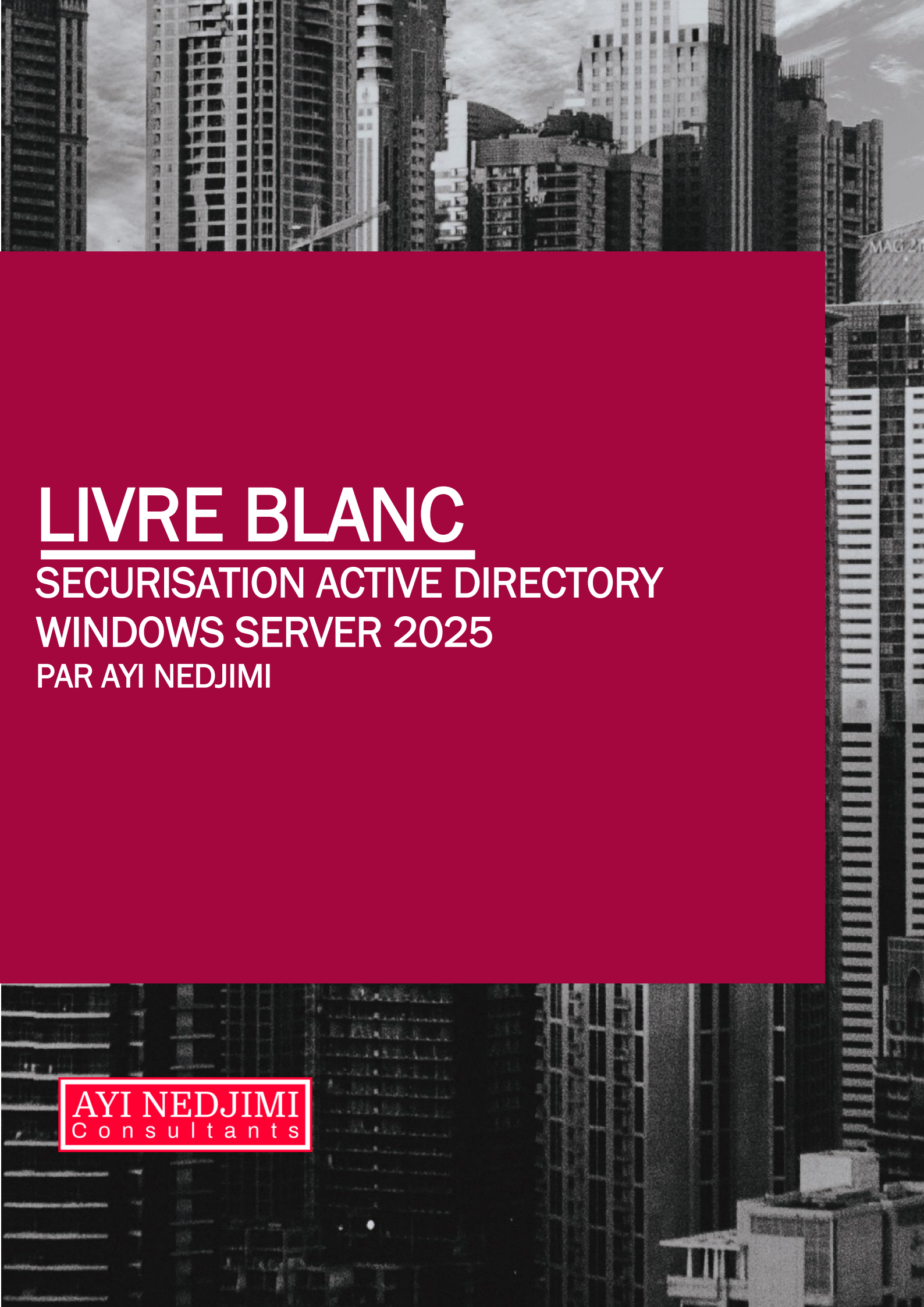

LIVRE BLANC

SECURISATION ACTIVE DIRECTORY WINDOWS SERVER 2025

PAR AYI NEDJIMI

AYI NEDJIMI Consultants

Livre Blanc: Sécurisation Active d'Active Directory sous Windows Server 2025

I. Introduction: Le Rôle Central d'Active Directory et les Enjeux de Sécurité

L'importance d'Active Directory comme pilier de l'identité et de l'accès

Active Directory (AD) est le service d'annuaire fondamental de Microsoft Windows, servant de pierre angulaire à la gestion des identités et des accès au sein des infrastructures informatiques d'entreprise. Il orchestre l'authentification des utilisateurs, la gestion des autorisations et les contrôles d'accès à l'ensemble des systèmes, applications et ressources d'une organisation.[1] Cette centralisation du contrôle d'accès confère à Active Directory un rôle critique, en faisant la cible privilégiée des cyberattaques. Une gestion rigoureuse de la sécurité d'AD est donc impérative pour protéger les informations d'identification, les applications métiers et les données confidentielles contre les accès non autorisés.[1]

La position d'Active Directory en tant que "clé du royaume" signifie que sa compromission peut entraîner un contrôle total du réseau par un attaquant.[1] Cette réalité souligne l'impératif d'une sécurité proactive et multicouche, où la défense d'AD ne peut être une réflexion après coup, mais doit s'inscrire au cœur de la stratégie de cybersécurité de l'entreprise. La capacité d'un attaquant à manipuler Active Directory lui confère le pouvoir d'élever ses privilèges, de créer ou de supprimer des comptes, d'accéder à des données critiques et de maintenir une présence indétectée au sein de l'environnement.[2]

Vue d'ensemble des vulnérabilités courantes et des menaces persistantes

Le paysage des menaces d'Active Directory est complexe, marqué par des vulnérabilités courantes et des techniques d'attaque sophistiquées. Parmi les lacunes de sécurité les plus fréquentes figurent les déploiements incomplets d'antivirus et d'anti-malware, l'application irrégulière des correctifs de sécurité, l'utilisation d'applications et de systèmes d'exploitation obsolètes, et des erreurs de configuration.[3] Ces faiblesses peuvent être exploitées par des attaquants pour voler des informations d'identification, infiltrer des systèmes à l'aide de malwares, se déplacer latéralement au sein du réseau, et finalement exfiltrer des données sensibles ou corrompre l'ensemble du système.[1]

Une préoccupation majeure est la capacité des attaquants à rester indétectés pendant de longues périodes après avoir obtenu un accès initial.[1] Cette persistance prolongée permet aux acteurs malveillants d'infliger des dommages considérables et rend le traçage de leurs activités et l'identification de toutes les zones compromises particulièrement difficiles.[1] L'absence de détection rapide est une conséquence directe des lacunes en matière de surveillance et d'audit. Cela met en évidence que les mesures préventives seules sont insuffisantes ; la détection et la

réponse actives sont essentielles pour minimiser le "temps de présence" (dwell time) de l'attaquant et réduire l'impact d'une brèche. L'objectif est de réduire le "temps d'évasion" (breakout time), c'est-à-dire le temps qu'il faut à un intrus pour commencer à se déplacer latéralement après avoir compromis une machine, qui est en moyenne de moins de deux heures.[5]

Pourquoi Windows Server 2025 est une opportunité pour renforcer la sécurité

Windows Server 2025 représente une évolution significative pour la sécurité d'Active Directory, introduisant de nombreuses améliorations pour les services de domaine Active Directory (AD DS) et les services d'annuaire léger Active Directory (AD LDS).[6] Ces avancées sont conçues pour optimiser la gestion des domaines et renforcer la posture de sécurité globale grâce à de nouvelles fonctionnalités et à la mise à jour de protocoles.[6]

Windows Server 2025 ne se contente pas de corriger les vulnérabilités passées ; il intègre des fonctionnalités de sécurité "security-first" [7] qui, si elles sont pleinement exploitées, peuvent transformer fondamentalement la posture de sécurité d'AD. Des changements fondamentaux, tels que le chiffrement LDAP obligatoire par défaut et l'activation par défaut de Credential Guard [7], signalent une orientation stratégique de Microsoft vers une approche de conception plus sécurisée. Pour les organisations, cela constitue une opportunité stratégique de moderniser leurs défenses, de passer d'une approche réactive de correction des vulnérabilités à une posture de sécurité proactive, et d'aligner leurs infrastructures sur des cadres de sécurité modernes tels que le Zero Trust.[9] La mise à niveau vers Windows Server 2025 offre des avantages tels qu'une réplication améliorée, de meilleures options de chiffrement et un support renforcé pour l'intégration cloud, des éléments essentiels pour maintenir la résilience et la sécurité des environnements.[12]

II. Les Nouveautés de Sécurité d'Active Directory dans Windows Server 2025

Améliorations Fondamentales d'AD DS

Taille de page de base de données 32k et son impact sur la sécurité et la performance

Historiquement, Active Directory a utilisé une taille de page de base de données de 8k depuis son introduction. Windows Server 2025 lève cette limitation en offrant un format de page de base de données optionnel de 32k, ce qui améliore considérablement les domaines affectés par ces restrictions héritées.[6] Par exemple, les attributs à valeurs multiples peuvent désormais contenir environ 3 200 valeurs, soit une augmentation de 2,6 fois. Les nouveaux contrôleurs de domaine (DCs) peuvent être installés avec une base de données de 32k pages en utilisant des IDs de valeur longue (LIDs) de 64 bits, tout en pouvant fonctionner en mode 8k pages pour la compatibilité avec les versions antérieures.[6]

Bien que cette augmentation de la taille de page soit principalement une amélioration de performance et de scalabilité, elle peut indirectement renforcer la sécurité en permettant des

configurations plus complexes et granulaires pour les objets de stratégie de groupe (GPOs) et les objets AD. La capacité accrue de stockage peut faciliter la mise en œuvre de politiques de sécurité plus détaillées et de contrôles d'accès plus fins directement dans l'annuaire. Cependant, cette transition vers une base de données de 32k pages est un changement à l'échelle de la forêt, exigeant que tous les DCs de la forêt soient compatibles avec cette taille de page.[6] Cela implique une mise à niveau de forêt significative, nécessitant une planification minutieuse pour éviter les perturbations et les erreurs de configuration qui pourraient, si mal gérées, créer de nouvelles vulnérabilités ou des problèmes opérationnels.

Mises à jour du schéma Active Directory et réparation d'objets

Windows Server 2025 introduit trois nouveaux fichiers de journal de base de données (sch89.ldf, sch90.ldf, et sch91.ldf) pour étendre le schéma Active Directory, avec des mises à jour équivalentes pour AD LDS dans MS-ADAM-Upgrade3.ldf.[6] Ces extensions permettent d'intégrer de nouvelles fonctionnalités et d'améliorer la gestion des attributs.

De plus, les administrateurs d'entreprise peuvent désormais réparer des objets AD qui ont des attributs essentiels manquants, tels que SamAccountType et ObjectCategory, et réinitialiser l'attribut LastLogonTimeStamp à l'heure actuelle.[6] Ces opérations sont effectuées via une nouvelle fonctionnalité de modification

RootDSE sur l'objet affecté, appelée fixupObjectState.[6] La capacité de réparer directement des objets AD corrompus et de gérer des attributs critiques est une amélioration significative pour la résilience opérationnelle et la sécurité. Les attributs manquants ou incorrects, ou les

LastLogonTimeStamp obsolètes, peuvent indiquer des problèmes de santé d'AD ou des tentatives de compromission. La possibilité de corriger ces problèmes directement réduit la nécessité d'interventions manuelles complexes ou de restaurations complètes, qui sont souvent des points de vulnérabilité ou de perturbation. Cela permet de maintenir plus facilement l'intégrité de l'annuaire, ce qui est crucial pour une posture de sécurité robuste.

Renforcement des algorithmes de recherche Nom/SID et du localisateur de contrôleur de domaine

Windows Server 2025 améliore la sécurité des communications fondamentales d'Active Directory. Les recherches Nom/SID de l'autorité de sécurité locale (LSA) entre les comptes machine ne dépendent plus du canal sécurisé Netlogon hérité. Elles utilisent désormais l'authentification Kerberos et l'algorithme de localisation des DCs, bien que le canal sécurisé Netlogon reste disponible en tant que solution de secours pour la compatibilité avec les systèmes d'exploitation plus anciens.[6] De plus, l'algorithme de découverte des DCs inclut de nouvelles fonctionnalités qui améliorent le mappage des noms de domaine NetBIOS courts aux noms de domaine de style DNS.[6]

La transition de Netlogon vers Kerberos pour les recherches Nom/SID est une étape cruciale pour éliminer les vulnérabilités associées aux protocoles hérités, tels que celles exploitées par des attaques comme Zerologon. En forçant l'utilisation de protocoles plus robustes par défaut, Microsoft réduit activement la surface d'attaque en durcissant les chemins de communication fondamentaux au sein d'AD. Cela rend plus difficile pour les adversaires d'exploiter les

mécanismes d'authentification plus anciens et plus faibles pour la reconnaissance ou le mouvement latéral.

Sécurité des Authentifications et des Comptes

Chiffrement LDAP par défaut et support TLS 1.3

Windows Server 2025 renforce considérablement la sécurité des communications LDAP. Toutes les communications client LDAP après une liaison Simple Authentication and Security Layer (SASL) utilisent désormais le scellement LDAP par défaut.[6] De plus, LDAP utilise la dernière implémentation SCHANNEL et prend en charge TLS 1.3 pour les connexions LDAP sur TLS, la version la plus récente et la plus sécurisée du protocole TLS, qui élimine les algorithmes cryptographiques obsolètes.[6] Les contrôleurs de domaine (DCs) et les instances AD LDS autorisent désormais les opérations LDAP impliquant des attributs confidentiels uniquement lorsque la connexion est chiffrée.[6]

Le chiffrement LDAP par défaut et le support de TLS 1.3 sont des améliorations fondamentales pour la confidentialité et l'intégrité des données transitant vers et depuis Active Directory. Le trafic LDAP non chiffré constitue une vulnérabilité significative, permettant aux attaquants d'intercepter des informations sensibles. En rendant le chiffrement LDAP obligatoire par défaut et en prenant en charge TLS 1.3, Windows Server 2025 élève considérablement le niveau de sécurité des données en transit. Cela atténue de manière significative les risques d'écoute clandestine et de falsification des données d'annuaire, en particulier pour les attributs sensibles comme les mots de passe et les informations d'identification, protégeant directement contre les attaques de l'homme du milieu.

Améliorations de Kerberos (PKINIT, suppression RC4, configuration des types de chiffrement)

Le protocole Kerberos bénéficie également d'améliorations substantielles. L'implémentation du protocole Public Key Cryptography for Initial Authentication in Kerberos (PKINIT) a été mise à jour pour prendre en charge l'agilité cryptographique, permettant plus d'algorithmes et supprimant les algorithmes codés en dur.[6] Le centre de distribution de clés (KDC) Kerberos ne délivrera plus de Ticket Granting Tickets (TGTs) utilisant le chiffrement RC4, tel que RC4-HMAC(NT).[6] De plus, la clé de registre

REG_DWORD SupportedEncryptionTypes n'est plus prise en compte, Microsoft recommandant d'utiliser la stratégie de groupe (GPO) à la place pour la configuration des types de chiffrement pris en charge.[6]

La suppression du chiffrement RC4 pour les TGTs est une réponse directe aux vulnérabilités connues (comme celles exploitées par les attaques de Kerberoasting et Golden Ticket) qui tirent parti de la faiblesse de RC4.[2] En forçant l'utilisation d'algorithmes plus robustes et en centralisant la configuration via GPO, Microsoft renforce la sécurité des tickets Kerberos, rendant ces attaques plus difficiles et plus détectables. Les attaques de Kerberoasting et Golden Ticket reposent fortement sur le craquage des tickets Kerberos, souvent en exploitant des chiffrements plus faibles comme RC4. En éliminant RC4 pour les TGTs et en prenant en charge des algorithmes plus puissants, Windows Server 2025 améliore directement la force cryptographique de Kerberos, un

protocole d'authentification AD essentiel. Cela rend considérablement plus difficile pour les attaquants de craquer les hachages volés hors ligne, réduisant ainsi l'efficacité de ces méthodes d'attaque courantes contre AD.

Sécurité accrue des mots de passe de comptes machine par défaut

Windows Server 2025 améliore la sécurité des comptes machine par défaut. Active Directory utilise désormais des mots de passe de comptes d'ordinateur par défaut générés aléatoirement.[6] Les DCs Windows 2025 bloquent la définition des mots de passe de comptes d'ordinateur sur le nom du compte d'ordinateur par défaut, un comportement qui peut être contrôlé via le paramètre de GPO "Contrôleur de domaine : Refuser de définir le mot de passe par défaut du compte machine".[6] Les utilitaires comme Active Directory Administrative Center (ADAC), Active Directory Users and Computers (ADUC),

net computer, et dsmod respectent également ce nouveau comportement, et ADAC et ADUC ne permettent plus la création de comptes pré-Windows 2000.[6]

Les mots de passe par défaut ou facilement devinables constituent un point d'entrée principal pour les attaquants.[14] En imposant des mots de passe générés aléatoirement pour les comptes machine et en bloquant les mots de passe par défaut faibles, Microsoft s'attaque à un problème fondamental d'hygiène de sécurité au niveau du système d'exploitation dès le déploiement. Cette mesure proactive réduit considérablement le vecteur de compromission initial pour de nombreuses attaques automatisées qui ciblent les informations d'identification par défaut faibles.

Évolutions de Windows LAPS (gestion automatique des comptes, détection de restauration d'image, support des phrases de passe)

Windows LAPS (Local Administrator Password Solution) reçoit plusieurs améliorations cruciales. Il offre désormais une nouvelle gestion automatique des comptes locaux, permettant aux administrateurs informatiques de créer facilement un compte local géré, de personnaliser son nom et de le randomiser pour une sécurité accrue.[6] L'intégration avec les politiques de gestion des comptes locaux existantes de Microsoft est également améliorée.[6]

Une fonctionnalité innovante est la détection de restauration d'image : Windows LAPS détecte désormais les restaurations d'image et, si le mot de passe stocké dans Active Directory ne correspond plus au mot de passe stocké localement sur l'appareil (un état "torn"), il fait pivoter immédiatement le mot de passe.[6] Cette fonctionnalité est activée après l'ajout d'un nouvel attribut de schéma (

msLAPS-CurrentPasswordVersion) et ne nécessite aucune configuration de politique.[6] Enfin, Windows LAPS prend en charge les phrases de passe, permettant la génération de phrases moins complexes mais faciles à lire, à mémoriser et à taper (par exemple, "EatYummyCaramelCandy") à partir de listes de mots intégrées.[6]

Ces évolutions de Windows LAPS sont cruciales pour la gestion sécurisée des comptes administrateurs locaux, un point faible souvent exploité pour le mouvement latéral.[18] Les comptes administrateurs locaux sont fréquemment ciblés pour le mouvement latéral car ils partagent souvent le même mot de passe sur plusieurs systèmes. LAPS y remédie en garantissant des mots de passe uniques et complexes. La détection des restaurations d'image est particulièrement

innovante, car elle résout un problème persistant de désynchronisation des mots de passe, assurant que LAPS reste efficace même après des opérations de récupération ou de déploiement d'images. Cela a un impact direct sur la capacité de l'attaquant à se déplacer au sein du réseau.

Introduction des Comptes de Service Gérés Délégués (dMSA)

Windows Server 2025 introduit les Comptes de Service Gérés Délégués (dMSA), un nouveau type de compte qui permet la migration des comptes de service existants vers des dMSA.[6] Ces nouveaux comptes sont dotés de clés gérées et entièrement randomisées, visant à minimiser les changements d'application tout en désactivant les mots de passe des comptes de service originaux.[6]

Les dMSA sont une évolution significative pour la sécurisation des comptes de service, une cible privilégiée pour les attaques de Kerberoasting.[2] Les comptes de service sont un vecteur d'attaque courant en raison de mots de passe faibles ou statiques. Bien que les comptes de service gérés de groupe (gMSAs) aient déjà amélioré cette situation, les dMSA offrent un chemin de migration pour les comptes de service existants avec des modifications minimales des applications. Cela se traduit directement par une surface d'attaque réduite en automatisant l'hygiène des mots de passe pour une catégorie de comptes historiquement vulnérable, rendant les attaques de Kerberoasting et similaires beaucoup plus difficiles.

Fonctionnalités de Sécurité Système Impactant AD

Credential Guard activé par défaut

Windows Server 2025 renforce la protection des informations d'identification en activant Credential Guard par défaut sur le matériel compatible.[7] Credential Guard offre une protection significativement meilleure contre les attaques de vol d'informations d'identification, telles que Pass-the-Hash ou Pass-the-Ticket, en isolant les secrets dans un conteneur virtualisé que le système d'exploitation lui-même ne peut pas accéder.[7]

L'activation par défaut de Credential Guard est une avancée majeure dans la protection des informations d'identification. Les attaques Pass-the-Hash [10] exploitent la présence de hachages de mots de passe dans la mémoire du processus LSASS. Credential Guard atténue directement ce risque en isolant ces secrets, rendant beaucoup plus difficile pour les attaquants d'extraire les hachages de mots de passe de la mémoire. L'activation par défaut signifie que les organisations bénéficient de cette protection critique sans configuration manuelle, augmentant ainsi considérablement la sécurité de base contre le vol d'informations d'identification et le mouvement latéral subséquent.

Améliorations de la sécurité SMB (signature obligatoire, blocage NTLM)

Des améliorations significatives ont été apportées au Server Message Block (SMB) dans Windows Server 2025. La signature SMB est désormais obligatoire par défaut pour toutes les connexions sortantes, protégeant l'intégrité des données et prévenant les attaques de l'homme du milieu.[7] Le client SMB prend également en charge le blocage NTLM pour les connexions sortantes,

empêchant l'utilisation de ce protocole d'authentification plus ancien et moins sécurisé.[7] De plus, une nouvelle fonctionnalité de limiteur de taux d'authentification SMB aide à prévenir les attaques par force brute contre les serveurs SMB.[7]

Ces améliorations de la sécurité SMB sont essentielles pour durcir les communications réseau, qui sont souvent exploitées pour le mouvement latéral et le vol d'informations d'identification. Les protocoles SMB et NTLM sont fréquemment abusés dans les attaques de mouvement latéral et de vol d'informations d'identification.[7] En rendant la signature SMB obligatoire et en activant le blocage NTLM, Windows Server 2025 s'attaque directement à ces vulnérabilités de longue date. Cela réduit la surface d'attaque pour les attaques réseau courantes et améliore l'hygiène globale du réseau, ce qui est crucial pour protéger AD et ses systèmes joints au domaine.

Hypervisor-Enforced Paging Translation (HVPT)

HVPT (Hypervisor-Enforced Paging Translation) est une fonctionnalité de sécurité matérielle puissante qui applique l'intégrité des traductions d'adresses linéaires.[7] Cette technologie agit comme une protection contre les attaques de type "write-what-where", où un code malveillant tente d'écrire des données arbitraires à des emplacements de mémoire arbitraires. En garantissant que seules les modifications de mémoire autorisées se produisent, HVPT aide à prévenir l'escalade de privilèges et la corruption de données, renforçant ainsi la posture de sécurité globale de Windows Server 2025.[7]

HVPT représente une couche de défense en profondeur au niveau de l'hyperviseur, protégeant contre des techniques d'attaque avancées qui tentent de manipuler la mémoire du système. Bien que n'étant pas directement liée à Active Directory, cette fonctionnalité renforce la sécurité des hôtes sur lesquels les contrôleurs de domaine (DCs) sont exécutés. Les attaquants avancés ciblent souvent la mémoire pour réaliser une escalade de privilèges ou une corruption de données. HVPT opère à un niveau très bas, assisté par le matériel, pour prévenir de telles attaques. Cela rend plus difficile pour les attaquants de compromettre le système d'exploitation sous-jacent et, par extension, les services AD, ajoutant ainsi une couche de défense cruciale pour les contrôleurs de domaine, qui sont les actifs les plus critiques dans un environnement AD.

Hotpatching pour une disponibilité accrue

Windows Server 2025 introduit le Hotpatching, une fonctionnalité qui permet d'installer des mises à jour de sécurité sélectionnées sans avoir à redémarrer le système d'exploitation.[8] Cela promet une installation beaucoup plus rapide des mises à jour et une plus grande disponibilité des systèmes.[8] Bien que certaines mises à jour majeures puissent encore nécessiter des redémarrages, le nombre de redémarrages annuels est sensiblement réduit par rapport aux versions précédentes du serveur.[8]

Le Hotpatching améliore la résilience des contrôleurs de domaine en réduisant les temps d'arrêt pour l'application des correctifs. Les correctifs incomplets et les systèmes obsolètes sont des vulnérabilités courantes.[3] Le Hotpatching y remédie directement en permettant l'application de mises à jour de sécurité critiques sans redémarrage. Cela signifie que les vulnérabilités peuvent être corrigées plus rapidement, minimisant la fenêtre d'exposition aux attaques et contribuant à une posture de sécurité plus agile et réactive. Cette capacité est particulièrement précieuse pour les DCs, qui sont souvent difficiles à mettre hors ligne, garantissant qu'ils peuvent rester protégés

contre les dernières menaces avec une perturbation minimale, améliorant ainsi la sécurité et la disponibilité globales d'AD.

III. Bonnes Pratiques Fondamentales pour le Durcissement d'Active Directory

Gestion des Privilèges et Accès

Le Principe du Moindre Privilège (PoLP) et sa mise en œuvre

Le Principe du Moindre Privilège (PoLP) est un concept de sécurité fondamental qui stipule que les utilisateurs, les programmes et les processus ne devraient disposer que des droits d'accès minimaux nécessaires pour accomplir leurs tâches.[2] Les utilisateurs ayant des privilèges excessifs posent un risque de sécurité important car, si leurs comptes sont compromis, les attaquants peuvent obtenir un point d'appui plus large dans l'environnement.[1]

La mise en œuvre du PoLP implique plusieurs étapes clés :

1. **Séparer les comptes privilégiés et non privilégiés** : Les administrateurs informatiques devraient utiliser des comptes distincts pour leurs fonctions professionnelles non administratives (navigation web, e-mail, travail sur documents) et des comptes dédiés pour les tâches administratives.[26]
2. **Limiter les privilèges des utilisateurs** : Cela nécessite un audit approfondi pour s'assurer que chaque compte utilisateur dispose uniquement des droits nécessaires à la réalisation de son travail.[23] Les autorisations doivent être mises à jour dès que des changements surviennent dans le poste ou les missions d'un collaborateur.[23]
3. **Réduire le nombre d'utilisateurs ayant accès aux comptes administrateurs** : Qu'il s'agisse des comptes administrateurs locaux sur les postes de travail ou des comptes administrateurs de domaine dans Active Directory, le nombre d'utilisateurs ayant accès à ces types de comptes doit être réduit au minimum.[26]

Le PoLP est la pierre angulaire de la sécurité d'Active Directory. Sa mise en œuvre rigoureuse réduit drastiquement la surface d'attaque en limitant l'impact potentiel d'une compromission de compte. De nombreuses attaques, comme Kerberoasting ou Pass-the-Hash, visent à obtenir un accès privilégié.[1] Si les utilisateurs ne disposent que des privilèges minimaux nécessaires, même si leur compte est compromis, l'impact immédiat de l'attaquant est sévèrement limité. Cela force l'attaquant à un effort d'escalade de privilèges plus complexe, augmentant ainsi ses chances de détection.

Gestion des Accès Privilégiés (PAM) et Accès Juste-à-Temps (JIT)

Les solutions de Gestion des Accès Privilégiés (PAM) sont conçues pour restreindre l'accès privilégié, isoler l'utilisation des comptes privilégiés et réduire le risque de vol d'informations d'identification.[1] PAM ajoute une protection aux groupes privilégiés, une surveillance accrue, une

visibilité améliorée et des contrôles plus granulaires, permettant aux organisations de voir qui sont leurs administrateurs privilégiés et ce qu'ils font.[28]

L'Accès Juste-à-Temps (JIT) est une approche dynamique qui accorde des droits d'accès uniquement lorsque cela est spécifiquement requis et pour la période minimale nécessaire.[30] Cette approche réduit considérablement l'exposition des actifs critiques en éliminant les privilèges permanents ("standing privileges").[30] Les avantages du JIT incluent une réduction de la surface d'attaque d'identité, une protection contre l'utilisation abusive des comptes privilégiés et une simplification des processus de conformité et d'audit grâce à des pistes d'audit claires.[30]

L'adoption de PAM et JIT va au-delà du PoLP statique en introduisant un contrôle dynamique et temporel des privilèges. Cela est crucial pour les environnements modernes où les administrateurs ont besoin d'un accès élevé mais intermittent. Les solutions PAM et JIT minimisent la fenêtre d'opportunité pour les attaquants qui ciblent les privilèges permanents. L'accès est accordé juste avant d'être nécessaire et automatiquement révoqué une fois la tâche terminée ou un délai prédéfini écoulé, ou encore en cas d'incident critique.[30] Cela rend beaucoup plus difficile pour les acteurs malveillants de maintenir un accès étendu au sein d'un système.

Mise en place de Postes de Travail à Accès Privilégié (PAW)

Les Postes de Travail à Accès Privilégié (PAW) fournissent un système d'exploitation dédié et durci, protégé des attaques Internet et des vecteurs de menaces courants, pour l'exécution de tâches sensibles.[22] Un principe fondamental de sécurité est de ne jamais administrer un système de confiance à partir d'un hôte moins fiable.[3]

Les PAW sont un élément essentiel du modèle d'administration hiérarchisé, créant une barrière physique et logique entre les tâches administratives sensibles (souvent classées comme Tier 0, les plus critiques) et les activités quotidiennes à risque (Tier 2, postes de travail utilisateurs).[23] Cette isolation empêche le vol d'informations d'identification des comptes privilégiés à partir de postes de travail compromis par des menaces courantes comme le phishing. Les attaquants compromettent souvent les postes de travail des utilisateurs, puis tentent de voler les informations d'identification pour escalader les privilèges vers les serveurs ou les contrôleurs de domaine.[1] Les PAW perturbent directement ces chemins de mouvement latéral et protègent les comptes les plus critiques en garantissant que les informations d'identification privilégiées ne sont jamais exposées sur des machines moins sécurisées.

Modèle d'Administration Hiérarchisé (Tiered Administration)

Le modèle d'administration hiérarchisé de Microsoft implique de séparer les différents éléments de l'infrastructure selon leur degré d'importance.[23] Ce modèle est généralement divisé en trois niveaux :

- **Niveau 0 (Tier 0)** : Inclut les objets les plus critiques, tels que les contrôleurs de domaine, les services de contrôle d'identité (AD FS, PKI) et les maîtres d'opérations de schéma.[23]
- **Niveau 1 (Tier 1)** : Concerne les serveurs et applications.[23]
- **Niveau 2 (Tier 2)** : Comprend les machines des utilisateurs (ordinateurs fixes, portables, terminaux mobiles, etc.).[23]

Pour chaque couche, un compte d'administration différent doit être attribué.[23] Le mouvement latéral est une phase clé de presque toutes les attaques avancées.[1] Le modèle d'administration hiérarchisé y répond directement en segmentant le réseau et les accès en fonction de la criticité. Si un attaquant compromet un poste de travail de Niveau 2, il ne peut pas directement accéder aux contrôleurs de domaine de Niveau 0, car des comptes administratifs distincts et des PAW sont utilisés. Cette approche compartimente le réseau pour contenir les brèches, rendant le mouvement latéral beaucoup plus difficile pour les attaquants en les empêchant d'accéder aux couches plus sensibles à partir de points d'entrée moins critiques.[27]

Politiques de Mots de Passe et Hygiène des Comptes

Politiques de mots de passe modernes (longueur, entropie, phrases de passe)

Les politiques de mots de passe traditionnelles sont souvent insuffisantes face aux attaques modernes, telles que les attaques par "password spraying" où des mots de passe courants sont testés sur de nombreux utilisateurs.[13] Une stratégie plus efficace implique l'élimination des mots de passe courants à l'aide de filtres de mots de passe tiers ou de Microsoft Azure AD Password Protection.[13]

Il est recommandé de privilégier la longueur (un minimum de 14 à 25 caractères) et l'entropie, en incluant des nombres et des caractères spéciaux, et même des phrases de passe (par exemple, "EatYummyCaramelCandy"), qui sont plus faciles à mémoriser pour les utilisateurs mais difficiles à deviner pour les attaquants.[2] Il est déconseillé de forcer l'expiration régulière des mots de passe, car cela peut conduire à des modèles de mots de passe facilement cassables ; les mots de passe ne devraient être mis à jour qu'en cas de brèche ou de compromission avérée.[13] Enfin, l'utilisation de politiques de mots de passe à grain fin (FGPP) permet de définir des exigences de mots de passe plus strictes pour des utilisateurs individuels et des groupes globaux spécifiques.[13]

Des politiques de mots de passe robustes et modernes constituent la première ligne de défense contre les attaques basées sur les informations d'identification, telles que le Kerberoasting et le password spraying. Les informations d'identification volées sont au centre de nombreuses attaques.[3] Les mots de passe faibles facilitent les attaques par force brute et par pulvérisation.[1] Le passage de la complexité arbitraire à l'accent sur la longueur et l'entropie, ainsi que l'utilisation de phrases de passe [6], reconnaissent les limites des politiques traditionnelles, rendant les mots de passe à la fois plus forts et plus faciles à gérer pour les utilisateurs, réduisant ainsi le risque de réutilisation ou de faiblesse et, par conséquent, le taux de réussite des attaques basées sur les informations d'identification.

Authentification Multi-Facteurs (MFA) pour les comptes privilégiés

L'authentification Multi-Facteurs (MFA) ajoute une couche de sécurité supplémentaire en exigeant au moins deux méthodes de vérification pour confirmer l'identité d'un utilisateur.[3] Cela rend l'accès non autorisé significativement plus difficile.[25] La MFA est fortement recommandée pour tous les comptes administratifs et les mécanismes de connexion administrative.[22]

La MFA est une défense critique contre la réutilisation d'informations d'identification volées. Même si un attaquant parvient à obtenir un mot de passe, la MFA empêche l'accès non autorisé,

transformant le vol d'informations d'identification en un vecteur d'attaque beaucoup moins efficace. Les mots de passe, même robustes, peuvent être volés.[13] La MFA agit comme une deuxième ligne de défense cruciale. Si un attaquant a un hachage de mot de passe volé suite à une attaque Pass-the-Hash [10], la MFA peut toujours introduire un défi que l'adversaire ne peut pas surmonter [10], arrêtant efficacement la chaîne d'attaque. C'est un contrôle vital pour les comptes privilégiés.

Sécurisation des comptes de service (mots de passe complexes, gMSAs)

Les comptes de service sont une cible privilégiée pour les attaques de Kerberoasting, une méthode courante pour compromettre les comptes privilégiés et prendre le contrôle d'un serveur AD.[2] Pour contrer cela, les mots de passe des comptes de service doivent être extrêmement difficiles à craquer : ils doivent avoir une longueur minimale de 25 caractères, être complexes et générés avec une forte entropie, puis stockés dans un coffre-fort de mots de passe.[2]

L'utilisation de comptes de service gérés de groupe (gMSAs) est également une bonne pratique, car ils offrent une gestion automatique des mots de passe complexes.[13] La sécurisation des comptes de service est une mesure d'atténuation directe et essentielle contre les attaques de Kerberoasting. L'accent mis sur des mots de passe très longs et l'adoption de gMSAs (et des nouveaux dMSAs dans Windows Server 2025) vise à rendre le craquage hors ligne des hachages de mots de passe de service impraticable, protégeant ainsi un vecteur d'attaque très courant. Les attaques de Kerberoasting sont efficaces car les mots de passe des comptes de service sont souvent faibles et peuvent être craqués hors ligne.[15] En exigeant des mots de passe extrêmement longs, complexes et générés aléatoirement, et en tirant parti des gMSAs ou dMSAs pour la rotation automatisée, le coût et le temps nécessaires à un attaquant pour craquer ces hachages deviennent prohibitifs, neutralisant ainsi ce vecteur d'attaque.

Audit et nettoyage régulier des comptes inactifs

Les comptes d'utilisateurs et de services inactifs représentent un risque de sécurité important, car ils sont souvent non surveillés et peuvent conserver des droits d'accès inutiles.[1] Ces comptes constituent une "mine d'or" pour les attaquants, qui peuvent les compromettre et les utiliser pour maintenir une persistance sans être détectés.

Des audits réguliers et des politiques de nettoyage automatisées sont essentiels pour identifier et désactiver ou supprimer ces comptes dormants.[1] Le nettoyage régulier est une mesure d'hygiène fondamentale qui réduit la surface d'attaque et la complexité de la gestion d'Active Directory, améliorant ainsi la posture de sécurité globale. Les attaquants cherchent une "persistance indétectée".[1] Les comptes inactifs fournissent un vecteur idéal pour cela, car ils sont moins susceptibles d'être surveillés. En auditant et en nettoyant régulièrement ces comptes, les organisations suppriment les portes dérobées potentielles et réduisent le nombre total de cibles disponibles pour un attaquant, rendant l'environnement plus difficile à compromettre et à maintenir un accès.

Sécurisation des Contrôleurs de Domaine (DCs)

Restriction stricte de l'accès aux DCs

La restriction de l'accès aux contrôleurs de domaine (DCs) est cruciale pour atténuer la menace de compromission par malware.[2] Il est impératif d'interdire la navigation web sur les DCs [2] et de configurer les GPOs liées à toutes les unités d'organisation (OUs) des DCs dans une forêt pour ne permettre les connexions RDP (Remote Desktop Protocol) qu'à partir d'utilisateurs et de systèmes autorisés.[2]

Les DCs sont les cibles les plus critiques dans un environnement Active Directory, souvent considérés comme les "joyaux de la couronne".[36] La restriction stricte de leur accès, y compris la prohibition de la navigation web et la limitation des connexions RDP, est une mesure de segmentation essentielle qui réduit considérablement les vecteurs d'attaque directs contre ces actifs de Niveau 0. Autoriser la navigation web ou le RDP sans restriction sur les DCs introduit des vecteurs d'attaque inutiles (par exemple, les téléchargements "drive-by", les malwares). En limitant strictement l'accès, les organisations créent un périmètre durci autour de leurs actifs les plus critiques, rendant beaucoup plus difficile pour les attaquants d'obtenir un contrôle direct.

Désactivation des services non essentiels (Print Spooler, SMBv1, NTLM)

La désactivation des services non essentiels et des protocoles hérités est une mesure de durcissement proactive. Le service Print Spooler, activé par défaut sur les clients et serveurs Windows, présente une vulnérabilité connue qui peut exposer les informations d'identification du compte d'ordinateur du DC.[13] Par conséquent, il est recommandé de le désactiver sur tous les DCs.[13] De même, le protocole SMBv1 est obsolète et vulnérable à de multiples attaques, ce qui justifie sa désactivation sur les DCs.[7] Enfin, bien que cela puisse avoir un impact, il est conseillé de restreindre l'utilisation de NTLM autant que possible en raison de ses risques de sécurité.[7]

La désactivation de ces services et protocoles hérités élimine les points d'entrée connus et les faiblesses architecturales. Cela force l'environnement à utiliser des protocoles plus sécurisés et réduit le nombre de services potentiellement exploitables sur les DCs. Les services et protocoles hérités comme Print Spooler, SMBv1 et NTLM ont des vulnérabilités connues que les attaquants exploitent fréquemment. En les désactivant, les organisations suppriment de manière proactive ces vecteurs d'attaque courants de leurs systèmes les plus critiques (DCs), obligeant les attaquants à trouver des méthodes plus complexes et moins courantes, augmentant ainsi la posture de sécurité globale.

Sécurité physique et utilisation du TPM

La sécurité physique des contrôleurs de domaine est aussi importante que leur sécurité logique.[3] Il est recommandé d'installer les DCs physiques dans des racks ou des cages sécurisés dédiés, séparés de la population générale des serveurs.[2] De plus, la configuration des DCs avec des puces Trusted Platform Module (TPM) est une bonne pratique.[2]

L'utilisation de TPM renforce l'intégrité du processus de démarrage et protège les clés cryptographiques, ajoutant une couche de défense contre les attaques physiques ou les manipulations au niveau du firmware. Si un attaquant obtient un accès physique à un DC, de nombreux contrôles logiques peuvent être contournés. Le TPM ajoute une racine de confiance

matérielle, garantissant que le DC démarre en toute sécurité et que ses clés cryptographiques sont protégées, rendant considérablement plus difficile la falsification du système à un niveau bas.

Sécurité des Forêts et Relations d'Approbation

Filtrage SID sur toutes les approbations de forêt

Le filtrage SID (Security Identifier) est une mesure de sécurité cruciale qui supprime les SID étrangers du jeton d'accès d'un utilisateur, prévenant ainsi les attaques d'escalade de privilèges.[13] Cette mesure est essentielle pour prévenir les attaques où un attaquant pourrait ajouter un SID d'un domaine de confiance (par exemple, le SID d'un membre du groupe Domain Admins) à l'attribut

sIDHistory d'un principal de sécurité dans le domaine de confiance.[13]

Le filtrage SID doit être activé sur toutes les approbations de forêt, sauf si un processus de migration ou de consolidation est activement en cours et que l'attribut sIDHistory est requis.[13] Il est important de noter que certaines erreurs de configuration, comme la définition de

TRUST_ATTRIBUTE_TREAT_AS_EXTERNAL à true ou l'activation de TRUST_ATTRIBUTE_CROSS_ORGANIZATION_ENABLE_TGT_DELEGATION ou TRUST_ATTRIBUTE_PIM_TRUST, peuvent réduire l'efficacité du filtrage SID.[13] Le filtrage SID est une mesure d'atténuation cruciale contre les attaques de "Golden Ticket" et d'autres formes d'escalade de privilèges à travers les relations d'approbation de forêt. Il garantit que les privilèges ne peuvent pas être falsifiés ou hérités de manière inattendue entre les domaines, protégeant ainsi l'intégrité de l'authentification inter-forêts.

Gestion des niveaux fonctionnels de forêt et de domaine

Windows Server 2025 introduit un nouveau niveau fonctionnel pour le support général, qui est requis pour la nouvelle fonctionnalité de taille de page de base de données 32k.[6] Ce nouveau niveau fonctionnel correspond à

DomainLevel 10 et ForestLevel 10 pour les installations sans assistance.[6] La mise à niveau des niveaux fonctionnels débloque de nouvelles fonctionnalités d'Active Directory et des améliorations de sécurité.[9]

La mise à niveau des niveaux fonctionnels n'est pas seulement une formalité, mais un prérequis technique pour activer les fonctionnalités de sécurité avancées de Windows Server 2025. Cela implique que les organisations doivent planifier soigneusement leur processus de mise à niveau des DCs pour s'assurer qu'elles peuvent tirer pleinement parti des nouvelles capacités de durcissement. De nombreuses nouvelles fonctionnalités de sécurité de Windows Server 2025 sont liées aux nouveaux niveaux fonctionnels.[6] Cela signifie que la simple mise à niveau du système d'exploitation pourrait ne pas être suffisante ; les niveaux fonctionnels doivent également être élevés pour débloquer ces améliorations. Cela implique une décision stratégique et un processus de mise à niveau structuré [12] pour garantir que l'organisation puisse pleinement tirer parti des avantages de sécurité de Windows Server 2025.

IV. Défense Active: Détection, Surveillance et Réponse aux Incidents

Surveillance et Audit Proactifs d'Active Directory

L'importance de la surveillance continue pour détecter les activités suspectes

La surveillance vigilante et continue est essentielle pour détecter les accès non autorisés et arrêter une attaque avant que le système ne soit corrompu ou ne subisse des dommages irréparables.[1] Les attaquants exploitent souvent les configurations erronées pour escalader les privilèges et rester indétectés.[13] Une surveillance continue transforme la sécurité d'Active Directory d'une approche réactive à une approche proactive. En détectant les anomalies et les activités suspectes en temps réel, les organisations peuvent réduire considérablement le "temps de présence" et le "temps d'évasion", limitant ainsi les dommages potentiels d'une attaque. Les attaquants cherchent à rester indétectés.[1] La surveillance continue est le mécanisme principal pour contrer cela.[1] En recherchant activement les déviations par rapport au comportement normal, les organisations peuvent identifier et répondre aux menaces avant qu'elles ne s'aggravent, transformant ainsi une brèche potentielle en un incident contenu.

Configuration des stratégies d'audit avancées et des ID d'événements clés

L'audit d'Active Directory est le processus de suivi, d'enregistrement et d'examen des activités au sein de l'environnement AD.[36] Il est crucial de configurer les stratégies d'audit avancées pour collecter des événements de manière granulaire et éliminer le "bruit" des journaux.[3] Bien que l'Observateur d'événements natif de Microsoft puisse être utilisé, ses limitations en termes de capacité de stockage et de clarté des journaux le rendent insuffisant pour un audit complet dans les grandes infrastructures.[38]

Les ID d'événements clés à surveiller fournissent des indicateurs essentiels de compromission. Voici une sélection d'événements critiques et de leur signification pour la surveillance de la sécurité :

ID d'Événement Windows Actuel	ID d'Événement Windows Hérité	Criticité Potentielle	Résumé de l'Événement
4618	N/A	Élevée	Un modèle d'événement de sécurité surveillé s'est produit.
4649	N/A	Élevée	Une attaque par rejeu a été détectée. Peut être un faux positif inoffensif dû à une erreur de configuration.

4719	612	Élevée	La politique d'audit système a été modifiée.
4765	N/A	Élevée	L'historique SID a été ajouté à un compte.
4766	N/A	Élevée	Une tentative d'ajout de l'historique SID à un compte a échoué.
4794	N/A	Élevée	Une tentative de définition du mode de restauration des services d'annuaire a été effectuée.
4897	801	Élevée	La séparation des rôles a été activée.
4964	N/A	Élevée	Des groupes spéciaux ont été attribués à une nouvelle connexion.
5124	N/A	Élevée	Un paramètre de sécurité a été mis à jour sur le service de répondeur OCSP.
N/A	550	Moyenne à Élevée	Attaque par déni de service (DoS) possible.
1102	517	Moyenne à Élevée	Le journal d'audit a été effacé.
4624	528, 540	Moyenne	Connexion réussie à un compte.
4625	529-537, 539	Moyenne	Échec de connexion à un compte.
4634	538	Moyenne	Un compte a été déconnecté.
4648	552	Moyenne	Une connexion a été tentée avec des informations d'identification explicites.
4724	628	Moyenne	Une tentative de réinitialisation du mot de passe d'un compte a été effectuée.
4727	631	Moyenne	Un groupe global à sécurité activée a été créé.
4728	632	Moyenne	Un membre a été ajouté à un groupe global à sécurité activée.

4729	633	Moyenne	Un membre a été supprimé d'un groupe global à sécurité activée.
4735	639	Moyenne	Un groupe local à sécurité activée a été modifié.
4737	641	Moyenne	Un groupe global à sécurité activée a été modifié.
4739	643	Moyenne	La politique de domaine a été modifiée.
4740	644	Moyenne	Un compte d'utilisateur a été verrouillé.
4768	672, 676	Moyenne	Un ticket d'authentification Kerberos (TGT) a été demandé.
4769	673	Moyenne	Un ticket de service Kerberos a été demandé.
4776	680, 681	Moyenne	Le contrôleur de domaine a tenté de valider les informations d'identification d'un compte.
5136	566	Moyenne	Un objet de service d'annuaire a été modifié.
5137	566	Moyenne	Un objet de service d'annuaire a été créé.
5141	N/A	Moyenne	Un objet de service d'annuaire a été supprimé.

La configuration précise des stratégies d'audit avancées et la surveillance ciblée des ID d'événements critiques fournissent l'intelligence nécessaire pour identifier les indicateurs de compromission (IoCs).[39] Cela permet aux équipes de sécurité de passer d'un examen manuel fastidieux à une détection automatisée et priorisée des menaces. En comprenant les ID d'événements spécifiques qui indiquent une compromission (par exemple, les modifications de politique, les ajouts à l'historique SID, les modifications de groupes privilégiés), les organisations peuvent créer des alertes ciblées, transformant les journaux bruts en informations de sécurité exploitables.

Intégration avec les solutions SIEM et ITDR pour une visibilité centralisée

De nombreuses organisations ne parviennent pas à centraliser efficacement leurs journaux d'événements avec des outils SIEM (Security Information and Event Management).[27] Les solutions SIEM sont conçues pour collecter, agréger et analyser les données provenant de diverses sources (applications, périphériques réseau, pare-feu) afin de repérer les menaces et d'identifier la source

des incidents de sécurité.[44] Elles sont cruciales pour la conformité réglementaire et la surveillance des accès privilégiés.[44]

Les outils ITDR (Identity Threat Detection and Response) complètent les SIEM en aidant à atténuer les risques d'exploitation des attaques Pass-the-Hash (PtH) pour le mouvement latéral ou la connexion aux contrôleurs de domaine (DCs).[10] L'intégration d'Active Directory avec les solutions SIEM et ITDR est essentielle pour une détection sophistiquée des menaces. Les journaux AD seuls peuvent ne pas fournir suffisamment de contexte pour détecter des attaques complexes.[38] Ces outils permettent la corrélation d'événements à travers différents systèmes, identifiant des schémas d'attaque complexes (comme le mouvement latéral) qui seraient invisibles dans des journaux isolés, et facilitent une réponse automatisée. Cette vue holistique permet la détection de comportements anormaux et de modèles inhabituels, qui sont des indicateurs clés d'attaques en cours comme le mouvement latéral ou le Kerberoasting.[5]

Comprendre et Atténuer les Vecteurs d'Attaque Courants

Un vecteur d'attaque est la méthode ou la combinaison de méthodes que les cybercriminels utilisent pour pénétrer ou infiltrer le réseau d'une victime.[17] Les attaques peuvent être classées en deux grandes catégories : passives, où l'adversaire surveille le système pour des vulnérabilités sans l'altérer, et actives, où l'adversaire modifie le système ou perturbe son fonctionnement.[17] Comprendre les vecteurs d'attaque courants contre Active Directory est fondamental pour une défense efficace. Cela permet aux organisations de ne pas se contenter de mesures génériques, mais de cibler leurs défenses contre les techniques spécifiques que les attaquants sont connus pour utiliser, optimisant ainsi l'allocation des ressources de sécurité.

Le tableau suivant récapitule les vecteurs d'attaque courants contre Active Directory et les stratégies d'atténuation clés :

Voici un tableau propre et facile à lire qui résume les vecteurs d'attaque courants et les stratégies d'atténuation correspondantes.

Vecteur d'Attaque	Description Succincte de l'Attaque	Stratégies d'Atténuation Clés
Kerberoasting	Un attaquant extrait et craque hors ligne les hachages de mots de passe de comptes de service Active Directory (AD) en demandant des tickets Kerberos pour des **Service Principal Names (SPNs)**.	- Exiger des mots de passe très longs (min. 25 caractères) et complexes pour les comptes de service. - Utiliser des gMSAs ou dMSAs pour une gestion automatique des mots de passe. - Supprimer les SPNs des comptes utilisateurs. - Surveiller les demandes de tickets Kerberos pour détecter les anomalies. - Appliquer le **Principe du Moindre Privilège (PoLP)** aux comptes de service. - Utiliser le chiffrement AES 128/256 bits pour les tickets de service Kerberos.
Pass-the-Hash (PtH)	Un attaquant vole le hachage du mot de passe d'un utilisateur et l'utilise pour créer une nouvelle session sur le même réseau sans connaître le mot de passe réel.	- Limiter l'accès réseau et les privilèges des comptes (PoLP, Zero Trust, PAM, segmentation d'identité). - Activer **Windows Defender Credential Guard** pour isoler les secrets. - Désactiver les hachages Lan Management (LM). - Limiter le nombre de comptes avec des droits d'administrateur. - Ne pas utiliser RDP pour gérer les postes de travail utilisateurs. - Utiliser **Microsoft LAPS** pour des mots de passe administrateur locaux uniques. - Mettre en place des règles de pare-feu pour prévenir les connexions latérales non nécessaires. - Implémenter une solution **ITDR** pour détecter les comportements anormaux.
Golden Ticket	Un attaquant vole le hachage du compte **KRBTGT** pour forger des **Tickets d'Octroi de Tickets (TGTs)** avec des permissions arbitraires, obtenant un accès persistant et illimité au domaine.	- Protéger le compte KRBTGT en réinitialisant son mot de passe deux fois de suite (avec un délai d'au moins 10 heures). - Implémenter le PoLP pour limiter l'exposition des comptes à forte valeur. - Utiliser l'**authentification multifacteur (MFA)**. - Déployer des solutions **EDR** pour détecter les outils d'attaque (ex: Mimikatz). - Surveiller les anomalies dans l'activité Kerberos (TGTs avec des durées de vie inhabituelles, utilisateurs inexistants, etc.). - Durcir la sécurité d'AD avec un modèle architectural hiérarchisé.

Vecteur d'Attaque	Description Succincte de l'Attaque	Stratégies d'Atténuation Clés
		- Contrôler la période de validité des tickets Kerberos.
Attaques DCSync	Un attaquant simule le comportement d'un contrôleur de domaine pour extraire des informations d'identification et d'autres données sensibles d'AD via le protocole **DRS Remote**.	- Implémenter des contrôles d'accès stricts et limiter l'utilisation des comptes à privilèges élevés (PoLP). - Surveiller et auditer les permissions de réplication pour identifier les requêtes inhabituelles ou non autorisées. - Utiliser des méthodes d'authentification robustes comme la MFA. - Mettre à jour et patcher régulièrement les systèmes. - Mener des évaluations de sécurité fréquentes et former le personnel à la sensibilisation à la sécurité.
Mouvement Latéral	Techniques utilisées par un attaquant pour se déplacer plus profondément dans un réseau après un accès initial, cherchant des données sensibles et des actifs de grande valeur.	- Segmentation réseau pour limiter l'accès entre les segments. - Surveiller le comportement des utilisateurs pour détecter les anomalies. - Examiner régulièrement les comptes privilégiés et les comptes de service. - Déployer des systèmes de détection et de prévention des intrusions (**IDS/IPS**) et des solutions EDR. - Implémenter une authentification forte (MFA). - Maintenir une bonne hygiène informatique (patching, mises à jour, suppression des vulnérabilités). - Utiliser des **PAW (Privileged Access Workstations)** pour les tâches administratives. - Utiliser LAPS pour des mots de passe administrateur locaux uniques.

Planification de la Réponse aux Incidents et de la Récupération

Élaboration d'un plan de réponse aux incidents AD détaillé

Même avec les meilleures mesures préventives, les brèches peuvent survenir. La criticité d'Active Directory signifie qu'une compromission est une question de "quand", pas de "si".[1] Par conséquent, l'élaboration d'un plan de réponse aux incidents (IRP) détaillé et testé est un élément essentiel de la résilience cybernétique. Un IRP doit définir son objectif et sa portée, identifier l'équipe de réponse aux incidents de cybersécurité (CSIRT) avec les rôles et responsabilités clairs, et inclure une matrice de classification des risques pour déterminer la gravité et l'urgence des incidents.[49]

Le plan doit également décrire un processus détaillé de réponse aux incidents, comprenant les phases suivantes [49]:

- **Préparation** : Formation des équipes et préparation des systèmes.
- **Détection et Analyse** : Identification et évaluation des événements pour déterminer s'ils nécessitent une escalade.
- **Confinement, Atténuation et Éradication** : Processus pour limiter l'impact de l'incident, remédier et éliminer la menace.
- **Récupération** : Étapes pour restaurer les opérations commerciales normales, souvent en référence à un plan de reprise après sinistre (DRP).
- **Désactivation de l'IRP** : Critères pour désactiver formellement le plan une fois l'incident entièrement contenu et résolu.
- **Activité post-incident** : Documentation des événements historiques, identification de la cause profonde, leçons apprises et intégration des améliorations pour les futures itérations de l'IRP.

Les IRP doivent être révisés et mis à jour au moins une fois par an, ou après des changements significatifs dans l'environnement opérationnel, ou suite à l'exécution simulée ou réelle du plan.[49] Un IRP bien défini et testé permet une réponse rapide et coordonnée, minimisant les temps d'arrêt et les dommages. L'accent mis sur la révision et les mises à jour régulières garantit que le plan reste efficace face à l'évolution des menaces.

Stratégies de sauvegarde et de récupération de forêt AD

Un plan de récupération complet et détaillé d'Active Directory est vital pour la cyber-résilience.[13] Les attaques de ransomware et autres attaques destructrices peuvent paralyser Active Directory, rendant la récupération primordiale.[1] Pour garantir une récupération efficace, il est essentiel de sauvegarder au moins deux contrôleurs de domaine (DCs) par domaine, y compris le domaine racine, et de conserver ces sauvegardes hors ligne pour prévenir l'infection par malware.[13] Les sauvegardes hors ligne sont cruciales pour éviter la réinfection.

La complexité de la récupération d'une forêt AD peut prendre des jours avec les outils natifs.[50] Des solutions tierces peuvent orchestrer et automatiser la récupération de forêt, réduisant le temps de restauration de jours à des heures.[50] Ces solutions simplifient la planification et la préparation, et leurs runbooks flexibles et interactifs facilitent la création et le test régulier du plan de reprise après sinistre d'AD.[50] La capacité à récupérer rapidement et de manière fiable Active Directory

après une attaque est la mesure ultime de la résilience. Les sauvegardes hors ligne et les plans de récupération automatisés sont essentiels pour éviter la réintroduction de malwares et pour restaurer les opérations normales dans les plus brefs délais, un aspect souvent négligé jusqu'à ce qu'il soit trop tard.

V. Conclusion: Vers une Posture de Sécurité AD Résiliente en 2025

La sécurisation active d'Active Directory sous Windows Server 2025 est une entreprise complexe mais indispensable, qui exige une approche stratégique et multicouche. Ce livre blanc a mis en lumière l'importance critique d'Active Directory en tant que pilier central de l'identité et de l'accès, ainsi que les vulnérabilités persistantes qui en font une cible privilégiée pour les cyberattaques. Windows Server 2025 offre une opportunité unique de renforcer cette posture de sécurité grâce à des améliorations fondamentales d'AD DS, à des avancées significatives en matière d'authentification et de gestion des comptes, et à des fonctionnalités de sécurité système qui impactent directement la résilience d'AD.

Les recommandations clés pour une posture de sécurité AD résiliente en 2025 peuvent être synthétisées comme suit :

- **Gestion des privilèges** : Mettre en œuvre rigoureusement le Principe du Moindre Privilège (PoLP), adopter des solutions de Gestion des Accès Privilégiés (PAM) et d'Accès Juste-à-Temps (JIT), et utiliser des Postes de Travail à Accès Privilégié (PAW) dans le cadre d'un Modèle d'Administration Hiérarchisé. Ces mesures réduisent la surface d'attaque et limitent l'impact d'une compromission de compte en compartimentant les accès.
- **Hygiène des comptes et authentification** : Appliquer des politiques de mots de passe modernes axées sur la longueur et l'entropie, y compris les phrases de passe. Déployer l'Authentification Multi-Facteurs (MFA) pour tous les comptes privilégiés. Sécuriser les comptes de service avec des mots de passe complexes et l'utilisation de gMSAs/dMSAs. Effectuer des audits et des nettoyages réguliers des comptes inactifs. Ces pratiques sont la première ligne de défense contre le vol d'informations d'identification.
- **Durcissement des contrôleurs de domaine (DCs)** : Restreindre strictement l'accès aux DCs, désactiver les services non essentiels (Print Spooler, SMBv1, NTLM) et renforcer la sécurité physique des DCs avec l'utilisation du TPM. Ces mesures protègent les actifs les plus critiques de l'environnement AD.
- **Sécurité des forêts et relations d'approbation** : Assurer le filtrage SID sur toutes les approbations de forêt et gérer les niveaux fonctionnels de forêt et de domaine pour activer les fonctionnalités de sécurité les plus récentes.
- **Défense active** : Mettre en place une surveillance et un audit proactifs d'Active Directory en configurant des stratégies d'audit avancées et en surveillant les ID d'événements clés. Intégrer les journaux AD avec les solutions SIEM et ITDR pour une visibilité centralisée et une détection des menaces sophistiquées. Comprendre et atténuer les vecteurs d'attaque courants tels que Kerberoasting, Pass-the-Hash, Golden Ticket, DCSync et le mouvement latéral par des stratégies ciblées.
- **Préparation et récupération** : Élaborer un plan de réponse aux incidents AD détaillé et tester régulièrement les stratégies de sauvegarde et de récupération de forêt AD, en privilégiant les sauvegardes hors ligne.

La sécurité d'Active Directory en 2025 ne repose pas sur une solution unique, mais sur une combinaison stratégique de mesures préventives, de détection proactive et de capacités de réponse robustes. La synergie entre les nouvelles fonctionnalités de Windows Server 2025 et les

meilleures pratiques établies est la clé d'une posture de sécurité résiliente. Le paysage des menaces évolue constamment, ce qui rend l'adaptation et l'amélioration continues impératives pour maintenir une défense efficace.[1] Les organisations doivent adopter une mentalité de "penser comme un attaquant" pour identifier les vulnérabilités.[2] L'intégration d'outils de sécurité avancés (SIEM, EDR, PAM) et la formation continue du personnel sont cruciales pour maintenir un haut niveau de préparation face aux menaces émergentes.[1] La sécurisation active d'Active Directory est un cycle de vie continu d'évaluation, de durcissement, de surveillance, de détection et de réponse. Cet engagement continu est essentiel pour protéger les actifs numériques les plus précieux d'une organisation.

Sources des citations

1. What is Active Directory Security? | CrowdStrike, consulté le juillet 29, 2025, https://www.crowdstrike.com/en-us/cybersecurity-101/identity-protection/active-directory-security/
2. Active Directory Hardening Best Practices | Semperis AD 101, consulté le juillet 29, 2025, https://www.semperis.com/blog/top-active-directory-hardening-strategies/
3. Meilleures pratiques pour la sécurisation d'Active Directory ..., consulté le juillet 29, 2025, https://learn.microsoft.com/fr-fr/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory
4. Best practices for securing Active Directory | Microsoft Learn, consulté le juillet 29, 2025, https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory
5. What is Lateral Movement? | CrowdStrike, consulté le juillet 29, 2025, https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/lateral-movement/
6. What's new in Windows Server 2025 | Microsoft Learn, consulté le juillet 29, 2025, https://learn.microsoft.com/en-us/windows-server/get-started/whats-new-windows-server-2025
7. Overview of Changes and New Security Features in Windows Server 2025 | Mondoo, consulté le juillet 29, 2025, https://mondoo.com/blog/overview-of-changes-and-new-security-features-in-windows-server-2025
8. Windows Server 2025: nouvelles fonctionnalités et améliorations pour l'avenir, consulté le juillet 29, 2025, https://www.firestorm.ch/fr/news/windows-server-2025-nouvelles-fonctionnalites-et-ameliorations-pour-lavenir/
9. Windows Server 2025: Major Enhancements & Step-by-Step Upgrade Guide - Server Simply, consulté le juillet 29, 2025, https://www.serversimply.com/blog/windows-server-2025
10. What is a Pass-the-Hash Attack? | CrowdStrike, consulté le juillet 29, 2025, https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/pass-the-hash-attack/
11. What is a Golden Ticket Attack? - CrowdStrike, consulté le juillet 29, 2025, https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/golden-ticket-attack/
12. Upgrading from Active Directory Forest 2016 to 2025: | by Nathan Vincent | Medium, consulté le juillet 29, 2025, https://medium.com/@zero_4583/upgrading-from-active-directory-forest-2016-to-2025-a-step-by-step-guide-to-upgrade-and-use-new-6b120ae5c02b
13. Active Directory Security Best Practices | Semperis, consulté le juillet 29, 2025, https://www.semperis.com/blog/active-directory-security/active-directory-security-best-practices-checklist/
14. www.lepide.com, consulté le juillet 29, 2025, https://www.lepide.com/blog/top-10-active-directory-attack-methods/

15. What is a Kerberoasting Attack? | CrowdStrike, consulté le juillet 29, 2025, https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/kerberoasting/
16. How to Prevent Kerberoasting Attacks - Lepide Software, consulté le juillet 29, 2025, https://www.lepide.com/blog/how-to-prevent-kerberoasting-attacks/
17. What are Attack Vectors: Definition & Vulnerabilities | CrowdStrike, consulté le juillet 29, 2025, https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/attack-vector/
18. What are pass the hash (PtH) attacks and how to prevent them - Comparitech, consulté le juillet 29, 2025, https://www.comparitech.com/blog/information-security/pass-the-hash-attacks/
19. What Is Lateral Movement? Detect and Prevent It | Exabeam, consulté le juillet 29, 2025, https://www.exabeam.com/explainers/what-are-ttps/what-is-lateral-movement-and-how-to-detect-and-prevent-it/
20. Pass the Hash Attack Defense | AD Security 101 - Semperis, consulté le juillet 29, 2025, https://www.semperis.com/blog/how-to-defend-against-pass-the-hash-attack/
21. Lateral Movement - Timur Engin, consulté le juillet 29, 2025, https://timurengin.com/lateral-movement-813ea27980db
22. Azure Identity Management and access control security best practices - Learn Microsoft, consulté le juillet 29, 2025, https://learn.microsoft.com/en-us/azure/security/fundamentals/identity-management-best-practices
23. 9 bonnes pratiques pour augmenter la sécurité Active Directory - Appvizer, consulté le juillet 29, 2025, https://www.appvizer.fr/magazine/services-informatiques/securite-informatique/securite-active-directory
24. Qu'est-ce que l'APA (Attack Path Analysis) ? | Tenable®, consulté le juillet 29, 2025, https://fr.tenable.com/cybersecurity-guide/learn/attack-path-analysis-apa
25. Active Directory hardening checklist & (actionable) best practices - HackTheBox, consulté le juillet 29, 2025, https://www.hackthebox.com/blog/active-directory-hardening-checklist-and-best-practices
26. Le principe du moindre privilège : la gestion de toutes les connexions d'utilisateurs, consulté le juillet 29, 2025, https://www.isdecisions.com/fr/blog/gestion-d-acces/moindre-privilege-gestion-toutes-connexions-utilisateurs
27. Top Active Directory Security Best Practices - miniOrange, consulté le juillet 29, 2025, https://www.miniorange.com/blog/active-directory-security-best-practices/
28. Privileged Access Management for Active Directory Domain Services | Microsoft Learn, consulté le juillet 29, 2025, https://learn.microsoft.com/en-us/microsoft-identity-manager/pam/privileged-identity-management-for-active-directory-domain-services
29. Privileged Access Management Solutions | One Identity, consulté le juillet 29, 2025, https://www.oneidentity.com/privileged-access-management/
30. What is Just-in-Time (JIT) Access? | CrowdStrike, consulté le juillet 29, 2025, https://www.crowdstrike.com/en-us/cybersecurity-101/identity-protection/just-in-time-access/
31. What is a Golden Ticket Attack and How to Prevent It? - Lepide Software, consulté le juillet 29, 2025, https://www.lepide.com/blog/what-is-a-golden-ticket-attack/
32. Just in Time Access to Active Directory - Entitle, consulté le juillet 29, 2025, https://www.entitle.io/integrations/active-directory
33. Active Directory Tiering Explained: Secure Your AD Now! - Truesec, consulté le juillet 29, 2025, https://www.truesec.com/security/active-directory-tiering
34. Understand and investigate Lateral Movement Paths (LMPs) with Microsoft Defender for Identity, consulté le juillet 29, 2025, https://learn.microsoft.com/en-us/defender-for-identity/understand-lateral-movement-paths

35. What Is Lateral Movement? - Palo Alto Networks, consulté le juillet 29, 2025, https://www.paloaltonetworks.com/cyberpedia/what-is-lateral-movement
36. What is active directory auditing? - CrowdStrike, consulté le juillet 29, 2025, https://www.crowdstrike.com/en-us/cybersecurity-101/identity-protection/active-directory-ad-auditing/
37. Suspicious Active Directory Operations | Vectra AI Detections, consulté le juillet 29, 2025, https://www.vectra.ai/detections/suspicious-active-directory-operations
38. How to view Active Directory (AD) event logs - ManageEngine, consulté le juillet 29, 2025, https://www.manageengine.com/products/active-directory-audit/kb/how-to/how-to-view-ad-logs.html
39. Top 10 Events to Audit in Active Directory to Uncover Security Risks, consulté le juillet 29, 2025, https://petri.com/top-10-events-to-audit-in-active-directory/
40. Configure an Arctic Wolf GPO Advanced Audit Policy, consulté le juillet 29, 2025, https://docs.arcticwolf.com/bundle/m_active_directory/page/configure_an_arctic_wolf_gpo_advanced_audit_policy.html
41. Advanced Audit Policy Configuration | Microsoft Learn, consulté le juillet 29, 2025, https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn452415(v=ws.11)
42. Appendix L - Events to Monitor | Microsoft Learn, consulté le juillet 29, 2025, https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/appendix-l--events-to-monitor
43. Event ID AD Account login - Microsoft Q&A, consulté le juillet 29, 2025, https://learn.microsoft.com/en-us/answers/questions/1529208/event-id-ad-account-login
44. SIEM Integration best practices | ADAudit|Plus - ManageEngine, consulté le juillet 29, 2025, https://www.manageengine.com/products/active-directory-audit/kb/best-practices/siem-integration-best-practices.html
45. Kerberos Attack: How to Stop Golden Tickets? - Varonis, consulté le juillet 29, 2025, https://www.varonis.com/blog/kerberos-how-to-stop-golden-tickets
46. Persistence Attack in Active Directory: The Golden Ticket Attack - CovertSwarm, consulté le juillet 29, 2025, https://www.covertswarm.com/post/the-golden-ticket-attack
47. Complete Guide: Understanding and Preventing DCSync Attacks - NinjaOne, consulté le juillet 29, 2025, https://www.ninjaone.com/blog/dcsync-attacks/
48. Securing Against DCSync Attacks | Fidelis Security, consulté le juillet 29, 2025, https://fidelissecurity.com/cybersecurity-101/cyberattacks/dcsync-attack/
49. What Is an Incident Response Plan (IRP)? - Palo Alto Networks, consulté le juillet 29, 2025, https://www.paloaltonetworks.com/cyberpedia/incident-response-plan
50. Forest Recovery for Active Directory (Enterprise Edition) - Commvault Cloud Documentation, consulté le juillet 29, 2025, https://docs.metallic.io/metallic/forest_recovery_for_active_directory_enterprise_edition.html