AYI NEDJIMI Consultants

Durcissement VMware ESXi : Guide Complet de Sécurisation

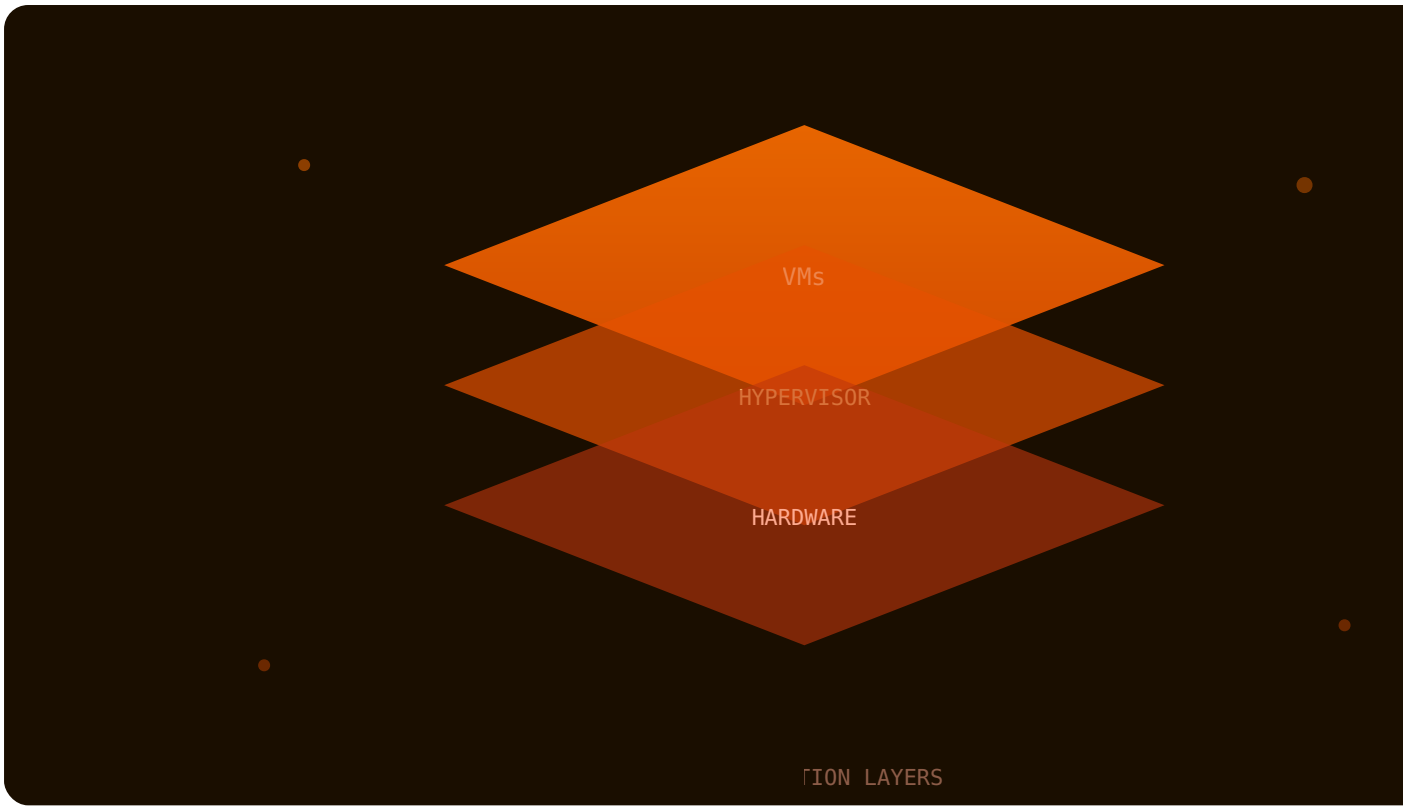
Catégorie : Virtualisation Lecture : 11 min Publié le : 08/03/2026 Auteur : Ayi NEDJIMI

Guide complet de durcissement VMware ESXi : SSH, firewall, lockdown mode, vSphere security baseline, chiffrement VM, patching et protection contre.

Durcissement VMware ESXi : Guide Complet de Sécurisation constitue un enjeu majeur pour les professionnels de la sécurité informatique et les équipes techniques. Guide complet de durcissement VMware ESXi : SSH, firewall, lockdown mode, vSphere security baseline, chiffrement VM, patching et protection contre. Ce guide détaillé sur durcissement vmware esxi securisation propose une méthodologie structurée, des outils éprouvés et des recommandations opérationnelles directement applicables. L'objectif est de fournir aux praticiens — consultants, ingénieurs sécurité, administrateurs systèmes — les connaissances et les techniques nécessaires pour aborder ce sujet avec rigueur. Chaque section s'appuie sur des retours d'expérience terrain et intègre les évolutions les plus récentes du domaine. Les recommandations présentées sont adaptées aux environnements d'entreprise et tiennent compte des contraintes opérationnelles réelles.

Avertissement : Les techniques présentées dans cet article sont destinées exclusivement à des fins éducatives et de tests autorisés. Toute utilisation malveillante est illégale et contraire à l'éthique professionnelle.

Résumé exécutif



VMware ESXi est devenu la cible numéro un des groupes de ransomware. Royal, LockBit 3.0, ALPHV/BlackCat, Play et Akira ont tous développé des variantes spécifiques pour chiffrer les machines virtuelles directement sur l'hyperviseur. Un seul hôte ESXi compromis peut entraîner le chiffrement simultané de dizaines, voire de centaines de VMs en quelques minutes. Face à cette menace, le durcissement d'ESXi n'est plus une option mais une nécessité absolue. Cet article propose un guide exhaustif de sécurisation couvrant la configuration réseau, l'authentification, le chiffrement, le patching, le logging, la conformité aux benchmarks STIG/CIS et les mesures anti-ransomware spécifiques. Chaque recommandation est accompagnée des commandes `esxcli` et configurations nécessaires à sa mise en oeuvre. Ce guide approfondi examine en detail les aspects fondamentaux et avances de Durcissement VMware ESXi, en proposant une analyse structuree et documentee des enjeux actuels.

