GUIDE MÉTHODOLOGIQUE & OPÉRATOIRE

Référentiel d'audit Active Directory

Édition 2026 — état de l'art août 2026 · plan de contrôle étendu

BadSuccessor CVE-2025-53779 | AD CS ESC1-17 + Certighost | RC4/NTLM 2026 | ReCyF v2.5 | Plan de contrôle étendu | Post-quantique

Ayi NEDJIMI Consultants

https://ayinedjimi-consultants.fr

Dernière vérification technique : 6 août 2026 · Document vivant (v1.1)

Sommaire

Guide méthodologique et opératoire — état de l'art août 2026

> **Bloc de fraîcheur.** Dernière vérification technique : 6 août 2026. Plateformes : Windows Server 2016 à 2025. Taxonomie AD CS : ESC1–ESC16 (SpecterOps), plus ESC17 (WSUS) et les CVE traitées à part. Outils : BloodHound CE, Certipy v5+, Certify 2.0, PingCastle, PSPKIAudit, ORADAD, DSInternals, Impacket, Rubeus. Référentiels : ANSSI (guide AD, PA-022, ReCyF v2.5), CIS Benchmarks, NIST SP 800-53/63 et CSF 2.0, ISO/IEC 27001:2022, MITRE ATT&CK et D3FEND. Document vivant : revérifier toute affirmation datée à chaque révision, en particulier la veille CVE et le calendrier de la loi Résilience.
> **Convention de lecture.** Les commandes sont fournies à titre opératoire et s'exécutent en lecture seule sauf mention contraire explicite (⚠ *modification*). Adapter les noms de domaine, DN et serveurs. Les commandes offensives (Rubeus, Impacket, mimikatz, Certipy en mode exploitation) ne s'emploient que dans le périmètre autorisé et tracé défini par la lettre de mission.

Introduction — pourquoi ce référentiel, et ce qui change en 2026

Active Directory reste, en 2026, la colonne vertébrale de l'authentification et de l'autorisation de la quasi-totalité des systèmes d'information d'entreprise, et par conséquent la cible privilégiée des attaquants : dans la grande majorité des intrusions à impact — ransomware comme espionnage — la prise de contrôle du domaine est le point de bascule à partir duquel l'adversaire obtient une liberté d'action quasi totale. Auditer Active Directory, ce n'est donc pas cocher des cases : c'est mesurer la résistance du cœur du SI.

Ce référentiel est le **pendant méthodologique et diagnostique** du guide de durcissement Active Directory publié par ailleurs sur ce site. Le guide de durcissement dit *quoi mettre en œuvre* ; ce document dit *comment constater* l'état réel d'un annuaire, comment le prouver, comment prioriser les écarts et comment les restituer. La remédiation renvoie systématiquement au guide de durcissement plutôt que d'en dupliquer les contrôles.

Six repères ancrent cette édition dans l'état de l'art d'août 2026.

La forêt est la frontière de sécurité native d'Active Directory — mais pas la frontière réelle du SI. Un objectif de remédiation n'est atteint que lorsqu'il l'est sur l'ensemble des domaines de la forêt, traités en parallèle, faute de quoi un domaine assaini est recompromis depuis un domaine qui ne l'est pas encore. Aller un cran plus loin : la frontière pertinente est le **plan de contrôle étendu**, c'est-à-dire Active Directory *plus* tout composant capable de modifier, restaurer, intercepter, signer ou administrer ses actifs de Tier 0 — hyperviseurs, sauvegarde, PAM, EDR/RMM, PKI, tenant Entra, chaînes de déploiement (MECM), comptes DNS/DHCP privilégiés, dépôts de scripts et pipelines d'infrastructure-as-code. Un administrateur de l'hyperviseur hébergeant les DC peut dominer la forêt sans compte AD privilégié.

BadSuccessor a été corrigé mais reste résiduel. Documentée par Akamai début 2025, la technique permettait à quiconque contrôlait un objet dMSA de Windows Server 2025 de prendre le contrôle de n'importe quel compte du domaine. Elle porte l'identifiant **CVE-2025-53779** (CVSS 7.2, « exploitation moins probable » car elle exige un DC 2025) et a été **corrigée le 12 août 2025** : le KDC impose désormais un lien dMSA mutuel, ce qui ferme l'escalade directe « instant Domain Admin » sur les DC à jour (build 26100.4946 ou supérieur). La mécanique dMSA

reste exploitable pour le vol d'identifiants et le mouvement latéral. Contrôler à la fois le niveau de patch des DC 2025 et les droits de création d'objets (CreateChild) sur les OU — pas la seule présence d'objets dMSA. Le correctif ne règle pas tout.

AD CS impose une rigueur de nomenclature. La taxonomie SpecterOps stable va de **ESC1 à ESC16**. **ESC17 — « Enrollee-Supplied Subject for Server Authentication »** est un ajout récent (Troopers 2026, adopté par Certipy v5+, hors set d'origine) : un gabarit permettant au demandeur de fournir le sujet/SAN avec un EKU Server Authentication autorise l'usurpation d'un service TLS. L'usurpation d'un WSUS HTTPS n'en est qu'un cas d'exploitation particulier ; l'impact peut se limiter à de l'exécution de code, pas nécessairement Domain Admin. **Certighost / CVE-2026-54121** n'est *pas* une ESC : c'est une **vulnérabilité logicielle distincte** (faille d'autorisation dans le « chase » d'enrôlement où l'AC contacte un DC fourni par le demandeur sans le valider), CVSS 8.8, corrigée le 14 juillet 2026, exploit public le 24 juillet 2026, permettant à un simple utilisateur authentifié d'usurper un DC puis d'exécuter un DCSync. Distinguer donc défauts de configuration (ESC) et vulnérabilités logicielles (CVE).

La dépréciation des protocoles hérités se formule avec précision. RC4 : Windows Server 2025 n'émet plus de TGT en RC4 et le durcissement 2026 retire RC4 des types de chiffrement supposés par défaut du KDC ; mais RC4 ne disparaît pas — un compte, un trust ou une application explicitement configurés en RC4 continuent. Rechercher ces exceptions et prouver que la bascule a été testée. NTLM : distinguer trois trajectoires — retrait protocolaire de NTLMv1 (Windows 11 24H2 / Windows Server 2025), blocage des cryptographies dérivées de NTLMv1 pour le SSO (`BlockNTLMv1SSO`, mode Enforce visé pour octobre 2026), et dépréciation générale de NTLM/NTLMv2 (que IAKerb et le Local KDC réduisent sans la supprimer). La coercition NTLM reste active (CVE-2025-24054, CVE-2026-33829).

Le contexte réglementaire français est en tension. La loi Résilience (transposition unique de NIS2, de la directive REC et de DORA) a été adoptée par le Sénat le 12 mars 2025 et examinée en commission spéciale à l'Assemblée en septembre 2025, mais n'a jamais été inscrite en séance publique, le texte achoppant sur ses dispositions anti-portes dérobées relatives au chiffrement ; son examen est repoussé à septembre 2026 au plus tôt. La Commission européenne a saisi la CJUE le 8 juillet 2026 contre la France (avec l'Irlande, les Pays-Bas et l'Espagne) pour non-transposition de NIS2, la France ayant déjà été renvoyée depuis avril 2026 pour la directive REC. Périmètre attendu : environ 15 000 entités. Le **ReCyF v2.5** (ANSSI, 17 mars 2026) est un **document de travail** (référentiel préparatoire, non obligatoire par défaut à ce stade) ; il structure 20 objectifs en quatre blocs, les entités importantes étant concernées par les objectifs 1 à 15 et les entités essentielles par les objectifs 1 à 20. Les objectifs 16 à 20 imposent explicitement aux entités essentielles des audits réguliers, le durcissement et l'administration dédiée : l'audit devient un moyen de conformité.

L'unité de risque est le chemin d'attaque vers le plan de contrôle, pas la vulnérabilité isolée. Un droit `GenericAll` est bénin sur un groupe de laboratoire vide, critique sur un compte synchronisé vers Entra, catastrophique sur une AC ou une sauvegarde. Coter selon la portée du contrôle, les prérequis, la fiabilité d'exploitation, la proximité du plan de contrôle, le rayon d'impact, la persistance, la détectabilité et la réversibilité. Réserver le CVSS aux CVE logicielles, en information secondaire.

Encadré — Quick wins « 0 à 30 jours ». Traiter en priorité dès la restitution : `ms-DS-MachineAccountQuota` à 0 ; Spouleur d'impression désactivé sur les DC ; signature LDAP + channel binding en enforcement (après inventaire) ; comptes d'administration humains Tier 0 *éligibles* dans Protected Users (après test de compatibilité) et Authentication Silos pour les autres

catégories ; nettoyage d'AdminSDHolder et d'`adminCount` résiduel ; correctifs Certighost (AC) et BadSuccessor (DC 2025) ; suppression des `cpassword` et SYSVOL en lecture seule ; désactivation de LLMNR, NBT-NS et mDNS ; réinitialisation des comptes dont le mot de passe a fuité ou est partagé avec un compte privilégié.

Partie 0 — Cadrage, méthodologie et éthique de mission

0.1 Fixer les objectifs et la typologie d'audit

Déterminer la finalité avant toute collecte : conformité (écarts à un référentiel, avec preuve), technique (configuration et exposition réelles), red-team-like / assumed breach (validation de chemins d'attaque en supposant une brèche), ou forensique (recherche de compromission). Choisir selon la maturité du commanditaire et l'objectif réglementaire ; pour une entité essentielle, rattacher explicitement la mission aux objectifs 16 à 20 du ReCyF. Poser dès l'origine un **modèle de menace** (ransomware opportuniste, APT étatique, insider) : il conditionne les approfondissements — un APT ciblera AD CS et la persistance, un insider les secrets dans les attributs et les réutilisations de mots de passe.

0.2 Verrouiller le cadre contractuel et légal

Formaliser la lettre de mission : périmètre précis (forêt, domaines, tenants Entra, actifs du plan de contrôle inclus ou exclus), autorisations écrites d'audit actif, fenêtres de test, points de contact d'escalade. **Obtenir une autorisation explicite et distincte pour la manipulation des empreintes de mots de passe** (cf. Partie 4), qui sont des secrets. Préciser la propriété des livrables, le traitement des données personnelles collectées et la responsabilité en cas d'incident provoqué, avec kill switch et plan de retour arrière.

0.3 Constituer la matrice de correspondance des référentiels

Réunir les référentiels mobilisés : guide AD de l'ANSSI, PA-022, ReCyF v2.5, EBIOS RM ; CIS Benchmarks (Windows Server, DC, serveur membre) ; NIST SP 800-53, 800-171, **SP 800-63-4** (63A-4/63B-4/63C-4) et CSF 2.0 (qui intègre désormais la chaîne d'approvisionnement et l'identité) ; ISO/IEC 27001:2022 annexe A ; MITRE ATT&CK avec ses sous-techniques (T1558.003 Kerberoasting, T1606.002 Golden SAML) et D3FEND. Construire dès le cadrage la table de traçabilité **objectif réglementaire → contrôle → preuve** qui structurera le rapport.

0.4 Choisir la posture et le mode d'audit

Arbitrer entre boîte noire, grise et blanche selon le rapport couverture/coût/réalisme. Appliquer la méthode **« read-only first »** : conduire toute la collecte non intrusive avant la moindre validation active. Définir les fenêtres de test, la charge acceptable sur les DC, les quotas de requêtes LDAP, les critères d'arrêt et la procédure de « stop test ».

0.5 Sécuriser l'environnement d'audit

Opérer depuis un poste dédié, contrôlé et isolé (VM jetable, réseau isolé) ; n'adhérer au domaine que si un scénario de collecte le nécessite (RSoP, GPO, Kerberos intégré) et uniquement sur autorisation explicite. Créer des identifiants temporaires dédiés, les révoquer et les tracer en fin de mission. Chiffrer les collectes, les conserver dans un coffre de secrets, prouver leur effacement post-mission. Ne jamais réutiliser d'identifiants ni mélanger les artefacts entre clients.

0.6 Poser le modèle de criticité et de scoring

Coter par chemin et rayon d'impact (portée × prérequis × fiabilité × proximité du plan de contrôle × persistance × détectabilité × réversibilité). Réserver le CVSS aux CVE logicielles. Considérer par défaut comme critique toute capacité d'action sur un actif du plan de contrôle.

0.7 Garantir la chaîne de custody et l'intégrité des preuves

Horodater, hacher en SHA-256 et journaliser chaque collecte. Conserver de façon probante (support write-once, scellés, registre d'accès) pour le volet judiciaire. Minimiser les données personnelles dans les preuves (RGPD).

```
# Sceller une collecte
Get-FileHash .\collecte_ad_2026-08-06.zip -Algorithm SHA256 |
  Tee-Object -FilePath .\collecte_ad_2026-08-06.sha256.txt
```

0.8 Piloter la mission

Établir un RACI (auditeur, RSSI, équipe AD, DPO, direction), un planning jalonné, une comitologie. Anticiper la gestion des incidents survenant *pendant* l'audit. Versionner scripts et collectes pour garantir la reproductibilité des ré-audits.

0.9 Préparer et cadrer l'exécution

Formaliser les prérequis : compte de lecture dédié, exports LDAP/DNS/PKI, snapshots, accès aux consoles. Sur les très grands annuaires, définir une stratégie d'échantillonnage priorisant la proximité du plan de contrôle plutôt que l'exhaustivité mécanique. Mettre en place un workflow de tri des faux positifs et un registre d'acceptation du risque (critères de durée, revue périodique). Vérifier les versions d'outils et leur compatibilité avec le niveau fonctionnel (certains collecteurs BloodHound se comportent différemment sur de très vieux DFL).

