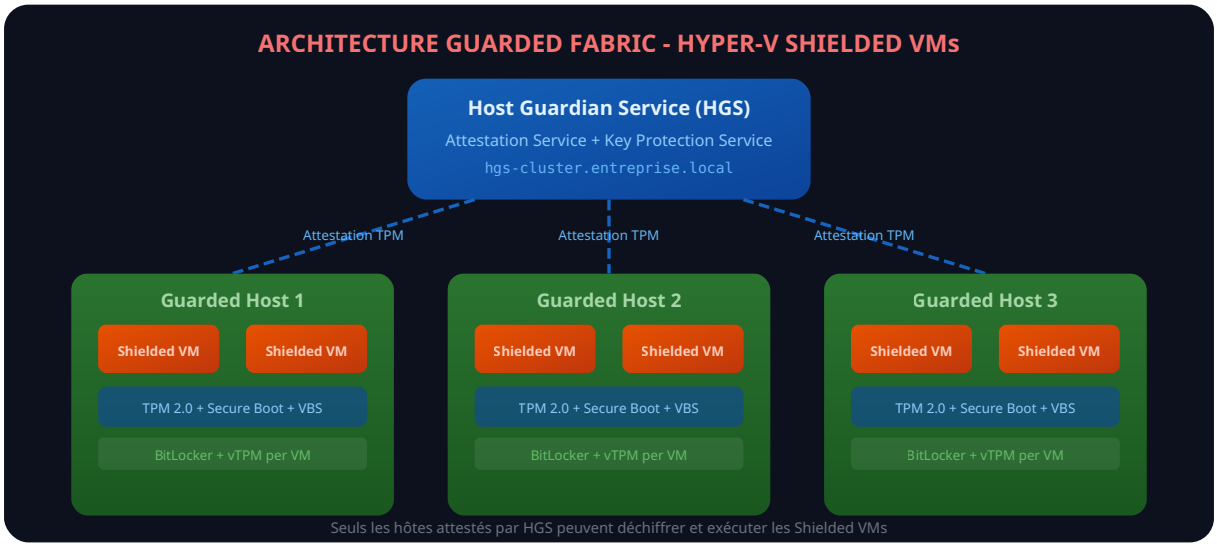
AYI NEDJIMI Consultants

Hyper-V Shielded VMs : Sécurisation Avancée du : Guide

Catégorie : Virtualisation Lecture : 9 min Publié le : 08/03/2026 Auteur : Ayi NEDJIMI

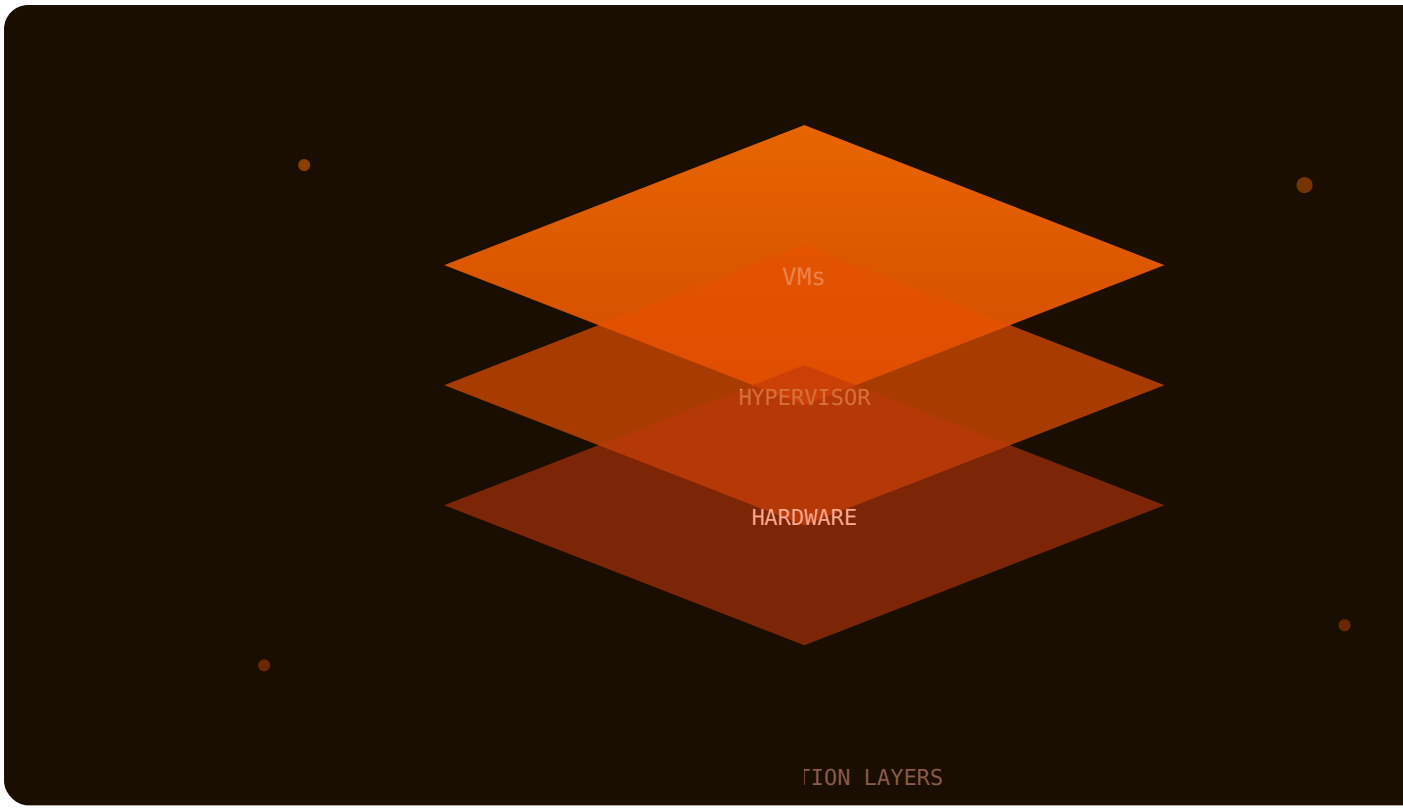
Guide complet Hyper-V Shielded VMs : Guarded Fabric, Host Guardian Service, attestation TPM, déploiement sécurisé, BitLocker, isolation réseau et.

Hyper-V Shielded VMs : Sécurisation Avancée du : Guide constitue un enjeu majeur pour les professionnels de la sécurité informatique et les équipes techniques. Guide complet Hyper-V Shielded VMs : Guarded Fabric, Host Guardian Service, attestation TPM, déploiement sécurisé, BitLocker, isolation réseau et. Ce guide détaillé sur hyperv shielded vms securite datacenter 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.

1. Introduction : la menace de l'administrateur compromis



Dans un datacenter traditionnel, l'administrateur Hyper-V détient un pouvoir absolu sur les machines virtuelles : il peut les inspecter, copier leurs disques, lire leur mémoire et modifier leur configuration. **Les Shielded VMs de Microsoft renversent ce approche en protégeant les workloads virtualisés contre les administrateurs eux-mêmes** -- qu'ils soient malveillants ou compromis. Cette technologie, introduite avec Windows Server 2016 et considérablement améliorée dans Windows Server 2025, constitue la réponse de Microsoft au problème fondamental de la confiance dans l'infrastructure virtualisée. Ce guide approfondi examine en detail les aspects fondamentaux et avances de Hyper, en proposant une analyse structuree et documentee des enjeux actuels. Les professionnels y trouveront des recommandations concretes, des methodologies eprouvees et des retours d'experience terrain directement applicables en environnement de production. L'analyse integre les dernieres evolutions technologiques, les tendances emergentes du secteur et les meilleures pratiques recommandees par les experts du domaine.

Points cles :

- 1. Introduction : la menace de l'administrateur compromis
- 2. Architecture Guarded Fabric : concepts fondamentaux
- 3. Déploiement du Host Guardian Service
- 4. Création et gestion des Shielded VMs
- 5. BitLocker et chiffrement : protection des données au repos

Le scénario de menace est concret : un attaquant qui compromet un compte d'administrateur d'infrastructure peut, dans un environnement classique, accéder à toutes les VMs hébergées. Il peut monter les disques virtuels, extraire les secrets, injecter des backdoors ou exfiltrer des données sensibles. Les Shielded VMs neutralisent ce vecteur d'attaque en chiffrant les disques virtuels avec BitLocker et en restreignant l'exécution aux seuls **hôtes de confiance attestés** par le Host Guardian Service (HGS). Pour plus d'informations, consultez les ressources de ANSSI.

Ce guide explore l'architecture complète des Shielded VMs : du déploiement du Host Guardian Service à la création de Shielded VMs en production, en passant par les mécanismes d'attestation TPM, les Shielding Data Files, l'intégration BitLocker et les stratégies d'isolation réseau. Chaque section intègre des commandes PowerShell testées et des recommandations issues de nos audits de sécurité virtualisation. Pour plus d'informations, consultez les ressources de MITRE ATT&CK.

Point clé : Les Shielded VMs ne protègent pas seulement contre les attaquants externes -- elles protègent contre les *insiders* et les administrateurs compromis. C'est un changement de cadre fondamental dans la sécurité de la virtualisation.

Prérequis de cet article

Cet article suppose une connaissance de base de Hyper-V et de Windows Server. Pour un comparatif global des hyperviseurs, consultez notre article Proxmox vs VMware vs Hyper-V : comparatif sécurité. Pour les techniques d'attaque sur les identités Active Directory qui motivent l'adoption des Shielded VMs, consultez notre guide sur l'exploitation Kerberos dans AD.

2. Architecture Guarded Fabric : concepts fondamentaux

2.1 Les composants de la Guarded Fabric

L'architecture Guarded Fabric repose sur trois composants fondamentaux :

- **Host Guardian Service (HGS)** : cluster Windows Server dédié qui fournit deux services critiques : l'**Attestation Service** (vérifie l'identité et l'intégrité des hôtes Hyper-V) et le **Key Protection Service** (libère les clés de chiffrement uniquement aux hôtes attestés).
- **Guarded Hosts** : serveurs Hyper-V qui ont prouvé leur identité et leur intégrité au HGS. Seuls ces hôtes peuvent exécuter des Shielded VMs. Ils doivent disposer d'un TPM 2.0, du Secure Boot UEFI et de la Virtualization-Based Security (VBS).

- **Shielded VMs** : machines virtuelles dont les disques sont chiffrés par BitLocker via un vTPM (virtual Trusted Platform Module). Elles ne peuvent être déchiffrées et exécutées que sur des Guarded Hosts attestés par le HGS.

