

## Documentation technique

# Durcissement Linux en environnement isolé

Application des recommandations ANSSI BP-028 sur Ubuntu Server

<b>Type de document</b>	Compte rendu technique
<b>Environnement</b>	Ubuntu Server sous Hyper-V
<b>Contrainte principale</b>	Machine isolée du réseau (Air-Gap)
<b>Référentiel</b>	Guide de configuration GNU/Linux ANSSI BP-028

**Synthèse exécutive**

Le durcissement vise à réduire la surface d'attaque locale d'un serveur critique isolé. Les mesures portent sur le démarrage, le noyau, les privilèges, les permissions, les comptes locaux, les services, le maintien en condition de sécurité et la validation par tests de robustesse.

## 1. Contexte et objectif

Ce document présente la démarche de durcissement d'un serveur Ubuntu Server déployé sous Hyper-V, dans un environnement totalement isolé du réseau. L'intervention s'inscrit dans une logique de sécurisation locale renforcée, en appliquant autant que possible les recommandations du guide ANSSI BP-028.

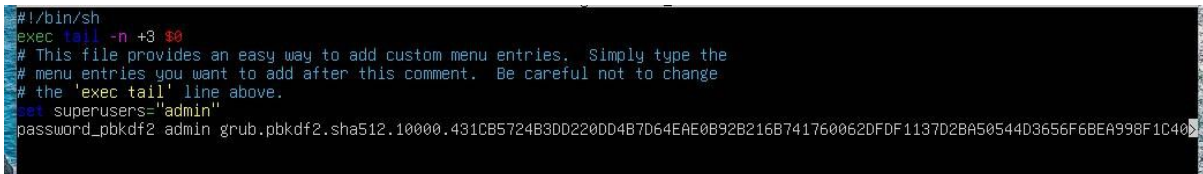
La machine étudiée ne dispose pas d'accès SSH, n'est pas connectée au réseau de l'entreprise et repose sur un compte administrateur local unique. Cette contrainte impose une approche pragmatique : certaines mesures réseau ou centralisées sont inapplicables, tandis que les protections locales sont renforcées en profondeur.

## 2. Sécurisation du démarrage GRUB

Le premier niveau de protection consiste à verrouiller le chargeur de démarrage afin d'empêcher toute modification non autorisée des paramètres du noyau depuis la console de prédémarrage.

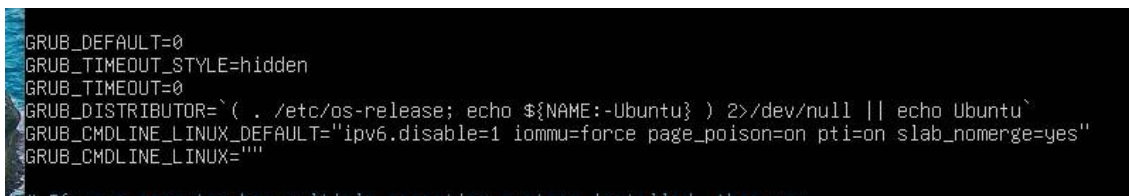
Un mot de passe GRUB chiffré a été généré, puis intégré dans le fichier de configuration personnalisé. Les options du noyau ont également été renforcées pour désactiver IPv6 dès le démarrage et activer plusieurs protections mémoire.

```
grub-mkpasswd-pbkdf2 > /tmp/grub_pass.txt
# Modification de /etc/grub.d/40_custom
# Ajout de ipv6.disable=1 iommu=force page_poison=on pti=on slab_nomerge=yes
update-grub
rm /tmp/grub_pass.txt
```



```
#1/bin/sh
exec tail -n +3 $0
# This file provides an easy way to add custom menu entries. Simply type the
# menu entries you want to add after this comment. Be careful not to change
# the 'exec tail' line above.
set superusers="admin"
password_pbkdf2 admin grub.pbkdf2.sha512.10000.431CB5724B3DD220DD4B7D64EAE0B92B216B741760062DFDF1137D2BA50544D3656F6BEA998F1C40
```

Figure 1 - Déclaration du super-utilisateur GRUB et ajout du condensé PBKDF2.



```
GRUB_DEFAULT=0
GRUB_TIMEOUT_STYLE=hidden
GRUB_TIMEOUT=0
GRUB_DISTRIBUTOR=`(. /etc/os-release; echo ${NAME:-Ubuntu}) 2>/dev/null || echo Ubuntu`
GRUB_CMDLINE_LINUX_DEFAULT="ipv6.disable=1 iommu=force page_poison=on pti=on slab_nomerge=yes"
GRUB_CMDLINE_LINUX=""
```

Figure 2 - Options de démarrage renforcées dans la configuration GRUB.

