

DOCUMENTATION DU LAB · JP CONSULTING

Dossier d'exploitation

Faire tourner le lab au quotidien

Jean-Philippe Rebischung

Dossier d'exploitation

Comment faire tourner le lab JP Consulting au quotidien : démarrage, tâches périodiques, mises à jour, pannes connues

IDENTIFICATION DU DOCUMENT		
VERSION 1.0	DATE 01/11/2026	STATUT Édition publique
AUTEUR Jean-Philippe Rebischung	PUBLIC VISÉ Technicien d'exploitation, formateur, recruteur	RÉFÉRENCE DEX-01

OBJET DU DOCUMENT

Ce dossier dit **comment on fait vivre** le lab une fois qu'il est construit : dans quel ordre l'allumer et l'éteindre, quelles tâches reviennent chaque jour ou chaque mois, comment surveiller, comment mettre à jour sans casser, qui a quels droits, comment une demande est traitée, et que faire devant les pannes déjà rencontrées. Il décrit le lab **tel qu'il est au 01/11/2026**. Il s'appuie sur le DAT-01 (ce qui existe) et le PRA-01 (après un sinistre).

SOMMAIRE

1. L'essentiel
2. Démarrage et arrêt
3. Tâches périodiques
4. Sauvegardes et tests de restauration
5. Supervision et journaux
6. Mises à jour
7. Comptes et droits d'administration
8. Problèmes connus
9. Lexique

1. L'essentiel

En clair

Le DAT dit **ce qui existe**. Le DEX dit **ce qu'il faut faire, régulièrement, pour que ça continue de marcher**. C'est le carnet de bord de la personne qui s'occupe du parc.

Avec les mots du métier

Un **dossier d'exploitation** (DEX) regroupe les consignes de **run** : procédures de démarrage et d'arrêt, tâches périodiques, supervision, sauvegardes, gestion des changements, comptes à privilèges. Il est distinct du **build** (les procédures d'installation) et du PRA (le sinistre).

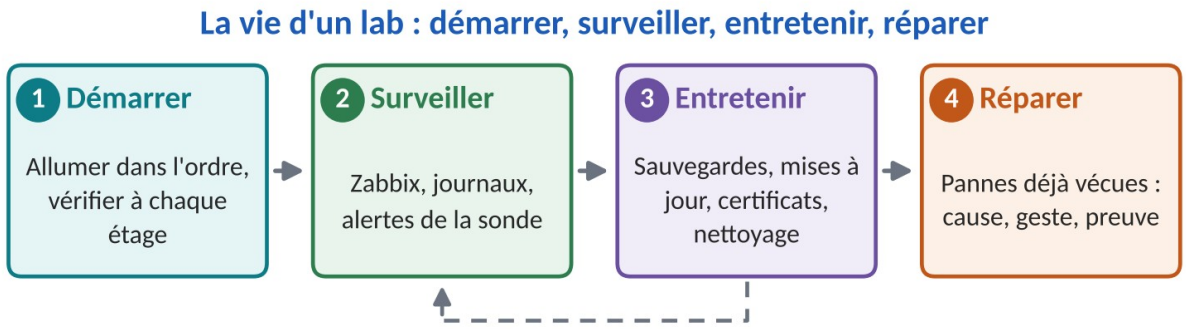


Figure 1 — le cycle d'exploitation ; chaque chapitre du dossier correspond à une étape

Si vous voulez…	Aller au chapitre
Allumer ou éteindre le lab	2 — Démarrage et arrêt
Savoir ce qu'il y a à faire chaque jour, chaque mois	3 — Tâches périodiques
Vérifier que les copies se font, et les tester	4 — Sauvegardes et tests de restauration
Savoir ce qui est surveillé et ce qui ne l'est pas	5 — Supervision et journaux
Mettre un composant à jour	6 — Mises à jour
Savoir qui a quels droits, et comment une demande de droits se traite	7 — Comptes et droits d'administration
Dépanner une panne qu'on a déjà vue	8 — Problèmes connus

Dans le lab

Le lab est exploité par **une seule personne**, qui joue tour à tour les trois niveaux du support (voir 7.3), sur deux PC de bureau **qui ne tournent pas la nuit** : aucune VM n'est allumée hors des séances. Beaucoup de tâches sont donc « à la demande » ou rattrapées au prochain allumage, ce qu'une entreprise ne ferait pas.

Ce dossier ne contient ni mot de passe, ni clé, ni secret : ils sont conservés à part.

2. Démarrage et arrêt

2.1 Démarrer

L'ordre complet, avec ce qu'il faut vérifier à chaque étage, est dans le chapitre 5 du PRA-01. L'essentiel : **réseau, puis identité, puis services, puis postes**. On ne passe à l'étage suivant que quand le précédent répond. Seul un **socle** reste allumé pendant une séance : SRV-DC01, PFSENSE01, PFSENSE02 et SRV-FREEIPA01. Les autres machines sont allumées **selon la tâche** : la mémoire est comptée (environ six VM en même temps sur le PC hôte du site A, un poste Windows 11 prenant près de 5 Go).

Ordre	Machines	Contrôle avant de continuer
1	PC hôte du site A, PFSENSE01 ; PC hôte du site B (HOTE-PROXMOX), qui relance seul PFSENSE02 et SRV-FREEIPA01	Interfaces web des pare-feux joignables
2	Tunnel IPsec entre les sites	Tunnel *Established* ; ping du site B vers le site A
3	SRV-DC01 (le DHCP démarre volontairement en différé), puis vérification de SRV-FREEIPA01	dcdiag /q ; ipactl status
4	SRV-ADCS01, SRV-WSUS01 — seulement si la tâche en a besoin	Autorité joignable ; liste de révocation publiée
5	SRV-SYSLOG01, puis SRV-ZABBIX01, SRV-GLPI01 — selon la séance	Ports du collecteur en écoute ; interfaces web en HTTPS
6	Postes clients et poste technicien (WinTech01)	Ouverture de session, adresse reçue

> **Cinq dépendances à connaître**
>
> **Un service qui dépend d'une machine éteinte tombe avec elle.** Il faut savoir quelles VM doivent tourner pour quelle tâche.
>
> **SRV-ADCS01 doit être allumée pour signer** un certificat : éteinte, la demande échoue avec l'erreur 0x800706ba.
>
> **SRV-DC01 doit être allumé à 13 h** pour que la sauvegarde quotidienne ait lieu : elle ne se rattrape pas.
>
> **GLPI dépend du contrôleur pour la connexion avec un compte du domaine** (annuaire en LDAPS, certificat du contrôleur) : SRV-DC01 éteint ou certificat expiré, plus personne ne se connecte avec son compte.
>
> **Zabbix muet ne signifie pas « tout va bien »** : si la VM Zabbix est éteinte, personne ne surveille.

2.2 Éteindre (à la fin de chaque séance : aucune VM ne tourne la nuit)

1. Éteindre les postes clients et le poste technicien.
2. Éteindre SRV-GLPI01, SRV-ZABBIX01, SRV-WSUS01, SRV-ADCS01 (arrêt propre depuis le système, pas par coupure).
3. Éteindre SRV-SYSLOG01 en dernier des services : les émetteurs gardent leurs messages en file pendant la coupure.
4. Éteindre SRV-DC01 en dernier des serveurs Windows, après les machines qui s'y authentifient.
5. **Éteindre toutes les VM avant de fermer VMware Workstation**, puis éteindre le PC hôte.
   → Fermer Workstation en laissant le contrôleur « en arrière-plan » l'a rendu non pilotable.

Piège vécu. Un instantané se prend **VM éteinte**, **avant un exercice ou une mise à jour**, et se **supprime après**. Le contrôleur en a déjà porté cinq, vieux de quatre mois : tous supprimés depuis, aucun n'existe aujourd'hui.

3. Tâches périodiques

3.1 Ce qui se fait tout seul

Tâche	Fréquence	Où	À savoir
Sauvegarde du contrôleur (système complet et E:)	Tous les jours à 13 h	SRV-DC01, Sauvegarde Windows Server	Réussie chaque jour. VM allumée à cette heure, sinon pas de copie
Copies instantanées du volume E: (versions précédentes des partages)	Tous les jours à 12 h et 17 h	SRV-DC01	Actives ; un passage manqué est rattrapé
Sauvegarde de GLPI (base et fichiers)	Tous les jours à 13 h 30	SRV-GLPI01 (script et minuteur)	14 copies gardées ; le minuteur rattrape un passage manqué
Récupération des copies de GLPI par un second serveur	Toutes les 2 heures	SRV-FREEIPA01 (site B)	Compte restreint, 60 jours gardés. C'est la copie sur une **seconde machine physique**
Installation des mises à jour des postes	Tous les jours à 12 h	GPO *WSUS - Postes*	Postes allumés à cette heure seulement ; WinClt5 est exclu de la GPO
Installation des mises à jour des serveurs Windows	À la notification	GPO *WSUS - Serveurs*	Installation à la notification, sans redémarrage forcé
Rotation des journaux du collecteur	Quotidienne, 30 jours conservés, compressés	SRV-SYSLOG01 (minuteur systemd)	Le minuteur rattrape un passage manqué ; un journal vu pour la première fois ne tourne qu'au passage suivant
Renouvellement du mot de passe administrateur local	Tous les 30 jours	Windows LAPS, par GPO	Stocké chiffré dans l'annuaire

À noter. Les mises à jour de sécurité automatiques de SRV-GLPI01 (unattended-upgrades) ont déjà été activées sans effet réel : vérifier de temps en temps qu'elles s'appliquent.

3.2 Ce qui se fait à la main

Tâche	Quand	Comment	Objectif
Vérifier que la sauvegarde du contrôleur a eu lieu	Chaque semaine	wbadmin get versions sur SRV-DC01	Voir une version récente, avec la bonne date (heure UTC, format américain)
Vérifier la copie de GLPI sur le second serveur	Chaque semaine	Date du dernier fichier reçu sur SRV-FREEIPA01	Un fichier de moins de 24 h
Regarder l'état de la supervision	À chaque allumage	Interface web de Zabbix	Aucun problème non traité
Synchroniser WSUS	À la demande (VM non permanente)	Console *Services WSUS*, *Synchroniser maintenant*	Relever la date de dernière synchronisation avant d'approuver
Exporter la configuration d'un pare-feu	**Après chaque modification**	pfSense, *Diagnostics*, *Backup & Restore*, export chiffré	Ne jamais perdre une règle (exports des deux pare-feux à jour)
Tester une restauration	Après un changement important de la sauvegarde	Voir le PRA-01, chapitre 6	Prouver que la copie sert
Contrôler les instantanés VMware	Après chaque exercice, puis chaque mois	VMware Workstation, *Gestionnaire d'instantanés*	Aucun instantané ne doit rester sans raison
Contrôler l'espace du collecteur	Chaque mois	df -h / et du -sh /var/log/distant	Le dossier est sur la partition racine : un disque plein arrêterait toute la VM
Vérifier les échéances de certificats	Chaque trimestre	Zabbix (certificat GLPI) ; lecture en ligne de commande pour les autres	Renouveler 30 jours avant

3.3 Échéances connues

Élément	Échéance
Certificat du contrôleur (connexion LDAPS de GLPI)	**04/10/2027**
Certificats HTTPS signés par l'autorité interne (GLPI, pare-feux, Proxmox)	Octobre 2028
Certificats de la chaîne de journalisation (DC, GLPI, Zabbix, WSUS)	Début janvier 2029
Autorité racine interne	Dix ans après sa création

Pistes d'évolution

Seul le certificat de GLPI est supervisé dans Zabbix. Celui du contrôleur est le plus proche, et le plus lourd de conséquences : expiré, GLPI n'authentifie plus par l'annuaire.

4. Sauvegardes et tests de restauration

Ce qui est sauvegardé, où, et ce qui a été restauré pour de vrai est décrit en détail dans le PRA-01 (chapitres 2 et 7). Ici, ce qu'il faut **faire** pour que cela reste vrai.

Élément	Fait par	Vérification d'exploitation
Contrôleur de domaine	Sauvegarde planifiée à 13 h	wbadmin get versions ; Get-WBPolicy pour relire l'horaire et le contenu
Partages (versions précédentes)	Copies instantanées de E: à 12 h et 17 h	Onglet *Versions précédentes* d'un dossier ; une restauration a été jouée
GLPI	Script local à 13 h 30, puis récupération toutes les 2 h par un second serveur	Dernier fichier de moins de 24 h sur les deux machines ; restauration de la base testée
VM du site B	**À la main** (vzdump), pas de planification ; une archive existe, à renouveler	Date de l'archive sur le disque externe ; refaire après un changement important
Pare-feux	Export à la main après chaque modification	Deux exemplaires, supports différents, mot de passe de chiffrement conservé à part
GPO	Backup-GPO -All avant toute refonte ; la planification reste à programmer	Dossier daté dans C:\Outils et copie sur le PC hôte
Avant une mise à jour applicative	Copie manuelle de la base et des fichiers, puis instantané VM éteinte	Voir le chapitre 6

Machine : SRV-DC01 · **Compte : admin.domaine** · **liste les versions disponibles et relit la planification**

```
wbadmin get versions
Get-WBPolicy
```

Résultat attendu

Une version datée de moins de 24 heures (l'identifiant est en **heure UTC**, format américain), et une planification à 13 h qui contient la récupération complète et le volume E:.

Si ce n'est pas le cas

Si la dernière version est ancienne : la VM était éteinte à 13 h, ou le disque dédié n'est plus visible (Get-Disk). Lancer une sauvegarde unique avec les options de la planification, puis chercher la cause.

Pistes d'évolution

Les copies du site A sont sur le **même PC** que les machines : la règle 3-2-1 n'est pas tenue. Seule la copie de GLPI sort du PC, vers une seconde machine.

La sauvegarde de l'hôte avec AOMEI manque de place : elle n'est pas comptée parmi les sauvegardes fiables.

Les sauvegardes de Zabbix et du collecteur ne sont pas planifiées.

5. Supervision et journaux

5.1 Ce que Zabbix surveille

Élément	Méthode	Ce qu'on regarde
PC hôte du site A, SRV-DC01, SRV-SYSLOG01, SRV-FREEIPA01	Agent Zabbix	Processeur, mémoire, disque, disponibilité
PFSENSE01, PFSENSE02	SNMP v2c (le second à travers le tunnel)	Interfaces, disponibilité
Hôte Proxmox	API, compte en lecture seule	Charge, disque, machines
Certificat de GLPI	Agent 2	Validité et jours restants

L'interface de Zabbix est ouverte en **lecture seule** aux techniciens N1 et N2 (groupe *Support - Lecture seule*, accès depuis le poste technicien) : ils regardent, ils ne modifient rien. Une **liste de bruit connu** (alertes attendues, sans action) est tenue à jour : la consulter avant d'ouvrir un ticket.

> **Ce qui n'est pas surveillé**
>
> Les clients Windows et Linux ne sont **pas** supervisés (choix du périmètre).
>
> Il n'existe pas de sonde du tunnel IPsec : une coupure se découvre par l'usage ou par les journaux.
>
> SNMP v2c n'est pas chiffré. Les VM ne tournent pas la nuit : pas de supervision continue.
>
> Nagios XI supervise le PC hôte, à la demande ; il n'est pas allumé en permanence et n'alimente pas Zabbix.

5.2 Journaux

Le collecteur SRV-SYSLOG01 reçoit les journaux de toutes les machines, rangés dans `/var/log/distant/<machine>/<programme>.log`. Trois canaux : RELP sur TLS (20514) pour les machines Linux, syslog TLS (6514) pour les serveurs Windows, UDP 514 pour les pare-feux et les alertes de la sonde Suricata.

Je veux vérifier…	Commande	Où
Que le collecteur écoute	ss -tulnp | grep -E '20514|514|6514'	SRV-SYSLOG01
Qu'un émetteur Linux parle	logger -p auth.warning 'test' puis tail -f /var/log/distant/<machine>/*.log	Émetteur, puis collecteur
Les erreurs d'envoi	journalctl -u rsyslog -e	Émetteur ou collecteur

> **Piège rencontré**
>
> Après tout redémarrage du collecteur, **retester chaque émetteur** : des connexions à moitié ouvertes peuvent subsister et les messages se perdent sans erreur visible. Lancer logger **sans** sudo, car chaque sudo produit lui-même des messages d'authentification qui fausseraient le compte.

5.3 Détection d'intrusion

Suricata tourne en **détection seule** sur les deux pare-feux, avec le jeu de règles ET Open. Ses alertes arrivent au collecteur. La règle 2210044 est désactivée par une liste de gestion des règles, sur PFSENSE01. Aucune alerte ne déclenche de notification : il faut aller les lire. Dans les exercices de sécurité, c'est là qu'on cherche la trace des attaques lancées depuis les postes d'audit.

6. Mises à jour

Règle commune : **sauvegarder avant, changer une chose à la fois, vérifier après**. Pour les machines virtuelles, un instantané pris VM éteinte sert de point de retour, mais pas de sauvegarde ; on le **supprime** une fois le changement vérifié.

Composant	Comment	Précautions
Postes et serveurs Windows	WSUS : approuver d'abord pour **un poste pilote**, observer, puis élargir ; serveurs : installation à la notification (GPO *WSUS - Serveurs*)	Instantané du poste avant une mise à niveau de version ; synchroniser WSUS avant
Mise à niveau de version de Windows	Classification *Upgrades* dans WSUS, approuver la seule version voulue pour les postes. WinClt2 à 4 sont en 23H2 (hors support) ; les autres sont en 26H2	Peut échouer avec 0xC1900107 : réinitialiser Windows Update puis recommencer
Machines Linux	Mises à jour système, par Ansible pour les serveurs d'administration. Ansible est la **source unique** du pare-feu et du SSH des serveurs Linux du site A	Instantané avant ; redémarrer si le noyau change ; tester le service ensuite ; relancer Ansible : zéro changement attendu (*changed=0*)
Zabbix	**Le serveur avant les agents**	Copier la configuration de l'agent avant le changement
GLPI	Cinq temps : sauvegarder (base **et** fichiers), poser un point de retour, remplacer le programme, migrer la base par l'outil de l'éditeur, contrôler	Sauvegarder aussi la clé de chiffrement glpicrypt.key, sinon les secrets stockés sont perdus
Pare-feux pfSense	Depuis l'interface web	Exporter la configuration avant et après
Règles Suricata	Mise à jour automatique des règles ET Open	Contrôler que les règles désactivées le restent

> **Exemple vécu**
> Une faille critique de PHP a été annoncée. Elle a été corrigée dans les deux jours sur GLPI (PHP 8.4.27), Zabbix et Nagios, **un snapshot avant chacun, supprimé après**. Le serveur FreeIPA n'était pas concerné. C'est le modèle à suivre : repérer ce qui est touché, traiter une machine à la fois, vérifier, nettoyer.

6.1 Mettre à jour GLPI : le geste type

Objectif	Passer GLPI à une version corrective de la même branche (10.0.x) sans perdre de données.
Machine	SRV-GLPI01
Compte	Compte d'administration Linux
Outil	Terminal, navigateur

1. Copier la base et les fichiers dans un dossier daté.
   → La dernière ligne de la copie dit *Dump completed*.
2. Éteindre la VM, prendre un instantané, la rallumer.
   → Point de retour.
3. Arrêter Apache, **déplacer** (et non supprimer) l'ancien programme, extraire le nouveau, recopier le fichier downstream.php, rendre la main à www-data.

4. Lancer la migration de la base (commande ci-dessous).
   → Le message *Migration effectuée* apparaît.
5. Contrôler dans le navigateur : connexion (avec un compte du domaine **et** le compte local), version affichée, un ticket, l'inventaire, aucun bandeau d'alerte.
6. Quand tout est vérifié, **supprimer l'instantané**.

Machine : SRV-GLPI01 · **Compte : compte sudo**

```
sudo -u www-data php /var/www/html/glpi/bin/console db:update
```

Résultat attendu

La nouvelle version est affichée et les données (tickets, inventaire) sont intactes.

Si ce n'est pas le cas

Si la migration signale une clé de chiffrement absente, recopier glpicrypt.key depuis l'ancienne configuration (droits 640) avant de continuer.

Niveau réel

Mise à jour d'une version corrective, dans la même branche, sans module, sur un GLPI de test. Un changement de branche est un autre exercice.

7. Comptes et droits d'administration

Compte	Où	Usage	Règle
admin.domaine	Domaine Windows	Administration du domaine	Pas pour le quotidien ; session élevée seulement quand il le faut. Le technicien N2 ne se connecte pas au contrôleur : c'est ce compte qui sert
adm-ray.boot, adm-sarah.fraichit	Domaine Windows	Comptes d'administration limités des techniciens N2 et N1	Droits strictement délégués ; jamais le compte du domaine entier
admin.linux	FreeIPA	Administration Linux, sudo par un rôle	Un compte local du même nom existe sur trois serveurs Linux : c'est celui qu'utilise Ansible
svc.glpi-ldap	Domaine Windows	Compte de service : lecture de l'annuaire pour la connexion à GLPI	Lecture seule ; ne sert à aucun humain
adm.secours	Poste technicien	Accès local si l'annuaire est injoignable	À n'utiliser qu'en cas de panne
Compte DSRM	SRV-DC01	Restauration de l'annuaire	Mot de passe fixé à la promotion, conservé hors du serveur
Mot de passe administrateur local des postes	Postes Windows	Dépannage local	Géré par LAPS : lu dans l'annuaire, jamais noté

7.1 Règles d'hygiène

- Un compte d'administration pour administrer, un compte ordinaire pour le reste.
- Les connexions SSH se font par clé ; le mot de passe SSH est refusé sur les machines Linux.
- Les accès aux consoles des pare-feux sont protégés par mot de passe ; l'administration de PFSENSE02 passe par le tunnel.
- Les invites de commande sont colorées selon la criticité : rouge pour les serveurs critiques, jaune pour les secondaires, vert pour les clients. Regarder la couleur avant de taper.
- Aucun mot de passe, clé ou secret ne figure dans un document ou un script versionné.
- Verrouillage d'un compte : 5 essais, 15 minutes, remise à zéro après 15 minutes. Mot de passe : 7 caractères, 42 jours, historique de 24.

7.2 Traiter une demande de droits

Toute demande de droits suit le même chemin, **dans GLPI** (il n'y a pas de messagerie). Le lab ne connaît qu'une règle d'or : **personne ne donne un accès sur la seule demande de celui qui le veut**.

1. **sarah.fraichit (N1)** prend le ticket et **vérifie l'identité** du demandeur.
   → Catégorie *Comptes et accès*, priorité selon l'impact.
2. Le **propriétaire des données** (le responsable du dossier) **valide dans le ticket**.
   → Sa réponse reste écrite dans le suivi.
3. **ray.boot (N2)** exécute : ajout au groupe de domaine, selon le modèle **AGDLP** (comptes dans un groupe global, groupe global dans un groupe de domaine local, droits donnés au groupe local).
   → Jamais de droit donné à un compte seul.

4. ray.boot **vérifie** l'effet (connexion de l'utilisateur, lecteur réseau présent) et rédige la solution dans le ticket.
5. Le **demandeur approuve** la solution ; **admin.domaine (N3)** ne peut que **clore**.
   → Un ticket sans approbation ne se clôt pas.

7.3 Les trois niveaux

Niveau	Qui	Rôle	Point d'attention
N1	sarah.fraichit	Prise du ticket, qualification, vérification d'identité, réponses simples	Ne modifie pas l'annuaire
N2	ray.boot	Exploitation courante : arrivées et départs, droits, WSUS, restaurations de fichiers	Ne se connecte pas au contrôleur : compte d'administration utilisé ; les délégations dédiées aux groupes de support ne sont pas encore posées
N3	admin.domaine	Diagnostic complexe, sécurité, architecture, clôture	Clôt seulement ce que le demandeur a approuvé

Pistes d'évolution

Une seule personne tient les trois rôles : il n'y a ni séparation réelle des tâches, ni astreinte, ni escalade. La séparation est **jouée** : comptes, droits et circuit de ticket sont distincts, même si la main est la même.

8. Problèmes connus

Tableau des pannes **réellement rencontrées** dans le lab. Chaque ligne donne le symptôme, la cause trouvée et le geste. Les **playbooks** (un par grande catégorie de ticket GLPI) et les procédures PROC-01 à PROC-31 en sont le prolongement : ils existent et sont en cours de refonte. Les causes sont celles qui ont été **prouvées** ; une cause supposée n'y figure pas. Les lignes « constaté, pas encore traité » sont des défauts connus, non des causes à rechercher.

8.1 Réseau, sites et machines

Symptôme	Cause trouvée	Geste
Plus de liaison entre les sites après un redémarrage de PFSENSE02	La configuration IPsec n'a pas été chargée au démarrage	Vérifier le tunnel ; une garde planifiée recharge la configuration
Une règle de pare-feu correcte n'a aucun effet	Le blocage automatique des réseaux privés est évalué **avant** la règle (le « WAN » du lab est un réseau privé)	Lire le journal de filtrage : le numéro de la règle qui bloque le dit ; désactiver ce blocage (légitime dans le lab)
Un poste reste en adresse 169.254	Aucun DHCP n'a répondu : le seul DHCP du réseau est celui du contrôleur, éteint	Allumer le contrôleur ; un poste d'administration reçoit une adresse fixe, pour ne pas dépendre du serveur qu'il administre
Au démarrage, le DHCP du contrôleur signale des erreurs	Il démarre avant l'annuaire	Démarrage différé du service
Trois VM tombent en même temps, code d'arrêt 0x124	Le disque NVMe virtuel a cessé de répondre : SSD d'entrée de gamme, sans cache, bien rempli (pile d'appels du vidage mémoire dans le pilote NVMe)	VM serveurs sur un SSD plus rapide, instantanés supprimés ; lire le vidage mémoire **avant** les hypothèses. Aucun arrêt depuis
Contrôleur « non pilotable » après fermeture de Workstation	Workstation fermé, VM laissées en arrière-plan	Arrêt par la ligne de commande de VMware ; ensuite, éteindre les VM avant de fermer
Disque externe invisible	Branché sur un port USB 2.0 (dmesg : liaison *full-speed*)	Changer de port
Disque externe qui refuse de s'éjecter	Cause non établie	Set-Disk -IsOffline $true

8.2 Services Windows, GLPI et supervision

Symptôme	Cause trouvée	Geste
Demande de certificat refusée, erreur 0x800706ba	La VM SRV-ADCS01 est éteinte	Allumer la VM de l'autorité, réessayer
GLPI : erreur 403 sur l'inventaire	Réglage d'inventaire non enregistré (prouvé en base)	Enregistrer le réglage, retester
Un contrôleur ne se met plus à jour	Mises à jour de juin et juillet préparées à moitié puis annulées ; DISM répare 0 fichier sur 442	Savoir s'arrêter : un nouveau contrôleur à jour a remplacé l'ancien
Une GPO n'arrive pas sur le poste	Absente : jamais liée à l'UO. Refusée : lecture retirée aux ordinateurs du domaine dans le filtrage	gpresult sur le poste : absente = lien, refusée = filtrage (onglet *Délégation*), appliquée sans effet = paramètres
Mise à niveau Windows refusée, 0xC1900107	Nettoyage d'une tentative précédente en attente	Réinitialiser Windows Update, recommencer
La GPO d'imprimantes cible un serveur éteint	Elle vise SRV-WSUS01, souvent hors tension	Allumer la VM avant de tester les imprimantes ; corriger la cible reste à faire
Lettres de lecteur fantômes dans d'anciens profils	Elles viennent d'anciennes sessions, hors du mappage actuel (GPO *Mappage lecteurs*, par nom de serveur)	À nettoyer : constaté, pas encore traité
Page Rocky par défaut à la racine web de Zabbix	Elle est toujours servie à la racine	À remplacer : constaté, pas encore traité
Groupes d'hôtes en double dans Zabbix	Deux groupes portent le même nom	À fusionner : constaté, pas encore traité
Les clichés de E: décalés d'une heure après le changement d'heure	Le chemin des clichés suit le temps universel : heure locale moins 1 h désormais, moins 2 h avant	Recalculer le chemin avant de chercher la version

8.3 Journaux et sécurité

Symptôme	Cause trouvée	Geste
Des journaux n'arrivent plus au collecteur	Collecteur redémarré : connexions à moitié ouvertes	Retester chaque émetteur avec logger
Journaux Linux en double dossier	Casse différente dans le nom de machine	Option de passage en minuscules dans rsyslog
dcdiag /q signale une erreur de journal système au démarrage	Événements du démarrage : hyperviseur absent en VM	Normal dans le lab ; vérifier qu'elle est la seule
SSH qui expire sur des serveurs Windows (après la migration du contrôleur)	Service OpenSSH arrêté, **et** règle livrée valable pour le profil Privé alors que le serveur est en profil Domaine	Démarrage automatique du service, règle pour le profil Domaine limitée au poste d'administration, clé publique déposée

9. Lexique

Terme	En clair
DEX	Dossier d'exploitation : ce document.
Run / build	Faire tourner l'existant / le construire.
Supervision	Surveillance automatique de l'état des machines.
Instantané	Photo de l'état d'une VM, sur le même disque ; point de retour, pas sauvegarde.
Copie instantanée	Version précédente d'un fichier d'un partage, gardée par le serveur à heure fixe.
Collecteur de journaux	Serveur qui rassemble les journaux de toutes les machines.
Rotation de journaux	Archivage et nettoyage périodique des fichiers de journaux.
LAPS	Mot de passe administrateur local unique et renouvelé par machine.

Terme	En clair
WSUS	Serveur de mises à jour Windows de l'entreprise.
Poste pilote	Machine qui reçoit un changement en premier, pour tester.
AGDLP	Méthode de droits : comptes, groupes globaux, groupes locaux de domaine, permissions.
N1, N2, N3	Les trois niveaux de support : accueil, exploitation, expertise.
Playbook	Fiche réflexe : la marche à suivre pour une catégorie de ticket.
DSRM	Mode de démarrage d'un contrôleur de domaine pour restaurer l'annuaire.
IDS	Détection d'intrusion, sans blocage.
SNMP	Protocole de supervision des équipements réseau.