ALCINOUS SANDJAY

AUDIT DE SECURITE

ACTIVE DIRECTORY

BUT-RT3

UNIVERSITÉ DE LA RÉUNION

Table des matières

1. CONTEXTE DE LA MISSION

Cette mission d'audit, commanditée par la Direction des Systèmes d'Information (DSI) de TAAFictive, s'inscrit dans une démarche de sécurisation offensive du Système d'Information. L'objectif est d'évaluer la surface d'attaque interne réelle. Il s'agit ici d'établir un diagnostic technique de la robustesse de l'infrastructure, au-delà de la simple conformité théorique. Le cœur du réseau repose sur une architecture Microsoft standardisée, centrée autour des Services de Domaine Active Directory (AD DS) hébergés sur un contrôleur de domaine en Windows Server 2022. En tant que pilier de l'infrastructure, ce service centralise la gestion des identités et assure l'intégrité des mécanismes d'authentification ainsi que la distribution des autorisations d'accès aux ressources critiques et applicatives du parc.

La sécurité de l'Active Directory constitue un enjeu prioritaire. Comme le soulignent les rapports de l'ANSSI, la majorité des cyberattaques abouties exploitent une compromission de l'AD pour effectuer des mouvements latéraux et obtenir une élévation de privilèges (Domain Admin). La perte de contrôle de cet annuaire exposerait TAAFictive à des risques critiques, allant du déploiement massif de rançongiciels à l'exfiltration de données sensibles, compromettant directement la continuité d'activité.

2. OBJECTIFS DE L'AUDIT

Cette mission a pour objectif principal d'évaluer la sécurité du domaine Active Directory à travers trois axes majeurs :

État des lieux de la configuration : Il s'agit dans un premier temps de réaliser une analyse technique du contrôleur de domaine à l'instant T. L'enjeu est de mesurer l'écart entre la configuration actuelle de l'infrastructure et les standards de sécurité attendus (bonnes pratiques Microsoft).

Détection des anomalies et défauts d'hygiène : L'audit se focalise sur l'identification des mauvaises configurations plutôt que sur la recherche de vulnérabilités logicielles pures (CVE). L'analyse vise à remonter les dérives d'administration courantes qui affaiblissent le niveau de sécurité global : comptes non désactivés, délégations de droits hasardeuses ou privilèges excessifs.

Préconisations et durcissement : Enfin, l'audit doit déboucher sur un plan d'action opérationnel. L'objectif est de fournir une liste de recommandations pour permettre aux équipes de durcir le système, en se référant sur les référentiels de l'ANSSI (notamment le guide de sécurisation AD).

3. PÉRIMÈTRE DE L'AUDIT

La délimitation précise du périmètre technique est un prérequis pour garantir la pertinence de l'analyse et le respect des délais impartis.

L'audit se concentre exclusivement sur le domaine **taaf.audit.re**, dont l'architecture repose sur un contrôleur de domaine exécutant Windows Server 2022. L'investigation couvre la structure globale de l'annuaire et la sécurité logique associée. Cela inclut l'examen approfondi des comptes utilisateurs et administratifs, la gestion des privilèges, ainsi que les politiques de sécurité appliquées par défaut ou via les Stratégies de Groupe (GPO).

L'analyse s'étend également à la couche protocolaire et au système. Une attention particulière est portée aux protocoles d'authentification actifs, aux configurations réseau propres à l'Active Directory, ainsi qu'à l'intégrité des objets du domaine, notamment la détection de comptes inactifs ou obsolètes.

L'audit ne couvre pas la sécurité physique des salles serveurs ni celle des équipements d'infrastructure périmétrique comme les pare-feux, les routeurs ou les concentrateurs

VPN. De même, la couche applicative hébergée sur les serveurs membres est exclue du champ d'analyse, tout comme la réalisation de tests d'intrusion externes.

4. MÉTHODOLOGIE

Phase 1 : Cadrage et préparation

Cette étape a permis d'établir le cadre légal et technique de l'intervention. Le périmètre exact (**taaf.audit.re**) ainsi que les fenêtres d'intervention ont été validés en amont avec la DSI pour garantir la continuité de service. Les référentiels de conformité, dont le guide d'hygiène et le document **DAT-NT-17 de l'ANSSI**, ont été sélectionnés pour servir de base normative à l'évaluation.

Phase 2 : Collecte des données

L'objectif de cette phase consiste à récupérer un maximum d'informations sur l'état du système, sans altération de la configuration existante. L'extraction des données techniques a été réalisée via l'outil spécialisé **PingCastle** en mode "Healthcheck".

Phase 3 : Analyse et tests techniques

Cœur technique de l'audit, cette étape repose sur le croisement des résultats automatisés avec des vérifications manuelles approfondies. Chaque alerte remontée par l'outil à donner une validation directe dans la console Active Directory afin d'éliminer les faux positifs. La réalité des droits d'accès a également été éprouvée par la simulation du comportement d'un utilisateur standard, permettant de confirmer la faisabilité technique de certains vecteurs d'attaque.