## 3. Durcissement du noyau avec sysctl

Le fichier `/etc/sysctl.conf` a été utilisé pour appliquer des restrictions persistantes au niveau du noyau Linux. L'objectif est de limiter les capacités d'observation, de réduire les vecteurs d'attaque réseau locaux et d'empêcher le chargement de modules supplémentaires après durcissement.

Les paramètres appliqués couvrent notamment la désactivation IPv6, la restriction de `dmesg`, la protection des pointeurs mémoire, le contrôle de `ptrace`, la protection des liens symboliques et physiques, ainsi que la protection contre les redirections ICMP et le spoofing.

```
kernel.modules_disabled = 1
net.ipv6.conf.all.disable_ipv6 = 1
net.ipv6.conf.default.disable_ipv6 = 1
kernel.dmesg_restrict = 1
kernel.kptr_restrict = 2
kernel.yama.ptrace_scope = 1
fs.protected_symlinks = 1
fs.protected_hardlinks = 1
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.all.rp_filter = 1
sysctl -p
```

```
# Désactivation de l'ipv6 (ANSSI R13)
net.ipv6.conf.all.disable_ipv6 = 1
net.ipv6.conf.default.disable_ipv6 = 1
```

Figure 3 - Désactivation d IPv6 au niveau sysctl.

```
# Refuser les redirections ICMP (R12)
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.default.accept_redirects = 0

# Protection contre le Spoofing (R12)
net.ipv4.conf.all.rp_filter = 1
net.ipv4.conf.default.rp_filter = 1
```

Figure 4 - Protection contre les redirections ICMP et le spoofing.

## 4. Contrôle d'accès et durcissement de sudo

Le principe du moindre privilège a été appliqué en limitant l'usage de sudo à un groupe dédié. Les directives globales ont été renforcées afin de réduire les risques liés aux shells interactifs, aux variables d'environnement et à l'exécution de sous-processus.

```
groupadd sudogrp
usermod -aG sudogrp mbappe
visudo
Defaults noexec, requiretty, use_pty, umask=0027
Defaults ignore_dot, env_reset
```

```
#Directives ANSSI R39
Defaults noexec, requiretty, use_pty, umask=0027
Defaults ignore_dot, env_reset
# This process may not be able to read your environment
```

Figure 5 - Directives sudo renforcées conformément au principe de moindre privilège.

## 5. Synthèse des mesures locales appliquées

Domaine	Mesure appliquée	Recommandation	Effet recherché
Démarrage	Mot de passe GRUB et options noyau	R5, R7, R8, R13	Empêcher la modification du boot et renforcer la mémoire
Noyau	Paramètres sysctl restrictifs	R9 à R14	Réduire la surface d attaque

			système et réseau
Privilèges	Groupe sudo dédié et directives strictes	R38, R39	Limiter les actions administratives
Fichiers	Sticky bit, /boot en 700, umask 0077	R29, R36, R54	Protéger les fichiers sensibles et temporaires
Comptes	Root verrouillé, compte sync neutralisé	R33, R34	Fermer les accès locaux non nécessaires
Services	Désactivation des démons inutiles	R62	Réduire les processus exposés
MCS	Mise à jour manuelle via ISO	R61	Maintenir le système sans connexion réseau

## 6. Système de fichiers et permissions

Les permissions locales ont été renforcées afin d'empêcher la lecture ou la suppression non autorisée de fichiers. Le sticky bit a été vérifié sur /tmp, l'accès à /boot a été restreint et un umask strict a été appliqué pour les nouveaux fichiers.

```
root@vinicius:~# chmod 700 /boot
```

Figure 6 - Restriction des droits sur /boot.

```
root@vinicius:~# source /etc/profile
root@vinicius:~# umask
0077
root@vinicius:~#
```

Figure 7 - Application et vérification du masque umask 0077.

## 7. Verrouillage des comptes locaux

Les comptes capables d'ouvrir une session interactive ont été inventoriés. Le compte root a été verrouillé pour empêcher toute connexion directe, et le compte système sync a été neutralisé en lui retirant son shell interactif.

```
root@vinicius:~# grep -E -v '/bin/false|sbin/nologin' /etc/passwd
root:x:0:0:root:/root:/bin/bash
sync:x:4:65534:sync:/bin:/bin/sync
mbappe:x:1000:1000:mbappe:/home/mbappe:/bin/bash
root@vinicius:~#
```

Figure 8 - Inventaire des comptes disposant d'un shell interactif.

