-6.1.0-41-amd64
Found initrd image: /boot/initrd.img-6.1.0-41-amd64
Found linux image: /boot/vmlinuz-5.10.0-36-amd64
Found initrd image: /boot/initrd.img-5.10.0-36-amd64
Warning: os-prober will not be executed to detect other bootable partitions.
Systems on them will not be added to the GRUB boot configuration.
Check GRUB_DISABLE_OS_PROBER documentation entry.
done
```

Redémarrez la VM :

```
root@debian12:~# reboot
```

Vérification de l'Activation d'AppArmor

Connectez-vous à la VM et vérifiez qu'AppArmor est activé :

```
trainee@debian12:~$ su -
Password: fenestros

root@debian12:~# cat /sys/module/apparmor/parameters/enabled
Y

root@debian12:~# aa-enabled
Yes

root@debian12:~# systemctl status apparmor
● apparmor.service - Load AppArmor profiles
     Loaded: loaded (/lib/systemd/system/apparmor.service; enabled; preset: enabled)
     Active: active (exited) since Wed 2025-12-03 12:46:51 CET; 4min 56s ago
       Docs: man:apparmor(7)
             https://gitlab.com/apparmor/apparmor/wikis/home/
    Process: 342 ExecStart=/lib/apparmor/apparmor.systemd reload (code=exited, status>
   Main PID: 342 (code=exited, status=0/SUCCESS)
        CPU: 403ms

Dec 03 12:46:50 debian12 apparmor.systemd[342]: Restarting AppArmor
Dec 03 12:46:50 debian12 apparmor.systemd[342]: Reloading AppArmor profiles
Dec 03 12:46:48 debian12 systemd[1]: Starting apparmor.service - Load AppArmor profil>
Dec 03 12:46:51 debian12 systemd[1]: Finished apparmor.service - Load AppArmor profil>
```

Les paquets **apparmor-profiles** et **apparmor-profiles-extra** fournissent des profiles supplémentaires qui se trouvent dans **/usr/share/apparmor/extra-profiles/** :

```
root@debian12:~# ls /usr/share/apparmor/extra-profiles/
bin.netstat                  postfix-qmgr             usr.bin.apropos          usr.bin.svnserve
```

```
usr.lib.dovecot.script-login                                usr.sbin.lighttpd
etc.cron.daily.logrotate     postfix-qmqpd           usr.bin.dumpcap          usr.bin.wireshark
usr.lib.dovecot.ssl-params                                  usr.sbin.oidentd
etc.cron.daily.slocate.cron  postfix-scache          usr.bin.evolution-2.10   usr.bin.xfs
usr.lib.dovecot.stats                                       usr.sbin.popper
etc.cron.daily.tmpwatch      postfix-showq           usr.bin.fam              usr.lib64.GConf.2.gconfd-2
usr.lib.evolution-data-server.evolution-data-server-1.10  usr.sbin.postalias
postfix-anvil                postfix-smtp            usr.bin.gaim             usr.lib.bonobo.bonobo-activation-
server  usr.lib.firefox.firefox                                    usr.sbin.postdrop
postfix-bounce               postfix-smtpd           usr.bin.man              usr.lib.dovecot.anvil
usr.lib.firefox.firefox.sh                                  usr.sbin.postmap
postfix-cleanup              postfix-spawn           usr.bin.mlmmj-bounce     usr.lib.dovecot.auth
usr.lib.firefox.mozilla-xremote-client                      usr.sbin.postqueue
postfix-discard              postfix-tlsmgr          usr.bin.mlmmj-maintd     usr.lib.dovecot.config
usr.lib.GConf.2.gconfd-2                                    usr.sbin.sendmail
postfix-dnsblog              postfix-trivial-rewrite  usr.bin.mlmmj-make-ml.sh  usr.lib.dovecot.deliver
usr.lib.man-db.man                                          usr.sbin.sendmail.postfix
postfix-error                postfix-verify          usr.bin.mlmmj-process    usr.lib.dovecot.dict
usr.lib.RealPlayer10.realplay                               usr.sbin.sendmail.sendmail
postfix-flush                postfix-virtual         usr.bin.mlmmj-receive    usr.lib.dovecot.dovecot-auth
usr.NX.bin.nxclient                                         usr.sbin.spamd
postfix-lmtp                 README                  usr.bin.mlmmj-recieve    usr.lib.dovecot.dovecot-lda
usr.sbin.dhcpd                                              usr.sbin.squid
postfix-local                sbin.dhclient           usr.bin.mlmmj-send       usr.lib.dovecot.imap
usr.sbin.dovecot                                            usr.sbin.sshd
postfix-master               sbin.dhclient-script    usr.bin.mlmmj-sub        usr.lib.dovecot.imap-login
usr.sbin.httpd2-prefork                                     usr.sbin.useradd
postfix-nqmgr                sbin.dhcpcd             usr.bin.mlmmj-unsub      usr.lib.dovecot.lmtp
usr.sbin.imapd                                              usr.sbin.userdel
postfix-oqmgr                sbin.portmap            usr.bin.opera            usr.lib.dovecot.log
usr.sbin.in.fingerd                                         usr.sbin.vsftpd
postfix-pickup               sbin.resmgrd            usr.bin.passwd           usr.lib.dovecot.managesieve
usr.sbin.in.ftpd                                            usr.sbin.xinetd
postfix-pipe                 sbin.rpc.lockd          usr.bin.procmail         usr.lib.dovecot.managesieve-login
```

```
usr.sbin.in.ntalkd
postfix-postscreen          sbin.rpc.statd          usr.bin.skype            usr.lib.dovecot.pop3
usr.sbin.ipop2d
postfix-proxymap            usr.bin.acroread        usr.bin.spamc            usr.lib.dovecot.pop3-login
usr.sbin.ipop3d
```

Copiez donc les profils dans **/usr/share/apparmor/extra-profiles/** vers **/etc/apparmor.d** :

```
root@debian12:~# cp /usr/share/apparmor/extra-profiles/* /etc/apparmor.d/

root@debian12:~# ls /etc/apparmor.d
abi                         postfix-pickup          sbin.rpc.lockd           usr.bin.spamc
usr.lib.firefox.firefox                 usr.sbin.lighttpd
abstractions                postfix-pipe            sbin.rpc.statd           usr.bin.svnserve
usr.lib.firefox.firefox.sh              usr.sbin.mdnsd
apache2.d                   postfix-postscreen      sbin.syslogd             usr.bin.totem
usr.lib.firefox.mozilla-xremote-client  usr.sbin.nmbd
bin.netstat                 postfix-proxymap        sbin.syslog-ng           usr.bin.totem-previewers
usr.lib.GConf.2.gconfd-2                usr.sbin.nscd
bin.ping                    postfix-qmgr            tunables                 usr.bin.wireshark
usr.lib.libreoffice.program.oosplash    usr.sbin.oidentd
disable                     postfix-qmqpd           usr.bin.acroread         usr.bin.xfs
usr.lib.libreoffice.program.senddoc     usr.sbin.popper
etc.cron.daily.logrotate    postfix-scache          usr.bin.apropos          usr.lib64.GConf.2.gconfd-2
usr.lib.libreoffice.program.soffice.bin usr.sbin.postalias
etc.cron.daily.slocate.cron postfix-showq           usr.bin.dumpcap          usr.lib.bonobo.bonobo-activation-
server                  usr.lib.libreoffice.program.xpdfimport  usr.sbin.postdrop
etc.cron.daily.tmpwatch     postfix-smtp            usr.bin.evolution-2.10   usr.lib.dovecot.anvil
usr.lib.man-db.man                      usr.sbin.postmap
force-complain              postfix-smtpd           usr.bin.fam              usr.lib.dovecot.auth
usr.lib.RealPlayer10.realplay           usr.sbin.postqueue
lightdm-guest-session       postfix-spawn           usr.bin.gaim             usr.lib.dovecot.config
usr.lib.snapd.snap-confine.real         usr.sbin.sendmail
local                       postfix-tlsmgr          usr.bin.irssi            usr.lib.dovecot.deliver
```

```
usr.NX.bin.nxclient                    usr.sbin.sendmail.postfix
lsb_release                 postfix-trivial-rewrite  usr.bin.man              usr.lib.dovecot.dict
usr.sbin.apt-cacher-ng                 usr.sbin.sendmail.sendmail
nvidia_modprobe             postfix-verify           usr.bin.mlmmj-bounce     usr.lib.dovecot.dovecot-auth
usr.sbin.avahi-daemon                  usr.sbin.smbd
php-fpm                     postfix-virtual          usr.bin.mlmmj-maintd     usr.lib.dovecot.dovecot-lda
usr.sbin.cups-browsed                  usr.sbin.smbldap-useradd
postfix-anvil               README                   usr.bin.mlmmj-make-ml.sh  usr.lib.dovecot.imap
usr.sbin.cupsd                         usr.sbin.spamd
postfix-bounce              samba-bgqd               usr.bin.mlmmj-process     usr.lib.dovecot.imap-login
usr.sbin.dhcpd                         usr.sbin.squid
postfix-cleanup             samba-dcerpcd            usr.bin.mlmmj-receive     usr.lib.dovecot.lmtp
usr.sbin.dnsmasq                       usr.sbin.sshd
postfix-discard             samba-rpcd               usr.bin.mlmmj-recieve     usr.lib.dovecot.log
usr.sbin.dovecot                       usr.sbin.traceroute
postfix-dnsblog             samba-rpcd-classic       usr.bin.mlmmj-send        usr.lib.dovecot.managesieve
usr.sbin.httpd2-prefork                usr.sbin.useradd
postfix-error               samba-rpcd-spoolss       usr.bin.mlmmj-sub         usr.lib.dovecot.managesieve-login
usr.sbin.identd                        usr.sbin.userdel
postfix-flush               sbin.dhclient            usr.bin.mlmmj-unsub       usr.lib.dovecot.pop3
usr.sbin.imapd                         usr.sbin.vsftpd
postfix-lmtp                sbin.dhclient-script     usr.bin.opera             usr.lib.dovecot.pop3-login
usr.sbin.in.fingerd                    usr.sbin.xinetd
postfix-local               sbin.dhcpcd              usr.bin.passwd            usr.lib.dovecot.script-login
usr.sbin.in.ftpd
postfix-master              sbin.klogd               usr.bin.pidgin            usr.lib.dovecot.ssl-params
usr.sbin.in.ntalkd
postfix-nqmgr               sbin.portmap             usr.bin.procmail          usr.lib.dovecot.stats
usr.sbin.ipop2d
postfix-oqmgr               sbin.resmgrd             usr.bin.skype             usr.lib.evolution-data-
server.evolution-data-server-1.10  usr.sbin.ipop3d
```

Redémarrez le service AppArmor :

```
root@debian12:~# systemctl restart apparmor

root@debian12:~# systemctl status apparmor
● apparmor.service - Load AppArmor profiles
     Loaded: loaded (/lib/systemd/system/apparmor.service; enabled; preset: enabled)
     Active: active (exited) since Wed 2025-12-03 13:48:24 CET; 7s ago
       Docs: man:apparmor(7)
             https://gitlab.com/apparmor/apparmor/wikis/home/
    Process: 1618 ExecStart=/lib/apparmor/apparmor.systemd reload (code=exited, statu>
   Main PID: 1618 (code=exited, status=0/SUCCESS)
        CPU: 16.409s

Dec 03 13:48:22 debian12 systemd[1]: Starting apparmor.service - Load AppArmor profil>
Dec 03 13:48:22 debian12 apparmor.systemd[1618]: Restarting AppArmor
Dec 03 13:48:22 debian12 apparmor.systemd[1618]: Reloading AppArmor profiles
Dec 03 13:48:24 debian12 systemd[1]: Finished apparmor.service - Load AppArmor profil>
```

LAB #5 - Travailler avec AppArmor

5.1 - Consulter la Liste des Profils Chargés

Pour consulter la liste de tous les profils Apparmor chargés pour les applications et les processus et détaille leur statut (loaded., complain mode, enforce mode), utilisez la commande **aa-status** :

```
root@debian12:~# aa-status
apparmor module is loaded.
193 profiles are loaded.
148 profiles are in enforce mode.
   /etc/cron.daily/logrotate
   ...
   snap.john-the-ripper.zip2john
```

```
45 profiles are in complain mode.
   /usr/bin/irssi
   ...
    traceroute
0 profiles are in kill mode.
0 profiles are in unconfined mode.
7 processes have profiles defined.
2 processes are in enforce mode.
   /usr/sbin/cups-browsed (1190)
   /usr/sbin/cupsd (1018)
2 processes are in complain mode.
   /usr/sbin/avahi-daemon (646) avahi-daemon
   /usr/sbin/avahi-daemon (664) avahi-daemon
3 processes are unconfined but have a profile defined.
   /usr/sbin/sshd (1067)
   /usr/sbin/sshd (1472)
   /usr/sbin/sshd (1521)
0 processes are in mixed mode.
0 processes are in kill mode.
```

Options de la Commande

```
root@debian12:~# aa-status --help
Usage: aa-status [OPTIONS]
Displays various information about the currently loaded AppArmor policy.
OPTIONS (one only):
  --enabled       returns error code if AppArmor not enabled
  --profiled      prints the number of loaded policies
  --enforced      prints the number of loaded enforcing policies
  --complaining   prints the number of loaded non-enforcing policies
  --kill          prints the number of loaded enforcing policies that kill tasks on policy violations
  --special-unconfined   prints the number of loaded non-enforcing policies in the special unconfined mode
  --process-mixed prints the number processes with mixed profile modes
```

```
  --json          displays multiple data points in machine-readable JSON format
  --pretty-json   same data as --json, formatted for human consumption as well
  --verbose       (default) displays multiple data points about loaded policy set
  --help          this message
```

5.2 - Passer le Mode d'un Profil de Complain à Enforce

Le profil **traceroute** est actuellement en mode **complain**. Pour passer ce profil en mode **enforce**, saisissez la commande suivante :

```
root@debian12:~# aa-enforce /etc/apparmor.d/usr.sbin.traceroute
Setting /etc/apparmor.d/usr.sbin.traceroute to enforce mode.

root@debian12:~# aa-status
apparmor module is loaded.
193 profiles are loaded.
149 profiles are in enforce mode.
   /etc/cron.daily/logrotate
...
   snap.john-the-ripper.zip2john
   traceroute
44 profiles are in complain mode.
   /usr/bin/irssi
...
   syslogd
0 profiles are in kill mode.
0 profiles are in unconfined mode.
7 processes have profiles defined.
2 processes are in enforce mode.
   /usr/sbin/cups-browsed (1190)
   /usr/sbin/cupsd (1018)
2 processes are in complain mode.
   /usr/sbin/avahi-daemon (646) avahi-daemon
   /usr/sbin/avahi-daemon (664) avahi-daemon
```

```
3 processes are unconfined but have a profile defined.
   /usr/sbin/sshd (1067)
   /usr/sbin/sshd (1472)
   /usr/sbin/sshd (1521)
0 processes are in mixed mode.
0 processes are in kill mode.
```

Options de la Commande

```
root@debian12:~# aa-enforce --help
usage: aa-enforce [-h] [-d DIR] [--no-reload] program [program ...]

Switch the given program to enforce mode

positional arguments:
  program            name of program

options:
  -h, --help         show this help message and exit
  -d DIR, --dir DIR  path to profiles
  --no-reload        Do not reload the profile after modifying it
```

5.3 - Passer le Mode d'un Profil d'Enforce à Complain

Pour repasser le profil en mode **enforce**, saisissez la commande suivante :

```
root@debian12:~# aa-complain /etc/apparmor.d/usr.sbin.traceroute
Setting /etc/apparmor.d/usr.sbin.traceroute to complain mode.

root@debian12:~# aa-status
apparmor module is loaded.
```

```
193 profiles are loaded.
148 profiles are in enforce mode.
   /etc/cron.daily/logrotate
...
   snap.john-the-ripper.zip2john
45 profiles are in complain mode.
   /usr/bin/irssi
...
   syslogd
   traceroute
0 profiles are in kill mode.
0 profiles are in unconfined mode.
7 processes have profiles defined.
2 processes are in enforce mode.
   /usr/sbin/cups-browsed (1190)
   /usr/sbin/cupsd (1018)
2 processes are in complain mode.
   /usr/sbin/avahi-daemon (646) avahi-daemon
   /usr/sbin/avahi-daemon (664) avahi-daemon
3 processes are unconfined but have a profile defined.
   /usr/sbin/sshd (1067)
   /usr/sbin/sshd (1472)
   /usr/sbin/sshd (1521)
0 processes are in mixed mode.
0 processes are in kill mode.
```

Options de la Commande

```
root@debian12:~# aa-complain --help
usage: aa-complain [-h] [-d DIR] [--no-reload] program [program ...]

Switch the given program to complain mode
```

```
positional arguments:
  program            name of program

options:
  -h, --help         show this help message and exit
  -d DIR, --dir DIR  path to profiles
  --no-reload        Do not reload the profile after modifying it
```

5.4 - Désactiver et Réactiver tous les Profils

Pour déactiver tous les profils, utilisez la commande **aa-teardown** :

```
root@debian12:~# aa-teardown
Unloading AppArmor profiles

root@debian12:~# aa-status
apparmor module is loaded.
```

Pour réactiver les profils, réinstallez AppArmor :

```
root@debian12:~# apt reinstall apparmor -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
0 upgraded, 0 newly installed, 1 reinstalled, 0 to remove and 0 not upgraded.
Need to get 616 kB of archives.
After this operation, 0 B of additional disk space will be used.
Get:1 http://deb.debian.org/debian bookworm/main amd64 apparmor amd64 3.0.8-3 [616 kB]
Fetched 616 kB in 0s (10.6 MB/s)
Preconfiguring packages ...
(Reading database ... 186665 files and directories currently installed.)
Preparing to unpack .../apparmor_3.0.8-3_amd64.deb ...
Unpacking apparmor (3.0.8-3) over (3.0.8-3) ...
```

```
Setting up apparmor (3.0.8-3) ...
Reloading AppArmor profiles
Processing triggers for man-db (2.11.2-2) ...
```

root@debian12:~# aa-notify -p -w 1 –user trainee Notification emitter started in the background

5.5 - Créer un Profil

Créez le script **newusercheck.sh** qui a pour but d'envoyer un email à un récipent chaque fois qu'un nouvel utilisateur est créé dans Debian 12 :

```
root@debian12:~# mkdir scripts

root@debian12:~# vi scripts/newusercheck.sh

root@debian12:~# cat scripts/newusercheck.sh
#!/bin/bash
# Send an email alert if a new account is added to the /etc/passwd file
# CRONJOB BELOW RUNS EVERY 5 MINUTES
# */5 * * * * /bin/bash /root/scripts/newusercheck.sh 1>/dev/null 2>/dev/null


HOSTNAME=$(hostname)
TO="<to@domain.com>"
FROM="<from@domain.com>"
USERLIST="/root/scripts/.user.lst"
NEWUSERLIST="/root/scripts/.userlist.txt"
PASSWDFILE="/etc/passwd"
COMPARE=0

trap "/bin/rm -rf --preserve-root -- $NEWUSERLIST" 0


if [ -s "$USERLIST" ] ; then
```

```
    /usr/bin/printf "[*] Checking previously known list of users\n"
    LASTREV="$(/bin/cat $USERLIST)"
    COMPARE=1
fi



/usr/bin/printf "[*] Obtaining current user list\n"
/bin/cat $PASSWDFILE | /usr/bin/cut -d: -f1 > $NEWUSERLIST


CURRENT="$(/bin/cat $NEWUSERLIST)"


if [ $COMPARE -eq 1 ] ; then
    if [ "$CURRENT" != "$LASTREV" ] ; then
        /usr/bin/printf "[!] WARNING: password file has changed\n"
        /usr/bin/diff $USERLIST $NEWUSERLIST | /bin/grep '^[<>]' | /bin/sed 's/</Removed: /;s/>/Added:/'
    /usr/bin/printf "[*] Sending email alert\n"
        /usr/bin/mail -r $FROM -A $NEWUSERLIST -s "WARNING: New Account Created on $HOSTNAME" $TO <<< "You are
receiving this email because a new user account has been created on $HOSTNAME. Attached to this email is a file
containing the CURRENT user accounts on the system. The user list has been updated so you will not receive this
alert until an account is created again."
    /usr/bin/printf "[!] WARNING: Previously known user list has been updated so you do not keep receiving this
warning\n"
    /bin/mv $NEWUSERLIST $USERLIST
    else
        /usr/bin/printf "[*] No new users have been created since the last check\n"
    fi
else
    /usr/bin/printf "[*] Creating initial database of previously known users\n"
    /bin/mv $NEWUSERLIST $USERLIST
fi

/bin/chmod 600 $USERLIST
```

```
exit 0
```

Rendez ce script exécutable et testez-le :

```
root@debian12:~# cd scripts

root@debian12:~/scripts# chmod u+x newusercheck.sh

root@debian12:~/scripts# ./newusercheck.sh
[*] Obtaining current user list
[*] Creating initial database of previously known users
```

La Commande aa-genprof

Utilisez maintenant la commande **aa-genprof** pour créer un profil :

```
root@debian12:~/scripts# aa-genprof /root/scripts/newusercheck.sh
Updating AppArmor profiles in /etc/apparmor.d.
Writing updated profile for /root/scripts/newusercheck.sh.
Setting /root/scripts/newusercheck.sh to complain mode.

Before you begin, you may wish to check if a
profile already exists for the application you
wish to confine. See the following wiki page for
more information:
https://gitlab.com/apparmor/apparmor/wikis/Profiles

Profiling: /root/scripts/newusercheck.sh

Please start the application to be profiled in
another window and exercise its functionality now.
```

```
Once completed, select the "Scan" option below in
order to scan the system logs for AppArmor events.

For each AppArmor event, you will be given the
opportunity to choose whether the access should be
allowed or denied.

[(S)can system log for AppArmor events] / (F)inish
```

Dans une deuxième connexion à votre VM Debian 12, exécutez le script **newusercheck.sh** :

```
trainee@debian12:~$ su -
Password: fenestros

root@debian12:~# cd scripts

root@debian12:~/scripts# ./newusercheck.sh
[*] Checking previously known list of users
[*] Obtaining current user list
[*] No new users have been created since the last check
```

Dans la première connexion, appuyez sur la touche **S** :

```
Reading log entries from /var/log/audit/audit.log.

Profile:  /root/scripts/newusercheck.sh
Execute:  /usr/bin/hostname
Severity: unknown

(I)nherit / (C)hild / (P)rofile / (N)amed / (U)nconfined / (X) ix On / (D)eny / Abo(r)t / (F)inish
```

Important - Notez que le script exécute la commande **/usr/bin/hostname**

et qu'AppArmor indique que la sévérité est **unknown**.

Appuyez maintenant sur la touche **I** pour **hériter** des permissions du processus parent du script, c'est-à-dire, **bash** :

```
Reading log entries from /var/log/audit/audit.log.

Profile:  /root/scripts/newusercheck.sh
Execute:  /usr/bin/hostname
Severity: unknown

(I)nherit / (C)hild / (P)rofile / (N)amed / (U)nconfined / (X) ix On / (D)eny / Abo(r)t / (F)inish

Profile:  /root/scripts/newusercheck.sh
Execute:  /usr/bin/printf
Severity: 1

(I)nherit / (C)hild / (P)rofile / (N)amed / (U)nconfined / (X) ix On / (D)eny / Abo(r)t / (F)inish
```

Important - Notez que le script exécute la commande **/usr/bin/printf** et qu'AppArmor indique que la sévérité est **1**.

De nouveau appuyez sur la touche **I** et continuez ce processus jusqu'à la question concernant **/dev/pts/1** :

```
Reading log entries from /var/log/audit/audit.log.

Profile:  /root/scripts/newusercheck.sh
Execute:  /usr/bin/hostname
Severity: unknown

(I)nherit / (C)hild / (P)rofile / (N)amed / (U)nconfined / (X) ix On / (D)eny / Abo(r)t / (F)inish
```

```
Profile:  /root/scripts/newusercheck.sh
Execute:  /usr/bin/printf
Severity: 1

(I)nherit / (C)hild / (P)rofile / (N)amed / (U)nconfined / (X) ix On / (D)eny / Abo(r)t / (F)inish

Profile:  /root/scripts/newusercheck.sh
Execute:  /usr/bin/cat
Severity: unknown

(I)nherit / (C)hild / (N)amed / (X) ix On / (D)eny / Abo(r)t / (F)inish

Profile:  /root/scripts/newusercheck.sh
Execute:  /usr/bin/cut
Severity: 2

(I)nherit / (C)hild / (P)rofile / (N)amed / (U)nconfined / (X) ix On / (D)eny / Abo(r)t / (F)inish

Profile:  /root/scripts/newusercheck.sh
Execute:  /usr/bin/chmod
Severity: unknown

(I)nherit / (C)hild / (N)amed / (X) ix On / (D)eny / Abo(r)t / (F)inish

Profile:  /root/scripts/newusercheck.sh
Execute:  /usr/bin/rm
Severity: unknown

(I)nherit / (C)hild / (N)amed / (X) ix On / (D)eny / Abo(r)t / (F)inish
Complain-mode changes:

Profile:  /root/scripts/newusercheck.sh
Path:     /dev/pts/1
New Mode: rw
```

```
Severity: 9

 [1 - include <abstractions/consoles>]
  2 - include <abstractions/lightdm>
  3 - include <abstractions/xdg-open>
  4 - /dev/pts/1 rw,
(A)llow / [(D)eny] / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Audi(t) / Abo(r)t / (F)inish
```

Appuyez sur la touche **A** pour toutes les questions suivantes :

```
Reading log entries from /var/log/audit/audit.log.

Profile:  /root/scripts/newusercheck.sh
Execute:  /usr/bin/hostname
Severity: unknown

(I)nherit / (C)hild / (P)rofile / (N)amed / (U)nconfined / (X) ix On / (D)eny / Abo(r)t / (F)inish

Profile:  /root/scripts/newusercheck.sh
Execute:  /usr/bin/printf
Severity: 1

(I)nherit / (C)hild / (P)rofile / (N)amed / (U)nconfined / (X) ix On / (D)eny / Abo(r)t / (F)inish

Profile:  /root/scripts/newusercheck.sh
Execute:  /usr/bin/cat
Severity: unknown

(I)nherit / (C)hild / (N)amed / (X) ix On / (D)eny / Abo(r)t / (F)inish

Profile:  /root/scripts/newusercheck.sh
Execute:  /usr/bin/cut
Severity: 2
```

```
(I)nherit / (C)hild / (P)rofile / (N)amed / (U)nconfined / (X) ix On / (D)eny / Abo(r)t / (F)inish

Profile:  /root/scripts/newusercheck.sh
Execute:  /usr/bin/chmod
Severity: unknown

(I)nherit / (C)hild / (N)amed / (X) ix On / (D)eny / Abo(r)t / (F)inish

Profile:  /root/scripts/newusercheck.sh
Execute:  /usr/bin/rm
Severity: unknown

(I)nherit / (C)hild / (N)amed / (X) ix On / (D)eny / Abo(r)t / (F)inish
Complain-mode changes:

Profile:  /root/scripts/newusercheck.sh
Path:     /dev/pts/1
New Mode: rw
Severity: 9

 [1 - include <abstractions/consoles>]
  2 - include <abstractions/lightdm>
  3 - include <abstractions/xdg-open>
  4 - /dev/pts/1 rw,
(A)llow / [(D)eny] / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Audi(t) / Abo(r)t / (F)inish
Adding include <abstractions/consoles> to profile.

Profile:  /root/scripts/newusercheck.sh
Path:     /root/scripts/.userlist.txt
New Mode: owner w
Severity: unknown

 [1 - owner /root/scripts/.userlist.txt w,]
(A)llow / [(D)eny] / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Audi(t) / (O)wner permissions off /
```

```
Abo(r)t / (F)inish
Adding owner /root/scripts/.userlist.txt w, to profile.

Profile:  /root/scripts/newusercheck.sh
Path:     /etc/ld.so.cache
New Mode: owner r
Severity: 1

 [1 - include <abstractions/lightdm>]
  2 - owner /etc/ld.so.cache r,
(A)llow / [(D)eny] / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Audi(t) / (O)wner permissions off /
Abo(r)t / (F)inish
Adding include <abstractions/lightdm> to profile.

Profile:  /root/scripts/newusercheck.sh
Path:     /root/scripts/.user.lst
New Mode: owner r
Severity: unknown

 [1 - owner /root/scripts/.user.lst r,]
(A)llow / [(D)eny] / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Audi(t) / (O)wner permissions off /
Abo(r)t / (F)inish
Adding owner /root/scripts/.user.lst r, to profile.

Profile:  /root/scripts/newusercheck.sh
Path:     /root/scripts/.userlist.txt
Old Mode: owner w
New Mode: owner r
Severity: unknown

 [1 - owner /root/scripts/.userlist.txt r,]
(A)llow / [(D)eny] / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Audi(t) / (O)wner permissions off /
Abo(r)t / (F)inish
Adding owner /root/scripts/.userlist.txt r, to profile.
```

```
Profile:  /root/scripts/newusercheck.sh
Path:     /root/scripts/.user.lst
Old Mode: owner r
New Mode: owner w
Severity: unknown

 [1 - owner /root/scripts/.user.lst w,]
(A)llow / [(D)eny] / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Audi(t) / (O)wner permissions off /
Abo(r)t / (F)inish
Adding owner /root/scripts/.user.lst w, to profile.

= Changed Local Profiles =

The following local profiles were changed. Would you like to save them?

 [1 - /root/scripts/newusercheck.sh]
(S)ave Changes / Save Selec(t)ed Profile / [(V)iew Changes] / View Changes b/w (C)lean profiles / Abo(r)t
```

Appuyez sur la touche **S** :

```
...
Writing updated profile for /root/scripts/newusercheck.sh.

Profiling: /root/scripts/newusercheck.sh

Please start the application to be profiled in
another window and exercise its functionality now.

Once completed, select the "Scan" option below in
order to scan the system logs for AppArmor events.

For each AppArmor event, you will be given the
opportunity to choose whether the access should be
allowed or denied.
```

```
[(S)can system log for AppArmor events] / (F)inish
```

Retournez dans la deuxième connexion à votre VM et exécutez de nouveau le script **newusercheck.sh** :

```
root@debian12:~/scripts# ./newusercheck.sh
[*] Checking previously known list of users
[*] Obtaining current user list
[*] No new users have been created since the last check
```

Dans la première connexion, appuyez de nouveau sur la touche **S** :

```
...
Writing updated profile for /root/scripts/newusercheck.sh.

Profiling: /root/scripts/newusercheck.sh

Please start the application to be profiled in
another window and exercise its functionality now.

Once completed, select the "Scan" option below in
order to scan the system logs for AppArmor events.

For each AppArmor event, you will be given the
opportunity to choose whether the access should be
allowed or denied.

[(S)can system log for AppArmor events] / (F)inish
Reading log entries from /var/log/audit/audit.log.

Profiling: /root/scripts/newusercheck.sh

Please start the application to be profiled in
another window and exercise its functionality now.
```

```
Once completed, select the "Scan" option below in
order to scan the system logs for AppArmor events.

For each AppArmor event, you will be given the
opportunity to choose whether the access should be
allowed or denied.

[(S)can system log for AppArmor events] / (F)inish
```

Important - Notez l'abscence d'erreurs.

Appuyez maintenant sur la touch **F** :

```
...
Reloaded AppArmor profiles in enforce mode.