2.2 Modes d'attestation : TPM vs Admin-trusted

Le HGS supporte deux modes d'attestation, chacun offrant un niveau de garantie différent :

Critère	Attestation TPM (recommandé)	Attestation Admin-trusted
Niveau de sécurité	Élevé -- vérifie matériel + logiciel	Modéré -- vérifie l'appartenance AD
Prérequis matériel	TPM 2.0, UEFI Secure Boot	Aucun prérequis matériel
Vérifie l'intégrité du boot	Oui (mesure TCG log)	Non
Vérifie Code Integrity	Oui (politique CI)	Non
Protection contre admin compromis	Forte	Limitée
Cas d'usage	Production, conformité	Lab, preuve de concept

Recommandation : attestation TPM obligatoire en production
L'attestation Admin-trusted offre une protection insuffisante en production. Un administrateur de domaine compromis pourrait ajouter un hôte non autorisé au groupe AD de Guarded Hosts, contournant ainsi toute la chaîne de confiance. En mode TPM, l'attestation vérifie cryptographiquement l'identité du matériel et l'intégrité de la chaîne de boot -- un niveau de garantie impossible à contourner par un simple accès AD. Cette distinction est similaire aux enjeux d'exploitation des certificats AD.

2.3 Flux de sécurité : comment une Shielded VM démarre

Le processus de démarrage d'une Shielded VM illustre la chaîne de confiance :

1. Le Guarded Host démarre et le TPM 2.0 mesure chaque composant de la chaîne de boot (firmware UEFI, bootloader, noyau Windows, politiques Code Integrity).
2. Le Guarded Host envoie son rapport d'attestation (TCG log + certificat TPM EK) au HGS.
3. Le HGS vérifie que les mesures correspondent aux valeurs de référence connues (baselines) et que le certificat TPM est approuvé.
4. Si l'attestation réussit, le HGS libère la **Key Protector** -- la clé qui permet au Guarded Host de déchiffrer le vTPM de la Shielded VM.
5. Le vTPM déverrouille BitLocker sur le disque virtuel, et la VM démarre normalement.
6. A aucun moment l'administrateur Hyper-V n'a accès aux clés de chiffrement en clair.

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.

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

3. Déploiement du Host Guardian Service

3.1 Architecture de déploiement HGS

Le HGS doit être déployé sur un cluster dédié, **isolé de la forêt Active Directory de production**. Cette isolation est critique : si un attaquant compromet le domaine de production (via des techniques comme Kerberoasting ou Golden Ticket), il ne doit pas pouvoir atteindre le HGS. Microsoft recommande un minimum de 3 noeuds HGS pour la haute disponibilité.

```
# Installation du rôle HGS sur le premier noeud
# Prérequis : Windows Server 2022/2025 Datacenter, forêt AD dédiée

# 1. Installer le rôle Host Guardian Service
Install-WindowsFeature HostGuardianServiceRole -IncludeManagementTools -Restart

# 2. Initialiser le cluster HGS avec une nouvelle forêt AD
# IMPORTANT : utiliser une forêt dédiée, PAS la forêt de production
$AdminPassword = ConvertTo-SecureString -AsPlainText "P@ssw0rd!Complex2026" -Force
Install-HgsServer -HgsDomainName "hgs.securefabric.local" `
    -SafeModeAdministratorPassword $AdminPassword `
    -ClusterName "HgsCluster" `
    -Restart

# 3. Après redémarrage, initialiser HGS en mode TPM
Initialize-HgsServer -HgsServiceName "GuardianService" `
    -TrustTpm `
    -Http -Https `
    -SigningCertificateThumbprint $SigningCertThumbprint `
    -EncryptionCertificateThumbprint $EncryptionCertThumbprint

# 4. Vérifier l'état du service
Get-HgsServer
Get-HgsTrace -RunDiagnostics
```

3.2 Configuration de l'attestation TPM

L'attestation TPM nécessite l'enregistrement des identifiants TPM (Endorsement Key) de chaque Guarded Host et la définition des politiques d'intégrité de code (CI policies). Cette étape garantit que seuls les hôtes avec un matériel connu et un logiciel intègre peuvent héberger des Shielded VMs.

```
# Sur chaque Guarded Host : exporter l'identifiant TPM
# Exécuter en tant qu'administrateur sur le Guarded Host

# Collecter l'identifiant TPM (EK Certificate)
$ekCert = Get-PlatformIdentifier -Name "GuardedHost01"
$ekCert | Export-Clixml "C:\HGS\GuardedHost01-EK.xml"

# Exporter la politique Code Integrity de référence
New-CIPolicy -Level FilePublisher -Fallback Hash `
    -FilePath "C:\HGS\CI-Policy-Reference.xml" `
    -UserPEs
ConvertFrom-CIPolicy -XmlFilePath "C:\HGS\CI-Policy-Reference.xml" `
    -BinaryFilePath "C:\HGS\CI-Policy-Reference.p7b"

# Capturer la baseline TCG (mesures de boot)
Get-HgsAttestationBaselinePolicy -Path "C:\HGS\TCG-Baseline-Host01.tcglog"

# Sur le serveur HGS : enregistrer l'hôte
# Importer l'identifiant TPM
Add-HgsAttestationTpmHost -Path "C:\HGS\GuardedHost01-EK.xml" `
    -Name "GuardedHost01" -Force

# Enregistrer la politique Code Integrity
Add-HgsAttestationCIPolicy -Path "C:\HGS\CI-Policy-Reference.p7b" `
    -Name "Production-CI-Policy"

# Enregistrer la baseline TPM
Add-HgsAttestationTpmPolicy -Path "C:\HGS\TCG-Baseline-Host01.tcglog" `
    -Name "Baseline-Host01"

# Vérifier l'attestation
Get-HgsAttestationTpmHost
Get-HgsAttestationCIPolicy
```

3.3 Certificats et Key Protection Service

Le Key Protection Service (KPS) utilise deux paires de certificats : un certificat de **signature** (authentifie les réponses du HGS) et un certificat de **chiffrement** (protège les clés des vTPM en transit). Ces certificats doivent être émis par une PKI d'entreprise ou un HSM pour les environnements de haute sécurité.

```
# Générer des certificats auto-signés (lab uniquement)
$signingCert = New-SelfSignedCertificate -DnsName "hgs.securefabric.local" `
    -CertStoreLocation "Cert:\LocalMachine\My" `
    -KeyUsage DigitalSignature -KeyLength 4096

$encryptionCert = New-SelfSignedCertificate -DnsName "hgs.securefabric.local" `
    -CertStoreLocation "Cert:\LocalMachine\My" `
    -KeyUsage KeyEncipherment -KeyLength 4096

# Production : utiliser des certificats PKI
# Demander un certificat auprès de votre CA d'entreprise
# Template : Key Recovery Agent (chiffrement), Code Signing (signature)

# Configurer les certificats dans HGS
Set-HgsKeyProtectionConfiguration `
    -SigningCertificateThumbprint $signingCert.Thumbprint `
    -EncryptionCertificateThumbprint $encryptionCert.Thumbprint

# Sauvegarder les certificats (critique pour le DR)
$password = ConvertTo-SecureString "BackupP@ss!" -AsPlainText -Force
Export-PfxCertificate -Cert $signingCert `
    -FilePath "C:\HGS-Backup\signing-cert.pfx" `
    -Password $password
Export-PfxCertificate -Cert $encryptionCert `
    -FilePath "C:\HGS-Backup\encryption-cert.pfx" `
    -Password $password

# IMPORTANT : stocker les backups hors ligne dans un coffre-fort
```

4. Création et gestion des Shielded VMs

4.1 Shielding Data Files (PDK)

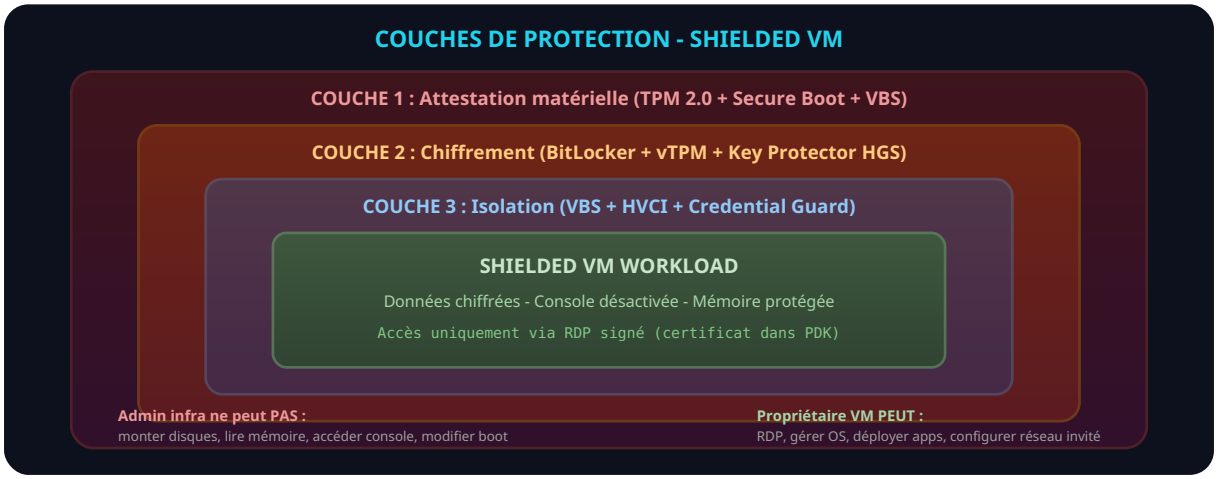
Le **Shielding Data File** (fichier .pdk) est l'élément clé du provisioning des Shielded VMs. Il contient les secrets nécessaires au déploiement : les clés de protection, les certificats des Guardians autorisés, le fichier unattend.xml chiffré, et les certificats RDP pour la connexion sécurisée. Le propriétaire de la VM (le tenant) crée ce fichier et le fournit à l'infrastructure -- sans jamais exposer les secrets aux administrateurs de l'infrastructure.

```
# Création d'un Shielding Data File (PDK)
# Exécuter par le propriétaire de la VM (pas l'admin infra)

# 1. Obtenir le Guardian du HGS (métadonnées publiques)
$Guardian = Get-HgsGuardian -Name "FabricGuardian"

# Si le Guardian n'existe pas encore, l'importer depuis le HGS
Invoke-WebRequest -Uri "https://hgs.securefabric.local/KeyProtection/service/metadata/
2014-07/metadata.xml" `
    -OutFile "C:\Temp\hgs-metadata.xml"
$Guardian = Import-HgsGuardian -Path "C:\Temp\hgs-metadata.xml" `
    -Name "FabricGuardian" -AllowUntrustedRoot

# 2. Créer le Owner Guardian (le propriétaire de la VM)
$OwnerGuardian = New-HgsGuardian -Name "VMOwner" -GenerateCertificates

# 3. Préparer le fichier unattend.xml (personnalisation Windows)
$UnattendFile = "C:\ShieldingData\unattend.xml"

# 4. Créer le Key Protector
$KP = New-HgsKeyProtector -Owner $OwnerGuardian `
    -Guardian $Guardian -AllowUntrustedRoot

# 5. Créer le Shielding Data File
$AdminCredentials = Get-Credential -Message "Mot de passe admin de la VM"
New-ShieldingDataFile -ShieldingDataFilePath "C:\ShieldingData\ShieldedVM.pdk" `
    -Owner $OwnerGuardian `
    -Guardian $Guardian `
    -UnattendFile $UnattendFile `
    -Policy Shielded `
    -RDPCertificatePath "C:\ShieldingData\rdp-cert.pfx" `
    -RDPCertificatePassword $password
```

