



## Intervention d'incident sur Eve NG avec les Images Cisco

Dans le cadre de la construction d'un **lab de cybersécurité offensive** sous EVE-NG, j'ai rencontré un incident bloquant lors du déploiement des images cisco.

Ce retour d'expérience est volontairement orienté **architecture, virtualisation avancée et diagnostic de cause racine**, car ce type de problème révèle souvent une mauvaise compréhension de la stack sous-jacente.

### 1. Contexte Architecture

- Poste : Dell
- OS : Windows 11 Professionnel
- Hyperviseur : VMware Workstation
- RAM : 32 Go
- Usage : Lab Red Team / Offensive Security
- Plateforme : EVE-NG (virtualisation imbriquée requise)

Objectif : exécuter des environnements réseau réalistes (segmentation, pivoting, simulation d'infrastructure d'entreprise).

### 2. Symptômes Critiques

- vIOS-L2 ne démarre pas
- Aucun module KVM chargé côté EVE
- VMware retourne : - “Nested virtualization not supported”  
- “Virtualized Intel VT-x/EPT is not supported”

Commande clé sur PowerShell :

```
systeminfo
```

Résultat : > “Un hyperviseur a été détecté”

À ce stade, il ne s'agit plus d'un problème applicatif mais d'un conflit d'architecture de virtualisation.



### 3. Analyse Architecture – Cause Racine

Le problème n'était ni matériel ni lié à l'image.

La cause réelle : **Virtualization Based Security (VBS)** activé par défaut sous Windows 11.

Concrètement :

- Windows charge son propre hyperviseur (Hyper-V) en arrière-plan
- Les extensions VT-x sont monopolisées
- VMware ne peut plus exposer correctement la virtualisation imbriquée
- KVM ne peut pas se charger dans EVE-NG

Résultat : l'infrastructure offensive lab est inutilisable.

C'est un conflit entre hyperviseurs de niveau 1.

### 4. Remédiation Niveau Architecte

Approche adoptée : éliminer toute couche concurrente et restaurer un contrôle total de la virtualisation matérielle.

#### a. Suppression complète de la stack Hyper-V

Je saisi :

Win + R → optionalfeatures

Et je passe à la désactivation de :

- Hyper-V
- Windows Hypervisor Platform
- Virtual Machine Platform
- Windows Sandbox
- WSL (si non requis)

Redémarrage complet (pas simple reboot rapide).



## b. Désactivation de l'Isolation du Noyau

Chemin

```
Paramètres → Sécurité Windows → Sécurité des appareils → Isolation du noyau
```

Désactiver :

- Intégrité de la mémoire
- c. Neutralisation VBS via registre

Exécuter PowerShell en administrateur :

```
reg add "HKLM\System\CurrentControlSet\Control\DeviceGuard" /v  
EnableVirtualizationBasedSecurity /t REG_DWORD /d 0 /f
```

```
reg add "HKLM\System\CurrentControlSet\Control\Lsa" /v LsaCfgFlags  
/t REG_DWORD /d 0 /f
```

Redémarrage complet.

## d. Validation d'architecture

Exécuter PowerShell en administrateur :

```
systeminfo
```

Résultat attendu : > “Un hyperviseur n'a pas été détecté”

Puis validation côté EVE :

```
lsmod | grep kvm
```

Résultat attendu :



- kvm
- kvm\_intel

## 5. Résultat

- Virtualisation imbriquée pleinement fonctionnelle
- KVM chargé
- vIOS-L2 opérationnel
- Lab Red Team stable
- Capacité à simuler AD, VLAN, pivot interne et scénarios post-exploitation

## 6. Moral de la journée

Dans un lab de cybersécurité offensive, comprendre la **couche hyperviseur** est indispensable.

Un Red Teamer ou Security Engineer qui ne maîtrise pas la virtualisation sous-jacente perd en efficacité.

Avant de blâmer une image ou un outil :

- Vérifier la présence d'un hyperviseur concurrent
- Vérifier l'accès réel aux extensions VT-x
- Comprendre la hiérarchie des hyperviseurs

La cybersécurité offensive commence par une architecture maîtrisée.