# Credential Guard Windows Server 2025 : Guide Complet de Déploiement

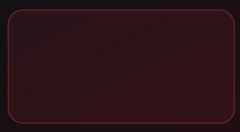
> Credential Guard Windows Server 2025 : activer la protection VSB/HVCI, bloquer Mimikatz et Pass-the-Hash, déployer via GPO ou Intune. Guide expert 2026.

Credential Guard est la réponse de Microsoft au vol de credentials en mémoire : en isolant le processus LSASS (Local Security Authority Subsystem Service) dans un environnement d'exécution sécurisé basé sur la virtualisation, il rend inaccessibles les hachages NTLM et les tickets Kerberos TGT stockés en mémoire vive. Concrètement, lorsqu'un attaquant exécute Mimikatz après une compromission initiale sur un serveur Windows Server 2025 correctement configuré, la commande `sekurlsa::logonpasswords` retourne systématiquement "KO - LSA Isolated" plutôt que la liste des credentials en clair. Cette protection s'appuie sur la Virtualization Based Security (VBS) et HVCI (Hypervisor-Protected Code Integrity) pour créer un monde isolé — LSAIso — où tournent les secrets d'authentification, physiquement inaccessible depuis le système d'exploitation principal, même pour un processus tournant avec les privilèges SYSTEM. Pour les RSSI, DSI et architectes sécurité déployant Windows Server 2025 dans des environnements soumis à NIS2 ou aux recommandations de l'ANSSI, Credential Guard constitue un contrôle technique de premier rang contre les attaques Pass-the-Hash et Pass-the-Ticket qui alimentent la grande majorité des mouvements latéraux observés lors des incidents ransomware en France. Ce guide couvre l'architecture technique, les prérequis, le déploiement GPO/Intune/PowerShell, la vérification, les limites et l'intégration dans un écosystème PAM.

📋 EN BREF

ATTAQUES ACTIVE DIRECTORY

## Credential Guard Windows Server 2025 : Guide Complet



## Architecture : comment VBS et HVCI protègent LSASS

La Virtualization Based Security (VBS) exploite les extensions de virtualisation du processeur (Intel VT-x / AMD-V) pour créer deux mondes d'exécution étanches : le monde normal (VTL0), où tourne Windows Server 2025 et toutes les applications, et le monde sécurisé (VTL1), géré par le Secure Kernel de Microsoft. L'hyperviseur Hyper-V arbitre les communications entre ces deux niveaux via des interfaces étroitement contrôlées.

> ⚡ **Retour terrain**
>
> Lors d'un red team pour un groupe industriel, j'ai pu dumper des hashes NTLM depuis la mémoire LSASS d'un poste standard — via une vulnérabilité d'une application tierce installée sur tous les postes. Avec ces hashes, le mouvement latéral vers 60 % du parc s'est fait en 20 minutes sans craquer un seul mot de passe. La protection NTLM (Credential Guard + Protected Users) était pourtant dans la roadmap depuis 18 mois.

Credential Guard exploite VTL1 pour héberger un processus spécial baptisé **LSAIso** (LSA Isolated). Ce processus est une instance allégée du LSASS traditionnel qui gère exclusivement les secrets d'authentification : hachages NT, hachages LM (obsolètes), tickets Kerberos TGT et clés de session. Le LSASS standard qui tourne en VTL0 reçoit des handles opaques (références chiffrées) lorsqu'il a besoin d'un secret — il n'obtient jamais le matériau cryptographique brut.

### Rôle d'HVCI (Hypervisor-Protected Code Integrity)

HVCI complète VBS en imposant que tout code exécuté en mode noyau soit signé et validé par l'hyperviseur avant exécution. Cette fonctionnalité bloque les drivers non signés et les techniques d'injection de code noyau, qui sont les vecteurs classiques de contournement de Credential Guard. Un attaquant qui parviendrait à charger un driver malveillant signé aurait encore à

contourner les vérifications de l'hyperviseur, ce qui élève considérablement le niveau d'attaque requis.

### Secure Boot et chaîne de confiance UEFI

Le démarrage sécurisé UEFI garantit l'intégrité de la chaîne depuis le firmware jusqu'au chargeur Windows. Sans Secure Boot, un attaquant disposant d'un accès physique pourrait modifier le bootloader pour désactiver VBS avant le démarrage du système. Credential Guard avec UEFI lock (LsaCfgFlags = 1) ancre sa configuration dans les variables UEFI, rendant sa désactivation impossible depuis Windows sans redémarrage en mode récupération — ce qui génère des traces auditables.

---

## Prérequis matériels et logiciels

### Matériel requis

**TPM 2.0** : puce Trusted Platform Module version 2.0 obligatoire (TPM 1.2 insuffisant). Vérification : `Get-Tpm | Select-Object TpmPresent, TpmReady, TpmActivated, ManufacturerId`

**UEFI natif** : le firmware doit fonctionner en mode UEFI natif (pas de mode CSM/Legacy). BIOS UEFI version 2.3.1 ou supérieure recommandée

**Secure Boot** activé dans le firmware UEFI

**Extensions de virtualisation** : Intel VT-x avec SLAT (EPT) ou AMD-V avec RVI/NPT activées dans le BIOS

**64 bits obligatoire** : pas de support 32 bits

**RAM** : minimum 8 Go recommandé (VBS réserve une portion de mémoire pour VTL1)

**Processeur** : Intel 8e génération ou supérieur, AMD Zen 2 ou supérieur pour une compatibilité optimale avec HVCI

### Logiciels et rôles Windows

**Windows Server 2025** Standard ou Datacenter (64 bits) — édition Core également supportée

**Hyper-V** activé (rôle ou fonctionnalité Windows) — requis pour VBS même si le serveur n'héberge pas de VMs

**Pas de Nested Virtualization** : si le serveur est lui-même une VM, la virtualisation imbriquée doit être activée sur l'hyperviseur hôte (voir section Incompatibilités)

Absence de drivers incompatibles avec HVCI (liste disponible dans le rapport de compatibilité Device Guard)

### Vérification de compatibilité préalable

Avant déploiement, l'outil **DGREADINESS** (Device Guard and Credential Guard hardware readiness tool) de Microsoft permet de valider la compatibilité du matériel :

```
 # Télécharger et exécuter l'outil de compatibilité
# DG_Readiness_Tool_v3.6.ps1 disponible sur Microsoft Download Center
.\DG_Readiness_Tool_v3.6.ps1 -Ready

# Vérification rapide des prérequis VBS
$ci = Get-CimInstance -Namespace "root\Microsoft\Windows\DeviceGuard" -ClassName "Win32_DeviceGua
$ci.AvailableSecurityProperties
# Valeurs : 1=Base Virtualization, 2=Secure Boot, 3=DMA Protection,
# 4=Secure Memory Overwrite, 5=NX Protections, 6=SMM Security, 7=MBEC/GMET
```

---

## Activation via GPO (méthode recommandée en domaine AD)

Pour les environnements Active Directory, la GPO est la méthode de déploiement standard. Elle permet un déploiement progressif par OU et une gestion centralisée.

### Chemin GPO

Ouvrir la **Group Policy Management Console** (GPMC) et naviguer vers :

```
Computer Configuration → Administrative Templates → System → Device Guard
```

### Paramètres à configurer

**Turn On Virtualization Based Security → Enabled**

**Select Platform Security Level** :
*Secure Boot* : protection minimale, sans DMA protection

*Secure Boot and DMA Protection* : recommandé (bloque les attaques DMA via Thunderbolt/PCIe)

**Credential Guard Configuration** :
*Enabled with UEFI lock* : la configuration est ancrée dans les variables UEFI — impossible à désactiver depuis Windows sans intervention physique. **Recommandé pour la production.**

*Enabled without lock* : peut être désactivé via GPO sans redémarrage en mode récupération — utile en phase de test

**Secure Launch Configuration** (optionnel) → Enabled pour les machines compatibles (DRTM)

### Déploiement progressif recommandé

En production, adopter une approche par vagues :

Créer une OU de test, appliquer la GPO sur 5-10 serveurs non critiques

Valider via `Get-CimInstance Win32_DeviceGuard` après redémarrage

Tester les applications métier (VPN, antivirus, solutions de sauvegarde) — 48h minimum

Étendre progressivement aux contrôleurs de domaine en dernier (risque de breaking change maximal)

## Activation via PowerShell et registre

Pour les serveurs isolés, les scripts d'automatisation ou les environnements sans AD, l'activation directe via le registre est possible. Le script suivant est complet et commenté :

```
 # Vérifier si Credential Guard est actif
$dg = Get-CimInstance -Namespace "root\Microsoft\Windows\DeviceGuard" -ClassName "Win32_DeviceGua
$dg | Select-Object -Property SecurityServicesRunning, SecurityServicesConfigured,
    VirtualizationBasedSecurityStatus, AvailableSecurityProperties

# Statuts : 0=Off, 1=Configured, 2=Running
# SecurityServicesRunning : 1=VSB, 2=Credential Guard, 4=HVCI

# Activer Credential Guard via registre (nécessite redémarrage)
$path = "HKLM:\SYSTEM\CurrentControlSet\Control\DeviceGuard"
New-Item -Path $path -Force | Out-Null
Set-ItemProperty -Path $path -Name "EnableVirtualizationBasedSecurity" -Value 1
Set-ItemProperty -Path $path -Name "RequirePlatformSecurityFeatures" -Value 1

$path2 = "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa"
Set-ItemProperty -Path $path2 -Name "LsaCfgFlags" -Value 1
# 0 = désactivé, 1 = activé avec UEFI lock (recommandé), 2 = activé sans lock

# Tester que Mimikatz ne peut pas extraire les credentials
# sekurlsa::logonpasswords devrait retourner "KO - LSA Isolated"

# Vérifier via msinfo32 en CLI
Get-ComputerInfo | Select-Object -Property DeviceGuard*

# Script de vérification post-déploiement complet
function Test-CredentialGuard {
    $dg = Get-CimInstance -Namespace "root\Microsoft\Windows\DeviceGuard" -ClassName "Win32_Devic
    $status = @{
        VBSStatus = switch ($dg.VirtualizationBasedSecurityStatus) {
            0 { "Désactivé" }
            1 { "Activé mais non opérationnel" }
            2 { "Opérationnel" }
        }
        CredentialGuard = if ($dg.SecurityServicesRunning -contains 2) { "ACTIF" } else { "INACTI
        HVCI = if ($dg.SecurityServicesRunning -contains 4) { "ACTIF" } else { "INACTIF" }
        SecureBoot = Confirm-SecureBootUEFI
    }
    return $status
}
Test-CredentialGuard
```

## Activation via Microsoft Intune (environnements hybrides)

Pour les architectures hybrides Azure AD / Microsoft Entra ID avec des serveurs Windows Server 2025 gérés via Microsoft Endpoint Manager, Intune propose des profils de configuration dédiés à Device Guard.

### Profil Endpoint Security

Dans le portail Intune, naviguer vers **Endpoint Security → Attack Surface Reduction → Create Policy**

Plateforme : **Windows 10 and later** (s'applique aussi à Windows Server 2025)

Profil : **Device Control** ou **Endpoint Detection and Response**

Sous **Device Guard** :
*Turn On Virtualization Based Security* : Enable

*Enable Credential Guard* : Enable with UEFI lock

*Require Platform Security Features* : Secure Boot

### Configuration via Custom OMA-URI

Pour un contrôle précis, utiliser les OMA-URI custom :

```
 # OMA-URI pour activer VBS
# URI: ./Device/Vendor/MSFT/Policy/Config/DeviceGuard/EnableVirtualizationBasedSecurity
# Type: Integer, Value: 1

# OMA-URI pour Credential Guard avec UEFI lock
# URI: ./Device/Vendor/MSFT/Policy/Config/DeviceGuard/LsaCfgFlags
# Type: Integer, Value: 1

# OMA-URI pour le niveau de sécurité plateforme
# URI: ./Device/Vendor/MSFT/Policy/Config/DeviceGuard/RequirePlatformSecurityFeatures
# Type: Integer, Value: 3 (Secure Boot + DMA)
```

## Vérification de l'activation

Après redémarrage, plusieurs méthodes permettent de confirmer que Credential Guard est opérationnel.

### Via PowerShell (méthode principale)

```
 # Vérification complète de l'état Device Guard
$dg = Get-CimInstance -Namespace "root\Microsoft\Windows\DeviceGuard" -ClassName "Win32_DeviceGua

# SecurityServicesRunning contient la valeur 2 si Credential Guard est actif
if ($dg.SecurityServicesRunning -contains 2) {
    Write-Host "Credential Guard : ACTIF" -ForegroundColor Green
} else {
    Write-Host "Credential Guard : INACTIF" -ForegroundColor Red
}

# VirtualizationBasedSecurityStatus = 2 si VBS est opérationnel
Write-Host "VBS Status: $($dg.VirtualizationBasedSecurityStatus)" # 2 = Running
Write-Host "Services configurés: $($dg.SecurityServicesConfigured)"
Write-Host "Services actifs: $($dg.SecurityServicesRunning)"
Write-Host "Propriétés de sécurité disponibles: $($dg.AvailableSecurityProperties)"
```

### Via msinfo32

Dans **msinfo32.exe** → **Résumé du système**, vérifier les champs :

**Virtualization-based security** : Running

**Virtualization-based security Services Running** : Credential Guard, Hypervisor enforced Code Integrity

**Virtualization-based security Services Configured** : Credential Guard

### Via les logs d'événements Windows

Les événements VBS/Credential Guard sont journalisés dans le journal `Microsoft-Windows-DeviceGuard/Operational` :

**Event ID 3080** : LSAIso démarré avec succès (Credential Guard opérationnel)

**Event ID 3082** : LSAIso configuration changée (désactivation ou modification de la politique)

**Event ID 3033** : Code Integrity vérifié (HVCI en action — log fréquent en production)

**Event ID 3065/3066** : Driver bloqué par HVCI (incompatibilité)

```
 # Récupérer les événements Credential Guard récents
Get-WinEvent -LogName "Microsoft-Windows-DeviceGuard/Operational" |
    Where-Object { $_.Id -in @(3080, 3082, 3033) } |
    Select-Object TimeCreated, Id, Message |
    Format-List
```

---

## Ce que Credential Guard ne protège PAS

Il est critique pour les RSSI de comprendre les limites de Credential Guard pour ne pas croire à une protection complète. Plusieurs vecteurs d'attaque restent actifs même avec CG déployé.

### Attaques non bloquées

**NTLM en transit réseau** : Credential Guard protège les hachages en mémoire, mais les authentifications NTLM sur le réseau restent captables via des relais NTLM (NTLM Relay, Responder). La désactivation de NTLM v1 et le passage à SMB Signing obligatoire restent nécessaires.

**Kerberoasting** : un attaquant authentifié peut toujours demander des tickets de service (TGS) pour les comptes de service et les casser hors ligne. Credential Guard n'intervient pas dans ce processus.

**AS-REP Roasting** : les comptes configurés sans pré-authentification Kerberos restent vulnérables.

**Comptes de service (MSA/gMSA) dans certains contextes** : des configurations spécifiques peuvent exposer des credentials de service.

**Mots de passe en clair dans les GPO** : les anciennes préférences GPO (Groups.xml, Drives.xml) contenant des mots de passe chiffrés avec la clé publique connue de Microsoft restent exploitables via Mimikatz (gpp-decrypt).

**DPAPI (Data Protection API)** : les secrets protégés par DPAPI (credentials navigateurs, certificats utilisateur) ne sont pas couverts par Credential Guard.

**Tokens et sessions actives** : un attaquant disposant d'une session RDP active d'un administrateur peut toujours voler son token via des techniques de token impersonation.

**Dump du processus LSASS lui-même** : bien que le contenu mémoire soit protégé, la liste des processus actifs reste visible — des solutions de détection complémentaires sont nécessaires.

**Comptes sans hachage NT (RODC)** : les contrôleurs de domaine en lecture seule (RODC) maintiennent un sous-ensemble de comptes dont les hachages sont répliqués localement.

### Complémentarité indispensable

Credential Guard doit être combiné avec : désactivation de NTLM v1, SMB Signing, LAPS pour les comptes locaux, tiering AD, Protected Users Security Group, et durcissement Active Directory complet pour une posture défensive robuste.

---

## Interactions avec LAPS, PAM et CyberArk

### LAPS (Local Administrator Password Solution)

Credential Guard et LAPS sont complémentaires et non redondants. LAPS gère les mots de passe des comptes administrateurs locaux (stockés dans l'attribut AD `ms-Mcs-AdmPwd` ou via le nouveau LAPS Windows 2023), tandis que Credential Guard protège les credentials des

utilisateurs de domaine en mémoire LSASS. Un poste compromis avec Credential Guard actif ne peut pas extraire les hachages NT des utilisateurs de domaine connectés, mais LAPS garantit que chaque machine a un mot de passe administrateur local unique — limitant le mouvement latéral via les comptes locaux.

### PAM (Privileged Access Management) — CyberArk, BeyondTrust

Les solutions PAM comme CyberArk Privileged Access Manager ou BeyondTrust Password Safe s'intègrent nativement avec Credential Guard :

CyberArk PSM (Privileged Session Manager) crée des sessions isolées qui ne stockent pas les credentials en mémoire LSASS des serveurs cibles — CG renforce ce modèle

La rotation automatique des passwords par CyberArk est compatible avec Credential Guard (les mots de passe sont mis à jour dans l'AD, les hachages LSASS sont protégés)

**Point d'attention** : CyberArk CPM (Central Policy Manager) peut nécessiter des exceptions pour certains agents si HVCI est activé. Vérifier la compatibilité avec la version déployée avant activation en production

BeyondTrust Endpoint Privilege Management est compatible avec Credential Guard et peut compléter la protection des sessions administratives

### Intégration Microsoft Defender for Identity

MDI (anciennement Azure ATP) surveille les tentatives d'extraction de credentials et génère des alertes spécifiques aux attaques sur LSASS. Couplé à Credential Guard, MDI détecte les tentatives de bypass (chargement de drivers suspects, modifications de la politique LSA) et permet une réponse aux incidents en temps réel.

## Cas d'incompatibilité et limitations

### Virtualisation imbriquée (Nested Hyper-V)

Si Windows Server 2025 est déployé comme VM sur un hyperviseur Hyper-V hôte, la virtualisation imbriquée doit être activée sur l'hyperviseur hôte pour que Credential Guard fonctionne :

```
 # Sur l'hôte Hyper-V, activer la virtualisation imbriquée pour la VM cible
Set-VMProcessor -VMName "NomDeLaVM" -ExposeVirtualizationExtensions $true
# Nécessite l'arrêt de la VM et un processeur compatible
```

Sur VMware ESXi, la virtualisation imbriquée (VHV) est supportée depuis vSphere 6.7 — activer "Expose hardware-assisted virtualization to the guest OS" dans les paramètres CPU de la VM.

### Clients VPN

**Cisco AnyConnect** : les versions antérieures à 4.10 présentent des incompatibilités avec HVCI. Migrer vers Cisco Secure Client (v5.x) avant d'activer Credential Guard

**Palo Alto GlobalProtect** : compatible depuis la version 5.2 avec les drivers HVCI-compliant. Vérifier que le driver pangpa.sys est dans la liste des drivers compatibles

**Fortinet FortiClient** : versions 7.0+ généralement compatibles, mais tester en environnement de préproduction

### Network Level Authentication (NLA) et CredSSP

NLA pour RDP utilise CredSSP qui délègue des credentials au serveur distant. Credential Guard **n'empêche pas** la délégation de credentials via CredSSP — c'est la politique "Restricted Admin Mode" ou "Remote Credential Guard" qui adresse ce risque pour RDP. Configurer Remote Credential Guard pour les connexions RDP administratives sensibles :

```
 # Activer Remote Credential Guard sur le client (Windows 10/11 ou Server 2016+)
$path = "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa"
Set-ItemProperty -Path $path -Name "DisableRestrictedAdmin" -Value 0

# Connexion RDP avec Remote Credential Guard
mstsc /remoteGuard /v:serveur-cible.domaine.fr
```

### Autres incompatibilités connues

Certains solutions DLP avec drivers noyau non signés WHQL

Agents de sauvegarde legacy (vérifier avec Veeam v12+ qui est compatible)

Cartes réseau avec drivers anciens non-HVCI compliant (rares sur matériel récent)

WDigest authentication (déjà désactivée par défaut depuis Windows 8.1 — mais à vérifier si la valeur de registre UseLogonCredential a été modifiée)

---

## Monitoring et détection des tentatives de bypass

### Événements à surveiller

Configurer votre SIEM pour alerter sur les événements suivants :

| Event ID | Source | Signification | Priorité |
|---|---|---|---|
| 3080 | DeviceGuard | LSAIso démarré — CG opérationnel | Info |
| 3082 | DeviceGuard | Configuration CG modifiée | CRITIQUE |
| 3033 | CodeIntegrity | Driver bloqué par HVCI | Haute |
| 3065 | CodeIntegrity | Driver non signé chargement tenté | Haute |
| 4657 | Security | Modification clé registre LSA/DeviceGuard | CRITIQUE |
| 4688 | Security | Processus Mimikatz connu créé | CRITIQUE |
| 10 | Sysmon | Accès mémoire processus LSASS | Haute |

