Désactivation de VBS sur Windows 11

Contexte

Sur Windows 11, la **Virtualization Based Security (VBS)** est activée par défaut. Elle monopolise AMD-V/Intel VT-x et empêche les hyperviseurs tiers (VirtualBox, VMware Workstation) d'accéder à la virtualisation matérielle pour faire du **nested virtualization**.

Symptômes :

- VMware Workstation : `La fonction hv.capable était 0, mais doit être au minimum 0x1`
- VirtualBox : nested virtualization désactivée malgré la case cochée
- `msinfo32` → Sécurité basée sur la virtualisation : **En cours d'exécution**

Diagnostic

Vérifier l'état de VBS

```
# Hyperviseur présent ?
Get-CimInstance Win32_ComputerSystem | Select HypervisorPresent

# État de la virtualisation CPU
Get-CimInstance Win32_Processor | Select
Name,VMMonitorModeExtensions,VirtualizationFirmwareEnabled,SecondLevelAddressTranslationExtens
ions

# Type de lancement hyperviseur
bcdedit /enum "{current}" | findstr /i "hypervisorlaunchtype vsmlaunchtype isolatedcontext"
```

```
# État registre DeviceGuard
reg query "HKLM\SYSTEM\CurrentControlSet\Control\DeviceGuard" /s
```

Identifier la cause dans msinfo32

```
msinfo32
```

Lignes à surveiller :

- `Sécurité basée sur la virtualisation` → doit être `Désactivé`
- `Stratégie Contrôle des applications pour entreprise` → si `Appliqué`, VBS est forcé
- `Services en cours d'exécution pour la sécurité basée sur la virtualisation` → doit être vide

Solution — Désactivation complète de VBS

Étape 1 — Registre DeviceGuard

```
reg add "HKLM\SYSTEM\CurrentControlSet\Control\DeviceGuard" /v
"EnableVirtualizationBasedSecurity" /t REG_DWORD /d 0 /f
reg add "HKLM\SYSTEM\CurrentControlSet\Control\DeviceGuard" /v
"HyperVVirtualizationBasedSecurityOptout" /t REG_DWORD /d 1 /f
reg add "HKLM\SYSTEM\CurrentControlSet\Control\DeviceGuard" /v
"RequirePlatformSecurityFeatures" /t REG_DWORD /d 0 /f
reg add "HKLM\SYSTEM\CurrentControlSet\Control\DeviceGuard" /v "Locked" /t REG_DWORD /d 0 /f
```

Étape 2 — Désactiver HVCI (Hypervisor Protected Code Integrity)

```
reg add
"HKLM\SYSTEM\CurrentControlSet\Control\DeviceGuard\Scenarios\HypervisorEnforcedCodeIntegrity"
```

```
/v "Enabled" /t REG_DWORD /d 0 /f
```

Étape 3 — Désactiver Credential Guard et LSA

```
reg add "HKLM\SYSTEM\CurrentControlSet\Control\DeviceGuard\Scenarios\CredentialGuard" /v "Enabled" /t REG_DWORD /d 0 /f
reg add "HKLM\SYSTEM\CurrentControlSet\Control\Lsa" /v "LsaCfgFlags" /t REG_DWORD /d 0 /f
```

Étape 4 — Désactiver KeyGuard (Windows Hello maintient VBS actif)

> **Point clé** : Windows Hello force KeyGuard qui maintient VBS actif même si toutes les autres clés sont désactivées.

```
reg add "HKLM\SYSTEM\CurrentControlSet\Control\DeviceGuard\Scenarios\WindowsHello" /v "Enabled" /t REG_DWORD /d 0 /f
reg add "HKLM\SYSTEM\CurrentControlSet\Control\DeviceGuard\Scenarios\KeyGuard" /v "KeyGuardEnabled" /t REG_DWORD /d 0 /f
```

Étape 5 — Désactiver l'hyperviseur au boot

```
bcdedit /set hypervisorlaunchtype off
bcdedit /set vsmlaunchtype off
```

Étape 6 — Redémarrer

```
shutdown /r /t 0
```

Vérification finale

```
# Vérifier que VBS est bien désactivé
reg query "HKLM\SYSTEM\CurrentControlSet\Control\DeviceGuard" /v
"EnableVirtualizationBasedSecurity"
bcdedit | findstr "hypervisor"
```

Dans `msinfo32` après redémarrage :

- **Sécurité basée sur la virtualisation** → `Désactivé`
- **Hyper-V - Virtualisation activée dans le microprogramme** → `Oui`
- **Hyper-V - Extensions du mode de moniteur** → `Oui`

Points bloquants courants

Symptôme	Cause	Solution
VBS reste actif après reboot	KeyGuard/Windows Hello	Étape 4 ci-dessus
VBS revient après chaque reboot	Politique WDAC (`driversipolicy.p7b`)	Vérifier `C:\Windows\System32\CodeIntegrity\`
`hypervisorlaunchtype Off` mais hyperviseur actif	`hvservice` démarré par VBS	Désactiver KeyGuard et HVCI
Workstation : `hv.capable = 0`	AMD-V monopolisé par Windows Hypervisor Platform	Désactiver VBS complètement

---

Problème de persistance — Windows Hello réactive VBS

Pourquoi VBS revient

Si le compte principal est un **compte Microsoft** (ex: `k.vegadelgado@gmail.com`), Windows force Windows Hello (PIN, empreinte, reconnaissance faciale) à la reconnexion. Dès qu'un PIN est reconfiguré, **KeyGuard réactive VBS** au prochain reboot.

De plus, avec un compte Microsoft, il est impossible d'ajouter un mot de passe local depuis les Paramètres — Windows Hello est forcé et masque les autres méthodes de connexion.

Solution — Créer un compte local administrateur dédié

Créer le compte

```
# Créer un compte local avec mot de passe
net user kvega_admin MonMotDePasse123! /add

# Lui donner les droits administrateur
net localgroup Administrateurs kvega_admin /add
```

Conséquences

Aspect	Impact
Compte Microsoft	Conservé, inchangé
Windows Hello	Toujours actif sur le compte Microsoft
VBS	Reste désactivé tant qu'on utilise `kvega_admin`
VBS au reboot	Peut revenir si on se reconnecte avec le compte Microsoft et reconfigure un PIN
VMware/VirtualBox	À installer et utiliser depuis `kvega_admin`

> **Recommandation** : utiliser `kvega_admin` exclusivement pour les sessions de lab virtualisation. Le compte Microsoft peut être utilisé pour le reste sans impact sur VBS tant qu'on ne reconfigure pas de PIN.

Solution — Tâche planifiée pour maintenir VBS désactivé

Pour éviter que VBS ne revienne même si Windows Hello est reconfiguré sur le compte Microsoft, créer une tâche planifiée qui s'exécute à chaque démarrage en tant que SYSTEM :

```
$action = New-ScheduledTaskAction -Execute "powershell.exe" -Argument '-NonInteractive -WindowStyle Hidden -Command "reg add \"HKLM\SYSTEM\CurrentControlSet\Control\DeviceGuard\Scenarios\WindowsHello\" /v Enabled /t REG_DWORD /d 0 /f; reg add \"HKLM\SYSTEM\CurrentControlSet\Control\DeviceGuard\Scenarios\KeyGuard\" /v KeyGuardEnabled /t REG_DWORD /d 0 /f"'

$trigger = New-ScheduledTaskTrigger -AtStartup

$principal = New-ScheduledTaskPrincipal -UserId "SYSTEM" -RunLevel Highest

Register-ScheduledTask -TaskName "DisableKeyGuard" -Action $action -Trigger $trigger -Principal $principal -Force
```

Cette tâche désactive KeyGuard avant que Windows Hello ne puisse le réactiver, quel que soit le compte connecté.

Notes importantes

- **Ne pas supprimer** `VbsSiPolicy.p7b` manuellement — risque de rendre Windows non démarrable
- Ces modifications **réduisent la sécurité** du poste — à faire uniquement sur un PC dédié au lab
- Windows Update peut réactiver VBS — vérifier après chaque mise à jour majeure
- La tâche planifiée `DisableKeyGuard` est la solution la plus robuste pour maintenir VBS désactivé durablement

---

Revision #3
Created 2026-09-09 11:50:59 UTC by kvega
Updated 2026-09-09 14:01:22 UTC by kvega