Phase 4 : Évaluation des risques

Une vulnérabilité technique ne constitue un risque avéré que si elle est exploitable et impactante. Chaque écart constaté a donc été qualifié selon une matrice de criticité (Gravité x Vraisemblance). Cette méthode permet de hiérarchiser les résultats et de

distinguer les simples non-conformités des risques critiques exigeant une action corrective immédiate. Ces tableaux de niveau de risques se trouvent dans la partie “ANALYSE ET DIAGNOSTIC”.

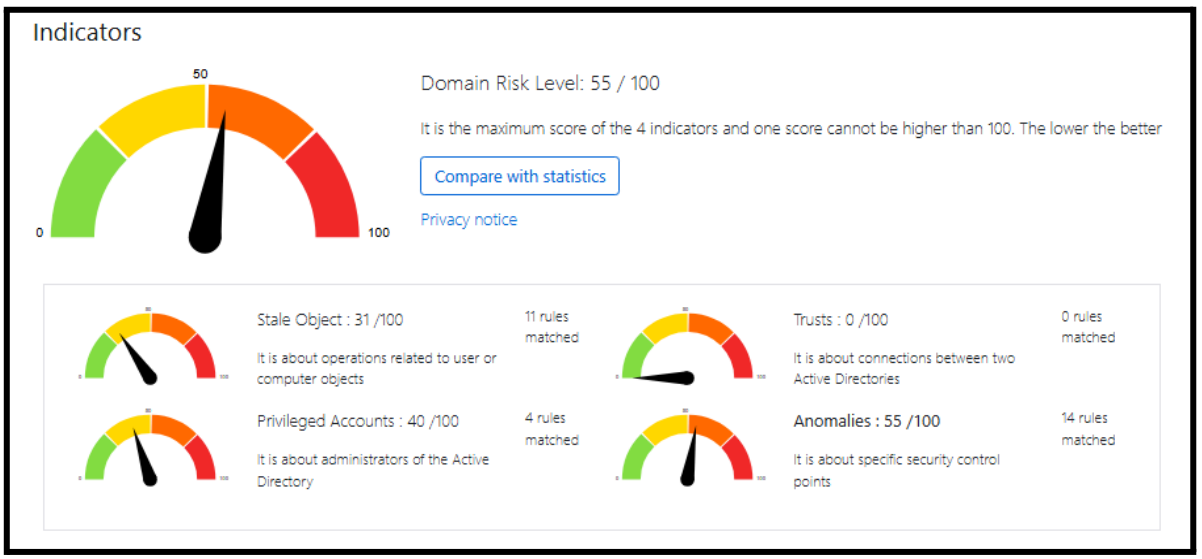
Phase 5 : Reporting et restitution

La phase finale synthétise l'ensemble des observations au sein du présent rapport. Elle contient la traduction des éléments techniques en enjeux stratégiques pour la direction, tout en fournissant les procédures de remédiation opérationnelles nécessaires aux équipes techniques pour le durcissement de l'infrastructure.

5. RÉSULTATS DE L’AUDIT

5.1. Indicateurs de Risque PingCastle

L'exécution de l'outil d'analyse PingCastle sur le domaine **taaf.audit.re** a permis de générer une cartographie précise des vulnérabilités. Le score de risque global calculé par l'algorithme de l'outil place le domaine dans une zone préoccupante avec un score de 55/100. Ce score reflète l'accumulation de mauvaises pratiques qui fragilisent l'ensemble de la sécurité de l’Active Directory.

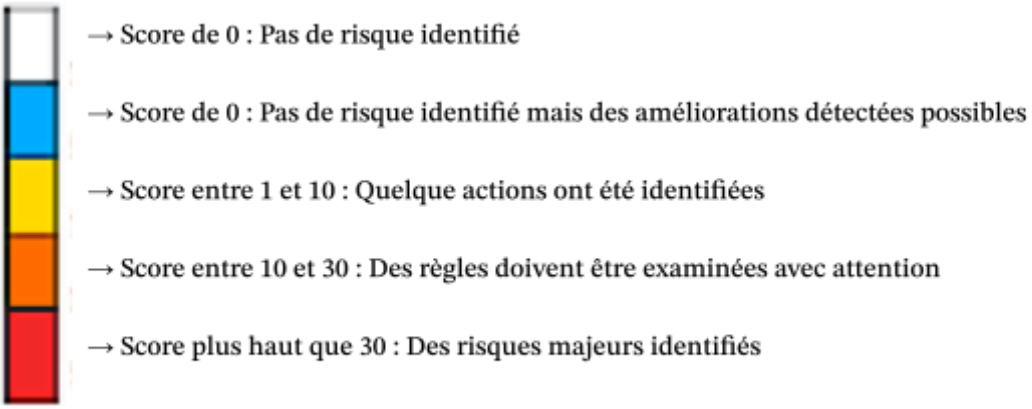


5.2. Détails du Risk Model

L'analyse PingCastle a révélé un niveau de risque global de 55/100, correspondant à un niveau de risque modéré. Ce score global se décompose selon les quatre catégories d'indicateurs suivantes :

