Seguridad y mantenimiento de sistemas Linux

1. Configuración de Actualizaciones Automáticas

Objetivo: Configurar el sistema para que aplique automáticamente actualizaciones de seguridad.

Herramienta utilizada: dnf-automatic

Es un módulo de DNF que permite descargar y aplicar actualizaciones de forma automática según un cron o timer de systemd. Soporta aplicar solo parches de seguridad, actualizaciones completas o solo descargar sin aplicar

Procedimiento:

Instalación de la herramienta:

```
maca@localhost:~
[maca@localhost ~]$ sudo dnf install dnf-automatic -y
[sudo] password for maca:
Rocky Linux 9 - BaseOS                                          3.6 kB/s | 4.1 kB     00:01
Rocky Linux 9 - BaseOS                                          1.6 MB/s | 2.5 MB     00:01
Rocky Linux 9 - AppStream                                       7.5 kB/s | 4.5 kB     00:00
Rocky Linux 9 - AppStream                                       1.8 MB/s | 9.5 MB     00:05
Rocky Linux 9 - Extras                                          4.9 kB/s | 2.9 kB     00:00
Dependencias resueltas.
================================================================================================
 Paquete                    Arquitectura        Versión                    Repositorio        Tam.
================================================================================================
Instalando:
 dnf-automatic              noarch              4.14.0-25.el9              baseos             31 k

Resumen de la transacción
================================================================================================
Instalar  1 Paquete

Tamaño total de la descarga: 31 k
Tamaño instalado: 57 k
Descargando paquetes:
dnf-automatic-4.14.0-25.el9.noarch.rpm                          94 kB/s |  31 kB     00:00
------------------------------------------------------------------------------------------------
Total                                                           37 kB/s |  31 kB     00:00
Ejecutando verificación de operación
Verificación de operación exitosa.
Ejecutando prueba de operaciones
Prueba de operación exitosa.
Ejecutando operación
  Preparando          :                                                                     1/1
```

Configuración en /etc/dnf/automatic.conf:

maca@localhost:~

```
  GNU nano 5.6.1                                    /etc/dnf/automatic.conf
[commands]
#  What kind of upgrade to perform:
# default                            = all available upgrades
# security                           = only the security upgrades
upgrade_type = security
random_sleep = 0
download_updates = yes
apply_updates = yes

# Maximum time in seconds to wait until the system is on-line and able to
# connect to remote repositories.
network_online_timeout = 60

# To just receive updates use dnf-automatic-notifyonly.timer

# Whether updates should be downloaded when they are available, by
# dnf-automatic.timer. notifyonly.timer, download.timer and
# install.timer override this setting.
download_updates = yes

# Whether updates should be applied when they are available, by
# dnf-automatic.timer. notifyonly.timer, download.timer and
# install.timer override this setting.
apply_updates = no

# When the system should reboot following upgrades:
```

```
maca@localhost:~

  GNU nano 5.6.1                                  /etc/dnf/automatic.conf
# How to send messages.  Valid options are stdio, email and motd.  If
# emit_via includes stdio, messages will be sent to stdout; this is useful
# to have cron send the messages.  If emit_via includes email, this
# program will send email itself according to the configured options.
# If emit_via includes motd, /etc/motd file will have the messages. if
# emit_via includes command_email, then messages will be send via a shell
# command compatible with sendmail.
# Default is email,stdio.
# If emit_via is None or left blank, no messages will be sent.
emit_via = motd


[email]
# The address to send email messages from.
email_from = root@localhost

# List of addresses to send messages to.
email_to = root

# Name of the host to connect to to send email messages.
email_host = localhost


[command]
# The shell command to execute. This is a Python format string, as used in
# str.format(). The format function will pass a shell-quoted argument called

^G Ayuda      ^O Guardar    ^W Buscar     ^K Cortar     ^T Ejecutar
^X Salir      ^R Leer fich  ^\ Reemplazar ^U Pegar      ^J Justificar
```

- upgrade_type = security → filtra solo parches de seguridad.
- download_updates y apply_updates → descargan e instalan automáticamente.
- emit_via = motd → notifica en el mensaje de login.