4.2 Déploiement d'une Shielded VM

Le déploiement d'une Shielded VM utilise un **template disk signé** et le Shielding Data File. Le processus garantit que la VM est provisionnée de manière sécurisée, avec BitLocker activé et le vTPM protégé par le HGS.

```
# Déploiement d'une Shielded VM sur un Guarded Host

# 1. Préparer un template disk signé
# Le template doit être préparé avec sysprep et signé
$templateDisk = "C:\Templates\WS2025-Template.vhdx"

# Signer le template disk
Protect-TemplateDisk -Path $templateDisk `
    -TemplateName "Windows Server 2025 Datacenter" `
    -Version "1.0.0"

# 2. Créer la Shielded VM avec le template et le PDK
$VMName = "ShieldedVM-SQL01"
New-VM -Name $VMName -Generation 2 -MemoryStartupBytes 8GB `
    -VHDPath "C:\VMs\$VMName\$VMName.vhdx" `
    -SwitchName "ProductionSwitch"

# Appliquer le Shielding Data
Initialize-ShieldedVM -VM $VMName `
    -ShieldingDataFilePath "C:\ShieldingData\ShieldedVM.pdk" `
    -TemplateDiskPath $templateDisk

# 3. Configurer les ressources
Set-VM -Name $VMName -ProcessorCount 4 `
    -AutomaticStartAction Start `
    -AutomaticStopAction ShutDown

# 4. Vérifier le statut de protection
Get-VM $VMName | Select-Object Name, SecurityPolicy
Get-VMSecurity -VMName $VMName

# Sortie attendue :
# Shielded : True
# TpmEnabled : True
# EncryptStateAndVMMigrationTraffic : True
# VirtualizationBasedSecurityOptOut : False
```



4.3 Conversion d'une VM existante en Shielded VM

Les VMs existantes peuvent être converties en Shielded VMs. Ce processus active le vTPM, chiffre les disques avec BitLocker et protège la VM avec un Key Protector lié au HGS. La conversion nécessite un arrêt temporaire de la VM.

```
# Conversion d'une VM Gen2 existante en Shielded VM

# 1. Arrêter la VM
Stop-VM -Name "ExistingVM-Web01" -Force

# 2. Vérifier que c'est une VM Génération 2
Get-VM "ExistingVM-Web01" | Select-Object Generation
# Doit retourner : 2

# 3. Activer le vTPM
Set-VMKeyProtector -VMName "ExistingVM-Web01" `
    -NewLocalKeyProtector
Enable-VMTPM -VMName "ExistingVM-Web01"

# 4. Configurer le Key Protector avec le HGS
$KP = New-HgsKeyProtector -Owner $OwnerGuardian `
    -Guardian $Guardian -AllowUntrustedRoot
Set-VMKeyProtector -VMName "ExistingVM-Web01" `
    -KeyProtector $KP.RawData

# 5. Activer le mode Shielded
Set-VMSecurityPolicy -VMName "ExistingVM-Web01" -Shielded $true

# 6. Configurer les options de sécurité
Set-VMSecurity -VMName "ExistingVM-Web01" `
    -EncryptStateAndVmMigrationTraffic $true `
    -VirtualizationBasedSecurityOptOut $false

# 7. Démarrer la VM et activer BitLocker depuis l'invité
Start-VM -Name "ExistingVM-Web01"

# Dans la VM (via RDP) :
# Enable-BitLocker -MountPoint "C:" -TpmProtector -EncryptionMethod XtsAes256
# Resume-BitLocker -MountPoint "C:"
```

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.

5. BitLocker et chiffrement : protection des données au repos

5.1 Intégration BitLocker avec vTPM

Le chiffrement BitLocker dans une Shielded VM repose sur le **virtual TPM (vTPM)**, qui est lui-même protégé par le Key Protector du HGS. Cette chaîne de confiance garantit que les disques ne peuvent être déchiffrés que sur un Guarded Host attesté. Le vTPM est un composant logiciel qui émule un TPM 2.0 physique pour la VM, mais dont l'état est chiffré et stocké dans la configuration de la VM.

```
# Configuration BitLocker dans une Shielded VM
# Exécuter depuis l'intérieur de la VM (session RDP)

# Vérifier la présence du vTPM
Get-TPM
# Sortie : TpmPresent = True, TpmReady = True

# Activer BitLocker sur le disque système
Enable-BitLocker -MountPoint "C:" `
    -TpmProtector `
    -EncryptionMethod XtsAes256 `
    -SkipHardwareTest

# Activer BitLocker sur les disques de données
Enable-BitLocker -MountPoint "D:" `
    -TpmAndPinProtector `
    -EncryptionMethod XtsAes256 `
    -Pin (ConvertTo-SecureString "DataDisk#2026!" -AsPlainText -Force)

# Vérifier le statut du chiffrement
Get-BitLockerVolume | Select-Object MountPoint, VolumeStatus, `
    EncryptionMethod, ProtectionStatus, KeyProtector

# Configurer la sauvegarde des clés de récupération dans AD
Backup-BitLockerKeyProtector -MountPoint "C:" `
    -KeyProtectorId (Get-BitLockerVolume -MountPoint "C:").KeyProtector[0].KeyProtectorId
```

5.2 Chiffrement du trafic de migration

Lorsqu'une Shielded VM est migrée entre Guarded Hosts (live migration), le trafic de migration est automatiquement chiffré. Cela empêche un attaquant réseau de capturer les données en transit -- y compris la mémoire de la VM qui peut contenir des clés cryptographiques, des tokens d'authentification ou des données sensibles.

```
# Vérifier que le chiffrement de migration est activé
Get-VMSecurity -VMName "ShieldedVM-SQL01" |
    Select-Object EncryptStateAndVmMigrationTraffic

# Configurer les hôtes pour la migration chiffrée
Enable-VMMigration -ComputerName "GuardedHost01"
Set-VMMigrationNetwork -ComputerName "GuardedHost01" `
    -Subnet "10.0.50.0/24" -Priority 1

# Activer SMB chiffré pour le stockage partagé
Set-SmbServerConfiguration -EncryptData $true -Force

# Tester une migration live entre Guarded Hosts
Move-VM -Name "ShieldedVM-SQL01" `
    -DestinationHost "GuardedHost02" `
    -IncludeStorage `
    -DestinationStoragePath "C:\VMs\ShieldedVM-SQL01"
```

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

6. Isolation réseau et micro-segmentation

6.1 Network isolation pour les Shielded VMs

L'isolation réseau des Shielded VMs complète la protection offerte par le chiffrement des disques. Microsoft recommande d'utiliser des **VLANs dédiés** et des **ACL de ports** Hyper-V pour restreindre les flux réseau. Le SDN (Software-Defined Networking) de Windows Server, via le Network Controller, offre une micro-segmentation avancée comparable à VMware NSX, comme nous l'avons exploré dans notre guide de migration VMware.

```
# Configuration de l'isolation réseau Hyper-V

# Créer un vSwitch dédié aux Shielded VMs
New-VMSwitch -Name "ShieldedSwitch" `
    -NetAdapterName "Ethernet2" `
    -AllowManagementOS $false `
    -EnableEmbeddedTeaming $true

# Configurer l'isolation VLAN
Set-VMNetworkAdapterVlan -VMName "ShieldedVM-SQL01" `
    -VMNetworkAdapterName "Network Adapter" `
    -Access -VlanId 500

# Appliquer des ACL de ports (micro-segmentation)
# Bloquer tout par défaut
Add-VMNetworkAdapterExtendedAcl -VMName "ShieldedVM-SQL01" `
    -Action Deny -Direction Inbound -Weight 1

# Autoriser SQL Server uniquement depuis le VLAN applicatif
Add-VMNetworkAdapterExtendedAcl -VMName "ShieldedVM-SQL01" `
    -Action Allow -Direction Inbound `
    -RemoteIPAddress "10.0.100.0/24" `
    -LocalPort "1433" -Protocol TCP -Weight 10

# Autoriser RDP uniquement depuis le VLAN admin
Add-VMNetworkAdapterExtendedAcl -VMName "ShieldedVM-SQL01" `
    -Action Allow -Direction Inbound `
    -RemoteIPAddress "10.0.10.0/24" `
    -LocalPort "3389" -Protocol TCP -Weight 10

# Autoriser les réponses sortantes (stateful)
Add-VMNetworkAdapterExtendedAcl -VMName "ShieldedVM-SQL01" `
    -Action Allow -Direction Outbound `
    -Weight 10 -Stateful $true
```

6.2 Isolation du plan de gestion

Le réseau de gestion du Guarded Fabric (HGS, consoles d'administration) doit être strictement isolé des réseaux de production et des réseaux des VMs. Un attaquant qui accède au réseau de gestion pourrait tenter des attaques de type man-in-the-middle sur les communications HGS, une technique documentée dans nos analyses de détournement DNS.

```
# Architecture réseau recommandée pour Guarded Fabric
#
# VLAN 10  : Management (HGS, SCVMM, consoles)
# VLAN 20  : Stockage (SMB, iSCSI) - chiffré
# VLAN 30  : Live Migration - dédié, chiffré
# VLAN 50  : Attestation HGS (trafic TPM)
# VLAN 100 : Production VMs
# VLAN 200 : DMZ VMs
# VLAN 500 : Shielded VMs isolées

# Configurer le pare-feu Windows sur les Guarded Hosts
# Autoriser l'attestation HGS
New-NetFirewallRule -DisplayName "HGS Attestation" `
    -Direction Inbound -Protocol TCP `
    -LocalPort 80,443 `
    -RemoteAddress "10.0.50.0/24" `
    -Action Allow

# Restreindre WinRM aux admins autorisés
Set-Item WSMan:\localhost\Service\IPv4Filter -Value "10.0.10.0/24"
Restart-Service WinRM
```

7. Monitoring, audit et détection d'incidents

7.1 Journalisation des événements Guarded Fabric

La supervision de la Guarded Fabric nécessite la collecte centralisée des événements de sécurité provenant du HGS, des Guarded Hosts et des Shielded VMs. Les événements clés à surveiller incluent les échecs d'attestation (tentative d'exécution sur un hôte non autorisé), les modifications de politique HGS et les tentatives d'accès à la console des Shielded VMs.

```
# Événements critiques à surveiller (Event IDs)

# HGS - Attestation Service
# Event ID 4001 : Attestation réussie (informatif)
# Event ID 4002 : Attestation échouée (CRITIQUE - potentielle compromission)
# Event ID 4003 : Politique modifiée (ALERTE)

# Configurer l'audit avancé sur le HGS
auditpol /set /subcategory:"Certification Services" /success:enable /failure:enable
auditpol /set /subcategory:"Other Object Access Events" /success:enable /failure:enable

# Requête des événements d'échec d'attestation
Get-WinEvent -FilterHashtable @{
    LogName = 'Microsoft-Windows-HostGuardianService-Attestation/Admin'
    Level = 2,3  # Error + Warning
} -MaxEvents 50 | Format-Table TimeCreated, Id, Message -Wrap

# Monitoring via SIEM - transfert des événements
# Configurer Windows Event Forwarding (WEF)
# ou agent Syslog pour intégration SIEM

# Créer une alerte pour les échecs d'attestation
$subscription = @"


    *[System[(Level=2)]]


"@

# Alerte email sur échec d'attestation (via Task Scheduler)
$trigger = New-ScheduledTaskTrigger -AtStartup
$action = New-ScheduledTaskAction -Execute "powershell.exe" `
    -Argument "-File C:\Scripts\Alert-AttestationFailure.ps1"
Register-ScheduledTask -TaskName "HGS-AttestationAlert" `
    -Trigger $trigger -Action $action
```

7.2 Diagnostics et dépannage HGS

Microsoft fournit un module de diagnostic complet pour la Guarded Fabric. L'outil `Get-HgsTrace` permet d'identifier rapidement les problèmes de configuration et d'attestation. Intégrez ces vérifications dans votre surveillance proactive, en complément des approches de détection post-exploitation.

```
# Diagnostic complet de la Guarded Fabric
Get-HgsTrace -RunDiagnostics -Detailed

# Vérifier l'état de santé du cluster HGS
Get-HgsServer
Test-HgsServer -AttestationServerUrl "https://hgs.securefabric.local/Attestation" `
    -KeyProtectionServerUrl "https://hgs.securefabric.local/KeyProtection"

# Tester l'attestation d'un hôte spécifique
Get-HgsClientConfiguration
# Vérifier IsHostGuarded = True

# Diagnostic réseau
Test-NetConnection -ComputerName "hgs.securefabric.local" -Port 443
Resolve-DnsName "hgs.securefabric.local"

# Export des logs pour analyse
Get-HgsTrace -RunDiagnostics | Export-Clixml "C:\Diag\hgs-trace.xml"
```

8. Comparaison avec VMware et Proxmox VE

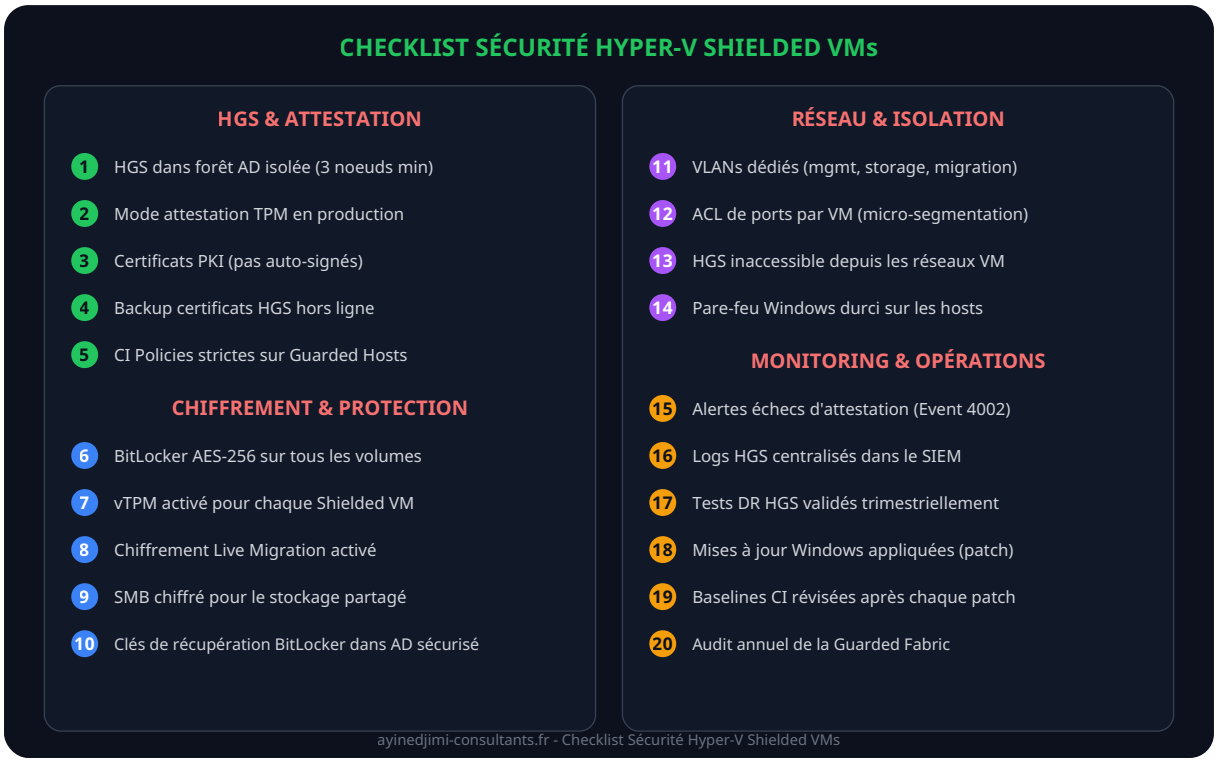
Les Shielded VMs de Microsoft adressent un problème de sécurité que les autres hyperviseurs traitent différemment. Voici un comparatif des approches de protection des VMs confidentielles :

Fonctionnalité	Hyper-V Shielded VMs	VMware Confidential VMs	Proxmox VE (KVM)
Chiffrement des disques	BitLocker via vTPM	VM Encryption (vSphere 6.5+)	LUKS/ZFS encryption
Protection mémoire VM	VBS + Secure Enclave	AMD SEV / Intel TDX (vSphere 8)	AMD SEV support (expérimental)
Attestation matérielle	HGS avec TPM 2.0	Non natif (VMware Trust Authority)	Non natif
Protection contre l'admin	Forte (console désactivée)	Partielle (VM Encryption only)	Non disponible
Migration sécurisée	Live migration chiffrée	vMotion chiffré	SSH tunnel (non natif)
Coût	Windows Server Datacenter	vSphere Enterprise+ / VCF	Gratuit (open source)
Maturité	Élevée (depuis WS 2016)	Bonne (vSphere 8+)	En développement
Complexité	Élevée (HGS cluster requis)	Modérée	Faible

Les Shielded VMs restent la solution la plus mature et la plus complète pour protéger les workloads contre les administrateurs compromis. VMware Trust Authority (introduit dans vSphere 7) offre des fonctionnalités similaires mais avec une architecture différente. Proxmox

VE, malgré le support expérimental d'AMD SEV, ne propose pas encore de solution intégrée comparable. Pour un comparatif détaillé des trois hyperviseurs, consultez notre comparatif sécurité complet.

9. Checklist sécurité Guarded Fabric



Questions frequentes

Comment mettre en place Hyper dans un environnement de production ?

La mise en place de Hyper 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.

Quel hyperviseur choisir pour un environnement de production sécurisé avec Hyper-V Shielded VMs : Sécurisation Avancée ?

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.

Comment sécuriser l'accès à l'interface d'administration pour Hyper-V Shielded VMs : Sécurisation Avancée ?

Placez l'interface de gestion sur un VLAN dédié, activez le 2FA, utilisez des certificats TLS valides et limitez l'accès par IP source. Ne laissez jamais l'interface exposée sur Internet.

Pour approfondir ce sujet, consultez notre outil open-source docker-security-audit qui facilite la vérification de conformité des configurations Docker.

Sources et références : Proxmox VE Wiki · ANSSI

10. Conclusion : quand déployer des Shielded VMs ?

Les Shielded VMs ne sont pas destinées à toutes les charges de travail. Leur déploiement se justifie pour les **workloads hautement sensibles** : bases de données contenant des données personnelles (RGPD), contrôleurs de domaine Active Directory, serveurs PKI, applications financières soumises à DORA, ou toute VM hébergeant des secrets cryptographiques.

Le coût de déploiement est significatif : infrastructure HGS dédiée (3 serveurs minimum), licences Windows Server Datacenter, matériel avec TPM 2.0, et complexité opérationnelle accrue. Mais pour les organisations où la compromission d'un administrateur pourrait entraîner une violation de données catastrophique, l'investissement est largement justifié.

Les tendances futures vont dans le sens du **Confidential Computing** : AMD SEV-SNP, Intel TDX et ARM CCA apportent des protections matérielles au niveau du processeur, réduisant la surface d'attaque même en cas de compromission complète de l'hyperviseur. Microsoft intègre progressivement ces technologies dans Azure (Confidential VMs) et Windows Server. L'avenir de la virtualisation sécurisée passe par cette convergence entre attestation matérielle, chiffrement de la mémoire et isolation cryptographique.

Pour aller plus loin

Consultez nos autres articles sur la virtualisation sécurisée : Durcissement VMware ESXi, Migration VMware vers Proxmox VE et le comparatif sécurité des hyperviseurs. Pour les attaques spécifiques sur l'infrastructure Windows, consultez notre guide sur les escalades de privilèges Windows.

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

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