AYI NEDJIMI Consultants

GPO Sécurisation Active Directory : Hardening par : Guide

Catégorie : Attaques Active Directory Lecture : 10 min Publié le : 08/03/2026 Auteur : Ayi NEDJIMI

Guide complet de sécurisation Active Directory par GPO : password policy, account lockout, audit policy, AppLocker, BitLocker, Credential Guard, WMI.

2.1 Qu'est-ce qu'une GPO ?

Une **Group Policy Object** est un conteneur de paramètres de configuration stocké dans Active Directory (partie logique dans le conteneur `CN=Policies,CN=System,DC=domain`) et dans le dossier **SYSVOL** (partie physique sous `\\domain\SYSVOL\domain\Policies\{GUID}`). Chaque GPO possède un identifiant unique (GUID), un numéro de version et deux sections distinctes : Guide complet de sécurisation Active Directory par GPO : password policy, account lockout, audit policy, AppLocker, BitLocker, Credential Guard, WMI. Active Directory reste la cible privilégiée des attaquants en environnement Windows. Comprendre gpo securisation active directory hardening est indispensable pour les équipes offensives comme défensives. Nous abordons notamment : 8. checklist gpo sécurité : 20 points de contrôle, questions frequentes et 9. conclusion : les gpo comme fondation de la posture de sécurité ad. Les professionnels y trouveront des recommandations actionnables, des commandes prêtes à l'emploi et des stratégies de mise en œuvre adaptées aux environnements d'entreprise.

- **Computer Configuration** : paramètres appliqués au démarrage de la machine, indépendamment de l'utilisateur connecté. C'est ici que se trouvent les paramètres de sécurité critiques (audit, droits, services, pare-feu).
- **User Configuration** : paramètres appliqués à l'ouverture de session. Utile pour les restrictions d'interface, les scripts de logon et les redirections de dossiers.

Les GPO sont **liées** (linked) à des conteneurs Active Directory : sites, domaines ou Unités d'Organisation (OU). Cette liaison détermine le périmètre d'application. Un point critique souvent méconnu : une GPO non liée existe dans AD mais **ne s'applique à rien**. Inversement, une GPO peut être liée à plusieurs OU simultanément, ce qui en fait un outil de déploiement puissant mais potentiellement complexe à auditer.

2.2 L'ordre de traitement LSDOU

L'ordre de traitement des GPO suit l'acronyme **LSDOU** : Local, Site, Domain, Organizational Unit. Cet ordre est fondamental pour comprendre quelle configuration prévaut en cas de conflit :

Ordre	Niveau	Description	Priorité
1	Local	GPO locale sur chaque machine (`gpedit.msc`)	La plus basse
2	Site	GPO liées au site AD (rarement utilisé pour la sécurité)	Basse
3	Domain	GPO liées au domaine (Default Domain Policy)	Moyenne
4	OU	GPO liées aux OU (du plus haut au plus bas dans la hiérarchie)	La plus haute

Le principe est simple : **le dernier paramètre appliqué gagne**. Une GPO liée à une OU enfant écrase le même paramètre défini dans une GPO de domaine. Deux mécanismes modifient ce comportement :

- **Enforced (No Override)** : force la GPO parente à prévaloir sur les GPO enfants. Utilisez-le pour les politiques de sécurité critiques qui ne doivent jamais être surchargées par les OU métier.
- **Block Inheritance** : empêche les GPO parentes de s'appliquer à une OU. Dangereux en sécurité car il peut désactiver des contrôles essentiels. Une GPO Enforced ignore ce blocage.

Bonne pratique LSDOU
Créez une GPO de sécurité de base liée au domaine en mode **Enforced** pour garantir que les paramètres critiques (audit, password policy, verrouillage) s'appliquent partout, même si un administrateur délégué utilise Block Inheritance sur son OU. C'est le principe de la **baseline non contournable**.