Points clés de cet article

- Configuration réseau sécurisée : vSwitch, port groups, firewall ESXi, micro-segmentation NSX-T
- Contrôle d'accès : SSH, DCUI, Active Directory, Lockdown Mode normal et strict
- Chiffrement complet : VM Encryption, vTPM, Encrypted vMotion, KMS
- Patching sécurisé via VLCM avec validation des signatures VIB
- Logging et audit : syslog, intégration SIEM, corrélation d'événements
- Protection anti-ransomware : snapshots, sauvegardes immutables, détection
- Checklist de 25 points de durcissement actionnable

Que se passerait-il si un attaquant s'échappait d'une de vos machines virtuelles ?

1. ESXi : cible prioritaire des ransomwares

1.1 Pourquoi ESXi est visé

La stratégie des groupes de ransomware est simple et redoutablement efficace : plutôt que de chiffrer chaque VM individuellement (ce qui nécessite de contourner les EDR dans chaque guest OS), ils ciblent directement l'hyperviseur ESXi. Un accès root à ESXi donne un contrôle total sur tous les fichiers .vmdk (disques virtuels), .vmx (configuration), .vswp (swap) et .nvram (BIOS) de chaque VM hébergée.

Les avantages pour l'attaquant sont multiples :

- **Impact maximal** : un seul point de compromission affecte toutes les VMs de l'hôte.
- **Absence d'EDR** : les agents de sécurité type EDR/XDR ne s'exécutent pas nativement sur ESXi. VMkernel n'est pas un OS généraliste, et les solutions tierces de protection ESXi sont rares.
- **Rapidité de chiffrement** : les fichiers vmdk sont de gros fichiers séquentiels, facilement chiffrables en parallèle. LockBit 3.0 ESXi utilise du multithreading pour chiffrer un datastore de plusieurs To en minutes.
- **Destruction des sauvegardes** : les attaquants recherchent et détruisent systématiquement les snapshots et les datastores de backup accessibles depuis l'hôte.

1.2 Chronologie des attaques majeures

Date	Groupe	CVE exploitée	Impact
Fév 2023	ESXiArgs	CVE-2021-21974 (OpenSLP)	3200+ serveurs, mondiale
2023	Royal	SSH + credentials volées	Santé, finance US/EU
2023-2024	ALPHV/BlackCat	CVE-2024-37085 (AD bypass)	Grandes entreprises
2024	LockBit 3.0	SSH brute force + 0-day	Toutes industries
2024	Play	Exploitation vCenter	ESXi via pivot vCenter
2025	Akira	Vulnérabilités SLP/CIM	PME européennes

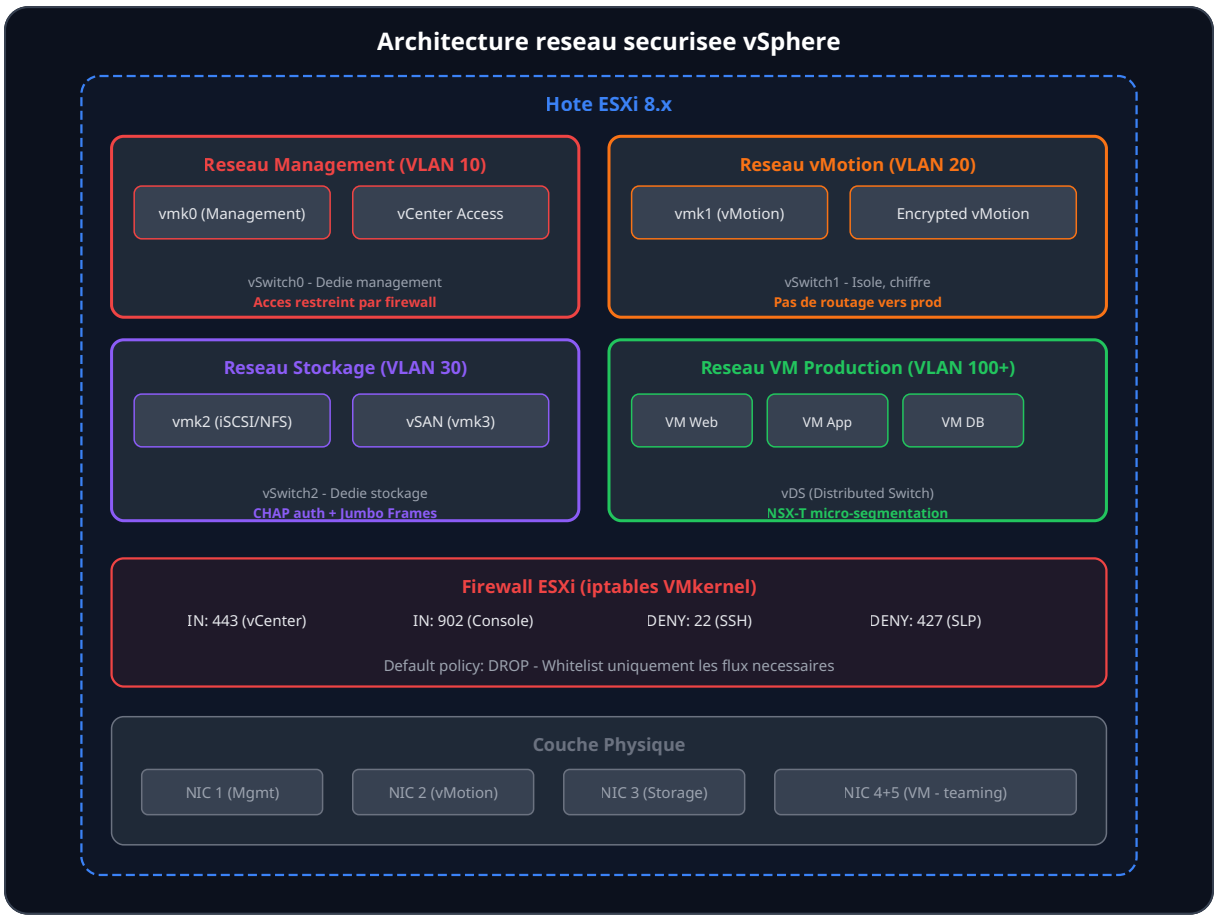
Pour une analyse détaillée de la kill chain ransomware, consultez notre article sur l'anatomie d'une kill chain ransomware.