Activación del temporizador:

```
maca@localhost:~
[maca@localhost ~]$ sudo nano /etc/dnf/automatic.conf
[maca@localhost ~]$ sudo systemctl enable --now dnf-automatic.timer
Created symlink /etc/systemd/system/timers.target.wants/dnf-automatic.timer → /usr/lib/systemd/system/dnf-automatic.time
r.
[maca@localhost ~]$ systemctl status dnf-automatic.timer
● dnf-automatic.timer - dnf-automatic timer
     Loaded: loaded (/usr/lib/systemd/system/dnf-automatic.timer; enabled; preset: disabled)
     Active: active (waiting) since Mon 2025-08-11 16:30:41 -04; 7s ago
      Until: Mon 2025-08-11 16:30:41 -04; 7s ago
    Trigger: Tue 2025-08-12 06:26:52 -04; 13h left
   Triggers: ● dnf-automatic.service

ago 11 16:30:41 localhost.localdomain systemd[1]: Started dnf-automatic timer.
[maca@localhost ~]$
```

---

2. Verificación y Rollback de Actualizaciones

Objetivo: Simular una actualización con problemas y revertirla.

Procedimiento:

Buscar un paquete a actualizar:

```
maca@localhost:~
[maca@localhost ~]$ dnf list --upgrades nano
Rocky Linux 9 - BaseOS                                          1.3 MB/s | 2.5 MB     00:01
Rocky Linux 9 - AppStream                                       2.7 MB/s | 9.5 MB     00:03
Rocky Linux 9 - Extras                                           21 kB/s |  17 kB     00:00
Última comprobación de caducidad de metadatos hecha hace 0:00:01, el lun 11 ago 2025 16:31:39.
Error: No hay paquetes que se correspondan con la lista
[maca@localhost ~]$
```

Actualizar:

```
maca@localhost:~
[maca@localhost ~]$ sudo dnf upgrade nano -y
Última comprobación de caducidad de metadatos hecha hace 0:05:50, el lun 11 ago 2025 16:26:26.
Dependencias resueltas.
Nada por hacer.
¡Listo!
[maca@localhost ~]$
```

Ver historial:

```
maca@localhost:~
[maca@localhost ~]$ dnf history
ID     | Línea de comandos                                          | Día y hora       | Acción(es)     | Modific
-------------------------------------------------------------------------------------------------------------------
     9 | install dnf-automatic -y                                   | 2025-08-11 16:26 | Install        |    1
     8 | install sysstat -y                                         | 2025-08-06 03:47 | Install        |    4 EE
     7 | install nfs-utils -y                                       | 2025-07-31 20:20 | Install        |    7 EE
     6 | install samba samba-client samba-common -y                 | 2025-07-31 20:01 | Install        |    7
     5 | install mod_ssl -y                                         | 2025-07-29 22:04 | Install        |    1 EE
     4 | install httpd                                              | 2025-07-29 21:45 | Install        |   11
     3 | install bind bind-utils                                    | 2025-07-22 06:36 | Install        |    5
     2 | update                                                     | 2025-07-21 21:49 | I, U           |  115  <
     1 |                                                            | 2025-06-08 11:35 | Install        | 1215 >E
[maca@localhost ~]$
```

Revertir la transacción:

```
maca@localhost:~
 Paquete                    Arquitectura        Versión                     Repositorio          Tam.
==================================================================================================
Eliminando:
 dnf-automatic              noarch              4.14.0-25.el9               @baseos              57 k

Resumen de la transacción
==================================================================================================
Eliminar  1 Paquete

Espacio liberado: 57 k
Ejecutando verificación de operación
Verificación de operación exitosa.
Ejecutando prueba de operaciones
Prueba de operación exitosa.
Ejecutando operación
  Preparando          :                                                                        1/1
  Ejecutando scriptlet: dnf-automatic-4.14.0-25.el9.noarch                                     1/1
Removed "/etc/systemd/system/timers.target.wants/dnf-automatic.timer".

  Eliminando          : dnf-automatic-4.14.0-25.el9.noarch                                     1/1
advertencia:/etc/dnf/automatic.conf saved as /etc/dnf/automatic.conf.rpmsave

  Ejecutando scriptlet: dnf-automatic-4.14.0-25.el9.noarch                                     1/1
  Verificando         : dnf-automatic-4.14.0-25.el9.noarch                                     1/1

Eliminado:
  dnf-automatic-4.14.0-25.el9.noarch

¡Listo!
[maca@localhost ~]$
```

Verificar versión del paquete:

```
maca@localhost:~
[maca@localhost ~]$ nano --version
 GNU nano, versión 5.6.1
 (C) 1999-2011, 2013-2021 Free Software Foundation, Inc.
 (C) 2014-2021 los colaboradores de nano
 Opciones compiladas: --enable-utf8
[maca@localhost ~]$
```

Explicación del funcionamiento:

- undo → deshace exactamente la transacción seleccionada.

- rollback → restaura el sistema al estado de una transacción anterior, eliminando todas las posteriores.

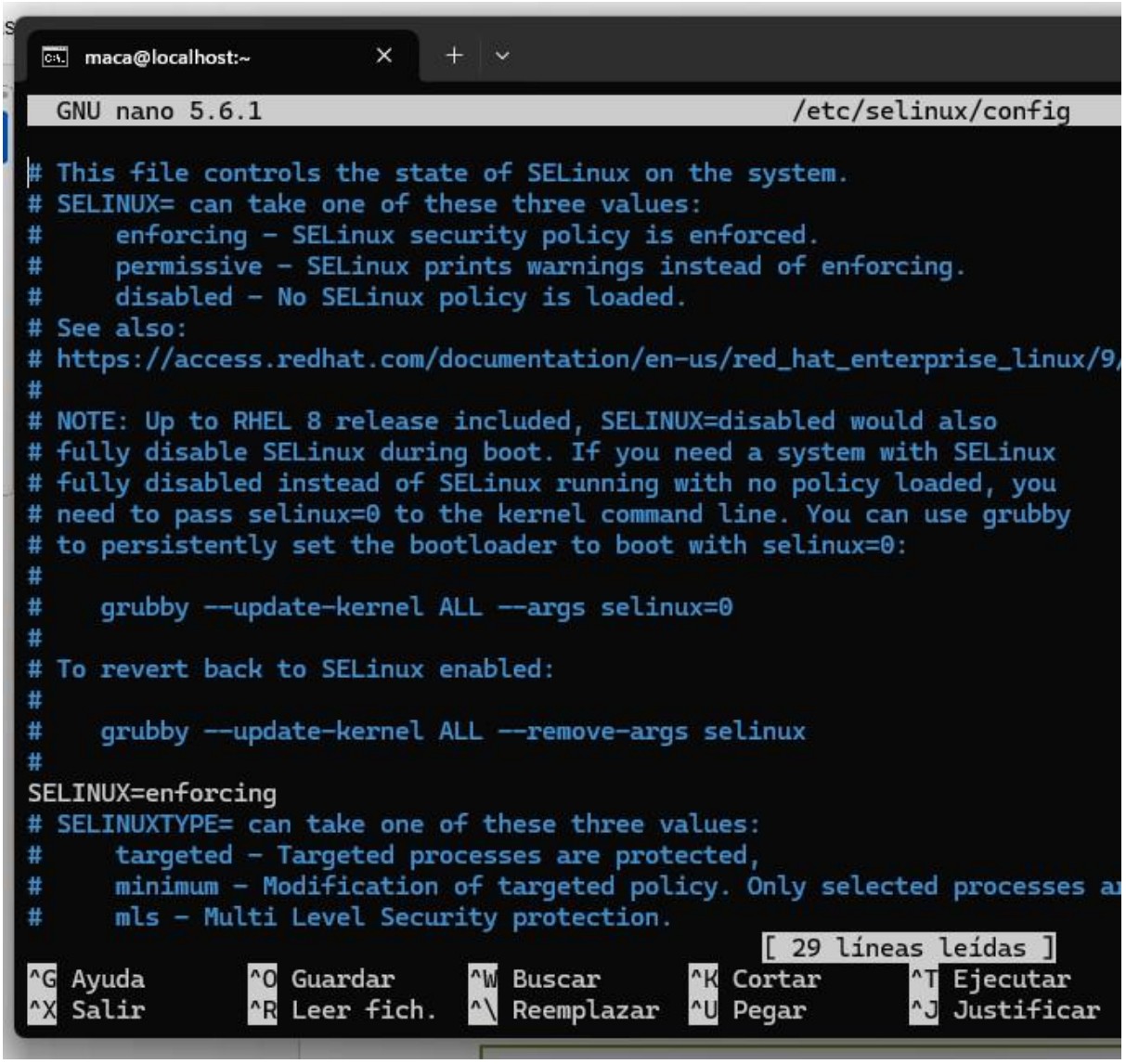
---

3. Configuración y Monitoreo de SELinux

Objetivo: Habilitar SELinux en modo *enforcing*, aplicar política de restricción a un servicio y monitorear accesos denegados.

Procedimiento:

A) Habilitar SELinux:



Aplicar cambios:

```
maca@localhost:~
[maca@localhost ~]$ sudo nano /etc/selinux/config
[maca@localhost ~]$ sudo setenforce 1
[maca@localhost ~]$ getenforce
Enforcing
[maca@localhost ~]$
```

B) Restringir acceso de Apache a /home:

Instalar Apache:

```
maca@localhost:~
[maca@localhost ~]$ sudo dnf install httpd policycoreutils-python-utils -y
Última comprobación de caducidad de metadatos hecha hace 0:09:27, el lun 11 ago 2025 16:26:26.
El paquete httpd-2.4.62-4.el9.x86_64 ya está instalado.
El paquete policycoreutils-python-utils-3.6-2.1.el9.noarch ya está instalado.
Dependencias resueltas.
Nada por hacer.
¡Listo!
[maca@localhost ~]$ sudo systemctl enable --now httpd
[maca@localhost ~]$
```

Crear carpeta de prueba:

```
maca@localhost:~
[maca@localhost ~]$ sudo dnf install httpd policycoreutils-python-utils -y
Última comprobación de caducidad de metadatos hecha hace 0:09:27, el lun 11 ago 2025 16:26:26.
El paquete httpd-2.4.62-4.el9.x86_64 ya está instalado.
El paquete policycoreutils-python-utils-3.6-2.1.el9.noarch ya está instalado.
Dependencias resueltas.
Nada por hacer.
¡Listo!
[maca@localhost ~]$ sudo systemctl enable --now httpd
[maca@localhost ~]$
```

1. Configurar Apache para apuntar a esa carpeta en /etc/httpd/conf/httpd.conf.

```
maca@localhost:~
 GNU nano 5.6.1                                  /etc/httpd/conf/httpd.conf
<Directory />
    AllowOverride none
    Require all denied
</Directory>

#
# Note that from this point forward you must specifically allow
# particular features to be enabled - so if something's not working as
# you might expect, make sure that you have specifically enabled it
# below.
#

#
# DocumentRoot: The directory out of which you will serve your
# documents. By default, all requests are taken from this directory, but
# symbolic links and aliases may be used to point to other locations.
#
/home/usuario/prueba "/var/www/html"

#
# Relax access to content within /var/www.
#
<Directory "/var/www">
    AllowOverride None
    # Allow open access:
    Require all granted

^G Ayuda      ^O Guardar    ^W Buscar     ^K Cortar     ^T Ejecutar   ^C Ubicación   M-U
^X Salir      ^R Leer fich. ^\ Reemplazar ^U Pegar      ^J Justificar ^_ Ir a línea   M-E
```

C) Monitorear intentos denegados:

sudo ausearch -m avc

```
maca@localhost:~
[maca@localhost ~]$ sudo ausearch -m avc
----
time->Sun Jun  8 12:34:23 2025
type=PROCTITLE msg=audit(1749400463.162:26): proctitle=2F7573722F62696E2F6C736D64002D64
type=SYSCALL msg=audit(1749400463.162:26): arch=c000003e syscall=262 success=no exit=-13 a0=ffffff9c a1=5624098a2850 a2=
7fffd11be930 a3=100 items=0 ppid=1 pid=720 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(
none) ses=4294967295 comm="lsmd" exe="/usr/bin/lsmd" subj=system_u:system_r:lsmd_t:s0 key=(null)
type=AVC msg=audit(1749400463.162:26): avc:  denied  { getattr } for  pid=720 comm="lsmd" path="/usr/bin/passt-repair" d
ev="dm-0" ino=101805921 scontext=system_u:system_r:lsmd_t:s0 tcontext=system_u:object_r:passt_repair_exec_t:s0 tclass=fi
le permissive=0
----
time->Mon Jul 21 20:13:24 2025
type=PROCTITLE msg=audit(1753143204.378:31): proctitle=2F7573722F62696E2F6C736D64002D64
type=SYSCALL msg=audit(1753143204.378:31): arch=c000003e syscall=262 success=no exit=-13 a0=ffffff9c a1=558265abd850 a2=
7ffe54d62ca0 a3=100 items=0 ppid=1 pid=714 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(
none) ses=4294967295 comm="lsmd" exe="/usr/bin/lsmd" subj=system_u:system_r:lsmd_t:s0 key=(null)
type=AVC msg=audit(1753143204.378:31): avc:  denied  { getattr } for  pid=714 comm="lsmd" path="/usr/bin/passt-repair" d
ev="dm-0" ino=101805921 scontext=system_u:system_r:lsmd_t:s0 tcontext=system_u:object_r:passt_repair_exec_t:s0 tclass=fi
le permissive=0
----
time->Mon Jul 21 21:11:54 2025
type=PROCTITLE msg=audit(1753146714.610:29): proctitle=2F7573722F62696E2F6C736D64002D64
type=SYSCALL msg=audit(1753146714.610:29): arch=c000003e syscall=262 success=no exit=-13 a0=ffffff9c a1=557c39136850 a2=
7ffc0e1e5390 a3=100 items=0 ppid=1 pid=714 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(
none) ses=4294967295 comm="lsmd" exe="/usr/bin/lsmd" subj=system_u:system_r:lsmd_t:s0 key=(null)
type=AVC msg=audit(1753146714.610:29): avc:  denied  { getattr } for  pid=714 comm="lsmd" path="/usr/bin/passt-repair" d
ev="dm-0" ino=101805921 scontext=system_u:system_r:lsmd_t:s0 tcontext=system_u:object_r:passt_repair_exec_t:s0 tclass=fi
le permissive=0
----
time->Mon Jul 21 21:25:23 2025
```

sudo ausearch -m avc --raw | audit2why

```
maca@localhost:~
[maca@localhost ~]$ sudo ausearch -m avc --raw | audit2why
type=AVC msg=audit(1749400463.162:26): avc:  denied  { getattr } for  pid=720 comm="lsmd" path="/usr/bin/passt-repair" d
ev="dm-0" ino=101805921 scontext=system_u:system_r:lsmd_t:s0 tcontext=system_u:object_r:passt_repair_exec_t:s0 tclass=fi
le permissive=0

        Was caused by:
                Unknown - would be allowed by active policy
                Possible mismatch between this policy and the one under which the audit message was generated.

                Possible mismatch between current in-memory boolean settings vs. permanent ones.

type=AVC msg=audit(1753143204.378:31): avc:  denied  { getattr } for  pid=714 comm="lsmd" path="/usr/bin/passt-repair" d
ev="dm-0" ino=101805921 scontext=system_u:system_r:lsmd_t:s0 tcontext=system_u:object_r:passt_repair_exec_t:s0 tclass=fi
le permissive=0

        Was caused by:
                Unknown - would be allowed by active policy
                Possible mismatch between this policy and the one under which the audit message was generated.

                Possible mismatch between current in-memory boolean settings vs. permanent ones.

type=AVC msg=audit(1753146714.610:29): avc:  denied  { getattr } for  pid=714 comm="lsmd" path="/usr/bin/passt-repair" d
ev="dm-0" ino=101805921 scontext=system_u:system_r:lsmd_t:s0 tcontext=system_u:object_r:passt_repair_exec_t:s0 tclass=fi
le permissive=0

        Was caused by:
                Unknown - would be allowed by active policy
                Possible mismatch between this policy and the one under which the audit message was generated.

                Possible mismatch between current in-memory boolean settings vs. permanent ones.
```

sudo sealert -a /var/log/audit/audit.log

```
maca@localhost:~
[maca@localhost ~]$ sudo sealert -a /var/log/audit/audit.log
100% done
found 5 alerts in /var/log/audit/audit.log
--------------------------------------------------------------------------------

SELinux está negando a /usr/sbin/sshd de name_bind el acceso a tcp_socket puerto 2222.

*****  El complemento bind_ports (92.2 confidence) sugiere*******************

Si quiere permitir que /usr/sbin/sshd se asocie al puerto de red 2222
Entoncesyou need to modify the port type.
Hacer
# semanage port -a -t TIPO_DE_PUERTO -p tcp 2222
    donde TIPO_DE_PUERTO es uno de los siguientes: ssh_port_t, vnc_port_t, xserver_port_t.

*****  El complemento catchall_boolean (7.83 confidence) sugiere**************

Si quiere allow nis to enabled
Entoncesdebe informar a SELinux de ello activando el indicador 'nis_enabled'.

Hacer
setsebool -P nis_enabled 1

*****  El complemento catchall (1.41 confidence) sugiere**********************

Si cree que de manera predeterminada se debería permitir a sshd el acceso name_bind sobre  puerto 2222 tcp_socket.
Entoncesdebería reportar esto como un error.
Puede generar un módulo de política local para permitir este acceso.
Hacer
permita el acceso temporalmente ejecutando:
```