2.3 WMI Filters et Security Filtering

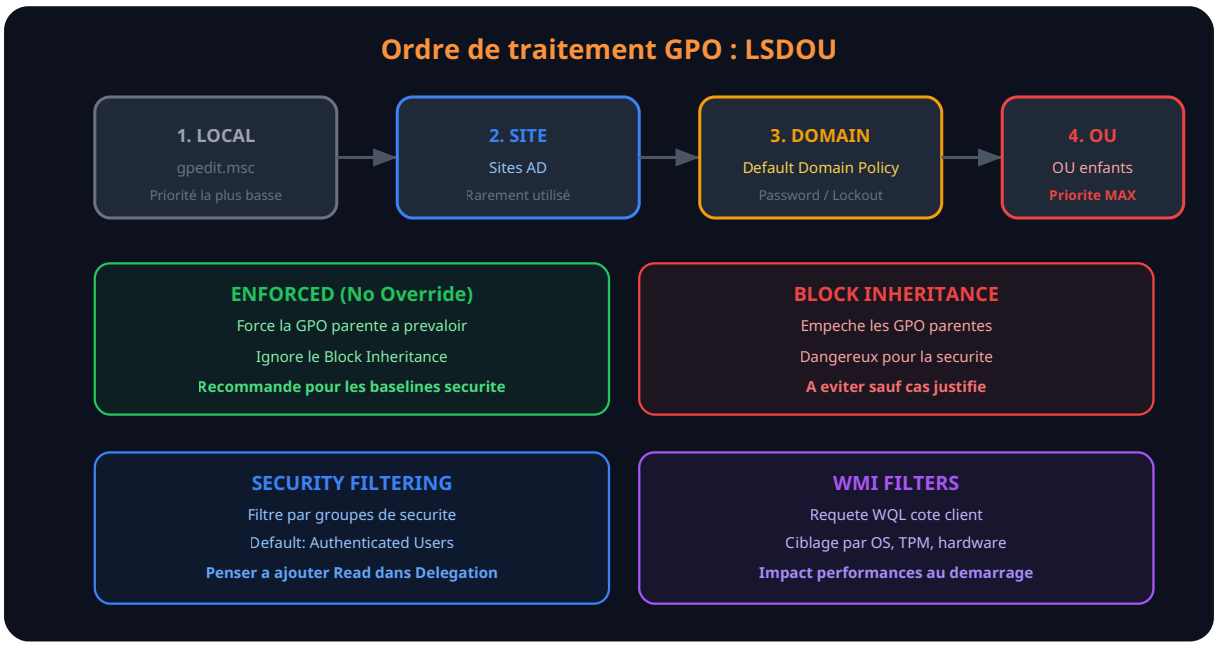
Une compromission d'un seul poste de travail pourrait-elle mener à votre contrôleur de domaine ?

Les **WMI Filters** permettent de conditionner l'application d'une GPO à une requête WQL (WMI Query Language). Par exemple, appliquer une GPO BitLocker uniquement aux machines équipées d'un TPM 2.0 :

```
SELECT * FROM Win32_Tpm WHERE IsEnabled_InitialValue = TRUE AND SpecVersion LIKE "2.0%"
```

Les WMI Filters sont évalués côté client, ce qui peut impacter les performances de démarrage. Utilisez-les avec parcimonie et préférez le **Security Filtering** (filtrage par groupes de sécurité) lorsque c'est possible. Le Security Filtering par défaut est `Authenticated Users`, ce qui signifie que la GPO s'applique à tous les objets dans le périmètre de la liaison. Pour restreindre l'application :

1. Retirez `Authenticated Users` de la section Security Filtering.
2. Ajoutez le groupe de sécurité cible.
3. **Critique** : ajoutez `Authenticated Users` ou `Domain Computers` avec la permission **Read** uniquement dans l'onglet Delegation. Sans cette permission, le client ne peut pas lire la GPO et elle ne s'applique pas du tout -- un bug classique qui a piégé des milliers d'administrateurs depuis Windows Server 2016.



Cas concret

L'attaque ZeroLogon (CVE-2020-1472) permettait d'obtenir les privilèges d'administrateur de domaine en envoyant simplement des zéros dans le challenge Netlogon. Cette vulnérabilité critique, exploitable en quelques secondes, a rappelé que les protocoles historiques d'AD restent des surfaces d'attaque majeures.

Les sous-categories critiques a activer en **Success and Failure** :

Sous-catégorie	Event IDs clés	Détection
Logon/Logoff > Logon	4624, 4625	Connexions reussies/echouees, brute force, lateral movement
Logon/Logoff > Special Logon	4672	Attribution de privileges administrateurs
Account Management > User Account Management	4720, 4722, 4724, 4738	Creation, activation, reset password, modification de comptes
Account Management > Security Group Management	4728, 4732, 4756	Ajout de membres aux groupes (Domain Admins, etc.)
DS Access > Directory Service Changes	5136, 5137, 5141	Modifications AD : attributs, objets, suppressions. Essentiel pour detecter DCSync, DCShadow
Object Access > File System	4663	Acces aux fichiers sensibles (SYSVOL, partages admin)
Privilege Use > Sensitive Privilege Use	4673, 4674	Utilisation de privileges sensibles (SeDebugPrivilege, etc.)
Policy Change > Audit Policy Change	4719	Modification de la politique d'audit elle-meme (signe de compromission)

```
# Verifier la politique d'audit effective sur un serveur
auditpol /get /category:*

# Exporter dans un fichier CSV pour analyse
auditpol /get /category:* /r > C:\audit-policy-export.csv
```

3.4 User Rights Assignment (Attribution des droits utilisateurs)

Cette section de la GPO definit **qui peut faire quoi** sur les machines ciblees. Plusieurs droits sont critiques du point de vue securite et constituent des vecteurs d'elevation de privileges :

Droit	Risque	Recommandation
Debug programs (SeDebugPrivilege)	Permet l'injection de code dans tout processus, y compris LSASS. Vecteur de credential dumping via Mimikatz	Administrateurs uniquement. **Retirer** pour les postes de travail
Act as part of the operating system (SeTcbPrivilege)	Permet de se faire passer pour n'importe quel utilisateur	Vide (aucun compte)
Allow log on through Remote Desktop	Acces RDP. Vecteur de lateral movement	Groupe restreint d'administrateurs. Jamais Domain Users
Access this computer from the network	Acces reseau (partages, RPC). Necessaire mais a restreindre	Authenticated Users + Administrators. **Retirer** le compte Guest
Deny log on locally / Deny log on through RDP	Protection des comptes de service et comptes privilegies	Ajouter les comptes de service et les Tier 0 sur les postes Tier 1/2
Back up files and directories (SeBackupPrivilege)	Permet de lire tout fichier, y compris NTDS.dit et SAM	Backup Operators uniquement sur les DC

Votre Active Directory résisterait-il à une attaque Kerberoasting ?

BitLocker protege les donnees en cas de vol ou de perte d'un poste de travail. La configuration par GPO permet un deploiement uniforme et le stockage centralise des cles de recuperation dans Active Directory.

Parametres GPO essentiels (`Computer Configuration > Policies > Administrative Templates > Windows Components > BitLocker Drive Encryption`) :

- **Require additional authentication at startup** : `Enabled`, avec TPM + PIN. Le TPM seul ne protege pas contre les attaques Evil Maid ou les attaques DMA.
- **Choose drive encryption method** : `XTS-AES 256-bit` pour les disques systeme, `AES-CBC 256-bit` pour les disques amovibles (compatibilite).
- **Store BitLocker recovery information in AD DS** : `Enabled`. Stocke les cles de recuperation dans l'attribut `ms-FVE-RecoveryPassword` de l'objet ordinateur.
- **Do not enable BitLocker until recovery information is stored** : `Enabled`. Empeche le chiffrement si la cle de recuperation n'est pas sauvegardee dans AD.

4.4 Credential Guard : protection des identifiants en mémoire

Windows Defender Credential Guard utilise la virtualisation (VBS - Virtualization Based Security) pour isoler les secrets (hashes NTLM, tickets Kerberos TGT) dans un conteneur securise inaccessible meme avec les privileges SYSTEM. Il rend inefficaces les attaques de type **Pass-the-Hash** et **credential dumping** via Mimikatz.

Activation via GPO : `Computer Configuration > Policies > Administrative Templates > System > Device Guard > Turn On Virtualization Based Security` :

- **Select Platform Security Level** : `Secure Boot and DMA Protection`
- **Credential Guard Configuration** : `Enabled with UEFI lock` (irreversible sans acces physique -- le niveau le plus securise)
- **Secure Launch Configuration** : `Enabled`

Prerequis materiels : CPU avec virtualisation (Intel VT-x/AMD-V), TPM 2.0, UEFI Secure Boot, 64 bits. La plupart des postes recents (2020+) supportent Credential Guard. Testez la compatibilite avec `msinfo32` (verifier "Virtualization-based security" = Running).

Credential Guard et compatibilite
Credential Guard bloque l'utilisation de NTLMv1, WDigest et Kerberos DES/RC4 non contraint. Avant le deploiement, verifiez qu'aucune application ne depend de ces protocoles obsoletes. Credential Guard est incompatible avec certaines technologies de virtualisation legacy (notamment les anciennes versions de VMware Workstation). Pour les details sur les attaques que Credential Guard previent, voir notre article sur les techniques de credential dumping.

Le processus de deploiement :

1. **Telecharger** le SCT depuis le Microsoft Download Center (gratuit).
2. **Extraire** les baselines dans un repertoire dedie.
3. **Analyser** avec l'outil `Policy Analyzer` (compare vos GPO actuelles avec la baseline Microsoft).
4. **Importer** les GPO baseline via le script `Baseline-LocalInstall.ps1` dans un environnement de test.
5. **Comparer et adapter** : la baseline Microsoft est un point de depart, pas une solution universelle. Certains parametres peuvent casser des applications metier.
6. **Deployer** progressivement en production, OU par OU.

```
# Importer une baseline Microsoft dans GPMC
# Depuis le dossier extrait de la baseline Windows 11 24H2
.\Baseline-LocalInstall.ps1

# Comparer vos GPO avec la baseline
# Ouvrir Policy Analyzer > Add > pointer vers vos GPO exportees
# Resultat : tableau de differences parametre par parametre
```

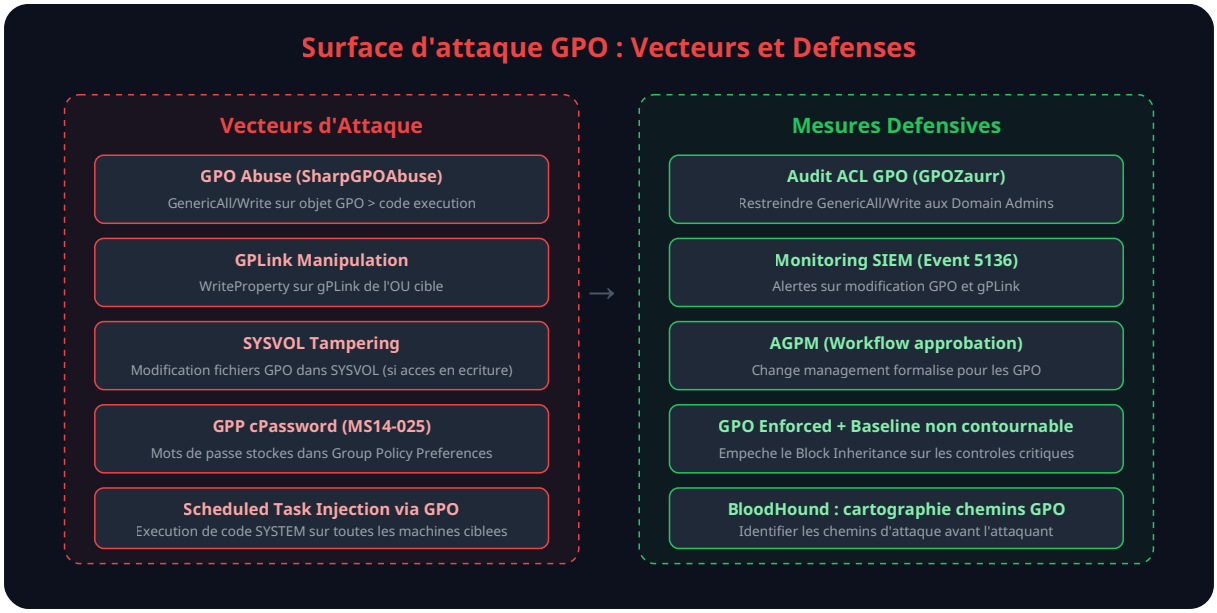
L'outil **Policy Analyzer** est particulierement utile pour identifier les ecarts entre votre configuration actuelle et les recommandations Microsoft. Il genere un rapport Excel detaillant chaque parametre, sa valeur actuelle, la valeur recommandee et l'impact potentiel de la modification.

Un attaquant disposant du droit **WriteProperty** sur l'attribut `gPLink` d'une OU peut lier une GPO malveillante a cette OU. Il peut egalement modifier l'ordre de liaison (`gPOptions`) ou supprimer la liaison d'une GPO de securite, desactivant ainsi les controles en place.

Cette attaque est plus subtile que la modification directe d'une GPO car elle ne necessite pas de droits sur l'objet GPO lui-meme, mais sur l'objet OU. Les ACL des OU sont souvent moins surveillees que celles des GPO.

Detection et prevention des attaques GPO
Pour proteger vos GPO contre l'abus :

- **Auditer les permissions GPO** regulierement avec GPOZaurr. Seuls les `Domain Admins` et `Group Policy Creator Owners` devraient pouvoir modifier les GPO de securite.
- **Monitorer les evenements 5136** (modification d'objet AD) sur les objets `groupPolicyContainer` et l'attribut `gPLink` des OU.
- **Configurer des alertes SIEM** sur toute modification des GPO critiques (security baseline, audit policy, password policy).
- **Utiliser AGPM** (Advanced Group Policy Management) de MDOP pour implementer un workflow d'approbation sur les modifications GPO.



8. Checklist GPO Sécurité : 20 points de contrôle

Cette checklist resume les 20 points de controle essentiels a verifier et implementer dans votre environnement Active Directory. Utilisez-la comme base d'audit periodique (trimestriel recommande).

#	Point de controle	Priorite	Statut
1	Password Policy : 14+ caracteres, complexite activee	Critique	☐
2	Account Lockout : 5 tentatives, 30 min de verrouillage	Critique	☐
3	FGPP pour les comptes privilegies (20+ caracteres)	Haute	☐
4	Advanced Audit Policy active avec sous-categories critiques	Critique	☐
5	SeDebugPrivilege restreint aux administrateurs	Haute	☐
6	NTLM restreint (NTLMv2 only, audit puis blocage)	Haute	☐
7	SMB Signing active (always)	Haute	☐
8	Tiering model enforce via Deny log on	Critique	☐
9	AppLocker deploye en mode Enforce	Haute	☐
10	Windows Firewall : bloquer SMB/RDP/WinRM entre postes	Haute	☐
11	BitLocker avec TPM + PIN, cles dans AD	Moyenne	☐
12	Credential Guard active avec UEFI lock	Haute	☐
13	PowerShell Script Block Logging active	Haute	☐
14	Macros Office bloquees pour fichiers Internet	Haute	☐
15	LAPS deploye pour les mots de passe admin locaux	Critique	☐
16	Security Baseline Microsoft importee et comparee	Moyenne	☐
17	GPO de securite en mode Enforced	Haute	☐
18	Audit GPOZaurr trimestriel (GPO vides, orphelines, permissions)	Moyenne	☐
19	Monitoring SIEM des modifications GPO (Event 5136)	Haute	☐
20	Enumeration anonyme desactivee (SAM, LSA)	Haute	☐

Pour approfondir ce sujet, consultez notre outil open-source ad-security-audit qui facilite l'audit de sécurité complet d'Active Directory.