Please consider contributing your new profile!
See the following wiki page for more information:
https://gitlab.com/apparmor/apparmor/wikis/Profiles

Finished generating profile for /root/scripts/newusercheck.sh.
```

Le profil à été créé dans le répertoire **/etc/apparmor.d/** :

```
root@debian12:~/scripts# ls /etc/apparmor.d | grep root
root.scripts.newusercheck.sh

root@debian12:~/scripts# cat /etc/apparmor.d/root.scripts.newusercheck.sh
# Last Modified: Wed Dec  3 16:36:43 2025
abi <abi/3.0>,
```

```
include <tunables/global>

/root/scripts/newusercheck.sh {
  include <abstractions/base>
  include <abstractions/bash>
  include <abstractions/consoles>
  include <abstractions/lightdm>

  /root/scripts/newusercheck.sh r,
  /usr/bin/bash ix,
  /usr/bin/cat mrix,
  /usr/bin/chmod mrix,
  /usr/bin/cut mrix,
  /usr/bin/hostname mrix,
  /usr/bin/printf mrix,
  /usr/bin/rm mrix,
  owner /root/scripts/.user.lst r,
  owner /root/scripts/.user.lst w,
  owner /root/scripts/.userlist.txt r,
  owner /root/scripts/.userlist.txt w,

}
```

Ce fichier inclut le contenu du profil **/etc/apparmor.d/tunables/global** :

```
root@debian12:~/scripts# cat /etc/apparmor.d/tunables/global
# ------------------------------------------------------------------
#
#    Copyright (C) 2006-2009 Novell/SUSE
#    Copyright (C) 2010-2014 Canonical Ltd.
#
#    This program is free software; you can redistribute it and/or
#    modify it under the terms of version 2 of the GNU General Public
#    License published by the Free Software Foundation.
```

```
#
# ----------------------------------------------------------------

# All the tunables definitions that should be available to every profile
# should be included here

include <tunables/home>
include <tunables/multiarch>
include <tunables/proc>
include <tunables/alias>
include <tunables/kernelvars>
include <tunables/xdg-user-dirs>
include <tunables/share>
include <tunables/etc>
include <tunables/run>
```

Options de la Commande

```
root@debian12:~/scripts# aa-genprof --help
usage: aa-genprof [-h] [-d DIR] [-f FILE] [-j] program

Generate profile for the given program

positional arguments:
  program               name of program to profile

options:
  -h, --help            show this help message and exit
  -d DIR, --dir DIR     path to profiles
  -f FILE, --file FILE  path to logfile
  -j, --json            Input and Output in JSON
```

La Commande aa-logprof

Exécutez maintenant la commande **aa-logprof** pour vérifier que toutes les permissions sont adéquatement placées :

```
root@debian12:~/scripts# aa-logprof
Updating AppArmor profiles in /etc/apparmor.d.
Reading log entries from /var/log/audit/audit.log.
Complain-mode changes:
Enforce-mode changes:

Profile:    /usr/sbin/cupsd
Capability: net_admin
Severity:   8

 [1 - capability net_admin,]
(A)llow / [(D)eny] / (I)gnore / Audi(t) / Abo(r)t / (F)inish
```

Appuyez sur la touche **A** :

</code> Adding capability net_admin, to profile.

= Changed Local Profiles =

The following local profiles were changed. Would you like to save them?

[1 - /usr/sbin/cupsd] (S)ave Changes / Save Selec(t)ed Profile / [(V)iew Changes] / View Changes b/w (C)lean profiles / Abo®t

Appuyez sur la touche **S** :

</code> Writing updated profile for /usr/sbin/cupsd. </code>

Exécutez de nouveau la commande **aa-logprof** :

```
root@debian12:~/scripts# aa-logprof
```

```
Updating AppArmor profiles in /etc/apparmor.d.
Reading log entries from /var/log/audit/audit.log.
Complain-mode changes:
Enforce-mode changes:
```

Options de la Commande

```
root@debian12:~/scripts# aa-logprof --help
usage: aa-logprof [-h] [-d DIR] [-f FILE] [-m MARK] [-j]

Process log entries to generate profiles

options:
  -h, --help            show this help message and exit
  -d DIR, --dir DIR     path to profiles
  -f FILE, --file FILE  path to logfile
  -m MARK, --mark MARK  mark in the log to start processing after
  -j, --json            Input and Output in JSON
```

Dernièrement passez le nouveau profil en mode **enforce** :

```
root@debian12:~/scripts# aa-enforce /etc/apparmor.d/root.scripts.newusercheck.sh
Setting /etc/apparmor.d/root.scripts.newusercheck.sh to enforce mode.

root@debian12:~/scripts# aa-logprof
Updating AppArmor profiles in /etc/apparmor.d.
Reading log entries from /var/log/audit/audit.log.
Complain-mode changes:
Enforce-mode changes:
```

5.6 - Supprimer un Profil

Afin de supprimer le profil **root.scripts.newusercheck.sh**, il faut de d'abord le décharger du noyau avant de supprimer le fichier profil :

```
root@debian12:~/scripts# apparmor_parser -R /etc/apparmor.d/root.scripts.newusercheck.sh

root@debian12:~/scripts# rm -f /etc/apparmor.d/root.scripts.newusercheck.sh
```

Options de la Commande

```
root@debian12:~/scripts# apparmor_parser --help
AppArmor parser version 3.0.8
Copyright (C) 1999-2008 Novell Inc.
Copyright 2009-2018 Canonical Ltd.

Usage: apparmor_parser [options] [profile]

Options:
--------
-a, --add               Add apparmor definitions [default]
-r, --replace           Replace apparmor definitions
-R, --remove            Remove apparmor definitions
-C, --Complain          Force the profile into complain mode
-B, --binary            Input is precompiled profile
-N, --names             Dump names of profiles in input.
-S, --stdout            Dump compiled profile to stdout
-o n, --ofile n         Write output to file n
-b n, --base n          Set base dir and cwd
-I n, --Include n       Add n to the search path
-f n, --subdomainfs n   Set location of apparmor filesystem
-m n, --match-string n  Use only features n
-M n, --features-file n Set compile & kernel features to file n
```

```
--policy-features n     Policy features set in file n
--override-policy-abi n     As policy-features but override ABI rules
--kernel-features n     Kernel features set in file n
-n n, --namespace n     Set Namespace for the profile
-X, --readimpliesX      Map profile read permissions to mr
-k, --show-cache        Report cache hit/miss details
-K, --skip-cache        Do not attempt to load or save cached profiles
-T, --skip-read-cache   Do not attempt to load cached profiles
-W, --write-cache       Save cached profile (force with -T)
    --skip-bad-cache    Don't clear cache if out of sync
    --purge-cache       Clear cache regardless of its state
    --debug-cache       Debug cache file checks
    --print-cache-dir   Print the cache directory path
-L, --cache-loc n       Set the location of the profile caches
-q, --quiet             Don't emit warnings
-v, --verbose           Show profile names as they load
-Q, --skip-kernel-load  Do everything except loading into kernel
-V, --version           Display version info and exit
-d [n], --debug         Debug apparmor definitions OR [n]
-p, --preprocess        Dump preprocessed profile
-D [n], --dump          Dump internal info for debugging
-O [n], --Optimize      Control dfa optimizations
-h [cmd], --help[=cmd]  Display this text or info about cmd
-j n, --jobs n          Set the number of compile threads
--max-jobs n            Hard cap on --jobs. Default 8*cpus
--abort-on-error        Abort processing of profiles on first error
--skip-bad-cache-rebuild Do not try rebuilding the cache if it is rejected by the kernel
--config-file n         Specify the parser config file location, processed early before other options.
--print-config          Print config file location
--warn n                Enable warnings (see --help=warn)
--Werror [n]            Convert warnings to errors. If n is specified turn warn n into an error
```

Terminez par procéder à un nettoyage d'AppArmor et le redémarrage du service :

```
root@debian12:~/scripts# aa-remove-unknown
root@debian12:~/scripts# systemctl restart apparmor
root@debian12:~/scripts# systemctl status apparmor
● apparmor.service - Load AppArmor profiles
     Loaded: loaded (/lib/systemd/system/apparmor.service; enabled; preset: enabled)
     Active: active (exited) since Wed 2025-12-03 17:32:36 CET; 8s ago
       Docs: man:apparmor(7)
             https://gitlab.com/apparmor/apparmor/wikis/home/
    Process: 2992 ExecStart=/lib/apparmor/apparmor.systemd reload (code=exited, status=0/SUCCESS)
   Main PID: 2992 (code=exited, status=0/SUCCESS)
        CPU: 1.261s

Dec 03 17:32:35 debian12 systemd[1]: Starting apparmor.service - Load AppArmor profiles...
Dec 03 17:32:35 debian12 apparmor.systemd[2992]: Restarting AppArmor
Dec 03 17:32:35 debian12 apparmor.systemd[2992]: Reloading AppArmor profiles
Dec 03 17:32:36 debian12 systemd[1]: Finished apparmor.service - Load AppArmor profiles.
```

Options de la Commande

```
root@debian12:~/scripts# aa-remove-unknown --help
usage: /usr/sbin/aa-remove-unknown [options]

Remove profiles unknown to the system

Options:
 -h, --help     Show this help message and exit
 -n             Dry run; don't remove profiles
```

LAB #6 - Mise en place de SELinux pour sécuriser le serveur

6.1 - Présentationn

Désactivez AppArmor :

```
root@debian12:~# systemctl disable apparmor --now
Synchronizing state of apparmor.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install disable apparmor
Removed "/etc/systemd/system/sysinit.target.wants/apparmor.service".

root@debian12:~# systemctl status apparmor
○ apparmor.service - Load AppArmor profiles
     Loaded: loaded (/lib/systemd/system/apparmor.service; disabled; preset: enabled)
     Active: inactive (dead) since Sun 2025-11-30 09:59:03 CET; 1min 30s ago
   Duration: 5d 48min 44.395s
       Docs: man:apparmor(7)
             https://gitlab.com/apparmor/apparmor/wikis/home/
    Process: 57991 ExecStop=/bin/true (code=exited, status=0/SUCCESS)
   Main PID: 322 (code=exited, status=0/SUCCESS)
        CPU: 1ms

Nov 25 09:10:18 debian12 apparmor.systemd[322]: Restarting AppArmor
Nov 25 09:10:18 debian12 apparmor.systemd[322]: Reloading AppArmor profiles
Nov 25 09:10:17 debian12 systemd[1]: Starting apparmor.service - Load AppArmor profiles...
Nov 25 09:10:19 debian12 systemd[1]: Finished apparmor.service - Load AppArmor profiles.
Nov 30 09:59:03 debian12 systemd[1]: Stopping apparmor.service - Load AppArmor profiles...
Nov 30 09:59:03 debian12 systemd[1]: apparmor.service: Deactivated successfully.
Nov 30 09:59:03 debian12 systemd[1]: Stopped apparmor.service - Load AppArmor profiles.
```

Editez la ligne **GRUB_CMDLINE_LINUX_DEFAULT** dans le fichier **/etc/default/grub** :

```
root@debian12:~/scripts# cd ~

root@debian12:~# vi /etc/default/grub
```

```
root@debian12:~# cat /etc/default/grub
# If you change this file, run 'update-grub' afterwards to update
# /boot/grub/grub.cfg.
# For full documentation of the options in this file, see:
#   info -f grub -n 'Simple configuration'

GRUB_DEFAULT=0
GRUB_TIMEOUT=5
GRUB_DISTRIBUTOR=`lsb_release -i -s 2> /dev/null || echo Debian`
GRUB_CMDLINE_LINUX_DEFAULT="quiet"
GRUB_CMDLINE_LINUX=""

# If your computer has multiple operating systems installed, then you
# probably want to run os-prober. However, if your computer is a host
# for guest OSes installed via LVM or raw disk devices, running
# os-prober can cause damage to those guest OSes as it mounts
# filesystems to look for things.
#GRUB_DISABLE_OS_PROBER=false

# Uncomment to enable BadRAM filtering, modify to suit your needs
# This works with Linux (no patch required) and with any kernel that obtains
# the memory map information from GRUB (GNU Mach, kernel of FreeBSD ...)
#GRUB_BADRAM="0x01234567,0xfefefefe,0x89abcdef,0xefefefef"

# Uncomment to disable graphical terminal
#GRUB_TERMINAL=console

# The resolution used on graphical terminal
# note that you can use only modes which your graphic card supports via VBE
# you can see them in real GRUB with the command `vbeinfo'
#GRUB_GFXMODE=640x480

# Uncomment if you don't want GRUB to pass "root=UUID=xxx" parameter to Linux
#GRUB_DISABLE_LINUX_UUID=true
```

```
# Uncomment to disable generation of recovery mode menu entries
#GRUB_DISABLE_RECOVERY="true"

# Uncomment to get a beep at g
```

Mettez à jour GRUB :

```
root@debian12:~# update-grub
Generating grub configuration file ...
Found background image: /usr/share/images/desktop-base/desktop-grub.png
Found linux image: /boot/vmlinuz-6.1.0-41-amd64
Found initrd image: /boot/initrd.img-6.1.0-41-amd64
Found linux image: /boot/vmlinuz-5.10.0-36-amd64
Found initrd image: /boot/initrd.img-5.10.0-36-amd64
Warning: os-prober will not be executed to detect other bootable partitions.
Systems on them will not be added to the GRUB boot configuration.
Check GRUB_DISABLE_OS_PROBER documentation entry.
done
```

Redémarrez la VM :

```
root@debian12:~# reboot
```

Reconnectez-vous à la VM et passez en tant que l'utilisateur **root** :

```
trainee@debian12:~$ su -
Password: fenestros

root@debian12:~#
```

Installez SELinux :

```
root@debian12:~# apt install selinux-basics selinux-policy-default selinux-utils policycoreutils -y
```

```
root@debian12:~# selinux-activate
Activating SE Linux
Generating grub configuration file ...
Found background image: /usr/share/images/desktop-base/desktop-grub.png
Found linux image: /boot/vmlinuz-6.1.0-41-amd64
Found initrd image: /boot/initrd.img-6.1.0-41-amd64
Found linux image: /boot/vmlinuz-5.10.0-36-amd64
Found initrd image: /boot/initrd.img-5.10.0-36-amd64
Warning: os-prober will not be executed to detect other bootable partitions.
Systems on them will not be added to the GRUB boot configuration.
Check GRUB_DISABLE_OS_PROBER documentation entry.
done
SE Linux is activated.  You may need to reboot now.

root@debian12:~# reboot
```

Important - La commande **selinux-activate** modifie la configuration de GRUB afin que SELinux soit activé au démarrage de la VM et crée ensuite le fichier **/.autorelabel**. Le fichier **/.autorelabel** force SELinux à étiqueter les fichiers, services, etc avec un **Security Context**.

Lors de votre reconnexion à la VM, saisissez la commande **ls -l** :

```
root@debian12:~# ls -l
total 3528
drwxr-xr-x. 3 root root    4096 Nov 25 15:16 attributs
-rw-r--r--. 1 root root       0 Nov 27 14:07 mypasswd
```

Important - Notez le caractère **.** à la fin du masque des permissions de chaque objet. Ceci implique que SELinux a étiqueté l'objet concerné.

6.2 - 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** :

Type de Sécurité	Nom	Description
DAC	*Discretional Access Control*	L'accès aux objets est en fonction de l'identité (utilisateur,groupe). Un utilisateur peut rendre accessibles aux autres ses propres objets.
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 de 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. Pour résumer, SELinux prime sur les droits DAC.

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.

6.3 - 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 Debian, le fichier **/etc/selinux/default/setrans.conf** contient la correspondance entre les niveaux et leurs valeurs compréhensibles par l'utilisateur :

```
root@debian12:~# cat /etc/selinux/default/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
```

Important - Notez que sous RedHat, le fichier setrans.conf se trouve dans le répertoire **/etc/selinux/targeted/setrans.conf**.

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@debian12:~# /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       *
sddm                 xdm                  s0-s0                *
```

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/default/policy** :

```
root@debian12:~# ls -l /etc/selinux/default/policy
total 2100
-rw-r--r--. 1 root root 2148201 Nov 30 10:19 policy.33
```

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

```
root@debian12:~# seinfo
Statistics for policy file: /sys/fs/selinux/policy
```

```
Policy Version:             33 (MLS enabled)
Target Policy:              selinux
Handle unknown classes:     allow
  Classes:             134    Permissions:         425
  Sensitivities:         1    Categories:         1024
  Types:              3936    Attributes:          217
  Users:                 7    Roles:                15
  Booleans:            291    Cond. Expr.:         321
  Allow:            104302    Neverallow:            0
  Auditallow:           21    Dontaudit:         16813
  Type_trans:         9245    Type_change:         123
  Type_member:          16    Range_trans:          14
  Role allow:           32    Role_trans:          376
  Constraints:         133    Validatetrans:         0
  MLS Constrain:       110    MLS Val. Tran:         0
  Permissives:           0    Polcap:                5
  Defaults:              0    Typebounds:            0
  Allowxperm:            0    Neverallowxperm:       0
  Auditallowxperm:       0    Dontauditxperm:        0
  Ibendportcon:          0    Ibpkeycon:             0
  Initial SIDs:         27    Fs_use:               29
  Genfscon:             93    Portcon:             479
  Netifcon:              0    Nodecon:               0
```

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***.

6.4 - 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
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

6.5 - 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@debian12:~# 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=permissive
# SELINUXTYPE= can take one of these two values:
# default - equivalent to the old strict and targeted policies
# mls     - Multi-Level Security (for military and educational use)
# src     - Custom policy built from source
SELINUXTYPE=default

# SETLOCALDEFS= Check local definition changes
SETLOCALDEFS=0
```

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

```
root@debian12:~# getenforce
Permissive
```

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

```
root@debian12:~# setenforce enforcing

root@debian12:~# getenforce
Enforcing
```

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

```
root@debian12:~# sestatus
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             default
Current mode:                   enforcing
Mode from config file:          permissive
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Memory protection checking:     actual (secure)
Max kernel policy version:      33
```

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

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

```
root@debian12:~# sestatus -v
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             default
Current mode:                   enforcing
Mode from config file:          permissive
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Memory protection checking:     actual (secure)
Max kernel policy version:      33

Process contexts:
Current context:                unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
Init context:                   system_u:system_r:init_t:s0
/sbin/agetty                    system_u:system_r:getty_t:s0
```

```
/usr/sbin/sshd                  system_u:system_r:sshd_t:s0

File contexts:
Controlling terminal:           unconfined_u:object_r:user_devpts_t:s0
/etc/passwd                     system_u:object_r:etc_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
```

6.6 - 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@debian12:~# getsebool -a | more
aide_mmap_files --> off
allow_cvs_read_shadow --> off
allow_execheap --> off
allow_execmem --> off
allow_execmod --> off
allow_execstack --> off
allow_ftpd_anon_write --> off
allow_ftpd_full_access --> off
allow_ftpd_use_cifs --> off
allow_ftpd_use_nfs --> off
allow_gssd_read_tmp --> off
allow_gssd_write_tmp --> off
allow_httpd_anon_write --> off
```

```
allow_httpd_apcupsd_cgi_script_anon_write --> off
allow_httpd_awstats_script_anon_write --> off
allow_httpd_collectd_script_anon_write --> off
allow_httpd_cvs_script_anon_write --> off
allow_httpd_lightsquid_script_anon_write --> off
allow_httpd_man2html_script_anon_write --> off
allow_httpd_mediawiki_script_anon_write --> off
allow_httpd_mod_auth_pam --> off
allow_httpd_mojomojo_script_anon_write --> off
allow_httpd_munin_script_anon_write --> off
allow_httpd_nagios_script_anon_write --> off
allow_httpd_nutups_cgi_script_anon_write --> off
allow_httpd_prewikka_script_anon_write --> off
allow_httpd_smokeping_cgi_script_anon_write --> off
allow_httpd_squid_script_anon_write --> off
allow_httpd_sys_script_anon_write --> off
allow_httpd_unconfined_script_anon_write --> off
allow_httpd_user_script_anon_write --> off
allow_httpd_webalizer_script_anon_write --> off
allow_java_execstack --> off
allow_kerberos --> off
allow_mount_anyfile --> off
allow_mplayer_execstack --> off
allow_nfsd_anon_write --> off
allow_polyinstantiation --> off
allow_ptrace --> off
allow_raw_memory_access --> off
allow_rsync_anon_write --> off
allow_saslauthd_read_shadow --> off
allow_smbd_anon_write --> off
allow_ssh_keysign --> off
allow_user_mysql_connect --> off
allow_user_postgresql_connect --> off
allow_write_xshm --> off
```

```
allow_ypbind --> off
allow_zebra_write_config --> off
amavis_use_jit --> off
authlogin_nsswitch_use_ldap --> off
authlogin_pam --> on
awstats_purge_apache_log_files --> off
boinc_execmem --> on
boinc_gpu --> on
--More--
```

ou la commande **sestatus -b** :

```
root@debian12:~# sestatus -b | more
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             default
Current mode:                   enforcing
Mode from config file:          permissive
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Memory protection checking:     actual (secure)
Max kernel policy version:      33

Policy booleans:
aide_mmap_files                             off
allow_cvs_read_shadow                       off
allow_execheap                              off
allow_execmem                               off
allow_execmod                               off
allow_execstack                             off
allow_ftpd_anon_write                       off
allow_ftpd_full_access                      off
allow_ftpd_use_cifs                         off
```

```
allow_ftpd_use_nfs                          off
allow_gssd_read_tmp                         off
allow_gssd_write_tmp                        off
allow_httpd_anon_write                      off
allow_httpd_apcupsd_cgi_script_anon_write   off
allow_httpd_awstats_script_anon_write       off
allow_httpd_collectd_script_anon_write      off
allow_httpd_cvs_script_anon_write           off
allow_httpd_lightsquid_script_anon_write    off
allow_httpd_man2html_script_anon_write      off
allow_httpd_mediawiki_script_anon_write     off
allow_httpd_mod_auth_pam                    off
allow_httpd_mojomojo_script_anon_write      off
allow_httpd_munin_script_anon_write         off
allow_httpd_nagios_script_anon_write        off
allow_httpd_nutups_cgi_script_anon_write    off
allow_httpd_prewikka_script_anon_write      off
allow_httpd_smokeping_cgi_script_anon_write off
allow_httpd_squid_script_anon_write         off
allow_httpd_sys_script_anon_write           off
allow_httpd_unconfined_script_anon_write    off
allow_httpd_user_script_anon_write          off
allow_httpd_webalizer_script_anon_write     off
allow_java_execstack                        off
allow_kerberos                              off
allow_mount_anyfile                         off
allow_mplayer_execstack                     off
allow_nfsd_anon_write                       off
allow_polyinstantiation                     off
allow_ptrace                                off
allow_raw_memory_access                     off
allow_rsync_anon_write                      off
allow_saslauthd_read_shadow                 off
allow_smbd_anon_write                       off
```

```
--More--
```

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

```
root@debian12:~# setsebool allow_ftpd_anon_write 1

root@debian12:~# getsebool allow_ftpd_anon_write
allow_ftpd_anon_write --> on

root@debian12:~# setsebool allow_ftpd_anon_write 0

root@debian12:~# getsebool allow_ftpd_anon_write
allow_ftpd_anon_write --> off
```

LAB #7 - Travailler avec SELinux

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

```
root@debian12:~# semodule -DB
libsemanage.add_user: user sddm not in password file
```

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

```
root@debian12:~# seinfo
Statistics for policy file: /sys/fs/selinux/policy
Policy Version:             33 (MLS enabled)
Target Policy:              selinux
Handle unknown classes:     allow
  Classes:             134    Permissions:         425
  Sensitivities:         1    Categories:         1024
  Types:              3936    Attributes:          217
  Users:                 7    Roles:                15
```

```
  Booleans:            291    Cond. Expr.:         321
  Allow:            104302    Neverallow:            0
  Auditallow:           21    Dontaudit:             0
  Type_trans:         9245    Type_change:         123
  Type_member:          16    Range_trans:          14
  Role allow:           32    Role_trans:          376
  Constraints:         133    Validatetrans:         0
  MLS Constrain:       110    MLS Val. Tran:         0
  Permissives:           0    Polcap:                5
  Defaults:              0    Typebounds:            0
  Allowxperm:            0    Neverallowxperm:       0
  Auditallowxperm:       0    Dontauditxperm:        0
  Ibendportcon:          0    Ibpkeycon:             0
  Initial SIDs:         27    Fs_use:               29
  Genfscon:             93    Portcon:             479
  Netifcon:              0    Nodecon:               0
```

7.1 - Copier et Déplacer des Fichiers

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

```
root@debian12:~# exit
logout

trainee@debian12:~$ touch file1 file2

trainee@debian12:~$ ls -lZ file*
-rw-r--r--. 1 trainee trainee unconfined_u:object_r:user_home_t:s0 0 Nov 30 15:11 file1
-rw-r--r--. 1 trainee trainee unconfined_u:object_r:user_home_t:s0 0 Nov 30 15:11 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@debian12:~$ cp file1 /tmp

trainee@debian12:~$ ls -lZ /tmp/file1
-rw-r--r--. 1 trainee trainee unconfined_u:object_r:user_tmp_t:s0 0 Nov 30 15:13 /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@debian12:~$ mv file2 /tmp

trainee@debian12:~$ ls -lZ /tmp/file2
-rw-r--r--. 1 trainee trainee unconfined_u:object_r:user_home_t:s0 0 Nov 30 15:11 /tmp/file2
```

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

7.2 - Vérifier les SC des Processus

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

```
trainee@debian12:~$ 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  0.2 211972 48516 ?        Ss   10:22   0:02 /sbin/init
system_u:system_r:kernel_t:s0   root           2  0.0  0.0      0     0 ?        S    10:22   0:00 [kthreadd]
system_u:system_r:kernel_t:s0   root           3  0.0  0.0      0     0 ?        I<   10:22   0:00 [rcu_gp]
system_u:system_r:kernel_t:s0   root           4  0.0  0.0      0     0 ?        I<   10:22   0:00 [rcu_par_gp]
system_u:system_r:kernel_t:s0   root           5  0.0  0.0      0     0 ?        I<   10:22   0:00 [slub_flushwq]
system_u:system_r:kernel_t:s0   root           6  0.0  0.0      0     0 ?        I<   10:22   0:00 [netns]
system_u:system_r:kernel_t:s0   root           8  0.0  0.0      0     0 ?        I<   10:22   0:00 [kworker/0:0H-
events_highpri]
system_u:system_r:kernel_t:s0   root          10  0.0  0.0      0     0 ?        I<   10:22   0:00 [mm_percpu_wq]
system_u:system_r:kernel_t:s0   root          11  0.0  0.0      0     0 ?        I    10:22   0:00
```

```
[rcu_tasks_kthread]
system_u:system_r:kernel_t:s0   root          12  0.0  0.0      0     0 ?        I    10:22   0:00
[rcu_tasks_rude_kthread]
system_u:system_r:kernel_t:s0   root          13  0.0  0.0      0     0 ?        I    10:22   0:00
[rcu_tasks_trace_kthread]
system_u:system_r:kernel_t:s0   root          14  0.0  0.0      0     0 ?        S    10:22   0:00 [ksoftirqd/0]
system_u:system_r:kernel_t:s0   root          15  0.0  0.0      0     0 ?        I    10:22   0:00 [rcu_preempt]
system_u:system_r:kernel_t:s0   root          16  0.0  0.0      0     0 ?        S    10:22   0:00 [migration/0]
system_u:system_r:kernel_t:s0   root          18  0.0  0.0      0     0 ?        S    10:22   0:00 [cpuhp/0]
system_u:system_r:kernel_t:s0   root          19  0.0  0.0      0     0 ?        S    10:22   0:00 [cpuhp/1]
system_u:system_r:kernel_t:s0   root          20  0.0  0.0      0     0 ?        S    10:22   0:00 [migration/1]
system_u:system_r:kernel_t:s0   root          21  0.0  0.0      0     0 ?        S    10:22   0:00 [ksoftirqd/1]
system_u:system_r:kernel_t:s0   root          23  0.0  0.0      0     0 ?        I<   10:22   0:00 [kworker/1:0H-
events_highpri]
system_u:system_r:kernel_t:s0   root          24  0.0  0.0      0     0 ?        S    10:22   0:00 [cpuhp/2]
system_u:system_r:kernel_t:s0   root          25  0.0  0.0      0     0 ?        S    10:22   0:00 [migration/2]
system_u:system_r:kernel_t:s0   root          26  0.0  0.0      0     0 ?        S    10:22   0:00 [ksoftirqd/2]
system_u:system_r:kernel_t:s0   root          27  0.0  0.0      0     0 ?        I    10:22   0:00 [kworker/2:0-
events]
system_u:system_r:kernel_t:s0   root          28  0.0  0.0      0     0 ?        I<   10:22   0:00 [kworker/2:0H-
events_highpri]
system_u:system_r:kernel_t:s0   root          29  0.0  0.0      0     0 ?        S    10:22   0:00 [cpuhp/3]
system_u:system_r:kernel_t:s0   root          30  0.0  0.0      0     0 ?        S    10:22   0:00 [migration/3]
system_u:system_r:kernel_t:s0   root          31  0.0  0.0      0     0 ?        S    10:22   0:00 [ksoftirqd/3]
system_u:system_r:kernel_t:s0   root          33  0.0  0.0      0     0 ?        I<   10:22   0:00 [kworker/3:0H-
events_highpri]
system_u:system_r:kernel_t:s0   root          34  0.0  0.0      0     0 ?        S    10:22   0:00 [cpuhp/4]
system_u:system_r:kernel_t:s0   root          35  0.0  0.0      0     0 ?        S    10:22   0:00 [migration/4]
system_u:system_r:kernel_t:s0   root          36  0.0  0.0      0     0 ?        S    10:22   0:00 [ksoftirqd/4]
system_u:system_r:kernel_t:s0   root          38  0.0  0.0      0     0 ?        I<   10:22   0:00 [kworker/4:0H-
events_highpri]
system_u:system_r:kernel_t:s0   root          39  0.0  0.0      0     0 ?        S    10:22   0:00 [cpuhp/5]
system_u:system_r:kernel_t:s0   root          40  0.0  0.0      0     0 ?        S    10:22   0:00 [migration/5]
system_u:system_r:kernel_t:s0   root          41  0.0  0.0      0     0 ?        S    10:22   0:00 [ksoftirqd/5]
```

```
system_u:system_r:kernel_t:s0   root          43  0.0  0.0      0     0 ?        I<   10:22   0:00 [kworker/5:0H-
events_highpri]
system_u:system_r:kernel_t:s0   root          44  0.0  0.0      0     0 ?        S    10:22   0:00 [cpuhp/6]
system_u:system_r:kernel_t:s0   root          45  0.0  0.0      0     0 ?        S    10:22   0:00 [migration/6]
system_u:system_r:kernel_t:s0   root          46  0.0  0.0      0     0 ?        S    10:22   0:00 [ksoftirqd/6]
system_u:system_r:kernel_t:s0   root          48  0.0  0.0      0     0 ?        I<   10:22   0:00 [kworker/6:0H-
events_highpri]
system_u:system_r:kernel_t:s0   root          49  0.0  0.0      0     0 ?        S    10:22   0:00 [cpuhp/7]
system_u:system_r:kernel_t:s0   root          50  0.0  0.0      0     0 ?        S    10:22   0:00 [migration/7]
system_u:system_r:kernel_t:s0   root          51  0.0  0.0      0     0 ?        S    10:22   0:00 [ksoftirqd/7]
system_u:system_r:kernel_t:s0   root          53  0.0  0.0      0     0 ?        I<   10:22   0:00 [kworker/7:0H-
events_highpri]
system_u:system_r:kernel_t:s0   root          62  0.0  0.0      0     0 ?        S    10:22   0:00 [kdevtmpfs]
system_u:system_r:kernel_t:s0   root          63  0.0  0.0      0     0 ?        I<   10:22   0:00 [inet_frag_wq]
system_u:system_r:kernel_t:s0   root          64  0.0  0.0      0     0 ?        S    10:22   0:00 [kauditd]
system_u:system_r:kernel_t:s0   root          65  0.0  0.0      0     0 ?        I    10:22   0:06 [kworker/1:1-
events]
system_u:system_r:kernel_t:s0   root          66  0.0  0.0      0     0 ?        S    10:22   0:00 [khungtaskd]
system_u:system_r:kernel_t:s0   root          67  0.0  0.0      0     0 ?        S    10:22   0:00 [oom_reaper]
system_u:system_r:kernel_t:s0   root          68  0.0  0.0      0     0 ?        I<   10:22   0:00 [writeback]
system_u:system_r:kernel_t:s0   root          69  0.0  0.0      0     0 ?        S    10:22   0:00 [kcompactd0]
system_u:system_r:kernel_t:s0   root          70  0.0  0.0      0     0 ?        SN   10:22   0:00 [ksmd]
system_u:system_r:kernel_t:s0   root          71  0.0  0.0      0     0 ?        SN   10:22   0:00 [khugepaged]
--More--
```

7.3 - Visualiser la SC d'un Utilisateur

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

```
trainee@debian12:~$ 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@debian12:~$ id root
uid=0(root) gid=0(root) groups=0(root)

trainee@debian12:~$ id -Z root
id: cannot print security context when user specified
```

7.4 - Vérifier la SC d'un fichier

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

```
trainee@debian12:~$ cd /etc

trainee@debian12:/etc$ ls -lZ l* -d
drwxr-xr-x. 2 root root system_u:object_r:etc_t:s0           4096 Nov 24 16:47 ldap
-rw-r--r--. 1 root root system_u:object_r:ld_so_cache_t:s0  71363 Nov 30 10:11 ld.so.cache
-rw-r--r--. 1 root root system_u:object_r:etc_t:s0             34 Jul 29  2019 ld.so.conf
drwxr-xr-x. 2 root root system_u:object_r:etc_t:s0           4096 Nov 24 17:22 ld.so.conf.d
-rw-r--r--. 1 root root system_u:object_r:etc_t:s0             26 Dec 20  2020 libao.conf
-rw-r--r--. 1 root root system_u:object_r:etc_t:s0            191 Jan  6  2021 libaudit.conf
drwxr-xr-x. 3 root root system_u:object_r:etc_t:s0           4096 Apr 25  2022 libblockdev
drwxr-xr-x. 2 root root system_u:object_r:etc_t:s0           4096 Nov 24 17:22 libnl-3
drwxr-xr-x. 2 root root system_u:object_r:etc_t:s0           4096 Aug 18  2019 libpaper.d
drwxr-xr-x. 3 root root system_u:object_r:etc_t:s0           4096 Nov 24 17:26 libreoffice
drwxr-xr-x. 2 root root system_u:object_r:etc_t:s0           4096 Nov 24 17:27 lightdm
drwxr-xr-x. 4 root root system_u:object_r:httpd_config_t:s0  4096 Apr 25  2022 lighttpd
-rw-r--r--. 1 root root system_u:object_r:locale_t:s0        2996 Aug 25 21:11 locale.alias
-rw-r--r--. 1 root root system_u:object_r:etc_t:s0           9449 Nov 24 17:22 locale.gen
lrwxrwxrwx. 1 root root system_u:object_r:etc_t:s0             32 Nov 24 15:49 localtime ->
/usr/share/zoneinfo/Europe/Paris
drwxr-xr-x. 4 root root system_u:object_r:etc_t:s0           4096 Nov 27 14:27 logcheck
-rw-r--r--. 1 root root system_u:object_r:etc_t:s0          12569 Apr  7  2025 login.defs
-rw-r--r--. 1 root root system_u:object_r:etc_t:s0            494 Feb 28  2021 logrotate.conf
```

```
drwxr-xr-x. 2 root root system_u:object_r:etc_t:s0          4096 Nov 27 14:54 logrotate.d
drwxr-xr-x. 3 root root system_u:object_r:etc_t:s0          4096 Nov 30 07:51 lynis
drwxr-xr-x. 2 root root system_u:object_r:etc_t:s0          4096 Nov 24 17:22 lynx
```

7.5 - 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.

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@debian12:/etc$ cd ~

trainee@debian12:~$ systemctl status apache2
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apache2.service; enabled; preset: enabled)
     Active: active (running) since Sun 2025-11-30 10:23:14 CET; 4h 54min ago
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 982 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 1109 (apache2)
      Tasks: 55 (limit: 19123)
     Memory: 23.7M
        CPU: 1.074s
     CGroup: /system.slice/apache2.service
             ├─1109 /usr/sbin/apache2 -k start
             ├─1111 /usr/sbin/apache2 -k start
```

```
             └─1112 /usr/sbin/apache2 -k start

Warning: some journal files were not opened due to insufficient permissions.

trainee@debian12:~$ su -
Password: fenestros

root@debian12:~# mkdir /www

root@debian12:~# vi /www/index.html

root@debian12:~# cat /www/index.html
<html>
<title>
This is a test
</title>
<body>
www test page
</body>
</html>
```

Modifiez ensuite la directive **DocumentRoot** dans le fichier **/etc/apache2/sites-enabled/000-default.conf** :

```
root@debian12:~# vi /etc/apache2/sites-enabled/000-default.conf

root@debian12:~# cat /etc/apache2/sites-enabled/000-default.conf
<VirtualHost *:80>
        # The ServerName directive sets the request scheme, hostname and port that
        # the server uses to identify itself. This is used when creating
        # redirection URLs. In the context of virtual hosts, the ServerName
        # specifies what hostname must appear in the request's Host: header to
        # match this virtual host. For the default virtual host (this file) this
        # value is not decisive as it is used as a last resort host regardless.
        # However, you must set it for any further virtual host explicitly.
```

```
        #ServerName www.example.com

        ServerAdmin webmaster@localhost
        #DocumentRoot /var/www/html
        DocumentRoot /www

        # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
        # error, crit, alert, emerg.
        # It is also possible to configure the loglevel for particular
        # modules, e.g.
        #LogLevel info ssl:warn

        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined

        # For most configuration files from conf-available/, which are
        # enabled or disabled at a global level, it is possible to
        # include a line for only one particular virtual host. For example the
        # following line enables the CGI configuration for this host only
        # after it has been globally disabled with "a2disconf".
        #Include conf-available/serve-cgi-bin.conf
</VirtualHost>
```

Ajoutez la section **<Directory “/www”>** au fichier **/etc/apache2/apache2.conf/** :

```
...
# Sets the default security model of the Apache2 HTTPD server. It does
# not allow access to the root filesystem outside of /usr/share and /var/www.
# The former is used by web applications packaged in Debian,
# the latter may be used for local directories served by the web server. If
# your system is serving content from a sub-directory in /srv you must allow
# access here, or in any related virtual host.
<Directory />
        Options FollowSymLinks
```

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

<Directory /usr/share>
        AllowOverride None
        Require all granted
</Directory>

<Directory /var/www/>
        Options Indexes FollowSymLinks
        AllowOverride None
        Require all granted
</Directory>

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

#<Directory /srv/>
#       Options Indexes FollowSymLinks
#       AllowOverride None
#       Require all granted
#</Directory>
...
```

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

```
root@debian12:~# chown -R www-data:www-data /www
```

Redémarrez maintenant le service apache2 :

```
root@debian12:~# systemctl restart apache2

root@debian12:~# systemctl status apache2
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apache2.service; enabled; preset: enabled)
     Active: active (running) since Sun 2025-11-30 15:28:15 CET; 11s ago
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 2234 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 2239 (apache2)
      Tasks: 55 (limit: 19123)
     Memory: 21.0M
        CPU: 45ms
     CGroup: /system.slice/apache2.service
             ├─2239 /usr/sbin/apache2 -k start
             ├─2241 /usr/sbin/apache2 -k start
             └─2242 /usr/sbin/apache2 -k start

Nov 30 15:28:15 debian12 systemd[1]: Starting apache2.service - The Apache HTTP Server...
Nov 30 15:28:15 debian12 apachectl[2234]: /usr/sbin/apachectl: 99: ulimit: error setting limit (Permission
denied)
Nov 30 15:28:15 debian12 apachectl[2234]: Setting ulimit failed. See README.Debian for more information.
Nov 30 15:28:15 debian12 apachectl[2238]: AH00557: apache2: apr_sockaddr_info_get() failed for debian12
Nov 30 15:28:15 debian12 apachectl[2238]: AH00558: apache2: Could not reliably determine the server's fully
qualified domain name, using 127.0.0.1. Set the 'ServerName' directive globally to suppress this mess>
Nov 30 15:28:15 debian12 systemd[1]: Started apache2.service - The Apache HTTP Server.
```

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

```
root@debian12:~# lynx localhost
```

Pour consulter les messages d'alerte de SELinux, vous disposez de la commande **audit2why** :

```
root@debian12:~# ausearch -m avc -ts recent | audit2why | grep apache2
type=AVC msg=audit(1764512954.745:600): avc:  denied  { map } for  pid=2241 comm="apache2" path="/www/index.html"
```

```
dev="sda1" ino=1700626 scontext=system_u:system_r:httpd_t:s0 tcontext=unconfined_u:object_r:etc_runtime_t:s0
tclass=file permissive=0
```

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@debian12:~# ls -Z /www/index.html
unconfined_u:object_r:etc_runtime_t:s0 /www/index.html

root@debian12:~# ls -Z /var/www/html
system_u:object_r:httpd_sys_content_t:s0 index.html
```

L'exemple ci-dessus nous montre clairement que le type pour **/www/index.html** est **etc_runtime_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@debian12:~# chcon -Rv --type=httpd_sys_content_t /www
changing security context of '/www/index.html'
changing security context of '/www'

root@debian12:~# ls -Z /www/index.html
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@debian12:~# semanage fcontext -a -t httpd_sys_content_t "/www(/.*)?"
libsemanage.add_user: user sddm not in password file
```

Options de la Commande

```
root@debian12:~# chcon --help
Usage: chcon [OPTION]... CONTEXT FILE...
  or:  chcon [OPTION]... [-u USER] [-r ROLE] [-l RANGE] [-t TYPE] FILE...
  or:  chcon [OPTION]... --reference=RFILE FILE...
Change the SELinux security context of each FILE to CONTEXT.
With --reference, change the security context of each FILE to that of RFILE.

Mandatory arguments to long options are mandatory for short options too.
      --dereference      affect the referent of each symbolic link (this is
                         the default), rather than the symbolic link itself
  -h, --no-dereference   affect symbolic links instead of any referenced file
  -u, --user=USER        set user USER in the target security context
  -r, --role=ROLE        set role ROLE in the target security context
  -t, --type=TYPE        set type TYPE in the target security context
  -l, --range=RANGE      set range RANGE in the target security context
      --no-preserve-root  do not treat '/' specially (the default)
      --preserve-root    fail to operate recursively on '/'
      --reference=RFILE  use RFILE's security context rather than specifying
                         a CONTEXT value
  -R, --recursive        operate on files and directories recursively
  -v, --verbose          output a diagnostic for every file processed

The following options modify how a hierarchy is traversed when the -R
option is also specified.  If more than one is specified, only the final
one takes effect.

  -H                     if a command line argument is a symbolic link
                         to a directory, traverse it
  -L                     traverse every symbolic link to a directory
                         encountered
  -P                     do not traverse any symbolic links (default)

      --help        display this help and exit
      --version     output version information and exit
```

```
GNU coreutils online help: <https://www.gnu.org/software/coreutils/>
Full documentation <https://www.gnu.org/software/coreutils/chcon>
or available locally via: info '(coreutils) chcon invocation'
```

La commande restorecon

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

```
root@debian12:~# cd /tmp ; touch copy.html move.html

root@debian12:/tmp# ls -lZ | grep html
-rw-r--r--. 1 root    root unconfined_u:object_r:user_tmp_t:s0     0 Nov 30 15:46 copy.html
-rw-r--r--. 1 root    root unconfined_u:object_r:user_tmp_t:s0     0 Nov 30 15:46 move.html
```

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

```
root@debian12:/tmp# cp copy.html /var/www/html/

root@debian12:/tmp# mv move.html /var/www/html/

root@debian12:/tmp# ls -lZ /var/www/html
total 12
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0     0 Nov 30 15:48 copy.html
-rw-r--r--. 1 root root system_u:object_r:httpd_sys_content_t:s0     10701 Nov 27 14:54 index.html
-rw-r--r--. 1 root root unconfined_u:object_r:user_tmp_t:s0             0 Nov 30 15:46 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@debian12:/tmp# restorecon -v /var/www/html/move.html
Relabeled /var/www/html/move.html from unconfined_u:object_r:user_tmp_t:s0 to
unconfined_u:object_r:httpd_sys_content_t:s0

root@debian12:/tmp# ls -lZ /var/www/html
total 12
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0     0 Nov 30 15:48 copy.html
-rw-r--r--. 1 root root system_u:object_r:httpd_sys_content_t:s0     10701 Nov 27 14:54 index.html
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0     0 Nov 30 15:46 move.html
```

Options de la Commande

```
root@debian12:/tmp# restorecon --help
restorecon: invalid option -- '-'
usage:  restorecon [-iIDFmnprRv0xT] [-e excludedir] pathname...
usage:  restorecon [-iIDFmnprRv0xT] [-e excludedir] -f filename
```

7.7 - La commande semanage

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@debian12:/tmp# semanage port -l | grep http
http_cache_port_t              tcp      3128, 8080, 8118, 10001-10010
http_cache_port_t              udp      3130
http_port_t                    tcp      80, 443, 488, 8008, 8009, 8443, 8448
pegasus_http_port_t            tcp      5988
pegasus_https_port_t           tcp      5989
```

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

```
http_port_t                    tcp      80, 443, 488, 8008, 8009, 8443, 8448
```

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@debian12:/tmp# 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@debian12:/tmp# semanage port -a -t http_port_t -p tcp 8090
libsemanage.add_user: user sddm not in password file

root@debian12:/tmp# semanage port -l | grep http
http_cache_port_t              tcp      3128, 8080, 8118, 10001-10010
http_cache_port_t              udp      3130
http_port_t                    tcp      8090, 80, 443, 488, 8008, 8009, 8443, 8448
pegasus_http_port_t            tcp      5988
pegasus_https_port_t           tcp      5989
```

Options de la Commande

```
root@debian12:/tmp# semanage --help
usage: semanage [-h]
{import,export,login,user,port,ibpkey,ibendport,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,ibpkey,ibendport,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
    ibpkey              Manage infiniband ibpkey type definitions
    ibendport           Manage infiniband end 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

options:
  -h, --help            show this help message and exit
```

7.8 - La commande audit2allow

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@debian12:/tmp# mkdir /www1

root@debian12:/tmp# vi /www1/index.html

root@debian12:/tmp# cat /www1/index.html
<html>
```

```
<title>
This is a test
</title>
<body>
www test page
</body>
</html>
```

Modifiez ensuite la directive **DocumentRoot** dans le fichier **/etc/apache2/sites-enabled/000-default.conf** :

```
root@debian12:~# vi /etc/apache2/sites-enabled/000-default.conf

root@debian12:~# cat /etc/apache2/sites-enabled/000-default.conf
<VirtualHost *:80>
        # The ServerName directive sets the request scheme, hostname and port that
        # the server uses to identify itself. This is used when creating
        # redirection URLs. In the context of virtual hosts, the ServerName
        # specifies what hostname must appear in the request's Host: header to
        # match this virtual host. For the default virtual host (this file) this
        # value is not decisive as it is used as a last resort host regardless.
        # However, you must set it for any further virtual host explicitly.
        #ServerName www.example.com

        ServerAdmin webmaster@localhost
        #DocumentRoot /var/www/html
        DocumentRoot /www

        # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
        # error, crit, alert, emerg.
        # It is also possible to configure the loglevel for particular
        # modules, e.g.
        #LogLevel info ssl:warn

        ErrorLog ${APACHE_LOG_DIR}/error.log
```

```
        CustomLog ${APACHE_LOG_DIR}/access.log combined

        # For most configuration files from conf-available/, which are
        # enabled or disabled at a global level, it is possible to
        # include a line for only one particular virtual host. For example the
        # following line enables the CGI configuration for this host only
        # after it has been globally disabled with "a2disconf".
        #Include conf-available/serve-cgi-bin.conf
</VirtualHost>
```

Modifiez la section **<Directory “/www”>** au fichier **/etc/apache2/apache2.conf/** :

```
...
# Sets the default security model of the Apache2 HTTPD server. It does
# not allow access to the root filesystem outside of /usr/share and /var/www.
# The former is used by web applications packaged in Debian,
# the latter may be used for local directories served by the web server. If
# your system is serving content from a sub-directory in /srv you must allow
# access here, or in any related virtual host.
<Directory />
        Options FollowSymLinks
        AllowOverride None
        Require all denied
</Directory>

<Directory /usr/share>
        AllowOverride None
        Require all granted
</Directory>

<Directory /var/www/>
        Options Indexes FollowSymLinks
        AllowOverride None
        Require all granted
```

```
</Directory>

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

#<Directory /srv/>
#       Options Indexes FollowSymLinks
#       AllowOverride None
#       Require all granted
#</Directory>
...
```

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

```
root@debian12:~# chown -R www-data:www-data /www
```

Redémarrez maintenant le service apache2 :

```
root@debian12:/tmp# systemctl restart apache2

root@debian12:/tmp# systemctl status apache2
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apache2.service; enabled; preset: enabled)
     Active: active (running) since Sun 2025-11-30 16:04:11 CET; 14s ago
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 2421 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 2425 (apache2)
      Tasks: 55 (limit: 19123)
     Memory: 21.2M
        CPU: 47ms
     CGroup: /system.slice/apache2.service
```

```
             ├─2425 /usr/sbin/apache2 -k start
             ├─2426 /usr/sbin/apache2 -k start
             └─2427 /usr/sbin/apache2 -k start

Nov 30 16:04:11 debian12 systemd[1]: Starting apache2.service - The Apache HTTP Server...
Nov 30 16:04:11 debian12 apachectl[2421]: /usr/sbin/apachectl: 99: ulimit: error setting limit (Permission
denied)
Nov 30 16:04:11 debian12 apachectl[2421]: Setting ulimit failed. See README.Debian for more information.
Nov 30 16:04:11 debian12 apachectl[2424]: AH00557: apache2: apr_sockaddr_info_get() failed for debian12
Nov 30 16:04:11 debian12 apachectl[2424]: AH00558: apache2: Could not reliably determine the server's fully
qualified domain name, using 127.0.0.1. Set the 'ServerName' directive globally to suppress this mess>
Nov 30 16:04:11 debian12 systemd[1]: Started apache2.service - The Apache HTTP Server.
root@debian12:/tmp#
```

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

```
root@debian12:/tmp# lynx --dump localhost
   www test page
```

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

```
root@debian12:/tmp# cat /var/log/audit/audit.log | grep AVC | grep apache2
type=AVC msg=audit(1764494594.988:204): avc:  denied  { watch } for  pid=984 comm="fail2ban-server"
path="/var/log/apache2" dev="sda1" ino=1572133 scontext=system_u:system_r:fail2ban_t:s0
tcontext=system_u:object_r:httpd_log_t:s0 tclass=dir permissive=1
type=AVC msg=audit(1764494594.988:205): avc:  denied  { watch } for  pid=984 comm="fail2ban-server"
path="/var/log/apache2/error.log" dev="sda1" ino=1574561 scontext=system_u:system_r:fail2ban_t:s0
tcontext=system_u:object_r:httpd_log_t:s0 tclass=file permissive=1
type=AVC msg=audit(1764512954.745:600): avc:  denied  { map } for  pid=2241 comm="apache2" path="/www/index.html"
dev="sda1" ino=1700626 scontext=system_u:system_r:httpd_t:s0 tcontext=unconfined_u:object_r:etc_runtime_t:s0
tclass=file permissive=0
type=AVC msg=audit(1764515158.228:660): avc:  denied  { map } for  pid=2427 comm="apache2"
path="/www1/index.html" dev="sda1" ino=1700628 scontext=system_u:system_r:httpd_t:s0
tcontext=unconfined_u:object_r:etc_runtime_t:s0 tclass=file permissive=0
```

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@debian12:/tmp# grep httpd_t /var/log/audit/audit.log | audit2allow -m httpdlocal > httpdlocal.te

root@debian12:/tmp# cat httpdlocal.te

module httpdlocal 1.0;

require {
        type selinux_config_t;
        type etc_runtime_t;
        type httpd_t;
        class dir search;
        class process setrlimit;
        class file map;
}

#============= httpd_t ==============
allow httpd_t etc_runtime_t:file map;

#!!!! This avc can be allowed using the boolean 'httpd_setrlimit'
allow httpd_t self:process setrlimit;

#!!!! This avc can be allowed using the boolean 'allow_kerberos'
allow httpd_t selinux_config_t:dir search;
```

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

```
root@debian12:/tmp# 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@debian12:/tmp# semodule -i httpdlocal.pp
libsemanage.add_user: user sddm not in password file
```

Vérifiez que le module est chargé :

```
root@debian12:/tmp# semodule -l | grep httpd
httpdlocal
```

Redémarrez le service apache2 :

```
root@debian12:/tmp# systemctl restart apache2

root@debian12:/tmp# systemctl status apache2
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apache2.service; enabled; preset: enabled)
     Active: active (running) since Sun 2025-11-30 16:12:47 CET; 9s ago
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 2538 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 2542 (apache2)
      Tasks: 55 (limit: 19123)
     Memory: 17.1M
        CPU: 43ms
     CGroup: /system.slice/apache2.service
             ├─2542 /usr/sbin/apache2 -k start
             ├─2543 /usr/sbin/apache2 -k start
             └─2544 /usr/sbin/apache2 -k start

Nov 30 16:12:47 debian12 systemd[1]: Starting apache2.service - The Apache HTTP Server...
Nov 30 16:12:47 debian12 apachectl[2541]: AH00557: apache2: apr_sockaddr_info_get() failed for debian12
Nov 30 16:12:47 debian12 apachectl[2541]: AH00558: apache2: Could not reliably determine the server's fully
```

```
qualified domain name, using 127.0.0.1. Set the 'ServerName' directive globally to suppress this mess>
Nov 30 16:12:47 debian12 systemd[1]: Started apache2.service - The Apache HTTP Server.
```

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

```
root@debian12:/tmp# ls -l /var/log/audit/audit.log
-rw-r-----. 1 root adm 0 Nov 30 16:15 /var/log/audit/audit.log
```

Consultez le site localhost :

```
root@debian12:/tmp# lynx --dump localhost
   www test page
```

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

```
root@debian12:/tmp# cat /var/log/audit/audit.log
root@debian12:/tmp#
```

Options de la Commande

```
root@debian12:/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
  -x, --xperms          generate extended permission rules
  --debug               leave generated modules for -M
  -w, --why             Translates SELinux audit messages into a description
                        of why the access was denied
```