Notre avis d'expert
Les évasions de conteneurs représentent un risque croissant avec l'adoption massive de Docker et Kubernetes. Nos tests montrent que les configurations par défaut sont rarement suffisantes pour isoler efficacement les workloads. L'approche defense-in-depth est non négociable dans un environnement conteneurisé.

2. Configuration réseau sécurisée

2.1 Architecture vSwitch et port groups

La première ligne de défense est la segmentation réseau au niveau de l'hyperviseur. Une architecture vSphere sécurisée sépare les flux en plusieurs réseaux distincts, chacun avec son propre vSwitch ou port group :




```
# Configuration vSwitch sécurisée via esxcli

# Désactiver le Promiscuous Mode sur tous les port groups
esxcli network vswitch standard policy security set -v vSwitch0 \
  --allow-promiscuous=false --allow-mac-change=false --allow-forged-transmits=false

# Idem pour le vSwitch VM
esxcli network vswitch standard policy security set -v vSwitch1 \
  --allow-promiscuous=false --allow-mac-change=false --allow-forged-transmits=false

# Configurer le port group Management avec VLAN
esxcli network vswitch standard portgroup set -p "Management Network" --vlan-id 10

# Créer un port group isolé pour vMotion
esxcli network vswitch standard portgroup add -v vSwitch1 -p "vMotion-Isolated"
esxcli network vswitch standard portgroup set -p "vMotion-Isolated" --vlan-id 20

# Configurer le traffic shaping pour limiter les flux
esxcli network vswitch standard policy shaping set -v vSwitch0 \
  --enabled=true --avg-bandwidth=1000000 --peak-bandwidth=1500000 --burst-size=819200
```

2.2 Firewall ESXi

ESXi intègre un firewall basé sur iptables au niveau du VMkernel. Par défaut, il est permissif -- tous les services activés sont accessibles depuis n'importe quelle IP. Le durcissement consiste à restreindre chaque service aux seules IP autorisées :

```
# Activer le firewall ESXi
esxcli network firewall set --enabled true

# Politique par défaut : bloquer tout
esxcli network firewall set --default-action DROP

# Lister les rulesets actifs
esxcli network firewall ruleset list

# Désactiver les services non nécessaires
esxcli network firewall ruleset set -e false -r CIMSLP     # SLP (vecteur ESXiArgs)
esxcli network firewall ruleset set -e false -r snmp       # SNMP si non utilisé
esxcli network firewall ruleset set -e false -r CIMHttpServer
esxcli network firewall ruleset set -e false -r CIMHttpsServer

# Restreindre SSH aux seuls postes d'administration
esxcli network firewall ruleset set -r sshServer --allowed-all false
esxcli network firewall ruleset allowedip add -r sshServer -i 10.0.1.10/32
esxcli network firewall ruleset allowedip add -r sshServer -i 10.0.1.11/32

# Restreindre l'accès vSphere Client
esxcli network firewall ruleset set -r webAccess --allowed-all false
esxcli network firewall ruleset allowedip add -r webAccess -i 10.0.1.0/24

# Restreindre vCenter
esxcli network firewall ruleset set -r vSphereClient --allowed-all false
esxcli network firewall ruleset allowedip add -r vSphereClient -i 10.0.1.50/32

# Vérifier la configuration
esxcli network firewall ruleset list | grep -i "true"
esxcli network firewall ruleset allowedip list
```

2.3 Micro-segmentation NSX-T

Pour les environnements disposant de NSX-T (VMware NSX), la micro-segmentation apporte une couche de sécurité supplémentaire. Le Distributed Firewall (DFW) s'exécute au niveau du VMkernel et inspecte le trafic entre VMs, même sur le même hôte. Cela empêche les mouvements latéraux qu'un attaquant pourrait réaliser après une compromission initiale.

Les politiques NSX-T permettent de créer des zones de sécurité dynamiques basées sur des tags, des noms de VM ou des critères réseau. Par exemple, isoler toutes les VMs tagguées "PCI" dans un segment dédié avec des règles strictes d'accès. Pour comprendre les techniques de mouvement latéral que NSX-T peut contrer, consultez notre article sur l'exfiltration furtive.

3. Accès et authentification

3.1 Désactiver SSH

SSH est le vecteur d'attaque le plus exploité contre ESXi. Les groupes de ransomware utilisent des credentials volées, du brute force ou des clés SSH compromises pour obtenir un accès root. La recommandation est catégorique : **SSH doit être désactivé en permanence**, sauf pour les opérations de maintenance planifiées.

```
# Arrêter et désactiver le service SSH
vim-cmd hostsvc/disable_ssh
vim-cmd hostsvc/stop_ssh

# Vérifier le statut
vim-cmd hostsvc/runtimeinfo | grep ssh

# Configurer un timeout automatique si SSH est temporairement activé
esxcli system settings advanced set -o /UserVars/ESXiShellInteractiveTimeOut -i 300
esxcli system settings advanced set -o /UserVars/ESXiShellTimeOut -i 600

# Désactiver aussi le ESXi Shell (DCUI local)
vim-cmd hostsvc/disable_esx_shell
vim-cmd hostsvc/stop_esx_shell

# Configurer le warning DCUI pour SSH activé
esxcli system settings advanced set -o /UserVars/SuppressShellWarning -i 0

# Si SSH doit rester actif temporairement, renforcer la config
# /etc/ssh/sshd_config sur ESXi :
# PermitRootLogin no          # Forcer un compte non-root
# MaxAuthTries 3              # Limiter les tentatives
# Banner /etc/issue           # Bannière légale
# AllowUsers esxadmin         # Restreindre les utilisateurs
```

3.2 Intégration Active Directory

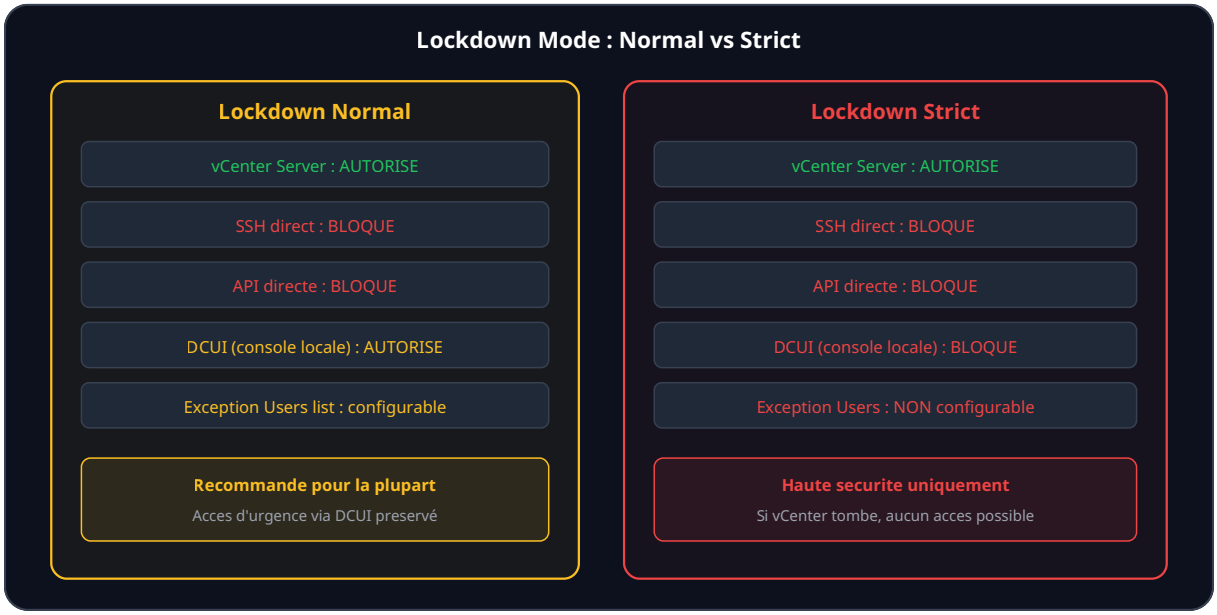
L'intégration AD permet de centraliser l'authentification et d'éliminer les comptes locaux. Cependant, elle introduit un nouveau vecteur d'attaque : la compromission du groupe AD "ESX Admins" (CVE-2024-37085) donne automatiquement un accès administrateur à tous les hôtes ESXi du domaine.

```
# Joindre ESXi au domaine AD
esxcli system account add -d "CORP.LOCAL" -u "esxi-join@corp.local"

# Configurer les groupes AD autorisés (CRITIQUE : ne PAS utiliser "ESX Admins" par défaut)
# Renommer ou supprimer le groupe "ESX Admins" dans AD
# Créer un groupe dédié avec un nom non prédictible
esxcli system permission set -i -r Admin -e "CORP\\ESXi-SecureAdmins"

# Configurer la politique de mot de passe
esxcli system security password set --min-length 14 --min-uppercase 2 \
  --min-lowercase 2 --min-numeric 2 --min-special 1 --max-lifetime 90

# Configurer le verrouillage de compte
esxcli system security lockout set --max-failures 5 --unlock-time 900
```

CVE-2024-37085 : le piège du groupe "ESX Admins"
Par défaut, ESXi accorde un accès administrateur complet à tout membre du groupe AD "ESX Admins". Un attaquant ayant compromis Active Directory peut créer ce groupe (s'il n'existe pas) ou y ajouter un compte compromis, obtenant ainsi un accès root à tous les hôtes ESXi du domaine. **Mesure immédiate** : renommer ce groupe, restreindre sa création via les ACL AD, et auditer régulièrement les membres.

3.3 Lockdown Mode

Le Lockdown Mode est la fonctionnalité de sécurité la plus importante d'ESXi. Il restreint l'accès à l'hôte aux seules connexions via vCenter Server, éliminant les accès directs SSH, API et DCUI.




```
# Activer le Lockdown Mode Normal via esxcli
vim-cmd vimsvc/auth/lockdown_mode_enter

# Vérifier le statut
vim-cmd vimsvc/auth/lockdown_is_enabled

# Configurer les Exception Users (comptes qui peuvent bypass le lockdown)
# Via vCenter : Host > Configure > System > Security Profile > Lockdown Mode
# Ajouter uniquement le compte de service de monitoring

# Configurer le timeout DCUI
esxcli system settings advanced set -o /UserVars/DcuiTimeOut -i 600

# Pour le mode Strict (via vCenter uniquement) :
# Host > Configure > System > Security Profile > Lockdown Mode > Strict
```

Cas concret
En 2024, la vulnérabilité CVE-2024-21626 (Leaky Vessels) dans runc a démontré qu'une évasion de conteneur Docker était possible via une manipulation du répertoire de travail. Cette faille affectait l'ensemble de l'écosystème de conteneurs et a nécessité des patches d'urgence sur toutes les plateformes Kubernetes majeures.

Vos conteneurs sont-ils réellement isolés les uns des autres ?

4. Chiffrement

4.1 VM Encryption

Le VM Encryption de vSphere chiffre les fichiers de la VM (vmdk, vswp, vmx, nvram) avec AES-256-XTS. Le chiffrement est transparent pour le guest OS et ne nécessite aucune modification dans la VM. La gestion des clés utilise un KMS externe compatible KMIP (Key Management Interoperability Protocol).

```
# Prérequis : KMS configuré dans vCenter
# vCenter > Administration > Key Providers > Add Standard Key Provider

# Chiffrer une VM existante (PowerCLI)
$vm = Get-VM -Name "CriticalServer"
$storagePolicy = Get-SpbmStoragePolicy -Name "VM Encryption Policy"
Set-SpbmEntityConfiguration -Entity $vm -StoragePolicy $storagePolicy

# Vérifier le statut de chiffrement
Get-VM "CriticalServer" | Get-HardDisk | Select Name, Filename, StorageFormat

# Chiffrer uniquement les disques (sans les fichiers de configuration)
# Utile pour réduire l'overhead de performance
New-VDisk -VM $vm -StorageFormat EagerZeroedThick -CapacityGB 100 -Encrypted

# Activer le chiffrement vTPM pour une VM
New-VM -Name "SecureVM" -ResourcePool "Production" | `
  New-Tpm -Type TpmV2
```

4.2 Encrypted vMotion

Le vMotion (migration live de VMs entre hôtes) transmet la mémoire vive de la VM en clair par défaut. Pour les VMs chiffrées, vSphere 6.5+ propose l'Encrypted vMotion qui chiffre le flux de migration avec une clé dérivée de la KEK (Key Encryption Key) du KMS. Trois modes sont disponibles :

- **Disabled** : pas de chiffrement vMotion (déconseillé)
- **Opportunistic** : chiffrement si les deux hôtes le supportent (recommandé minimum)
- **Required** : chiffrement obligatoire, vMotion échoue si impossible (haute sécurité)

4.3 vTPM (Virtual Trusted Platform Module)

Le vTPM émule un TPM 2.0 dans chaque VM, permettant d'activer BitLocker, Credential Guard et Measured Boot dans les VMs Windows. Sur Linux, il permet le chiffrement LUKS avec scellement TPM et l'attestation d'intégrité au boot. Le vTPM stocke ses secrets dans le fichier .nvram de la VM, qui est lui-même protégé par le VM Encryption.

5. Stockage sécurisé

5.1 Permissions VMFS

Les datastores VMFS stockent les fichiers des VMs. Les permissions d'accès doivent être strictement contrôlées pour empêcher un attaquant ayant accès à un hôte de modifier les fichiers d'une VM d'un autre cluster :

```
# Vérifier les permissions sur les datastores
ls -la /vmfs/volumes/

# S'assurer que les fichiers VM sont en 700 (propriétaire root uniquement)
find /vmfs/volumes/datastore1/ -name "*.vmdk" -exec ls -la {} \;

# Configurer le verrouillage des fichiers VM
esxcli system settings advanced set -o /VMFS3/UseATSForHBOnVMFS5 -i 1

# Désactiver l'accès anonymous aux datastores NFS
# Dans /etc/vmware/hostd/config.xml, vérifier :
# false
```

5.2 Sécurité iSCSI et NFS

Les protocoles de stockage réseau (iSCSI, NFS) doivent être sécurisés pour éviter l'interception ou la manipulation des données :

- **iSCSI CHAP** : activer l'authentification bidirectionnelle CHAP (Challenge-Handshake Authentication Protocol) pour empêcher les accès non autorisés aux LUNs.
- **NFS v4.1 + Kerberos** : utiliser NFSv4.1 avec authentification Kerberos au lieu de NFSv3 (pas d'authentification). Configurer krb5p pour le chiffrement et l'intégrité.
- **Réseau dédié** : isoler le trafic de stockage sur un VLAN dédié avec des ACL strictes au niveau switch.
- **Jumbo Frames** : configurer MTU 9000 sur le réseau de stockage pour les performances, mais s'assurer que le firewall gère correctement les trames jumbo.

6. Patching et gestion des mises à jour

6.1 vSphere Lifecycle Manager (VLCM)

Le patching ESXi est critique car les vulnérabilités non corrigées sont le premier vecteur d'exploitation (cf. ESXiArgs avec CVE-2021-21974, patchée 2 ans avant l'attaque massive). VLCM (anciennement Update Manager) permet une gestion centralisée des mises à jour :

```
# Vérifier la version et le build actuel
esxcli system version get
esxcli system maintenanceMode get

# Lister les VIB (VMware Installation Bundles) installés
esxcli software vib list

# Vérifier les signatures des VIB (détection de VIB malicieux)
esxcli software vib signature verify

# Installer un patch offline (bundle zip)
esxcli software vib install -d /vmfs/volumes/datastore1/patches/ESXi800-202401001.zip

# Ou via profil d'image (recommandé)
esxcli software profile update -d /vmfs/volumes/datastore1/patches/ESXi800-202401001.zip \
  -p ESXi-8.0U2c-23305546-standard

# Configurer les baselines de sécurité dans vCenter VLCM :
# 1. Menu > Lifecycle Manager > Baselines
# 2. Créer une baseline "Security Critical Patches"
# 3. Attacher aux clusters
# 4. Planifier la remédiation mensuelle avec pre-check
```

6.2 Vérification d'intégrité des VIB

Les VIB sont signés cryptographiquement par VMware. Un VIB non signé ou avec une signature invalide peut indiquer la présence d'un rootkit ou d'un implant de persistance au niveau hyperviseur. Les APT (comme UNC3886 découvert par Mandiant) ont utilisé des VIB malicieux pour maintenir un accès persistant à ESXi. Pour comprendre ces techniques de persistance, consultez notre article sur les UEFI bootkits et la persistance firmware.

```
# Vérifier que le niveau d'acceptation est au minimum "CommunitySupported"
esxcli software acceptance get
# Recommandé : VMwareCertified ou VMwareAccepted

# Définir le niveau d'acceptation strict
esxcli software acceptance set --level=VMwareCertified

# Vérifier toutes les signatures VIB
esxcli software vib signature verify
# Tout VIB avec "Signature Not Available" ou "Signature Invalid" est suspect

# Lister les VIB par acceptance level
esxcli software vib list --rebooting-image | grep -v "VMware"
# Tout VIB non VMware doit être justifié et documenté
```

7. Logging et audit

7.1 Configuration syslog

Les logs ESXi sont la clé pour la détection d'intrusion et l'investigation forensique. Par défaut, les logs sont stockés localement dans `/var/log/` sur une partition de taille limitée. En cas de compromission, l'attaquant peut supprimer ces logs pour effacer ses traces. Le forwarding vers un serveur syslog externe est donc indispensable :

```
# Configurer le forwarding syslog vers un serveur distant
esxcli system syslog config set --loghost="tcp://siem.corp.local:514,udp://backup-
syslog.corp.local:514"

# Configurer le niveau de log (info recommandé, debug pour investigation)
esxcli system syslog config set --default-rotate=20 --default-size=10240

# Activer le logging des commandes shell
esxcli system settings advanced set -o /Config/HostAgent/log/level -s "info"

# Recharger la configuration syslog
esxcli system syslog reload

# Vérifier la configuration
esxcli system syslog config get

# Logs critiques à surveiller :
# /var/log/auth.log       - Authentification (SSH, DCUI)
# /var/log/hostd.log      - Service hostd (API, gestion VM)
# /var/log/vpxa.log       - Communication avec vCenter
# /var/log/vobd.log       - Événements d'observation
# /var/log/shell.log      - Commandes shell exécutées
# /var/log/vmkernel.log   - Messages noyau VMkernel
```

7.2 Intégration SIEM

L'intégration des logs ESXi dans un SIEM permet la corrélation avec les événements des autres couches (réseau, AD, endpoints). Voici les règles de détection prioritaires à configurer :

```
# Règle SIEM : Détection d'activation SSH sur ESXi
# Source : syslog ESXi
ESXiLogs
| where Message contains "SSH login" or Message contains "SSH session opened"
| where TimeGenerated > ago(1h)
| summarize LoginCount=count() by SourceIP, HostName
| where LoginCount > 3
| project TimeGenerated, HostName, SourceIP, LoginCount

# Règle : Détection de modification de VIB (persistance APT)
ESXiLogs
| where Message contains "esxcli software vib install"
  or Message contains "VIB" and Message contains "install"
| project TimeGenerated, HostName, Message

# Règle : Détection d'arrêt massif de VMs (pré-ransomware)
ESXiLogs
| where Message contains "VM_POWER_OFF" or Message contains "vim.VirtualMachine.powerOff"
| summarize VMsPoweredOff=count() by HostName, bin(TimeGenerated, 5m)
| where VMsPoweredOff > 5
| project TimeGenerated, HostName, VMsPoweredOff

# Règle : Détection de chiffrement de fichiers vmdk
ESXiLogs
| where Message contains "openssl" or Message contains "encrypt"
  or Message contains ".locked" or Message contains ".args"
| project TimeGenerated, HostName, Message

# Règle : Détection de désactivation du firewall
ESXiLogs
| where Message contains "firewall" and Message contains "disabled"
| project TimeGenerated, HostName, Message
```

7.3 Log rotation et rétention

La rétention des logs doit être configurée pour satisfaire les exigences de conformité tout en évitant la saturation du stockage local :

```
# Configurer la rotation des logs
esxcli system syslog config set --default-rotate=20 --default-size=10240

# Configurer un datastore persistant pour les logs (scratch partition)
vim-cmd hostsvc/advopt/update ScratchConfig.ConfiguredScratchLocation \
  string "/vmfs/volumes/datastore1/scratch"

# Vérifier l'espace disque des logs
vdf -h
du -sh /var/log/

# S'assurer que les logs ne sont PAS sur le ramdisk (non persistant après reboot)
esxcli system syslog config get | grep logdir
```

8. Conformité : STIG, CIS et vSphere SCG

8.1 vSphere Security Configuration Guide (SCG)

Le SCG est le guide officiel de Broadcom/VMware pour la sécurisation de vSphere. Il couvre les paramètres de sécurité de l'hôte ESXi, de vCenter et des VMs. Depuis vSphere 8, le SCG est disponible sous forme de fichiers JSON/YAML importables dans VLCM pour une remédiation automatisée.

8.2 DISA STIG ESXi

Le STIG (Security Technical Implementation Guide) du DoD est le standard le plus strict pour le durcissement ESXi. Il est obligatoire pour les systèmes gouvernementaux américains mais constitue une excellente référence pour toute organisation. Les contrôles STIG couvrent :

- **Authentification** : complexité mot de passe, verrouillage compte, timeout session
- **Réseau** : firewall, isolation vSwitch, VLAN, port group security
- **Chiffrement** : TLS 1.2 minimum, algorithmes approuvés FIPS 140-2
- **Logging** : syslog distant, rétention 1 an, intégrité des logs
- **Patching** : délai maximum de 30 jours pour les patchs critiques

8.3 CIS Benchmarks

Les benchmarks CIS (Center for Internet Security) proposent deux niveaux de durcissement : Level 1 (baseline) et Level 2 (haute sécurité). Ils sont plus accessibles que les STIG et couvrent les mêmes domaines avec des recommandations pragmatiques. Pour une approche complète de la conformité, consultez notre guide ISO 27001.

```
# Vérification automatisée CIS - exemples de contrôles

# CIS 1.1 : Vérifier que le Lockdown Mode est activé
vim-cmd vimsvc/auth/lockdown_is_enabled

# CIS 2.1 : Vérifier que SSH est désactivé
chkconfig --list | grep SSH

# CIS 3.1 : Vérifier la politique de sécurité des port groups
esxcli network vswitch standard policy security get -v vSwitch0

# CIS 4.1 : Vérifier la configuration NTP
esxcli system ntp get

# CIS 5.1 : Vérifier que le firewall est actif
esxcli network firewall get

# CIS 6.1 : Vérifier la configuration syslog
esxcli system syslog config get

# CIS 7.1 : Vérifier le niveau d'acceptation VIB
esxcli software acceptance get

# Script d'audit CIS automatisé (exemple)
#!/bin/bash
echo "=== ESXi CIS Benchmark Audit ==="
echo "Lockdown: $(vim-cmd vimsvc/auth/lockdown_is_enabled)"
echo "SSH: $(chkconfig --list | grep SSH)"
echo "Firewall: $(esxcli network firewall get | grep Enabled)"
echo "Syslog: $(esxcli system syslog config get | grep Remote)"
echo "VIB Acceptance: $(esxcli software acceptance get)"
echo "NTP: $(esxcli system ntp get | grep server)"
```

9. Protection anti-ransomware

9.1 Snapshots protégés

Les attaquants ransomware suppriment systématiquement les snapshots avant de chiffrer les vmdk. Protéger les snapshots est donc essentiel pour la récupération :

- **Snapshots hors site** : ne jamais stocker les sauvegardes uniquement sur un datastore accessible depuis l'hôte ESXi compromis.
- **Sauvegardes immutables** : utiliser des solutions de backup qui supportent l'immutabilité (Veeam avec immutable backups, Cohesity DataLock, Commvault WORM). Une sauvegarde immutable ne peut pas être supprimée ou modifiée pendant la durée de rétention, même par un administrateur.
- **Air-gapped backups** : maintenir au moins une copie de sauvegarde déconnectée physiquement du réseau (tape, disques hors ligne).
- **Règle 3-2-1-1-0** : 3 copies des données, 2 types de médias différents, 1 copie hors site, 1 copie immutable/air-gapped, 0 erreurs de restauration (testé).

9.2 Détection de patterns ransomware sur ESXi

Les patterns d'activité ransomware sur ESXi sont caractéristiques et détectables :

```
# Pattern 1 : Arrêt massif de VMs (pré-chiffrement)
# Les ransomwares arrêtent les VMs pour libérer les locks sur les vmdk
# Commandes suspectes dans shell.log :
# vim-cmd vmsvc/power.off
# esxcli vm process kill --type=force --world-id=

# Pattern 2 : Énumération des datastores
# find /vmfs/volumes/ -name "*.vmdk" -o -name "*.vmx"
# ls -la /vmfs/volumes/*/

# Pattern 3 : Utilisation d'openssl pour le chiffrement
# openssl enc -aes-256-cbc -in file.vmdk -out file.vmdk.locked

# Pattern 4 : Suppression des snapshots
# vim-cmd vmsvc/snapshot.removeall

# Pattern 5 : Modification des fichiers VMX (note de rançon)
# Ajout de "annotation" dans les fichiers .vmx

# Script de détection (à exécuter via cron ou monitoring) :
#!/bin/bash
# Alerte si plus de 3 VMs arrêtées en 5 minutes
STOPPED=$(grep "vim.VirtualMachine.powerOff" /var/log/hostd.log | \
  awk -v d="$(date -d '5 minutes ago' '+%Y-%m-%dT%H:%M')" '$0 >= d' | wc -l)
if [ "$STOPPED" -gt 3 ]; then
  logger -t RANSOMWARE_ALERT "CRITICAL: $STOPPED VMs powered off in last 5 min"
fi

# Alerte si fichiers .locked ou .encrypted détectés
LOCKED=$(find /vmfs/volumes/ -name "*.locked" -o -name "*.encrypted" -o -name "*.args" 2>/
dev/null | wc -l)
if [ "$LOCKED" -gt 0 ]; then
  logger -t RANSOMWARE_ALERT "CRITICAL: $LOCKED encrypted files detected on datastores"
fi
```

9.3 Backup immutable avec Veeam

Veeam Backup & Replication est la solution de backup la plus utilisée dans les environnements VMware. Pour une protection anti-ransomware efficace :

- **Immutable Backups** : configurer les repositories Linux Hardened avec le flag d'immutabilité. Les fichiers de backup ne peuvent pas être supprimés ou modifiés pendant la période définie.
- **Séparation des credentials** : le compte de service Veeam ne doit PAS utiliser les mêmes credentials que l'administration ESXi ou vCenter.
- **Réseau dédié** : isoler le trafic de backup sur un VLAN dédié, inaccessible depuis les VMs de production.
- **Test de restauration automatisé** : configurer le SureBackup pour tester automatiquement la restauration de VMs critiques chaque semaine.

10. Monitoring et alertes

10.1 vRealize / Aria Operations

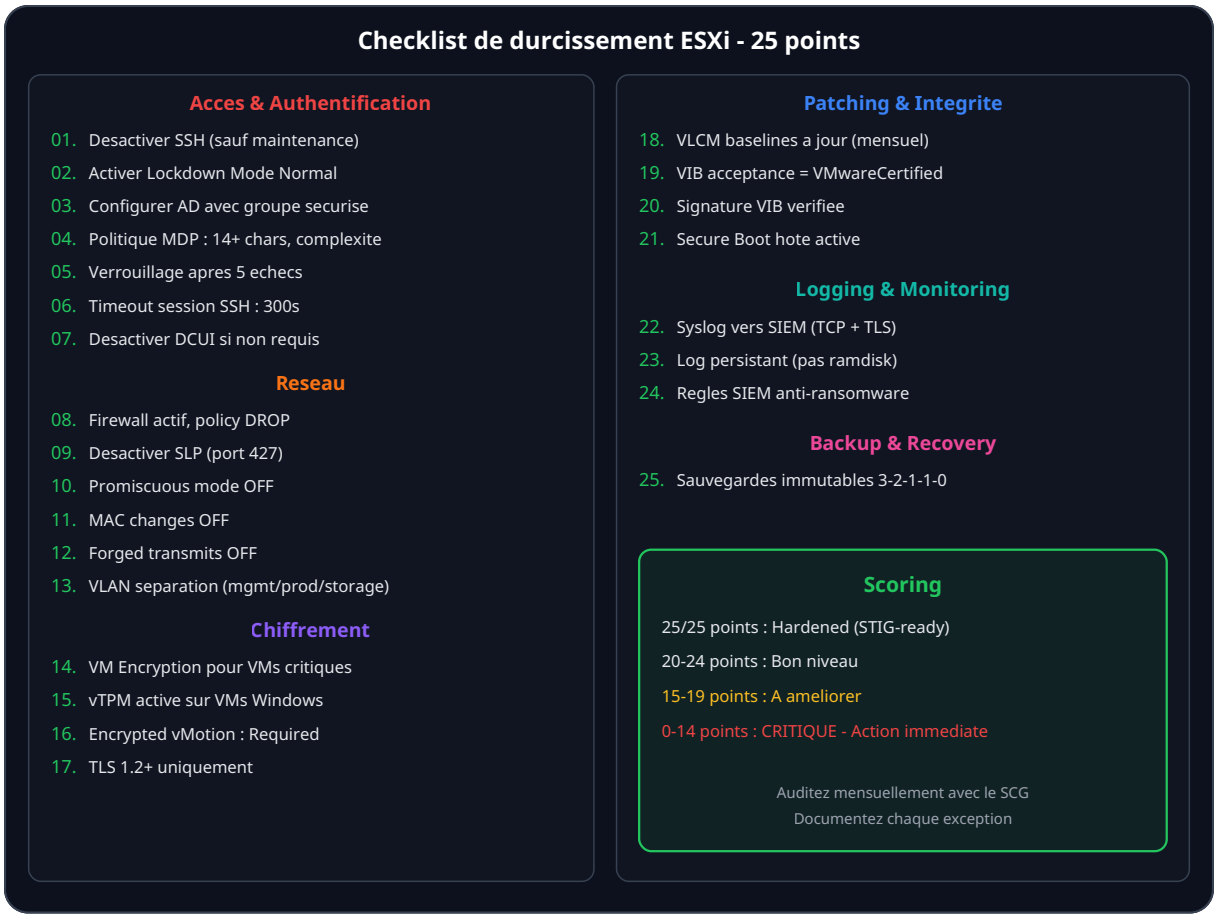
VMware Aria Operations (anciennement vRealize Operations) fournit un monitoring avancé avec des dashboards de sécurité. Les alertes critiques à configurer incluent :

- **SSH activé** : alerte immédiate si le service SSH est démarré sur un hôte.
- **Lockdown Mode désactivé** : alerte si un hôte sort du lockdown mode.
- **VIB non signé installé** : alerte sur l'installation de VIB avec un acceptance level inférieur au seuil.
- **Firewall modifié** : alerte sur toute modification des rulesets du firewall ESXi.
- **Comptes créés/modifiés** : alerte sur les modifications de permissions locales ou AD.
- **Configuration drift** : alerte si un hôte s'écarte de la baseline de sécurité définie.

10.2 Intégration SIEM avancée

Au-delà des logs syslog, l'intégration SIEM doit inclure les événements vCenter (via l'API Events), les alertes VMware Aria, et les logs réseau (NetFlow depuis les vSwitch distribués). La corrélation entre ces sources permet de détecter les attaques multi-étapes qui traversent plusieurs couches. Pour les techniques d'évasion que les attaquants utilisent pour contourner la détection, consultez notre article sur l'évasion EDR/XDR.

11. Checklist de durcissement ESXi (25 points)



Pour approfondir ce sujet, consultez notre outil open-source container-security-scanner qui facilite l'audit de sécurité des conteneurs Docker et Kubernetes.

Questions frequentes

Comment mettre en place Durcissement VMware ESXi dans un environnement de production ?

La mise en place de Durcissement VMware ESXi en production necessite une planification rigoureuse, incluant l'evaluation des prerequis techniques, la definition d'une architecture cible, des tests de validation approfondis et un plan de deploiement progressif avec des points de controle a chaque etape.

Pourquoi Durcissement VMware ESXi est-il essentiel pour la securite des systemes d'information ?

Durcissement VMware ESXi constitue un element fondamental de la securite des systemes d'information car il permet de reduire significativement la surface d'attaque, d'ameliorer la detection des menaces et de renforcer la posture globale de securite de l'organisation face aux cybermenaces actuelles.

Quel hyperviseur choisir pour un environnement de production sécurisé avec Durcissement VMware ESXi : Guide Complet de Sécurisation ?

Le choix dépend de votre budget et de vos compétences. Proxmox VE est open source et gratuit, VMware offre un écosystème mature, Hyper-V s'intègre nativement à Windows Server.

Sources et références : Proxmox VE Wiki · ANSSI

12. Conclusion

Le durcissement de VMware ESXi n'est pas un projet ponctuel mais un processus continu qui doit s'adapter à l'évolution des menaces. En 2026, avec la multiplication des ransomwares ciblant spécifiquement les hyperviseurs, chaque hôte ESXi non durci représente un risque critique pour l'ensemble de l'infrastructure.

Les fondamentaux sont clairs : **désactiver SSH**, **activer le Lockdown Mode**, **configurer le firewall**, **désactiver SLP**, **segmenter les réseaux**, **chiffrer les VMs critiques**, **patcher régulièrement**, **forwarder les logs au SIEM** et **maintenir des sauvegardes immutables**. Ces mesures, combinées, réduisent drastiquement la surface d'attaque et augmentent considérablement le coût pour l'attaquant.

N'oubliez pas que le durcissement de l'hyperviseur ne suffit pas isolément. Il doit s'inscrire dans une stratégie de sécurité globale incluant la protection d'Active Directory (vecteur de CVE-2024-37085), la surveillance réseau, la formation des équipes et les tests réguliers. Pour une vue d'ensemble, consultez notre comparatif sécurité des hyperviseurs et notre guide sur l'anatomie d'une kill chain ransomware.

Récapitulatif des actions prioritaires

1. **Immédiat (J+0)** : Désactiver SSH et SLP, activer le firewall avec policy DROP, patcher les CVE critiques.
2. **Court terme (J+7)** : Activer le Lockdown Mode, configurer le syslog vers SIEM, restreindre les accès par IP.
3. **Moyen terme (J+30)** : Déployer VM Encryption pour les VMs critiques, configurer l'intégration AD sécurisée, mettre en place les sauvegardes immutables.
4. **Long terme (J+90)** : Atteindre la conformité CIS Level 2 ou STIG, déployer NSX-T pour la micro-segmentation, automatiser les audits de conformité.

Références et ressources externes

- vSphere Security Configuration Guide 8 -- Guide officiel de sécurisation VMware/Broadcom
- CIS VMware ESXi Benchmark -- Benchmarks CIS pour le durcissement ESXi
- DISA STIG VMware ESXi 8.0 -- Security Technical Implementation Guide du DoD
- Mandiant - ESXi Hypervisor Malware -- Analyse des techniques de persistance APT sur ESXi
- NVD -- National Vulnerability Database -- base de vulnérabilités du NIST

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr