Checklist Sécurité HYPER-V

Ayi NEDJIMI Consultants
ayinedjimi-consultants.fr
v1.0 — 2026-04-04 · 199 controles

Sommaire

Section 18 — GOUVERNANCE ET CONFORMITÉ

Section 18 — GOUVERNANCE ET CONFORMITÉ

18.0 GOUVERNANCE ET CONFORMITÉ

Annexe : Checklist

1.0 — SÉCURITÉ DE L'HÔTE HYPER-V

1.1.1 *Installation en mode Server Core (installation minimale)*

DESCRIPTION :
L'hôte Hyper-V doit être installé en mode Server Core (sans interface graphique Desktop Experience) pour minimiser la surface d'attaque. Le mode Server Core élimine l'interface graphique complète, Internet Explorer, Windows Explorer et de nombreux composants non essentiels. Cela réduit considérablement le nombre de vulnérabilités potentielles, diminue la fréquence des mises à jour nécessaires et limite les vecteurs d'attaque disponibles pour un attaquant ayant compromis l'hôte.

```
# Vérifier le type d'installation
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion" | Select-Object InstallationType

# Vérifier si le shell graphique est installé
Get-WindowsFeature Server-Gui-Shell, Server-Gui-Mgmt-Infra

# Vérifier la présence de l'interface Desktop Experience
Get-WindowsFeature Desktop-Experience
```

AUDIT :

- **GUI :** Non applicable en Server Core
- **Valeur attendue :** InstallationType = "Server Core"

REMÉDIATION :

1. **Réinstallation :** Réinstaller Windows Server 2025 en sélectionnant l'option "Server Core" lors de l'installation
2. **Conversion (si possible) :**

```
# Supprimer l'interface graphique (redémarrage requis)
Remove-WindowsFeature Server-Gui-Shell, Server-Gui-Mgmt-Infra -Restart
```

REMÉDIATION :

1. **Administration à distance :** Utiliser Windows Admin Center, RSAT, PowerShell Remoting ou SCVMM pour l'administration

VALEUR PAR DÉFAUT :
Desktop Experience (si sélectionné lors de l'installation)

Aucun impact fonctionnel sur Hyper-V — toutes les fonctionnalités de virtualisation sont disponibles en Server Core.

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

1.1.2 *Rôle Hyper-V comme rôle unique sur l'hôte*

DESCRIPTION :
L'hôte Hyper-V ne doit exécuter que le rôle Hyper-V et les fonctionnalités strictement nécessaires à son fonctionnement. L'installation de rôles supplémentaires (serveur web, contrôleur de domaine, serveur de fichiers, etc.) augmente significativement la surface d'attaque et peut compromettre l'isolation entre l'hyperviseur et les services hébergés. Le principe de fonction unique est une exigence fondamentale pour la sécurité de la virtualisation.

```
# Lister tous les rôles installés
Get-WindowsFeature | Where-Object { $_.Installed -eq $true } | Select-Object Name, DisplayName

# Vérifier que seul Hyper-V est installé comme rôle serveur
Get-WindowsFeature | Where-Object { $_.Installed -eq $true -and $_.FeatureType -eq "Role" } | Select-Object Name, DisplayName

# Rôles attendus : Hyper-V, File-Services (requis), Failover-Clustering (si cluster)
```

AUDIT :

- **Valeur attendue :** Uniquement Hyper-V + Failover-Clustering (si applicable) + fonctionnalités de base

REMÉDIATION :

1. **PowerShell :**

```
# Supprimer les rôles non nécessaires
Remove-WindowsFeature -Name Web-Server, DNS, DHCP, AD-Domain-Services -Restart
```

REMÉDIATION :

1. **Documentation :** Documenter et justifier chaque rôle/fonctionnalité installé

VALEUR PAR DÉFAUT :
Aucun rôle installé par défaut après installation initiale

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

1.1.3 *Services Windows non essentiels désactivés*

DESCRIPTION :

Tous les services Windows non essentiels au fonctionnement de l'hôte Hyper-V doivent être désactivés. Chaque service actif représente un vecteur d'attaque potentiel et consomme des ressources système. Les services tels que Print Spooler, Windows Search, SNMP (si non utilisé), Remote Registry (si non requis), Xbox services doivent être désactivés sur un hôte de virtualisation dédié.

```
# Lister les services en cours d'exécution
Get-Service | Where-Object { $_.Status -eq 'Running' } | Select-Object Name, DisplayName, StartType | Sort-Object Name

# Services à vérifier spécifiquement (doivent être désactivés)
$servicesToCheck = @('Spooler', 'WSearch', 'SNMP', 'RemoteRegistry', 'XblAuthManager', 'XblGameSave', 'XboxNetApiSvc', 'DiagTrack',
foreach ($svc in $servicesToCheck) {
    Get-Service -Name $svc -ErrorAction SilentlyContinue | Select-Object Name, Status, StartType
}

# Vérifier les services démarrage automatique non Microsoft
Get-WmiObject Win32_Service | Where-Object { $_.StartMode -eq 'Auto' -and $_.PathName -notlike '*Windows*' } | Select-Object Name,
```

AUDIT :

- **Valeur attendue :** Services non essentiels à l'état "Disabled" ou "Stopped"

REMÉDIATION :

1. **PowerShell :**

```
# Désactiver les services non essentiels
$servicesToDisable = @('Spooler', 'WSearch', 'RemoteRegistry', 'DiagTrack', 'MapsBroker', 'lfsvc')
foreach ($svc in $servicesToDisable) {
    Set-Service -Name $svc -StartupType Disabled -ErrorAction SilentlyContinue
    Stop-Service -Name $svc -Force -ErrorAction SilentlyContinue
}
```

REMÉDIATION :

1. **GPO :** Configuration ordinateur > Paramètres Windows > Paramètres de sécurité > Services système

VALEUR PAR DÉFAUT :

La plupart des services sont activés par défaut

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

1.1.4 *Fonctionnalités Windows non essentielles supprimées*

DESCRIPTION :

Les fonctionnalités Windows (Features) non requises pour le fonctionnement d'Hyper-V doivent être désinstallées. La suppression des fonctionnalités non utilisées réduit la surface d'attaque et les besoins en mises à jour correctives. Sur un hôte Hyper-V, les fonctionnalités comme PowerShell v2, SMB 1.0, Telnet Client, TFTP Client doivent être retirées.

```
# Lister les fonctionnalités installées
Get-WindowsFeature | Where-Object Installed | Select-Object Name, DisplayName

# Vérifier les fonctionnalités dangereuses
Get-WindowsFeature PowerShell-V2, SMB1Protocol, Telnet-Client, TFTP-Client

# Fonctionnalités optionnelles (appx)
Get-WindowsOptionalFeature -Online | Where-Object State -eq "Enabled" | Select-Object FeatureName
```

REMÉDIATION :

1. **PowerShell :**

```
# Supprimer les fonctionnalités non nécessaires
Remove-WindowsFeature PowerShell-V2
Disable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol -NoRestart
Remove-WindowsFeature Telnet-Client
```

VALEUR PAR DÉFAUT :

Plusieurs fonctionnalités installées par défaut

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

1.2.1 *Version du système d'exploitation hôte à jour*

DESCRIPTION :
Le système d'exploitation hôte Hyper-V doit être maintenu à la dernière version de Windows Server 2025 avec tous les correctifs de sécurité cumulatifs appliqués. Les vulnérabilités non corrigées dans l'hyperviseur ou le noyau Windows peuvent permettre l'évasion de VM (VM Escape), l'escalade de privilèges ou le déni de service affectant toutes les machines virtuelles hébergées. Les correctifs Hyper-V sont critiques car ils protègent la couche d'isolation.

```
# Version et build actuels
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion" | Select-Object ProductName, DisplayVersion, CurrentBui

# Dernière mise à jour installée
Get-HotFix | Sort-Object InstalledOn -Descending | Select-Object -First 10 HotFixID, Description, InstalledOn

# Vérifier les mises à jour en attente
$UpdateSession = New-Object -ComObject Microsoft.Update.Session
$UpdateSearcher = $UpdateSession.CreateUpdateSearcher()
$SearchResult = $UpdateSearcher.Search("IsInstalled=0 and Type='Software'")
$SearchResult.Updates | Select-Object Title, MsrcSeverity
```

REMÉDIATION :

1. **PowerShell :**

```
# Installer les mises à jour via Windows Update
Install-Module PSWindowsUpdate -Force
Get-WindowsUpdate -Install -AcceptAll -AutoReboot

# Ou via WSUS/SCCM selon la politique de l'organisation
```

REMÉDIATION :

1. **Planification :** Définir une fenêtre de maintenance mensuelle pour les mises à jour Hyper-V

VALEUR PAR DÉFAUT :
Mises à jour automatiques activées (configuration WSUS recommandée)

Preuve d'audit :

```
| Résultat | _____________________________________________ |
| Capture  | ☐ Oui ☐ Non                                   |
| Note     | _____________________________________________ |
```

1.2.2 *Correctifs spécifiques Hyper-V appliqués*

DESCRIPTION :
Les correctifs spécifiques au composant Hyper-V doivent être installés en priorité. Les vulnérabilités dans l'hyperviseur (comme les CVE liés à vmswitch.sys, vmwp.exe, ou au moteur d'émulation) sont particulièrement critiques car elles peuvent permettre à un attaquant depuis une VM invitée d'exécuter du code sur l'hôte (VM Escape). Les CVE récentes pour Hyper-V doivent être suivies et corrigées dans les 72 heures.

```
# Vérifier la version des composants Hyper-V critiques
Get-Item C:\Windows\System32\vmms.exe | Select-Object VersionInfo
Get-Item C:\Windows\System32\vmwp.exe | Select-Object VersionInfo
Get-Item C:\Windows\System32\drivers\vmswitch.sys | Select-Object VersionInfo

# Vérifier les KB spécifiques Hyper-V récentes
Get-HotFix | Where-Object { $_.Description -like "*Security*" } | Sort-Object InstalledOn -Descending | Select-Object -First 20
```

REMÉDIATION :

1. Appliquer immédiatement les correctifs Hyper-V critiques via WSUS/SCCM
2. Surveiller les bulletins de sécurité Microsoft pour les CVE Hyper-V
3. Planifier des redémarrages rapides pour les correctifs critiques

VALEUR PAR DÉFAUT :
Dépend de la politique de mise à jour

Preuve d'audit :

```
| Résultat | _____________________________________________ |
| Capture  | ☐ Oui ☐ Non                                   |
| Note     | _____________________________________________ |
```

1.3.1 *Pare-feu Windows activé sur tous les profils*

DESCRIPTION :
Le pare-feu Windows Defender Firewall doit être activé sur les trois profils réseau (Domaine, Privé, Public) de l'hôte Hyper-V. Le pare-feu constitue la première ligne de défense contre les connexions réseau non autorisées vers l'hôte. Les règles doivent être configurées pour n'autoriser que les ports strictement nécessaires à la gestion Hyper-V et au trafic de cluster.

```
# Vérifier l'état du pare-feu sur tous les profils
Get-NetFirewallProfile | Select-Object Name, Enabled, DefaultInboundAction, DefaultOutboundAction

# Vérifier les règles actives
Get-NetFirewallRule | Where-Object { $_.Enabled -eq 'True' -and $_.Direction -eq 'Inbound' } | Select-Object Name, DisplayName, Act

# Vérifier les règles Hyper-V spécifiques
Get-NetFirewallRule | Where-Object { $_.DisplayName -like "*Hyper-V*" } | Select-Object DisplayName, Enabled, Action, Direction
```

AUDIT :

- **Valeur attendue :** Tous les profils activés, action par défaut "Block" pour le trafic entrant

REMÉDIATION :

1. **PowerShell :**

```
# Activer le pare-feu sur tous les profils
Set-NetFirewallProfile -Profile Domain,Public,Private -Enabled True
Set-NetFirewallProfile -Profile Domain,Public,Private -DefaultInboundAction Block -DefaultOutboundAction Allow
```

REMÉDIATION :

1. **GPO :** Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Pare-feu Windows Defender avec sécurité avancée

VALEUR PAR DÉFAUT :
Activé sur tous les profils

Preuve d'audit :

```
| Résultat | _____________________________________________ |
| Capture  | ☐ Oui ☐ Non                                   |
| Note     | _____________________________________________ |
```

1.3.2 *Règles de pare-feu restrictives pour la gestion Hyper-V*

DESCRIPTION :
Les règles de pare-feu de l'hôte Hyper-V doivent être configurées de manière restrictive. Seuls les ports nécessaires à l'administration (WinRM 5985/5986, RDP 3389 si requis), à la Live Migration (6600, 3343), au clustering (3343, 445, 135, 139) et à la réplication (80/443) doivent être autorisés. Chaque règle doit être limitée aux adresses IP sources des postes d'administration autorisés.

```
# Lister les règles entrantes actives avec les ports
Get-NetFirewallRule -Direction Inbound -Enabled True | ForEach-Object {
    $portFilter = $_ | Get-NetFirewallPortFilter
    [PSCustomObject]@{
        Name = $_.DisplayName
        Action = $_.Action
        Protocol = $portFilter.Protocol
        LocalPort = $portFilter.LocalPort
        RemoteAddress = ($_ | Get-NetFirewallAddressFilter).RemoteAddress
    }
} | Sort-Object LocalPort

# Vérifier les règles autorisant "Any" en source
Get-NetFirewallRule -Direction Inbound -Enabled True | ForEach-Object {
    $addrFilter = $_ | Get-NetFirewallAddressFilter
    if ($addrFilter.RemoteAddress -contains 'Any') {
        [PSCustomObject]@{
            Name = $_.DisplayName
            RemoteAddress = $addrFilter.RemoteAddress
        }
    }
}
```

REMÉDIATION :

1. **PowerShell :**

```
# Restreindre les règles à des IP spécifiques
$adminSubnet = "10.0.1.0/24"
Get-NetFirewallRule -DisplayName "Windows Remote Management*" | Set-NetFirewallRule -RemoteAddress $adminSubnet
Get-NetFirewallRule -DisplayName "Remote Desktop*" | Set-NetFirewallRule -RemoteAddress $adminSubnet
```

VALEUR PAR DÉFAUT :
Règles ouvertes à toutes les adresses

Preuve d'audit :

```
| Résultat | _____________________________________________ |
| Capture  | ☐ Oui ☐ Non                                   |
| Note     | _____________________________________________ |
```

1.3.3 *Journalisation du pare-feu activée*

DESCRIPTION :
La journalisation du pare-feu Windows doit être activée sur l'hôte Hyper-V pour enregistrer les connexions autorisées et refusées. Ces journaux sont essentiels pour la détection d'intrusion, l'analyse forensique et la vérification de la conformité des flux réseau vers l'hôte de virtualisation.

```
# Vérifier la configuration de journalisation du pare-feu
Get-NetFirewallProfile | Select-Object Name, LogFileName, LogMaxSizeKilobytes, LogAllowed, LogBlocked

# Vérifier l'existence des fichiers de log
Test-Path "C:\Windows\System32\LogFiles\Firewall\pfirewall.log"
```

AUDIT :

- **Valeur attendue :** LogAllowed = True, LogBlocked = True, LogMaxSizeKilobytes >= 16384

REMÉDIATION :

1. **PowerShell :**

```
Set-NetFirewallProfile -Profile Domain,Public,Private -LogBlocked True -LogAllowed True -LogMaxSizeKilobytes 32768 -LogFileName "%S
```

REMÉDIATION :

1. **GPO :** Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Pare-feu Windows > Propriétés > Journalisation

VALEUR PAR DÉFAUT :
LogBlocked = False, LogAllowed = False

Preuve d'audit :

```
| Résultat | _____________________________________________ |
| Capture  | ☐ Oui ☐ Non                                   |
| Note     | _____________________________________________ |
```

1.4.1 *Windows Defender Antivirus activé avec exclusions Hyper-V*

DESCRIPTION :
Windows Defender Antivirus (ou toute solution antivirus d'entreprise) doit être activé sur l'hôte Hyper-V. Cependant, des exclusions spécifiques doivent être configurées pour éviter les impacts de performance et les problèmes de stabilité. Les processus Hyper-V (vmms.exe, vmwp.exe, vmcompute.exe), les répertoires de VMs et les extensions de fichiers VM (.vhd, .vhdx, .avhd, .avhdx, .vsv, .iso) doivent être exclus de l'analyse en temps réel.

```
# Vérifier l'état de Windows Defender
Get-MpComputerStatus | Select-Object AntivirusEnabled, RealTimeProtectionEnabled, AntivirusSignatureLastUpdated

# Vérifier les exclusions configurées
Get-MpPreference | Select-Object -ExpandProperty ExclusionPath
Get-MpPreference | Select-Object -ExpandProperty ExclusionProcess
Get-MpPreference | Select-Object -ExpandProperty ExclusionExtension

# Exclusions attendues pour Hyper-V
# Processus : vmms.exe, vmwp.exe, vmcompute.exe, vmsp.exe
# Extensions : .vhd, .vhdx, .avhd, .avhdx, .vsv, .iso, .rct, .vmcx, .vmrs
# Répertoires : C:\ProgramData\Microsoft\Windows\Hyper-V, répertoires des VMs
```

REMÉDIATION :

1. **PowerShell :**

```
# Ajouter les exclusions Hyper-V recommandées par Microsoft
Add-MpPreference -ExclusionProcess "vmms.exe", "vmwp.exe", "vmcompute.exe", "vmsp.exe"
Add-MpPreference -ExclusionExtension ".vhd", ".vhdx", ".avhd", ".avhdx", ".vsv", ".iso", ".rct", ".vmcx", ".vmrs"
Add-MpPreference -ExclusionPath "C:\ProgramData\Microsoft\Windows\Hyper-V"
Add-MpPreference -ExclusionPath "C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks"
# Ajouter le chemin des VMs personnalisé si différent
```

VALEUR PAR DÉFAUT :
Windows Defender activé sans exclusions Hyper-V

Preuve d'audit :

```
| Résultat | _____________________________________________ |
| Capture  | ☐ Oui ☐ Non                                   |
| Note     | _____________________________________________ |
```

1.4.2 *Mises à jour des signatures antivirus*

DESCRIPTION :
Les signatures antivirus de l'hôte Hyper-V doivent être mises à jour quotidiennement. Des signatures obsolètes laissent l'hôte vulnérable aux malwares récents. La mise à jour doit être automatisée via WSUS, SCCM ou Microsoft Update directement.

```
# Vérifier l'ancienneté des signatures
Get-MpComputerStatus | Select-Object AntivirusSignatureLastUpdated, AntivirusSignatureVersion, AntivirusSignatureAge

# Vérifier la source de mise à jour
Get-MpPreference | Select-Object SignatureDefinitionUpdateSourceOrder, SignatureFallbackOrder
```

AUDIT :

- **Valeur attendue :** AntivirusSignatureAge <= 1 jour

REMÉDIATION :

1. **PowerShell :**

```
# Forcer la mise à jour des signatures
Update-MpSignature

# Configurer la mise à jour automatique
Set-MpPreference -SignatureUpdateInterval 4
```

VALEUR PAR DÉFAUT :
Mise à jour automatique activée

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

1.5.1 *BitLocker activé sur le volume système de l'hôte*

DESCRIPTION :
BitLocker Drive Encryption doit être activé sur le volume système (C:) de l'hôte Hyper-V pour protéger les données au repos, y compris la configuration de l'hyperviseur, les fichiers de configuration des VMs et les éventuels fichiers temporaires contenant des données sensibles. Le chiffrement empêche l'accès aux données en cas de vol physique du serveur ou des disques.

```
# Vérifier l'état de BitLocker sur tous les volumes
Get-BitLockerVolume | Select-Object MountPoint, VolumeStatus, EncryptionPercentage, ProtectionStatus, KeyProtector

# Vérifier le protecteur TPM
(Get-BitLockerVolume -MountPoint C:).KeyProtector | Select-Object KeyProtectorType
```

AUDIT :

- **Valeur attendue :** VolumeStatus = "FullyEncrypted", ProtectionStatus = "On"

REMÉDIATION :

1. **PowerShell :**

```
# Activer BitLocker avec TPM
Enable-BitLocker -MountPoint "C:" -EncryptionMethod XtsAes256 -TpmProtector
Add-BitLockerKeyProtector -MountPoint "C:" -RecoveryPasswordProtector

# Stocker la clé de récupération dans Active Directory
Backup-BitLockerKeyProtector -MountPoint "C:" -KeyProtectorId (Get-BitLockerVolume -MountPoint C:).KeyProtector[1].KeyProtectorId
```

VALEUR PAR DÉFAUT :
BitLocker désactivé

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

1.5.2 *BitLocker activé sur les volumes de stockage VM*

DESCRIPTION :
Les volumes de stockage contenant les fichiers des machines virtuelles (VHDX, fichiers de configuration, checkpoints) doivent être chiffrés avec BitLocker. Les données des VMs au repos sur les disques physiques de l'hôte sont particulièrement sensibles car elles contiennent l'intégralité des systèmes invités, y compris les données et les identifiants en mémoire sauvegardés dans les fichiers .vmrs.

```
# Identifier les volumes de stockage VM
Get-VMHost | Select-Object VirtualHardDiskPath, VirtualMachinePath
Get-VM | Select-Object Name, Path, @{N='VHDPaths';E={($_ | Get-VMHardDiskDrive).Path}}

# Vérifier BitLocker sur ces volumes
Get-BitLockerVolume | Select-Object MountPoint, VolumeStatus, ProtectionStatus
```

REMÉDIATION :
1. **PowerShell :**

```
# Activer BitLocker sur le volume de stockage VM
Enable-BitLocker -MountPoint "D:" -EncryptionMethod XtsAes256 -TpmProtector
Enable-BitLocker -MountPoint "E:" -EncryptionMethod XtsAes256 -TpmProtector
```

REMÉDIATION :
1. **Note :** Si les VMs sont sur un CSV (Cluster Shared Volume), utiliser BitLocker sur les volumes CSV

VALEUR PAR DÉFAUT :
BitLocker désactivé

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

1.6.1 *Secure Boot activé sur l'hôte physique*

DESCRIPTION :
Le Secure Boot UEFI doit être activé sur le serveur physique hébergeant Hyper-V. Le Secure Boot garantit que seuls les logiciels signés et de confiance sont chargés lors du démarrage du système, empêchant les bootkits et rootkits de se charger avant l'hyperviseur. Cette protection est fondamentale pour l'intégrité de la chaîne de démarrage de l'hyperviseur.

```
# Vérifier l'état du Secure Boot
Confirm-SecureBootUEFI

# Informations détaillées sur le firmware
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SecureBoot\State" -Name UEFISecureBootEnabled

# Mode de démarrage
bcdedit /enum | Select-String "path|device|description"
```

AUDIT :
- **Valeur attendue :** Confirm-SecureBootUEFI = True

REMÉDIATION :
1. **BIOS/UEFI :** Accéder au firmware UEFI du serveur et activer Secure Boot
2. **Prérequis :** Le système doit être installé en mode UEFI (non Legacy/BIOS)
3. **Vérification post-activation :** Redémarrer et vérifier que le système démarre correctement

VALEUR PAR DÉFAUT :
Dépend du fabricant du serveur (généralement activé)

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

1.6.2 *TPM 2.0 présent et fonctionnel*

DESCRIPTION :
Un module TPM (Trusted Platform Module) version 2.0 doit être présent, activé et fonctionnel sur l'hôte Hyper-V. Le TPM est requis pour BitLocker, l'attestation TPM du Host Guardian Service (Guarded Fabric), Credential Guard et la mesure d'intégrité du démarrage (Measured Boot). Sans TPM, de nombreuses fonctionnalités de sécurité avancées de Hyper-V ne peuvent pas être déployées.

```
# Vérifier la présence et la version du TPM
Get-Tpm | Select-Object TpmPresent, TpmReady, TpmEnabled, TpmActivated, ManufacturerVersion
Get-WmiObject -Namespace "root\cimv2\Security\MicrosoftTpm" -Class Win32_Tpm | Select-Object SpecVersion

# Vérifier la version TPM (doit être 2.0)
(Get-WmiObject -Namespace "root\cimv2\Security\MicrosoftTpm" -Class Win32_Tpm).SpecVersion
```

AUDIT :

- **Valeur attendue :** TpmPresent = True, TpmReady = True, SpecVersion commence par "2.0"

REMÉDIATION :

1. **BIOS/UEFI :** Activer le TPM dans les paramètres du firmware
2. **Initialisation :** `Initialize-Tpm` si le TPM n'est pas initialisé
3. **Remplacement matériel :** Si TPM 1.2, planifier le remplacement ou la mise à jour du firmware TPM

VALEUR PAR DÉFAUT :
Dépend du matériel serveur

Preuve d'audit :

```
| Résultat | _____________________________________________ |
| Capture  | ☐ Oui ☐ Non                                   |
| Note     | _____________________________________________ |
```

1.7.1 *Credential Guard activé sur l'hôte*

DESCRIPTION :
Windows Defender Credential Guard doit être activé sur l'hôte Hyper-V pour protéger les identifiants NTLM et Kerberos TGT en mémoire. Credential Guard utilise la sécurité basée sur la virtualisation (VBS) pour isoler les secrets dans un conteneur sécurisé inaccessible même aux processus en mode noyau. Sur un hôte Hyper-V, la compromission des identifiants d'administration permettrait l'accès à toutes les VMs.

```
# Vérifier l'état de Credential Guard
Get-CimInstance -ClassName Win32_DeviceGuard -Namespace root\Microsoft\Windows\DeviceGuard | Select-Object *

# Vérification simplifiée
(Get-CimInstance -ClassName Win32_DeviceGuard -Namespace root\Microsoft\Windows\DeviceGuard).SecurityServicesRunning
# Valeur 1 = Credential Guard en cours d'exécution

# Vérification via le registre
Get-ItemProperty "HKLM:\SYSTEM\CurrentControlSet\Control\DeviceGuard" -Name EnableVirtualizationBasedSecurity
Get-ItemProperty "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa" -Name LsaCfgFlags
```

AUDIT :

- **Valeur attendue :** SecurityServicesRunning contient 1 (Credential Guard), LsaCfgFlags = 1 ou 2

REMÉDIATION :

1. **GPO :** Configuration ordinateur > Stratégies > Modèles d'administration > Système > Device Guard > Activer la sécurité basée sur la virtualisation
2. **PowerShell :**

```
# Activer via le registre
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\DeviceGuard" -Name EnableVirtualizationBasedSecurity -Value 1
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa" -Name LsaCfgFlags -Value 1
```

REMÉDIATION :

1. **Redémarrage requis** après activation

VALEUR PAR DÉFAUT :
Désactivé

Preuve d'audit :

```
| Résultat | _____________________________________________ |
| Capture  | ☐ Oui ☐ Non                                   |
| Note     | _____________________________________________ |
```

1.7.2 *Hypervisor-Protected Code Integrity (HVCI) activé*

DESCRIPTION :
HVCI (Hypervisor-Protected Code Integrity), aussi appelé Memory Integrity, doit être activé sur l'hôte Hyper-V. HVCI utilise la virtualisation matérielle pour protéger le processus de validation de l'intégrité du code en mode noyau. Cela empêche l'injection de code malveillant non signé dans le noyau, réduisant considérablement le risque de rootkits et d'exploits kernel-level sur l'hôte hyperviseur.

```
# Vérifier HVCI
(Get-CimInstance -ClassName Win32_DeviceGuard -Namespace root\Microsoft\Windows\DeviceGuard).SecurityServicesRunning
# Valeur 2 = HVCI en cours d'exécution

# Registre
Get-ItemProperty "HKLM:\SYSTEM\CurrentControlSet\Control\DeviceGuard\Scenarios\HypervisorEnforcedCodeIntegrity" -Name Enabled
```

AUDIT :

- **Valeur attendue :** SecurityServicesRunning contient 2, Enabled = 1

REMÉDIATION :

1. **GPO :** Configuration ordinateur > Stratégies > Modèles d'administration > Système > Device Guard > Activer la sécurité basée sur la virtualisation > Code Integrity = Activé avec verrouillage UEFI
2. **PowerShell :**

```
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\DeviceGuard\Scenarios\HypervisorEnforcedCodeIntegrity" -Name Enabled
```

VALEUR PAR DÉFAUT :
Désactivé

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

1.7.3 *Virtualization Based Security (VBS) activée*

DESCRIPTION :
La sécurité basée sur la virtualisation (VBS) doit être activée sur l'hôte Hyper-V. VBS crée une région mémoire isolée du système d'exploitation normal en utilisant l'hyperviseur Windows. Cette isolation est le fondement de Credential Guard, HVCI et d'autres mécanismes de sécurité avancés. Sur un hôte Hyper-V, VBS fonctionne conjointement avec l'hyperviseur pour renforcer la sécurité de l'hôte.

```
# Vérifier l'état de VBS
Get-CimInstance -ClassName Win32_DeviceGuard -Namespace root\Microsoft\Windows\DeviceGuard | Select-Object VirtualizationBasedSecur

# VirtualizationBasedSecurityStatus : 0=Non activé, 1=Activé mais non en cours, 2=En cours d'exécution
```

AUDIT :

- **Valeur attendue :** VirtualizationBasedSecurityStatus = 2

REMÉDIATION :

1. **GPO :** Configuration ordinateur > Stratégies > Modèles d'administration > Système > Device Guard
2. **Prérequis matériels :** CPU avec virtualisation (Intel VT-x/AMD-V), SLAT, TPM 2.0, Secure Boot

VALEUR PAR DÉFAUT :
Varie selon l'édition et le matériel

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

1.8.1 *Politique de mot de passe renforcée sur l'hôte*

DESCRIPTION :
La politique de mot de passe de l'hôte Hyper-V doit respecter les exigences de complexité, de longueur minimale (14 caractères minimum) et de renouvellement. Les mots de passe des comptes locaux et de domaine utilisés pour administrer l'hôte Hyper-V doivent être particulièrement robustes car ils donnent accès à l'ensemble de l'infrastructure virtualisée.

```
# Vérifier la politique de mot de passe locale
net accounts

# Ou via PowerShell (politique de domaine si joint au domaine)
Get-ADDefaultDomainPasswordPolicy

# Vérifier la politique locale
secedit /export /cfg C:\secpol.cfg
Select-String -Path C:\secpol.cfg -Pattern "MinimumPasswordLength|PasswordComplexity|MaximumPasswordAge|MinimumPasswordAge|Password
Remove-Item C:\secpol.cfg
```

AUDIT :

- **Valeur attendue :** MinimumPasswordLength >= 14, PasswordComplexity = 1, MaximumPasswordAge <= 60

REMÉDIATION :

1. **GPO :** Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies de comptes > Stratégie de mot de passe
2. Longueur minimale : 14 caractères
3. Complexité : Activée
4. Historique : 24 mots de passe

VALEUR PAR DÉFAUT :
Longueur minimale = 0, Complexité = Désactivée

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

1.8.2 *Politique de verrouillage de compte configurée*

DESCRIPTION :
Une politique de verrouillage de compte doit être configurée sur l'hôte Hyper-V pour se protéger contre les attaques par force brute. Le seuil de verrouillage, la durée de verrouillage et la fenêtre de réinitialisation doivent être définis pour bloquer les tentatives d'authentification répétées sans impacter l'administration légitime.

```
# Vérifier la politique de verrouillage
net accounts

# Via GPO
secedit /export /cfg C:\secpol.cfg
Select-String -Path C:\secpol.cfg -Pattern "LockoutBadCount|ResetLockoutCount|LockoutDuration"
Remove-Item C:\secpol.cfg
```

AUDIT :

- **Valeur attendue :** LockoutBadCount <= 5, LockoutDuration >= 30, ResetLockoutCount >= 30

REMÉDIATION :

1. **GPO :** Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies de comptes > Stratégie de verrouillage du compte
2. Seuil de verrouillage : 5 tentatives
3. Durée de verrouillage : 30 minutes
4. Réinitialiser le compteur : 30 minutes

VALEUR PAR DÉFAUT :
Verrouillage désactivé (0 tentatives)

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

1.8.3 *Compte Administrateur local renommé et désactivé*

DESCRIPTION :
Le compte Administrateur local intégré (SID S-1-5-21-*-500) doit être renommé et idéalement désactivé sur l'hôte Hyper-V. Ce compte est une cible privilégiée pour les attaquants car il est présent par défaut sur tous les systèmes Windows. Le renommage complique l'énumération, et la désactivation empêche son utilisation comme vecteur d'attaque.

```
# Vérifier le nom du compte Administrateur (SID -500)
Get-LocalUser | Where-Object { $_.SID -like "*-500" } | Select-Object Name, Enabled, SID

# Vérifier si le compte invité est désactivé
Get-LocalUser | Where-Object { $_.SID -like "*-501" } | Select-Object Name, Enabled, SID
```

AUDIT :

- **Valeur attendue :** Compte -500 renommé (pas "Administrateur" ou "Administrator"), Enabled = False

REMÉDIATION :

1. **PowerShell :**

```
# Renommer le compte Administrateur
Rename-LocalUser -Name "Administrateur" -NewName "AdminHV_Custom"
# Désactiver le compte
Disable-LocalUser -Name "AdminHV_Custom"
```

REMÉDIATION :

1. **GPO :** Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Options de sécurité > Comptes : Renommer le compte administrateur

VALEUR PAR DÉFAUT :
"Administrateur" (FR) ou "Administrator" (EN), Activé

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

1.8.4 *LAPS (Local Administrator Password Solution) déployé*

DESCRIPTION :
Microsoft LAPS (Local Administrator Password Solution) doit être déployé sur l'hôte Hyper-V pour gérer automatiquement les mots de passe des comptes administrateurs locaux. LAPS génère des mots de passe aléatoires uniques, les stocke de manière sécurisée dans Active Directory et les renouvelle automatiquement. Cela élimine le risque de mots de passe partagés entre les hôtes Hyper-V.

```
# Vérifier si LAPS est installé (Windows LAPS intégré à Server 2025)
Get-WindowsFeature LAPS -ErrorAction SilentlyContinue

# Vérifier la politique LAPS
Get-ItemProperty "HKLM:\SOFTWARE\Policies\Microsoft Services\AdmPwd" -ErrorAction SilentlyContinue
Get-ItemProperty "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\LAPS\Config" -ErrorAction SilentlyContinue

# Windows LAPS (natif Server 2025)
Get-LapsAADPassword -DeviceIds (Get-ADComputer $env:COMPUTERNAME).ObjectGUID -ErrorAction SilentlyContinue
```

REMÉDIATION :

1. **GPO :** Configuration ordinateur > Stratégies > Modèles d'administration > LAPS
2. Configurer la longueur, complexité et durée de vie du mot de passe LAPS

VALEUR PAR DÉFAUT :
LAPS non configuré

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

1.9.1 *Politique d'audit avancée configurée sur l'hôte*

DESCRIPTION :
La politique d'audit avancée (Advanced Audit Policy Configuration) doit être configurée sur l'hôte Hyper-V pour enregistrer les événements de sécurité critiques. Les catégories d'audit suivantes doivent être activées : ouverture/fermeture de session, gestion des comptes, accès aux objets, changement de stratégie, utilisation de privilèges et événements système.

```
# Vérifier la configuration d'audit avancée
auditpol /get /category:*

# Catégories critiques à vérifier
auditpol /get /subcategory:"Logon"
auditpol /get /subcategory:"Special Logon"
auditpol /get /subcategory:"Logoff"
auditpol /get /subcategory:"Account Lockout"
auditpol /get /subcategory:"Security Group Management"
auditpol /get /subcategory:"User Account Management"
auditpol /get /subcategory:"Process Creation"
auditpol /get /subcategory:"Audit Policy Change"
```

AUDIT :

- **Valeur attendue :** Success and Failure pour les catégories critiques

REMÉDIATION :

1. **GPO :** Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Configuration avancée de la stratégie d'audit
2. **PowerShell :**

```
auditpol /set /subcategory:"Logon" /success:enable /failure:enable
auditpol /set /subcategory:"Special Logon" /success:enable /failure:enable
auditpol /set /subcategory:"Account Lockout" /success:enable /failure:enable
auditpol /set /subcategory:"Security Group Management" /success:enable /failure:enable
auditpol /set /subcategory:"User Account Management" /success:enable /failure:enable
auditpol /set /subcategory:"Process Creation" /success:enable /failure:enable
```

VALEUR PAR DÉFAUT :
Audit minimal activé

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

1.9.2 *Taille des journaux d'événements configurée*

DESCRIPTION :
La taille maximale des journaux d'événements Windows doit être augmentée sur l'hôte Hyper-V pour garantir la rétention d'un historique suffisant. Les journaux Security, System, Application et Microsoft-Windows-Hyper-V doivent être dimensionnés pour conserver au minimum 90 jours d'événements.

```
# Vérifier la taille des journaux principaux
Get-WinEvent -ListLog Security, System, Application, "Microsoft-Windows-Hyper-V-VMMS-Admin", "Microsoft-Windows-Hyper-V-Worker-Admi
```

AUDIT :

- **Valeur attendue :** Security >= 1 Go, System >= 256 Mo, Hyper-V logs >= 256 Mo

REMÉDIATION :

1. **PowerShell :**

```
wevtutil sl Security /ms:1073741824
wevtutil sl System /ms:268435456
wevtutil sl Application /ms:268435456
wevtutil sl "Microsoft-Windows-Hyper-V-VMMS-Admin" /ms:268435456
wevtutil sl "Microsoft-Windows-Hyper-V-Worker-Admin" /ms:268435456
```

REMÉDIATION :

1. **GPO :** Configuration ordinateur > Stratégies > Modèles d'administration > Composants Windows > Service Journal des événements

VALEUR PAR DÉFAUT :
20 Mo pour la plupart des journaux

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

1.9.3 *Journalisation PowerShell activée*

DESCRIPTION :
La journalisation avancée de PowerShell doit être activée sur l'hôte Hyper-V, incluant Module Logging, Script Block Logging et Transcription. PowerShell est l'outil principal d'administration d'Hyper-V et un vecteur d'attaque courant. L'enregistrement de toutes les commandes exécutées permet la détection d'activités malveillantes et l'analyse forensique post-incident.

```
# Vérifier Module Logging
Get-ItemProperty "HKLM:\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ModuleLogging" -ErrorAction SilentlyContinue

# Vérifier Script Block Logging
Get-ItemProperty "HKLM:\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging" -ErrorAction SilentlyContinue

# Vérifier Transcription
Get-ItemProperty "HKLM:\SOFTWARE\Policies\Microsoft\Windows\PowerShell\Transcription" -ErrorAction SilentlyContinue
```

AUDIT :

- **Valeur attendue :** EnableModuleLogging = 1, EnableScriptBlockLogging = 1, EnableTranscripting = 1

REMÉDIATION :

1. **GPO :** Configuration ordinateur > Stratégies > Modèles d'administration > Composants Windows > Windows PowerShell
2. Activer "Activer la journalisation des modules"
3. Activer "Activer la journalisation des blocs de script PowerShell"
4. Activer "Activer la transcription PowerShell"

VALEUR PAR DÉFAUT :
Désactivé

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

1.9.4 *Sysmon déployé sur l'hôte Hyper-V*

DESCRIPTION :
Microsoft Sysmon (System Monitor) devrait être déployé sur l'hôte Hyper-V pour une surveillance avancée des processus, connexions réseau, modifications de fichiers et chargement de pilotes. Sysmon fournit une visibilité détaillée qui complète la journalisation Windows standard et est essentiel pour la détection de menaces avancées ciblant l'hyperviseur.

```
# Vérifier si Sysmon est installé et en cours d'exécution
Get-Service Sysmon64 -ErrorAction SilentlyContinue | Select-Object Name, Status, StartType

# Vérifier la configuration Sysmon
sysmon64 -c 2>$null

# Vérifier les événements Sysmon
Get-WinEvent -LogName "Microsoft-Windows-Sysmon/Operational" -MaxEvents 5 -ErrorAction SilentlyContinue
```

REMÉDIATION :

1. Télécharger Sysmon depuis Sysinternals
2. Déployer avec une configuration adaptée à Hyper-V

```
sysmon64 -accepteula -i sysmonconfig-hyperv.xml
```

VALEUR PAR DÉFAUT :
Non installé

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

1.9.5 *Transfert des journaux vers un SIEM*

DESCRIPTION :
Les journaux d'événements de l'hôte Hyper-V doivent être transférés en temps réel vers un SIEM centralisé (Microsoft Sentinel, Splunk, ELK, QRadar, etc.). La centralisation des logs permet la corrélation d'événements entre les hôtes Hyper-V, la détection de patterns malveillants et la protection contre la suppression de traces par un attaquant ayant compromis l'hôte.

```
# Vérifier la configuration Windows Event Forwarding (WEF)
wecutil gs 2>$null

# Vérifier l'agent SIEM installé
Get-Service *splunk*, *elastic*, *winlogbeat*, *nxlog*, *omsagent* -ErrorAction SilentlyContinue | Select-Object Name, Status

# Vérifier la subscription WEF
wecutil es 2>$null
```

REMÉDIATION :

1. Configurer Windows Event Forwarding (WEF) ou installer l'agent SIEM approprié
2. S'assurer que les journaux Hyper-V spécifiques sont inclus dans la collecte

VALEUR PAR DÉFAUT :
Non configuré

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

1.9.6 *NTP synchronisé et sécurisé*

DESCRIPTION :
Le service de temps Windows (W32Time) de l'hôte Hyper-V doit être synchronisé avec une source de temps fiable et authentifiée. La précision de l'horodatage est critique pour la corrélation des journaux entre les hôtes Hyper-V, les VMs et les équipements réseau. Hyper-V fournit également le service de synchronisation temporelle aux VMs invitées.

```
# Vérifier la configuration NTP
w32tm /query /configuration
w32tm /query /status
w32tm /query /peers

# Vérifier la source de temps
Get-ItemProperty "HKLM:\SYSTEM\CurrentControlSet\Services\W32Time\Parameters" | Select-Object NtpServer, Type
```

AUDIT :

- **Valeur attendue :** Source de temps fiable (DC ou NTP externe), Type = "NTP" ou "NT5DS"

REMÉDIATION :

1. **PowerShell :**

```
# Configurer le serveur NTP
w32tm /config /manualpeerlist:"ntp.organization.local" /syncfromflags:manual /reliable:yes /update
Restart-Service W32Time
w32tm /resync
```

VALEUR PAR DÉFAUT :
Synchronisation avec le contrôleur de domaine (si joint au domaine)

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

VALEUR PAR DÉFAUT :
═══

2.0 — GESTION DES ACCÈS ET RBAC

2.1.1 *Membres du groupe Hyper-V Administrators audités*

DESCRIPTION :
Le groupe local « Hyper-V Administrators » donne un accès complet à toutes les fonctionnalités Hyper-V sur l'hôte, y compris la création, modification et suppression de VMs, la gestion des réseaux virtuels et l'accès aux fichiers de configuration. Les membres de ce groupe doivent être strictement limités, documentés et revus régulièrement. Tout ajout non autorisé doit déclencher une alerte.

```
# Lister les membres du groupe Hyper-V Administrators
Get-LocalGroupMember -Group "Hyper-V Administrators" | Select-Object Name, ObjectClass, PrincipalSource

# Si le serveur est membre d'un domaine, vérifier les groupes imbriqués
Get-ADGroupMember -Identity "Hyper-V Administrators" -Recursive -ErrorAction SilentlyContinue | Select-Object Name, SamAccountName,

# Vérifier le groupe Administrateurs local (qui a aussi accès Hyper-V)
Get-LocalGroupMember -Group "Administrateurs" | Select-Object Name, ObjectClass, PrincipalSource
```

AUDIT :

- **Valeur attendue :** Liste minimale et documentée de comptes administratifs dédiés

REMÉDIATION :

1. **PowerShell :**

```
# Supprimer les membres non autorisés
Remove-LocalGroupMember -Group "Hyper-V Administrators" -Member "DOMAIN\UserNonAutorise"

# Documenter les membres autorisés
Get-LocalGroupMember -Group "Hyper-V Administrators" | Export-Csv "C:\Audit\HyperV-Admins-$(Get-Date -Format 'yyyyMMdd').csv"
```

REMÉDIATION :

1. Mettre en place une revue trimestrielle des membres du groupe

VALEUR PAR DÉFAUT :
Groupe vide par défaut

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

2.1.2 *Séparation des comptes d'administration*

DESCRIPTION :
Les administrateurs Hyper-V doivent disposer de comptes dédiés et séparés pour l'administration de l'hyperviseur, distincts de leurs comptes utilisateur quotidiens et de leurs comptes d'administration de domaine. Cette séparation limite l'impact d'une compromission de compte et respecte le principe de moindre privilège tiering (Tier 0 pour les contrôleurs de domaine, Tier 1 pour les serveurs dont Hyper-V).

```
# Vérifier la convention de nommage des comptes admin Hyper-V
Get-LocalGroupMember -Group "Hyper-V Administrators" | Select-Object Name

# Vérifier que les comptes admin HV ne sont pas des comptes de domaine admin
Get-ADGroupMember "Domain Admins" | ForEach-Object {
    $member = $_.SamAccountName
    if (Get-LocalGroupMember -Group "Hyper-V Administrators" | Where-Object { $_.Name -like "*$member*" }) {
        Write-Warning "Le compte Domain Admin '$member' est aussi dans Hyper-V Administrators"
    }
}
```

AUDIT :

- **Valeur attendue :** Comptes dédiés type "adm-hv-prenom.nom", pas de comptes Domain Admins

REMÉDIATION :

1. Créer des comptes dédiés pour l'administration Hyper-V (ex: adm-hv-dupont)
2. Retirer les comptes Domain Admins du groupe Hyper-V Administrators (sauf si strictement nécessaire)
3. Documenter la matrice des accès

VALEUR PAR DÉFAUT :
Aucune séparation par défaut

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

2.1.3 *Comptes de service Hyper-V avec mots de passe gérés (gMSA)*

DESCRIPTION :
Les comptes de service utilisés par Hyper-V et les services associés (SCVMM, agents de monitoring, solutions de sauvegarde) doivent utiliser des comptes de service gérés de groupe (gMSA — Group Managed Service Accounts). Les gMSA éliminent la gestion manuelle des mots de passe, les changent automatiquement et réduisent le risque de compromission de comptes de service avec des mots de passe statiques.

```
# Lister les services Hyper-V et leurs comptes d'exécution
Get-WmiObject Win32_Service | Where-Object { $_.DisplayName -like "*Hyper-V*" -or $_.DisplayName -like "*Virtual*" } | Select-Objec

# Vérifier les gMSA existants
Get-ADServiceAccount -Filter * | Select-Object Name, SamAccountName, Enabled

# Vérifier si les services utilisent des gMSA
Get-WmiObject Win32_Service | Where-Object { $_.StartName -like "*$*" } | Select-Object Name, StartName
```

AUDIT :

- **Valeur attendue :** Comptes de service gMSA (terminant par $) ou comptes système (LocalSystem, NetworkService)

REMÉDIATION :

1. **PowerShell :**

```
# Créer un gMSA pour les services Hyper-V
New-ADServiceAccount -Name "gMSA-HyperV-Svc" -DNSHostName "gmsa-hyperv.domain.local" -PrincipalsAllowedToRetrieveManagedPassword "H
Install-ADServiceAccount -Identity "gMSA-HyperV-Svc"
```

VALEUR PAR DÉFAUT :
Services Hyper-V sous LocalSystem

Preuve d'audit :

```
| Résultat | _____________________________________________ |
| Capture  | ☐ Oui ☐ Non                                   |
| Note     | _____________________________________________ |
```

2.2.1 *Délégation d'administration via SCVMM (rôles utilisateur)*

DESCRIPTION :
Si System Center Virtual Machine Manager (SCVMM) est déployé, les rôles utilisateur doivent être configurés pour fournir une délégation d'administration granulaire. SCVMM propose des rôles prédéfinis (Administrator, Delegated Administrator, Read-Only Administrator, Tenant Administrator, Self-Service User) qui permettent de limiter précisément les actions de chaque administrateur selon son périmètre de responsabilité.

```
# Lister les rôles utilisateur SCVMM
Get-SCUserRole | Select-Object Name, UserRoleProfile, Description

# Détail des permissions par rôle
Get-SCUserRole | ForEach-Object {
    [PSCustomObject]@{
        Name = $_.Name
        Profile = $_.UserRoleProfile
        Members = ($_.Members -join ', ')
        AllowedActions = ($_.Permission -join ', ')
    }
}

# Vérifier les membres de chaque rôle
Get-SCUserRole | Select-Object Name, @{N='Members';E={$_.Members -join '; '}}
```

REMÉDIATION :

1. **SCVMM Console :** Settings > Security > User Roles
2. Créer des rôles personnalisés correspondant aux responsabilités de chaque équipe
3. Appliquer le principe du moindre privilège

VALEUR PAR DÉFAUT :
Rôle Administrator unique

Preuve d'audit :

```
| Résultat | _____________________________________________ |
| Capture  | ☐ Oui ☐ Non                                   |
| Note     | _____________________________________________ |
```

2.2.2 *Self-Service Portal — limites et quotas*

DESCRIPTION :
Si un portail Self-Service est configuré (via SCVMM ou Windows Admin Center), les quotas et limites doivent être définis pour chaque utilisateur ou groupe. Les quotas couvrent le nombre maximum de VMs, la mémoire totale, le nombre de CPU virtuels, le stockage et les points de quota. Sans quotas, un utilisateur pourrait consommer toutes les ressources de l'hôte, affectant les autres VMs.

```
# Vérifier les rôles Self-Service et leurs quotas (SCVMM)
Get-SCUserRole | Where-Object { $_.UserRoleProfile -eq "SelfServiceUser" } | Select-Object Name, @{N='Quota';E={$_.Quota}}

# Vérifier les quotas spécifiques
Get-SCUserRoleQuota -UserRole (Get-SCUserRole -Name "SelfService-Equipe1")
```

REMÉDIATION :
1. **SCVMM :** Configurer des quotas par rôle Self-Service
2. Limiter le nombre de VMs, la mémoire et le stockage par utilisateur/groupe

VALEUR PAR DÉFAUT :
Aucun quota (SCVMM), Self-Service désactivé

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

2.3.1 *JEA (Just Enough Administration) configuré pour Hyper-V*

DESCRIPTION :
Just Enough Administration (JEA) doit être configuré pour permettre l'administration Hyper-V avec des privilèges minimaux via des endpoints PowerShell contraints. JEA permet de définir précisément quelles commandes PowerShell un administrateur peut exécuter, sur quels paramètres, et sous quel contexte de sécurité. Cela réduit drastiquement le risque de mouvements latéraux et d'abus de privilèges.

```
# Vérifier les endpoints JEA configurés
Get-PSSessionConfiguration | Where-Object { $_.Name -like "*JEA*" -or $_.Name -like "*HyperV*" } | Select-Object Name, Permission,

# Vérifier les fichiers de capacité de rôle
Get-ChildItem "C:\Program Files\WindowsPowerShell\Modules\*\RoleCapabilities\*.psrc" -Recurse -ErrorAction SilentlyContinue

# Vérifier la configuration de session JEA
Get-PSSessionConfiguration | Select-Object Name, Permission
```

AUDIT :
- **Valeur attendue :** Au moins un endpoint JEA pour Hyper-V avec des capacités de rôle restreintes

REMÉDIATION :
1. **Créer un fichier de capacité de rôle :**

```
New-PSRoleCapabilityFile -Path "C:\Program Files\WindowsPowerShell\Modules\HyperVJEA\RoleCapabilities\HVOperator.psrc" -VisibleCmdl
```

REMÉDIATION :
1. **Créer la configuration de session :**

```
New-PSSessionConfigurationFile -Path "C:\JEA\HyperVJEA.pssc" -SessionType RestrictedRemoteServer -RoleDefinitions @{ 'DOMAIN\HV-Ope
Register-PSSessionConfiguration -Name "HyperVJEA" -Path "C:\JEA\HyperVJEA.pssc"
```

VALEUR PAR DÉFAUT :
JEA non configuré

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

2.3.2 *PAW (Privileged Access Workstation) pour l'administration Hyper-V*

DESCRIPTION :
L'administration de l'hôte Hyper-V doit être effectuée exclusivement depuis des postes d'administration sécurisés (PAW — Privileged Access Workstations). Les PAW sont des postes dédiés, durcis et isolés utilisés uniquement pour les tâches d'administration. Cette approche protège les identifiants d'administration contre les keyloggers, malwares et attaques man-in-the-middle présents sur les postes de travail standard.

```
# Vérifier les restrictions de connexion RDP/WinRM par adresse IP source
Get-NetFirewallRule -DisplayName "*Remote Desktop*" | Get-NetFirewallAddressFilter | Select-Object RemoteAddress
Get-NetFirewallRule -DisplayName "*Windows Remote Management*" | Get-NetFirewallAddressFilter | Select-Object RemoteAddress

# Vérifier les GPO de restriction de connexion
Get-ItemProperty "HKLM:\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" -Name UserAuthentication

# Vérifier les dernières connexions d'administration
Get-WinEvent -FilterHashtable @{LogName='Security'; Id=4624; StartTime=(Get-Date).AddDays(-7)} | Where-Object { $_.Properties[8].Va
```

REMÉDIATION :
1. Déployer des PAW dédiées pour l'administration Hyper-V
2. Restreindre les connexions WinRM/RDP aux seules adresses IP des PAW
3. **GPO :** Stratégie > Droits d'utilisateur > Autoriser l'ouverture de session via les services Bureau à distance

VALEUR PAR DÉFAUT :
Aucune restriction de source de connexion

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

2.4.1 *WinRM configuré avec HTTPS et certificat*

DESCRIPTION :
Windows Remote Management (WinRM), utilisé pour l'administration à distance d'Hyper-V via PowerShell Remoting, doit être configuré pour utiliser HTTPS (port 5986) avec un certificat TLS valide au lieu du HTTP non chiffré (port 5985). Le trafic WinRM en clair expose les identifiants d'administration et les commandes PowerShell sensibles à l'interception réseau.

```
# Vérifier les listeners WinRM
winrm enumerate winrm/config/Listener

# Vérifier si HTTPS est configuré
Get-WSManInstance -ResourceURI winrm/config/Listener -Enumerate | Select-Object Transport, Port, CertificateThumbprint

# Vérifier que HTTP est désactivé
Get-Item WSMan:\localhost\Listener\* | Select-Object Name, @{N='Transport';E={$_.Transport}}

# Vérifier le certificat utilisé
$listener = Get-WSManInstance -ResourceURI winrm/config/Listener -Enumerate | Where-Object { $_.Transport -eq "HTTPS" }
if ($listener.CertificateThumbprint) {
    Get-ChildItem Cert:\LocalMachine\My | Where-Object Thumbprint -eq $listener.CertificateThumbprint | Select-Object Subject, NotA
}
```

AUDIT :
- **Valeur attendue :** Listener HTTPS actif avec certificat valide, Listener HTTP désactivé ou restreint

REMÉDIATION :
1. **PowerShell :**

```
# Créer un listener HTTPS WinRM
$cert = Get-ChildItem Cert:\LocalMachine\My | Where-Object { $_.Subject -like "*$env:COMPUTERNAME*" -and $_.EnhancedKeyUsageList.Ob
New-WSManInstance -ResourceURI winrm/config/Listener -SelectorSet @{Address="*";Transport="HTTPS"} -ValueSet @{CertificateThumbprin

# Supprimer le listener HTTP
Remove-WSManInstance -ResourceURI winrm/config/Listener -SelectorSet @{Address="*";Transport="HTTP"}
```

VALEUR PAR DÉFAUT :
WinRM HTTP (port 5985) activé

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

2.4.2 *RDP sécurisé avec NLA et chiffrement élevé*

DESCRIPTION :
Si RDP est activé sur l'hôte Hyper-V (idéalement uniquement en mode Server Core avec accès restreint), il doit être sécurisé avec NLA (Network Level Authentication), un niveau de chiffrement élevé (High), et TLS 1.2 comme couche de sécurité. RDP sans NLA est vulnérable aux attaques BlueKeep et autres exploits ciblant le protocole.

```
# Vérifier NLA
Get-ItemProperty "HKLM:\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" -Name UserAuthentication, SecurityLay

# Vérifier la version TLS
Get-ItemProperty "HKLM:\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" -Name SecurityLayer

# Vérifier si RDP est activé
Get-ItemProperty "HKLM:\SYSTEM\CurrentControlSet\Control\Terminal Server" -Name fDenyTSConnections
```

AUDIT :

- **Valeur attendue :** UserAuthentication = 1 (NLA), SecurityLayer = 2 (TLS), MinEncryptionLevel = 3 (High)

REMÉDIATION :

1. **GPO :** Configuration ordinateur > Stratégies > Modèles d'administration > Composants Windows > Services Bureau à distance > Hôte de session > Sécurité
2. **PowerShell :**

```
Set-ItemProperty "HKLM:\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" -Name UserAuthentication -Value 1
Set-ItemProperty "HKLM:\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" -Name SecurityLayer -Value 2
Set-ItemProperty "HKLM:\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" -Name MinEncryptionLevel -Value 3
```

VALEUR PAR DÉFAUT :
NLA activé, SecurityLayer = 1 (Negotiate)

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

2.4.3 *SSH désactivé ou sécurisé si utilisé*

DESCRIPTION :
OpenSSH Server, s'il est installé sur l'hôte Hyper-V, doit être soit désactivé s'il n'est pas nécessaire, soit sécurisé avec une authentification par clé, des algorithmes de chiffrement forts et des restrictions d'accès. SSH n'est généralement pas nécessaire sur un hôte Hyper-V où WinRM/PowerShell Remoting est le protocole d'administration privilégié.

```
# Vérifier si OpenSSH Server est installé
Get-WindowsCapability -Online | Where-Object Name -like "*OpenSSH.Server*" | Select-Object Name, State

# Vérifier le service
Get-Service sshd -ErrorAction SilentlyContinue | Select-Object Name, Status, StartType

# Si SSH est actif, vérifier la configuration
Get-Content "C:\ProgramData\ssh\sshd_config" -ErrorAction SilentlyContinue | Select-String -Pattern "PasswordAuthentication|PermitR
```

REMÉDIATION :

1. **Si non requis :**

```
Stop-Service sshd -Force
Set-Service sshd -StartupType Disabled
Remove-WindowsCapability -Online -Name OpenSSH.Server~~~~0.0.1.0
```

REMÉDIATION :

1. **Si requis :** Configurer l'authentification par clé et désactiver l'authentification par mot de passe

VALEUR PAR DÉFAUT :
OpenSSH Server non installé par défaut

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

2.5.1 *Audit des connexions réussies et échouées*

DESCRIPTION :
L'audit des tentatives de connexion réussies et échouées doit être activé sur l'hôte Hyper-V. Les événements de connexion (Event ID 4624, 4625, 4634, 4647, 4648) fournissent une traçabilité complète des accès à l'infrastructure de virtualisation et permettent la détection de tentatives d'intrusion, de mouvements latéraux et d'abus de privilèges.

```
# Vérifier la politique d'audit de connexion
auditpol /get /subcategory:"Logon" /subcategory:"Logoff" /subcategory:"Special Logon" /subcategory:"Account Lockout"

# Vérifier les événements récents
Get-WinEvent -FilterHashtable @{LogName='Security'; Id=@(4624,4625); StartTime=(Get-Date).AddHours(-24)} | Group-Object Id | Select
```

AUDIT :

- **Valeur attendue :** Success and Failure pour Logon, Special Logon, Account Lockout

REMÉDIATION :

1. **PowerShell :**

```
auditpol /set /subcategory:"Logon" /success:enable /failure:enable
auditpol /set /subcategory:"Special Logon" /success:enable
auditpol /set /subcategory:"Account Lockout" /success:enable /failure:enable
```

VALEUR PAR DÉFAUT :
Success uniquement pour Logon

Preuve d'audit :

```
| Résultat | _____________________________________________ |
| Capture  | ☐ Oui ☐ Non                                   |
| Note     | _____________________________________________ |
```

2.5.2 *Audit de l'utilisation des privilèges élevés*

DESCRIPTION :
L'utilisation des privilèges sensibles sur l'hôte Hyper-V doit être auditée. Les événements 4672 (Special Privileges Assigned) et 4673 (Sensitive Privilege Use) permettent de détecter l'utilisation de privilèges élevés tels que SeDebugPrivilege, SeTakeOwnershipPrivilege ou SeBackupPrivilege, qui pourraient être utilisés pour compromettre l'hyperviseur ou accéder aux données des VMs.

```
# Vérifier l'audit des privilèges
auditpol /get /subcategory:"Sensitive Privilege Use" /subcategory:"Non Sensitive Privilege Use"

# Vérifier les événements récents de privilèges spéciaux
Get-WinEvent -FilterHashtable @{LogName='Security'; Id=4672; StartTime=(Get-Date).AddDays(-1)} | Select-Object -First 10 TimeCreate
```

REMÉDIATION :

1. **PowerShell :**

```
auditpol /set /subcategory:"Sensitive Privilege Use" /success:enable /failure:enable
```

VALEUR PAR DÉFAUT :
Non configuré

Preuve d'audit :

```
| Résultat | _____________________________________________ |
| Capture  | ☐ Oui ☐ Non                                   |
| Note     | _____________________________________________ |
```

2.5.3 *Droits d'utilisateur restrictifs (User Rights Assignment)*

DESCRIPTION :
Les droits d'utilisateur Windows (User Rights Assignment) doivent être configurés de manière restrictive sur l'hôte Hyper-V. Les droits critiques comme "Act as part of the operating system" (SeTcbPrivilege), "Debug programs" (SeDebugPrivilege), "Take ownership" (SeTakeOwnershipPrivilege) doivent être limités aux seuls comptes strictement nécessaires.

```
# Exporter les droits d'utilisateur
secedit /export /cfg C:\secpol.cfg
Select-String -Path C:\secpol.cfg -Pattern "SeTcbPrivilege|SeDebugPrivilege|SeTakeOwnershipPrivilege|SeBackupPrivilege|SeRestorePri
Remove-Item C:\secpol.cfg

# Vérifier qui peut se connecter à distance
secedit /export /cfg C:\secpol.cfg
Select-String -Path C:\secpol.cfg -Pattern "SeRemoteInteractiveLogonRight|SeNetworkLogonRight|SeDenyNetworkLogonRight"
Remove-Item C:\secpol.cfg
```

REMÉDIATION :

1. **GPO :** Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Attribution des droits utilisateur
2. Appliquer les valeurs recommandées par le CIS Benchmark

VALEUR PAR DÉFAUT :
Valeurs Windows par défaut

Preuve d'audit :

```
| Résultat | _____________________________________________ |
| Capture  | ☐ Oui ☐ Non                                   |
| Note     | _____________________________________________ |
```

2.5.4 *Revue périodique des accès administratifs*

DESCRIPTION :
Une revue périodique (au minimum trimestrielle) des accès administratifs à l'infrastructure Hyper-V doit être effectuée. Cette revue couvre les membres des groupes Hyper-V Administrators, Administrators locaux, les rôles SCVMM, les endpoints JEA et les comptes de service. Toute permission non justifiée doit être révoquée immédiatement.

```
# Script de revue des accès
$report = @()
$report += "=== Hyper-V Administrators ==="
$report += Get-LocalGroupMember -Group "Hyper-V Administrators" | Format-Table | Out-String
$report += "=== Local Administrators ==="
$report += Get-LocalGroupMember -Group "Administrateurs" | Format-Table | Out-String
$report += "=== Dernière revue ==="
# Vérifier si un processus de revue est documenté

$report | Out-File "C:\Audit\AccessReview-$(Get-Date -Format 'yyyyMMdd').txt"
```

AUDIT :

- **Valeur attendue :** Revue documentée datant de moins de 90 jours

REMÉDIATION :

1. Mettre en place un processus de revue trimestrielle
2. Documenter chaque revue avec les actions correctives
3. Automatiser la génération de rapports d'accès

VALEUR PAR DÉFAUT :
Aucune revue automatisée

Preuve d'audit :

```
| Résultat | _____________________________________________ |
| Capture  | ☐ Oui ☐ Non                                   |
| Note     | _____________________________________________ |
```

2.6.1 *MFA pour l'administration Hyper-V*

DESCRIPTION :
L'authentification multi-facteurs (MFA) doit être requise pour toute connexion administrative à l'hôte Hyper-V. Le MFA protège contre la compromission des identifiants par phishing, keylogging, pass-the-hash ou fuite de mots de passe. Les solutions incluent les smart cards, Windows Hello for Business, Azure MFA avec NPS Extension, ou des solutions tierces (Duo, RSA SecurID).

```
# Vérifier si les smart cards sont requises
Get-ADUser -Filter { SmartcardLogonRequired -eq $true } | Where-Object { $_.MemberOf -like "*Hyper-V*" } -ErrorAction SilentlyConti

# Vérifier Windows Hello for Business
Get-ItemProperty "HKLM:\SOFTWARE\Policies\Microsoft\PassportForWork" -ErrorAction SilentlyContinue

# Vérifier NPS/RADIUS pour MFA
Get-Service IAS -ErrorAction SilentlyContinue | Select-Object Name, Status
```

REMÉDIATION :

1. Déployer Windows Hello for Business ou smart cards pour les administrateurs Hyper-V
2. Configurer Azure MFA avec NPS Extension pour RDP/WinRM
3. Exiger les smart cards via GPO pour les comptes administratifs

VALEUR PAR DÉFAUT :
MFA non configuré

Preuve d'audit :

```
| Résultat | _____________________________________________ |
| Capture  | ☐ Oui ☐ Non                                   |
| Note     | _____________________________________________ |
```

VALEUR PAR DÉFAUT :
═══

3.0 — ISOLATION DES MACHINES VIRTUELLES

3.1.1 *Isolation mémoire entre machines virtuelles*

DESCRIPTION :
L'hyperviseur Hyper-V doit garantir une isolation mémoire stricte entre les machines virtuelles. Chaque VM doit disposer d'un espace mémoire dédié et inaccessible aux autres VMs. L'isolation mémoire est assurée par le SLAT (Second Level Address Translation) via Intel EPT ou AMD RVI. Les attaques par canal auxiliaire (side-channel) comme Spectre, Meltdown et L1TF ciblent spécifiquement cette isolation.

```
# Vérifier la configuration mémoire de chaque VM
Get-VM | Select-Object Name, MemoryAssigned, MemoryStartup, MemoryMinimum, MemoryMaximum, DynamicMemoryEnabled

# Vérifier SLAT (Second Level Address Translation)
Get-WmiObject -Class Win32_Processor | Select-Object Name, SecondLevelAddressTranslationExtensions

# Vérifier les protections contre les canaux auxiliaires
Get-ItemProperty "HKLM:\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management" -Name FeatureSettingsOverride, FeatureS

# Vérifier l'état des mitigations
Get-SpeculationControlSettings 2>$null
```

AUDIT :

- **Valeur attendue :** SLAT = True, mitigations contre Spectre/Meltdown activées

REMÉDIATION :

1. Vérifier que le CPU supporte SLAT (Intel EPT / AMD RVI)
2. Appliquer les correctifs contre les attaques par canal auxiliaire
3. **PowerShell :**

```
# Activer les mitigations spectre/meltdown pour l'hôte
Set-ItemProperty "HKLM:\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management" -Name FeatureSettingsOverride -Value 72
Set-ItemProperty "HKLM:\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management" -Name FeatureSettingsOverrideMask -Valu
```

VALEUR PAR DÉFAUT :
Isolation mémoire native de l'hyperviseur activée, mitigations side-channel dépendent des correctifs

Preuve d'audit :

```
| Résultat | _____________________________________________ |
| Capture  | ☐ Oui ☐ Non                                   |
| Note     | _____________________________________________ |
```

3.1.2 *Mémoire dynamique — configuration sécurisée*

DESCRIPTION :
Si la mémoire dynamique (Dynamic Memory) est activée sur les VMs Hyper-V, les paramètres de mémoire minimale, maximale et de tampon doivent être configurés de manière à éviter qu'une VM ne puisse consommer toute la mémoire disponible de l'hôte, provoquant un déni de service pour les autres VMs. La mémoire minimale doit être suffisante pour le fonctionnement de base de la VM, et la mémoire maximale doit être plafonnée.

```
# Vérifier la configuration mémoire dynamique de toutes les VMs
Get-VM | Where-Object { $_.DynamicMemoryEnabled -eq $true } | Select-Object Name, MemoryMinimum, MemoryMaximum, MemoryStartup, @{N=

# Calculer la mémoire totale maximale possible vs mémoire physique disponible
$totalMaxMemory = (Get-VM | Where-Object DynamicMemoryEnabled | Measure-Object -Property MemoryMaximum -Sum).Sum
$physicalMemory = (Get-CimInstance Win32_PhysicalMemory | Measure-Object -Property Capacity -Sum).Sum
Write-Output "Ratio max allocable/physique: $([math]::Round($totalMaxMemory/$physicalMemory*100,2))%"
```

AUDIT :

- **Valeur attendue :** Ratio max/physique < 150%, mémoire minimale adéquate pour chaque VM

REMÉDIATION :

1. **PowerShell :**

```
# Configurer les limites de mémoire dynamique
Set-VM -Name "VMName" -DynamicMemory -MemoryMinimumBytes 512MB -MemoryMaximumBytes 4GB -MemoryStartupBytes 1GB
```

REMÉDIATION :

1. **Hyper-V Manager :** Paramètres de la VM > Mémoire > Configurer les valeurs min/max

VALEUR PAR DÉFAUT :
Mémoire statique (Dynamic Memory désactivée)

Preuve d'audit :

```
| Résultat | _____________________________________________ |
| Capture  | ☐ Oui ☐ Non                                   |
| Note     | _____________________________________________ |
```

3.2.1 *Limites de ressources CPU par VM*

DESCRIPTION :
Des limites de ressources CPU doivent être configurées pour chaque VM afin d'empêcher une VM compromise ou défaillante de monopoliser les ressources CPU de l'hôte. Hyper-V permet de configurer des poids relatifs (Relative Weight), des réservations minimales (Reserve) et des limites maximales (Limit) pour chaque processeur virtuel.

```
# Vérifier la configuration CPU de chaque VM
Get-VM | Get-VMProcessor | Select-Object VMName, Count, Maximum, Reserve, RelativeWeight, CompatibilityForMigrationEnabled, Compati

# Vérifier le ratio vCPU/pCPU
$totalVCPU = (Get-VM | Get-VMProcessor | Measure-Object -Property Count -Sum).Sum
$physicalCPU = (Get-CimInstance Win32_Processor | Measure-Object -Property NumberOfLogicalProcessors -Sum).Sum
Write-Output "Ratio vCPU/pCPU: $totalVCPU`:$physicalCPU ($([math]::Round($totalVCPU/$physicalCPU,2)):1)"
```

AUDIT :

- **Valeur attendue :** Maximum < 100 pour les VMs non critiques, ratio vCPU/pCPU < 8:1

REMÉDIATION :

1. **PowerShell :**

```
# Configurer les limites CPU
Set-VMProcessor -VMName "VMName" -Maximum 80 -Reserve 10 -RelativeWeight 100
```

REMÉDIATION :

1. **Hyper-V Manager :** Paramètres VM > Processeur > Contrôle des ressources

VALEUR PAR DÉFAUT :
Maximum = 100 (pas de limite), Reserve = 0, Weight = 100

Preuve d'audit :

```
| Résultat | _____________________________________________ |
| Capture  | ☐ Oui ☐ Non                                   |
| Note     | _____________________________________________ |
```

3.2.2 *Limites de bande passante réseau par VM*

DESCRIPTION :
Des limites de bande passante réseau doivent être configurées sur les adaptateurs réseau virtuels de chaque VM pour empêcher une VM de saturer la bande passante réseau de l'hôte. Hyper-V permet de configurer des limites minimales et maximales de bande passante via le QoS (Quality of Service) réseau.

```
# Vérifier la configuration QoS réseau de chaque VM
Get-VM | Get-VMNetworkAdapter | Select-Object VMName, Name, BandwidthSetting, @{N='MinBandwidth';E={$_.BandwidthSetting.MinimumBand

# Vérifier le mode de bande passante du switch virtuel
Get-VMSwitch | Select-Object Name, BandwidthReservationMode
```

REMÉDIATION :

1. **PowerShell :**

```
# Configurer le QoS réseau sur un switch
Set-VMSwitch -Name "vSwitch1" -DefaultFlowMinimumBandwidthAbsolute 100000000 -DefaultFlowMinimumBandwidthWeight 50

# Configurer par adaptateur VM
Set-VMNetworkAdapter -VMName "VMName" -MaximumBandwidth 1000000000 -MinimumBandwidthAbsolute 100000000
```

VALEUR PAR DÉFAUT :
Aucune limite de bande passante

Preuve d'audit :

```
| Résultat | _____________________________________________ |
| Capture  | ☐ Oui ☐ Non                                   |
| Note     | _____________________________________________ |
```

3.2.3 *Limites d'IOPS de stockage par VM*

DESCRIPTION :
Des limites d'IOPS (Input/Output Operations Per Second) de stockage doivent être configurées pour les disques virtuels de chaque VM via Storage QoS. Cela empêche une VM de saturer le sous-système de stockage de l'hôte, ce qui affecterait les performances de toutes les autres VMs. Storage QoS est particulièrement important dans les environnements multi-locataires.

```
# Vérifier les politiques Storage QoS
Get-StorageQosPolicy -ErrorAction SilentlyContinue | Select-Object Name, PolicyType, MinimumIops, MaximumIops, Status

# Vérifier les flux Storage QoS
Get-StorageQosFlow -ErrorAction SilentlyContinue | Select-Object InitiatorName, PolicyId, MinimumIOPS, MaximumIOPS, StorageNodeIOPS

# Vérifier si Storage QoS est activé sur le cluster
Get-ClusterResource -ErrorAction SilentlyContinue | Where-Object ResourceType -eq "Storage QoS Policy Manager"
```

REMÉDIATION :

1. **PowerShell :**

```
# Créer une politique Storage QoS
New-StorageQosPolicy -Name "Standard-VM-Policy" -PolicyType Dedicated -MinimumIops 100 -MaximumIops 1000

# Appliquer la politique à un disque VM
Get-VM "VMName" | Get-VMHardDiskDrive | Set-VMHardDiskDrive -QoSPolicyID (Get-StorageQosPolicy -Name "Standard-VM-Policy").PolicyId
```

VALEUR PAR DÉFAUT :
Storage QoS non configuré
Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

3.3.1 *Integration Services — inventaire et contrôle*

DESCRIPTION :
Les Integration Services (services d'intégration) Hyper-V constituent des canaux de communication entre l'hôte et la VM invitée. Chaque service d'intégration activé augmente la surface d'attaque en créant un canal potentiel d'évasion de VM. Seuls les services d'intégration strictement nécessaires au fonctionnement de chaque VM doivent être activés. Les services non requis (Guest Service Interface, Data Exchange, etc.) doivent être désactivés.

```
# Lister tous les Integration Services pour chaque VM
Get-VM | ForEach-Object {
    $vm = $_
    Get-VMIntegrationService -VMName $vm.Name | Select-Object @{N='VM';E={$vm.Name}}, Name, Enabled, PrimaryStatusDescription
}

# Résumé par service
Get-VM | ForEach-Object {
    $vm = $_
    Get-VMIntegrationService -VMName $vm.Name | Where-Object Enabled | Select-Object @{N='VM';E={$vm.Name}}, Name
} | Group-Object Name | Select-Object Name, Count
```

AUDIT :

- **Valeur attendue :** Seuls les services nécessaires sont activés (Heartbeat, Time Synchronization minimum)

REMÉDIATION :

1. **PowerShell :**

```
# Désactiver les services d'intégration non nécessaires
Disable-VMIntegrationService -VMName "VMName" -Name "Guest Service Interface"
Disable-VMIntegrationService -VMName "VMName" -Name "Data Exchange"
Disable-VMIntegrationService -VMName "VMName" -Name "Shutdown"
```

REMÉDIATION :

1. **Hyper-V Manager :** Paramètres VM > Integration Services > Décocher les services non nécessaires

VALEUR PAR DÉFAUT :
Tous les services d'intégration activés
Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

3.3.2 *Time Synchronization Service — configuration sécurisée*

DESCRIPTION :
Le service de synchronisation temporelle Hyper-V (Time Synchronization Service) permet à l'hôte de fournir l'heure aux VMs invitées. Pour les VMs jointes à un domaine Active Directory, ce service peut entrer en conflit avec le service W32Time du domaine. Il est recommandé de désactiver ce service d'intégration sur les VMs jointes à un domaine et de laisser la synchronisation NTP du domaine gérer l'heure.

```
# Vérifier le service Time Synchronization pour chaque VM
Get-VM | ForEach-Object {
    Get-VMIntegrationService -VMName $_.Name -Name "Time Synchronization" | Select-Object @{N='VM';E={$_.VMName}}, Enabled
}
```

AUDIT :

- **Valeur attendue :** Désactivé pour les VMs jointes au domaine, Activé pour les VMs standalone

REMÉDIATION :

1. **PowerShell :**

```
# Désactiver pour les VMs de domaine
Disable-VMIntegrationService -VMName "DC01" -Name "Time Synchronization"
Disable-VMIntegrationService -VMName "SRV-APP01" -Name "Time Synchronization"
```

VALEUR PAR DÉFAUT :
Activé

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

3.3.3 *Data Exchange (KVP) — désactivation si non requis*

DESCRIPTION :
Le service Data Exchange (Key-Value Pair Exchange) permet l'échange de données entre l'hôte et la VM via des paires clé-valeur dans le registre. Ce canal peut être utilisé pour l'exfiltration de données ou comme canal de commande et contrôle (C2). Il doit être désactivé sur les VMs qui n'en ont pas besoin, en particulier les VMs exposées à Internet ou les VMs hébergeant des données sensibles.

```
# Vérifier le service Data Exchange
Get-VM | ForEach-Object {
    Get-VMIntegrationService -VMName $_.Name -Name "Key-Value Pair Exchange" | Select-Object @{N='VM';E={$_.VMName}}, Enabled
}

# Vérifier les données KVP existantes
Get-VM | ForEach-Object {
    $vm = $_
    $kvp = Get-WmiObject -Namespace "root\virtualization\v2" -Query "SELECT * FROM Msvm_KvpExchangeComponent WHERE SystemName='$($v
    if ($kvp) { Write-Output "VM: $($vm.Name), KVP Items: $($kvp.GuestExchangeItems.Count)" }
}
```

REMÉDIATION :

1. **PowerShell :**

```
Disable-VMIntegrationService -VMName "VMName" -Name "Key-Value Pair Exchange"
```

VALEUR PAR DÉFAUT :
Activé

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

3.3.4 *Heartbeat Service — surveillance de l'état des VMs*

DESCRIPTION :
Le service Heartbeat permet à l'hôte de détecter si la VM est en cours d'exécution et responsive. Ce service est généralement requis pour le monitoring et la haute disponibilité. Il est recommandé de le maintenir activé sur toutes les VMs pour la surveillance de santé, mais les alertes de perte de heartbeat doivent être configurées.

```
# Vérifier le service Heartbeat
Get-VM | ForEach-Object {
    Get-VMIntegrationService -VMName $_.Name -Name "Heartbeat" | Select-Object @{N='VM';E={$_.VMName}}, Enabled, PrimaryStatusDescr
}
```

AUDIT :

- **Valeur attendue :** Activé sur toutes les VMs, PrimaryStatusDescription = "OK"

REMÉDIATION :

1. **PowerShell :**

```
Enable-VMIntegrationService -VMName "VMName" -Name "Heartbeat"
```

VALEUR PAR DÉFAUT :
Activé

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

3.3.5 *Guest Service Interface — désactivation recommandée*

DESCRIPTION :
Le service Guest Service Interface permet la copie de fichiers entre l'hôte et la VM invitée sans réseau (via la commande Copy-VMFile). Ce canal constitue un risque de sécurité important car il peut être utilisé pour l'exfiltration de données ou le déploiement d'outils malveillants dans la VM. Ce service doit être désactivé par défaut et activé temporairement uniquement en cas de besoin opérationnel documenté.

```
# Vérifier le service Guest Service Interface
Get-VM | ForEach-Object {
    Get-VMIntegrationService -VMName $_.Name -Name "Guest Service Interface" | Select-Object @{N='VM';E={$_.VMName}}, Enabled
}
```

AUDIT :

- **Valeur attendue :** Désactivé sur toutes les VMs

REMÉDIATION :

1. **PowerShell :**

```
Get-VM | ForEach-Object {
    Disable-VMIntegrationService -VMName $_.Name -Name "Guest Service Interface"
}
```

VALEUR PAR DÉFAUT :
Désactivé (depuis Windows Server 2016+)

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

3.3.6 *VSS (Volume Shadow Copy) Integration Service*

DESCRIPTION :
Le service d'intégration VSS (Volume Shadow Copy Service) permet la sauvegarde cohérente des VMs en quiescent le système de fichiers invité avant la prise de snapshot. Ce service est essentiel pour les sauvegardes cohérentes et doit rester activé sur les VMs nécessitant une sauvegarde applicativement cohérente.

```
# Vérifier le service VSS
Get-VM | ForEach-Object {
    Get-VMIntegrationService -VMName $_.Name -Name "VSS" | Select-Object @{N='VM';E={$_.VMName}}, Enabled
}
```

AUDIT :

- **Valeur attendue :** Activé sur les VMs avec sauvegarde requise

REMÉDIATION :

1. **PowerShell :**

```
Enable-VMIntegrationService -VMName "VMName" -Name "VSS"
```

VALEUR PAR DÉFAUT :
Activé

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

3.4.1 *Enhanced Session Mode — restriction d'utilisation*

DESCRIPTION :
Le mode de session améliorée (Enhanced Session Mode) permet des fonctionnalités avancées lors de la connexion à une VM via VMConnect, notamment le partage du presse-papiers, la redirection des imprimantes, la redirection USB et le transfert de fichiers par glisser-déposer. Ces fonctionnalités créent des canaux de communication entre l'hôte et la VM qui peuvent être utilisés pour l'exfiltration de données. L'Enhanced Session Mode doit être désactivé sur les hôtes en production.

```
# Vérifier si Enhanced Session Mode est activé au niveau de l'hôte
Get-VMHost | Select-Object EnableEnhancedSessionMode

# Vérifier la politique Enhanced Session Mode
Get-ItemProperty "HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Virtualization" -Name AllowEnhancedSessionMode -ErrorAction Si
```

AUDIT :

- **Valeur attendue :** EnableEnhancedSessionMode = False (en production)

REMÉDIATION :

1. **PowerShell :**

```
Set-VMHost -EnableEnhancedSessionMode $false
```

REMÉDIATION :

1. **Hyper-V Manager :** Hyper-V Settings > Enhanced Session Mode Policy > Décocher "Allow enhanced session mode"

VALEUR PAR DÉFAUT :
Activé

Preuve d'audit :

```
| Résultat | _____________________________________________ |
| Capture  | ☐ Oui ☐ Non                                   |
| Note     | _____________________________________________ |
```

3.4.2 *Redirection du presse-papiers désactivée*

DESCRIPTION :
La redirection du presse-papiers entre l'hôte et les VMs doit être désactivée pour empêcher la fuite de données sensibles (mots de passe, données confidentielles) via le copier-coller entre environnements de sécurité différents. Cette mesure est liée à la désactivation de l'Enhanced Session Mode.

```
# Vérifier Enhanced Session Mode (contrôle le presse-papiers)
Get-VMHost | Select-Object EnableEnhancedSessionMode

# Vérifier la GPO de redirection du presse-papiers RDP
Get-ItemProperty "HKLM:\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services" -Name fDisableClip -ErrorAction SilentlyContinue
```

AUDIT :

- **Valeur attendue :** Enhanced Session Mode désactivé ou fDisableClip = 1

REMÉDIATION :

1. Désactiver Enhanced Session Mode (voir contrôle 3.4.1)
2. **GPO :** Configuration ordinateur > Modèles d'administration > Composants Windows > Services Bureau à distance > Redirection périphériques > Ne pas autoriser la redirection du Presse-papiers

VALEUR PAR DÉFAUT :
Presse-papiers activé avec Enhanced Session Mode

Preuve d'audit :

```
| Résultat | _____________________________________________ |
| Capture  | ☐ Oui ☐ Non                                   |
| Note     | _____________________________________________ |
```

3.5.1 *Discrete Device Assignment (DDA) — contrôle strict*

DESCRIPTION :
Le Discrete Device Assignment (DDA) permet l'assignation directe de périphériques PCIe (GPU, NVMe, cartes réseau) à une VM, contournant l'hyperviseur pour l'accès au périphérique. DDA affaiblit considérablement l'isolation car la VM obtient un accès DMA direct au matériel, ce qui peut potentiellement permettre une évasion de VM via des vulnérabilités dans le firmware du périphérique. DDA ne doit être utilisé que pour des cas d'usage spécifiques et documentés.

```
# Vérifier les périphériques assignés en DDA
Get-VM | ForEach-Object {
    $vm = $_
    Get-VMAssignableDevice -VMName $vm.Name -ErrorAction SilentlyContinue | Select-Object @{N='VM';E={$vm.Name}}, InstanceID, Locat
}

# Lister les périphériques démontés de l'hôte (potentiellement assignés)
Get-PnpDevice | Where-Object { $_.Status -eq 'Error' -or $_.Status -eq 'Unknown' } | Select-Object Class, FriendlyName, InstanceId,
```

AUDIT :

- **Valeur attendue :** Aucun périphérique DDA assigné (ou liste documentée et justifiée)

REMÉDIATION :

1. **PowerShell :**

```
# Retirer l'assignation DDA d'une VM
Remove-VMAssignableDevice -VMName "VMName" -InstanceID "PCIe-Device-ID"
```

REMÉDIATION :

1. Documenter et justifier chaque utilisation de DDA
2. S'assurer que l'IOMMU est activé si DDA est utilisé

VALEUR PAR DÉFAUT :
Aucun périphérique DDA assigné

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

3.5.2 *RemoteFX vGPU — désactivation (déprécié et vulnérable)*

DESCRIPTION :
RemoteFX vGPU est une technologie dépréciée qui permettait le partage de GPU entre VMs. Microsoft a désactivé cette fonctionnalité en raison de vulnérabilités critiques de sécurité (CVE-2020-1036, CVE-2020-1032, CVE-2020-1040, CVE-2020-1041, CVE-2020-1043) permettant l'évasion de VM et l'exécution de code à distance. RemoteFX vGPU ne doit jamais être activé.

```
# Vérifier si RemoteFX vGPU est configuré sur des VMs
Get-VM | Get-VMRemoteFx3dVideoAdapter -ErrorAction SilentlyContinue

# Vérifier si le rôle RemoteFX est installé
Get-WindowsFeature RDS-Virtualization -ErrorAction SilentlyContinue | Select-Object Name, Installed

# Vérifier les GPOs liées
Get-ItemProperty "HKLM:\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services" -Name fEnableRemoteFXAdvancedRemoteApp -ErrorActi
```

AUDIT :

- **Valeur attendue :** Aucun adaptateur RemoteFX vGPU, fonctionnalité non installée

REMÉDIATION :

1. **PowerShell :**

```
# Supprimer RemoteFX vGPU de toutes les VMs
Get-VM | Get-VMRemoteFx3dVideoAdapter -ErrorAction SilentlyContinue | Remove-VMRemoteFx3dVideoAdapter

# Désinstaller la fonctionnalité si installée
Remove-WindowsFeature RDS-Virtualization
```

VALEUR PAR DÉFAUT :
Déprécié et désactivé dans Windows Server 2025

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

3.6.1 *Fichiers de configuration VM protégés (ACL)*

DESCRIPTION :
Les fichiers de configuration des machines virtuelles (.vmcx, .vmrs, .vmgs) doivent être protégés par des ACL restrictives. Seuls le compte SYSTEM, les administrateurs Hyper-V et le service VMMS doivent avoir accès à ces fichiers. Des permissions trop ouvertes permettraient à un attaquant de modifier la configuration des VMs, d'extraire des données de mémoire (fichiers .vmrs) ou de compromettre les VMs blindées.

```
# Vérifier les ACL sur les répertoires de VMs
Get-VM | ForEach-Object {
    $vmPath = $_.Path
    if (Test-Path $vmPath) {
        Write-Output "=== VM: $($_.Name) - Path: $vmPath ==="
        Get-Acl $vmPath | Select-Object -ExpandProperty Access | Select-Object IdentityReference, FileSystemRights, AccessControlTy
    }
}

# Vérifier les ACL sur le répertoire par défaut des VMs
$defaultPath = (Get-VMHost).VirtualMachinePath
Get-Acl $defaultPath | Select-Object -ExpandProperty Access | Format-Table IdentityReference, FileSystemRights, AccessControlType
```

AUDIT :

- **Valeur attendue :** Accès limité à SYSTEM, BUILTIN\Administrators, NT VIRTUAL MACHINE\Virtual Machines

REMÉDIATION :

1. **PowerShell :**

```
$vmPath = "D:\VMs"
$acl = Get-Acl $vmPath
$acl.SetAccessRuleProtection($true, $false) # Désactiver l'héritage
$acl.Access | ForEach-Object { $acl.RemoveAccessRule($_) }
$acl.AddAccessRule((New-Object System.Security.AccessControl.FileSystemAccessRule("SYSTEM","FullControl","ContainerInherit,ObjectIn
$acl.AddAccessRule((New-Object System.Security.AccessControl.FileSystemAccessRule("BUILTIN\Administrators","FullControl","Container
$acl.AddAccessRule((New-Object System.Security.AccessControl.FileSystemAccessRule("NT VIRTUAL MACHINE\Virtual Machines","FullContro
Set-Acl $vmPath $acl
```

VALEUR PAR DÉFAUT :
Permissions héritées du volume parent

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

3.6.2 *Génération de VM (Generation 2) requise*

DESCRIPTION :
Toutes les nouvelles VMs doivent être créées en Génération 2 (Generation 2) qui supporte Secure Boot UEFI, vTPM, et est requise pour les Shielded VMs. Les VMs de Génération 1 utilisent un BIOS émulé Legacy qui ne supporte pas les fonctionnalités de sécurité modernes comme le démarrage sécurisé. Les VMs de Génération 1 existantes doivent être migrées vers la Génération 2 lorsque possible.

```
# Vérifier la génération de chaque VM
Get-VM | Select-Object Name, Generation, State, Status | Sort-Object Generation

# Compter les VMs par génération
Get-VM | Group-Object Generation | Select-Object Name, Count

# Identifier les VMs Gen1 qui pourraient être migrées
Get-VM | Where-Object Generation -eq 1 | Select-Object Name, State, OperatingSystemShutdownEnabled
```

AUDIT :

- **Valeur attendue :** 100% des VMs en Génération 2

REMÉDIATION :

1. Créer les nouvelles VMs en Génération 2
2. Pour les VMs Gen1 existantes : recréer en Gen2 et migrer les données
3. **Note :** La conversion Gen1 vers Gen2 n'est pas supportée nativement — nécessite une recréation

VALEUR PAR DÉFAUT :
Choix lors de la création (Gen2 recommandé depuis Server 2016)

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

3.6.3 *Secure Boot activé sur les VMs*

DESCRIPTION :
Le Secure Boot UEFI doit être activé sur toutes les VMs de Génération 2. Le Secure Boot dans les VMs empêche le chargement de code non signé lors du démarrage, protégeant contre les bootkits et rootkits au niveau de la VM. Le template de Secure Boot doit correspondre à l'OS invité (MicrosoftWindows pour Windows, MicrosoftUEFICertificateAuthority pour Linux).

```
# Vérifier Secure Boot sur toutes les VMs Gen2
Get-VM | Where-Object Generation -eq 2 | Get-VMFirmware | Select-Object VMName, SecureBoot, SecureBootTemplate

# VMs Gen2 sans Secure Boot
Get-VM | Where-Object Generation -eq 2 | Get-VMFirmware | Where-Object SecureBoot -ne "On" | Select-Object VMName
```

AUDIT :

- **Valeur attendue :** SecureBoot = On, SecureBootTemplate adapté à l'OS

REMÉDIATION :

1. **PowerShell :**

```
# Activer Secure Boot (VM doit être arrêtée)
Set-VMFirmware -VMName "VMName" -EnableSecureBoot On -SecureBootTemplate MicrosoftWindows

# Pour les VMs Linux
Set-VMFirmware -VMName "LinuxVM" -EnableSecureBoot On -SecureBootTemplate MicrosoftUEFICertificateAuthority
```

REMÉDIATION :

1. **Hyper-V Manager :** Paramètres VM > Sécurité > Secure Boot

VALEUR PAR DÉFAUT :
Activé sur les VMs Gen2 Windows, désactivé par défaut sur les VMs Linux

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

VALEUR PAR DÉFAUT :
═══

4.0 — MACHINES VIRTUELLES BLINDÉES (SHIELDED VMs)

4.1.1 *Host Guardian Service (HGS) déployé et fonctionnel*

DESCRIPTION :
Le Host Guardian Service (HGS) est le composant central du Guarded Fabric qui fournit les services d'attestation et de protection de clé pour les hôtes Hyper-V. HGS vérifie l'intégrité et la configuration de chaque hôte avant de lui fournir les clés nécessaires au démarrage des Shielded VMs. HGS doit être déployé sur un cluster dédié, isolé du réseau de production, avec une haute disponibilité.

```
# Vérifier si HGS est configuré sur l'hôte
Get-HgsClientConfiguration | Select-Object IsHostGuarded, Mode, AttestationServerUrl, KeyProtectionServerUrl, AttestationStatus

# Vérifier l'état d'attestation
Get-HgsClientConfiguration | Select-Object AttestationStatus
# Valeurs : Passed, UnauthorizedHost, InsecureHostConfiguration, NotConfigured

# Sur le serveur HGS : vérifier le service
Get-HgsServer -ErrorAction SilentlyContinue | Select-Object AttestationUrl, KeyProtectionUrl
Get-HgsAttestationPolicy -ErrorAction SilentlyContinue
```

AUDIT :

- **Valeur attendue :** IsHostGuarded = True, AttestationStatus = Passed

REMÉDIATION :

1. Déployer HGS sur un cluster dédié (minimum 3 noeuds)
2. **PowerShell sur le serveur HGS :**

```
Install-WindowsFeature HostGuardianServiceRole -IncludeManagementTools
Initialize-HgsServer -HgsServiceName "HGS" -SigningCertificateThumbprint $signingCert -EncryptionCertificateThumbprint $encCert
```

REMÉDIATION :

1. **Sur l'hôte Hyper-V :**

```
Set-HgsClientConfiguration -AttestationServerUrl "https://hgs.domain.local/Attestation" -KeyProtectionServerUrl "https://hgs.domain
```

VALEUR PAR DÉFAUT :
HGS non déployé

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

4.1.2 *Mode d'attestation TPM (et non Admin-trusted)*

DESCRIPTION :
Le mode d'attestation du Guarded Fabric doit être TPM (Trusted Platform Module) et non Admin-trusted (basé sur Active Directory). L'attestation TPM vérifie cryptographiquement l'identité du matériel, l'intégrité du firmware, la configuration du démarrage sécurisé et les politiques d'intégrité du code de l'hôte. L'attestation Admin-trusted repose uniquement sur l'appartenance à un groupe AD, ce qui est insuffisant car un administrateur compromis peut ajouter un hôte non sécurisé.

```
# Vérifier le mode d'attestation
Get-HgsClientConfiguration | Select-Object Mode
# Mode doit être "Tpm" et non "AD"

# Sur le serveur HGS
Get-HgsServer | Select-Object AttestationOperationMode
```

AUDIT :

- **Valeur attendue :** Mode = "Tpm"

REMÉDIATION :

1. **Migrer de Admin-trusted vers TPM :**

```
# Sur le serveur HGS
Set-HgsServer -TrustTpm
# Ajouter les endorsement keys TPM des hôtes
Add-HgsAttestationTpmHost -Path "C:\Attestation\host1-ek.xml"
Add-HgsAttestationTpmPolicy -Name "SecureBootPolicy" -Path "C:\Attestation\secureboot-policy.xml"
```

VALEUR PAR DÉFAUT :
Non configuré (choix lors du déploiement)

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

4.1.3 *Haute disponibilité du cluster HGS*

DESCRIPTION :
Le cluster HGS doit être hautement disponible (minimum 3 noeuds) car il est le point central de confiance du Guarded Fabric. Si HGS est indisponible, aucune Shielded VM ne peut démarrer et les VMs en cours d'exécution ne peuvent pas être migrées. Un déni de service sur HGS paralyse l'ensemble de l'infrastructure de virtualisation sécurisée.

```
# Vérifier le cluster HGS (depuis le serveur HGS)
Get-ClusterNode -ErrorAction SilentlyContinue | Select-Object Name, State
Get-ClusterResource -ErrorAction SilentlyContinue | Select-Object Name, State, ResourceType

# Vérifier les URLs HGS et leur disponibilité
$hgsConfig = Get-HgsClientConfiguration
Invoke-WebRequest -Uri "$($hgsConfig.AttestationServerUrl)/metadata" -UseBasicParsing -ErrorAction SilentlyContinue | Select-Object
```

AUDIT :

- **Valeur attendue :** Cluster HGS avec 3+ noeuds, tous en état "Up"

REMÉDIATION :

1. Déployer HGS sur un cluster à 3 noeuds minimum
2. Configurer la surveillance de la disponibilité du cluster HGS
3. Documenter le plan de reprise en cas de défaillance HGS

VALEUR PAR DÉFAUT :
Noeud unique (non recommandé en production)

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

4.2.1 *Shielded VMs déployées pour les charges sensibles*

DESCRIPTION :
Les machines virtuelles hébergeant des données sensibles (bases de données, contrôleurs de domaine, serveurs d'applications critiques) doivent être déployées en tant que Shielded VMs. Les Shielded VMs protègent contre l'inspection mémoire par l'administrateur de l'hôte, le vol de fichiers VHD, les modifications non autorisées de la configuration, et empêchent le démarrage sur des hôtes non attestés.

```
# Vérifier le statut de blindage de chaque VM
Get-VM | Get-VMSecurity | Select-Object VMName, Shielded, TpmEnabled, KsdEnabled, EncryptStateAndVmMigrationTraffic, Virtualization

# Identifier les VMs non blindées
Get-VM | Get-VMSecurity | Where-Object { $_.Shielded -ne $true } | Select-Object VMName

# Vérifier les Key Protectors
Get-VM | Get-VMKeyProtector -ErrorAction SilentlyContinue
```

AUDIT :

- **Valeur attendue :** Shielded = True pour les VMs sensibles

REMÉDIATION :

1. **Créer une Shielded VM :**

```
# Créer le Key Protector avec le certificat HGS
$kp = New-HgsKeyProtector -Owner $owner -Guardian $guardian -AllowExpired
Set-VMKeyProtector -VMName "SensitiveVM" -KeyProtector $kp.RawData
Enable-VMTPM -VMName "SensitiveVM"
Set-VMSecurityPolicy -VMName "SensitiveVM" -Shielded $true
```

REMÉDIATION :

1. **Utiliser les Shielding Data Files (.pdk)** pour automatiser le déploiement

VALEUR PAR DÉFAUT :
VMs non blindées

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

4.2.2 *vTPM (Virtual TPM) activé sur les VMs*

DESCRIPTION :
Le vTPM (Virtual Trusted Platform Module) doit être activé sur les VMs de Génération 2 pour permettre BitLocker dans la VM, le Measured Boot, la protection des clés Credential Guard et d'autres fonctionnalités de sécurité dépendant du TPM. Le vTPM est un prérequis pour les Shielded VMs et offre une protection cryptographique pour les secrets de la VM.

```
# Vérifier vTPM sur toutes les VMs Gen2
Get-VM | Where-Object Generation -eq 2 | Get-VMSecurity | Select-Object VMName, TpmEnabled

# VMs Gen2 sans vTPM
Get-VM | Where-Object Generation -eq 2 | Get-VMSecurity | Where-Object { $_.TpmEnabled -ne $true } | Select-Object VMName
```

AUDIT :

- **Valeur attendue :** TpmEnabled = True pour toutes les VMs Gen2

REMÉDIATION :

1. **PowerShell :**

```
# Activer vTPM (VM doit être arrêtée)
Enable-VMTPM -VMName "VMName"

# Configurer le Key Protector (prérequis pour vTPM)
$owner = New-HgsGuardian -Name "Owner" -GenerateCertificates
Set-VMKeyProtector -VMName "VMName" -NewLocalKeyProtector
Enable-VMTPM -VMName "VMName"
```

VALEUR PAR DÉFAUT :
vTPM désactivé

Preuve d'audit :

```
| Résultat | _____________________________________________ |
| Capture  | ☐ Oui ☐ Non                                   |
| Note     | _____________________________________________ |
```

4.2.3 *Chiffrement de l'état et du trafic de migration*

DESCRIPTION :
Le chiffrement de l'état de la VM (EncryptStateAndVmMigrationTraffic) doit être activé pour protéger le contenu mémoire de la VM lors des opérations de sauvegarde, checkpoint et Live Migration. Sans ce chiffrement, les données en mémoire (y compris les mots de passe, clés de chiffrement et données sensibles) transitent en clair sur le réseau lors de la migration ou sont stockées en clair dans les fichiers de checkpoint.

```
# Vérifier le chiffrement de l'état et du trafic de migration
Get-VM | Get-VMSecurity | Select-Object VMName, EncryptStateAndVmMigrationTraffic, Shielded

# VMs sans chiffrement de l'état
Get-VM | Get-VMSecurity | Where-Object { $_.EncryptStateAndVmMigrationTraffic -ne $true } | Select-Object VMName
```

AUDIT :

- **Valeur attendue :** EncryptStateAndVmMigrationTraffic = True

REMÉDIATION :

1. **PowerShell :**

```
Set-VMSecurityPolicy -VMName "VMName" -EncryptStateAndVmMigrationTraffic $true
```

VALEUR PAR DÉFAUT :
Désactivé (sauf pour les Shielded VMs)

Preuve d'audit :

```
| Résultat | _____________________________________________ |
| Capture  | ☐ Oui ☐ Non                                   |
| Note     | _____________________________________________ |
```

4.3.1 *Key Protectors et Shielding Data Files (.pdk) sécurisés*

DESCRIPTION :
Les Key Protectors et les Shielding Data Files (.pdk) contiennent les clés de chiffrement et les métadonnées nécessaires au démarrage des Shielded VMs. Ces fichiers doivent être stockés de manière sécurisée avec des ACL restrictives. Les certificats Guardian Owner doivent être protégés et sauvegardés de manière sécurisée. La compromission de ces clés permettrait le démarrage de Shielded VMs sur des hôtes non autorisés.

```
# Vérifier les Guardians (propriétaires de clés)
Get-HgsGuardian | Select-Object Name, HasCertificates, SigningCertificate, EncryptionCertificate

# Vérifier les Key Protectors des VMs
Get-VM | ForEach-Object {
    $kp = Get-VMKeyProtector -VMName $_.Name -ErrorAction SilentlyContinue
    if ($kp) {
        [PSCustomObject]@{VM=$_.Name; HasKeyProtector=$true}
    }
}

# Vérifier les certificats Guardian dans le magasin
Get-ChildItem Cert:\LocalMachine\Shielded* -ErrorAction SilentlyContinue
```

AUDIT :

- **Valeur attendue :** Guardians configurés avec certificats valides, Key Protectors appliqués

REMÉDIATION :

1. **Sauvegarder les clés Guardian :**

```
Export-HgsGuardian -Name "Owner" -Path "C:\Secure\GuardianBackup.xml"
```

REMÉDIATION :

1. Protéger les fichiers .pdk et les clés Guardian par des ACL restrictives
2. Stocker les sauvegardes des clés dans un coffre-fort sécurisé

VALEUR PAR DÉFAUT :
Non configuré

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

4.3.2 *Politiques d'attestation Code Integrity*

DESCRIPTION :
Les politiques d'intégrité du code (Code Integrity Policies) doivent être configurées sur les hôtes Hyper-V du Guarded Fabric et enregistrées auprès du HGS. Ces politiques définissent quels pilotes et logiciels sont autorisés à s'exécuter sur l'hôte, empêchant l'exécution de code malveillant qui pourrait compromettre la sécurité des Shielded VMs.

```
# Vérifier les politiques CI sur l'hôte
Get-CIPolicy -FilePath "C:\Windows\System32\CodeIntegrity\SIPolicy.p7b" -ErrorAction SilentlyContinue

# Vérifier les politiques enregistrées au HGS
Get-HgsAttestationPolicy -Name "CI-Policy*" -ErrorAction SilentlyContinue

# Vérifier l'état HVCI/CI
Get-CimInstance -ClassName Win32_DeviceGuard -Namespace root\Microsoft\Windows\DeviceGuard | Select-Object CodeIntegrityPolicyEnfor
```

REMÉDIATION :

1. **Créer une politique CI :**

```
New-CIPolicy -FilePath "C:\CI\HVHostPolicy.xml" -Level Publisher -Fallback Hash
ConvertFrom-CIPolicy "C:\CI\HVHostPolicy.xml" "C:\CI\HVHostPolicy.p7b"
```

REMÉDIATION :

1. **Enregistrer au HGS :**

```
Add-HgsAttestationCIPolicy -Name "HV-Host-CI-Policy" -Path "C:\CI\HVHostPolicy.p7b"
```

VALEUR PAR DÉFAUT :
Aucune politique CI (mode audit)

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

4.3.3 *Certificates HGS — validité et renouvellement*

DESCRIPTION :
Les certificats utilisés par le Host Guardian Service (certificats de signature et de chiffrement) doivent être surveillés pour leur date d'expiration et renouvelés avant leur expiration. L'expiration d'un certificat HGS empêche l'attestation des hôtes et le démarrage des Shielded VMs, provoquant un déni de service critique sur l'ensemble du Guarded Fabric.

```
# Vérifier les certificats HGS (depuis le serveur HGS)
Get-HgsServer | Select-Object SigningCertificate, EncryptionCertificate
$sigCert = Get-HgsServer | Select-Object -ExpandProperty SigningCertificate
$encCert = Get-HgsServer | Select-Object -ExpandProperty EncryptionCertificate

# Vérifier la date d'expiration
Get-ChildItem Cert:\LocalMachine\My | Where-Object { $_.Thumbprint -in @($sigCert, $encCert) } | Select-Object Subject, NotAfter, @
```

AUDIT :

- **Valeur attendue :** Certificats valides avec > 90 jours avant expiration

REMÉDIATION :

1. Renouveler les certificats HGS avant expiration
2. Configurer des alertes pour les certificats expirant dans < 60 jours
3. Documenter la procédure de renouvellement des certificats HGS

VALEUR PAR DÉFAUT :
Certificats auto-signés si non configurés avec une PKI

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

4.3.4 *Encryption-Supported vs Shielded — classification des VMs*

DESCRIPTION :
Hyper-V offre deux niveaux de protection pour les VMs : Encryption-Supported (chiffrement sans restriction complète de la console) et Shielded (chiffrement complet avec restrictions d'accès à la console, pas de connexion VMConnect en mode amélioré). Les VMs sensibles doivent être classifiées et le niveau de protection approprié doit être appliqué. Les VMs Shielded offrent une protection maximale mais limitent les options de dépannage.

```
# Classifier les VMs par niveau de protection
Get-VM | Get-VMSecurity | Select-Object VMName, Shielded, TpmEnabled, EncryptStateAndVmMigrationTraffic | Sort-Object Shielded -Des
```

REMÉDIATION :

1. Définir une politique de classification des VMs (Standard, Encryption-Supported, Shielded)
2. Appliquer le niveau Shielded aux VMs les plus sensibles
3. Documenter les exceptions

VALEUR PAR DÉFAUT :
VMs Standard (non protégées)

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

VALEUR PAR DÉFAUT :
═══

5.0 — RÉSEAU VIRTUEL (Virtual Networking)

5.1.1 *Types de Virtual Switch — utilisation appropriée*

DESCRIPTION :
Hyper-V propose trois types de commutateurs virtuels : External (connecté au réseau physique), Internal (communication hôte-VMs uniquement) et Private (communication inter-VMs uniquement). Le type de switch doit être choisi en fonction du besoin de connectivité de chaque groupe de VMs. Les VMs qui n'ont pas besoin d'accéder au réseau externe doivent utiliser des switches Internal ou Private pour limiter la surface d'attaque réseau.

```
# Lister tous les commutateurs virtuels avec leurs types
Get-VMSwitch | Select-Object Name, SwitchType, NetAdapterInterfaceDescription, AllowManagementOS, IovEnabled, BandwidthReservationM

# Vérifier quelles VMs sont connectées à chaque switch
Get-VMSwitch | ForEach-Object {
    $sw = $_
    $vms = Get-VMNetworkAdapter -All | Where-Object SwitchName -eq $sw.Name
    [PSCustomObject]@{Switch=$sw.Name; Type=$sw.SwitchType; VMs=($vms.VMName -join ', ')}
}

# Vérifier les adaptateurs réseau des VMs
Get-VM | Get-VMNetworkAdapter | Select-Object VMName, Name, SwitchName, MacAddress, Status
```

AUDIT :

- **Valeur attendue :** Utilisation de switches Private/Internal pour les VMs sans besoin d'accès externe

REMÉDIATION :

1. **PowerShell :**

```
# Créer des switches adaptés à chaque zone
New-VMSwitch -Name "vSwitch-Production" -SwitchType External -NetAdapterName "NIC1" -AllowManagementOS $false
New-VMSwitch -Name "vSwitch-Management" -SwitchType Internal
New-VMSwitch -Name "vSwitch-Isolated" -SwitchType Private
```

VALEUR PAR DÉFAUT :
Aucun switch virtuel (à créer)

Preuve d'audit :

```
| Résultat | _____________________________________________ |
| Capture  | ☐ Oui ☐ Non                                   |
| Note     | _____________________________________________ |
```

5.1.2 *Management OS séparé du réseau VM*

DESCRIPTION :
Le réseau de gestion de l'hôte Hyper-V (Management OS) ne doit pas partager le même adaptateur réseau physique et le même VLAN que les VMs de production. Si l'option "Allow management operating system to share this network adapter" est activée sur un switch External, le trafic de gestion de l'hôte transite sur le même réseau que les VMs, permettant potentiellement à une VM compromise d'intercepter ou d'attaquer le trafic de gestion.

```
# Vérifier si AllowManagementOS est activé sur les switches External
Get-VMSwitch | Where-Object SwitchType -eq "External" | Select-Object Name, AllowManagementOS, NetAdapterInterfaceDescription

# Vérifier les adaptateurs réseau de gestion
Get-VMNetworkAdapter -ManagementOS | Select-Object Name, SwitchName, MacAddress, IPAddresses
```

AUDIT :

- **Valeur attendue :** AllowManagementOS = False sur les switches de production, ou VLAN de gestion dédié

REMÉDIATION :

1. **Option 1 — NIC dédié pour la gestion :**

```
# Créer le switch production sans gestion OS
Set-VMSwitch -Name "vSwitch-Production" -AllowManagementOS $false

# Utiliser un NIC séparé pour la gestion
New-VMSwitch -Name "vSwitch-Mgmt" -SwitchType External -NetAdapterName "NIC-Mgmt" -AllowManagementOS $true
```

REMÉDIATION :

1. **Option 2 — VLAN dédié :**

```
Set-VMNetworkAdapterVlan -ManagementOS -VMNetworkAdapterName "Management" -Access -VlanId 100
```

VALEUR PAR DÉFAUT :
AllowManagementOS = True

Preuve d'audit :

```
| Résultat | _____________________________________________ |
| Capture  | ☐ Oui ☐ Non                                   |
| Note     | _____________________________________________ |
```

5.2.1 *VLAN Tagging configuré pour l'isolation réseau*

DESCRIPTION :
Le VLAN tagging doit être configuré sur les adaptateurs réseau virtuels des VMs pour assurer l'isolation réseau de couche 2 entre les différentes zones de sécurité (production, développement, DMZ, gestion). Chaque zone doit avoir son propre VLAN ID, empêchant le trafic inter-zones non autorisé. Le VLAN tagging Hyper-V doit être cohérent avec la configuration des switches physiques.

```
# Vérifier la configuration VLAN de chaque VM
Get-VM | Get-VMNetworkAdapter | Get-VMNetworkAdapterVlan | Select-Object VMName, VMNetworkAdapterName, OperationMode, AccessVlanId,

# VMs sans VLAN configuré
Get-VM | Get-VMNetworkAdapter | Get-VMNetworkAdapterVlan | Where-Object { $_.OperationMode -eq 'Untagged' -or $_.AccessVlanId -eq 0

# Vérifier la cohérence des VLANs par zone
Get-VM | Get-VMNetworkAdapter | Get-VMNetworkAdapterVlan | Group-Object AccessVlanId | Select-Object Name, Count, @{N='VMs';E={$_.G
```

AUDIT :

- **Valeur attendue :** Toutes les VMs avec un VLAN ID approprié à leur zone

REMÉDIATION :

1. **PowerShell :**

```
# Configurer le VLAN sur un adaptateur VM
Set-VMNetworkAdapterVlan -VMName "VMName" -Access -VlanId 100

# Configuration Trunk pour les VMs multi-VLAN (routeurs virtuels)
Set-VMNetworkAdapterVlan -VMName "RouterVM" -Trunk -AllowedVlanIdList "100-200" -NativeVlanId 1
```

REMÉDIATION :

1. **Hyper-V Manager :** Paramètres VM > Carte réseau > VLAN

VALEUR PAR DÉFAUT :
Pas de VLAN (mode Untagged)

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

5.3.1 *DHCP Guard activé sur les adaptateurs VM*

DESCRIPTION :
Le DHCP Guard doit être activé sur les adaptateurs réseau virtuels des VMs qui ne sont pas des serveurs DHCP autorisés. Le DHCP Guard empêche une VM compromise de se comporter comme un serveur DHCP rogue, distribuant des configurations réseau malveillantes (DNS, passerelle) aux autres VMs et postes du réseau. Une VM avec un DHCP rogue peut rediriger tout le trafic réseau vers elle-même pour l'interception.

```
# Vérifier DHCP Guard sur toutes les VMs
Get-VM | Get-VMNetworkAdapter | Select-Object VMName, Name, DhcpGuard

# VMs sans DHCP Guard
Get-VM | Get-VMNetworkAdapter | Where-Object { $_.DhcpGuard -ne 'On' } | Select-Object VMName, Name
```

AUDIT :

- **Valeur attendue :** DhcpGuard = On pour toutes les VMs sauf les serveurs DHCP légitimes

REMÉDIATION :

1. **PowerShell :**

```
# Activer DHCP Guard sur toutes les VMs
Get-VM | Get-VMNetworkAdapter | Set-VMNetworkAdapter -DhcpGuard On

# Désactiver pour les serveurs DHCP légitimes
Set-VMNetworkAdapter -VMName "DHCP-Server" -DhcpGuard Off
```

REMÉDIATION :

1. **Hyper-V Manager :** Paramètres VM > Carte réseau > Fonctionnalités avancées > DHCP Guard

VALEUR PAR DÉFAUT :
DhcpGuard = Off

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

5.3.2 *Router Guard activé sur les adaptateurs VM*

DESCRIPTION :
Le Router Guard empêche une VM de se comporter comme un routeur en envoyant des messages Router Advertisement (RA) et DHCP redirect non autorisés. Une VM compromise pourrait utiliser ces messages pour rediriger le trafic réseau IPv6 à travers elle-même, permettant l'interception et la modification du trafic. Le Router Guard doit être activé sur toutes les VMs sauf les routeurs virtuels légitimes.

```
# Vérifier Router Guard sur toutes les VMs
Get-VM | Get-VMNetworkAdapter | Select-Object VMName, Name, RouterGuard

# VMs sans Router Guard
Get-VM | Get-VMNetworkAdapter | Where-Object { $_.RouterGuard -ne 'On' } | Select-Object VMName, Name
```

AUDIT :

- **Valeur attendue :** RouterGuard = On pour toutes les VMs sauf les routeurs

REMÉDIATION :

1. **PowerShell :**

```
Get-VM | Get-VMNetworkAdapter | Set-VMNetworkAdapter -RouterGuard On
```

REMÉDIATION :

1. **Hyper-V Manager :** Paramètres VM > Carte réseau > Fonctionnalités avancées > Router Guard

VALEUR PAR DÉFAUT :
RouterGuard = Off

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

5.3.3 *MAC Address Spoofing Protection*

DESCRIPTION :
La protection contre l'usurpation d'adresses MAC (MAC Address Spoofing) doit être désactivée (= protection active) sur les adaptateurs réseau virtuels des VMs. Quand le MAC spoofing est autorisé, une VM peut modifier son adresse MAC pour usurper l'identité d'une autre machine sur le réseau, contourner les ACL basées sur MAC, ou mener des attaques ARP poisoning. Le MAC spoofing ne doit être autorisé que pour des cas spécifiques (NIC teaming dans la VM, NLB).

```
# Vérifier MAC Address Spoofing sur toutes les VMs
Get-VM | Get-VMNetworkAdapter | Select-Object VMName, Name, MacAddressSpoofing

# VMs avec MAC spoofing autorisé
Get-VM | Get-VMNetworkAdapter | Where-Object { $_.MacAddressSpoofing -eq 'On' } | Select-Object VMName, Name
```

AUDIT :

- **Valeur attendue :** MacAddressSpoofing = Off (protection active)

REMÉDIATION :

1. **PowerShell :**

```
Get-VM | Get-VMNetworkAdapter | Set-VMNetworkAdapter -MacAddressSpoofing Off
```

REMÉDIATION :

1. **Hyper-V Manager :** Paramètres VM > Carte réseau > Fonctionnalités avancées > MAC Address Spoofing = Désactivé

VALEUR PAR DÉFAUT :
MacAddressSpoofing = Off

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

5.3.4 *Port ACLs et Extended Port ACLs*

DESCRIPTION :
Les Extended Port ACLs doivent être configurées sur les adaptateurs réseau virtuels pour filtrer le trafic réseau au niveau du port du switch virtuel. Les Port ACLs permettent de définir des règles de filtrage basées sur les adresses IP source/destination, les ports TCP/UDP et les protocoles, créant un pare-feu de micro-segmentation au niveau de l'hyperviseur. Cela complète les pare-feux dans les VMs invitées.

```
# Vérifier les Extended Port ACLs
Get-VM | Get-VMNetworkAdapter | Get-VMNetworkAdapterExtendedAcl | Select-Object VMName, Direction, Action, LocalIPAddress, RemoteIP

# Vérifier les Port ACLs (legacy)
Get-VM | Get-VMNetworkAdapter | Get-VMNetworkAdapterAcl | Select-Object VMName, Direction, Action, LocalAddress, RemoteAddress
```

REMÉDIATION :
1. **PowerShell :**

```
# Ajouter une Extended Port ACL (autoriser HTTPS sortant)
Add-VMNetworkAdapterExtendedAcl -VMName "WebServer" -Direction Outbound -Action Allow -RemotePort "443" -Protocol TCP -Weight 10

# Bloquer tout autre trafic sortant
Add-VMNetworkAdapterExtendedAcl -VMName "WebServer" -Direction Outbound -Action Deny -Weight 1
```

VALEUR PAR DÉFAUT :
Aucune ACL (tout le trafic est autorisé)
Preuve d'audit :

```
| Résultat | _____________________________________________ |
| Capture  | ☐ Oui ☐ Non                                   |
| Note     | _____________________________________________ |
```

5.4.1 *NIC Teaming — configuration sécurisée*

DESCRIPTION :
Si le NIC Teaming (association de cartes réseau) est utilisé pour la haute disponibilité réseau des VMs, il doit être configuré en mode Switch-Independent avec Hyper-V Port comme algorithme de répartition de charge pour les switches virtuels Hyper-V. Le teaming au niveau de l'hôte (SET — Switch Embedded Teaming) est recommandé plutôt que le teaming traditionnel pour les environnements Hyper-V.

```
# Vérifier le NIC Teaming traditionnel
Get-NetLbfoTeam | Select-Object Name, TeamingMode, LoadBalancingAlgorithm, Status

# Vérifier le Switch Embedded Teaming (SET)
Get-VMSwitch | Select-Object Name, EmbeddedTeamingEnabled, @{N='TeamMembers';E={$_.NetAdapterInterfaceDescription -join ', '}}

# Vérifier les adaptateurs SR-IOV
Get-VMSwitch | Select-Object Name, IovEnabled, IovSupport
```

REMÉDIATION :
1. **PowerShell (SET recommandé) :**

```
New-VMSwitch -Name "SET-vSwitch" -NetAdapterName "NIC1","NIC2" -EnableEmbeddedTeaming $true -AllowManagementOS $true
```

VALEUR PAR DÉFAUT :
Aucun teaming
Preuve d'audit :

```
| Résultat | _____________________________________________ |
| Capture  | ☐ Oui ☐ Non                                   |
| Note     | _____________________________________________ |
```

5.4.2 *SR-IOV — contrôle de l'utilisation*

DESCRIPTION :
SR-IOV (Single Root I/O Virtualization) permet aux VMs d'accéder directement au matériel réseau physique, contournant le switch virtuel Hyper-V. Si cela améliore les performances réseau, SR-IOV réduit l'isolation car les VMs interagissent directement avec le firmware du NIC physique. SR-IOV désactive également certaines fonctionnalités de sécurité du switch virtuel (Port ACLs, DHCP Guard, etc.). Son utilisation doit être limitée et documentée.

```
# Vérifier SR-IOV sur les switches
Get-VMSwitch | Select-Object Name, IovEnabled, IovSupport, IovVirtualFunctionCount

# Vérifier les VMs utilisant SR-IOV
Get-VM | Get-VMNetworkAdapter | Where-Object { $_.IovWeight -gt 0 } | Select-Object VMName, Name, IovWeight

# Vérifier les Virtual Functions SR-IOV en usage
Get-NetAdapterSriov | Select-Object Name, NumVFs, CurrentVFs
```

AUDIT :

- **Valeur attendue :** SR-IOV désactivé sauf besoin documenté de performance

REMÉDIATION :

1. **Désactiver SR-IOV si non requis :**

```
Set-VMNetworkAdapter -VMName "VMName" -IovWeight 0
```

VALEUR PAR DÉFAUT :
SR-IOV désactivé

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

5.5.1 *Network QoS (Quality of Service) configuré*

DESCRIPTION :
Le QoS réseau (Quality of Service) doit être configuré sur les adaptateurs réseau virtuels pour garantir une bande passante minimale aux VMs critiques et empêcher les VMs non prioritaires de consommer toute la bande passante disponible. Le QoS réseau Hyper-V supporte les modes Absolute (en Mbps) et Weight (poids relatif).

```
# Vérifier la configuration QoS du switch
Get-VMSwitch | Select-Object Name, BandwidthReservationMode, DefaultFlowMinimumBandwidthAbsolute, DefaultFlowMinimumBandwidthWeight

# Vérifier le QoS par adaptateur
Get-VM | Get-VMNetworkAdapter | Select-Object VMName, Name, BandwidthSetting, @{N='MinBandwidthAbsolute';E={$_.BandwidthSetting.Min
```

REMÉDIATION :

1. **PowerShell :**

```
# Configurer le mode de bande passante du switch
Set-VMSwitch -Name "vSwitch1" -DefaultFlowMinimumBandwidthWeight 10

# Configurer le QoS par VM
Set-VMNetworkAdapter -VMName "CriticalVM" -MinimumBandwidthWeight 50 -MaximumBandwidth 5000000000
```

VALEUR PAR DÉFAUT :
QoS non configuré

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

5.5.2 *Protected Network — isolation de sous-réseau VM*

DESCRIPTION :
La fonctionnalité Protected Network (réseau protégé) doit être activée sur les adaptateurs réseau des VMs critiques dans un cluster Hyper-V. Si la connectivité réseau est perdue, la VM est automatiquement migrée vers un autre noeud du cluster ayant une connectivité réseau fonctionnelle. Cela assure la continuité réseau des VMs critiques en cas de défaillance réseau sur un hôte.

```
# Vérifier Protected Network
Get-VM | Get-VMNetworkAdapter | Select-Object VMName, IsFailoverNetworkAdapterEnabled

# Vérifier la configuration du cluster pour la migration automatique réseau
Get-ClusterResource | Where-Object ResourceType -eq "Virtual Machine" | Get-ClusterParameter -Name ProtectedNetwork -ErrorAction Si
```

REMÉDIATION :

1. **PowerShell :**

```
Set-VMNetworkAdapter -VMName "CriticalVM" -ProtectedNetwork $true
```

VALEUR PAR DÉFAUT :
Non activé

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

5.6.1 *Virtual Switch Extensions — audit et contrôle*

DESCRIPTION :
Les extensions du switch virtuel (Virtual Switch Extensions) — telles que les solutions de monitoring réseau, de filtrage ou de capture de paquets — doivent être inventoriées, approuvées et contrôlées. Les extensions malveillantes ou non autorisées pourraient intercepter, modifier ou rediriger le trafic réseau de toutes les VMs connectées au switch.

```
# Lister toutes les extensions de switch virtuel
Get-VMSwitch | Get-VMSwitchExtension | Select-Object SwitchName, Name, Vendor, Enabled, Running, ExtensionType

# Extensions actives
Get-VMSwitch | Get-VMSwitchExtension | Where-Object Enabled | Select-Object SwitchName, Name, Vendor
```

AUDIT :

- **Valeur attendue :** Seules les extensions approuvées et documentées sont activées

REMÉDIATION :

1. **PowerShell :**

```
# Désactiver une extension non autorisée
Disable-VMSwitchExtension -VMSwitchName "vSwitch1" -Name "Suspicious Extension"
```

REMÉDIATION :

1. Documenter et approuver chaque extension déployée

VALEUR PAR DÉFAUT :
Extension Microsoft NDIS Capture (activée par défaut)

Preuve d'audit :

```
| Résultat | _____________________________________________ |
| Capture  | ☐ Oui ☐ Non                                   |
| Note     | _____________________________________________ |
```

5.6.2 *SDN (Software Defined Networking) — sécurité du Network Controller*

DESCRIPTION :
Si le SDN (Software Defined Networking) est déployé avec Hyper-V, le Network Controller doit être sécurisé avec des certificats TLS, une authentification Kerberos et des ACL restrictives. Le Network Controller est le cerveau du SDN et sa compromission permettrait la modification de toutes les règles réseau, le contournement de la segmentation et l'interception du trafic.

```
# Vérifier le Network Controller (si déployé)
Get-NetworkController -ErrorAction SilentlyContinue | Select-Object Node, ClusterAuthentication, ServerCertificate

# Vérifier les règles de sécurité SDN
Get-NetworkControllerAccessControlList -ErrorAction SilentlyContinue | Select-Object ResourceId, Properties
```

REMÉDIATION :

1. Déployer le Network Controller en cluster haute disponibilité
2. Utiliser des certificats TLS pour toutes les communications
3. Configurer l'authentification Kerberos pour le cluster SDN

VALEUR PAR DÉFAUT :
SDN non déployé

Preuve d'audit :

```
| Résultat | _____________________________________________ |
| Capture  | ☐ Oui ☐ Non                                   |
| Note     | _____________________________________________ |
```

VALEUR PAR DÉFAUT :
═══

6.0 — STOCKAGE VIRTUEL (Virtual Storage Security)

6.1.1 *Format VHDX utilisé (pas VHD legacy)*

DESCRIPTION :
Le format VHDX doit être utilisé pour tous les disques virtuels au lieu du format VHD legacy. Le VHDX supporte une taille maximale de 64 To (contre 2 To pour VHD), offre une meilleure résilience contre la corruption de données grâce à un journal de métadonnées, et est requis pour les fonctionnalités avancées comme les Shared VHDX, les checkpoints de production et le redimensionnement en ligne.

```
# Identifier les disques VHD legacy
Get-VM | Get-VMHardDiskDrive | Where-Object { $_.Path -like "*.vhd" -and $_.Path -notlike "*.vhdx" } | Select-Object VMName, Contro

# Compter les formats
Get-VM | Get-VMHardDiskDrive | Group-Object @{E={if ($_.Path -like "*.vhdx") {"VHDX"} else {"VHD"}}} | Select-Object Name, Count
```

AUDIT :

- **Valeur attendue :** 100% des disques en format VHDX

REMÉDIATION :

1. **Convertir VHD en VHDX :**

```
Convert-VHD -Path "C:\VMs\disk.vhd" -DestinationPath "C:\VMs\disk.vhdx" -VHDType Dynamic
```

REMÉDIATION :

1. Mettre à jour la configuration VM pour pointer vers le nouveau VHDX

VALEUR PAR DÉFAUT :
VHDX pour les nouvelles VMs (depuis Server 2012 R2)

Preuve d'audit :

```
| Résultat | _____________________________________________ |
| Capture  | ☐ Oui ☐ Non                                   |
| Note     | _____________________________________________ |
```

6.1.2 *Permissions ACL restrictives sur les fichiers VHD/VHDX*

DESCRIPTION :
Les fichiers VHD/VHDX contiennent l'intégralité du système de fichiers de la VM invitée. Des permissions trop ouvertes permettraient à un utilisateur non autorisé de monter le fichier VHDX, d'accéder aux données de la VM, de modifier le système de fichiers ou d'y injecter du code malveillant. Les ACL doivent limiter l'accès à SYSTEM, NT VIRTUAL MACHINE\Virtual Machines et les administrateurs Hyper-V.

```
# Vérifier les ACL sur chaque fichier VHDX
Get-VM | Get-VMHardDiskDrive | ForEach-Object {
    if (Test-Path $_.Path) {
        $acl = Get-Acl $_.Path
        [PSCustomObject]@{
            VM = $_.VMName
            Path = $_.Path
            Access = ($acl.Access | ForEach-Object { "$($_.IdentityReference):$($_.FileSystemRights)" }) -join '; '
        }
    }
}

# Vérifier les permissions sur le répertoire de stockage VM
Get-VMHost | Select-Object VirtualHardDiskPath | ForEach-Object {
    Get-Acl $_.VirtualHardDiskPath | Select-Object -ExpandProperty Access | Select-Object IdentityReference, FileSystemRights, Acce
}
```

AUDIT :

- **Valeur attendue :** Accès restreint à SYSTEM, NT VIRTUAL MACHINE\Virtual Machines, Hyper-V Administrators

REMÉDIATION :

1. **PowerShell :**

```
$vhdPath = "D:\VMs\VM01\disk.vhdx"
$acl = Get-Acl $vhdPath
$acl.SetAccessRuleProtection($true, $false)
$acl.Access | ForEach-Object { $acl.RemoveAccessRule($_) } | Out-Null
$acl.AddAccessRule((New-Object System.Security.AccessControl.FileSystemAccessRule("SYSTEM","FullControl","Allow")))
$acl.AddAccessRule((New-Object System.Security.AccessControl.FileSystemAccessRule("NT VIRTUAL MACHINE\Virtual Machines","FullContro
$acl.AddAccessRule((New-Object System.Security.AccessControl.FileSystemAccessRule("BUILTIN\Hyper-V Administrators","FullControl","A
Set-Acl $vhdPath $acl
```

VALEUR PAR DÉFAUT :
Permissions héritées du répertoire parent

Preuve d'audit :

```
| Résultat | _____________________________________________ |
| Capture  | ☐ Oui ☐ Non                                   |
| Note     | _____________________________________________ |
```

6.2.1 *BitLocker dans les VMs invitées (chiffrement interne)*

DESCRIPTION :
BitLocker doit être activé à l'intérieur des VMs invitées contenant des données sensibles, en utilisant le vTPM comme protecteur de clé. Le chiffrement BitLocker dans la VM protège les données même si le fichier VHDX est copié ou exfiltré depuis l'hôte, car les clés de chiffrement sont liées au vTPM qui est lui-même protégé par le Key Protector de la Shielded VM.

```
# Vérifier que vTPM est activé (prérequis pour BitLocker dans VM)
Get-VM | Get-VMSecurity | Where-Object TpmEnabled | Select-Object VMName, TpmEnabled

# Dans la VM invitée (via PowerShell Direct) :
Invoke-Command -VMName "VMName" -ScriptBlock {
    Get-BitLockerVolume | Select-Object MountPoint, VolumeStatus, ProtectionStatus, EncryptionMethod
} -Credential $cred
```

REMÉDIATION :
1. Activer vTPM sur la VM (voir contrôle 4.2.2)
2. **Dans la VM invitée :**

```
Enable-BitLocker -MountPoint "C:" -EncryptionMethod XtsAes256 -TpmProtector
```

VALEUR PAR DÉFAUT :
BitLocker désactivé dans la VM

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

6.2.2 *Storage QoS — politiques appliquées*

DESCRIPTION :
Les politiques Storage QoS (Quality of Service de stockage) doivent être appliquées aux disques virtuels des VMs pour garantir des performances minimales aux VMs critiques et empêcher les « voisins bruyants » (noisy neighbors) de dégrader les performances du sous-système de stockage partagé.

```
# Vérifier les politiques Storage QoS
Get-StorageQosPolicy -ErrorAction SilentlyContinue | Select-Object Name, PolicyType, MinimumIops, MaximumIops

# Vérifier les flux et leur conformité
Get-StorageQosFlow -ErrorAction SilentlyContinue | Select-Object InitiatorName, Status, MinimumIOPS, MaximumIOPS, StorageNodeIOPS
```

REMÉDIATION :
1. **PowerShell :**

```
New-StorageQosPolicy -Name "Critical-VMs" -PolicyType Dedicated -MinimumIops 500 -MaximumIops 5000
New-StorageQosPolicy -Name "Standard-VMs" -PolicyType Aggregated -MinimumIops 200 -MaximumIops 2000
```

VALEUR PAR DÉFAUT :
Aucune politique QoS

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

6.3.1 *Shared VHDX / VHD Sets — sécurité du partage*

DESCRIPTION :
Les Shared VHDX et VHD Sets (.vhds) permettent à plusieurs VMs de partager un même disque virtuel (scénarios de clustering invité). Ce partage crée des dépendances et des risques de sécurité : une VM compromise avec accès au disque partagé pourrait compromettre les données des autres VMs. Les permissions et l'isolation doivent être strictement contrôlées.

```
# Identifier les Shared VHDX et VHD Sets
Get-VM | Get-VMHardDiskDrive | Where-Object { $_.SupportPersistentReservations -eq $true -or $_.Path -like "*.vhds" } | Select-Obje

# Vérifier les permissions
Get-VM | Get-VMHardDiskDrive | Where-Object { $_.Path -like "*.vhds" } | ForEach-Object {
    Get-Acl $_.Path | Select-Object Path, @{N='Access';E={$_.Access.IdentityReference -join '; '}}
}
```

REMÉDIATION :
1. Limiter l'utilisation de Shared VHDX aux scénarios de clustering invité documentés
2. Appliquer des ACL restrictives sur les fichiers partagés
3. Privilégier VHD Sets (.vhds) au lieu de Shared VHDX pour les backups

VALEUR PAR DÉFAUT :
Aucun disque partagé

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

6.3.2 *Storage Spaces Direct (S2D) — sécurité du cluster de stockage*

DESCRIPTION :
Si Storage Spaces Direct (S2D) est utilisé pour le stockage des VMs dans un cluster hyperconvergé, la sécurité du pool de stockage doit être vérifiée. Cela inclut le chiffrement au repos (BitLocker sur les CSV), la résilience du pool (Mirror ou Parity), les permissions sur les CSV et la protection du cluster de stockage contre les accès non autorisés.

```
# Vérifier Storage Spaces Direct
Get-StoragePool -ErrorAction SilentlyContinue | Select-Object FriendlyName, OperationalStatus, HealthStatus, Size, AllocatedSize

# Vérifier les volumes CSV
Get-ClusterSharedVolume -ErrorAction SilentlyContinue | Select-Object Name, State, SharedVolumeInfo

# Vérifier la résilience
Get-VirtualDisk -ErrorAction SilentlyContinue | Select-Object FriendlyName, ResiliencySettingName, OperationalStatus, HealthStatus
```

REMÉDIATION :

1. Vérifier la santé du pool de stockage S2D
2. Activer BitLocker sur les volumes CSV
3. Configurer des alertes sur la dégradation du pool

VALEUR PAR DÉFAUT :
S2D non déployé par défaut

Preuve d'audit :

```
| Résultat | _____________________________________________ |
| Capture  | ☐ Oui ☐ Non                                   |
| Note     | _____________________________________________ |
```

6.4.1 *ReFS vs NTFS — système de fichiers approprié*

DESCRIPTION :
ReFS (Resilient File System) est recommandé pour les volumes de stockage VM car il offre une meilleure résilience contre la corruption de données, des opérations de merge de checkpoints plus rapides (block clone) et une meilleure performance pour les opérations VHDX. ReFS est requis pour Storage Spaces Direct et les checkpoints de production haute performance.

```
# Vérifier le système de fichiers des volumes de stockage VM
$vmPaths = (Get-VMHost).VirtualHardDiskPath, (Get-VMHost).VirtualMachinePath
foreach ($path in $vmPaths) {
    $volume = Get-Volume -FilePath $path -ErrorAction SilentlyContinue
    Write-Output "Path: $path - FileSystem: $($volume.FileSystemType) - Size: $([math]::Round($volume.Size/1GB))GB"
}

# Lister tous les volumes
Get-Volume | Where-Object { $_.FileSystemType -in @('NTFS','ReFS') } | Select-Object DriveLetter, FileSystemType, Size, SizeRemaini
```

REMÉDIATION :

1. Formater les nouveaux volumes de stockage VM en ReFS
2. **Note :** La conversion NTFS vers ReFS nécessite un reformatage (sauvegarde requise)

VALEUR PAR DÉFAUT :
NTFS

Preuve d'audit :

```
| Résultat | _____________________________________________ |
| Capture  | ☐ Oui ☐ Non                                   |
| Note     | _____________________________________________ |
```

6.4.2 *SMB 3.x avec chiffrement pour le stockage réseau*

DESCRIPTION :
Si les fichiers VM sont stockés sur un partage SMB, le chiffrement SMB 3.x doit être activé pour protéger les données en transit. Le trafic SMB non chiffré peut être intercepté sur le réseau, exposant l'intégralité du contenu des disques virtuels et des fichiers de configuration VM. SMB 3.x offre le chiffrement AES-128-GCM ou AES-256-GCM.

```
# Vérifier la configuration SMB du serveur
Get-SmbServerConfiguration | Select-Object EncryptData, RejectUnencryptedAccess, EnableSMB1Protocol, EnableSMB2Protocol

# Vérifier les partages avec chiffrement
Get-SmbShare | Where-Object { $_.Path -like "*VM*" -or $_.Path -like "*Hyper*" } | Select-Object Name, Path, EncryptData

# Vérifier les connexions SMB actives
Get-SmbConnection | Select-Object ServerName, ShareName, Dialect, Encrypted
```

AUDIT :

- **Valeur attendue :** EncryptData = True, SMB1 = False, Dialect >= 3.0

REMÉDIATION :

1. **PowerShell :**

```
# Activer le chiffrement SMB global
Set-SmbServerConfiguration -EncryptData $true -RejectUnencryptedAccess $true -Force

# Désactiver SMB1
Set-SmbServerConfiguration -EnableSMB1Protocol $false -Force

# Chiffrement par partage
Set-SmbShare -Name "VMStorage" -EncryptData $true
```

VALEUR PAR DÉFAUT :
EncryptData = False, SMB1 souvent activé

Preuve d'audit :

```
| Résultat | _____________________________________________ |
| Capture  | ☐ Oui ☐ Non                                   |
| Note     | _____________________________________________ |
```

6.4.3 *iSCSI et Fibre Channel — sécurité du stockage SAN*

DESCRIPTION :
Si le stockage iSCSI ou Fibre Channel est utilisé pour les VMs, la sécurité du réseau de stockage (SAN) doit être vérifiée. L'iSCSI doit utiliser CHAP mutual pour l'authentification, les réseaux iSCSI doivent être isolés sur des VLANs dédiés, et le Fibre Channel doit utiliser le zoning pour restreindre l'accès aux LUNs. Le Virtual Fibre Channel d'Hyper-V doit être sécurisé avec des NPIV correctement configurés.

```
# Vérifier les initiateurs iSCSI
Get-IscsiTargetPortal -ErrorAction SilentlyContinue | Select-Object TargetPortalAddress, TargetPortalPortNumber
Get-IscsiSession -ErrorAction SilentlyContinue | Select-Object TargetNodeAddress, IsConnected, AuthenticationType

# Vérifier les adaptateurs Fibre Channel virtuels
Get-VM | Get-VMFibreChannelHba -ErrorAction SilentlyContinue | Select-Object VMName, WorldWideNodeNameSetA, WorldWidePortNameSetA

# Vérifier le MPIO (Multipath I/O)
Get-MSDSMGlobalDefaultLoadBalancePolicy -ErrorAction SilentlyContinue
```

REMÉDIATION :

1. Configurer l'authentification CHAP mutual pour iSCSI
2. Isoler le trafic iSCSI sur des VLANs/sous-réseaux dédiés
3. Configurer le zoning Fibre Channel pour restreindre l'accès

VALEUR PAR DÉFAUT :
Dépend de l'infrastructure de stockage

Preuve d'audit :

```
| Résultat | _____________________________________________ |
| Capture  | ☐ Oui ☐ Non                                   |
| Note     | _____________________________________________ |
```

VALEUR PAR DÉFAUT :
═══

7.0 — LIVE MIGRATION ET HAUTE DISPONIBILITÉ

7.1.1 *Live Migration — authentification Kerberos (CredSSP non recommandé)*

DESCRIPTION :
La Live Migration doit utiliser l'authentification Kerberos avec la délégation contrainte (Constrained Delegation) plutôt que CredSSP. CredSSP transmet les identifiants de l'administrateur au serveur distant, ce qui permet les attaques de type credential relay. Kerberos avec délégation contrainte limite la délégation aux seuls services spécifiés (Microsoft Virtual System Migration Service) et ne transmet pas les identifiants en clair.

```
# Vérifier le protocole d'authentification Live Migration
Get-VMHost | Select-Object VirtualMachineMigrationAuthenticationType

# Vérifier la délégation contrainte dans AD
Get-ADComputer $env:COMPUTERNAME -Properties msDS-AllowedToDelegateTo | Select-Object -ExpandProperty msDS-AllowedToDelegateTo
```

AUDIT :

- **Valeur attendue :** VirtualMachineMigrationAuthenticationType = Kerberos

REMÉDIATION :

1. **PowerShell :**

```
Set-VMHost -VirtualMachineMigrationAuthenticationType Kerberos
```

REMÉDIATION :

1. **Active Directory :** Configurer la délégation contrainte :
2. Propriétés du compte ordinateur > Délégation > "N'approuver cet ordinateur que pour la délégation aux services spécifiés"
3. Ajouter le service "Microsoft Virtual System Migration Service" et "cifs"

VALEUR PAR DÉFAUT :
CredSSP

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

7.1.2 *Live Migration — chiffrement du transfert*

DESCRIPTION :
Le transfert de données lors de la Live Migration doit être chiffré. Pendant la migration, le contenu complet de la mémoire de la VM (y compris les mots de passe, clés de chiffrement et données sensibles en mémoire) est transféré sur le réseau. Sans chiffrement, ces données peuvent être interceptées. Hyper-V supporte le chiffrement SMB pour la migration.

```
# Vérifier les options de performance/chiffrement de la migration
Get-VMHost | Select-Object VirtualMachineMigrationPerformanceOption
# Options : TCPIP (pas de chiffrement), Compression, SMB (chiffré si SMB encryption activé)

# Vérifier le chiffrement SMB
Get-SmbServerConfiguration | Select-Object EncryptData
```

AUDIT :

- **Valeur attendue :** VirtualMachineMigrationPerformanceOption = SMB avec EncryptData = True

REMÉDIATION :

1. **PowerShell :**

```
Set-VMHost -VirtualMachineMigrationPerformanceOption SMB
Set-SmbServerConfiguration -EncryptData $true -Force
```

VALEUR PAR DÉFAUT :
TCPIP (pas de chiffrement)

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

7.1.3 *Live Migration — réseau dédié et isolé*

DESCRIPTION :
La Live Migration doit utiliser un réseau dédié et isolé, séparé du réseau de production des VMs et du réseau de gestion. Le réseau de migration transporte les données mémoire des VMs en transit, ce qui représente un risque élevé d'interception. Ce réseau doit être sur un VLAN dédié avec un sous-réseau IP distinct, idéalement sur des interfaces réseau physiques dédiées.

```
# Vérifier les réseaux autorisés pour la migration
Get-VMHost | Select-Object -ExpandProperty VirtualMachineMigrationEnabled
$networks = (Get-VMHostMigrationNetwork).Subnet
Write-Output "Réseaux de migration autorisés : $($networks -join ', ')"

# Vérifier l'isolation du réseau de migration
Get-VMHostMigrationNetwork | Select-Object Subnet, Priority
```

AUDIT :

- **Valeur attendue :** Sous-réseau de migration dédié (ex: 10.0.100.0/24), pas sur le réseau de production

REMÉDIATION :

1. **PowerShell :**

```
# Configurer un réseau dédié pour la migration
Add-VMMigrationNetwork -Subnet "10.0.100.0/24" -Priority 1
Remove-VMMigrationNetwork -Subnet "0.0.0.0/0" # Supprimer le réseau par défaut (tout réseau)
```

VALEUR PAR DÉFAUT :
Migration autorisée sur tous les réseaux

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

7.1.4 *Live Migration — nombre de migrations simultanées limité*

DESCRIPTION :
Le nombre de migrations simultanées et de connexions de migration simultanées doit être limité pour éviter la surcharge de l'hôte et du réseau. Un nombre excessif de migrations simultanées peut dégrader les performances des VMs en cours d'exécution et saturer la bande passante réseau, créant un risque de déni de service.

```
Get-VMHost | Select-Object MaximumVirtualMachineMigrations, MaximumStorageMigrations
```

AUDIT :

- **Valeur attendue :** MaximumVirtualMachineMigrations <= 4, MaximumStorageMigrations <= 2

REMÉDIATION :

1. **PowerShell :**

```
Set-VMHost -MaximumVirtualMachineMigrations 2 -MaximumStorageMigrations 2
```

VALEUR PAR DÉFAUT :
MaximumVirtualMachineMigrations = 2

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

7.2.1 *Hyper-V Replica — chiffrement HTTPS avec certificats*

DESCRIPTION :
La réplication Hyper-V (Hyper-V Replica) doit utiliser HTTPS avec des certificats X.509 pour le chiffrement et l'authentification mutuelle. La réplication transfère l'intégralité des données des disques virtuels et les modifications en cours sur le réseau. L'utilisation de HTTP (port 80) sans chiffrement expose toutes ces données à l'interception. La réplication via certificats garantit également que seuls les serveurs autorisés peuvent recevoir les réplicas.

```
# Vérifier la configuration de la réplication sur l'hôte
Get-VMReplicationServer | Select-Object ReplicationEnabled, AuthenticationType, AllowedAuthenticationType, CertificateThumbprint, D

# Vérifier les VMs répliquées
Get-VM | Get-VMReplication -ErrorAction SilentlyContinue | Select-Object VMName, State, Health, Mode, ReplicaServerName, Authentica
```

AUDIT :

- **Valeur attendue :** AuthenticationType = Certificate (HTTPS, port 443)

REMÉDIATION :

1. **PowerShell :**

```
# Configurer la réplication avec certificats
$cert = Get-ChildItem Cert:\LocalMachine\My | Where-Object { $_.EnhancedKeyUsageList.ObjectId -contains "1.3.6.1.5.5.7.3.1" }
Set-VMReplicationServer -ReplicationEnabled $true -AllowedAuthenticationType Certificate -CertificateThumbprint $cert.Thumbprint -D
```

VALEUR PAR DÉFAUT :
Réplication désactivée

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

7.2.2 *Hyper-V Replica — autorisation par serveur*

DESCRIPTION :
La réplication Hyper-V doit être configurée avec une liste explicite de serveurs autorisés plutôt que d'accepter les réplications de n'importe quel serveur authentifié. Cette restriction empêche un serveur compromis ou non autorisé de recevoir les données de réplication des VMs sensibles.

```
# Vérifier les serveurs autorisés pour la réplication
Get-VMReplicationServer | Select-Object -ExpandProperty ReplicationAllowedFromAnyServer

# Si la liste est restreinte
Get-VMReplicationAuthorizationEntry | Select-Object AllowedPrimaryServer, ReplicaStorageLocation, TrustGroup
```

AUDIT :

- **Valeur attendue :** ReplicationAllowedFromAnyServer = False, liste explicite de serveurs

REMÉDIATION :

1. **PowerShell :**

```
# Ajouter un serveur autorisé spécifique
New-VMReplicationAuthorizationEntry -AllowedPrimaryServer "HV-PRIMARY.domain.local" -ReplicaStorageLocation "D:\Replica\HV-PRIMARY"
```

VALEUR PAR DÉFAUT :
Accepter tout serveur authentifié

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

7.3.1 *Failover Clustering — sécurité du cluster*

DESCRIPTION :
Le Failover Cluster hébergeant les hôtes Hyper-V doit être sécurisé avec une authentification Kerberos, un chiffrement des communications inter-noeuds, et des permissions d'administration restrictives. L'objet Cluster Name Object (CNO) dans Active Directory doit avoir des permissions minimales. Le cluster doit utiliser un réseau dédié pour le heartbeat et les communications inter-noeuds.

```
# Vérifier la configuration du cluster
Get-Cluster | Select-Object Name, SharedVolumesRoot, QuorumResource, SecurityLevel

# Vérifier les noeuds et leur état
Get-ClusterNode | Select-Object Name, State, NodeWeight

# Vérifier les réseaux du cluster
Get-ClusterNetwork | Select-Object Name, State, Role, Address

# Vérifier le chiffrement du cluster (Server 2025)
(Get-Cluster).BlockCacheSize
(Get-Cluster).SecurityLevel
```

AUDIT :

- **Valeur attendue :** Tous les noeuds en état "Up", SecurityLevel = "EncryptMessages"

REMÉDIATION :

1. **PowerShell :**

```
# Activer le chiffrement des communications cluster
(Get-Cluster).SecurityLevel = 2  # Chiffrer les messages
```

REMÉDIATION :

1. Séparer les réseaux cluster (heartbeat, migration, CSV)

VALEUR PAR DÉFAUT :
SecurityLevel = Sign (signature sans chiffrement)

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

7.3.2 *Cluster Shared Volumes (CSV) — sécurité*

DESCRIPTION :
Les Cluster Shared Volumes (CSV) utilisés pour stocker les fichiers VM dans un cluster Hyper-V doivent être sécurisés. Les permissions sur les CSV doivent être restrictives, le chiffrement BitLocker doit être activé sur les CSV contenant des données sensibles, et la redirection des I/O CSV doit être surveillée.

```
# Vérifier les CSV et leur état
Get-ClusterSharedVolume | Select-Object Name, State, @{N='FreeSpace';E={$_.SharedVolumeInfo.Partition.FreeSpace}}

# Vérifier BitLocker sur les CSV
Get-BitLockerVolume | Where-Object { $_.MountPoint -like "*ClusterStorage*" } | Select-Object MountPoint, VolumeStatus, ProtectionS

# Vérifier les permissions
Get-Acl "C:\ClusterStorage\Volume1" | Select-Object -ExpandProperty Access | Select-Object IdentityReference, FileSystemRights
```

REMÉDIATION :

1. Activer BitLocker sur les volumes CSV
2. Restreindre les ACL des CSV
3. Surveiller la redirection des I/O CSV

VALEUR PAR DÉFAUT :
Permissions héritées, BitLocker désactivé

Preuve d'audit :

```
| Résultat | _____________________________________________ |
| Capture  | ☐ Oui ☐ Non                                   |
| Note     | _____________________________________________ |
```

7.3.3 *Quorum et témoin du cluster — résilience*

DESCRIPTION :
Le quorum du cluster Hyper-V doit être correctement configuré avec un témoin (File Share Witness, Cloud Witness ou Disk Witness) pour assurer la résilience en cas de défaillance de noeuds. Le témoin du quorum ne doit pas être hébergé sur les mêmes systèmes de stockage que les VMs pour éviter un point de défaillance unique.

```
# Vérifier la configuration du quorum
Get-ClusterQuorum | Select-Object Cluster, QuorumResource, QuorumType

# Détails du témoin
Get-ClusterResource | Where-Object ResourceType -like "*Witness*" | Get-ClusterParameter | Select-Object Name, Value
```

AUDIT :

- **Valeur attendue :** QuorumType avec témoin configuré (Cloud Witness recommandé)

REMÉDIATION :

1. **PowerShell :**

```
# Configurer un Cloud Witness
Set-ClusterQuorum -CloudWitness -AccountName "storageaccount" -AccessKey "key" -Endpoint "core.windows.net"

# Ou File Share Witness
Set-ClusterQuorum -FileShareWitness "\\fileserver\witness"
```

VALEUR PAR DÉFAUT :
Quorum automatique (node majority)

Preuve d'audit :

```
| Résultat | _____________________________________________ |
| Capture  | ☐ Oui ☐ Non                                   |
| Note     | _____________________________________________ |
```

7.3.4 *Anti-affinity rules pour les VMs critiques*

DESCRIPTION :
Des règles d'anti-affinité doivent être configurées dans le cluster pour garantir que les VMs critiques interdépendantes (contrôleurs de domaine redondants, noeuds de base de données HA, etc.) ne s'exécutent jamais sur le même hôte physique. Cela assure qu'une défaillance d'un seul hôte ne provoque pas la perte de toutes les instances d'un service critique.

```
# Vérifier les groupes d'anti-affinité
Get-ClusterGroup | Get-ClusterParameter -Name AntiAffinityClassNames -ErrorAction SilentlyContinue | Select-Object ClusterObject, V

# Vérifier la répartition des VMs critiques
Get-ClusterGroup | Where-Object GroupType -eq "VirtualMachine" | Select-Object Name, OwnerNode, State
```

REMÉDIATION :

1. **PowerShell :**

```
# Configurer l'anti-affinité entre deux VMs
$group1 = Get-ClusterGroup "VM-DC01"
$group2 = Get-ClusterGroup "VM-DC02"
$group1 | Set-ClusterParameter -Name AntiAffinityClassNames -Value "DomainControllers"
$group2 | Set-ClusterParameter -Name AntiAffinityClassNames -Value "DomainControllers"
```

VALEUR PAR DÉFAUT :
Aucune règle d'anti-affinité

Preuve d'audit :

```
| Résultat | _____________________________________________ |
| Capture  | ☐ Oui ☐ Non                                   |
| Note     | _____________________________________________ |
```

VALEUR PAR DÉFAUT :
═══

Section 8 — SAUVEGARDE ET REPRISE D'ACTIVITÉ

8.0 — SAUVEGARDE ET REPRISE D'ACTIVITÉ

8.1.1 *Stratégie de sauvegarde des VMs documentée*

DESCRIPTION :
Une stratégie de sauvegarde documentée doit couvrir toutes les VMs hébergées sur l'infrastructure Hyper-V. La stratégie doit définir la fréquence de sauvegarde (RPO), le temps de restauration cible (RTO), les méthodes de sauvegarde (niveau hôte, niveau invité, snapshots), la rétention et les procédures de test. La règle 3-2-1 (3 copies, 2 supports, 1 hors site) doit être respectée.

```
# Vérifier Windows Server Backup
Get-WBPolicy -ErrorAction SilentlyContinue | Select-Object Schedule, BackupTargets, VolumesToBackup

# Vérifier les VMs incluses dans la sauvegarde
Get-WBPolicy -ErrorAction SilentlyContinue | Get-WBVirtualMachine

# Vérifier l'historique des sauvegardes
Get-WBBackupSet -ErrorAction SilentlyContinue | Select-Object BackupTime, BackupTarget | Sort-Object BackupTime -Descending | Selec
```

AUDIT :

- **Valeur attendue :** Politique de sauvegarde active, toutes les VMs critiques incluses

REMÉDIATION :

1. Documenter la stratégie de sauvegarde
2. Configurer la sauvegarde automatique
3. Tester la restauration régulièrement

VALEUR PAR DÉFAUT :
Aucune sauvegarde configurée

Preuve d'audit :

```
| Résultat | _____________________________________________ |
| Capture  | ☐ Oui ☐ Non                                   |
| Note     | _____________________________________________ |
```

8.1.2 *Sauvegardes chiffrées et stockées hors site*

DESCRIPTION :
Les sauvegardes des VMs doivent être chiffrées au repos et en transit, et stockées dans un emplacement sécurisé hors site (géographiquement distinct). Les sauvegardes non chiffrées contiennent l'intégralité des données des VMs et constituent une cible de choix pour l'exfiltration. Le stockage hors site protège contre les sinistres physiques (incendie, inondation) et les ransomwares qui ciblent les sauvegardes locales.

```
# Vérifier les cibles de sauvegarde
Get-WBPolicy -ErrorAction SilentlyContinue | Select-Object -ExpandProperty BackupTargets

# Vérifier si les sauvegardes sont sur un emplacement distant
# Dépend de la solution de sauvegarde (Veeam, DPM, Azure Backup, etc.)
```

REMÉDIATION :

1. Configurer le chiffrement des sauvegardes
2. Configurer un site de sauvegarde secondaire
3. Utiliser Azure Backup ou une solution tierce avec chiffrement AES-256

VALEUR PAR DÉFAUT :
Sauvegardes locales non chiffrées

Preuve d'audit :

```
| Résultat | _____________________________________________ |
| Capture  | ☐ Oui ☐ Non                                   |
| Note     | _____________________________________________ |
```

8.2.1 *Checkpoints/Snapshots — politique d'utilisation restrictive*

DESCRIPTION :
L'utilisation des checkpoints (snapshots) Hyper-V doit être encadrée par une politique stricte. Les checkpoints ne doivent pas être utilisés comme mécanisme de sauvegarde. Les checkpoints standard capturent l'état mémoire de la VM (y compris les identifiants en mémoire) dans des fichiers .vsv/.vmrs accessibles depuis l'hôte. Les checkpoints de production (utilisant VSS) sont préférables car ils ne capturent pas l'état mémoire.

```
# Vérifier le type de checkpoint configuré
Get-VM | Select-Object Name, CheckpointType
# Standard, ProductionOnly, Production (Production avec fallback Standard)

# Vérifier les checkpoints existants
Get-VM | Get-VMCheckpoint | Select-Object VMName, Name, CreationTime, @{N='AgeDays';E={(New-TimeSpan -Start $_.CreationTime -End (G

# Vérifier les checkpoints anciens (> 7 jours)
Get-VM | Get-VMCheckpoint | Where-Object { (New-TimeSpan -Start $_.CreationTime -End (Get-Date)).Days -gt 7 } | Select-Object VMNam
```

AUDIT :

- **Valeur attendue :** CheckpointType = Production ou ProductionOnly, pas de checkpoints anciens

REMÉDIATION :

1. **PowerShell :**

```
# Configurer les checkpoints de production uniquement
Set-VM -Name "VMName" -CheckpointType ProductionOnly

# Supprimer les checkpoints anciens
Get-VM | Get-VMCheckpoint | Where-Object { (New-TimeSpan -Start $_.CreationTime -End (Get-Date)).Days -gt 7 } | Remove-VMCheckpoint
```

VALEUR PAR DÉFAUT :
CheckpointType = Production (avec fallback Standard)

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

8.2.2 *Checkpoints désactivés sur les VMs de production critiques*

DESCRIPTION :
Sur les VMs de production critiques (contrôleurs de domaine, serveurs de base de données), les checkpoints doivent être complètement désactivés pour éviter les problèmes de cohérence (notamment l'USN rollback sur les DC) et pour empêcher la capture non autorisée de l'état mémoire. La sauvegarde de ces VMs doit utiliser des solutions de sauvegarde dédiées (Windows Server Backup, DPM, Veeam, etc.).

```
# Vérifier si les checkpoints sont activés
Get-VM | Select-Object Name, CheckpointType, @{N='CheckpointsEnabled';E={$_.CheckpointType -ne 'Disabled'}}

# VMs critiques avec checkpoints activés
Get-VM | Where-Object { $_.CheckpointType -ne 'Disabled' -and $_.Name -match "DC|SQL|AD|ADDS" } | Select-Object Name, CheckpointTyp
```

REMÉDIATION :

1. **PowerShell :**

```
# Désactiver les checkpoints sur les VMs critiques
Set-VM -Name "DC01" -CheckpointType Disabled
Set-VM -Name "SQL-PROD" -CheckpointType Disabled
```

VALEUR PAR DÉFAUT :
Checkpoints activés (type Production)

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

8.3.1 *Export/Import de VMs — procédure sécurisée*

DESCRIPTION :
L'export et l'import de VMs doivent suivre une procédure documentée et contrôlée. L'export d'une VM crée une copie complète incluant les disques virtuels, la configuration et potentiellement l'état mémoire. Ces fichiers exportés contiennent toutes les données de la VM et doivent être protégés contre l'accès non autorisé, chiffrés lors du transport et supprimés de manière sécurisée après utilisation.

```
# Vérifier les exports récents (journaux d'événements)
Get-WinEvent -FilterHashtable @{LogName='Microsoft-Windows-Hyper-V-VMMS-Admin'; Id=@(13002,13003)} -MaxEvents 20 -ErrorAction Silen

# Vérifier les répertoires d'export par défaut
Get-VMHost | Select-Object VirtualMachinePath, VirtualHardDiskPath
```

REMÉDIATION :
1. Documenter la procédure d'export/import avec approbation
2. Chiffrer les fichiers exportés (BitLocker sur le volume de destination)
3. Journaliser toutes les opérations d'export/import

VALEUR PAR DÉFAUT :
Export autorisé pour les administrateurs Hyper-V

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

8.3.2 *Tests de restauration réguliers*

DESCRIPTION :
Des tests de restauration des sauvegardes VM doivent être effectués régulièrement (au minimum trimestriellement) pour vérifier l'intégrité des sauvegardes et la capacité à restaurer les VMs dans les délais RTO définis. Les tests doivent couvrir la restauration complète de VMs (y compris les Shielded VMs) et la vérification de la cohérence des données restaurées.

AUDIT :
- Vérifier la date du dernier test de restauration documenté
- Vérifier les rapports de tests de restauration
- Vérifier le RTO mesuré vs RTO cible

REMÉDIATION :
1. Planifier des tests de restauration trimestriels
2. Documenter les résultats et les temps de restauration
3. Corriger les problèmes identifiés lors des tests

VALEUR PAR DÉFAUT :
Aucun test de restauration planifié

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

VALEUR PAR DÉFAUT :
═══

9.0 — JOURNALISATION ET MONITORING

9.1.1 *Journaux Hyper-V VMMS activés et surveillés*

DESCRIPTION :
Les journaux d'événements Hyper-V VMMS (Virtual Machine Management Service) doivent être activés et surveillés. Ces journaux enregistrent les événements critiques de gestion des VMs : création, suppression, modification de configuration, démarrage, arrêt, migration. Les Event IDs clés incluent : 13000-13010 (opérations VM), 18500-18512 (migration), 20400-20500 (réplication), 12400-12500 (sécurité).

```
# Vérifier les journaux Hyper-V
$hvLogs = @(
    "Microsoft-Windows-Hyper-V-VMMS-Admin",
    "Microsoft-Windows-Hyper-V-VMMS-Operational",
    "Microsoft-Windows-Hyper-V-Worker-Admin",
    "Microsoft-Windows-Hyper-V-Worker-Operational",
    "Microsoft-Windows-Hyper-V-Hypervisor-Admin",
    "Microsoft-Windows-Hyper-V-Hypervisor-Operational"
)
foreach ($log in $hvLogs) {
    Get-WinEvent -ListLog $log -ErrorAction SilentlyContinue | Select-Object LogName, IsEnabled, MaximumSizeInBytes, RecordCount
}

# Événements critiques récents
Get-WinEvent -FilterHashtable @{LogName='Microsoft-Windows-Hyper-V-VMMS-Admin'; StartTime=(Get-Date).AddDays(-7)} -MaxEvents 50 -Er
```

AUDIT :

- **Valeur attendue :** Tous les journaux Hyper-V activés, taille appropriée

REMÉDIATION :

1. **PowerShell :**

```
# Activer et dimensionner les journaux Hyper-V
foreach ($log in $hvLogs) {
    wevtutil sl $log /e:true /ms:268435456
}
```

VALEUR PAR DÉFAUT :
Activés avec taille par défaut (1 Mo)

Preuve d'audit :

```
| Résultat | _____________________________________________ |
| Capture  | ☐ Oui ☐ Non                                   |
| Note     | _____________________________________________ |
```

9.1.2 *Event IDs critiques Hyper-V surveillés*

DESCRIPTION :
Les Event IDs suivants doivent être spécifiquement surveillés et transmis au SIEM pour analyse et alerting :

```
# Vérifier les événements critiques récents
$criticalIds = @(13000,13002,13003,13010,18500,18502,18504,18512,20400,20500)
Get-WinEvent -FilterHashtable @{LogName='Microsoft-Windows-Hyper-V-VMMS-Admin'; Id=$criticalIds; StartTime=(Get-Date).AddDays(-30)}
```

REMÉDIATION :

1. Configurer des règles d'alerte dans le SIEM pour ces Event IDs
2. Créer des tableaux de bord de suivi des événements Hyper-V

VALEUR PAR DÉFAUT :
Événements enregistrés localement sans alerting

Preuve d'audit :

```
| Résultat | _____________________________________________ |
| Capture  | ☐ Oui ☐ Non                                   |
| Note     | _____________________________________________ |
```

9.2.1 *Performance monitoring — métriques clés*

DESCRIPTION :
Les métriques de performance de l'hôte Hyper-V et des VMs doivent être surveillées en continu pour détecter les anomalies de consommation de ressources (CPU, mémoire, disque, réseau) qui pourraient indiquer un crypto-mining, un déni de service, une exfiltration de données ou une compromission.

```
# Vérifier les compteurs de performance Hyper-V
Get-Counter -ListSet "Hyper-V*" | Select-Object CounterSetName

# Métriques clés
Get-Counter "\Hyper-V Hypervisor Logical Processor(_Total)\% Total Run Time" -ErrorAction SilentlyContinue
Get-Counter "\Hyper-V Dynamic Memory Balancer(*)\Available Memory" -ErrorAction SilentlyContinue

# Métriques de ressources VM
Get-VM | Measure-VMResourcePool -ErrorAction SilentlyContinue
Get-VM | Select-Object Name, CPUUsage, MemoryAssigned, MemoryDemand, Uptime
```

REMÉDIATION :
1. Configurer la collecte de métriques de performance Hyper-V
2. Définir des seuils d'alerte (CPU > 90%, Mémoire > 95%)
3. Intégrer avec SCOM ou une solution de monitoring

VALEUR PAR DÉFAUT :
Monitoring de base via Hyper-V Manager

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

9.2.2 *SIEM integration — collecte des événements Hyper-V*

DESCRIPTION :
Tous les journaux d'événements Hyper-V doivent être collectés et transmis au SIEM centralisé pour permettre la corrélation d'événements entre les hôtes Hyper-V, les VMs, les équipements réseau et les systèmes de stockage. La centralisation des logs protège contre la suppression de traces par un attaquant ayant compromis l'hôte.

```
# Vérifier l'agent SIEM
Get-Service *splunk*, *elastic*, *winlogbeat*, *nxlog*, *MMA*, *HealthService* -ErrorAction SilentlyContinue | Select-Object Name,

# Vérifier Windows Event Forwarding (WEF)
wecutil es 2>$null | Select-Object -First 10

# Vérifier les subscriptions WEF
wecutil gs HyperV-Events 2>$null
```

REMÉDIATION :
1. Déployer un agent SIEM ou configurer Windows Event Forwarding
2. Inclure les journaux Hyper-V dans la collecte
3. Créer des règles de corrélation et d'alerte spécifiques

VALEUR PAR DÉFAUT :
Aucune intégration SIEM

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

9.3.1 *Alertes critiques VM/Host configurées*

DESCRIPTION :
Des alertes automatiques doivent être configurées pour les événements critiques suivants : perte de heartbeat d'une VM, échec de Live Migration, échec de réplication, perte de quorum du cluster, dégradation du pool de stockage, ajout/suppression non autorisé de VM, échec d'attestation HGS, expiration de certificats HGS.

```
# Vérifier les actions programmées d'alerte
Get-ScheduledTask | Where-Object { $_.TaskName -like "*Hyper*" -or $_.TaskName -like "*VM*" -or $_.TaskName -like "*Alert*" } | Sel

# Vérifier les règles d'alerte SCOM (si déployé)
# Dépend de la solution de monitoring
```

REMÉDIATION :
1. Configurer des alertes dans le SIEM/SCOM pour les événements critiques
2. Configurer des notifications par email/SMS pour les alertes critiques
3. Documenter le processus d'escalade

VALEUR PAR DÉFAUT :
Aucune alerte configurée

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

VALEUR PAR DÉFAUT :
═══

Section 10 — SÉCURITÉ DES CONTENEURS (Windows Containers sur Hyper-V)

10.0 — SÉCURITÉ DES CONTENEURS (Windows Containers sur Hyper-V)

10.1.1 *Isolation Hyper-V pour les conteneurs sensibles*

DESCRIPTION :
Les conteneurs Windows exécutant des charges de travail sensibles ou multi-locataires doivent utiliser l'isolation Hyper-V plutôt que l'isolation de processus. L'isolation Hyper-V exécute chaque conteneur dans une VM utilitaire légère, fournissant une isolation au niveau de l'hyperviseur qui empêche les attaques d'évasion de conteneur d'affecter l'hôte ou les autres conteneurs.

```
# Vérifier les conteneurs en cours d'exécution et leur type d'isolation
docker ps --format "table {{.ID}}\t{{.Image}}\t{{.Status}}" 2>$null
Get-ComputeProcess | Select-Object Id, Type, Owner

# Vérifier le type d'isolation d'un conteneur
docker inspect --format '{{.HostConfig.Isolation}}' <container_id> 2>$null
```

AUDIT :

- **Valeur attendue :** Isolation = "hyperv" pour les conteneurs sensibles

REMÉDIATION :

1. **Docker :**

```
# Exécuter un conteneur avec isolation Hyper-V
docker run --isolation=hyperv -d mcr.microsoft.com/windows/servercore:ltsc2025 cmd
```

REMÉDIATION :

1. Configurer l'isolation par défaut dans le daemon Docker :

```
{
  "exec-opts": ["isolation=hyperv"]
}
```

VALEUR PAR DÉFAUT :
Isolation de processus

Preuve d'audit :

```
| Résultat | _____________________________________________ |
| Capture  | ☐ Oui ☐ Non                                   |
| Note     | _____________________________________________ |
```

10.1.2 *Images de base conteneurs — sources approuvées*

DESCRIPTION :
Seules les images de conteneurs provenant de sources approuvées (Microsoft Container Registry — mcr.microsoft.com, registre privé d'entreprise) doivent être utilisées. Les images tierces non vérifiées peuvent contenir des malwares, des backdoors ou des vulnérabilités connues. Les images doivent être scannées pour les vulnérabilités avant utilisation.

```
# Lister les images disponibles
docker images --format "table {{.Repository}}\t{{.Tag}}\t{{.Size}}\t{{.CreatedAt}}" 2>$null

# Vérifier les registres configurés
docker info 2>$null | Select-String "Registry"

# Vérifier les politiques de pull d'images
Get-Content "C:\ProgramData\Docker\config\daemon.json" -ErrorAction SilentlyContinue
```

AUDIT :

- **Valeur attendue :** Images provenant de mcr.microsoft.com ou registre privé d'entreprise uniquement

REMÉDIATION :

1. Configurer un registre privé (Azure Container Registry, Harbor)
2. Scanner les images avec des outils de vulnérabilité (Trivy, Qualys)
3. Restreindre les registres autorisés dans la configuration Docker

VALEUR PAR DÉFAUT :
Accès à Docker Hub et MCR

Preuve d'audit :

```
| Résultat | _____________________________________________ |
| Capture  | ☐ Oui ☐ Non                                   |
| Note     | _____________________________________________ |
```

10.2.1 *Réseau de conteneurs — isolation et segmentation*

DESCRIPTION :
Les réseaux de conteneurs doivent être segmentés pour isoler les conteneurs par zone de sécurité. Les réseaux Docker (NAT, Transparent, Overlay, L2Bridge) doivent être choisis en fonction des besoins d'isolation. Les conteneurs multi-locataires doivent utiliser des réseaux séparés avec des règles de pare-feu appropriées.

```
# Lister les réseaux Docker
docker network ls 2>$null
docker network inspect bridge 2>$null

# Vérifier les réseaux HNS (Host Networking Service)
Get-HNSNetwork | Select-Object Name, Type, Subnets
```

REMÉDIATION :
1. Créer des réseaux séparés par zone de sécurité
2. Appliquer des politiques réseau pour restreindre la communication inter-conteneurs

VALEUR PAR DÉFAUT :
Réseau NAT par défaut

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

10.2.2 *Mises à jour des images de conteneurs*

DESCRIPTION :
Les images de conteneurs doivent être régulièrement mises à jour pour intégrer les correctifs de sécurité. Les images Windows Server Core et Nano Server sont mises à jour mensuellement par Microsoft. Un processus de reconstruction et de redéploiement des images doit être en place pour appliquer les correctifs de manière continue.

```
# Vérifier l'ancienneté des images
docker images --format "table {{.Repository}}\t{{.Tag}}\t{{.CreatedAt}}" 2>$null

# Comparer avec la dernière version disponible
docker pull mcr.microsoft.com/windows/servercore:ltsc2025 --dry-run 2>$null
```

REMÉDIATION :
1. Automatiser la mise à jour des images de base
2. Reconstruire les images applicatives après chaque mise à jour de l'image de base
3. Intégrer la mise à jour dans le pipeline CI/CD

VALEUR PAR DÉFAUT :
Pas de mise à jour automatique des images

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

10.2.3 *Privilèges des conteneurs — moindre privilège*

DESCRIPTION :
Les conteneurs Windows ne doivent pas être exécutés avec des privilèges élevés sauf nécessité absolue. Les conteneurs privilégiés ont accès à des ressources système supplémentaires et un risque accru d'évasion vers l'hôte. Les conteneurs doivent s'exécuter avec un utilisateur non-root/non-administrateur lorsque possible.

```
# Vérifier les conteneurs privilégiés
docker inspect --format '{{.HostConfig.Privileged}} {{.Config.User}}' $(docker ps -q) 2>$null
```

REMÉDIATION :
1. Utiliser l'instruction USER dans le Dockerfile pour un utilisateur non-administrateur
2. Ne pas utiliser --privileged
3. Utiliser l'isolation Hyper-V pour les conteneurs nécessitant des privilèges élevés

VALEUR PAR DÉFAUT :
ContainerAdministrator (privilégié)

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

VALEUR PAR DÉFAUT :
═══

11.0 — SCVMM ET GESTION CENTRALISÉE

11.1.1 *SCVMM — compte de service sécurisé*

DESCRIPTION :
Le compte de service SCVMM doit être un gMSA (Group Managed Service Account) avec des permissions minimales. Ce compte a accès à tous les hôtes Hyper-V gérés et sa compromission donnerait un contrôle total sur l'ensemble de l'infrastructure de virtualisation.

```
# Vérifier le compte de service SCVMM
Get-WmiObject Win32_Service | Where-Object { $_.Name -like "*SCVMM*" -or $_.Name -like "*VMMService*" } | Select-Object Name, Start

# Vérifier si c'est un gMSA
Get-ADServiceAccount -Filter { Name -like "*VMM*" } -ErrorAction SilentlyContinue
```

REMÉDIATION :
1. Migrer le service SCVMM vers un compte gMSA
2. Appliquer le principe de moindre privilège au compte de service

VALEUR PAR DÉFAUT :
Compte de service local ou de domaine standard

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

11.1.2 *SCVMM — base de données chiffrée*

DESCRIPTION :
La base de données SQL Server de SCVMM contient les configurations de toutes les VMs, les informations sur les hôtes Hyper-V, les modèles de VM et les bibliothèques. Cette base doit être chiffrée avec TDE (Transparent Data Encryption) et les communications avec SQL Server doivent utiliser TLS. L'accès à la base de données doit être restreint.

```
# Vérifier la connexion SQL SCVMM
Get-ItemProperty "HKLM:\SOFTWARE\Microsoft\Microsoft System Center Virtual Machine Manager Server\Setup" -ErrorAction SilentlyConti

# Sur le serveur SQL : vérifier TDE
# SELECT name, is_encrypted FROM sys.databases WHERE name = 'VirtualManagerDB'
```

REMÉDIATION :
1. Activer TDE sur la base de données SCVMM
2. Configurer TLS pour les connexions SQL
3. Restreindre l'accès à la base de données

VALEUR PAR DÉFAUT :
Base non chiffrée, TLS non configuré

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

11.1.3 *SCVMM — communications chiffrées avec les hôtes*

DESCRIPTION :
Les communications entre le serveur SCVMM et les hôtes Hyper-V gérés doivent être chiffrées. SCVMM utilise WinRM pour communiquer avec les hôtes. Le chiffrement WinRM (HTTPS) et l'authentification Kerberos doivent être configurés pour protéger les commandes d'administration et les identifiants en transit.

```
# Vérifier la configuration SCVMM
Get-SCVMMServer | Select-Object Name, Port, FQDN

# Vérifier les paramètres de communication
Get-SCVMHost | Select-Object ComputerName, CommunicationState, OperatingSystemVersion
```

REMÉDIATION :
1. Configurer WinRM HTTPS sur tous les hôtes Hyper-V gérés
2. Utiliser l'authentification Kerberos
3. Vérifier les certificats utilisés pour WinRM

VALEUR PAR DÉFAUT :
Communication chiffrée via Kerberos

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

11.2.1 *Windows Admin Center — certificat HTTPS et accès restreint*

DESCRIPTION :
Windows Admin Center (WAC) doit utiliser un certificat TLS valide émis par une autorité de certification d'entreprise (pas un certificat auto-signé). L'accès à WAC doit être restreint aux administrateurs Hyper-V autorisés via des permissions RBAC intégrées. WAC doit être déployé sur un serveur dédié en mode passerelle (Gateway mode).

```
# Vérifier le certificat WAC
$wacCert = Get-ChildItem Cert:\LocalMachine\My | Where-Object { $_.FriendlyName -like "*Windows Admin Center*" }
if ($wacCert) {
    $wacCert | Select-Object Subject, Issuer, NotAfter, @{N='DaysRemaining';E={($_.NotAfter - (Get-Date)).Days}}
}

# Vérifier le service WAC
Get-Service ServerManagementGateway -ErrorAction SilentlyContinue | Select-Object Name, Status
```

REMÉDIATION :

1. Configurer un certificat TLS d'entreprise pour WAC
2. Restreindre l'accès via des groupes AD dédiés
3. Déployer WAC en mode Gateway sur un serveur dédié

VALEUR PAR DÉFAUT :
Certificat auto-signé, accès local

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

11.3.1 *PowerShell Direct — contrôle d'utilisation*

DESCRIPTION :
PowerShell Direct permet l'exécution de commandes PowerShell dans une VM depuis l'hôte Hyper-V via VMBus, sans nécessiter de connectivité réseau. Cette fonctionnalité contourne les pare-feux et la segmentation réseau. L'utilisation de PowerShell Direct doit être surveillée et restreinte aux opérations de maintenance documentées. Les commandes Invoke-Command -VMName et Enter-PSSession -VMName doivent être auditées.

```
# Vérifier les connexions PowerShell Direct récentes (journaux d'événements)
Get-WinEvent -FilterHashtable @{LogName='Microsoft-Windows-Hyper-V-VmSwitch-Operational'; StartTime=(Get-Date).AddDays(-7)} -MaxEve

# Vérifier la journalisation PowerShell pour les commandes Invoke-Command -VMName
Get-WinEvent -FilterHashtable @{LogName='Microsoft-Windows-PowerShell/Operational'; Id=4104; StartTime=(Get-Date).AddDays(-7)} -Err
```

REMÉDIATION :

1. Activer la journalisation PowerShell Script Block Logging
2. Créer des alertes SIEM pour les commandes PowerShell Direct
3. Restreindre l'accès aux seuls administrateurs nécessitant un accès direct aux VMs

VALEUR PAR DÉFAUT :
Disponible pour tous les administrateurs Hyper-V

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

11.3.2 *Automatisation et scripting — contrôle des scripts*

DESCRIPTION :
Les scripts d'automatisation Hyper-V (PowerShell, DSC) doivent être signés numériquement, versionnés et stockés dans un dépôt de code sécurisé. La politique d'exécution de scripts PowerShell doit être configurée en AllSigned ou RemoteSigned pour empêcher l'exécution de scripts non autorisés. Les scripts modifiant la configuration des VMs ou de l'hôte doivent suivre un processus d'approbation.

```
# Vérifier la politique d'exécution PowerShell
Get-ExecutionPolicy -List

# Vérifier la politique de signature de scripts via GPO
Get-ItemProperty "HKLM:\SOFTWARE\Microsoft\PowerShell\1\ShellIds\Microsoft.PowerShell" -Name ExecutionPolicy -ErrorAction SilentlyC

# Vérifier les scripts déployés
Get-ChildItem -Path "C:\Scripts\Hyper-V\" -Recurse -Filter "*.ps1" -ErrorAction SilentlyContinue | ForEach-Object {
    $sig = Get-AuthenticodeSignature $_.FullName
    [PSCustomObject]@{Script=$_.Name; Status=$sig.Status; Signer=$sig.SignerCertificate.Subject}
}
```

REMÉDIATION :

1. **PowerShell :**

```
Set-ExecutionPolicy -ExecutionPolicy AllSigned -Scope LocalMachine
```

REMÉDIATION :

1. Signer tous les scripts avec un certificat de signature de code d'entreprise
2. Versionner les scripts dans un dépôt Git

VALEUR PAR DÉFAUT :
ExecutionPolicy = RemoteSigned

Preuve d'audit :

```
| Résultat | _____________________________________________ |
| Capture  | ☐ Oui ☐ Non                                   |
| Note     | _____________________________________________ |
```

VALEUR PAR DÉFAUT :
═══

Section 12 — CONFORMITÉ DES VMs INVITÉES

12.0 — CONFORMITÉ DES VMs INVITÉES

12.1.1 *Durcissement des systèmes d'exploitation invités*

DESCRIPTION :
Chaque système d'exploitation invité doit être durci conformément au CIS Benchmark applicable (Windows Server 2025, Windows Server 2022, Linux distributions). Le durcissement couvre les services, les comptes, les pare-feux, les politiques de mots de passe, les droits d'utilisateur et les paramètres de sécurité spécifiques à l'OS. Les templates de VM pré-durcis doivent être utilisés pour les nouveaux déploiements.

```
# Via PowerShell Direct — Vérifier le durcissement basique
Invoke-Command -VMName "VMName" -ScriptBlock {
    $results = @()
    $results += "Firewall: " + (Get-NetFirewallProfile | Where-Object Enabled | Select-Object -ExpandProperty Name) -join ', '
    $results += "PasswordComplexity: " + (net accounts | Select-String "complexity")
    $results += "WindowsUpdate: " + (Get-HotFix | Sort-Object InstalledOn -Descending | Select-Object -First 1).InstalledOn
    $results
} -Credential $cred
```

REMÉDIATION :

1. Appliquer le CIS Benchmark via GPO ou DSC
2. Utiliser des templates de VM pré-durcis
3. Auditer régulièrement la conformité avec des outils automatisés

VALEUR PAR DÉFAUT :
Configuration par défaut de l'OS (non durci)

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

12.1.2 *Antivirus dans les VMs invitées*

DESCRIPTION :
Chaque VM invitée doit disposer d'une protection antivirus/EDR active avec des signatures à jour. L'antivirus de l'hôte Hyper-V ne protège pas les VMs invitées — chaque VM doit avoir sa propre protection. Les solutions EDR (Endpoint Detection and Response) sont recommandées pour une détection avancée des menaces.

```
# Via PowerShell Direct
Invoke-Command -VMName "VMName" -ScriptBlock {
    Get-MpComputerStatus | Select-Object AntivirusEnabled, RealTimeProtectionEnabled, AntivirusSignatureLastUpdated, AntivirusSigna
} -Credential $cred
```

REMÉDIATION :

1. Déployer Windows Defender ou une solution EDR d'entreprise dans chaque VM
2. Configurer la mise à jour automatique des signatures
3. Centraliser la gestion antivirus (SCCM, Intune, console EDR)

VALEUR PAR DÉFAUT :
Windows Defender activé (Windows Server 2025)

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

12.1.3 *Mises à jour des VMs invitées*

DESCRIPTION :
Les systèmes d'exploitation et les applications dans les VMs invitées doivent être maintenus à jour avec les derniers correctifs de sécurité. Les VMs non corrigées sont vulnérables aux exploits connus et constituent un vecteur d'attaque pour les mouvements latéraux dans l'infrastructure virtualisée.

```
# Via PowerShell Direct — vérifier les mises à jour
Invoke-Command -VMName "VMName" -ScriptBlock {
    Get-HotFix | Sort-Object InstalledOn -Descending | Select-Object -First 5 HotFixID, Description, InstalledOn
    Write-Output "Dernière mise à jour : $((Get-HotFix | Sort-Object InstalledOn -Descending | Select-Object -First 1).InstalledOn)
} -Credential $cred
```

REMÉDIATION :
1. Configurer WSUS/SCCM pour les mises à jour automatiques des VMs
2. Planifier des fenêtres de maintenance régulières
3. Auditer la conformité des mises à jour

VALEUR PAR DÉFAUT :
Mises à jour automatiques (dépend de la configuration)

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

12.2.1 *Integration Services à jour dans les VMs invitées*

DESCRIPTION :
Les Integration Services (composants d'intégration Hyper-V) installés dans les VMs invitées doivent être à jour. Les versions obsolètes des Integration Services peuvent contenir des vulnérabilités et ne pas bénéficier des correctifs de sécurité les plus récents. Depuis Windows Server 2016/Windows 10, les Integration Services sont mis à jour via Windows Update.

```
# Vérifier la version des Integration Services de chaque VM
Get-VM | Select-Object Name, IntegrationServicesVersion, IntegrationServicesState

# VMs avec IS obsolètes
Get-VM | Where-Object { $_.IntegrationServicesState -ne 'UpToDate' } | Select-Object Name, IntegrationServicesVersion, IntegrationS
```

AUDIT :
- **Valeur attendue :** IntegrationServicesState = "UpToDate"

REMÉDIATION :
1. Mettre à jour les Integration Services via Windows Update dans la VM invitée
2. Pour les anciens OS invités : installer manuellement les Integration Services depuis le média Hyper-V

VALEUR PAR DÉFAUT :
Version installée lors de la création de la VM

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

12.2.2 *Agent de monitoring dans les VMs*

DESCRIPTION :
Un agent de monitoring (SCOM, Azure Monitor, Prometheus, etc.) doit être installé et fonctionnel dans chaque VM pour la surveillance des performances, la détection d'anomalies et l'alerte. Le monitoring au niveau de l'hôte Hyper-V ne fournit pas de visibilité sur les processus et services exécutés à l'intérieur des VMs.

```
# Via PowerShell Direct
Invoke-Command -VMName "VMName" -ScriptBlock {
    Get-Service *SCOM*, *Monitor*, *HealthService*, *MMA*, *AzureMonitor* -ErrorAction SilentlyContinue | Select-Object Name, Displ
} -Credential $cred
```

REMÉDIATION :
1. Déployer l'agent de monitoring dans toutes les VMs
2. Vérifier la connectivité de l'agent avec la console de monitoring centrale
3. Configurer les alertes spécifiques aux charges de travail de chaque VM

VALEUR PAR DÉFAUT :
Aucun agent de monitoring

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

VALEUR PAR DÉFAUT :
═══

13.0 — NESTED VIRTUALIZATION ET SCÉNARIOS AVANCÉS

13.1.1 *Nested Virtualization — contrôle d'utilisation*

DESCRIPTION :
La virtualisation imbriquée (Nested Virtualization) permet d'exécuter Hyper-V à l'intérieur d'une VM Hyper-V. Cette fonctionnalité augmente significativement la surface d'attaque et la complexité de l'isolation. Les VMs imbriquées sont plus difficiles à sécuriser et à surveiller. L'utilisation de la virtualisation imbriquée doit être strictement limitée aux scénarios de test/développement et ne doit jamais être utilisée en production sans justification forte et mesures de sécurité supplémentaires.

```
# Vérifier les VMs avec Nested Virtualization activée
Get-VM | Get-VMProcessor | Where-Object { $_.ExposeVirtualizationExtensions -eq $true } | Select-Object VMName, ExposeVirtualizatio

# Vérifier la mémoire dynamique (incompatible avec NV)
Get-VM | Where-Object { (Get-VMProcessor -VMName $_.Name).ExposeVirtualizationExtensions } | Select-Object Name, DynamicMemoryEnabl
```

AUDIT :

- **Valeur attendue :** ExposeVirtualizationExtensions = False (sauf environnements de test documentés)

REMÉDIATION :

1. **PowerShell :**

```
# Désactiver la virtualisation imbriquée
Set-VMProcessor -VMName "VMName" -ExposeVirtualizationExtensions $false
```

REMÉDIATION :

1. Documenter et justifier chaque utilisation de virtualisation imbriquée

VALEUR PAR DÉFAUT :
Désactivé

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

13.1.2 *VMs masquant leur environnement de virtualisation*

DESCRIPTION :
Certaines VMs peuvent être configurées pour masquer leur environnement de virtualisation (compatible mode pour les anciennes applications ou pour les VMs utilisant du licensing sensible à la virtualisation). Cette configuration peut être utilisée par des attaquants pour créer des VMs indétectables par les outils de sécurité et pour exécuter des malwares qui détectent et évitent les environnements virtualisés.

```
# Vérifier les VMs avec CompatibilityForOlderOperatingSystemsEnabled
Get-VM | Get-VMProcessor | Where-Object { $_.CompatibilityForOlderOperatingSystemsEnabled } | Select-Object VMName

# Vérifier les paramètres de compatibilité
Get-VM | Get-VMProcessor | Select-Object VMName, CompatibilityForMigrationEnabled, CompatibilityForOlderOperatingSystemsEnabled
```

REMÉDIATION :

1. Désactiver CompatibilityForOlderOperatingSystemsEnabled sauf nécessité documentée
2. Surveiller les VMs avec des configurations de masquage

VALEUR PAR DÉFAUT :
Désactivé

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

13.1.3 *Contrôle des VMs avec accès matériel direct (passthrough)*

DESCRIPTION :
Les VMs avec accès matériel direct (passthrough disks, DDA, Virtual Fibre Channel) doivent être inventoriées et leur justification documentée. L'accès matériel direct contourne l'abstraction de l'hyperviseur et augmente la surface d'attaque. Chaque accès passthrough doit être justifié par un besoin de performance ou de fonctionnalité spécifique.

```
# Vérifier les disques passthrough
Get-VM | Get-VMHardDiskDrive | Where-Object { $_.DiskNumber -ne $null } | Select-Object VMName, DiskNumber, Path

# Vérifier les Fibre Channel HBAs virtuels
Get-VM | Get-VMFibreChannelHba -ErrorAction SilentlyContinue | Select-Object VMName, WorldWideNodeNameSetA

# Vérifier les DDA
Get-VM | ForEach-Object {
    Get-VMAssignableDevice -VMName $_.Name -ErrorAction SilentlyContinue | Select-Object @{N='VM';E={$_.VMName}}, InstanceID
}
```

REMÉDIATION :
1. Documenter et justifier chaque accès matériel direct
2. Remplacer le passthrough par des VHDX lorsque possible
3. S'assurer que l'IOMMU est activé pour DDA

VALEUR PAR DÉFAUT :
Aucun accès matériel direct

Preuve d'audit :

```
| Résultat | _____________________________________________ |
| Capture  | ☐ Oui ☐ Non                                   |
| Note     | _____________________________________________ |
```

VALEUR PAR DÉFAUT :
═══

14.0 — SÉCURITÉ AZURE STACK HCI

14.1.1 *Azure Stack HCI — version et mises à jour*

DESCRIPTION :
Azure Stack HCI doit être maintenu à la dernière version avec les mises à jour de sécurité appliquées. Azure Stack HCI suit un modèle de mise à jour différent de Windows Server standard, avec des mises à jour mensuelles (Quality Updates) et des mises à jour de fonctionnalité (Feature Updates). Les mises à jour peuvent être gérées via Windows Admin Center ou Azure Update Manager.

```
# Vérifier la version Azure Stack HCI
Get-ItemProperty "HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion" | Select-Object ProductName, DisplayVersion, CurrentBuildNumb

# Vérifier les mises à jour en attente via Azure
Get-AzStackHciUpdate -ErrorAction SilentlyContinue

# Vérifier l'état de la solution-update
Get-SolutionUpdate -ErrorAction SilentlyContinue | Select-Object Version, State, Description
```

REMÉDIATION :
1. Appliquer les mises à jour via Windows Admin Center ou Azure Update Manager
2. Configurer la mise à jour automatique si applicable

VALEUR PAR DÉFAUT :
Mises à jour manuelles

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

14.1.2 *Azure Arc — enregistrement et conformité*

DESCRIPTION :
Azure Stack HCI doit être enregistré dans Azure Arc pour la gestion centralisée, la conformité des politiques Azure et la surveillance de sécurité. Azure Arc permet d'appliquer des politiques Azure (Azure Policy), d'auditer la conformité et de déployer des extensions de sécurité comme Microsoft Defender for Cloud.

```
# Vérifier l'enregistrement Azure Arc
Get-AzureStackHCI | Select-Object ClusterStatus, RegistrationStatus, ConnectionStatus

# Vérifier l'agent Azure Arc
Get-Service himds -ErrorAction SilentlyContinue | Select-Object Name, Status

# Vérifier les extensions Arc installées
azcmagent show 2>$null
```

REMÉDIATION :
1. Enregistrer le cluster Azure Stack HCI dans Azure Arc
2. Configurer les politiques Azure de conformité
3. Activer Microsoft Defender for Cloud

VALEUR PAR DÉFAUT :
Non enregistré dans Azure Arc

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

14.1.3 *Azure Policy — conformité de sécurité*

DESCRIPTION :
Des politiques Azure doivent être assignées au cluster Azure Stack HCI pour vérifier la conformité de sécurité en continu. Les politiques recommandées incluent : vérification du chiffrement BitLocker, validation de la configuration de sécurité, audit des accès administratifs et conformité aux benchmarks de sécurité.

AUDIT :

- Vérifier dans le portail Azure : Azure Stack HCI > Politiques > Conformité
- Vérifier les politiques assignées et leur statut de conformité

REMÉDIATION :

1. Assigner les politiques Azure de sécurité recommandées
2. Configurer la remédiation automatique lorsque possible
3. Surveiller le tableau de bord de conformité Azure

VALEUR PAR DÉFAUT :
Aucune politique assignée

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

VALEUR PAR DÉFAUT :
═══

15.0 — PROTECTION CONTRE LES ATTAQUES DE VIRTUALISATION

15.1.1 *Mitigations VM Escape — correctifs et configuration*

DESCRIPTION :
L'évasion de VM (VM Escape) est l'attaque la plus critique en virtualisation : un attaquant exploite une vulnérabilité de l'hyperviseur depuis une VM invitée pour exécuter du code sur l'hôte et accéder à toutes les VMs. Les mitigations incluent : application des correctifs Hyper-V, réduction de la surface d'attaque (désactivation des services d'intégration non nécessaires), utilisation de Shielded VMs, et isolation de la mémoire via SLAT et les mitigations side-channel.

```
# Vérifier les correctifs critiques Hyper-V récents
Get-HotFix | Where-Object { $_.Description -like "*Security*" } | Sort-Object InstalledOn -Descending | Select-Object -First 10

# Vérifier les mitigations de surface d'attaque
Get-VM | ForEach-Object {
    $vm = $_
    $services = Get-VMIntegrationService -VMName $vm.Name | Where-Object Enabled
    [PSCustomObject]@{
        VM = $vm.Name
        EnabledServices = ($services.Name -join ', ')
        ServiceCount = $services.Count
    }
}

# Vérifier les composants d'émulation (vecteur d'attaque principal)
Get-Item C:\Windows\System32\vmwp.exe | Select-Object -ExpandProperty VersionInfo
Get-Item C:\Windows\System32\drivers\vmswitch.sys | Select-Object -ExpandProperty VersionInfo
```

REMÉDIATION :
1. Appliquer immédiatement les correctifs de sécurité Hyper-V
2. Minimiser les services d'intégration activés
3. Utiliser des VMs de Génération 2 avec Secure Boot
4. Déployer des Shielded VMs pour les charges sensibles

VALEUR PAR DÉFAUT :
Dépend du niveau de correctifs

Preuve d'audit :

```
| Résultat | _____________________________________________ |
| Capture  | ☐ Oui ☐ Non                                   |
| Note     | _____________________________________________ |
```

15.1.2 *Attaques par canal auxiliaire (Spectre, Meltdown, L1TF, MDS, MMIO)*

DESCRIPTION :
Les attaques par canal auxiliaire (side-channel attacks) exploitent les failles microarchitecturales des processeurs pour extraire des données entre les contextes d'isolation (entre VMs, entre VM et hôte). Les variantes connues incluent Spectre (CVE-2017-5753, CVE-2017-5715), Meltdown (CVE-2017-5754), L1 Terminal Fault/Foreshadow (CVE-2018-3615, CVE-2018-3646), MDS/Zombieload (CVE-2018-12126, CVE-2019-11091) et MMIO Stale Data (CVE-2022-21123). Les correctifs microcode et OS doivent être appliqués.

```
# Installer le module de vérification
Install-Module SpeculationControl -Force -ErrorAction SilentlyContinue
Get-SpeculationControlSettings

# Vérifier les mitigations activées dans le registre
Get-ItemProperty "HKLM:\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management" -Name FeatureSettingsOverride, FeatureS

# Vérifier le microcode CPU
Get-WmiObject Win32_Processor | Select-Object Name, Description, Revision

# Vérifier l'exposition des mitigations aux VMs invitées
Get-VM | Get-VMProcessor | Select-Object VMName, @{N='HwThreadCountPerCore';E={$_.HwThreadCountPerCore}}
```

AUDIT :

- **Valeur attendue :** Toutes les mitigations activées (BTIHardwarePresent, BTIKernelRetpolineEnabled, etc.)

REMÉDIATION :

1. Appliquer les mises à jour du microcode CPU (via BIOS/UEFI firmware update)
2. Appliquer les correctifs Windows contre les side-channel attacks
3. **PowerShell :**

```
# Activer les mitigations (valeurs pour Spectre + L1TF + MDS)
Set-ItemProperty "HKLM:\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management" -Name FeatureSettingsOverride -Value 72
Set-ItemProperty "HKLM:\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management" -Name FeatureSettingsOverrideMask -Valu
```

REMÉDIATION :

1. Considérer la désactivation de l'HyperThreading pour les charges ultra-sensibles

VALEUR PAR DÉFAUT :
Mitigations activées après application des correctifs

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

15.2.1 *Réduction de la surface d'attaque Hyper-V*

DESCRIPTION :
La surface d'attaque de l'hyperviseur Hyper-V doit être réduite au minimum. Cela inclut la désactivation des interfaces d'émulation non nécessaires (COM ports, disquettes, IDE pour les VMs Gen2), la limitation des services d'intégration, la désactivation de l'Enhanced Session Mode, la suppression de RemoteFX vGPU, et la restriction des accès DDA/SR-IOV.

```
# Audit de surface d'attaque par VM
Get-VM | ForEach-Object {
    $vm = $_
    $is = Get-VMIntegrationService -VMName $vm.Name | Where-Object Enabled
    $sec = Get-VMSecurity -VMName $vm.Name
    $proc = Get-VMProcessor -VMName $vm.Name
    [PSCustomObject]@{
        VM = $vm.Name
        Generation = $vm.Generation
        IntServicesCount = $is.Count
        SecureBoot = if ($vm.Generation -eq 2) { (Get-VMFirmware -VMName $vm.Name).SecureBoot } else { "N/A" }
        vTPM = $sec.TpmEnabled
        Shielded = $sec.Shielded
        NestedVirt = $proc.ExposeVirtualizationExtensions
        EnhancedSession = (Get-VMHost).EnableEnhancedSessionMode
    }
}
```

REMÉDIATION :

1. Appliquer les recommandations des contrôles précédents (sections 1, 3, 4)
2. Créer un baseline de sécurité VM et le vérifier régulièrement
3. Automatiser la vérification de conformité

VALEUR PAR DÉFAUT :
Surface d'attaque par défaut (non optimisée)

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

15.2.2 *Protection contre les attaques firmware*

DESCRIPTION :
Le firmware du serveur physique (UEFI/BIOS, BMC/IPMI/iLO/iDRAC) doit être à jour et sécurisé. Les attaques de firmware sont persistantes (survivent aux réinstallations OS) et peuvent compromettre l'hyperviseur avant même son chargement. Le Secure Boot et le Measured Boot (via TPM) protègent la chaîne de démarrage mais le firmware lui-même doit être sécurisé.

```
# Vérifier le Secure Boot
Confirm-SecureBootUEFI

# Vérifier la version du firmware UEFI
Get-WmiObject -Class Win32_BIOS | Select-Object Manufacturer, Name, Version, SMBIOSBIOSVersion, ReleaseDate

# Vérifier l'accès BMC/IPMI
Get-WmiObject -Namespace root\WMI -Class MSAcpi_ThermalZoneTemperature -ErrorAction SilentlyContinue
```

REMÉDIATION :
1. Mettre à jour le firmware UEFI à la dernière version
2. Configurer le mot de passe du BIOS/UEFI
3. Sécuriser l'accès BMC/iLO/iDRAC (réseau de gestion dédié, HTTPS, mot de passe fort)
4. Activer Secure Boot et le verrouillage UEFI

VALEUR PAR DÉFAUT :
Firmware installé en usine

Preuve d'audit :

```
| Résultat | _____________________________________________ |
| Capture  | ☐ Oui ☐ Non                                   |
| Note     | _____________________________________________ |
```

15.3.1 *Contrôle de la chaîne d'approvisionnement des images VM*

DESCRIPTION :
Les images de VM (templates VHDX, ISO, Shielding Data Files) doivent provenir de sources fiables et vérifiées. Les images doivent être signées numériquement ou vérifiées par hash avant utilisation. L'utilisation d'images non vérifiées peut introduire des malwares, des backdoors ou des configurations vulnérables dans l'infrastructure. Les bibliothèques de templates SCVMM doivent être protégées.

```
# Vérifier les templates dans la bibliothèque SCVMM
Get-SCVMTemplate | Select-Object Name, Owner, AddedTime -ErrorAction SilentlyContinue

# Vérifier les ISO disponibles
Get-ChildItem -Path (Get-VMHost).VirtualHardDiskPath -Filter "*.iso" -ErrorAction SilentlyContinue | Select-Object Name, LastWriteT

# Vérifier les VHDX templates
Get-ChildItem -Path (Get-VMHost).VirtualHardDiskPath -Filter "*.vhdx" -ErrorAction SilentlyContinue | Where-Object { $_.Name -like
```

REMÉDIATION :
1. Créer et maintenir des templates sécurisés (golden images)
2. Signer les images avec des certificats d'entreprise
3. Vérifier les hash des images avant utilisation
4. Protéger les bibliothèques SCVMM avec des ACL restrictives

VALEUR PAR DÉFAUT :
Aucun contrôle de chaîne d'approvisionnement

Preuve d'audit :

```
| Résultat | _____________________________________________ |
| Capture  | ☐ Oui ☐ Non                                   |
| Note     | _____________________________________________ |
```

VALEUR PAR DÉFAUT :
═══

16.0 — RÉSEAU ET SEGMENTATION AVANCÉE

16.1.1 *Micro-segmentation — isolation inter-VM*

DESCRIPTION :
La micro-segmentation doit être implémentée pour contrôler le trafic réseau entre les VMs au sein d'un même segment réseau (East-West traffic). Contrairement à la segmentation traditionnelle (North-South), la micro-segmentation utilise des politiques réseau au niveau du port virtuel pour empêcher les mouvements latéraux entre VMs sur le même VLAN. Cela est réalisable via les Extended Port ACLs, le SDN Network Controller ou des solutions tierces (NSX-T, Cisco ACI).

```
# Vérifier les ACLs de port étendues
Get-VM | Get-VMNetworkAdapter | Get-VMNetworkAdapterExtendedAcl | Select-Object VMName, Direction, Action, LocalIPAddress, RemoteIP

# Vérifier les Network Security Groups SDN (si déployé)
Get-NetworkControllerAccessControlList -ErrorAction SilentlyContinue | ForEach-Object {
    [PSCustomObject]@{
        Name = $_.ResourceId
        Rules = ($_.Properties.AclRules | Measure-Object).Count
    }
}

# Vérifier l'isolation entre VMs du même VLAN
Get-VM | Get-VMNetworkAdapter | Select-Object VMName, Name, SwitchName, @{N='VLAN';E={(Get-VMNetworkAdapterVlan -VMNetworkAdapter $
```

AUDIT :

- **Valeur attendue :** ACLs ou politiques SDN en place pour le trafic East-West

REMÉDIATION :

1. **Option 1 — Extended Port ACLs :**

```
# Autoriser uniquement les flux nécessaires entre VMs
Add-VMNetworkAdapterExtendedAcl -VMName "WebServer" -Direction Outbound -Action Allow -RemoteIPAddress "10.0.1.20" -RemotePort "143
Add-VMNetworkAdapterExtendedAcl -VMName "WebServer" -Direction Outbound -Action Deny -Weight 1
```

REMÉDIATION :

1. **Option 2 — SDN Network Controller** avec Network Security Groups
2. **Option 3 — Solutions tierces** de micro-segmentation

VALEUR PAR DÉFAUT :
Aucune micro-segmentation

Preuve d'audit :

```
| Résultat | _____________________________________________ |
| Capture  | ☐ Oui ☐ Non                                   |
| Note     | _____________________________________________ |
```

16.1.2 *Zones de sécurité réseau documentées et appliquées*

DESCRIPTION :
Les zones de sécurité réseau (DMZ, Production, Développement, Gestion, Sauvegarde) doivent être clairement documentées et appliquées via des Virtual Switches séparés et/ou des VLANs distincts. Chaque zone doit avoir des règles de filtrage explicites pour le trafic inter-zones. Les VMs ne doivent pas être connectées simultanément à plusieurs zones de sécurité (sauf les pare-feux virtuels).

```
# Vérifier les switches par zone
Get-VMSwitch | Select-Object Name, SwitchType, Notes

# Vérifier les VMs multi-connectées (potentiel bridge entre zones)
Get-VM | ForEach-Object {
    $adapters = Get-VMNetworkAdapter -VMName $_.Name
    if ($adapters.Count -gt 1) {
        [PSCustomObject]@{
            VM = $_.Name
            Adapters = $adapters.Count
            Switches = ($adapters.SwitchName -join ', ')
            VLANs = (($adapters | Get-VMNetworkAdapterVlan).AccessVlanId -join ', ')
        }
    }
}
```

AUDIT :

- **Valeur attendue :** Documentation des zones, pas de VMs bridgeant des zones (sauf pare-feux)

REMÉDIATION :

1. Documenter l'architecture des zones de sécurité
2. Créer des Virtual Switches dédiés par zone quand possible
3. Appliquer le filtrage inter-zones via VLAN + pare-feu physique/virtuel

VALEUR PAR DÉFAUT :
Aucune segmentation en zones

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

16.1.3 *Port Mirroring — contrôle et audit*

DESCRIPTION :
Le Port Mirroring sur les switches virtuels Hyper-V doit être contrôlé et audité. Le Port Mirroring permet de copier tout le trafic réseau d'un port vers un autre pour l'analyse ou le monitoring. Si mal configuré ou exploité par un attaquant, le port mirroring peut être utilisé pour l'interception de trafic réseau de toutes les VMs du switch.

```
# Vérifier les configurations de Port Mirroring
Get-VM | Get-VMNetworkAdapter | Where-Object { $_.PortMirroringMode -ne 'None' } | Select-Object VMName, Name, PortMirroringMode

# PortMirroringMode : None, Source, Destination
```

AUDIT :

- **Valeur attendue :** Aucun port mirroring non documenté et approuvé

REMÉDIATION :

1. **Désactiver le port mirroring non autorisé :**

```
Get-VM | Get-VMNetworkAdapter | Where-Object { $_.PortMirroringMode -ne 'None' } | Set-VMNetworkAdapter -PortMirroringMode None
```

REMÉDIATION :

1. Documenter et approuver chaque configuration de port mirroring
2. Surveiller les changements de configuration de port mirroring

VALEUR PAR DÉFAUT :
Port Mirroring désactivé (None)

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

16.2.1 *IPv6 — configuration sécurisée ou désactivation*

DESCRIPTION :
Si IPv6 n'est pas utilisé dans l'infrastructure Hyper-V, il doit être désactivé sur les adaptateurs réseau virtuels pour empêcher les attaques IPv6 (RA spoofing, DHCPv6 rogue, etc.). Si IPv6 est utilisé, le Router Guard et le DHCP Guard doivent être configurés pour les deux protocoles.

```
# Vérifier IPv6 sur l'hôte
Get-NetAdapterBinding -ComponentID ms_tcpip6 | Select-Object Name, Enabled

# Vérifier IPv6 sur les adaptateurs VM
Get-VM | Get-VMNetworkAdapter | Select-Object VMName, Name, @{N='IPv6Addresses';E={$_.IPAddresses | Where-Object { $_ -match ':' }}
```

REMÉDIATION :

1. **Désactiver IPv6 si non utilisé :**

```
# Sur l'hôte
Disable-NetAdapterBinding -Name "*" -ComponentID ms_tcpip6
```

REMÉDIATION :

1. **Si IPv6 est utilisé :** Activer Router Guard et DHCP Guard

VALEUR PAR DÉFAUT :
IPv6 activé

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

VALEUR PAR DÉFAUT :
═══

17.0 — RÉPONSE AUX INCIDENTS VIRTUALISATION

17.1.1 *Plan de réponse aux incidents virtualisation documenté*

DESCRIPTION :
Un plan de réponse aux incidents spécifique à la virtualisation doit être documenté et testé. Ce plan doit couvrir les scénarios suivants : compromission de l'hôte Hyper-V, évasion de VM, ransomware dans une VM, compromission du cluster, perte du HGS, attaque sur la Live Migration, compromission d'un template VM. Le plan doit définir les procédures d'isolation, de collecte de preuves et de restauration.

AUDIT :

- Vérifier l'existence du plan de réponse aux incidents virtualisation
- Vérifier la date de la dernière révision (< 12 mois)
- Vérifier la date du dernier exercice/simulation

REMÉDIATION :

1. Rédiger un plan de réponse aux incidents virtualisation
2. Former les équipes d'exploitation Hyper-V aux procédures
3. Effectuer des exercices de simulation annuels

VALEUR PAR DÉFAUT :
Aucun plan spécifique

Preuve d'audit :

```
| Résultat | _____________________________________________ |
| Capture  | ☐ Oui ☐ Non                                   |
| Note     | _____________________________________________ |
```

17.1.2 *Procédure d'isolation d'une VM compromise*

DESCRIPTION :
Une procédure documentée doit décrire les étapes d'isolation d'une VM compromise sans détruire les preuves forensiques. L'isolation doit pouvoir être effectuée rapidement tout en préservant l'état de la VM pour l'analyse. Les actions incluent : déconnexion des adaptateurs réseau, prise de checkpoint forensique, sauvegarde de l'état mémoire, préservation des journaux.

```
# Commandes d'isolation rapide d'une VM (à documenter dans la procédure)
# Étape 1 : Déconnecter du réseau (sans éteindre)
# Disconnect-VMNetworkAdapter -VMName "CompromisedVM"
# Étape 2 : Prendre un checkpoint pour préserver l'état
# Checkpoint-VM -VMName "CompromisedVM" -SnapshotName "Forensic-$(Get-Date -Format 'yyyyMMdd-HHmmss')"
# Étape 3 : Exporter pour analyse forensique
# Export-VM -VMName "CompromisedVM" -Path "D:\Forensic\"

# Vérifier la documentation de la procédure
Test-Path "C:\Procedures\Incident-Response-VM-Isolation.pdf" -ErrorAction SilentlyContinue
```

REMÉDIATION :

1. Documenter la procédure d'isolation pas à pas
2. Créer des scripts d'isolation automatisés
3. Former les administrateurs à la procédure d'isolation
4. Tester la procédure régulièrement

VALEUR PAR DÉFAUT :
Aucune procédure documentée

Preuve d'audit :

```
| Résultat | _____________________________________________ |
| Capture  | ☐ Oui ☐ Non                                   |
| Note     | _____________________________________________ |
```

17.1.3 *Collecte de preuves forensiques virtualisées*

DESCRIPTION :
Les procédures de collecte de preuves forensiques doivent être adaptées à l'environnement virtualisé. La collecte doit inclure : l'état mémoire de la VM (fichiers .vmrs), les fichiers de disque virtuel (VHDX), les fichiers de configuration VM (.vmcx), les journaux Hyper-V de l'hôte, les journaux du switch virtuel, l'historique des checkpoints et les journaux de la VM invitée. L'intégrité des preuves doit être garantie par des hash cryptographiques.

```
# Outils et procédures de collecte forensique
# Vérifier la présence d'outils forensiques
Test-Path "C:\Tools\Forensic\" -ErrorAction SilentlyContinue

# Vérifier la capacité de stockage pour les exports forensiques
Get-Volume | Where-Object { $_.FileSystemLabel -like "*Forensic*" } -ErrorAction SilentlyContinue | Select-Object DriveLetter, Size
```

REMÉDIATION :
1. Préparer un kit forensique virtualisé (scripts, outils, espace de stockage)
2. Documenter la procédure de collecte de preuves
3. Former l'équipe de réponse aux incidents aux spécificités de la forensique virtualisée

VALEUR PAR DÉFAUT :
Aucun kit forensique préparé

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

17.2.1 *Procédure de réponse à une compromission de l'hôte Hyper-V*

DESCRIPTION :
Une procédure spécifique doit couvrir le scénario de compromission de l'hôte Hyper-V lui-même (le pire scénario en virtualisation). Ce scénario implique que toutes les VMs hébergées doivent être considérées comme potentiellement compromises. Les actions incluent : isolation réseau de l'hôte, migration d'urgence des VMs critiques vers un hôte de confiance, collecte forensique de l'hôte, reconstruction de l'hôte et re-attestation HGS.

AUDIT :
- Vérifier l'existence de la procédure spécifique
- Vérifier les critères de détection d'une compromission hôte
- Vérifier le plan de migration d'urgence des VMs

REMÉDIATION :
1. Rédiger la procédure de réponse à la compromission de l'hôte
2. Définir les critères d'escalade (quand considérer l'hôte comme compromis)
3. Préparer un plan de migration d'urgence vers des hôtes de secours
4. Tester la procédure lors d'exercices de sécurité

VALEUR PAR DÉFAUT :
Aucune procédure spécifique

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

17.2.2 *Communication et escalade en cas d'incident*

DESCRIPTION :
Un plan de communication et d'escalade doit définir les contacts d'urgence, les procédures de notification (interne, ANSSI si applicable, clients si données personnelles affectées), et les niveaux d'escalade selon la gravité de l'incident. La compromission d'un hôte Hyper-V peut affecter de nombreuses VMs et nécessite une communication rapide et efficace.

AUDIT :
- Vérifier l'existence du plan de communication
- Vérifier la liste des contacts d'urgence
- Vérifier la procédure de notification réglementaire (RGPD, NIS2)

REMÉDIATION :
1. Documenter le plan de communication et d'escalade
2. Maintenir la liste des contacts d'urgence à jour
3. Définir les obligations de notification (ANSSI, CNIL si données personnelles)

VALEUR PAR DÉFAUT :
Aucun plan de communication spécifique

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

VALEUR PAR DÉFAUT :
═══

18.0 — GOUVERNANCE ET CONFORMITÉ

18.1.1 *Politique de sécurité de la virtualisation documentée*

DESCRIPTION :
Une politique de sécurité spécifique à la virtualisation Hyper-V doit être documentée, approuvée par la direction et communiquée aux parties prenantes. Cette politique doit couvrir : les standards de configuration des hôtes et des VMs, la gestion des accès, la classification des VMs, les procédures de sauvegarde, la gestion des correctifs, la surveillance et la réponse aux incidents.

AUDIT :

- Vérifier l'existence de la politique de sécurité virtualisation
- Date de la dernière révision (< 12 mois)
- Approbation par la direction

REMÉDIATION :

1. Rédiger la politique de sécurité de la virtualisation
2. Faire approuver par le RSSI et la direction
3. Communiquer et former les équipes
4. Planifier une révision annuelle

VALEUR PAR DÉFAUT :
Aucune politique spécifique

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

18.1.2 *Gestion des changements pour l'infrastructure Hyper-V*

DESCRIPTION :
Un processus de gestion des changements (Change Management) formel doit être appliqué pour toutes les modifications de l'infrastructure Hyper-V : ajout/suppression de VMs, modification de la configuration des hôtes, changements réseau virtuel, mises à jour, modifications du Guarded Fabric. Chaque changement doit être approuvé, documenté et réversible.

AUDIT :

- Vérifier l'existence du processus de gestion des changements
- Vérifier les derniers changements documentés
- Vérifier le processus d'approbation des changements

REMÉDIATION :

1. Mettre en place un processus ITIL de gestion des changements
2. Utiliser un outil de ticketing pour les changements
3. Exiger une approbation avant chaque changement critique

VALEUR PAR DÉFAUT :
Aucun processus formel

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

18.1.3 *Inventaire des machines virtuelles à jour*

DESCRIPTION :
Un inventaire complet et à jour de toutes les machines virtuelles hébergées sur l'infrastructure Hyper-V doit être maintenu. L'inventaire doit inclure : le nom de la VM, l'hôte, le propriétaire, la classification de sécurité, la criticité métier, les systèmes d'exploitation, les applications hébergées, les ressources allouées, la date de création et la date de dernière vérification. Les VMs orphelines ou non documentées doivent être identifiées et traitées.

```
# Générer l'inventaire des VMs
Get-VM | Select-Object Name, State, CPUUsage, @{N='MemoryGB';E={[math]::Round($_.MemoryAssigned/1GB,2)}}, Generation, Version, Path

# Identifier les VMs arrêtées depuis longtemps
Get-VM | Where-Object { $_.State -eq 'Off' } | Select-Object Name, State, CreationTime, @{N='Notes';E={$_.Notes}}
```

REMÉDIATION :
1. Mettre en place un processus d'inventaire automatisé
2. Assigner un propriétaire à chaque VM
3. Supprimer ou archiver les VMs orphelines
4. Vérifier l'inventaire trimestriellement

VALEUR PAR DÉFAUT :
Inventaire Hyper-V Manager (non formalisé)

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

18.2.1 *Conformité RGPD — données personnelles dans les VMs*

DESCRIPTION :
Les VMs contenant des données personnelles soumises au RGPD doivent être identifiées et des mesures de protection appropriées doivent être en place : chiffrement des données au repos (BitLocker, Shielded VMs), chiffrement en transit, contrôle d'accès strict, journalisation des accès, procédures de notification en cas de violation de données, et documentation de l'analyse d'impact (DPIA).

AUDIT :
- Vérifier l'inventaire des VMs contenant des données personnelles
- Vérifier les mesures de protection en place
- Vérifier la DPIA si traitements à risque
- Vérifier la procédure de notification en cas de violation

REMÉDIATION :
1. Identifier et classifier les VMs avec données personnelles
2. Appliquer les Shielded VMs pour les VMs les plus sensibles
3. Documenter l'analyse d'impact (DPIA)
4. Mettre en place la procédure de notification sous 72h

VALEUR PAR DÉFAUT :
Aucune classification des données

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

18.2.2 *Conformité NIS2 — infrastructure essentielle*

DESCRIPTION :
Si l'organisation est soumise à la directive NIS2 (Network and Information Security), les exigences spécifiques de sécurité doivent être appliquées à l'infrastructure Hyper-V : gestion des risques, gestion des incidents, continuité d'activité, sécurité de la chaîne d'approvisionnement, tests de sécurité et notification des incidents significatifs.

AUDIT :
- Vérifier si l'organisation est soumise à NIS2
- Vérifier la conformité aux exigences NIS2 pour l'infrastructure de virtualisation
- Vérifier les procédures de notification d'incidents

REMÉDIATION :
1. Évaluer l'applicabilité de NIS2 à l'organisation
2. Réaliser une analyse de risques sur l'infrastructure Hyper-V
3. Mettre en oeuvre les mesures de sécurité requises par NIS2
4. Préparer les procédures de notification

VALEUR PAR DÉFAUT :
Non évalué

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

18.2.3 *Audit de sécurité périodique de l'infrastructure Hyper-V*

DESCRIPTION :
Un audit de sécurité de l'infrastructure Hyper-V doit être réalisé au minimum annuellement (et après chaque changement majeur). L'audit doit couvrir la configuration de l'hôte, les VMs, le réseau virtuel, le stockage, la gestion des accès, la journalisation et la conformité réglementaire. Les résultats de l'audit doivent être documentés et les actions correctives suivies.

AUDIT :

- Date du dernier audit de sécurité Hyper-V
- Rapport d'audit disponible
- Plan de remédiation des non-conformités identifiées
- Suivi des actions correctives

REMÉDIATION :

1. Planifier un audit de sécurité annuel de l'infrastructure Hyper-V
2. Utiliser cette checklist ANC comme référentiel d'audit
3. Documenter les résultats et suivre les actions correctives

VALEUR PAR DÉFAUT :
Aucun audit planifié

Preuve d'audit :

```
| Résultat | _____________________________________ |
| Capture  | ☐ Oui ☐ Non                           |
| Note     | _____________________________________ |
```

VALEUR PAR DÉFAUT :
═══

CONTRÔLES COMPLÉMENTAIRES — SECTIONS 1 À 18

═══

CONTRÔLES COMPLÉMENTAIRES

> **Note :** Les contrôles suivants complètent les sections précédentes avec des vérifications supplémentaires couvrant des aspects spécifiques de la sécurité Hyper-V.

1.10.1 *Protocole SMBv1 désactivé sur l'hôte*

DESCRIPTION :
SMBv1 est un protocole obsolète et vulnérable (WannaCry, EternalBlue) qui doit être complètement désactivé sur l'hôte Hyper-V. SMBv1 ne supporte pas le chiffrement et est sujet à de nombreuses vulnérabilités critiques.

```
Get-SmbServerConfiguration | Select-Object EnableSMB1Protocol
Get-WindowsOptionalFeature -Online -FeatureName SMB1Protocol
```

```
Set-SmbServerConfiguration -EnableSMB1Protocol $false -Force
Disable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol -NoRestart
```

VALEUR PAR DÉFAUT :
Désactivé sur Server 2025

1.10.2 *TLS 1.2/1.3 uniquement — protocoles obsolètes désactivés*

DESCRIPTION :
Les protocoles SSL 2.0, SSL 3.0, TLS 1.0 et TLS 1.1 doivent être désactivés sur l'hôte Hyper-V. Seuls TLS 1.2 et TLS 1.3 doivent être autorisés pour toutes les communications chiffrées.

```
$protocols = @("SSL 2.0", "SSL 3.0", "TLS 1.0", "TLS 1.1", "TLS 1.2", "TLS 1.3")
foreach ($p in $protocols) {
    $serverKey = "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\$p\Server"
    $val = Get-ItemProperty $serverKey -Name Enabled -ErrorAction SilentlyContinue
    Write-Output "$p Server: Enabled=$($val.Enabled)"
}
```

```
# Désactiver TLS 1.0 et 1.1
foreach ($p in @("SSL 2.0","SSL 3.0","TLS 1.0","TLS 1.1")) {
    New-Item "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\$p\Server" -Force
    Set-ItemProperty "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\$p\Server" -Name Enabled -Value 0
}
```

VALEUR PAR DÉFAUT :
TLS 1.0 et 1.1 encore disponibles

1.10.3 *Suites de chiffrement renforcées (Cipher Suites)*

DESCRIPTION :
Les suites de chiffrement faibles (RC4, DES, 3DES, NULL, Export) doivent être désactivées. Seules les suites utilisant AES-128-GCM, AES-256-GCM ou ChaCha20-Poly1305 avec échange de clés ECDHE ou DHE doivent être autorisées.

```
Get-TlsCipherSuite | Select-Object Name, CipherBlockLength, HashLength | Format-Table
```

```
# Désactiver les suites faibles
Disable-TlsCipherSuite -Name "TLS_RSA_WITH_3DES_EDE_CBC_SHA"
Disable-TlsCipherSuite -Name "TLS_RSA_WITH_RC4_128_SHA"
```

VALEUR PAR DÉFAUT :
Toutes les suites activées par défaut

1.10.4 *Windows Defender Application Control (WDAC)*

DESCRIPTION :
Windows Defender Application Control (WDAC) doit être configuré sur l'hôte Hyper-V pour n'autoriser que l'exécution des applications et scripts approuvés. WDAC utilise des politiques d'intégrité du code pour contrôler quels binaires peuvent s'exécuter.

```
Get-CimInstance -ClassName Win32_DeviceGuard -Namespace root\Microsoft\Windows\DeviceGuard | Select-Object CodeIntegrityPolicyEnfor
citool --list-policies 2>$null
```

```
# Créer et appliquer une politique WDAC
New-CIPolicy -FilePath "C:\CI\HVHostPolicy.xml" -Level Publisher -Fallback Hash -UserPEs
```

VALEUR PAR DÉFAUT :
WDAC non configuré

1.10.5 *Démarrage mesuré (Measured Boot) activé*

DESCRIPTION :
Le Measured Boot doit être activé sur l'hôte Hyper-V pour enregistrer les mesures de chaque composant chargé lors du démarrage dans les PCR (Platform Configuration Registers) du TPM. Ces mesures sont utilisées par le HGS pour l'attestation TPM.

```
Get-Tpm | Select-Object TpmReady
bcdedit /enum | Select-String "measuredboot"
Get-WinEvent -LogName "Microsoft-Windows-Measured Boot" -MaxEvents 5 -ErrorAction SilentlyContinue
```

```
bcdedit /set {default} measuredboot yes
```

VALEUR PAR DÉFAUT :
Activé si TPM présent

1.10.6 *Restriction des connexions sortantes de l'hôte*

DESCRIPTION :
Les connexions réseau sortantes depuis l'hôte Hyper-V doivent être restreintes aux seules destinations nécessaires (WSUS, KMS, NTP, DNS, DC, SIEM, SCVMM). Un hôte Hyper-V n'a pas besoin d'accéder à Internet directement.

```
Get-NetFirewallProfile | Select-Object Name, DefaultOutboundAction
Get-NetFirewallRule -Direction Outbound -Enabled True | Where-Object Action -eq "Allow" | Select-Object DisplayName | Sort-Object D
```

```
Set-NetFirewallProfile -Profile Domain,Private,Public -DefaultOutboundAction Block
# Créer des règles sortantes spécifiques pour les flux autorisés
```

VALEUR PAR DÉFAUT :
DefaultOutboundAction = Allow

2.7.1 *Restriction de connexion interactive sur l'hôte*

DESCRIPTION :
La connexion interactive locale et à distance sur l'hôte Hyper-V doit être restreinte aux seuls comptes d'administration Hyper-V autorisés. Les comptes utilisateur standard ne doivent pas pouvoir se connecter à l'hôte.

```
secedit /export /cfg C:\secpol.cfg
Select-String -Path C:\secpol.cfg -Pattern "SeInteractiveLogonRight|SeDenyInteractiveLogonRight|SeRemoteInteractiveLogonRight"
Remove-Item C:\secpol.cfg
```

REMÉDIATION :
GPO : Stratégie > Droits d'utilisateur > Autoriser/Refuser l'ouverture de session locale

VALEUR PAR DÉFAUT :
Tous les utilisateurs autorisés

2.7.2 *Timeout de session d'administration*

DESCRIPTION :
Un timeout d'inactivité doit être configuré pour les sessions d'administration (RDP, WinRM, VMConnect) afin de fermer automatiquement les sessions inactives et réduire le risque de détournement de session.

```
Get-ItemProperty "HKLM:\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services" -Name MaxIdleTime, MaxDisconnectionTime -ErrorAct
```

```
Set-ItemProperty "HKLM:\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services" -Name MaxIdleTime -Value 900000
Set-ItemProperty "HKLM:\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services" -Name MaxDisconnectionTime -Value 60000
```

VALEUR PAR DÉFAUT :
Pas de timeout

2.7.3 *Bannière d'avertissement légal à la connexion*

DESCRIPTION :
Un message d'avertissement légal doit être affiché avant la connexion à l'hôte Hyper-V pour informer les utilisateurs que le système est surveillé et que l'accès non autorisé est interdit.

```
Get-ItemProperty "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name LegalNoticeCaption, LegalNoticeText
```

```
Set-ItemProperty "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name LegalNoticeCaption -Value "AVERTISSEMENT"
Set-ItemProperty "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name LegalNoticeText -Value "Accès réservé aux
```

VALEUR PAR DÉFAUT :
Aucune bannière

3.7.1 *Automatic Start Action sécurisée*

DESCRIPTION :
L'action de démarrage automatique de chaque VM doit être configurée de manière appropriée. Les VMs critiques doivent être configurées pour démarrer automatiquement avec un délai approprié. Les VMs de test/développement ne doivent pas démarrer automatiquement.

```
Get-VM | Select-Object Name, AutomaticStartAction, AutomaticStartDelay, AutomaticStopAction
```

```
Set-VM -Name "CriticalVM" -AutomaticStartAction Start -AutomaticStartDelay 30
Set-VM -Name "TestVM" -AutomaticStartAction Nothing
Set-VM -Name "CriticalVM" -AutomaticStopAction ShutDown
```

VALEUR PAR DÉFAUT :
AutomaticStartAction = Nothing

3.7.2 *Automatic Stop Action — arrêt propre des VMs*

DESCRIPTION :
L'action d'arrêt automatique doit être configurée sur "ShutDown" (arrêt propre via les Integration Services) plutôt que "TurnOff" (coupure brutale) ou "Save" (sauvegarde de l'état mémoire sur disque) pour éviter la corruption de données et les fuites d'état mémoire.

```
Get-VM | Select-Object Name, AutomaticStopAction | Where-Object { $_.AutomaticStopAction -ne 'ShutDown' }
```

```
Get-VM | Set-VM -AutomaticStopAction ShutDown
```

VALEUR PAR DÉFAUT :
Save

3.7.3 *Notes et documentation des VMs*

DESCRIPTION :
Chaque VM doit avoir un champ Notes documenté contenant le propriétaire, la criticité, la date de création, la justification et le contact responsable.

```
Get-VM | Select-Object Name, Notes | Where-Object { [string]::IsNullOrWhiteSpace($_.Notes) }
```

```
Set-VM -Name "VMName" -Notes "Propriétaire: Equipe-Infra | Criticité: Haute | Application: ERP | Contact: admin@org.local"
```

VALEUR PAR DÉFAUT :
Notes vides

3.7.4 *Version de configuration VM à jour*

DESCRIPTION :
La version de configuration des VMs doit être mise à jour vers la dernière version supportée par l'hôte pour bénéficier des dernières fonctionnalités de sécurité et des correctifs.

```
Get-VM | Select-Object Name, Version, @{N='IsLatest';E={$_.Version -eq (Get-VMHostSupportedVersion | Sort-Object Version -Descendin
```

```
Update-VMVersion -VMName "VMName" -Force
```

VALEUR PAR DÉFAUT :
Version au moment de la création

4.4.1 *Politique de déploiement des Shielded VMs documentée*

DESCRIPTION :
Une politique définissant les critères de déploiement des Shielded VMs (quelles VMs, quel niveau de protection, quel mode d'attestation) doit être documentée et appliquée.

AUDIT :
Vérifier l'existence de la politique de classification et de déploiement des Shielded VMs.

REMÉDIATION :
Rédiger et faire approuver une politique de déploiement des Shielded VMs.

VALEUR PAR DÉFAUT :
Aucune politique

4.4.2 *HGS backup et disaster recovery*

DESCRIPTION :
Le Host Guardian Service doit être sauvegardé régulièrement, y compris les certificats de signature et de chiffrement, les politiques d'attestation et la base de données HGS. La perte du HGS empêche le démarrage de toutes les Shielded VMs.

```
# Sur le serveur HGS
Get-HgsServer | Select-Object *
Test-Path "C:\Backup\HGS\" -ErrorAction SilentlyContinue
```

```
# Sauvegarder les clés HGS
Export-HgsServerState -Path "C:\Backup\HGS\hgs-state-$(Get-Date -Format 'yyyyMMdd').xml"
```

VALEUR PAR DÉFAUT :
HGS non sauvegardé

5.7.1 *Adresses MAC statiques pour les VMs sensibles*

DESCRIPTION :
Les VMs sensibles doivent utiliser des adresses MAC statiques pour empêcher les changements d'adresse MAC non autorisés et faciliter le suivi réseau. Les adresses MAC dynamiques peuvent changer après un redémarrage.

```
Get-VM | Get-VMNetworkAdapter | Select-Object VMName, Name, MacAddress, DynamicMacAddressEnabled
Get-VM | Get-VMNetworkAdapter | Where-Object DynamicMacAddressEnabled | Select-Object VMName, Name
```

```
Set-VMNetworkAdapter -VMName "SensitiveVM" -StaticMacAddress "00155D010101"
```

VALEUR PAR DÉFAUT :
Adresse MAC dynamique

5.7.2 *IPsec pour le trafic inter-VM sensible*

DESCRIPTION :
Le trafic réseau sensible entre VMs (base de données, réplication AD, etc.) doit être protégé par IPsec pour assurer la confidentialité et l'intégrité des données en transit au sein du réseau virtuel.

```
Get-NetIPsecRule | Where-Object Enabled -eq True | Select-Object DisplayName, InboundSecurity, OutboundSecurity
Get-NetIPsecMainModeSA | Select-Object LocalAddress, RemoteAddress
```

REMÉDIATION :
Configurer des règles IPsec via GPO pour le trafic inter-VM sensible.

VALEUR PAR DÉFAUT :
IPsec non configuré

5.7.3 *Surveillance des flux réseau anormaux*

DESCRIPTION :
Les flux réseau entre les VMs et vers l'extérieur doivent être surveillés pour détecter les communications anormales (C2, exfiltration, scan de ports, mouvements latéraux). L'analyse des métadonnées de flux (NetFlow/IPFIX) sur le switch virtuel permet cette surveillance.

```
# Vérifier les compteurs réseau
Get-VM | Get-VMNetworkAdapter | Select-Object VMName, @{N='BytesSent';E={$_.BandwidthSetting}}, Status
# Vérifier les outils de monitoring réseau
Get-Service *NetFlow*, *ntopng* -ErrorAction SilentlyContinue
```

REMÉDIATION :
Déployer un IDS/IPS virtuel ou configurer la capture réseau sur le switch virtuel pour l'analyse.

VALEUR PAR DÉFAUT :
Aucune surveillance des flux

6.5.1 *Disques de différenciation — usage restreint en production*

DESCRIPTION :
Les disques de différenciation (differencing disks / AVHD/AVHDX) ne doivent pas être utilisés en production car ils créent une chaîne de dépendance fragile et des problèmes de performance. Les AVHDX résultant de checkpoints doivent être mergés régulièrement.

```
Get-VM | Get-VMHardDiskDrive | ForEach-Object {
    $vhd = Get-VHD $_.Path -ErrorAction SilentlyContinue
    if ($vhd.VhdType -eq 'Differencing') {
        [PSCustomObject]@{VM=$_.VMName; Path=$_.Path; Type=$vhd.VhdType; ParentPath=$vhd.ParentPath}
    }
}
```

```
# Merger les disques de différenciation
Merge-VHD -Path "C:\VMs\disk-diff.avhdx" -DestinationPath "C:\VMs\disk.vhdx"
```

VALEUR PAR DÉFAUT :
Pas de disques de différenciation (sauf checkpoints)

6.5.2 *Disques VHDX — taille fixe vs dynamique*

DESCRIPTION :
Les disques VHDX à taille fixe offrent de meilleures performances et prévisibilité. Les disques dynamiques peuvent croître et saturer le stockage de l'hôte. Pour les VMs de production, les disques à taille fixe sont recommandés.

```
Get-VM | Get-VMHardDiskDrive | ForEach-Object {
    $vhd = Get-VHD $_.Path -ErrorAction SilentlyContinue
    [PSCustomObject]@{VM=$_.VMName; Path=$_.Path; Type=$vhd.VhdType; Size=[math]::Round($vhd.Size/1GB,2); FileSize=[math]::Round($v
}
```

```
Convert-VHD -Path "C:\VMs\disk-dynamic.vhdx" -DestinationPath "C:\VMs\disk-fixed.vhdx" -VHDType Fixed
```

VALEUR PAR DÉFAUT :
Dynamique

7.4.1 *Drain roles before maintenance*

DESCRIPTION :
Avant toute maintenance planifiée d'un hôte Hyper-V dans un cluster, les VMs doivent être migrées (drainées) vers les autres noeuds de manière contrôlée pour éviter les interruptions de service.

```
Get-ClusterNode | Select-Object Name, State, DrainStatus, DrainTarget
```

```
Suspend-ClusterNode -Name "HV-Node01" -Drain -Wait
# Effectuer la maintenance
Resume-ClusterNode -Name "HV-Node01"
```

VALEUR PAR DÉFAUT :
Migration manuelle requise

7.4.2 *Preferred owners pour les VMs critiques*

DESCRIPTION :
Les propriétaires préférés (Preferred Owners) doivent être configurés pour les VMs critiques dans le cluster afin d'optimiser la répartition et garantir que les VMs reviennent sur leur hôte préféré après une maintenance.

```
Get-ClusterGroup | Where-Object GroupType -eq "VirtualMachine" | Get-ClusterOwnerNode | Select-Object ClusterObject, OwnerNodes
```

```
Set-ClusterOwnerNode -Group "VM-CriticalApp" -Owners "HV-Node01","HV-Node02"
```

VALEUR PAR DÉFAUT :
Tous les noeuds sont propriétaires

8.4.1 *DR avec Hyper-V Replica — test de basculement*

DESCRIPTION :
Les tests de basculement (failover) de la réplication Hyper-V doivent être effectués régulièrement pour valider la capacité de reprise d'activité. Le test de basculement crée une VM de test à partir du réplica sans interrompre la réplication en cours.

```
# Vérifier les réplications actives et leur santé
Get-VM | Get-VMReplication -ErrorAction SilentlyContinue | Select-Object VMName, State, Health, LastReplicationTime, FrequencySec
# Vérifier la date du dernier test de basculement
Get-VM | Get-VMReplication -ErrorAction SilentlyContinue | Select-Object VMName, @{N='LastTestFailover';E={$_.LastTestFailoverStart
```

```
# Exécuter un test de basculement
Start-VMFailover -VMName "CriticalVM" -AsTest -Confirm:$false
# Nettoyer après le test
Stop-VMFailover -VMName "CriticalVM"
```

VALEUR PAR DÉFAUT :
Aucun test planifié

8.4.2 *RPO et RTO définis et mesurés*

DESCRIPTION :
Les objectifs de point de reprise (RPO) et de temps de reprise (RTO) doivent être définis pour chaque catégorie de VM et mesurés lors des tests de basculement. Le RPO est déterminé par la fréquence de réplication (de 30 secondes à 15 minutes avec Hyper-V Replica).

```
Get-VM | Get-VMReplication -ErrorAction SilentlyContinue | Select-Object VMName, FrequencySec, @{N='RPO_Minutes';E={$_.FrequencySec
```

REMÉDIATION :
Configurer la fréquence de réplication en fonction du RPO défini pour chaque VM.

VALEUR PAR DÉFAUT :
RPO 5 minutes (300 secondes)

9.4.1 *Audit des modifications de configuration VM*

DESCRIPTION :
Toutes les modifications de configuration des VMs (ajout/suppression de matériel virtuel, changement de réseau, modification des Integration Services, changement de sécurité) doivent être auditées et enregistrées.

```
Get-WinEvent -FilterHashtable @{LogName='Microsoft-Windows-Hyper-V-VMMS-Admin'; Id=@(13001,32022); StartTime=(Get-Date).AddDays(-30
```

REMÉDIATION :
Configurer des alertes SIEM pour les Event IDs de modification de configuration VM.

VALEUR PAR DÉFAUT :
Événements enregistrés localement

9.4.2 *Monitoring de l'état de réplication*

DESCRIPTION :
L'état de la réplication Hyper-V doit être surveillé en continu. Les alertes doivent être configurées pour les échecs de réplication, les décalages de réplication supérieurs au RPO et les changements d'état de santé de la réplication.

```
Get-VM | Get-VMReplication -ErrorAction SilentlyContinue | Where-Object { $_.Health -ne 'Normal' } | Select-Object VMName, Health,
```

REMÉDIATION :
Configurer des alertes pour les réplications en erreur ou avertissement.

VALEUR PAR DÉFAUT :
Pas d'alerte automatique

9.4.3 *Surveillance de l'espace disque des volumes VM*

DESCRIPTION :
L'espace disque disponible sur les volumes hébergeant les fichiers VM doit être surveillé avec des seuils d'alerte. Un volume plein peut provoquer la pause automatique des VMs avec des disques dynamiques et la corruption de données.

```
Get-Volume | Where-Object { $_.DriveLetter } | Select-Object DriveLetter, FileSystemType, @{N='SizeGB';E={[math]::Round($_.Size/1GB
```

REMÉDIATION :
Configurer des alertes pour les volumes < 20% d'espace libre.

VALEUR PAR DÉFAUT :
Pas d'alerte configurée

10.3.1 *Runtime de conteneurs — version sécurisée*

DESCRIPTION :
Le runtime de conteneurs (Docker Engine, containerd) doit être à la dernière version stable avec les correctifs de sécurité appliqués.

```
docker version 2>$null
Get-Service docker -ErrorAction SilentlyContinue | Select-Object Name, Status
```

REMÉDIATION :
Mettre à jour le runtime Docker vers la dernière version.

VALEUR PAR DÉFAUT :
Version au moment de l'installation

10.3.2 *Logging des conteneurs centralisé*

DESCRIPTION :
Les journaux des conteneurs doivent être collectés et centralisés dans le SIEM pour la détection d'anomalies et l'investigation forensique.

```
docker info 2>$null | Select-String "Logging Driver"
```

REMÉDIATION :
Configurer un logging driver centralisé (fluentd, gelf, syslog).

VALEUR PAR DÉFAUT :
json-file (local)

11.4.1 *SCVMM — audit des actions administratives*

DESCRIPTION :
Les actions administratives effectuées via SCVMM doivent être journalisées et auditées, y compris les créations/suppressions de VMs, les modifications de configuration et les changements de permissions.

```
Get-SCJob | Where-Object { $_.StartTime -gt (Get-Date).AddDays(-7) } | Select-Object Name, StartTime, ResultName, Status, Owner | S
```

REMÉDIATION :
Activer l'audit complet dans SCVMM et intégrer avec le SIEM.

VALEUR PAR DÉFAUT :
Journalisation basique

11.4.2 *SCVMM — Run As Accounts protégés*

DESCRIPTION :
Les Run As Accounts dans SCVMM contiennent les identifiants utilisés pour gérer les hôtes Hyper-V et les ressources. Ces comptes doivent utiliser des gMSA lorsque possible et les mots de passe doivent être renouvelés régulièrement.

```
Get-SCRunAsAccount | Select-Object Name, UserName, Description -ErrorAction SilentlyContinue
```

REMÉDIATION :
Migrer les Run As Accounts vers des gMSA et auditer régulièrement.

VALEUR PAR DÉFAUT :
Comptes statiques avec mots de passe

12.3.1 *Templates de VM pré-durcis*

DESCRIPTION :
Des templates de VMs pré-durcis conformes aux CIS Benchmarks doivent être utilisés pour la création de nouvelles VMs. Cela garantit que chaque nouvelle VM démarre avec un niveau de sécurité minimal et réduit le risque de configurations par défaut vulnérables.

```
# Vérifier les templates dans la bibliothèque SCVMM
Get-SCVMTemplate | Select-Object Name, Description, Owner -ErrorAction SilentlyContinue

# Vérifier les VHDX templates
Get-ChildItem -Path (Get-VMHost).VirtualHardDiskPath -Filter "*template*" -Recurse -ErrorAction SilentlyContinue
```

REMÉDIATION :
Créer et maintenir des templates pré-durcis pour chaque OS supporté (Windows Server 2025, Windows Server 2022, Linux).

VALEUR PAR DÉFAUT :
Aucun template pré-durci

12.3.2 *Inventaire des logiciels installés dans les VMs*

DESCRIPTION :
L'inventaire des logiciels installés dans les VMs doit être maintenu et audité pour détecter les logiciels non autorisés, les versions obsolètes et les vulnérabilités connues.

```
Invoke-Command -VMName "VMName" -ScriptBlock {
    Get-WmiObject Win32_Product | Select-Object Name, Version, Vendor | Sort-Object Name
} -Credential $cred
```

REMÉDIATION :
Utiliser SCCM, Intune ou un outil d'inventaire pour maintenir un inventaire centralisé.

VALEUR PAR DÉFAUT :
Aucun inventaire centralisé

13.2.1 *VMs de test/développement isolées de la production*

DESCRIPTION :
Les VMs de test et développement doivent être strictement isolées des VMs de production, idéalement sur des hôtes Hyper-V séparés ou au minimum sur des réseaux virtuels distincts sans connectivité vers les VMs de production.

```
# Vérifier l'isolation réseau entre les environnements
Get-VM | Select-Object Name, @{N='Switch';E={(Get-VMNetworkAdapter -VMName $_.Name).SwitchName}}, Notes | Sort-Object Switch
```

REMÉDIATION :
Séparer les environnements de test et de production sur des réseaux distincts.

VALEUR PAR DÉFAUT :
Pas de séparation

14.2.1 *Microsoft Defender for Cloud activé sur Azure Stack HCI*

DESCRIPTION :
Microsoft Defender for Cloud doit être activé pour les clusters Azure Stack HCI pour fournir une évaluation de sécurité continue, des recommandations de durcissement et une détection des menaces avancées.

AUDIT :
Vérifier dans le portail Azure : Azure Stack HCI > Security > Microsoft Defender for Cloud

REMÉDIATION :
Activer Microsoft Defender for Cloud via le portail Azure ou Azure CLI.

VALEUR PAR DÉFAUT :
Non activé

14.2.2 *Azure Monitor pour Azure Stack HCI*

DESCRIPTION :
Azure Monitor Insights doit être configuré pour les clusters Azure Stack HCI pour la collecte de métriques de performance, la détection d'anomalies et les alertes de santé du cluster.

AUDIT :
Vérifier dans le portail Azure : Azure Stack HCI > Monitoring > Insights

REMÉDIATION :
Configurer Azure Monitor Insights et les alertes recommandées.

VALEUR PAR DÉFAUT :
Non configuré

15.4.1 *Protection contre les attaques DoS sur l'hyperviseur*

DESCRIPTION :
Des protections contre les attaques de déni de service (DoS) ciblant l'hyperviseur doivent être en place, incluant les limites de ressources par VM, la surveillance des charges anormales et les alertes de surcharge.

```
# Vérifier les limites de ressources
Get-VM | Get-VMProcessor | Select-Object VMName, Maximum, Reserve
Get-VM | Select-Object Name, DynamicMemoryEnabled, MemoryMaximum
```

REMÉDIATION :
Configurer des limites de ressources CPU, mémoire et réseau pour chaque VM.

VALEUR PAR DÉFAUT :
Pas de limites

15.4.2 *Protection contre les attaques de timing*

DESCRIPTION :
Les attaques de timing exploitent les variations de temps d'exécution pour extraire des informations cryptographiques. Les mitigations incluent les correctifs microcode, le core scheduling de l'hyperviseur et la limitation du HyperThreading pour les VMs hautement sensibles.

```
Get-VM | Get-VMProcessor | Select-Object VMName, HwThreadCountPerCore, ExposeVirtualizationExtensions
# HwThreadCountPerCore = 1 désactive le partage de core entre VMs
```

```
# Restreindre à 1 thread par core pour les VMs sensibles
Set-VMProcessor -VMName "SensitiveVM" -HwThreadCountPerCore 1
```

VALEUR PAR DÉFAUT :
HwThreadCountPerCore = 0 (pas de restriction)

16.3.1 *DNS sécurisé pour les VMs*

DESCRIPTION :
Les VMs doivent utiliser des serveurs DNS internes sécurisés. Les requêtes DNS des VMs ne doivent pas pouvoir être interceptées ou redirigées. DNS-over-HTTPS (DoH) ou DNSSEC sont recommandés pour les VMs sensibles.

```
Get-VM | Get-VMNetworkAdapter | Select-Object VMName, @{N='DNS';E={$_.IPAddresses}}
```

REMÉDIATION :
Configurer les serveurs DNS internes via DHCP ou configuration statique.

VALEUR PAR DÉFAUT :
DNS fourni par DHCP

16.3.2 *Filtrage du trafic de gestion SNMP/WMI*

DESCRIPTION :
Les protocoles de gestion (SNMP, WMI) doivent être filtrés et restreints aux seules sources autorisées. WMI est un vecteur d'attaque courant pour les mouvements latéraux dans les environnements Windows.

```
Get-Service SNMP -ErrorAction SilentlyContinue | Select-Object Name, Status
Get-Service Winmgmt | Select-Object Name, Status
Get-NetFirewallRule -DisplayName "*WMI*" | Select-Object DisplayName, Enabled, Action
```

REMÉDIATION :
Désactiver SNMP si non utilisé. Restreindre WMI aux adresses IP de gestion.

VALEUR PAR DÉFAUT :
WMI activé, SNMP généralement non installé

17.3.1 *Exercice de simulation d'incident de virtualisation*

DESCRIPTION :
Des exercices de simulation d'incidents de virtualisation (tabletop exercises) doivent être effectués annuellement pour tester les procédures de réponse aux incidents, la communication et l'escalade.

AUDIT :
Vérifier la date du dernier exercice et le rapport de retour d'expérience.

REMÉDIATION :
Planifier un exercice de simulation annuel couvrant les scénarios critiques.

VALEUR PAR DÉFAUT :
Aucun exercice planifié

18.3.1 *Formation sécurité Hyper-V des administrateurs*

DESCRIPTION :
Les administrateurs Hyper-V doivent recevoir une formation spécifique sur la sécurité de la virtualisation couvrant les menaces spécifiques (VM Escape, side-channel attacks), les bonnes pratiques de configuration, la gestion des Shielded VMs et la réponse aux incidents.

AUDIT :
Vérifier le registre de formation des administrateurs Hyper-V.

REMÉDIATION :
Planifier une formation sécurité Hyper-V annuelle pour tous les administrateurs.

VALEUR PAR DÉFAUT :
Aucune formation spécifique

18.3.2 *Veille sécuritaire Hyper-V*

DESCRIPTION :
Un processus de veille sécuritaire doit être en place pour suivre les nouvelles vulnérabilités, les CVE et les mises à jour de sécurité spécifiques à Hyper-V et à la virtualisation Microsoft. Les sources incluent les bulletins de sécurité Microsoft, CERT-FR, NVD et les flux de menaces.

AUDIT :
Vérifier le processus de veille sécuritaire et les sources suivies.

REMÉDIATION :
Mettre en place un processus de veille avec les sources Microsoft Security Response Center, CERT-FR et les bulletins de sécurité.

VALEUR PAR DÉFAUT :
Aucune veille structurée

═══
TABLEAUX DE SYNTHÈSE
═══
TABLEAUX DE SYNTHÈSE
Synthèse par Section
Synthèse par Niveau de Criticité
Score Global de Maturité
═══
RÉSUMÉ EXÉCUTIF
═══
RÉSUMÉ EXÉCUTIF
Résultats Généraux
Points Forts Identifiés
Points Faibles Critiques
Recommandations Prioritaires
═══
MAPPING MULTI-RÉFÉRENTIEL
═══
MAPPING MULTI-RÉFÉRENTIEL
Mapping NIST SP 800-125 (Virtualisation)
Mapping NIST SP 800-53 Rev5
Mapping ISO 27001:2022
Mapping MITRE ATT&CK Enterprise (Techniques de Virtualisation)
Mapping RGPD / NIS2
═══

Annexe : Checklist (199 controles)

#	Recommandation	Niveau	Oui	Non	N/A
Section 1 — SÉCURITÉ DE L'HÔTE HYPER-V					
Section 1 — SÉCURITÉ DE L'HÔTE HYPER-V					
1.1.1	Installation en mode Server Core (installation minimale)	●	☐	☐	☐
1.1.2	Rôle Hyper-V comme rôle unique sur l'hôte	●	☐	☐	☐
1.1.3	Services Windows non essentiels désactivés	●	☐	☐	☐
1.1.4	Fonctionnalités Windows non essentielles supprimées	●	☐	☐	☐
1.2.1	Version du système d'exploitation hôte à jour	●	☐	☐	☐
1.2.2	Correctifs spécifiques Hyper-V appliqués	●	☐	☐	☐
1.3.1	Pare-feu Windows activé sur tous les profils	●	☐	☐	☐
1.3.2	Règles de pare-feu restrictives pour la gestion Hyper-V	●	☐	☐	☐
1.3.3	Journalisation du pare-feu activée	●	☐	☐	☐
1.4.1	Windows Defender Antivirus activé avec exclusions Hyper-V	●	☐	☐	☐
1.4.2	Mises à jour des signatures antivirus	●	☐	☐	☐
1.5.1	BitLocker activé sur le volume système de l'hôte	●	☐	☐	☐
1.5.2	BitLocker activé sur les volumes de stockage VM	●	☐	☐	☐
1.6.1	Secure Boot activé sur l'hôte physique	●	☐	☐	☐
1.6.2	TPM 2.0 présent et fonctionnel	●	☐	☐	☐
1.7.1	Credential Guard activé sur l'hôte	●	☐	☐	☐
1.7.2	Hypervisor-Protected Code Integrity (HVCI) activé	●	☐	☐	☐
1.7.3	Virtualization Based Security (VBS) activée	●	☐	☐	☐
1.8.1	Politique de mot de passe renforcée sur l'hôte	●	☐	☐	☐
1.8.2	Politique de verrouillage de compte configurée	●	☐	☐	☐
1.8.3	Compte Administrateur local renommé et désactivé	●	☐	☐	☐
1.8.4	LAPS (Local Administrator Password Solution) déployé	●	☐	☐	☐
1.9.1	Politique d'audit avancée configurée sur l'hôte	●	☐	☐	☐
1.9.2	Taille des journaux d'événements configurée	●	☐	☐	☐
1.9.3	Journalisation PowerShell activée	●	☐	☐	☐
1.9.4	Sysmon déployé sur l'hôte Hyper-V	●	☐	☐	☐
1.9.5	Transfert des journaux vers un SIEM	●	☐	☐	☐
1.9.6	NTP synchronisé et sécurisé	●	☐	☐	☐
Section 2 — GESTION DES ACCÈS ET RBAC					
Section 2 — GESTION DES ACCÈS ET RBAC					
2.1.1	Membres du groupe Hyper-V Administrators audités	●	☐	☐	☐
2.1.2	Séparation des comptes d'administration	●	☐	☐	☐
2.1.3	Comptes de service Hyper-V avec mots de passe gérés (gMSA)	●	☐	☐	☐
2.2.1	Délégation d'administration via SCVMM (rôles utilisateur)	●	☐	☐	☐
2.2.2	Self-Service Portal — limites et quotas	●	☐	☐	☐
2.3.1	JEA (Just Enough Administration) configuré pour Hyper-V	●	☐	☐	☐
2.3.2	PAW (Privileged Access Workstation) pour l'administration Hyper-V	●	☐	☐	☐
2.4.1	WinRM configuré avec HTTPS et certificat	●	☐	☐	☐
2.4.2	RDP sécurisé avec NLA et chiffrement élevé	●	☐	☐	☐
2.4.3	SSH désactivé ou sécurisé si utilisé	●	☐	☐	☐
2.5.1	Audit des connexions réussies et échouées	●	☐	☐	☐
2.5.2	Audit de l'utilisation des privilèges élevés	●	☐	☐	☐
2.5.3	Droits d'utilisateur restrictifs (User Rights Assignment)	●	☐	☐	☐
2.5.4	Revue périodique des accès administratifs	●	☐	☐	☐
2.6.1	MFA pour l'administration Hyper-V	●	☐	☐	☐
Section 3 — ISOLATION DES MACHINES VIRTUELLES					
Section 3 — ISOLATION DES MACHINES VIRTUELLES					
3.1.1	Isolation mémoire entre machines virtuelles	●	☐	☐	☐
3.1.2	Mémoire dynamique — configuration sécurisée	●	☐	☐	☐
3.2.1	Limites de ressources CPU par VM	●	☐	☐	☐
3.2.2	Limites de bande passante réseau par VM	●	☐	☐	☐
3.2.3	Limites d'IOPS de stockage par VM	●	☐	☐	☐
3.3.1	Integration Services — inventaire et contrôle	●	☐	☐	☐

#	Recommandation	Niveau	Oui	Non	N/A
3.3.2	Time Synchronization Service — configuration sécurisée	●	☐	☐	☐
3.3.3	Data Exchange (KVP) — désactivation si non requis	●	☐	☐	☐
3.3.4	Heartbeat Service — surveillance de l'état des VMs	●	☐	☐	☐
3.3.5	Guest Service Interface — désactivation recommandée	●	☐	☐	☐
3.3.6	VSS (Volume Shadow Copy) Integration Service	●	☐	☐	☐
3.4.1	Enhanced Session Mode — restriction d'utilisation	●	☐	☐	☐
3.4.2	Redirection du presse-papiers désactivée	●	☐	☐	☐
3.5.1	Discrete Device Assignment (DDA) — contrôle strict	●	☐	☐	☐
3.5.2	RemoteFX vGPU — désactivation (déprécié et vulnérable)	●	☐	☐	☐
3.6.1	Fichiers de configuration VM protégés (ACL)	●	☐	☐	☐
3.6.2	Génération de VM (Generation 2) requise	●	☐	☐	☐
3.6.3	Secure Boot activé sur les VMs	●	☐	☐	☐
Section 4 — MACHINES VIRTUELLES BLINDÉES (SHIELDED VMs)					
Section 4 — MACHINES VIRTUELLES BLINDÉES (SHIELDED VMs)					
4.1.1	Host Guardian Service (HGS) déployé et fonctionnel	●	☐	☐	☐
4.1.2	Mode d'attestation TPM (et non Admin-trusted)	●	☐	☐	☐
4.1.3	Haute disponibilité du cluster HGS	●	☐	☐	☐
4.2.1	Shielded VMs déployées pour les charges sensibles	●	☐	☐	☐
4.2.2	vTPM (Virtual TPM) activé sur les VMs	●	☐	☐	☐
4.2.3	Chiffrement de l'état et du trafic de migration	●	☐	☐	☐
4.3.1	Key Protectors et Shielding Data Files (.pdk) sécurisés	●	☐	☐	☐
4.3.2	Politiques d'attestation Code Integrity	●	☐	☐	☐
4.3.3	Certificates HGS — validité et renouvellement	●	☐	☐	☐
4.3.4	Encryption-Supported vs Shielded — classification des VMs	●	☐	☐	☐
Section 5 — RÉSEAU VIRTUEL (Virtual Networking)					
Section 5 — RÉSEAU VIRTUEL (Virtual Networking)					
5.1.1	Types de Virtual Switch — utilisation appropriée	●	☐	☐	☐
5.1.2	Management OS séparé du réseau VM	●	☐	☐	☐
5.2.1	VLAN Tagging configuré pour l'isolation réseau	●	☐	☐	☐
5.3.1	DHCP Guard activé sur les adaptateurs VM	●	☐	☐	☐
5.3.2	Router Guard activé sur les adaptateurs VM	●	☐	☐	☐
5.3.3	MAC Address Spoofing Protection	●	☐	☐	☐
5.3.4	Port ACLs et Extended Port ACLs	●	☐	☐	☐
5.4.1	NIC Teaming — configuration sécurisée	●	☐	☐	☐
5.4.2	SR-IOV — contrôle de l'utilisation	●	☐	☐	☐
5.5.1	Network QoS (Quality of Service) configuré	●	☐	☐	☐
5.5.2	Protected Network — isolation de sous-réseau VM	●	☐	☐	☐
5.6.1	Virtual Switch Extensions — audit et contrôle	●	☐	☐	☐
5.6.2	SDN (Software Defined Networking) — sécurité du Network Controller	●	☐	☐	☐
Section 6 — STOCKAGE VIRTUEL (Virtual Storage Security)					
Section 6 — STOCKAGE VIRTUEL (Virtual Storage Security)					
6.1.1	Format VHDX utilisé (pas VHD legacy)	●	☐	☐	☐
6.1.2	Permissions ACL restrictives sur les fichiers VHD/VHDX	●	☐	☐	☐
6.2.1	BitLocker dans les VMs invitées (chiffrement interne)	●	☐	☐	☐
6.2.2	Storage QoS — politiques appliquées	●	☐	☐	☐
6.3.1	Shared VHDX / VHD Sets — sécurité du partage	●	☐	☐	☐
6.3.2	Storage Spaces Direct (S2D) — sécurité du cluster de stockage	●	☐	☐	☐
6.4.1	ReFS vs NTFS — système de fichiers approprié	●	☐	☐	☐
6.4.2	SMB 3.x avec chiffrement pour le stockage réseau	●	☐	☐	☐
6.4.3	iSCSI et Fibre Channel — sécurité du stockage SAN	●	☐	☐	☐
Section 7 — LIVE MIGRATION ET HAUTE DISPONIBILITÉ					
Section 7 — LIVE MIGRATION ET HAUTE DISPONIBILITÉ					
7.1.1	Live Migration — authentification Kerberos (CredSSP non recommandé)	●	☐	☐	☐
7.1.2	Live Migration — chiffrement du transfert	●	☐	☐	☐
7.1.3	Live Migration — réseau dédié et isolé	●	☐	☐	☐
7.1.4	Live Migration — nombre de migrations simultanées limité	●	☐	☐	☐
7.2.1	Hyper-V Replica — chiffrement HTTPS avec certificats	●	☐	☐	☐

#	Recommandation	Niveau	Oui	Non	N/A
7.2.2	Hyper-V Replica — autorisation par serveur	●	☐	☐	☐
7.3.1	Failover Clustering — sécurité du cluster	●	☐	☐	☐
7.3.2	Cluster Shared Volumes (CSV) — sécurité	●	☐	☐	☐
7.3.3	Quorum et témoin du cluster — résilience	●	☐	☐	☐
7.3.4	Anti-affinity rules pour les VMs critiques	●	☐	☐	☐
Section 8 — SAUVEGARDE ET REPRISE D'ACTIVITÉ					
Section 8 — SAUVEGARDE ET REPRISE D'ACTIVITÉ					
8.1.1	Stratégie de sauvegarde des VMs documentée	●	☐	☐	☐
8.1.2	Sauvegardes chiffrées et stockées hors site	●	☐	☐	☐
8.2.1	Checkpoints/Snapshots — politique d'utilisation restrictive	●	☐	☐	☐
8.2.2	Checkpoints désactivés sur les VMs de production critiques	●	☐	☐	☐
8.3.1	Export/Import de VMs — procédure sécurisée	●	☐	☐	☐
8.3.2	Tests de restauration réguliers	●	☐	☐	☐
Section 9 — JOURNALISATION ET MONITORING					
Section 9 — JOURNALISATION ET MONITORING					
9.1.1	Journaux Hyper-V VMMS activés et surveillés	●	☐	☐	☐
9.1.2	Event IDs critiques Hyper-V surveillés	●	☐	☐	☐
9.2.1	Performance monitoring — métriques clés	●	☐	☐	☐
9.2.2	SIEM integration — collecte des événements Hyper-V	●	☐	☐	☐
9.3.1	Alertes critiques VM/Host configurées	●	☐	☐	☐
Section 10 — SÉCURITÉ DES CONTENEURS (Windows Containers sur Hyper-V)					
Section 10 — SÉCURITÉ DES CONTENEURS (Windows Containers sur Hyper-V)					
10.1.1	Isolation Hyper-V pour les conteneurs sensibles	●	☐	☐	☐
10.1.2	Images de base conteneurs — sources approuvées	●	☐	☐	☐
10.2.1	Réseau de conteneurs — isolation et segmentation	●	☐	☐	☐
10.2.2	Mises à jour des images de conteneurs	●	☐	☐	☐
10.2.3	Privilèges des conteneurs — moindre privilège	●	☐	☐	☐
Section 11 — SCVMM ET GESTION CENTRALISÉE					
Section 11 — SCVMM ET GESTION CENTRALISÉE					
11.1.1	SCVMM — compte de service sécurisé	●	☐	☐	☐
11.1.2	SCVMM — base de données chiffrée	●	☐	☐	☐
11.1.3	SCVMM — communications chiffrées avec les hôtes	●	☐	☐	☐
11.2.1	Windows Admin Center — certificat HTTPS et accès restreint	●	☐	☐	☐
11.3.1	PowerShell Direct — contrôle d'utilisation	●	☐	☐	☐
11.3.2	Automatisation et scripting — contrôle des scripts	●	☐	☐	☐
Section 12 — CONFORMITÉ DES VMs INVITÉES					
Section 12 — CONFORMITÉ DES VMs INVITÉES					
12.1.1	Durcissement des systèmes d'exploitation invités	●	☐	☐	☐
12.1.2	Antivirus dans les VMs invitées	●	☐	☐	☐
12.1.3	Mises à jour des VMs invitées	●	☐	☐	☐
12.2.1	Integration Services à jour dans les VMs invitées	●	☐	☐	☐
12.2.2	Agent de monitoring dans les VMs	●	☐	☐	☐
Section 13 — NESTED VIRTUALIZATION ET SCÉNARIOS AVANCÉS					
Section 13 — NESTED VIRTUALIZATION ET SCÉNARIOS AVANCÉS					
13.1.1	Nested Virtualization — contrôle d'utilisation	●	☐	☐	☐
13.1.2	VMs masquant leur environnement de virtualisation	●	☐	☐	☐
13.1.3	Contrôle des VMs avec accès matériel direct (passthrough)	●	☐	☐	☐
Section 14 — SÉCURITÉ AZURE STACK HCI					
Section 14 — SÉCURITÉ AZURE STACK HCI					
14.1.1	Azure Stack HCI — version et mises à jour	●	☐	☐	☐
14.1.2	Azure Arc — enregistrement et conformité	●	☐	☐	☐
14.1.3	Azure Policy — conformité de sécurité	●	☐	☐	☐
Section 15 — PROTECTION CONTRE LES ATTAQUES DE VIRTUALISATION					
Section 15 — PROTECTION CONTRE LES ATTAQUES DE VIRTUALISATION					
15.1.1	Mitigations VM Escape — correctifs et configuration	●	☐	☐	☐

#	Recommandation	Niveau	Oui	Non	N/A
15.1.2	Attaques par canal auxiliaire (Spectre, Meltdown, L1TF, MDS, MMIO)	●	☐	☐	☐
15.2.1	Réduction de la surface d'attaque Hyper-V	●	☐	☐	☐
15.2.2	Protection contre les attaques firmware	●	☐	☐	☐
15.3.1	Contrôle de la chaîne d'approvisionnement des images VM	●	☐	☐	☐
Section 16 — RÉSEAU ET SEGMENTATION AVANCÉE					
Section 16 — RÉSEAU ET SEGMENTATION AVANCÉE					
16.1.1	Micro-segmentation — isolation inter-VM	●	☐	☐	☐
16.1.2	Zones de sécurité réseau documentées et appliquées	●	☐	☐	☐
16.1.3	Port Mirroring — contrôle et audit	●	☐	☐	☐
16.2.1	IPv6 — configuration sécurisée ou désactivation	●	☐	☐	☐
Section 17 — RÉPONSE AUX INCIDENTS VIRTUALISATION					
Section 17 — RÉPONSE AUX INCIDENTS VIRTUALISATION					
17.1.1	Plan de réponse aux incidents virtualisation documenté	●	☐	☐	☐
17.1.2	Procédure d'isolation d'une VM compromise	●	☐	☐	☐
17.1.3	Collecte de preuves forensiques virtualisées	●	☐	☐	☐
17.2.1	Procédure de réponse à une compromission de l'hôte Hyper-V	●	☐	☐	☐
17.2.2	Communication et escalade en cas d'incident	●	☐	☐	☐
Section 18 — GOUVERNANCE ET CONFORMITÉ					
Section 18 — GOUVERNANCE ET CONFORMITÉ					
18.1.1	Politique de sécurité de la virtualisation documentée	●	☐	☐	☐
18.1.2	Gestion des changements pour l'infrastructure Hyper-V	●	☐	☐	☐
18.1.3	Inventaire des machines virtuelles à jour	●	☐	☐	☐
18.2.1	Conformité RGPD — données personnelles dans les VMs	●	☐	☐	☐
18.2.2	Conformité NIS2 — infrastructure essentielle	●	☐	☐	☐
18.2.3	Audit de sécurité périodique de l'infrastructure Hyper-V	●	☐	☐	☐
1.10.1	Protocole SMBv1 désactivé sur l'hôte	●	☐	☐	☐
1.10.2	TLS 1.2/1.3 uniquement — protocoles obsolètes désactivés	●	☐	☐	☐
1.10.3	Suites de chiffrement renforcées (Cipher Suites)	●	☐	☐	☐
1.10.4	Windows Defender Application Control (WDAC)	●	☐	☐	☐
1.10.5	Démarrage mesuré (Measured Boot) activé	●	☐	☐	☐
1.10.6	Restriction des connexions sortantes de l'hôte	●	☐	☐	☐
2.7.1	Restriction de connexion interactive sur l'hôte	●	☐	☐	☐
2.7.2	Timeout de session d'administration	●	☐	☐	☐
2.7.3	Bannière d'avertissement légal à la connexion	●	☐	☐	☐
3.7.1	Automatic Start Action sécurisée	●	☐	☐	☐
3.7.2	Automatic Stop Action — arrêt propre des VMs	●	☐	☐	☐
3.7.3	Notes et documentation des VMs	●	☐	☐	☐
3.7.4	Version de configuration VM à jour	●	☐	☐	☐
4.4.1	Politique de déploiement des Shielded VMs documentée	●	☐	☐	☐
4.4.2	HGS backup et disaster recovery	●	☐	☐	☐
5.7.1	Adresses MAC statiques pour les VMs sensibles	●	☐	☐	☐
5.7.2	IPsec pour le trafic inter-VM sensible	●	☐	☐	☐
5.7.3	Surveillance des flux réseau anormaux	●	☐	☐	☐
6.5.1	Disques de différenciation — usage restreint en production	●	☐	☐	☐
6.5.2	Disques VHDX — taille fixe vs dynamique	●	☐	☐	☐
7.4.1	Drain roles before maintenance	●	☐	☐	☐
7.4.2	Preferred owners pour les VMs critiques	●	☐	☐	☐
8.4.1	DR avec Hyper-V Replica — test de basculement	●	☐	☐	☐
8.4.2	RPO et RTO définis et mesurés	●	☐	☐	☐
9.4.1	Audit des modifications de configuration VM	●	☐	☐	☐
9.4.2	Monitoring de l'état de réplication	●	☐	☐	☐
9.4.3	Surveillance de l'espace disque des volumes VM	●	☐	☐	☐
10.3.1	Runtime de conteneurs — version sécurisée	●	☐	☐	☐
10.3.2	Logging des conteneurs centralisé	●	☐	☐	☐
11.4.1	SCVMM — audit des actions administratives	●	☐	☐	☐
11.4.2	SCVMM — Run As Accounts protégés	●	☐	☐	☐
12.3.1	Templates de VM pré-durcis	●	☐	☐	☐
12.3.2	Inventaire des logiciels installés dans les VMs	●	☐	☐	☐

#	Recommandation	Niveau	Oui	Non	N/A
13.2.1	VMs de test/développement isolées de la production	●	☐	☐	☐
14.2.1	Microsoft Defender for Cloud activé sur Azure Stack HCI	●	☐	☐	☐
14.2.2	Azure Monitor pour Azure Stack HCI	●	☐	☐	☐
15.4.1	Protection contre les attaques DoS sur l'hyperviseur	●	☐	☐	☐
15.4.2	Protection contre les attaques de timing	●	☐	☐	☐
16.3.1	DNS sécurisé pour les VMs	●	☐	☐	☐
16.3.2	Filtrage du trafic de gestion SNMP/WMI	●	☐	☐	☐
17.3.1	Exercice de simulation d'incident de virtualisation	●	☐	☐	☐
18.3.1	Formation sécurité Hyper-V des administrateurs	●	☐	☐	☐
18.3.2	Veille sécuritaire Hyper-V	●	☐	☐	☐