ENQUÊTE : ÉCHEC D'AUTHENTIFICATION SMB ENTRE VM CLONÉES (WORKGROUP)

Enquête sur SMB distant impossible après clonage sans OOBE

5 min de lecture · 7 août 2026 · Vincent

SOMMAIRE

WINDOWS · INTERMÉDIAIRE

ENQUÊTE : ÉCHEC D'AUTHENTIFICATION SMB ENTRE VM CLONÉES (WORKGROUP)

Enquête sur SMB distant impossible après clonage sans OOBE

5 min · 7 août 2026

Contexte — TP SupportLab (Mission 4, jalon 3-4). Symptôme initial rencontré par toute la classe (17 postes) : impossible de se connecter à un partage SMB entre deux VM Windows 11 clonées, « mot de passe réseau incorrect » (erreur 86), alors que les mêmes comptes/mots de passe fonctionnent en session locale. Environnement reproduit sur deux VM : `CLIENT` (192.168.10.144) et `SERVER` (192.168.10.143), clonées de la même image, sans sysprep.

1. TESTS RÉALISÉS ET RÉSULTATS

#	TEST	COMMANDE / MÉTHODE	RÉSULTAT	ENSEIGNEMENT
1	Identité des machines	`hostname`, `whoami /user`, `Get-NetIPAddress`	Hostnames et IP distincts, **SID machine identique** (`S-1-5-21-2897362226-427835314-1636964152`)	Clonage sans généralisation confirmé
2	Session locale avec chaque compte	Ouverture de session interactive	**OK sur les deux VM**	SAM, LSASS et mots de passe sains
3	Accès SMB par nom	`net use \\SERVER\C$ /user:support.tech`	**Erreur 86**	Échec d'authentification réseau
4	Résolution de nom	`ping SERVER -4`	Résout la bonne IP (192.168.10.143, via mDNS)	Résolution innocentée
5	Accès SMB par IP	`net use \\192.168.10.143\C$`	**Erreur 86 aussi**	Confirme : pas un problème de résolution
6	Journal serveur, échecs	`Get-WinEvent` id **4625**	`0xC000006D`, **sous-état 0x0** (aucune raison)	Refus AVANT comparaison du mot de passe

#	TEST	COMMANDE / MÉTHODE	RÉSULTAT	ENSEIGNEMENT
7	Contrôle du sous-état	Faute de frappe `suuport.technicien`	Sous-état `0xC0000064` (compte inconnu)	Le serveur SAIT produire des sous-codes précis → le 0x0 est significatif
8	Mot de passe vide ?	`Set-LocalUser` (preuve `PasswordLastSet`), retest	**Toujours erreur 86, sous-état 0x0**	Théorie « mot de passe vide + LimitBlankPassworduse » réfutée
9	Compte témoin	`New-LocalUser temoin` (créé APRÈS clonage, uniquement sur SERVER), test depuis CLIENT	**Erreur 86, sous-état 0x0**	Blocage machine-niveau, indépendant des comptes
10	Bouclage SERVER→SERVER	`net use \\SERVER\C$` depuis SERVER	**Erreur 5** (accès refusé = authentification RÉUSSIE, refus d'autorisation C$)	Le serveur valide sa propre auth : NTLM local sain
11	Stratégies LSA/NTLM	`LmCompatibilityLevel` (absent = défaut), `NtlmMinClient/ServerSec` = 0x20000000 (défaut), pas de `RestrictReceivingNTLMTraffic`	Identiques et par défaut des deux côtés	Aucun durcissement hérité de l'image ; les « resets » suggérés par une IA ne visaient rien
12	Configuration SMB	`Get-SmbServer/ClientConfiguration`	Signature exigée des deux côtés, SMB1 off, invité off — symétrique	Négociation SMB hors de cause
13	Capture réseau (échec)	`pktmon` + dissection SMB2/NTLMSSP	Négociation OK → CHALLENGE émis → AUTHENTICATE rejeté `STATUS_LOGON_FAILURE`. AUTHENTICATE de CLIENT parfaitement formé (NTLMv2, MIC, AV pairs, `cifs/SERVER`)	Le rejet tombe au traitement du 3e message NTLM, message pourtant irréprochable

#	TEST	COMMANDE / MÉTHODE	RÉSULTAT	ENSEIGNEMENT
14	Comparaison MachineID NTLM	Extraction du champ `MsvAvSingleHost` des deux AUTHENTICATE (CLIENT puis SERVER)	CLIENT `6b16d192…623f` ≠ SERVER `bf014331…a050`	Théorie « réflexion NTLM par MachineID dupliqué » **réfutée** — le MachineID n'est pas cloné
15	Pare-feu CLIENT	Capture des SYN sans réponse sur 445 entrant	Règle `FPS-SMB-In-TCP` désactivée (attendu : jamais configuré côté CLIENT)	Cause de l'erreur 67 dans le sens SERVER→CLIENT (problème annexe, corrigé)
16	**Contre-épreuve : sysprep**	`sysprep /generalize /oobe /reboot` sur SERVER uniquement, puis retest depuis CLIENT	**4624 : ouverture de session RÉUSSIE** (NTLM V2, clé 128 bits, support.tech depuis CLIENT), nouveau SID machine `S-1-5-21-266589952-…`, puis erreur 5 (autorisation C$, normale)	Une seule variable changée (identité machine régénérée) → authentification rétablie

2. THÉORIES ÉLIMINÉES (AVEC LA PREUVE QUI LES TUE)

1. **SAM/LSASS corrompus** — réfuté par les sessions locales fonctionnelles (test 2) et le bouclage réussi (test 10).
2. **Résolution de nom / mauvaise machine jointe** — réfuté par le test par IP (test 5) et les 4625 bien générés côté SERVER (test 6).
3. **`LmCompatibilityLevel` incompatible** — réfuté : valeur par défaut, identique, jamais déviée (test 11).
4. **Mot de passe vide bloqué en réseau** — réfuté par le retest avec mot de passe frais horodaté (test 8).
5. **Problème lié à un compte précis** — réfuté par le compte témoin post-clonage (test 9).
6. **Réflexion NTLM via MachineID dupliqué** — réfuté par la capture : MachineID différents avant sysprep (test 14).

3. CONCLUSION

Cause racine : identité machine dupliquée par le clonage des VM sans `sysprep /generalize` — dont le marqueur observable est le SID machine identique. En workgroup, l'authentification NTLM entre deux clones échoue côté serveur avec `STATUS_LOGON_FAILURE` (0xC000006D) et un sous-état vide (0x0), **avant toute comparaison de mot de passe**, quel que soit le compte utilisé. Les sessions locales et le bouclage restent fonctionnels, ce qui rend le symptôme trompeur (« mot de passe incorrect » alors que le mot de passe n'est jamais évalué).

Correctif validé : `sysprep /generalize` sur une seule des deux machines suffit à rétablir l'authentification (démontré par le 4624 post-sysprep). **Prévention** : toujours généraliser une image avant de la cloner.

Réserve d'honnêteté : sysprep régénère le SID machine et d'autres secrets d'identité locale en un seul geste ; la formulation rigoureuse est donc « identité machine clonée », le SID identique en étant le marqueur de détection fiable (`whoami /user`).

4. RÉFLEXES À RETENIR (TRANSPOSABLES EN ENTREPRISE)

- **Un droit/un accès ne se lit pas, il se teste** — et un échec d'authentification se diagnostique par le sous-état du 4625 côté serveur : `0xC000006A` = mot de passe comparé et rejeté ; `0xC0000064` = compte inconnu ; `0x0` = refus hors comparaison (stratégie/identité machine).
- **Erreur 5 ≠ erreur 86** : la 86 est un échec d'authentification, la 5 un refus d'autorisation — donc une authentification réussie. Savoir situer l'étage qui rejette évite d'élargir des droits au hasard.
- **`whoami /user` détecte le clonage** en 5 secondes (SID machine identique = image non généralisée).
- **Souder `hostname;` aux commandes** sur des machines jumelles : cinq erreurs de fenêtre dans cette seule enquête. Astuce : `function prompt { "[$env:COMPUTERNAME] PS $($pwd)> " }` dans `$PROFILE`.
- **Chaque modification doit produire sa preuve immédiate** (`PasswordLastSet`, `Get-LocalGroup`, « 1 fichiers traités ») avant le test suivant — trois « commandes fantômes » ont pollué cette enquête.
- **Un correctif qui échoue ne se rejoue pas à l'identique** (boucle des « resets » de LmCompatibilityLevel) : exiger un critère de vérification avant toute modification, y compris quand c'est une IA qui la propose.
- **Méfiance envers les variables confondantes** : sysprep corrige plusieurs choses à la fois ; c'est la capture réseau (MachineID différents) qui a permis d'isoler la bonne.