## 8. Gestion des limites liées à l'Air-Gap

L'isolement complet du serveur rend certaines recommandations inapplicables : centralisation SYSLOG, authentification Kerberos ou Active Directory, supervision, EDR, mise à jour automatique et installation classique d'auditd. Ces points ont été documentés comme limitations techniques et compensés par des mesures locales.

## 9. Audit des droits SUID et SGID

Les exécutables disposant de droits spéciaux ont été audités. Les droits nécessaires aux composants vitaux ont été conservés, tandis que les bits SUID de commandes interactives inutiles ont été retirés afin de réduire les possibilités d'escalade locale.

```
find / -type f -perm /6000 -ls 2>/dev/null
chmod u-s /usr/bin/chfn /usr/bin/chsh /usr/bin/newgrp
```

```
find: unknown predicate `-e'
root@vinicius:~# find / -type f -perm /6000 -ls 2>/dev/null
 393515   304 -rwxr-sr-x   1 root   _ssh      309688 août 26  2025 /usr/bin/ssh-agent
 392966    72 -rwsr-xr-x   1 root    root     72792 mai 30  2024 /usr/bin/chfn
 393285    64 -rwsr-xr-x   1 root    root     64152 mai 30  2024 /usr/bin/passwd
 393063    28 -rwxr-sr-x   1 root   shadow   27152 mai 30  2024 /usr/bin/expiry
 393096    76 -rwsr-xr-x   1 root    root     76248 mai 30  2024 /usr/bin/gpasswd
 393080    40 -rwsr-xr-x   1 root    root     39296 avril  8  2024 /usr/bin/fusermount3
 393608    40 -rwsr-xr-x   1 root    root     39296 sept. 16  2025 /usr/bin/umount
 392962    72 -rwxr-sr-x   1 root   shadow   72184 mai 30  2024 /usr/bin/chage
 393236    52 -rwsr-xr-x   1 root    root     51584 sept. 16  2025 /usr/bin/mount
 393526    56 -rwsr-xr-x   1 root    root     55680 sept. 16  2025 /usr/bin/su
 393527   272 -rwsr-xr-x   1 root    root    277936 juin 25  2025 /usr/bin/sudo
 392972    44 -rwsr-xr-x   1 root    root     44760 mai 30  2024 /usr/bin/chsh
 392997    40 -rwxr-sr-x   1 root   crontab  39664 févr. 10 00:34 /usr/bin/crontab
 393249    40 -rwsr-xr-x   1 root    root     40664 mai 30  2024 /usr/bin/newgrp
 410870    32 -rwxr-sr-x   1 root   shadow   31040 sept. 15  2025 /usr/sbin/unix_chkpwd
 410824    28 -rwxr-sr-x   1 root   shadow   26944 sept. 15  2025 /usr/sbin/pam_extrausers_chkpwd
 410120    16 -rwxr-sr-x   1 root    utmp     14488 févr. 10 00:34 /usr/lib/x86_64-linux-gnu/utempter/utempter
 393808    36 -rwsr-xr--   1 root   messagebus 34960 août  9  2024 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
 394039    20 -rwsr-xr-x   1 root    root     18736 déc.  2  2024 /usr/lib/polkit-1/polkit-agent-helper-1
 394018    336 -rwsr-xr-x   1 root    root    342632 août 26  2025 /usr/lib/openssh/ssh-keysign
root@vinicius:~#
```

Figure 9 - Liste des fichiers SUID/SGID recensés sur le système.

```
root@vinicius:~# chmod u-s /usr/bin/chfn /usr/bin/chsh /usr/bin/newgrp
root@vinicius:~#
```

Figure 10 - Retrait du bit SUID sur les commandes non nécessaires.

## 10. Protection cryptographique et confinement

La politique de hachage des mots de passe a été vérifiée dans PAM afin d'utiliser un algorithme robuste tel que yescrypt. Le confinement AppArmor a également été contrôlé en interrogeant directement le noyau, confirmant l'activation du module de contrôle d'accès obligatoire.

```
# here are the per-package modules (the "Primary" block)
password      [success=1 default=ignore]      pam_unix.so obscure yescrypt
# here's the fallback if no module succeeds
```

Figure 11 - Configuration PAM utilisant yescrypt.

```
0 processes are in mixed mode.
root@vinicius:~# cat /sys/module/apparmor/parameters/enabled
Y
root@vinicius:~#
```

État : Exécution |

Figure 12 - Vérification de l'activation d'AppArmor.

## 11. Nettoyage du système et services inutiles

Les services actifs ont été listés avec systemctl. Les démons inutiles dans ce contexte de machine virtuelle isolée ont été désactivés : ModemManager, fwupd, upower, multipathd, unattended-upgrades et systemd-timesyncd.

```
systemctl list-units --type=service --state=running
```

```
systemctl disable --now ModemManager unattended-upgrades systemd-timesyncd fwupd upower multipathd
```

```

root@vinicius:~# find / -type f\( -nouser -o -nogroup \) -ls 2>/dev/null http://googleusercontent.com/immersive_entry_chip/0
root@vinicius:~# find / -type f\( -nouser -o -nogroup \) -ls 2>/dev/null
root@vinicius:~# systemctl list-units --type=service --state=running
UNIT                                LOAD    ACTIVE SUB    DESCRIPTION
cron.service                        loaded active running Regular background program processing daemon
dbus.service                        loaded active running D-BUS System Message Bus
fwupd.service                       loaded active running Firmware update daemon
getty@tty1.service                 loaded active running Getty on tty1
ModemManager.service               loaded active running Modem Manager
multipathd.service                 loaded active running Device-Mapper Multipath Device Controller
polkit.service                     loaded active running Authorization Manager
rsyslog.service                   loaded active running System Logging Service
systemd-journald.service           loaded active running Journal Service
systemd-logind.service             loaded active running User Login Management
systemd-networkd.service           loaded active running Network Configuration
systemd-resolved.service           loaded active running Network Name Resolution
systemd-timesyncd.service          loaded active running Network Time Synchronization
systemd-udev.service               loaded active running Rule-based Manager for Device Events and Files
udisks2.service                   loaded active running Disk Manager
unattended-upgrades.service        loaded active running Unattended Upgrades Shutdown
upower.service                     loaded active running Daemon for power management
user@1000.service                  loaded active running User Manager for UID 1000

Legend: LOAD → Reflects whether the unit definition was properly loaded.
         ACTIVE → The high-level unit activation state, i.e. generalization of SUB.
         SUB → The low-level unit activation state, values depend on unit type.
18 loaded units listed.

```

Figure 13 - Inventaire des services actifs.

```

root@vinicius:~# systemctl disable --now ModemManager unattended-upgrades systemd-timesyncd fwupd upower multipathd
Synchronizing state of unattended-upgrades.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install disable unattended-upgrades
Removed "/etc/systemd/system/dbus-org.freedesktop.ModemManager1.service".
Removed "/etc/systemd/system/sysinit.target.wants/systemd-timesyncd.service".
Removed "/etc/systemd/system/sysinit.target.wants/multipathd.service".
Removed "/etc/systemd/system/sockets.target.wants/multipathd.socket".
Removed "/etc/systemd/system/dbus-org.freedesktop.timesync1.service".
Removed "/etc/systemd/system/multi-user.target.wants/ModemManager.service".
Removed "/etc/systemd/system/multi-user.target.wants/unattended-upgrades.service".
Disabling 'multipathd.service', but its triggering units are still active:
multipathd.socket
Stopping 'multipathd.service', but its triggering units are still active:
multipathd.socket
root@vinicius:~#

```

Figure 14 - Désactivation groupée des services superflus.

## 12. Maintien en Condition de Sécurité en Air-Gap

L'absence d'accès réseau impose une procédure de mise à jour manuelle. Le maintien en condition de sécurité repose sur le téléchargement mensuel d'une image ISO de paquets depuis une machine connectée, son montage dans Hyper-V, puis sa déclaration comme source locale de confiance via apt-cdrom.

```

sudo mount /dev/cdrom /media/cdrom
sudo apt-cdrom -m -d /media/cdrom add
sudo apt update

