cyberelements

Déployer du PAM en respectant les principes du silotage AD (« AD tiering »)

Introduction

A presque 25 ans, l'annuaire **Active Directory** de Microsoft a su grandir en maturité et a toujours le vent en poupe auprès d'une grande majorité des directions informatiques. Son rôle est **crucial au sein d'un système d'information** car c'est souvent à lui que l'on confie l'ensemble des services d'identification et d'authentification d'une organisation.

Il est donc primordial de renforcer sa protection, surtout dans le contexte actuel où les cyber-menaces ne cessent de s'amplifier. Prendre le contrôle de l'annuaire Active Directory d'une organisation équivaut à prendre le contrôle de ses données, et on peut aisément imaginer ce qu'une personne malveillante pourrait en faire. Une attaque de type « Golden Ticket » par exemple, permettrait à un cybercriminel doté d'un outil tel que Mimikatz, d'extraire le hash du mot de passe d'un compte d'administration authentifié pour accéder à la totalité des objets d'un domaine Active Directory, donc à l'ensemble des serveurs et des contrôleurs de domaines. Dans son document PA-022 « Recommandations relatives à l'administration sécurisée des systèmes d'information », l'ANSSI explique dans sa recommandation R28 que le ou les annuaires contenant les comptes d'administration doivent être protégés en confidentialité et en intégrité et ne doivent pas être exposés sur des environnements de moindre confiance.

L'ANSSI précise aussi que dans le cas spécifique d'un système d'information (SI) administré reposant sur un annuaire Microsoft Active Directory, il est recommandé **en premier lieu d'adopter un modèle de gestion des comptes à privilèges** (modèle en trois tiers) pour cet annuaire et de **sécuriser sa configuration**. Cette recommandation précise également que des mesures techniques complémentaires restreignant l'emploi des comptes d'administration sur les postes de travail doivent être mises en œuvre.

Il est donc primordial que l'ensemble de ces mesures et de ces recommandations soient appliquées lors des actes d'administration dans des environnements critiques.

Les solutions de gestion de comptes à privilèges (PAM) vont donc devoir s'interfacer dans ces contextes de protection Active Directory, et ce, sans amoindrir le niveau de sécurité attendu.

Dans ce document, nous détaillons les aspects du silotage Active Directory et nous présentons comment mettre en œuvre facilement une solution PAM comme cyberelements pour apporter une couverture optimale en termes de sécurité.

1

Silotage Active Directory

Le principe

Le cloisonnement

Microsoft propose depuis Active Directory 2012 R2, un **modèle d'administration multi-niveaux qui permet de partitionner les secrets d'authentification.**

Dans le modèle en trois tiers que recommande l'ANSSI, un silotage permet de référencer un ensemble de ressources en fonction de leurs criticités et d'affecter à chacun des tiers, des comptes d'administration dédiés pour protéger les secrets d'authentification.

En fait, on cloisonne sur trois niveaux d'administration les différentes strates de l'infrastructure du système d'information pour garantir qu'en cas de cyber-attaque, un poste de travail corrompu ne vienne corrompre les serveurs d'infrastructure et les contrôleurs de domaine Active Directory qui abritent les secrets d'authentification. L'objectif est de limiter les déplacements latéraux d'un attaquant entre les différents tiers.

La description des tiers est la suivante :

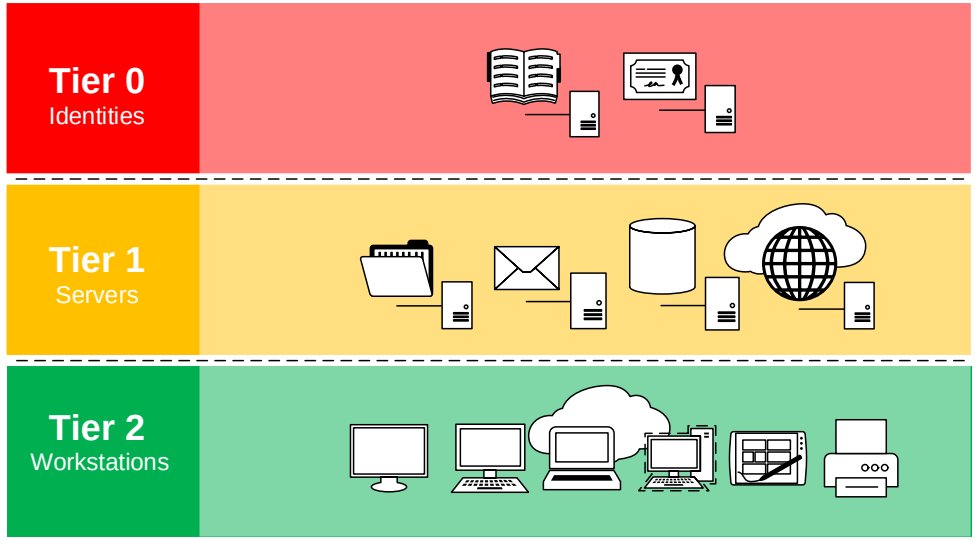
- **Tiers 0** (Identités) : il intègre les serveurs possédant les identités et les secrets d'authentification de l'organisation.
- **Tiers 1** (Serveurs) : il intègre les serveurs qui ne portent pas les identités.
- **Tiers 2** (Postes de travail) : il intègre les postes clients, bureautiques, etc…

Le tiers 0 est le niveau le plus sensible de ce modèle car la compromission de l'annuaire par exemple compromettrait implicitement les éléments des autres tiers. Si l'Active Directory s'arrête, toute l'organisation s'arrête. Le tiers 1 quant à lui est très certainement le niveau le plus important car il contient en général l'ensemble des données de l'organisation. Le tiers 2 lui est le plus vulnérable.

Le cloisonnement

Ce modèle multi-niveaux permet d'opérer une séparation des rôles d'administration du tiers 2 « postes de travail », de celui du tiers 1 « serveurs », de celui du tiers 0 « identités ». Ceci implique la création d'un ou plusieurs comptes d'administration dans chacun des tiers. Comme ces comptes seront différents dans chaque tiers, un administrateur qui doit accéder aux ressources des trois tiers devra au minimum posséder trois comptes d'administration différents.

Dans sa recommandation R29, l'ANSSI dit que les comptes d'administration sont exclusivement réservés à des actions d'administration.



L'administrateur d'une organisation devra donc utiliser au moins quatre comptes s'il veut accéder à la fois à ses applications métier et aux ressources des trois tiers :

- Le compte tiers0_adm pour administrer les ressources du tiers 0.
- Le compte tiers1_adm pour administrer les ressources du tiers 1.
- Le compte tiers2_adm pour administrer les ressources du tiers 2.
- Son compte personnel pour se connecter à ses applications métier.

Les protocoles d’authentification

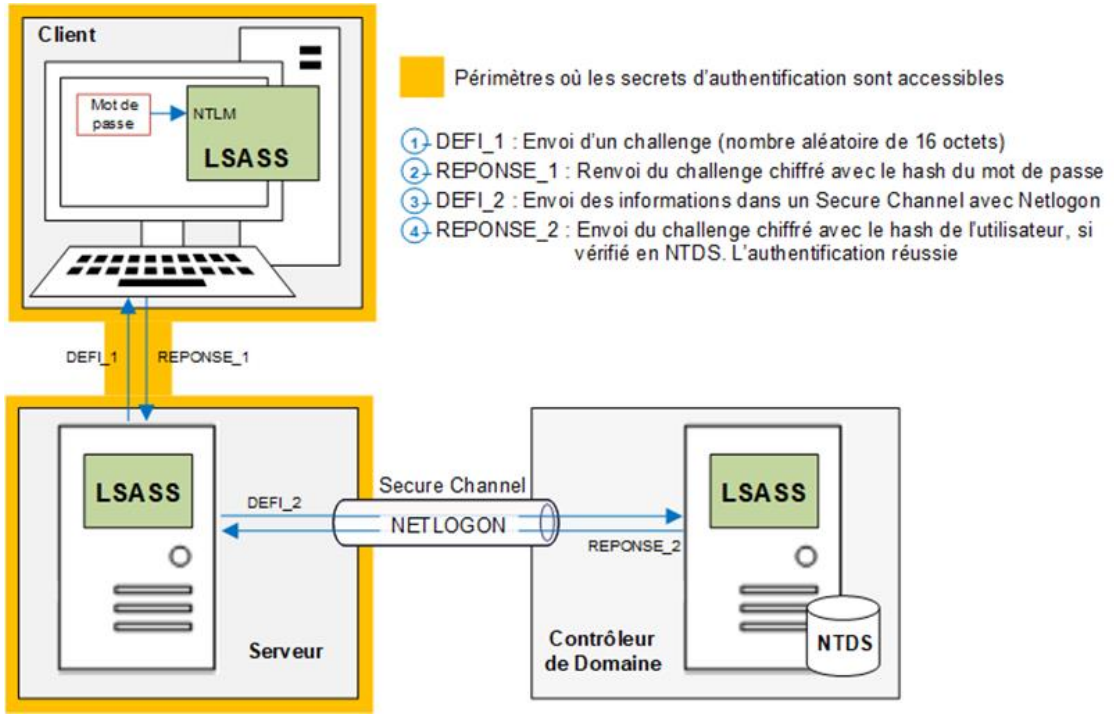
La protection des secrets d’authentification est donc devenue l’une des priorités en matière de sécurité des comptes d’administration. Dans un environnement Active Directory, ils vont circuler sous des formes différentes selon le protocole d’authentification utilisé. Ils peuvent se présenter sous la forme de mots de passe, de clés Kerberos, d’empreintes NTLM, de blocs chiffrés ou encore de couples défi/réponse.

Les protocoles d’authentification proposés par Microsoft dans Windows sont NTLM et Kerberos. Le choix du modèle de protocole sera donc crucial pour maximiser la protection des secrets d’authentification contre les tentatives de corruption de personnes malveillantes.

Le protocole NTLM

NTLM est le protocole d'authentification historique de Windows et encore aujourd'hui, nombre d'applications l'utilisent toujours. Même si le protocole Kerberos est à privilégier dans les domaines Active Directory, NTLM dans sa deuxième version, couplé à une politique de mots de passe complexe, reste toléré, mais très limité pour les comptes à privilèges.

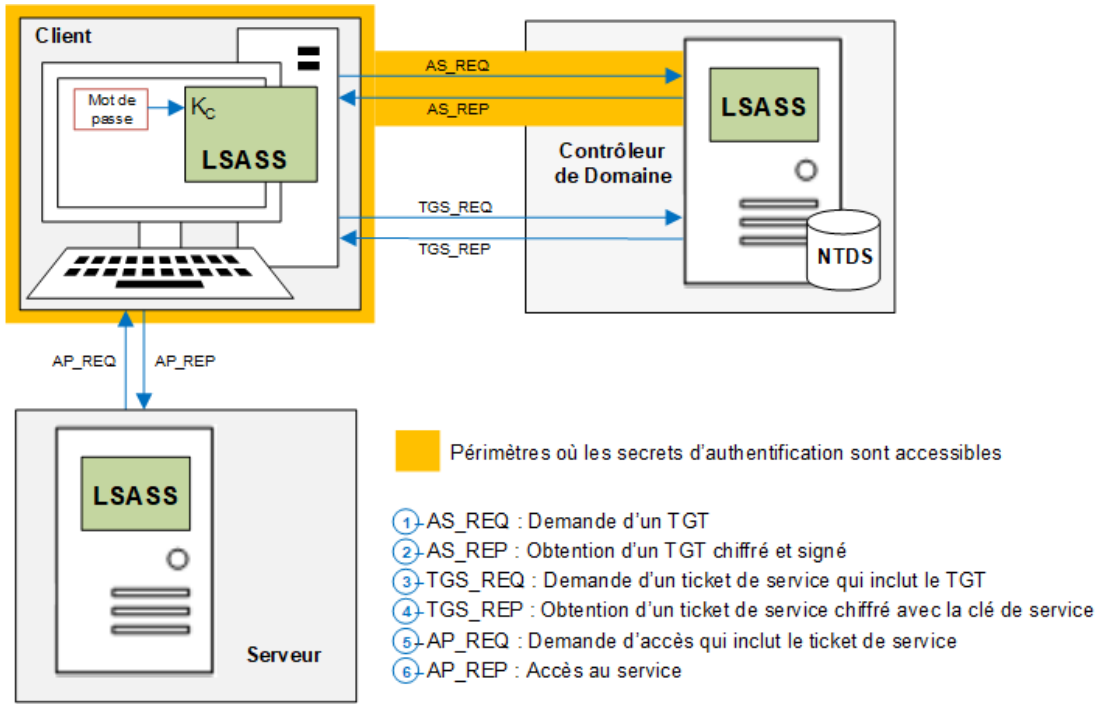
La figure ci-dessous présente un synoptique de l'authentification NTLM. Il met en évidence le périmètre où les secrets d'authentification sont accessibles. Il les protège assez mal car il impacte à la fois le poste client, le serveur de ressources distant et les échanges défi/réponse entre le poste et le serveur distant.



Le protocole Kerberos

Kerberos est un protocole d'authentification qui repose sur un mécanisme de clés secrètes (cryptographie symétrique) et l'utilisation de tickets. C'est le protocole d'authentification par défaut utilisé par Microsoft Windows car il améliore radicalement la protection des secrets d'authentification par rapport au protocole NTLM. En fait, le serveur de ressources cible n'est pas concerné par les informations d'authentification.

La figure ci-dessous présente un synoptique de l'authentification Kerberos. Il met en évidence le périmètre où les secrets d'authentification sont accessibles. On voit qu'il les protège mieux que celui de l'authentification NTLM car il n'impacte que le poste client et les échanges AS (Authentication Service).



La sécurisation de l'authentification

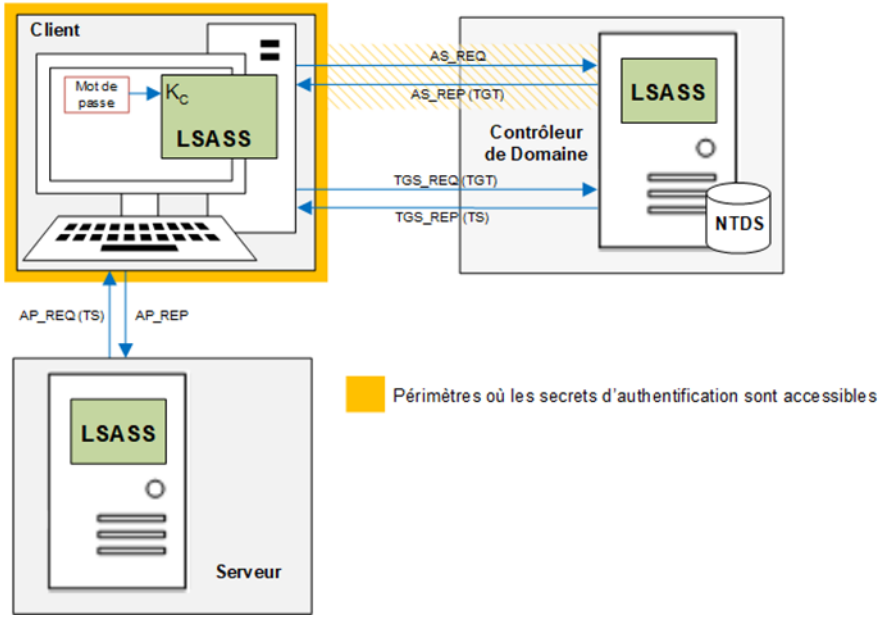
L'authentification et le choix du protocole jouent donc un rôle clé dans la protection du système d'information. Dans les environnements d'administration Active Directory, Microsoft recommande de renforcer la sécurité d'authentification de la manière suivante :

- Côté NTLM : Interdire l'utilisation de NTLM.
- Côté Kerberos :
  - Durcir la protection des échanges AS.
  - Interdire la délégation Kerberos.
  - Dédier des Privileged Access Workstation (PAW) aux comptes d'administration.

Le blindage Kerberos

L'échange « AS-REQ » entre le poste et le contrôleur de domaine est très certainement le talon d'Achille de Kerberos. Il est possible de le sécuriser en rajoutant à la demande d'authentification de l'utilisateur les informations du compte d'ordinateur de son poste. En effet, depuis Windows Server 2012, Microsoft a renforcé l'authentification Kerberos. Ce renforcement se traduit par l'intégration du protocole FAST (Flexible Authentication via Secure Tunneling). Il renforce la protection située au niveau des échanges AS (Authentication Service) et utilise le TGT du poste associé à la clé de session. On parle alors de blindage Kerberos.

La figure ci-contre présente un synoptique de l'authentification avec blindage Kerberos. On constate que le périmètre où les secrets d'authentification sont accessibles est mieux protégé que celui de l'authentification Kerberos car il impacte le poste client et les échanges AS sont plus sécurisés.



cyberelements

La sécurisation de l'authentification

Le groupe de sécurité « Protected Users »

Le groupe de sécurité « Protected Users », apparu avec Windows Server 2012 R2, modifie la manière dont l'authentification se réalise en apportant, entre autres, une réponse aux deux exigences de sécurité suivantes concernant l'authentification : Interdire la délégation Kerberos et interdire l'utilisation de NTLM. Tous les administrateurs affectés à ce groupe bénéficient de ces restrictions.

Le silo d'authentification

Le rôle du silo d'authentification permet de dédier le poste PAW d'un tiers (que nous verrons juste après) aux comptes d'administration du même tiers. Cette affectation se fait au travers d'une stratégie d'authentification. De cette manière, un administrateur ne pourra se connecter aux ressources d'un tiers qu'avec les comptes d'administration et le PAW associés à ce même tiers au travers d'une stratégie d'authentification.

Les recommandations

Il est donc recommandé d'appliquer les protections listées ci-dessous dans les contextes d'administration avec silotage AD :

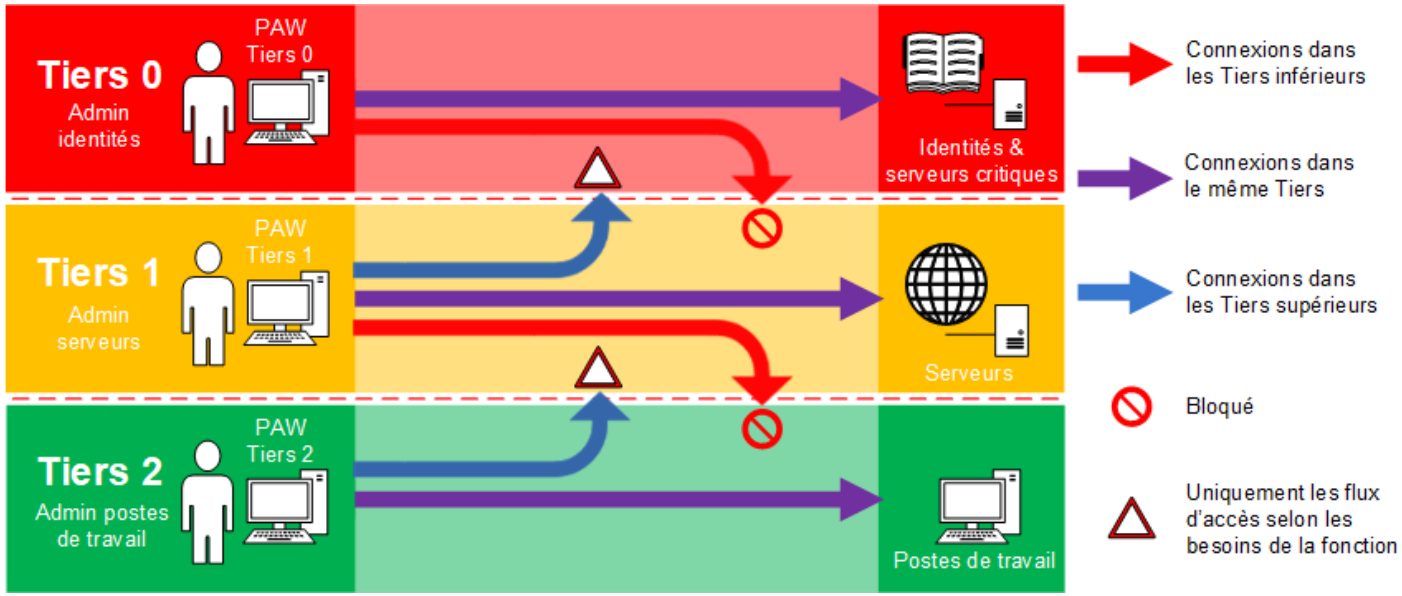
- ❑ NTLM : Interdire l'utilisation de NTLM → Utilisation du groupe « Protected Users ».
- ❑ Kerberos :
  - Durcir la protection des échanges AS → Utilisation du blindage Kerberos.
  - Interdire la délégation Kerberos → Utilisation du groupe « Protected Users ».
  - Dédier des PAW aux comptes d'administration → Configuration des silos d'authentification.

Le poste PAW

Pour administrer les ressources d'un tiers dans un modèle Active Directory multi-niveaux, l'administrateur doit se connecter avec un compte d'administration du tiers et à partir d'un poste de travail qui se trouve aussi dans ce même tiers.

Or tous les postes de travail sont dans le tiers 2, ce qui pose un problème majeur si l'administrateur a besoin d'accéder aux ressources des tiers 0 et 1.

Pour lever cette restriction, des postes de travail physiques sécurisés et dédiés à l'administration sont implémentés dans chacun des tiers. Pour limiter leur exposition, ces postes, appelés **PAW** (**P**rivileged **A**ccess **W**orkstation), ne peuvent pas échanger avec des instances externes au tiers où ils sont implémentés. En tout cas, il faudra procéder à une gestion très fine des connexions réseaux entrantes ou sortantes si le besoin le justifiait. Ces postes d'administration PAW ne doivent pas avoir accès à Internet, doivent bloquer les remontées de périphériques USB, etc…



Le poste PAW

L'ANSSI, dans son document PA-022, explique dans sa recommandation R9 que la principale mesure de sécurité consiste à dédier un poste de travail physique aux actions d'administration. Ce poste d'administration doit être distinct du poste qui permet d'accéder aux ressources conventionnelles accessibles sur le SI de l'organisation (ressources métier, messagerie interne, gestion documentaire, Internet, etc.).

Les postes à accès privilégiés (PAW) répondent à cette recommandation car ils ne sont dédiés qu'à des fins d'administration. Leur sécurité est renforcée et ils sont exclusivement utilisés pour accéder à des ressources critiques pour effectuer des tâches d'administration.

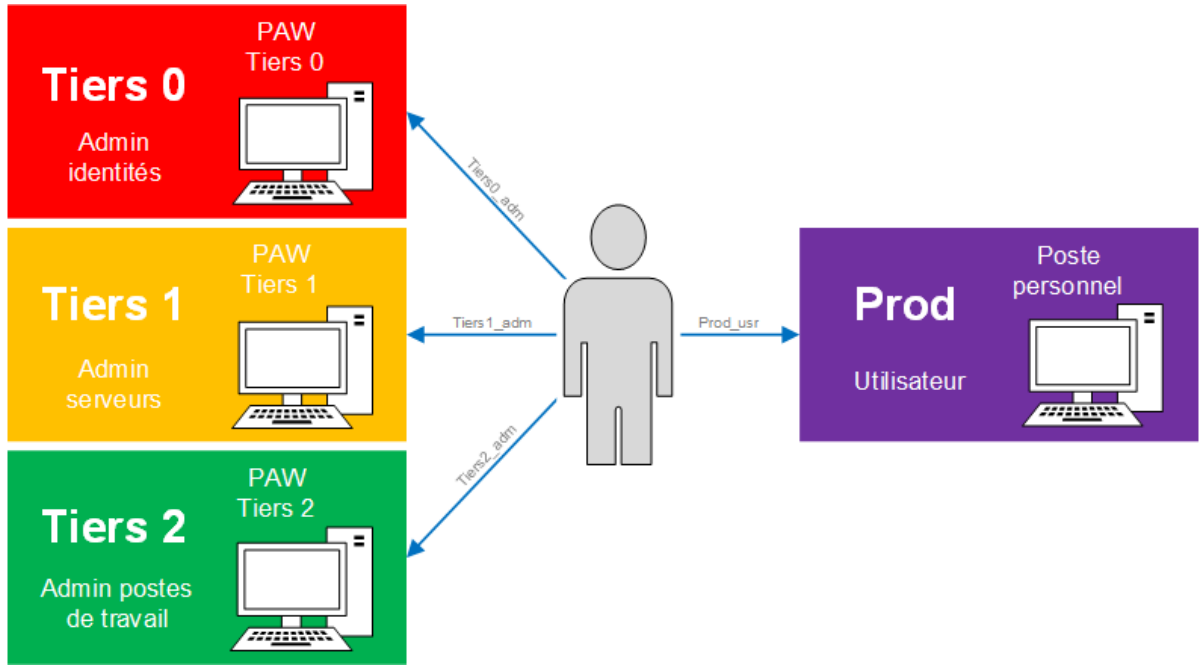
La sécurité des comptes d'administration du poste PAW doit être également renforcée. Elle peut se faire au travers d'outils gratuits tels que Microsoft LAPS qui gère la complexité et la rotation des comptes administrateurs locaux du poste PAW. LAPS a néanmoins des limites sur le nombre de comptes qu'il peut gérer, il faudra donc passer par des solutions tierces de type PAM, qui vont à minima gérer la complexité et la rotation des comptes administrateurs, mais sur un nombre de comptes illimités.

Le poste PAW

Le modèle d'administration trois tiers demande une démultiplication des comptes mais surtout des postes de travail pour effectuer les tâches d'administration.

Comme expliqué précédemment, un administrateur aura potentiellement besoin de :

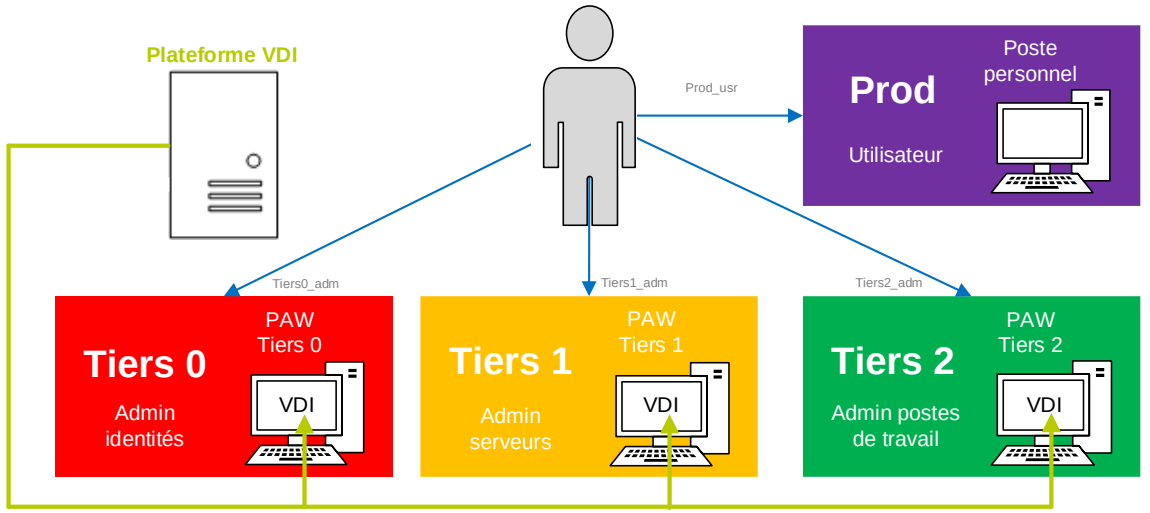
- Quatre postes de travail physiques : 3 PAW et 1 poste d'usage.
- Quatre comptes Active Directory : 3 d'administration et 1 d'usage.



Le poste PAW

Ce modèle d'administration trois tiers est plutôt contraignant sur le plan opérationnel, mais aussi économique car les coûts matériels additionnés aux coûts d'exploitation des postes PAW sont loin d'être neutres. Des technologies VDI peuvent être implémentées pour faciliter le déploiement des postes PAW et optimiser leur MCS (**M**aintien en **C**ondition de **S**écurité). Tout comme les postes physiques, les postes PAW virtuels apportent des capacités clés pour satisfaire certaines recommandations de l'ANSSI proposées dans le guide PA-022.

- Le durcissement de l'OS du poste d'administration.
- La possibilité d'avoir des mises à jour automatiques et régulières.
- La sécurité pour interdire les connexions entrantes.
- La restriction des droits d'administration sur le poste d'administration.
- La gestion des droits des administrateurs selon la règle du moindre privilège.
- La limitation des seuls logiciels installés sur le poste d'administration.



cyberelements

2

cyberelements

cyberelements est la seule plateforme SaaS Zero Trust qui sécurise les accès des utilisateurs standards ou privilégiés à leurs applications et ressources critiques. cyberelements consolide au sein d'une expérience unifiée, tous les éléments dont une organisation a besoin pour sécuriser les accès des collaborateurs aux systèmes IT et OT: la gestion des identités (IAM), la gestion des accès (AM), les accès distants (ZTNA) et les accès à privilèges(PAM).

Opérationnelle en quelques minutes, cyberelements pour répondre aux exigences de les plus strictes en matière de sécurité, grâce à ses fonctionnalités Zero Trust natives : double barrière, rupture protocolaire break, ports réseaux volatiles et aléatoires, tunnel d'accès sécurisé avec votre propre clé, connexion à la ressource uniquement pour la durée d'utilisation, flux sortants et aucune ouverture de port.

3

Intégration de cyberelements dans un contexte siloté

Les différents éléments qui viennent d'être abordés mettent en évidence les bonnes pratiques à appliquer dans un contexte d'administration en environnement Active Directory.

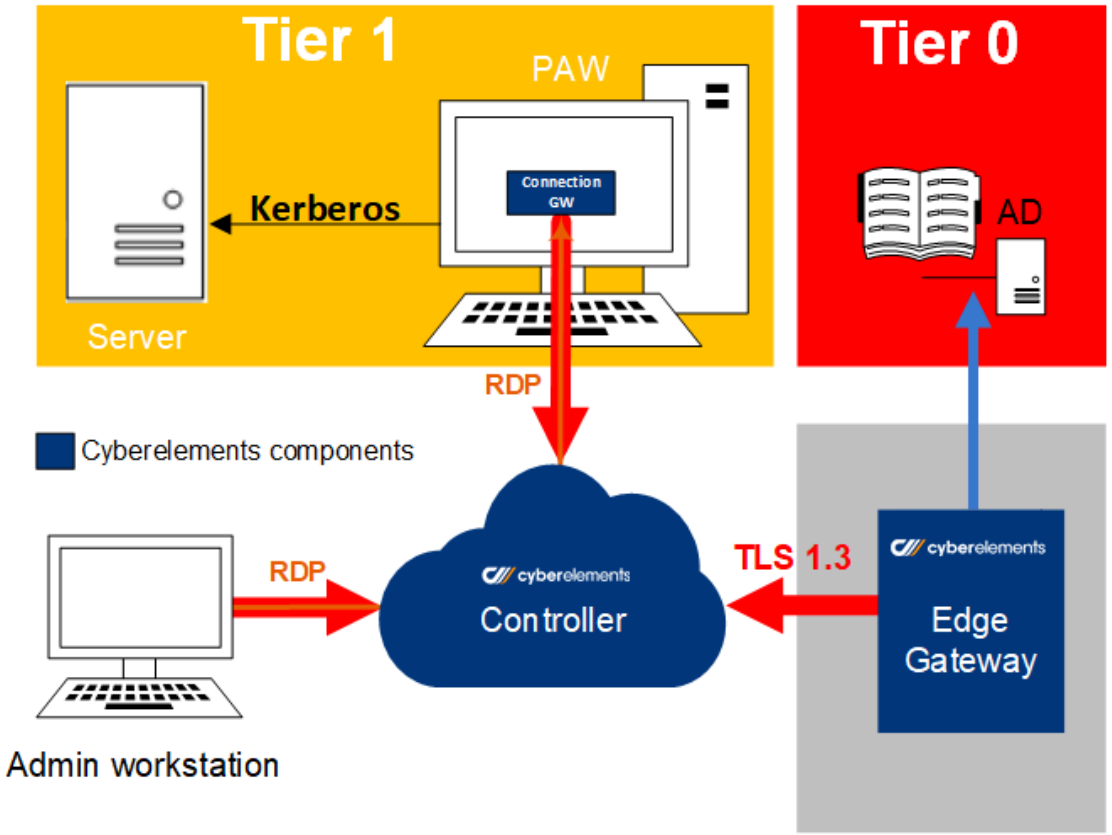
Les actes d'administration doivent se faire dans un modèle en trois tiers qui permet de cloisonner les ressources en fonction de leurs criticités. Chaque tiers doit posséder au moins un compte d'administration et un poste PAW pour administrer les ressources qui sont référencées dans ce tiers. Les échanges réseaux entre le poste PAW et les différents éléments d'infrastructure doivent se faire avec le protocole d'authentification Kerberos avec blindage.

Le principe

Pour respecter l'ensemble des prérequis au silotage AD, cyberelements s'interface entre le poste de l'administrateur et le poste PAW.

Un composant cyberelements sera à implémenter sur le poste PAW :

- **Edge Gateway**: c'est une passerelle logicielle qui initie un tunnel sécurisé TLS1.3 en flux sortant vers cyberelements. Aucun flux entrant n'est possible sur le poste PAW.



cyberelements

Le principe

La connexion de l'administrateur sur le poste PAW est faite via le protocole RDP. Le flux de connexion est entièrement encapsulé dans le tunnel TLS 1.3 issu de la Connexion Gateway, et aucun flux entrant n'est nécessaire vers le poste PAW pour une sécurité maximale.

L'authentification sur le poste PAW se fait via le protocole Kerberos blindé. Le token d'authentification est généré par cyberelements via un échange entre l'Edge Gateway cyberelements et le contrôleur Active Directory.

Les postes PAW ne doivent pas échanger avec des instances externes au tiers où ils sont implémentés. Mais dans le cas d'une politique d'accès qui nécessite une administration à distance, pour des tiers mainteneurs par exemple, il faudra configurer l'accès en s'assurant que le poste PAW n'accède qu'à un seul point de terminaison et qu'il ne peut pas naviguer sur Internet.

Les accès réseaux basés sur une approche Zero Trust, c'est-à-dire de non confiance, plus communément appelés ZTNA (Zero Trust Network Access), répondent à cette politique d'accès et cyberelements intègre nativement cette technologie ZTNA.

Cette approche permet de conserver les avantages de cyberelements dont :

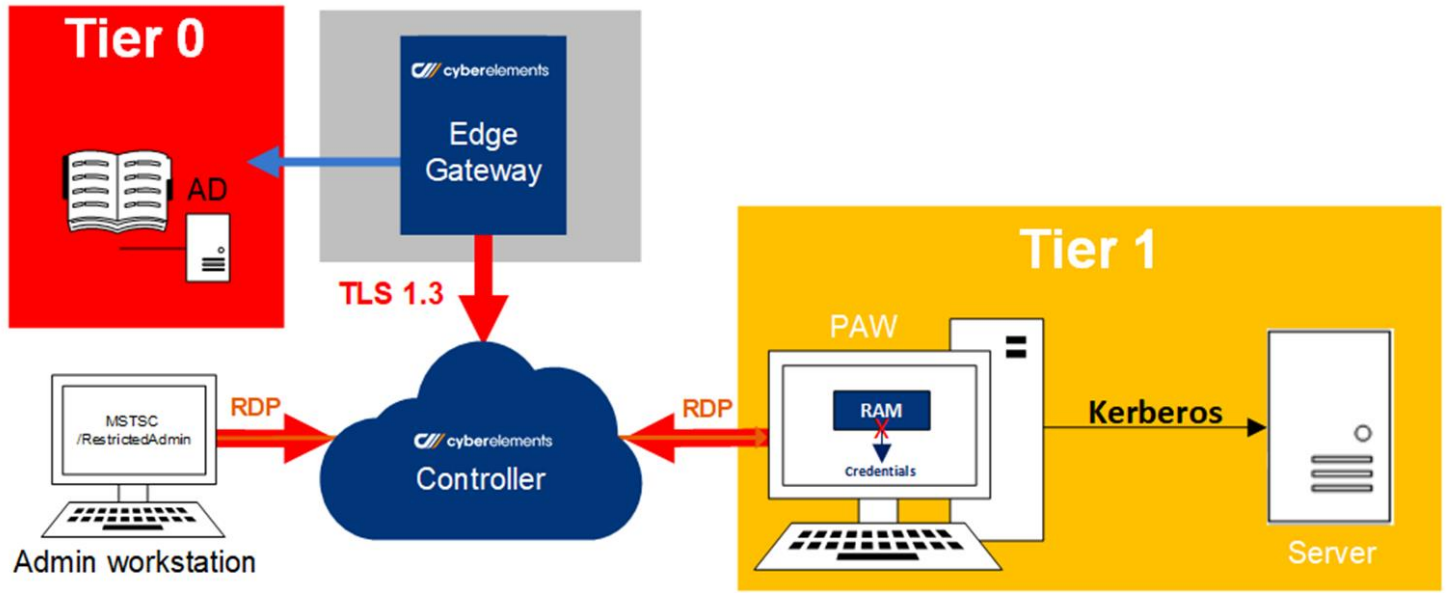
- ❑ Traçabilité vidéo des accès.
- ❑ Contrôle des actions réalisées.
- ❑ Coffre-fort de mot de passe.
- ❑ Etc...

Le mode "Restricted Admin"

cyberelements s'interface entre le poste de l'administrateur et le poste PAW. Lors du processus d'authentification via le protocole RDP, le service LSASS, en charge de fournir le mécanisme de SSO (Single Sign-On), charge en mémoire du poste PAW le hash du mot de passe de l'administrateur. Si ce dernier venait à être compromis, une attaque de type « Pass-the-Hash », qui consiste justement à utiliser le hash du mot de passe pour s'authentifier sur une ressource, pourrait compromettre toutes les ressources du tiers administré.

En activant le mode « **Restricted Admin** », disponible depuis Windows Server 2012 R2, les informations d'identification qui sont saisies lors de la connexion RDP, notamment le hash du mot de passe, ne sont pas mémorisées et stockées dans la mémoire du poste PAW.

Il est donc nécessaire d'activer le mode « Restricted Admin » pour renforcer la protection des ressources du tiers. L'activation peut se faire par GPO ou par clé de registre.



Le mode "Restricted Admin"

Le tableau ci-dessous met en évidence que de nombreuses méthodes d'authentification stockent les secrets d'authentification en mémoire, surtout dans les environnements Active Directory où la sécurité n'est pas renforcée.

		KERB	HASHES		MOTS DE PASSE EN CLAIR				
		TGT	LM	NT	Tspkg	Wdigest	Kerb	LiveSSP	Third Party SSP
Sans renfort de la sécurité	Compte Microsoft								~
	Compte Local								~
	Compte de Domaine								~
Avec renfort de la sécurité	Compte Microsoft				*	**			~
	Compte Local				*	**			~
	Compte de Domaine				*	**			~
Nouvelles foncionnalités	Protected Users								~
	Restricted Admin RDP								

~ Uniquement si installé

* Désactivé par défaut

** Uniquement par défaut avec Windows 8.1 et Windows Server 2012 R2

Mots de passe en mémoire

Mots de passe hors mémoire

cyberelements

Abréviations techniques et références

Pour faciliter la lisibilité et la compréhension de ce document, vous trouverez dans le tableau ci-dessous la liste des abréviations techniques (acronymes) utilisées.

ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
AS	Authentication Service
FAST	Flexible Authentication via Secure Tunneling
LAPS	Local Administrator Password Solution
LM	LAN Manager
LSASS	Local Security Authority Subsystem Service
MCS	Maintien en Condition de Sécurité
NT	New Technology
NTDS	NT Directory Services
NTLM	NT Lan Manager
PAM	Privileged Access Management
PAW	Privileged Access Workstation
SI	Système d'Information
TGT	Ticket Granting Ticket
ZTNA	Zero Trust Network Access

Références

L'administration en silo — Aurélien Bordes :
https://www.sstic.org/2017/presentation/administration_en_silo/

Recommandations relatives à l'administration sécurisée des systèmes d'information :
https://www.ssi.gouv.fr/entreprise/guide/securiser-ladministration-des-systemes-dinformation/