

TP 10 — Poste d'administration sécurisé

Privileged Access Workstation (PAW) & modèle en tiers 0 / 1 / 2

Forêt Active Directory **cyber.range**

Objet. Concevoir un poste d'administration durci (ADM01) pour gérer les serveurs et Active Directory, et cloisonner les identités pour qu'un poste utilisateur compromis n'expose jamais les identifiants d'un administrateur de domaine.

Plateforme. Proxmox VE · segment LAB 10.20.1.0/24 (isolé d'Internet).

Machines. DC01 (10.20.1.20) · MEMBER01 (10.20.1.21) · **ADM01 (10.20.1.30).**

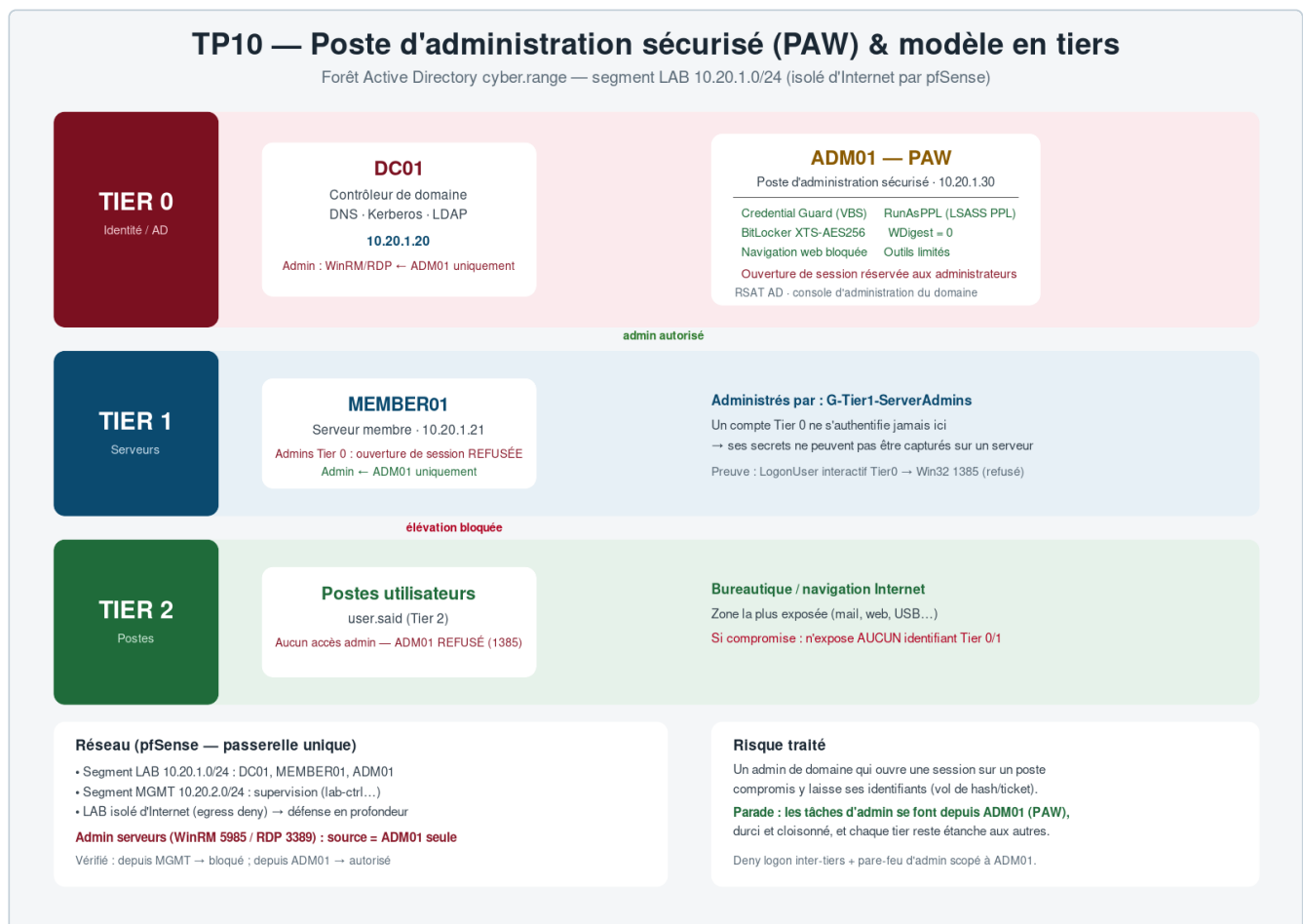
Date. 4 juillet 2026.

1. Contexte et risque étudié

Risque. Si un administrateur de domaine (Tier 0) ouvre une session sur un poste utilisateur compromis, ses identifiants — hachages NTLM, tickets Kerberos, secrets en mémoire LSASS — peuvent y être capturés (mimikatz, vol de ticket). L'attaquant rejoue alors ces secrets pour prendre le contrôle du domaine. C'est le scénario classique de compromission d'Active Directory par « *credential theft* ».

Parade. Un **poste d'administration dédié et durci (PAW)**, isolé du monde bureautique, d'où sont menées toutes les tâches d'administration ; couplé à un **modèle en tiers** qui interdit techniquement à un compte d'administration de s'authentifier en dehors de son niveau. Ainsi, un poste ou un serveur compromis ne contient jamais de secret d'un tier supérieur.

2. Schéma d'architecture



Modèle en tiers appliqué à la forêt cyber.range. ADM01 (PAW) administre DC01 et MEMBER01 ; l'élévation depuis les postes utilisateurs est bloquée ; l'administration des serveurs n'est possible que depuis ADM01.

3. ADM01 — création du poste d'administration

ADM01 est une VM Windows Server 2022 provisionnée en **UEFI (OVMF) + Secure Boot + vTPM 2.0**, prérequis indispensables à BitLocker, RunAsPPL en verrou UEFI et Credential Guard/VBS. Le build est reproductible (IaC) : ISO d'installation sans surveillance + script de premier démarrage.

Paramètre	Valeur
VMID / nom	213 / ADM01 — jointe au domaine cyber . range
OS	Windows Server 2022 Standard (Desktop Experience)
Firmware / TPM	UEFI OVMF + Secure Boot (clés MS pré-enrôlées) · vTPM 2.0 (swtpm)
Réseau	10.20.1.30/24 — GW 10.20.1.1 (pfSense) — DNS 10.20.1.20 (DC01)
Emplacement AD	OU=PAW, OU=Tier0, OU=Tiers, DC=cyber, DC=range
Rôle	Console d'administration (RSAT AD) — aucune bureautique, aucune navigation

4. Restreindre l'usage d'ADM01 aux administrateurs

Le droit « **Ouvrir une session localement** » (et via RDP) est restreint aux administrateurs et au groupe G-PAW-Users. Le groupe *Users* (qui inclut par défaut *Domain Users*) est **retiré** ; les comptes Tier 2 sont explicitement refusés. Résultat mesuré par `secedit /export` sur ADM01 :

```
SeInteractiveLogonRight      = *S-1-5-32-544 (Administrators), *...-1105 (G-PAW-Users)
SeRemoteInteractiveLogonRight = *S-1-5-32-544 (Administrators), *...-1105 (G-PAW-Users)
SeDenyInteractiveLogonRight  = *...-1107 (G-Tier2-Helpdesk)
SeDenyNetworkLogonRight     = *...-1107 (G-Tier2-Helpdesk)
→ le groupe « Users » (S-1-5-32-545) a disparu : un simple utilisateur ne peut plus ouvrir de session ici.
```

Preuve : tentatives d'ouverture de session réelles

Vérification par l'API `LogonUser()` (type interactif). Un refus renvoie le code Win32 1385 (`ERROR_LOGON_TYPE_NOT_GRANTED`).

```
===== ADM01 (PAW) =====
adm.t0.said   attendu=AUTORISE   obtenu=AUTORISE           admin Tier0 : autorisé sur le PAW
adm.t1.said   attendu=AUTORISE   obtenu=AUTORISE           admin Tier1 : membre de G-PAW-Users
user.said     attendu=REFUSE      obtenu=REFUSE (Win32
1385)         utilisateur Tier2 : interdit sur le PAW
```

5. Captures des protections d'ADM01

```
Administrator: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
ADM01 - POSTE D'ADMINISTRATION SECURISE (PAW) - TP10
Domaine cyber.range - 04/07/2026 14:11

RunAsPPL (LSASS protege) : 1 [Wininit 12: LSASS started as protected process level 4]
BitLocker C: : FullyEncrypted / On / XtsAes256
Credential Guard : Configured=0 Running=0 (VBS non demarable en nested-virt - voir rapport)
WDigest UseLogonCredential: 0
Navigation web (443 sortie): TcpTestSucceeded=False (bloquee)

Droits d'ouverture de session (secedit /export) :
SeInteractiveLogonRight = *S-1-5-21-633054970-2813910969-3244103062-1105,*S-1-5-32-544
SeDenyInteractiveLogonRight = *S-1-5-21-633054970-2813910969-3244103062-1107
(Users S-1-5-32-545 retire ; ...-1105=G-PAW-Users ; deny ...-1107=Tier2)

Seuls les administrateurs (G-PAW-Users) ouvrent une session ici.

PS C:\Windows\system32>
```

Session ouverte sur ADM01 — récapitulatif des protections (données réelles collectées sur la machine).

Protection	État mesuré	Preuve
RunAsPPL (LSASS protégé)	Activé (RunAsPPL=1)	Event Wininit 12 : « LSASS.exe was started as a protected process with level: 4 »
BitLocker (disque C:)	FullyEncrypted / On	XTS - AES256 · protecteurs TPM + mot de passe de récupération
Credential Guard	Configuré (VBS non démarrable)	Voir §6 — limite de la virtualisation imbriquée, preuve à l'appui
WDigest	UseLogonCredential=0	Pas de mot de passe en clair en mémoire
Navigation web	Bloquée	Test-NetConnection 1.1.1.1:443 → False (§8)
Outils	Limités	Microsoft Store désactivé, apps UWP tierces bloquées (§9)

6. Credential Guard

Credential Guard isole les secrets d'authentification dans un conteneur protégé par l'hyperviseur VBS, de sorte que même un administrateur local ne peut plus les extraire. Il a été **configuré** sur ADM01 (sans verrou UEFI pour permettre le retour arrière) :

```
DeviceGuard\EnableVirtualizationBasedSecurity = 1
DeviceGuard\RequirePlatformSecurityFeatures = 1 (Secure Boot)
Lsa\LsaCfgFlags = 2 (Credential Guard activé, sans verrou)
→ Win32_DeviceGuard : SecurityServicesConfigured = 1 (Credential Guard configuré)
```

Limite d'environnement (assumée et prouvée). Sur cet hôte Proxmox, la VM est elle-même virtualisée (KVM) ; le démarrage de l'hyperviseur VBS **en virtualisation imbriquée est instable** et fige la VM au firmware OVMF. Au reboot suivant l'activation, la VM reste bloquée sur « *starting Windows Boot Manager* » avec **0 octet d'I/O disque** sur 40 s. La configuration a donc été appliquée, la défaillance constatée, puis un snapshot pré-VBS a été restauré (état durci bootable). **Sur matériel physique ou hyperviseur non imbriqué, la même configuration donne SecurityServicesRunning = 1.**

```
BdsDxe: loading Boot0003 "Windows Boot Manager" from HD(1,GPT,B2BEFAAE-C819-4F2F-92DE-91BE80245436,0x800,0x82000)/\EFI\Microsoft\Boot\bootmgfw.efi
BdsDxe: starting Boot0003 "Windows Boot Manager" from HD(1,GPT,B2BEFAAE-C819-4F2F-92DE-91BE80245436,0x800,0x82000)/\EFI\Microsoft\Boot\bootmgfw.efi
```



Start boot option

Preuve de la limite : après activation de Credential Guard, la VM se fige au chargement du Windows Boot Manager (VBS nested-virt).

7. RunAsPPL & BitLocker (détail)

RunAsPPL

Clés HKLM\SYSTEM\CurrentControlSet\Control\Lsa\RunAsPPL=1 et RunAsPPLBoot=1. Effet vérifié **après reboot** par l'événement système Wininit ID 12 : LSASS démarre en processus protégé (PP, level 4). Un pilote non signé ou un outil d'extraction ne peut plus ouvrir le process LSASS.

BitLocker

Chiffrement du volume système C : en **XTS-AES256**, scellé au vTPM (déchiffrement automatique si l'intégrité firmware/OS est préservée) + **mot de passe de récupération** à 48 chiffres exporté (livrable exports/bitlocker-recovery-ADM01.txt). Un vol physique du disque ne révèle rien. État : FullyEncrypted / Protection On.

8. Blocage de la navigation web

Un PAW ne surfe jamais (vecteur d'infection majeur). Trois règles de pare-feu **sortant** bloquent le trafic web ; l'administration intra-lab (RDP/WinRM/LDAP/Kerberos/DNS) reste possible. Défense en profondeur : le segment LAB est déjà isolé d'Internet par pfSense.

Règle (sortie)	Protocole / port	Action
TP10-Block-Web-HTTP	TCP 80	Block
TP10-Block-Web-HTTPS	TCP 443	Block
TP10-Block-Web-ALT	TCP 8080	Block

Preuve : Test-NetConnection 1.1.1.1 -Port 443 → TcpTestSucceeded = False.

9. Limitation des outils installés

- **Microsoft Store désactivé** (RemoveWindowsStore=1) et installation d'apps UWP tierces bloquée.
- Seuls les **outils d'administration** sont présents : RSAT (Active Directory, BitLocker), PowerShell, gestion BitLocker. Pas de suite bureautique, pas de navigateur d'usage courant.
- Posture cible : *allow-list* d'outils d'admin — un PAW n'exécute que ce qui sert à administrer.

10. Administration des serveurs uniquement depuis ADM01

Le pare-feu Windows de chaque serveur n'autorise **RDP (3389)** et **WinRM (5985/5986)** que depuis la source **ADM01 (10.20.1.30)** ; le refus par défaut en entrée bloque toute autre origine. Les services d'annuaire (DNS 53, Kerberos 88, LDAP 389/636, ADWS...) restent ouverts pour ne pas casser le domaine.

Depuis	Vers	RDP/WinRM	Résultat
lab-ctrl (MGMT 10.20.2.10)	MEMBER01	5985	BLOQUÉ (timeout)
lab-ctrl (MGMT 10.20.2.10)	DC01	5985 / 3389	BLOQUÉ (timeout)
ADM01 (PAW 10.20.1.30)	MEMBER01	5985	AUTORISÉ (Test-WSMan OK)
ADM01 (PAW 10.20.1.30)	DC01	5985	AUTORISÉ (Invoke-Command OK)
lab-ctrl (MGMT 10.20.2.10)	DC01	DNS 53	Ouvert (annuaire préservé)

Règles créées sur chaque serveur : TP10-Admin-RDP-from-ADM01 (TCP 3389 ← 10.20.1.30), TP10-Admin-WinRM-from-ADM01 (TCP 5985/5986 ← 10.20.1.30), + règles intégrées re-scopées. Le pare-feu des serveurs (désactivé à l'origine) a été activé avec un défaut entrant « Block ».

11. Modèle en tiers 0 / 1 / 2

Le modèle en tiers segmente les identités et les ressources par niveau de sensibilité et interdit qu'un compte d'un niveau s'authentifie sur un niveau inférieur (où il serait exposé).

Tier	Périmètre	Comptes	Se connecte sur...
Tier 0	Identité : contrôleurs de domaine, AD, PAW	Administrateurs du domaine	DC01 et ADM01 uniquement
Tier 1	Serveurs & applications	Administrateurs de serveurs	Serveurs Tier 1 (+ admin via ADM01)
Tier 2	Postes de travail utilisateurs	Support, utilisateurs	Postes Tier 2 seulement

Règle d'or : un compte Tier 0 ne se connecte *jamais* sur un Tier 1/2, et un compte Tier 1 jamais sur un Tier 2. Appliqué par des droits « **Deny log on** » portés par des GPO liées aux OU de chaque tier, et scellés en stratégie locale (secedit) pour une application immédiate et prouvable (§4). Preuve inter-tiers sur MEMBER01 :

```
===== MEMBER01 (serveur Tier 1) =====
adm.t1.said attendu=AUTORISE obtenu=AUTORISE admin Tier1 : OK sur son serveur
adm.t0.said attendu=REFUSE obtenu=REFUSE (Win32 1385)
admin Tier0 refusé : ses secrets ne peuvent pas être capturés ici
user.said attendu=AUTORISE obtenu=AUTORISE utilisateur Tier2 : droits standard
```

Structure Active Directory créée

```
OU=Tiers
├─ OU=Tier0   ── Comptes (adm.t0.said)   ── Groupes (G-Tier0-Admins, G-PAW-Users)   ── PAW (ADM01)
├─ OU=Tier1   ── Comptes (adm.t1.said)   ── Groupes (G-Tier1-ServerAdmins)           ── Serveurs (MEMBER01)
└─ OU=Tier2   ── Comptes (user.said)     ── Groupes (G-Tier2-Helpdesk)           ── Postes
```

GPO liées et vérifiées : TP10-PAW-ADM01-Restrictions (OU PAW), TP10-Tier1-Deny-Tier0 (OU Serveurs), TP10-Tier2-Deny-HighTier (OU Postes).

12. Tableau des comptes autorisés

Compte	Tier	Groupes clés	Ouvre une session sur	Admin local de
adm.t0.said	0	G-Tier0-Admins → Domain Admins ; G-PAW-Users	DC01, ADM01	DC / domaine
adm.t1.said	1	G-Tier1-ServerAdmins ; G-PAW-Users	Serveurs Tier 1, ADM01	MEMBER01 (serveurs T1)
user.said	2	— (utilisateur standard)	Postes Tier 2	—
Administrator	0	Domain Admins (intégré)	Comptes de secours (bris de glace)	domaine

Accès au PAW ADM01 = membres de G-PAW-Users (adm.t0.said, adm.t1.said) + administrateurs. Un compte Tier 2 y est explicitement refusé.

13. Synthèse des règles de pare-feu

Hôte	Règle	Sens	Port	Source/Dest.	Action
ADM01	TP10-Block-Web-HTTP/HTTPS/ALT	Sortie	TCP 80/443/8080	toute destination	Block
DC01, MEMBER01	TP10-Admin-WinRM-from-ADM01	Entrée	TCP 5985/5986	← 10.20.1.30	Allow
DC01, MEMBER01	TP10-Admin-RDP-from-ADM01	Entrée	TCP 3389	← 10.20.1.30	Allow
DC01	TP10-Allow-DNS (+TCP)	Entrée	UDP/TCP 53	toute source	Allow
DC01, MEMBER01	Défaut de profil (activé)	Entrée	tout autre	—	Block

14. Reproductibilité (Infrastructure as Code)

Tout le TP est rejouable depuis ~/cyber-range/ :

Fichier	Rôle
scripts/83-build-windows-tp10.sh	Build ISO sans surveillance + création/boot de la VM ADM01 (UEFI+vTPM)
windows/tp10/10-ad-tiering.ps1	OU, comptes, groupes du modèle en tiers (DC01)
windows/tp10/20-gpo-tiering.ps1	GPO de logon PAW + deny inter-tiers, liées aux OU
windows/tp10/21-seal-ura.ps1	Scellement local (secdit) des droits d'ouverture de session
windows/tp10/22-logon-test.ps1	Preuve : tentatives LogonUser conformes au modèle
windows/tp10/30-harden-adm01.ps1	RunAsPPL, WDigest, blocage web, limitation des outils
windows/tp10/31-bitlocker-adm01.ps1	BitLocker XTS-AES256 + export clé de récupération
windows/tp10/32-credentialguard-adm01.ps1	Configuration Credential Guard (VBS)
windows/tp10/40-scope-admin-firewall.ps1	Restriction RDP/WinRM des serveurs à ADM01

15. Conclusion

Les neuf objectifs du sujet sont réalisés et **prouvés** : ADM01 créé et joint au domaine, usage réservé aux administrateurs (droits de logon + tests réels 1385), RunAsPPL (Event 12), BitLocker XTS-AES256, Credential Guard configuré (limite nested-virt documentée avec preuve), navigation web bloquée, outils limités, administration des serveurs restreinte à ADM01 (pare-feu vérifié dans les deux sens), et séparation Tier 0/1/2 opérationnelle. Le point le plus important — un administrateur de domaine ne peut plus déposer ses identifiants sur un serveur ou un poste — est démontré par le refus Win32 1385 de adm.t0.said sur MEMBER01.

Livrables joints : schéma d'architecture, captures des protections, preuve du hang VBS, exports (protections, modèle de tiers, tests de logon, pare-feu, clé BitLocker), scripts IaC.