Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général
de la défense
et de la sécurité nationale

*Agence nationale de la sécurité
des systèmes d'information*

Paris, le 10 septembre 2014

N° DAT-NT-17/ANSSI/SDE/NP

Nombre de pages du document
(y compris cette page) : 49

Note technique

Recommandations de sécurité relatives à Active Directory.

Public visé:

Développeur	
Administrateur	✓
RSSI	✓
DSI	
Utilisateur	

Informations

Avertissement

Ce document rédigé par l'ANSSI présente les « **Recommandations de sécurité relatives à Active Directory.** ». Il est téléchargeable sur le site www.ssi.gouv.fr. Il constitue une production originale de l'ANSSI. Il est à ce titre placé sous le régime de la « Licence ouverte » publiée par la mission Etalab (`www.etalab.gouv.fr`). Il est par conséquent diffusable sans restriction.

Ces recommandations 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.

Personnes ayant contribué à la rédaction de ce document:

Contributeurs	Rédigé par	Approuvé par	Date
BAI, SIS	BSS	SDE	10 septembre 2014

Évolutions du document :

Version	Date	Nature des modifications
1.0	19 août 2014	Version initiale
1.1	10 septembre 2014	Corrections mineures

Pour toute remarque:

Contact	Adresse	@mél	Téléphone
Bureau Communication de l'ANSSI	51 bd de La Tour-Maubourg 75700 Paris Cedex 07 SP	communication@ssi.gouv.fr	01 71 75 84 04

Table des matières

1 Introduction

Active Directory (AD) est un annuaire introduit par Windows 2000 Server. Son implémentation permet de centraliser des informations relatives aux utilisateurs et aux ressources d'une entreprise en fournissant des mécanismes d'identification et d'authentification tout en sécurisant l'accès aux données.

1.1 Quels risques de sécurité ?

La diversité des informations qu'un annuaire AD contient et le rôle central qu'il occupe dans le système d'information ont induit la création d'un véritable écosystème applicatif pour l'administrer, le maintenir et le surveiller. Il est important de souligner qu'un annuaire Active Directory contient des secrets des utilisateurs, comme, par exemple, leurs informations d'identification. De fait, il constitue une cible privilégiée pour une personne malveillante.

En effet, s'il dispose des droits d'administration du domaine, un attaquant est libre de mener toutes les opérations souhaitées telles que l'exfiltration de données ou le sabotage. La compromission d'un seul compte avec des droits privilégiés peut ainsi faire perdre la maîtrise totale du système d'information.

La complexité de cet annuaire est telle qu'un individu malveillant peut y dissimuler sa présence de différentes manières plus ou moins subtiles et, pour certaines, difficilement détectables. Un tel individu se trouve alors en mesure de laisser des portes dérobées dans de multiples services et applicatifs du système d'information. Il en résulte un risque important d'attaques complexes persistantes. Un système d'information ayant fait l'objet d'une telle compromission est parfois impossible à *nettoyer* et doit faire l'objet d'une reconstruction complète nécessitant d'importants moyens financiers et humains.

Par conséquent, il est primordial de maîtriser et de bien sécuriser son annuaire AD.

1.2 Objectifs et périmètre du document

Ce document a pour objectif de fournir des recommandations et des procédures permettant la sécurisation d'un annuaire AD.

Il est nécessaire de disposer de notions élémentaires du fonctionnement d'AD pour les appréhender ; Microsoft a publié des articles de référence sur ce sujet [1]. Cependant, afin de présenter ces recommandations, de brèves explications sur le fonctionnement de l'AD ou de ses composants sont apportées lorsque cela est nécessaire.

1.3 Priorisation des recommandations

Les recommandations liées à la sécurisation de l'annuaire AD sont priorisées en fonction de la criticité de leur périmètre de protection ainsi que de leur complexité de mise en œuvre.

1. http://technet.microsoft.com/fr-fr/library/cc780336.aspx.

Priorité 1	La recommandation proposée permet de mettre en place une protection contre l'exploitation de vulnérabilités pouvant engendrer une compromission de l'AD.
Priorité 2	L'application de la recommandation est utile pour protéger l'AD contre les accès non autorisés.
Priorité 3	La recommandation est motivée par la protection de l'intégrité des données contenues dans l'AD et leur non-divulgation.
Priorité 4	Le périmètre de protection de la recommandation ne couvre pas d'éléments critiques ou sa complexité de mise en œuvre la rend moins prioritaire.

TABLE 1 – Priorisation des recommandations

Les coûts de mise en œuvre de certaines recommandations peuvent s'avérer élevés mais ils restent néanmoins minimes comparés aux coûts qui découleraient d'une compromission de l'AD.

1.4 Concepts

1.4.1 Annuaire Active Directory

Le service d'annuaire AD utilise une base de données (ayant un moteur ESE) pour stocker toutes les informations d'annuaire. Ce dernier contient des informations sur les objets tels que les utilisateurs, les groupes, les ordinateurs, les domaines, les unités d'organisation et les stratégies de sécurité. Sa taille peut varier de quelques centaines d'objets pour de petites installations à plusieurs millions pour des configurations volumineuses.

AD comprend également :
- un ensemble de règles, le *schéma*, qui définit les classes d'objets et d'attributs contenus dans l'annuaire, les contraintes et limites qui s'appliquent aux instances de ces objets et le format de leurs noms ;
- un *catalogue global* qui contient des informations sur chaque objet de l'annuaire. Ceci 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 ;
- un mécanisme de requête et d'index utilisant principalement le protocole LDAP qui permet aux utilisateurs et aux applications du réseau de publier et de retrouver les objets et leurs propriétés ;
- un service de réplication qui distribue les données de l'annuaire sur un réseau. Tous les *contrôleurs de domaine* (DC) en écriture d'un domaine participent à la réplication et stockent une copie complète de toutes les informations de l'annuaire concernant leur domaine (les contrôleurs de domaine en lecture seule ne possèdent que des informations partielles).

L'annuaire est stocké sur des DC : chacun dispose d'une copie de l'annuaire pour l'ensemble de son domaine. Les modifications apportées à l'annuaire sur un DC sont répliquées sur les autres DC du domaine, de l'arborescence de domaine ou de la forêt (les notions de domaine et de forêt sont abordées dans la section 1.4.2).

AD utilise quatre types de partitions d'annuaire distinctes pour stocker et copier les différents types de données. Cette structure de stockage et le mécanisme de réplication permet aux utilisateurs de disposer des informations d'annuaire n'importe où dans le domaine. Les partitions sont les suivantes :

Données du domaine Les données du domaine contiennent des informations sur les objets d'un domaine. Il s'agit notamment des attributs de compte d'utilisateur et d'ordinateur et des ressources publiées.

Données de configuration Les données de configuration décrivent la topologie de l'annuaire. Ces données de configuration comprennent une liste complète des domaines, arborescences et forêts ainsi que les emplacements des contrôleurs de domaines et des catalogues globaux.

Données du schéma Le schéma est la définition formelle de toutes les données relatives aux objets et attributs pour les objets existants. Les objets du schéma sont protégés par des listes de contrôle d'accès. Ainsi, seuls les utilisateurs autorisés peuvent modifier le schéma.

Données d'application Les données stockées dans la partition d'application sont répliquées, mais pas nécessairement à l'échelle globale. Les partitions d'annuaire destinées aux applications ne font pas partie de l'annuaire par défaut ; elles doivent être créées, configurées et gérées par l'administrateur. On parle alors de partition NDNC (Non-Domain Naming Context). Cette partition n'existe pas dans AD 2000.

Dans un environnement Microsoft, les zones DNS peuvent être intégrées aux partitions du domaine ou d'applications.

1.4.2 Forêt et domaine

La notion de domaine Windows a été introduite avec Windows NT et pouvait être vue comme un ensemble d'ordinateurs partageant une base de données commune pour l'authentification. Depuis Windows 2000, cette notion a évolué. Avant Windows 2000, un domaine Windows NT est une frontière pour la sécurité : le périmètre d'administration des comptes privilégiés ne dépasse pas les frontières d'un domaine.

Depuis Windows 2000, les comptes d'administration d'un domaine de la forêt ont des privilèges dans tous les domaines de la forêt (cette élévation de privilège est bloquée par l'utilisation des outils d'administration Microsoft mais est techniquement possible par conception). Les termes d'isolation et d'autonomie sont utilisés pour qualifier une forêt et un domaine : les privilèges d'administration ne dépassent pas les frontières de la forêt ; un domaine peut être administré indépendamment des autres mais certains privilèges traversent les frontières des domaines d'une même forêt.

D'autres éléments architecturaux caractérisent les forêts et domaines AD :
- un compte est défini dans un seul et unique domaine d'une forêt et peut être utilisé dans n'importe quel domaine de la forêt (si les droits d'accès le permettent) grâce aux relations d'approbation implicite entre les domaines ;
- lorsqu'un utilisateur appartenant à un domaine accède à une ressource d'un autre domaine de la même forêt et que l'authentification par Kerberos est utilisée, un DC de confiance pour l'ordinateur de l'utilisateur et le serveur de la ressource est utilisé dans le processus d'authentification.

2 Prérequis à la sécurisation de l'Active Directory

La sécurisation d'un annuaire AD n'est pas uniquement une question de configuration logicielle ; elle doit être mise en œuvre dès la conception de l'architecture. Ainsi, les éléments qui suivent doivent être pris en compte.

2.1 Architecture physique

La sécurisation d'un annuaire AD doit être prise en compte dès sa phase de conception et lors de son implémentation.

2.1.1 Sites Active Directory

Lorsque les ordinateurs d'une forêt sont répartis sur différentes zones géographiques connectées entre elles par des liens réseaux (hors LAN), il est commun de définir des sites AD. Ainsi, l'implémentation des sites AD reflète en général l'architecture physique du réseau et implique de prendre en compte les éléments suivants :

- l'implémentation de sites implique la création de liens de site. Ces derniers impactent directement la topologie de réplication garante de la mise à jour de la base de données de tous les contrôleurs de domaine ;
- un client AD s'authentifiant sur un domaine va contacter, de préférence, un contrôleur de domaine dans le même site AD. La configuration des sites AD influencera donc le trafic sur le réseau ainsi que la disponibilité des DC.

2.1.2 La réplication

La réplication correspond au processus de propagation des mises à jour effectuées sur l'annuaire entre les différents DC.

La topologie de réplication définit comment les informations vont être répliquées entre les différents DC. Deux types de réplications sont à distinguer :

Réplication intra-site
: Les informations d'annuaire situées à l'intérieur d'un site sont répliquées automatiquement à des intervalles réguliers. La topologie de réplication est générée automatiquement par le KCC (*Knowledge Consistency Checker*). Ce dernier tente d'établir une topologie qui permet d'avoir au moins deux connexions logiques sur chaque DC.

Réplication inter-site
: Les informations d'annuaire sont répliquées entre les sites grâce à la topologie de réplication inter-site. Le KCC utilise les objets de l'annuaire AD tels que les *liens de sites* et les *serveurs tête de pont* pour définir cette topologie de réplication.

Dans le cas de la réplication inter-site, deux types de transport peuvent être utilisés :

Transport synchrone par RPC (Remote Procedure Call) au-dessus de TCP/IP
: Ce mode de transport peut être utilisé pour répliquer n'importe quel type d'information.

Transport asynchrone par SMTP (Simple Mail Transport Protocol)
: Ce mode de transport ne peut être utilisé que pour répliquer les informations de configuration, du schéma et du catalogue global. SMTP ne peut pas être utilisé pour répliquer les informations intra-domaine qui sont les données du contexte de domaine échangées entre tous les contrôleurs de domaine d'un même domaine Windows.

Le tableau suivant présente les avantages et les inconvénients liés à chaque type de transport :

	Transport synchrone par RPC	**Transport asynchrone par SMTP**
Avantages	– simplicité de mise en œuvre. – utilisé pour la réplication inter et intra-site pour toutes les données.	– protocole adapté à des bandes passantes limitées ; plusieurs transactions peuvent être traitées simultanément. – peut être sécurisé, surveillé et administré à travers un réseau WAN.
Inconvénients	– utilisation d'un port dynamique affecté par le point de terminaison RPC utilisant le port 135. – inadapté sur les liens à faible bande passante.	– complexe à mettre en œuvre. – ne peut pas être utilisé pour répliquer les informations intra-domaine. – ne permet pas de répliquer les stratégies de groupes (GPO).

TABLE 2 – Types de transport utilisés par la réplication

2.1.2.1 Port utilisé par la réplication

Par défaut, la réplication par RPC utilise un port dynamique affecté par le point de terminaison RPC utilisant le port 135. Il est toutefois possible de fixer le port utilisé par la réplication inter-site en modifiant sur tous les DCs la valeur *TCP/IP Port* de la clé de registre :
HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Parameters.

R1 - Priorité 4

> Il est recommandé de fixer les ports de réplication afin de maîtriser au mieux les flux réseau. La définition de ports statiques est obligatoire si le DC est derrière un pare-feu.

2.1.2.2 Utilisation du KCC

Le KCC est un service présent sur chaque DC qui ajuste dynamiquement la topologie de réplication des données lorsque :
– un DC est ajouté, supprimé ou indisponible ;
– un lien de site est créé, modifié ou supprimé ;
– la planification de la réplication des données a été modifiée.

À partir des objets de l'AD décrivant la topologie réseau (objets *Site*, *Lien de site*, *Serveur tête de pont*, ...), le KCC crée des objets de type *Connexion* qui vont être utilisés pour définir les réplications entrantes.

Par défaut, toutes les 15 minutes, ce service recalcule la topologie de réplication. Cette fréquence est configurable en modifiant la valeur *Repl topology update period (secs)* de la clé de registre :
HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Parameters.

R2 - Priorité 4

> Il est recommandé de laisser le KCC générer la topologie de réplication, une fois les coûts des liens de site définis, si la règle mathématique suivante est vraie :
> (1 + *Nombre de domaine*) * *Nombre de site*^{2} <= 100 000.
> Dans le cas contraire, une réduction du nombre de liens de site, une planification de l'exécution du KCC durant les heures creuses ou une désactivation du KCC (création manuelle des objets *Connexion*) peuvent être envisagées pour optimiser la topologie de réplication.

Note : la règle mathématique est extraite d'un article [2] de Microsoft.

2.1.2.3 Planification et fréquence de la réplication

Le flux de réplication dépend de deux paramètres :

Planification de la réplication
- ce paramètre définit, par jour de la semaine, la période d'ouverture d'un lien de site à la réplication ;
- la granularité de la planification se fait au niveau de l'heure ;
- par défaut, le lien de site est toujours ouvert à la réplication.

Fréquence de la réplication
- ce paramètre définit la fréquence de réplication souhaitée durant la période d'ouverture d'un lien de site à la réplication ;
- la granularité de la fréquence se fait au niveau de la minute ;
- par défaut, la fréquence de réplication est de 180 minutes (3 heures).

En prenant en compte ces deux paramètres ainsi que l'architecture physique de l'AD (sites et liens de sites), il est possible de calculer le temps de convergence : le temps maximal pour qu'une modification soit prise en compte par tous les DCs de la forêt.

2.1.3 Placement des contrôleurs de domaine

Les DC ne possèdent pas tous les mêmes rôles, ce qui peut influencer leur nombre et leur emplacement géographique. Ainsi, le placement des *catalogues globaux* (GC) est déterminant.

Un *catalogue global* est un DC détenant toutes les informations de son domaine ainsi qu'une partie des informations des autres domaines de la forêt. Les principales fonctions d'un GC sont les suivantes :
- fournir les informations sur l'appartenance aux groupes universels lors d'une procédure d'authentification ;
- trouver les informations d'annuaire quel que soit le domaine de la forêt qui contient les données.

Les règles suivantes peuvent aider à déterminer le nombre et les emplacements d'un GC dans une infrastructure AD :

Contrôleur de domaine
Seul un DC peut être un catalogue global.

Applications utilisant le serveur de catalogue global
Certaines applications comme Microsoft Exchange requièrent une bonne connectivité (temps de réponse faible, disponibilité) avec un GC. Il convient donc d'identifier ces applications et de placer les GC en conséquence. Microsoft recommande que tous les contrôleurs de domaine soient GC.

2. http://support.microsoft.com/kb/244368.

Nombre d'utilisateurs sur le site
Il est recommandé de placer un GC sur les sites ayant plus de 100 utilisateurs afin d'optimiser le lien et le trafic réseau.

Disponibilité du lien réseau
Une perte de connectivité au réseau peut nuire à la productivité sur des sites sans GC.

Cache de membres des groupes universels
Cette fonctionnalité apportée par Windows 2003 permet d'optimiser le trafic réseau en conservant en cache les membres des groupes universels sur un DC.

Nombre d'utilisateurs nomades sur le site
Les utilisateurs nomades doivent accéder au GC lors de leur première authentification dans l'environnement AD.

Le placement des contrôleurs de domaine en lecture seule (RODC) est également un élément de sécurité à prendre en considération. Ce type de DC est déployé lorsque la sécurité physique du DC n'est pas optimale ou par manque d'administrateur sur le site géographique. En effet, ce type de DC ne possède qu'une copie partielle en lecture seule des informations de l'annuaire.

R3 - Priorité 1
> Si la sécurité physique d'un DC n'est pas assurée, il est primordial que celui-ci soit configuré comme RODC et qu'un système de chiffrement des disques soit mis en œuvre.

Note : Un RODC dont les disques sont chiffrés devrait idéalement être installé en Windows Server Core. Chaque redémarrage nécessite une saisie du mot de passe de déchiffrement des disques. Par conséquent, le mode Core permettrait de réduire la fréquence des redémarrages puisque ce dernier ne possède qu'un nombre limité d'applicatifs et de composants système à mettre à jour.

R4 - Priorité 1
> La fonctionnalité permettant la mise en cache des informations d'identification des utilisateurs sur un RODC doit être utilisée uniquement pour mettre en cache les informations de connexion des comptes utilisateurs sans privilège du site. Si la sécurité physique du RODC n'est pas garantie, les informations de connexions des comptes avec privilèges ou des comptes d'utilisateurs n'appartenant pas au site ne doivent pas y être stockées afin de limiter les risques de compromission de l'annuaire.

R5 - Priorité 4
> Il est recommandé de placer un DC en écriture dans le site AD sécurisé le plus proche du site hébergeant le RODC.

2.2 Architecture réseau

Les données de l'annuaire AD sont transmises sur le réseau par différents services utilisant de multiples ports et protocoles.

2.2.1 DNS

Avant Microsoft Windows 2000, la résolution de noms de machine reposait principalement sur NetBIOS et son service de résolution des noms (WINS). Depuis Windows Server 2000, DNS devient le service de résolution de noms à la fois pour les clients et les serveurs. Par la suite, son implémentation devient dynamique permettant ainsi aux machines de s'enregistrer automatiquement (Dynamic DNS -

DDNS). Enfin, le format des noms de l'arborescence des domaines et celui de DNS fusionnent impliquant une très forte relation entre les domaines Windows 2003 ou plus récents et DNS.

2.2.1.1 Rappel sur la méthode de résolution des noms d'hôtes

Pour résoudre un nom d'hôte, le résolveur DNS consulte dans un premier temps le cache de résolution de nom d'hôte :

- si le nom d'hôte a déjà été résolu et que le TTL (*Time To Live*) de l'enregistrement n'a pas expiré alors l'adresse IP correspondante est utilisée ;
- si le nom d'hôte recherché n'est pas présent dans le cache, le résolveur DNS consultera le fichier HOST local à la machine ;
- si le nom d'hôte n'est pas présent dans le fichier HOST alors le résolveur DNS va effectuer une requête de résolution de nom auprès du serveur DNS configuré ;
- si le DNS ne peut pas résoudre le nom d'hôte alors une résolution NETBIOS sera initiée (dans le cas où le nom recherché est un nom court). Ainsi, le cache NETBIOS, le serveur WINS et enfin le fichier LMHOST seront sollicités.

2.2.1.2 Rappel sur les zones de recherche

Un serveur DNS gère plusieurs zones de recherche :

Zone de recherche directe
Cette zone est utilisée pour trouver les adresses IP des noms recherchés.

Zone de recherche indirecte
Cette zone est utilisée pour trouver les noms associés aux adresses IP données. Un fichier de cette zone existe pour chaque sous-réseau.

2.2.1.3 Rappel sur les types de zones

Un serveur DNS gère plusieurs types de zones :

Zone primaire
Contient la copie maîtresse des enregistrements. Le serveur DNS a accès en lecture et en écriture aux enregistrements de cette zone.

Zone secondaire
Contient une copie de la zone primaire. Cette zone est utilisée pour répondre aux requêtes de résolution de noms.

Zone de stub
Disponible uniquement depuis Windows 2003, cette zone contient uniquement des enregistrements de type *SOA* (Start Of Authority), *NS* (Name Server) et *A* (Address) des serveurs DNS responsables de la zone. Elle est utilisée pour maintenir une liste à jour des serveurs DNS de référence pour la zone et améliorer la résolution de noms sans avoir à interroger un serveur racine interne ou Internet.

Zone GlobalNames
Depuis Windows 2008, il est possible de créer cette zone pour prendre en charge la résolution des noms courts (dans un optique de migration de WINS vers DNS).

Lorsque le rôle DNS de Microsoft est hébergé sur un DC, les types de zones *primaire* et *stub* peuvent être intégrées à AD.

2.3 Santé des contrôleurs de domaine

Les contrôleurs de domaine hébergent le service Active Directory, de ce fait, il est important de pouvoir vérifier l'état de santé de la machine et de ses logiciels.

2.3.1 Journalisation

Par défaut, la politique de journalisation des systèmes Windows diffère suivant les versions et omet certains évènements liés à la sécurité pourtant très utiles lors d'une analyse en cas d'incident ou bien pour une supervision en continu.

R6 - Priorité 1

> Il est recommandé d'augmenter la taille des journaux d'évènements en utilisant une GPO idéalement placée à la racine du domaine. Pour les systèmes ayant un noyau en version 5.x, il est recommandé de fixer les valeurs suivantes :
> – taille maximale du journal de sécurité : 179200 Ko (175 Mo) ;
> – taille maximale du journal des applications : 51200 Ko (50 Mo) ;
> – taille maximale du journal système : 51200 Ko (50 Mo).
> Pour les systèmes ayant une version du noyau supérieure ou égale à 6 :
> – taille maximale du journal de sécurité : 1024000 Ko (1 Go) ;
> – taille maximale du journal des applications : 204800 Ko (200 Mo) ;
> – taille maximale du journal système : 204800 Ko (200 Mo).

Note : il est possible de déterminer la version du noyau grâce à l'outil intégré *winver.exe*.

R7 - Priorité 1

> Il est recommandé d'activer les fonctionnalités d'audit (journalisation des opérations réussies et des échecs) pour les éléments listés dans l'annexe II.

.

Le tableau suivant énumère les évènements liés à la sécurité à surveiller dans un environnement AD, regroupés par criticité :

	ID	Fournisseur	**Description**
Haute	4610 (514)	Security-Auditing	Un package d'authentification a été chargé par l'autorité de sécurité locale
	4614 (518)	Security-Auditing	Un package de notification a été chargé par le gestionnaire de comptes de sécurité
	4618 (522)	Security-Auditing	Un évènement de sécurité surveillé est survenu
	4649 (552)	Security-Auditing	Une attaque par rejeu a été détectée
	4719 (612)	Security-Auditing	Une stratégie d'audit a été modifiée
	4765 (669)	Security-Auditing	Un SID History (historique d'identifiants uniques) a été ajouté à un compte
	4766 (670)	Security-Auditing	Une tentative d'ajout d'un SID History a échoué
	4794 (698)	Security-Auditing	Une tentative d'activation du mode de restauration AD a échoué
	4964 (868)	Security-Auditing	Un compte membre d'un groupe surveillé s'est authentifié
	1102 (517)	Eventlog	Le journal d'audit a été effacé

	ID	Fournisseur	Description
Moyenne	4706 (610)	Security-Auditing	Une relation d'approbation a été créée
	4713 (617)	Security-Auditing	La stratégie Kerberos a été modifiée
	4716 (620)	Security-Auditing	Une relation d'approbation a été modifiée
	4724 (628)	Security-Auditing	Une tentative de réinitialisation de mot de passe d'un compte a échoué
	4739 (643)	Security-Auditing	La stratégie de domaine a été modifiée
	4740 (644)	Security-Auditing	Un compte d'utilisateur a été verrouillé
	4768 (672)	Security-Auditing	Un ticket d'authentification Kerberos (TGT) a été demandé
	4769 (673)	Security-Auditing	Un ticket de service Kerberos a été demandé
	4770 (674)	Security-Auditing	Un ticket de service Kerberos a été renouvelé
	4771 (675)	Security-Auditing	La pré-authentification Kerberos a échoué
	4772 (676)	Security-Auditing	Une demande de ticket d'authentification Kerberos a échoué
	4773 (677)	Security-Auditing	Une demande de ticket de service Kerberos a échoué
	4774 (678)	Security-Auditing	Un compte a été mappé pour l'ouverture de session
	4775 (679)	Security-Auditing	Impossible de mapper un compte pour l'ouverture de session
	4776 (680)	Security-Auditing	L'ordinateur a tenté de valider les informations d'identification d'un compte
	4777 (681)	Security-Auditing	Le contrôleur de domaine n'a pas réussi à valider les informations d'identification d'un compte
	4780 (684)	Security-Auditing	Des droits ont été modifiés sur des comptes membres du groupe Administrateurs
	4865 (769)	Security-Auditing	Une relation d'approbation de forêt a été ajoutée
	4867 (771)	Security-Auditing	Une relation d'approbation de forêt a été modifiée
	4907 (811)	Security-Auditing	Des paramètres d'audit ont été modifiés
	4908 (812)	Security-Auditing	La liste des groupes spéciaux a été modifiée
	5030 (934)	Security-Auditing	Le service Pare-feu n'a pas pu démarrer
	5038 (942)	Security-Auditing	L'intégrité d'un fichier n'a pas pu être vérifiée
	6145 (2049)	Security-Auditing	Des erreurs sont survenues lors de l'application d'une stratégie de groupe
Faible	4608 (512)	Security-Auditing	Le système démarre
	4609 (513)	Security-Auditing	Le système s'arrête
	4616 (520)	Security-Auditing	L'heure du système a été modifiée
	4698 (602)	Security-Auditing	Une tâche planifiée a été créée
	4702 (602)	Security-Auditing	Une tâche planifiée a été modifiée
	4704 (608)	Security-Auditing	Un droit utilisateur a été ajouté
	4782 (686)	Security-Auditing	Un accès à l'empreinte d'un mot de passe a été effectué

TABLE 3 – Liste des évènements Active Directory à surveiller

Remarque : La colonne ID spécifie l'identifiant de l'évènement dans les systèmes d'exploitation Vista ou 2008 et supérieurs avec son équivalent sous XP et 2003 entre parenthèses.

R8 - Priorité 2

> Il est pertinent de mettre en place une infrastructure de collecte des journaux d'évènements et de les conserver au format natif Microsoft (pas de transformation en syslog, par exemple) afin d'éviter toute perte d'information.

2.4 Accès à distance

L'accès à distance à une machine peut se faire avec les principaux moyens suivants :

Le bureau à distance
L'accès au bureau à distance expose l'empreinte du mot de passe utilisé pour la connexion sur la machine distante. Cette fonctionnalité ne devrait donc pas être utilisée vers des postes de travail des utilisateurs mais vers des serveurs d'infrastructure comme les contrôleurs de domaine. Toutefois, depuis 2012 R2 et Windows 8.1, l'accès au bureau à distance n'expose plus cette empreinte de mot de passe en utilisant le paramètre *restrictedAdmin* et depuis mai 2014, cette fonctionnalité a été ajoutée à Windows 7 et 2008 R2 [3] ;

Gestion à distance
L'utilisation de *WinRM* (Windows Remote Management) devient de plus en plus répandue. Ce service Windows natif aux systèmes d'exploitation depuis 2008 permet d'administrer les composants logiciels d'une machine à distance. Le principal outil permettant l'exploitation de cette fonctionnalité est Windows PowerShell (un langage de script et un interpréteur en ligne de commande). Cette fonctionnalité passe par le protocole HTTP(S).

Protocole RPC
L'utilisation des consoles de type *MMC* utilisant le protocole RPC reste l'outil le plus utilisé.

R9 - Priorité 1

> Il est important de filtrer les connexions entrantes sur chaque machine à l'aide du pare-feu local Windows afin de n'autoriser que certaines machines à se connecter à distances. Cela implique d'utiliser des postes d'administration dédiés (ou passerelle de rebond) centralisant les outils d'administration. De plus, l'utilisation de WinRM (avec HTTPS) est à privilégier afin de limiter le nombre de ports ouverts sur les machines.

2.5 Environnement logiciel

L'environnement logiciel gravitant autour de l'annuaire AD est un vecteur courant d'attaques. Cet écosystème applicatif peut créer des brèches exploitées par des personnes malveillantes :

Logiciels antivirus et antimalware non mis à jour
La présence d'un antivirus ou antimalware sur les serveurs membres et postes de travail n'est efficace que s'il est mis à jour régulièrement.

Système non mis à jour
L'application des mises à jour de sécurité du système est une protection nécessaire.

Système et applications trop anciens
L'identification des systèmes et applications utilisant des technologies dépassées est primordial afin d'identifier un potentiel risque pour la sécurité.

Mauvaise configuration
Un système à jour mal configuré peut être plus exposé aux attaques (pare-feu désactivé, stratégie

3. https ://support.microsoft.com/kb/2871997.

de gestion de mot de passe inexistante, réutilisation d'un même mot de passe pour tous les administrateurs, etc.)

Normes de sécurité des développements applicatifs trop permissives ou inexistantes
Les comptes de services possèdent parfois plus de droits que nécessaire, les requêtes générées par l'application mal protégées, des mots de passe diffusés en clair sur le réseau ou dans un fichier : ces éléments créent une brèche au niveau de la sécurité.

Par conséquent, les contrôleurs de domaine ne devraient pas héberger de services autres que ceux nécessaires au fonctionnement de l'annuaire afin de ne pas augmenter la surface d'attaque de la machine.

R10 - Priorité 1

Il est important de noter qu'un antivirus est un applicatif. De ce fait, des failles logicielles pourraient être exploitées afin de compromettre la machine. L'installation d'un antivirus sur des serveurs critiques (comme les DC) augmente la surface d'attaque. Ainsi, il n'est pas recommandé d'installer de logiciels (que ce soit un antivirus, un agent de sauvegarde, d'inventaire, etc.) sur un contrôleur de domaine.
Il est envisageable d'utiliser une solution de surveillance pour les DC si elle répond aux critères suivants :
- mise en œuvre d'une infrastructure de surveillance dédiée aux DC ;
- utilisation de comptes de service dédiés à la solution ;
- aucun agent en écoute installé sur les DC ;
- outils utilisés développés par une source de confiance.

R11 - Priorité 1

Les comptes de services doivent faire l'objet d'une attention particulière et il est recommandé de :
- minimiser leurs privilèges ;
- les inventorier régulièrement ;
- formaliser des procédures de changement de leur mot de passe (création de fiches informatives sur les comptes de services).

3 Éléments de sécurité Active Directory

Un annuaire AD est composé de plusieurs éléments (composants ou services) pour lesquels la sécurité est à prendre en considération.

3.1 Niveaux fonctionnels

Pour supporter les environnements ayant différentes versions du système d'exploitation Microsoft Windows Server, le concept de niveau fonctionnel a été implémenté. Un niveau fonctionnel est un ensemble de services que tous les DC de ce niveau peuvent fournir. Afin de définir un niveau fonctionnel, il est nécessaire de s'assurer que les systèmes d'exploitation de tous les DC soient dans la même version.

Le niveau fonctionnel de la forêt active des fonctionnalités dans tous les domaines de la forêt tandis que le niveau fonctionnel du domaine active des fonctionnalités dans le domaine. Tous deux sont caractérisés par les éléments suivants :
- les niveaux les plus hauts requièrent une version du système d'exploitation plus récente ;

- tous les DC d'un domaine doivent avoir le même niveau fonctionnel ;
- une fois un niveau fonctionnel atteint, le retour en arrière est impossible. Des exceptions existent si la corbeille AD est désactivée et que le niveau fonctionnel de la forêt est strictement inférieur à celui du domaine et supérieur ou égal à 2008. Par exemple :
  - le niveau fonctionnel du domaine est en 2012 R2 et celui de la forêt en 2012 : il est possible de revenir au niveau fonctionnel 2012 pour le domaine ;
  - le niveau fonctionnel du domaine est en 2012 et celui de la forêt en 2008 R2 : il est possible de revenir au niveau fonctionnel 2008 R2 pour le domaine ;
  - le niveau fonctionnel du domaine est en 2008 R2 et celui de la forêt en 2008 : il est possible de revenir au niveau fonctionnel 2008 pour le domaine.

Le tableau suivant récapitule les différents niveaux fonctionnels ainsi que le système d'exploitation qu'ils supportent sur les DC :

Type	**Niveau fonctionnel**	**Système d'exploitation supporté**						
		NT 4	2000	2003	2008	2008 R2	2012	2012 R2
Forêt	Windows 2000 natif		✓	✓	✓	✓		
	Windows Server 2003 Interim	✓		✓				
	Windows Server 2003			✓	✓	✓	✓	✓
	Windows Server 2008				✓	✓	✓	✓
	Windows Server 2008 R2					✓	✓	✓
	Windows Server 2012						✓	✓
	Windows Server 2012 R2							✓
Domaine	Windows 2000 mixte	✓	✓	✓				
	Windows 2000 natif		✓	✓	✓	✓		
	Windows Server 2003 Interim	✓		✓				
	Windows Server 2003			✓	✓	✓	✓	✓
	Windows Server 2008				✓	✓	✓	✓
	Windows Server 2008 R2					✓	✓	✓
	Windows Server 2012						✓	✓
	Windows Server 2012 R2							✓

TABLE 4 – Récapitulatif des niveaux fonctionnels

Ainsi, plus le niveau fonctionnel est élevé, plus la version du système d'exploitation des contrôleurs de domaine est récente.

R12 - Priorité 1

> La sécurisation de l'Active Directory passe par la version du système d'exploitation de ses contrôleurs de domaine. Viser le niveau fonctionnel le plus haut permet d'augmenter le niveau de sécurité ; les versions les plus récentes prennent en effet en compte les lacunes liées à la sécurité des versions précédentes.

3.2 Schéma

Le schéma est la définition formelle de toutes les données relatives aux objets et attributs contenus dans l'AD. Les objets du schéma sont protégés par des listes de contrôle d'accès. Ainsi, seuls les utilisateurs autorisés peuvent modifier le schéma.

Des modifications sont nécessaires lorsque les définitions préexistantes du schéma ne sont pas adaptées à certains besoins. Ainsi, il est possible d'ajouter des classes d'objets ou d'attributs. Néanmoins, lors de ces modifications, il faut considérer les points suivants :

- les modifications du schéma sont globales : elles impactent toute la forêt ;
- les modifications du schéma sont irréversibles mais peuvent être désactivées.

R13 - Priorité 1

Avant d'effectuer une extension de schéma, plusieurs étapes préparatoires sont recommandées :

- vérifier que les identifiants uniques (OIDs) des objets ajoutés sont enregistrés auprès de Microsoft pour éviter tout conflit avec d'autres applications ;
- utiliser un environnement différent de celui de production pour valider la procédure d'extension ;
- écrire un plan de retour arrière (restauration complète de la forêt) ;
- vérifier la présence d'erreurs ou de conflits entre la version cible et la version courante du schéma ;
- isoler le DC ayant le rôle Maître du schéma sur lequel l'extension est effectuée (couper les réplications entrantes et sortantes afin de limiter le risque de propagation d'erreur) ;
- laisser le groupe Administrateur du schéma vide. Ajouter le compte utilisateur faisant l'extension comme membre de ce groupe le temps de l'opération uniquement.

3.3 Architecture logique

La hiérarchisation et la ventilation des objets (comptes ordinateurs, utilisateurs, imprimantes, etc.) dans des conteneurs AD (unités organisationnelles) définissent, entre autre, l'architecture logique de l'annuaire. De cette dernière va découler le modèle d'administration et de délégation des droits.

3.3.1 Relations d'approbation

Une relation d'approbation est un mécanisme permettant à un utilisateur de s'authentifier sur un domaine et d'accéder aux ressources d'un autre domaine sans se réauthentifier. Au sein d'une forêt, les relations d'approbation sont implicites. Elles sont explicites entre deux forêts, entre domaines appartenant à des forêts différentes ou bien entre un domaine d'une forêt et un domaine Windows NT, par exemple.

Une relation d'approbation est définie par trois principales propriétés : le type, la transitivité et la direction.

3.3.1.1 Types des relations d'approbation

Les différents types de relations d'approbation sont décrits dans le tableau ci-dessous :

Type d'approbation	Description
De domaine Kerberos	Type de relation utilisé entre un domaine Kerberos non-Windows et un domaine AD
De forêt	Type de relation utilisé entre deux forêts afin de partager des ressources
Externe	Permet l'accès à des ressources d'un domaine Windows NT ou d'un domaine appartenant à une forêt non liée par une relation d'approbation de type forêt
Raccourci	Permet d'optimiser l'ouverture de session des utilisateurs entre deux domaines d'une même forêt

TABLE 5 – Les types de relations d'approbation

3.3.1.2 Transitivité des relations d'approbation

Une relation d'approbation peut être :

Transitive Cette relation est capable de se déplacer du bas vers le haut d'une arborescence (des domaines enfants vers les domaines parents).

Non transitive Cette relation lie uniquement les deux domaines sans possibilité d'accéder aux autres domaines enfants.

3.3.1.3 Direction des relations d'approbation

Deux directions sont à distinguer :

Sens unique Crée un chemin d'authentification unidirectionnel entre deux domaines. Les utilisateurs d'un domaine peuvent accéder aux ressources de l'autre domaine mais l'inverse n'est pas possible.

Bidirectionnelle Les demandes d'authentification peuvent être effectuées depuis les deux domaines liés par la relation d'approbation.

3.3.1.4 Étendue de l'authentification des utilisateurs

Les étendues d'authentification suivantes sont à différencier :

Authentification à l'échelle du domaine Les utilisateurs peuvent accéder aux ressources du domaine lié par la relation d'approbation.

Authentification à l'échelle de la forêt Les utilisateurs peuvent accéder aux ressources de la forêt liée par la relation d'approbation.

Authentification sélective Disponible uniquement pour les approbations externes et les approbations de forêts, cette étendue d'authentification oblige à déclarer explicitement qui peut accéder à quelles ressources.

R14 - Priorité 4

> L'authentification sélective est à privilégier lors de la mise en place d'une relation d'approbation entre deux forêts. Cette dernière permet d'adopter une approche simple et sécurisée : toutes les authentifications sont refusées à l'exception de celles autorisées explicitement sur les ressources. Ces autorisations sont données sur la ressource (objet AD) par un groupe de domaine local.

3.3.1.5 Historique des SIDs

Afin de préserver l'accès à des ressources d'un domaine AD lors d'une migration vers un autre domaine, l'attribut *SIDHistory* d'un objet AD peut être peuplé avec les SID provenant d'une forêt en cours de migration. Dans ce scénario, lorsqu'un utilisateur s'authentifie dans le domaine AD cible, son SID d'origine (provenant du domaine source) ainsi que son nouveau SID sont ajoutés à son jeton d'accès.

L'utilisation de cette fonctionnalité facilite largement les migrations puisqu'il n'est pas nécessaire de modifier les ACL sur les ressources, cependant, elle rend l'AD vulnérable puisqu'il est possible d'usurper l'identité d'une personne en ajoutant son SID au *SIDHistory* d'un nouveau compte.

Cette fonctionnalité ne peut exister qu'entre deux domaines liés par une relation d'approbation.

R15 - Priorité 4

> L'utilisation du *SIDHistory* ne doit être que temporaire (durant la phase de migration par exemple) : les valeurs de cet attribut doivent être supprimées à la fin de la migration.

3.3.1.6 Filtrage des SIDs

Afin de maîtriser le *SIDHistory*, un filtrage peut être opéré afin de n'autoriser que certains SIDs. Depuis Windows Server 2003, cette fonctionnalité est activée par défaut sur les relations d'approbation externes.

R16 - Priorité 4

> De manière générale, afin d'éviter un risque de rebond entre les forêts, le filtrage des SIDs doit toujours être activé sur une relation d'approbation liant deux forêts. Lors des opérations de migration, cette fonctionnalité peut être désactivée temporairement.

3.3.2 Les unités organisationnelles

Les unités organisationnelles (OU) sont des conteneurs du service AD qui sont utilisés pour placer des utilisateurs, des groupes, des ordinateurs, des imprimantes et d'autres OU. Leur utilisation permet de créer des conteneurs dans un domaine représentant les structures hiérarchiques et logiques de l'organisation.

La création des OU peut être guidée selon les modèles suivants :

L'emplacement géographique Si le modèle d'administration est distribué géographiquement et si des administrateurs sont présents dans chaque emplacement, la structure des OU peut être organisée par zone géographique.

L'organisation Si l'administration informatique est partagée par plusieurs services ou divisions, la structure des OU peut être organisée en fonction de la structure de l'organisation. Il est préférable de ne pas se baser sur l'organigramme lorsque ce modèle est appliqué afin de ne pas être dépendant de chaque modification de ce dernier.

Les fonctions métier Si l'administration informatique est décentralisée (qu'il n'y a pas de service ou division dédiés), la structure AD peut être organisée autour des métiers de l'organisation.

Le modèle hybride Dans le cas d'une organisation fortement distribuée avec une fonction informatique décentralisée et une forte séparation de services, la structure AD peut être organisée en

créant les OU de premier niveau par emplacement géographique et les OU enfants par organisation.

R17 - Priorité 4

Lors de la création des OU, les points suivants doivent être gardés à l'esprit :

Simplicité Malgré toutes les possibilités de découpage des OU offertes par AD, une architecture simple sera plus à même d'évoluer.

Éviter une architecture basée sur l'organisation Comme décrit ci-dessus, c'est dans l'entreprise un des éléments qui est à même d'évoluer le plus souvent, il aura donc un impact direct sur l'administration.

La création d'OU doit être évitée dans les cas suivants :

Pour plaire aux utilisateurs finaux Bien que les utilisateurs puissent naviguer dans une arborescence d'OU, ce n'est pas la manière la plus efficace de découvrir les ressources : l'interrogation d'un catalogue global est préféré.

Pour représenter un regroupement de type projet La notion de groupe est préférée puisque les OU ne sont pas des éléments de sécurité.

R18 - Priorité 4

Il est recommandé de créer des OU dans les cas suivants :

Délégation d'administration. Il est possible de déléguer le contrôle administratif à n'importe quel niveau d'une arborescence de domaine en créant des OU puis en déléguant le contrôle administratif d'OU spécifiques à des utilisateurs ou des groupes.

Stratégie de groupe. Les OU sont la plus petite étendue à laquelle il est possible d'attribuer des paramètres Stratégie de groupe qui définissent les différents composants relatifs à l'environnement de Bureau de l'utilisateur qu'un administrateur système doit gérer.

3.3.3 Rôles de maître d'opérations

Dans toutes les forêts AD, cinq rôles de maître d'opérations sont attribués à un ou plusieurs DC qui sont alors chargés d'effectuer des traitements spécifiques.

Le tableau suivant décrit les rôles de maître d'opérations (FSMO) :

Périmètre	Rôle	Description
Forêt	Contrôleur de schéma	Contrôle les mises à jour du schéma
	Maître d'attribution de noms de domaine	Contrôle l'ajout et la suppression de domaines dans la forêt
Domaine	Maître des identifiants relatifs (RID)	Alloue des séquences d'identifiants relatifs aux contrôleurs de domaine de son domaine afin qu'ils puissent générer des SID pour chaque nouvel objet créé
	Maître d'émulateur du contrôleur principal de domaine (PDCe)	Traite les modifications de mot de passe, synchronise l'heure sur tous les contrôleurs de domaine, joue le rôle de contrôleur principal de domaine Windows NT (si des clients pre-Windows 2000 sont présents dans le domaine)
	Maître d'infrastructure	Assure la mise à jour des données dans un domaine

TABLE 6 – Description des rôles FSMO

R19 - Priorité 1

Dans un environnement composé d'une forêt mono-domaine, il est recommandé de placer tous les rôles FSMO sur un même DC. Dans un environnement multi-domaines, il est recommandé de suivre les règles suivantes lors du placement des rôles FSMO :
- placement du PDC sur une machine robuste dans un site AD ayant d'autres DC du même domaine ;
- placement du contrôleur de schéma sur le PDC du domaine racine ;
- placement du maître d'attribution de noms de domaine sur le PDC du domaine racine ;
- placement du maître RID sur le PDC du même domaine ;
- placement du maître d'infrastructure sur un DC non GC sauf si tous les DC sont GC.

3.4 Les stratégies de groupe

Une stratégie de groupe (Group Policy Object - GPO), est un ensemble de paramètres de configuration pouvant être appliqué à un groupe d'utilisateurs ou d'ordinateurs. Une stratégie de groupe est utilisée pour :
- imposer un niveau de sécurité ;
- créer des configurations communes ;
- simplifier le processus d'installation des ordinateurs ;
- limiter la distribution d'applications.

L'application des stratégies de groupe respecte l'ordre suivant :

1. stratégies de groupe locales à la machine ;
2. stratégies de groupe appliquées au niveau du site AD ;
3. stratégies de groupe appliquées au niveau du domaine ;

4. stratégies de groupe appliquées au niveau de chaque OU composant l'arborescence depuis la racine.

Les paramètres définis par une stratégie peuvent être écrasés par une autre stratégie qui est appliquée postérieurement. Par conséquent, les paramètres définis par la dernière GPO appliquée sont ceux qui seront utilisés.

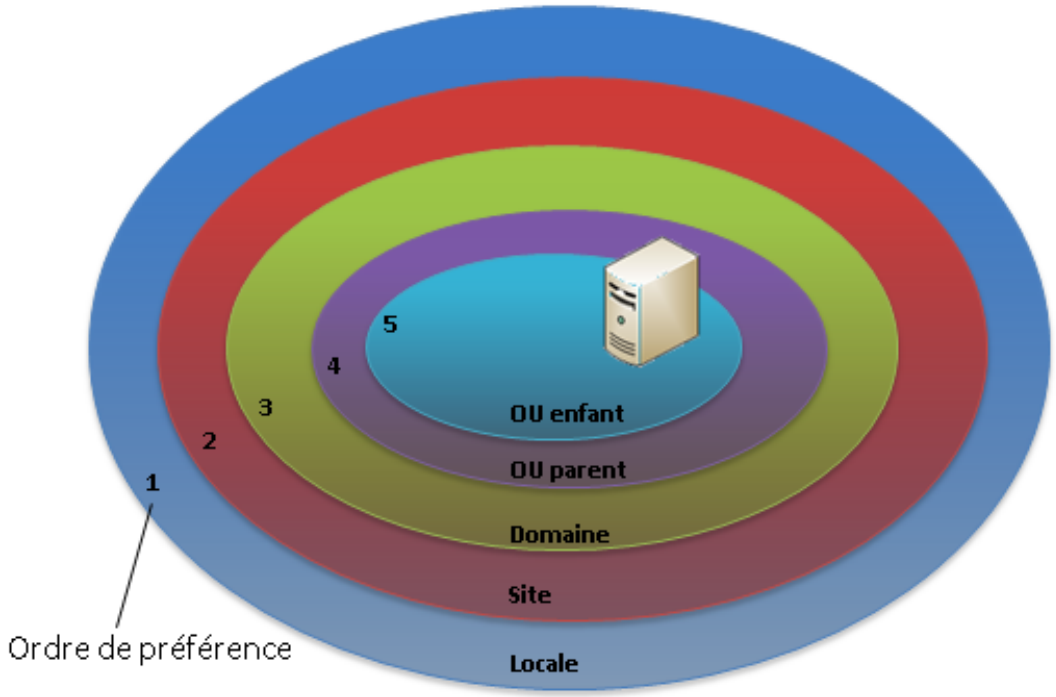

FIGURE 1 – Ordre d'application des stratégies de groupe

Une stratégie de groupe est divisée en deux parties pouvant être activées ou désactivées :

Ordinateur Décrit la configuration de l'ordinateur.

Utilisateur Décrit la configuration de l'environnement de l'utilisateur.

Enfin, une GPO intègre différents composants :

Composant	Description
Modèle d'administration	Configure la base de registre. Peut être enrichi par des modèles au format ".adm" (ou .admx depuis Windows Server 2008)
Sécurité	Configure les options de sécurité
Installation logicielle	Permet le déploiement de logiciels en s'appuyant sur la technologie Intellimirror
Scripts	Permet l'exécution de scripts lors de l'arrêt et du démarrage des ordinateurs et lors de la connexion et déconnexion des utilisateurs

TABLE 7 – Composants principaux d'une stratégie de groupe

3.4.1 Règles de nommage

Normaliser le nom des stratégies de groupes permet de les identifier rapidement.

R20 - Priorité 4

> Il est recommandé de définir une convention de nommage pour les stratégies de groupe pour y faire apparaître :
> – le type d'objet ciblé (Ordinateur ou Utilisateur) ;
> – la population ciblée (Site géographique, un applicatif, etc.).
> Par exemple, une GPO définissant des paramètres de sécurité d'Internet Explorer pour des utilisateurs (symbolisé par la lettre *U*) d'un site français pourrait se nommer *GPO-U-Fr-SécuritéIE*.

3.4.2 Règles d'implémentation

Le nombre de stratégies de groupe s'appliquant à un objet Active Directory peut fortement influencer les performances générales. En effet, des lenteurs peuvent être par exemple constatées lors du démarrage d'une machine ou de l'ouverture de session d'un utilisateur.

R21 - Priorité 4

> Il est recommandé de limiter le nombre de stratégies de groupe qui s'appliquent à un objet Active Directory afin de limiter les incidences sur les performances et le risque de redéfinition ou d'écrasement de paramètres.

R22 - Priorité 4

> Il est recommandé de désactiver la partie utilisateur ou ordinateur d'une GPO si aucun paramètre n'est configuré et de limiter l'utilisation de filtre WMI afin d'optimiser le temps de traitement d'application de la stratégie.

R23 - Priorité 4

> Il est recommandé de limiter l'utilisation de la fonctionnalité de blocage de l'héritage afin de ne pas complexifier l'administration.

R24 - Priorité 4

> Il est recommandé de ne pas lier une GPO à une même OU plus d'une fois : des comportements imprévisibles pourraient survenir.

3.5 Groupes de sécurité

Les groupes de sécurité constituent une méthode efficace pour autoriser l'accès aux ressources. Ils permettent d'effectuer les tâches suivantes :
– leur assigner des droits d'utilisateur ;
– leur assigner des autorisations sur les ressources.

Dans AD, des groupes prédéfinis existent. Parmi eux :

Admins du domaine Les membres de ce groupe ont des droits sur tous les objets du domaine AD. De fait, ils sont administrateurs locaux des machines.

Administrateurs de l'entreprise Les membres de ce groupe ont des droits sur tous les objets de la forêt AD. Ils sont également administrateurs locaux des machines.

Administrateurs du schéma Les membres de ce groupe peuvent modifier le schéma AD.

Propriétaires créateurs de la stratégie de groupe Les membres de ce groupe peuvent ajouter, supprimer ou modifier des GPOs. Ils peuvent donc s'octroyer des droits d'administration sur toutes les machines.

Accès compatible pré-Windows 2000 Autorise les membres de ce groupe à lire des propriétés sur des objets AD.

Générateurs d'approbations de forêt entrante Les membres de ce groupe peuvent créer des relations d'approbation unidirectionnelles entrantes.

Opérateurs de compte Les membres de ce groupe peuvent créer, supprimer et modifier les comptes utilisateurs et machines (sauf dans l'OU Contrôleurs de domaine). Ils sont donc administrateurs locaux.

Opérateurs de sauvegarde Les membres de ce groupe peuvent sauvegarder et restaurer des fichiers sur un DC ainsi qu'ouvrir une session sur ces derniers et les arrêter. Ces privilèges sont assimilés à ceux d'un administrateur local et donc de domaine puisque la machine visée est un DC.

Opérateurs d'impression Les membres de ce groupe peuvent gérer les objets de type imprimante dans l'annuaire et ouvrir une session sur les DC ainsi que les arrêter. Ces comptes sont donc assimilés à des administrateurs locaux du serveur et donc du domaine si la machine ciblée est un DC.

Opérateurs de serveur Les opérateurs de serveur peuvent ouvrir une session sur les DC, modifier l'heure du système, gérer les services, sauvegarder et restaurer des fichiers, arrêter la machine. Les membres de ce groupe sont également administrateurs locaux de la machine. Sur un DC, ils possèdent donc les mêmes privilèges que les administrateurs du domaine.

Des mécanismes de sécurité dans AD sont liés aux groupes de sécurité ayant des privilèges comme *AdminSDHolder* et les groupes restreints. *AdminSDHolder*[4] est un objet AD comparable à un modèle de référence. En effet, toutes les heures, le DC ayant le rôle maître d'émulateur du contrôleur principal de domaine compare les ACL de l'objet *AdminSDHolder* et les ACL des comptes membres de certains groupes privilégiés. Les ACL des comptes sont alors écrasées par les ACL de l'objet *AdminSDHolder* si une différence est détectée permettant ainsi de garantir leur intégrité.

R25 - Priorité 1

> Il est recommandé de surveiller les ACL positionnées sur l'objet *AdminSDHolder* de manière fréquente et régulière pour détecter tout changement.

Les groupes restreints sont utilisés pour contrôler les membres des groupes par GPO. À chaque fois qu'une GPO ayant le paramètre *groupes restreints* configuré est appliquée, la liste des membres des groupes concernés est écrasée permettant ainsi de garder son intégrité.

R26 - Priorité 1

> Afin de réduire les risques de compromission du domaine, il est nécessaire de restreindre le nombre de comptes ayant des droits d'administration sur le domaine entier.

4. Pour plus de détails sur l'AdminSDHolder : http://technet.microsoft.com/fr-fr/library/cc780336.aspx.

R27 - Priorité 1

> Il est recommandé de conserver les groupes Opérateurs toujours vides. En effet, être membre de certains de ces groupes prédéfinis se traduit par devenir Administrateur du domaine sur un DC. Il est alors conseillé de créer des groupes de sécurité afin de gérer les droits et ne pas utiliser ces groupes prédéfinis.

3.5.1 Périmètre des groupes

Il existe trois types de groupe : Universel, Global et Domaine local :

- les groupes Universels peuvent inclure des groupes et comptes provenant de n'importe quel domaine de la forêt et peuvent également se voir assigner des autorisations dans n'importe lequel de ces domaines. Le niveau fonctionnel doit cependant être en mode natif (tous les DC ont la même version du système d'exploitation) ;
- un groupe Global peut inclure d'autres groupes et comptes issus du domaine auquel il appartient et peut se voir assigner des autorisations dans n'importe quel domaine de la forêt ;
- un groupe de Domaine local peut inclure des groupes ou comptes issus de n'importe quel domaine Windows et peut se voir assigner des autorisations au sein de son domaine uniquement.

3.5.2 Utilisation des groupes de Domaine local

Les groupes de Domaine local aident à définir et à gérer l'accès aux ressources à l'intérieur d'un domaine. Les membres de ces groupes peuvent être :

- d'autres groupes de Domaine local ;
- des groupes Globaux ;
- des groupes Universels ;
- des comptes.

3.5.3 Utilisation des groupes Globaux

Les groupes Globaux ne sont pas répliqués à l'extérieur de leur domaine d'appartenance, les membres de ces derniers peuvent donc être modifiés sans provoquer de réplication sur le catalogue global. C'est pourquoi, leur utilisation est recommandée pour gérer les objets qui nécessitent une maintenance quotidienne comme les comptes d'utilisateurs et d'ordinateurs.

3.5.4 Utilisation des groupes Universels

Ce type de groupe utilisable uniquement en mode natif permet de consolider des groupes qui s'étendent sur plusieurs domaines. Pour cela, des groupes Globaux sont ajoutés comme membres des groupes Universels. Ainsi, une modification des groupes Globaux n'entraîne pas de réplication entre les domaines.

3.5.5 Modification de l'étendue de groupe

Par défaut, à la création d'un nouveau groupe, son étendue est Globale. Hormis pour les niveaux fonctionnels Windows 2000 mixte et Windows 2003 Intérim, il est possible de modifier l'étendue d'un groupe. En outre, les conversions suivantes sont possibles :

Global vers Universel Cette conversion n'est autorisée que si le groupe n'est pas membre d'un autre groupe Global.

Domaine local vers Universel Cette conversion n'est autorisée que si le groupe n'a pas comme membre un autre groupe de Domaine local.

Universel vers Global Cette conversion n'est autorisée que si le groupe n'a aucun autre groupe Universel comme membre.

Universel vers Domaine local Cette conversion n'est soumise à aucune restriction.

R28 - Priorité 4

Il est recommandé de respecter l'inclusion suivante afin de donner accès à une ressource d'un domaine à un utilisateur :

1. ajouter un compte utilisateur à un groupe Global ;
2. ajouter le groupe Global à un groupe Universel ;
3. ajouter le groupe Universel à un groupe de Domaine local ;
4. ajouter le groupe de Domaine local dans les ACL de la ressource pour y accéder.

3.5.6 Bouclage

Un bouclage survient lorsque l'imbrication de groupes est circulaire. Par exemple, un groupe A incluant un groupe B qui lui même contient le groupe A.

Active Directory n'est pas affecté par cette problématique, cependant, ce n'est pas toujours le cas pour les outils et applications liés à l'annuaire. En effet, ces derniers pourraient ne plus être opérationnels s'ils effectuent un traitement sur des groupes formant une boucle (risque de crash applicatif).

R29 - Priorité 4

Il est recommandé de vérifier régulièrement l'imbrication des groupes à l'aide d'un script afin d'éviter des bouclages.

3.5.7 Contrôle d'accès basé sur des rôles

Active Directory permet de définir un modèle de délégation des droits de manière simple et granulaire. En effet, il est possible d'attribuer des droits sur un périmètre donné (une unité d'organisation, un type d'objet, des attributs spécifiques, etc.).

R30 - Priorité 1

Il est recommandé de limiter le nombre de comptes Administrateur du domaine.

R31 - Priorité 1

Il est recommandé d'utiliser un modèle de délégation de droits octroyant le moins de pouvoir possible aux comptes utilisateurs. Cette précaution permet de limiter les risques d'élévation de privilèges d'un attaquant par rebonds successifs sur des machines.

3.5.8 Taille du ticket Kerberos

Lorsqu'un utilisateur ouvre une session Windows, l'autorité de sécurité locale (LSA) génère un ticket d'accès représentant le contexte de sécurité de l'utilisateur. Ce ticket contient l'identifiant de sécurité unique (SID) du compte utilisateur ainsi que les SIDs de tous les groupes dont il est membre dans le domaine dans lequel il s'authentifie. Le nombre de groupes dont l'utilisateur est membre est

directement proportionnel à la taille du ticket. Ce nombre ne peut toutefois pas excéder 1015 [5] : l'utilisateur ne pourra plus ouvrir de session Windows si ce nombre est dépassé.

Lors de la sortie de Windows 2000, la taille maximale du ticket Kerberos était de 8000 octets par défaut. Depuis Windows 2000 SP2, cette taille est passée à 12000 octets puis à 48000 octets avec Windows Server 2012.

R32 - Priorité 4

La taille du ticket Kerberos doit être maîtrisée : il est recommandé de ne pas dépasser celle par défaut. Dans ce but, il convient de :
- réduire le nombre de groupes de sécurité en les supprimant ou en les consolidant ;
- supprimer le SID History ;
- réduire le nombre de comptes utilisateur ayant le paramètre « Approuver cet utilisateur pour la délégation ». En effet, avec ce paramètre activé, la taille du ticket Kerberos pourrait doubler.

3.5.9 Règles de nommage

La définition d'une convention de nommage pour les groupes peut permettre une identification rapide de leurs fonctions ainsi qu'une facilité dans les tâches d'administration.

R33 - Priorité 4

Il est recommandé de définir une convention de nommage pour les groupes pour y faire apparaître :
- le type : groupe de sécurité ou groupe de distribution. Ce dernier type de groupe étant utilisé par les applications mail afin de diffuser un message à plusieurs destinataires ;
- l'étendue (Universel, Global, Domaine Local) ;
- les droits et privilèges octroyés ;
- la fonction (par exemple, une position hiérarchique, un nom de projet ou d'application, etc.).

Par exemple, *GS-PARIS-PDT-ADM* pourrait définir un nom de groupe de sécurité (S) d'étendue globale (G) dont les membres seraient les administrateurs (ADM) des postes de travail (PDT) du site de Paris.

3.6 Gestion des comptes

Les comptes utilisateurs et les comptes de service sont l'un des principaux vecteurs d'attaque dans un environnement AD. La compromission d'un compte local d'une station de travail peut parfois mener à une compromission de tout l'annuaire. De même, un compte de service ayant de forts privilèges peut rendre vulnérable l'ensemble du système d'information.

Il convient donc de définir un contrôle d'accès basé sur des rôles afin de limiter les risques d'élévation de privilèges par les attaques les plus répandues :

Pass-the-hash

Le système d'authentification sous Windows est basé sur des fonctions cryptographiques générant

5. http://technet.microsoft.com/fr-fr/library/active-directory-maximum-limits-scalability.aspx#BKMK_Groups

des empreintes des mots de passe des comptes. Dans un environnement Windows, les empreintes sont stockés à plusieurs endroits : dans la base du gestionnaire de comptes local (SAM) et/ou dans la base de données AD ainsi qu'en mémoire vive. Pour que cette attaque soit effective, il convient de récupérer l'empreinte d'un mot de passe (généralement en mémoire vive) puis de réutiliser cette empreinte telle quelle[6].

Accès à la base SAM
Cette base de données est un fichier binaire sur le disque local (*%windir%\System32\Config\SAM*) ainsi qu'une clé de registre (*HKLM\SAM\SAM*) qui contient toutes les informations de connexion des utilisateurs de la machine : le nom d'utilisateur et l'empreinte des mots de passe y sont stockés. Il est important d'être particulièrement sensible à ce chemin d'attaque dans des scénarios de clonage de la machine.

Cache de domaine
Par défaut, un serveur garde une trace (identifiant de connexion ainsi que l'empreinte du mot de passe) des dix dernières ouvertures de session.

Key logger
Logiciel malveillant installé capable d'enregistrer les évènements du clavier et donc de récupérer les mots de passe saisis par les utilisateurs.

R34 - Priorité 1

> Il est recommandé de mettre en place des mécanismes de restriction d'authentification distante des comptes locaux (en utilisant une GPO ainsi que le pare-feu local et l'UAC) pour filtrer les jetons d'accès privilégiés des comptes administrateurs locaux.

R35 - Priorité 1

> Il est recommandé de limiter la taille du cache de domaine sur les serveurs à 0 et sur les stations de travail à 1. En effet, les serveurs n'ont pas à vocation d'être déconnectés du réseau.

R36 - Priorité 1

> Il est recommandé de mettre en place une politique de gestion des objets de l'annuaire afin de prendre en compte les objets obsolètes (comptes qui ne sont plus utilisés, reliquats d'une migration, etc.), dormants (comptes n'ayant pas accès à l'annuaire devenant actifs pour effectuer une procédure spécifique comme par exemple une restauration) ou inactifs (comptes non utilisés depuis une date précise). Concernant les comptes de services, une procédure de modification des mots de passe est à prévoir (depuis 2008 R2, les comptes de services gérés permettent de répondre à cette problématique de manière satisfaisante). De plus, il convient de ne pas utiliser de mot de passe sans date d'expiration.

3.6.1 Stockage des secrets d'authentification

Dans un environnement Windows, les mots de passe des utilisateurs sont stockés à plusieurs endroits et sous différentes formes :

Active Directory
La base de données AD (NTDS.DIT) sur les DC contient les empreintes de tous les mots de

6. Les méthodes permettant d'atténuer l'exposition aux attaques de type *pass-the-hash* ont fait l'objet d'un article de Microsoft dont la version 2 date du 7 juillet 2014. L'article est disponible, en anglais, à l'adresse http ://www.microsoft.com/en-us/download/details.aspx ?id=36036.

passe ainsi que l'empreinte des anciens mots de passe utilisés (si l'historisation des mots de passe est activée). Seuls les RODCs ne possèdent qu'une partie des informations de connexions des comptes du domaine (seules les empreintes des mots de passe des utilisateurs mis en cache sont présents).

Base SAM

Stockée localement sur le disque dur, cette base contient les empreintes des mots de passe des comptes locaux. Par défaut, les mots de passe sont stockés sous la forme d'une empreinte NTLM et LM. Depuis Windows Vista, les empreintes des mots de passe au format LM ne sont plus stockées : seuls les empreintes NTLM sont utilisées.

Mémoire

Le processus LSASS enregistre les secrets en mémoire lors de l'authentification afin d'éviter à l'utilisateur de ressaisir ces informations à chaque accès réseau (répertoire partagé, boîte aux lettres Exchange, sites Intranet utilisant l'authentification Windows, etc.). Les informations de connexion sont stockées sous forme d'empreintes pour les mots de passe ou bien de tickets Kerberos.

3.6.2 Authentification

L'authentification Windows est un point clé dans une stratégie de sécurisation d'un environnement Microsoft et particulièrement dans un environnement Active Directory : les protocoles utilisés sont déterminants. Deux grandes familles de protocoles sont à distinguer : LanManager (ainsi que ses successeurs) et Kerberos. Du moins sécurisé au plus sécurisé, les protocoles suivants sont à distinguer : LM, NTLM et NTLMv2 puis Kerberos.

3.6.2.1 Protocoles

Les protocoles LM et NTLM opèrent de manière similaire ; leur différence réside dans l'empreinte du mot de passe. En effet, l'algorithme LM possède plusieurs faiblesses comme par exemple le fait que les caractères minuscules sont transformés en majuscules limitant ainsi le nombre de caractères utilisables.

NTLMv2 a été développé en réponse aux différentes attaques sur les protocoles LM et NTLM et est donc plus robuste à la cryptanalyse.

L'utilisation des protocoles est configurable avec un paramètre de stratégie de groupe nommé *Paramètre de sécurité/Stratégies locales/Options de sécurité/Sécurité réseau : Niveau d'authentification LAN Manager*. Plusieurs niveaux de configuration existent cependant, Microsoft élimine progressivement LM et NTLM (dont le principal problème est l'absence d'authentification du serveur par le client) au profit de Kerberos à l'aide de fonctions qui sont implémentées par Microsoft comme l'audit de l'utilisation de NTLM sur le domaine ou la mise en place de listes blanches ou noires des serveurs et clients pouvant utiliser NTLM.

R37 - Priorité 2

Il est recommandé de définir le paramètre *Paramètre de sécurité/Stratégies locales/Options de sécurité/Sécurité réseau : Niveau d'authentification LAN Manager* au niveau le plus haut possible. Au minimum, le niveau 3 doit être implémenté dans un premier temps afin de cibler le niveau 5 dans un second temps. Cette précaution permet de se protéger contre la cryptanalyse des empreintes de mots de passe récupérées lors d'une éventuelle écoute du réseau.

3.6.2.2 Authentification multi-facteurs

Une authentification est dite multi-facteurs lorsque celle-ci requiert au moins deux facteurs d'authentification de nature distincte, ceux-ci étant classiquement :

- ce que je suis (empreintes digitales, iris, etc.) ;
- ce que je sais (mot de passe, code PIN, etc.) ;
- ce que je possède (carte à puce, etc.).

L'authentification multi-facteurs n'apporte pas de réelle sécurité si l'authentification par simple mot de passe reste autorisée en parallèle.

Bien que ce mécanisme d'authentification soit souvent recommandé, il est toutefois important d'avoir conscience de ses limites du point de vue de la sécurité. Lorsqu'un compte utilisateur de l'AD est configuré pour utiliser une authentification par carte à puce uniquement, un nouveau mot de passe AD complexe sans expiration est automatiquement généré. Il est stocké dans l'annuaire AD sous forme d'une empreinte de mot de passe. Cette empreinte est transmise au poste client lorsqu'il s'authentifie sur l'AD par carte à puce et le garde en mémoire vive. Ensuite tout se passe exactement comme lors d'une authentification par simple mot de passe ; l'empreinte peut éventuellement être récupérée en mémoire vive par un attaquant puis utilisée par une attaque de type *Pass-the-hash* (y compris pour les authentifications Kerberos puisque l'empreinte sert de secret dans l'échange défi-réponse). L' annexe VII aborde plus en détail cette problématique.

R38 - Priorité 2

> Dès lors que l'authentification se fait uniquement par carte à puce, il est conseillé aux administrateurs de renouveler régulièrement les mots de passe générés automatiquement, puisqu'il n'est plus demandé aux utilisateurs de le faire.

3.6.3 Catégorisation des comptes

La catégorisation des comptes par rôles, la définition de cas d'usage précis, ainsi que la séparation des droits et privilèges doivent être effectuées de manière rigoureuse et selon la règle essentielle de *moindre privilège* (c'est-à-dire avoir le moins de privilèges possible). L'adoption d'un modèle de sécurité à base de rôles et de criticité est une étape stratégique de la démarche de sécurisation. Le modèle de sécurité doit être pensé pour être non seulement adapté au contexte métier de l'organisme, mais encore une fois, pour éviter qu'une simple compromission de poste de travail ne débouche sur une compromission de comptes privilégiés du domaine.

Un modèle découpé en plusieurs niveaux de criticité remplit généralement cet objectif. Il est important qu'un nombre suffisant de niveaux soient définis de manière à véritablement cloisonner les cas d'usage et limiter au maximum les risques d'élévation de privilèges. Une structure à quatre niveaux peut par exemple être définie de la manière suivante :

Niveau de criticité	Cas d'usage
Niveau 1 Comptes des simples utilisateurs du domaine sans droits ni privilèges spécifiques, pour des rôles tout à fait standards	Utilisés pour les ouvertures de session sur les postes de travail dans le but d'y effectuer des tâches ne nécessitant aucun droit ni privilège (navigation sur internet, bureautique, correspondance par courrier électronique, exécution d'applications, etc.) ainsi que pour l'accès à certains applicatifs par authentification centralisée. La majorité des rôles sont de niveau de criticité 1 dans la plupart des contextes métier.
Niveau 2 Comptes disposant de droits administrateurs ou de privilèges spécifiques sur un poste de travail en particulier.	Utilisés pour des ouvertures de sessions sur des postes de travail spécifiques, dans le but d'y effectuer exclusivement et de manière temporaire des tâches nécessitant des droits ou privilèges particuliers ne pouvant être réalisées avec un compte de niveau 1. Ces comptes sont normalement très peu utilisés et sont, par exemple, détenus par les rôles de support et de télé-assistance pouvant nécessiter des ouvertures de session interactive ou bien même, par certains utilisateurs ayant de fortes contraintes d'autonomie sur leur poste de travail.
Niveau 3 Comptes disposant de droits ou de privilèges sur une partie du domaine via des délégations d'unités organisationnelles ou des droits d'administration de serveurs, de services, d'applicatifs ou d'un ensemble de postes de travail.	Utilisés uniquement pour des tâches d'administration effectuées exclusivement par ouverture de sessions réseau et, ce qui est très important, sans ouverture de session interactive, qu'elles soient locales ou distantes. Ces comptes seront utilisés quotidiennement par les équipes de support et d'administration. L'organisation est alors décentralisée de manière à répartir les droits selon des périmètres de responsabilité fonctionnels ou géographiques. En fonction de la sensibilité des droits octroyés, il est recommandé que l'utilisation de ces comptes ne se fasse que depuis des postes d'administration dédiés à cet usage, c'est à dire au minimum : – le moins exposés possible à quelconque vecteur de compromission (ne servant donc pas à la navigation sur Internet, ni à l'utilisation d'applications de bureautique, ni à la consultation de courriers électroniques provenant d'Internet par exemple) ; – faisant l'objet d'un durcissement plus strict et d'une surveillance particulière ; – isolés dans des segments réseau filtrés en entrée comme en sortie par un pare-feu n'autorisant que les flux d'administration strictement nécessaires à leur activité.
Niveau 4 Comptes administrateurs du domaine.	Utilisés avec au minimum les mêmes contraintes que les comptes de niveau 3, et pour les seules tâches d'administration du domaine pouvant difficilement être déléguées à des comptes moins privilégiés. Il s'agit des seuls comptes disposant des droits d'administration du domaine Active Directory. Ils sont détenus par un nombre d'acteurs très limité et leur utilisation, aussi peu fréquente que possible, doit rester strictement temporaire.

Table 8 – Catégorisation des comptes d'utilisateur

Il est important de garder à l'esprit que la compromission des comptes de niveau 1 et 2 est vraisemblable. Leurs droits doivent donc être fortement limités et les mesures de sécurité mises en œuvre doivent permettre d'éviter une élévation de privilèges depuis ces derniers. Il doit par conséquent être formellement interdit (et idéalement impossible) d'utiliser une catégorie de compte à la place d'une autre, comme par exemple un compte utilisateur de niveau 1 pour l'administration d'un serveur ou un compte d'administration de niveau 3 pour ouvrir une session utilisateur sur un poste de travail bureautique pour naviguer sur Internet. Des exceptions temporaires peuvent toutefois être faites, comme par exemple en phase d'intégration d'un nouveau service, avec la vigilance nécessaire.

R39 - Priorité 1

> Adopter un modèle de sécurité définissant des rôles permettant de bien différencier les cas d'usage et les privilèges associés afin de limiter les possibilités d'élévation de privilèges.

L'annexe V rappelle certains points à considérer lors de la gestion des privilèges.

3.6.3.1 Comptes privilégiés

Le compte Administrateur est le seul compte privilégié prédéfini. Les autres comptes privilégiés seront donc nécessairement créés par des administrateurs de l'AD grâce à :
- l'appartenance à un groupe privilégié (prédéfini ou non) ;
- l'octroi manuel de privilèges.

Certains privilèges sont considérés comme particulièrement sensibles du point de vue de la sécurité du fait qu'ils peuvent permettre des élévations de privilèges aux utilisateurs qui se les voient octroyés (voir annexe V).

Remarque : l'attribut *adminCount* d'un objet AD, lorsque sa valeur est à *1*, traduit le fait qu'il a fait partie à un moment donné d'un groupe d'administration prédéfini. Cette valeur n'est jamais réinitialisée à *0* lorsque l'appartenance au groupe est supprimée. L'héritage des permissions AD ne s'appliquant pas sur les objets ayant la valeur à *1* dans cet attribut, des problèmes de sécurité peuvent alors survenir.

R40 - Priorité 1

> L'attribut *adminCount* doit être positionné à *1* uniquement sur les comptes membres d'un groupe d'administration protégé. Il est impératif de désactiver un compte lorsqu'il est retiré de la liste des membres d'un groupe d'administration protégé.

3.6.4 Règles de nommage

La définition d'une convention de nommage pour les utilisateurs peut permettre une identification rapide de leurs fonctions ainsi qu'une facilité dans les tâches d'administration.

Dans un premier temps, il est important de pouvoir identifier par leur nom les comptes de service utilisés par des processus et non par un individu. Les mots de passe des comptes de service sont nécessairement stockés d'une manière ou d'une autre sur la machine (en base de registre, dans des fichiers de configuration ou même codés en dur dans les applications, etc.), ce qui leur confère une certaine faiblesse en termes de sécurité. Des comptes de service courants sont par exemple :
- des comptes utilisés pour démarrer des tâches planifiées ;
- des comptes utilisés dans des scripts (Batch, PowerShell, etc.) ;

– des comptes utilisés pour démarrer des applications ou utilisés en interne dans des applications ;
– des comptes utilisés pour exécuter des objets COM, des Workers IIS, etc.

R41 - Priorité 4

Il est recommandé de définir une convention de nommage pour les utilisateurs pour y faire apparaître :
– le nom (les comptes attribués à des individus doivent être nominatifs et leurs propriétaires doivent être identifiables dans l'annuaire par une règle simple)
– le type (permet d'identifier un compte utilisé par une personne ou un compte de service) ;
– les droits et privilèges octroyés (compte d'administration, compte privilégié) ;
– la fonction (par exemple, une position hiérarchique, un nom de projet ou d'application, etc.).
Par exemple :
– le compte de l'utilisateur nommé Jean Dupont pourrait être *jdupont* (première lettre du prénom et son nom) et son compte Administrateur *jdupont-adm* ;
– le compte de service utilisé par le site Intranet d'une entreprise pourrait se nommer *SVC-Intranet*.

3.6.5 Scripts

Il est courant d'exécuter des scripts au démarrage ou à l'arrêt d'une machine ainsi qu'à l'ouverture ou la fermeture d'une session de l'utilisateur.

R42 - Priorité 1

Aucun mot de passe ne doit apparaître dans les scripts. Il est possible d'utiliser l'authentification Kerberos, un compte de service, etc.

3.6.6 Sécurité des comptes

La gestion des comptes est un point sensible dans un annuaire et doit donc être un point d'attention particulier.

3.6.6.1 Mots de passe

R43 - Priorité 1

Configurer une politique de sécurité des mots de passe imposant techniquement un niveau déterminé de complexité en fonction de la criticité du compte dans le modèle de contrôle d'accès adopté. Dans un domaine AD avec un niveau fonctionnel 2008 ou supérieur, il est possible de définir plusieurs stratégies de mot de passe.

Note : Les niveaux de complexité imposés doivent dépendre des niveaux de criticité de chaque type de compte dans l'organisation de l'annuaire. L'annexe VIII donne un exemple de politique de complexité des mots de passe. Il est également recommandé de se référer à la note précisant les recommandations de sécurité relatives aux mots de passe [7] publiée par l'ANSSI.

7. http ://www.ssi.gouv.fr/IMG/pdf/NP_MDP_NoteTech.pdf.

R44 - Priorité 1

> Configurer une politique d'expiration des mots de passe s'appliquant à tous les types de comptes, y compris les comptes d'administration ou de service. Depuis 2008, il est possible de définir plusieurs stratégies de mot de passe facilitant ainsi la mise en œuvre de cette recommandation.

Note :
- la durée d'expiration des mots de passe dépend des résultats d'une analyse de risques. Il est toutefois important de considérer le fait qu'un changement de mot de passe trop rapproché dans le temps peut conduire à des oublis et donc à des mauvaises pratiques de la part des utilisateurs, sans pour autant renforcer le niveau de sécurité global ;
- la règle d'expiration des mots de passe peut admettre certaines exceptions concernant les comptes de service si des contraintes de fonctionnement n'admettent pas la moindre interruption. Dans ce cas, de tels comptes devront faire l'objet d'une surveillance particulière et constante.

3.6.6.2 Comptes inactifs

Le choix de la durée d'inactivité dépend des résultats d'une analyse de risques.

R45 - Priorité 1

> Mettre en place une politique de désactivation automatique des comptes non utilisés pendant un certain laps de temps.

R46 - Priorité 3

> Tout compte désactivé doit perdre l'ensemble de ses droits et privilèges et être déplacé dans une unité organisationnelle prévue à cet effet.

R47 - Priorité 3

> Tout compte désactivé peut être facilement réactivé, il est donc primordial d'enlever ses droits et privilèges. Par contre, il est conseillé de ne pas supprimer les comptes désactivés, de manière à garder une trace des comptes utilisateurs qui ont été en vigueur dans le système d'information.

4 Mesures organisationnelles préventives

Les mesures de sécurité doivent être considérées dans leur ensemble et avec la même rigueur, qu'elles soient techniques ou organisationnelles. Une approche partielle dans la mise en œuvre de mesures organisationnelles peut fortement réduire l'efficacité des mesures de sécurité techniques.

Il convient également de rappeler que les mesures de sécurité se focalisent bien trop souvent, et à tort, sur la seule protection du périmètre extérieur. Pourtant les vols de données sensibles provenant de l'intérieur ne doivent pas être négligés. Les mesures organisationnelles prennent alors tout leur intérêt.

4.1 Gestion des ressources humaines

Les aspects relatifs à la gestion des ressources humaines ne doivent pas être sous-estimés. Des actes malveillants ou de négligence passés inaperçus peuvent se traduire par une compromission invisible et

durable au cœur même du système d'information.

R48 - Priorité 1

> Sensibiliser régulièrement les administrateurs à l'administration sécurisée d'AD, et plus particulièrement à l'état des menaces et des attaques, ainsi qu'aux bonnes réactions à avoir en cas d'incident.

R49 - Priorité 2

> Faire en sorte que les administrateurs de l'annuaire AD soient régulièrement formés non seulement à l'administration AD mais également aux règles de gestion de l'annuaire qu'ils administrent, de manière à limiter les mauvaises pratiques ou négligences.

R50 - Priorité 2

> Procéder à un roulement des administrateurs dans les différentes tâches qui relèvent de l'administration de l'annuaire Active Directory, de façon à détecter toute éventuelle négligence d'exécution par un traitant ou toute malveillance qui pourrait sans cela passer inaperçue.

Note : Il s'agit d'une mesure de sécurité organisationnelle qui s'applique d'une manière générale à toute tâche d'administration.

R51 - Priorité 3

> Disposer de suffisamment de ressources humaines d'un niveau d'expertise sur l'AD dans l'optique :
> – d'assurer une continuité de service en cas de crise ;
> – d'assurer le roulement des tâches d'administration.

4.2 Intégrer la gestion des comptes dans les processus métier

Les processus relatifs aux départs, arrivées ou mutations de personnel par exemple devraient intégrer de manière fiable et systématique les opérations de gestion des comptes utilisateurs dans l'annuaire. Ceci inclut :

- la désactivation des comptes utilisateurs, accompagnée des règles de traitement associées telles que la suppression des droits ou le déplacement des comptes dans des OU spécifiques ;
- la création des comptes avec des droits et privilèges selon des règles et rôles formalisés et non à la libre appréciation d'un individu.

4.3 Audits et amélioration continue

La fréquence des audits et des revues est à définir en adéquation avec les résultats d'analyses de risques.

R52 - Priorité 1

> Effectuer une revue régulière de la pertinence des droits et privilèges accordés aux différents comptes privilégiés (comptes d'administration, comptes de machine, de service, etc.), puis traiter les anomalies mises en évidence.

Note : La détection d'une anomalie doit faire l'objet d'une alerte de sécurité remontée à la direction. Elle ne doit pas être simplement corrigée sans chercher à savoir comment elle est apparue et si elle a pu avoir un quelconque impact. Il est fréquent qu'une simple anomalie soit signe de compromission mais ne soit pas considérée comme telle.

R53 - Priorité 1

> Commanditer des audits réguliers de l'annuaire Active Directory, idéalement réalisés par des organismes ou services indépendants.

Note : L'ANSSI a publié un référentiel d'exigences[8] qui pourra permettre de sélectionner un prestataire d'audit de la sécurité des systèmes d'information (PASSI).

8. http ://www.ssi.gouv.fr/IMG/pdf/RGS_PASSI_v2-0.pdf.

Annexes

Annexe I :
Acronymes et terminologie

Nom ou sigle	Autre nom d'usage	Définition
ACL	Access Control List	Liste des permissions contrôlant l'accès à un objet de type fichier, imprimante ou Active Directory
AD	Active Directory	Service d'annuaire de Microsoft Windows 2000 ou plus récent
ADWS	Active Directory Web Services	Permet la gestion d'un annuaire Active Directory avec des services Web
Attribut	-	Caractéristique d'un objet de l'annuaire
API	Application Programming Interface	Interface de programmation
DC	Domain Controler	Contrôleur de domaine
DFS	Distributed File System	Système de fichier distribué
DHCP	Dynamic Host Configuration Protocol	Protocole réseau utilisé pour configurer les paramètres IP d'une machine
DNS	Domain Name System	Système de résolution de noms
DPAPI	Data Protection API	Interface de programmation développée pour la protection des données
ESE	Extensible Storage Engine	Moteur de base de données
FSMO	Flexible Single Master Operation	Rôle d'un contrôleur de domaine
GPO	Group Policy Object	Objet de stratégie de groupe
ICMP	Internet Control Message Protocol	Protocole réseau utilisé pour des messages de contrôle et d'erreur
KDC	Key Distribution Center	Système permettant un échange de clés sécurisé
LAN	Local Area Network	Réseau local
LDAP	Lightweight Directory Access Protocol	Protocole réseau utilisé lors du questionnement et lors de la modification d'un annuaire
LM	LAN Manager	Protocole utilisé lors de l'authentification
LSA	Local Security Authority	Système gérant l'authentification et les autorisations d'accès sur un système Windows
MPSSVC	Microsoft Protection Service	Service chargé de la protection du système (pare-feu)
NTLM	NT LAN Manager	Protocole utilisé lors de l'authentification
NTP	Network Time Protocol	Protocole réseau synchronisant l'horloge d'une machine sur une référence de temps
OID	Object Identifier	Identifiant d'objet

Nom ou sigle	Autre nom d'usage	Définition
OU	Unité Organisationnelle	Conteneur Active Directory permettant de hiérarchiser les objets de l'annuaire
PDC	Primary Domain Controler	Contrôleur de domaine primaire
RODC	Read Only Domain Controller	Contrôleur de domaine en lecture seule
SAM	Security Accounts Manager	Gestionnaire de comptes utilisé pour le stockage sécurisé des identifiants
SID	Security IDentifier	Identifiant unique généré par un contrôleur de domaine lors de la création d'un nouvel objet
SMB	Server Message Block	Protocole réseau utilisé lors du partage de ressources sur un réseau Microsoft
SMTP	Simple Mail Transfer Protocol	Protocole réseau pouvant être utilisé dans la réplication inter-sites Active Directory
SPN	Service Principal Names	Nom défini par un ordinateur lorsqu'il rejoint un domaine et lorsqu'un service est installé sur celui-ci
WINS	Windows Internet Naming Service	Système de résolution de noms dans un environnement Microsoft

Table 9 – Acronymes et terminologie

Annexe II : Journalisation

Pour les systèmes XP/2003, les stratégies locales suivantes doivent être paramétrées pour journaliser les opérations (par GPO, dans la partie *Configuration Ordinateur/Paramètres Windows/Paramètre de sécurité/Stratégies locales/Stratégies d'audit*) :

- auditer l'accès au service d'annuaire (opération réussie, échec) ;
- auditer l'accès aux objets (non défini)[1] ;
- auditer l'utilisation des privilèges (non défini)[1] ;
- auditer la gestion des comptes (opération réussie, échec) ;
- auditer le suivi des processus (opération réussie, échec)[2] ;
- auditer les évènements de connexions (opération réussie, échec) ;
- auditer le suivi des connexions aux comptes (ou évènement de connexion) (opération réussie, échec) ;
- auditer les évènements système (opération réussie, échec) ;
- auditer les modifications de stratégie (opération réussie, échec).

Pour les systèmes Vista/2008 et plus récents, il est recommandé d'activer la journalisation avancée (segmentée en sous-catégories) grâce au paramètre de GPO *Audit : force les paramètres de sous-catégorie de stratégie d'audit à se substituer aux paramètres de catégorie de stratégie d'audit* et d'activer la journalisation des opérations suivantes a minima :

- connexion de compte :
  - auditer la validation des informations d'identification (opération réussie, échec) ;
  - auditer le service d'authentification Kerberos (opération réussie, échec) ;
  - auditer les opérations de ticket du service Kerberos (opération réussie, échec) ;
  - auditer d'autres évènements d'ouverture de session (opération réussie, échec).
- gestion du compte :
  - auditer les gestion des groupes d'applications (non défini) ;
  - auditer la gestion des comptes d'ordinateur (opération réussie, échec) ;
  - auditer la gestion des groupes de distribution (opération réussie, échec) ;
  - auditer d'autres évènements de gestion des comptes (opération réussie, échec) ;
  - auditer la gestion des groupes de sécurité (opération réussie, échec) ;
  - auditer la gestion des comptes d'utilisateur (opération réussie, échec).
- suivi détaillé :
  - auditer l'activité DPAPI (opération réussie, échec) ;
  - auditer la création de processus (opération réussie, échec)[2] ;
  - auditer la fin du processus (non défini) ;
  - auditer les évènements RPC (non défini).
- accès DS :
  - auditer la réplication du service d'annuaire détaillé (non défini) ;
  - auditer l'accès au service d'annuaire (opération réussie, échec) ;
  - auditer les modifications du service d'annuaire (non défini)[1] ;
  - auditer la réplication du service d'annuaire (opération réussie, échec).
- ouvrir/fermer la session :
  - auditer le verrouillage de compte (opération réussie, échec) ;
  - auditer le mode étendu IPsec (non défini) ;

1. Ce paramètre pourra être défini pour un besoin d'analyse ponctuel. Le nombre important d'évènements générés ne permet pas de l'utiliser sur le long terme.
2. Ce paramètre peut générer une grande quantité d'évènements. Il est recommandé de l'appliquer au minimum sur les contrôleurs de domaine.