### Règle de détection Sigma pour tentative bypass

```
 # Requête PowerShell pour détecter des modifications de la politique DeviceGuard
$filter = @{
    LogName = "Microsoft-Windows-DeviceGuard/Operational"
    Id = 3082
    StartTime = (Get-Date).AddDays(-7)
}
Get-WinEvent -FilterHashtable $filter |
    Select-Object TimeCreated, Message |
    Format-List

# Surveiller les accès au processus LSASS (nécessite audit ProcessAccess activé)
Get-WinEvent -FilterHashtable @{LogName="Security"; Id=4656} |
    Where-Object { $_.Message -match "lsass" } |
    Select-Object TimeCreated, Message -First 20
```

### Intégration Defender for Endpoint (MDE)

Microsoft Defender for Endpoint détecte nativement les tentatives d'injection dans LSASS et les chargements de drivers suspects. Avec Credential Guard actif, les alertes MDE sur LSASS indiquent généralement des tentatives plus sophistiquées (exploitation de drivers légitimes signés pour bypass) qui méritent une investigation immédiate en CTI.

---

## Déploiement en France : administrations et secteur bancaire

### Contexte réglementaire

L'ANSSI recommande Credential Guard dans son guide de durcissement Windows Server (ANSSI-BP-028) comme mesure de niveau "Renforcé". Dans le cadre de NIS2, la protection des

secrets d'authentification en mémoire est un contrôle technique attendu pour les entités essentielles (EE) et importantes (EI). Les auditeurs de conformité NIS2 vérifient notamment :

La protection des comptes privilegiés (tier 0) via Credential Guard sur les contrôleurs de domaine

L'activation de Protected Users Security Group pour les administrateurs de domaine

La journalisation des événements DeviceGuard dans le SIEM central

### Déploiement dans les administrations françaises

Plusieurs ministères et agences publiques françaises ont déployé Credential Guard dans le cadre de leur plan de durcissement AD post-incidents ransomware (LockBit, Cl0p). Les points clés observés en terrain :

**Inventaire matériel préalable** : 15 à 30% des serveurs en parc vieux de plus de 5 ans ne supportent pas TPM 2.0 — prévoir un plan de renouvellement ou une exception documentée

**Tests de non-régression** : les applications métier développées en interne avec des composants COM/DCOM anciens présentent parfois des incompatibilités avec HVCI

**Formation des équipes SOC** : les analystes doivent distinguer les faux positifs HVCI (Event ID 3033 légitimes) des vraies tentatives de bypass

**Déploiement par criticité** : contrôleurs de domaine et serveurs d'administration en priorité (tier 0), puis serveurs applicatifs critiques

### Secteur bancaire et DSP2

Les établissements bancaires français (soumis à DSP2, DORA à partir de 2025) ont généralement déjà déployé des solutions PAM comme CyberArk. Credential Guard s'inscrit comme un contrôle de défense en profondeur qui renforce l'isolation des sessions CyberArk PSM et réduit le risque de compromission des jumpboxes d'administration. La vérification de la protection du fichier NTDS.dit et de LSASS via Credential Guard fait partie des contrôles attendus lors des audits TIBER-EU.

## Désactivation contrôlée (scénarios de break-glass)

Dans les scénarios d'urgence nécessitant la désactivation temporaire de Credential Guard (incompatibilité critique découverte en production), la procédure dépend du mode d'activation :

```
 # Désactivation sans UEFI lock (LsaCfgFlags = 2) via registre
$path = "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa"
Set-ItemProperty -Path $path -Name "LsaCfgFlags" -Value 0
# Redémarrage requis

# ATTENTION : avec UEFI lock (LsaCfgFlags = 1), la désactivation via registre seul
# ne suffit pas — il faut aussi effacer les variables UEFI via WMI
# ou via l'outil de désactivation officiel Microsoft :
# DG_Readiness_Tool_v3.6.ps1 -Disable
# Cette opération génère l'Event ID 3082 et doit être tracée dans le SIEM
```

**À RETENIR**

Points clés à retenir

Credential Guard isole les secrets LSASS dans VTL1 — inaccessible même avec SYSTEM, même avec Mimikatz

Prérequis non négociables : TPM 2.0 + UEFI Secure Boot + Hyper-V

Privilégier l'activation avec UEFI lock (LsaCfgFlags = 1) en production pour éviter la désactivation silencieuse

Tester la compatibilité VPN et agents tiers avant déploiement à grande échelle

Credential Guard ne remplace pas LAPS, PAM ou le tiering AD — il les complète

Surveiller l'Event ID 3082 (modification config) comme signal d'alarme critique dans votre SIEM

## Questions fréquentes sur Credential Guard Windows Server 2025

### Credential Guard protège-t-il contre Mimikatz ?

Oui, Credential Guard bloque efficacement les modules Mimikatz qui ciblent la mémoire LSASS, notamment `sekurlsa::logonpasswords` et `sekurlsa::wdigest`. Ces commandes retournent "KO - LSA Isolated" car les hachages NTLM et tickets Kerberos sont stockés dans LSAIso (VTL1), un environnement d'exécution sécurisé inaccessible depuis le système d'exploitation principal. En revanche, Credential Guard ne protège pas contre les modules Mimikatz qui n'accèdent pas à LSASS, comme `lsadump::dcsync` (qui interroge l'AD directement) ou `kerberos::ptt` (injection de tickets obtenus par d'autres moyens).

### Quels sont les prérequis matériels pour Credential Guard ?

Les prérequis matériels obligatoires pour Credential Guard sur Windows Server 2025 sont : un TPM 2.0 (puce Trusted Platform Module version 2.0), un firmware UEFI natif (pas de mode Legacy/CSM) avec Secure Boot activé, des extensions de virtualisation processeur (Intel VT-x avec EPT ou AMD-V avec NPT), un processeur 64 bits, et au minimum 8 Go de RAM. Le rôle Hyper-V doit également être installé même si le serveur n'héberge pas de machines virtuelles, car VBS repose sur l'hyperviseur. Les serveurs de plus de 5 ans peuvent ne pas satisfaire ces prérequis — un audit matériel préalable avec l'outil DG_Readiness_Tool est recommandé.

### Credential Guard est-il compatible avec Hyper-V ?

Credential Guard est compatible avec Hyper-V lorsque Windows Server 2025 est l'hyperviseur hôte. En revanche, si Windows Server 2025 est lui-même une VM tournant sur un hôte Hyper-V, la virtualisation imbriquée (Nested Virtualization) doit être activée sur l'hôte via la commande `Set-VMProcessor -VMName "NomVM" -ExposeVirtualizationExtensions $true`. Sur VMware ESXi, l'option "Expose hardware-assisted virtualization to the guest OS" doit être cochée dans

les paramètres CPU. La virtualisation imbriquée introduit une légère surcharge de performance (généralement inférieure à 5%) à prendre en compte dans les environnements virtualisés denses.

### Comment vérifier que Credential Guard est bien actif ?

La méthode la plus fiable est d'utiliser PowerShell : `Get-CimInstance -Namespace "root\Microsoft\Windows\DeviceGuard" -ClassName "Win32_DeviceGuard"`. Credential Guard est actif si la propriété `SecurityServicesRunning` contient la valeur **2**. La propriété `VirtualizationBasedSecurityStatus` doit afficher **2** (Running) pour que VBS soit opérationnel. Vous pouvez aussi vérifier dans msinfo32.exe sous "Virtualization-based security Services Running" — la mention "Credential Guard" doit y apparaître. Un troisième indicateur est l'Event ID 3080 dans le journal "Microsoft-Windows-DeviceGuard/Operational" qui confirme le démarrage de LSAIso.

### Credential Guard remplace-t-il LAPS ou PAM ?

Non, Credential Guard ne remplace ni LAPS ni une solution PAM — ces technologies sont complémentaires et adressent des risques différents. Credential Guard protège les credentials des utilisateurs de domaine stockés en mémoire LSASS (hachages NTLM, tickets Kerberos). LAPS gère les mots de passe uniques des comptes administrateurs locaux, empêchant le mouvement latéral via des comptes locaux partagés. Une solution PAM comme CyberArk gère l'accès privilegié bout-en-bout : coffre-fort de mots de passe, rotation automatique, enregistrement des sessions. Un environnement robuste déploie les trois : Credential Guard contre le vol de credentials en mémoire, LAPS pour les comptes locaux, et PAM pour l'accès administrateur structuré et auditable.

## Références et documentation

Microsoft Learn — Sécurité Windows Server

ANSSI — Guide de sécurisation Active Directory

MITRE ATT&CK — Techniques Active Directory