ACTIVE DIRECTORY

Attribution des droits utilisateurs

Gestion des comptes, des habilitations et des groupes de sécurité pour un accès adapté et sécurisé au Système d'Information

Direction	Direction des Systèmes d'Information (DSI)
Classification	INTERNE — Confidentiel
Version	2.0
Date	20 April 2026
Auteur	Responsable Sécurité & Identité numérique

Table des matières

1. Introduction et enjeux de l'Active Directory

L'Active Directory (AD) de Microsoft est le service d'annuaire central de la plupart des systèmes d'information d'entreprise. Il constitue la colonne vertébrale de la gestion des identités numériques, des authentifications et des autorisations d'accès aux ressources informatiques. Une mauvaise gestion des droits dans l'AD représente l'une des principales surfaces d'attaque exploitées lors des incidents de sécurité.

1.1 Rôle de l'AD dans le système d'information

L'Active Directory remplit plusieurs fonctions critiques au sein du système d'information :

- Centralisation de l'**authentification** : vérification de l'identité de chaque utilisateur et machine.
- **Autorisation** : contrôle de l'accès aux ressources en fonction des groupes et des stratégies appliquées.
- **Administration** des stratégies de groupe (GPO) appliquées aux postes de travail et serveurs.
- **Annuaire d'entreprise** : référentiel unique des utilisateurs, groupes, ordinateurs et services.
- Support de la **confiance inter-domaines** pour les architectures multi-forêts.

1.2 Principes fondamentaux de sécurité

Principe	Description	Application AD
Moindre privilège	N'accorder que les droits strictement nécessaires à l'exercice des fonctions.	Groupes de sécurité granulaires, révision régulière
Séparation des pouvoirs	Séparer les rôles d'administration et d'utilisation.	Comptes admin dédiés, délégation fine
Besoin d'en connaître	L'accès n'est accordé que si justifié par le poste ou la mission.	Validation RH + Responsable métier
Défense en profondeur	Multiplier les couches de contrôle d'accès.	MFA + audit + alertes SIEM
Traçabilité	Toute action doit être journalisée et attribuable.	Journaux d'audit AD, SIEM

1.3 Cadre réglementaire et conformité

La gestion des droits dans l'Active Directory s'inscrit dans un cadre réglementaire et normatif auquel l'entreprise doit se conformer :

• RGPD (Règlement Général sur la Protection des Données)

Impose de limiter l'accès aux données personnelles au strict nécessaire (minimisation). Les droits doivent être documentés et révisés.

• ISO 27001 / 27002

Exige la mise en œuvre d'un contrôle d'accès formel, la gestion du cycle de vie des comptes et la revue périodique des privilèges.

• Directive NIS2

Renforce les obligations de sécurité pour les opérateurs de services essentiels, notamment sur la gestion des accès privilégiés.

• SOX / PCI-DSS

Imposent la séparation des fonctions et la traçabilité des accès aux systèmes financiers et de paiement.

• ANSSI — Guide d'hygiène informatique

Recommande la limitation des comptes à privilèges, la désactivation rapide des comptes sortants et l'audit régulier des droits.

2. Architecture de l'Active Directory

2.1 Domaines, forêts et unités d'organisation (OU)

L'Active Directory est organisé selon une hiérarchie logique qui conditionne directement l'application des stratégies de groupe et la délégation administrative :

Forêt (Forest)

Périmètre de sécurité ultime de l'AD. Contient un ou plusieurs domaines. Les forêts séparées sont utilisées pour isoler des entités avec des niveaux de confiance différents.

Domaine

Unité administrative principale. Partage une base de données commune et des politiques de sécurité uniformes. Un domaine correspond généralement à une entreprise ou une filiale.

Arborescence (Tree)

Ensemble de domaines partageant un espace de noms DNS continu, liés par des relations de confiance transitives bidirectionnelles.

Unité d'Organisation (OU)

Conteneur logique permettant de regrouper des objets (utilisateurs, ordinateurs, groupes) pour y appliquer des GPO et déléguer l'administration.

Site AD

Représentation logique de la topologie réseau physique. Optimise la réplication des contrôleurs de domaine et l'authentification Kerberos.

2.2 Structure des objets AD

Type d'objet	Attributs clés	Usage principal
Utilisateur (User)	sAMAccountName, UPN, objectSID, memberOf	Représente un individu physique ou fonctionnel
Ordinateur (Computer)	dNSHostName, operatingSystem, lastLogon	Objets machines joints au domaine
Groupe (Group)	groupType, member, memberOf	Regroupement pour l'attribution de droits
Unité d'org. (OU)	ou, gPLink, managedBy	Conteneur d'administration
Compte de service (gMSA)	msDS-ManagedPassword, servicePrincipalName	Comptes pour les services Windows
Contact	mail, telephoneNumber	Représentation d'entités externes (annuaire)
Stratégie de groupe (GPO)	gPCFileSysPath, versionNumber	Politiques appliquées aux objets

2.3 Catalogue global et réplication

Le **Catalogue Global (GC)** est un contrôleur de domaine qui stocke une copie partielle de tous les objets de la forêt. Il est indispensable pour les authentifications cross-domaines et la résolution des appartenances aux groupes universels. La réplication AD s'appuie sur le protocole **DRSUAPI** et utilise

un modèle multi-maître : chaque contrôleur de domaine peut recevoir des modifications, qui sont ensuite propagées. Certaines opérations restent centralisées sur les rôles **FSMO** (Flexible Single Master Operations).

■ Rôles FSMO critiques : PDC Emulator (politiques de mots de passe, heure), RID Master (génération des SID), Schema Master (modifications de schéma), Domain Naming Master (ajout/suppression de domaines), Infrastructure Master (références inter-domaines). La perte d'un rôle FSMO sans procédure de reprise peut bloquer l'authentification.

3. Gestion des comptes utilisateurs

3.1 Cycle de vie d'un compte

Chaque compte utilisateur suit un cycle de vie structuré, piloté conjointement par la Direction des Ressources Humaines et la DSI. Une gestion rigoureuse de ce cycle est indispensable pour éviter l'accumulation de comptes orphelins ou sur-habilités.

1. Création

Déclenchée par le service RH à l'arrivée d'un collaborateur. Le compte est créé selon le gabarit du profil métier. Les droits initiaux sont attribués via les groupes de sécurité correspondant au rôle.

2. Activation

Le compte est activé le jour de l'arrivée. Le mot de passe initial est communiqué de façon sécurisée. L'utilisateur est contraint de le modifier à la première connexion.

3. Modification

Tout changement de poste, de service ou de mission donne lieu à une révision des droits. L'ancien profil est retiré et le nouveau appliqué (principe de clean slate pour éviter l'accumulation de droits résiduels).

4. Suspension

En cas d'absence longue durée (congé maternité, longue maladie, mise à pied), le compte est désactivé. Les données sont conservées.

5. Désactivation

À la fin du contrat, le compte est désactivé immédiatement le dernier jour (ou dès notification RH). Le compte n'est pas supprimé immédiatement pour préserver la traçabilité des actions passées.

6. Archivage / Suppression

Après une période de conservation définie (généralement 3 à 12 mois selon la politique interne), le compte est supprimé et ses ressources archivées ou transférées.

3.2 Politique de nommage et d'identité

Une politique de nommage cohérente facilite l'administration et améliore la lisibilité de l'annuaire. Voici les conventions recommandées :

Type de compte	Format recommandé	Exemple	Remarque
Utilisateur standard	p.nom (initiale + nom)	j.dupont	Max 20 caractères (sAMAccountName)
Compte administrateur local	adm-p.nom	adm-j.dupont	Compte séparé, non utilisé au quotidien
Compte admin de domaine	da-p.nom	da-j.dupont	Usage strictement limité à l'administration AD
Compte de service	svc-nomservice	svc-sqlprod	Préférer les gMSA ou sMSA quand possible
Compte applicatif	app-nomapp	app-erp2024	Créé par la DSI, géré par l'équipe applicative

Type de compte	Format recommandé	Exemple	Remarque
Compte générique	gen-usage	gen-accueil	Utilisation exceptionnelle, traçabilité renforcée

3.3 Comptes de service et comptes privilégiés

Les comptes de service et les comptes à privilèges représentent les cibles prioritaires des attaquants. Leur gestion doit être particulièrement rigoureuse :

- **Group Managed Service Accounts (gMSA)** : comptes dont le mot de passe est géré automatiquement par l'AD (rotation toutes les 30 jours). Solution recommandée pour tous les services Windows.
- **Comptes admin de domaine (Domain Admins)** : groupe à effectif minimal. Chaque membre doit être justifié. Connexion uniquement depuis des postes d'administration sécurisés (PAW).
- **Privileged Access Workstation (PAW)** : poste dédié à l'administration, sans accès Internet ni messagerie, protégé par des GPO restrictives.
- **Just-In-Time (JIT) Administration** : les droits élevés sont accordés temporairement à la demande via des solutions comme Microsoft PAM ou CyberArk, puis révoqués automatiquement.
- **Credential Guard** : fonctionnalité Windows qui protège les secrets LSASS contre l'extraction via des attaques de type Pass-the-Hash ou Pass-the-Ticket.

> DANGER — Les comptes Domain Admins ne doivent JAMAIS être utilisés pour des tâches courantes (consultation de mails, navigation web, etc.). Chaque administrateur doit disposer d'un compte standard pour son usage quotidien et d'un compte admin séparé pour les tâches d'administration.

3.4 Comptes inactifs et désactivation

La détection et la gestion des comptes inactifs est un processus continu essentiel à la sécurité de l'annuaire :

Seuil d'inactivité	Action recommandée	Responsable
30 jours sans connexion	Alerte envoyée au manager du compte	SIEM / Script PowerShell
60 jours sans connexion	Désactivation automatique du compte	DSI (automatisé)
90 jours sans connexion	Déplacement vers OU 'Comptes-Désactivés'	DSI
180 jours sans connexion	Archivage des données et suppression du compte	DSI + RH
Compte de service inactif	Désactivation immédiate après vérification applicative	DSI + Équipe applicative

4. Groupes de sécurité et habilitations

4.1 Types de groupes AD

L'Active Directory distingue deux dimensions pour les groupes : leur **type** (sécurité ou distribution) et leur **étendue** (portée de la visibilité et de l'utilisation).

Étendue	Membres acceptés	Peut être utilisé dans	Usage recommandé
Local de domaine (Domain Local)	Utilisateurs, groupes globaux, universels de tout domaine de la forêt	ACL du domaine local uniquement	Attribuer des permissions sur les ressources locales
Global	Utilisateurs et groupes globaux du même domaine	ACL dans toute la forêt	Regrouper des utilisateurs d'un même domaine partageant le même rôle
Universel	Utilisateurs, groupes globaux et universels de tout domaine de la forêt	ACL dans toute la forêt	Multi-domaines ; attention à l'impact sur le catalogue global

4.2 Stratégie AGDLP / AGUDLP

Microsoft recommande la stratégie **AGDLP** (Account - Global group - Domain Local group - Permission) pour structurer l'attribution des droits. Cette approche garantit la maintenabilité et l'évolutivité de la gestion des accès :

A — Account (Compte utilisateur)

Le compte individuel de l'utilisateur est ajouté dans un groupe Global, jamais directement dans une ACL.

G — Global Group (Groupe Global)

Regroupe des comptes utilisateurs partageant le même rôle métier (ex : GG-ComptaFournisseurs). Ce groupe est ajouté dans un groupe Domain Local.

DL — Domain Local Group (Groupe Local de Domaine)

Groupe sur lequel les permissions effectives sont attribuées (ex : DL-Partage-Comptabilite-RW). C'est ce groupe qui est placé dans les ACL des ressources.

P — Permission

Droit effectif attribué sur la ressource (lecture, écriture, contrôle total, etc.). Les permissions sont appliquées au groupe DL, jamais directement aux utilisateurs.

> ✔ Avantages de l'AGDLP : modification d'un droit = modification d'un seul groupe DL. Ajout d'un utilisateur = ajout dans le groupe GG de son rôle. Audit simplifié : les groupes DL reflètent directement les permissions sur les ressources.

4.3 Modèle de délégation des droits

La délégation permet de confier certaines tâches d'administration à des responsables métier ou à des assistants techniques sans leur accorder les droits d'administrateur de domaine. Elle s'applique au niveau des OU :

Tâche déléguée	Étendue recommandée	Groupe bénéficiaire
Réinitialiser les mots de passe	OU du service concerné	HelpDesk-N1
Déverrouiller les comptes	OU du service concerné	HelpDesk-N1
Créer / Modifier des utilisateurs	OU RH — périmètre RH uniquement	GestionnairesRH
Gérer les membres d'un groupe	Groupe(s) spécifiques	Responsables métier
Joindre des ordinateurs au domaine	OU Ordinateurs du service	Tech-Support
Lire les attributs AD	Domaine entier (lecture seule)	Auditeurs-SI
Gérer les GPO d'une OU	OU spécifique	Admins-GPO

4.4 Gestion des groupes imbriqués

L'imbrication de groupes (groupe dans un groupe) est une pratique puissante mais qui peut rapidement devenir ingérable si elle n'est pas encadrée :

- **Documenter chaque imbrication** dans un référentiel de groupes mis à jour en temps réel.
- **Limiter la profondeur d'imbrication** à 3 niveaux maximum pour conserver la lisibilité.
- **Éviter les groupes circulaires** (groupe A membre de B, B membre de A) qui peuvent provoquer des comportements imprévisibles.
- **Revoir régulièrement** les imbrications lors des audits trimestriels.
- **Utiliser des outils de visualisation** (BloodHound en mode défensif, AD Topology Diagrammer) pour cartographier les chemins d'accès.

5. Attribution et gestion des droits d'accès

5.1 Droits sur les ressources (fichiers, dossiers, partages)

L'attribution des droits sur les ressources de fichiers est l'une des activités les plus fréquentes et les plus sensibles. Elle repose sur la combinaison des **droits de partage NTFS** et des **permissions au niveau du partage réseau**.

Règle fondamentale : appliquer des droits restrictifs au niveau du partage réseau (ex : Contrôle total pour les administrateurs, Lecture/Écriture pour les utilisateurs) et affiner via les ACL NTFS. En cas de conflit, c'est la permission la plus restrictive des deux niveaux qui s'applique.

Permission NTFS	Hérite ?	Lecture	Écriture	Exécution	Suppression	Modifier ACL
Contrôle total	Oui	✔	✔	✔	✔	✔
Modifier	Oui	✔	✔	✔	✔	✘
Lecture et exécution	Oui	✔	✘	✔	✘	✘
Lecture seule	Oui	✔	✘	✘	✘	✘
Écriture seule	Oui	✘	✔	✘	✘	✘
Affichage du contenu	Non	Partiel	✘	✘	✘	✘

5.2 Droits sur les applications métier

Pour chaque application métier (ERP, CRM, GED, outils métier spécifiques), un référentiel d'habilitations doit être tenu à jour. Ce référentiel précise :

- Les **rôles fonctionnels** disponibles dans l'application (lecteur, contributeur, valideur, administrateur).
- La **correspondance avec les groupes AD** qui contrôlent l'accès à ces rôles.
- Le **processus de demande et de validation** (qui peut demander, qui valide, qui crée le droit).
- La **durée de validité** des accès accordés, notamment pour les accès temporaires.
- Les **exigences de sécurité** spécifiques (MFA obligatoire, accès uniquement depuis le réseau interne, etc.).

5.3 Droits d'administration et délégation

Les droits d'administration dans l'AD sont organisés en niveaux de privilèges croissants. Chaque niveau doit être attribué au nombre minimal de personnes :

Niveau	Groupe(s) AD	Périmètre	Nb max recommandé
Helpdesk N1	HelpDesk-ResetPwd	Réinitialisation MDP, déverrouillage	Selon effectif support
Admin OU métier	OUAdmin-[Service]	Gestion des comptes du service	2 par service
Admin serveurs	Admins-Serveurs	Administration des serveurs (non DC)	5-10 personnes

Niveau	Groupe(s) AD	Périmètre	Nb max recommandé
Admin domaine	Domain Admins	Administration complète du domaine	3-5 personnes MAX
Admin de schéma	Schema Admins	Modification du schéma AD	1-2 personnes MAX
Admin de forêt	Enterprise Admins	Administration de toute la forêt	1-2 personnes MAX

5.4 Least Privilege et séparation des pouvoirs

Le principe du moindre privilège (Least Privilege) est le fondement de toute politique d'accès sécurisée. Il se traduit concrètement par plusieurs pratiques :

- **Aucun droit par défaut** : un nouveau compte ne reçoit que les droits du groupe de base de son département.
- **Droits basés sur le rôle** (RBAC — Role-Based Access Control) : l'appartenance à un groupe de rôle détermine les accès.
- **Revue systématique lors des changements de poste** : les droits de l'ancien poste sont retirés avant l'attribution des nouveaux.
- **Pas d'accumuluation silencieuse** : les appartenances aux groupes sont auditées trimestriellement.
- **Séparation des environnements** : production, recette et développement ont des groupes et des accès séparés.
- **Validation croisée** : un droit d'accès sensible nécessite la double validation du manager et de la DSI.

6. Politiques de mots de passe et d'authentification

6.1 Fine-Grained Password Policy (FGPP)

Les Fine-Grained Password Policies permettent d'appliquer des politiques de mots de passe différenciées selon les groupes d'utilisateurs, en dérogation à la politique de domaine par défaut (Default Domain Policy). Elles sont applicables à partir de Windows Server 2008 et se configurent via des objets PSO (Password Settings Object).