  - auditer le mode principal IPsec (non défini) ;
  - auditer le mode rapide IPsec (non défini) ;
  - auditer la fermeture de session (opération réussie) ;
  - auditer l'ouverture de session (opération réussie, échec) ;
  - auditer le serveur NPS (Network Policy Server) (opération réussie, échec) ;
  - auditer d'autres évènements d'ouverture/fermeture de session (opération réussie, échec) ;
  - auditer l'ouverture de session spéciale (opération réussie, échec).
- accès à l'objet :
  - auditer l'application générée (non défini) ;
  - auditer les services de certification (non défini) ;
  - auditer le partage de fichier détaillé (non défini)[1] ;
  - auditer le partage de fichier (non défini)[1] ;
  - auditer le système de fichier (non défini) ;
  - auditer la connexion de la plateforme de filtrage (non défini) ;
  - auditer le rejet de paquet parla plateforme de filtrage (non défini)[1] ;
  - auditer la manipulation de handle (non défini) ;
  - auditer l'objet de noyau (non défini) ;
  - auditer d'autres évènements d'accès à l'objet (opération réussie, échec) ;
  - auditer le registre (non défini) ;
  - auditer SAM (non défini).
- changement de stratégie :
  - auditer la modification de la stratégie d'audit (opération réussie, échec) ;
  - auditer la modification de la stratégie d'authentification (opération réussie, échec) ;
  - auditer la modification de la stratégie d'autorisation (opération réussie, échec) ;
  - auditer la modification de la stratégie de plate-forme de filtrage (opération réussie, échec) ;
  - auditer la modification de la stratégie de niveau règle MPSSVC (opération réussie, échec) ;
  - auditer d'autres évènements de modification de stratégie (échec)[1].
- utilisation de privilège :
  - auditer l'utilisation de privilèges non sensibles (non défini) ;
  - auditer d'autres évènements d'utilisation de privilèges (non défini) ;
  - auditer l'utilisation de privilèges sensibles (non défini)[1].
- système :
  - auditer le pilote IPSEC (non défini) ;
  - auditer d'autres évènements système (opération réussie, échec) ;
  - auditer la modification de l'état de la sécurité (opération réussie) ;
  - auditer l'extension du système de sécurité (opération réussie) ;
  - auditer l'intégrité du système (opération réussie, échec).
- Audit de l'accès global aux fichiers :
  - Système de fichiers (non défini)[1] ;
  - Registre (non défini)[1].

Annexe III :
Outils

Le tableau suivant liste quelques outils liés à l'administration et à la sécurisation d'un environnement Active Directory.

Nom de l'outil	Description
ADSIEdit	Console de gestion Microsoft utilisée pour visualiser tous les objets de l'annuaire (schéma, configuration et domaine). Permet également de modifier les objets et les ACL sur ces objets
DCDIAG	Vérifie la santé d'un DC
DNSCMD	Vérifie les enregistrements DNS dynamiques, liste les zones DNS
DSACLS	Visualise et modifie les ACL sur les objets AD
DSAStat	Permet de comparer deux arborescences AD et de fournir des statistiques
GPMC	Console de gestion des stratégies de groupe
GPOTOOL	Liste les GPOs d'un domaine et vérifie leur état sur tous les DCs
KLIST	Vérifie, liste et purge les tickets Kerberos
LDP	Permet d'effectuer des opérations LDAP sur un annuaire AD
NETDIAG	Vérifie de bout en bout le réseau et les fonctions de services distribuées
NLTest	Teste les relations d'approbation et l'état de réplication d'un DC. Permet également de tester et réinitialiser le canal sécurisé du service NetLogon établi entre le client et le DC
REPAdmin	Vérifie la consistance des réplications entre les partenaires de réplication
REPLMon	Affiche la topologie de réplication, force la réplication et le recalcul du KCC
RSAT	Suite d'outils d'administration à distance (extension des consoles MMC)
Security Configuration Wizard	Aide à limiter la surface d'attaque d'un serveur Windows
Setspn	Permet la gestion des noms SPN

Table 10 – Liste d'outils Active Directory.

Annexe IV :
Ports et protocoles

Le tableau suivant liste les ports et protocoles utilisés par Active Directory :

Ports	**Type de trafic**	**Outil ou technologie**
-	ICMP	
TCP 25	SMTP	Réplication par SMTP
TCP/UDP 42	WINS	WINS
TCP/UDP 53	DNS	DNS
TCP/UDP 88	Kerberos	Key Distribution Center
UDP 123	NTP/SNTP	Service de Temps
TCP 135, dynamique	RPC Endpoint Mapper, ECM	LSA, Réplication
UDP 137	NetBIOS	Résolution de noms NetBIOS
UDP 138	NetBIOS	Service de datagramme NetBIOS
TCP/UDP 389	LDAP	Requête sur l'annuaire
TCP/UDP 445	DFS, LsaRpc, NbtSS, NetLogonR, SamR, SMB, SMB2, CIFS, SrvSvc	Contrôleur de domaine
TCP/UDP 464	Kerberos	Modification et définition des mots de passe
TCP 636	LDAPS	Requêtes sur l'annuaire (TLS)
TCP 3268	MS Global Catalog	Contrôleur de domaine
TCP 3269	MS Global Catalog SSL	LSA
TCP 9389	SOAP	ADWS

Table 11 – Liste des ports et protocoles utilisés dans un environnement Active Directory

Note : La plage de ports dynamiques mentionnée est comprise entre 1025 et 5000 par défaut sur les systèmes Windows Server 2003 et antérieurs et entre 49152 et 65535 à partir de Windows Server 2008.

Annexe V :
Rappels concernant les comptes et privilèges

Il convient de considérer les comptes suivants comme des comptes disposant de privilèges particuliers :

- les comptes appartenant à un groupe d'administration prédéfini de l'AD présent par défaut : Admins domaine, Administrateurs de l'entreprise, Opérateurs de compte, etc. ;
- les comptes membres des groupes locaux « Administrateurs » de serveurs ou de plusieurs postes de travail ;
- les comptes ayant au moins un privilège sensible sur des serveurs ou des postes de travail ;
- les comptes ayant une délégation d'administration sur tout ou partie de l'AD ;
- les comptes propriétaires d'un objet (de type utilisateur, groupe, ordinateur, GPO, etc.) dans l'AD ;
- les comptes étant approuvés pour la délégation d'administration (une des 3 formes possibles) ;
- les comptes de relation d'approbation inter-domaines.

Annexe VI :
Droits et privilèges

Les systèmes Microsoft Windows proposent nativement un certain nombre de droits et privilèges qui permettent différentes actions aux utilisateurs qui se les voient octroyés (les éléments en gras sont considérés comme particulièrement sensibles du point de vue de la sécurité du fait qu'ils peuvent permettre des élévations de privilèges) :

Nom	Description
SeAssignPrimaryTokenPrivilege	Assigner un nouveau jeton à un processus
SeAuditPrivilege	Créer des événements dans les journaux de sécurité
SeBackupPrivilege	Accéder à tout objet, sans prise en compte de ses ACL, de manière à pouvoir effectuer une sauvegarde
SeChangeNotifyPrivilege	Permet à un utilisateur de traverser un dossier auquel il n'a pas accès. Ce privilège est par défaut octroyé à tout le monde
SeCreateGlobalPrivilege	Créer des objets tels que des liens symboliques dans des espaces de noms de gestionnaires d'objets d'autres sessions
SeCreatePagefilePrivilege	Créer un fichier de pagination
SeCreatePermanentPrivilege	Créer des objets qui seront permanents et ne seront pas désalloués lorsqu'ils ne seront plus utiles. Peut entraîner une consommation de ressources excessive
SeCreateSymbolicLinkPrivilege	Création de liens symboliques
SeCreateTokenPrivilege	Créer un objet-jeton, pour par exemple devenir un autre utilisateur
SeDebugPrivilege	Déboguer les programmes. Permet par extension d'injecter du code dans un processus ou de faire un dump de la mémoire pour par exemple obtenir des empreintes de mots de passe
SeEnableDelegationPrivilege	Permettre à l'ordinateur et aux comptes d'utilisateurs d'être approuvés pour la délégation. Permet également la création d'objets-jetons
SeImpersonatePrivilege	Emprunter l'identité d'un client après l'authentification
SeIncreaseBasePriorityPrivilege	Changer la priorité d'un processus
SeIncreaseQuotaPrivilege	Changer la quantité de mémoire allouée à un processus
SeIncreaseWorkingSetPrivilege	Changer la quantité d'espace de travail en mémoire virtuelle
SeLoadDriverPrivilege	Charger et décharger les pilotes de périphériques. Les pilotes peuvent potentiellement contenir du code malveillant qui sera exécuté dans le noyau et sans aucune restriction
SeLockMemoryPrivilege	Empêcher la pagination de certaines pages mémoire
SeMachineAccountPrivilege	Ajouter des ordinateurs au domaine
SeManageVolumePrivilege	Exécuter certaines tâches directement sur un volume disque
SeProfileSingleProcessPrivilege	Récolter des données relatives à la performance du préchargement de fichiers d'un processus
SeRelabelPrivilege	Changer le nom de n'importe quel objet quelles que soient ses ACL
SeRemoteShutdownPrivilege	Éteindre la machine à distance

Nom	Description
SeRestorePrivilege	Restaurer les fichiers et les répertoires
SeSecurityPrivilege	Gérer le journal d'audit et de sécurité
SeShutdownPrivilege	Éteindre la machine
SeSyncAgentPrivilege	Lire tous les objets et du domaine AD et leurs propriétés
SeSystemEnvironmentPrivilege	Modifier des variables d'environnement dans les NVRAM
SeSystemProfilePrivilege	Récolter des données relatives à la performance du système en général
SeSystemtimePrivilege	Changer l'heure du système
SeTakeOwnershipPrivilege	Prendre possession de fichiers ou d'autres objets
SeTcbPrivilege	Agir en tant que partie du système d'exploitation
SeTimeZonePrivilege	Changer le fuseau horaire du système
SeTrustedCredManAccessPrivilege	Accès avancé au sous-système de gestion des crédences. Par défauts seuls les processus WinLogon et LSASS disposent de ce privilège
SeUndockPrivilege	Retirer de manière logicielle un portable de sa station d'accueil

TABLE 12 – Droits et privilèges

Les comptes qui se voient octroyer certains privilèges sensibles doivent donc être considérés avec le niveau de criticité qui convient.

Annexe VII : Précisions concernant l'authentification par carte à puce en environnement AD

Lorsqu'un compte utilisateur de l'AD est configuré en authentification par carte à puce uniquement, un nouveau mot de passe AD complexe lui est automatiquement généré et sans expiration. Celui-ci est stocké dans l'annuaire AD sous forme d'une empreinte de mot de passe. Cette empreinte est transmise aux postes clients qui la gardent en mémoire lorsqu'ils s'authentifient sur l'AD par carte à puce. Ensuite tout se passe exactement comme lors d'une authentification par simple mot de passe, l'empreinte pouvant éventuellement être récupérée en mémoire vive par un attaquant puis utilisée par Pass-the-hash (y compris pour les authentifications Kerberos puisque l'empreinte sert de secret dans l'échange défi-réponse).

En mode d'authentification standard par mot de passe, l'utilisateur peut changer son mot de passe, réinitialisant de fait l'empreinte. Par contre, en authentification par carte à puce, le changement de mot de passe opéré par un utilisateur, bien que s'effectuant par la même interface graphique, ne change que le code PIN de déverrouillage de sa carte à puce et non pas le mot de passe AD. Autrement dit, le mot de passe de l'utilisateur dans l'AD, et donc son empreinte, restent inchangés.

Il est malgré tout possible et facile de changer ces mots de passe de manière propre et légitime dans l'AD en utilisant la fonction de « réinitialisation de mot de passe » (graphiquement dans une MMC, par script PowerShell ou bien directement en RPC par exemple). Les utilisateurs n'ont par défaut pas cette permission qui est seulement donnée aux comptes privilégiés du domaine. Il est alors possible, par script, de réinitialiser tous les mots de passe des comptes utilisateurs s'authentifiant par carte à puce (la permission peut être octroyée à un compte de service par exemple). Le seul effet de bord d'un tel script serait qu'une session utilisateur ouverte dont l'empreinte a entre-temps été changée dans l'annuaire n'a alors plus de jeton d'authentification valide en mémoire vive, obligeant donc à fermer (ou verrouiller) puis rouvrir (ou déverrouiller) la session. Cet effet de bord est toutefois minime puisque la procédure de réinitialisation des mots de passe n'a pas de raison de se dérouler fréquemment ni pendant les horaires de travail.

Annexe VIII :
Complexité des mots de passe

En environnement Active Directory, les niveaux de complexité de mots de passe suivants sont recommandés :

- niveau *moyen* : au moins 10 caractères comprenant au minimum 3 des 5 catégories suivantes : minuscules, majuscules, caractères alphanumériques, caractères spéciaux et caractères accentués ;
- niveau *fort* : au moins 12 caractères comprenant minuscules, majuscules, caractères alphanumériques, caractères spéciaux et caractères accentués ;
- niveau *extrême* : génération aléatoire d'un minimum de 15 caractères comprenant minuscules, majuscules, caractères alphanumériques, caractères spéciaux et caractères accentués.

Le niveau de complexité minimum à associer à chaque niveau de criticité des comptes dans l'organisation Active Directory dépend des résultats de l'analyse de risques. Une telle stratégie pourrait être la suivante :

- comptes de niveau 4 : complexité *extrême* ;
- comptes de niveau 3 : complexité *forte* ;
- comptes de niveau 2 : complexité *forte* ;
- comptes de niveau 1 : complexité *moyenne*.

La stratégie de complexité dépend fortement du contexte. Par exemple, lorsque les utilisateurs s'authentifient exclusivement par carte à puce, la complexité des comptes de niveau 1 peut être augmentée à *forte*.

Il est également important de noter que depuis 2008, de multiples stratégies de mots de passe peuvent être définies dans un domaine Active Directory.