Catégorie	Score	Niveau de risque
Stale Objects	31/100	Risques majeurs identifiés
Privileged Accounts	40/100	Des règles doivent être examinées avec attention
Trusts	0/100	Pas de risque identifié
Anomalies	55/100	Risques majeurs identifiés

Légende d'interprétation des scores :



Le domaine **taaf.audit.re** a été segmenté par ces quatres catégories d'indicateurs permettant de comprendre la menace niveau sécurité de l'Active Directory :

A. Anomalies :

Cette catégorie présente le score le plus critique de l'audit. Ce résultat de 55/100 signale l'existence de configurations s'écartant significativement des standards de sécurité. L'analyse met en évidence **la divulgation d'informations sensibles** où le champ "Description" de certains objets utilisateurs est utilisé pour stocker des données confidentielles (telles que des codes d'accès physiques), rendant ces informations lisibles par l'ensemble des utilisateurs du réseau. Et **la gestion des mots de passe** dont l'attribut *PasswordNeverExpires* (Le mot de passe n'expire jamais) est activé sur plusieurs comptes, ce qui contrevient aux règles d'hygiène de base. Ces anomalies constituent des vecteurs d'attaque triviaux exploitables par un acteur interne malveillant.

B. Privileged Accounts :

Cet indicateur évalue la sécurité des comptes disposant de droits d'administration. Un score de 40/100, bien qu'intermédiaire, révèle une structure de privilèges inadéquate. Ce niveau de risque résulte d'une gestion trop permissive du groupe "Administrateurs du domaine". L'audit révèle la présence de comptes non techniques (notamment celui du Directeur Général, dgeneral) au sein de ce groupe critique. Cette configuration constitue une violation du principe de moindre privilège. L'augmentation du nombre d'administrateurs élargit mécaniquement la surface d'attaque : la compromission d'un seul de ces comptes par ingénierie sociale donnerait à l'attaquant un contrôle total sur le domaine.

C. Stale Objects :

Cet indicateur mesure l'hygiène numérique de l'Active Directory, en ciblant les objets obsolètes (comptes utilisateurs ou ordinateurs inactifs depuis une longue période).

D. Trusts :

Cette catégorie analyse les relations d'approbation avec d'autres domaines ou forêts Active Directory.

6. ANALYSE ET DIAGNOSTIC

6.1. Synthèse des forces et faiblesses :

L'exploitation de **Windows Server 2022** permet à l'infrastructure de bénéficier des derniers standards en matière de cryptographie et de protection du noyau. Par ailleurs, une structuration logique est visible dans l'architecture des Unités d'Organisation (OU), reflétant un effort de segmentation par départements (RH, Direction, Comptabilité).

Cependant, ces acquis techniques sont fragilisés par des **faiblesses structurelles** dans les pratiques d'administration. L'analyse révèle un arbitrage systématique en faveur de la facilité d'usage au détriment de la sécurité. La gestion des comptes à privilèges constitue le point le plus critique : l'absence de ségrégation entre les rôles "métier" (Directeur) et les rôles "techniques" (Administrateur) crée un point de défaillance unique (SPOF).

6.2. Interprétation :

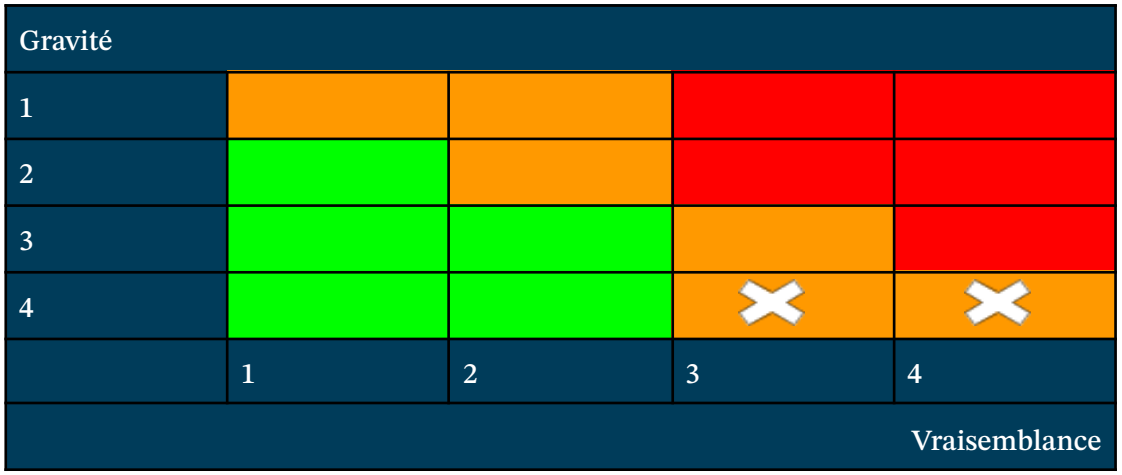
L'analyse de deux scénarios concrets, basés sur les mauvaises configurations détectées, permet d'illustrer la matérialité du risque.

Cas n°1 : Compromission d'un compte hybride (Compte "dgeneral") :

Ce compte cumule une activité bureautique standard (navigation web, messagerie) et une appartenance au groupe hautement critique "Administrateurs du Domaine". **Risque projeté :** L'exposition de ce compte est maximale. En cas d'ouverture d'une

pièce jointe malveillante (phishing) ou de navigation sur un site compromis, le code malveillant s'exécute immédiatement avec les privilèges les plus élevés du domaine. L'attaquant disposerait alors instantanément des droits nécessaires pour neutraliser les solutions antivirus, détruire les sauvegardes en ligne et déployer un rançongiciel sur l'intégralité du parc.

Tableau de niveau de risque 1 :



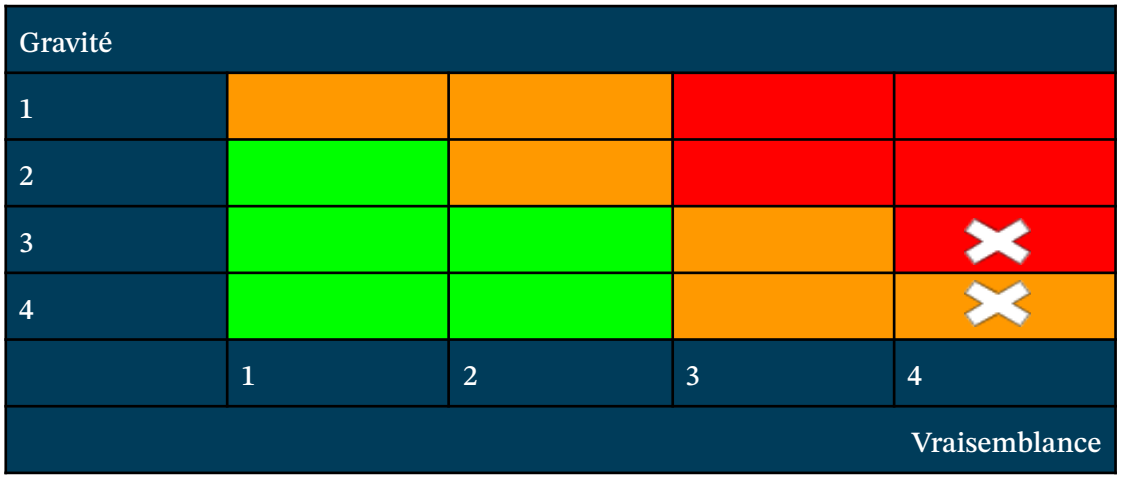
Vraisemblance (3/4) : C'est élevé car un Directeur peut être piégé par un mail de phishing.

Gravité (4/4) : C'est critique car si ce compte est piraté, l'attaquant devient maître du domaine. Il peut tout chiffrer avec un ransomware.

Cas n°2 : Fuite d'information et persistance (Compte "saudit") :

Ce compte présente une double anomalie : l'option "Le mot de passe n'expire jamais" est active, et l'attribut public "Description" contient une donnée sensible ("Code porte entrée : 9988"). **Risque projeté :** Tout attaquant ayant un accès, même restreint, au réseau (interne ou via Wi-Fi) peut interroger l'annuaire et récupérer ce code d'accès physique. Par ailleurs, la non-expiration du mot de passe offre une fenêtre temporelle illimitée pour mener une attaque par force brute lente (*password spraying*), constituant un vecteur idéal pour établir un accès persistant et discret au système d'information.

Tableau de niveau de risque 2 :



Vraisemblance (4/4) : C'est certain (100%). Il n'y a même pas besoin d'attaquer, l'information est écrite en clair. N'importe quel employé curieux peut la lire.

Gravité (3/4) : C'est majeur car cela donne un accès physique aux locaux, ce qui peut entraîner des vols de matériel, mais cela ne permet pas forcément de détruire tout le système informatique à distance.

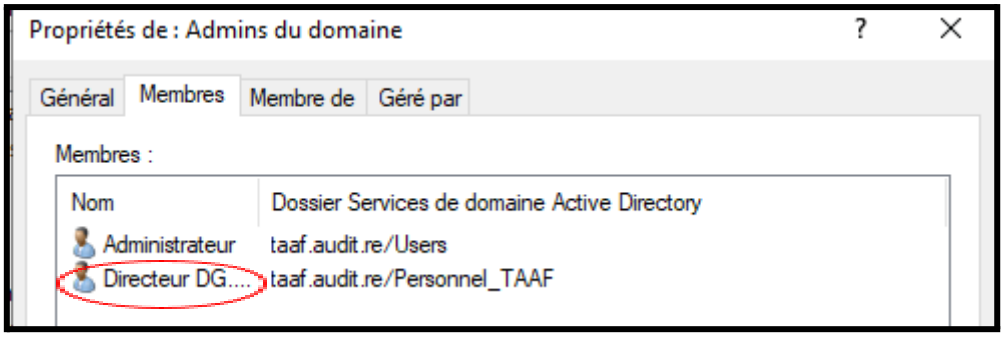
7. DÉTAILS DES VULNÉRABILITÉS IDENTIFIÉES

Les failles identifiées sont présentées ci-après selon le format PRIR : (Périmètre, Résumé du risque, Impact, Recommandation).

V1 : Violation du principe de moindre privilège

Périmètre : Active Directory / Groupes de Sécurité / **Domain Admins**

Risque : Lors de l'analyse du groupe hautement critique "Administrateurs du domaine", nous avons identifié la présence du compte utilisateur **dgeneral** (Directeur Général). L'analyse des journaux d'événements montre que ce compte est utilisé quotidiennement pour des activités bureautiques (navigation web, messagerie), ce qui l'expose directement aux menaces externes.



Impact : Le niveau de criticité est maximal (**CRITIQUE**). En cas de compromission de ce compte (via un mail de phishing ou un téléchargement malveillant), l'attaquant hérite immédiatement des droits d'administration totale sur le domaine. Il peut alors déployer un rançongiciel (ransomware) sur l'ensemble du parc informatique, chiffrant serveurs et sauvegardes.

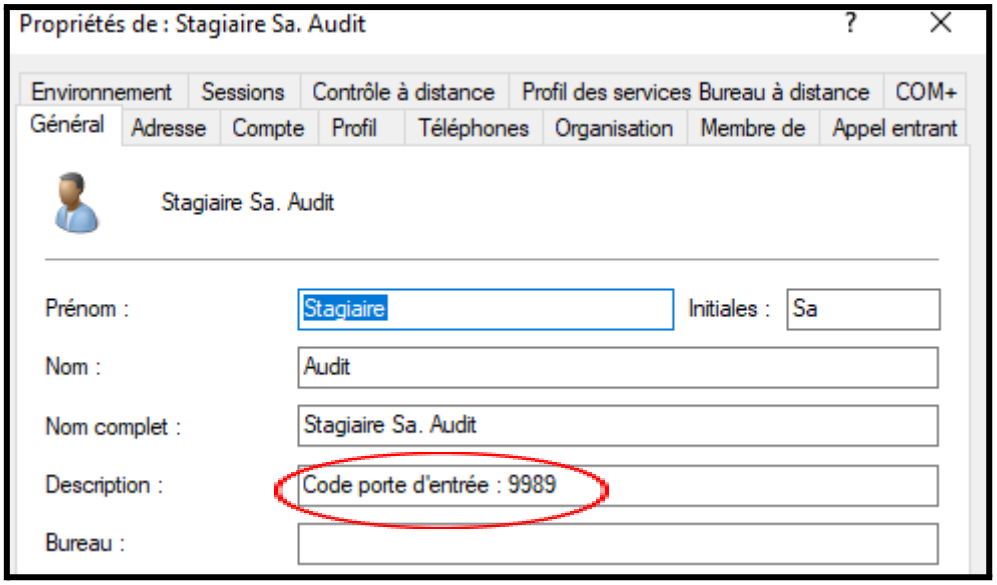
Recommandation :

1. **Immédiat :** Retirer le compte **dgeneral** du groupe "Domain Admins".
2. **Cible :** Créer un compte d'administration dédié (ex: **adm_dgeneral**) qui ne possède ni boîte mail ni accès internet, à n'utiliser que pour les tâches de maintenance serveur.

V2 : Fuite d'informations sensibles en clair

Périmètre : Active Directory / Objets Utilisateurs / Attribut **Description**

Description (Risque) : L'audit des attributs publics de l'annuaire a révélé que des informations confidentielles sont stockées en clair. Spécifiquement, le compte de l'utilisateur **saudit** contient la chaîne de caractères : *"Code porte entrée : 9988"* dans son champ **Description**. Par défaut, cet attribut est lisible par n'importe quel utilisateur authentifié sur le réseau, sans droits d'administration.



Impact : Le niveau de criticité est **ÉLEVÉ**. Cette fuite d'information compromet la sécurité physique des locaux de l'entreprise. Un stagiaire, un prestataire ou un attaquant interne peut récupérer ce code pour s'introduire dans des zones restreintes (salle serveur, bureaux direction) et voler du matériel ou accéder physiquement aux machines.

Recommandation :

1. **Immédiat :** Supprimer le contenu du champ description via la commande PowerShell : **Set-ADUser saudit -Description $null**.
2. **Prévention :** Sensibiliser les équipes IT à ne jamais utiliser les champs AD comme bloc-notes pour des secrets.

V3 : Absence de rotation des mots de passe

Périmètre : Active Directory / Configuration des comptes

Description (Risque) : L'outil d'audit PingCastle a relevé que plusieurs comptes utilisateurs (notamment saudit et les comptes du service RH) ont l'attribut **PasswordNeverExpires** positionné à True. Cela signifie que ces utilisateurs ne sont jamais forcés de changer leur mot de passe, même après plusieurs années.

```
PS C:\Users\Administrateur> Get-ADUser -Filter
{PasswordNeverExpires -eq $true} | Select Name
Name
Administrateur
Invité
Directeur DG. General
Stagiaire Sa. Audit
Sandjay SAl. Alcinous
```

Impact : Le niveau de criticité est **MAJEUR**. Si un mot de passe est faible ou s'il a été compromis dans une fuite de données précédente, il reste valide indéfiniment. Cela laisse une fenêtre d'opportunité illimitée à un attaquant pour mener une attaque par force brute (Brute Force) lente et discrète.

Recommandation :

1. **Correction :** Exécuter un script pour forcer l'expiration sur tous les comptes concernés.
2. **Politique :** Appliquer une GPO imposant un changement de mot de passe tous les 90 jours (valeur recommandée par l'ANSSI pour les comptes standard).

V4 : Présence de comptes obsolètes (Stale Objects)

Périmètre : Active Directory / Hygiène du parc

Description (Risque) : L'audit a mis en évidence un grand nombre de comptes utilisateurs (ex: RH_User_01 à RH_User_20) créés il y a plus de 90 jours mais n'ayant jamais enregistré de connexion. Ces comptes sont considérés comme des "comptes zombies".

Impact : Le niveau de criticité est **MOYEN**. Ces comptes augmentent inutilement la surface d'attaque. Ils peuvent servir de porte dérobée (Backdoor) à un attaquant qui les réactiverait discrètement pour se maintenir dans le réseau. Étant "oubliés" des administrateurs, leur activité suspecte risque de ne pas être détectée.

Recommandation : Mettre en place un processus de nettoyage automatisé :

1. Désactiver automatiquement les comptes inactifs depuis plus de 180 jours.
2. Supprimer les comptes désactivés depuis plus de 1 an.

V5 : Cycle de vie de l'OS

Périmètre : Infrastructure / Système d'Exploitation

Description (Risque) : Le contrôleur de domaine fonctionne sous **Windows Server 2022**. Bien qu'actuellement supporté, la fin de support standard (*Mainstream Support*) est fixée par Microsoft au **13 octobre 2026**.

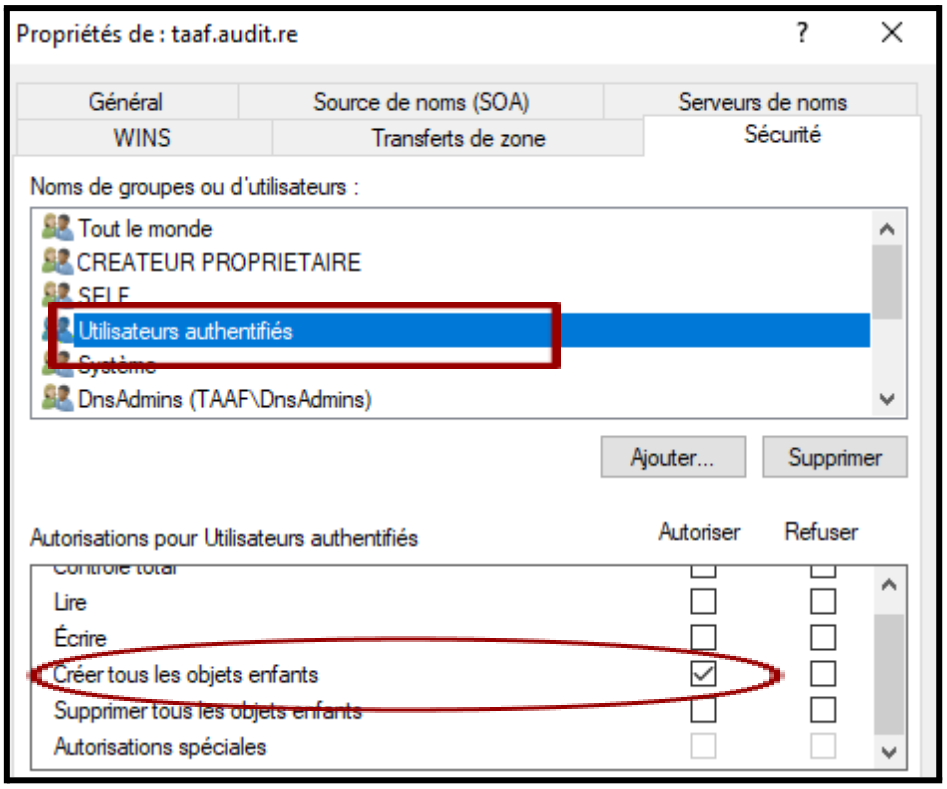
Impact : Le niveau de criticité est **FAIBLE** (à court terme) mais devient **MAJEUR** à moyen terme. L'absence d'anticipation entraînera une possible exposition potentielle à des failles de sécurité non corrigées après la fin du support étendu (2031).

Recommandation : Inscrire au schéma directeur de l'année prochaine l'étude de migration vers la version ultérieure (Windows Server 2025) afin de garantir la pérennité des correctifs de sécurité.

V6 : Permissions DNS permissives (Risque ADIDNS)

Périmètre : Infrastructure Active Directory / Zone DNS (`taaf.audit.re`)

Description (Risque) : L'analyse des listes de contrôle d'accès (ACL) sur le service DNS a mis en évidence une configuration par défaut risquée. Le groupe « Utilisateurs authentifiés » dispose de l'autorisation spéciale « Créer tous les objets enfants » à la racine de la zone.



Concrètement, cela signifie que n'importe quel compte valide sur le réseau (qu'il s'agisse d'un utilisateur standard, d'un stagiaire ou d'un compte compromis) a la capacité technique d'ajouter de nouveaux enregistrements dans l'annuaire DNS sans être administrateur.

Impact : Le niveau de criticité est **ÉLEVÉ**. Cette faiblesse expose le domaine à des attaques d'empoisonnement (ADIDNS Poisoning). Un attaquant peut exploiter ce droit pour créer un enregistrement malveillant, notamment un faux serveur `wpad` (Web Proxy Auto-Discovery). Cela forcerait les ordinateurs du réseau à transiter par la machine de l'attaquant, permettant une interception du trafic (Man-in-the-Middle) et la capture d'identifiants NTLM, compromettant ainsi l'intégrité et la confidentialité du réseau.

Recommandation : Technique (Immédiat) : Durcir les permissions de la zone DNS en retirant le droit d'écriture (« Créer tous les objets enfants ») au groupe « Utilisateurs authentifiés » pour le restreindre aux administrateurs ou aux comptes

machines uniquement. Et mettre en place un enregistrement statique de prévention pour `wpad` (pointant vers `0.0.0.0` ou le proxy légitime) et configurer la ***GlobalQueryBlockList*** pour empêcher sa modification.

8. RECOMMANDATIONS

Au regard des constats établis, l'application d'un plan de remédiation strict est nécessaire. Ce plan s'aligne sur les référentiels de l'état de l'art, et spécifiquement sur la note technique DAT-NT-17 de l'ANSSI relative à la sécurisation de l'Active Directory.

8.1. Mesures correctives par domaine

A. Gestion des privilèges et cloisonnement :

La priorité absolue réside dans la séparation des tâches (*Segregation of Duties*). Il est impératif de mettre fin à l'usage de comptes nominatifs standards pour l'administration du système. Concrètement, le compte "dgeneral" doit être retiré sans délai du groupe "Administrateurs du Domaine". La cible technique à atteindre repose sur la création de comptes d'administration dédiés (nomenclature type *adm_user*). Pour garantir l'intégrité du système, ces comptes privilégiés ne doivent disposer d'aucun accès à Internet ni de boîte de messagerie, limitant ainsi leur exposition aux vecteurs d'attaque courants.

B. Politique de mots de passe :

Le durcissement des secrets d'authentification doit être uniformisé sur l'ensemble du parc. L'option "Le mot de passe n'expire jamais", identifiée sur des comptes critiques comme "saudit", constitue une vulnérabilité majeure qui doit être corrigée. Il est recommandé de configurer la Stratégie de Groupe (GPO) par défaut (*Default Domain Policy*) pour imposer une entropie minimale (12 caractères incluant majuscules, chiffres et caractères spéciaux) et forcer un renouvellement des mots de passe tous les 90 jours.

C. Hygiène et cycle de vie de l'annuaire :

L'Active Directory ne doit pas servir de zone de stockage pour des informations confidentielles en clair. Les champs "Description" contenant des données sensibles (codes d'accès, mots de passe) doivent être purgés immédiatement. Sur le long terme, le maintien d'un niveau de sécurité acceptable nécessite l'instauration d'une procédure de revue trimestrielle, visant à identifier et désactiver systématiquement les comptes inactifs depuis plus de six mois.

8.2. Plan d'action priorisé

Afin d'optimiser la charge de travail des équipes techniques de TAAFictive, le déploiement des correctifs est structuré selon un phasage critique.

Priorité 1 : Actions immédiates (Dans les 24h qui suivent):

Cette première phase vise la réduction drastique du risque sans impact majeur sur la production. Les actions se concentrent sur la suppression des droits d'administration du compte "dgeneral", l'effacement des données sensibles dans la description du compte "saudit", ainsi que le renouvellement préventif du mot de passe du compte "Administrateur" par défaut.

Priorité 2 : Actions à court terme (Dans 1 semaine) :

La seconde phase concerne le durcissement de la configuration globale. Elle implique la modification de la GPO de mots de passe pour renforcer les exigences de complexité et d'expiration. En parallèle, l'exécution d'un script de correction est préconisée pour retirer massivement l'attribut *PasswordNeverExpires* sur l'ensemble des comptes utilisateurs concernés.

Priorité 3 : Actions à moyen terme (Dans 1 mois) :

Planification de la migration de l'OS par rapport au cycle de vie du serveur. Bien que le serveur fonctionne actuellement sous une version récente, nous devons anticiper l'obsolescence technologique. La version Windows Server 2022 atteindra sa date de fin de support standard (Mainstream Support) le 13 octobre 2026.

Passé cette date, Microsoft ne fournira plus de mises à jour fonctionnelles ni de support gratuit, bien que les correctifs de sécurité critiques continuent jusqu'au 14 octobre 2031 (Support Étendu). Action recommandée : Pour éviter une dette technique et des coûts de support supplémentaires, nous recommandons à TAAFictive de planifier, dès le budget 2026, une migration vers la version ultérieure (Windows Server 2025) avant l'échéance d'octobre.

9. SUIVI ET AMÉLIORATION

Le maintien du niveau de sécurité de TAAFictive repose d'abord sur des cycles de contrôle réguliers. Il est recommandé d'industrialiser l'audit de l'Active Directory via une exécution trimestrielle de l'outil PingCastle. Cette démarche permet non seulement de valider la baisse du risque suite aux correctifs, mais aussi d'alerter les équipes en cas de dégradation du niveau de sécurité (nouvelles failles, erreurs humaines)

Par ailleurs, il est indispensable d'améliorer la visibilité sur l'activité du réseau. L'activation et la centralisation des journaux d'événements constituent un prérequis indispensable pour identifier les tentatives d'intrusion. Enfin, la fiabilité du contrôleur de domaine dépend d'une **veille technologique active, cycle de vie (comme précisé dans la partie 8.2) et de l'application systématique des correctifs de sécurité mensuels fournis par Microsoft**.

10. CONCLUSION

En conclusion, l'audit du domaine taaf.audit.re a mis en lumière un environnement techniquement fonctionnel mais fragilisé par des pratiques d'administration perfectibles.

Si l'infrastructure serveur est robuste, la configuration humaine (droits excessifs, négligence sur les mots de passe) expose aujourd'hui TAAFictive à un risque élevé de compromission. Un attaquant interne ou externe pourrait exploiter ces faiblesses triviales pour prendre le contrôle du réseau en quelques minutes.

Cependant, la situation n'est pas irréversible. La prise de conscience matérialisée par cet audit est la première étape vers la sécurisation. L'application rigoureuse du plan d'action proposé, et notamment le respect intransigeant du principe de moindre privilège, permettra d'élever significativement le niveau de maturité de la sécurité du domaine. TAAFictive passera ainsi d'une posture de vulnérabilité à une posture de défense en profondeur, alignée sur les standards professionnels exigés par son secteur d'activité.

11. ANNEXE

Annexe A : Extrait du Guide ANSSI utilisé

La définition de la politique de mot de passe s'appuie sur le guide DAT-NT-17 (p.48). Ce référentiel de l'ANSSI préconise un niveau de robustesse 'Fort', imposant une longueur minimale de 12 caractères pour les comptes standards.

Lien vers la note technique sur les recommandations de sécurité relatives à Active Directory de l'ANSSI :

https://messervices.cyber.gouv.fr/documents-guides/NP_ActiveDirectory_NoteTech.pdf

Annexe B : Liste des comptes audités

- dgeneral (Compte critique mal configuré)
- saudit (Compte stagiaire avec fuite d'info)
- svc_sql (Compte de service)
- Groupe Domain Admins

Annexe C : Glossaire

- AD : Active Directory.
- GPO : Group Policy Object (Stratégie de groupe).
- ANSSI : Agence Nationale de la Sécurité des Systèmes d'Information.
- PingCastle : Outil d'audit de sécurité pour AD.