Paramètre PSO	Comptes standard	Comptes admin	Comptes de service
Longueur minimale	12 caractères	16 caractères	25 caractères (aléatoire)
Complexité obligatoire	Oui	Oui	Oui
Durée de vie max	90 jours	60 jours	Gérée auto (gMSA)
Durée de vie min	1 jour	1 jour	N/A
Historique des MDP	12 derniers	24 derniers	N/A
Priorité (Precedence)	100	10	5
Verrouillage (seuil)	10 tentatives	5 tentatives	3 tentatives
Durée de verrouillage	15 minutes	30 minutes	Manuelle

✔ Recommandation ANSSI / NIST : privilégier la longueur sur la complexité. Un mot de passe de 16 caractères composé de mots communs est plus sûr qu'un mot de passe court avec des caractères spéciaux. Les passphrases sont à encourager.

6.2 Authentification multi-facteurs (MFA)

Le MFA est désormais indispensable pour sécuriser les accès, en particulier pour les comptes à privilèges et les accès distants. Il repose sur la combinaison d'au moins deux facteurs parmi :

- **Connaissance** : mot de passe, code PIN.
- **Possession** : token TOTP (Google Authenticator, Microsoft Authenticator), carte à puce, clé FIDO2 (YubiKey).
- **Inhérence** : empreinte digitale, reconnaissance faciale (Windows Hello for Business).

Périmètre d'application recommandé du MFA :

Contexte d'accès	MFA obligatoire ?	Méthode recommandée
Accès VPN / Remote Desktop (RDP)	OUI	TOTP ou FIDO2
Portails d'administration (Azure AD, GPO, etc.)	OUI	FIDO2 / Carte à puce
Accès aux applications métier critiques	OUI	TOTP / Push mobile
Accès aux ressources internes (réseau local)	Recommandé	Windows Hello / Kerberos

Contexte d'accès	MFA obligatoire ?	Méthode recommandée
Connexion au poste de travail standard	Optionnel	Windows Hello for Business
Comptes de service (gMSA)	N/A	Pas d'authentification interactive

6.3 Politique de verrouillage des comptes

La politique de verrouillage protège contre les attaques par force brute. Elle doit être calibrée pour allier sécurité et confort d'utilisation :

- Configurer le **seuil de verrouillage** à 5-10 tentatives échouées (selon le niveau de sensibilité du compte).
- Utiliser une **fenêtre d'observation** (Observation Window) de 15-30 minutes pour réinitialiser le compteur.
- Appliquer un **déverrouillage automatique** après 15-30 minutes pour les comptes standard, manuel pour les comptes admin.
- Mettre en place des **alertes temps réel** en cas de verrouillage répété d'un même compte (attaque potentielle ou DoS).
- Distinguer les verrouillages **légitimes** (utilisateur qui a oublié son MDP) des verrouillages **suspects** (tentatives depuis des IP inconnues).

7. Processus de gestion des habilitations

7.1 Procédure d'entrée (onboarding)

La procédure d'onboarding définit le processus de création et d'initialisation d'un compte utilisateur à l'arrivée d'un nouveau collaborateur. Elle doit être déclenchée au minimum 5 jours ouvrés avant l'arrivée effective.

Étape 1 — Notification RH

Le service RH émet une demande de création de compte via le système de ticketing (ITSM) en précisant : nom complet, poste, service, responsable, date d'arrivée, type de contrat.

Étape 2 — Validation

Le responsable hiérarchique valide la demande et précise les accès nécessaires. Pour les accès sensibles, une validation additionnelle de la DSI est requise.

Étape 3 — Création du compte

La DSI crée le compte AD selon la politique de nommage, l'affecte à l'OU du service, applique le gabarit du profil métier et attribue les groupes de sécurité correspondants.

Étape 4 — Attribution des équipements

Le poste de travail est préparé, joint au domaine, et les logiciels métier déployés via SCCM/Intune.

Étape 5 — Activation et communication

Le compte est activé le jour J. Le mot de passe initial est transmis de façon sécurisée (SMS ou remise en main propre). L'utilisateur est informé de la politique de sécurité.

Étape 6 — Clôture du ticket

Un email de confirmation est envoyé au RH et au manager. Le ticket ITSM est clos avec documentation des accès accordés.

7.2 Procédure de sortie (offboarding)

L'offboarding est la procédure la plus critique en termes de sécurité. Un compte non désactivé après un départ représente un risque majeur (utilisation malveillante par l'ex-employé ou exploitation par un attaquant).

Immédiatement (J0)

- Désactivation du compte AD dès confirmation du départ par RH.
- Révocation des sessions actives (invalidation des tokens Kerberos/NTLM).
- Désactivation des accès VPN et accès distants.
- Changement des mots de passe des comptes génériques partagés connus de l'utilisateur.

Sous 24h (J+1)

- Transfert des données et de la messagerie vers le manager ou successeur.
- Sauvegarde du profil utilisateur et archivage.
- Notification aux applications métier nécessitant une gestion manuelle des accès.
- Récupération des équipements (badge, PC, téléphone, token MFA).

Sous 7 jours (J+7)

- Vérification de la suppression des accès dans toutes les applications métier.
- Audit des groupes AD dont l'utilisateur était membre.
- Clôture du ticket ITSM avec documentation complète.

Sous 30 jours (J+30)

- Suppression ou archivage du compte AD selon la politique interne.
- Libération de la licence logicielle associée.

> ■ En cas de départ conflictuel ou de mise à pied immédiate, la DSI doit être notifiée en priorité pour désactiver le compte AVANT que l'employé soit informé de son départ, afin d'éviter toute action malveillante.

7.3 Revue périodique des droits (re-certification)

La revue des habilitations (ou re-certification des accès) est un processus périodique permettant de vérifier que chaque utilisateur dispose uniquement des droits nécessaires à l'exercice de ses fonctions actuelles.

Périmètre	Fréquence	Responsable de validation	Outils
Groupes de sécurité (tous)	Trimestrielle	Manager + DSI	Script PowerShell, AD Reports
Comptes à privilèges (Admin)	Mensuelle	RSSI + DSI	PAM, CyberArk
Accès aux applications critiques	Semestrielle	Responsable applicatif + RH	ITSM, IAM
Comptes de service	Semestrielle	DSI	Script AD, CMDB
Comptes inactifs (> 30j)	Mensuelle	DSI (automatisé)	Script PowerShell automatisé
Droits sur les partages de fichiers	Annuelle	Manager + DSI	File Server Audit

7.4 Gestion des accès temporaires et exceptions

Certains accès ont une durée de vie limitée ou constituent des exceptions à la politique standard. Ces cas doivent être gérés avec une rigueur accrue :

- **Accès pour un prestataire externe** : compte créé dans une OU dédiée, limité dans le temps (date d'expiration obligatoire), avec accès minimal nécessaire à la mission.
- **Accès temporaire pour un projet** : création d'un groupe de projet temporaire, dissolution automatique à la fin du projet.
- **Escalade d'urgence (Break Glass)** : comptes d'urgence ultra-privilégiés dont le mot de passe est scellé dans un coffre physique ou numérique. Toute utilisation déclenche une alerte immédiate.
- **Exception documentée** : tout accès dérogatoire doit être documenté avec justification, valideur et date de fin, et intégré dans la revue périodique.

8. Audit, traçabilité et supervision

8.1 Journalisation des événements AD

L'activation de l'audit dans l'Active Directory est une obligation réglementaire et un prérequis indispensable à la détection des incidents. Les événements clés à surveiller dans les journaux Windows Security sont :

ID Événement	Description	Niveau de priorité
4624	Connexion réussie	Moyen
4625	Échec de connexion	ÉLEVÉ
4648	Connexion avec credentials explicites (runas)	ÉLEVÉ
4720	Création d'un compte utilisateur	ÉLEVÉ
4722 / 4725	Activation / Désactivation de compte	ÉLEVÉ
4728 / 4732 / 4756	Ajout d'un membre dans un groupe (Global/Local/Universel)	ÉLEVÉ
4740	Verrouillage d'un compte	ÉLEVÉ
4756 / 4757	Modification d'un groupe de sécurité	Moyen
4768 / 4769	Demande de ticket Kerberos (TGT / TGS)	Moyen
4771	Échec Kerberos Pre-Authentication	ÉLEVÉ
4776	Tentative de validation NTLM	Moyen
5136 / 5141	Modification / Suppression d'un objet AD	CRITIQUE
4673 / 4674	Utilisation de privilèges sensibles	CRITIQUE

8.2 Outils de supervision et alertes

- **SIEM (Security Information and Event Management)**

Centralise et corrèle les journaux de tous les contrôleurs de domaine. Permet la création de règles d'alerte automatiques (ex : ajout dans Domain Admins, multiples échecs d'auth depuis la même IP). Solutions : Microsoft Sentinel, Splunk, IBM QRadar, Elastic SIEM.

- **ATA / Defender for Identity (Microsoft)**

Solution dédiée à la détection des attaques ciblant l'AD (Pass-the-Hash, Pass-the-Ticket, Golden Ticket, DCSync, reconnaissance Kerberos). Analyse le trafic réseau AD et les journaux pour détecter les comportements anormaux.

- **Microsoft Entra ID Protection**

Pour les environnements hybrides ou cloud (Azure AD), détecte les connexions risquées, les comptes compromis et applique des politiques d'accès conditionnelles.

- **Scripts PowerShell d'audit**

Permettent des vérifications régulières et automatisées : comptes inactifs, membres des groupes sensibles, droits sur les OU, GPO orphelines, etc.

- **BloodHound (mode défensif)**

Outil de cartographie des chemins d'élévation de privilèges. Utilisé par les équipes défensives pour identifier les raccourcis d'élévation dans la configuration AD et les corriger avant qu'un attaquant ne les exploite.

8.3 Rapports de conformité

Des rapports périodiques doivent être produits pour garantir la traçabilité et répondre aux exigences des auditeurs internes et externes :

Rapport	Contenu	Fréquence	Destinataires
Comptes AD	Liste complète, statut, dernière connexion	Mensuel	DSI, RSSI
Groupes à privilèges	Membres des groupes Admin, DA, EA	Mensuel	DSI, RSSI, DG
Comptes inactifs	Comptes sans connexion > 30/60 jours	Mensuel	DSI, RH
Revue des habilitations	Résultats de la re-certification	Trimestriel	RSSI, Audit interne
Incidents IAM	Verrouillages, anomalies, alertes SIEM	Mensuel	DSI, RSSI
Rapport de conformité	Écarts par rapport à la politique de sécurité	Semestriel	RSSI, DG, Audit

9. Bonnes pratiques et recommandations

Sécuriser le Tier 0 (Contrôleurs de domaine)

- Isoler les DC sur des VLAN dédiés, inaccessibles depuis les postes utilisateurs.
- Limiter les services installés sur les DC au strict minimum (pas d'antivirus tiers, pas d'applications métier).
- Appliquer des GPO de durcissement sur les DC (CIS Benchmark, ANSSI).
- Auditer régulièrement les accès aux DC et les changements de configuration.

Sécuriser les comptes à privilèges

- Imposer l'utilisation de PAW (Privileged Access Workstation) pour toute administration.
- Mettre en œuvre une solution PAM (Privileged Access Management) pour les comptes critiques.
- Implémenter le modèle de niveau d'administration Microsoft (Tier 0 / Tier 1 / Tier 2).
- Activer Protected Users Security Group pour les comptes admin (désactive NTLM, Kerberos RC4, délégation).

Durcir l'Active Directory

- Désactiver NTLM v1 et v2 sur l'ensemble du parc dès que possible.
- Activer SMB Signing pour se protéger contre les attaques de relais NTLM.
- Désactiver le spooler d'impression (PrintSpooler) sur les DC.
- Activer les fonctionnalités de protection LSASS (RunAsPPL, Credential Guard).
- Appliquer les niveaux fonctionnels les plus élevés supportés par l'infrastructure.

Maintenir l'hygiène de l'annuaire

- Nettoyer régulièrement les groupes vides, les GPO orphelines, les comptes inutilisés.
- Documenter chaque groupe de sécurité (description, responsable, usage).
- Tenir à jour un inventaire des comptes de service et de leurs applications associées.
- Revoir les héritages de permissions NTFS suite aux réorganisations d'équipes.

Former et sensibiliser

- Former les administrateurs AD aux attaques courantes (Kerberoasting, AS-REP Roasting, DCSync).
- Sensibiliser les utilisateurs aux risques du phishing ciblé visant les identifiants AD.
- Organiser des exercices de simulation d'attaque (Red Team AD) pour évaluer la résilience.
- Publier et maintenir à jour la charte informatique et la politique de sécurité des mots de passe.

10. Annexes

10.1 Matrice des droits par profil

Tableau de correspondance entre les profils métier et les groupes de sécurité AD associés :

Profil métier	Groupes AD	Ressources accessibles	Niveau de droits
Collaborateur standard	GG-Collaborateurs, GG-[Service]	Partage réseau du service, applications métier de base, messagerie	Lecture / Écriture sur son espace
Manager / Responsable	GG-Managers, GG-[Service]-Managers	Idem collaborateur + rapports RH, tableaux de bord, accès lecture équipe	Lecture étendue
Comptabilité / Finance	GG-Finance, GG-Compta	ERP Financier, partages financiers, outils de reporting	Lecture / Écriture selon rôle
RH	GG-RH, GG-RH-Sensible	SIRH, données personnelles, partages RH confidentiels	Lecture / Écriture + données sensibles
Administrateur IT N1	HelpDesk-N1, HelpDesk-ResetPwd	Console helpdesk, reset MDP, déverrouillage comptes	Admin délégué (OU utilisateurs)
Administrateur IT N2	Admins-Serveurs, Tech-Support	Serveurs applicatifs, infrastructure réseau, outils de monitoring	Admin local serveurs
Administrateur AD	Domain Admins (compte séparé)	Contrôleurs de domaine, structure AD, GPO	Admin domaine complet
Prestataire externe	GG-Prestataires-[Mission]	Ressources spécifiques à la mission uniquement	Lecture / accès limité

10.2 Commandes PowerShell essentielles

› Lister les membres d'un groupe

```
Get-ADGroupMember -Identity 'Domain Admins' -Recursive | Select Name,
SamAccountName
```

› Lister les groupes d'un utilisateur

```
Get-ADPrincipalGroupMembership -Identity 'j.dupont' | Select Name
```

› Comptes inactifs depuis 60 jours

```
Search-ADAccount -AccountInactive -TimeSpan 60.00:00:00 -UsersOnly | Select
Name, LastLogonDate
```

› Désactiver un compte utilisateur

```
Disable-ADAccount -Identity 'j.dupont'
```

› Créer un compte utilisateur

```
New-ADUser -Name 'Jean Dupont' -GivenName 'Jean' -Surname 'Dupont'
-SamAccountName 'j.dupont' -UserPrincipalName 'j.dupont@domaine.fr' -Path
'OU=Comptabilite,OU=Utilisateurs,DC=domaine,DC=fr' -AccountPassword
(Read-Host -AsSecureString) -Enabled $true
```

› Ajouter un utilisateur dans un groupe

```
Add-ADGroupMember -Identity 'GG-Finance' -Members 'j.dupont'
```

› Lister tous les comptes avec MDP n'expirant pas

```
Get-ADUser -Filter {PasswordNeverExpires -eq $true} -Properties
PasswordNeverExpires | Select Name, SamAccountName
```

› Rapport des comptes verrouillés

```
Search-ADAccount -LockedOut | Select Name, SamAccountName, LockedOut,
LastLogonDate
```

› Exporter la liste des groupes et membres

```
Get-ADGroup -Filter * | ForEach-Object { $g = $_.Name Get-ADGroupMember $_ |
Select @{N='Groupe';E={$g}}, Name, SamAccountName } | Export-Csv
'groupes_membres.csv' -NoTypeInformation
```

10.3 Glossaire

Terme	Définition
ACL	Access Control List — Liste de contrôle d'accès définissant les permissions sur un objet.
AD	Active Directory — Service d'annuaire de Microsoft pour la gestion des identités et des accès.
AGDLP	Account - Global group - Domain Local group - Permission. Stratégie de gestion des groupes recommandée par Microsoft.
DA / EA	Domain Admins / Enterprise Admins — Groupes aux privilèges les plus élevés de l'AD.
FGPP / PSO	Fine-Grained Password Policy / Password Settings Object — Politique de mots de passe granulaire.
FSMO	Flexible Single Master Operations — Rôles AD nécessitant un maître unique.
gMSA	Group Managed Service Account — Compte de service à mot de passe géré automatiquement.
GPO	Group Policy Object — Stratégie de groupe appliquée aux objets AD.
IAM	Identity and Access Management — Gestion des identités et des accès.
JIT	Just-In-Time — Accès accordé temporairement à la demande puis révoqué automatiquement.
Kerberoasting	Attaque ciblant les comptes de service avec SPN pour extraire et cracker leurs tickets Kerberos.
LSASS	Local Security Authority Subsystem Service — Processus Windows gérant l'authentification locale.
MFA	Multi-Factor Authentication — Authentification à plusieurs facteurs.
NTLM	NT LAN Manager — Protocole d'authentification Windows, moins sécurisé que Kerberos.
OU	Organizational Unit — Unité d'organisation, conteneur logique dans l'AD.
PAM	Privileged Access Management — Solution de gestion et de supervision des accès privilégiés.
PAW	Privileged Access Workstation — Poste de travail dédié à l'administration sécurisée.
RBAC	Role-Based Access Control — Contrôle d'accès basé sur les rôles.
RSSI	Responsable de la Sécurité des Systèmes d'Information.
SID	Security Identifier — Identifiant unique d'un objet AD (utilisateur, groupe, ordinateur).
SIEM	Security Information and Event Management — Outil de centralisation et d'analyse des journaux de sécurité.
SPN	Service Principal Name — Identifiant unique d'un service dans Kerberos.
UPN	User Principal Name — Identifiant de connexion sous la forme utilisateur@domaine.