```

```
visudo: /etc/sudoers.tmp unchanged
root@vinicius:~# mkdir -p /media/cdrom
mkdir: cannot create directory 'p': File exists
root@vinicius:~# mkdir -p /media/cdrom
root@vinicius:~# mount /dev/cdrom /media/cdrom
mount: /media/cdrom: WARNING: source write-protected, mounted read-only.
root@vinicius:~# apt-cdrom -m -d /media/cdrom add
Utilisation du point de montage /mnt/cdrom/ pour le cédérom
Identification ...[0e161da508f6663298a50dc7b08e300b-2]
Examen du disque à la recherche de fichiers d'index...
2 index de paquets trouvés, 0 index de sources, 0 index de traductions et 1 signatures
Ce disque s'appelle :
« Ubuntu-Server 24.04.4 LTS _Noble Numbat_ - Release amd64 (20260210) »
Copie des listes de paquets...gpgv: Signature made mar. 10 févr. 2026 06:52:40 UTC
gpgv: using RSA key 843938DF228D22F7B3742BC0D94AA3F0EFE21092
gpgv: Good signature from "Ubuntu CD Image Automatic Signing Key (2012) <cdimage@ubuntu.com>"
gpgv: asserted signer '843938DF228D22F7B3742BC0D94AA3F0EFE21092' with algo rsa4096
Reading Package Indexes... Fait
Écriture de la nouvelle liste de sources
Les entrées de listes de sources pour ce disque sont :
deb cdrom:[Ubuntu-Server 24.04.4 LTS _Noble Numbat_ - Release amd64 (20260210)]/ noble main restricted
Veuillez répéter cette opération pour tous les disques de votre jeu de cédéroms.
root@vinicius:~#
```

Figure 15 - Ajout du support ISO comme source APT locale.

```
root@vinicius:~# apt update
Ign :1 cdrom://Ubuntu-Server 24.04.4 LTS _Noble Numbat_ - Release amd64 (20260210) noble InRelease
Atteint :2 cdrom://Ubuntu-Server 24.04.4 LTS _Noble Numbat_ - Release amd64 (20260210) noble Release
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Tous les paquets sont à jour.
root@vinicius:~#
```

Figure 16 - Mise à jour depuis le dépôt local monté.

### 13. Validation de l'audit

Les tests de robustesse ont confirmé l'efficacité des protections : absence d'IPv6, rejet des connexions directes au compte root, arrêt des services inutiles et blocage d'opérations administratives par la directive `sudo noexec`.

Ce dernier point illustre la puissance du durcissement : la restriction empêche l'exécution de sous-processus furtifs, mais peut aussi bloquer des opérations de maintenance légitimes si elle n'est pas accompagnée d'une procédure d'administration dédiée.

```
root@vinicius:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:15:5d:3f:48:15 brd ff:ff:ff:ff:ff:ff
    inet 172.25.229.115/20 metric 100 brd 172.25.239.255 scope global dynamic eth0
        valid_lft 75667sec preferred_lft 75667sec
root@vinicius:~#
```

Figure 17 - Validation de la désactivation IPv6 avec `ip a`.

### 14. Incident majeur : verrouillage de l'administrateur

Le durcissement extrême a provoqué un cas d'école : la perte d'accès administratif légitime. Les tentatives de correction via `sudo -i`, `visudo`, modification GRUB, puis Live CD ont été arrêtées par les différentes couches de protection : `noexec`, mot de passe GRUB, Secure Boot et restrictions Hyper-V.

Cet incident démontre qu'un durcissement efficace doit toujours être accompagné d'une stratégie de réversibilité : compte de secours, sauvegarde de configuration, snapshot Hyper-V, procédure de restauration documentée et validation progressive des règles.



```
mbappe@vinicius:~$ sudo -l
Matching Defaults entries for mbappe on vinicius:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/bin\:/snap/bin, use_pty,
  noexec, requiretty, use_pty, umask=0027, ignore_dot, env_reset

User mbappe may run the following commands on vinicius:
  (ALL : ALL) ALL
mbappe@vinicius:~$
```

Figure 18 - Blocage des commandes administratives par la directive sudo noexec.

## 15. Bilan final

Le projet aboutit à un serveur localement très fortement durci, mais met en évidence un équilibre fondamental : confidentialité et intégrité ont été maximisées au détriment de la disponibilité. Dans un environnement Air-Gap critique, ce choix peut être cohérent, mais il doit rester maîtrisé par des mécanismes de récupération prévus avant l'application des règles les plus restrictives.

### Recommandation

Avant toute généralisation, appliquer les mesures par lots, réaliser un snapshot avant chaque phase, conserver un compte de secours documenté et tester les procédures de reprise. Le durcissement doit être sécurisé, mais aussi administrable.