0.10 Auditer les processus et la gouvernance

Évaluer le processus de jonction au domaine (qui, approbation, traçabilité), la gestion des changements AD, les revues d'accès et attestations (existence, formalisme, périodicité) et la matrice de responsabilités d'administration. Un annuaire techniquement propre mais sans gouvernance dérive inévitablement.

Partie 1 — Reconnaissance et cartographie

1.1 Cartographier la topologie forêt, domaines et approbations

Dénombrer forêts et domaines, relever les niveaux fonctionnels, cartographier les approbations (type, sens, transitivité). Repérer les domaines legacy ou de test rattachés à la forêt, souvent oubliés.

```
Get-ADForest | Select-Object Name,ForestMode,Domains,GlobalCatalogs,SchemaMaster
Get-ADDomain | Select-Object DNSRoot,DomainMode,PDCEmulator,RIDMaster,InfrastructureMaster
Get-ADTrust -Filter * | Select-Object Name,Direction,TrustType,IntraForest,ForestTransitive
nltest /domain_trusts /all_trusts /v
```

1.2 Inventorier contrôleurs de domaine, sites et FSMO

Lister les DC (OS, patch, physiques ou virtuels), les RODC et leur périmètre de réplication, la topologie de sites, les DC exposés en site distant ou en DMZ, la localisation et la redondance des rôles FSMO. Traiter la sécurité du catalogue global (ports 3268/3269) : il réplique des attributs partiels de *tous* les objets de la forêt et se trouve souvent moins durci qu'un DC standard.

```
Get-ADDomainController -Filter * |
  Select-Object
HostName,Site,IsGlobalCatalog,IsReadOnly,OperatingSystem,OperatingSystemVersion
netdom query fsmo
Get-ADDomainController -Filter {IsReadOnly -eq $true} | Select-Object HostName,Site
```

1.3 Cartographier les OU et l'arborescence LDAP

Confronter la structure des OU au modèle de délégation. Repérer les objets rangés dans les conteneurs par défaut (`Users`, `Computers`) et les OU « poubelle ». Auditer les conteneurs système sensibles — `Configuration`, `Sites`, `Services`, `LostAndFound`, `Infrastructure`, `NTDS Quotas`, `Program Data` — qui hébergent des objets critiques ou orphelins aux ACL parfois dangereuses.

```
Get-ADObject -SearchBase (Get-ADDomain).UsersContainer -Filter {ObjectClass -eq 'user'} |
  Measure-Object   # comptes restés dans CN=Users
Get-ADObject -LDAPFilter '(objectClass=*)' `
  -SearchBase ("CN=LostAndFound,"+(Get-ADDomain).DistinguishedName) -SearchScope OneLevel
```

1.4 Cartographier les groupes et l'imbrication

Distinguer groupes de sécurité et de distribution, analyser les portées, calculer l'appartenance effective au-delà des imbrications profondes. Repérer groupes circulaires, groupes vides et groupes à membre unique privilégié.

```
# Membres effectifs (récursifs) des groupes privilégiés
foreach ($g in 'Domain Admins','Enterprise Admins','Administrators') {
  Get-ADGroupMember -Identity $g -Recursive | Select-Object
@{n='Groupe';e={$g}},SamAccountName
}
```

1.5 Établir l'inventaire exhaustif des comptes

Recenser utilisateurs, machines, comptes de service et d'administration, comptes désactivés ou obsolètes, prestataires expirés, comptes système non nominatifs. S'appuyer sur les attributs révélateurs pour trier l'actif du résiduel.

```
Get-ADUser -Filter * -Properties
LastLogonTimestamp,PasswordLastSet,Enabled,userAccountControl |
  Select-Object SamAccountName,Enabled,
    @{n='DernierLogon';e={[datetime]::FromFileTime($_.LastLogonTimestamp)}},PasswordLastSet
```

1.6 Automatiser le recensement

Combiner SharpHound/BloodHound CE, ADRecon, ORADAD (outil souverain de l'ANSSI), PingCastle en collecte, PowerView, `dsquery`, `dsacls`, le module AD et DSInternals. Maîtriser volume, bruit et détectabilité ; réserver le scan actif de PingCastle au scoring (cf. 19.2).

```
SharpHound.exe -c All --zipfilename collecte_bh.zip
# ou depuis Linux :
bloodhound-python -d corp.local -u auditeur -p '***' -c All -ns 10.0.0.10
```

1.7 Cartographier les applications tierces dépendantes de l'AD

Recenser les binds LDAP applicatifs (secrets souvent en clair côté application), les serveurs RADIUS/NPS, les fédérations SSO/SAML/OIDC, et les dépendances silencieuses (imprimantes, NAS, hyperviseurs joints). Énumérer les Service Connection Points, qui révèlent les applications critiques et offrent une voie de persistance.

```
Get-ADObject -LDAPFilter '(objectClass=serviceConnectionPoint)' `
  -Properties serviceBindingInformation,keywords |
  Select-Object Name,serviceBindingInformation,keywords
```

1.8 Amorcer la surface d'exposition externe

Corréler nomenclature interne et empreinte externe (renvoi à la méthodologie EASM/OSINT, Partie 16). Vérifier la fuite éventuelle de certificats internes via les journaux de Certificate Transparency lorsqu'une AC est mal exposée.

1.9 Cartographier le plan de contrôle étendu

Dresser la liste complète des actifs du plan de contrôle — DC et groupes d'administration, PKI, hyperviseurs, sauvegarde, MECM/SCCM, EDR/RMM, PAM, Entra Connect, ADFS, comptes de déploiement, comptes DNS/DHCP privilégiés, dépôts de scripts, pipelines d'image et de configuration. Identifier les dépendances inter-forêts partageant un même composant (un seul

hyperviseur, une seule sauvegarde ou PAM pour plusieurs forêts). Retenir le principe directeur : **un chemin vers l'administrateur de la sauvegarde ou du cluster de virtualisation peut être plus dangereux qu'un chemin direct vers Domain Admin.**

Partie 2 — Architecture, forêt et modèle de confiance

2.1 Statuer sur la frontière de sécurité et le modèle d'administration

Traiter la forêt comme frontière native (conduire la remédiation à son échelle et en parallèle) mais raisonner la frontière réelle comme le plan de contrôle étendu (cf. 1.9). Confronter le tiering ANSSI (Tier 0/1/2, segmentation opérationnelle) et l'**Enterprise Access Model** de Microsoft (plans de contrôle et de gestion). Lire ESAE/Red Forest comme une architecture historique ou transitionnelle, non comme cible universelle par défaut.

2.2 Auditer les relations d'approbation

Énumérer chaque trust ; relever type, direction, transitivité et état du filtrage SID. Vérifier que le SID Filtering (quarantaine) est actif sur les trusts externes et de forêt et que l'authentification sélective est appliquée là où elle est requise. Retenir que le SID Filtering bloque l'injection de SID History mais **non** l'abus de délégation cross-forest ni le pillage de ressources (Exchange l'a historiquement démontré). Auditer la santé et la rotation *automatique* des secrets de trust (cycle Microsoft d'environ 30 jours), la validité du canal sécurisé et la cohérence des TDO des deux côtés ; ne pas déduire l'âge du secret de `whenChanged`, qui reflète la dernière modification de l'objet TDO, pas le renouvellement de la clé. Rechercher tout mécanisme ayant désactivé ou cassé la rotation. Après compromission, effectuer une rotation explicite du secret de trust selon le scénario de Forest Recovery ; un trust compromis ouvre une compromission bidirectionnelle.

```
Get-ADTrust -Filter * |
  Select-Object Name,Direction,TrustType,SIDFilteringForestAware,
    SIDFilteringQuarantined,SelectiveAuthentication
Get-ADObject -LDAPFilter '(objectClass=trustedDomain)' -Properties whenChanged |
  Select-Object Name,whenChanged   # NB : dernière modif du TDO, PAS l'âge du secret de
trust
Get-ADTrust -Filter * | Select Name,Direction,TrustType   # santé ; secret renouvelé ~tous
les 30 j
```

2.3 Contrôler la délégation d'administration native

Confronter les ACL déléguées sur les OU au modèle cible. Traquer la dérive dans le temps (ACE ajoutées au fil de l'eau, jamais revues) et les délégations « fantômes » sur des OU vides ou obsolètes.

```
dsacls "OU=Utilisateurs,DC=corp,DC=local"
# Cartographie fine des ACE : PowerView Get-DomainObjectAcl -ResolveGUIDs
```

2.4 Vérifier l'intégrité du schéma

Recenser les extensions de schéma (Exchange, Entra Connect, produits tiers) et les attributs sensibles ajoutés. Relever l'historique des modifications. Contrôler les attributs confidentiels (bit confidentiel dans `searchFlags`) et vérifier lesquels *devraient* l'être (LAPS, secrets). Établir une baseline (empreinte) du schéma pour détecter l'ajout ultérieur de classes ou d'attributs non standards, susceptibles de servir de persistance.

```
Get-ADObject -SearchBase (Get-ADRootDSE).schemaNamingContext `
  -Filter {objectClass -eq 'attributeSchema'} -Properties searchFlags,whenChanged |
  Where-Object { $_.searchFlags -band 128 } |   # bit confidentiel
  Select-Object Name,whenChanged
```

2.5 Auditer les objets sensibles et SDProp

Examiner AdminSDHolder et l'attribut `adminCount`, identifier les résidus après retrait de privilège, et appliquer une procédure de nettoyage des comptes marqués `adminCount=1` sans privilège effectif. Vérifier la fréquence de SDProp et l'ACL propagée. Considérer le détournement d'AdminSDHolder comme mécanisme de persistance à rechercher.

```
Get-ADUser -LDAPFilter '(adminCount=1)' -Properties adminCount,memberOf |
  Select-Object SamAccountName,memberOf   # recouper avec l'appartenance réelle aux groupes
T0
```

2.6 Éprouver le tiering en pratique

Vérifier l'existence formelle d'un Tier 0, son périmètre réel (presque toujours sous-estimé) et son étanchéité effective (restrictions d'ouverture de session, isolation, séparation des identités). Traquer le **Shadow Tier 0** : les administrateurs Exchange, SCCM, VMware ou de la sauvegarde sont *de facto* Tier 0. Contrôler la cohérence OU ↔ GPO ↔ tiering ↔ pare-feu et le rattachement des hyperviseurs des DC au Tier 0.

2.7 Passer en revue les groupes et comptes à privilèges intrinsèques

Examiner Domain/Enterprise/Schema Admins, Administrators, les Operators, DNSAdmins, Group Policy Creator Owners, Cert Publishers, DHCP Administrators. Auditer le groupe Pre-Windows 2000 Compatible Access, en retenant qu'il n'accorde pas systématiquement une lecture anonyme — le résultat dépend de ses membres et des ACL. Vérifier l'état des comptes intégrés (Administrator, `krbtgt`, `Guest`).

2.8 Traiter SID History et le quota de comptes machine

Détecter le SID History résiduel et en évaluer la légitimité. **Ramener `ms-DS-MachineAccountQuota` à 0** : à 10 par défaut, il autorise tout utilisateur à créer dix comptes machine, porte d'entrée du RBCD, des Shadow Credentials et de la jonction abusive. La création de comptes machine doit devenir une délégation explicite (cf. 3.13).

```
# Lecture
Get-ADObject (Get-ADDomain).DistinguishedName -Properties ms-DS-MachineAccountQuota |
  Select-Object -ExpandProperty ms-DS-MachineAccountQuota
# ⚠ Modification (remédiation)
Set-ADDomain -Identity (Get-ADDomain) -Replace @{'ms-DS-MachineAccountQuota'=0}
# Comptes portant un SID History
Get-ADObject -LDAPFilter '(sIDHistory=*)' -Properties sIDHistory |
  Select-Object Name,sIDHistory
```

Partie 3 — Identités, comptes et authentification

3.1 Auditer la politique de mots de passe

Lire la politique par défaut du domaine et les Fine-Grained Password Policies. Vérifier l'alignement sur le NIST SP 800-63B (passphrases, bannissement des mots de passe compromis) et l'existence de filtres (Entra Password Protection). Renvoyer à la Partie 4 pour l'écart entre politique déclarée et robustesse réelle.

```
Get-ADDefaultDomainPasswordPolicy |
  Select-Object MinPasswordLength,PasswordHistoryCount,ComplexityEnabled,
    LockoutThreshold,MaxPasswordAge
Get-ADFineGrainedPasswordPolicy -Filter * | Select-Object
Name,Precedence,MinPasswordLength,AppliesTo
```

3.2 Évaluer le verrouillage et la résistance au spraying

Relever seuil, fenêtre d'observation et durée de verrouillage au niveau du domaine et des PSO. Surveiller les sprays distribués via les événements 4625 et 4740. Retenir que le « Smart Lockout » relève d'Entra ID et se traite séparément de l'AD local. Conduire, si autorisé, un test à faible volume hors production critique.

3.3 Contrôler le cycle de vie des comptes à privilèges

Vérifier provisioning et déprovisioning, revues d'accès, séparation des rôles entre compte nominatif quotidien et compte d'administration dédié, proscription des comptes partagés et traçabilité.

3.4 Auditer postes d'administration et PAM

Vérifier l'existence, le durcissement et l'isolation des PAW ; la présence de bastions et d'un PAM (coffre, rotation, enregistrement) ; la gestion des comptes break-glass (stockage hors-ligne, alerte à l'usage, exclusion des automatismes).

3.5 Contrôler Protected Users, Authentication Policies et Silos

Vérifier le périmètre de Protected Users (suppression de NTLM et de la délégation, TGT court), le cantonnement des comptes de Tier 0 par silos et politiques d'authentification, et les effets de bord sur les services et systèmes legacy.

```
Get-ADGroupMember 'Protected Users' | Select-Object SamAccountName
Get-ADAuthenticationPolicySilo -Filter * | Select-Object Name,Enforce,ProtectedAccounts
```

3.6 Vérifier les protections mémoire et LSASS

Contrôler Credential Guard (VBS), LSA Protection (RunAsPPL), Restricted Admin et Remote Credential Guard pour RDP, et les règles ASR anti-dump LSASS. Pour les DC virtuels, vérifier la compatibilité de Credential Guard avec la virtualisation imbriquée.

```
# RunAsPPL
Get-ItemProperty 'HKLM:\SYSTEM\CurrentControlSet\Control\Lsa' -Name RunAsPPL -EA
SilentlyContinue
# État Credential Guard
Get-CimInstance -ClassName Win32_DeviceGuard -Namespace root\Microsoft\Windows\DeviceGuard
|
  Select-Object SecurityServicesRunning
```

3.7 Auditer LAPS

Vérifier la couverture de **Legacy Microsoft LAPS** et de **Windows LAPS** (terminologie Microsoft ; éviter « LAPS v2 ») sur postes et serveurs, la rotation et le chiffrement (y compris l'historique `msLAPS-EncryptedPasswordHistory`), le principal autorisé à déchiffrer, la séparation entre lecture, déchiffrement et administration du schéma, l'audit des lectures, les post-authentication actions et la compatibilité avec les images et clones. Ne pas oublier la sauvegarde et la rotation du mot de passe DSRM. Rechercher les délégations de lecture excessives.

```
# Postes sans mot de passe LAPS (couverture)
Get-ADComputer -Filter * -Properties ms-Mcs-AdmPwdExpirationTime,msLAPS-
PasswordExpirationTime |
  Where-Object { -not $_.'ms-Mcs-AdmPwdExpirationTime' -and -not $_.'msLAPS-
PasswordExpirationTime' }
# Qui peut lire le mot de passe LAPS ? (Windows LAPS)
Find-LapsADExtendedRights -Identity 'OU=Serveurs,DC=corp,DC=local'
```

3.8 Auditer les comptes de service

Vérifier la couverture des gMSA/sMSA, la rotation et l'ACL de récupération. **Auditer l'infrastructure KDS** : inventorier les clés racine (`Get-KdsRootKey`), vérifier leur date effective et leur réplication, et **rechercher la présence anormale de plusieurs clés** — cause documentée d'échecs d'authentification gMSA en 2026. **Ne pas** faire tourner périodiquement la clé racine KDS : elle se crée normalement une seule fois par forêt (`Add-KdsRootKey`). Détecter l'extraction hors-ligne (GoldenGMSA). Pour les dMSA (Windows Server 2025), contrôler le niveau de patch post-CVE-2025-53779 et la surface résiduelle (cf. 6.5). Repérer les comptes de service dotés d'un SPN (exposition Kerberoasting) et les secrets de service en clair (scripts, GPP, partages, attributs). Rechercher deux angles morts fréquents : l'abus du droit `ReadGMSAPassword` (lecture de `msDS-ManagedPassword`), chemin direct vers le Tier 0 si le gMSA est privilégié, et les comptes machine pré-créés pour le déploiement (WDS/SCCM), souvent en mot de passe faible ou `PASSWD_NOTREQD`.

```
# Comptes Kerberoastables (SPN + type de chiffrement)
Get-ADUser -LDAPFilter '(servicePrincipalName=*)' `
  -Properties servicePrincipalName,msDS-SupportedEncryptionTypes,PasswordLastSet |
  Select-Object SamAccountName,PasswordLastSet,msDS-SupportedEncryptionTypes
# gMSA et leur ACL de récupération
Get-ADServiceAccount -Filter * -Properties PrincipalsAllowedToRetrieveManagedPassword |
  Select-Object Name,PrincipalsAllowedToRetrieveManagedPassword
```

3.9 Vérifier l'hygiène du référentiel

Recenser comptes dormants, doublons, comptes de test oubliés, indicateurs `PASSWD_NOTREQD`, `DONT_EXPIRE_PASSWORD`, `PASSWD_CANT_CHANGE`, secrets stockés dans les attributs (`description`, `info`, `userPassword`, `unixUserPassword`) et délégations activées sans besoin métier. Pour la fuite passive via LDAP, collecter systématiquement les attributs libres et les corréler à des expressions régulières recherchant mots de passe, clés d'API, jetons JWT et adresses de messagerie.

```
Get-ADUser -Filter * -Properties Description,Info |
  Where-Object { $_.Description -match 'pw|pass|mdp|motdepasse|secret|token' -or $_.Info }
|
  Select-Object SamAccountName,Description,Info
Get-ADUser -Filter {userAccountControl -band 0x0020} |   # PASSWD_NOTREQD
  Select-Object SamAccountName
```

3.10 Auditer MFA, passwordless et intégration hybride

Cartographier les points d'intégration de la MFA (VPN, RDS Gateway, Entra, ADFS), identifier les flux qui y échappent (authentification legacy, comptes de service), évaluer la résistance au phishing (FIDO2/WHfB) face aux facteurs faibles. Pour Windows Hello for Business, distinguer key trust, cert trust et cloud trust et analyser les abus de key credential et l'attestation. Couvrir les déploiements de passkeys et de FIDO2 en entreprise (attestation, récupération, surface en cas de mauvaise configuration).

3.11 Évaluer la gouvernance des identités

Vérifier le processus JML (Joiner-Mover-Leaver) et son automatisation, la recertification périodique des accès et la séparation des tâches (détection des cumuls toxiques).

3.12 Auditer les accès des tiers, infogérance et MSP

Recenser les comptes d'administration externes, les tunnels ou accès permanents, le break-glass partagé et le cloisonnement des prestataires. Traiter explicitement la chaîne d'approvisionnement comme vecteur ransomware : sur 2024-2026, la compromission d'un accès MSP est l'un des points d'entrée les plus fréquents vers l'AD.

3.13 Gouverner la jonction au domaine et le cycle de vie des comptes ordinateur

Au-delà du quota, examiner le privilège `SeMachineAccountPrivilege`, les délégations de création d'objets ordinateur et le propriétaire initial des objets créés, la réutilisation d'un compte ordinateur existant, les blobs d'Offline Domain Join, le durcissement NetJoin, les comptes de jonction surprivilégiés, la précréation et le nettoyage des objets après réinstallation.

Partie 4 — Audit des mots de passe et des secrets d'authentification

L'audit des mots de passe traduit un risque abstrait en chiffres concrets pour la direction, mais manipule des secrets : il obéit à un cadre strict.

4.1 Encadrer et sécuriser l'extraction des empreintes

Obtenir une autorisation écrite spécifique (les empreintes sont des secrets, cf. custody Partie 0). Extraire de façon contrôlée — `ntdsutil` en Install From Media, snapshot VSS d'un DC, ou DCSync autorisé — et toujours dans un environnement cloisonné et déconnecté. Ne jamais manipuler les empreintes en clair hors de l'enclave, chiffrer les extractions, prouver leur effacement, tracer chaque opération.

```
# Extraction hors-ligne (enclave isolée, autorisation requise)
# 1) IFM sur un DC : ntdsutil "ac in ntds" "ifm" "create full C:\ifm" q q
# 2) Analyse avec DSInternals (réplication autorisée) :
$hashes = Get-ADReplAccount -All -Server dc01.corp.local
```

4.2 Détecter les mots de passe compromis / ayant fuité (HIBP)

Utiliser la liste hors-ligne « Pwned Passwords » de Have I Been Pwned (formats NTLM et SHA-1). Comparer **en local** les empreintes NT du domaine à ce corpus, sans qu'aucune empreinte ne quitte l'environnement. Réserver le modèle *k-anonymity* de l'API HIBP (préfixe de cinq caractères) au filtre de prévention, non à l'audit rétrospectif. Enrichir éventuellement avec des corpus sectoriels sous gouvernance de provenance. Refermer la boucle par la prévention continue (filtres LSA de bannissement, Entra Password Protection).

```
# Télécharger la liste NTLM triée par hash (haveibeenpwned.com / outil haveibeenpwned-
downloader)
$hashes | Test-PasswordQuality `
  -WeakPasswordHashesSortedFile .\pwned-passwords-ntlm-ordered-by-hash.txt |
  Select-Object -ExpandProperty WeakPassword   # comptes dont le mot de passe a fuité
```

4.3 Détecter la réutilisation et le partage de mots de passe

Appliquer le principe : **deux comptes dont l'empreinte NT est identique partagent le même mot de passe.** Regrouper les comptes par empreinte identique et analyser la taille des clusters. Signaler en priorité les cas où un compte utilisateur partage le mot de passe d'un compte privilégié, de service ou d'administration, et la réutilisation entre compte quotidien et compte d'administration d'un même individu (rupture de la séparation des rôles, cf. 3.3). Traiter les mots de passe de « master image » partagés en masse (postes clonés, comptes locaux — ce que LAPS résout, cf. 3.7) et les réutilisations silencieuses entre comptes machine et de service.

```
$q = $hashes | Test-PasswordQuality
$q.DuplicatePasswordGroups   # groupes de comptes partageant le même mot de passe
# Repérer les clusters incluant un compte privilégié :
$priv = (Get-ADGroupMember 'Domain Admins' -Recursive).SamAccountName
$q.DuplicatePasswordGroups | Where-Object { $_ | Where-Object { $priv -contains $_ } }
```

4.4 Mesurer la robustesse réelle et la politique effective

Recenser mots de passe vides ou faibles, comptes `PASSWD_NOTREQD`, présence de LM hash, chiffrement réversible. Mesurer, en enclave isolée, la robustesse des empreintes de service Kerberoastables et des comptes sensibles par un cassage encadré (hashcat) — **mesure de robustesse, jamais exfiltration** — restituée en métriques (taux cassé, temps, longueur effective). Relever l'âge des mots de passe (`pwdLastSet`), notamment `krbtgt` et trusts, et les comptes qui n'expirent jamais.

```
$q.LMHash                   # comptes avec empreinte LM
$q.ClearTextPassword        # chiffrement réversible activé
$q.PasswordNotRequired      # PASSWD_NOTREQD
Get-ADUser krbtgt -Properties PasswordLastSet | Select-Object PasswordLastSet
# Cassage encadré (enclave) : hashcat -m 1000 ntlm.hashes wordlist.txt -r rules/best64.rule
```

4.5 Restituer et remédier

Exprimer le livrable de direction en indicateurs — taux de mots de passe compromis, taux de réutilisation, comptes privilégiés concernés — **sans jamais divulguer de mot de passe en clair.** Prioriser les réinitialisations (comptes privilégiés, comptes partageant un secret avec le Tier 0), le bannissement continu par filtres, l'adoption de passphrases et la trajectoire passwordless (cf. 3.10). Refermer la custody : destruction sécurisée des extractions, des empreintes et des résultats de cassage, avec preuve d'effacement.

Fin du bloc 1 (réécrit — style prescriptif + commandes). À suivre : Partie 5 (Kerberos), Partie 6 (délégations et chemins d'attaque), Partie 7 (AD CS — dont audit PKI, NTAuth, ESC1-16, Certighost).

Partie 5 — Kerberos : protocole et surface d'abus

5.1 Cadrer le fonctionnement et la surface

Cartographier les échanges (AS-REQ/AS-REP, TGT, TGS, PAC) et l'état de déploiement de FAST/armoring. Retenir que FAST protège la préauthentification et permet l'armoring, mais **n'offre pas de protection autonome** contre le password spraying ou le Kerberoasting. Vérifier la source de temps (NTP) : Kerberos dépend de la synchronisation, dont la source doit être maîtrisée et sécurisée.

5.2 Auditer le Kerberoasting et les SPN

Énumérer les comptes porteurs de SPN, relever leur type de chiffrement et l'âge de leur mot de passe, et confier la robustesse au cassage encadré de la Partie 4. Rechercher les SPN dupliqués (confusion Kerberos, rétrogradation possible) et les SPN portés par des comptes privilégiés.

```
Get-ADUser -LDAPFilter '(servicePrincipalName=*)' `
  -Properties servicePrincipalName,msDS-SupportedEncryptionTypes,PasswordLastSet,memberOf
setspn -F -X   # SPN dupliqués au niveau FORÊT (le -F est indispensable ; sans lui,
périmètre domaine)
# Validation offensive (périmètre autorisé) : Rubeus.exe kerberoast /tgtdeleg /nowrap
```

5.3 Détecter l'AS-REP Roasting

Lister les comptes sans préauthentification Kerberos et remonter l'origine de chaque exception.

```
Get-ADUser -LDAPFilter '(userAccountControl:1.2.840.113556.1.4.803:=4194304)' `
  -Properties userAccountControl | Select-Object SamAccountName   # DONT_REQ_PREAUTH
```

5.4 Auditer Golden / Diamond / Sapphire Ticket

Relever l'âge du compte `krbtgt` et planifier sa **double rotation** — opération contrôlée, pertinente surtout après compromission ou suspicion, **pas** un geste routinier. Espacer les deux réinitialisations d'un délai **supérieur à la durée de vie maximale effective des tickets** (10 h par défaut, mais adapter si la stratégie a été modifiée) et **valider la réplication AD entre les deux**. Connaître Diamond/Sapphire, qui contournent les détections « golden » classiques. Détecter les anomalies comportementales du PAC (RID « ronds » 512/513/519 sans imbrication réelle) et corréler aux événements 4768/4769.

```
Get-ADUser krbtgt -Properties PasswordLastSet,msDS-KeyVersionNumber |
  Select-Object PasswordLastSet,msDS-KeyVersionNumber
# ⚠ Remédiation : rotation krbtgt (script officiel Microsoft New-KrbtgtKeys.ps1, x2)
```

5.5 Auditer le Silver Ticket

Comprendre que le Silver Ticket forge un TGS sans passer par le KDC, en s'appuyant sur la clé du compte de service — d'où l'importance des gMSA et de la rotation des secrets de service (cf. 3.8).

5.6 Auditer les délégations Kerberos

Recenser les délégations non contraintes (à proscrire hors DC), contraintes (S4U2Self/S4U2Proxy, avec audit de `msDS-AllowedToDelegateTo` — repérer les SPN sensibles et les jokers) et basées sur les ressources (RBCD). Rechercher le chaînage délégation + coercition + MAQ, et le contournement Bronze Bit (CVE-2020-17049).

```
Get-ADComputer -Filter {TrustedForDelegation -eq $true} -Properties TrustedForDelegation
# non contrainte
Get-ADObject -LDAPFilter '(msDS-AllowedToActOnBehalfOfOtherIdentity=*)' `
  -Properties msDS-AllowedToActOnBehalfOfOtherIdentity   # RBCD
Get-ADObject -LDAPFilter '(msDS-AllowedToDelegateTo=*)' -Properties msDS-
AllowedToDelegateTo
```

5.7 Auditer la coercition et le relais

Tester (en périmètre autorisé) les primitives de coercition — PetitPotam, PrinterBug, ShadowCoerce, DFSCoerce — et les vecteurs de relais (LDAP/SMB/HTTP, KrbRelay). Intégrer les primitives NTLM récentes (CVE-2025-24054, CVE-2026-33829). Retenir que la chaîne **Coercition → Relais NTLM → AD CS (ESC8) → Domain Admin** reste le vecteur n°1 d'obtention de Domain Admin en boîte grise, MS-RPRN n'étant pas patché par défaut et la signature LDAP/EPA rarement en enforcement. Contre-mesures : EPA, signature LDAP/SMB, filtres RPC, Spouleur désactivé sur les DC (cf. Parties 9 et 10).

5.8 Auditer le chiffrement, les etypes et les exceptions

Relever les etypes autorisés par compte (`msDS-SupportedEncryptionTypes`). Constater que le durcissement 2026 traite en AES les comptes sans configuration explicite, **sans supprimer RC4** : rechercher les comptes, trusts et applications explicitement limités à RC4 ou DES, vérifier les comptes `Account is sensitive and cannot be delegated`, les keytabs obsolètes et la validation du PAC côté service. Prouver que la bascule AES a été testée.

```
Get-ADObject -LDAPFilter '(msDS-SupportedEncryptionTypes=*)' `
  -Properties msDS-SupportedEncryptionTypes,sAMAccountName |
  Where-Object { $_.'msDS-SupportedEncryptionTypes' -band 0x4 }   # RC4 explicite
```

5.9 Contrôler le cycle de vie des tickets

Vérifier les durées TGT/TGS et MaxTicketAge, et rechercher les anomalies temporelles (durée forgée, incohérences de PAC).

Partie 6 — Délégations, ACL/ACE et chemins d'attaque

6.1 Cartographier les droits délégués

Relever les droits sur OU, groupes, comptes sensibles et conteneurs système, ainsi que les propriétaires (`Owner`) atypiques et les ACE explicites face à l'héritage.

```
dsacls "DC=corp,DC=local"
# PowerView : Get-DomainObjectAcl -Identity "Domain Admins" -ResolveGUIDs
```

6.2 Identifier les ACE à risque

Rechercher GenericAll, GenericWrite, WriteDACL, WriteOwner, WriteProperty, ForceChangePassword, Self-Membership, AddMember, et les droits étendus (`User-Force-Change-Password` , `DS-Replication-Get-Changes*`). Prioriser par proximité au plan de contrôle.

6.3 Analyser les chemins d'attaque vers Tier 0

Exploiter BloodHound (chemins les plus courts, requêtes Cypher), Adalanche et AD Miner. Identifier les choke points — les nœuds à fort degré qui, une fois traités, coupent plusieurs chemins.

```
// Cypher — chemins vers les Domain Admins
MATCH p=shortestPath((n)-[*1..]->(g:Group {name:'DOMAIN ADMINS@CORP.LOCAL'}))
WHERE n<>g RETURN p LIMIT 25
// Choke points
MATCH (n) WHERE n.highvalue=false
MATCH p=shortestPath((n)-[*1..]->(m {highvalue:true})) RETURN n, count(p) ORDER BY count(p)
DESC
```

6.4 Auditer les Shadow Credentials

Rechercher l'abus de `msDS-KeyCredentialLink` (Key Trust) et les clés illégitimes ; nettoyer.

```
Get-ADObject -LDAPFilter '(msDS-KeyCredentialLink=*)' -Properties msDS-KeyCredentialLink |
  Select-Object Name
# Whisker.exe list /target:<compte>   (validation encadrée)
```

6.5 Auditer l'abus des dMSA — BadSuccessor (post-patch)

Vérifier en priorité le niveau de patch des DC 2025 (build ≥ 26100.4946, CVE-2025-53779) et les droits CreateChild sur les OU. Auditer la surface résiduelle (vol de credentials, mouvement latéral). Détecter via SACL sur la création de dMSA, les modifications de `msDS-DelegatedMSAState` et l'émission de TGT vers des dMSA. Poser en défense en profondeur un deny ACE de création de dMSA à grande échelle.

6.6 Auditer DCSync

Rechercher les principals disposant hors DC des droits `DS-Replication-Get-Changes`, `-All` et `-In-Filtered-Set` (comptes de connecteurs, tiers, `MSOL_*`). Détecter via l'événement 4662 depuis une source non-DC.

```
# PowerView : Get-ObjectAcl "DC=corp,DC=local" -ResolveGUIDs |
#   ? { $_.ObjectAceType -match 'Replication-Get-Changes' } | Select SecurityIdentifier
```

6.7 Auditer DCShadow

Comprendre les conditions (enregistrement d'un faux DC) et détecter les modifications de `nTDSDSA` et les réplications anormales.

6.8 Auditer le RBCD sur objets machine

Rechercher les écritures de `msDS-AllowedToActOnBehalfOfOtherIdentity`, le chaînage MAQ + coercition, et nettoyer.

6.9 Auditer les ACL sur GPO

Relever les droits d'édition/liaison des GPO liées au Tier 0, le détournement possible d'une GPO pour exécution de code, et les Group Policy Creator Owners.

6.10 Structurer la méthodologie d'analyse des chemins

Croiser l'approche target-centric (partir du plan de contrôle, remonter aux sources de privilège) et source-centric (partir des principals à droits, voir où ils mènent). Identifier et prioriser les choke points. Élargir la cible BloodHound au plan de contrôle (« obtenir la capacité de modifier/restaurer/signer/surveiller/exécuter »), pas seulement « atteindre Domain Admin ».

6.11 Auditer les ACE sur les conteneurs système

Rechercher les ACL par défaut modifiées sur `System`, `Users`, `Computers`. Un `GenericAll`/`CreateChild` sur `CN=Users` fournit une **primitive de création/modification d'objets** susceptible d'entrer dans un chemin d'élévation — analyser les droits effectifs par classe d'objet (créer un utilisateur ne confère pas en soi un privilège).

Partie 7 — Active Directory Certificate Services (PKI)

7.1 Cartographier la PKI

Recenser AC racine hors-ligne et AC émettrices, hiérarchie, exposition, et les rôles additionnels (CES, CEP, NDES/SCEP + connecteurs Intune, web enrollment). Renvoyer à l'article d'exploitation AD CS du site pour le détail offensif.

```
certutil -config - -ping
certutil -CAInfo
Get-CertificationAuthority   # module PSPKI
```

7.2 Auditer les modèles et droits d'inscription

Relever les droits d'enrôlement et d'auto-enrôlement, l'indicateur `Enrollee Supplies Subject`, les EKU d'authentification (Client Auth, Smart Card, PKINIT, Any Purpose), l'approbation de gestionnaire, `mspki-enrollment-flag`, la supersedence et les versions de gabarits.

7.3 Dérouler la taxonomie des failles AD CS (par type)

Défauts de gabarit — ESC1, ESC2, ESC3, ESC9, ESC10, ESC13, ESC14, **ESC15/EKUwu (CVE-2024-49019)** ; traiter en priorité **ESC4** (un `WriteDacl` / `WriteOwner` sur un gabarit permet de le transformer en ESC1). **Défauts d'AC** — ESC6, ESC7 (ManageCA/ManageCertificates), ESC12, **ESC16** (extension de sécurité SID désactivée globalement). **Défauts d'endpoint** — ESC8 (web enrollment + relais NTLM, la kill chain la plus efficace), ESC11 (RPC). **Défauts d'objets PKI** — ESC5, et surtout le conteneur **`NTAuthCertificates`** : une écriture y déclare une AC rogue comme autorité de confiance pour l'authentification AD. **ESC17** (Enrollee-Supplied Subject for Server Authentication, Troopers 2026, hors set d'origine) : usurpation d'un service TLS ; le WSUS HTTPS n'est qu'un cas d'exploitation. **Vulnérabilités logicielles distinctes** — **Certighost / CVE-2026-54121** (CVSS 8.8, faille du « chase » d'enrôlement, patch 14/07/2026, PoC 24/07/2026) : à traiter comme CVE, pas comme ESC.

```
# Énumération complète des ESC (lecture)
certipy find -u auditeur@corp.local -p '***' -dc-ip 10.0.0.10 -stdout -vulnerable
# Audit PKI global
Invoke-PKIAudit -CA 'ca01.corp.local\CORP-CA01'   # PSPKIAudit
# Inspecter le magasin NTAuth
certutil -viewstore -enterprise NTAuth
```

7.4 Protéger les clés privées de CA

Vérifier la présence d'un HSM (niveau FIPS), les permissions sur le magasin de clés, la sauvegarde/restauration et la séparation des rôles (CA Officer / Auditor / Backup) ainsi que les cérémonies de clés. Prévenir le « Golden Certificate » (vol de la clé de l'AC).

7.5 Auditer l'authentification par certificat et le mapping fort

Depuis les mises à jour du 9 septembre 2025, le retour au mode Compatibility via `StrongCertificateBindingEnforcement` n'est plus supporté : cette clé de registre est désormais un **artefact historique / de dérive de configuration**, pas l'état de sécurité réel. Vérifier l'**application effective du strong mapping** via les Event ID associés (Kerberos), la présence de l'extension SID de sécurité et les mappings explicites `altSecurityIdentities` (ex. X509IssuerSerialNumber). Rechercher les mappings faibles ou implicites résiduels. Correctif Certifried (KB5014754 / CVE-2022-26923) appliqué.

```
Get-ItemProperty 'HKLM:\SYSTEM\CurrentControlSet\Services\Kdc' -Name
StrongCertificateBindingEnforcement -EA SilentlyContinue
```

7.6 Contrôler le cycle de vie des certificats

Vérifier les durées de validité (et la sur-longévité), la révocation (AIA, CDP, CRL et delta CRL, OCSP : chevauchement et disponibilité), et rechercher les certificats à durée ou EKU anormaux, ceux de comptes désactivés et les certificats d'authentification expirés ou orphelins.

7.7 Auditer l'exploitation opérationnelle de la PKI

Vérifier la journalisation de l'AC et la sauvegarde base + configuration, les modules de stratégie et de sortie, les Key Recovery Agents et l'archivage de clés, les restrictions des Enrollment Agents, l'exportabilité des clés privées, les ACL des objets PKI dans la partition Configuration, NDES/SCEP + Intune, CES/CEP + EPA, les interfaces RPC/DCOM, l'auto-enrollment, la révocation d'urgence, le scénario de compromission de la racine hors-ligne et la séparation réelle des rôles.

7.8 Auditer les certificats utilisateurs et EFS

Contrôler le smart card logon (vecteur d'authentification moins surveillé) et S/MIME, et surtout les agents de récupération EFS (un Data Recovery Agent rogue = persistance et déchiffrement). Vérifier durée de vie, EKU, révocation et mapping des certificats utilisateurs.

Partie 8 — GPO et durcissement des postes/serveurs

8.1 Inventorier les GPO

Lister les GPO liées, orphelines, désactivées, en conflit ou non appliquées ; relever l'ordre d'application (LSDOU), les indicateurs `Enforced` / `Block Inheritance`, le loopback ; vérifier les résultats effectifs (RSoP) et comparer configuration déclarée et réellement appliquée.

```
Get-GPO -All | Select-Object DisplayName,GpoStatus,CreationTime,ModificationTime
Get-GPInheritance -Target (Get-ADDomain).DistinguishedName
gpresult /h rsop.html   # sur une cible représentative
```

8.2 Analyser les paramètres de sécurité

Passer les GPO à Group3r et PolicyAnalyzer (Security Compliance Toolkit), mesurer les écarts au socle CIS/ANSSI, et rechercher les scripts de démarrage/logon exposés dans SYSVOL.

8.3 Rechercher les résidus d'identifiants dans les GPP

Détecter les `cpassword` (clé AES publique), les autres secrets dans SYSVOL, les GPP à identifiants (tâches planifiées, mappages de lecteurs, services, sources de données), et vérifier les permissions SYSVOL/NETLOGON (une écriture illégitime = exécution de code massive).

```
Get-ChildItem \\corp.local\SYSVOL -Recurse -Include *.xml -EA SilentlyContinue |
  Select-String -Pattern 'cpassword'
# Restricted Groups / groupes locaux via GPP à contrôler également
```

8.4 Vérifier le durcissement socle/renforcé

Confronter au CIS Benchmarks (L1/L2) et à l'ANSSI, prioriser par efficacité observée (renvoi guide de durcissement), documenter les exceptions.

8.5 Contrôler l'exécution

Vérifier AppLocker/WDAC (couverture, mode audit vs enforce), la robustesse face aux contournements courants et l'alignement avec l'EDR.

8.6 Vérifier la segmentation Tier

Contrôler le pare-feu Windows piloté par GPO, les restrictions de logon croisées entre tiers (`Deny log on`) et la micro-segmentation des flux d'administration.

8.7 Vérifier les correctifs et CVE de référence

Contrôler Zerologon (CVE-2020-1472), noPac, PrintNightmare, sAMAccountName spoofing et les dérivés de coercition, la cadence de patch des DC et le traitement des DC non patchables.

8.8 Vérifier la redirection des conteneurs par défaut

Confirmer l'exécution de `redirusr` et `redircmp` (sinon les nouveaux objets héritent d'ACL laxistes des conteneurs par défaut).

8.9 Auditer le GPO Central Store et la chaîne d'approvisionnement administrative

Vérifier l'intégrité de l'ADMX Central Store, les droits sur `PolicyDefinitions`, la provenance et la signature des ADMX tiers, les écarts de version AD/SYSVOL d'une GPO, `gPLink` et les droits de liaison, les GPO liées au niveau site, les filtres WMI, le security filtering, et la sauvegarde/restauration/revue des changements de GPO.

8.10 Rechercher les GPO à paramètres contradictoires

Repérer deux GPO appliquées au même OU avec des paramètres de sécurité opposés (ex. signature SMB activée par l'une, désactivée par l'autre).

Partie 9 — Contrôleurs de domaine : réduction de surface et protocoles réseau

9.1 Réduire les services et rôles inutiles sur un DC

Vérifier qu'aucun rôle applicatif ni service superflu ne tourne sur un DC. **Désactiver le Spouleur d'impression** (vecteur PrinterBug/coercition), WebClient/WebDAV, les services d'impression, le navigateur, RDS. Repérer les rôles cohabitant à risque (IIS/AD CS web enrollment, DHCP sur DC). Comparer les services en écoute à une baseline « DC minimal ». Contrôler la légitimité des agents tiers (EDR, supervision, sauvegarde).

```
$dcs = (Get-ADDomainController -Filter *).HostName
# PowerShell 7 : -ComputerName a disparu de Get-Service -> utiliser Invoke-Command
Invoke-Command -ComputerName $dcs -ScriptBlock { Get-Service -Name Spooler,WebClient } |
  Select-Object PSComputerName,Name,Status
# ⚠ Remédiation : Stop-Service Spooler ; Set-Service Spooler -StartupType Disabled (via GPO
T0)
```

9.2 Réduire la surface locale et l'administration du DC

Vérifier l'absence de comptes locaux (hors DSRM), restreindre RDP/WinRM vers les DC (PAW-only, Restricted Admin), contrôler partages et tâches planifiées, réduire les ports/services exposés vers les postes utilisateurs.

9.3 Désactiver les protocoles de résolution de noms hérités

Désactiver LLMNR, NBT-NS et mDNS, désactiver WPAD (et poser l'entrée DNS `wpad` dans la Global Query Block List), et maîtriser l'IPv6 (mitm6, DHCPv6 rogue, RA guard). Tester au préalable avec Responder (périmètre autorisé) pour mesurer l'exposition à l'empoisonnement et au relais de hashes.

```
# LLMNR (GPO / registre)
Set-ItemProperty 'HKLM:\Software\Policies\Microsoft\Windows NT\DNSClient' -Name
EnableMulticast -Value 0
# mDNS
Set-ItemProperty 'HKLM:\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters' -Name
EnableMDNS -Value 0
# NBT-NS : par interface NetbiosOptions=2 (ou GPO "Configure NetBIOS settings" sur Win11
24H2 / WS2025)
Get-ChildItem 'HKLM:\SYSTEM\CurrentControlSet\Services\NetBT\Parameters\Interfaces' |
  ForEach-Object { Set-ItemProperty $_.PSPath -Name NetbiosOptions -Value 2 }
```

9.4 Auditer les protocoles de session, de partage et d'annuaire

Désactiver SMBv1, imposer la signature/chiffrement SMB, activer la signature LDAP et le channel binding. Suivre une méthode de migration LDAP : activer les événements de diagnostic, inventorier les binds simples et non signés, identifier application/hôte/propriétaire, classifier SASL/StartTLS/LDAPS, tester le channel binding, traiter les exceptions, passer en enforcement, prouver l'absence de régression. Contrôler les null sessions / anonymous bind

(`RestrictAnonymous`, `dsHeuristics`) et le filtrage RPC (MS-RPRN, MS-EFSR, MS-FSRVP, MS-DFSNM). Activer l'EPA sur les services exposés.

```
Get-SmbServerConfiguration | Select-Object
EnableSMB1Protocol,RequireSecuritySigning,EncryptData
Get-ItemProperty 'HKLM:\SYSTEM\CurrentControlSet\Services\NTDS\Parameters' -Name
'LDAPServerIntegrity' -EA SilentlyContinue
Get-ItemProperty 'HKLM:\SYSTEM\CurrentControlSet\Services\NTDS\Parameters' -Name
'LdapEnforceChannelBinding' -EA SilentlyContinue
```

9.5 Auditer l'administration à distance

Restreindre WinRM/PowerShell Remoting (périmètre, chiffrement des listeners) et déployer JEA. Poser le vrai contrôle applicatif — **WDAC/App Control (ou AppLocker)** — puis vérifier que PowerShell bascule bien en `ConstrainedLanguage` / `NoLanguage` pour le code non approuvé (le CLM est une *conséquence* de la politique de contrôle applicatif, pas un contrôle autonome). Restreindre CredSSP pour RDP.

9.6 Cartographier et valider le réseau

Scanner ports et services des DC et des actifs du plan de contrôle, détecter les services d'écoute non attendus (drift), renvoyer à la coercition/relais (5.7) et à la méthodologie DNS/EASM.

9.7 Évaluer la résilience au déni de service (DoS)

Éprouver la résistance au LDAP flooding (connexions max, timeouts) et à l'AS-REQ flooding, la saturation du catalogue global, et traiter le PDC Emulator comme **dépendance opérationnelle critique et point de concentration de fonctions** (temps, préférence pour les changements de mot de passe, verrouillage, Netlogon) — sa perte n'efface pas le domaine mais dégrade fortement ces fonctions. Auditer la résilience, pas seulement la sécurité.

Partie 10 — Audit cryptographique et protocoles de chiffrement

10.1 Auditer SChannel / TLS

Désactiver SSLv2/v3 et TLS 1.0/1.1 (n'autoriser que TLS 1.2/1.3), bannir les suites RC4, 3DES, DES, export et NULL, privilégier les courbes et l'échange de clés à confidentialité persistante (PFS), et vérifier les certificats des services internes (LDAPS, RDP/TLS, IIS).

```
# testssl.sh --full ldaps://dc01.corp.local:636   (analyse externe)
# IISCrypto (lecture) pour l'état SChannel
```

10.2 Auditer le chiffrement Kerberos

Relever les etypes par KDC et par compte, migrer RC4 vers AES tout en vérifiant l'état effectif du flag `msDS-SupportedEncryptionTypes` sur les comptes sensibles, contrôler le support des etypes AES-SHA2 (RFC 8009) et détecter les tickets RC4 (4768/4769) comme indicateur de dette.

10.3 Auditer NTLM et les empreintes

Supprimer le LM hash (`NoLMHash`), relever `LmCompatibilityLevel` et la répartition NTLMv1/NTLMv2, traiter les cryptographies dérivées de NTLMv1 (MS-CHAPv2), contrôler le cache d'identifiants (MSCache v2) et suivre les trois trajectoires NTLM comme contrôles distincts.

10.4 Auditer la signature et l'intégrité

Vérifier la signature/chiffrement SMB et la signature/channel binding LDAP (recoupe 9.4), la signature GPO/SYSVOL et l'intégrité des scripts, la signature de code (WDAC).

10.5 Auditer la cryptographie de la PKI (recoupe Partie 7)

Contrôler les tailles de clés (RSA ≥ 2048/3072, ECC P-256/384). Distinguer trois usages de SHA-1 : **SHA-1 en signature de certificat** (à éliminer), **HMAC-SHA1 dans les etypes AES historiques** (construction protocolaire, à ne pas confondre) et **AES-SHA2 RFC 8009** (récent, pas activé partout). Vérifier durées de validité, renouvellement et protection matérielle des clés d'AC (HSM).

10.6 Auditer DPAPI et les secrets de domaine

Protéger la DPAPI backup key du domaine, les secrets LSA, les comptes de service et les clés de confiance, et durcir l'extraction hors-ligne depuis `ntds.dit` et via VSS (cf. 12.3).

10.7 Auditer les clés et secrets systèmes sensibles

Contrôler la clé racine KDS (gMSA/dMSA, GoldenGMSA — renvoi 3.8), le chiffrement Windows LAPS, le mot de passe/clé DSRM, et BitLocker des volumes DC avec ses clés de récupération dans l'AD.

10.8 Auditer la conformité, la migration et la crypto-agilité (dont post-quantique)

Aligner sur l'ANSSI (RGS annexe B1, guides TLS), inventorier les algorithmes obsolètes et bâtir un plan de migration. Pour le **post-quantique** : inventorier les dépendances asymétriques RSA/ECC (PKI — AC, certificats, TLS/LDAPS — Kerberos PKINIT, signatures, VPN) ; suivre les standards (NIST FIPS 203/204/205 : ML-KEM, ML-DSA, SLH-DSA) et la position ANSSI, en privilégiant l'approche hybride (classique + PQC) durant la transition ; traiter la menace « harvest now, decrypt later » pour les données et secrets à longue durée de vie (priorité PKI, clés d'AC, sauvegardes chiffrées) ; instaurer la **crypto-agilité** (capacité à changer d'algorithme/taille sans refonte : gabarits de certificats, hiérarchie d'AC, TLS), l'inventaire cartographié étant le prérequis ; poser une feuille de route de migration dépendante de la disponibilité produit.

Partie 11 — DNS et DHCP intégrés à l'AD

11.1 Auditer les ACL des zones et les mises à jour dynamiques

Vérifier la sécurité des zones intégrées à l'AD et des mises à jour dynamiques (n'autoriser que les mises à jour sécurisées), et contrôler les droits d'écriture sur zones et enregistrements ainsi que l'ownership des enregistrements créés dynamiquement.

```
Get-DnsServerZone | Select-Object ZoneName,ZoneType,DynamicUpdate,IsDsIntegrated
```

11.2 Auditer DNSAdmins

Contrôler l'appartenance au groupe DNSAdmins et le risque d'exécution de code via `ServerLevelPluginDll`.

11.3 Auditer l'empoisonnement et les mises à jour non sécurisées

Rechercher les enregistrements wildcard, le détournement WPAD via DNS et l'ADIDNS spoofing (ajout d'enregistrements par des comptes non privilégiés).

11.4 Auditer la sécurité opérationnelle du DNS

Contrôler l'aging/scavenging et les enregistrements obsolètes ou dangling ; **restreindre les transferts de zone (AXFR non autorisés)** ; limiter la récursion et vérifier forwarders/conditional forwarders, root hints et délégations abandonnées ; contrôler la Global Query Block List et la résolution vers des domaines externes non maîtrisés ; activer la journalisation analytique DNS ; se tenir informé des CVE du service DNS (ex. CVE-2021-26877).

```
Get-DnsServerZoneAging -Name corp.local
Get-DnsServerZone | ForEach-Object { Get-DnsServerZoneTransferPolicy -ZoneName $_.ZoneName
-EA SilentlyContinue }
dnscmd /Info /EnableGlobalQueryBlockList
Get-DnsServerRecursion
Get-DnsServerForwarder
```

11.5 Évaluer le besoin et auditer DNSSEC lorsqu'il est déployé

Vérifier l'état de déploiement de DNSSEC et la gestion des clés (KSK/ZSK), signer les zones sensibles et contrôler l'intégrité des enregistrements. Renvoyer à la méthodologie DNS dédiée du site pour le détail. Surveiller l'exposition des enregistrements `_msdcs`, SRV (Kerberos/LDAP/GC) et de DC (fuite de topologie).

```
Get-DnsServerDnsSecZoneSetting -ZoneName corp.local
# ⚠ Signature : Invoke-DnsServerZoneSign -ZoneName corp.local -SignWithDefault
Get-DnsServerSigningKey -ZoneName corp.local
```

11.6 Auditer la sécurité DHCP

Vérifier l'autorisation des serveurs DHCP dans l'AD (repérer les serveurs rogue non autorisés), contrôler l'appartenance aux groupes DHCP Administrators/Users, les étendues et réservations,

éviter l'hébergement DHCP sur un DC, valider le failover et la disponibilité, activer la journalisation (baux, forensic). **Auditer spécifiquement le compte de mise à jour DNS dynamique utilisé par DHCP**, souvent surprivilégié, et activer Name Protection (anti-écrasement).

```
Get-DhcpServerInDC                      # serveurs autorisés
Get-DhcpServerv4DnsSetting              # comportement de MAJ DNS + Name Protection
netsh dhcp server show dnsconfig
# Compte de MAJ DNS (à vérifier / restreindre)
Get-DhcpServerDnsCredential
```

11.7 Auditer l'intégration DHCP ↔ DNS dynamique

Contrôler le compte de mise à jour DNS (surprivilégié à corriger), Name Protection, et les collisions DHCP / clients / comptes ordinateurs.

Partie 12 — Réplication, FSMO, sauvegarde, PRA et plateforme

12.1 Contrôler la santé et l'intégrité de la réplication

Vérifier l'absence d'échec et la latence de réplication, rechercher les lingering objects, les USN rollback et l'invalidation de journal, contrôler la cohérence multi-DC des ACL/secrets/GPO, l'état de la migration FRS → DFSR du SYSVOL, la sécurité du transport (RPC/IP, ports, chiffrement) et la topologie (sites, liens, KCC/ISTG, bridgeheads). **Détecter les promotions de DC non autorisées** (nouveaux objets `nTDSDSA`) et auditer les objets de connexion de réplication (créés par le KCC vs manuellement).

```
repadmin /replsummary
repadmin /showrepl * /csv
dcdiag /v /c
```

12.2 Contrôler FSMO et la bascule

Vérifier la localisation, la redondance et le plan de saisie d'urgence des rôles FSMO, et mesurer l'impact d'une perte de PDC Emulator ou de RID Master.

12.3 Auditer la sauvegarde et la rétention

Vérifier System State, la corbeille AD (AD Recycle Bin) et le tombstone lifetime, et **contrôler les droits de restauration de la corbeille** (restaurer un compte Tier 0 supprimé avec son SIDHistory est un rebond). Exiger l'immutabilité et la résilience ransomware (air-gap, WORM, non modifiable par les admins de production). Auditer **qui peut invoquer VSS / Shadow Copy sur un DC** (dump `ntds.dit` furtif sans DCSync). Tester la restauration et la fraîcheur ; traiter le serveur de sauvegarde comme Tier 0 (produit audité en 14.4).

12.4 Auditer le plan de reprise (Forest Recovery)

Vérifier que la procédure de Forest Recovery est documentée et testée : ordre de restauration des domaines, restauration des trusts, validation DNS/SYSVOL, reconstruction de la PKI, rotation `krbtgt`/secrets gMSA-dMSA/keytabs, dépendances Entra Connect/ADFS. Poser le critère « nettoyer vs reconstruire » et **exiger la preuve que le runbook fonctionne sans accès au domaine compromis** (un test de restauration de VM ou de fichier n'est pas un test de Forest Recovery).

12.5 Évaluer la résilience à une compromission totale

Arbitrer rebuild vs remédiation et vérifier l'existence d'une forêt d'administration/récupération isolée.

12.6 Vérifier la préparation à la réponse à incident AD

Contrôler les playbooks de containment (isolation de DC, rotation krbtgt d'urgence, révocation PKI), l'existence d'exercices sur table (tabletop) sous stress et la coordination CERT/CSIRT avec conservation des preuves.

12.7 Auditer la sécurité physique, matérielle et la virtualisation des DC

Vérifier l'accès physique aux salles serveurs et la destruction sécurisée des supports, le firmware/BMC (iLO/iDRAC : comptes par défaut, isolation réseau, supply chain firmware). Pour les DC virtualisés : VM-Generation ID, clonage autorisé, prévention de l'USN rollback sur snapshot, synchronisation du temps, vTPM/Secure Boot, chiffrement des fichiers de VM, interdiction des checkpoints non maîtrisés, protection des exports et snapshots.

12.8 Auditer la plateforme et les niveaux fonctionnels

Relever la version du schéma et les niveaux fonctionnels (DFL/FFL) et la dette de compatibilité. Pour Windows Server 2025, faire de la base 32 Kio un contrôle à part entière : relever `msDs-JetDBPageSize` de chaque DC, l'état DFL/FFL 2025 et l'état de la *fonctionnalité optionnelle de forêt* « Database 32k pages » — **irréversible**. Une nouvelle forêt 2025 est *compatible* 32 Kio mais reste par défaut en **simulation 8 Kio** ; un DC mis à niveau in-place conserve une base 8 Kio. Vérifier la compatibilité du logiciel de sauvegarde, tester sauvegarde/restauration et identifier les anciens médias 8 Kio avant toute activation. Contrôler aussi le support AES-SHA2 et le comportement de signature LDAP des nouveaux déploiements. Retenir qu'une nouvelle forêt 2025 et un domaine simplement mis à niveau ne reçoivent pas les mêmes paramètres de sécurité par défaut ; préparer et valider toute montée de niveau.

Partie 13 — Hybridation cloud (Entra ID / Azure AD Connect)

13.1 Auditer l'architecture de synchronisation

Distinguer Entra Connect Sync et Cloud Sync, auditer les comptes `MSOL_*` / `AAD_*` (droits de réplication DCSync local), traiter le serveur Entra Connect comme Tier 0 (base SQL, secrets DPAPI, staging mode, version/auto-upgrade/fin de support), vérifier le périmètre synchronisé, les filtres et les attributs sensibles.

13.2 Auditer les méthodes d'authentification hybride

Comprendre que PHS synchronise une **valeur dérivée** du hash (et non le hash NT brut), auditer PTA et la fédération ADFS, et traiter le Seamless SSO / `AZUREADSSOACC` (clé statique → Silver Ticket vers le cloud, rotation) et les agents PTA compromis.

13.3 Auditer les risques ADFS et de fédération

Vérifier la protection de la clé de signature de jetons (vol → Golden SAML, jamais patché, seulement atténué), les certificats token signing/decrypting, les règles de transformation de claims, l'Extranet Smart Lockout et les serveurs WAP, et la trajectoire de migration ADFS → authentification managée Entra.

13.4 Auditer les ponts de synchronisation (chaque fonctionnalité = risque distinct)

Traiter séparément Password/Group/Device/Exchange Hybrid Writeback, Cloud Kerberos Trust et l'objet AzureADKerberos, les droits du compte de synchronisation, et cartographier le graphe d'attaque **on-prem → cloud ET cloud → on-prem** (applications capables de revenir vers l'AD).

13.5 Superviser la synchronisation

Contrôler Entra Connect Health et les anomalies, et repérer les comptes hybrides à privilèges cloud (Global Admin) adossés à un compte on-prem.

13.6 Vérifier l'étanchéité et le Zero Trust hybride

Séparer les identités d'administration on-prem et cloud, et contrôler Conditional Access, PIM, Authentication Strength et l'usage de comptes cloud-only pour l'administration Entra.

13.7 Situer la trajectoire Microsoft (Entra-first)

Mesurer les implications sur la feuille de route AD on-premise et la réduction de la dépendance NTLM/Kerberos legacy.

13.8 Auditer le tenant Entra ID

Vérifier les Conditional Access : deux comptes emergency access cloud-only, **exclus des CA bloquantes** (recommandation Microsoft) mais protégés par une authentification résistante au

phishing, à credentials distincts, supervisés et testés périodiquement ; aucune CAP ne doit désactiver la MFA pour des comptes ordinaires. Auditer aussi App Registrations et Service Principals (permissions Graph excessives, secrets/certificats expirants, consentements OAuth, owners, Federated Identity Credentials), les workload identities, le cross-tenant access, PIM (permanent vs éligible, justification, approbation) et l'Identity Governance (access reviews). Renvoyer à la méthodologie Entra/M365 compagnon.

13.9 Auditer les contournements MFA et abus de jetons

Traiter le MFA fatigue, l'extraction/replay de PRT et le device compliance bypass. Rechercher la **Basic Authentication résiduelle** sur POP, IMAP et SMTP AUTH sans assimiler l'activation du protocole à Basic Auth (ces protocoles peuvent s'appuyer sur OAuth2/Modern Auth).

Partie 14 — Briques applicatives et infrastructures dépendantes de l'AD

14.1 Auditer Exchange on-premise / hybride

Vérifier les extensions de schéma et les groupes Organization Management / Exchange Trusted Subsystem, les droits historiques excessifs sur l'objet domaine (PrivExchange), le niveau de patch ProxyLogon/ProxyShell/ProxyNotShell, et l'état du serveur de gestion Exchange hybride ou du décommissionnement résiduel.

14.2 Auditer SCCM / MECM

Rechercher le site takeover, auditer la hiérarchie de sites, les comptes NAA (Network Access Account), le PXE non authentifié, CMPivot et le client push. Cartographier les chemins avec Misconfiguration Manager (SpecterOps) et SCCMHound.

14.3 Auditer WSUS

Vérifier que la distribution de correctifs n'est pas détournable en exécution de code (lien avec ESC17 : AD CS → WSUS), imposer HTTPS et la signature des mises à jour, contrôler les comptes du service.

14.4 Auditer l'infrastructure de sauvegarde (produit)

Auditer les comptes de service à privilèges et les secrets stockés, imposer MFA et une console cloud-only, surveiller les CVE récurrentes et l'exposition des consoles, et vérifier la séparation logique/cryptographique du domaine de sauvegarde (recoupe 12.3).

14.5 Auditer la virtualisation et les hyperviseurs

Traiter vCenter/ESXi et Hyper-V comme Tier 0 de fait, comprendre que le vol d'un snapshot/VMDK équivaut au vol de `ntds.dit`, et vérifier l'isolation des hôtes, le chiffrement et les comptes d'administration (protections DC virtuels en 12.7).

14.6 Auditer les autres dépendances privilégiées

Contrôler PAM/coffres et leurs connecteurs privilégiés, IAM/SSO, RADIUS/NPS et passerelles VPN, ainsi que les outils ITSM, de déploiement et d'inventaire à fort privilège.

14.7 Auditer la chaîne d'approvisionnement logicielle et firmware

Vérifier la provenance et la signature des logiciels d'administration et des firmwares, et le risque de compromission en amont (build/pipeline).

14.8 Auditer l'EDR sur les DC

Rechercher les exclusions abusives (`ntds.dit`, `C:\Windows\NTDS`), la possibilité de désactivation par l'attaquant, et vérifier l'intégrité et la supervision de l'agent sur les actifs du plan de contrôle.

Partie 15 — Journalisation, détection et supervision

15.1 Vérifier la politique d'audit avancée et les SACL

Contrôler la politique d'audit avancée (vs legacy) et les SACL sur les objets sensibles (AdminSDHolder, OU Tier 0, dMSA/gMSA, gabarits PKI, NTAuth), et auditer les modifications d'ACL critiques.

```
auditpol /get /category:*
```

15.2 Prioriser les Event ID et les enchaînements

Surveiller 4624/4625, 4672, 4768/4769/4776 ; 4662 (DCSync), 5136/5137/5141 ; 4720/4728/4732/4756 ; les événements dMSA (création, `msDS-DelegatedMSAState`, TGT), AD CS 4886/4887 (dont Certighost) et les logs FAST/armoring.

15.3 Détecter les techniques majeures

Mettre en détection Kerberoasting, AS-REP Roasting, DCSync, Golden/Diamond Ticket, coercition/relais, failles AD CS, Shadow Credentials, BadSuccessor/abus dMSA, et les skeleton keys (modification de `msv1_0.dll`, succès d'authentification avec un mauvais mot de passe).

15.4 Évaluer les solutions ITDR

Vérifier la couverture de Microsoft Defender for Identity (+ Sentinel/XDR), Semperis DSP, Tenable Identity Exposure, Purple Knight, et la capacité de continuous attack path monitoring (indicateurs d'exposition IOE vs IoC).

15.5 Contrôler centralisation, intégrité et rétention

Vérifier la collecte DC exhaustive dans le SIEM, l'intégrité (WORM/hachage), la rétention (ANSSI/CNIL, NIS2) et la protection de la chaîne de collecte contre l'effacement.

15.6 Vérifier les comptes leurres et objets canari

Déployer des honey-SPN, honey accounts et honey groups (objets d'apparence privilégiée sans privilège réel) et des changements d'ACL canari supervisés ; **éviter de modifier AdminSDHolder/SDProp** pour créer des leurres. Définir les bonnes pratiques de déploiement, gérer les faux positifs, intégrer aux solutions ITDR/MDI.

15.7 Auditer la journalisation PowerShell et l'administration

Vérifier ScriptBlock/Module/Transcription, l'audit WinRM/JEA (cf. 9.5) et la détection des techniques « living off the land » (LOLBAS).

```
Get-ItemProperty 'HKLM:\Software\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging'
-EA SilentlyContinue
```

15.8 Constituer des playbooks d'investigation

Rédiger des playbooks par technique clé (ex. DCSync : sur 4662 par un compte non-DC, vérifier le compte source, les connexions réseau et le contexte ; puis Golden Ticket, ESC8, BadSuccessor résiduel).

15.9 Outiller la chasse aux menaces (threat hunting)

Écrire des requêtes KQL/Splunk pour les anomalies comportementales (ex. pic de tickets Kerberos RC4 sur 4769) et corréler les logs AD ↔ réseau ↔ DNS.

15.10 Mesurer la couverture de détection

Documenter, par technique : source de journal, Event ID, niveau requis, filtre de collecte, parseur SIEM, règle, seuil, faux positifs, test atomique, délai de détection, propriétaire, date du dernier test. Contrôler la santé des capteurs MDI/ITDR, les événements perdus, la latence d'ingestion et la synchronisation temporelle, et la capacité d'un attaquant Tier 0 à effacer les traces. Réaliser des tests de bout en bout réguliers.

Partie 16 — Surface d'exposition externe (OSINT/ EASM appliqué à l'AD)

16.1 Recenser les services d'authentification exposés

Identifier RDP/RDS Gateway, VPN, ADFS, Exchange hybride, OWA/ECP et les endpoints de web enrollment AD CS accessibles, et fingerprinter les versions vulnérables.

16.2 Rechercher les fuites d'identifiants réutilisables

Corréler credential stuffing, breach data et surveillance dark web avec l'audit interne (Partie 4) et la politique interne, et rechercher les secrets exposés dans des dépôts publics.

16.3 Conduire l'OSINT sur la nomenclature interne

Exploiter conventions de nommage, organigramme et métadonnées pour reconstruire la structure AD depuis l'externe.

16.4 Corréler avec la méthodologie EASM/OSINT dédiée

Renvoyer à la méthodologie du site et prioriser les expositions (choke points externes).

Partie 17 — Conformité et référentiels

17.1 Cartographier au guide ANSSI

Confronter les mesures prioritaires du guide « Administration sécurisée d'un SI reposant sur AD » aux findings.

17.2 Cartographier aux CIS Benchmarks

Scorer la conformité aux benchmarks Windows Server, DC et serveur membre (niveaux L1/L2).

17.3 Cartographier au NIST

Rattacher aux familles SP 800-53 et à **SP 800-63-4** (63A-4/63B-4/63C-4, qui remplace 800-63-3 depuis 2025), et au NIST CSF 2.0 (chaîne d'approvisionnement, identité).

17.4 Cartographier à l'ISO/IEC 27001:2022 — Annexe A

Rattacher aux contrôles d'accès, de gestion des identités et des privilèges, de journalisation et de gestion des vulnérabilités.

17.5 Rattacher à NIS2 / Loi Résilience / ReCyF

Documenter le statut (Sénat 03/2025, commission AN 09/2025, jamais en séance publique — blocage anti-portes dérobées —, examen ≥ 09/2026, saisine CJUE 08/07/2026 + REC depuis 04/2026). Traiter ReCyF v2.5 (17/03/2026) comme **référentiel préparatoire** ; mapper les findings aux 20 objectifs (EI 1–15, EE 1–20), en insistant sur les objectifs 16–20 (audits réguliers, durcissement, administration dédiée) qui rattachent directement l'audit. Vérifier l'enregistrement Mon Espace NIS2 et le mapping ReCyF ↔ ISO 27001/27002/27005 ↔ CIS. Rappeler le périmètre (~15 000 entités) et les sanctions (somme forfaitaire + astreintes).

17.6 Traiter le RGPD dans l'annuaire

Contrôler la minimisation des données personnelles et les durées de conservation, la rétention des logs et l'articulation droit à l'effacement / besoins de forensic.

17.7 Couvrir les exigences sectorielles

Rattacher aux exigences OIV/OSE, LPM, DORA (règlement déjà applicable), santé et énergie.

Partie 18 — Threat intelligence et paysage de la menace 2025-2026

18.1 Cartographier les groupes ransomware/APT ciblant l'AD

Documenter les TTP dominants (accès → escalade → domination → exfiltration/chiffrement), le rôle central d'AD CS et de la coercition/relais, et l'industrialisation par les access brokers.

18.2 Cartographier MITRE ATT&CK (avec sous-techniques)

Couvrir Credential Access, Privilege Escalation et Lateral Movement, la persistance (Golden Ticket, AdminSDHolder, certificats, Shadow Credentials) et la defense evasion.

18.3 Suivre les techniques émergentes

Intégrer le post-BadSuccessor (BetterSuccessor, BadTakeover), AD CS (ESC17 WSUS, Certighost/CVE-2026-54121), les primitives de coercition NTLM et l'abus hybride on-prem ↔ Entra.

18.4 Exploiter les retours d'expérience incident response

Analyser dwell time, vecteurs, points de bascule Tier 0, et l'arbitrage rebuild vs nettoyage.

18.5 Structurer la veille

S'appuyer sur CERT-FR, MSRC, CISA KEV, SpecterOps, Semperis, Akamai, Unit 42, TrustedSec, et suivre les release notes Certipy/BloodHound comme signal d'émergence.

18.6 Encadrer l'automatisation offensive assistée par IA

Mesurer l'accélération de l'exploitation des chemins et de la génération de PoC, et poser les garde-fous (pas de données AD sensibles vers des LLM publics, vérification humaine). Traiter cette section comme un encadré « état de la menace à la date de révision » pour ne pas périmer le guide.

Partie 19 — Outillage de l'auditeur

19.1 Cartographie et chemins

Employer BloodHound CE/SharpHound (Cypher), Adalanche, AD Miner.

19.2 Scoring automatisé

Employer PingCastle (scan actif → bruit), Purple Knight, Tenable Identity Exposure ; recouper et dédoublonner.

19.3 Recensement souverain et scripts natifs

Employer ORADAD (ANSSI), le module AD, DSInternals.

19.4 Audit des mots de passe (renvoi Partie 4)

Employer DSInternals (`Test-PasswordQuality`) avec le corpus HIBP NTLM hors-ligne ; impacket-secretsdump / ntdsutil IFM (cadre autorisé), hashcat (enclave isolée).

19.5 Outillage AD CS

Employer Certipy v5+, Certify 2.0, PSPKIAudit ; PKINITtools ; corréler ESC ↔ gabarit.

19.6 Analyse GPO et cryptographie

Employer Group3r, PolicyAnalyzer, GPRegistryPolicy ; analyse TLS/SChannel (testssl.sh, IISCrypto en lecture) et etypes Kerberos.

19.7 Écosystème dépendant

Employer Misconfiguration Manager/SCCMHound, l'outillage Exchange/WSUS, l'audit virtualisation et sauvegarde.

19.8 Validation offensive encadrée (« read-only first »)

Employer Impacket, Rubeus, mimikatz dans un cadre strictement autorisé et tracé ; documenter par outil les privilèges requis, les données collectées, les requêtes générées, l'impact, la détectabilité, les secrets en sortie et le nettoyage ; distinguer PoC et exploitation intrusive.

19.9 Outillage propriétaire

Référencer CHECKSEC et normaliser les sorties.

19.10 Assistants IA

Employer l'analyse de chemins (prompts Cypher) et la génération de rapports depuis les findings JSON ; anonymiser/tokeniser les logs avant soumission ; vérifier humainement (limites et biais).

Partie 20 — Scoring, maturité et restitution

20.1 Établir la grille de scoring

Coter par chemin et rayon d'impact (cf. 0.6), consolider à l'échelle de la forêt et du plan de contrôle, produire une heat map des chemins.

20.2 Positionner la maturité

Situer sur une échelle par niveaux avec benchmarking sectoriel, positionner EI/EE (ReCyF) et comparer aux audits antérieurs.

20.3 Structurer le rapport

Rédiger une synthèse exécutive orientée risque, des findings au format normalisé (annexe 22.6), des annexes techniques et chemins BloodHound, et la traçabilité finding ↔ objectif réglementaire.

20.4 Prioriser la remédiation

Distinguer quick wins et projets structurants, cibler les choke points, renvoyer au guide de durcissement AD 2026.

20.5 Bâtir la feuille de route

Séquencer 0-3 mois (chemins directs vers le plan de contrôle), 3-12 mois (tiering, PAM, LAPS, AD CS, migration AES/NTLM), 12-24 mois (Zero Trust hybride, réduction de dette, amorce PQC).

20.6 Assurer le suivi post-audit et le ré-audit

Définir KPI/KRI et tableaux de bord direction, la périodicité de ré-audit (exigence EE ReCyF) et la **preuve de clôture** (état initial → modification → non-régression → nouvelle collecte → disparition du chemin → validation de la détection → acceptation des risques résiduels).

Partie 21 — Industrialisation, automatisation et audit continu

21.1 Passer du point-in-time au continu

Dépasser les limites de l'audit ponctuel par un continuous exposure management (ITDR + drift).

21.2 Détecter la dérive

Baseliner configuration, services et chemins, alerter sur tout nouveau chemin vers le plan de contrôle, suivre ACE, délégations, gabarits PKI et services en écoute.

21.3 Rendre le pipeline d'audit reproductible

Versionner les scripts, horodater et hacher les collectes, générer semi-automatiquement les findings et la matrice de correspondance, produire un diff de posture inter-campagnes et suivre en continu les mots de passe compromis/partagés (Partie 4).

21.4 Valider en continu (purple team)

Exécuter un set Atomic Red Team par technique (Kerberoasting, DCSync, ESC8, BadSuccessor résiduel, Shadow Credentials), mesurer la couverture SIEM/ITDR (cf. 15.10), boucler détection ↔ remédiation.

21.5 Gouverner l'amélioration continue

Intégrer au SMSI (ISO 27001) et aux objectifs 16–20 ReCyF (EE), assurer un reporting récurrent et une trajectoire de maturité.

21.6 Auditer l'Infrastructure as Code (IaC) et l'AD

Revoir les pipelines (Terraform/GitLab) poussant GPO/ACL et contrôler les droits et le stockage du secret du compte de service du pipeline.

Partie 22 — Annexes

22.1 Glossaire technique FR/EN

Définir dMSA, RBCD, PAC, TGT, RODC, SPN, ESC, PRT, PQC, etc., et fournir un index des acronymes.

22.2 Bibliographie et sources 2025-2026

ANSSI (guide AD, PA-022, ReCyF v2.5, RGS), MITRE ATT&CK/D3FEND, CIS, NIST 800-53/63/CSF 2.0, ISO ; SpecterOps (Misconfiguration Manager, ESC1-16), TrustedSec (EKUwu/ESC15), Akamai (BadSuccessor), Semperis, Certipy/Certify, HIBP (Pwned Passwords), MSRC, CERT-FR, dossier Assemblée nationale (loi Résilience).

22.3 Check-lists

Fournir des check-lists avant / pendant / post-mission, et des variantes par public (Auditeur, RSSI/Direction, Administrateur). *(Livrées en annexe Word et Excel — cf. classeur d'audit.)*

22.4 Matrice de correspondance

Croiser ANSSI / CIS / NIST / ISO / MITRE ATT&CK / D3FEND / ReCyF.

22.5 Modèles

Lettre de mission, règles d'engagement, fiche de finding, registre de custody, registre d'exceptions.

22.6 Fiche de contrôle normalisée

Réf. · Objectif · Risque/scénario · Périmètre · Collecte passive · Validation active autorisée · Preuves · Faux positifs/exceptions · Cotation (chemin/blast radius) · Détection · Remédiation · Critère de clôture · Correspondances · Validité technique (version testée, date, source primaire).

22.7 Tableau de veille CVE AD 2020-2026

Zerologon, PetitPotam, PrintNightmare, noPac, Certifried (CVE-2022-26923), EKUwu (CVE-2024-49019), BadSuccessor (CVE-2025-53779), Certighost (CVE-2026-54121)… avec statut de patch, impact et méthode de détection.

22.8 Matrice de maturité par objectif ReCyF (16–20 EE)

Contrôles ↔ preuves attendues ↔ niveau de maturité cible.

22.9 Guide de lecture par niveau

Décideur / Auditeur / Administrateur / Expert.

22.10 Politique de fraîcheur documentaire

Dernière vérification, versions couvertes, prochaine revue ; chaque affirmation datée porte une source primaire.

Partie 23 — Cas d'étude, scénarios et findings type

23.1 Scénarios réels anonymisés

- **Ransomware** : coercition → relais NTLM → ESC8 → DCSync → chiffrement, et comment l'audit l'aurait détecté avant (signature LDAP/EPA absente, MS-RPRN actif, absence de SACL sur les gabarits).
- **Insider** : RBCD + MAQ pour une escalade silencieuse (MAQ resté à 10, droit d'écriture sur un objet machine).
- **Supply chain** : compromission d'un accès MSP → AD → persistance via Shadow Credentials.
- **Post-BadSuccessor** : dMSA créé par l'attaquant, détecté via SACL (6.5).
- **Credential harvesting** : mot de passe d'un compte de service Tier 0 partagé par 40 comptes utilisateurs, détecté en Partie 4.

23.2 Findings entièrement rédigés (exemples de restitution)

Chemin d'attaque composite vers le plan de contrôle ; gabarit AD CS vulnérable (ESC1) ; compte de service RC4/Kerberoastable ; délégation GPO dangereuse ; serveur de sauvegarde contournant le tiering.

23.3 Temps-to-Compromise (TTC) observé pendant le scénario

Ne pas publier de constantes universelles (un Kerberoast va de quelques secondes à impraticable selon la robustesse du secret). Mesurer le TTC *par mission* en consignant hypothèses, niveau d'accès initial, versions d'outils, latence, contrôles de sécurité en place, temps humain vs automatisé et date du test.

23.4 Anti-patterns et patterns de remédiation

Par famille (MAQ=10, Spouleur sur DC, LDAP non signé, GPP cpassword, RC4 explicite, délégations non contraintes, SYSVOL accessible en écriture, gabarits ESC1/4/8, mots de passe partagés…), opposer l'anti-pattern *fréquemment rencontré* à la cible de remédiation.

Fin du référentiel. Édition 2026 — document vivant, à réviser au rythme de la veille CVE AD et du calendrier de la loi Résilience.

Compléments v1.1 (révision août 2026) — nouveaux contrôles et précisions

Ce bloc étend le corps du référentiel avec des contrôles issus de la revue technique. Chaque section porte le numéro de la partie qu'elle complète.

0.11 Classer chaque commande par niveau d'intrusivité (P0–P3)

« Ne rien modifier » ne signifie pas « passif » : `SharpHound -c All`, un Kerberoast Rubeus ou un test Responder ne changent rien dans l'annuaire mais génèrent de la télémétrie et sollicitent des services. Classer donc chaque commande : **P0** purement passif (lecture LDAP d'attributs) ; **P1** actif non modifiant (énumération de sessions, RPC, SharpHound All) ; **P2** validation contrôlée (demande de TGS, enrôlement Certipy de test) ; **P3** modification/exploitation (RBCD, DCSync, changement de gabarit, relais). Réserver P2/P3 au périmètre explicitement autorisé et tracé.

1.10 Auditer Sites, Subnets et DC Locator

Cartographier les sites *et* les subnets ; un subnet manquant renvoie les clients vers de mauvais DC (sécurité, résilience et performance).

```
Get-ADReplicationSite -Filter * | Select Name
Get-ADReplicationSubnet -Filter * | Select Name,Site
```

Rechercher : subnets absents, supernets trop larges, sites sans DC, site links mal configurés, coûts incohérents, schedules trop restrictifs, bridgeheads forcés historiques.

2.9 Auditer ForeignSecurityPrincipals, SID orphelins et protection contre suppression

Recenser les ForeignSecurityPrincipals et les SID orphelins (ACE pointant vers des SID non résolus — trusts cassés, comptes supprimés). Vérifier `ProtectedFromAccidentalDeletion` sur les OU Tier 0, l'OU des DC et les objets de services critiques.

```
Get-ADObject -LDAPFilter '(objectClass=foreignSecurityPrincipal)' -SearchBase
("CN=ForeignSecurityPrincipals,"+(Get-ADDomain).DistinguishedName)
Get-ADOrganizationalUnit -Filter * -Properties ProtectedFromAccidentalDeletion |
  Where-Object { -not $_.ProtectedFromAccidentalDeletion }
```

3.14 Auditer les RODC et la Password Replication Policy (section dédiée)

Ne pas se limiter à recenser les RODC : auditer leur PRP et leurs secrets réellement mis en cache. Contrôler `Allowed` / `Denied RODC Password Replication Group`, `msDS-RevealOnDemandGroup` (comptes révélables) et `msDS-NeverRevealGroup` (protection Tier 0), la population réellement authentifiée sur le RODC, le compte `krbtgt_<RID>` propre à chaque RODC, l'administrateur local délégué, l'exposition physique du site, le runbook de reset des secrets après vol, l'absence de `Replicating Directory Changes All` indu et les données DNS/GC exposées.

```
Get-ADDomainController -Filter {IsReadOnly -eq $true} | ForEach-Object {
  repadmin /prp view $_.HostName Reveal
  repadmin /prp view $_.HostName Allow
}
Get-ADObject -LDAPFilter '(sAMAccountName=krbtgt_*)' -Properties sAMAccountName
```

3.15 Auditer les SSP, packages d'authentification et filtres de mot de passe

Un AD parfaitement configuré peut rester compromis par une persistance LSA/SSP sur DC ou PAW. Inventorier `Security Packages`, `Authentication Packages`, `Notification Packages` (filtres de mot de passe), rechercher `WDigest\UseLogonCredential=1`, les SSP personnalisés et les DLL de filtre de mot de passe non signées ou hors emplacement standard (un filtre compromis est Tier 0). Recouper avec la détection Skeleton Key (15.3.4).

```
$p='HKLM:\SYSTEM\CurrentControlSet\Control\Lsa'
Get-ItemProperty $p -Name 'Security Packages','Authentication Packages','Notification
Packages' -EA SilentlyContinue
Get-ItemProperty "$p\OSConfig" -EA SilentlyContinue
Get-ItemProperty 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest' -Name
UseLogonCredential -EA SilentlyContinue
```

5.10 Auditer la chaîne de temps (w32tm)

La cohérence temporelle est vitale pour Kerberos ; un attaquant qui manipule le temps peut provoquer des dysfonctionnements d'authentification sans « casser AD ». Vérifier la hiérarchie : PDC Emulator racine de forêt → source NTP externe maîtrisée → autres DC → membres.

```
w32tm /query /configuration
w32tm /query /status
w32tm /query /peers
```

Contrôler la dérive, la GPO de temps, la synchronisation hôte/invité en virtualisation (à désactiver sur le PDC), la bascule du PDC et l'alerting.

5.11 Auditer les certificats KDC/PKINIT et l'inventaire etypes au niveau forêt

Auditer les certificats KDC (dépendance critique de WHfB, smartcard, PKINIT), l'inventaire des etypes par compte (`msDS-SupportedEncryptionTypes` absent vs explicite — significations différentes depuis 2026), l'analyse séparée des 4768 **et** 4769 par type de chiffrement (détection de la dette RC4), les keytabs UNIX/Linux (RC4/DES, secrets non renouvelés), les etypes des trusts, la validation du PAC côté service, et l'état de KDC Proxy / IAKerb / Local KDC selon les versions.

6.12 Traduire les ACE en matrice de primitives (edges BloodHound)

Ne pas se contenter de « GenericWrite dangereux » : dire ce que l'ACE *permet réellement*. Cartographier les primitives : `WriteSPN` (Kerberoasting forcé), `AddKeyCredentialLink` (Shadow Credentials), `WriteAccountRestrictions` (RBCD), `AddMember` / `AddSelf` (groupes), `WriteGPLink` (OU/

site/domaine), `WriteDACL` / `WriteOwner` (toute cible), `ReadLAPSPassword`, `ReadGMSAPassword`, `DCSync`, `AllowedToDelegate`, `AllowedToAct`, `Owns`, droits d'enrôlement (gabarits), `ManageCA` / `ManageCertificates` (AC). Chaque finding nomme la primitive et sa cible.

7.9 Auditer les mappings de certificats Schannel (distincts de Kerberos/PKINIT)

Angle mort fréquent : le durcissement du mapping KDC/PKINIT ne couvre pas Schannel, qui possède sa propre logique de mapping (pertinente pour ESC10). Contrôler `CertificateMappingMethods` sur tous les DC et serveurs faisant de l'authentification par certificat client TLS ; signaler l'activation du mapping UPN faible `0x4` ; distinguer clairement mapping **KDC/PKINIT** et mapping **Schannel/TLS**.

```
Get-ItemProperty 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL' -Name
CertificateMappingMethods -EA SilentlyContinue
```

7.10 Approfondir AD CS : RPC (ESC11), endpoints et Issuance Policies

Auditer le chiffrement RPC d'AD CS (`IF_ENFORCEENCRYPTICERTREQUEST`, exigence de packet privacy — ESC11). Pour chaque endpoint (`/certsrv`, CES, CEP, NDES, SCEP, connecteur Intune), contrôler séparément TLS, NTLM, EPA, Require SSL, droits d'accès, identité de l'App Pool/service et exposition externe. Cartographier les Issuance Policies et OID : `Certificate Policy OIDs`, groupes de politique d'émission, `msDS-OIDToGroupLink`, ACL sur les OID et chemins vers des groupes privilégiés (ESC13).

8.11 Auditer la baseline OSConfig de Windows Server 2025

Microsoft fournit pour Windows Server 2025 une Security Baseline pilotée par **OSConfig**, avec un scénario dédié contrôleur de domaine (`SecurityBaseline/WindowsServer/2025/DomainController`) et une gestion de conformité/dérive. Comparer : état effectif du DC ↔ baseline OSConfig DC ↔ CIS ↔ ANSSI ↔ exceptions internes.

```
Get-OSConfigDesiredConfiguration -Scenario 'SecurityBaseline/WindowsServer/2025/
DomainController' -Default -EA SilentlyContinue
```

9.8 Auditer les politiques Restrict NTLM et inventorier NTLM avant suppression

Contrôler systématiquement les sept politiques *Network security: Restrict NTLM* (audit du trafic entrant, audit de l'authentification NTLM dans le domaine, trafic entrant, trafic sortant vers serveurs distants, authentification NTLM dans le domaine, exceptions serveur distant, exceptions serveur dans le domaine). Constituer un **inventaire NTLM** avant toute suppression : qui → utilise NTLM → vers quel serveur → pour quelle application → quel propriétaire → justification → exception → date de suppression cible. Point de calendrier : `BlockNTLMv1SSO` passe d'Audit à Enforce par défaut à une date visée en octobre 2026 (encore provisoire).

```
$lsa='HKLM:\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0'
Get-ItemProperty $lsa -Name
RestrictSendingNTLMTraffic,AuditReceivingNTLMTraffic,RestrictReceivingNTLMTraffic -EA
SilentlyContinue
```

9.9 Auditer RestrictRemoteSAM et l'énumération SAMR distante

Vérifier *Network access: Restrict clients allowed to make remote calls to SAM* (SDDL restreint aux administrateurs), particulièrement sur serveurs membres et postes qui alimentent les chemins d'attaque.

```
Get-ItemProperty 'HKLM:\SYSTEM\CurrentControlSet\Control\Lsa' -Name RestrictRemoteSAM -EA
SilentlyContinue
```

12.9 Exiger un environnement de récupération propre (clean-room)

Remplacer « forêt d'administration isolée » par la vérification d'un **environnement de récupération indépendant du domaine compromis** : comptes recovery indépendants, secrets hors-ligne, DNS minimal, média OS propre, logiciels de sauvegarde accessibles sans AD, procédures imprimées, PKI recovery, et surtout **clés BitLocker des DC disponibles hors de l'AD qu'elles protègent** (sinon la clé de récupération se trouve dans le domaine qu'on tente de restaurer). Vérifier aussi un accès hyperviseur indépendant de l'AD compromis.

12.10 Auditer les droits de promotion de DC et la provenance des images

Au-delà de la détection des objets `nTDSDSA`, répondre à : **qui, hors des admins AD prévus, peut introduire un DC dans la forêt ?** Contrôler les droits nécessaires, les comptes utilisés, l'accès aux secrets DSRM, les permissions DNS et de création d'objets serveur/NTDS Settings, les scripts d'automatisation et les templates de VM. Auditer la **provenance des images de DC** (golden image, ISO, templates VMware/Hyper-V, images cloud, scripts post-install, DSC/Ansible/Terraform, drivers, agents EDR, firmware) : un pipeline d'image de DC compromis est une persistance *pré-AD*, à rattacher au Tier 0.

13.10 Auditer les identités workload et le contrôle d'accès inter-tenant (Entra)

Compléter l'audit du tenant : Federated Identity Credentials des applications (secrets workload sans mot de passe), owners d'App Registrations (un owner peut devenir très puissant), workload identities et leur Conditional Access, permissions de device registration/join, cross-tenant access, consent grants OAuth (persistance applicative), secrets/certificats expirants (app takeover / outage), hard vs soft matching Entra Connect et `sourceAnchor` / `ImmutableID` (takeover d'identité hybride), Cloud Kerberos Trust et objet AzureADKerberos, âge/rotation de `AZUREADSSOACC`, agents PTA (Tier 0 réel), PRT/device token (vol et replay), gaps de Conditional Access (device code, workload, invités), Authentication Strength réellement phishing-resistant, PIM for Groups et test périodique documenté du break-glass. On passe alors d'un audit « AD + un peu Entra » à un audit du **plan de contrôle d'identité hybride**.

14.9 Traiter l'identité SaaS EDR/RMM et l'accès mémoire hyperviseur comme Tier 0

Le tenant cloud EDR/RMM capable d'exécuter une commande sur un DC appartient au plan de contrôle : auditer MFA, résistance au phishing, rôles, API keys, service principals, SSO, break-glass, journaux d'audit, remote shell, bibliothèque de scripts et supply chain. Pour la virtualisation, préciser que l'**accès mémoire d'une VM DC** (dump live) donne accès aux secrets en mémoire, pas seulement le vol de VMDK/snapshot ; vérifier Shielded VM / vTPM / Secure Boot / HGS lorsque l'architecture le permet.

14.10 Auditer la trajectoire de sortie de WSUS

WSUS est déprécié (plus activement développé) sur Windows Server 2025, bien que supporté. Auditer la trajectoire de réduction de dépendance en plus de la sécurité actuelle. Préciser qu'avec ESC17, **HTTPS seul n'est pas une mitigation suffisante**, puisque l'attaque repose précisément sur l'usurpation d'un serveur TLS via un certificat frauduleusement obtenu.

15.11 Auditer Windows Event Forwarding et les familles d'événements complémentaires

Auditer explicitement WEF/WEC : subscriptions (source-initiated vs collector-initiated), ACL des subscriptions, certificat si HTTPS, latence, backlog, taille des journaux locaux, anti-tamper du collector, redondance WEC, heartbeat et perte d'événements — en priorité pour DC, PAW, CA et Tier 0. Ajouter les familles d'Event ID : **LDAP signing 2886–2889**, **channel binding 3039–3041**, 4719 (altération de la politique d'audit), 1102 (journal effacé), 4882–4890 (AD CS), 7045 (installation de service), création/modification de tâches planifiées, arrêt/tamper/exclusion Defender-EDR, DNS analytique + modification de zones, 4103/4104 (PowerShell) + transcription, et la santé du forwarding WEF/SIEM.

19.11 Outillage complémentaire

Ajouter, pour la détection/forensique, la collecte ETW (ex. SilkETW) — source de logs que les attaquants connaissent moins bien. Pour l'audit hybride, s'appuyer sur Microsoft Graph PowerShell (`Get-MgUser`, `Get-MgServicePrincipal`, `Get-MgPolicyConditionalAccessPolicy`…), `Get-ADUser` seul étant insuffisant côté cloud.

20.7 Rendre le scoring opérationnel (grille 0–4 par dimension)

Décliner les sept dimensions en une grille 0–4 pour rendre les cotations comparables entre auditeurs (sans prétendre à une précision mathématique) : proximité du plan de contrôle (0 = aucun chemin → 4 = contrôle direct Tier 0), prérequis (0 = très élevés → 4 = Domain User seul), exploitabilité (0 = théorique → 4 = fiable/reproductible), blast radius (0 = objet isolé → 4 = forêt/tenant), persistance (0 = aucune → 4 = survit à un reset de mot de passe), détectabilité (0 = alerte fiable → 4 = actuellement invisible), réversibilité (0 = immédiate → 4 = rebuild/recovery).

22.11 Enrichir la fiche de contrôle normalisée

Ajouter à la fiche (22.6) les champs : version d'OS concernée (2016/2019/2022/2025), version d'outil testée, niveau d'intrusivité de la collecte (P0–P3), niveau de bruit SOC, modification effectuée (oui/non), secret produit (oui/non), technique ATT&CK et contre-mesure D3FEND, edge

BloodHound, Event ID de détection, caractère automatisable, état (OK/KO/N-A/exception), source primaire et date d'expiration du contrôle.

> **Note de version.** Le corps du référentiel intègre déjà les corrections v1.1 sur : rotation KDS (à ne pas faire), santé des secrets de trust (vs `whenChanged` /180 j), `StrongCertificateBindingEnforcement` (artefact historique depuis 09/2025), ESC17 (Enrollee-Supplied Subject for Server Auth, pas seulement WSUS), break-glass Entra (exclus des CA bloquantes mais phishing-resistant), `GenericAll` sur `CN=Users` (primitive, pas élévation automatique), PDC Emulator (dépendance critique, pas SPOF), Constrained Language Mode (conséquence de WDAC/App Control), DNSSEC (selon besoin), pages 32 Kio WS2025 (feature optionnelle irréversible), `Get-Service` (Invoke-Command en PS7), Legacy LAPS vs Windows LAPS, POP/IMAP/SMTP (Basic Auth ≠ protocole), NIST SP 800-63-4, ReCyF « document de travail », TTC (mesure de mission), et honeytokens hors AdminSDHolder.