Questions frequentes

Comment mettre en place GPO Sécurisation Active Directory dans un environnement de production ?

La mise en place de GPO Sécurisation Active Directory en production necessite une planification rigoureuse, incluant l'evaluation des prerequis techniques, la definition d'une architecture cible, des tests de validation approfondis et un plan de deploiement progressif avec des points de controle a chaque etape.

Comment détecter rapidement une attaque de type GPO Sécurisation Active Directory : Hardening ?

Surveillez les événements Windows 4662, 4624 type 3 et 4672 via votre SIEM. Corrélez-les avec des connexions inhabituelles vers les contrôleurs de domaine en dehors des heures de travail.

Quels sont les premiers gestes de remédiation après GPO Sécurisation Active Directory : Hardening ?

Isolez le compte compromis, forcez la rotation de krbtgt deux fois à 12h d'intervalle, et analysez les logs Kerberos. Lancez ensuite un scan BloodHound pour cartographier les chemins d'attaque restants.

Sources et références : MITRE ATT&CK Privilege Escalation · ADSecurity.org

> Points clés à retenir
>
> - 8. Checklist GPO Sécurité : 20 points de contrôle
> - Questions frequentes
> - 9. Conclusion : les GPO comme fondation de la posture de sécurité AD

9. Conclusion : les GPO comme fondation de la posture de sécurité AD

Les Group Policy Objects constituent la **fondation technique** du durcissement Active Directory. Sans GPO de securite correctement configurees, auditees et maintenues, toute strategie de protection de l'annuaire repose sur du sable. Les attaquants l'ont bien compris : les GPO sont a la fois leur obstacle principal et leur vecteur d'attaque preferentiel une fois qu'ils disposent de permissions suffisantes.

L'approche recommandee repose sur trois piliers :

1. **Defense en profondeur** : empiler les couches de protection (password policy + audit + AppLocker + Credential Guard + firewall). Chaque couche compense les faiblesses des autres.
2. **Audit continu** : deployer GPOZaurr et les rapports SIEM pour detecter les derives et les modifications non autorisees. Un audit trimestriel des GPO devrait faire partie du plan de securite de toute organisation.
3. **Alignement sur les baselines** : utiliser le Microsoft Security Compliance Toolkit comme reference et adapter les parametres au contexte metier. Ne pas reinventer ce que Microsoft a deja documente et teste.

La securisation par GPO s'inscrit dans une demarche plus large de hardening Active Directory qui inclut le tiering model, la securisation des identites cloud, la conformite ISO 27001 et la surveillance continue via un SOC. Les GPO ne sont qu'une piece du puzzle, mais elles en constituent le socle indispensable.

Articles connexes

Active Directory
Top 10 Attaques Active Directory
Kerberoasting, DCSync, Pass-the-Hash, Golden Ticket
Hardening
Guide Securisation Active Directory 2025
Tiering model, LAPS, AdminSDHolder, delegation
Techniques Hacking
Password Attacks : Cracking, Spraying, Credential Stuffing
Techniques d'attaque et detection des attaques par mots de passe
Techniques Hacking
Credential Dumping : LSASS, SAM, NTDS.dit
Mimikatz, secretsdump, Credential Guard comme contre-mesure
Techniques Hacking
Lateral Movement et Techniques de Pivoting
PsExec, WMIExec, SMBExec, WinRM -- et comment les bloquer
Conformite
ISO 27001 : Guide Complet
Cadre de reference pour la securite de l'information

References et ressources externes

- Microsoft Learn -- Credential Guard -- Documentation officielle Credential Guard / VBS
- Microsoft Learn -- AppLocker -- Configuration et deploiement AppLocker
- Microsoft Security Compliance Toolkit -- Telecharger les baselines de securite
- GPOZaurr (GitHub) -- Module PowerShell d'audit GPO
- ANSSI -- Recommandations Active Directory -- Guide de durcissement officiel ANSSI

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

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