RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

RECOMMANDATIONS RELATIVES À L'ADMINISTRATION SÉCURISÉE DES SYSTÈMES D'INFORMATION REPOSANT SUR MICROSOFT ACTIVE DIRECTORY

GUIDE ANSSI

ANSSI-PA-099
02/10/2023

PUBLIC VISÉ :

Développeur | **Administrateur** | **RSSI** | **DSI** | Utilisateur

Informations

Attention

Ce document rédigé par l'ANSSI présente les **« Recommandations relatives à l'administration sécurisée des systèmes d'information reposant sur Microsoft Active Directory »**. Il est téléchargeable sur le site `www.ssi.gouv.fr`.

Il constitue une production originale de l'ANSSI placée sous le régime de la « Licence Ouverte v2.0 » publiée par la mission Etalab [41].

Conformément à la Licence Ouverte v2.0, le guide peut être réutilisé librement, sous réserve de mentionner sa paternité (source et date de la dernière mise à jour). La réutilisation s'entend du droit de communiquer, diffuser, redistribuer, publier, transmettre, reproduire, copier, adapter, modifier, extraire, transformer et exploiter, y compris à des fins commerciales.

Sauf disposition réglementaire contraire, ces recommandations n'ont pas de caractère normatif ; elles sont livrées en l'état et adaptées aux menaces au jour de leur publication. Au regard de la diversité des systèmes d'information, l'ANSSI ne peut garantir que ces informations puissent être reprises sans adaptation sur les systèmes d'information cibles. Dans tous les cas, la pertinence de l'implémentation des éléments proposés par l'ANSSI doit être soumise, au préalable, à la validation de l'administrateur du système et/ou des personnes en charge de la sécurité des systèmes d'information.

Évolutions du document :

VERSION	DATE	NATURE DES MODIFICATIONS
1.0	02/10/2023	Version initiale

Table des matières

1
Introduction

Convaincue que l'administration d'un système d'information (SI) est une activité critique qui doit être traitée avec la plus grande attention, l'ANSSI a publié un guide qui présente ses « recommandations relatives à l'administration sécurisée des systèmes d'information » [16] (par simplicité, ce dernier est appelé « guide ADMIN » dans le présent document).

Le guide ADMIN [16] se veut volontairement générique et agnostique des technologies informatiques mises en œuvre sur le SI à administrer. Or, certains concepts et certaines recommandations développés dans le guide ADMIN [16] sont difficilement transposables aux SI reposant sur Microsoft Active Directory (AD).

En outre, l'ANSSI fait régulièrement le constat que des compromissions de SI reposant sur AD résultent de l'application de mauvaises pratiques d'administration et d'un cloisonnement insuffisant. Pour ces raisons, le présent document se veut complémentaire au guide ADMIN [16] en abordant des aspects spécifiques à l'administration des environnements AD et en guidant dans le cloisonnement du SI en zones de confiance. Il ne se substitue pas au guide ADMIN [16] dont la lecture préalable est recommandée pour appréhender au mieux les concepts évoqués dans le présent document.

Lorsque qu'un AD est placé au cœur de l'infrastructure d'un SI (gestions des authentifications, attribution des droits d'accès aux ressources, paramétrage des politiques de sécurité, etc.) il est alors considéré que le SI repose sur AD. Dans ce contexte, une compromission de l'annuaire AD conduit souvent à une compromission globale du SI.

1.1 Objectif du guide

De nombreuses compromissions de SI commencent par des attaques qui ciblent les postes de travail. Les attaquants exploitent ensuite des faiblesses du SI pour opérer des déplacements, dits latéraux et élever progressivement leurs privilèges jusqu'à obtenir le contrôle total de l'annuaire AD. À ce niveau de contrôle de l'AD, un attaquant est en mesure de s'aménager des portes dérobées qui lui assurent un contrôle persistant du SI. Pour un SI qui s'appuie sur AD, il est capital d'en maîtriser la sécurité car l'AD est une cible prioritaire pour de nombreux attaquants.

Ce cheminement, potentiellement rapide, depuis des systèmes de faible sensibilité jusqu'à d'autres ressources de haute sensibilité est souvent rendu possible par une absence de cloisonnement logique des ressources de l'AD. Les conséquences d'une compromission des ressources de haute sensibilité de l'AD peuvent être désastreuses : atteinte à la confidentialité, à l'intégrité ou à la disponibilité des informations et des traitements portés par le SI, atteinte d'image, coût de la remédiation et de la reconstruction du SI.

Ce guide a pour principaux objectifs de faire comprendre :

- que l'administration d'un SI reposant sur un annuaire AD nécessite l'application de mesures de sécurité propres à cette technologie ;
- que le cloisonnement du SI en zones de confiance est fondamental. Ce document propose une méthodologie pour identifier ces zones et pour les cloisonner ;
- qu'un attaquant peut compromettre l'AD en exploitant de nombreux vecteurs (infrastructures de stockage, de virtualisation, de sauvegarde, etc.). Ces derniers doivent également faire l'objet d'une sécurisation adéquate sans quoi ils pourraient permettre le cheminement d'un attaquant jusqu'aux ressources les plus sensibles de l'AD.

Les recommandations de ce guide ainsi que la méthodologie proposée sont applicables aussi bien en conception initiale qu'en amélioration continue d'un SI en production.

Objectif

L'objectif principal de ce guide est de proposer des conseils et recommandations pour la mise en œuvre d'un cloisonnement logique des annuaires AD ainsi que pour la conception d'une architecture d'administration adaptée à l'état de la menace.

Attention

Ce guide n'aborde pas les aspects relatifs au traitement d'un incident de sécurité informatique affectant le SI. Les guides de remédiation [24] et [4] publiés par l'ANSSI sont des lectures recommandées dans le cadre du traitement d'un incident de sécurité.

Attention

Les problématiques de sécurité ayant trait à l'utilisation du *Cloud* (informatique en nuage) sont hors périmètre de ce guide. Il n'aborde donc ni les risques liés à l'extension du SI dans le *Cloud*, ni les problématiques d'administration des annuaires Microsoft Entra ID (ex Azure Active Directory).

Attention

La sécurisation des postes d'administration est essentielle. Toutefois, il est rappelé que ce sujet n'est pas traité dans le présent document car il est détaillé dans le guide ADMIN [16] : absence d'accès internet et de messagerie électronique, durcissement système, limitation des logiciels installés, chiffrement du stockage, etc.

1.2 Organisation du guide

Le chapitre 2 commence par rappeler les concepts fondamentaux de l'AD. Il explique ensuite les différents aspects d'une démarche de cloisonnement logique d'un SI reposant sur AD, tant du point de vue technique que méthodologique. Sont abordées les questions relatives au modèle mis en œuvre et à son périmètre d'application, puis une méthodologie itérative de cloisonnement du SI est proposée. Les recommandations du chapitre 2 sont des recommandations qui sont volontairement générales, au contraire des recommandations des autres chapitres qui sont plus techniques.

Le chapitre 3 s'attache à guider dans l'identification et le cloisonnement pertinents des ressources du SI qui correspondent au plus haut niveau de sensibilité de l'AD. Ce chapitre se concentre uniquement sur ce périmètre de sensibilité, le lecteur étant ensuite invité à adopter une approche similaire pour la sécurisation et le cloisonnement des zones de moindre confiance du SI.

Le chapitre 4 traite de l'importance de maîtriser la configuration et l'usage des protocoles NTLM et Kerberos pour parvenir à un cloisonnement du SI en zones de confiance.

Le chapitre 5 aborde quant à lui les principes d'élaboration d'une architecture d'administration adaptée aux besoins de sécurité des ressources du SI les plus sensibles. Il traite notamment des conditions de mutualisation des postes d'administration et propose des éléments d'aide à la conception d'une telle architecture. Il précise également certaines recommandations génériques du guide ADMIN [16] pour leur application dans le contexte spécifique d'un SI reposant sur un annuaire AD.

Les annexes permettent enfin de préciser la mise en œuvre technique de certaines recommandations présentées dans ces chapitres :

- l'annexe A apporte des compléments techniques à l'analyse des chemins d'attaque vers le plus haut niveau de sensibilité de l'AD. Cette analyse fait l'objet de la section 3.2 ;
- l'annexe B détaille l'utilisation du groupe de sécurité des utilisateurs protégés, dont l'utilisation est recommandée en section 4.10 ;
- l'annexe C aide à la mise en œuvre d'un silo d'authentification. Il s'agit d'une mesure de sécurité recommandée en sections 4.9 et 5.2.1 ;
- l'annexe D aide à la mise en œuvre de paramètres de restriction d'ouvertures de session. Il s'agit d'une mesure de sécurité également recommandée en sections 4.9 et 5.2.1 ;
- l'annexe E détaille l'utilisation du déport d'affichage distant avec l'option *Restricted Admin*, comme réponse aux risques de sécurité évoquées en sections 4.7 et 4.9 ;
- l'annexe F aborde les principes d'une forêt AD dédiée aux ressources obsolètes, l'usage d'une telle forêt étant évoqué en section 5.3.2.2 ;
- l'annexe G apporte quelques considérations de sécurité relatives à Microsoft Exchange, tant sa présence dans une forêt AD est une problématique complexe à traiter des points de vue du cloisonnement et de l'administration du SI.

Enfin, l'annexe H liste les acronymes utilisés dans le document.

1.3 Conventions de lecture

Pour certaines recommandations, il est proposé, au vu des menaces constatées lors de la rédaction de ce guide, plusieurs solutions qui se distinguent par le niveau de sécurité qu'elles permettent d'atteindre. Le lecteur a ainsi la possibilité de choisir une solution offrant la meilleure protection en fonction du contexte et de ses objectifs de sécurité.

Ainsi, les recommandations sont présentées de la manière suivante :

R

Recommandation à l'état de l'art

Cette recommandation permet de mettre en œuvre un niveau de sécurité à l'état de l'art.

R -

Recommandation alternative de premier niveau

Cette recommandation permet de mettre en œuvre une première alternative, d'un niveau de sécurité moindre que la recommandation R.

R +

Recommandation renforcée

Cette recommandation permet de mettre en œuvre un niveau de sécurité renforcé. Elle est destinée aux organisations qui sont matures en sécurité des systèmes d'information.

Dans une démarche permanente de gestion du risque numérique et d'amélioration continue de la sécurité des systèmes d'information [1], la pertinence de mise en œuvre des recommandations décrites dans ce document doit être périodiquement réévaluée.

La liste récapitulative des recommandations est disponible en page 150.

1.4 Comment aborder ce guide ?

Bien que ce guide puisse aider tout lecteur qui cherche à comprendre les enjeux de sécurité spécifiques à un SI reposant sur un annuaire AD, il s'adresse plus particulièrement à des lecteurs qui connaissent le fonctionnement d'un annuaire AD. Un lecteur éloigné de la technique ou qui souhaite aller à l'essentiel pourrait se contenter de lire le chapitre 2, puis uniquement les recommandations des autres chapitres.

Ce guide tente d'aborder l'ensemble des thèmes liés à l'administration d'un SI reposant sur un annuaire AD et liste des recommandations dont la difficulté d'implémentation variera d'un contexte à l'autre. La mise en œuvre des recommandations techniques de ce guide nécessite une certaine adaptation, car il ne peut pas aborder exhaustivement tous les cas de figure ni être applicable quelles que soient l'architecture du SI et les contraintes de l'organisation. Le choix a donc été fait de considérer des architectures de SI classiques [2], qui représentent la grande majorité des annuaires AD rencontrés tant dans le secteur privé que public. Il se veut applicable aussi bien à un SI de petite organisation qu'aux SI complexes et étendus de grandes organisations.

Après une première lecture du guide pour s'approprier les concepts, il est recommandé d'évaluer le niveau de maturité de l'organisation à l'aide de la liste des recommandations (p. 150). Pour chaque recommandation, préciser si elle est « *respectée* », « *partiellement respectée* » ou « *non respectée* ». Une fois synthétisée, cette analyse peut être le point de départ d'un plan d'actions dans un objectif d'amélioration continue.

1. Se reporter au guide ANSSI relatif à la maîtrise du risque numérique [12].
2. Il est convenu de parler de moyens de bureautique au sens large dans ce document, mais ces derniers pourraient tout aussi bien être des consoles industrielles ou quelconque autre moyen d'accès à un SI métier.

2
Méthodologie de cloisonnement logique de l'annuaire AD et du SI

2.1 Rappel des concepts fondamentaux de l'AD

AD est un service d'annuaire introduit par Microsoft sous Windows 2000 Serveur. Il permet de centraliser des informations relatives aux utilisateurs et aux ressources d'un SI.

Il inventorie et gère un ensemble d'objets que sont les comptes et groupes utilisateurs d'une organisation, mais également les serveurs, les postes de travail, les imprimantes, les domaines, les stratégies de sécurité, etc. Il a notamment vocation à permettre aux utilisateurs de trouver et d'accéder aux ressources connues de l'annuaire en fournissant des mécanismes d'identification, d'authentification et d'autorisation.

Pour être gérés par l'AD, les ordinateurs doivent être intégrés à un « domaine » AD. Il devient alors possible de s'y authentifier avec des comptes utilisateurs de l'AD puis d'accéder aux différentes ressources du SI gérées par l'AD. Au sein d'un domaine, les objets peuvent être organisés dans une arborescence de conteneurs logiques appelés des unités organisationnelles (OU, *organizational units*).

Le regroupement hiérarchique de plusieurs domaines forme un « arbre », lequel est constitué d'un domaine racine et éventuellement d'un ou plusieurs domaines enfants. Une « forêt » AD est un ensemble d'arbres partageant un annuaire central (*global catalog*) dont le schéma est commun à tous les arbres de la forêt. Un SI construit sur des technologies Microsoft se compose d'une ou plusieurs forêts pouvant avoir des liens entre elles. Ces liens sont appelés des « relations d'approbation » (*trust relationship*). Ces forêts sont elles-mêmes composées d'un ou plusieurs domaines qui ont des relations d'approbation entre eux. Cette structure logique [49] est pensée pour s'adapter aux contraintes et particularités des organisations les plus étendues, permettant notamment une adaptation technique de l'architecture AD en fonction des fusions et scissions des entités juridiques qui les composent. En revanche, les organisations les plus petites adoptent généralement une architecture AD mono-forêt, mono-domaine (une seule forêt contenant un seul domaine).

Le service d'annuaire AD utilise une base de données intégrée pour stocker toutes les informations des objets de l'annuaire. Sa taille peut varier de quelques centaines d'objets pour de petites organisations, à plusieurs millions pour les plus conséquentes. L'annuaire AD repose notamment sur :

- un ensemble de règles, le schéma, qui définit principalement les classes [46] d'objets et les attributs [46] contenus dans l'annuaire, ainsi que les contraintes et limites qui s'appliquent aux

instances de ces objets. La classe « ordinateur », par exemple, définit les dizaines d'attributs d'un ordinateur ainsi que ses liens avec les autres objets de l'annuaire ;

- le *global catalog* qui contient des informations sur chaque objet de la forêt AD. Il permet aux utilisateurs et aux administrateurs de retrouver des informations de l'annuaire quel que soit le domaine de l'annuaire qui stocke réellement les données.

Les services AD (authentification, annuaire, réplication, etc.) sont portés par des serveurs appelés des *contrôleurs de domaine*. Le service de réplication distribue les données de l'annuaire aux différents contrôleurs de domaine qui stockent, entre autres, une copie des informations de l'annuaire concernant leur domaine.

2.2 Modèle de gestion des accès privilégiés

Dans un SI, les besoins en droits d'accès des utilisateurs sont hétérogènes et dépendent de leurs missions. Un administrateur se distingue ainsi des autres utilisateurs par les droits et privilèges dont il a besoin pour mener à bien les actions d'administration qui relèvent de ses fonctions.

Droits et privilèges

Selon la terminologie Microsoft [90] :

- les droits (*permissions* en anglais) sont des autorisations (lecture, écriture, etc.) appliquées à des objets sécurisables tels que les fichiers, clés de registre et objets AD (comptes, groupes, unités organisationnelles, stratégies de groupe, etc.) ;
- un privilège (*user right*[104] ou *privilege* en anglais) octroie en revanche une capacité d'action spécifique sur un système d'exploitation (OS, *Operating System*), telle que par exemple : « changer l'heure du système » ou « charger ou décharger des pilotes de périphériques ». Des privilèges sont ainsi octroyés aux différents comptes et groupes utilisateurs intégrés par défaut dans les OS Microsoft Windows.

Par la suite, le terme « privilèges » est toutefois employé comme un terme générique englobant autant les notions de droits que de privilèges et c'est également le cas lorsqu'il est par exemple évoqué le principe de moindre privilège [3].

Compte privilégié et accès privilégié

Un compte est dit privilégié dès lors qu'il dispose de droits et privilèges qui sont interdits aux utilisateurs. C'est notamment le cas d'un compte d'administration du domaine AD, et cela peut également être le cas d'un compte d'administration fonctionnelle d'une application métier. Un compte est dit privilégié (ou « compte à privilèges ») lorsqu'il permet des accès privilégiés. Toutefois, des accès privilégiés sont aussi possibles sans compte à privilèges, en utilisant par exemple des certificats cryptographiques ou des clés d'accès à des interfaces de programmation applicative (API).

3. Le principe de moindre privilège consiste à mettre en place les autorisations strictement nécessaires aux activités prévues pour chaque compte et à interdire par défaut toutes les autres activités.

Compte privilégié local

Un compte privilégié est dit « local » (administrateur local, comptes d'administration locaux, etc.) lorsque ce compte est géré par un système particulier (serveur ou poste de travail généralement) et non pas de manière centralisée par l'annuaire AD. Il n'est donc valide et utilisable que sur ce système particulier et n'est pas connu des autres ressources du domaine AD. Un compte du domaine AD peut néanmoins se voir octroyer des droits et privilèges d'administration locaux sur un système particulier ou sur un ensemble de systèmes. La distinction entre compte local et compte du domaine AD est importante pour la gestion des accès privilégiés étant donné que leur portée d'action est différente.

Selon le principe de moindre privilège, les droits et privilèges de chaque administrateur doivent être octroyés en fonction du juste besoin opérationnel; deux administrateurs n'ayant pas nécessairement les mêmes besoins. La catégorisation des comptes par rôles doit ainsi être effectuée en regroupant des familles de cas d'usage et en séparant les droits et privilèges nécessaires aux administrateurs de manière rigoureuse.

L'adoption d'un modèle de gestion des accès privilégiés de l'AD – à base de rôles et de criticité des droits et privilèges octroyés – est une étape stratégique du découpage logique du SI administré en zones de confiance (ce concept de zone est détaillé dans le guide ADMIN [16] de l'ANSSI).

Zone de confiance

Une zone de confiance est un sous-ensemble logique d'un SI dont les besoins de sécurité, le niveau d'exposition ou de sensibilité, entre autres, sont homogènes. Toutes les ressources de ce sous-ensemble ont donc un niveau de confiance équivalent.

Objectif

Un découpage du SI en zones de confiance est réalisé de sorte à cloisonner logiquement ces zones les unes des autres, l'objectif étant de contenir une potentielle compromission au sein d'une zone et ainsi préserver la sécurité des autres. La mise en œuvre d'un tel découpage est le fondement d'un cloisonnement logique de l'AD et d'une démarche de gestion des accès privilégiés. Il concourt à ce que, par exemple, la compromission d'un poste de travail ne débouche pas *de facto* sur un contrôle total de l'AD par les attaquants.

Ce chapitre s'attache à clarifier la catégorisation des privilèges en niveaux de sensibilité ou de criticité et donc en zones de confiance. Il propose des méthodes pour l'identification initiale des niveaux de droits et de privilèges des comptes d'administration et plus largement de tous les objets de l'AD. Il se penche enfin sur la question de l'optimisation pas-à-pas de cette catégorisation et sur les actions à mener pour tendre vers un cloisonnement optimal des zones de confiance.

2.2.1 Choix du modèle

Un modèle de gestion des accès privilégiés repose sur un découpage pertinent du SI en plusieurs niveaux de confiance, réalisé essentiellement sur la base de la sensibilité ou de la criticité des ressources pour l'organisation ainsi que de leur exposition à la menace. Il est important qu'un nombre suffisant de niveaux soit défini de manière à véritablement cloisonner le SI en zones de confiance pertinentes vis-à-vis des valeurs métiers et à limiter au maximum les chemins d'attaque qui pourraient permettre le passage d'un attaquant d'une zone de confiance à l'autre.

Chemin d'attaque

Un chemin d'attaque est une suite de faiblesses humaines, matérielles ou logicielles avérées, suspectées ou plausibles et exploitables successivement par un attaquant pour la prise de contrôle d'une ressource cible du SI. Une ressource est généralement la cible d'un attaquant lorsqu'elle supporte une valeur métier de l'organisation ou lorsqu'elle lui est d'une quelconque utilité dans sa stratégie globale d'attaque du SI. Un chemin d'attaque peut notamment faire intervenir :

- des élévations de privilèges, qui octroient la capacité de mener des actions qui requièrent des privilèges supérieurs. Une élévation de privilèges peut alors être locale (sur une même ressource en passant de simple utilisateur à administrateur local par exemple) ou distante vers une autre ressource du SI à travers le réseau ;
- des déplacements latéraux (ou « latéralisation »), qui consistent à s'authentifier à travers le réseau sur différents ordinateurs du SI avec les droits et privilèges déjà obtenus, avec généralement l'intention de trouver d'autres faiblesses exploitables et qui permettraient des élévations de privilèges.

Microsoft a historiquement défini un modèle de cloisonnement du SI en trois niveaux de confiance (c'est-à-dire trois zones de confiance caractérisées par leur niveau de sensibilité ou de criticité) nommés « *Tiers* » et dont les concepts sont abordés dans le centre de documentation en ligne de l'éditeur [83].

Information

Le terme de « *Tier* » – prononcé `ti(ə)r` – est un terme anglophone qui signifie « niveau » et donc sans rapport avec le mot « tiers » de la langue française.

Dans la suite de ce document, tant pour éviter des confusions que pour en faciliter la compréhension, le terme « *Tier* » est utilisé en anglais tel quel dans le texte et sans traduction dans la mesure où son usage en français est aujourd'hui un anglicisme répandu dans la communauté Microsoft ainsi que dans le domaine de la sécurité des systèmes d'information (SSI). Le modèle en trois *Tiers* de Microsoft est présenté par le tableau 1.

Tier	Description
0	Ce *Tier* représente **le cœur de confiance de l'organisation**. Les privilèges d'administration de ce *Tier* sont les plus élevés : ils permettent l'octroi de privilèges sur les autres *Tiers* et donc le contrôle de toutes les ressources de l'annuaire AD. Les ressources de ce *Tier* – telles que les contrôleurs de domaine AD par exemple – ont *de facto* un niveau de sensibilité équivalent dans la mesure où la détention de privilèges d'administration sur l'une d'elles induit l'acquisition des privilèges d'administration sur les autres. La compromission d'une ressource de ce *Tier*, au delà de permettre la compromission de l'ensemble des ressources de l'AD, permet aussi l'aménagement de portes dérobées potentiellement complexes à identifier et à éradiquer. Une telle compromission nécessiterait une remédiation extrêmement longue, compliquée et couteuse à mettre en œuvre pour rétablir la confiance dans le SI.
1	Ce *Tier* représente la confiance dans les données et plus précisément, au sens de la méthode EBIOS RM [10], **la confiance dans les valeurs métiers de l'organisation**. Il représente ainsi la confiance dans les biens métiers ainsi que dans les biens supports qui les portent (stockage, traitement, etc.). Ces derniers peuvent par exemple être des serveurs de gestion de code source pour une entreprise de développement logiciel, ou bien les équipements critiques d'une chaîne de production pour un industriel. Les privilèges d'administration afférents à ce *Tier* permettent le contrôle de tout ou d'un ensemble de ces biens supports et sont généralement octroyés à des administrateurs système ou à des responsables d'applications ou de services du SI.
2	Ce *Tier* représente **la confiance dans les postes de travail des utilisateurs du SI** et plus largement dans tout moyens d'accès à la donnée métier. Les ressources du *Tier* 2 sont généralement des postes de travail de bureautique, mais peuvent également être des consoles industrielles ou tout autre type de moyen d'accès utilisateur ou de programmation. Les privilèges d'administration afférents à ce *Tier* permettent le contrôle de tout ou d'un ensemble de ces moyens d'accès. Un tel niveau de droits et privilèges est généralement accordé à des téléadministrateurs des postes bureautiques, des administrateurs de services de déploiement des postes bureautiques, des déployeurs de consoles industrielles, etc. Ces moyens d'accès hébergent des portions de valeurs métiers de l'organisation ou permettent d'y accéder. La compromission d'un ensemble de moyens d'accès peut ainsi permettre un large accès aux données de l'organisation ou à ses valeurs métiers, depuis le SI interne ou même parfois depuis Internet. Il arrive par ailleurs que des utilisateurs haut placés dans la hiérarchie de l'organisation aient des droits d'accès très larges sur les valeurs métiers, ce qui en fait des cibles de choix pour des attaquants.

Tableau 1 – Description des *Tiers* dans le modèle en trois *Tiers* de Microsoft

De manière générale, le nombre de ressources contenues dans un *Tier* et leur degré d'exposition aux menaces sont inversement proportionnels à la sensibilité ou à la criticité de ce *Tier*. Les *Tiers* peuvent ainsi être représentés sous forme hiérarchique : en haut de la hiérarchie se trouvent les ressources sensibles ou critiques, en nombre réduit ; tandis qu'en bas de la hiérarchie se trouvent les ressources moins sensibles, mais en quantité beaucoup plus importante. Cette symbolique illustrée par la figure 1 sera utilisée dans la suite de ce document pour représenter les *Tiers* dans les différents schémas qui composent ce guide.

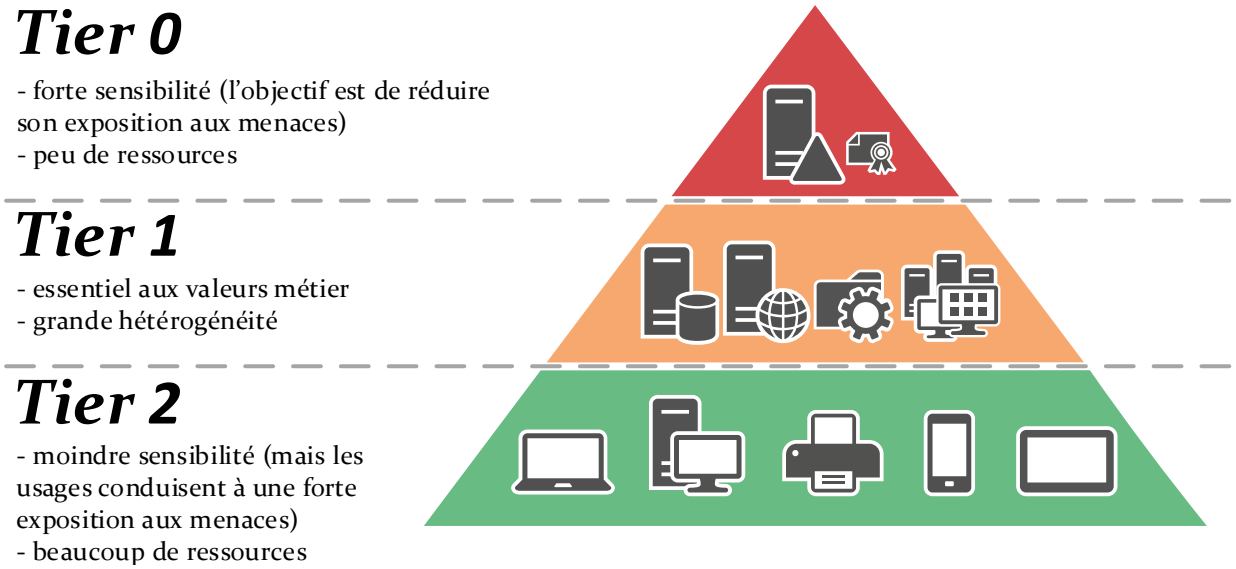

FIGURE 1 – Représentation hiérarchique du modèle en trois *Tiers* de Microsoft.

Microsoft a fait évoluer ce modèle fin 2020 principalement pour en faciliter l'application à des SI étendus dans le *cloud* et mettant par exemple en œuvre des architectures hybrides. Cette nouvelle version du modèle porte le nom d'*enterprise access model* [82]. Parmi ses évolutions [4], le découpage en trois niveaux a été affiné et la terminologie utilisée a été harmonisée avec celle utilisée par Microsoft pour ses services *cloud*. Les évolutions de ce modèle peuvent être synthétisées de la manière suivante :

- le niveau 0 porte désormais le nom de *control plane* ;
- le niveau 1 a été séparé en *data workload plane* et *management plane* qui correspondent d'une part aux biens métiers et aux biens supports qui les portent (tels que décrits dans le tableau 1 page 13) et d'autre part aux ressources informatiques nécessaires au fonctionnement du SI (gestion centralisée, supervision, détection, sécurité, etc.), mais dont les biens métiers dépendent indirectement. L'accent est mis sur une catégorie d'utilisateurs (appelés « comptes spécialisés ») qui ne sont pas administrateurs de ressources informatiques, mais qui ont néanmoins des accès hautement privilégiés à des valeurs métiers sensibles.
- le niveau 2 a été séparé en *user access* et *app access*, qui correspondent respectivement aux moyens d'accès utilisateur et aux accès programmatiques évoqués dans le tableau 1 page 13.

4. Le centre de documentation de Microsoft [83] peut être consulté pour de plus amples informations sur les évolutions du modèle historique en trois *Tiers*.

R1

Mettre en œuvre un modèle de gestion des accès privilégiés

L'adoption d'un modèle de gestion des accès privilégiés est importante pour structurer la démarche de cloisonnement du SI et de sécurisation de l'annuaire AD. Dans cette optique, il est recommandé de définir et d'appliquer un modèle de gestion des accès privilégiés reposant sur plusieurs niveaux de confiance.

Le modèle préconisé est le modèle historique proposé par Microsoft découpé en trois *Tiers* ou l'*enterprise access model* [82] avec sa nouvelle terminologie.

Le modèle en trois *Tiers* historiquement proposé par Microsoft a l'avantage d'être simple, tout en restant une référence communément partagée et connue des acteurs de la SSI. Par ailleurs, la séparation entre *data workload plane* et *management plane* reste de rigueur sans pour autant changer de terminologie. Pour sa plus grande facilité d'adoption, le modèle historique en trois *Tiers* est le modèle utilisé dans ce guide. La catégorisation de 0 à 2 sera toutefois associée à un code couleur « (rouge, orange, vert) » et représentée à l'aide des pictogrammes *Tier 0*, *Tier 1* et *Tier 2* de sorte que cette catégorisation apparaisse comme familière pour le plus grand nombre de lecteurs.

2.2.2 Mise en perspective du modèle vis-à-vis des valeurs métiers

Quel que soit le modèle appliqué, il est important de garder à l'esprit que les biens supportant les missions et valeurs métiers de l'organisation ne se situent généralement pas au niveau le plus sensible et sont normalement des équipements du *Tier 1*. Les valeurs métiers se trouvent par ailleurs souvent disséminées par portions sur les postes de travail administrés par des comptes de *Tier 2* et sont notamment accessibles par des comptes utilisateurs de bureautique ou à travers des API.

Un attaquant va généralement chercher à réaliser des élévations de privilèges vers le *Tier 0*, qui permet *de facto* le contrôle du *Tier 1* et du *Tier 2*. L'exfiltration de données et la persistance de l'attaquant dans le SI sont ainsi facilitées. Dans certains cas toutefois, une attaque ciblée peut se concentrer sur de l'espionnage discret et ainsi consister à exfiltrer des valeurs métiers à l'aide d'accès peu ou pas privilégiés (incluant les accès aux API, qui sont généralement moins supervisés et dont les secrets d'accès sont rarement renouvelés). Bien que la protection du *Tier 0* soit la priorité des organisations, elles doivent garder à l'esprit que leurs missions et leurs valeurs métiers sont *in fine* les plus importantes et qu'elles sont portées par le *Tier 1*. Des compromissions étendues du *Tier 1* voire du *Tier 2* sont des évènements redoutés dont les conséquences peuvent être dramatiques pour l'entité, y compris sans compromission du *Tier 0*.

R2

Protéger chaque niveau du modèle de manière proportionnée

La protection du *Tier 0* est une priorité. Toutefois, la mise en œuvre d'un modèle de gestion des accès privilégiés doit avoir pour objectif de protéger ce qui est le plus important pour l'organisation : ses missions et ses valeurs métiers. Une fois que le niveau de sécurité du *Tier 0* ne représente plus un péril immédiat pour l'organisation, des efforts doivent rapidement être consacrés à la protection et au cloisonnement du *Tier 1*. Chacun des niveaux doit être protégé de manière proportionnée.

2.2.3 Enjeux de la mise en œuvre du modèle

Objectif

L'enjeu principal d'un découpage du SI en niveaux et en zones est de véritablement cloisonner les zones de confiance entre elles. L'objectif est ainsi que les zones les plus sensibles (les contrôleurs de domaine notamment) soient les moins exposées aux menaces et que les zones les moins sensibles soient au contraire les seules à être directement exposées aux menaces (les postes bureautiques généralement). Le cloisonnement consiste donc à identifier et traiter les chemins d'attaque qui pourraient permettre à un attaquant le déplacement d'une zone de confiance vers une autre, et en l'occurrence d'un *Tier* vers un autre de niveau supérieur (c'est-à-dire du *Tier 2* au *Tier 1* ou du *Tier 1* au *Tier 0* voire directement du *Tier 2* au *Tier 0*). Il s'agit là du principal fil directeur de la démarche de gestion des accès privilégiés et de tout modèle mis en œuvre à cet effet.

Le découpage d'un SI en niveaux et en zones de confiance repose en grande partie sur un cloisonnement logique de l'annuaire AD, qui nécessite de traiter les chemins d'attaque propres aux environnements AD et Windows. Mais il repose également sur un cloisonnement relatif à l'architecture générale du SI : cloisonnement réseau, cloisonnement système, cloisonnement physique, etc. La mise en œuvre d'un modèle de gestion des accès privilégiés dans un SI reposant sur un annuaire AD n'est donc pas uniquement l'affaire des administrateurs de l'AD : il s'agit d'un projet qui doit être piloté à plus haut niveau et qui s'appuie sur un large spectre de compétences touchant aux SI.

Pour assurer le cloisonnement des zones de confiance, l'identification des chemins d'attaque est une étape décisive : si elle n'est pas menée de manière consciencieuse, la catégorisation des ressources au sein des différents *Tiers* sera sans doute très perfectible et le cloisonnement qui en résultera sera très probablement inefficace puisqu'il subsistera des chemins d'attaque d'un *Tier* vers un autre.

Attention

Il est fréquent que des organisations, par habitude historique, comptent exagérément sur le cloisonnement réseau pour assurer le cloisonnement d'un SI reposant sur un annuaire AD. Mais l'utilisation d'un annuaire AD implique l'autorisation de flux réseau entre les systèmes et les contrôleurs de domaines, qui dialoguent à l'aide de différents protocoles de communication sous-jacents aux environnements Windows et AD : RPC, SMB, Kerberos, etc. Les pare-feu réseau doivent autoriser ces protocoles pour le bon fonctionnement de l'AD, mais n'en contrôlent pas le contenu qui peut être légitime ou malveillant. Lorsqu'un domaine AD est transverse à plusieurs zones réseau, ces zones sont donc séparées par des pare-feu dont les fonctionnalités de filtrage sont incapables de contrôler la plupart des communications entre ressources de l'AD, que ces communications soient légitimes ou malveillantes. Le cloisonnement des zones de confiance d'un SI reposant sur un annuaire AD ne peut donc pas reposer uniquement sur un cloisonnement réseau.

La mise en œuvre d'une politique de sécurité renforcée peut s'avérer compliquée voire particulièrement contre-productive si elle est appliquée à l'échelle d'un SI. Le découpage en zones de confiance permet d'appliquer des politiques différenciées et adaptées aux niveaux de sensibilité de chaque *Tier*. L'application d'une politique de sécurité renforcée est ainsi recommandée sur le strict périmètre des systèmes qui présentent un fort besoin de sécurité, comme c'est le cas pour de nombreuses recommandations de ce guide. Les différentes politiques en vigueur dans le SI peuvent alors se distinguer sous plusieurs aspects, tels que :

- les mesures de sécurité physique ;
- les mécanismes de contrôle d'accès (physique et logique) ;
- le durcissement des serveurs, des postes de travail et des postes d'administration ;
- les mécanismes de cloisonnement mis en œuvre ;
- les procédures de vérification d'antécédents des utilisateurs ou des administrateurs du SI (habilitation de sécurité au sens de l'IGI 1300 [22], enquêtes administratives, etc.).

La figure 2 vulgarise le principe de cloisonnement des *Tiers*. Les restrictions sur les relations de contrôle représentées sont inhérentes à la logique de cloisonnement des *Tiers* : un *Tiers* ne doit avoir aucune relation de contrôle d'un *Tiers* de plus haut niveau de confiance, en revanche il peut avoir le contrôle d'un *Tiers* de moindre de confiance (complet ou seulement d'un sous-ensemble), mais cette relation de contrôle est à limiter et à encadrer en fonction des risques qu'elle induit.

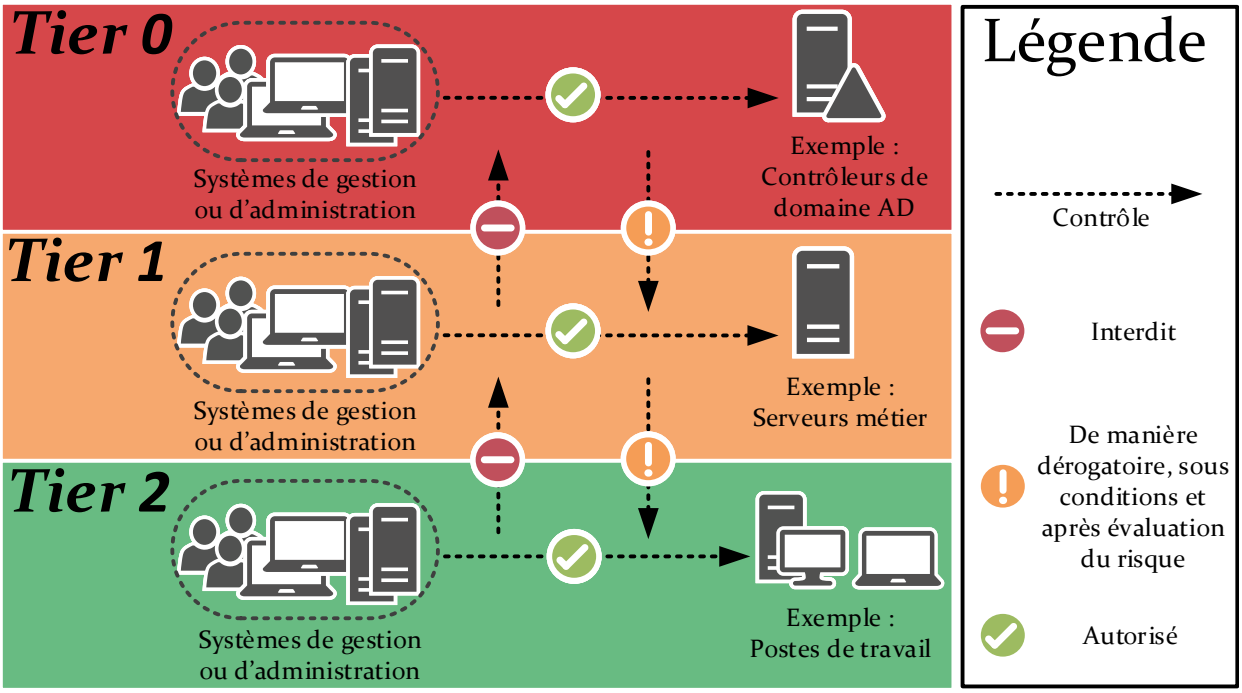

FIGURE 2 – Illustration du principe de cloisonnement des *Tiers*.

2.2.4 Périmètre d'application du modèle

Pour un SI reposant sur un annuaire AD, le périmètre idéal d'application du modèle de gestion des accès privilégiés est la forêt AD, car il s'agit d'un ensemble logique de ressources délimité par

une frontière de sécurité stricte. Pour autant, cette frontière peut être rendue poreuse dans des SI multiforêts (c'est-à-dire composés de plusieurs forêts généralement interconnectées entre elles par des relations d'approbation). Dans ce cas, le périmètre idéal d'application du modèle dépend des relations d'approbation configurées.

Il existe différents types de relations d'approbation entre forêts, qui peuvent être plus ou moins permissives et qui peuvent ainsi créer des chemins d'attaque d'une forêt à l'autre (les risques liés aux relations d'approbation sont détaillés en section 3.2.3). En effet, des comptes d'une forêt peuvent disposer de privilèges sur une autre forêt qui l'approuve, que ce soit notamment par des délégations nominatives de droits, par l'absence de filtrage des SID [96] ou simplement par appartenance à des groupes. Les périmètres des différents *Tiers* d'une forêt se trouvent alors potentiellement étendus à des objets des forêts approuvées (puis, par transitivité, à des forêts qu'elles-mêmes approuvent éventuellement).

L'application d'un modèle de gestion des accès privilégiés sur le strict périmètre d'une forêt AD est donc une bonne pratique, si tant est que cette forêt soit dans une de ces situations :

- elle n'accorde sa confiance (relation d'approbation sortante, ou *outbound trust relationship*) à aucune autre forêt ;
- elle accorde sa confiance uniquement à des forêts d'un niveau de sécurité et de sensibilité supérieurs (cas de l'approbation d'une forêt d'administration par exemple, abordé en section 5.3.2) ;
- elle accorde sa confiance à d'autres forêts, mais de manière sécurisée et maîtrisée (critères détaillés en section 3.2.3).

Dans le cas contraire, le périmètre d'application du modèle de gestion des accès privilégiés doit respecter la frontière de sécurité logique. Il peut donc être étendu à un ensemble de forêts AD, voire parfois au SI dans sa globalité s'il n'y a aucune frontière de sécurité stricte entre toutes les forêts qui le composent.

La mise en œuvre du modèle sur le périmètre restreint d'une forêt AD est toutefois plus simple à mener qu'à l'échelle d'un SI multiforêts entier. Elle permet notamment de prioriser sa mise en œuvre aux forêts les plus sensibles (telles que celles contenant des SIIV [5], des SI sensibles au sens de l'instruction interministérielle n°901 [21] ou des SI essentiels [14]) : opportunité appréciable dans le cas de SI complexes ou simplement pour se concentrer prioritairement sur la protection des ressources du SI qui sont les plus sensibles.

Il est à noter, par ailleurs, que de nouveaux besoins et contraintes peuvent émerger au fil du temps. Ils pourraient se traduire par de nouvelles relations d'approbation, de nouvelles délégations de droits octroyées à des comptes d'autres forêts, voire de nouvelles mutualisations d'infrastructures. Le périmètre d'application du modèle peut donc évoluer dans le temps.

Enfin, l'externalisation des SI est une pratique qui peut également peser sur le choix du périmètre du modèle si l'organisation fait confiance à des sous-ensembles du SI ou de l'AD sans pour autant

5. Les systèmes d'information d'importance vitale (SIIV) sont les SI essentiels des opérateurs d'importance vitale (OIV), privés et publics, qui permettent la production et la distribution de biens ou de services indispensables à l'exercice de l'autorité de l'État, au fonctionnement de l'économie, au maintien du potentiel de défense ou à la sécurité de la Nation. Consulter l'article [110] sur le site de l'ANSSI pour de plus amples informations.

en avoir la maîtrise. Ce guide n'a toutefois pas vocation à traiter le sujet de l'infogérance, le lecteur est invité à consulter le guide « Maîtriser les risques de l'infogérance » [5] de l'ANSSI.

R3

Définir le périmètre d'application du modèle

Il est recommandé de délimiter des périmètres cohérents d'application du modèle de gestion des accès privilégiés qui soient pertinents au regard de l'architecture AD des SI de l'organisation et de leurs dépendances (structuration du SI en forêts et domaines, nature des relations d'approbation entre les forêts, dépendance à des SI infogérés, etc.).

Ces périmètres doivent être revus périodiquement au regard de l'architecture AD et des chemins d'attaque identifiés entre forêts. Ces derniers sont détaillés dans le chapitre 3 dédié à l'identification et au cloisonnement du *Tier 0*.

Attention

Il n'est pas rare de rencontrer des architectures AD découpées en plusieurs domaines AD dans un objectif de cloisonnement en zones de confiance. Il s'agit d'une mauvaise pratique puisque le domaine AD n'est pas une réelle frontière de sécurité. Par injection de *SID History* [98] [96] notamment, la détention de privilèges de *Tier 0* dans un domaine AD aboutit à l'obtention aisée de ce même niveau de privilèges au sein de tous les domaines de la forêt.

Il est donc strictement déconseillé d'appliquer un modèle de gestion des accès privilégiés sur le seul périmètre d'un domaine AD dans la mesure où sa sécurité dépend directement des autres domaines de sa forêt. Le véritable périmètre de sécurité minimum d'une architecture AD est la forêt.

2.3 Le cloisonnement du SI en Tiers : un processus itératif

Le cloisonnement du SI en *Tiers* ne doit pas être considéré comme un travail réalisé une fois pour toutes. Au contraire, ce cloisonnement doit être envisagé comme une démarche d'amélioration continue, réalisé pas à pas et revu au gré des évolutions du SI.

R4

Mettre en œuvre un processus itératif d'amélioration continue du cloisonnement du SI

Il est recommandé de mettre en œuvre un processus itératif d'amélioration continue du cloisonnement du SI. Ce processus vise à tendre progressivement vers un cloisonnement optimal des zones de confiance et à le maintenir, tout en s'assurant que le périmètre d'application du modèle reste pertinent (cf. section 2.2.4).

Ce processus itératif doit être piloté par des interlocuteurs ayant une vision globale du SI et de ses évolutions à venir (architectes des systèmes d'information, membres de la direction informatique, etc.). Ce processus ne doit pas être uniquement piloté par des administrateurs de l'AD.

Les itérations du processus d'amélioration continue du cloisonnement du SI devraient donner lieu à la production de documents de synthèse nécessaires aux prises de décisions. Ces documents servent à apporter de la visibilité à la direction, tant sur les risques qui pèsent sur les valeurs métiers de l'organisation et sur le SI de manière générale que sur les actions identifiées et planifiées pour traiter ou réduire ces risques.

Objectif

L'objectif de cette section est de proposer un processus itératif d'amélioration continue du cloisonnement du SI en *Tiers*. Ce processus se déroule en deux phases principales, chacune composée de plusieurs étapes :

- une première phase d'étude et d'analyse qui permet notamment d'identifier les ressources à catégoriser au sein des différents *Tiers* (sections 2.3.1 à 2.3.3). De bonnes connaissances du SI et de l'organisation sont des prérequis pour mener à bien cette première phase ;
- une deuxième phase de mise en œuvre des actions nécessaires à l'amélioration du cloisonnement des *Tiers* (sections 2.3.4 à 2.3.8).

La figure 3 illustre ce processus itératif et les étapes qui le composent.

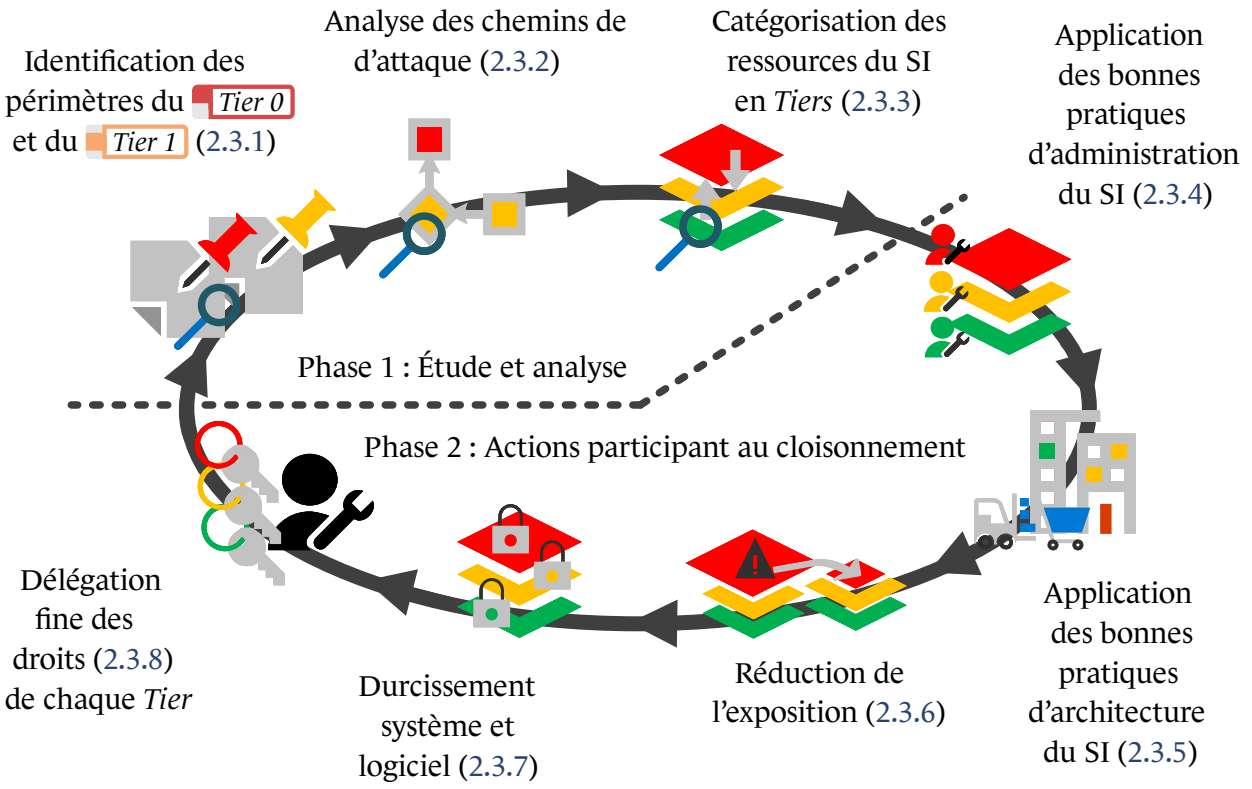

FIGURE 3 – Représentation graphique du cycle itératif d'amélioration continue du cloisonnement du SI en *Tiers*

2.3.1 Identification des périmètres du Tier 0 et du Tier 1

La démarche de gestion des accès privilégiés commence par une identification des périmètres du *Tier 0* et du *Tier 1*. Au tout début du cycle itératif de cloisonnement du SI en *Tiers*, les ressources de *Tier 0* se limitent aux contrôleurs de domaine AD et ce périmètre initial va généralement s'étendre au gré des chemins d'attaque identifiés dans les prochaines étapes.

Concernant le périmètre initial du *Tier 1*, celui-ci n'est pas immédiatement défini et nécessite de préalablement identifier les missions et valeurs métiers [6] de l'organisation. La liste des biens supports identifiés par cette étude constitue l'ensemble des ressources du SI qui représentent la confiance dans les données et valeurs métiers de l'organisation, c'est-à-dire celles du *Tier 1* selon la définition donnée dans le tableau 1 page 13.

R5

Identifier les valeurs métiers du Tier 1

Il est recommandé d'identifier les missions et valeurs métiers[6] de l'organisation. La liste des biens supports qui en découle représente le périmètre métier initial du *Tier 1* [7].

Ce périmètre métier du *Tier 1* est très susceptible d'évoluer au fur et à mesure des cycles itératifs de cloisonnement du SI, car les activités d'une organisation évoluent et les biens supports des valeurs métiers également.

2.3.2 Analyse des chemins d'attaque

L'identification du périmètre des différents *Tiers* implique nécessairement d'analyser les chemins d'attaque vers ces derniers. Ces analyses doivent notamment prendre en considération les chemins de contrôle indirects par transitivité (si A contrôle B et que B contrôle C, alors la compromission de A permet la compromission de C. A, B et C devraient donc logiquement faire partie de la même zone de confiance).

Elles ne sont toutefois pas aisées à mener et elles requièrent un certain niveau d'expertise permettant d'identifier des chemins d'attaque parfois complexes et des enchaînements non triviaux de relations de contrôle légitimes entre objets de l'AD. C'est la raison pour laquelle l'identification du *Tier 0* est une étape qui fait l'objet d'un approfondissement spécifique en chapitre 3.

Par ailleurs, il est à noter qu'un SI ne se limite pas à des ressources reposant sur des OS Microsoft Windows. D'autres ressources y sont présentes, comme par exemple :

- des équipements réseau (routeurs, commutateurs, pare-feu, etc.);
- des équipements Unix/Linux et dérivés;
- des équipements industriels.

6. L'atelier 1 du guide EBIOS RM [10] de l'ANSSI aide à identifier les missions et valeurs métiers de l'organisation. À noter que le guide de cartographie du système d'information [9] de l'ANSSI est une lecture recommandée en prérequis pour mener à bien cet atelier EBIOS RM.
7. Ce périmètre métier initial représente le *data workload plane* de l'*enterprise access model* [82] de Microsoft évoqué page 14.

Des ressources non Microsoft peuvent parfois être intégrées à l'AD et ainsi disposer, par exemple, d'un compte d'ordinateur dans l'annuaire pour bénéficier des fonctionnalités portées par l'AD (annuaire, authentification centralisée Kerberos, etc.). Ces ressources non Microsoft peuvent aussi simplement stocker ou manipuler des comptes de l'AD pour se connecter à des ressources du SI. Bien que les trois *Tiers* du modèle de Microsoft soient généralement considérés comme des zones de confiance contenant des ressources intégrées à l'AD et reposant sur des OS Microsoft Windows, en réalité ces zones doivent nécessairement être élargies aux autres types d'équipements dès lors que ces derniers présentent des chemins d'attaque vers des ressources de ces zones.

R6

Analyser les chemins d'attaque vers le Tier 0 et le Tier 1

L'analyse des chemins d'attaque est une étape essentielle. Le chapitre 3 détaille ce travail d'analyse à destination des ressources de *Tier 0* ; il doit être mené en priorité, car il s'agit du *Tier* le plus sensible et sa sécurité est primordiale. À chaque itération, le périmètre du *Tier 0* va donc s'étendre au gré des chemins d'attaque identifiés. Il peut également rétrécir au gré des chemins d'attaque supprimés (grâce aux actions de sécurisation et de cloisonnement qui font l'objet de la deuxième phase).

Cette analyse doit ensuite être menée à destination des valeurs métiers et de leurs biens supports du *Tier 1* qui ont été identifiés précédemment (recommandation R5). Des chemins d'attaque vers les biens support du *Tier 1* doivent ainsi légitimement apparaître depuis des ressources informatiques du SI[8] (services de télédéploiement, de gestion centralisée, etc.).

Les chemins d'attaque dont la difficulté d'exploitation est jugée trop importante au regard du niveau d'attaquant considéré (par l'analyse de risques) et des besoins de sécurité exprimés peuvent être ignorés dès lors que le risque résiduel est accepté.

L'analyse des chemins d'attaque doit être menée avec justesse et rigueur sans quoi la catégorisation puis le cloisonnement des *Tiers* faits par la suite seraient inefficaces. Il est donc primordial de s'appuyer sur des conseils d'experts en SSI et d'impliquer les personnes qui ont la connaissance technique et métier du SI de l'organisation.

Bien que ce guide ait pour ambition d'aider à l'identification d'une large variété de chemins d'attaque, il ne saurait toutefois traiter le sujet de manière exhaustive étant donné leur multitude. Le chapitre 3 apporte néanmoins un aperçu des nombreux aspects à considérer.

Pour finir, les résultats de l'analyse des chemins d'attaque sont susceptibles d'évoluer dans le temps au gré des évolutions du SI, des menaces et des connaissances en SSI. Il est par conséquent nécessaire de les remettre en question chaque fois que de nouveaux éléments modifient l'analyse de risques.

8. Les ressources IT du SI qui permettent le contrôle – direct ou indirect – des valeurs métiers et de leurs biens supports représentent le *management plane* de l'*enterprise access model* [82] de Microsoft évoqué page 14.

2.3.3 Catégorisation des ressources du SI en Tiers

L'identification des périmètres initiaux du *Tier 0* et du *Tier 1* puis l'analyse des chemins d'attaque vers chacun d'eux permettent d'aboutir à une catégorisation effective des ressources du SI.

R7

Catégoriser les ressources du SI en Tiers

Les ressources du SI (équipements, systèmes, mais également comptes, groupes et objets AD au sens large) doivent être catégorisées au sein des différents *Tiers* sur la base du travail d'analyse des chemins d'attaque mené précédemment (recommandation R6).

Pour catégoriser les ressources du SI, le principe à appliquer est le suivant : dès qu'un chemin d'attaque est identifié depuis une ressource A vers une ressource B d'un *Tier* plus sensible, alors la ressource A doit être catégorisée dans le même *Tier* que la ressource B. Logiquement, une ressource ne peut donc jamais être catégorisée dans plusieurs *Tiers*.

En suivant ce principe, différentes ressources du SI vont être progressivement catégorisées en *Tier 0* ou en *Tier 1*, élargissant ainsi leurs périmètres initiaux. Appliquer à nouveau la recommandation R6 d'analyse des chemins d'attaque vers ces ressources nouvellement recatégorisées aura ainsi de suite pour effet de progressivement constituer les différents *Tiers*.

Enfin, la catégorisation d'une ressource n'est pas définitive et doit être réévaluée quand des chemins d'attaque sont supprimés. Le périmètre des différents *Tiers* va donc s'étendre et se resserrer au fil des itérations, du fait que de nouveaux chemins d'attaque soient identifiés et que d'autres soient supprimés.

Tant que la majorité des chemins d'attaque identifiés n'ont pas été traités ou atténués pour permettre, autant que possible, la recatégorisation des ressources du SI vers des *Tiers* de moindre sensibilité, la catégorisation des ressources en *Tiers* conduit généralement à placer un nombre disproportionné de ressources en *Tier 0*. Cela est d'autant plus le cas quand le SI est complexe, étendu ou que la maturité SSI de l'organisation est faible.

Il arrive, par exemple, que des biens support de valeurs métiers se trouvent catégorisés en *Tier 0* lorsqu'ils pourraient permettre le contrôle de l'annuaire AD, alors que la description du modèle en trois *Tiers* prévoit qu'ils soient placés dans le *Tier 1*. Des postes de travail de bureautique peuvent également se trouver catégorisés en *Tier 0* s'ils servent aussi à administrer les ressources les plus sensibles de l'annuaire AD, alors que la description du modèle en trois *Tiers* prévoit qu'ils soient placés en *Tier 2* (puisqu'ils permettent un usage bureautique et sont, à ce titre, davantage exposés à des menaces que d'autres ressources du SI). Or, le niveau de sécurité d'une zone de confiance est celui de son maillon le plus faible et la sécurité du *Tier 0* ne doit pas dépendre de celle des postes de bureautique. À l'extrême, l'ensemble des ressources de l'AD peut logiquement se trouver catégorisé en *Tier 0* si des chemins d'attaque permettent une prise de contrôle triviale des contrôleurs de domaine depuis n'importe quelle ressource de l'AD [9].

9. Cela peut notamment être le cas si un contrôleur de domaine reste exposé à une vulnérabilité critique et triviale à exploiter (par exemple la CVE-2020-1472 [33] mieux connue sous le nom de *ZeroLogon*), mais dont le correctif n'aurait pas été appliqué.

À noter que la catégorisation de certaines ressources en *Tier 1* malgré des chemins d'attaque qu'elles présentent vers le *Tier 0* peut dans certains cas être décidé pour répondre à des contraintes purement organisationnelles ou de gouvernance. C'est notamment le cas lorsque :

- ces ressources sont complexes à administrer et couteuses en temps d'administration au quotidien (les serveurs de messagerie Microsoft Exchange en sont un exemple typique). Ainsi, il peut s'avérer délicat de les faire administrer par des administrateurs de *Tier 0* tout en satisfaisant aux politiques de sécurité en vigueur pour le *Tier 0* et aux recommandations du chapitre 5 (qui traite des architectures d'administration et des possibilités de mutualisation) ;
- l'administration de ces ressources a été externalisée, mais pour des raisons de sécurité ou de gouvernance, l'organisation souhaite paradoxalement que l'administration du *Tier 0* ne le soit pas.

L'objectif de la démarche de cloisonnement du SI en *Tiers* est d'améliorer le niveau de résilience du SI face à des compromissions. À ce titre, il convient de veiller à ne pas créer un *Tier 0* « fourre-tout » qui présenterait une importante surface d'attaque, ni à catégoriser des ressources en *Tier 1* ou en *Tier 2* en ignorant sciemment des chemins d'attaque identifiés vers le *Tier 0*.

Finalement, il est courant (et même tout à fait normal lors des premières itérations du cycle itératif) de constater un décalage plus ou moins important entre la catégorisation effective des ressources du SI et ce qu'elle devrait être selon la description du modèle de gestion des accès privilégiés (tableau 1 page 13). Ce travail de catégorisation doit fidèlement représenter l'état du SI tel qu'il est, et non pas tel qu'il devrait idéalement être d'après la description du modèle. À tout moment il doit être possible de facilement visualiser les risques qui pèsent sur le SI et d'identifier les ressources dont la compromission pourrait entraîner une perte de confiance dans le SI ou dans des valeurs métiers (voire leur perte de contrôle ou leur destruction).

Les anomalies de catégorisation des ressources apparaissent en confrontant la catégorisation effective des ressources du SI à leur catégorisation cible décrite par le modèle. Ces anomalies forment l'écart entre l'état réel du SI et la situation idéale permettant un découpage pertinent du SI en zones de confiance cloisonnées les uns des autres. Cet écart va progressivement se réduire pendant la deuxième phase du cycle itératif, en supprimant des chemins d'attaque grâce à l'accomplissement des actions de sécurisation et de cloisonnement.

Pour faciliter le travail de suivi des anomalies de catégorisation, il est donc utile de maintenir une liste des ressources à plusieurs colonnes contenant par exemple :

- nom de la ressource ou d'un groupe de ressources équivalentes ;
- *Tier* de catégorisation effective après analyse des chemins d'attaque ;
- chemins d'attaque identifiés expliquant cette catégorisation ;
- *Tier* de catégorisation ciblé (c'est à dire, généralement, sa catégorisation idéale au regard de son exposition à la menace et de sa sensibilité, telle que décrite par le modèle de gestion des accès privilégiés) ;
- criticité au regard de la facilité d'exploitation des chemins d'attaque identifiés, du niveau d'attaquant considéré et des besoins de sécurité pour la zone de confiance dont il est question ;
- actions de sécurisation à mener pour traiter ces chemins d'attaque (pour ainsi recatégoriser la ressource vers un *Tier* de moindre sensibilité) ;

- priorité de traitement (qui devrait principalement découler de la criticité et de la nature des actions de sécurisation à mener).

En menant des actions de sécurisation, les ressources du SI vont pouvoir être recatégorisées au fur et à mesure des itérations, de manière à tendre vers un découpage pertinent du SI en zones de confiance et vers un cloisonnement satisfaisant de ces dernières. Le cloisonnement du SI en zones de confiance ne peut donc pas se limiter à la seule catégorisation des ressources, cette dernière étant surtout un prérequis permettant d'identifier et de prioriser les actions concrètes à mener. Cette recherche d'optimisation du cloisonnement du SI en zones de confiance est le fil directeur de la deuxième phase du cycle itératif, développée dans les sections 2.3.4 à 2.3.7.

2.3.4 Application des bonnes pratiques d'administration du SI

Le guide ADMIN [16] précise que l'utilisation du SI et l'administration du SI sont deux usages qu'il convient de séparer, pour éviter qu'une compromission de poste bureautique n'entraîne la compromission de l'AD. Cette séparation des usages est nécessaire pour se prémunir de certains chemins d'attaque. Elle est un des principes fondamentaux de la gestion des accès privilégiés. Sans cette séparation, il est logique que des chemins d'attaque permettent la compromission du *Tier 0* depuis des ressources du *Tier 2* (typiquement, depuis des postes de bureautique).

De la même manière et dans un objectif de cloisonnement des *Tiers*, l'administration d'un *Tier* et l'administration d'un autre *Tier* doivent également être considérés comme étant deux usages distincts et dont la mutualisation ne peut être envisagée que sous certaines conditions.

R8

Cloisonner l'administration de chaque Tier

Les comptes d'administration, postes d'administration et méthodes d'administration utilisés ne doivent en aucun cas nuire au cloisonnement des *Tiers* ; ils ne doivent donc pas créer des chemins d'attaque d'un *Tier* depuis un autre de moindre sensibilité.

L'utilisation de comptes et de postes d'administration dédiés à chaque zone de confiance est une manière de garantir ce cloisonnement. Toutefois, leur mutualisation pour l'administration de plusieurs *Tiers* ou pour différents usages peut être acceptable dès lors que certaines conditions de sécurité sont respectées. Ces conditions revêtent de nombreuses subtilités techniques. Les principales sont abordées dans le chapitre 4 traitant des protocoles NTLM et Kerberos et des implications de ces protocoles sur les bonnes pratiques liées aux comptes et méthodes d'administration utilisés. D'autres sont abordées dans le chapitre 5 dédié aux architectures d'administration.

Attention

Dans ce guide le terme « poste d'administration » est utilisé de manière générale pour désigner les moyens d'administration, qu'il s'agisse de postes d'administration ou de ressources d'administration intermédiaires (c'est à dire des serveurs de rebond d'administration, par exemple, ou des serveurs outils d'administration qui mettent à disposition des outils d'administration centralisés, cf. guide ADMIN [16]).

L'application de la recommandation R8 de cloisonnement de l'administration justifie notamment d'interdire que des postes bureautiques n'administrent des ressources de *Tier 0* et se retrouvent alors catégorisés en *Tier 0* en dépit des risques de sécurité que cela représente (car la compromission d'un de ces postes de bureautique pourrait être le vecteur d'une prise de contrôle de l'AD par un attaquant). En effet, il est rappelé que la zone de confiance la plus sensible doit également être la moins exposée du SI ; les postes de bureautique font partie des ressources les plus exposées aux menaces et le niveau de sécurité d'une zone de confiance est celui de son maillon le plus faible.

2.3.5 Application des bonnes pratiques d'architecture du SI

Les travaux liés aux architectures d'administration sont primordiaux pour préserver le cloisonnement des *Tiers*. D'autres problématiques d'architecture sont également à considérer : architecture AD, architecture de virtualisation, moyens de sauvegarde, réseau, infrastructure de mises à jour, etc. Ces différents aspects ont des implications plus ou moins fortes dans le cloisonnement du SI en zones de confiance, car ils peuvent créer des chemins d'attaque d'une zone à l'autre. Ces travaux d'architecture sont rarement des actions de sécurisation rapides à mener. Ils doivent être anticipés et planifiés au plus tôt puis être pris en considération dès les premières itérations du cycle itératif.

R9

Identifier et mener les travaux d'architecture du SI nécessaires à son cloisonnement

Il est recommandé d'identifier au plus tôt les problèmes d'architecture du SI qui nuisent au cloisonnement des *Tiers*, puis de prioriser et planifier les travaux d'architecture du SI qui sont nécessaires pour tendre vers un cloisonnement optimal des zones de confiance.

Les recommandations relatives à des problématiques d'architecture courantes sont abordées en chapitre 3 (dédié à l'identification et au cloisonnement du *Tier 0*), tandis que celles ayant trait aux architectures d'administration sont développées plus spécifiquement dans le chapitre 5.

2.3.6 Réduction de l'exposition de chaque Tier

Les ressources de *Tier 0* ont généralement vocation à communiquer avec différentes ressources de *Tier 1* et de *Tier 2* pour leur fournir un service, comme c'est par exemple le cas pour les services AD DS (les *Active Directory Domain Services* sont ceux qui portent l'annuaire AD) des contrôleurs de domaine. Toutes les interactions entre ces ressources de *Tier 0* et les autres (de *Tier 1* ou de *Tier 2*) sont de nature à augmenter l'exposition du *Tier 0* à des menaces, car ces ressources ont des niveaux de robustesse variables et elles sont rarement exemptes de vulnérabilités [10]. Si certaines interactions sont inévitables, comme c'est le cas avec les services AD DS et à travers différents protocoles (MS-RPC, MS-Kerberos, DNS, etc.), celles qui sont facultatives sont en revanche à limiter autant que possible afin de minimiser l'exposition du *Tier 0* à des menaces.

Réduire cette exposition implique donc une sélection rigoureuse des ressources et solutions logicielles à intégrer au SI en fonction des garanties de robustesse et de maintien en condition de

10. La vulnérabilité CVE-2021-34527 [34] touchant le service Windows de « spouleur d'impression » peut être citée à titre d'exemple parmi de nombreuses autres. Les contrôleurs de domaine AD exécutant ce service (pourtant inutiles sur de tels serveurs, sauf dans quelques rares exceptions) étaient vulnérables à de l'exécution de code arbitraire à distance depuis n'importe quel poste de travail.

sécurité (MCS) qu'elles présentent. Cette exposition impose également de restreindre au strict minimum nécessaire les interactions qu'elles peuvent avoir avec les autres ressources du SI, à l'aide notamment de segmentation et de filtrage réseau. La sélection de ces solutions logicielles nécessite une analyse qui peut s'appuyer sur différents critères tels que leur réputation, la confiance dans leur éditeur, l'historique de leurs vulnérabilités, les résultats des évaluations de sécurité dont elles font l'objet, leur degré d'exposition à des menaces sur le SI, etc.

Par ailleurs, moins il y a de ressources catégorisées en *Tier 0* et de solutions logicielles qui y sont déployées, moins il y a d'actions d'exploitation et d'administration de *Tier 0* à opérer, ce qui permet de réduire le nombre d'administrateurs de *Tier 0* et donc également le nombre de postes d'administration (ce sujet est abordé plus en détail par le chapitre 5 dédié aux architectures d'administration). Satisfaire à de nombreuses recommandations de ce guide s'en trouve alors facilité et, bien souvent, seul un nombre limité de postes d'administration du *Tier 0* peut suffire. En outre, cela permet de simplifier le *Tier 0* en l'allégeant au maximum ; il est ainsi plus aisé de porter une attention particulière à son durcissement et à la veille quotidienne en SSI (cf. chapitre 8 du guide ADMIN [16]).

R10

Minimiser l'exposition de chaque Tiers

Chaque zone de confiance doit avoir une exposition minimale, et cela est particulièrement prioritaire en ce qui concerne le *Tier 0* et le *Tier 1*.

Réduire cette exposition consiste notamment à limiter et sélectionner rigoureusement les ressources et solutions logicielles intégrées au *Tier 0* et au *Tier 1*, ainsi qu'à réduire au strict minimum leurs interactions possibles avec d'autres zones de confiance. Dans cette optique, il convient de souligner l'importance de tenir à jour un catalogue des applications en usage au sein de l'organisation.

La démarche de réduction de l'exposition du *Tier 0* est traitée spécifiquement dans le chapitre 3 dédié à l'identification et au cloisonnement du *Tier 0*.

Il arrive toutefois que des solutions logicielles déjà déployées sur le SI nuisent au cloisonnement du *Tier 0* ou du *Tier 1*, de par leur complexité, leur conception, ou tout simplement lorsqu'elles ne présentent pas de garanties de robustesse ou de MCS suffisantes. Traiter ces problématiques peut parfois nécessiter d'engager des actions longues ou complexes à mener, notamment lorsque ces solutions logicielles sont fortement ancrées dans le SI ou dans l'activité métier, lorsqu'elles ne sont plus maîtrisées, ou lorsque leur remplacement implique des développements spécifiques. Ces actions à mener ne sont pas seulement techniques, mais peuvent notamment revêtir des contraintes financières ou contractuelles. Il est donc préférable d'identifier ces éventuels points de blocage dès les premières itérations du cycle d'amélioration continue du cloisonnement du SI pour être en mesure de débuter leur traitement au plus tôt.

Information

Certaines solutions logicielles complexes peuvent avoir une forte adhérence avec l'AD, tout en étant compliquées à administrer au quotidien et sans que leur remplacement soit pour autant envisageable. C'est par exemple le cas souvent rencontré de Microsoft Exchange, solution de messagerie qu'il n'est pas toujours évident de

catégoriser en *Tier 1*. Cet exemple de cas particulier est abordé en annexe G de manière à illustrer la problématique. Ces situations ne peuvent être traitées qu'au cas par cas. Elles nécessitent généralement une expertise technique particulière qu'il peut être judicieux de chercher auprès de prestataires de services compétents.

2.3.7 Durcissement système et logiciel

Les solutions logicielles (système d'exploitation, services AD DS, applications et services tiers déployés sur le SI, etc.) disposent généralement de paramètres qui peuvent être utilisés pour les rendre plus ou moins robustes aux attaques. Dans ce cas, il est essentiel de mettre en œuvre ces durcissements pour traiter ou atténuer des chemins d'attaque. À l'inverse, certains de ces paramètres peuvent créer des chemins d'attaque et leur utilisation, bien que parfois courante, n'en constitue pas moins une mauvaise pratique [11].

Une étape importante du cloisonnement du SI consiste donc à utiliser au mieux les configurations sécurisées et les mécanismes de sécurité offerts par les systèmes et solutions logicielles déployés. Les configurations qui affaiblissent la sécurité d'une zone de confiance doivent être repérées et des actions correctives doivent être entreprises. De manière générale, il est conseillé de se référer aux recommandations de sécurisation proposées par les éditeurs eux-mêmes, ainsi qu'aux guides et recommandations de l'ANSSI ou des institutions internationales équivalentes en termes de confiance. Il est par ailleurs à noter que le MCS par l'application des correctifs et des mises à jour participe grandement à assurer la robustesse des systèmes et des solutions logicielles déployés : il doit être mené de manière sérieuse et réactive.

R11

Appliquer les durcissements systèmes et logiciels

Il est recommandé de mettre en œuvre les mesures de durcissement système et logiciel qui participent au cloisonnement des *Tiers*, pour réduire la probabilité d'existence de chemins d'attaque qui permettraient la compromission d'un *Tier* depuis un autre de moindre sensibilité.

Plusieurs recommandations de ce guide impliquent la mise en œuvre de mécanismes de sécurité natifs de Windows et de l'AD qui participent au cloisonnement. En application du principe de défense en profondeur [12], il est par ailleurs recommandé que ce cloisonnement repose sur l'application de mesures de sécurité complémentaires et indépendantes.

Du fait de sa sensibilité, il est particulièrement recommandé de sécuriser et cloisonner prioritairement le *Tier 0* afin d'assurer sa résilience face à des compromissions dans le *Tier 2* ou dans le *Tier 1*. Les différents chapitres de ce guide dressent des recommandations de sécurisation qui ont pour objectif de renforcer ce cloisonnement.

Il convient de préciser que ces configurations et mécanismes de sécurité évoluent au fur et à mesure des versions et des mises à jour, que ce soit des systèmes, de leurs fonctionnalités optionnelles ou

11. C'est le cas par exemple de l'utilisation des attributs *DsHeuristics* [56] pour débrayer des mécanismes de sécurité de l'AD. Certains permettent d'autoriser des opérations LDAP sans authentification, de désactiver la protection apportée par des correctifs de sécurité, etc.
12. Le lecteur est invité à consulter le guide « La défense en profondeur appliquée aux systèmes d'information » [7] de l'ANSSI.

des logiciels installés. Un travail de veille en sécurité est donc nécessaire afin de les identifier et de les mettre en œuvre en continu.

2.3.8 Délégation fine des droits

En environnement AD, les comptes de *Tier 0* doivent être réservés à des actions d'administration rares : configurer les relations d'approbation entre forêts, rajouter de nouveaux domaines, procéder à des extensions de schéma, gérer les comptes et privilèges de *Tier 0*, etc. Les actions courantes d'administration qui ne nécessitent pas un tel niveau de privilèges ne doivent pas être faites par des comptes de *Tier 0*, mais par des comptes de *Tier 1* ou de *Tier 2* grâce aux délégations de droits et de privilèges dont ils bénéficient.

L'application d'un modèle de gestion des accès privilégiés repose donc fortement sur les délégations de droits et privilèges à des comptes d'administration de *Tier 1* ou de *Tier 2*. Ces délégations peuvent notamment prendre les formes suivantes : délégations d'administration [47] sur des objets de l'annuaire AD (comptes utilisateurs, unités organisationnelles, etc.), appartenance à des groupes utilisateurs intégrés [90], ACL (*Access Control List* [13]) sur les systèmes de fichiers ou les clés de registre. La granularité des droits offerte par les systèmes d'exploitation et les applicatifs permet généralement de faire de la délégation fine en accord avec le principe de moindre privilège.

L'usage à bon escient du modèle de permissions RBAC (*Role Base Access Control*) permet d'octroyer des droits et privilèges à des groupes utilisateurs spécifiques. Déléguer l'administration de certaines ressources à des administrateurs revient dans ces conditions à simplement intégrer leurs comptes d'administration à l'ensemble des groupes utilisateurs adéquats. L'affectation des droits et privilèges par utilisation exclusive de groupes utilisateurs est préférable à leur affectation directe à des comptes utilisateurs ; cette bonne pratique facilite l'octroi, le suivi et la suppression des droits aux administrateurs.

R12

Octroyer les droits et privilèges par délégation fine

Il est tout particulièrement recommandé de proscrire ou d'encadrer l'utilisation de droits et privilèges du *Tier 0* pour réaliser des actions d'administration du *Tier 1* ou du *Tier 2*. De la même manière, les droits et privilèges du *Tier 1* doivent aussi peu que possible servir aux actions d'administration du *Tier 2*.

Dans cette optique, il est nécessaire de procéder à de la délégation fine de droits, de sorte à octroyer uniquement les droits et privilèges nécessaires à chaque groupe d'administrateurs pour la réalisation des actions d'administration qui leur incombent (principe de moindre privilège).

L'application de cette recommandation permet de restreindre le périmètre du *Tier 0* en limitant fortement les actions d'administration réalisées avec des droits et privilèges de ce niveau de sensibilité, puisque la grande majorité peut être déléguée à des comptes d'administration du *Tier 1* ou du *Tier 2* sans pour autant créer de chemins d'attaque vers le *Tier 0*.

13. Les ACL sont des listes d'autorisations en lecture, écriture, modification et d'autres autorisations spéciales.

Information

Lorsque des administrateurs sont habitués à réaliser des actions d'administration en PowerShell [84], le principe de JEA [70] (*Just Enough Administration* : « droits strictement suffisants ») peut être mis en œuvre afin de spécifier précisément les capacités PowerShell autorisées aux différents administrateurs : modules, *Cmdlets*, fonctions et paramètres, scripts, etc. Il est ainsi possible de déléguer des actions d'administration très précises et qui requièrent des privilèges élevés (de *Tier 0* par exemple), mais en les restreignant dans un cadre d'exécution maîtrisé qui permet ainsi leur délégation à des comptes d'administration d'un moindre niveau de confiance (de *Tier 1* ou de *Tier 2* par exemple) sans pour autant créer des chemins d'attaque. La mise en œuvre du JEA en PowerShell est largement documentée par le centre de documentation de Microsoft [70].

En conclusion, la délégation fine des droits est un pilier du cloisonnement du SI en *Tiers*. Elle peut être longue à réaliser, mais sans elle la catégorisation des *Tiers* se solderait systématiquement par un résultat peu exploitable composé d'un nombre de ressources appartenant au *Tier 0* disproportionné au regard des ressources du *Tier 1*. Cela nécessiterait une large population d'administrateurs du *Tier 0* et ne permettrait pas de satisfaire à de nombreuses recommandations de ce guide.

2.4 Journalisation et détection

Bien que la journalisation et la détection ne participent pas au cloisonnement du SI, elles jouent un rôle important dans un modèle de gestion des accès privilégiés. En effet, le cloisonnement s'accompagne d'une mise en œuvre de nombreuses mesures de sécurité telles que du filtrage réseau, de la gestion fine des droits, des restrictions à l'authentification, etc. Tout comportement anormal bloqué par ces mesures de sécurité devrait donc attirer l'attention sur la potentielle présence d'un attaquant essayant de progresser d'une zone de confiance à l'autre (c'est à dire par déplacement latéral ou par élévation de privilèges).

R13

Journaliser et centraliser les évènements de sécurité

Il est recommandé de journaliser et centraliser les évènements de sécurité importants du SI. En particulier, il est recommandé de journaliser et centraliser tout évènement pouvant signaler une tentative de contournement des mesures de sécurité mises en œuvre pour assurer le cloisonnement des *Tiers* ou pour bloquer les déplacements latéraux.

La journalisation n'est pas un sujet traité dans ce document, mais elle fait l'objet de deux guides complémentaires de l'ANSSI : « recommandations de sécurité pour l'architecture d'un système de journalisation » [17] et « recommandations de sécurité pour la journalisation des systèmes Microsoft Windows en environnement AD » [18].

R14 +

Détecter automatiquement les potentiels incidents de sécurité

Dans l'idéal, il est recommandé de mettre en œuvre un système de détection des incidents de sécurité reposant sur l'analyse automatique des journaux d'évènements centralisés. En particulier, il est recommandé de configurer des alertes automatiques déclenchées par tout évènement pouvant révéler une tentative de contournement des mesures de sécurité mises en œuvre pour assurer le cloisonnement des *Tiers* ou pour bloquer les déplacements latéraux.

La détection des incidents de sécurité n'est pas un sujet traité dans ce document, mais il est abordé en annexe C du guide « recommandations de sécurité pour l'architecture d'un système de journalisation » [17] de l'ANSSI.

3
Identification et cloisonnement du Tier 0

Le *Tier 0* représente le cœur de confiance d'un SI reposant sur AD et sa protection est une priorité. Les premières itérations du processus d'amélioration continue du cloisonnement du SI en *Tiers* (cf. section 2.3) devraient porter sur l'identification du périmètre du *Tier 0* et sur sa capacité à rester intègre en cas de compromissions dans des zones de moindre confiance. Le chapitre 2 a évoqué la nécessité d'identifier les différentes ressources du SI qui composent le *Tier 0*, étape ayant pour prérequis de mener une analyse des chemins d'attaque vers ces dernières. Cette analyse n'est pas aisée à mener et requiert un certain niveau d'expertise permettant d'identifier des chemins d'attaque parfois complexes et des enchaînements non triviaux de relations de contrôle légitimes entre objets de l'AD. Il est en effet souvent constaté que la catégorisation des *Tiers* est incomplète et que leur cloisonnement est insuffisant, ce qui souligne un besoin d'aide à l'identification et au cloisonnement du *Tier 0*.

Objectif

Ce chapitre a pour objectif de guider dans l'identification du périmètre du *Tier 0* et d'introduire des axes de travail permettant de le circonscrire. Il s'attache à identifier différentes catégories de chemins d'attaque vers le *Tier 0* qui peuvent apparaître pendant le cycle de vie de l'annuaire AD et du SI.

La section 3.1 commence ce chapitre en précisant quelques prérequis de base pour assurer un cloisonnement minimum du *Tier 0*.

La section 3.2 poursuit en dressant une liste des objets sensibles qui sont intégrés par défaut dans un annuaire AD. Elle détaille l'identification des chemins de contrôle AD qui peuvent impliquer ces objets sensibles.

Les chemins d'attaque ne passant pas nécessairement par l'exploitation de chemin de contrôle AD, la suite du chapitre 3 aborde différentes problématiques qui ne relèvent pas spécifiquement de l'annuaire AD. Elles sont essentielles pour éradiquer les chemins d'attaque du *Tier 0* :

- l'accès aux secrets d'authentification, sous leurs nombreuses formes (section 3.3) ;
- l'accès logique au stockage (section 3.4) ;
- les infrastructures de virtualisation (section 3.5) ;
- les agents de gestion (section 3.6) ;
- les protocoles de communication (section 3.7) ;
- l'accès physique aux systèmes (section 3.8).

Information

Bien que les sections 3.3 à 3.8 aient pour ambition d'aider autant que possible à l'identification des différents chemins d'attaque vers le *Tier 0*, elles abordent des problématiques courantes qui sont souvent rencontrées dans les SI reposant sur AD, mais ne sauraient toutefois traiter le sujet de manière exhaustive. En effet, les problématiques rencontrées lors de la mise en œuvre d'un modèle de gestion des accès privilégiés peuvent être nombreuses, car elles dépendent des solutions logicielles déployées dans les SI et des caractéristiques de leur déploiement. Chaque organisation doit adapter les principes détaillés dans ce chapitre à son contexte, les compléter et en décliner des actions de cloisonnement adaptées aux problématiques spécifiques qu'elle peut rencontrer.

Les sections 3.9 à 3.11 portent quant à elles respectivement sur l'utilité d'une structure hiérarchique des unités organisationnelles de l'annaire AD, puis sur le cas particulier de Samba 4 et sur les risques liés au *Cloud*. La section 3.12 termine enfin ce chapitre en rappelant la nécessité d'étendre les principes d'identification des chemins d'attaque et de cloisonnement aux autres zones de confiance du *Tier 1* et de *Tier 2*.

3.1 Prérequis de sécurité

3.1.1 Niveaux fonctionnels des forêts et domaines AD

Dans les environnements AD, certains mécanismes sont liés aux niveaux fonctionnels des forêts (FFL, *forest functional level*) ou des domaines (DFL, *domain functional level*). Ces niveaux fonctionnels désignent les fonctionnalités de l'AD dans ses versions successives, en particulier les fonctionnalités relatives à la sécurité. Ils sont caractérisés par un chiffre allant de 0 (niveau fonctionnel de Windows 2000) à 7 (niveau fonctionnel de Windows Serveur 2016, 2019 et 2022).

Afin de bénéficier de certaines fonctionnalités de sécurité dont la mise en œuvre est recommandée dans ce guide, il est nécessaire d'augmenter préalablement les FFL et DFL. Les niveaux fonctionnels et les fonctionnalités de sécurité principales qu'ils apportent sont les suivantes :

- Niveau de fonctionnalité 2 (Windows Serveur 2003) : ajoute les relations d'approbation de forêts et le support des contrôleurs de domaine en lecture seule (sujet traité en section 3.8.2) ;
- Niveau de fonctionnalité 3 (Windows Serveur 2008) : permet la prise en charge des stratégies de mot de passe affinées (mécanisme abordé en section 3.3.7), de l'algorithme de chiffrement AES (*advanced encryption standard*) pour Kerberos et d'une réplication des partages `SYSVOL` améliorée par DFS-R (*distributed file system replication*) ;
- Niveau de fonctionnalité 4 (Windows Serveur 2008R2) : permet l'utilisation de la fonctionnalité de corbeille AD (protection contre les suppressions accidentelles d'objets) ;
- Niveau de fonctionnalité 5 (Windows Serveur 2012) : permet l'utilisation des fonctionnalités avancées de Kerberos comme l'authentification composée, le blindage et les revendications ;
- Niveau de fonctionnalité 6 (Windows Serveur 2012R2) : introduit de nombreuses fonctionnalités de sécurité, comme les politiques et silos d'authentification (cf. annexe C) et le groupe

de sécurité des utilisateurs protégés (*protected users*, cf. annexe B), qui font l'objet de recommandations de mise en œuvre dans le chapitre 4 dédié à NTLM et Kerberos. Ce niveau de fonctionnalité est donc un prérequis pour la mise en œuvre des recommandations de ce guide ;

- Niveau de fonctionnalité 7 (Windows Serveur 2016, 2019 et 2022) : améliore la sécurité des comptes lorsque l'authentification par carte à puce est utilisée et ajoute les relations d'approbation de forêt de type *privileged identity management* (*PIM trust*).

Pour pouvoir augmenter le DFL, il est nécessaire de préalablement mettre à niveau l'ensemble des contrôleurs de domaine vers un système d'exploitation supportant le niveau désiré. De même, pour augmenter le FFL il est nécessaire que l'ensemble des domaines de la forêt soient d'un DFL équivalent ou supérieur. La documentation [64] de Microsoft présente plus en détail les différents niveaux fonctionnels et décrit la méthodologie d'augmentation des DFL et FFL.

R15

Augmenter les niveaux fonctionnels des domaines et des forêts AD

Les niveaux fonctionnels de l'AD doivent rester les plus élevés possibles afin de profiter des dernières fonctionnalités de sécurité offertes par Windows Serveur pour les services AD DS, Kerberos, etc. Le niveau de fonctionnalité 6 (Windows Serveur 2012R2) est le minimum requis pour mettre en œuvre les recommandations de ce guide.

Attention

Avant toute augmentation du niveau fonctionnel qui pourrait être irréversible, il est primordial de vérifier la compatibilité des DFL et FFL avec les solutions logicielles déployées dans le SI. Certaines ont une adhérence forte au niveau fonctionnel, c'est par exemple le cas de *Microsoft Exchange* (sa matrice de support est disponible dans la documentation [63] de Microsoft). Dans ce cas, la mise à jour de ces solutions logicielles est un prérequis à l'augmentation du DFL et du FFL. Les mises à jour de certaines solutions logicielles complexes sont des projets parfois longs et couteux, il est par conséquent préférable d'identifier au plus tôt les actions s'y rapportant.

3.1.2 Mise à jour des systèmes

Le maintien à jour du SI relève de l'hygiène informatique. Il est d'autant plus important en ce qui concerne les contrôleurs de domaine AD, mais également le *Tier 0* de manière générale du fait de son niveau de sensibilité.

R16

Procéder aux montées de versions Windows des systèmes du Tier 0

Les systèmes d'exploitation des contrôleurs de domaine doivent être mis à jour régulièrement vers les dernières versions stables de Windows Serveur. Cela permet notamment de satisfaire à la recommandation R15 d'augmentation des niveaux fonctionnels des domaines et des forêts AD.

Cette recommandation est également applicable à toutes les autres ressources du *Tier 0*, mais d'une manière bien plus rigoureuse pour celles qui peuvent communiquer avec des ressources de moindre sensibilité.

Attention

Avant toute montée de version de Windows, il est primordial de vérifier sa compatibilité avec les systèmes et solutions logicielles déployés dans le SI. En effet, les montées de version de Windows s'accompagnent de changements qui peuvent entraîner des incompatibilités avec certaines ressources du SI.

À noter également que la montée de version d'un contrôleur de domaine AD peut *de facto* entraîner une augmentation du DFL ou du FFL (cf. section 3.1.1). Il est donc nécessaire de s'informer des nouveautés apportées par une version de Windows, de vérifier les matrices de support des solutions logicielles déployées dans le SI (la compatibilité de *Microsoft Exchange* doit par exemple faire l'objet d'une attention particulière), puis de réaliser des tests avant toute montée de version en production.

R17

Assurer un MCS réactif des systèmes du Tier 0

Les contrôleurs de domaine doivent être tenus à jour de leurs correctifs de sécurité de manière aussi réactive que possible. Il est pour cela recommandé de configurer les contrôleurs de domaine pour qu'ils se mettent à jour directement auprès du service en ligne *Microsoft Update* ou par l'intermédiaire de serveurs WSUS (*Windows Server Update Services*) déployés dans le SI (des points de vigilance concernant la sécurité des services WSUS font l'objet de la section 3.6.2).

Cette recommandation est également applicable à toutes les autres ressources du *Tier 0*, mais d'une manière bien plus rigoureuse pour celles qui peuvent communiquer avec des ressources de moindre sensibilité.

Information

Pour éviter l'application de correctifs de sécurité et le redémarrage éventuel de tous les contrôleurs de domaine dans une courte fenêtre de temps pouvant nuire à la continuité de service, il est conseillé d'échelonner leur mise à jour.

3.1.3 Durcissement des systèmes

Le durcissement des systèmes d'exploitation déployés sur le *Tier 0* est hors du périmètre de ce guide, mais il est un prérequis pour assurer un niveau de sécurité minimum du *Tier 0*.

R18

Appliquer les security baselines aux systèmes du Tier 0

Les systèmes d'exploitation déployés dans le *Tier 0* doivent être durcis en appliquant idéalement les *security baselines* [93] publiées par Microsoft ou des *security baselines* plus restrictives. Ce durcissement doit être fait en cohérence avec les contraintes qui pèsent sur le SI ainsi qu'avec les besoins et objectifs de sécurité.

Il est à noter que les *security baselines* publiées par Microsoft pour les systèmes d'exploitation Windows Serveur contiennent des *baselines* spécifiques pour les serveurs ayant le rôle de contrôleur de domaine.

Les systèmes d'exploitation Windows Serveur dépourvus d'interface utilisateur graphique (c'est-à-dire installés en « *Server Core* » [107]) ont une surface d'attaque réduite. En contrepartie, l'absence d'interface graphique utilisateur peut s'avérer contraignante pour l'administration du système : elle doit se faire par Powershell ou à distance à l'aide des outils d'administration distante (RSAT [92]) ou d'outils équivalents (*Windows Admin Center* [105] par exemple).

R19 +

Utiliser Windows en « Server Core » sur le périmètre du Tier 0

Dans l'idéal, le déploiement de Windows en « *Server Core* » est à privilégier sur les contrôleurs de domaine car cette option d'installation réduit la surface d'attaque.

Cette recommandation est également applicable à tous les serveurs Windows du *Tier 0*, mais plus particulièrement à ceux qui peuvent communiquer avec des ressources de moindre sensibilité.

3.2 Risques relatifs aux chemins de contrôle AD

La présente section guide dans l'identification des objets sensibles d'un annuaire AD et détaille les chemins de contrôle AD qui peuvent exister par leur biais. L'article « chemins de contrôle en environnement AD » [39] traite le sujet des relations de contrôle AD bien plus en détail que ne le fait le présent guide ; il s'agit d'une lecture complémentaire fortement recommandée pour les lecteurs qui souhaiteraient approfondir ce sujet.

Chemin de contrôle AD

Un chemin de contrôle AD est un chemin d'attaque spécifique reposant sur une suite de relations de contrôle logique entre objets de l'annuaire AD. Ces relations de contrôle traduisent la maîtrise légitime d'un objet sur un autre à travers ses droits et propriétés spécifiques. Certains chemins de contrôle AD peuvent mettre en jeu des enchaînements non triviaux de relations de contrôle entre objets, dont l'identification peut donc nécessiter un certain niveau d'expertise.

Les chemins de contrôle AD entre objets de zones de confiance différentes constituent des chemins d'attaque potentiels pour les attaquants.

Ces chemins de contrôle AD sont créés par les administrateurs lors de l'octroi de droits et privilèges sur des objets de l'AD tout au long du cycle de vie de l'annuaire, par modification d'ACL, par ajout d'utilisateurs à des groupes privilégiés, par délégations de droits sur des OU ou des GPO (*Group Policy Object* [65]), etc. Par opposition à ces chemins de contrôle légitimes et créés par les équipes d'administration, des chemins de contrôle AD anormaux et suspects peuvent être le signe d'une compromission de l'AD, récente ou ancienne, par un attaquant ayant cherché a consolider sa persistance sur le SI en s'emménageant des portes dérobées.

La figure 4 illustre deux exemples de chemins de contrôle du *Tier 2* vers le *Tier 0*.

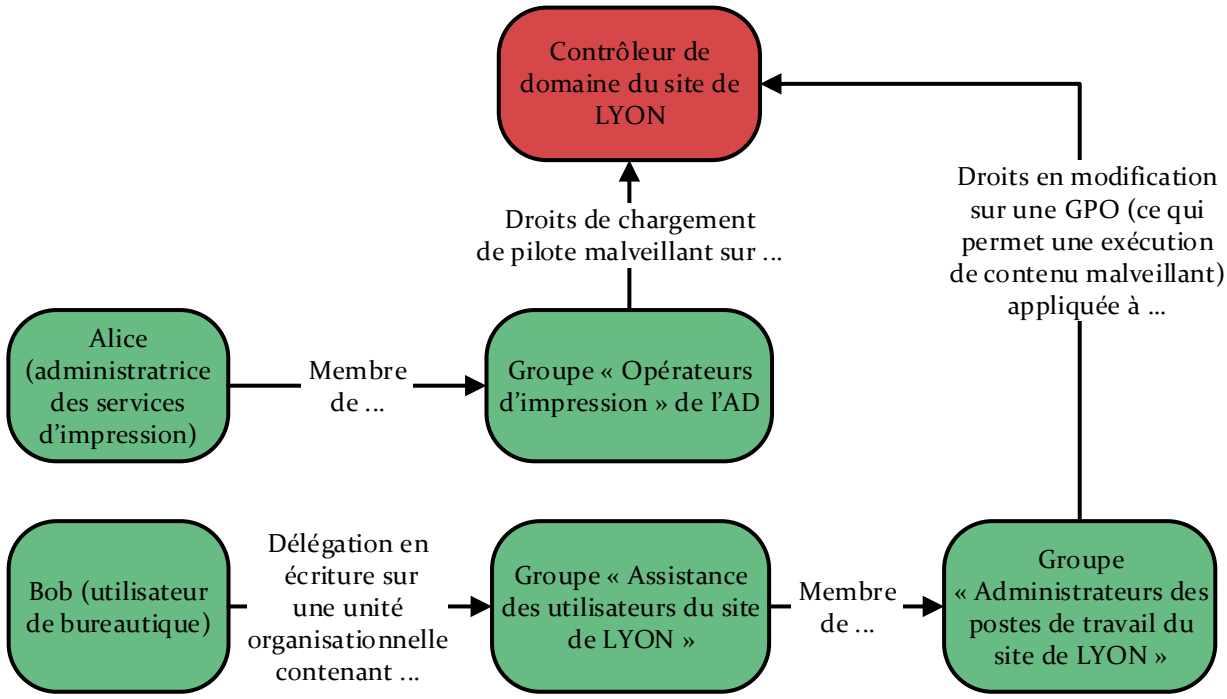

FIGURE 4 – Exemples de chemins de contrôle du *Tier 0* depuis des comptes de *Tier 2*.

L'AD est construit sur un annuaire LDAP intégré [14]. Cet annuaire se compose de différentes partitions permettant le stockage d'objets, chaque objet étant caractérisé par un ensemble d'attributs. Dans les partitions, ces objets sont organisés au sein d'une hiérarchie de conteneurs.

Les trois principales [15] partitions à mentionner sont :

- la partition du domaine AD (il s'agit du « Contexte d'attribution de noms par défaut ») dont la *Microsoft Management Console* (MMC [78]) « Utilisateurs et Ordinateurs Active Directory » offre une vue filtrée. Cette partition fait l'objet de modifications fréquentes et elle est unique par domaine AD ;
- la partition « Configuration », qui contient les informations de configuration et de topologie de la forêt AD, peuplée automatiquement par plusieurs intermédiaires de configuration (Cmdlets PowerShell, consoles MMC, etc.). Cette partition est unique par forêt ;
- la partition de « Schema », qui définit le schéma de l'annuaire LDAP, c'est-à-dire principalement les classes d'objets qui peuvent être créées ainsi que leurs caractéristiques sous forme d'attributs. Cette partition peuplée automatiquement à la promotion d'un contrôleur de domaine est ensuite modifiée lors des rares extensions de schéma réalisées au cours du cycle de vie d'un annuaire AD. Le schéma est lui aussi unique par forêt.

14. Le contenu de l'annuaire LDAP intégré à l'AD peut par exemple être consulté avec l'utilitaire `ADSI Edit` [48] nativement intégré à Microsoft Windows.
15. Il peut également exister des partitions supplémentaires. Le service DNS, par exemple, stocke des informations dans les partitions applicatives « DomainDnsZones » et « ForestDnsZones ».

Information

Bien qu'il soit techniquement possible à un administrateur de modifier manuellement le contenu des partitions LDAP de l'AD, il est fortement déconseillé de le faire. L'administration de l'annuaire devrait se faire exclusivement au moyen des divers Cmdlets PowerShell, consoles MMC et autres interfaces spécialement prévues à cet effet.

Certains objets des partitions LDAP de l'AD sont sensibles dans la mesure où ils permettent le contrôle administratif direct ou indirect des ressources du *Tier 0*. Il est primordial de veiller à les considérer comme des objets de *Tier 0* et à les catégoriser comme tels. C'est le cas notamment de certains conteneurs systèmes ou de configuration, ainsi que de plusieurs comptes et groupes de sécurité intégrés par défaut de l'AD (c'est-à-dire présents dès la mise en service du domaine AD). Tout chemin de contrôle AD identifié vers ces objets doit se traduire par la catégorisation adéquate des objets qui les contrôlent, conformément aux recommandations d'analyse des chemins d'attaque (section 2.3.2) et de catégorisation des ressources (section 2.3.3).

3.2.1 Chemins de contrôle via les conteneurs système ou de configuration

Les trois principales partitions de l'annuaire AD (listées en section 3.2) se composent de conteneurs système ou de configuration dans lesquels sont organisés différents objets sensibles de l'annuaire. La figure 5 illustre une représentation partielle des partitions de l'annuaire AD où ne sont représentés que les conteneurs qui doivent être catégorisés en *Tier 0*. L'annexe A.1 est à consulter pour plus de détails sur la catégorisation en *Tier 0* des conteneurs système ou de configuration.

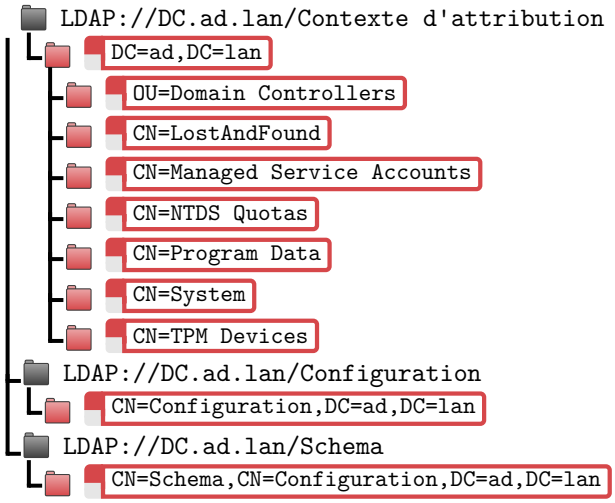

FIGURE 5 – Conteneurs système ou de configuration de l'AD à catégoriser en *Tier 0*.

R20

Analyser les chemins de contrôle vers les conteneurs système ou de configuration du Tier 0

Les conteneurs système ou de configuration sensibles de l'AD listés en figure 5 et détaillés en annexe A.1 doivent être catégorisés en *Tier 0*, ainsi que tout objet de l'AD ayant une relation de contrôle sur ces derniers (généralement du fait de droits en écriture octroyés sur ces conteneurs).

R21

Préserver les permissions des conteneurs système ou de configuration du Tier 0

Comme le contrôle des conteneurs système ou de configuration requiert le plus haut niveau de privilèges, il se trouve déjà délégué à des groupes de sécurité intégrés par défaut de l'AD (cf. section 3.2.2). Il est donc recommandé de ne jamais changer les permissions par défaut de ces conteneurs systèmes ou de configuration. Sauf exception, l'utilisation des groupes de sécurité susmentionnés est à privilégier pour toute délégation de droits d'écriture sur ces conteneurs.

3.2.2 Chemins de contrôle par les comptes et groupes de sécurité intégrés par défaut

Certains comptes et groupes de sécurité intégrés par défaut de l'AD disposent des plus hauts privilèges sur un domaine ou une forêt. Ils sont répartis dans les conteneurs `CN=BuiltIn` et `CN=Users` (du « contexte d'attribution de noms par défaut », cf. section 3.2). La figure 6 illustre une représentation partielle de ces deux conteneurs du « contexte d'attribution de noms par défaut » où ne sont représentés que les objets qui doivent être catégorisés en *Tier 0*. L'annexe A.2 est à consulter pour plus de détails sur la catégorisation en *Tier 0* des comptes et groupes de sécurité intégrés par défaut de l'AD.

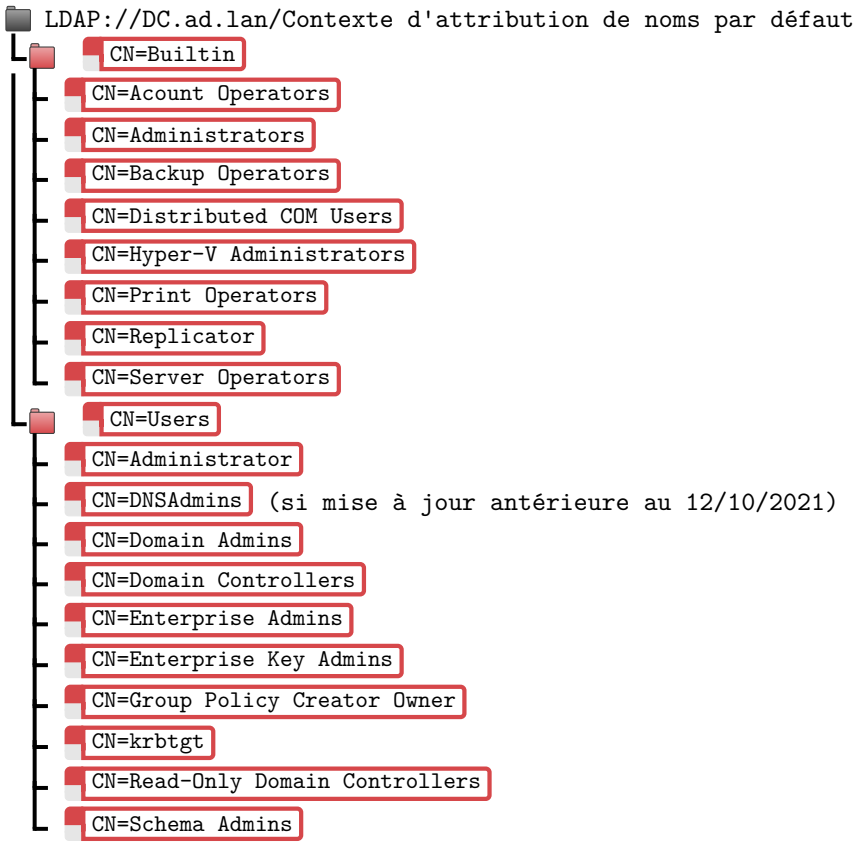

FIGURE 6 – Comptes et groupes de sécurité intégrés par défaut de l'AD à catégoriser en *Tier 0*.

R22

Analyser les chemins de contrôle vers les comptes et groupes de sécurité du Tier 0

Les comptes et groupes de sécurité intégrés par défaut de l'AD listés en figure 6 et détaillés en annexe A.2 sont sensibles et doivent être catégorisés en *Tier 0*. Il en va de même pour tout compte membre de ces groupes et pour tout objet ayant une relation de contrôle sur ces derniers.

Il est à noter que la majorité de ces comptes et groupes de sécurité sensibles listés en figure 6 et détaillés en annexe A.2 font partie des « comptes et groupes protégés » [81] de l'AD (à ne pas confondre avec le groupe des *Protected Users* qui fait l'objet de l'annexe B) ; ils sont donc contrôlés par le mécanisme d'`adminSDHolder` (détaillé dans la documentation [81] de Microsoft) dont le rôle est de préserver les permissions qui leur sont appliquées. Tout objet de l'AD catégorisé en *Tier 0* (car présentant un chemin d'attaque vers le *Tier 0*) devrait donc également faire l'objet d'une sécurisation comparable à celles des « comptes et groupes protégés » [81] de l'AD en leur appliquant la recommandation R23.

R23

Contrôler les permissions appliquées aux comptes et groupes de Tier 0 dans l'annuaire

Les permissions appliquées aux comptes et groupes utilisateurs de l'AD identifiés comme étant de *Tier 0* (c'est-à-dire non pas les permissions que ces derniers ont dans l'AD, mais les permissions qu'ont d'autres objets sur ceux-ci) doivent être suffisamment restrictives pour éviter toute relation de contrôle indirecte du *Tier 0* par leur biais.

Lorsque ces comptes et groupes utilisateurs de *Tier 0* sont membres (directement ou par imbrication) des « groupes protégés » [81] de l'AD, alors les permissions qui leur sont appliquées sont fréquemment et automatiquement corrigées par le mécanisme natif d'`adminSDHolder` [16].

Lorsqu'ils n'en sont pas membres (cas notamment d'un chemin de contrôle AD plus subtil ou d'une capacité d'élévation de privilèges vers *Tier 0* qui ne serait pas liée à un chemin de contrôle AD), il est dans ce cas recommandé de s'assurer que les permissions appliquées à ces comptes de *Tier 0* soient au moins aussi restrictives que celles appliquées par l'*adminSDHolder* (c'est-à-dire en les comparant aux autorisations de l'objet *adminSDHolder*).

3.2.3 Chemins de contrôle par les relations d'approbation

3.2.3.1 Relations d'approbation sortantes extraforêt

Les relations d'approbation sortantes extraforêt – c'est-à-dire qui approuvent le(s) domaine(s) d'une autre forêt – peuvent créer des chemins d'attaque si elles présentent des faiblesses de configuration. Dans ce cas, un attaquant qui compromettrait un domaine extraforêt approuvé (en qui la

16. L'application du mécanisme d'`adminSDHolder` sur un compte utilisateur se traduit par l'affectation automatique de la valeur « 1 » à son attribut `adminCount`. Cette valeur reste ensuite à « 1 », indiquant que le compte a été membre – à un moment donné – d'un groupe protégé [81] de l'AD.

confiance est donnée) serait susceptible d'usurper l'identité de certains comptes utilisateurs ou machines du domaine approuvant (qui fait confiance), incluant potentiellement des comptes et groupes utilisateurs du *Tier 0* de ce dernier.

Information

Les comptes et groupes utilisateurs ayant un RID inférieur à 1000[17] sont de base filtrés (sauf cas particulier des relations de type `PIM_TRUST`) et sont donc exclus des approbations extraforêt. Ces comptes et groupes utilisateurs ayant un RID inférieur à 1000 sont ceux présents par défaut dans l'AD (par opposition à ceux ayant un RID supérieur à 1000, qui sont créés par l'organisation), ce qui inclut les comptes et groupes sensibles listés en figure 6 et détaillés en annexe A.2. En revanche, des objets de l'annuaire peuvent être catégorisés en *Tier 0* sans pour autant être membres de ces groupes sensibles qui sont présents par défaut. C'est par ces derniers que des chemins d'attaque peuvent exister lorsque les relations d'approbation ne les filtrent pas.

Deux configurations dangereuses de relations d'approbation sortantes extraforêt peuvent créer de tels chemins de contrôle AD du *Tier 0* depuis le(s) domaine(s) AD approuvé(s). Il s'agit des relations d'approbation sortantes de type forêt avec *SID history* activé, ainsi que des relations d'approbation sortantes de type domaine (ou « externe ») sans quarantaine.

R24

Durcir la configuration des relations d'approbation AD sortantes extraforêt

Les relations d'approbation sortantes de type forêt ne doivent pas utiliser le mécanisme de « *SID history* » qui réduit leur filtrage. (c'est-à-dire qu'il est recommandé de retirer l'attribut `TREAT_AS_EXTERNAL` de ces relations d'approbation).

Les relations d'approbation sortantes extraforêt de type domaine (ou « externe ») doivent quant à elles voir leur filtrage renforcé par activation du mécanisme de « quarantaine » (ce qui se traduit par l'ajout de l'attribut `QUARANTINED_DOMAIN` sur ces relations d'approbation).

À défaut, appliquer la recommandation R25+ permet d'atténuer le risque de sécurité que représente un filtrage insuffisant des relations d'approbation sortantes extraforêt.

Sans ces précautions, les domaines approuvant et approuvés devraient être considérés comme formant un tout puisqu'ils n'ont pas une frontière de sécurité stricte entre eux. Ils devraient dans ce cas être de sensibilité équivalente et partager le même périmètre technique d'application du modèle de gestion des accès privilégiés (le choix de ce périmètre a été abordé en section 2.2.4).

Les commandes du listing 1 illustrent comment retirer l'attribut `TREAT_AS_EXTERNAL` ou ajouter l'attribut `QUARANTINED_DOMAIN` sur des relations d'approbation sortantes.

17. Pour plus d'informations sur les *relative identifiers*, se référer à la documentation [98] de Microsoft.

```
:: Désactivation du SIDHistory pour une relation d'approbation sortante de type forêt
:: (ce qui revient à retirer l'attribut "TREAT_AS_EXTERNAL")
netdom trust <forêt_approuvant> /domain:<forêt_approuvée> /EnableSIDHistory:no
:: Activation de la quarantaine pour une relation d'approbation sortante de type domaine
:: (ce qui revient à ajouter l'attribut "QUARANTINED_DOMAIN")
netdom trust <domaine_approuvant> /domain:<domaine_approuvé> /Quarantine:yes
:: Attention : sur certaines versions de Windows, les arguments "yes" et "no" doivent être
:: fournis dans la langue du système (c'est-à-dire "Oui" et "Non" pour une version française)
```

Listing 1 – Commandes batch de durcissement de la configuration des relations d'approbation AD sortantes

Information

Les relations d'approbation de type PIM (attribut `PIM_TRUST`), également appelées *PAM trusts* (*privileged access management*), sont généralement utilisées pour approuver des forêts dites « forêts d'administration » (concept développé en section 5.3.2). Ces relations d'approbation spécifiques utilisent le mécanisme de *SID history* et ne filtrent aucun RID. Elles constituent un exemple de relations d'approbation pour lesquelles il est recommandé de mettre en œuvre l'« authentification sélective » (cf. recommandation R25+).

R25 +

Utiliser des relations d'approbation sortantes avec authentification sélective

Dans l'idéal, les relations d'approbation sortantes extraforêt doivent utiliser le mécanisme d'« authentification sélective » (attribut `CROSS_ORGANIZATION`). Cette configuration permet de préciser :

1. quels utilisateurs [18] du(des) domaine(s) approuvé(s) peuvent s'authentifier dans la forêt approuvante (la *trusting forest*) ;
2. vers quelles ressources de la forêt approuvante ces derniers ont le droit de s'authentifier.

Les droits d'authentification doivent alors être accordés de sorte à ne créer aucune relation de contrôle du *Tier 0* d'un domaine à l'autre.

3.2.3.2 Relations d'approbation entrantes

Lorsqu'une forêt AD a une relation d'approbation entrante (elle est approuvée par un domaine AD externe qui lui fait confiance), des utilisateurs de cette forêt peuvent alors s'authentifier par Kerberos auprès de ressources du domaine externe. Ces ressources peuvent avoir été autorisées (légitimement ou par un attaquant) à faire de la délégation Kerberos non contrainte (les dangers des délégations Kerberos sont détaillés en section 4.10). Ce faisant, les utilisateurs de la forêt approuvée sont susceptibles de disséminer leurs secrets d'authentification Kerberos réutilisables sur le domaine externe approuvant, créant ainsi des chemins d'attaque depuis ce domaine externe.

18. Les bonnes pratiques consistent à octroyer les permissions d'authentification à des groupes utilisateurs et non pas directement à des comptes utilisateurs.

R26

Interdire la délégation Kerberos à travers les relations d'approbation entrantes

Les relations d'approbation entrantes doivent être configurées de manière à interdire la délégation Kerberos à travers elles. Cette configuration (réalisable à partir de Windows Serveur 2012) s'opère en désactivant l'option `EnableTGTDelegation`, comme illustré par le listing 2.

```
:: Interdiction de la délégation Kerberos à travers une relation d'approbation entrante
:: (commande à exécuter sur le domaine racine approuvé).
netdom.exe trust <domaine_externe_ou_forêt_tierce_approuvant> /domain:<domaine_racine_approuvé>
        /EnableTGTDelegation:No
```

Listing 2 – Commande batch d'interdiction de la délégation Kerberos à travers une relation d'approbation entrante

3.2.4 Outils d'analyse des chemins de contrôle AD

Si l'identification des comptes de *Tier 0* peut sembler simple lorsqu'il s'agit uniquement de considérer l'appartenance aux groupes de sécurité listés par la figure 6 et détaillés en annexe A.2, elle est en réalité délicate à mener, car les chemins de contrôle AD sont, dans leur majorité, bien plus difficiles à identifier. L'identification des chemins de contrôle AD est donc une tâche fastidieuse et difficile à réaliser manuellement. L'utilisation d'outils d'analyse des chemins de contrôle AD est recommandée pour la mener à bien.

R27

Utiliser régulièrement des outils d'analyse des chemins de contrôle AD

Il est recommandé d'utiliser des outils d'analyse des chemins de contrôle AD vers le *Tier 0* (pour tout type d'objet de *Tier 0* : comptes machines, comptes utilisateurs, groupes, etc.), puis vers toute autre zone de confiance dont le cloisonnement revêt une priorité au regard des besoins et des objectifs de sécurité.

L'utilisation de ces outils doit être régulière pour vérifier si des chemins de contrôle apparaissent ou disparaissent, soit par modification de l'Active Directory, soit par enrichissement des capacités de l'outil.

3.2.4.1 Outils d'analyse des chemins de contrôle AD utilisables en interne

Pour aider les administrateurs à identifier les chemins de contrôle AD dans le SI, ces outils publiés en source ouverte, gratuits et complémentaires, peuvent par exemple être cités :

- « BloodHound » [28] analyse un annuaire AD et produit un graphe illustrant les relations de contrôle AD entre objets. Il est maintenu par *BloodHound Enterprise* ;
- « PingCastle » [109], maintenu par la société du même nom, va au-delà de l'identification des relations de contrôle AD sous forme de graphe. Il s'attache à évaluer le niveau de sécurité de l'annuaire AD et à le retranscrire sous forme d'un tableau de bord ;
- « ADTimeLine » [1] est constitué d'un script PowerShell qui génère une chronologie reposant sur un certain nombre de métadonnées de l'AD considérées comme d'intérêt pour sa sécurité. Il s'agit d'un outil publié, maintenu et utilisé par l'ANSSI.

Information

Il existe également des outils gratuits en versions communautaires et d'autres en versions commerciales payantes pour analyser les chemins de contrôle AD, évaluer le niveau de sécurité d'un annuaire AD, tracer les changements importants, etc.

Attention

Les outils retenus pour l'analyse des chemins de contrôle AD devraient être utilisés à l'aide d'un compte utilisateur de l'AD sans privilèges et depuis un système du *Tier 2*.

La démarche générale à préconiser pour l'identification du *Tier 0* à l'aide de ce type d'outils est la suivante :

1. analyser l'annuaire AD en suivant la documentation de l'outil utilisé ;
2. exécuter des recherches successives de chemins de contrôle AD vers chaque objet de *Tier 0* connu (ceux listés en annexe A, ainsi que ceux identifiés au fur et à mesure des itérations du processus d'amélioration continue du cloisonnement du SI) ;
3. pour chaque graphe ou chemin résultant, vérifier que les chemins de contrôle détectés proviennent uniquement d'objets eux-mêmes catégorisés en *Tier 0*. Si ce n'est pas le cas, alors soit des travaux doivent être menés pour supprimer ces relations de contrôle, soit le *Tier 0* doit s'enrichir de ces objets supplémentaires (conformément au principe de cloisonnement du SI en *Tiers* détaillé en section 2.3).

Le principe du processus d'amélioration continue est d'exécuter à nouveau ces outils chaque fois que la catégorisation des objets de l'AD est modifiée (c'est-à-dire notamment lorsque de nouvelles ressources sont catégorisées en *Tier 0*). Ce processus doit être réitéré de sorte à tendre :

- vers un résultat d'analyse des chemins de contrôle AD qui valide le bon cloisonnement des *Tiers* ;
- vers une catégorisation idéale des ressources, telle que décrite dans le tableau 1 page 13.

La démarche à mener est exactement la même pour identifier les chemins de contrôle AD vers les valeurs métiers et les biens supports du *Tier 1* (dont l'identification a fait l'objet de la section 2.3.1) ou vers toute autre zone de confiance.

Attention

Ces outils se limitent globalement à l'analyse de l'annuaire AD à proprement parler. Les résultats qui en découlent se limitent eux aussi aux chemins d'attaque détectables par la seule analyse de l'annuaire AD ; ils ne représentent qu'une partie des chemins d'attaques qui peuvent exister entre les différentes zones de confiance d'un SI reposant sur AD (cf. sections 3.3 à 3.8).

3.2.4.2 Service en ligne ADS de l'ANSSI

Depuis 2019, l'ANSSI met à disposition un service d'analyse de l'annuaire AD. Ce service, baptisé ADS (*Active Directory Security*) [27], est accessible aux OIV et autorités administratives par courriel adressé à club [AT] ssi.gouv.fr. Les coordinateurs sectoriels ou territoriaux de l'ANSSI peuvent

également être consultés pour plus d'informations. Au-delà de l'analyse des chemins de contrôle vers les conteneurs ou les comptes et groupes intégrés sensibles de l'AD évoqués ci-avant, les différents points de contrôle offerts par ce service peuvent être consultés à l'adresse [27]. De manière simplifiée, ce service ADS repose sur :

- un outil de collecte (ORADAD [108]) à exécuter sur un poste utilisateur de *Tier 2* avec un compte utilisateur non privilégié du domaine AD. Cet outil produit une archive chiffrée qui sera transférée à l'ANSSI pour analyse ;
- un service en ligne de consultation des résultats de l'analyse. Ce service est construit sur le principe du *Zero Knowledge* [19] : le site Web ne contient que des résultats d'analyse chiffrés, leur déchiffrement se faisant à la volée par le navigateur client grâce à une clé privée d'authentification inconnue du site Web et uniquement délivrée au responsable du SI analysé.

R28

Utiliser régulièrement le service ADS de l'ANSSI (si applicable)

Les OIV et les autorités administratives doivent procéder à une analyse régulière de leur AD en utilisant l'outil ORADAD [108] couplé au service ADS [27] mis à disposition par l'ANSSI. Pour permettre un suivi continu des modifications de l'annuaire, cette analyse doit être réalisée à une fréquence inférieure à trois mois. Un rythme d'analyse bimestriel est conseillé pour rapidement détecter des dérives ou résurgences de problèmes potentiellement importants.

Ce service ne couvre que l'analyse de l'annuaire AD à proprement parler ainsi que l'analyse du partage `SYSVOL`. Comme pour les outils cités précédemment en section 3.2.4.1, les résultats qui en découlent se limitent donc aux chemins d'attaque détectables par la seule analyse de l'annuaire AD ; ils ne représentent qu'une partie des chemins d'attaques qui peuvent exister entre les différentes zones de confiance d'un SI reposant sur AD. Les sections qui suivent traitent de chemins d'attaque qui ne sont pas identifiés par les outils d'analyse des chemins de contrôle AD.

3.3 Risques relatifs aux accès à des secrets d'authentification

L'accès aux secrets d'authentification est une catégorie de chemins d'attaque primordiale à traiter et qui revêt certaines subtilités. En effet, les possibilités d'accéder à des secrets d'authentification sont nombreuses, et pour certaines, insuffisamment considérées.

Secret d'authentification

Dans ce guide, le terme « secret d'authentification » désigne tout élément ou combinaison d'éléments secrets permettant techniquement de réussir une authentification, légitimement ou non. Cette authentification peut être de type simple facteur ou multifacteur. Pour plus d'information, se référer au guide « Authentification multifacteur et mots de passe » [2] de l'ANSSI.

19. La conception d'un site Web en *Zero Knowledge* vise à continuer d'assurer la confidentialité des données traitées et stockées par le site Web dans l'hypothèse de sa propre compromission.

Certaines formes de secrets d'authentification sont simples (un mot de passe enregistré en clair par exemple) et d'autres sont plus complexes (condensats d'authentification en mémoire vive, cookies de session, etc.). Ces formes peuvent être physiques (mot de passe séquestré dans une armoire forte, par exemple) ou numériques (mot de passe enregistré dans un fichier texte, dans un navigateur Web, dans un client de connexion, dans un gestionnaire de mots de passe, etc.).

Il est important que toute personne pouvant accéder à un secret d'authentification d'un *Tier* donné soit considérée de ce même *Tier* dès lors que ce secret peut être réutilisé pour usurper le compte en question et ainsi profiter de ses droits et privilèges sur des ressources du SI. Cela est valable quelle que soit la forme du secret d'authentification à partir du moment où celui-ci est réutilisable, que cette réutilisabilité soit très simple (cas du mot de passe en clair) ou difficile (nécessitant par exemple une attaque par exhaustivité, également appelée « attaque par force brute »). Cela est également valable quelle que soit la durée de validité du secret réutilisable et que l'accès à ce secret soit possible constamment ou au contraire ponctuellement. En effet, l'aménagement d'une porte dérobée est une action rapide à réaliser et automatisable : l'obtention d'un secret pendant une courte période de temps est potentiellement suffisante à un attaquant pour obtenir les droits et privilèges associés de manière durable.

Cette réutilisabilité des secrets d'authentification motive en grande partie la recommandation générale R8 de cloisonnement de l'administration de chaque *Tier*, car la sécurisation de l'AD consiste principalement à empêcher la récupération de secrets d'authentification réutilisable d'un *Tier* depuis un autre moins sensible et, plus largement, d'une zone de confiance depuis une autre. Elle motive donc également la recommandation R29, qui consiste à restreindre le périmètre de dissémination des secrets d'authentification réutilisables. Elle est un pilier du cloisonnement des zones de confiance.

R29

Maîtriser la dissémination de toute forme de secret d'authentification réutilisable

De manière générale, tout secret d'authentification sensible et réutilisable catégorisé comme étant d'un *Tier* donné ne doit être accessible, saisi, stocké ou traité que par des comptes et sur des ressources de ce *Tier* ou d'un *Tier* de plus haut niveau de confiance. Ainsi, aucun secret d'authentification réutilisable du *Tier 0* ne doit être accessible, saisi, stocké ou traité sur le *Tier 1* ou le *Tier 2*. Sans cette précaution, des secrets d'authentification réutilisables du *Tier 0* pourraient servir de rebond de compromission d'une zone de confiance à l'autre, ouvrant par exemple la possibilité d'une compromission du *Tier 0* depuis des postes bureautiques du *Tier 2*.

Une vigilance particulière doit être portée à l'identification des secrets d'authentification réutilisables sous toutes leurs formes : mots de passe [20], condensats NTLM, tickets Kerberos, clés privées de certificats, clés SSH, etc. Certaines sont développées dans cette section et font l'objet de recommandations spécifiques. En revanche, les problématiques de sécurité relatives à NTLM et Kerberos sont traitées dans le chapitre 4.

20. À noter que l'utilisation d'un même mot de passe pour différents comptes utilisateurs destinés à l'administration de différentes zone de confiance revient à disséminer un secret d'authentification réutilisable. Ce dernier pourrait servir de rebond de compromission d'une zone de confiance à une autre.

Les condensats NTLM et les secrets Kerberos sont un premier exemple — le plus important — de secrets d'authentification dont la dissémination et la réutilisabilité expliquent qu'ils soient très souvent utilisés par les attaquants pour la latéralisation et l'élévation de leurs privilèges dans un SI reposant sur AD. Comprendre les subtilités liées à leur dissémination et à leur réutilisabilité peut sembler compliqué, mais revêt pourtant une importance capitale pour protéger le *Tier 0*.

Attention

La dissémination des condensats NTLM et des secrets Kerberos constitue un danger important pour un SI s'appuyant sur Active Directory. Le chapitre 4 est dédié à cette problématique et donne des recommandations pour réduire ces risques. L'attention du lecteur est attirée sur la nécessité de prendre en compte ces recommandations, faute de quoi la mise en œuvre de la recommandation R29 resterait très incomplète. La lecture du chapitre 4 est d'ailleurs conseillée avant de poursuivre la lecture du présent chapitre.

Les sections 3.3.1 à 3.3.7 abordent quant à elles d'autres catégories de dissémination de secrets d'authentification réutilisables auxquelles il convient également de prêter attention pour assurer le cloisonnement des zones de confiance.

3.3.1 Comptes d'administration locaux

De mauvaises pratiques de gestion des comptes d'administration locaux des systèmes déployés dans le SI ont pour effet de disséminer des secrets d'authentification réutilisables et peuvent ainsi rendre aisées la latéralisation et l'élévation de privilèges des attaquants. Ces mauvaises pratiques, qui concernent aussi bien les moyens d'accès du *Tier 2* que les serveurs du *Tier 0* et du *Tier 1*, sont principalement :

- la configuration d'un même mot de passe pour les comptes administrateurs locaux sur de nombreux systèmes, et surtout entre systèmes de différents niveaux de sensibilité ;
- la configuration de mots de passe différents pour les comptes administrateurs locaux des différents systèmes, mais qui sont prédictibles (par exemple : dérivés du nom d'ordinateur) ;
- le stockage des mots de passe des comptes administrateurs locaux par les équipes IT dans des fichiers non sécurisés.

Information

Les mots de passe locaux sont stockés par le système d'exploitation sous forme de condensats. Ils peuvent être trouvés par un attaquant à l'aide d'attaques par exhaustivité hors-ligne [21]. Ces attaques peuvent être fortement accélérées par l'utilisation de dictionnaires ou de tables précalculées (*rainbow tables*). Les condensats de ces mots de passe locaux peuvent également être extraits du registre et réutilisés (la réutilisation des condensats NTLM est détaillée en chapitre 4). Il est donc important de prendre en compte la haute probabilité de récupération des secrets d'authentification des comptes locaux par des attaquants, puis de mettre en œuvre des mesures de sécurité limitant leur réutilisation dans le SI.

R30

Diversifier et renouveler automatiquement les mots de passe des comptes admin locaux

Il est recommandé de mettre en œuvre une solution logicielle qui gère de manière sécurisée la diversification et le renouvellement automatique des mots de passe des comptes administrateurs locaux de toutes les ressources intégrées à l'AD (à l'exception des contrôleurs de domaine, cf. recommandation R44).

LAPS [22], de Microsoft, est une solution qui permet de mettre en œuvre cette recommandation ; elle est par ailleurs gratuite, intégrée à l'AD et simple à déployer. À noter que la configuration par défaut de LAPS respecte les recommandations de longueur et de complexité de mot de passe du guide « recommandations relatives à l'authentification multifacteur et aux mots de passe » [2] de l'ANSSI.

Les droits de lecture du mot de passe d'un compte administrateur local (géré par LAPS ou équivalent) d'une ressource de l'AD ne doivent par ailleurs être octroyés qu'à des comptes étant au minimum du même *Tier* que cette ressource. Seuls les administrateurs du *Tier 0* doivent donc avoir des droits de lecture des mots de passe administrateurs locaux des ressources du *Tier 0*.

R30 -

Diversifier manuellement les comptes admin locaux

À défaut de mettre en œuvre une solution logicielle comme LAPS [118] [44], il est alternativement recommandé de désactiver les comptes administrateurs locaux ou d'en faire une gestion manuelle. Dans ce deuxième cas, les mots de passe administrateurs locaux doivent être diversifiés et non prédictibles pour des ressources distinctes. S'ils ne sont jamais renouvelés, ces mots de passe doivent avoir une longueur de 15 caractères minimum (caractères numériques, alphanumériques, majuscules, minuscules et caractères spéciaux).

Ces mots de passe doivent être enregistrés dans des gestionnaires de mots de passe sécurisés (i.e. des coffres-forts numériques) et stockés uniquement sur des ressources du même *Tier* ou d'un *Tier* de plus haut niveau de confiance, puis accessibles uniquement depuis des postes d'administration du même *Tier* ou d'un *Tier* de plus haut niveau de confiance (c'est-à-dire que les mots de passe des comptes administrateurs locaux de ressources du *Tier 0* ne sont pas accessibles depuis le *Tier 1* ou le *Tier 2*).

3.3.2 Secrets accessibles dans les scripts et les partages de fichiers

Les scripts de démarrage, d'ouverture de session, de fermeture de session et d'extinction sont accessibles en lecture par les utilisateurs du domaine AD (de manière légitime, pour pouvoir les

21. Les attaques par exhaustivité menées hors-ligne sont généralement limitées par la seule performance du matériel utilisé, par opposition aux attaques en ligne qui sont généralement très freinées par les couches applicatives et réseaux. Une attaque par exhaustivité menée hors-ligne permet de retrouver un mot de passe de 8 caractères en moins d'une semaine avec du matériel grand public.

22. Windows LAPS [118] – qui est une évolution fonctionnelle de LAPS – est une fonctionnalité native de Windows depuis les versions 21H2 de Windows 10 et Windows 11 et depuis les mises à jour d'avril 2023 de Windows Serveur 2019 et Windows Serveur 2022. La version historique de LAPS [44] continue d'être utilisable, en revanche les deux solutions ne doivent pas être utilisées simultanément sur un système.

exécuter), que ce soit sur le partage SYSVOL ou dans tout autre partage de fichiers où ils seraient stockés. Ils peuvent donc être consultés par tout individu malveillant disposant d'un accès non privilégié sur un système du SI. C'est aussi potentiellement le cas des scripts utilisés par les équipes IT pour d'autres usages. Tout secret d'authentification (mot de passe, clé d'accès, etc.) qu'ils contiendraient serait dès lors trivialement réutilisable. La récupération de secrets d'authentification dans des scripts peut aider un attaquant dans sa recherche d'élévations de privilèges successives vers les zones de confiance les plus sensibles.

R31

Traiter les risques liés aux secrets réutilisables figurant dans des scripts

En application de la recommandation générale R29 de maîtrise de la dissémination de secrets d'authentification réutilisables du *Tier 0*, aucun mot de passe ou autre secret d'authentification réutilisable sensible ne doit figurer dans des scripts accessibles en lecture par des comptes de moindre privilège.

Une attention particulière doit donc être portée à tout le contenu du partage SYSVOL ainsi qu'à tout autre partage ayant un rôle similaire dans le SI. Cette attention vaut également pour tous les scripts qui seraient téléversés sur les systèmes par l'intermédiaire de solutions de gestion centralisée.

Les scripts ne sont toutefois pas les seuls dangers potentiels du partage SYSVOL : les préférences des stratégies de sécurité (les *Group Policy Preferences* ou GPP, c'est-à-dire la catégorie « Préférences » des GPO) font également peser un risque de divulgation de secrets d'authentification réutilisables. Plus précisément, toute configuration faisant intervenir le renseignement d'un mot de passe dans une GPP aboutit à la divulgation de ce dernier, que ce soit pour la configuration des lecteurs réseaux, utilisateurs et groupes locaux, sources de données, imprimantes, services Windows, tâches planifiées ou à exécution immédiate, etc. Ces mots de passe sont enregistrés dans des fichiers XML du partage SYSVOL et sont chiffrés avec une clé de chiffrement symétrique universelle qui a été révélée [51] par Microsoft. Ils peuvent donc être trivialement déchiffrés par un attaquant.

Information

Le correctif KB2962486 de Microsoft, publié en mai 2014, modifie la console MMC d'édition des GPP de manière à ce qu'elle bloque la saisie de mots de passe dans ces dernières. Il est à installer :

- sur les serveur antérieurs à Windows Serveur 2016 depuis lesquels l'AD serait administré à l'aide des MMC natives ;
- sur les systèmes antérieurs à Windows 10 et qui seraient équipés des outils d'administration AD distante.

Après s'être assuré du déploiement de ce correctif sur tous les systèmes utilisés pour l'administration AD par MMC, il est également nécessaire de vérifier que des GPP historiques du domaine AD ne contiennent pas de mots de passe enregistrés antérieurement à la date d'installation du correctif (la commande batch du listing 3 permet de les lister).

```
:: Remplacer <FQDN> par le nom de domaine complet de l'AD.
findstr /S /I cpassword \\<FQDN>\sysvol\<FQDN>\policies\*.xml
```

Listing 3 – Commande batch permettant de lister les mots de passe enregistrés dans des GPP du partage `SYSVOL`

R32

Prohiber les mots de passe enregistrés dans des GPP

En application de la recommandation générale R29 de maîtrise de la dissémination de secrets d'authentification réutilisables du *Tier 0*, aucun mot de passe ne doit être renseigné dans des GPP.

3.3.3 Comptes d'exécution des tâches planifiées et des services Windows

Les tâches planifiées et services Windows sont également sujets à de mauvaises pratiques de configuration qui peuvent aboutir à la présence de secrets d'authentification réutilisables sur les systèmes. Pour supprimer cette source de dissémination, aucune tâche planifiée ou service Windows ne devrait s'exécuter avec un compte utilisateur[23] sensible de l'AD, car cette mauvaise pratique entraîne :

- le stockage de son mot de passe sur le disque, dans le registre, par l'autorité de sécurité locale (*Local Security Authority*, LSA). Il peut en être extrait par un attaquant (après obtention des privilèges d'administration locaux, ou par accès physique au disque dur) puis réutilisé pour s'authentifier auprès d'autres ressources du SI ;
- le stockage en mémoire vive de son secret d'authentification, qui peut également être extrait et réutilisé par un attaquant pour s'authentifier auprès d'autres ressources du SI (se référer au chapitre 4 dédié aux problématiques de condensats NTLM et de secrets Kerberos).

L'utilisation de comptes système locaux [55] est à privilégier étant donné qu'ils n'ont pas de secrets d'authentification réutilisables sur d'autres ressources du SI (ils n'ont, pour ainsi dire, de validité que sur le système local). Il s'agit des comptes `NT AUTHORITY\SYSTEM`, `NT AUTHORITY\LocalService` ou `NT AUTHORITY\NetworkService`, le choix du compte le plus adapté se faisant en fonction des droits et privilèges [55] requis par la tâche planifiée ou le service Windows. Il est à noter qu'une tâche planifiée peut également s'exécuter dans le contexte d'une session utilisateur ouverte, donc sans être associée à un compte utilisateur spécifique.

R33

Traiter les risques liés aux secrets réutilisables des tâches planifiées et des services Windows

En application de la recommandation générale R29 de maîtrise de la dissémination de secrets d'authentification réutilisables du *Tier 0*, aucun secret d'authentification réutilisable sensible ne doit être exposé hors de sa zone de confiance par l'intermédiaire de tâches planifiées ou des services Windows.

Lorsque l'utilisation de comptes de service du domaine s'avère incontournable, alors il est recommandé de leur appliquer le principe de moindre privilège et de limiter leurs droits et privilèges à un périmètre de ressources le plus restreint possible au sein

23. Les comptes utilisateurs de l'AD utilisés pour des traitements automatisés tels que de l'exécution de tâches planifiées ou de service Windows sont communément appelés des « comptes de service ».

de leur zone de confiance. En complément, l'utilisation de *Managed Service Accounts* est une bonne pratique (sujet développé en section 4.14).

R34

Traiter les risques liés au contenu exécuté par les tâches planifiées et services Windows

Il est recommandé de s'assurer que les tâches planifiées et services Windows configurés pour s'exécuter avec des droits et privilèges élevés n'exécutent pas des fichiers (scripts ou binaires notamment) stockés à des emplacements – locaux ou sur des partages réseau – potentiellement accessibles en écriture avec des droits et privilèges moindres. Le cas échéant, un attaquant pourrait remplacer le contenu original et ainsi faire exécuter du code arbitraire avec des droits et privilèges plus élevés que les siens.

R35

Protéger les accès aux partages réseau hébergeant du contenu exécutable

Les partages réseaux depuis lesquels sont exécutés des fichiers (scripts ou binaires notamment) avec des droits et privilèges élevés doivent être accédés par les systèmes clients avec une authentification mutuelle et un contrôle d'intégrité. Les *security baselines* (cf. recommandation R18) recommandent à ce titre la configuration de la stratégie de sécurité activant la fonctionnalité *UNC Hardening* [67] pour l'accès aux partages SYSVOL et NETLOGON des contrôleurs de domaine. Cette liste doit être complétée avec tout autre partage réseau nécessitant une authentification mutuelle et un contrôle d'intégrité.

Dans le cas plus spécifique de comptes utilisateurs du domaine utilisés comme comptes de service gérés manuellement (c'est-à-dire dont le mot de passe n'est pas changé automatiquement, par opposition aux *Managed Service Accounts*), ceux qui ont un SPN (*Service Principal Name* [102]) Kerberos déclaré dans l'AD (généralement pour permettre une authentification au service par authentification Kerberos à travers le réseau) doivent faire l'objet d'une vigilance particulière. Ce sujet est développé dans le chapitre 4 dédié à NTLM et Kerberos (section 4.13).

3.3.4 Secrets délivrés par des infrastructures de gestion de clés

Les infrastructures de gestion de clés (IGC ou PKI pour *private key infrastructure*) délivrent des certificats qui peuvent parfois permettre des accès privilégiés à des zones de confiance sensibles allant jusqu'au *Tier 0* (via les authentifications par certificat notamment). De tels certificats (en réalité : les clés privées qui leur sont associées) sont des secrets cryptographiques qui doivent donc être considérés comme des secrets d'authentification potentiellement sensibles et réutilisables. Ils doivent à ce titre faire l'objet d'une sécurisation adéquate au niveau de confiance approprié.

R36

Traiter les risques inhérents aux IGC qui pèsent sur le Tier 0

Dès lors qu'une IGC permet la génération de certificats utilisables pour de l'authentification (en réalité : les clés privées qui leur sont associées) sur le *Tier 0* alors une préoccupation particulière doit être portée à sa sécurisation. Cette IGC ne doit pas

offrir de chemins d'attaque vers le *Tier 0* depuis des *Tiers* de moindre confiance, que ce soit par exemple à travers l'administration des systèmes qui la portent, à travers des délégations de droits sur des capacités de génération de certificats, ou à travers les modèles de certificats publiés.

Les services AD CS (*Active Directory Certificate Services*) de Microsoft sont souvent utilisés en environnement AD pour générer des certificats d'authentification. Ils doivent faire l'objet d'une sécurisation spécifique qui est hors du périmètre du présent guide.

Attention

Il est rappelé que les conteneurs de certificats de l'annuaire AD sont sensibles (se référer à la recommandation R20 d'analyse des chemins de contrôle AD vers les conteneurs système ou de configuration sensibles).

R37

Proscrire l'utilisation de certificats faibles ou vulnérables du Tier 0

Les certificats faibles ou vulnérables qui donnent accès à des droits ou privilèges de *Tier 0* sont à proscrire. Ces certificats doivent au minimum satisfaire aux contraintes suivantes :

- l'algorithme DSA n'est pas utilisé pour la signature du certificat (privilégier RSA ou ECDSA) ;
- les fonctions de hachage utilisées pour la signature du certificat doivent être SHA2 ou SHA3 ;
- la taille des clés RSA est d'au moins 2048 bits (pour une utilisation ne devant pas dépasser l'année 2030, sinon leur taille est d'au moins 3076 bits pour toute utilisation au delà de 2030, cf. le référentiel général de sécurité [19]) et les exposants publics strictement supérieurs à 65536 ;
- la biclé RSA est générée à l'aide d'une bibliothèque à jour (pour éviter les vulnérabilités d'implémentation connues, comme la CVE-2017-15361 [38]).

Enfin, il est à noter que les clés privées des certificats stockés dans le magasin de certificats de Windows avec la propriété « clé privée non exportable » peuvent en réalité être exportées avec des outils d'attaque grand public exécutés avec les plus hauts privilèges du système. Cette propriété n'est donc pas une mesure de sécurité évitant leur réutilisation.

3.3.5 Secrets d'accès des API

Les secrets d'accès à des API (ces secrets sont généralement appelés « clés API » et se présentent sous la forme d'une longue chaîne de caractères aléatoire) permettent parfois d'accéder à des données sensibles ou d'exécuter des actions avec des privilèges élevés. Ce cas de figure se présente le plus souvent lors de l'utilisation de services de *Cloud* privés ou publics. Pour autant, de tels secrets sont rarement renouvelés et lorsqu'un attaquant réussit à en obtenir, ils lui fournissent une porte dérobée durable et qui est, de surcroît, rarement supervisée.

R38

Traiter les risques inhérents aux secrets d'accès à des API sensibles

Les secrets d'accès à des API doivent être considérés comme des secrets d'authentification réutilisables.

Dans un SI – et plus particulièrement lorsque celui-ci s'étend dans des services de *Cloud* privés ou publics – des API peuvent disposer de droits et privilèges sensibles allant jusqu'au *Tier 0* dès lors qu'ils permettent l'exécution d'actions susceptibles d'en permettre le contrôle. En application de la recommandation générale R29 de maîtrise de la dissémination de secrets d'authentification réutilisables du *Tier 0*, les secrets d'accès à des API d'une zone de confiance donnée ne doivent être accessibles qu'au sein de cette même zone ou d'une zone de plus haut niveau de confiance.

3.3.6 Cas des secrets d'authentification stockés sur des supports physiques

Les équipes IT sont généralement amenées à stocker des secrets d'authentification en clair sur des supports physiques (qu'ils s'agisse de supports numériques tels que des clés USB, ou de supports non numériques en papier par exemple). Il s'agit typiquement des secrets d'authentification relatifs à des comptes de séquestre ou « bris de glace » sensibles qui visent notamment à permettre la reconstruction de systèmes en cas d'incident majeur (exemple : les mots de passe DSRM [24] [57]).

Pour protéger ces mots de passe, des mesures organisationnelles sont généralement mises en œuvre (typiquement, un support physique contenant des secrets d'authentification sera stocké dans une armoire forte). Quand ces secrets permettent la reconstruction de systèmes de *Tier 0*, alors ils doivent être accessibles et manipulables exclusivement par des administrateurs disposant de comptes de *Tier 0*.

R39

Traiter les risques liés aux accès physiques à des secrets réutilisables du Tier 0

En application de la recommandation générale R29 de maîtrise de la dissémination de secrets d'authentification réutilisables du *Tier 0*, seuls les administrateurs disposant de comptes de *Tier 0* doivent avoir un accès physique à des supports (numériques ou physiques) contenant des secrets d'authentification réutilisables du *Tier 0*.

Attention

La méthode d'installation d'un contrôleur de domaine AD depuis un média – méthode communément appelée AD IFM (*AD Install From Media*) – repose sur l'utilisation d'un fichier qui contient la base `NTDS.dit` de l'annuaire et donc les secrets d'authentification de l'AD. Il s'agit d'un fichier sensible à protéger au niveau *Tier 0*.

24. À noter que Windows LAPS [118] sait gérer le stockage sécurisé et le renouvellement automatique des mots de passe DSRM.

3.3.7 Renouvellement et robustesse des mots de passe

Les stratégies de mots de passe simples[25] ne peuvent s'appliquer qu'au niveau du domaine AD dans sa globalité. Elles ne sont pas utilisables pour configurer des stratégies applicables à certains groupes utilisateurs uniquement ; elles ne permettent donc pas de définir des stratégies différentes par zone de confiance par exemple.

Si ces stratégies simples sont la plupart du temps configurées, il est en revanche moins répandu que des stratégies plus contraignantes soient définies pour les comptes plus sensibles (d'administration ou de service notamment). Pour répondre à ce besoin, il est nécessaire de recourir à la configuration de « stratégies de mots de passe affinées » (*fine grained password policies*) (en créant des *password settings objects*, PSO [86]), comme cela est par exemple recommandé en section 4.13 pour les comptes de service. Pour plus de détails sur les stratégies de mot de passe affinées, le lecteur est invité à consulter la documentation [86] de Microsoft.

R40

Appliquer des stratégies de mot de passe affinées pour les comptes du Tier 0

Différentes « stratégies de mot de passe affinées » doivent être mises en œuvre pour garantir l'application de contraintes sur les mots de passe adaptées aux différents besoins de sécurité : par zone de confiance, par cas d'usage des comptes, etc. Les stratégies configurées doivent respecter les recommandations du guide « Recommandations relatives à l'authentification multifacteur et aux mots de passe » [2] de l'ANSSI. Le listing 4 illustre comment créer une stratégie satisfaisant à ces recommandations pour les comptes de *Tier 0*.

```
# Création d'un PSO requérant un mot de passe de 16 caractères, sans verrouillage, avec une durée
# d'expiration de 1 an (365 jours), prioritaire (precedence de 1), stocké sans chiffrement
# réversible, complexe et protégé contre la suppression accidentelle :
New-ADFineGrainedPasswordPolicy "PSO_T0_Accounts" -ComplexityEnabled:$true `
    -LockoutThreshold:"0" -MaxPasswordAge:"365.00:00:00" -MinPasswordLength:"16" `
    -Precedence:"1" -ReversibleEncryptionEnabled:$false `
    -ProtectedFromAccidentalDeletion:$true -ComplexityEnabled:$true
# Application de ce PSO au groupe "T0_Accounts"
# (exemple de groupe qui serait créé et peuplé par les équipes d'administration et qui
# contiendrait tous les comptes utilisateurs de l'AD de T0) :
Add-ADFineGrainedPasswordPolicySubject -Identity "PSO_T0_Accounts" -Subjects "T0_Accounts"
```

Listing 4 – Script PowerShell de création et d'affectation d'une stratégie de mot de passe affinée pour les comptes de *Tier 0*

Certains comptes de l'AD ont par ailleurs un mot de passe entièrement géré par les contrôleurs de domaine eux-mêmes. C'est le cas notamment des comptes d'ordinateur, mais pas seulement. Les comptes suivants qui répondent à ce cas de figure sont à considérer comme sensibles :

- le compte `krbtgt`, dont le condensat du mot de passe est utilisé pour chiffrer et signer tous les tickets Kerberos du domaine ;
- les comptes de *trust* (TDO, *trusted domain object*), qui portent les secrets d'authentification des relations d'approbation AD ;

25. Les stratégies de mots de passe simples sont celles qui se configurent par GPO à l'emplacement « `Configuration ordinateur\Paramètres Windows\Paramètres de sécurité\Stratégies de compte\Stratégie de mot de passe` ».

- les comptes d'ordinateur des ressources sensibles.

Il n'est pas suffisant de laisser les contrôleurs de domaine gérer automatiquement ces trois catégories de comptes : des contrôles manuels complémentaires sont nécessaires. Ces actions supplémentaires sont l'objet des recommandations R41 à R43.

R41

Renouveler régulièrement le mot de passe du compte krbtgt

Le mot de passe du compte `krbtgt` doit être renouvelé chaque année par les administrateurs. La procédure à suivre est expliquée dans la documentation [89] de Microsoft, elle doit être suivie scrupuleusement sous peine de causer d'importantes indisponibilités de services.

Le script PowerShell du listing 5 permet d'afficher le nombre de jours écoulés depuis le dernier changement de mot de passe du compte `krbtgt`.

```
(New-TimeSpan -Start (Get-ADUser krbtgt -Prop PasswordLastSet).PasswordLastSet `
    -end (Get-Date)).Days
```

Listing 5 – Script PowerShell de calcul du nombre de jours écoulés depuis le dernier changement de mot de passe du compte `krbtgt`

R42

Contrôler le renouvellement des mots de passe des comptes de trust

Les mots de passe des TDO sont renouvelés automatiquement tous les trente jours. Il convient néanmoins de régulièrement contrôler (chaque trimestre par exemple) qu'il n'existe pas de TDO échappant à cette règle, car cela pourrait être un signe de compromission ou de dysfonctionnement.

Le script PowerShell du listing 6 permet d'afficher le nombre de jours écoulés depuis le dernier changement de mot de passe de chaque TDO.

```
ForEach ($tdo in Get-ADObject -Filter "objectclass -eq 'trustedDomain'" -Prop PwdLastSet){
    $days = (New-TimeSpan -Start ([datetime]::FromFileTime($tdo.PwdLastSet)) `
        -end (Get-Date)).Days
    $tdo.name + " : " + $days + " jours"
}
```

Listing 6 – Script PowerShell d'affichage du nombre de jours écoulés depuis le dernier changement de mot de passe de chaque TDO

R43

Contrôler le renouvellement des mots de passe des comptes d'ordinateur sensibles

Les mots de passe des comptes d'ordinateur sont renouvelés automatiquement tous les trente jours. Il convient néanmoins de régulièrement contrôler qu'il n'existe pas de comptes d'ordinateur sensibles échappant à cette règle, car cela pourrait être un signe de compromission ou de dysfonctionnement. Les comptes d'ordinateur sensibles à considérer sont au minimum :

- tout compte d'ordinateur du *Tier 0* (contrôleurs de domaine, postes d'administration du *Tier 0*, etc.) ;

- les ordinateurs de type serveur du *Tier 1* et du *Tier 2* ;
- les comptes d'ordinateur des postes d'administration (quel que soit le *Tier* qu'ils administrent).

Il est toutefois à noter qu'un ordinateur hors-ligne ne peut pas changer son mot de passe. Des faux positifs sont donc attendus si des systèmes sont légitimement hors-ligne de manière prolongée. Une levée de doute est généralement recommandée après 45 jours d'absence de renouvellement de mot de passe.

Le script PowerShell du listing 7 permet de lister les ordinateurs (en indiquant également leur système d'exploitation) dont le mot de passe a été renouvelé il y a plus de 45 jours.

```
ForEach ($comp in Get-ADObject -Filter "objectclass -eq 'computer'" `
    -Prop pwdLastSet, operatingSystem){
    $days = (New-TimeSpan -Start ([datetime]::FromFileTime($comp.PwdLastSet)) `
        -end (Get-Date)).Days
    if ($days -gt 45){
        $comp.name + " : " + $days + " jours (" + $comp.operatingSystem + ")"
    }
}
```

Listing 7 – Script PowerShell qui liste les ordinateurs dont le mot de passe a été renouvelé il y a plus de 45 jours

Enfin, le compte administrateur intégré de l'AD (RID 500), qui est bien entendu du *Tier 0*, devrait être un compte bris de glace (ou compte de secours). C'est-à-dire que, sauf rares exceptions, il ne devrait pas être utilisé par les administrateurs du *Tier 0* et ces derniers devraient utiliser exclusivement des comptes d'administration nominatifs. La robustesse et le renouvellement du mot de passe du compte administrateur intégré de l'AD doivent donc faire l'objet d'une procédure spécifique.

R44

Assurer la robustesse du mot de passe du compte administrateur intégré de l'AD

Le compte administrateur intégré de l'AD (RID 500) doit se voir imposer un mot de passe complexe, d'une longueur supérieure à 32 caractères et renouvelé au minimum tous les 3 ans. Une procédure organisationnelle doit donc être définie pour procéder à son changement et pour y accéder.

Le script du listing 5 peut être adapté pour vérifier la date de dernier renouvellement du mot de passe du compte administrateur intégré de l'AD.

3.4 Risques relatifs aux accès logiques au stockage

Tout accès en lecture à des données sensibles telles que les fichiers du système d'exploitation d'une ressource de *Tier 0* peut induire l'obtention potentielle de ce niveau de droits et privilèges. En effet, les fichiers d'un système d'exploitation peuvent contenir certaines formes de secrets d'authentification qui pourraient être remplacés ou réutilisés de manière à octroyer des droits et privilèges du *Tier 0* (se rapporter à la section 3.3).

Il est par ailleurs nécessaire de prendre en compte tout type d'accès logique à du stockage, que ce soit par exemple une infrastructure de stockage en réseau, une infrastructure de sauvegarde, une image disque ou bien un support de stockage amovible (une clé USB par exemple), puis d'identifier les données sensibles qui y sont stockées et dont l'obtention pourrait permettre des chemins d'attaque vers le *Tier 0*. Il est à noter que la tendance actuelle à la mutualisation des ressources et à l'éclatement géographique des infrastructures de stockage participe à complexifier l'identification pertinente du périmètre du *Tier 0*.

Après plusieurs itérations du cycle d'amélioration continue de cloisonnement du SI en *Tiers*, les aménagements du SI concernant les infrastructures de sauvegarde et les infrastructures de stockage en réseau – abordés respectivement dans les sections 3.4.1 et 3.4.2 – devraient avoir été étudiés en vue de réduire au strict nécessaire le périmètre du *Tier 0*.

3.4.1 Infrastructures de sauvegarde

Des infrastructures de sauvegarde sont utilisées sur la quasi-totalité des SI afin d'en assurer la disponibilité. Se pose dans ce cas la question de leur catégorisation en *Tier 0* ou en *Tier 1*. En effet, des ressources du *Tier 0* doivent être sauvegardées et par défaut cela implique la catégorisation de l'infrastructure de sauvegarde en *Tier 0*. Pour autant, cela alourdirait la charge d'administration du *Tier 0* et en augmenterait significativement la surface d'attaque, ce qui n'est pas souhaitable.

Ce constat peut amener une organisation à privilégier une catégorisation des infrastructures de sauvegarde en *Tier 1* en les décorrélant du niveau de privilèges du *Tier 0*, ce qui implique qu'elles ne puissent pas se connecter à des ressources de *Tier 0* ou manipuler des données sensibles du *Tier 0*. Les sauvegardes du *Tier 0* seraient dans ce cas réalisées en respectant les contraintes suivantes :

1. elles sont faites (par script ou à l'aide d'une solution logicielle) et opérées uniquement sur des ressources catégorisées en *Tier 0* et des supports de stockage en ligne du *Tier 0* ;
2. elles sont chiffrées sur le *Tier 0*, à l'aide d'un secret long et complexe exclusivement stocké (et accessible) sur (et par) des ressources de *Tier 0* tout en suivant les règles de l'art en matière de chiffrement (le lecteur est notamment invité à consulter l'annexe B2 du référentiel général de sécurité [20] de l'ANSSI). Ce secret de chiffrement est également stocké sur des supports numériques amovibles ou sur papier dont l'accès physique est suffisamment protégé, pour être utilisable en cas d'incident nécessitant une restauration à partir des sauvegardes. Ces données, une fois chiffrées, ne sont plus considérées de *Tier 0* et peuvent donc être déplacées sur des *Tiers* d'un moindre niveau de confiance ;
3. elles sont téléversées (les archives chiffrées uniquement) vers une ressource de *Tier 1* (ou téléchargées depuis une ressource de *Tier 1*) afin d'y être sauvegardées de manière classique.

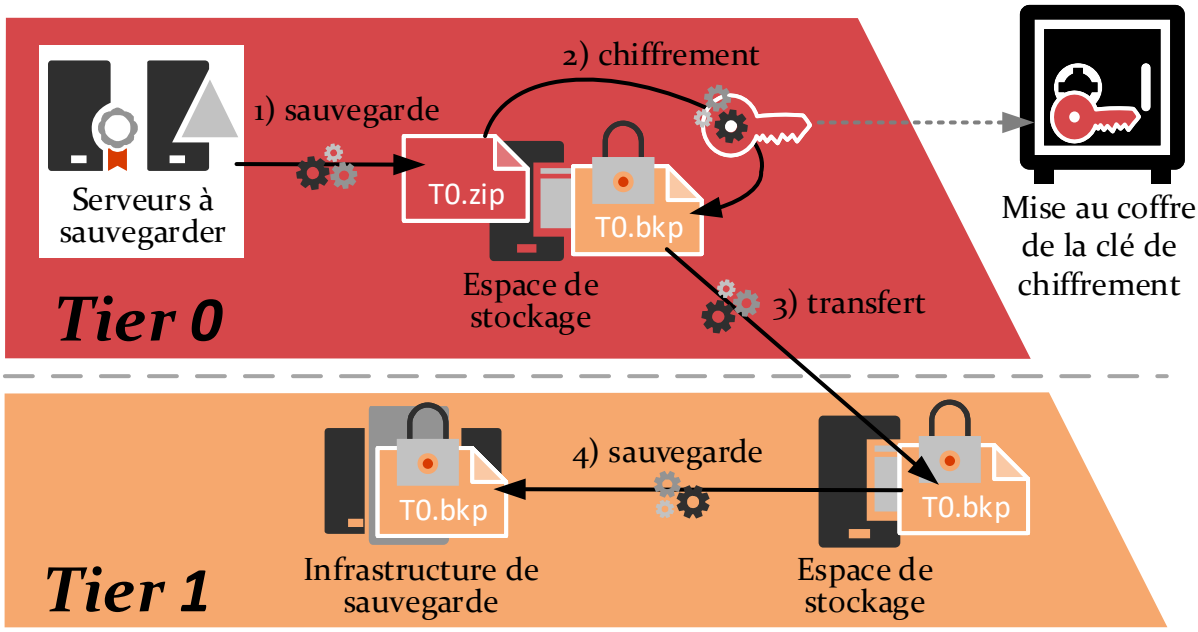

FIGURE 7 – Illustration d'un processus de sauvegarde du *Tier 0* vers une infrastructure de sauvegarde de moindre confiance.

Si ces contraintes sont jugées trop complexes ou ne permettent pas de répondre aux critères fixés par les plans de reprise d'activité, un choix devrait être fait parmi les deux possibilités suivantes :

- idéalement : mettre en œuvre des infrastructures de sauvegarde dédiées à un seul et unique *Tier* et bien cloisonnées les unes des autres. Pour la sauvegarde du *Tier 0*, il est à préciser que les dispositifs de stockage en ligne ou hors ligne qui en découlent (médias à bandes magnétiques par exemple) doivent être considérés comme des équipements de *Tier 0* à part entière et à protéger en conséquence ;
- à défaut et de manière fortement déconseillée : catégoriser l'unique infrastructure de sauvegarde du SI en *Tier 0*. Cette solution irait fortement à contre sens de l'objectif de réduction de l'exposition du *Tier 0* et de celui de délégation fine des droits. D'autre part, les sauvegardes du SI devraient dans ce cas être gérées par des comptes d'administration du *Tier 0*, ce qui serait difficilement compatible avec plusieurs recommandations de ce guide. En outre, il serait difficile de s'assurer que les composants serveurs de cette infrastructure ne présenteraient pas de surface d'attaque exploitable depuis les clients de sauvegarde.

R45

Traiter la problématique de catégorisation des infrastructures de sauvegarde

Les mécanismes de sauvegarde mis en œuvre dans le SI doivent faire l'objet d'une vigilance particulière afin de ne pas nuire au cloisonnement des zones de confiance.

Soit des infrastructures de sauvegarde sont dédiées à chaque zone de confiance, soit des mesures de sécurité sont mises en œuvre pour que la mutualisation de ces infrastructures pour différentes zones de confiance ne nuise pas à leurs cloisonnements respectifs.

La sécurité du *Tier 0* est une priorité. Quelle que soit la solution retenue, le périmètre identifié du *Tier 0* doit être pertinent au regard des éventuels chemins d'attaque du *Tier 0* via les infrastructures de sauvegarde.

3.4.2 Infrastructures de stockage en réseau

Généralement, plus le périmètre du *Tier 0* a été réduit, moins il est exposé à des scénarios de menace par accès logique à des infrastructures de stockage en réseau. En effet, plus il y a de ressources dans un *Tier* plus il y a nécessité de déployer des infrastructures de stockage centralisé pour en optimiser le cout. Alors qu'au contraire, lorsque les ressources de *Tier 0* sont en quantité limitée, il est moins nécessaire de recourir à des solutions de mutualisation de ce type.

À moins que des ressources complexes soient intégrées au *Tier 0* (infrastructure de messagerie, de virtualisation, etc.), les ressources de *Tier 0* ne devraient pas utiliser des infrastructures de stockage en réseau (SAN, NAS, etc.) pour le stockage de fichiers sensibles (le système d'exploitation, la base « `NTDS.dit` » d'un contrôleur de domaine AD, etc.). Dans le cas contraire, c'est qu'il reste *a priori* des actions d'architecture du SI à mener pour se conformer aux recommandations de cloisonnement du SI en *Tiers*. Un soin particulier doit alors être porté à décorréler ces infrastructures du périmètre du *Tier 0* et deux possibilités sont par exemple envisageables :

- idéalement : dédier des infrastructures de stockage en réseau au *Tier 0*, c'est-à-dire sans qu'elles soient mutualisées avec un autre *Tier* ;
- à défaut : généraliser le chiffrement de volumes sur tout le *Tier 0* afin que seules des données chiffrées soient stockées sur les infrastructures de stockage en réseau, ce qui permet de catégoriser ces infrastructures en *Tier 1* sans nuire au cloisonnement du *Tier 0*. Dans ce cas, ce sont les moyens de protection des secrets de chiffrement et leur robustesse qui doivent faire l'objet d'une attention particulière (sujet abordé en section 3.3). L'infrastructure de stockage en réseau ne doit bien entendu pas avoir accès à ces secrets de chiffrement, sans quoi ce chiffrement deviendrait inutile.

R46

Traiter la problématique de catégorisation des infrastructures de stockage en réseau

L'utilisation d'infrastructures de stockage en réseau doit faire l'objet d'une vigilance particulière pour de ne pas nuire au cloisonnement des zones de confiance.

Soit des infrastructures de stockage en réseau sont dédiées à chaque zone de confiance, soit des mesures de sécurité sont mises en œuvre pour que la mutualisation de ces infrastructures pour différentes zones de confiance ne nuise pas à leur cloisonnement.

La sécurité du *Tier 0* est une priorité. Quelle que soit la solution retenue, le périmètre identifié du *Tier 0* doit être pertinent au regard des éventuels chemins d'attaque du *Tier 0* via les infrastructures de stockage en réseau.

3.5 Risques relatifs aux infrastructures de virtualisation

Il est aujourd'hui fréquent de virtualiser des ressources du SI, quel que soit leur *Tier*. Une prise de conscience incomplète des problématiques de sécurité, conjuguée à des considérations budgétaires, conduit souvent à des architectures où les ressources de différents *Tiers* sont hébergées sur une unique infrastructure mutualisée. Or, l'accès logique à une machine virtuelle présente des risques similaires à l'accès à une machine physique, en conséquence de quoi les équipes en charge de l'administration d'une telle infrastructure de virtualisation doivent être catégorisées en *Tier 0* dès lors que des ressources de *Tier 0* y sont hébergées.

Le fait de mutualiser différents *Tiers* sur une même infrastructure de virtualisation s'oppose aux recommandations de réduction de l'exposition du *Tier 0* (section 2.3.6) et aux bonnes pratiques d'administration (section 2.3.5). Par ailleurs, l'évasion de machine virtuelle [26] est un risque qu'il peut également être nécessaire de prendre en compte si les besoins de sécurité le justifient. Ces éléments peuvent amener à renoncer à la mutualisation des infrastructures de virtualisation pour l'hébergement de ressources de différents *Tiers*.

Du point de vue de la catégorisation des *Tiers*, les infrastructures de virtualisation présentent *in fine* une problématique assez similaire aux infrastructures de stockage en réseau. C'est-à-dire que l'optimisation du cloisonnement du SI en *Tiers* amène à généralement préférer la catégorisation de ces infrastructures en *Tier 1*, ce qui implique qu'aucune ressource du *Tier 0* n'y soit virtualisée. Pour la virtualisation de ressources du *Tier 0*, deux cas de figure sont alors envisageables :

- elles sont hébergées par des infrastructures de virtualisation dédiées au *Tier 0* et administrées depuis le *Tier 0* ;
- des mécanismes de sécurité évalués et de confiance sont mis en œuvre pour assurer le cloisonnement des machines virtuelles sur une même infrastructure de virtualisation mutualisée pour les différents *Tiers*.

Information

Des mécanismes de sécurité tels que les *Shielded VMs* [97] sont de nature à atténuer le risque d'élévation de privilèges par accès logique à une machine virtuelle, mais ne le couvrent pas complètement, notamment à cause des éventuels instantanés de la mémoire vive. Les éditeurs de solutions logicielles d'hypervision tendent toutefois à proposer des solutions de cloisonnement adaptées à cette problématique. VMWare propose par exemple le chiffrement complet de machines virtuelles (incluant stockage, mémoire vive, instantanés de la mémoire vive, etc.) reposant sur l'utilisation d'un HSM (matériel spécifique pour la gestion d'éléments cryptographiques). Les administrateurs standards des hyperviseurs n'ont alors aucun contrôle ni sur la configuration du chiffrement ni sur les machines virtuelles chiffrées. Aucune solution de ce type n'a néanmoins fait l'objet d'une évaluation de sécurité reconnue par l'ANSSI à ce jour ; le principe de précaution doit donc prévaloir.

26. Par conception des infrastructures virtualisées, l'utilisateur d'une machine virtuelle n'est censé pouvoir accéder ni à d'autres machines virtuelles hébergées sur le même hyperviseur ni à l'hyperviseur lui-même. Une évasion de machine virtuelle consiste en l'exploitation d'une vulnérabilité qui va rendre caduque ce cloisonnement. Ces dernières années, des vulnérabilités logicielles ont été rencontrées sur les principales solutions logicielles d'hypervision du marché [117] [43] [115] [119]. Des vulnérabilités matérielles (« *spectre* » et « *meltdown* » [23] [31] par exemple) pourraient elles aussi permettre des évasions de machines virtuelles.

R47

Traiter la problématique de catégorisation des infrastructures de virtualisation

La virtualisation de ressources sensibles doit faire l'objet d'une vigilance particulière afin de ne pas nuire au cloisonnement de leurs zones de confiance respectives. Soit des infrastructures de virtualisation sont dédiées à chaque zone de confiance, soit leur virtualisation doit donner lieu à une étude préalable.

Les mesures de sécurité permettant de préserver le cloisonnement de ressources sensibles virtualisées sur des infrastructures de virtualisation de moindre confiance ne jouissent pas, à ce jour, d'un crédit suffisant pour répondre à tous les besoins de cloisonnement. Par conséquent, toute décision de mutualisation d'infrastructure de virtualisation doit être prise au regard des analyses de risques menées ainsi que des besoins et objectifs de sécurité identifiés pour chaque SI et pour chaque zone de confiance.

La sécurité du *Tier 0* est une priorité. Quels que soient les choix faits, le périmètre identifié du *Tier 0* doit être pertinent au regard des chemins d'attaque du *Tier 0* via les infrastructures de virtualisation.

En conséquence, l'utilisation de ressources exclusivement physiques et non virtualisées pour le *Tier 0* est un choix qui peut être fait sur des SI de petite ou moyenne taille. En revanche, des infrastructures de virtualisation dédiées au *Tier 0* sont souvent utilisées sur les SI plus étendus. Comme la virtualisation apporte de la souplesse et permet une meilleure continuité d'activité, elle tend à devenir un standard dans les organisations. À préciser enfin que le besoin de déploiement de contrôleurs de domaine dans des locaux où aucune de ces deux options n'est envisageable (c'est-à-dire ni serveurs physiques ni infrastructures de virtualisation dédiées au *Tier 0*) peut être couvert par le déploiement de RODC. Le sujet des RODC est traité en section 3.8.2.

3.6 Risques relatifs aux agents et serveurs de gestion centralisée

Les agents de gestion sont des logiciels qui communiquent par le réseau avec un ou plusieurs serveurs de gestion centralisée. Ces agents sont souvent installés sur les postes de travail et les serveurs pour :

- leur sauvegarde (cas évoqué en section 3.4) ;
- la protection contre les codes malveillants (antivirus, antimaliciel, etc.) ;
- l'administration centralisée du parc ;
- les télédéploiements de logiciels, des mises à jour et des correctifs de sécurité ;
- le contrôle de conformité ;
- la supervision opérationnelle du parc (des serveurs et des équipements réseau généralement) ;
- etc.

Il est ainsi courant que des agents de gestion soient installés sur des ressources sensibles du SI, tant sur des postes d'administration que des serveurs.

Ces agents logiciels s'exécutent généralement avec des privilèges élevés, via un compte système local ou via un compte de service local ou de domaine. Les agents de gestion peuvent dans certains cas présenter des chemins d'attaque, comme par exemple :

- lorsqu'ils permettent l'exécution d'actions sur une ressource avec des droits élevés et orchestrées depuis d'autres ressources (cas de la plupart des solutions de gestion centralisée). Ils permettent alors des élévations de privilèges sur les systèmes gérés depuis les serveurs de gestion centralisée. Dans ce cas et en application de la recommandation R7 de catégorisation des ressources en *Tiers*, une ressource gérée par un serveur ne doit pas être catégorisée dans une zone de plus haut niveau de confiance que lui ;
- lorsqu'ils utilisent un compte de service du domaine ou un compte de service local dont le mot de passe est identique sur un ensemble de postes de travail et de serveurs autorisés à se connecter à d'autres systèmes à travers le réseau. Dans ce cas et en application des recommandations de la section 3.3.3 traitant des comptes de service Windows, un tel compte ne doit pas être utilisé (ni même être techniquement utilisable) sur des systèmes catégorisés dans des zones de confiance différentes ;
- lorsqu'ils présentent des vulnérabilités qui permettent à un attaquant d'exécuter du code arbitraire avec les privilèges de l'agent (ce qui est assez fréquent) ;
- dès lors qu'ils permettent de communiquer avec des services d'infrastructure (serveur antivirus, serveur de sauvegarde, etc.) qui peuvent présenter des vulnérabilités dont l'exploitation est de nature à présenter des chemins d'attaque vers une autre zone de confiance.

Puisque ces agents de gestion centralisée offrent potentiellement de multiples chemins d'attaque vers les ressources sur lesquelles ils sont installés, leur utilisation courante au sein des SI amène à formuler les recommandations suivantes.

R48

Limiter la présence d'agents de gestion centralisée sur les ressources du Tier 0

Il est recommandé de réduire au strict besoin opérationnel le déploiement d'agents de gestion centralisée sur le périmètre du *Tier 0*.

Lorsqu'une organisation déploie des agents de gestion centralisée sur des ressources de *Tier 0*, il est dans ce cas impératif que les composants logiciels afférents installés sur ces ressources ne nuisent pas au cloisonnement des *Tiers* et ne dépendent que de serveurs de gestion centralisée eux aussi catégorisés en *Tier 0*.

Exemple

Si des agents antivirus sont installés sur les contrôleurs de domaine AD ou des postes d'administration du *Tier 0*, alors leurs éventuels serveurs antivirus de rattachement – utilisés pour leur gestion centralisée, leur mise à jour et la centralisation des journaux d'événements, entre autres – doivent être catégorisés en *Tier 0* également.

D'une manière générale, la catégorisation d'un serveur de gestion centralisée en *Tier 0* ne s'oppose pas à sa mutualisation à des fins de gestion de clients du *Tier 1* et du *Tier 2* également. C'est d'ailleurs le cas des services AD DS des contrôleurs de domaine AD puisqu'il n'est techniquement pas possible de procéder autrement. Il serait donc tentant de faire de même avec d'autres services de gestion centralisée (protection du poste de travail, télédéploiement de logiciels, etc.). Pour autant, cela :

- irait à l'encontre du principe de réduction de l'exposition du *Tier 0* en induisant notamment la multiplication des interactions entre le *Tier 0* et les autres *Tiers*, augmentant ainsi son exposition à des menaces depuis des zones de moindre confiance ;
- augmenterait les actions d'administration qui relèvent du *Tier 0* et rendrait donc plus difficile l'application des recommandations du chapitre 5 concernant les architectures d'administration ;
- ne permettrait pas forcément l'application de bonnes pratiques d'architecture du SI et de délégation fine des droits évoquées dans les sections 2.3.5 et 2.3.8, car toutes les solutions logicielles ne le permettent pas d'une manière qui offrirait un cloisonnement satisfaisant.

R49

Traiter la problématique de catégorisation des agents et serveurs de gestion centralisée

Lorsqu'un agent de gestion centralisée est déployé sur une ressource sensible, alors tout serveur qui en permet la gestion centralisée doit être catégorisé dans la même zone de confiance ou dans une zone d'un niveau de confiance supérieur. En complément, les serveurs de gestion centralisée ne devraient pouvoir communiquer sur le réseau qu'avec :

- les ressources dont ils assurent la gestion centralisée ;
- les serveurs dont ils dépendent éventuellement eux-mêmes – que ce soit pour leur administration ou leur gestion – et qui doivent nécessairement être d'un niveau de confiance équivalent ou supérieur.

La mutualisation de serveurs de gestion centralisée afin qu'ils gèrent des ressources de zones de moindre confiance que la leur (*Tier 1* ou *Tier 2*) peut créer des chemins d'attaque et nuit donc à un cloisonnement optimal. Mais bien qu'une telle mutualisation reste déconseillée, il s'agit d'un choix qui reste parfois acceptable en matière de SSI. Ce choix doit faire suite à une analyse de risques et être en adéquation avec les besoins et objectifs de sécurité fixés. La solution logicielle déployée doit notamment faire l'objet d'une sélection rigoureuse (comme évoqué en section 2.3.6) et d'une étude préalable contrôlant que cette mutualisation ne nuise pas au cloisonnement des zones de confiance.

Quels que soient les choix faits, le périmètre identifié du *Tier 0* doit être pertinent au regard des chemins d'attaque du *Tier 0* via les agents et serveurs de gestion centralisée.

Deux cas particuliers méritent toutefois d'être mentionnés ; ils font respectivement l'objet des sections 3.6.1 et 3.6.2.

3.6.1 Cas particulier des solutions de protection contre les menaces

Les solutions de protection contre les menaces (analyse antivirus, protection contre les rançongiciels, les maliciels, etc.) présentent, comme toute solution logicielle, une certaine surface d'attaque. Avant leur déploiement sur le *Tier 0*, une analyse des bénéfices qu'elles offrent au regard des inconvénients qu'elles présentent est nécessaire.

En l'occurrence, il se trouve que les ressources de *Tier 0* ne devraient pas être susceptibles de traiter (exécuter, lire, etc.) du contenu potentiellement malveillant (binaires exécutables, documents de bureautique, etc.), car le niveau de sécurité attendu du *Tier 0* justifie que :

- aucun utilisateur n'ait de droits en écriture sur ces ressources, à part les administrateurs du *Tier 0* eux-mêmes, qui sont donc les seuls à pouvoir leur faire exécuter ou traiter du contenu ;
- aucun fichier ne soit copié vers une ressource de *Tier 0* à moins d'avoir fait l'objet d'une analyse de sécurité qui comporte au minimum les étapes suivantes :
  - une analyse de risques, au cours de laquelle les questions suivantes se posent :
    - le contenu a-t-il toute légitimité pour être traité sur des ressources aussi sensibles que celles du *Tier 0* ?
    - quel est le niveau de confiance dans la source du contenu (le site de téléchargement par exemple) et le contenu lui-même (les développeurs ou l'éditeur notamment) ?
    - le besoin à couvrir justifie-t-il le risque encouru pour le *Tier 0* ?
    - etc.
  - une analyse antivirale préalable depuis une zone de moindre confiance et en recourant à des services en ligne comme « VirusTotal » [116] (si tant est que le fichier analysé ne présente aucun caractère de confidentialité) ;
  - un contrôle d'intégrité par empreinte ou signature cryptographique ;
  - une vérification avancée de son innocuité lorsque cela est possible (revue de code ou exécution en bac à sable par exemple).
- aucune action n'y soit menée en dehors de celles strictement nécessaires à leur installation, administration, maintenance et supervision, car ces ressources de *Tier 0* ne sont utilisées que pour délivrer un service précis.

Attention

L'utilisation du service « VirusTotal » [116] pour analyser un binaire suspect rencontré sur le SI n'est pas nécessairement une bonne idée. En effet, s'il s'agit d'une attaque ciblée avec un binaire spécialement compilé pour viser une organisation en particulier, un attaquant qui surveille l'utilisation de « VirusTotal » peut ainsi apprendre que son binaire malveillant a été analysé par sa victime. Un attaquant qui aurait compromis le SI dans un objectif d'espionnage discret, se sachant détecté, serait dès lors susceptible de nuire à l'intégrité du SI (par chiffrement des données par exemple). Les guides de remédiation [24] publiés par l'ANSSI sont une lecture recommandée dans le cadre du traitement d'un incident de sécurité.

Selon ce principe, si un contenu malveillant devait être exécuté sur des ressources de *Tier 0*, ce serait *a priori* soit par l'exploitation d'une CVE [27] non corrigée par l'organisation ou d'une vulnérabilité de type *Zero-Day* [28], soit par une action volontaire réalisée par un compte d'administration du *Tier 0* légitime ou non et qui aurait déjà les droits et privilèges nécessaires à une compromission de l'AD. Dans chacun des cas, une solution logicielle de protection contre les menaces n'offrirait donc qu'une barrière dérisoire.

En revanche, dans le cas contraire où des ressources de *Tier 0* sont susceptibles de traiter du contenu potentiellement malveillant et qu'une organisation fait donc le choix d'y déployer des solutions de protection contre les menaces, alors il serait impératif que les composants logiciels afférents installés sur ces ressources de *Tier 0* soient autonomes ou qu'ils ne dépendent que de serveurs de gestion centralisée eux aussi catégorisés en *Tier 0*. Puis, comme la surface d'attaque des serveurs de gestion centralisée est potentiellement non négligeable, il est rappelé que ces derniers doivent être dédiés au *Tier 0* et ne doivent techniquement pouvoir communiquer sur le réseau qu'avec des ressources du même niveau de confiance (cf. recommandation R49).

R50

Traiter le cas particulier de la catégorisation des solutions de protection contre les menaces

Une ressource de *Tier 0* ne doit pas être amenée à traiter du contenu potentiellement malveillant. C'est-à-dire que tout contenu traité par ces ressources doit avoir fait l'objet d'une analyse de sécurité préalable.

Lorsque ces bonnes pratiques sont respectées, les solutions de protection contre les menaces peuvent présenter plus de faiblesses que de bénéfices de sécurité sur le périmètre du *Tier 0*. Il est alors souvent fait le choix de ne pas en déployer sur ce périmètre ; choix généralement recommandé par l'ANSSI.

À défaut, soit les agents de protection contre les menaces sont déployés de manière autonome (c'est-à-dire non pilotés par un serveur de gestion centralisée du SI), soit la recommandation R49 s'applique.

3.6.2 Cas particulier des Windows Server Update Services

Les *Windows Server Update Services* (WSUS) de Microsoft sont utilisés pour gérer et superviser le télédéploiement des mises à jour et correctifs des produits de Microsoft au sein d'un parc informatique. Ils font office d'intermédiaires entre le service internet *Microsoft Update* public de Microsoft et les produits de Microsoft à mettre à jour dans les SI.

Dans la démarche de cloisonnement du SI, force est de constater que les problématiques de sécurité ayant trait aux services WSUS sont souvent mal appréhendées alors qu'il s'agit d'un service sensible et quasi incontournable dans tout SI s'appuyant sur des systèmes d'exploitation Microsoft.

27. Les CVE (*Common Vulnerabilities and Exposures*) sont des avis de sécurité publiés pour des vulnérabilités connues et référencées. La liste des CVE peut être consultée sur de nombreux sites Internet traitant de la réponse aux incidents de sécurité.
28. Une *Zero-Day* est une vulnérabilité exploitée par des attaquants, mais *a priori* pas encore connue de l'éditeur du logiciel ciblé. Elle n'a donc pas encore fait l'objet d'un référencement officiel ni d'un correctif de sécurité.

Le cas de WSUS est représentatif. Il illustre bien la problématique des agents de gestion à travers quelques-unes de ses particularités :

- certains agents de gestion sont nativement intégrés aux systèmes d'exploitation. C'est notamment le cas du service Windows « *Windows Update* » – qui est par défaut intégré au système d'exploitation Windows pour sa mise à jour et celle d'autres applications Microsoft – qui peut être géré de manière centralisée par un serveur WSUS déployé dans le SI. Les risques de sécurité posés par ces agents de gestion natifs doivent être considérés au même titre que ceux des agents de gestion tiers déployés sur le SI. Le sujet traité en section 3.6 leur est donc également applicable en tous points ;
- contrairement aux idées reçues, les serveurs WSUS, s'ils sont compromis, peuvent permettre à des attaquants de distribuer des binaires malveillants aux clients[29]. Ceci illustre à quel point il est important que les ressources de *Tier 0* ne récupèrent leurs mises à jour et correctifs Windows que depuis des serveurs de même niveau de confiance ou d'un niveau de confiance supérieur, sans quoi le cloisonnement des *Tiers* ne serait pas assuré ;
- les approbations de mises à jour, par exemple, sont uniquement réalisables avec le rôle d'administration WSUS et sans restriction possible à un sous-ensemble de ressources. Si un serveur WSUS de *Tier 0* devait également gérer des clients du *Tier 1* ou du *Tier 2*, il serait donc impossible d'en déléguer finement la gestion à des administrateurs de *Tier 1* ou de *Tier 2*. Dès lors, cela signifie qu'il incomberait à des administrateurs de *Tier 0* de les gérer ;
- par défaut, les flux réseau entre les clients et les serveurs WSUS passent en clair sur le réseau (les chemins d'attaque relatifs aux protocoles de communication sont abordés en section 3.7). L'utilisation des protocoles TLS requiert un effort de configuration complémentaire.

R51

Mettre en œuvre une architecture WSUS permettant de préserver le cloisonnement

Le service Windows « *Windows Update* » doit être considéré comme un agent de gestion à part entière dès lors qu'il est géré par un serveur WSUS. Le serveur WSUS doit donc être quant à lui considéré comme un serveur de gestion centralisée. Dès lors, la recommandation R49 s'applique, c'est-à-dire que les ressources du SI doivent être rattachées à un serveur WSUS de leur zone de confiance ou d'un niveau de confiance supérieur.

Dans le cas du *Tier 0*, il est conseillé d'utiliser des serveurs WSUS dédiés au *Tier 0*, c'est-à-dire sans mutualisation avec des zones de moindre confiance.

3.7 Risques relatifs aux communications réseau

3.7.1 Sécurité des protocoles de communication utilisés

Les solutions du marché tendent à proposer par défaut des protocoles de communication standards et sécurisés (TLS par exemple) dont la sécurité repose sur des algorithmes de chiffrement et des implémentations éprouvés. Néanmoins, les risques d'attaque (interception, altération, exploitation de CVE, etc.) restent d'actualité dans la mesure où par exemple :

29. Pour approfondir les faiblesses de WSUS, le lecteur est invité à lire l'article [111] présenté au SSTIC en 2017.

- des protocoles de communication non sécurisés restent encore régulièrement utilisés par défaut (c'est par exemple le cas du service WSUS abordé en section 3.6.2);
- certaines implémentations de mécanismes de chiffrement présentent des vulnérabilités (c'est par exemple le cas de la CVE-2020-1472 [33] critique, aussi appelée *ZeroLogon*, concernant le protocole *NETLOGON* de Microsoft);
- les progrès en cryptanalyse et les performances croissantes du matériel rendent vulnérables (car rapidement cassables) certaines tailles de clé ou certains algorithmes;
- l'authentification du client par le serveur est souvent réalisée, mais leur authentification mutuelle n'est généralement pas faite dans les configurations par défaut, ce qui peut notamment permettre des attaques de type « homme du milieu » (*man in the middle*, MITM) ou de l'usurpation de serveur.

Certains protocoles de communication peuvent donc présenter des risques de sécurité. Des attaques réseau peuvent ainsi nuire à l'intégrité ou à la confidentialité des données qui transitent sur le réseau, créant de potentiels chemins d'attaque. Ces attaques réseau peuvent être réalisées de différentes manières telles que :

- l'usurpation d'adresse (*spoofing*) sur le réseau local du SI;
- la compromission de serveurs mandataires (*proxy* et *reverse proxy*);
- l'accès physique aux câbles (fibre ou cuivre) du réseau local (prises réseau dans les locaux, passages de câbles dans les circulations, etc.) voire du réseau des centres de données;
- l'obtention d'accès à des réseaux sans-fil interconnectés au LAN;
- l'utilisation d'appareils d'interception des communications mobiles;
- l'accès physique aux infrastructures des opérateurs de télécommunications (pour les attaquants qui disposent de moyens très importants).

Ces risques doivent donc être appréciés au juste niveau dès lors que des protocoles non sécurisés ou peu robustes sont utilisés entre composants du SI, et plus particulièrement lorsqu'ils sont utilisés par des ressources sensibles. Pour aider à une configuration adéquate, l'ANSSI a par exemple publié des recommandations de sécurité relatives à TLS [13] et à IPSec [8]. Par ailleurs, les produits s'étant vus délivrer un visa de sécurité par l'ANSSI [26] utilisent des protocoles sécurisés et robustes sur le périmètre indiqué dans la cible de sécurité de l'évaluation.

R52

Sécuriser les protocoles de communication réseau utilisés par les ressources du Tier 0

De manière générale, les protocoles de communication utilisés (HTTP, SMB, etc.) par des ressources du *Tier 0* doivent être sécurisés et robustes puis avoir été configurés de manière à offrir un niveau de sécurité optimal. Autant que possible, ces protocoles doivent mettre en œuvre un mécanisme d'authentification mutuelle afin de limiter les possibilités d'attaques réseau. Dans le cas contraire, leur encapsulation par IPSec doit être considérée en suivant les recommandations de l'ANSSI [8].

3.7.2 Segmentation et filtrage réseau

Dans un objectif de réduction de la surface d'attaque du *Tier 0*, les communications réseau en entrée et en sortie du *Tier 0* doivent être strictement filtrées.

Ce filtrage concerne, pour commencer, les communications entre le *Tier 0* et les réseaux non maîtrisés.

R53

Filtrer les flux réseau entre le Tier 0 et les réseaux non maîtrisés

Les flux réseau entre les ressources du *Tier 0* et tout autre réseau non maîtrisé par l'organisation (notamment Internet) doivent être interdits, en entrée et en sortie. Ces interdictions doivent être mises en œuvre par des équipements de filtrage périmétrique ainsi que par du filtrage local (à l'aide du pare-feu Windows intégré, par exemple).

Toute exception à ces interdictions doit faire l'objet d'une analyse préalable du risque. Les flux autorisés doivent reposer sur des protocoles sécurisés et doivent permettre une authentification des partenaires de connexion.

En revanche, les seules exceptions éventuellement acceptables en entrée du *Tier 0* depuis Internet concernent l'infogérance de l'administration du *Tier 0* (cf. recommandations du chapitre 12 du guide ADMIN [16]) et l'administration du *Tier 0* à distance ou en nomadisme (sujet traité en chapitre 5).

Exemple

Une exception habituelle d'accès à Internet depuis le *Tier 0* concerne la connexion au service en ligne *Microsoft Update* pour assurer le MCO et le MCS des systèmes Windows du *Tier 0*. La connexion à ce service utilise le protocole TLS et un épinglage de certificat (*certificate pinning*) garantit l'authenticité des serveurs *Microsoft Update*.

Information

Le filtrage par pare-feu local est plus fin car il présente l'avantage de pouvoir s'appliquer uniquement à un processus particulier, ce que ne permet pas le filtrage périmétrique.

Le filtrage des communications réseau en entrée et en sortie du *Tier 0* concerne ensuite les communications entre le *Tier 0* et le reste du SI de l'organisation. Dans cette optique, il est nécessaire de s'assurer que seuls les flux strictement nécessaires sont autorisés. Bien que les contrôleurs de domaine et les systèmes membres de l'AD communiquent ensemble à l'aide d'une grande diversité de protocoles, ce n'est en revanche pas le cas des autres ressources du *Tier 0*. En effet, certaines ressources du *Tier 0* telles que les postes d'administration dédiés à l'administration du *Tier 0*

ne doivent pouvoir communiquer qu'avec les autres ressources du *Tier 0*, sur un nombre limité de protocoles.

R54

Filtrer les flux réseau entre le Tier 0 et le reste du SI

Les flux réseau entre les ressources du *Tier 0* et le reste du SI doivent être finement filtrés, en entrée et en sortie. Ce filtrage doit être local (à l'aide du pare-feu Windows intégré, par exemple) et éventuellement complété par des équipements de filtrage périmétrique et par de la segmentation réseau (VLAN par exemple).

Exemple

L'établissement d'une connexion RDP à destination d'une ressource de *Tier 0* doit être uniquement possible depuis des ressources d'administration du *Tier 0*. Les flux réseau associés à RDP doivent donc être bloqués en provenance de toute autre ressource du SI.

Exemple

Conformément à la recommandation R17 du guide ADMIN [16] (application d'un filtrage local sur les ressources administrées et qui correspond au juste besoin opérationnel), aucun flux réseau ne doit être autorisé en entrée des postes d'administration du *Tier 0*, car aucun besoin ne devrait justifier le moindre flux entrant.

Enfin et en application des recommandations R13 et R14+, les évènements de sécurité associés à des flux réseau interdits en entrée ou en sortie du *Tier 0* doivent être journalisés et centralisés, lesquels, idéalement, alimenteront un système de détection des incidents de sécurité (se reporter à l'annexe C du guide [17]).

3.8 Risques relatifs aux accès physiques aux systèmes

3.8.1 Sécurité physique des ressources du Tier 0

L'accès physique aux ressources de *Tier 0* est souvent négligé. Pourtant, il pourrait suffire à un individu malveillant de disposer d'un accès physique temporaire à une ressource de *Tier 0* pour lui permettre d'obtenir le contrôle total de l'annuaire AD.

Pour un acteur cybercriminel, il peut s'avérer plus rapide et économique d'avoir recours à l'ingénierie sociale (corruption de personnel, intrusions physiques, etc.) plutôt qu'à de complexes scénarios de compromission impliquant l'exploitation de vulnérabilités logicielles. L'état de la menace justifie que les risques ayant trait aux accès physiques soient également considérés avec la plus grande attention. Les scénarios de menace physique sont nombreux. Ils peuvent mettre en œuvre différentes attaques menées à chaud ou à froid, telles que :

- le simple vol de matériel ;

- les attaques DMA [30] ;
- le clonage d'un support de stockage pour récupération ultérieure des secrets d'authentification qu'ils contiennent (exemple : clonage du disque dur d'un contrôleur de domaine AD ou d'un poste d'administration du *Tier 0*). Il est à noter qu'en cas de panne matérielle, les disques durs du *Tier 0* ne doivent ni être manipulés par des tiers non autorisés ni être envoyés en support après vente ;
- la récupération de fichiers sur des supports de stockage du *Tier 0* qui n'ont pas été détruits ou effacés dans les règles de l'art. En fin de vie du matériel, les disques durs doivent être détruits ou effacés de manière sécurisée [31] ;
- le piégeage de la chaîne de démarrage du système (UEFI principalement) ;
- le piégeage des composants matériels ou des accessoires (claviers et câbles intercepteurs de frappes, périphériques USB malveillants, microprogrammes intégrant des portes dérobées, etc.).

Ainsi, toute personne disposant d'un accès physique à une ressource de *Tier 0* peut, dans de nombreux cas, obtenir des droits et privilèges du *Tier 0* et, par extension, le contrôle de l'annuaire AD. Pour cette raison, les ressources d'une même zone de confiance devraient être physiquement localisées dans des zones d'un niveau de sécurité physique adapté et cohérent.

Attention

Il est courant de constater que l'administration du *Tier 0* se fait depuis des bureaux dont le niveau de sécurité physique est insuffisant au regard de leur criticité. Il est donc souligné que la sécurité physique ne concerne pas uniquement les centres de données (*datacenters*). Il a été détaillé en section 3.3 (qui traite des risques liés aux accès à des secrets d'authentification) que la compromission d'un poste d'administration entraîne *de facto* la compromission des ressources administrées depuis ce poste. Tout contrôle d'accès physique mis en œuvre pour protéger l'accès physique aux systèmes et équipements du *Tier 0* aux seules personnes habilitées doit donc également concerner les postes d'administration du *Tier 0* même si ces derniers sont – la plupart du temps – hors des centres de données.

R55

Prêter une attention particulière à la sécurité physique des ressources du Tier 0

Le cloisonnement logique d'une zone de confiance ne peut pas être satisfaisant sans avoir également traité les scénarios de menace physique qui pèsent sur les ressources qui la composent. Le niveau de sécurité physique d'une zone de confiance doit ainsi être en adéquation avec les besoins et objectifs de sécurité de cette zone.

Du fait des nombreuses attaques physiques possibles sur le matériel, une ressource du *Tier 0* (et le matériel qui la compose, incluant ses accessoires) ne doit être

30. Le DMA (*direct memory access*) permet un accès direct à la mémoire vive – à chaud – par des périphériques sans passer par le processeur. Une attaque DMA consiste donc à accéder de cette manière à des espaces mémoire non autorisés afin de lire ou altérer leur contenu. L'IOMMU (*input-output memory management unit*), si le matériel en est pourvu et qu'il est activé, permet au système de se protéger contre ces attaques.

31. Le lecteur est invité à consulter la liste des produits certifiés pour l'effacement de données sécurisé sur le site de l'ANSSI [25]. Une mesure de sécurité alternative peut également consister en l'utilisation d'un chiffrement de disque avec stockage des secrets de déchiffrement sur puce TPM.

physiquement accessible que par des personnes disposant du niveau de confiance requis. Ce niveau de confiance peut être déterminé par des procédures organisationnelles telles qu'une vérification des antécédents personnels, l'obtention d'une décision d'habilitation, etc. Le niveau de confiance requis est à déterminer par l'organisation en fonction des besoins et objectifs de sécurité qu'elle identifie.

À défaut de sécurité physique adéquate, des mesures de sécurité logique peuvent être mises en œuvre pour atténuer certains risques. Toutefois, elles se substituent rarement à un contrôle d'accès physique adéquat.

À préciser enfin que le besoin de déploiement de contrôleurs de domaine dans des locaux où le niveau de sécurité physique est insuffisant peut être couvert par le déploiement de RODC. Le sujet des RODC est traité en section 3.8.2.

Attention

L'accès à des interfaces IPMI [32] ou à des équipements KVM réseau IP [33] pour l'administration distante de serveurs doit être considéré à l'identique d'un accès physique puisque ces interfaces et équipements permettent des interactions bas niveau très similaires à ce que permet un accès physique direct.

Attention

La compromission physique du matériel avant même sa livraison (appelée « attaque de la chaîne d'approvisionnement ») est un risque à prendre en compte lorsque les besoins de sécurité le justifient. Dans ce cas, la chaîne d'approvisionnement des équipements de *Tier 0* devrait présenter les garanties de sécurité minimum permettant de minimiser le risque de piégeage du matériel jusqu'à sa livraison à l'organisation finale. Un équipement devrait notamment être livré vierge de tout système d'exploitation installé et les micrologiciels (*firmwares*) de ses périphériques intégrés devraient être réinstallés avant toute insertion dans le système d'information.

Traiter la question de la sécurité physique des ressources de *Tier 0* oblige à analyser la sécurité des systèmes de contrôle d'accès physique ainsi que du processus d'octroi d'autorisations sur ces derniers. Si les contrôles d'accès sont gérés par des personnes ou depuis des ressources d'un moindre niveau de confiance que celui du *Tier 0*, alors elles peuvent constituer son maillon faible.

La sécurisation des contrôles d'accès physique est hors périmètre de ce guide. Sur ce sujet, le lecteur est notamment invité à :

- lire le guide « Recommandations sur la sécurisation des systèmes de contrôle d'accès physique et de vidéoprotection » [15] de l'ANSSI ;

32. Les IPMI (*Intelligent Platform Management Interface*) sont des interfaces de gestion intelligente du matériel, mises à disposition par le matériel lui-même et indépendantes de l'OS. Les IPMI les plus connus sont HP iLo et Dell iDRAC.

33. Les KVM (*Keyboard, Video, Mouse*) sont des équipements reliés à plusieurs ordinateurs et qui permettent de tous les contrôler avec un seul ensemble clavier + vidéo + souris. Lorsqu'ils sont reliés à ces ordinateurs à travers un réseau IP (sans que l'OS ne soit impliqué), alors ce sont des KVM réseau IP.

- consulter les documents techniques du CNPP [32] pour la mise en œuvre sécurisée d'un système de contrôle d'accès ;
- privilégier l'utilisation de matériel certifié (le CNPP [32] délivre par exemple des certifications de produits et des certifications de service).

Il apparaît par ailleurs inévitable de considérer les aspects organisationnels avec autant de rigueur que les aspects techniques puisque l'humain est partie prenante dans la problématique de sécurisation des accès physiques.

3.8.2 Cas des contrôleurs de domaine exposés

Certaines organisations sont géographiquement réparties dans des locaux de petite taille (agences et autres points de présence) qui disposent de moyens limités. Il est courant que les conditions de sécurité physique offertes par ces petits sites [34] ne permettent pas d'assurer un niveau de protection adapté pour des ressources de *Tier 0*. Aucune ressource de *Tier 0* ne doit être physiquement positionnée dans des locaux dont le niveau de sécurité physique est insuffisant. Pour autant et surtout pour des questions de continuité de service et de confort utilisateur (amélioration des temps d'ouverture de session notamment), des contrôleurs de domaine AD (qui sont des serveurs de *Tier 0*) sont généralement déployés dans chaque site d'une organisation, y compris dans ceux de petite taille et aux moyens limités.

Sur les serveurs Microsoft Windows, le rôle de contrôleur de domaine AD en lecture seule (RODC, *read-only domain controler*) a pour objectif de répondre à cette problématique de sécurité physique des contrôleurs de domaine. Un RODC peut être configuré pour ne contenir que les secrets d'authentification des utilisateurs non privilégiés présents sur le site. Dans ce cas, le RODC ne contient aucun secret susceptible de permettre le contrôle de *Tier 0* et n'a donc pas lieu d'être catégorisé en *Tier 0*.

R56

Déployer des RODC lorsque la sécurité physique n'est pas assurée

Aucun contrôleur de domaine ne doit être déployé dans des locaux qui ne présentent pas les conditions de sécurité physique suffisantes en adéquation avec les besoins de sécurité du *Tier 0*. Des RODC peuvent en revanche y être déployés, ils doivent dans ce cas satisfaire à la recommandation R57.

R57

Appliquer les recommandations de sécurisation des RODC

Pour pouvoir catégoriser des RODC en dehors du *Tier 0*, ils ne doivent présenter aucune relation de contrôle vers le *Tier 0*. Dans cette optique, les recommandations et bonnes pratiques de sécurité figurant dans la documentation [91] de Microsoft doivent donc leur être appliquées. En l'occurrence, aucun compte du *Tier 0* ne doit être présent dans les attributs de révélation des RODC, c'est-à-dire que :

- tous les comptes et groupes du *Tier 0* (intégrés par défaut ou non) doivent fi-

34. Un « site » est le nom donné à un point de présence géographique d'une organisation dans la terminologie AD. La topologie de l'annuaire se compose ainsi d'un ensemble de sites qui se caractérisent par leur plan d'adressage réseau.

gurer dans la liste des comptes qui ne sont pas autorisés à être répliqués sur les RODC (attribut *msDS-NeverRevealGroup* du RODC dans l'AD). Le groupe intégré par défaut « *Denied RODC Password Replication Group* » peut par exemple être peuplé dans cette optique ;

- seuls des comptes (comptes utilisateurs et comptes d'ordinateurs) du site géré par le RODC (généralement des comptes de *Tier 2*) doivent figurer dans la liste des comptes autorisés à y être répliqués (attribut *msDS-Reveal-OnDemandGroup* du RODC dans l'AD).

La pertinence de ces mesures de sécurité repose donc sur l'hypothèse que le périmètre du *Tier 0* ait été bien identifié, qu'il soit correctement cloisonné et qu'aucun compte de *Tier 0* mal catégorisé ne puisse avoir ses secrets d'authentification en cache sur un RODC. Tout chemin d'attaque résiduel vers le *Tier 0* depuis des zones de moindre confiance pourrait être exploité depuis un RODC compromis.

Information

Si la sécurisation d'un RODC s'est faite après son utilisation en production, l'attribut *msDS-RevealedList* d'un RODC peut être consulté pour connaître la liste des comptes utilisateurs ayant vu leurs secrets d'authentification exposés sur ce RODC préalablement à l'opération de sécurisation. En cas de présence d'un compte sensible dans cet attribut, le secret du compte en question doit être changé. Par ailleurs, une investigation numérique est conseillée pour identifier la raison de l'utilisation de ce compte sur le site du RODC et pour également s'assurer que ce compte n'ait pas fait l'objet d'un usage inopportun.

3.9 Structure hiérarchique des unités organisationnelles de l'annuaire AD

Le modèle de gestion des accès privilégiés mis en œuvre doit se refléter dans la structure hiérarchique des OU de l'annuaire AD. Une OU dédiée aux objets du *Tier 0* doit permettre de séparer ces objets des autres objets de l'annuaire.

Attention

Les comptes d'ordinateur des contrôleurs de domaine et les comptes et groupes utilisateurs intégrés par défaut (énumérés en section 3.2.2) doivent rester dans leurs OU par défaut.

R58

Créer une unité organisationnelle réunissant les objets du Tier 0

Une OU dédiée aux objets du *Tier 0* doit être créée au plus près de la racine du domaine, soit directement à la racine soit dans une sous-OU dédiée à l'administration.

Cette OU, qui ne doit être modifiable que par des administrateurs du *Tier 0*, doit contenir l'ensemble des objets du *Tier 0* (à l'exception des comptes d'ordinateur

des contrôleurs de domaine et des comptes et groupes utilisateurs intégrés par défaut) eux-mêmes organisés dans des sous-OU : ordinateurs, utilisateurs (c'est-à-dire les comptes d'administration du *Tier 0*), groupes utilisateurs, comptes de service.

Au-delà d'être une bonne pratique organisationnelle, réunir la majorité des objets de *Tier 0* dans une unique OU permet de bloquer l'héritage des GPO sur cette dernière. Cela facilite également l'application de GPO spécifiques aux ressources du *Tier 0* et limite le risque de délégation malencontreuse de droits sur le *Tier 0* à des objets de moindre confiance.

Attention

L'héritage des GPO sur l'OU intégrée par défaut « `OU=Domain Controllers` » doit être préservé : il ne doit pas être bloqué.

R59

Restreindre les stratégies de sécurité applicables à l'unité organisationnelle du Tier 0

Pour limiter les chemins de contrôle AD du *Tier 0* à travers des GPO liées ou appliquées à la racine du domaine, l'OU dédiée au *Tier 0* doit bloquer l'héritage (configuration réalisable par l'interface graphique de l'éditeur de stratégies de groupe ou par PowerShell [66]). La *Default Domain Policy* doit néanmoins être liée à l'OU dédiée au *Tier 0* avec la priorité la plus basse. Enfin, les GPO liées ou appliquées à cette OU doivent être dédiées aux ressources de *Tier 0* et ne doivent être modifiables que par des administrateurs du *Tier 0*.

Attention

Contrairement aux GPO qui sont simplement liées (*link enabled*), les GPO qui ont le status « appliqué » (*enforced*) sont appliquées y compris dans les sous-OU qui bloquent l'héritage. Dans ce deuxième cas, il est nécessaire de s'assurer qu'aucune GPO appliquée à une OU parente de celle dédiée au *Tier 0* n'ait ce statut, puis que seuls des administrateurs du *Tier 0* aient le droit de modifier ou appliquer des GPO sur une OU parente de celle dédiée au *Tier 0*.

3.10 Cas particulier de Samba 4 AD

Samba 4 AD [112] est une solution logicielle alternative à Microsoft AD. Elle implémente les protocoles et interfaces logicielles de Microsoft AD dans un objectif d'interopérabilité. Comme elle est publiée en source ouverte sous licence GPLv3, elle est utilisable gratuitement par les organisations. Cette gratuité et le développement soutenu de Samba 4 AD ces dernières années en font aujourd'hui une solution de plus en plus répandue en remplacement des services AD DS de Microsoft.

La particularité de Samba 4 AD réside dans le fait que les contrôleurs de domaine ne reposent pas sur des serveurs Microsoft Windows, mais sur un OS de type GNU/Linux. Cela a plusieurs implications en termes d'identification du *Tier 0* puisque des accès aux systèmes GNU/Linux

contrôleurs de domaine Samba 4 AD permettent l'administration de l'AD au niveau *Tier 0*. Le fait de catégoriser les serveurs contrôleurs de domaine Samba 4 AD en *Tier 0* oblige à identifier des chemins d'attaque propres aux environnements GNU/Linux. Il est donc notamment important de considérer :

- l'accès aux secrets d'authentification des comptes, locaux ou non (via des modules comme PAM, NSS, etc.) permettant l'administration de ces serveurs ;
- les possibilités d'administration distante de ces serveurs par SSH ainsi que par prise en main graphique à distance (X11, VNC, etc.) ou par WBEM (*Web-based enterprise management*) ;
- la confiance dans les binaires déployés sur ces serveurs (c'est-à-dire les serveurs de sources utilisés pour les installations par RPM, APT, etc.) et la vérification de l'intégrité de ces binaires ;
- les mécanismes de sauvegarde éventuellement utilisés (l'utilisation de `rsync` pour la copie de fichiers sensibles de Samba 4 AD vers d'autres serveurs par exemple) ;
- la sécurité des éventuels systèmes GNU/Linux d'administration distante de ces serveurs (les politiques de sécurité définies pour les postes d'administration du *Tier 0* doivent être appliquées autant aux systèmes Windows qu'aux systèmes GNU/Linux, même si la manière de les appliquer diffère).

Dans ce contexte et en complément des équipes ayant une expertise des environnements Microsoft AD, il convient de faire également appel à des profils compétents en systèmes GNU/Linux. Ces derniers doivent être capables d'identifier précisément les chemins d'attaque du *Tier 0* impliquant les environnements GNU/Linux.

Enfin, il convient de préciser que les limitations fonctionnelles et de sécurité actuelles de Samba 4 (dans sa version 4.19 datant du 4 septembre 2023) ne permettent pas de mettre en œuvre l'intégralité des recommandations de ce guide. Les *Managed Service Accounts* (cf. section 4.14), par exemple, ne sont pas supportés. Il est également à noter que Samba 4 AD n'implémente pas les *AD Web Services* [50], ce qui se traduit par l'impossibilité d'utiliser les Cmdlets PowerShell AD. Certaines configurations de l'AD doivent se faire directement sur les contrôleurs de domaine Samba 4 AD en ligne de commande à l'aide de l'utilitaire `samba-tool` [114].

La feuille de route des développements [113] de Samba 4 AD prévoit d'atteindre un équivalent du niveau fonctionnel 6 (Windows Serveur 2012R2) d'ici fin 2023. La version 4.19 de Samba 4 AD apporte notamment la prise en charge de certaines fonctionnalités avancées de Kerberos comme l'authentification composée, le blindage et les revendications. Elle supporte donc les silos d'authentification (cf. annexe C), qui peuvent être gérés à l'aide de l'utilitaire `samba-tool` [114].

3.11 Points d'attention concernant les usages du Cloud

L'usage du *Cloud* et l'extension des SI dans le *Cloud* peuvent parfois créer des chemins d'attaque du *Tier 0* depuis ces services. Dans de telles conditions, certains comptes fonctionnels ou techniques de haut niveau qui permettent la gestion de ces services (comptes propriétaires d'un *tenant* par exemple) pourraient potentiellement permettre le contrôle du *Tier 0*.

D'autre part, l'extension du SI dans le *Cloud* requiert parfois le déploiement de serveurs intégrés à l'AD qui portent par exemple des fonctionnalités de synchronisation, d'interconnexion ou de

fédération d'identités. Ces serveurs présentent généralement des chemins d'attaque du *Tier 0* et doivent donc être considérés de ce niveau de sensibilité le cas échéant. C'est par exemple le cas des serveurs *Microsoft Entra Connect* (ex *Azure AD Connect*) et *Active Directory Federation Services* (ADFS) de Microsoft.

Les problématiques de sécurité ayant trait à l'utilisation du *Cloud* sont hors périmètre de ce guide. Il n'aborde donc ni les risques liés à l'extension du SI dans le *Cloud*, ni les problématiques d'administration des annuaires Microsoft Entra ID (ex. Azure Active Directory).

R60

Identifier les chemins d'attaque du Tier 0 inhérents au Cloud

Il est recommandé d'analyser les chemins d'attaque du *Tier 0* qui existent depuis les services de *Cloud* privés ou publics utilisés par l'organisation. Cette analyse concerne non seulement les droits et privilèges octroyés au sein de ces services, mais également les composants logiciels dont le déploiement est nécessaire en interne (*on premises*) pour leur interconnexion au SI. Cette analyse est hors périmètre du présent guide.

3.12 Déclinaison de cette démarche de cloisonnement aux autres zones de confiance

Ce chapitre a illustré comment mener un travail d'identification et de cloisonnement du *Tier 0* qui s'intègre dans une démarche plus globale de cloisonnement du SI. Il a dressé un aperçu des différents types de chemins d'attaque à prendre en compte. Des pistes de réflexion ont été données pour traiter certaines problématiques courantes que de tels travaux soulèvent.

Bien que seul le *Tier 0* ait ici servi d'exemple, la sécurité du *Tier 1* et celle du *Tier 2* doivent également faire l'objet d'une attention similaire, notamment sur le périmètre des zones de confiance caractérisées par la présence de biens supports afférents à des valeurs métiers qui sont essentielles pour l'organisation.

Ce sont alors les analyses de risques et les objectifs de sécurité de chaque SI et de chaque zone de confiance qui déterminent les besoins de cloisonnement dans le *Tier 1* et dans le *Tier 2*. L'approche illustrée dans le présent chapitre ainsi que l'ensemble des recommandations formulées doivent donc, autant que possible, être déclinées sur ces *Tiers*. Pour autant, il est certain que le cloisonnement des zones de confiance du *Tier 1* et du *Tier 2* amène à traiter des problématiques spécifiques et se heurte à des contraintes et des besoins qui diffèrent du *Tier 0*. Cela se traduit notamment par de forts besoins de mutualisation induits par un grand nombre de ressources à administrer et une large population d'administrateurs IT ou métier qui les gèrent.

Pour clore ce chapitre, la figure 8 illustre un récapitulatif synthétique de la plupart des chemins d'attaque du *Tier 0* qui ont été mentionnés.

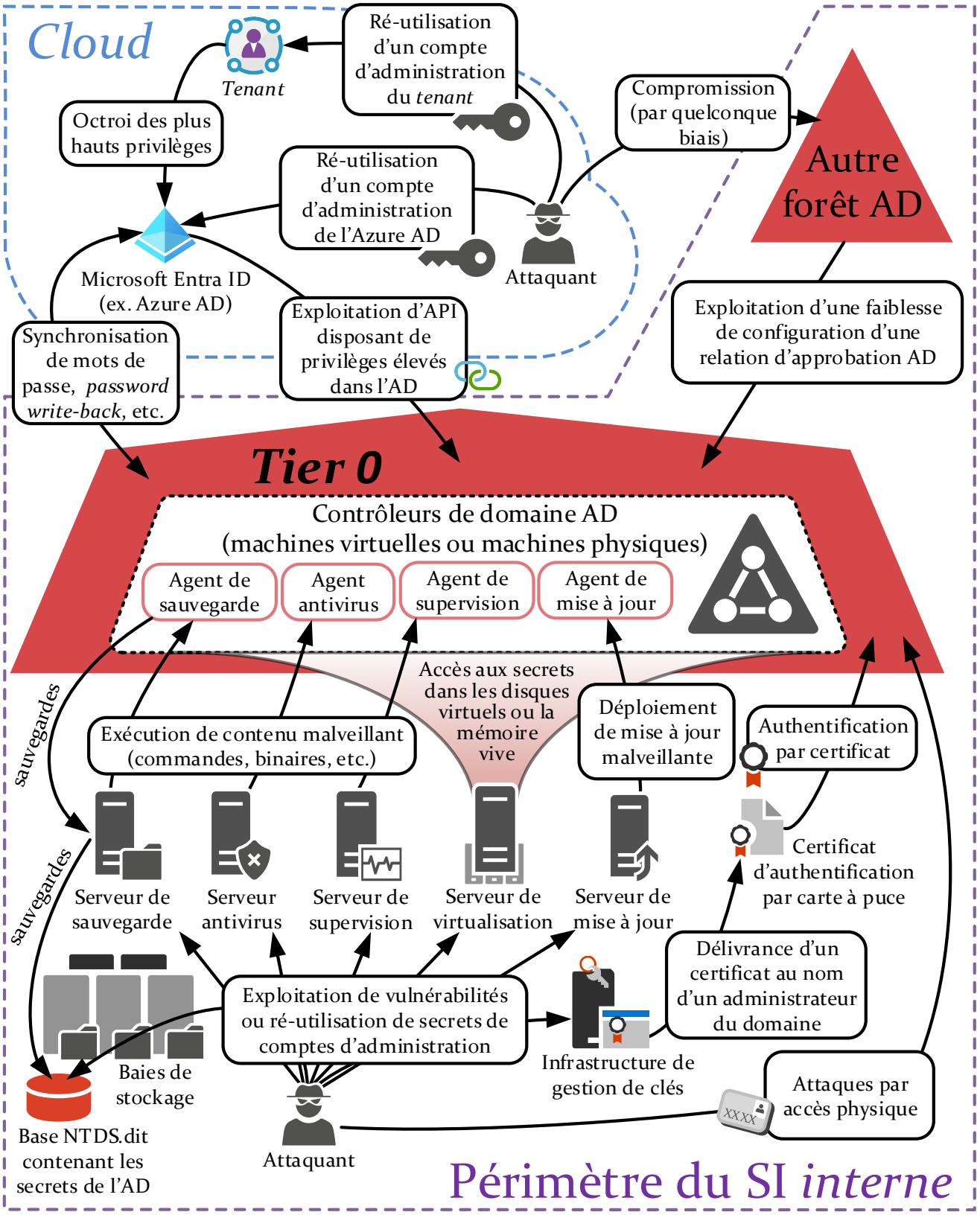

FIGURE 8 – Récapitulatif synthétique des chemins d'attaque du *Tier 0* mentionnés en chapitre 3.

4
Dangers de NTLM et Kerberos pour le cloisonnement du SI

Comme cela a été évoqué au chapitre 3, les condensats NTLM (*NTLM hash*) et les secrets Kerberos sont des secrets d'authentification réutilisables. En pratique, la dissémination non contrôlée de ces secrets sur un SI et leur réutilisation par un attaquant constituent la principale méthode de compromission d'un SI mettant en œuvre des technologies Microsoft. En conséquence, la prise de conscience, par les administrateurs AD, de cette problématique de non-prolifération des condensats NTLM et des secrets Kerberos entre *Tiers* est capitale pour limiter les conséquences d'une compromission (et en particulier, pour réduire les capacités d'élévation de privilège d'un attaquant qui aurait compromis une ressource appartenant au *Tier 2* ou au *Tier 1*).

Objectif

Ce chapitre traite en détail des problématiques de sécurité des protocoles d'authentification NTLM et Kerberos. Son objectif est d'expliquer en quoi la dissémination des secrets attachés à ces deux protocoles est de nature à nuire au cloisonnement du SI en zones de confiance et de proposer des contre-mesures permettant d'en contrôler la dissémination.

NTLM

NTLM (*NT lan manager*) désigne un ensemble de protocoles d'authentification réseau introduits par Microsoft et qui reposent sur des mécanismes de défis/réponses entre clients et serveurs. Les plus anciennes versions de NTLM datent de 1993 avec Windows NT 3.1. NTLM est toujours utilisé sur les systèmes Windows actuels dans sa version la plus récente : NTLMv2. L'utilisation des protocoles NTLM peut être interdite dans un domaine AD compte tenu des faiblesses de sécurité que ces protocoles présentent, mais cela est rarement fait par les organisations de crainte d'une incompatibilité de certaines ressources du SI avec des protocoles d'authentification plus récents comme Kerberos. Les dangers de NTLM sont abordés en section 4.15.

Kerberos

Kerberos est un protocole d'authentification réseau qui repose sur la délivrance de clés de session (chiffrement symétrique) et de tickets délivrés par des KDC (*Kerberos distribution center*). En environnement AD, ce rôle de KDC est porté par les contrôleurs de domaine. Kerberos permet l'authentification mutuelle de deux systèmes (l'un étant le « client » et l'autre le « service ») et évite le transit de mots de passe en clair sur le réseau. Créé par le MIT en 1988, ce protocole a d'abord été mis en œuvre

sur des systèmes Unix, puis implémenté sous Windows par Microsoft vers la fin des années 90. Il est à noter que l'authentification à un service par Kerberos requiert de joindre ce service par son nom de domaine complet (FQDN). Toute authentification Windows à un service qui est joint par son adresse IP ou par l'interface de boucle locale (*localhost* ou 127.0.0.1) implique un repli sur une authentification NTLM. Pour se familiariser au fonctionnement de Kerberos, se reporter à l'article [71] de Microsoft. Pour un approfondissement technique du sujet, la publication scientifique [29] est une lecture recommandée.

4.1 Conservation en mémoire vive des condensats NTLM et des secrets Kerberos

Il convient en préambule de mettre en évidence le danger des secrets d'authentification réutilisables qui résident en mémoire vive sous forme de condensats NTLM ou de secrets Kerberos. Cette mise en mémoire fait suite à des authentifications interactives (locales ou distantes) réussies en environnement AD.

Authentification interactive locale ou distante

Une authentification Windows est interactive lorsqu'elle est réalisée à l'aide de la mire de connexion (*logon*) Windows qui invite l'utilisateur à fournir les informations d'ouverture de session. Une authentification interactive est locale (*logon type 2* [75]) lorsqu'elle est, sauf rares exceptions, physiquement réalisée sur le système lui-même. Une authentification interactive est distante (*logon type 10* [75]) lorsqu'elle est réalisée à travers le réseau par déport d'affichage RDP [35].

Après une authentification initiale réussie, ces condensats NTLM et secrets Kerberos en mémoire vive sont légitimement réutilisés par le système pour réaliser les authentifications locales ou en réseau de l'utilisateur de manière transparente. Sans ce mécanisme, l'utilisateur serait sans cesse sollicité pour entrer à nouveau ses informations d'authentification.

Authentification réseau

Une authentification réseau (*logon type 3* [75]) est généralement réalisée sans saisie d'information d'ouverture de session. Le système procède à l'authentification à l'aide des secrets d'authentification réutilisables de l'utilisateur stockés en mémoire vive. Ces derniers résident en mémoire vive suite à une authentification interactive locale ou distante préalablement réussie par l'utilisateur.

35. RDP (*remote desktop protocol*) est un protocole de Microsoft utilisé pour le déport d'affichage à travers le réseau, que se soit pour des accès administrateur ou pour des accès utilisateur. Un client RDP (binaire `mstsc.exe`) et un composant serveur (*remote desktop services* ou *terminal services*) sont nativement intégrés au système d'exploitation Windows. RDP est également le protocole sous-jacent de la fonction d'« assistance à distance » de Windows, ainsi que de *remoteApp* ou encore des connexions réalisées à travers une *remote desktop gateway*.

4.2 Extraction des condensats NTLM et des secrets Kerberos de la mémoire vive

Sous Windows, les condensats NTLM et les secrets Kerberos sont stockés en mémoire vive par l'autorité de sécurité locale (LSA, *local security authority*) : le processus `lsass.exe` responsable de l'authentification utilisateur. De fait, il s'agit d'un processus sensible des systèmes d'exploitation Windows clients et serveurs. Pour les authentifications réalisées auprès d'un contrôleur de domaine AD lors d'une ouverture de session interactive, c'est ce processus qui stocke en mémoire vive les secrets d'authentification NTLM de l'utilisateur sous forme de condensats (*NTLM hash*) ainsi que les secrets d'authentification Kerberos sous forme de tickets et de clés de session Kerberos.

L'extraction de condensats NTLM et de secrets Kerberos de la mémoire vive est une opération rendue triviale par les outils très répandus et gratuitement disponibles sur Internet (le plus connu étant le célèbre « mimikatz »). Il est pour cela nécessaire de disposer des privilèges d'administration locale du système. Un attaquant peut, par exemple, avoir obtenu ces privilèges sur un système :

- *de facto* si l'utilisateur compromis est administrateur de son poste de travail (d'où l'importance que les utilisateurs n'utilisent pas leurs postes de travail avec des privilèges d'administration) ;
- par élévations de privilèges locales en exploitant des vulnérabilités non corrigées du système d'exploitation ou des applications installées ;
- à cause de mauvaises pratiques de configuration ou d'administration ;
- par des attaques physiques ou au moyen d'attaques par exhaustivité.

À noter que les mécanismes de sécurité *Windows defender credential guard* et *Windows defender remote credential guard* permettent une meilleure protection en mémoire des secrets d'authentification. Ces deux mécanismes présentent toutefois des limites détaillées en section 4.7. De la même manière, la protection LSA additionnelle [76] est contournable par un attaquant mais reste utile en défense en profondeur. Pour finir, *Microsoft Defender for Endpoint* propose une règle [77] bloquant le vol d'informations d'identification de la LSA mais un attaquant reste en capacité de le désactiver. Quels que soient les mécanismes de protection mis en œuvre, le risque d'extraction des condensats NTLM et des secrets Kerberos de la mémoire vive reste un risque bien réel.

4.3 Réutilisation des condensats NTLM et des secrets Kerberos

Les condensats NTLM extraits de la mémoire vive peuvent être utilisés par un attaquant à la place des secrets d'authentification eux-mêmes (tant qu'ils n'expirent pas) pour s'authentifier auprès des différentes ressources de l'AD. Cette technique d'authentification par réutilisation des condensats est communément appelée *pass-the-hash*. Elle est détaillée dans le document [45] de Microsoft.

La problématique est identique avec les secrets Kerberos. Les TGT (*ticket granting ticket*) Kerberos et leurs clés de session associées peuvent être extraits de la mémoire vive par un attaquant et être

utilisés à la place des secrets d'authentification eux-mêmes (tant qu'ils n'expirent pas) pour obtenir des TGS (*ticket granting service*) qui servent à réaliser des authentifications auprès des différentes ressources de l'AD à travers le réseau. Cette technique d'authentification par réutilisation des TGT et TGS Kerberos (et de leurs clés de session associées) est communément appelée *pass-the-ticket*. Elle est détaillée dans le document [45] de Microsoft.

Les techniques de *pass-the-hash* et de *pass-the-ticket* peuvent être facilement mises en œuvre à l'aide d'outils gratuits et répandus (« mimikatz » et « kekeo » étant les plus connus).

Attention

L'authentification par carte à puce pour l'ouverture de session interactive active l'extension PKINIT [36] du protocole d'authentification Kerberos. Toutefois, l'authentification par carte à puce ne protège pas des attaques de type *pass-the-hash* et *pass-the-ticket*. Elle peut donc, à ce titre, donner un faux sentiment de sécurité. En effet, lorsqu'un compte utilisateur de l'AD est configuré en authentification par carte à puce, le mot de passe n'est pas supprimé pour autant. Au contraire, un nouveau mot de passe AD aléatoire (complexe et sans expiration) est automatiquement généré pour ce compte utilisateur. Puis, après chaque authentification par carte à puce réussie, tout se passe exactement comme lors d'une authentification par simple mot de passe : un KDC transmet le condensat NTLM ou le TGT Kerberos (et sa clé de session associée) au poste client qui les stocke en mémoire vive. Ces secrets peuvent ensuite être extraits de la mémoire vive et réutilisés par *pass-the-hash* ou *pass-the-ticket* sans disposer de la carte à puce.

À savoir toutefois qu'en mode d'authentification standard par mot de passe, l'utilisateur peut changer son mot de passe. Cela se traduit par la génération de nouveaux condensats NTLM et secrets Kerberos et par l'invalidation des anciens. Par contre, dans un contexte d'authentification par carte à puce, le changement de secret d'authentification opéré par un utilisateur (bien que s'effectuant par la même interface graphique) ne change en réalité que le code PIN de déverrouillage de la carte à puce et non pas son mot de passe AD (qui a été initialement généré aléatoirement). Autrement dit, ses condensats NTLM et ses secrets Kerberos restent inchangés et peuvent donc continuer à être utilisés par *pass-the-hash* et *pass-the-ticket* même après changement du code PIN de l'utilisateur. Depuis Windows Serveur 2016, un nouvel attribut du schéma AD (*ms-DS-Expire-Passwords-On-Smart-Card-Only-Accounts* [99]) apporte une solution [37] à ce problème au niveau du domaine.

Information

La technique connue sous le nom de *golden ticket* (ticket en or) est également une technique d'authentification par réutilisation de secrets Kerberos. À la différence que ce super ticket très permissif est forgé par un attaquant au lieu d'être simplement récupéré en mémoire vive. Toutefois, forger un *golden ticket* Kerberos n'est possible

36. Avec PKINIT (*Public Key Cryptography for Initial Authentication*), une cryptographie asymétrique est mise en œuvre lors de l'échange initial Kerberos (échanges `AS_REQ` et `AS_REP`) pour l'obtention d'un TGT et de sa clé de session associée.

37. Lorsque l'attribut *ms-DS-Expire-Passwords-On-Smart-Card-Only-Accounts* [99] est activé (valeur « *TRUE* »), les mots de passe aléatoires des utilisateurs qui s'authentifient par carte à puce sont automatiquement renouvelés dès qu'ils arrivent à expiration (à une fréquence qui dépend donc de la stratégie de mots de passe appliquée à chaque compte).

qu'après avoir compromis un contrôleur de domaine et récupéré le secret du compte `krbtgt` dans sa base `NTDS.DIT`. Un *golden ticket* est généralement forgé par un attaquant dans le seul objectif de faciliter sa persistance et la suite de ses opérations malveillantes sur le SI.

L'extraction aisée des condensats NTLM et des secrets Kerberos couplée aux techniques de *pass-the-hash* et de *pass-the-ticket* en font des secrets d'authentification facilement réutilisables.

R61

Traiter les risques spécifiques de réutilisabilité des condensats NTLM et des secrets Kerberos

Les condensats NTLM et les secrets Kerberos stockés en mémoire vive doivent être considérés comme des secrets d'authentification réutilisables. À ce titre, ils sont assujettis à la recommandation R29 de maîtrise de la dissémination de secrets d'authentification réutilisables du *Tier 0*. Ces condensats NTLM et secrets Kerberos étant mis en jeu dans la grande majorité des scénarios de compromission, leurs facilités d'obtention et de réutilisation par un attaquant ne doivent pas être sous-estimées.

Le tableau 2 en section 4.6 dresse une liste, non exhaustive, des méthodes de connexion les plus courantes et indique, pour chacune, si elle laisse ou non des secrets d'authentification réutilisables sur les systèmes administrés.

4.4 Large dissémination des condensats NTLM et des secrets Kerberos dans un SI

Comme NTLM et Kerberos sont les protocoles d'authentification utilisés dans un domaine AD lors d'une ouverture de session interactive, les condensats NTLM ou les tickets et clés de session kerberos sur lesquels ils reposent se trouvent *de facto* disséminés sur la plupart des systèmes Windows membres de l'AD, au gré de ces ouvertures de session interactives. Il est important de comprendre que la dissémination de secrets sur les systèmes est techniquement inévitable. Les équipes de SSI et d'administration de l'AD ne doivent donc pas chercher à supprimer la dissémination des secrets, puisque ce n'est pas possible. En revanche, elles doivent chercher à en contrôler et en maîtriser la dissémination de manière à ce qu'elle ne nuise pas au cloisonnement logique de l'AD et des zones de confiance. C'est-à dire que, par exemple, la dissémination de secrets d'authentification réutilisables du *Tier 0* sur le périmètre du *Tier 0* est légitime et ne pose pas de problème de sécurité. Par contre, il est est impératif d'éviter leur dissémination sur des systèmes de moindre confiance (*Tier 1* et *Tier 2*).

Dans le cas d'un utilisateur bureautique du *Tier 2*, les condensats NTLM et secrets Kerberos de son compte se trouvent généralement disséminés sur peu de systèmes : sur son poste bureautique principal, mais également sur les systèmes partagés où il est amené à ouvrir des sessions interactives (postes de présentation en salles de réunion, serveurs de déport d'affichage pour accéder à des applications métiers, etc.).

Dans le cas des administrateurs en revanche, les risques sont bien plus importants. En effet, un annuaire AD n'est quasiment jamais administré par des authentifications interactives locales sur

les contrôleurs de domaine AD mais plutôt par différentes méthodes d'administration distante. Les plus courantes sont RDP, PowerShell (à travers *Windows remote management*, WinRM) et RPC (*remote procedure call*, c'est-à-dire généralement par l'utilisation des composants enfichables de la MMC [78]). L'administration distante des ressources du *Tier 0* implique que des secrets d'authentification du *Tier 0* soient saisis, stockés ou traités sur les équipements utilisés pour l'administration distante. C'est pourquoi la recommandation générale R29 de maîtrise de la dissémination des secrets d'authentification réutilisables et sa déclinaison R61 liée à la réutilisabilité des condensats NTLM et des secrets Kerberos, justifient que l'administration du *Tier 0* ne se fasse que depuis des postes d'administration également catégorisés en *Tier 0* (les aspects ayant trait aux architectures d'administration ainsi qu'à l'architecture des équipements d'administration font plus spécifiquement l'objet du chapitre 5).

D'autre part, les pratiques d'administration usuelles font que les administrateurs sont susceptibles d'ouvrir des sessions interactives locales ou distantes sur de nombreux systèmes du SI (postes bureautiques et serveurs) pour les administrer. Ce faisant, ils disséminent leurs condensats NTLM et secrets Kerberos privilégiés sur ces systèmes. Quand une session Windows interactive locale ou distante AD est par exemple réalisée avec un compte de *Tier 0* sur un poste de travail de *Tier 2*, les secrets d'authentification réutilisables du compte de *Tier 0* y sont mémorisés. Un attaquant qui aurait compromis ce poste de travail de *Tier 2* est donc en mesure de les extraire de la mémoire vive. En les réutilisant, il peut obtenir le contrôle de l'annuaire AD. Étant donné la haute probabilité de compromission des postes de travail (du fait de leur forte exposition à des attaques), ce constat met l'accent sur la nécessitée de bien cloisonner le SI en zones de confiance et de restreindre techniquement le périmètre de dissémination des secrets d'authentification réutilisables.

4.5 Cas particulier des mots de passe d'ouverture de session en cache

Il est à noter qu'après l'authentification interactive locale réussie d'un compte du domaine AD sur un système – qu'elle soit locale ou distante et par NTLM ou par Kerberos – un condensat de son mot de passe y est généralement stocké en cache dans le registre, en complément des condensats NTLM et des secrets Kerberos en mémoire vive. Grâce à ce cache, le système est en mesure de valider une ouverture de session ultérieure de l'utilisateur sans connectivité réseau (ce qui peut être nécessaire dans un contexte de nomadisme ou pour pallier à toute interruption réseau qui empêcherait de joindre un contrôleur de domaine, entre autres). Par défaut, Windows garde en cache les condensats des 10 derniers mots de passe d'ouverture de session. Souvent, la taille de ce cache est configurée[38] par les organisations à une valeur inférieure (1 ou 2 le plus souvent, sachant qu'une valeur de 0 permet de désactiver la mise en cache), car il s'agit d'un durcissement usuel. À savoir que dans ses *security baselines*, Microsoft ne recommande pas de taille pour ce cache (cf. documentation [80]), dans la mesure où la taille idéale dépend en réalité des besoins et des contraintes de l'organisation pour chaque catégorie de système.

Ces mots de passe d'ouverture de session en cache sont enregistrés par le système sous forme de condensats « MS-CACHE v1 » ou « MS-CACHE v2 » en fonction de la version du système d'ex-

38. La configuration du nombre de condensats de mots de passe d'ouverture de session gardés en cache est généralement réalisée par GPO à l'aide d'une stratégie de sécurité, comme indiqué par la page de documentation [80] de Microsoft.

ploitation. Dans les deux cas, le condensat MS-CACHE peut être aisément extrait du registre par un attaquant (qui dispose des droits d'administration locale). Il peut ensuite faire l'objet d'une attaque par exhaustivité hors-ligne, dans l'optique de découvrir le mot de passe de l'utilisateur. Ce dernier peut donc être découvert plus ou moins rapidement (mais beaucoup moins rapidement en MS-CACHE v2 qu'en MS-CACHE v1).

En termes de risques à traiter et de mesures de sécurité à mettre en œuvre pour assurer le cloisonnement d'un SI, il peut être considéré que le risque de réutilisation de secrets d'authentification NTLM et Kerberos englobe le risque de découverte et de réutilisation de mots de passe d'ouverture de session en cache sur les systèmes, dans la mesure ou leur risque de dissémination est équivalent. Dès lors et dans un objectif de simplification, il est inutile de traiter ces deux menaces de manière différenciée : le présent chapitre traite du risque général de dissémination de secrets d'authentification réutilisables suite à des ouvertures de session interactives.

4.6 Risques de dissémination en fonction de la méthode de connexion

Le tableau 2 liste les méthodes de connexion distante les plus répandues – que se soit pour des accès administrateur ou pour des accès utilisateur – et indique lesquelles disséminent des secrets d'authentification réutilisables sur les hôtes distants.

Méthode de connexion distante	Dissémination de secret réutilisable ?
Authentification interactive locale (autrement dit, par ouverture de session interactive locale)	Oui
Utilisation de *runAs*[a]	Oui
Ouverture de session interactive au travers d'interfaces IPMI	Oui
Ouverture de session interactive au travers d'un équipement commutateur KVM réseau IP	Oui
Ouverture de session interactive par RDP sans l'option *restricted admin* (ce qui est le cas par défaut[b])	Oui
Ouverture de session interactive par RDP à travers une *remote desktop gateway*	Oui
Authentification dite « basique »[c] (*basic authentication*) impliquant que le nom d'utilisateur et le mot de passe soient saisis au moment de la connexion et soient transmis en clair au service distant	Oui
PowerShell WinRM avec protocole d'authentification CREDSSP[d]	Oui
PsExec avec *credentials* explicites (c'est-à-dire en utilisant le commutateur « `-u utilisateur` »)	Oui

Ce tableau se poursuit sur la page suivante

Méthode de connexion distante	Dissémination de secret réutilisable ?
Ouverture de session interactive par RDP avec l'option *restricted admin* (RDP RA)[b]	Non
Authentification Windows intégrée[e] à des services par le réseau	Non
PowerShell WinRM avec le protocole d'authentification par défaut (c'est à dire par Kerberos ou NTLM)	Non
PsExec avec *credentials* implicites (c'est-à-dire sans utiliser le commutateur « `-u utilisateur` »)	Non
Commandes `NET USE`	Non
Appels RPC (par l'utilisation des composants logiciels enfichables de la MMC notamment)	Non
Registre à distance	Non

[a] L'utilisation de *runAs* (« exécuter en tant que ») sur un système a pour effet d'y réaliser une authentification interactive locale en arrière-plan et présente donc les mêmes risques qu'une authentification interactive locale.

[b] Le mode RDP RA, pour être activé, doit être explicitement indiqué à l'exécution du client RDP (à l'aide du commutateur `/RestrictedAdmin`) et accepté par le serveur RDP. Ces configurations ne sont pas celles définies par défaut (sujet abordé plus en détail en annexe E).

[c] L'authentification basique tend à disparaître et à être interdite par défaut. Pour autant, il reste probable que d'anciens applicatifs continuent de l'utiliser, ce qui peut par exemple être le cas d'applications Web (l'authentification basique étant alors réalisée via un formulaire Web ou une fenêtre surgissante – *popup* – du navigateur).

[d] Pour les Cmdlets PowerShell utilisant WinRM (c'est-à-dire « `New-PSSession` », « `Connect-WSMan` » ou « `Invoke-Command` » par exemple), le commutateur « `-authentication:CredSSP` » permet d'utiliser le protocole d'authentification CredSSP et cela a pour conséquence de déléguer les *credentials* de l'utilisateur à l'hôte distant (ils peuvent alors être extraits de la mémoire vive). L'authentification CredSSP est généralement utilisée pour rendre possible le rebond (*second hop* [94]) vers d'autres ressources du SI.

[e] L'authentification Windows intégrée (c'est-à-dire reposant sur du *single sign-on* NTLM ou Kerberos) est une authentification réseau (*logon type 3* [75]).

Tableau 2 – Dissémination de secrets d'authentification réutilisables sur les hôtes distants en fonction de la méthode de connexion ou d'administration utilisée

Information

Le tableau 2 s'inspire grandement des tableaux « *logon types* » et « *connection methods and where the credentials are created and cached* » du guide [45] de Microsoft dont la lecture est recommandée pour approfondir les problèmes de sécurité relatifs aux condensats NTLM et aux secrets Kerberos.

Exemple

Administrer une ressource de *Tier 1* par RPC à l'aide de la MMC (via le composant enfichable « utilisateurs et ordinateurs Active Directory » par exemple) depuis un poste d'administration du *Tier 0* et avec un compte d'administration du *Tier 0* est une pratique qui peut être tolérée du point de vue du cloisonnement des *Tiers* (elle correspond à la recommandation R80- de la section 5.2.1). En effet, il s'agit d'une méthode d'administration qui ne dissémine pas de secrets d'authentification réutilisables sur les hôtes administrés.

Information

Il est à noter que des solutions logicielles d'éditeurs tiers peuvent également reposer sur des mécanismes d'authentification propriétaires ou natifs au système Windows, amenant donc potentiellement à l'export de secrets d'authentification réutilisables sur les systèmes administrés. Par ailleurs, le processus `lsass.exe` n'est pas le seul à stocker des secrets d'authentification réutilisables. Des applications peuvent par exemple stocker des secrets dans des fichiers texte, dans le registre, etc. Ces risques doivent également être pris en compte préalablement à tout déploiement d'applications tierces.

4.7 Limites de Windows defender credential guard et remote credential guard

Depuis Windows 10 (1607) et Windows Serveur 2016, *Windows defender credential guard* (WDCG) [53] et *Windows defender remote credential guard* (WDRCG) [87] sont des mécanismes de sécurité qui visent à empêcher l'extraction des condensats NTLM et des secrets Kerberos réutilisables de la mémoire vive du système.

Attention

WDCG et WDRCG peuvent apporter un faux sentiment de sécurité, car un attaquant ayant compromis un système protégé par WDCG ou WDRCG reste en mesure de détourner (*hijacking*) une session interactive active (ou déconnectée, mais non fermée) d'un utilisateur du domaine connecté localement ou à distance par RDP.

En effet, le contexte utilisateur `NT AUTHORITY\SYSTEM` (qu'un administrateur local peut légitimement obtenir) peut, par emprunt d'identité (*impersonation*) [69], prendre le contrôle de n'importe quel contexte utilisateur actif sur le système (c'est-à-dire de n'importe quelle session utilisateur non fermée) sans avoir à fournir

d'authentification. Cette prise de contrôle consistant généralement à exécuter des processus en arrière plan ou en mode console, elle est donc invisible pour l'utilisateur dont l'identité est empruntée. L'emprunt d'identité et le contrôle d'une session utilisateur active peuvent être facilement réalisés à l'aide d'outils très répandus et gratuitement disponibles sur Internet (le célèbre « mimikatz » dispose notamment de cette fonctionnalité).

Par détournement de session, un attaquant est donc en mesure d'utiliser les droits et privilèges d'un utilisateur connecté sans pour autant avoir besoin d'extraire ses secrets d'authentification réutilisables. En termes de risques à traiter et de mesures de sécurité à mettre en œuvre pour assurer le cloisonnement d'un SI, il peut être considéré que le risque de réutilisation de secrets d'authentification englobe le risque de réutilisation de droits et privilèges par détournement de session. Dès lors et dans un objectif de simplification, il est inutile de traiter ces deux menaces de manière différenciée : le présent chapitre traite du risque général de dissémination de secrets d'authentification réutilisables suite à des ouvertures de session interactives.

4.7.1 Windows defender credential guard

Historiquement, WDCG n'était pas activé par défaut et de nombreux prérequis [54] matériels et logiciels étaient nécessaires à son activation. À compter de Windows 11 entreprise en version 22H2 et de Windows 11 éducation en version 22H2, ce n'est toutefois plus le cas et les systèmes compatibles ont désormais WDCG activé par défaut.

Le présent guide n'a pas vocation à détailler ce mécanisme de sécurité. Il est à noter toutefois que WDCG fait l'objet d'un chapitre du guide de « mise en œuvre des fonctionnalités de sécurité de Windows 10 reposant sur la virtualisation » [3] de l'ANSSI.

R62

Utiliser WDCG uniquement dans une démarche de défense en profondeur

Les limites et les méthodes de contournement dont souffre *Windows defender credential guard* ne permettent pas de considérer ce mécanisme comme une mesure de sécurité qui protègerait les systèmes contre les risques de réutilisation des droits et privilèges des administrateurs qui s'y connectent par ouverture de session interactive locale ou distante.

La mise en œuvre de *Windows defender credential guard* est uniquement recommandée dans une démarche de défense en profondeur. Son déploiement avec verrouillage UEFI est dans ce cas obligatoire pour éviter qu'un attaquant puisse désactiver le mécanisme de façon triviale.

4.7.2 Windows defender remote credential guard

WDRCG est un mécanisme de sécurité qui n'est pas activé par défaut. Son activation est simple étant donné qu'elle présente peu de prérequis [88].

L'utilisation de WDRCG n'est pas nécessairement recommandée, même dans une démarche de défense en profondeur. En effet, ce mécanisme s'utilise en remplacement d'autres pratiques de

connexion distante par RDP qui offrent un meilleur niveau de sécurité pour respecter le cloisonnement des zones de confiance.

R63

Ne pas utiliser WDRCG entre zones de confiance hétérogènes

Windows defender remote credential guard est un mécanisme de sécurité dont l'utilisation n'est pas recommandée pour les connexions RDP entre hôtes de différentes zones de confiance. Pour les connexions RDP dans un tel contexte, il est recommandé de privilégier l'une des deux méthodes de connexion suivantes :

- RDP avec l'option *RestrictedAdmin* (cf. annexe E) ;
- RDP sans l'option *RestrictedAdmin* mais en spécifiant un compte de connexion appartenant à la zone de confiance de l'hôte de destination (cf. section 4.8), ce que WDRCG ne permet pas de faire puisqu'il impose un *single sign-on* Kerberos.

L'utilisation de WDRCG reste néanmoins intéressante lorsque la connexion RDP est réalisée entre deux hôtes d'une même zone de confiance (et donc avec un compte utilisateur ayant de droits et privilèges uniquement au sein de cette zone), c'est-à-dire sans que le risque de détournement de session puisse nuire au cloisonnement des zones de confiance.

4.8 Méthodes de connexion permettant de spécifier le compte servant à l'authentification

Il convient de préciser une subtilité importante pour la bonne compréhension du tableau 2 et des risques associés aux différentes méthodes de connexion distante : une méthode de connexion distante qui dissémine des secrets d'authentification réutilisables n'est pas *de facto* à proscrire. L'attention doit en réalité être portée sur le couple (« méthode de connexion » + « compte ») utilisé.

En effet, certaines méthodes de connexion distante (cas de RDP) permettent la saisie du compte utilisateur utilisé pour l'authentification auprès de l'hôte distant. C'est dans ce cas le secret d'authentification réutilisable du compte de connexion saisi qui est disséminé sur l'hôte distant. Un administrateur peut alors saisir un compte de connexion appartenant à la zone de confiance de l'hôte distant, plutôt que d'utiliser le compte avec lequel il a ouvert sa session interactive locale sur son poste d'administration. Cette bonne pratique permet d'administrer des ressources de moindre confiance (de *Tier 1* ou de *Tier 2* par exemple) sans risquer d'y disséminer de secrets d'authentification réutilisables plus sensibles (du *Tier 0* notamment).

Lorsque la méthode de connexion distante utilisée est de nature à disséminer des secrets d'authentification réutilisables, alors le compte de connexion utilisé doit avoir des droits et privilèges uniquement dans la zone de confiance de destination de la connexion, cela afin d'éviter de créer des chemins d'attaque entre zones de confiance. Il est d'ailleurs possible d'obtenir un cloisonnement logique encore plus fin si le compte de connexion utilisé a uniquement des droits et privilèges sur une unique valeur métier ou sur un ensemble restreint de moyens d'accès au SI, voire même sur une unique ressource du SI. De manière générale plus le compte de connexion utilisé aura

des droits et privilèges limités au sein de sa zone de confiance, moins sa réutilisation présentera d'intérêt pour un attaquant.

En cherchant à réutiliser un secret d'authentification vers d'autres ressources du SI auprès desquelles son authentification sera refusée, un attaquant déclenchera la journalisation d'évènements d'échec d'authentification, alertant alors les équipes SSI sur une potentielle attaque en cours (cf. section 2.4 sur la journalisation et la détection). Finalement, plus les comptes de connexion ont des droits et privilèges limités à un périmètre restreint de ressources du SI, plus un attaquant sera susceptible de déclencher des alertes de sécurité lors de ses tentatives de réutilisation de secrets d'authentification à travers le réseau.

4.9 Connexion distante à des ressources de moindre confiance

La recommandation R8 de cloisonnement de l'administration de chaque *Tier* a précédemment énoncé que « la mutualisation des comptes et des ressources d'administration pour administrer plusieurs *Tiers* est envisageable dès lors que certaines conditions de sécurité relatives aux méthodes et postes d'administration utilisés sont respectées ». À ce stade des approfondissements techniques concernant les méthodes de connexion et la dissémination de secrets d'authentification NTLM et Kerberos réutilisables, les conditions de mutualisation évoquées ont été techniquement développées. Elles peuvent désormais être formulées plus précisément par la recommandation R64.

R64

Encadrer et restreindre la connexion à des ressources de moindre confiance

Pour maîtriser la dissémination de secrets d'authentification réutilisables, la connexion à des ressources de moindre confiance par des comptes de plus haut niveau de confiance que ces ressources doit être encadrée, organisationnellement et techniquement. Une telle connexion doit être proscrite lorsque la méthode de connexion est de nature à disséminer les secrets d'authentification réutilisables du compte de connexion (cf. tableau 2), que se soit pour des accès administrateur ou pour des accès utilisateur. En revanche, une telle connexion peut être tolérée dans le cas contraire (à noter que la dissémination de secrets d'authentification réutilisables n'est pas le seul risque à prendre en compte pour concevoir une architecture d'administration, ce sujet faisant l'objet du chapitre 5).

En particulier, la connexion à des ressources du *Tier 1* ou du *Tier 2* avec un compte du *Tier 0* doit être proscrite dès lors que la méthode de connexion employée est de nature à disséminer des secrets d'authentification réutilisables de ce compte de *Tier 0* (c'est-à-dire ses condensats NTLM ou ses secrets Kerberos dans la majorité des cas).

En complément des mesures organisationnelles, des mesures de sécurité techniques doivent être mises en œuvre pour appliquer cette restriction. Pour les comptes et les postes d'administration de *Tier 0*, il est notamment recommandé l'application cumulative des mesures de sécurité suivantes :

- mettre en œuvre un silo d'authentification du *Tier 0* ou des stratégies d'authentification équivalentes (leurs mises en œuvre sont détaillées en annexe C);
- configurer les paramètres de sécurité Windows permettant de restreindre les ouvertures de session des comptes de *Tier 0* sur les ressources de *Tier 1* et de *Tier 2* (l'application de ces paramètres de sécurité est détaillée en annexe D);
- imposer techniquement l'utilisation de l'option *restricted admin* pour les connexions RDP vers des ressources de moindre confiance depuis des postes d'administration du *Tier 0* (cette configuration de RDP est détaillée en annexe E);
- sécuriser les méthodes de connexion autorisées (sujet abordé en section 5.1);
- bloquer les flux réseau vers le *Tier 1* et le *Tier 2* qui correspondent à des méthodes de connexion interdites par l'organisation depuis le *Tier 0* (cf. section 3.7.2 sur la segmentation et le filtrage réseau).

Cette recommandation R64 est illustrée par la figure 9.

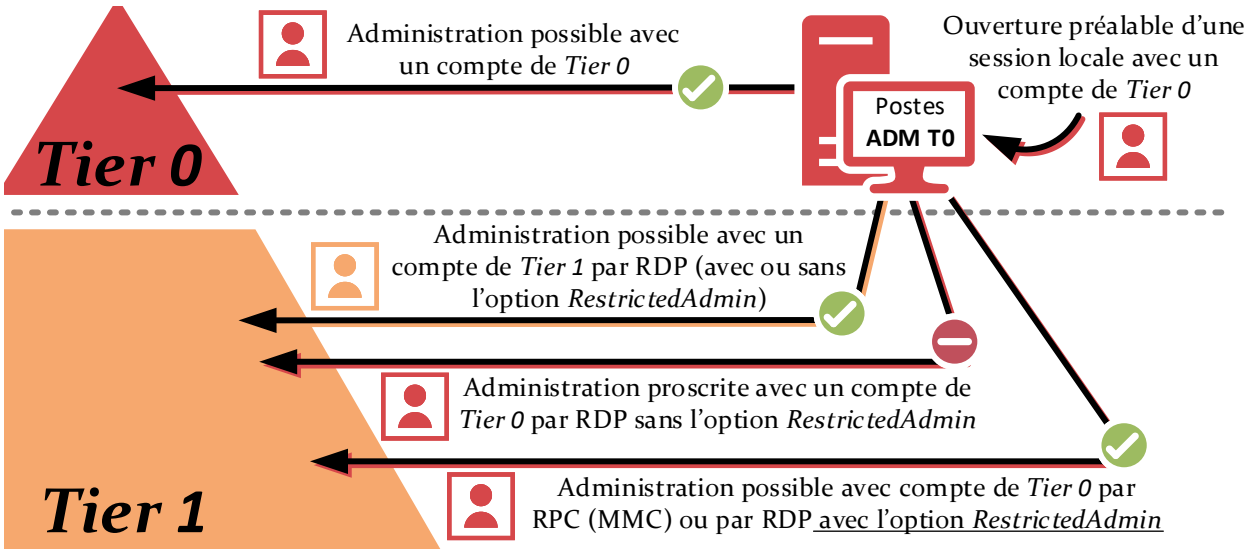

FIGURE 9 – Exemples de méthodes d'administration du *Tier 1* depuis le *Tier 0* et des risques de dissémination de secrets réutilisables qu'elles présentent.

4.10 Dangers des délégations Kerberos

Le protocole Kerberos prévoit un mécanisme de délégation qui, s'il est mis en œuvre sans précaution, peut aller à l'encontre du cloisonnement des zones de confiance.

Délégation Kerberos

Un service peut se voir octroyer la possibilité de faire de la délégation Kerberos. Après qu'un utilisateur s'est authentifié auprès d'un service disposant d'une telle capacité, ce service peut utiliser les secrets d'authentification Kerberos (les TGT et clés de session associées) de l'utilisateur pour s'authentifier, en se faisant passer pour l'utilisa-

teur, à d'autres ressources du SI. Ces secrets sont stockés dans la mémoire vive du serveur où s'exécute le service (comme si l'utilisateur y avait ouvert une session interactive).

La compromission de services autorisés à faire de la délégation Kerberos, ou des serveurs qui les portent, permet à un attaquant de récupérer de nombreux secrets Kerberos. Si des utilisateurs d'une zone de confiance A s'authentifient auprès d'un service faisant de la délégation Kerberos dans une autre zone B, alors cette mauvaise pratique créée un chemin d'attaque de la zone B vers la zone A et va donc à l'encontre de leur cloisonnement.

La délégation Kerberos est un mécanisme dont l'usage est courant dans un SI. Il existe plusieurs types de délégation Kerberos, plus ou moins contrainte et donc plus ou moins dangereuse. De manière simplifiée :

- une délégation Kerberos non contrainte (*Kerberos unconstrained delegation*, KUD), octroyée à un compte machine ou de service de l'AD, lui permet d'endosser l'identité des utilisateurs qui s'y connectent [39] pour s'authentifier auprès de toutes les ressources de l'AD sans restrictions. Si un administrateur du *Tier 0* se connecte à un service de *Tier 2* doté d'une KUD, son secret d'authentification réutilisable y sera stocké en mémoire vive et ce dernier pourra être réutilisé pour prendre le contrôle de n'importe quelle ressource de l'AD (incluant donc les contrôleurs de domaine) ;
- une délégation Kerberos contrainte (*Kerberos constrained delegation*, KCD) permet en revanche de préciser vers quelles ressources et vers quels services il est autorisé à endosser l'identité des utilisateurs qui s'y connectent. Un serveur Web, par exemple, peut avoir une KCD l'autorisant à endosser l'identité des utilisateurs qui s'y connectent, mais uniquement auprès d'un service de gestion de bases de données qui stocke des données métiers dont il a besoin. Dans ce cas, les secrets d'authentification Kerberos stockés en mémoire vive du serveur ne peuvent être techniquement réutilisés qu'à destination de cette seule base de données ;
- une délégation Kerberos de type ressource (*Ressource based constrained delegation*, RBCD), à l'inverse des deux autres, n'est pas octroyée au service qui va endosser l'identité des utilisateurs qui s'y connectent ; elle est octroyée au service cible de la délégation. Un service de base de données, par exemple, peut se voir octroyer une RBCD autorisant des serveurs Web de l'organisation à endosser, auprès de lui, l'identité des utilisateurs qui se connectent à ces serveurs Web. L'avantage de la RBCD est qu'elle peut être configurée par un administrateur du service de bases de données (*Tier 1* ou *Tier 2* généralement), tandis qu'octroyer des KUD ou KCD nécessite d'être administrateur du domaine (*Tier 0*).

R65

Traiter les risques inhérents aux délégations Kerberos

En application de la recommandation R29 de maîtrise de la dissémination des secrets d'authentification réutilisables et de la recommandation R64 d'encadrement de la connexion à des ressources de moindre confiance, les délégations Kerberos doivent être configurées avec précaution pour ne pas nuire au cloisonnement des zones de confiance. Il est notamment important que, de manière cumulative :

39. voire même d'un utilisateur arbitraire si la délégation a été configurée en autorisant la transition de protocole.

- les délégations contraintes configurées ne créent aucun chemin d'attaque d'une zone de confiance à une autre (c'est-à-dire depuis un service d'une zone de confiance et vers un service d'une autre zone de confiance), à moins que le risque ait été dûment évalué et accepté après analyse des scénarios de menace ;
- les délégations non contraintes soient exclusivement octroyées à des ressources du *Tier 0* (et idéalement, à des contrôleurs de domaine uniquement) ;
- les délégations contraintes soient systématiquement proscrites à destination de quelconque service du *Tier 0* ;
- la configuration de délégations contraintes basées sur les ressources soit prohibée sur des services du *Tier 0* depuis toute autre zone de confiance ;
- la délégation Kerberos des comptes d'administration (de *Tier 0* au minimum, et autant que possible également pour ceux du *Tier 1* et du *Tier 2*) soit interdite, soit en leur donnant l'appartenance au groupe de sécurité des utilisateurs protégés (*protected users*, cf. annexe B), soit en activant l'attribut « le compte est sensible et ne peut pas être délégué » sur tous les comptes utilisateurs du *Tier 0*.

4.11 Dangers de l'absence de préauthentification Kerberos

Avec la préauthentification Kerberos activée, la demande de TGT d'un utilisateur doit contenir un horodatage récent (datant de moins de 5 minutes par défaut) chiffré avec le condensat de son mot de passe. Le KDC s'assure ainsi que la demande de TGT provient d'un utilisateur légitime et qu'elle est récente (protection anti-rejeu). Sans préauthentification Kerberos activée, un attaquant peut :

1. réaliser une demande de TGT pour un utilisateur arbitraire et donc obtenir du KDC un message Kerberos chiffré avec le condensat du mot de passe de cet utilisateur ;
2. mener des attaques par exhaustivité hors-ligne sur le message Kerberos obtenu, dans l'optique de découvrir le mot de passe de l'utilisateur.

Cette attaque exploitant l'absence de préauthentification Kerberos est connue sous le nom de *AS-REP roasting*.

R66

Préserver la préauth. Kerberos pour les comptes de Tier 0

Par défaut, tous les comptes utilisateur de l'AD ont la préauthentification Kerberos activée (depuis Windows 2000). Cette préauthentification doit être obligatoire et ne doit donc jamais être optionnelle pour les comptes du *Tier 0*.

Il est recommandé de vérifier périodiquement que la préauthentification est imposée aux comptes de *Tier 0* et qu'il n'y a pas de régression à cette configuration.

La commande PowerShell du listing 8 permet de lister les comptes utilisateurs dont la préauthentification Kerberos a été désactivée.

```
Get-ADUser -Filter "useraccountcontrol -band 4194304" -Properties useraccountcontrol
```

Listing 8 – Commande PowerShell permettant de lister les comptes utilisateurs ayant la préauthentification Kerberos désactivée

R67

Traiter les risques inhérents à l'absence de préauth. Kerberos

En cas d'incompatibilité avec une application, rendre optionnelle la préauthentification Kerberos de certains comptes utilisateurs est acceptable si ces trois conditions sont réunies :

- une stratégie de mot de passe affinée (*password settings object* ou PSO [86]) est appliquée à ces comptes utilisateurs. Elle leur impose un mot de passe complexe, une longueur supérieure à 32 caractères et une durée d'expiration maximale de 3 ans (le listing 12 précise comment créer une telle stratégie). L'utilisation de *managed service accounts* (détaillés en section 4.14) permet de répondre automatiquement à ces contraintes de mots de passe ;
- les mots de passe de ces comptes ont été changés depuis que ce PSO leur est appliqué ;
- seuls des chiffrements Kerberos par AES (128 ou 256 bits) sont autorisés pour ces comptes. Et ce, soit par désactivation des algorithmes Kerberos `DES-CBC-*` et `RC4-HMAC-*` dans le domaine AD [72], soit par la configuration explicite [73] du support d'AES sur les comptes en question [72].

R67 -

Réduire la portée des secrets réutilisables exposés par l'absence de préauth. Kerberos

Dans l'alternative, il convient de limiter les conséquences d'une compromission des comptes utilisateurs dont la préauthentification Kerberos a été désactivée pour des questions de compatibilité applicative. C'est-à-dire que, si compte tenu de contraintes spécifiques pesant sur le SI, aucune des recommandations R66 et R67 n'est applicable à un compte utilisateur, alors ce dernier doit :

- avoir des droits et privilèges réduits au strict besoin opérationnel ;
- pouvoir se connecter uniquement sur un ensemble de ressources aussi restreint que possible et faisant exclusivement partie de la même zone de confiance que lui.

Dans le cas d'une application ne supportant pas la préauthentification Kerberos et qui mettrait l'AD en péril, alors cette application doit faire l'objet d'une évolution technique ou bien elle doit être isolée de la forêt AD (sujet traité en annexe F).

4.12 Renforcement de la protection des échanges Kerberos

L'interception réseau des échanges Kerberos utilisateurs pour l'obtention de TGT (échanges `AS_REQ` et `AS_REP`) et de TGS (échanges `TGS_REQ` et `TGS_REP`) permet à un attaquant de mener des attaques par exhaustivité hors-ligne pour tenter de découvrir les mots de passe des comptes utilisateurs que

ces échanges concernent. La protection de ces échanges peut être renforcée en activant le blindage Kerberos (*Kerberos armoring*). Ce blindage repose essentiellement sur la protection supplémentaire des échanges Kerberos utilisateurs à l'aide du compte d'ordinateur depuis lequel ces échanges sont initiés. Comme les comptes d'ordinateur ont un mot de passe complexe d'une taille de 240 bits, ils rendent ces attaques par exhaustivité hors-ligne irréalistes. Ce guide n'a pas vocation à expliquer en détail les principes de chiffrement relatifs au blindage Kerberos ; les lecteurs qui souhaitent approfondir ce sujet sont invités à lire l'article [30].

R68

Activer le blindage Kerberos sur les systèmes du Tier 0

Il est recommandé d'activer le blindage Kerberos sur les systèmes du *Tier 0* pour renforcer la protection des échanges Kerberos opérés sur ces derniers.

L'activation du blindage Kerberos sur les systèmes du *Tier 0* peut notamment se faire par GPO à l'aide des stratégies de sécurité indiquées par les listings 9 (appliquées aux systèmes du *Tier 0*) et 10 (appliquées aux contrôleurs de domaine). Il est à noter toutefois que le support des revendications, de l'authentification composée et du blindage Kerberos par les contrôleurs de domaine requiert un DFL supérieur ou égal à 5 (Windows Serveur 2012, cf. section 3.1.1), tandis que ce même support par les systèmes membres de l'AD est disponible à partir de Windows 8.

```
Chemin : Configuration ordinateur\Modèles d'administration\Système\Kerberos

Paramètre : Prise en charge du client Kerberos pour les revendications,
  l'authentification composée et le blindage Kerberos : Activé
```

Listing 9 – Paramètres de stratégie de sécurité pour le support des revendications de l'authentification composée et du blindage Kerberos par les systèmes membres de l'AD

```
Chemin : Configuration ordinateur\Modèles d'administration\Système\KDC

Paramètre : Prise en charge du contrôleur de domaine Kerberos pour les revendications,
  l'authentification composée et le blindage Kerberos : Activé avec la valeur "Pris en charge"
```

Listing 10 – Paramètres de stratégie de sécurité pour le support des revendications, de l'authentification composée et du blindage Kerberos par les contrôleurs de domaine

4.13 Dangers des attaques par Kerberoasting

Parmi les comptes utilisateurs du domaine utilisés comme comptes de service, ceux qui ont un SPN (*service principal name* [102]) Kerberos déclaré dans l'AD (généralement pour permettre une authentification Kerberos à travers le réseau auprès de ces services) doivent faire l'objet d'une vigilance particulière, car ils sont sujets à des attaques dites de *Kerberoasting*. De manière similaire à l'attaque *AS-REP roasting* décrite en section 4.11, le *Kerberoasting* consiste en :

1. une demande de ticket de service à un KDC pour s'authentifier auprès d'un service dont le SPN est porté par un compte utilisateur ;
2. la tentative de découvrir le mot de passe de ce compte en menant des attaques par exhaustivité hors-ligne sur le ticket de service Kerberos obtenu (qui est chiffré avec le condensat de ce mot de passe).

En conclusion, les secrets d'authentification réutilisables des comptes utilisateurs ayant un SPN déclaré dans l'AD peuvent être obtenus par *Kerberoasting*, et cette attaque peut être menée par n'importe quel utilisateur non privilégié de l'AD et depuis n'importe quel ordinateur.

R69

Proscrire l'exposition par SPN de secrets du Tier 0 réutilisables

Pour éliminer tout risque de *Kerberoasting* des comptes du *Tier 0*, les comptes utilisateurs ayant un SPN déclaré dans l'AD doivent être proscrits sur le *Tier 0*.

Le script PowerShell du listing 11 permet de lister les comptes utilisateurs ayant un SPN déclaré dans l'AD et qui peuvent donc faire l'objet d'une attaque par *Kerberoasting*.

```
Get-ADUser -filter * -Properties * `
    | Where {$_.ServicePrincipalName -ne $null -and $_.Name -ne "krbtgt"} `
    | Select Name, ServicePrincipalName
```

Listing 11 – Script PowerShell permettant de lister les comptes utilisateurs ayant un SPN déclaré dans l'AD et pouvant faire l'objet d'une attaque par *Kerberoasting*

Information

Le compte `krbtgt` est un compte utilisateur du *Tier 0* qui a un SPN déclaré dans l'AD mais comme aucun ticket de service Kerberos ne peut être émis pour ce compte utilisateur, il n'est pas concerné par le risque de *Kerberoasting*.

R70

Traiter les risques inhérents à l'exposition par SPN de secrets réutilisables

Les comptes utilisateurs ayant un SPN déclaré dans l'AD sont à éviter autant que possible. Lorsque ce n'est pas possible, ils peuvent être acceptés si ces trois conditions sont réunies :

- une stratégie de mot de passe affinée (*password settings object* ou PSO [86]) est appliquée à ces comptes utilisateurs, leur imposant un mot de passe complexe, une longueur supérieure à 32 caractères et une durée d'expiration maximale de 3 ans (le listing 12 illustre comment créer une telle stratégie). L'utilisation de *managed service accounts* (détaillés en section 4.14) permet de répondre automatiquement à ces contraintes de mots de passe ;
- les mots de passe de ces comptes ont été changés depuis que ce PSO leur est appliqué ;
- seuls des chiffrements Kerberos par AES (128 ou 256 bits) sont autorisés pour ces comptes, soit par désactivation [72] des algorithmes Kerberos `DES-CBC-*` et `RC4-HMAC-*` dans le domaine AD, soit par la configuration explicite [72] du support d'AES sur les comptes en question.

```
# Création d'un PSO requérant un mot de passe de 32 caractères, sans verrouillage, avec une durée
# d'expiration de 3 ans (1095 jours), prioritaire (precedence de 1), stocké sans chiffrement
# réversible, complexe et protégé contre la suppression accidentelle :
New-ADFineGrainedPasswordPolicy "PSO_ServiceAccounts" -ComplexityEnabled:$true `
    -LockoutThreshold:"0" -MaxPasswordAge:"1095.00:00:00" -MinPasswordLength:"32" `
    -Precedence:"1" -ReversibleEncryptionEnabled:$false `
    -ProtectedFromAccidentalDeletion:$true -ComplexityEnabled:$true
# Application de ce PSO au groupe "T1_ServiceAccounts"
# (exemple de groupe qui serait créé et peuplé par les équipes d'administration et qui
# contiendrait tous les comptes utilisateurs de l'AD ayant un SPN de déclaré) :
Add-ADFineGrainedPasswordPolicySubject -Identity "PSO_ServiceAccounts" -Subjects
    "T1_ServiceAccounts"
```

Listing 12 – Script PowerShell de création et d'affectation d'une stratégie de mot de passe affinée pour les comptes de service

R70 -

Réduire la portée des secrets réutilisables exposés par SPN

Dans l'alternative, il convient de limiter les conséquences d'une compromission des comptes utilisateurs qui ont un SPN déclaré dans l'AD pour des questions de compatibilité applicative. C'est-à-dire que, si compte tenu de contraintes spécifiques pesant sur le SI, aucune des recommandations R69 et R70 n'est applicable à un tel compte utilisateur, alors ce compte doit :

- avoir des droits et privilèges réduits au strict besoin opérationnel ;
- pouvoir se connecter uniquement sur un ensemble de ressources aussi restreint que possible et faisant exclusivement partie de la même zone de confiance que lui.

Attention

Il est conseillé de procéder à une revue régulière des comptes utilisateurs qui ont un SPN déclaré dans l'AD. L'exemple de script proposé par le listing 11 peut être utilisé à cet effet.

4.14 Intérêts et dangers des managed service accounts

Les *managed service accounts* ont des mots de passe dont la complexité (120 caractères) et la rotation (30 jours maximum par défaut) sont automatiquement gérées (la problématique de robustesse et de renouvellement des mots de passe est abordée en section 3.3.7). Ces *managed service accounts* peuvent être des sMSA (*standalone* MSA, pour utilisation sur un seul ordinateur) ou des gMSA (*group* MSA, pour une utilisation sur plusieurs ordinateurs). Leur fonctionnement est documenté sur le site de Microsoft [79].

L'utilisation de *managed service accounts* est une bonne pratique ; elle satisfait *de facto* aux contraintes de mots de passe formulées dans les recommandations :

- R33 (traiter les risques liés aux secrets réutilisables des tâches planifiées et des services Windows) ;
- R67 (traiter les risques inhérents à l'absence de préauthentification Kerberos) ;
- R70 (traiter les risques inhérents à l'exposition par SPN de secrets réutilisables).

Il est toutefois à noter que certains services ne supportent pas les *managed service accounts*, notamment lorsque le mot de passe du compte de service a besoin d'être renseigné dans la solution logicielle à laquelle le service est rattaché.

Attention

Les *managed service accounts* présentent le même risque de réutilisabilité de leurs secrets d'authentification qu'un compte utilisateur classique de l'AD. Il est ainsi rappelé qu'en application de la recommandation générale R29 de maîtrise de la dissémination des secrets d'authentification réutilisables, un même *managed service account* ne doit pas être utilisé de manière transverse à plusieurs zones de confiance.

Il est par ailleurs rappelé que le conteneur des *managed service accounts* de l'annuaire AD est potentiellement sensible (se référer à la recommandation R20 d'analyse des chemins de contrôle AD vers les conteneurs système et de configuration sensibles) dans la mesure où un chemin de contrôle AD vers ces derniers permet l'obtention de leurs secrets d'authentification réutilisables.

4.15 Dangers des attaques sur NTLM

L'utilisation des protocoles d'authentification NTLM apporte de nombreuses faiblesses dans un SI reposant sur AD et peut nuire au cloisonnement des zones de confiance.

R71

Interdire l'authentification NTLM des comptes du Tier 0

L'authentification NTLM doit être interdite pour les comptes du *Tier 0* en leur donnant l'appartenance au groupe de sécurité des utilisateurs protégés (*protected users*, cf. annexe B). Cette recommandation doit être étendue à tous les comptes d'administration du *Tier 1* et du *Tier 2* compatibles avec cette interdiction, mais il est habituel que certains équipements et applicatifs du *Tier 1* ou du *Tier 2* n'acceptent que les authentifications NTLM.

Toute ressource de *Tier 0* incompatible avec l'authentification Kerberos doit faire l'objet d'une évolution technique ou doit être isolée de la forêt AD (sujet traité en annexe F).

4.15.1 Dangers de NTLMv1

Tout d'abord, la première version de NTLM (NTLMv1) présente une faiblesse majeure qui permet l'obtention de condensats NTLM réutilisables par simple capture du trafic réseau entre clients et serveurs. Son utilisation est à proscrire, de même qu'est à proscrire l'utilisation des protocoles LM (*LAN manager*), prédécesseurs de NTLMv1 bien plus vulnérables encore.

R72

Durcir la configuration de NTLM sur les systèmes

Le protocole NTLM doit être exclusivement utilisé dans sa version NTLMv2, avec un chiffrement à 128 bits.

Le listing 13 indique les paramètres de stratégie de sécurité qui peuvent être appliqués en ce sens sur tous les systèmes membres de l'AD (par GPO idéalement).

```
Chemin : Configuration ordinateur\Paramètres Windows\Paramètres de sécurité\Stratégies locales\
        Options de sécurité\Sécurité Réseau

Trois paramètres à configurer :

Niveau d'authentification LAN Manager : Activé avec la valeur
"Envoyer uniquement une réponse NTLM version 2 et refuser LM et NTLM"

Sécurité de session minimale pour les clients basés sur NTLM SSP (y compris RPC sécurité) :
Activé avec "Exiger la sécurité de session NTLMv2" et "Exiger un niveau de chiffrement à 128 bits"

Sécurité de session minimale pour les serveurs basés sur NTLM SSP (y compris RPC sécurité) :
Activé avec "Exiger la sécurité de session NTLMv2" et "Exiger un niveau de chiffrement à 128 bits"
```

Listing 13 – Paramètres de stratégie de sécurité pour le durcissement de NTLM

4.15.2 Dangers de NTLMv2

Dans sa version la plus à jour (NTLMv2), NTLM souffre toujours de certaines faiblesses ; celles qui exposent les systèmes à des attaques par relai d'authentification NTLM (communément appelées « relai NTLM » ou « *NTLM relay* ») sont critiques. Ces attaques peuvent permettre le contrôle du *Tier 0* depuis des zones de moindre confiance et représentent donc un danger pour le cloisonnement d'un SI reposant sur AD. Ce danger est d'ailleurs renforcé par le constat que ces dernières années ont vu la multiplication des vulnérabilités exploitant le relai d'authentification NTLM.

En effet, cette classe d'attaque permet à un attaquant, sous certaines conditions, d'intercepter une authentification NTLMv2 (il s'agit ici d'une authentification réseau – *logon type 3* [75] – par opposition aux authentifications interactives qui sont à l'origine de la dissémination de condensats NTLM ou de secrets Kerberos en mémoire vive des systèmes) réalisée par une victime auprès d'un serveur, puis de la relayer ensuite vers un autre serveur cible. Plus précisément, c'est la réponse au défi NTLMv2 (*NTLMv2 challenge*) du serveur qui est relayée, c'est-à-dire le condensat « Net-NTLMv2 ». Le relai d'authentification NTLM peut potentiellement permettre à l'attaquant d'élever ses privilèges ou d'envoyer des commandes à exécuter à la cible de son choix sans connaître les secrets d'authentification détournés, mais en bénéficiant des droits d'accès de la victime.

Plusieurs recommandations sont à appliquer pour préserver le cloisonnement du SI face aux faiblesses de NTLMv2. Certaines consistent à restreindre l'usage de NTLM (cf. section 4.15.2.1), mais ces mesures de sécurité se heurtent généralement à des incompatibilités systèmes ou applicatives qui empêchent le bannissement complet de NTLM dans un SI. Dans ce cas, les mesures de sécurité efficaces pour se prémunir des attaques par relai d'authentification NTLM consistent à activer des protections pour les différents protocoles vers lesquels des condensats Net-NTLMv2 détournés peuvent être relayés (cf. sections 4.15.2.2 à 4.15.2.4). À noter que ces recommandations de restriction de NTLM dans le SI doivent être appliquées y compris quand l'authentification NTLM a été interdite pour les comptes sensibles (par application de la recommandation R71).

4.15.2.1 Restriction du trafic NTLM dans le SI

Les authentifications des services de l'AD entre systèmes Windows du *Tier 0* supportent nativement Kerberos et l'authentification NTLM sortante peut normalement être désactivée sur ces

systèmes. Or, ce sont les administrateurs et les serveurs [40] de *Tier 0* qui sont activement exploités par les attaquants, ces derniers tentant généralement de leurs faire établir des connexions NTLM sortantes vers un service qu'ils contrôlent et qu'ils relayeraient ensuite en bénéficiant de droits et privilèges de *Tier 0*.

R73

Bloquer le trafic NTLM sortant depuis les systèmes du Tier 0

Afin de limiter certaines attaques sur NTLM, les authentifications NTLM sortantes depuis tous les systèmes du *Tier 0* doivent être bloquées (le paramètre de stratégie de groupe indiqué par le listing 14 est à appliquer en ce sens sur tous les systèmes du *Tier 0*). Ceci aura pour effet d'empêcher de manière générique l'exploitation des vulnérabilités de type relai NTLM vis-à-vis de ces systèmes critiques.

Une phase d'audit préalable (journalisation sans aucun blocage et donc sans aucun risque de dysfonctionnement) peut être utilisée pour identifier les authentifications NTLM sortantes pendant un certain laps de temps. Cela permet de préalablement s'assurer de l'absence d'authentifications NTLM sortantes ou d'y remédier proprement avant de les bloquer pour éviter toute éventuelle indisponibilité de services. Pour activer cette journalisation, le paramètre de stratégie de groupe indiqué par le listing 15 peut être utilisé.

R74 +

Bloquer le trafic NTLM sortant depuis tous les systèmes du SI qui le permettent

Afin de limiter autant que possible les attaques sur NTLM dans le SI et en complément de la recommandation R73 appliquée seulement au *Tier 0*, il est idéal de bloquer les authentifications NTLM sortantes depuis tous les systèmes qui le permettent (le paramètre de stratégie de groupe indiqué par le listing 14 est à appliquer en ce sens sur les systèmes). L'objectif à viser est de réussir à désactiver les authentifications NTLM sortantes sur l'intégralité des systèmes du SI.

Une phase d'audit préalable (journalisation sans aucun blocage et donc sans aucun risque de dysfonctionnement) est recommandée pour identifier les authentifications NTLM sortantes pendant un certain laps de temps sur tous les systèmes du SI. Cela permet d'identifier quels sont les systèmes qui requièrent l'authentification NTLM sortante et qui, à ce titre, ne peuvent entrer dans le périmètre d'application de cette recommandation. Pour activer cette journalisation, le paramètre de stratégie de groupe indiqué par le listing 15 peut être utilisé.

```
Chemin : Configuration ordinateur\Paramètres Windows\Paramètres de sécurité\Stratégies locales\
         Options de sécurité\Sécurité Réseau : Restreindre NTLM : Trafic NTLM sortant
         vers des serveurs distants : Activé avec la valeur "Refuser tout"
```

Listing 14 – Paramètre de stratégie de sécurité pour la restriction du NTLM sortant

40. L'authentification NTLM détournée peut être celle d'un compte utilisateur, mais peut également être celle d'un compte d'ordinateur lorsque l'attaque force un ordinateur à se connecter à un autre.

```
Chemin : Configuration ordinateur\Paramètres Windows\Paramètres de sécurité\Stratégies locales\
         Options de sécurité\Sécurité Réseau : Restreindre NTLM : Trafic NTLM sortant
         vers des serveurs distants : Activé avec la valeur "Auditer tout"
```

Listing 15 – Paramètre de stratégie de sécurité pour la journalisation du NTLM sortant

Attention

L'utilisation de Kerberos et le blocage du trafic NTLM sortant depuis les ressources de *Tier 0* laisse supposer que les connexions de ces dernières vers d'autres services de l'AD se font exclusivement par FQDN et non pas par adresse IP, ce qui devrait être le cas sur le *Tier 0* à moins que de mauvaises configurations aient été réalisées. Une phase de journalisation préalable permet de les repérer. En cas de problème, la configuration du listing 14 est rapidement réversible.

Information

Tout trafic NTLM sortant bloqué (listing 14) génère un évènement 4001 dans le journal « `journaux des applications et des services/Microsoft/Windows/NTLM` ». Ces évènements doivent donc être surveillés pour détecter tout comportement anormal ou toute mauvaise configuration à corriger.

En revanche, tout trafic NTLM sortant journalisé mais non bloqué (listing 15) génère un évènement 8001 dans le journal « `journaux des applications et des services/Microsoft/Windows/NTLM` ».

Dès lors que le trafic NTLM reste autorisé sur certains systèmes, il est dans ce cas important d'activer des protections pour les différents protocoles vers lesquels des condensats Net-NTLMv2 détournés peuvent être relayés (cf. sections 4.15.2.2 à 4.15.2.4).

4.15.2.2 Protections contre les relais d'authentification NTLM vers LDAP

Les communications LDAP entre les clients et les contrôleurs de domaine AD présentent des risques, car aucun mécanisme de sécurisation des connexions LDAP n'est activé par défaut à l'installation d'un contrôleur de domaine. Les services LDAP sont donc une cible habituelle des relais d'authentifications NTLM.

R75

Protéger les services LDAP du Tier 0 contre les relais NTLM

Les communications LDAP avec les contrôleurs de domaine AD doivent être sécurisées de manière à empêcher le relai de condensat « Net-NTLMv2 » (c'est-à-dire les attaques par relai d'authentification NTLM) vers ces services.

Il est pour cela recommandé que les contrôleurs de domaine AD exigent la signature LDAP et exigent également la liaison de canal LDAP (*LDAP channel binding*). Ces deux mesures de sécurité peuvent être mises en œuvre par une GPO appliquée aux contrôleurs de domaine ou à l'aide de clés de registre sur chaque contrôleur de domaine, tel que détaillé par l'article [74] du support Microsoft.

Information

Les deux mesures de sécurité de la recommandation R75 sont couvertes par l'application des *security baselines* de Microsoft qui fait l'objet de la recommandation générale R18.

Attention

La signature et la liaison de canal LDAP peuvent potentiellement empêcher des clients (systèmes et applications) non compatibles d'accéder aux services LDAP des contrôleurs de domaine. Une phase d'audit est donc conseillée pour s'assurer de l'absence préalable d'incompatibilité. Ces aspects sont également détaillés par l'article [74] du support Microsoft.

4.15.2.3 Protections contre les relais d'authentification NTLM vers SMB

Bien que la signature SMB [41] soit, par défaut, exigée côté serveur par les contrôleurs de domaine, ce n'est en revanche pas le cas des systèmes membres de l'AD. Par défaut, les partages SMB des contrôleurs de domaine sont donc protégés et ne peuvent pas être une cible des relais d'authentifications NTLM. En revanche, il est tout à fait possible qu'il existe des partages SMB sur d'autres ressources du *Tier 0* et par le biais desquels un attaquant pourrait éventuellement élever ses privilèges.

R76

Protéger les services SMB du Tier 0 contre les relais NTLM

Les ressources du *Tier 0* doivent toujours exiger la signature SMB. La mise en œuvre de cette mesure de sécurité est détaillée par l'article [100] de Microsoft.

En complément, les ressources du *Tier 0* doivent accepter la validation du nom de la cible de serveur SPN (*Server SPN target name validation*) lorsqu'elle est fournie par le client. La mise en œuvre de cette mesure de sécurité est détaillée par l'article [103] de Microsoft.

Information

La signature SMB est une mesure de sécurité couverte par l'application des *security baselines* de Microsoft qui fait l'objet de la recommandation générale R18.

Il est à noter également que le protocole SMBv1 est déprécié (au profit de SMBv2 et SMBv3), car présentant d'importants risques de sécurité. SMBv1 est *de facto* prohibé et il ne permet pas d'exiger la signature SMB. Il n'est, par défaut, plus installé sur les systèmes d'exploitation Microsoft depuis les versions 1709 de Windows 10 et Windows Serveur 2016 (cf. article [101] de Microsoft).

Enfin, l'utilisation de SMBv3 peut être forcée en requérant le chiffrement Kerberos ou en limitant ses suites cryptographiques (paramètre de stratégie de sécurité « `Configuration ordinateur\Modèles d'administration\Network\Lanman Server\Cipher suite order` »).

41. SMB est le protocole utilisé pour le partage de fichiers et d'imprimantes sous Windows.

4.15.2.4 Protections contre les relais d'authentification NTLM vers HTTP

Il arrive que le *Tier 0* se compose de ressources exécutant des services Web. Par défaut, certains utilisent le protocole HTTP sans chiffrement TLS et acceptent l'authentification réseau NTLM. C'est, par exemple, le cas des rôles *Active Directory Certificat Services* (ADCS) qui proposent des services optionnels d'enrôlement Web de certificats (*Certificate Authority Web Enrollment* et *Certificate Enrollment Web Service*). Les services Web en HTTP non sécurisés peuvent être des cibles des relais d'authentifications NTLM.

R77

Protéger les services Web du Tier 0 contre les relais NTLM

Tout service Web exposé par des ressources du *Tier 0* doit être protégé contre les attaques par relai d'authentification NTLM. Pour cela, l'une ou l'autre des mesures de sécurité suivantes peuvent, entre autres, être appliquées :

- le service Web exige un chiffrement TLS ;
- le service Web refuse l'authentification NTLM (en autorisant uniquement les authentifications Kerberos, par exemple) ;
- le serveur n'est techniquement joignable que depuis les ressources du *Tier 0* (à l'aide de règles de pare-feu local et d'équipements de filtrage périmétriques) ;
- le service Web, s'il est porté par le rôle IIS (*Internet Information Services*), met en œuvre le mécanisme d'« *Extended Protection for Authentication* » (cf. article [68] de Microsoft).

5
Choix d'architecture d'administration et problématiques de mutualisation

Le guide ADMIN [16] donne des recommandations d'ordre générique pour l'administration sécurisée des SI et aborde notamment les problématiques de mutualisation des postes d'administration. C'est également le cas du guide de recommandations pour la protection des systèmes d'information essentiels [14], qui s'appuie sur le guide ADMIN [16]. Transposer ces concepts et recommandations pour les appliquer à un SI reposant sur AD requiert un travail d'adaptation du fait des spécificités que présente l'administration d'un SI et d'un annuaire cloisonnés en *Tiers*. Ce travail d'adaptation est l'objet du présent chapitre.

Les questions d'architecture et de mutualisation se posent à différents niveaux. Administrer des zones de confiance différentes depuis un même poste d'administration est un exemple de mutualisation tentante d'un point de vue pratique ou budgétaire. C'est également le cas de l'administration de plusieurs SI depuis un même SI d'administration pour limiter la multiplication des postes d'administration. Différentes recommandations formulées dans les chapitres précédents expriment des contraintes de cloisonnement qui fixent *de facto* des conditions à la mutualisation. C'est notamment le cas des contraintes liées à la dissémination des secrets d'authentification réutilisables et donc aux méthodes d'administration qui peuvent être utilisées entre zones de confiance. Les politiques de sécurité appliquées aux différentes zones doivent nécessairement être adaptées aux niveaux de sensibilité et aux besoins de sécurité propres à chaque zone. Ces adaptations se traduisent par différents degrés de mutualisation pour chaque zone, et différents niveaux de tolérance dans les méthodes d'administration autorisées.

Le sujet de la mutualisation peut difficilement être traité par l'application mécanique de règles d'aide à la décision. Il doit au contraire être traité par une appréciation méthodique du risque vis-à-vis d'un ensemble de facteurs propres au contexte de chaque organisation. Certaines organisations sont la cible d'attaquants disposant de moyens très importants et sont dès lors exposées à des menaces particulièrement sophistiquées. Ce haut niveau de menace est un facteur qui réduit la latitude de mutualisation qu'une organisation peut avoir. D'autres organisations peuvent présenter des besoins de sécurité plus standards, mais opérer des SI composés de ressources obsolètes difficiles à faire évoluer et dont l'administration expose les postes d'administration à des attaques [42]. Une telle situation est également de nature à réduire le niveau acceptable de mutualisation.

Il reste néanmoins possible de dégager quelques principes généraux permettant d'orienter les organisations dans leurs choix d'architecture et de mutualisation des moyens.

42. Par exemple, l'utilisation d'une ancienne version d'un navigateur ou d'un ancien environnement d'exécution par des postes d'administration les exposent à des attaques.

Ce chapitre traite dans un premier temps de la surface d'attaque des clients de connexion distante, à prendre en compte en complément des différents risques abordés dans les chapitres précédents.

Il traite ensuite des architectures des postes d'administration. Il précise, à cette occasion, les modalités de leur mutualisation pour l'administration de différents *Tiers* ou de plusieurs forêts AD. Comme précisé antérieurement, les problématiques de sécurité ayant trait à l'informatique en nuage sont hors périmètre de la première version de ce guide. L'administration des annuaires Microsoft Entra ID (ex. Azure Active Directory) n'est donc pas abordée.

Enfin, ce chapitre apporte quelques éléments de contexte à certaines recommandations du guide ADMIN [16] qui ne sont pas directement applicables à des SI reposant sur un annuaire AD.

5.1 Surface d'attaque des clients de connexion distante

Il est important d'examiner la question de la surface d'attaque des clients logiciels de connexion distante (clients RDP, navigateurs Web, clients SSH, etc.), que ces derniers soient utilisés pour des accès administrateur ou pour des accès utilisateur.

Certains clients de connexion distante, à défaut de disséminer des secrets d'authentification réutilisables par des attaquants, peuvent néanmoins présenter des vulnérabilités logicielles côté client. Ces vulnérabilités peuvent être exploitées par une ressource distante compromise. La dissémination de secrets d'authentification réutilisables n'est donc pas le seul critère à retenir pour déterminer si une méthode de connexion distante peut être tolérée d'une zone de confiance à l'autre, et surtout depuis le *Tier 0* vers le *Tier 1* ou depuis le *Tier 0* vers le *Tier 2*. Le risque de compromission par l'exploitation d'une vulnérabilité du client de connexion distante est également un critère à prendre en considération.

Exemple

L'historique des vulnérabilités des clients de déport d'affichage révèle[43] que ces clients logiciels peuvent présenter des vulnérabilités exploitables depuis les systèmes distants dont l'affichage est déporté. Ces vulnérabilités peuvent permettre une exécution de code arbitraire sur les postes clients. Plus les périphériques partagés par RDP sont nombreux et complexes (périphériques USB, accélération graphique matérielle, etc.), plus le client RDP s'expose à des vulnérabilités exploitables.

Il est à noter par ailleurs que les clients RDP divulguent en permanence[44] le presse-papier du poste client auprès du système distant, dès lors que le partage du presse-papier est activé (ce qui est le cas par défaut pour les connexions RDP établies par le client natif). Par ce biais, des informations sensibles (des mots de passe de comptes d'administration notamment) peuvent être divulguées à des attaquants sur des systèmes distants compromis.

L'utilisation de clients de déport d'affichage pour se connecter à des ressources de moindre confiance fait donc courir des risques de sécurité aux postes d'administration. Quand ces connexions sont de surcroît établies entre zones de confiance différentes, elles peuvent nuire au cloisonnement de ces dernières.

Exemple

Accéder à distance à des ressources informatiques au moyen d'un navigateur Web est une pratique très répandue, aussi bien pour les utilisateurs d'un SI que pour ses administrateurs. Typiquement, de nombreuses solutions logicielles du marché s'administrent en utilisant des interfaces Web. Pour autant, les navigateurs sont des logiciels qui présentent régulièrement des vulnérabilités critiques. Ces vulnérabilités peuvent être exploitées par un serveur Web compromis pour exécuter du code arbitraire sur les postes clients.

L'utilisation de navigateurs Web pour se connecter à des ressources de moindre confiance fait donc courir des risques de sécurité aux postes d'administration. Ceci est d'autant plus vrai lorsque des contraintes techniques imposent d'utiliser d'anciennes versions de navigateurs Web ou de greffons. Quand ces connexions sont de surcroît établies entre zones de confiance différentes, elles peuvent nuire au cloisonnement de ces dernières.

Ces exemples montrent que la surface d'attaque des clients de connexion distante peut non seulement nuire à la sécurité des postes d'administration, mais peut également nuire au bon cloisonnement des *Tiers* si elle créé des chemins d'attaque d'un *Tier* vers un autre. En complément des contraintes de dissémination de secrets d'authentification réutilisables (traitées en section 3.3 et en chapitre 4), la surface d'attaque des clients de connexion distante est une contrainte supplémentaire qui pèse sur la mutualisation des postes d'administration et qui justifie d'en encadrer l'usage.

R78

Encadrer et restreindre l'utilisation des clients de connexion distante

Les clients logiciels de connexion distante – qu'ils soient utilisés pour des accès administrateur ou pour des accès utilisateur – présentent des surfaces d'attaque variables. Lorsqu'ils sont utilisés depuis des postes d'administration ou pour se connecter à des ressources de zones de moindre confiance, ils doivent avoir fait l'objet d'une analyse de sécurité préalable. Cette analyse permet d'évaluer puis d'accepter ou de refuser le risque associé à leur utilisation en fonction des besoins de sécurité de chaque zone de confiance de l'organisation.

Les politiques de sécurité qui en découlent pour chaque zone de confiance doivent définir quels sont les clients de connexion distante autorisés ou interdits depuis les postes d'administration et, de manière encore plus stricte, quels sont les clients de connexion distante autorisés ou interdits à destination de zones de moindre confiance.

En complément de mesures organisationnelles, des mesures de sécurité techniques doivent être mises en œuvre pour appliquer cette restriction. Elles peuvent notamment consister en :

43. Par exemple, les récentes vulnérabilités CVE-2022-21990 [36] et CVE-2022-23285 [37] du client RDP natif permettent une exécution de code à distance sur le client depuis un serveur distant compromis.
44. Le contenu du presse-papier est exposé pendant toute la durée d'une session RDP active, qu'il ait été collé ou non dans l'environnement distant.

- des stratégies de contrôle d'application (par Applocker [52] ou WDAC [106], par exemple). Idéalement, ces stratégies devraient uniquement permettre l'exécution des logiciels autorisés (principe de liste blanche) ;
- un filtrage réseau à l'aide des pare-feu logiciels locaux [45] et des pare-feu périmétriques, idéalement complété par des mécanismes de segmentation réseau. Seules les connexions réseau, entrantes et sortantes, nécessaires au fonctionnement des clients logiciels devraient être autorisées (en complément des connexions qui sont nécessaires pour répondre aux cas d'usage des différents systèmes dans le SI).

R79

Durcir les clients de connexion distante dont les politiques de sécurité autorisent l'usage

Les clients de connexion distante dont les politiques de sécurité autorisent l'usage doivent être durcis. Ces durcissements ont pour objectif de limiter la surface d'attaque des clients de connexion distante, en bloquant notamment leurs fonctionnalités inutiles.

Exemple

La recommandation R79 s'applique notamment au cas du déport d'affichage à l'aide du client RDP natif, qui devrait être configuré (par GPO, par exemple) de manière à permettre uniquement :

- le déport d'affichage sans accélération graphique matérielle ;
- le partage de carte à puce, dans le seul cas où l'authentification par carte à puce est requise sur le système distant.

Toute autre fonctionnalité autorisée du client RDP doit faire l'objet d'une analyse de risques au regard de la sensibilité de la zone de confiance depuis laquelle la connexion RDP est initiée. C'est notamment le cas du partage du presse-papier, si certaines pratiques d'administration en vigueur le requièrent malgré les risques de divulgation mentionnés en section 5.1 ; Il est à noter qu'un client RDP continue d'avoir une surface d'attaque exploitable, y compris lorsqu'il est utilisé avec le minimum de fonctionnalités.

5.2 Mutualisation des postes d'administration

Le chapitre 4 du guide ADMIN [16] décrit « des architectures de poste d'administration permettant de répondre à la dualité des besoins des administrateurs : réalisation des actions d'administration depuis un environnement sécurisé d'une part et accès à un SI bureautique en tant qu'utilisateur d'autre part ».

Dans un SI reposant sur un annuaire AD et qui est cloisonné par la mise en œuvre d'un modèle de gestion des accès privilégiés, cette dualité des besoins des administrateurs d'un *Tier* donné peut en

45. Dans ce cas, l'avantage d'un pare-feu logiciel local (par exemple, le pare-feu nativement intégré à Windows) est qu'il permet la création de règles de filtrage qui s'appliquent uniquement à des services Windows ou à des exécutables spécifiques, ce qu'un équipement de filtrage périmétrique ne peut pas faire.

réalité être précisée de la manière suivante : réalisation des actions d'administration des ressources appartenant à ce même *Tier* d'une part et accès à des environnements de zones de moindre sensibilité d'autre part (qu'il s'agisse, par exemple, d'accéder à des ressources d'administration intermédiaires de zones de moindre sensibilité ou d'accéder à des ressources de bureautique en tant que utilisateur).

Pour répondre à la dualité des besoins d'administration, trois solutions d'architecture envisageables sont présentées par le guide ADMIN [16]. Dans le cas d'un SI cloisonné par la mise en œuvre d'un modèle de gestion des accès privilégiés, ces trois solutions peuvent être déclinées de la manière suivante, par niveau de sécurité décroissant au regard des objectifs de sécurité fixés :

- un poste d'administration dédié (**architecture recommandée**) ;
- un poste d'administration multiniveaux reposant sur des mécanismes évalués comme étant de confiance au niveau système (**première architecture alternative**) ;
- un poste d'administration avec accès distant à des environnements (physiques ou virtuels) de moindre confiance (**deuxième architecture alternative**), que ces environnements de zones de moindre confiance soient des environnements de bureautique ou qu'ils soient d'autres environnements d'administration d'un moindre niveau de confiance.

Les deux dernières architectures sont jugées d'un moindre niveau de sécurité dans la mesure où les clients d'accès distant ont une certaine surface d'attaque (cf. section 5.1) et que les mécanismes de cloisonnement des systèmes multiniveaux peuvent présenter des vulnérabilités. Elles présentent ainsi des risques de sécurité que ne présentent pas les postes d'administration dédiés.

Si ces deux architectures alternatives restent néanmoins envisageables dans le contexte de l'administration d'un SI reposant sur un annuaire AD, leur mise en œuvre doit prendre en compte les besoins et objectifs de sécurité de l'organisation et des différentes zones de confiance. La présente section a donc pour objectif de guider les choix de mutualisation en fonction des besoins et objectifs de sécurité, mais également en fonction des risques qui pèsent sur les postes d'administration, sur les systèmes administrés et sur les moyens d'accès au SI.

5.2.1 Postes d'administration dédiés

La haute sensibilité du *Tier 0* justifie de dédier des postes à son administration, sans que ces derniers n'aient d'interactions possibles avec des ressources de zones de moindre confiance (*Tier 1* ou *Tier 2*).

R80

Administrer le Tier 0 depuis des postes d'administration physiquement dédiés

L'administration du *Tier 0* doit être réalisée depuis des postes d'administration du *Tier 0* qui sont physiquement dédiés, c'est-à-dire sans mutualisation d'aucune sorte (ni par des systèmes multiniveaux, ni par accès distant à des environnements physiques ou virtuels de moindre confiance).

Pour cela et dans une démarche de défense en profondeur, il est notamment recommandé l'application cumulative des mesures de sécurité suivantes :

- mettre en œuvre un silo d'authentification du *Tier 0* (leur mise en œuvre est détaillée en annexe C) ou des stratégies d'authentification équivalentes ;
- configurer les paramètres de sécurité Windows permettant de restreindre les ouvertures de session des comptes de *Tier 0* sur les ressources de *Tier 1* et de *Tier 2* (l'application de ces paramètres de sécurité est détaillée en annexe D) ;
- autoriser les flux réseau sortants des postes d'administration du *Tier 0* uniquement vers les ressources du *Tier 0* et bloquer tous les flux réseau entrants vers les postes d'administration du *Tier 0* (cf. section 3.7.2 sur la segmentation et le filtrage réseau).

Cette recommandation R80 est illustrée par la figure 10.

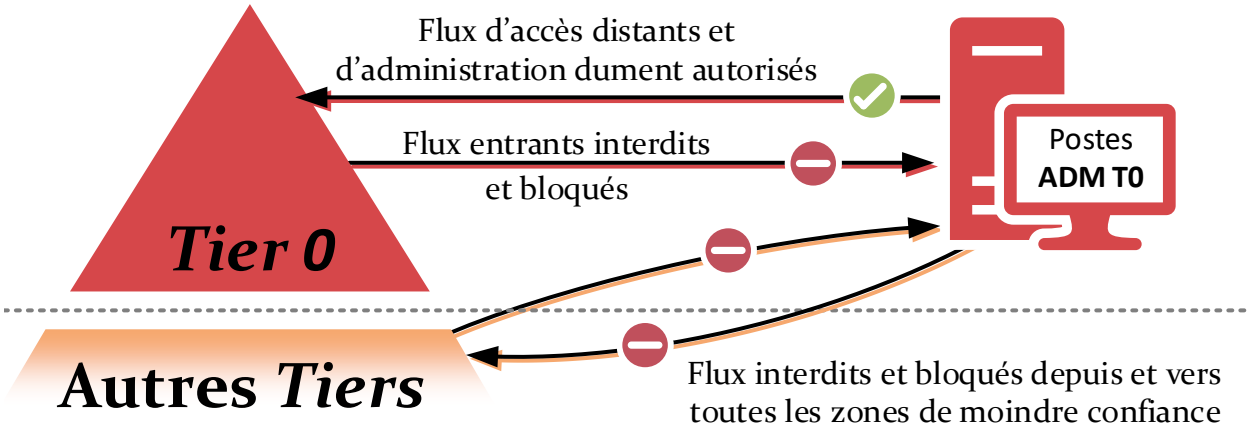

FIGURE 10 – Illustration de la recommandation R80 : architecture de postes d'administration physiquement dédiés à l'administration du *Tier 0* et n'ayant aucun accès à des ressources de zones de moindre confiance.

Information

L'application du cloisonnement du SI par le processus d'amélioration continue détaillé en section 2.3 permet d'atteindre rapidement un stade où les actions d'administration qui relèvent réellement du *Tier 0* devraient être peu fréquentes et où la population d'administrateurs du *Tier 0* devrait être réduite. De ce fait, les postes d'administration du *Tier 0* devraient être en nombre limité. Ils ne sont d'ailleurs pas nécessairement nominatifs, et peuvent être partagés entre administrateurs du *Tier 0*. Cette rareté des actions d'administration du *Tier 0* facilite l'application de la recommandation R80 d'administration du *Tier 0* depuis des postes d'administration qui lui sont physiquement dédiés.

Satisfaire à la recommandation R80 peut parfois s'avérer difficile. C'est notamment le cas en phase transitoire lorsque la démarche de cloisonnement du SI en *Tiers* vient de débuter. Cela l'est d'autant plus quand les pratiques d'administration de l'entité s'écartent des bonnes pratiques. Dans un tel contexte, l'obtention d'un périmètre trop large du *Tier 0* peut impliquer de nombreuses et fréquentes actions d'administration du *Tier 0* et peut par conséquent nécessiter un nombre important de postes dédiés à son administration. Il peut dans ce cas s'avérer contraignant de déployer

des postes physiquement dédiés à l'administration du *Tier 0*. Pour cette raison et en alternative à la recommandation R80, une organisation peut envisager de mutualiser les postes d'administration du *Tier 0*.

R80 -

Encadrer la mutualisation des postes d'administration du Tier 0

En alternative à la recommandation R80, il peut être envisagé de mutualiser les postes d'administration du *Tier 0*. Cette mutualisation doit prendre la forme d'une des deux architectures alternatives introduites en section 5.2. Elle doit scrupuleusement respecter les modalités de mise en œuvre décrites dans le chapitre 4 du guide ADMIN [16]. Cette autorisation de mutualisation doit être transitoire, le temps pour l'organisation de progresser dans l'amélioration continue du cloisonnement du SI en *Tiers*.

Cette recommandation alternative R80- est illustrée par la figure 9 en section 4.9.

R80 +

Étendre le principe de non mutualisation des postes d'administration

Une organisation qui vise un niveau de sécurité renforcé peut étendre le principe de non mutualisation des postes d'administration (de la recommandation R80) en dédiant physiquement des postes à l'administration des autres zones de confiance qu'elle juge sensibles pour son activité. Ces zones de confiance peuvent concerner, par exemple, l'ensemble ou une partie des ressources métier du *Tier 1* ou des moyens d'accès du *Tier 2*.

Attention

Il est à noter que si une organisation déploie des ressources d'administration intermédiaires dans le *Tier 0* d'une forêt AD, ces dernières doivent également respecter les recommandations du présent document applicables aux postes d'administration du *Tier 0*.

5.2.2 Mutualisation par des postes d'administration multiniveaux

La première architecture alternative consiste en la mutualisation par l'utilisation d'un poste multiniveaux. Cette architecture implique la mise en œuvre de mécanismes de cloisonnement systèmes avancés permettant l'exécution, sur un même socle physique, d'environnements catégorisés dans des zones de confiance différentes. Se pose donc la question de la catégorisation de ces socles physiques.

R81

Catégoriser les postes multiniveaux dans les Tiers adéquats

En cas de mise en œuvre de la première architecture alternative, tout poste multiniveaux (par virtualisation, conteneurisation ou toute autre technologie de cloisonnement système évaluée de confiance) doit être catégorisé dans le *Tier* correspondant à l'environnement le plus sensible qu'il exécute.

Exemple

Un poste multiniveaux hébergeant un niveau système dédié à l'administration du *Tier 1* et un niveau système dédié à la bureautique doit être considéré comme étant un poste d'administration de *Tier 1* du point de vue de sa sensibilité et des politiques de sécurité qui lui sont appliquées. En conséquence, les mesures de sécurité logiques, organisationnelles et physiques appliquées à ce poste sont celles applicables au *Tier 1*.

Le présent guide n'a pas vocation à préciser les technologies qui peuvent être utilisées pour la conception de postes multiniveaux. Les organisations sont de manière générale incitées à n'utiliser que des solutions de cloisonnement évaluées de confiance. Aucune solution de système multiniveaux n'a toutefois obtenu de visa de sécurité délivré par l'ANSSI à la date de publication de ce guide.

Il est enfin utile de préciser que les clients logiciels permettant le déport d'affichage local des conteneurs ou des machines virtuelles (VM) hébergées par un poste multiniveaux, bien que parfois intégrés de manière transparente à la solution de virtualisation ou de conteneurisation, sont assujettis aux mêmes contraintes et recommandations que les clients de connexion distante évoqués en section 5.1. Ces clients sont, en effet, susceptibles de présenter des chemins d'attaque entre le socle système principal du poste multiniveaux et les conteneurs ou VM qu'il héberge.

Exemple

Dans la solution de virtualisation Microsoft Hyper-V intégrée aux systèmes d'exploitation Windows, le déport d'affichage local d'une VM qu'il héberge se fait en réalité par RDP (et de manière transparente) entre l'hyperviseur et la VM.

Lorsque le déport d'affichage local d'une VM Hyper-V se fait en *enhanced session mode*, il se fait en réalité en RDP avec un large spectre de fonctionnalités et donc une large surface d'attaque. Ce mode peut dès lors fortement affaiblir le cloisonnement entre l'hyperviseur et les VM qu'il héberge.

À l'inverse, sans cet *enhanced session mode* les fonctionnalités de RDP se limitent au strict minimum : clavier, souris et déport d'affichage sans aucune accélération matérielle. La surface d'attaque qui en résulte est donc beaucoup plus limitée et rend plus robuste le cloisonnement entre l'hyperviseur et les VM qu'il héberge. Il est toutefois à noter que l'activation ou la désactivation du *enhanced session mode* du déport d'affichage local des VM Hyper-V ne peut pas être forcé par stratégie de sécurité locale. Son utilisation repose donc sur le bon vouloir de l'utilisateur.

5.2.3 Mutualisation par connexion distante à des environnements de moindre confiance

La deuxième architecture alternative consiste en la mutualisation par l'accès distant à des environnements de moindre confiance. Ces derniers peuvent être des moyens d'accès au SI (des environnements de bureautique, par exemple), mais peuvent également être des ressources d'administration intermédiaires d'un moindre niveau de confiance.

R82

Restreindre l'accès aux ressources de zones de moindre confiance depuis le Tier 0

En cas de mise en œuvre de la deuxième architecture alternative, seules les méthodes de connexion distante suivantes doivent être autorisées vers des ressources de zones de moindre confiance :

- RPC, c'est-à-dire par l'utilisation des MMC généralement ;
- PowerShell WinRM avec protocole d'authentification par défaut, c'est-à-dire par authentification réseau Kerberos ou NTLM et donc sans rebond possible et sans dissémination de secrets d'authentification réutilisables ;
- déport d'affichage RDP natif, avec l'option *RestrictedAdmin* ou à l'aide de comptes de *Tier 1* ou de *Tier 2* en fonction de l'environnement de moindre confiance de destination.

Ces méthodes de connexion distante sont les plus usuelles et couvrent la grande majorité des besoins d'administration. Toute autre méthode de connexion distante dérogatoire depuis le *Tier 0* ne doit être autorisée qu'après analyse et traitement du risque de dissémination de secrets qu'elle présente (comme dans le tableau 2 de la section 4.4), ainsi de la surface d'attaque du client de connexion distante utilisé (problématique abordée en section 5.1).

Enfin, dans une logique de défense en profondeur, ces restrictions doivent être mises en œuvre à l'aide de mesures techniques aussi cumulatives que possible : filtrage des flux réseau par des pare-feu logiciels locaux et par des pare-feu périmétriques, stratégies de restriction logicielle (AppLocker ou WDAC, par exemple), durcissement de la configuration des clients de connexion distante, etc.

Le cas de l'accès distant à des environnements de zones de moindre confiance par déport d'affichage implique des ouvertures de sessions interactives sur ces derniers. Le compte de connexion utilisé à cet effet voit donc ses secrets d'authentification réutilisables disséminés (cf. sections 4.4 et 4.8 dédiées aux risques de dissémination que font peser les différentes méthodes de connexion et d'administration). Ce constat amène à formuler la recommandation R83.

R83

Restreindre les comptes de connexion autorisés pour le déport d'affichage

En cas de mise en œuvre de la deuxième architecture alternative, le compte utilisateur saisi pour l'ouverture de session interactive distante par déport d'affichage à un environnement d'une zone de moindre confiance doit être un compte de la zone de confiance d'appartenance de cet environnement de moindre confiance. Tout compte d'un plus haut niveau de confiance doit s'y voir refuser l'ouverture de session interactive distante et ce refus doit intervenir sans qu'il y ait dissémination de ses secrets d'authentification réutilisables [46] sur le système distant.

46. Les stratégies de sécurité pour la restriction d'ouverture de session peuvent, par exemple, disséminer des condensats NTLM même en cas d'interdiction de l'authentification interactive (se reporter aux explications fournies en annexe D). Elles ne sont donc pas suffisantes pour appliquer la recommandation R83, sauf si l'authentification NTLM est interdite sur ces systèmes ou pour les comptes utilisateurs concernés.

Exemple

Depuis un poste d'administration du *Tier 1*, un administrateur ne doit pas pouvoir ouvrir une session interactive distante par RDP sur un poste bureautique (*Tier 2*) avec un compte de *Tier 1*, mais doit utiliser un compte nominatif de *Tier 2*. Sans cette précaution, la connexion RDP disséminerait des secrets d'authentification réutilisables du *Tier 1* sur le poste de *Tier 2* (cf. chapitre 4 relatif à NTLM et Kerberos).

5.3 Mutualisation de l'administration de plusieurs forêts AD

Il est possible de considérer un SI comme une zone de confiance à part entière. Des organisations peuvent en effet opérer plusieurs SI distincts : SI industriels, SI de bureautique ou SI de recherche et développement, par exemple. Une organisation peut également avoir la responsabilité de différents SI qui correspondent à des acquisitions d'entreprises, des filiales indépendantes, différents sites géographiques, des contraintes réglementaires particulières, etc. Les besoins de sécurité applicables à ces SI peuvent nécessiter des frontières de sécurité strictes, ce qui implique de les cloisonner les uns des autres.

Lorsqu'une organisation opère plusieurs SI, il est courant que ceux-ci soient interconnectés à différents degrés. Le travail d'analyse des chemins d'attaque (qui a été détaillé dans les chapitres 3 et 4) se trouve alors applicable à l'échelle de l'organisation en considérant les interactions des différents SI entre eux.

Dans un tel contexte, il est courant que les organisations souhaitent mutualiser leurs postes d'administration, permettant à ces derniers d'administrer différents SI sans pour autant multiplier les postes d'administration. Ce besoin de mutualisation est encore plus important quand des postes d'administration sont dédiés par *Tier* dans chacun de ces SI distincts. Une telle mutualisation se traduit par le regroupement des postes d'administration au sein d'un ou de plusieurs SI d'administration.

Deux architectures de SI d'administration sont à distinguer.

- **Cas 1** : les forêts AD administrées n'ont pas de relations d'approbation avec un éventuel annuaire AD du SI d'administration.
- **Cas 2** : les postes d'administration sont membres[47] d'une forêt d'administration qui leur est dédiée et cette dernière a des relations d'approbation avec les forêts administrées.

Dans la suite de ce document, l'expression « SI d'administration » se rapporte au **cas 1** tandis que l'expression « forêt d'administration » se rapporte au **cas 2**. Ces deux types d'architecture présentent des avantages et des inconvénients qui doivent être pris en compte pour parvenir à un cloisonnement pertinent des différents SI de l'organisation. Leurs spécificités sont abordées dans les sections 5.3.1 et 5.3.2.

47. Les notions d'appartenance ou d'intégration à une forêt sont utilisées pour désigner le fait qu'un ordinateur est joint à un domaine AD de cette forêt.

5.3.1 SI d'administration

Le cas des SI d'administration est le cas général largement développé dans le guide ADMIN [16] de l'ANSSI. Il doit donc en respecter les recommandations, qui n'ont pas lieu d'être particulièrement complétées dans le présent document.

Dans un SI d'administration, les postes peuvent être des postes sous Windows mais peuvent également être des postes sous Linux ou des terminaux légers, par exemple.

Attention

Quand des postes du SI d'administration sont sous Windows, ces derniers peuvent éventuellement être gérés de manière centralisée dans un annuaire AD dont ils sont membres. Dans ce cas, cet annuaire AD est une forêt dédiée au SI d'administration et qui n'a aucune relation d'approbation avec des forêts administrées. Il ne s'agit donc pas d'une forêt d'administration, dont le principe est développé en section 5.3.2.

Dans un SI d'administration, les postes du SI d'administration devraient se connecter à des ressources d'administration intermédiaires dédiées à chacun des SI administrés. Pour l'administration d'environnements Windows, la connexion distante à ces ressources intermédiaires se fait le plus souvent par déport d'affichage. Tout comme un poste d'administration du *Tier 0* peut, dans certaines conditions, administrer des environnements de moindre confiance par accès distant (cf. section 5.2.3), les postes du SI d'administration peuvent être mutualisés pour l'administration de zones de confiance hétérogènes. Dans ce cas, ils se connectent à différentes ressources d'administration intermédiaires dédiées à chacune des zones de confiance qu'ils administrent (cf. chapitre 13 du guide ADMIN [16]). Par ailleurs, il est important de préciser que les recommandations relatives à la surface d'attaque des clients de connexion distante (section 5.1) et les recommandations propres aux architectures alternatives de postes d'administration (sections 5.2.2 et 5.2.3) sont applicables aux connexions distantes réalisées depuis un SI d'administration.

À noter que quand ces ressources d'administration intermédiaires ne sont pas membres des forêts administrées, elles doivent dans ce cas être positionnées dans le SI d'administration (cas recommandé par le chapitre 13 du guide ADMIN [16]). Néanmoins certains besoins peuvent nécessiter que des ressources d'administration intermédiaires soient intégrées aux forêts administrées. C'est notamment le cas lorsque des méthodes d'administration utilisées reposent sur une authentification NTLM ou Kerberos (p. ex. pour l'administration distante à l'aide des composants MMC des RSAT). L'intégration à un domaine AD implique de nombreux flux réseau bidirectionnels entre les ressources d'administration intermédiaires et les contrôleurs de domaine qui les gèrent dans une forêt administrée. Comme ces flux sont incompatibles avec le besoin de filtrage réseau strict entre le SI d'administration et les SI administrés (recommandations de filtrage R16 et R19 du guide ADMIN [16]), les ressources intermédiaires intégrées à une forêt administrée doivent dans ce cas être positionnées hors du SI d'administration. Sans cette précaution et en cas de compromission d'une forêt AD administrée, un attaquant disposerait d'une porte dérobée dans le SI d'administration. Une telle porte dérobée rapprocherait l'attaquant d'autres ressources d'administration et d'autres ressources administrées.

R84

Respecter les règles de positionnement des ressources d'administration intermédiaires

Il est préférable que les ressources d'administration intermédiaires ne soient pas intégrées aux forêts administrées. Elles sont dans ce cas positionnées dans le SI d'administration (cf. chapitre 13 du guide ADMIN [16]).

En revanche, une ressource d'administration intermédiaire doit être positionnée hors du SI d'administration dès lors qu'elle est intégrée à une forêt administrée (ce qui peut être nécessaire pour certaines méthodes ou actions d'administration).

5.3.2 Forêt d'administration

Une forêt d'administration est une forêt utilisée pour l'administration mutualisée des *Tier 0* de plusieurs forêts. La forêt d'administration contient uniquement les ressources nécessaires à l'administration et celles nécessaires à son propre maintien en conditions opérationnelles (MCO) et de sécurité (MCS).

5.3.2.1 Principe d'une forêt d'administration

Le principe d'une forêt d'administration est que les différentes forêts AD administrées font confiance – par relation d'approbation AD – à une unique forêt AD dédiée à leur administration. Le niveau de confiance d'une forêt d'administration est donc supérieur à celui des forêts administrées. Elle est conçue et opérée de manière à préserver le cloisonnement des forêts administrées. Comme l'administration à l'état de l'art du *Tier 0* repose uniquement sur l'utilisation d'un nombre restreint de méthodes d'administration sécurisées (les MMC des RSAT, WinRM et éventuellement RDP), une forêt d'administration présente une surface d'attaque minimale qui permet d'assurer son cloisonnement et celui des forêts administrées. Le rapport de confiance entre la forêt d'administration et les forêts administrées s'apparente donc au rapport de confiance qui existe entre le *Tier 0* et le *Tier 1*. Les principes et recommandations de ce guide peuvent dès lors être appliqués au cloisonnement d'une forêt d'administration vis-à-vis des forêts qu'elle administre.

Une « forêt d'administration » peut être implémentée de différentes manières. Il n'existe pas de spécifications détaillées d'implémentation et de mise en œuvre d'une telle forêt. Néanmoins et pour éviter toute confusion, il est important d'expliciter deux termes couramment rencontrés lorsqu'il est question de forêt d'administration.

- L'ESAE (*Enhanced Security Administrative Environment*) [58] était une offre de service de Microsoft pour la mise en œuvre d'une forêt d'administration dédiée à la gestion exclusive des *Tier 0* de plusieurs forêts. Elle reposait sur un modèle construit autour de spécifications d'architecture et de configuration énoncées par Microsoft. Cette offre de service mettait en œuvre un certain nombre de solutions logicielles grand public de l'éditeur (*Microsoft System Center Operations Manager*, *Microsoft Deployment Toolkit*, *Microsoft Advanced Threat Analytics*, etc.), ces dernières étant toutes déployées par provisionnement automatisé. Il s'agissait *in fine* d'une forêt d'administration dont la complexité et le cout d'acquisition la destinaient *a priori* à des clients grands comptes. L'offre n'est plus proposée par Microsoft, mais reste déployée dans certaines organisations.

- Une *Red forest* désigne généralement une forêt d'administration minimale et dédiée à la gestion des *Tier 0* de plusieurs forêts. Bien que les termes *Red forest* et ESAE soient parfois considérés comme équivalents, la *Red forest* est en réalité l'ancêtre de l'ESAE avant que cette dernière ne devienne une offre de service commerciale reposant sur une architecture bien plus complexe. La distinction a donc son importance puisqu'elle tient essentiellement à ce critère de complexité (la *Red forest* est minimaliste tandis que l'ESAE est une architecture complexe).

Par cette absence de spécifications, il existe des implémentations aussi diverses que variées du principe de forêt d'administration au sein des organisations. Parfois, ces implémentations ne respectent pas l'état de l'art en matière de cloisonnement. Certaines organisations en étendent même l'usage à l'administration du *Tier 1* voire du *Tier 2*, ce qui implique souvent des cas d'usage contraires au principe de surface d'attaque minimale de la forêt d'administration. Une forêt d'administration mal implémentée ou mal opérée peut présenter des chemins d'attaque qui la met en péril en cas de compromission d'une forêt administrée. Dans ce cas, elle risque de ne pas préserver convenablement le cloisonnement des forêts qu'elle administre.

Enfin et contrairement aux forêts administrées, la forêt d'administration présente l'avantage de répondre à des cas d'usage très limités qui sont uniquement liés aux actions d'administration du *Tier 0*. Elle n'est, par exemple, pas concernée par les problèmes de compatibilité que présentent habituellement les ressources hétérogènes d'un SI et qui freinent souvent le MCO et le MCS des forêts. Les recommandations de ce guide lui sont donc plus aisément appliquées, par l'adoption simplifiée des systèmes et niveaux fonctionnels AD les plus récents et par la mise en œuvre facilitée des différents mécanismes de sécurité offerts par les systèmes et composants logiciels. En synthèse, une forêt d'administration AD bénéficie plus facilement d'un niveau de sécurité élevé, comparé à une forêt de production qui est soumise à nombreuses contraintes.

5.3.2.2 Utilité d'une forêt d'administration

Cette section vise à donner des éléments de décision permettant à une organisation de déterminer s'il y a un intérêt à ce que ses environnements AD soient administrés depuis une forêt d'administration AD. Il est donc important de commencer par préciser à quoi sert une forêt d'administration AD et ce qu'elle apporte.

Attention

Une forêt d'administration AD ne sert pas à renforcer le niveau de sécurité d'une forêt AD administrée ni de son administration. Au contraire, elle apporte des contraintes opérationnelles et de sécurité supplémentaires avec tout ce que cela implique en termes organisationnels, financiers, temps de déploiement initial et d'administration, efforts de MCO et MCS, etc. Elle est également susceptible d'affaiblir le cloisonnement si elle n'est pas implémentée et opérée à l'état de l'art ou si elle n'est pas parfaitement maîtrisée par les équipes d'administration. Une forêt d'administration AD a pour unique objectif de permettre la mutualisation de postes d'administration du *Tier 0*, de sorte que ces derniers permettent l'administration des *Tier 0* de différentes forêts cloisonnées les unes des autres.

Une forêt d'administration AD n'est pas déployée pour des raisons de sécurité, mais uniquement pour des raisons de mutualisation.

Exemple

Pour des raisons d'obsolescence des applicatifs et des ressources métiers ou de mauvaise gouvernance accumulée au fil des ans, entre autres, il arrive que le niveau de sécurité de certaines forêts AD soit faible. Dans ce cas, les règles d'hygiène des SI [6] les plus élémentaires sont rarement appliquées. Il en résulte généralement une difficulté à mettre en œuvre un modèle de gestion des accès privilégiés et cela se traduit par des problèmes de cloisonnement des zones de confiance.

Dans ces conditions, la compromission puis la prise de contrôle d'une forêt par un attaquant est un événement hautement probable. Comme expliqué dans la présente section, l'ajout d'une forêt d'administration n'est toutefois pas une solution permettant d'améliorer le niveau de sécurité ou de cloisonnement d'une forêt dont le niveau de sécurité est faible. Quand la présence de ressources obsolètes au sein de la forêt est un frein pour l'amélioration de son niveau de sécurité, il est dans ce cas préférable et prioritaire d'étudier la mise en œuvre d'une forêt dédiée aux ressources « obsolètes ». Cette problématique n'étant pas le cœur du sujet du présent guide, elle n'est abordée que succinctement en annexe F.

L'élément de décision principal pour le déploiement d'une forêt d'administration est relatif à l'importance du besoin de mutualisation des postes d'administration des *Tier 0* de plusieurs forêts, c'est-à-dire, *in fine*, le nombre d'administrateurs de *Tier 0* et la fréquence des actions d'administration qui relèvent des *Tier 0* de chacune des forêts. Le cloisonnement du SI par le processus d'amélioration continue détaillé en section 2.3 permet d'atteindre rapidement un stade où les actions d'administration qui relèvent réellement du *Tier 0* devraient être peu fréquentes et où la population d'administrateurs du *Tier 0* devrait être réduite. À partir du moment où seul un nombre restreint de postes d'administration du *Tier 0* peut suffire dans chaque forêt, l'intérêt de leur mutualisation au sein d'une forêt d'administration devient faible au regard du cout, des risques et de la complexité de gestion que cette forêt représenterait. En revanche, la mutualisation des postes d'administration des *Tier 0* de ces forêts au sein d'une forêt d'administration AD peut se justifier dans certains cas, si par exemple :

- les actions d'administration des *Tier 0* restent fréquentes et menées par un nombre significatif d'administrateurs. La mutualisation répond dans ce cas à des besoins financiers ;
- l'administration des *Tier 0* doit absolument être réalisée en astreinte à distance ou en nomadisme (cf. section 5.4.3) et les administrateurs peuvent légitimement ne pas vouloir se déplacer avec des postes d'administration dédiés pour chacune des forêts qu'ils administrent. La mutualisation répond dans ce cas à des besoins de confort d'administration et de continuité de service.

R85

Éviter le déploiement d'une forêt d'administration

Il est recommandé d'éviter le déploiement d'une forêt d'administration, à moins que le besoin de mutualisation des postes d'administration des *Tier 0* de plusieurs forêts AD soit important et contre-balance les fortes contraintes organisationnelles, opérationnelles et de sécurité qu'elle occasionne. Le choix de mettre en œuvre une forêt d'administration doit donc être un choix mûrement réfléchi et ses conséquences doivent être préalablement évaluées et comprises par l'organisation.

R86

Assurer le cloisonnement d'une éventuelle forêt d'administration AD

Dès lors qu'une forêt d'administration est déployée, alors elle doit être correctement cloisonnée des forêts qu'elle administre et doit également assurer le cloisonnement de ces dernières. Les recommandations de ce guide pour le cloisonnement du *Tier 0* vis-à-vis des *Tiers* de moindre sensibilité doivent être déclinées et appliquées de manière équivalente pour assurer le cloisonnement de la forêt d'administration vis-à-vis des forêts qu'elle administre. Quant aux relations d'approbation AD nécessaires entre la forêt d'administration et les forêts administrées, elles doivent satisfaire aux recommandations de sécurité figurant en section 3.2.3.

5.4 Contextualisation des recommandations du guide d'administration sécurisée des SI

Le guide ADMIN [16] formule des recommandations qui se veulent génériques et applicables à de multiples contextes et environnements, mais qui ne sont pas toutes adaptées à un SI reposant sur un annuaire AD. C'est notamment le cas :

- des recommandations R15 et R15- du chapitre 5 (traitant des réseaux d'administration), qui recommandent de connecter les ressources d'administration sur un réseau physique dédié à l'administration ou sur un réseau VPN IPsec dédié à l'administration. L'adaptation de ces recommandations au cas de l'administration d'un SI reposant sur un annuaire AD est détaillée en section 5.4.1 ;
- des recommandations R18 et R18- du chapitre 5, qui recommandent que les ressources du SI aient une interface réseau physique ou virtuelle dédiée à l'administration. L'adaptation de ces recommandations au cas de l'administration d'un SI reposant sur un annuaire AD est détaillée en section 5.4.2 ;
- de la recommandation R28 du chapitre 7 (relatif à l'identification, l'authentification et aux droits d'administration) qui recommande de protéger l'accès aux annuaires des comptes d'administration, en ne les exposant pas sur des environnements de moindre confiance. Il convient de préciser que cette recommandation s'applique uniquement aux annuaires qui sont dédiés à l'administration, c'est-à-dire ceux des SI d'administration et ceux des forêts d'administration AD ;
- des recommandations du chapitre 10 (concernant l'administration à distance et le nomadisme). L'adaptation de ces recommandations au cas de l'administration d'un SI reposant sur un annuaire AD est détaillée en section 5.4.3 ;
- des recommandations du chapitre 11 (traitant des système d'échanges sécurisés). L'adaptation de ces recommandations au cas de l'administration d'un SI reposant sur un annuaire AD est détaillée en section 5.4.4.

5.4.1 Ressources d'administration et réseau physique dédié à l'administration

Dans une forêt AD, les postes d'administration du *Tier 0* et les contrôleurs de domaine AD se contrôlent mutuellement. En effet, les postes d'administration du *Tier 0* administrent les res-

sources du *Tier 0* et les contrôlent donc légitimement. À l'inverse, les contrôleurs de domaine gèrent et contrôlent légitimement l'ensemble des ressources membres de l'AD, dont les postes d'administration du *Tier 0*. *De facto*, tout filtrage réseau, dans une forêt AD, entre les postes d'administration du *Tier 0* et les ressources du *Tier 0* est par conséquent superflu. Par ailleurs, si les postes d'administration du *Tier 0* sont positionnés dans un réseau d'administration séparé (physiquement ou logiquement), alors leur dépendance vis-à-vis des contrôleurs de domaine fait qu'en cas de compromission de la forêt AD du SI administré, un attaquant disposerait d'une porte dérobée dans ce réseau d'administration séparé. Cette porte dérobée rapprocherait l'attaquant d'autres ressources d'administration et d'autres ressources administrées, incluant potentiellement des ressources non intégrées à l'AD.

R87

Appliquer les recommandations R15 et R15- du guide ADMIN avec discernement

Les recommandations R15 et R15- du guide ADMIN [16] (qui recommandent de connecter les ressources d'administration sur un réseau physique dédié à l'administration ou sur un réseau VPN IPsec dédié à l'administration) ne sont pas applicables aux ressources d'administration du *Tier 0* dès lors qu'elles sont membres de la forêt AD qu'elles administrent.

En revanche, ces deux recommandations gardent tout leur sens dans le cas contraire, c'est à dire quand elles sont positionnées dans le SI d'administration (cf. section 5.3.1) ou quand elles sont membres d'une forêt d'administration (cf. section 5.3.2).

5.4.2 Interface réseau physique ou virtuelle dédiée à l'administration

Par défaut, un contrôleur de domaine AD opère sur l'ensemble de ses interfaces réseau (qu'il s'agisse de cartes réseau physiques ou d'interfaces réseau virtuelles). Bien qu'il soit techniquement possible d'éviter d'inscrire des interfaces réseau indésirables dans le DNS d'un contrôleur de domaine multirésident, ceci n'est pas une pratique conseillée. Un contrôleur restera dans tous les cas administrable (par RPC notamment) depuis son interface réseau de production (celle via laquelle il communique avec les ressources membres de l'AD), même s'il possède une interface réseau que l'organisation souhaite dédier à son administration. En effet, les interfaces RPC servent à tous types d'appels et de communication, sans possibilité de filtrage fin, que ces appels concernent donc des actions d'administration ou des accès utilisateurs. Il est ainsi normal et légitime d'administrer et de consommer les services d'un contrôleur de domaine depuis une seule et même interface réseau.

Ceci est également vrai pour tout serveur Windows membre d'un domaine AD. Bien qu'il soit possible de leur dédier des interfaces à l'administration, ces serveurs sont administrables par RPC depuis toutes leurs interfaces réseau. RPC étant nécessaire aux communications entre les serveurs Windows et leurs contrôleurs de domaine, il n'est techniquement pas possible d'interdire RPC sur les interfaces réseau de production.

R88

Appliquer les recommandations R18 et R18- du guide ADMIN avec discernement

L'application, aux contrôleurs de domaine, des recommandations R18 et R18- du guide ADMIN [16] (qui recommandent que les ressources du SI aient une interface réseau physique ou virtuelle dédiée à l'administration) ne présente aucun intérêt de sécurité et peut poser des problèmes de fonctionnement. Son application est déconseillé dans ce cas précis.

Par ailleurs, l'application, aux serveurs Windows membres de l'AD, des recommandations R18 et R18- du guide ADMIN [16] ne présente pas un intérêt de sécurité notable pour sécuriser leur administration ou contre la grande majorité des scénarios de menace qui pèsent sur le SI. Par contre, elle peut dans certains cas permettre la sécurisation de flux qui ne doivent pas transiter sur le réseau de production. Son application est donc possible et utile dans certains cas, mais ne fait pas l'objet d'une recommandation.

En revanche, la recommandation R18 garde tout son sens et reste donc applicable dans le cas particulier des interfaces réseau IPMI (se référer à la section 3.8). Ces interfaces doivent être uniquement joignables depuis un réseau d'administration.

5.4.3 Administration à distance et nomadisme

Le chapitre 10 du guide ADMIN [16] formule des recommandations générales pour l'administration à distance (c'est à dire l'accès au SI en dehors du réseau local de l'organisation) et le nomadisme (c'est-à-dire l'utilisation d'un poste d'administration dans un lieu extra-professionnel).

La sensibilité du *Tier 0* est telle qu'elle justifie l'interdiction de son administration à distance.

R89

Interdire l'administration du Tier 0 à distance ou en nomadisme

L'administration du *Tier 0* ne doit pas être possible à distance ou en nomadisme. Les postes d'administration du *Tier 0* ne doivent pas sortir des locaux sécurisés prévus à cet effet (cf. section 3.8.1 concernant la sécurité physique des ressources du *Tier 0*).

Il est important de prendre du recul quant à l'applicabilité de cette recommandation R89 : le cloisonnement du SI par le processus d'amélioration continue détaillé en section 2.3 permet d'atteindre rapidement un stade où les actions d'administration qui relèvent réellement du *Tier 0* devraient être peu fréquentes et ne devraient *a priori* pas revêtir un caractère d'urgence. Par conséquent, dans l'éventualité d'une urgence d'administration du *Tier 0* en heures non ouvrées par des équipes en astreinte, le déplacement des équipes dans les locaux de l'administration reste la solution à privilégier.

Pour autant, satisfaire à cette recommandation R89 peut s'avérer difficile dans certains contextes. C'est, par exemple, le cas des organisations dont les SI sont essentiellement administrés à distance ou lorsque le déplacement des équipes en astreinte est trop contraignant. C'est également le cas

en phase transitoire lorsque la démarche de cloisonnement du SI en *Tiers* vient de débuter et que les actions d'administration du *Tier 0* restent encore trop fréquentes et parfois urgentes. Les organisations peuvent alternativement autoriser l'administration à distance du *Tier 0*, que ce soit en phase transitoire ou de manière pérenne en fonction de leurs besoins et de leurs objectifs de sécurité.

R89 -

Sécuriser l'administration à distance ou en nomadisme du Tier 0

Si l'organisation autorise l'administration à distance ou en nomadisme du *Tier 0*, alors les recommandations du guide de nomadisme numérique de l'ANSSI [11] doivent être appliquées en complément des recommandations du chapitre 8 du guide ADMIN [16].

Dans ce cas, un ou plusieurs concentrateurs VPN doivent être dédiés à l'administration des zones de confiance les plus sensibles (c'est-à-dire le *Tier 0* et les SI d'administration par exemple). Puis, pour pallier le risque de vulnérabilités de ces concentrateurs VPN, ces derniers devraient être uniquement accessibles par une liste d'adresses IP publiques autorisées qui correspondent à des emplacements réseau de lieux privés non ouverts au public depuis lesquels l'organisation autorise l'administration à distance. Ces adresses IP peuvent, par exemple, être celles des éventuels infogérants d'administration ou des domiciles des administrateurs [48].

5.4.4 Systèmes d'échanges sécurisés

Le chapitre 11 du guide ADMIN [16] formule des recommandations pour la mise en œuvre d'un système d'échanges sécurisés entre le SI d'administration et le SI bureautique. Dans le contexte d'un SI reposant sur un annuaire AD et cloisonné selon les principes d'un modèle de gestion des accès privilégiés, le besoin de sécuriser les échanges se pose également entre *Tiers*.

Pour répondre à ce besoin d'échanges sécurisés entre *Tiers* au sein d'une même forêt AD, un partage SMB peut suffire. En effet, les administrateurs s'y connectent à l'aide d'une authentification réseau, c'est-à-dire sans disséminer des secrets d'authentification réutilisables. Par ailleurs, son utilisation repose sur les protocoles natifs de Windows déjà utilisés entre les clients et les contrôleurs de domaine AD, ce qui n'augmente donc pas la surface d'attaque des systèmes.

Ensuite, le serveur de fichiers utilisé doit mettre en œuvre une solution d'analyse de contenu à la recherche de codes malveillants, conformément à la recommandation R58 du guide ADMIN [16].

Pour finir, il convient de préciser que ce système d'échanges ne doit contenir que des données non sensibles. Aucune donnée ne doit permettre le moindre chemin d'attaque vers une zone d'un plus haut niveau de confiance. Sinon, cela signifie que cette donnée n'a pas lieu d'être accessible depuis un *Tier* de moindre sensibilité sans avoir été préalablement chiffrée (une problématique similaire a été détaillée en section 3.4.1 pour la sauvegarde des données du *Tier 0*).

48. Il est à noter que si la connexion Internet adossée à un emplacement réseau autorisé ne s'appuie pas sur une adresse IP fixe (cas fréquent des connexions Internet à usage non professionnel), l'organisation peut proposer la prise en charge financière de la souscription d'un abonnement ou d'une option d'abonnement permettant l'attribution d'une adresse IP fixe.

Annexe A
Détails complémentaires aux chemins de contrôle AD du Tier 0

Pour chaque objet de l'AD catégorisé en *Tier 0* dans les sous-sections 3.2.2 et 3.2.1 du chapitre 3, cette annexe apporte des arguments justifiant cette catégorisation. Bien que cette annexe A se veuille aussi complète que possible, elle reste néanmoins fournie sans garantie d'exhaustivité.

A.1 Conteneurs système ou de configuration

Objet	Justification
Partition de schéma :	
`CN=Schema`	Voir `CN=Schema Admins` en tableau 4.
Partition de configuration :	
`CN=Configuration` et sous-dossiers	Contient diverses informations de configuration de l'AD. Tout comme pour le conteneur système, toute la partition n'est pas à proprement parler de *Tier 0* car certains des objets qu'elle contient ne permettent pas réellement un contrôle du *Tier 0*, ils peuvent en revanche nuire à sa disponibilité et leur contrôle ne doit être délégué qu'à des administrateurs de *Tier 0*.
Partition de l'AD (contexte d'attribution de noms par défaut) :	
Racine `DC=...,DC=...`	Le conteneur racine du domaine dans le contexte d'attribution de noms par défaut est naturellement de *Tier 0*, mais ce n'est pas *de facto* le cas de ses sous-dossiers.
`CN=Builtin`	Contient des objets de *Tier 0* listés en tableau 4.
`OU=Domain Controllers`	Voir l'objet `CN=Domain Controllers` dans le tableau 4.
`CN=LostAndFound`	Il est probable que des objets de *Tier 0* orphelins se retrouvent dans ce conteneur, il devrait donc être considéré de ce même niveau de privilèges.

Ce tableau se poursuit sur la page suivante

Objet	Justification
`CN=Managed Service Accounts`	Il est possible que des *Managed Service Accounts* [79] aient des haut privilèges sur des objets de *Tier 0*. Le contrôle de ce conteneur induit le contrôle de ces comptes de service et donc l'obtention des droits et privilèges qui leur ont été octroyés.
`CN=NTDSQuota`	La modification des quotas peut nuire à la disponibilité et leur contrôle n'est généralement délégué qu'à des administrateurs de *Tier 0*.
`CN=Program Data` et sous-dossiers	Il existe une certaine probabilité que des applications du *Tier 0* stockent dans ce conteneur des informations sensibles permettant le contrôle de ce *Tier*. L'idéal serait de considérer indépendamment le niveau de privilèges de chaque sous-conteneur (un par éditeur généralement) mais pour éviter toute mauvaise appréciation du risque il reste tout de même recommandé de considérer l'ensemble du conteneur comme étant de *Tier 0*.
`CN=System` et sous-dossiers	Contient des informations de configuration pour différents services et mécanismes sensibles de l'AD, tels que les liens de réplications DFS et DFRS, le groupe `AdminSDHolder`, les stratégies de groupe, les clés DPAPI, le service Microsoft DNS, etc. Si les objets de ce conteneur sont essentiellement de *Tier 0*, l'ensemble n'est pas à proprement parler de *Tier 0* car certains des objets ne permettent pas réellement un contrôle du *Tier 0*. En revanche, ces derniers peuvent nuire à la disponibilité de l'annuaire et leur contrôle ne doit être délégué qu'à des administrateurs de *Tier 0*.
`CN=TPM Devices`	Les informations des puces TPM sont stockées dans ce conteneur puis liées à leurs comptes d'ordinateur d'appartenance. Concernant les puces TPM des ressources de *Tier 0*, l'accès à ces informations pourrait permettre la lecture de clés de recouvrement BitLocker ou d'empreintes de mots de passe stockées en TPM. Ce conteneur doit donc être considéré de *Tier 0*.
`CN=Users`	Contient des objets de *Tier 0* listés en tableau 4.

Tableau 3 – Arguments de catégorisation en *Tier* 0 des conteneurs système et de configuration de l'AD

A.2 Comptes et groupes de sécurité intégrés par défaut

La colonne « PAG » (*protected accounts and groups*) du tableau 4 indique quels comptes et groupes font partie des « comptes et groupes protégés de l'AD » [81] à partir de Windows Serveur 2008.

Objet	Justification	PAG ?
`CN=Account Operators`	Octroie les droits complets sur les comptes utilisateurs et ordinateurs de l'AD, dont celui de réinitialiser leurs mots de passe. Bien que ce droit ne permette pas de réinitialiser les mots de passe des comptes et groupes protégés [81] de l'AD, le *Tier 0* identifié en chapitre 3 ne se limite généralement pas à ces comptes et groupes protégés. L'usage du groupe `CN=Account Operators` est donc à proscrire (il devrait être vide) et il est recommandé de lui préférer la délégation de droits par unités organisationnelles ou directement sur certains objets de l'AD.	Oui
`CN=Administrators`	Octroie des privilèges d'administration du domaine.	Oui
`CN=Administrator`	Il s'agit du compte d'administration du domaine, il dispose du plus haut niveau de privilèges.	Oui
`CN=Backup Operators`, `CN=Server Operators`, `CN=Replicator`	Permettent des élévations de privilèges par accès logique au stockage à travers des opérations de sauvegarde qui contournent les droits NTFS (se référer à la section 3.4 concernant les élévations de privilèges par accès logique au stockage).	Oui
`CN=Distributed COM Users`	Octroie des privilèges d'activation et d'exécution distante de composants COM (et donc également des privilèges d'exécution distante de commandes et de processus), ces derniers présentant une surface d'attaque très importante pouvant être exploitée pour de l'élévation de privilèges. Ce groupe devrait être considéré de *Tier 0* par principe de précaution.	Non
`CN=DNSAdmins`	Permettait l'exécution de librairies arbitraires sur les contrôleurs de domaines, ces dernières pouvant alors être utilisées pour de l'élévation de privilèges. **Ce n'est plus le cas depuis la mise à jour Windows Serveur datant d'octobre 2021 (cf. CVE-2021-40469 [35]), mais reste valable pour tout contrôleur de domaine n'ayant pas appliqué cette mise à jour**.	Non
`CN=Domain Controllers`	Les comptes d'ordinateur des contrôleurs de domaine AD permettent le contrôle d'objets de *Tier 0*, ils peuvent donc être utilisés par un attaquant pour de l'élévation de privilèges ou de la persistance.	Oui
`CN=Domain Admins`, `CN=Enterprise Admins`	Octroient des privilèges d'administration du domaine et de la forêt.	Oui

Ce tableau se poursuit sur la page suivante

Objet	Justification	PAG ?
`CN=Enterprise Key Admins`	Généralement considéré de *Tier 0* en raison d'un bug connu d'`Adprep.exe` qui survient lors de la mise à niveau des contrôleurs de domaine vers Windows Serveur 2016 (sur les versions antérieures à la 1709) et qui a pour résultat que ce groupe se retrouve avec le contrôle total de l'annuaire AD. Si ce groupe n'a pas les permissions de contrôle total sur la racine du domaine, ou si ses permissions ont été corrigées [42], il n'est dans ce cas pas nécessaire de le considérer de *Tier 0*.	Non
`CN=Hyper-V Administrators`	Si des serveurs Hyper-V du domaine AD hébergent des machines virtuelles de *Tier 0* alors les serveurs Hyper-V eux-même ainsi que ce groupe devraient être considérés de *Tier 0* (se référer à la section 3.5 concernant les élévations de privilèges via les infrastructures de virtualisation).	Non
`CN=krbtgt`	Il s'agit du compte de service utilisé par le KDC Kerberos (*Key Distribution Center*) de l'AD. Ses privilèges lui permettent de générer des tickets Kerberos arbitraires contenant n'importe quelle PAC (*Privileged Attribute Certificate*), c'est-à- dire n'importe quels droits et privilèges. Ce compte est souvent désigné comme le Saint Graal de l'annuaire AD.	Oui
`CN=Group Policy Creator Owner`	Ce groupe peut contenir des comptes utilisateurs qui créeent des GPO se trouvant ensuite attachées à des ressources de *Tier 0*. En restant propriétaires de ces GPO, ces comptes gardent un contrôle administratif indirect des ressources en question. Dans ce cas, le groupe « `Group Policy Creator Owners` » est à considérer comme faisant partie du *Tier 0*. Pour l'éviter, une bonne pratique est de s'assurer du changement de propriétaire et des permissions de la GPO au moment de son rattachement à des ressources, ou bien de ne rattacher à des ressources de *Tier 0* que des GPO créées par des comptes de *Tier 0*. Dans tous les cas, le propriétaire d'une GPO doit être au moins du même *Tier* que les ressources rattachées à cette GPO.	Non
`CN=Print Operators`	Permet le chargement de pilotes de périphériques arbitraires sur les contrôleurs de domaines, ces pilotes pouvant être utilisés pour de l'élévation de privilèges.	Oui

Ce tableau se poursuit sur la page suivante

Objet	Justification	PAG ?
`CN=Read-only Domain Controllers`	En cas de mauvaise configuration des stratégies de réplication, des comptes de *Tier 0* peuvent voir leurs secrets répliqués sur des RODC. Diverses mauvaises pratiques peuvent par ailleurs occasionner une élévation de privilèges vers le *Tier 0* depuis un RODC. Dans ce cas, les RODC présentent la même sensibilité que les `CN=Domain Controllers`.	Oui
`CN=Schema Admins`	Un privilège de modification du schéma AD permet, par exemple, de modifier les droits par défaut appliqués aux classes et donc aux objets qui seront créés dans l'annuaire (quel que soit leur *Tier*).	Oui

Tableau 4 – Arguments de catégorisation en *Tier* 0 des comptes et groupes de sécurité intégrés par défaut de l'AD

Annexe B
Utilisation du groupe de sécurité des utilisateurs protégés

Le groupe de sécurité des utilisateurs protégés (*Protected Users*) est un dispositif de sécurité apparu avec Windows Serveur 2012 R2. Bien que le groupe soit créé par une simple extension de schéma vers Windows Serveur 2012 R2, un niveau fonctionnel AD 2012 R2 est nécessaire pour profiter pleinement des apports du dispositif[49]. Les comptes utilisateurs membres de ce groupe se voient automatiquement appliquer un niveau de sécurité accru qui consiste à :

- désactiver l'authentification NTLM pour ne plus leur autoriser que l'authentification Kerberos. Il est à noter que les services qui ne reposent pas sur l'authentification unique (*Single Sign On*, ou SSO) de l'AD ne sont pas impactés par cette restriction ;
- empêcher les algorithmes faibles DES et RC4 au niveau de la pré-authentification Kerberos ;
- limiter la mise en cache de jetons d'authentification à l'ouverture de session ;
- interdire leur délégation Kerberos contrainte ou non contrainte ;
- imposer une durée de validité maximale de leurs TGT de 4 heures.

Comme indiqué dans l'article [30], « *l'utilisation exclusive de Kerberos améliore grandement la protection des secrets d'authentification, les membres de ce groupe n'exposant pas leur secret d'authentification lors de l'authentification auprès d'un service. Cependant, peu d'applications supportent exclusivement l'authentification par Kerberos, ce qui limite la mise en œuvre du groupe des utilisateurs protégés* ». Néanmoins, avoir circonscrit le *Tier 0* et réduit son exposition aboutit généralement à une situation où le *Tier 0* se compose principalement voire exclusivement de composants logiciels de Microsoft qui supportent l'authentification Kerberos. La généralisation du groupe de sécurité des utilisateurs protégés est ainsi largement envisageable pour le *Tier 0* et sa mise en œuvre consiste à ajouter tous les comptes d'administration de *Tier 0* (identifiés en section 3.2) à ce groupe ;

En revanche, son utilisation pour la sécurisation des comptes d'administration de *Tier 1* et *Tier 2* requiert un recensement fin des authentifications supportées par les services administrés afin d'identifier les populations d'administrateurs auxquelles l'application de ce dispositif de sécurité est possible.

49. Le lecteur est invité à consulter le document de Microsoft [85] pour plus de détails sur ce dispositif de sécurité et ses prérequis, notamment la distinction entre les fonctionnalités appliquées côté client et celles côté KDC (*Key Distribution Center*).

Annexe C
Mise en œuvre d'un silo d'authentification du Tier 0

C.1 Introduction et prérequis des silos d'authentification

La configuration d'un silo d'authentification du *Tier 0* permet de faire en sorte que les comptes (utilisateurs et de service) du *Tier 0* ne puissent techniquement obtenir des TGT Kerberos que sur les systèmes (postes d'administration et serveurs) du *Tier 0*. Cela donne l'assurance qu'ils ne dissémineront pas leurs secrets d'authentification réutilisables sur les *Tiers* de moindre sensibilité (en application de la recommandation R64 d'encadrement de l'administration de ressources de moindre confiance). Cette restriction du périmètre d'authentification des membres du silo est en réalité appliquée par une stratégie d'authentification (*authentication policy*) Kerberos associée au silo.

Information

Les silos d'authentification sont apparus simultanément avec les stratégies d'authentification sous Windows Serveur 2012 R2. Ils ne peuvent pas être utilisés sur les systèmes d'exploitation antérieurs.

Attention

L'appartenance à un silo d'authentification doit s'accompagner de l'appartenance au groupe de sécurité des utilisateurs protégé (cf. annexe B) pour garantir que l'authentification Kerberos est obligatoire pour ses membres. Sans cette précaution, la stratégie d'authentification du silo (qui s'applique uniquement à Kerberos) pourrait notamment être contournée par l'utilisation de NTLM.

Pour rendre les stratégies d'authentification du silo de *Tier 0* fonctionnelles, il est nécessaire d'activer le support des revendications (*claims*) Kerberos dans l'AD. Cela peut notamment se faire par GPO, tel que cela est détaillé dans la section 4.12 dédiée au blindage Kerberos.

C.2 Utilisation d'un silo d'authentification en mode « audit »

Un silo d'authentification peut être configuré en mode *audit* (c'est-à-dire un mode de simple journalisation), par opposition au mode *enforced* (le mode par défaut) dans lequel la stratégie d'authentification est réellement activée. Dans ce mode *audit*, des évènements de sécurité sont générés à

chaque potentiel succès ou échec d'authentification. Cela permet de vérifier quelles authentifications auraient été bloquées et lesquelles auraient été autorisées par la stratégie d'authentification du silo. En phase de test, il est donc judicieux d'utiliser le mode *audit* pendant un certain temps afin de vérifier l'absence d'interdictions d'authentification imprévues.

Dans le script 16, l'argument « `-Enforce $True` » de la Cmdlet « `New-ADAuthenticationPolicy` » (ligne 25) précise d'appliquer la stratégie d'authentification. Dès lors que cet argument n'est pas présent (ou qu'il a pour valeur $False), la stratégie d'authentification fonctionne en mode *audit*.

Les évènements d'audit ainsi générés ont pour identifiant 305 et sont enregistrés dans le journal « `AuthenticationPolicyFailures-DomainController` » des journaux des applications et des services des contrôleurs de domaine à l'emplacement « `Microsoft\Windows\Authentication` ». Ces évènements précisent le compte, l'ordinateur, la stratégie d'authentification, le nom du silo ainsi que la durée de validité du TGT associés à l'interdiction qui aurait eu lieu si la stratégie avait été appliquée (*enforced*).

C.3 Configuration d'un silo d'authentification

Pour la mise en œuvre d'un silo, il est important de comprendre la nuance suivante : l'octroi du droit d'accès à un silo ne fait que donner le droit à un compte d'être membre du silo, mais il ne l'est pas *de facto*. L'appartenance au silo – possible seulement après l'octroi du droit d'accès au silo – est celle qui applique réellement la politique d'authentification du silo à ses membres (qu'ils soient des comptes utilisateur, des comptes de service ou des comptes d'ordinateur). Il est d'ailleurs à noter qu'un compte s'étant vu octroyer un droit d'accès à un silo peut ensuite lui-même se donner ou s'enlever l'appartenance à ce silo à l'aide des *Cmdlet* Powershell idoines.

Attention

Les droits d'accès à un silo et l'appartenance à ce dernier ne s'octroient que compte par compte et ne peuvent pas s'octroyer à un groupe. Ainsi, à chaque ajout ou suppression d'un administrateur du *Tier 0*, de même qu'à chaque ajout ou suppression d'une système dans le périmètre du *Tier 0*, il sera nécessaire d'octroyer ou de révoquer les accès au silo et les appartenances à ce dernier. Ces actions ne pourront pas être automatiques par la simple appartenance ou perte d'appartenance à un groupe. La difficulté de gestion de ce mécanisme de sécurité réside ainsi dans la maintenance nécessaire à chaque évolution de la liste des comptes de *Tier 0* ou de la liste des systèmes de *Tier 0*.

Le script 16 illustre la mise en œuvre d'un silo d'authentification du *Tier 0*. Il se compose de 3 étapes :

1. la création d'un silo d'authentification et de sa stratégie d'authentification ;
2. l'octroi d'accès à ce silo pour chacun des comptes utilisateurs et d'ordinateurs spécifiés ;
3. la configuration de l'appartenance au silo pour chacun des comptes utilisateurs et d'ordinateurs spécifiés.

```
# Script de mise en oeuvre d'un silo d'authentification pour le Tier 0.
# Ce script a uniquement vocation à illustrer la création d'un silo.
# Il doit être adapté au contexte et aux besoins de l'organisation.

# Les variables ci-dessous sont à renseigner pour la configuration du silo.
# 1) Nom et description de la politique d'authentification sous-jacente au silo :
$AuthPolicyName = "T0_AuthPol"
$AuthPolicyDesc = "T0 authentication policy"
# 2) Nom et description du silo :
$AuthSiloName = "T0_Silo"
$AuthSiloDesc = "T0 authentication silo"
# 3) Référence à un groupe du domaine contenant tous les comptes utilisateurs du Tier 0 qui doivent être membres du silo.
# Ce groupe devrait contenir les comptes de services du Tier 0 et les comptes administrateurs du Tier 0 (nominatifs)
# à l'exception du compte administrateur intégré du domaine (celui de RID 500) qui ne sera pas membre du silo :
$userGroup = "T0_Accounts"
# 4) Référence à un groupe du domaine contenant les ressources (ordinateurs et serveurs) du Tier 0 qui doivent
# être membres du silo. Attention de n'y inclure aucun contrôleur de domaine (ils sont ajoutés de facto par le script) :
$deviceGroup = "T0_Computers"
# ---

#  Etape 1 : configuration de la politique d'authentification et du silo.
## ---
## TGT de 2 heures :
New-ADAuthenticationPolicy -Name $AuthPolicyName -Description $AuthPolicyDesc `
 -UserTGTLifetimeMins 120 -Enforce $True -ProtectedFromAccidentalDeletion $True
## Authentification autorisée uniquement pour les utilisateurs ayant une revendication au nom du silo :
Set-ADAuthenticationPolicy -Identity $AuthPolicyName `
 -UserAllowedToAuthenticateFrom ("O:SYG:SYD:(XA;OICI;CR;;;WD;(@USER.ad://ext/AuthenticationSilo == `"" + $AuthSiloName + "`"))")
## Création du silo :
New-ADAuthenticationPolicySilo -Name $AuthSiloName -Description $AuthSiloDesc `
 -UserAuthenticationPolicy $AuthPolicyName -ComputerAuthenticationPolicy $AuthPolicyName
 -ServiceAuthenticationPolicy $AuthPolicyName `
 -Enforce -ProtectedFromAccidentalDeletion $True

# Etape 2 : Octroi des accès au silo.
## ---
## Note : Cette étape accorde uniquement les accès au silo, mais l'appartenance finale au silo est gérée à l'étape 3.
## Note : Par défaut, accorder l'accès à un silo est une action que seul un admin du domaine ou de l'entreprise peut réaliser.
## Note : Les utilisateurs, ordinateurs et comptes de service peuvent se voir accorder l'accès à plusieurs silos, mais ne peuvent
## être membres que d'un seul silo à la fois.
## Note : Accorder l'accès à un silo ne peut pas se faire dynamiquement par groupes, cela se fait compte par compte.
## Le script parcourt donc les variables $userGroup et $deviceGroup pour accorder l'accès compte par compte. Si le contenu de ces
## groupes change par la suite, le script devra être exécuté à nouveau car le silo ne sera pas mis à jour dynamiquement.
## Note : Révoquer l'accès à un silo peut se faire en exécutant la commande :
## Revoke-ADAuthenticationPolicySiloAccess -Identity $AuthSiloName -Account <utilisateur>
## Note : Les politiques d'authentification ne s'appliquent pas au compte administrateur intégré du domaine (RID 500).
## Ceci est une raison de plus pour que ce compte serve exclusivement de compte bris de glace, et ne soit donc pas utilisé pour
## l'administration courante.
## Note : Les controleurs de domaine en lecture seule (RODC) ne doivent, par définition, pas être membres du silo du Tier 0.
## ---
## Octroi d'accès aux utilisateurs membres de $userGroup :
Get-ADGroupMember -Identity $userGroup -Recursive | Where-Object {$_.objectclass -eq "user"} | `
    ForEach-Object {Grant-ADAuthenticationPolicySiloAccess -Identity $AuthSiloName -Account $_.DistinguishedName}
## Octroi d'accès aux ordinateurs (= RWDCs + contenu du $deviceGroup) :
### a) pour les contrôleurs de domaine (traités séparément car le primarygroup membership
### n'est pas retourné par la Cmdlet Get-ADGroupMember) :
Get-ADDomainController -Filter {IsReadOnly -eq $False} | `
    ForEach-Object {Grant-ADAuthenticationPolicySiloAccess -Identity $AuthSiloName -Account $_.ComputerObjectDN}
### b) pour les membres de $deviceGroup :
Get-ADGroupMember -Identity $deviceGroup -Recursive | Where-Object {$_.objectclass -eq "computer"} | `
    ForEach-Object {Grant-ADAuthenticationPolicySiloAccess -Identity $AuthSiloName -Account $_.DistinguishedName}

# Etape 3 : Appartenance au silo.
## ---
## Note : Les utilisateurs, ordinateurs et comptes de service peuvent se voir accorder l'accès à plusieurs silos, mais ne peuvent
## être membres que d'un silo à la fois. Configurer l'appartenance d'un compte à un silo lui fait donc perdre son appartenance
## antérieure à un autre silo.
## ---
## Configuration de l'appartenance au silo pour les utilisateurs membres de $userGroup :
Get-ADGroupMember -Identity $userGroup -Recursive | Where-Object {$_.objectclass -eq "user"} | `
    ForEach-Object {Set-ADAccountAuthenticationPolicySilo -AuthenticationPolicySilo $AuthSiloName -Identity $_.DistinguishedName}
## Configuration de l'appartenance au silo pour les ordinateurs :
### a) pour les contrôleurs de domaine :
Get-ADDomainController -Filter {IsReadOnly -eq $False} | `
    ForEach-Object {Set-ADAccountAuthenticationPolicySilo -AuthenticationPolicySilo $AuthSiloName -Identity
        $_.ComputerObjectDN}
### b) pour les membres de $deviceGroup :
Get-ADGroupMember -Identity $deviceGroup -Recursive | Where-Object {$_.objectclass -eq "computer"} | `
    ForEach-Object {Set-ADAccountAuthenticationPolicySilo -AuthenticationPolicySilo $AuthSiloName -Identity
        $_.DistinguishedName}
```

Listing 16 – Script de création ou de mise à jour d'un silo d'authentification de *Tier 0*

Alternativement, ce script peut être remplacé par une configuration manuelle dans le « Centre d'administration Active Directory » (disponible depuis le « Gestionnaire de serveur ») d'un contrôleur de domaine, comme illustré par les figures 11, 12 et 13.

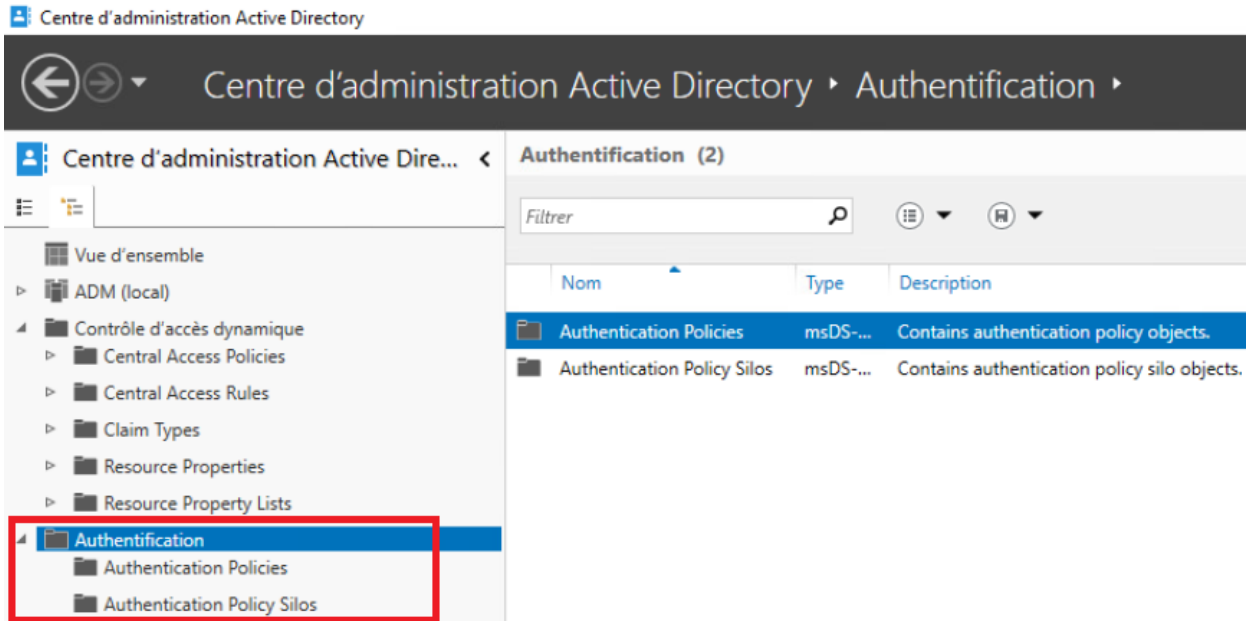

FIGURE 11 – Emplacement de configuration des stratégies d'authentification et des silos d'authentification dans le Centre d'administration Active Directory.

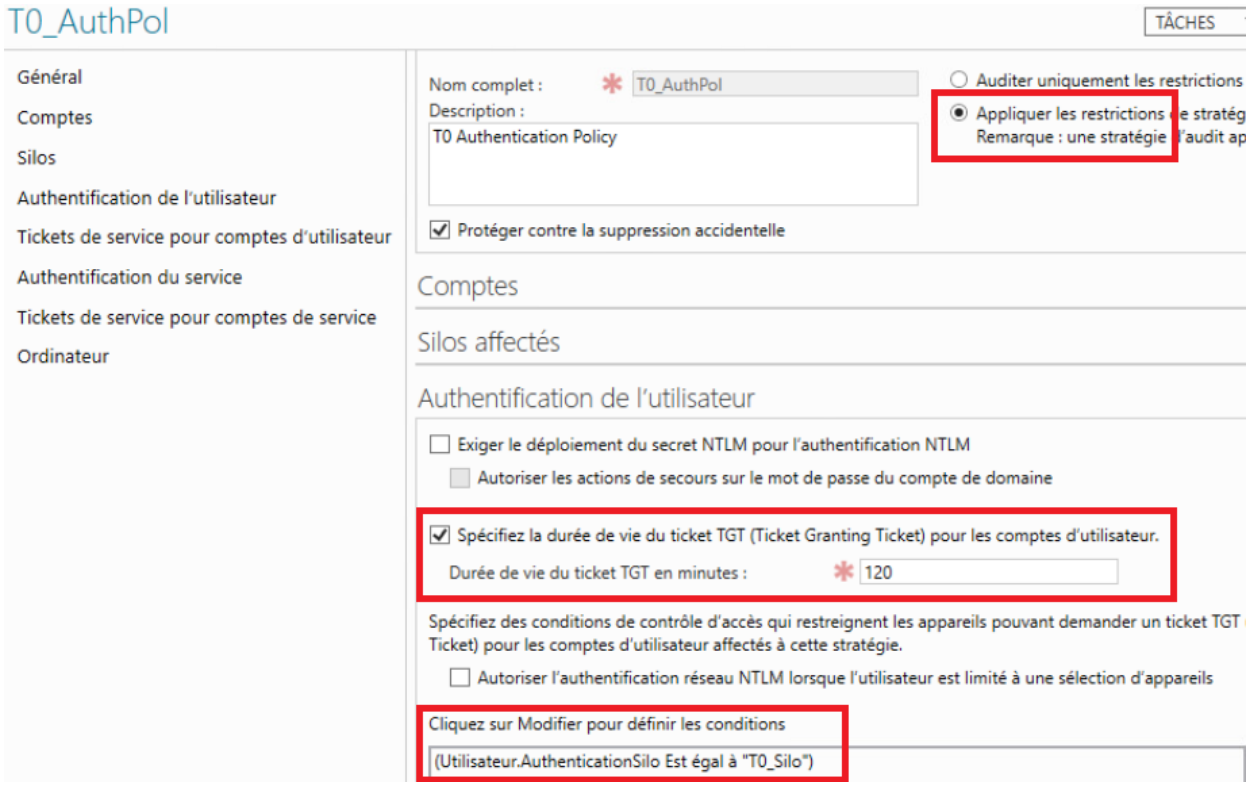

FIGURE 12 – Configuration de la stratégie d'authentification dans le Centre d'administration Active Directory.

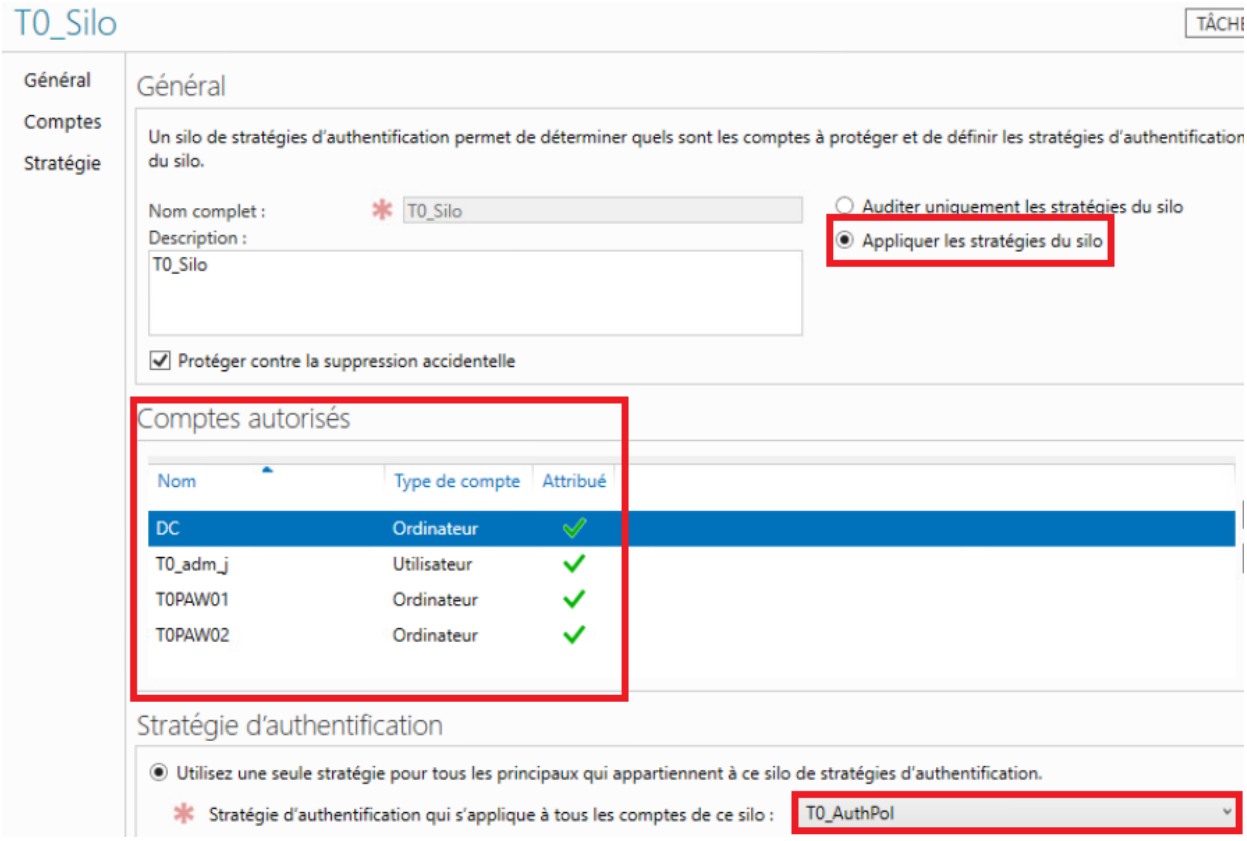

FIGURE 13 – Configuration du silo d'authentification dans le Centre d'administration Active Directory.

C.4 Utilisation de stratégies d'authentification sans silo d'authentification

La configuration d'un silo d'authentification s'accompagne d'une unique stratégie d'authentification relativement simple à configurer. Cela facilite la mise en œuvre de ce mécanisme qui impose que la délivrance de TGT Kerberos aux comptes du *Tier 0* ne soit permise que sur les seuls systèmes (postes d'administration et serveurs) du *Tier 0*.

Néanmoins et à défaut de mettre en œuvre un silo d'authentification du *Tier 0*, il reste également possible de créer des stratégies d'authentification ayant plus ou moins la même finalité.

Annexe D
Mise en œuvre des paramètres de restriction d'ouvertures de session

L'application d'un modèle de gestion des accès privilégiés consiste, entre autres, à faire en sorte que les comptes ne disséminent pas leurs secrets d'authentification réutilisables sur des *Tiers* de moindre confiance (recommandation R29). La recommandation R64 – d'encadrement de l'administration de ressources de moindre confiance – précise la nécessité d'imposer des restrictions par le biais de mesures techniques.

Quatre paramètres de stratégies de sécurité permettent de couvrir les risques de dissémination de tickets Kerberos abordés en chapitre 4 en interdisant l'ouverture de session interactive à certains comptes sur certaines ressources. Ces paramètres, indiqués par le listing 17 se configurent en précisant un ensemble de comptes ou de groupes utilisateurs auxquels interdire l'ouverture de session. Ils s'appliquent ensuite à un ensemble de ressources par GPO ou via leurs stratégies de sécurité locales.

```
Chemin : Configuration ordinateur\Paramètres Windows\Paramètres de sécurité\
        Stratégies locales\Attribution des droits d'utilisateur
Stratégies :
        Interdire l'ouverture de session locale
        Interdire l'ouverture de session en tant que service
        Interdire l'ouverture de session en tant que tâche
        Interdire l'ouverture de session par les services de bureau à distance
```

Listing 17 – Paramètres de stratégies de sécurité pour la restriction d'ouverture de session

Attention

Une limite importante à ces stratégies est qu'elles empêchent uniquement la dissémination de tickets Kerberos et n'empêchent en aucun cas la dissémination de condensats NTLM. En effet, les condensats NTLM se trouvent disséminés sur les ressources **AVANT** que l'interdiction d'ouverture de session soit arbitrée. En authentification Kerberos en revanche, l'arbitrage est opéré avant toute dissémination du TGT Kerberos de l'utilisateur (cf 4 pour les détails relatifs à NTLM et Kerberos).

Autrement dit, ces stratégies ne sont réellement efficaces que lorsque l'authentification NTLM est bloquée vers les ressources sur lesquelles ces stratégies sont appliquées (cf. section 4.15 abordant le blocage du trafic NTLM) ou lorsque les utilisateurs pour lesquels l'ouverture de session est interdite peuvent uniquement s'authentifier par Kerberos (ce qui est notamment le cas s'ils sont membres du groupe de sécurité des utilisateurs protégés détaillé en annexe B).

La mise en œuvre de la recommandation R64 consiste dans ce cas à interdire ces quatre types d'ouverture de session pour tous les comptes de *Tier 0* et sur toutes les ressources de *Tier 1* et de *Tier 2*. Les comptes de *Tier 0* en question doivent être les groupes de sécurité de *Tier 0* listés en annexe A ainsi que tous les autres comptes ayant une éventuelle relation de contrôle directe ou indirecte du *Tier 0*. Ces derniers ont été identifiés comme tels par l'analyse des chemins de contrôle et d'élévation de privilèges vers le *Tier 0* qui est déroulée en chapitre 3.

La difficulté de gestion de ce mécanisme de restriction des ouvertures de session réside dans la nécessité de maintenir la liste exhaustive des ressources de *Tier 1* et de *Tier 2* auxquelles appliquer ces paramètres de stratégie de sécurité, ainsi que la liste exhaustive des comptes de *Tier 0* auxquels interdire l'ouverture de session. L'utilisation d'un silo d'authentification du *Tier 0* (abordée en annexe C) est à privilégier pour restreindre la dissémination de secrets d'authentification réutilisables du *Tier 0* sur des ressources de moindre confiance.

Une bonne pratique pour une application exhaustive de ces paramètres aux ressources de *Tier 1* et de *Tier 2* est de le faire par GPO appliquée(s) aux « Utilisateurs authentifiés » (cas par défaut lors de la création d'une GPO) et liée(s) à toutes les OU susceptibles de contenir les ressources de *Tier 1* ou de *Tier 2* (dans l'hypothèse où les ressources de *Tier 0* sont dans des OU séparées sur lesquelles aucune GPO de restriction d'ouverture de session ne s'applique). Enfin, l'utilisation d'un groupe utilisateur qui contiendrait en permanence tous les comptes et groupes utilisateurs de *Tier 0* (éventuellement créé, peuplé et maintenu spécifiquement à cette fin) permet de simplement renseigner cet unique groupe utilisateur comme valeur de chacun des quatre paramètres de stratégie de sécurité indiqués par le listing 17.

Annexe E
Utilisation de RDP avec option Restricted Admin

E.1 Utilité et particularités de l'option Restricted Admin

L'option *Restricted Admin* de RDP (RDP RA) présente un avantage notable : elle permet à un administrateur d'utiliser RDP sans disséminer de secrets d'authentification réutilisables (condensats NTLM ou tickets Kerberos) sur l'hôte distant administré par déport d'affichage. Cela vient toutefois au prix d'une limitation fonctionnelle.

Avec RDP RA, la session interactive distante ouverte sur l'hôte distant administré est dépourvue de condensat NTLM ou de TGT Kerberos de l'utilisateur stockés en mémoire vive. Localement sur l'hôte distant administré, cette limitation est invisible pour l'administrateur puisque le contexte utilisateur local est bien celui du compte de domaine AD de l'administrateur avec ses droits et privilèges. Mais depuis l'hôte distant administré, il n'est en revanche plus possible de se connecter à d'autres ressources de l'AD dans le contexte du compte du domaine AD de l'administrateur, car sans condensat NTLM ni TGT Kerberos, il ne peut plus réaliser d'authentifications réseau (cf. section 4.1). Les connexions réseau aux autres ressources de l'AD depuis l'hôte distant administré par RDP RA se font dans le contexte du compte d'ordinateur de ce dernier dans l'AD. Il est donc toujours possible de se connecter à d'autres ressources de l'AD depuis l'hôte distant administré par RDP RA, mais cela implique d'octroyer des droits sur ces ressources au profit du compte d'ordinateur de cet hôte en remplacement des droits initialement octroyés au compte utilisateur AD de l'administrateur.

L'administration d'un hôte distant par RDP RA est par conséquent transparente pour un administrateur tant qu'elle consiste à réaliser des actions d'actions d'administration uniquement sur cet hôte. En revanche, si les actions d'administration nécessitent de se connecter à d'autres ressources de l'AD par authentification réseau depuis cet hôte, alors cela implique de passer en revue tous les droits d'accès nécessaires sur ces ressources et de les adapter en conséquence. Cela est toutefois sain d'un point de vue de sécurité puisque cette opération nécessite de clairement identifier quels accès sur le réseau sont nécessaires dans le cadre de l'administration distante d'un hôte en particulier.

Exemple

Le compte « `DOMAINE\jean` » ouvre une session RDP RA vers la machine « `DOMAINE\APPServer` » pour y réaliser des actions d'administration. Depuis cette dernière il accède au partage de fichiers « \\FileServer\Partage » du serveur « `DOMAINE\FileServer` ». Du point de vue du serveur « `DOMAINE\FileServer` » il n'est pas vu comme ayant l'identité « `DOMAINE\jean` » mais comme ayant l'identité « `DOMAINE\APPServer$` ». (le compte d'ordinateur de « `DOMAINE\APPServer` » dans l'AD).

Pour continuer d'accéder à ce partage de fichiers à travers la session RDP RA, il faut donc que les droits sur ce partage aient été octroyés à « `DOMAINE\APPServer$` » (ou à un groupe utilisateurs de l'AD dont il est membre) en remplacement des droits initialement octroyés à « `DOMAINE\jean` » (ou à un groupe utilisateur dont il est membre).

Les figures 14 et 15 illustrent les droits d'accès octroyés sur un partage de fichiers pour y accéder à travers une session RDP sans ou avec utilisation de l'option *Restricted Admin*.

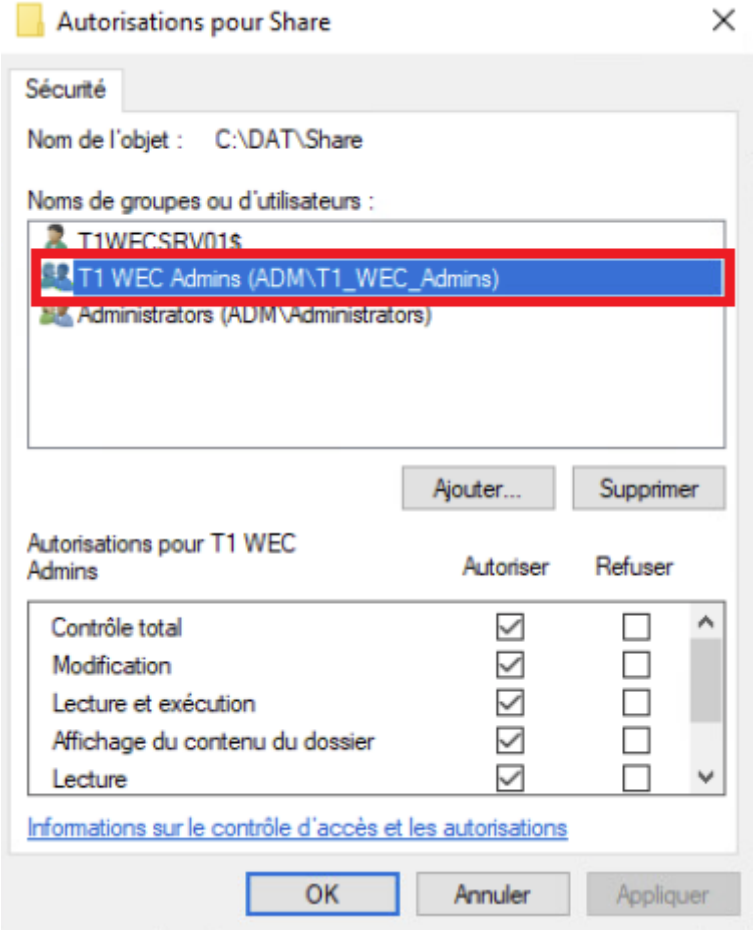

FIGURE 14 – Exemple de droits octroyés, sur un partage de fichiers, à un groupe d'administrateurs et qui y accèdent dans le cadre d'actions d'administration réalisées à travers une session RDP sans l'option *Restricted Admin*.

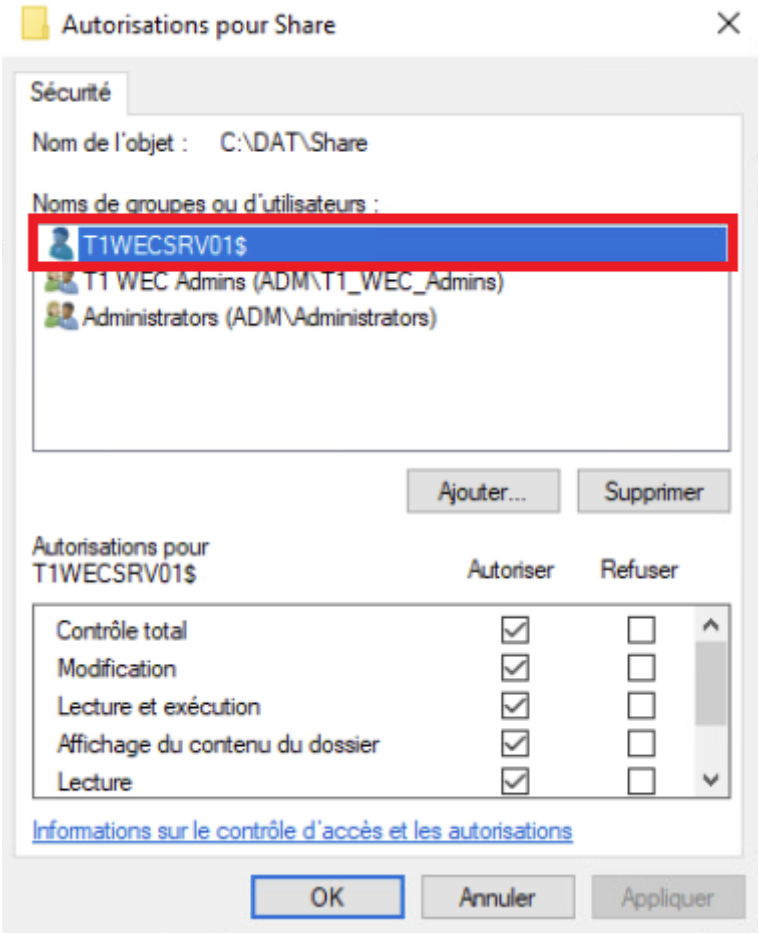

FIGURE 15 – Exemple de droits octroyés, sur un partage de fichiers, à un compte d'ordinateur pour que des administrateurs puissent y accéder depuis cet ordinateur dans le cadre d'actions d'administration réalisées à travers une session RDP avec l'option *Restricted Admin*.

Information

Par défaut, l'interface graphique permettant de sélectionner les comptes auxquels octroyer des droits ne liste pas les comptes d'ordinateur. Lors de la recherche, il convient de préalablement cliquer sur « type d'objet » puis de cocher « des ordinateurs » comme illustré par la figure 16.

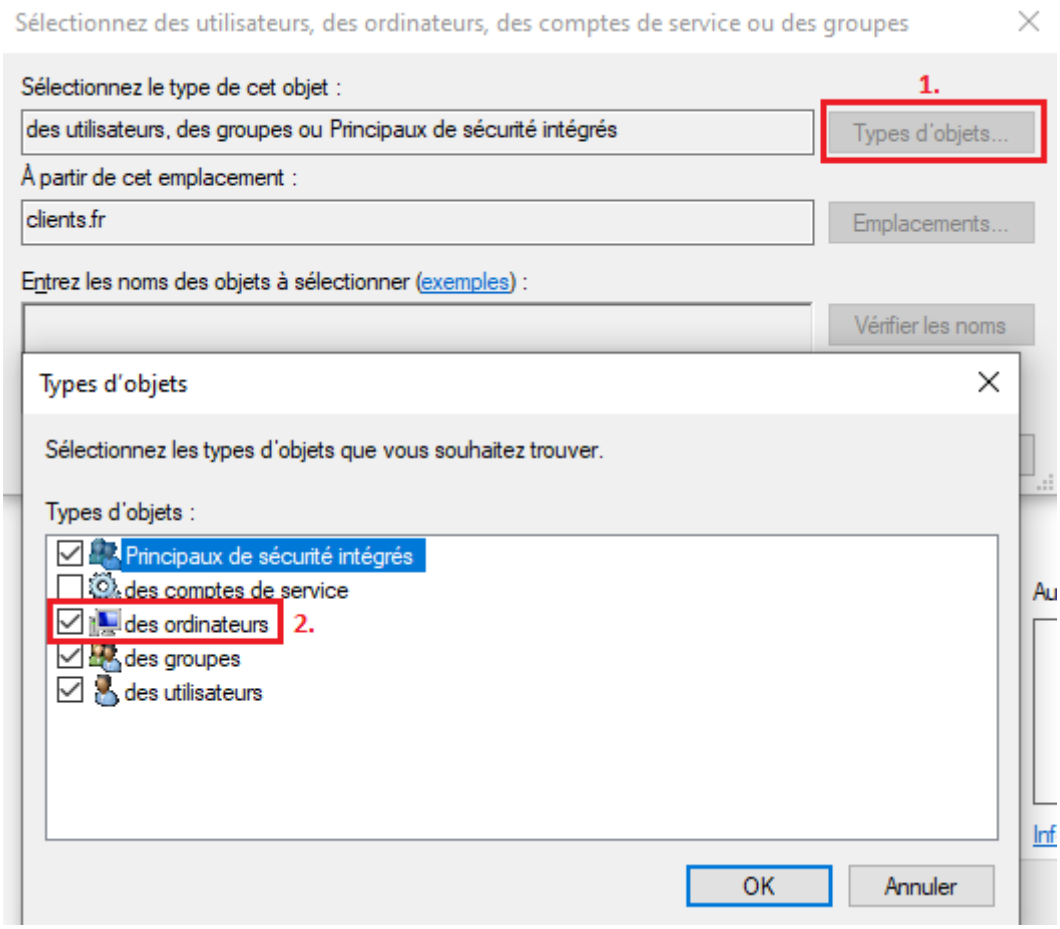

FIGURE 16 – Octroyer des droits à un compte d'ordinateur par interface graphique.

Attention

Les administrateurs qui administrent des ressources par RDP RA doivent être sensibilisés au fonctionnement et au bon usage de cette méthode d'administration. En l'occurrence, ils doivent être conscients qu'ils ne doivent ensuite saisir aucun secret d'authentification réutilisable (par la saisie d'un mot de passe généralement) au sein de la session RDP RA, sans quoi un attaquant ayant compromis l'hôte distant administré pourrait les récupérer par simple capture des frappes clavier virtuelles. Autrement dit, il est par exemple interdit d'effectuer un *RunAs* vers un compte de domaine dans une session RDP RA.

Information

RDP RA peut uniquement être utilisé pour de l'administration distante, ce qui implique que le compte utilisateur AD de l'administrateur doive être administrateur de l'hôte administré distant pour pouvoir y ouvrir une session RDA RA. RDP RA ne peut *a contrario* pas être utilisé pour un accès distant dans une session de simple utilisateur non privilégié sur l'hôte distant.

E.2 Mise en œuvre de RDP avec l'option Restricted Admin

L'utilisation de l'option *Restricted Admin* nécessite une configuration spécifique côté serveur (hôte distant administré par RDP) et côté client (poste d'administration). Ces configurations doivent être faites à la fois côté serveur et côté client pour permettre l'ouverture d'une session RDP RA.

Côté serveur, le paramètre de stratégie de sécurité indiqué par le listing 18 doit être configuré pour autoriser RDP RA. L'idéal est d'appliquer cette configuration à tous les ordinateurs de l'AD pour qu'ils supportent RDP RA.

```
Chemin : Configuration ordinateur\Modèles d'administration\Système\Délégation
        d'informations d'identification\L'hôte distant autorise la délégation d'informations
        d'identification non exportables : Activé
```

Listing 18 – Paramètre de stratégie de sécurité pour le support de *Restricted Admin* côté serveur

Information

Il est à noter que l'application de la stratégie 18 présente un inconvénient : après son application, il est désormais possible de s'authentifier en RDP par *pass-the-hash* (cf. section 4.3), ce qui n'est pas possible par défaut. Cet inconvénient doit toutefois être relativisé puisque :

1. sauf pour certains serveurs accessibles par des utilisateurs du *Tier 2*, les connexions RDP sont uniquement autorisées depuis des ressources d'administration ;
2. le cloisonnement logique du SI amène à traiter les risques de déplacement latéral ou d'élévation de privilèges réalisées par réutilisation de secrets d'authentification. Les mesures de protection restent donc les mêmes, que l'on considère les scenarii impliquant du *pass-the-hash* par RDP ou non.

Côté client, le paramètre de stratégie de sécurité indiqué par le listing 19 peut être configuré pour imposer l'option *Restricted Admin* au client RDP (binaire mstsc.exe).

```
Chemin : Configuration ordinateur\Modèles d'administration\Système\Délégation
        d'informations d'identification\Limiter la délégation d'informations d'identification à
        des serveurs distant : Activé avec pour valeur  "Requérir une administration restreinte"
```

Listing 19 – Paramètre de stratégie de sécurité pour imposer *Restricted Admin* côté client

L'option RDP RA côté client, si elle n'est pas imposée par le paramètre de sécurité du listing 19, peut être précisée à chaque exécution du client RDP à l'aide de l'argument « `/RestrictedAdmin` », ce qui revient à exécuter la commande `mstsc.exe /RestrictedAdmin` plutôt que d'utiliser le raccourci par défaut du client RDP dans le menu démarrer et intitulé « Connexion Bureau à distance ». Un administrateur pourrait par exemple avoir sur son bureau :

- un raccourci « Client RDP », exécutant la commande « `mstsc.exe` », pour établir des connexions RDP sans *Restricted Admin* (par exemple pour le déport d'affichage vers des serveurs du *Tier 0* depuis un poste d'administration du *Tier 0*) ;

- un raccourci « Client RDP RA », exécutant la commande « `mstsc.exe /RestrictedAdmin` », pour établir des connexions RDP avec l'option *Restricted Admin* vers les hôtes distants qui l'imposent (par exemple pour le déport d'affichage vers des serveurs du *Tier 1* depuis un poste d'administration du *Tier 0*).

Annexe F
Principes d'une forêt AD dédiée aux ressources obsolètes

Lorsque les SI de production ont un niveau de sécurité insuffisant (pour des raisons de compatibilité avec les applicatifs et ressources métiers, ou de mauvaise gouvernance accumulée au fil des ans notamment), ils sont alors rarement maintenus en conditions de sécurité satisfaisantes. Dans une telle situation, il est d'ailleurs fréquent que les règles d'hygiène des SI [6] les plus élémentaires ne soient pas correctement appliquées. Il est ainsi fréquent de constater par exemple que :

- la présence d'OS obsolètes perdure (Windows Serveur 2003 voire plus anciens), ce qui affaiblit le niveau de sécurité général ;
- les systèmes ne sont pas forcément maintenus à jour, les exposant à des vulnérabilités connues et donc bien souvent exploitées par les attaquants ;
- des protocoles obsolètes restent utilisés, tels que SMB1 qui a fait l'actualité en 2017 avec le rançongiciel « WannaCry » ;
- les niveaux fonctionnels AD ne sont pas mis à niveau (versions généralement antérieures à 2008 R2) ;
- le SI manque de maîtrise et le parc applicatif ainsi que les matrices de flux réseau et autres éléments d'inventaire et de cartographie sont obsolètes voire inexistants.

Dans ce cas, il peut être intéressant d'étudier la mise en œuvre d'une forêt dédiée aux ressources obsolètes (du strict point de vue de la SSI), dont le principe est similaire au concept de forêt de ressources surtout connu dans le cadre des architectures Microsoft Exchange.

L'idée générale est d'identifier les ressources qui sont un frein à l'amélioration du niveau de sécurité des forêts de production qui hébergent les valeurs métier du *Tier 1*, puis de les déplacer dans une forêt dédiée aux ressources obsolètes. En s'assurant que les forêts soient bien cloisonnées entre elles, le résultat est qu'une compromission de la forêt des ressources obsolètes ne débouche pas *de facto* sur une compromission de la forêt de production. C'est-à-dire qu'il y a une séparation des privilèges relativement similaire à ce qui devrait être mis en œuvre entre une forêt d'administration et des forêts de production. Il est notamment nécessaire de faire preuve de vigilance à l'égard de deux points d'attention principaux :

- un lien d'approbation entre les forêts permet généralement aux utilisateurs de la forêt de production de continuer à s'authentifier auprès des ressources obsolètes, et de les consommer de manière transparente. Ce lien d'approbation est généralement unidirectionnel et applique une restriction d'« authentification sélective » pour garantir le cloisonnement recherché. Pour s'af-

franchir d'un lien d'approbation, des solutions de fédération d'identité peuvent également être mises en œuvre ;

- la compromission de ces ressources obsolètes ne doit pas permettre une compromission triviale des utilisateurs qui s'y connectent, notamment via des vulnérabilités que pourraient présenter les applications clientes utilisées pour s'y connecter (par exemple : un client Web muni d'une version vulnérable du module complémentaire Java afin d'utiliser une application Web déplacée en forêt de ressources).

Cette segmentation logique de la forêt dédiée aux ressources obsolètes doit également s'accompagner d'un cloisonnement réseau pour réduire l'exposition de ces ressources obsolètes, mais surtout pour protéger le reste du SI vis-à-vis de l'éventuelle compromission de ces dernières.

La création de cette forêt de ressources obsolètes permet *in fine* d'améliorer le niveau de sécurité de la forêt de production, c'est-à-dire entre autres :

- ne plus avoir que des OS supportés et mis à jour ;
- ne plus utiliser de logiciels et protocoles obsolètes qui présentent des vulnérabilités connues mais non corrigées ;
- adopter les niveaux fonctionnels AD les plus récents ;
- pouvoir mettre en œuvre des mécanismes de sécurité récents tels que le groupe de sécurité des utilisateurs protégés (annexe B) ou les silos d'authentification (annexe C).

Enfin, il est possible de pousser le cloisonnement plus loin en cloisonnant les ressources obsolètes entre elles de sorte que la compromission de l'une n'entraine pas la compromission de toutes les autres. Un tel cloisonnement prend généralement la forme de plusieurs forêts de ressources.

Annexe G
Considérations de sécurité relatives à Microsoft Exchange

La recommandation R10 de réduction de l'exposition du *Tier 0* laisse penser que les serveurs Microsoft Exchange devraient idéalement être positionnés en *Tier 1* afin que le *Tier 0* soit allégé au maximum. En effet, un serveur de messagerie n'a *a priori* aucune raison d'être catégorisé en *Tier 0*. Qui plus est, il nécessite des actions d'administration courantes et ces dernières sont parfois sous-traitées dans le cadre de contrats de prestation de service.

Théoriquement, une installation de Microsoft Exchange à jour et qui respecte les bonnes pratiques de sécurité peut être catégorisée en *Tier 1* sans mettre en danger le *Tier 0*. Mais en réalité, les serveurs de boîte aux lettres (*mailbox servers*) de Microsoft Exchange peuvent présenter des chemins d'attaque vers le *Tier 0*. Cela dépend de plusieurs facteurs, incluant la version de Microsoft Exchange considérée ainsi que ses mises à jour cumulatives et de sécurité, le modèle d'autorisations appliqué [50], les délégations de droits mises en œuvre ou bien encore les mises à jour successives qui ont pu être faites de Microsoft Exchange depuis des versions antérieures. Cela dépend aussi beaucoup du SI et notamment du périmètre de son *Tier 0*.

G.1 Décomposition de l'administration de Microsoft Exchange

Certaines actions d'administration de Microsoft Exchange relèvent en réalité de la gestion de l'annuaire AD. C'est le cas par exemple de :

- la création d'utilisateurs ou de boîtes de messagerie dans Microsoft Exchange, qui requiert la création de principaux de sécurité [95] dans l'AD ;
- la configuration de l'appartenance à des groupes de sécurité, qui implique des opérations d'écriture sur des attributs d'objets de l'AD.

Les comptes de machine (c'est à dire les *computer accounts* dans l'AD) des serveurs de boîte aux lettres de Microsoft Exchange sont par défaut membres des groupes de sécurité universels hautement privilégiés `Exchange Trusted Subsystem` et `Exchange Windows Permissions`. Bien que ces derniers n'aient pas de droits en écriture sur les comptes et groupes protégés de l'AD [81] (listés en annexe A), ils peuvent dans certains cas présenter des chemins d'élévation de privilèges vers le *Tier 0* puisque :

50. Le lecteur est invité à lire les articles de Microsoft [60] et [62] pour une bonne compréhension des modèles d'autorisations de Microsoft Exchange depuis la version 2010.

- les droits qui leurs sont par défaut octroyés sur l'annuaire AD peuvent présenter des relations de contrôle AD vers le *Tier 0* malgré les restrictions qui existent sur les comptes et groupes protégés de l'AD (le dépôt GitHub [40] en donne quelques exemples). Pour adresser ces problèmes de relations de contrôle AD vers le *Tier 0*, Microsoft publie des correctifs et mises à jour [51]. Plus un serveur de boîte aux lettres de Microsoft Exchange est à jour, moins il présente donc de chemins de contrôle AD vers le *Tier 0* ;
- le *Tier 0* identifié en chapitre 3 ne se limite pas toujours aux comptes et groupes protégés de l'AD [81]. Les différents chemins d'attaque du *Tier 0* abordés en chapitre 3 illustrent ce constat. D'un SI à l'autre, un serveur de boîte aux lettres de Microsoft Exchange peut donc présenter plus ou moins de chemins d'élévation de privilèges vers le *Tier 0*.

Par défaut, lorsque des actions d'administration qui relèvent de l'annuaire AD sont menées depuis les outils d'administration de Microsoft Exchange [52], ces actions sont en réalité exécutées dans le contexte du groupe `Exchange Trusted Subsystem` et non pas dans le contexte du compte utilisateur qui réalise l'action (cf. article [62]). Cela rend ces actions d'administration possibles par des administrateurs de la messagerie Microsoft Exchange qui ne sont par ailleurs que de simples utilisateurs du domaine AD sans droits ni privilèges particuliers.

Pour être plus précis, les utilisateurs de Microsoft Exchange qui obtiennent la possibilité de mener des actions d'administration sensibles sur l'annuaire AD sont les utilisateurs s'étant par exemple vus octroyer un des rôles privilégiés suivants du modèle RBAC [61] de Microsoft Exchange :

- *Active Directory Permissions* ;
- *Security Group Creation and Membership* ;
- *Mail Recipient Creation*.

Ces rôles privilégiés peuvent être avoir été affectés directement aux utilisateurs ou par l'intermédiaire de groupes de rôles tels que « *Organization Management* » ou « *Recipient Management* ».

G.2 Les modèles d'autorisations de Microsoft Exchange

La problématique de catégorisation des serveurs de boîte aux lettres Microsoft Exchange en *Tier 0* ou en *Tier 1* repose en grande partie sur la séparation des actions d'administration qui relèvent de l'annuaire AD de celles qui relèvent de la messagerie Microsoft Exchange à proprement parler. Cette séparation dépend du modèle d'autorisations retenu et des délégations de droits mises en œuvre.

G.2.1 Modèle d'autorisations shared permissions

Le modèle de *shared Permissions* est le modèle par défaut utilisé par la grande majorité des installations de Microsoft Exchange.

51. La mise à jour cumulative de Microsoft Exchange de Juin 2019 [59] interdit par exemple aux comptes de machine des serveurs de boîte aux lettres Microsoft Exchange la modification du groupe de sécurité « `DNS Admins` » de l'AD (voir tableau A.2) et leur interdit l'assignation de SPN (voir section 4.13).

52. C.-à-d. l'environnement de commande *Exchange management shell* ou bien la console *Exchange admin center* d'administration par interface graphique.

Lorsque ce modèle d'autorisations est utilisé, les comptes de machine des serveurs de boîte aux lettres de Microsoft Exchange sont membres des groupes universels hautement privilégiés `Exchange Trusted Subsystem` et `Exchange Windows Permissions`. Dans ce cas et comme expliqué en section G.1, la compromission d'un serveur de boîte aux lettres de Microsoft Exchange par un attaquant pourrait aboutir à la compromission du *Tier 0*.

Avec ce modèle d'autorisations, il n'y a aucune séparation entre les actions d'administration qui relèvent de l'annuaire AD et celles qui relèvent de la messagerie Microsoft Exchange à proprement parler. C'est-à-dire qu'un administrateur s'étant vu octroyer un des rôles privilégiés de Microsoft Exchange obtient la possibilité de mener des actions d'administration sur l'annuaire AD dans le contexte du groupe `Exchange Trusted Subsystem`. Par ce biais, il peut éventuellement obtenir une capacité d'élévation de privilèges vers le *Tier 0*. En revanche, les autres administrateurs de Microsoft Exchange peuvent tout à fait être catégorisés en *Tier 1* ou en *Tier 2* si aucun rôle privilégié ne leur est octroyé.

Les serveurs de boîte aux lettres de Microsoft Exchange sont donc des ressources du SI qui pourraient être catégorisées en *Tier 0* en fonction du contexte. Mais dans ce cas, il reste raisonnable d'en déléguer l'administration par RBAC [61] (à l'exception des rôles privilégiés de Microsoft Exchange) à des administrateurs du *Tier 1* ou du *Tier 2*.

G.2.2 Modèle d'autorisations AD split permissions

Lorsque le modèle utilisé est l'*Active Directory split permissions* [60], il y a dans ce cas une réelle séparation entre les actions d'administration qui relèvent de l'annuaire AD et celles qui relèvent de la messagerie Microsoft Exchange à proprement parler. Les serveurs Microsoft Exchange ne sont plus membres des groupes universels hautement privilégiés `Exchange Trusted Subsystem` et `Exchange Windows Permissions`. De ce fait, la compromission d'un serveur de boîte aux lettres de Microsoft Exchange par un attaquant ne nuit pas à la sécurité du *Tier 0* ; ils peuvent donc être catégorisés en *Tier 1* sans présenter une menace potentielle pour le *Tier 0*.

D'autre part, les actions d'administration qui relèvent de l'annuaire AD ne sont plus possibles depuis les outils d'administration de Microsoft Exchange et elles doivent être réalisées par des administrateurs ayant les droits adéquats sur l'annuaire AD (par PowerShell ou à l'aide de la console MMC « `Utilisateurs et Ordinateurs Active Directory` », entre autres). Ces derniers peuvent par exemple être des administrateurs du *Tier 1* ou du *Tier 2* qui ont les délégations de droits adéquates sur l'annuaire AD.

Avec ce modèle, il appartient donc à l'organisation de déléguer :

- à certains administrateurs du *Tier 1*, les droits et privilèges nécessaires à l'administration système des serveurs de l'infrastructure Microsoft Exchange ;
- à certains administrateurs du *Tier 1* ou du *Tier 2*, des autorisations d'administration de la messagerie Microsoft Exchange à proprement parler, par RBAC [61] ;
- à certains administrateurs du *Tier 1* ou du *Tier 2*, les droits sur des objets de l'annuaire AD du *Tier 1* ou du *Tier 2* leur permettant de réaliser les actions d'administration complémentaires qui ne relèvent pas de Microsoft Exchange, telles que celles consistant à gérer les appartenances à des groupes de sécurité (car le rôle *Security Group Creation and Membership* de Microsoft Exchange n'est dans ce cas plus utilisable).

Ces délégations de droits doivent toujours se faire en respectant le principe de cloisonnement des *Tiers*. Bien que ce modèle d'autorisations soit recommandé en termes de sécurité, il est toutefois peu utilisé car :

- il est plus complexe à mettre en œuvre ;
- une certaine maturité SSI est nécessaire pour justifier son adoption ;
- l'administration de la messagerie Microsoft Exchange devient moins aisée au quotidien.

G.2.3 Modèle d'autorisations RBAC split permissions

Le modèle *RBAC split permissions* est, de manière peu intuitive, plus proche du modèle de *shared permissions* que du modèle *AD split permissions*.

En effet, comme en *shared permissions*, le modèle d'autorisations *RBAC split permissions* repose lui aussi sur les groupes de sécurité universels hautement privilégiés que sont l'`Exchange Trusted Subsystem` et l'`Exchange Windows Permissions`. En revanche, dans ce modèle, un processus manuel détaillé dans l'article [62] consiste globalement à :

- ôter les droits AD sensibles des rôles RBAC prédéfinis de Microsoft Exchange [61] ;
- créer un nouveau rôle RBAC de Microsoft Exchange qui sera le seul à permettre les actions d'administration sensibles qui relèvent du *Tier 0* de l'AD (*Security Group Creation and Membership* par exemple).

De cette manière, les membres des rôles RBAC par défaut de Microsoft Exchange ne sont plus en mesure de réaliser des élévations de privilèges vers le *Tier 0* par ce biais. Seuls les membres du nouveau rôle RBAC peuvent dans ce cas être considérés comme administrateurs du *Tier 0*. Ce modèle permet une séparation des usages entre l'administration AD et l'administration Exchange avec une frontière de sécurité nette entre les deux. Mais comme dans le cas du modèle de *shared permissions*, la compromission d'un serveur de boîte aux lettres de Microsoft Exchange par un attaquant pourrait éventuellement aboutir à la compromission du *Tier 0*.

G.3 Mises à jour depuis des versions antérieures à Microsoft Exchange 2010

Les mises à jour successives d'une version majeure de Microsoft Exchange à l'autre peuvent avoir pour résultat que le groupe `Exchange Trusted Subsystem` dispose de droits plus étendus que lors d'une nouvelle installation. Cette persistance d'anciens droits inappropriés augmente la probabilité de prise de contrôle du *Tier 0* par le biais des comptes de machine des serveurs de boîte aux lettres de Microsoft Exchange.

G.4 Conclusions de catégorisation

Il n'est au final pas surprenant que les experts en SSI placent alternativement l'infrastructure Microsoft Exchange en *Tier 1* ou en *Tier 0* en fonction du contexte et des différents critères évoqués dans cette annexe. Ceci illustre à quel point la catégorisation de certaines ressources du SI peut

s'avérer complexe, nécessitant parfois de profonds changements pour aboutir à un cloisonnement pertinent.

Par ailleurs et au delà des chemins d'élévation de privilèges vers le *Tier 0*, se pose également la question de l'étendue des privilèges délégués par RBAC aux administrateurs de *Tier 1* de Microsoft Exchange. Certains rôles (*Hygiene Management* ou *Recipients Management* par exemple) permettent la prise de contrôle de boîtes aux lettres, d'autres permettent des recherches étendues sur l'ensemble des boîtes, la configuration de transferts de courriels automatiques, etc. Sans être de *Tier 0*, ces rôles sont donc souvent sensibles pour une organisation et leur délégation à des administrateurs de *Tier 1* ou de *Tier 2* doit se faire de manière réfléchie.

Annexe H
Liste des acronymes

Acronyme	Désignation
ACL	Access Control List
AD	Active Directory
AD CS	Active Directory Certificate Services
AD DS	Active Directory Domain Services
ADFS	Active Directory Federation Services
AD IFM	Active Directory Install From Media
AES	Advanced Encryption Standard
API	Application Programming Interface
COM	Component Object Model
CVE	Common Vulnerabilities and Exposures
DC	Domain Controller
DES	Data Encryption Standard
DFL	Domain Functional Level
DFRS	Distributed File System Replication
DFS	Distributed File System
DMA	Direct Memory Access
DNS	Domain Name System
DPAPI	Data Protection Application Programming Interface
DSA	Digital Signature Algorithm
DSRM	Directory Services Restore Mode
EBIOS	Expression des Besoins et Identification des Objectifs de Sécurité
ECDSA	Elliptic Curve Digital Signature Algorithm
FFL	Forest Functional Level
FQDN	Fully Qualified Domain Name
GMSA	Group Managed Service Account
GPO	Group Policy Object

Ce tableau se poursuit sur la page suivante

Acronyme	Désignation
GPP	Group Policy of Preferences
ESAE	Enhanced Security Administrative Environment
HSM	Hardware Security Module
HTTP	HyperText Transfer Protocol
IGC	Infrastructure de Gestion de Clés (cf. PKI)
IOMMU	Input-Output Memory Management Unit
IPMI	Intelligent Platform Management Interface
IPSec	Internet Protocol Security
JEA	Just Enough Administration
KDC	Kerberos Distribution Center
KCD	Kerberos Constrained Delegation
KUD	Kerberos Unconstrained Delegation
KVM	Keyboard, Video, Mouse
LAN	Local Area Network
LAPS	Local Administrator Password Solution
LDAP	Lightweight Directory Access Protocol
LSA	Local Security Authority
MITM	Man In The Middle
MSA	Managed Service Account
MCS	Maintien en Conditions de Sécurité
MMC	Microsoft Management Console
NAS	Network Attached Storage
NTFS	New Technology File System
NTLM	New Technology LAN Manager
OIV	Opérateur d'Importance Vitale
OS	Operating System
OU	Organizational Unit
PAM	Privileged Access Management
PKI	Public Key Infrastructure
PKINIT	Public Key cryptography for INITial Authentication
PIM	Privileged Identity Management
PSO	Password Settings Objects
RBAC	Role Based Access Control

Ce tableau se poursuit sur la page suivante

Acronyme	Désignation
RBCD	Ressource Based Constrained Delegation
RDP	Remote Desktop Protocol
RID	Relative IDentifier
RODC	Read Only Domain Controller
RPC	Remote Procedure Call
RSAT	Remote System Administration Tools
SAN	Storage Area Network
SHA	Secure Hash Algorithm
SI	Système d'Information
SID	Security IDentifier
SIIV	Système d'Information d'Importance Vitale
SMB	Simple Message Block
SPN	Service Principal Name
SSI	Sécurité des Systèmes d'Information
TDO	Trusted Domain Object
TGT	Ticket Granting Ticket
TGS	Ticket Granting Service
TLS	Transport Layer Security
TPM	Trusted Platform Module
UEFI	Unified Extensible Firmware Interface
UNC	Universal Naming Conventio
VLAN	Virtual Local Area Network
VM	Virtual Machine
VPN	Virtual Private Network
WBEM	Web-Based Enterprise Management
WDAC	Windows Defender Application Control
WDCG	Windows Defender Credential Guard
WDRCG	Windows Defender Remote Credential Guard
WINRM	WINdows Remote Management
WSUS	Windows Server Update Services
XML	eXtensible Markup Language

Tableau 5 – Liste des acronymes utilisés dans le document

Liste des recommandations

Bibliographie

[1] *ADTimeLine*.
Git-hub, ANSSI.
https://github.com/ANSSI-FR/ADTimeline.

[2] *Recommandations de sécurité relatives aux mots de passe*.
Note technique DAT-NT-001/ANSSI/SDE/NP v1.1, ANSSI, juin 2012.
https://www.ssi.gouv.fr/mots-de-passe.

[3] *Mise en œuvre des fonctionnalités de sécurité de Windows 10 reposant sur la virtualisation*.
Guide ANSSI-BP-039 v1.0, ANSSI, novembre 2017.
https://www.ssi.gouv.fr/windows10-vsm.

[4] *Corpus documentaire sur la remédiation*.
Technical report, ANSSI, juin 2023.
https://www.ssi.gouv.fr/actualite/lanssi-publie-pour-appel-a-commentaires-un-corpus-documentaire-sur-la-remediation/.

[5] *Maîtriser les risques de l'infogérance. Externalisation des systèmes d'information*.
Guide Version 1.0, ANSSI, décembre 2010.
https://www.ssi.gouv.fr/infogerance.

[6] *Guide d'hygiène informatique : renforcer la sécurité de son système d'information en 42 mesures*.
Guide ANSSI-GP-042 v2.0, ANSSI, septembre 2017.
https://www.ssi.gouv.fr/hygiene-informatique.

[7] *La défense en profondeur appliquée aux systèmes d'information*.
Guide Version 1.1, ANSSI, juillet 2004.
https://www.ssi.gouv.fr/defense-profondeur.

[8] *Recommandations de sécurité relatives à IPsec pour la protection des flux réseau*.
Note technique DAT-NT-003/ANSSI/SDE/NP v1.1, ANSSI, août 2015.
https://www.ssi.gouv.fr/ipsec.

[9] *Cartographie du système d'information*.
Guide ANSSI-PA-046 v1.0, ANSSI, octobre 2018.
https://www.ssi.gouv.fr/administration/guide/cartographie-du-systeme-dinformation.

[10] *La méthode EBIOS Risk Manager - Le Guide*.
Guide ANSSI-PA-048 v1.0, ANSSI, octobre 2018.
https://www.ssi.gouv.fr/guide/la-methode-ebios-risk-manager-le-guide.

[11] *Recommandations sur le nomadisme numérique*.
Guide ANSSI-PA-054 v1.0, ANSSI, octobre 2018.
https://ssi.gouv.fr/nomadisme-numerique.

[12] *Maîtrise du risque numérique - l'atout confiance*.
Guide ANSSI-PA-070 v1.0, ANSSI, novembre 2019.
https://www.ssi.gouv.fr/administration/guide/maitrise-du-risque-numerique-latout-confiance.

[13] *Recommandations de sécurité relatives à TLS*.
Guide ANSSI-PA-035 v1.2, ANSSI, mars 2020.
https://www.ssi.gouv.fr/nt-tls.

[14] *Recommandations pour la protection des systèmes d'information essentiels*.
Guide ANSSI-PA-085 v1.0, ANSSI, décembre 2020.
https://www.ssi.gouv.fr/guide/recommandations-pour-la-protection-des-systemes-dinformation-essentiels.

[15] *Recommandations sur la sécurisation des systèmes de contrôle d'accès physique et de vidéoprotection*.
Guide ANSSI-PA-072 v2.0, ANSSI, mars 2020.
https://www.ssi.gouv.fr/controle-acces-videoprotection.

[16] *Recommandations relatives à l'administration sécurisée des systèmes d'information*.
Guide ANSSI-PA-022 v3.0, ANSSI, mai 2021.
https://www.ssi.gouv.fr/securisation-admin-si.

[17] *Recommandations de sécurité pour l'architecture d'un système de journalisation*.
Guide DAT-PA-012 v2.0, ANSSI, janvier 2022.
https://www.ssi.gouv.fr/journalisation.

[18] *Recommandations de sécurité pour la journalisation des systèmes Microsoft Windows en environnement Active Directory*.
Guide ANSSI-PB-090 v1.0, ANSSI, janvier 2022.
https://www.ssi.gouv.fr/journalisation-windows.

[19] *Référentiel général de sécurité (RGS)*.
Référentiel Version 2.0, ANSSI, juin 2012.
https://www.ssi.gouv.fr/rgs.

[20] *RGS Annexe B2 : Règles et recommandations concernant la gestion des clés utilisées dans les mécanismes cryptographiques*.
Référentiel Version 2.0, ANSSI, juin 2012.
https://www.ssi.gouv.fr/rgs.

[21] *Instruction interministérielle n°901*.
Référentiel Version 1.0, ANSSI, janvier 2015.
https://www.ssi.gouv.fr/ii901.

[22] *Instruction générale interministérielle n°1300*.
Référentiel, SGDSN, août 2021.
https://www.ssi.gouv.fr/igi1300.

[23] *Alerte : multiples vulnérabilités dans des processeurs - comprendre meltdown et spectre et leur impact*.
Technical report, ANSSI, 2018.

https://www.ssi.gouv.fr/entreprise/actualite/alerte-multiples-vulnerabilites-dans-des-processeurs-comprendre-meltdown-et-spectre-et-leur-impact/.

[24] *Traitement d'un incident de sécurité : quels métiers, quelles fonctions ?*
Technical report, ANSSI, juin 2017.
https://www.ssi.gouv.fr/actualite/traitement-dun-incident-de-securite-quels-metiers-quelles-fonctions/.

[25] *Certification CSPN*.
Page Web Version 1.0, ANSSI, mars 2016.
https://www.ssi.gouv.fr/cspn.

[26] *Visa de sécurité*.
Page Web Version 1.0, ANSSI, 2018.
https://www.ssi.gouv.fr/administration/visa-de-securite.

[27] *Active Directory Security (ADS)*.
Page Web Version 1.0, ANSSI, 2020.
https://www.ssi.gouv.fr/actualite/le-service-active-directory-security-ads-accompagner-la-securisation-des-annuaires-active-directory-des-acteurs-critiques/.

[28] *BloodHound*.
Git-hub, BLOODHOUND.
https://github.com/BloodHoundAD/BloodHound.

[29] *Secrets d'authentification épisode II - Kerberos contre-attaque*.
Aurélien Bordes.
Publication scientifique, SSTIC, 2014.
https://www.ssi.gouv.fr/publication/secrets-dauthentification-episode-ii-kerberos-contre-attaque/.

[30] *L'administration en silo*.
Aurélien Bordes.
Publication scientifique, SSTIC, 2017.
https://www.sstic.org/media/SSTIC2017/SSTIC-actes/administration_en_silo/SSTIC2017-Article-administration_en_silo-bordes.pdf.

[31] *Alerte CERTFR-2018-ALE-001 - Multiples vulnérabilités de fuite d'informations dans des processeurs*.
Technical report, CERT-FR, janvier 2018.
https://cert.ssi.gouv.fr/alerte/CERTFR-2018-ALE-001/.

[32] *Centre national de prévention et de protection (CNPP)*.
Technical report, CNPP.
https://www.cnpp.com/.

[33] *CVE-2020-1472 - Vulnérabilité d'élévation de privilèges dans NetLogon*.
Avis de sécurité, Microsoft, 2021.
https://msrc.microsoft.com/update-guide/fr-FR/vulnerability/CVE-2020-1472.

[34] *CVE-2021-34527 - Windows Print Spooler Remote Code Execution Vulnerability*.
Avis de sécurité, Microsoft, juillet 2021.
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527.

[35] *CVE-2021-40469 - Windows DNS Server Remote Code Execution Vulnerability*.
Avis de sécurité, Microsoft, octobre 2021.
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-40469.

[36] *CVE-2022-21990 - Remote Desktop Client Remote Code Execution Vulnerability*.
Avis de sécurité, Microsoft, mai 2022.
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21990.

[37] *CVE-2022-23285 - Remote Desktop Client Remote Code Execution Vulnerability*.
Avis de sécurité, Microsoft, mai 2022.
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-23285.

[38] *Alerte CERTFR-2017-ALE-015 - Vulnérabilités dans la bibliothèque Infineon RSA*.
Technical report, CERT-FR, octobre 2017.
https://cert.ssi.gouv.fr/alerte/CERTFR-2017-ALE-015/.

[39] *Chemins de contrôle en environnement Active Directory*.
Lucas Bouillot et Emmanuel Gras.
Publication scientifique, SSTIC, 2014.
https://www.ssi.gouv.fr/agence/publication/chemins-de-controle-en-environnement-active-directory-chacun-son-root-chacun-son-chemin/.

[40] *Exchange-AD-Privesc*.
Git-hub, Géraud de Drouas.
https://github.com/gdedrouas/Exchange-AD-Privesc.

[41] *Licence ouverte / Open Licence v2.0*.
Page web, Mission Etalab, avril 2017.
https://www.etalab.gouv.fr/licence-ouverte-open-licence.

[42] *Enterprise Key Admins group full control remediation PowerShell script*.
Git-hub, Michael Frommhold @ Microsoft.
https://github.com/ANSSI-FR/guide-admin-microsoft/EnterpriseKeyAdminsRemediation.ps1.

[43] *CVE-2017-0163 - Hyper-V Remote Code Execution Vulnerability*.
Avis de sécurité, Microsoft, novembre 2017.
https://msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0163.

[44] *Local Administrator Password Solution (LAPS)*.
Microsoft download center, Microsoft.
https://www.microsoft.com/en-us/download/details.aspx?id=46899.

[45] *Mitigating Pass-the-Hash Attacks and Other Credential Theft, versions 1 and 2 (anglais)*.
Microsoft download center, Microsoft.
https://microsoft.com/en-us/download/details.aspx?id=36036.

[46] *Attributes (AD Schema)*.
Microsoft learn, Microsoft.
https://learn.microsoft.com/en-us/windows/win32/adschema/attributes.

[47] *Delegating Administration by Using OU Objects*.
Microsoft learn, Microsoft.
https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/delegating-administration-by-using-ou-objects.

[48] *ADSI Edit (adsiedit.msc)*.
Microsoft learn, Microsoft.
https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc773354(v=ws.10).

[49] *What Are Domains and Forests ? Components of the Logical Structure*.
Microsoft learn, Microsoft.
https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc759073(v=ws.10)#components-of-the-logical-structure.

[50] *What's New in AD DS : Active Directory Web Services*.
Microsoft learn, Microsoft.
https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/dd391908(v=ws.10).

[51] *Password Encryption in Preferences Policy File Format*.
Microsoft learn, Microsoft.
https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-gppref/2c15cbf0-f086-4c74-8b70-1f2fa45dd4be.

[52] *AppLocker*.
Microsoft learn, Microsoft.
https://learn.microsoft.com/fr-fr/windows/security/threat-protection/windows-defender-application-control/applocker/applocker-overview.

[53] *Protect derived domain credentials with Windows Defender Credential Guard*.
Microsoft learn, Microsoft.
https://learn.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard.

[54] *Windows Defender Credential Guard requirements*.
Microsoft learn, Microsoft.
https://learn.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard-requirements.

[55] *Default local system accounts*.
Microsoft learn, Microsoft.
https://learn.microsoft.com/en-us/windows/security/identity-protection/access-control/local-accounts#default-local-system-accounts.

[56] *dSHeuristics*.
Microsoft learn, Microsoft.
https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-adts/e5899be4-862e-496f-9a38-33950617d2c5.

[57] *How to reset the Directory Services Restore Mode administrator account password in Windows Server*.

Microsoft learn, Microsoft.
https://learn.microsoft.com/en-us/troubleshoot/windows-server/identity/reset-directory-services-restore-mode-admin-pwd.

[58] *Enhanced Security Admin Environment retirement*.
Microsoft learn, Microsoft.
https://learn.microsoft.com/en-us/security/compass/esae-retirement.

[59] *Released : June 2019 Quarterly Exchange Updates*.
Microsoft tech community, Microsoft, juin 2019.
https://techcommunity.microsoft.com/t5/exchange-team-blog/released-june-2019-quarterly-exchange-updates/ba-p/698398.

[60] *Présentation des autorisations Exchange fractionnées*.
Microsoft learn, Microsoft.
https://learn.microsoft.com/fr-fr/exchange/understanding-split-permissions-exchange-2013-help.

[61] *Autorisations dans Exchange 2013*.
Microsoft learn, Microsoft.
https://learn.microsoft.com/fr-fr/exchange/permissions-exchange-2013-help.

[62] *Configurer Exchange 2013 pour les autorisations divisées*.
Microsoft learn, Microsoft.
https://learn.microsoft.com/fr-fr/exchange/configure-exchange-2013-for-split-permissions-exchange-2013-help.

[63] *Matrice de support d'Exchange Server*.
Microsoft learn, Microsoft.
https://learn.microsoft.com/fr-fr/exchange/plan-and-deploy/supportability-matrix?view=exchserver-2019.

[64] *Niveaux fonctionnels de domaine et de forêt*.
Microsoft learn, Microsoft.
https://learn.microsoft.com/fr-fr/windows-server/identity/ad-ds/active-directory-functional-levels.

[65] *Group Policy for Beginners*.
Microsoft learn, Microsoft.
https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-7/hh147307(v=ws.10).

[66] *Set-GPInheritance*.
Microsoft learn, Microsoft.
https://learn.microsoft.com/en-us/powershell/module/grouppolicy/set-gpinheritance?view=windowsserver2022-ps.

[67] *MS15-011, Configuring UNC Hardened Access through Group Policy*.
Avis de sécurité, Microsoft.
http://support.microsoft.com/kb/3000483.

[68] *IIS Extended Protection for Authentication*.
Avis de sécurité, Microsoft.
https://msrc.microsoft.com/blog/2009/12/extended-protection-for-authentication/.

[69] *Impersonation*.
Microsoft learn, Microsoft.
https://learn.microsoft.com/en-us/windows/win32/com/impersonation.

[70] *Just Enough Administration*.
Microsoft learn, Microsoft.
http://aka.ms/JEAdocs.

[71] *Kerberos Explained*.
Microsoft learn, Microsoft.
https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/bb742516(v=technet.10).

[72] *Windows Configurations for Kerberos Supported Encryption Type*.
Microsoft learn, Microsoft.
https://learn.microsoft.com/en-us/archive/blogs/openspecification/windows-configurations-for-kerberos-supported-encryption-type.

[73] *Decrypting the Selection of Supported Kerberos Encryption Types*.
Microsoft tech community, Microsoft, septembre 2020.
https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/decrypting-the-selection-of-supported-kerberos-encryption-types/ba-p/1628797.

[74] *2020 LDAP channel binding and LDAP signing requirements for Windows (KB4520412)*.
Support, Microsoft.
https://support.microsoft.com/kb/4520412.

[75] *Administrative tools and logon types*.
Microsoft learn, Microsoft.
https://learn.microsoft.com/en-us/windows-server/identity/securing-privileged-access/reference-tools-logon-types.

[76] *Configuring Additional LSA Protection*.
Microsoft learn, Microsoft.
https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn408187(v=ws.11).

[77] *Référence des règles de réduction de la surface d'attaque (ASR) : bloquer le vol d'informations d'identification à partir du sous-système d'autorité de sécurité locale Windows*.
Microsoft learn, Microsoft.
https://learn.microsoft.com/fr-fr/microsoft-365/security/defender-endpoint/attack-surface-reduction-rules-reference?view=o365-worldwide#block-credential-stealing-from-the-windows-local-security-authority-subsystem.

[78] *What is Microsoft Management Console ?*
Microsoft learn, Microsoft.
https://learn.microsoft.com/en-us/troubleshoot/windows-server/system-management-components/what-is-Microsoft-management-console.

[79] *Service Accounts*.
Microsoft learn, Microsoft.
https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn617203(v%3Dws.11).

[80] *Interactive logon : Number of previous logons to cache (in case domain controller is not available)*.
Microsoft learn, Microsoft.
https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/interactive-logon-number-of-previous-logons-to-cache-in-case-domain-controller-is-not-available.

[81] *Protected Accounts and Groups in Active Directory*.
Microsoft learn, Microsoft.
https://learn.microsoft.com/fr-fr/windows-server/identity/ad-ds/plan/security-best-practices/appendix-c--protected-accounts-and-groups-in-active-directory.

[82] *Enterprise access model*.
Microsoft learn, Microsoft.
https://learn.microsoft.com/en-us/security/privileged-access-workstations/privileged-access-access-model.

[83] *Évolution à partir du modèle de niveau AD hérité*.
Microsoft learn, Microsoft.
https://learn.microsoft.com/fr-fr/security/privileged-access-workstations/privileged-access-access-model#evolution-from-the-legacy-ad-tier-model.

[84] *Qu'est-ce que PowerShell ?*
Microsoft learn, Microsoft.
https://learn.microsoft.com/fr-fr/powershell/scripting/overview?view=powershell-7.2.

[85] *Groupe de sécurité utilisateurs protégés*.
Microsoft learn, Microsoft.
https://learn.microsoft.com/fr-fr/windows-server/security/credentials-protection-and-management/protected-users-security-group.

[86] *AD DS : Fine-Grained Password Policies*.
Microsoft learn, Microsoft.
https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc770394(v=ws.10).

[87] *Protect Remote Desktop credentials with Windows Defender Remote Credential Guard*.
Microsoft learn, Microsoft.
https://learn.microsoft.com/en-us/windows/security/identity-protection/remote-credential-guard.

[88] *Remote Credential Guard requirements*.
Microsoft learn, Microsoft.
https://learn.microsoft.com/en-us/windows/security/identity-protection/remote-credential-guard#remote-credential-guard-requirements.

[89] *AD Forest Recovery - Resetting the krbtgt password*.
Microsoft learn, Microsoft.
https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/ad-forest-recovery-resetting-the-krbtgt-password.

[90] *Comptes privilégiés et groupes dans Active Directory*.
Microsoft learn, Microsoft.
https://learn.microsoft.com/fr-fr/windows-server/identity/ad-ds/plan/security-best-practices/appendix-b--privileged-accounts-and-groups-in-active-directory.

[91] *Installer un contrôleur de domaine en lecture seule Active Directory Windows Server 2012*.
Microsoft learn, Microsoft.
https://learn.microsoft.com/fr-fr/windows-server/identity/ad-ds/deploy/rodc/install-a-windows-server-2012-active-directory-read-only-domain-controller--rodc---level-200-.

[92] *Outils d'administration de serveur distant*.
Microsoft learn, Microsoft.
https://learn.microsoft.com/fr-fr/windows-server/remote/remote-server-administration-tools.

[93] *Security baselines*.
Microsoft learn, Microsoft.
https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-security-configuration-framework/windows-security-baselines.

[94] *Making the second hop in PowerShell Remoting*.
Microsoft learn, Microsoft.
https://learn.microsoft.com/en-us/powershell/scripting/learn/remoting/ps-remoting-second-hop?view=powershell-7.3.

[95] *Principaux de sécurité*.
Microsoft learn, Microsoft.
https://learn.microsoft.com/fr-fr/windows-server/identity/ad-ds/manage/understand-security-principals.

[96] *Security Considerations for Trusts*.
Microsoft learn, Microsoft.
https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc755321(v=ws.10).

[97] *Vue d'ensemble de la structure protégée et des machines virtuelles dotées d'une protection maximale*.
Microsoft learn, Microsoft.
https://learn.microsoft.com/fr-fr/windows-server/security/guarded-fabric-shielded-vm/guarded-fabric-and-shielded-vms.

[98] *Security Identifiers*.
Microsoft learn, Microsoft.
https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-security-identifiers.

[99] *Attribute msDS-ExpirePasswordsOnSmartCardOnlyAccounts in Active Directory Schema*.
Microsoft learn, Microsoft.
https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-ada2/1ba3e699-77ab-4ba6-9d70-74616b1e11d4.

[100] *Microsoft network server : Digitally sign communications (always)*.
Microsoft learn, Microsoft.
https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/Microsoft-network-server-digitally-sign-communications-always.

[101] *SMBv1 is not installed by default in Windows 10 version 1709, Windows Server version 1709 and later versions*.
Microsoft learn, Microsoft.
https://learn.microsoft.com/en-us/windows-server/storage/file-server/troubleshoot/smbv1-not-installed-by-default-in-windows.

[102] *Service Principal Names*.
Microsoft learn, Microsoft.
https://learn.microsoft.com/en-us/windows/win32/ad/service-principal-names.

[103] *Microsoft network server : Server SPN target name validation level*.
Microsoft learn, Microsoft.
https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/Microsoft-network-server-server-spn-target-name-validation-level.

[104] *User Rights Assignment*.
Microsoft learn, Microsoft.
https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn221963(v=ws.11).

[105] *Windows Admin Center*.
Microsoft learn, Microsoft.
https://learn.microsoft.com/fr-fr/windows-server/manage/windows-admin-center/overview.

[106] *Contrôle d'application pour Windows*.
Microsoft learn, Microsoft.
https://learn.microsoft.com/fr-fr/windows/security/threat-protection/windows-defender-application-control/windows-defender-application-control.

[107] *En quoi consiste l'option d'installation minimale dans Windows Server ?*
Microsoft learn, Microsoft.
https://learn.microsoft.com/fr-fr/windows-server/administration/server-core/what-is-server-core.

[108] *ORADAD (Outil de récupération automatique de données de l'Active Directory)*.
Git-hub, ANSSI.
https://github.com/ANSSI-FR/ORADAD.

[109] *PingCastle*.
Git-hub, PINGCASTLE.
https://github.com/vletoux/pingcastle.

[110] *Protection des OIV en France*.
Technical report, ANSSI.
https://www.ssi.gouv.fr/entreprise/protection-des-oiv/protection-des-oiv-en-france/.

[111] *WSUSpendu*.
Yves Le-Provost Romain COLTEL.
Publication scientifique, SSTIC, 2017.
https://www.sstic.org/media/SSTIC2017/SSTIC-actes/wsus_pendu/SSTIC2017-Article-wsus_pendu-coltel_le-provost.pdf.

[112] *Samba main page*.
Technical report, Samba Team.
https://wiki.samba.org/index.php/Main_Page.

[113] *Samba release planning*.
Technical report, Samba Team.
https://wiki.samba.org/index.php/Samba_Release_Planning.

[114] *Samba-tool man page*.
Technical report, Mankier.
https://www.mankier.com/8/samba-tool.

[115] *Oracle Critical Patch Update Advisory - January 2018 | Oracle Virtualization Risk Matrix*.
Technical report, Oracle, janvier 2018.
https://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html#AppendixOVIR.

[116] *VirusTotal*.
Technical report, Chronicle LLC, décembre 2019.
https://www.virustotal.com/gui/home/upload.

[117] *VMSA-2018-0027 | VMware ESXi, Workstation, and Fusion updates address uninitialized stack memory usage*.
Technical report, VMWare, novembre 2018.
https://www.vmware.com/security/advisories/VMSA-2018-0027.html.

[118] *Windows Local Administrator Password Solution (Windows LAPS)*.
Microsoft learn, Microsoft.
https://learn.microsoft.com/en-us/windows-server/identity/laps/laps-overview.

[119] *Citrix XenServer Multiple Security Updates*.
Technical report, Citrix Systems, octobre 2017.
https://support.citrix.com/article/CTX228867.

Version 1.0 - 02/10/2023 - ANSSI-PA-099
Licence ouverte / Open Licence (Étalab - v2.0)
ISBN : 978-2-11-167144-7 (papier)
ISBN : 978-2-11-167145-4 (numérique)
Dépôt légal : octobre 2023

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI - 51, boulevard de La Tour-Maubourg, 75700 PARIS 07 SP
www.ssi.gouv.fr / conseil.technique@ssi.gouv.fr

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité