

DOCUMENTATION DU LAB · JP CONSULTING

Dossier d'architecture

Ce qui existe dans le lab, comment c'est relié, et pourquoi

Jean-Philippe Rebischung

Dossier d'architecture technique

Ce qui existe dans le lab JP Consulting, comment c'est relié, et pourquoi

IDENTIFICATION DU DOCUMENT		
VERSION 1.0	DATE 01/11/2026	STATUT Édition publique
AUTEUR Jean-Philippe Rebischung	PUBLIC VISÉ Responsable technique, formateur, recruteur	RÉFÉRENCE DAT-01

OBJET DU DOCUMENT

Ce dossier décrit l'architecture du lab **JP Consulting** : les deux sites, les réseaux, l'adressage, les serveurs et leurs rôles, l'identité et l'organisation des comptes, les flux autorisés, la sécurité, la supervision, la sauvegarde. Chaque choix y est accompagné de sa raison et de sa limite. Il décrit le lab **tel qu'il est au 01/11/2026**. Il sert de socle : le dossier d'exploitation, le plan de reprise, les playbooks et les procédures y renvoient.

SOMMAIRE

1. Contexte et objectifs
2. Vue d'ensemble
3. Sites et réseaux
4. Plan d'adressage
5. Serveurs et rôles
6. Services d'identité
7. Matrice de flux
8. Sécurité
9. Supervision et journaux
10. Sauvegarde
11. Choix d'architecture et justification
12. Points d'amélioration et évolutions
13. Lexique

1. Contexte et objectifs

En clair

Ce lab est une petite entreprise fictive, **JP Consulting**, montée sur deux ordinateurs personnels. Elle sert à s'entraîner sur tout ce qu'un technicien systèmes et réseaux croise en entreprise : monter une infrastructure, puis la faire vivre comme un service informatique.

Le lab est né pour rejouer ce qui a été vu en formation : un domaine Windows, quelques serveurs, des postes. Il a ensuite grossi pour couvrir une infrastructure complète, au sens **architecture technique** : identité, réseau et pare-feu, sauvegarde, supervision, journalisation, certificats, inventaire, automatisation. Les machines sont des **machines virtuelles** (VM) : des ordinateurs simulés, hébergés sur un ordinateur réel. Depuis la fin du montage, le lab sert aussi à **pratiquer le métier** : des utilisateurs fictifs ouvrent des tickets, des techniciens de niveaux différents les traitent, des pannes sont provoquées puis corrigées.

1.1 Objectifs

Objectif	Ce que cela implique dans le lab
Préserver les acquis de la formation	Chaque brique vue en cours (AD DS, DNS, DHCP, GPO, partages, WSUS) existe et fonctionne.
En apprendre de nouvelles	FreeIPA et l'approbation avec l'AD, tunnel IPsec, VPN, Zabbix, Ansible, PKI, journalisation centralisée. Linux, pfSense et GLPI avaient été vus en formation : le lab les approfondit.
S'exercer au métier	Installer, diagnostiquer, dépanner, documenter, sauvegarder et restaurer, comme en poste : tickets, niveaux N1 à N3, comptes à privilèges limités.
Pouvoir le défendre à l'oral	Chaque élément décrit ici a été réellement monté ; ses limites sont écrites.

1.2 Périmètre

Dans le périmètre	Hors périmètre
Deux sites reliés par un tunnel chiffré	Aucun service exposé à Internet, sauf l'accès VPN
Deux domaines : Windows (Active Directory) et Linux (FreeIPA), reliés par une approbation	Messagerie : GLPI est le seul canal de communication avec les utilisateurs
Pare-feux, VPN, détection d'intrusion	Un vrai matériel réseau administrable : le switch est non administrable
Sauvegarde, supervision, journalisation, inventaire, tickets	Un SIEM, une haute disponibilité, un second contrôleur de domaine en service
Autorité de certification interne	Une imprimante réelle (celle du lab est fictive)

Le cadre du lab

C'est un lab : deux ordinateurs de bureau, des VM, aucun utilisateur réel, aucune donnée réelle. Rien de ce dossier ne décrit un environnement de production.

Les noms de machines, de comptes et de domaines sont des noms fictifs ; les adresses IP privées et les numéros de port sont ceux du lab.

1.3 Documents liés

Document	Rôle
PROC-01 à PROC-31	Comment chaque composant a été construit, étape par étape.
DEX	Comment on le fait tourner : démarrage, tâches périodiques, supervision, mises à jour.
PRA	Que faire après un sinistre : scénarios, ordre de reprise, tests réellement faits.
Playbooks	Un document par catégorie du service de tickets : que faire face à un incident ou à une demande, cas par cas.

2. Vue d'ensemble

Le lab est réparti sur **deux sites**. Le site A, un PC de bureau sous VMware Workstation, héberge le domaine Windows et les outils d'exploitation. Le site B, un second PC sous Proxmox VE, héberge le domaine Linux. Un pare-feu pfSense protège chaque site, et un tunnel chiffré relie les deux.

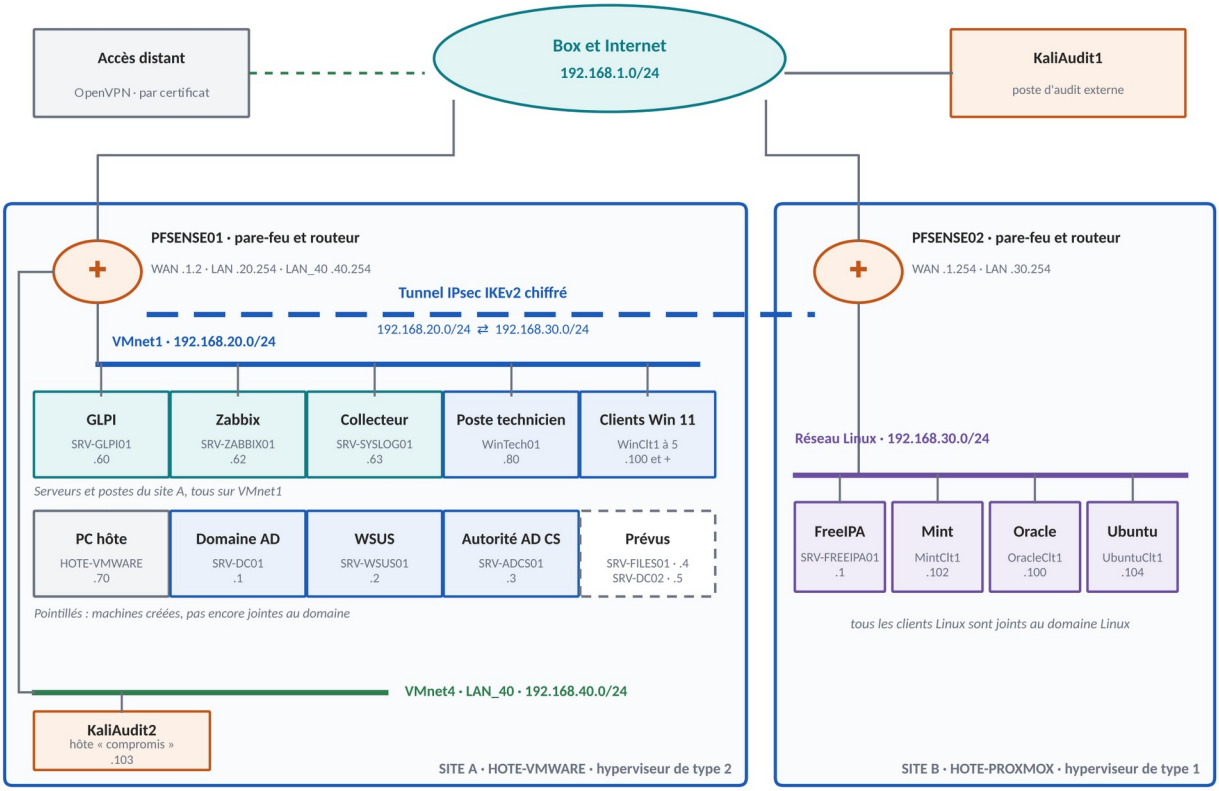


Figure 1 — architecture d'ensemble : deux sites, deux pare-feux, un tunnel IPsec, un accès distant par VPN

2.1 Principes d'architecture

Principe	En pratique
Un site, un hyperviseur, un pare-feu	Chaque site a son pare-feu pfSense, qui route et filtre tout ce qui entre ou sort.
Deux mondes d'identité	Active Directory pour Windows, FreeIPA pour Linux, reliés par une approbation à sens unique.
Segmentation par réseau	Quatre réseaux privés distincts ; un réseau est isolé (LAN_40) et n'a que l'accès à Internet.
Un accès distant minimal	Le VPN ne donne accès qu'à un seul poste d'administration.
Des comptes à la mesure du rôle	Chaque technicien a un compte courant et un compte d'administration restreint ; l'administrateur du domaine est réservé aux tâches d'administration.
Tout est vu et rien n'est caché	Supervision Zabbix, journaux centralisés, sondes Suricata, inventaire et tickets GLPI.
Allumé à la demande	Aucune VM ne tourne la nuit. Un socle reste allumé pendant les séances ; le reste s'allume pour l'usage.

À retenir

Le lab réunit les trois familles d'un système d'information : **l'infrastructure** (réseau, serveurs, sauvegarde), **les services** (identité, impression, mises à jour, certificats) et **l'exploitation** (supervision, journaux, tickets, automatisation).

Contrainte de fonctionnement

Socle allumé pendant les séances : le contrôleur de domaine, les deux pare-feux et le serveur FreeIPA. Le PC du site A supporte environ six VM en même temps : un poste Windows 11 coûte à lui seul environ 5 Go de mémoire à l'hôte.

Conséquence : les tâches planifiées doivent supporter une machine éteinte à l'heure dite (rattrapage au démarrage), et les rétentions se comptent en nombre de sauvegardes, pas en jours.

3. Sites et réseaux

3.1 Les deux sites

	Site A	Site B
Hyperviseur	VMware Workstation, **type 2** (installé sur un système d'exploitation)	Proxmox VE, **type 1** (installé directement sur la machine)
Machine	HOTE-VMWARE : PC de bureau Windows 11, 8 cœurs, 32 Go de mémoire	HOTE-PROXMOX : ancien PC de bureau (2014), 4 cœurs, 16 Go de mémoire, un seul disque (environ 1,7 To)
Disques	SSD NVMe (système, contrôleur de domaine), SSD SATA sans cache (autres VM), disque dur (données, images, exports)	Un disque, géré en LVM-thin
Contenu	Domaine Windows, WSUS, AD CS, GLPI, Zabbix, collecteur, clients Windows, poste technicien, poste d'audit interne	FreeIPA, clients Linux, pare-feu PFSENSE02, poste d'audit externe
Pare-feu	PFSENSE01	PFSENSE02 (VM)

En clair

Un hyperviseur de **type 2** est un logiciel posé sur Windows ; il dépend de son système. Un hyperviseur de **type 1** est le système lui-même : plus direct, plus proche de ce qu'on trouve en datacenter. Le lab en pratique un de chaque.

Leçon matérielle

Le disque SATA du PC hôte, sans mémoire cache, a provoqué des écrans bleus quand il était presque plein. Règle depuis : garder au moins 20 à 25 % d'espace libre sur ce disque ; le contrôleur de domaine est sur le disque NVMe.

3.2 Les réseaux

Réseau	Adresses	Rôle	Passerelle
Box et Internet	192.168.1.0/24	Réseau de la box ; WAN des deux pare-feux, administration de l'hôte Proxmox, poste d'audit externe	La box (.1)
LAN du site A (VMnet1)	192.168.20.0/24	Domaine Windows, services d'exploitation, clients Windows	.20.254
LAN_40 (VMnet4)	192.168.40.0/24	Réseau isolé : poste d'audit interne simulant un poste compromis, hors domaine	.40.254
Réseau Linux du site B (vmbr1)	192.168.30.0/24	FreeIPA et clients Linux, isolé du réseau de la box	.30.254
Tunnel VPN	172.30.100.0/24	Adresses données aux appareils connectés en VPN	172.30.100.1

3.3 Les pare-feux

Pare-feu	Interfaces	Particularités
PFSENSE01 (site A)	WAN .1.2 · LAN .20.254 · LAN_40 .40.254 · tunnel VPN .100.1	pfSense 2.7.2. Le réseau LAN_40 est bloqué vers le pare-feu lui-même et vers tout réseau privé : Internet seulement. Sonde Suricata sur le LAN Windows.
PFSENSE02 (site B)	WAN .1.254 · LAN .30.254	pfSense 2.7.2. Durci par dix règles de réseau local. Le site B ne joint ni le réseau de la box, ni le PC hôte. Sonde Suricata sur le LAN Linux.

3.4 Les liaisons entre sites

Liaison	Caractéristiques
Tunnel IPsec IKEv2, site à site	Phase 1 : AES-256-GCM, SHA-256, groupe DH 14, 28 800 s. Phase 2 : ESP AES-256-GCM, PFS 14, 3 600 s. Authentification par clé partagée (non écrite ici). Deux sous-réseaux protégés : .20 ↔ .30 et .40 ↔ .30.
Initiateur et répondeur	PFSENSE01 initie le tunnel (au démarrage, avec reconnexion). PFSENSE02 attend.
Garde de la configuration	Une tâche planifiée toutes les 5 minutes sur PFSENSE02 recharge la configuration IPsec. Elle fait suite à un incident vécu : la configuration n'était pas chargée au démarrage.
OpenVPN, accès distant	Accès distant par OpenVPN : autorité de certification dédiée, un certificat par appareil, deux connexions au maximum. Le tunnel ne donne accès qu'à un seul poste d'administration, et une tâche planifiée redémarre le service si besoin.

> **Contrainte du lab**
>
> Le switch est un modèle à cinq ports **non administrable** : pas de VLAN entre machines, pas de miroir de ports. La segmentation du lab se fait donc par réseaux virtuels de l'hyperviseur et par les pare-feux, pas par VLAN.
>
> Sur le PC hôte, deux routes statiques ramènent les réseaux .30 et .40 vers .20.254.

4. Plan d'adressage

L'adressage suit une convention : l'adresse donne la **famille** de la machine. On la lit de gauche à droite, et on sait en un coup d'œil à quoi sert une adresse.

Plage (dernier octet)	Famille	Exemples
.1 à .9	Infrastructure, serveurs Windows	.1 contrôleur de domaine · .2 à .5 autres serveurs Windows
.10 à .29	Services réseau	Réservé
.30 à .59	Serveurs d'application, périphériques	.50 imprimante fictive
.60 à .79	Supervision, tickets, administration	.60 GLPI · .62 Zabbix · .63 collecteur · .70 PC hôte
.80 à .84	Postes des techniciens (adresses fixes)	.80 poste technicien
.100 à .200	Postes clients (attribution automatique)	Clients Windows, clients Linux
.250 à .254	Passerelles	.254 pare-feu

> **Choix à connaître**
> Dans ce lab, la passerelle est en **.254** et **non en .1**. C'est un choix délibéré : l'adresse .1 est celle du contrôleur de domaine, et on évite la confusion « .1 égale routeur » des réseaux domestiques.

4.1 Attribution automatique (DHCP)

Paramètre	Valeur
Serveur	SRV-DC01
Étendue	192.168.20.10 à .200, avec exclusion de .10 à .99 : seuls .100 à .200 sont distribués
Durée du bail	8 jours
Options	003 passerelle : .254 · 006 DNS : .1 · 015 nom de domaine : jpconsulting.lan
Réservations	.60 (GLPI) et .61 (Nagios XI)
Démarrage du service	Automatique, début différé. Sans cela, le service vérifiait son autorisation avant que l'annuaire soit prêt, puis restait « en cours d'exécution » sans rien distribuer.

4.2 Adresses fixes par réseau

Adresse	Machine	Rôle
192.168.20.1	SRV-DC01	Contrôleur de domaine, DNS, DHCP, fichiers
192.168.20.2	SRV-WSUS01	WSUS, IIS, impression, NPS
192.168.20.3	SRV-ADCS01	Autorité de certification (Server Core)
192.168.20.4	SRV-FILES01	Futur serveur de fichiers : VM créée, pas encore jointe au domaine
192.168.20.5	SRV-DC02	Futur second contrôleur de domaine : VM créée, pas encore jointe au domaine
192.168.20.50	Imprimante fictive	Pour les exercices d'impression
192.168.20.60	SRV-GLPI01	Tickets, inventaire, authentification par l'AD
192.168.20.61	SRV-NAGIOS01	Nagios XI : supervise le PC hôte, allumé à la demande
192.168.20.62	SRV-ZABBIX01	Supervision
192.168.20.63	SRV-SYSLOG01	Collecteur de journaux
192.168.20.70	HOTE-VMWARE	Carte de l'hôte, sans passerelle ; poste d'administration
192.168.20.80	WinTech01	Poste de travail des techniciens
192.168.20.254	PFSENSE01	Passerelle du réseau .20

Adresse	Machine	Rôle
192.168.30.1	SRV-FREEIPA01	FreeIPA, contrôleur Ansible
192.168.30.100	OracleClt1	Client Oracle Linux
192.168.30.102	MintClt1	Client Linux Mint
192.168.30.104	UbuntuClt1	Client Ubuntu
192.168.30.254	PFSENSE02	Passerelle du réseau .30
192.168.40.103	KaliAudit2	Poste d'audit interne, hôte « compromis » simulé, hors domaine
192.168.40.254	PFSENSE01	Passerelle de LAN_40
192.168.1.2	PFSENSE01 (WAN)	Côté box
192.168.1.13	HOTE-VMWARE	Bail statique sur la box
192.168.1.254	PFSENSE02 (WAN)	Côté box

5. Serveurs et rôles

5.1 Serveurs Windows du site A

Machine	Système, mémoire	Rôles
SRV-DC01	Windows Server 2025, 4 Go, 4 vCPU	AD DS (seul contrôleur, cinq rôles FSMO), DNS, DHCP, serveur de fichiers (disque E:), espace de noms DFS, FSRM, LAPS, Sauvegarde Windows Server, LDAPS (636), agent GLPI
SRV-WSUS01	Windows Server 2025, 6 Go	WSUS en HTTPS (8531), IIS (publication des listes de révocation, alias pki), serveur d'impression, NPS (RADIUS, 1812). WDS installé mais non configuré
SRV-ADCS01	Windows Server 2025 en mode Core, 2 Go	Autorité de certification racine d'entreprise **JPConsulting-RootCA**. Doit être allumée pour signer un certificat

5.2 Serveurs Linux et outils d'exploitation

Machine	Système	Rôles
SRV-FREEIPA01	AlmaLinux 10.2 (site B)	FreeIPA 4.13.1 : annuaire, Kerberos, DNS, autorité de certification du domaine Linux. Contrôleur Ansible. Tire les copies des sauvegardes de GLPI
SRV-GLPI01	Ubuntu 24.04 (4 Go, 2 cœurs)	GLPI 10.0.28 : tickets et inventaire, utilisateurs authentifiés par l'AD. PHP 8.4, MariaDB locale
SRV-ZABBIX01	Rocky Linux 9.8	Zabbix 7.4.15, base MariaDB locale, accès HTTPS
SRV-SYSLOG01	Debian 13	Collecteur central de journaux (rsyslog). Les sondes Suricata tournent sur les deux pare-feux, pas ici
SRV-NAGIOS01	CentOS Stream 9	Nagios XI : supervise le PC hôte, en complément de Zabbix. Allumé à la demande, pas en permanence

5.3 Postes clients

Poste	Système	Particularité
WinClt1	Windows 11 26H2	Poste de l'utilisateur fictif : lecteurs et imprimante par GPO, LAPS
WinTech01	Windows 11 26H2	Poste de travail des techniciens, rangé dans l'UO Poste Technicien, adresse fixe .80, compte administrateur local propre
WinClt2 à WinClt4	Windows 11 23H2	Version hors support, laissée telle quelle pour un exercice de mise à niveau
WinClt5	Windows 11 26H2	Poste d'essai, rangé dans l'UO de test, hors WSUS
AnduinClt1, AnduinClt2	AnduinOS	Joints à l'Active Directory
UbuntuClt1, MintClt1, OracleClt1	Ubuntu, Linux Mint, Oracle Linux	Joints au domaine FreeIPA, sur le site B
KaliAudit1	Kali Linux	Poste d'audit externe, hors domaine, face au WAN de PFSENSE02. Éteint par défaut
KaliAudit2	Kali Linux	Poste d'audit interne, hors domaine, sur LAN_40

5.4 Machines présentes mais hors service courant

Machine	État	Règle
SRV-FILES01, SRV-DC02	VM créées, adresses fixes .4 et .5, non jointes au domaine	Futurs serveur de fichiers et second contrôleur : voir chapitre 12
SRV-DC-ANCIEN	Archive, carte réseau déconnectée	Ne jamais la reconnecter au réseau
Anciennes VM Linux du site A (avant migration vers Proxmox)	Conservées par précaution	Ne jamais les démarrer : elles portent les mêmes identités Kerberos que les VM actives

6. Services d'identité

> **En clair**
> L'**identité**, c'est la réponse à « qui es-tu et qu'as-tu le droit de faire ? ». Dans le lab, deux annuaires répondent : un pour Windows, un pour Linux. Le premier fait confiance à lui-même ; le second fait confiance au premier.

6.1 Active Directory

Élément	Valeur
Domaine	jpconsulting.lan (nom court JPCONSULTING)
Niveau fonctionnel	Windows Server 2016 : c'est normal sur Windows Server 2025, aucun niveau plus récent n'est nécessaire ici. Le relever est irréversible
Contrôleurs	Un seul, SRV-DC01, qui porte les cinq rôles FSMO et le catalogue global. Il a remplacé l'ancien contrôleur
Organisation	UO JP Consulting, avec cinq services (Administration, Commercial, Direction, Informatique, Production) et quatre UO techniques : Groupes, Ordinateurs-JPConsulting, Serveurs-JPConsulting, Ordinateurs-TEST-JPConsulting
UO hors de JP Consulting	**Comptes-Services** (comptes techniques des applications), **Comptes-Privilegies** (comptes d'administration nominatifs), **Poste Technicien** (poste des techniciens). Toutes protégées contre la suppression. Elles sont à part pour ne pas hériter des GPO des salariés et pour rester hors de la branche lue par GLPI
Nouvelles machines	Redirigées par redircmp vers Ordinateurs-JPConsulting
Mot de passe	7 caractères minimum, complexité exigée, expiration à 42 jours, historique de 24
Verrouillage	**5 essais**, verrouillage de **15 minutes**, compteur remis à zéro après 15 minutes
Droits	Modèle **AGDLP** : comptes dans des groupes globaux (GG_Informatique, GG_Direction, GG_Commercial, GG_Production, GG_Administration), eux-mêmes dans des groupes de domaine local (DL_Commun_L, DL_Commun_M, DL_Informatique_M) qui portent le droit sur les dossiers

6.2 L'entreprise fictive : services, fonctions, responsables

Les utilisateurs sont fictifs, mais leur organisation est précise : elle décide qui peut demander, qui valide et qui exécute. Un **responsable des données** décide qui accède aux données de son service ; le technicien exécute, il ne décide pas.

Compte	Service	Fonction	Responsable des données de
annie.versaire	Direction	Directrice	Direction
sam.plante	Administration	Responsable administrative	Administration et Commun
alex.terieur	Commercial	Responsable commercial	Commercial
otto.matique	Production	Responsable de production	Production
sarah.fraichit	Informatique	Technicien N1	—
ray.boot	Informatique	Technicien N2, référent	Informatique
admin.domaine	Hors annuaire métier	Administrateur N3	—

6.3 Stratégies de groupe

Stratégie	Rôle
Default Domain Policy, Default Domain Controllers Policy	Stratégies par défaut du domaine et des contrôleurs. La première porte les règles de mot de passe et de verrouillage
WSUS - Serveurs	Indique aux serveurs et aux contrôleurs d'utiliser WSUS en HTTPS (8531). Téléchargement automatique, **installation sur notification** : rien ne s'installe sans un administrateur
WSUS - Postes	Idem pour les postes, avec installation quotidienne à 12 h. Le poste d'essai WinClt5 en est exclu
Utilisateurs - Mappage lecteurs	P: (Commun) pour tous, I: (Informatique) pour les membres de DL_Informatique_M
Ordinateurs - LAPS	Mot de passe administrateur local de 14 caractères, renouvelé tous les 30 jours, stocké chiffré
Utilisateurs - Imprimantes	Connexion à l'imprimante du lab, partagée par SRV-WSUS01
Ordinateurs - Admin postes	Ajoute le groupe GG_AdminPostes aux administrateurs locaux du poste technicien, sans retirer les administrateurs déjà présents

> **Deux points d'attention**
>
> Les lecteurs P: et I: sont montés par le **nom du serveur** (\\SRV-DC01\Partages\...) et non par le nom de domaine de l'espace de noms DFS. Le chemin dépend donc du serveur : le jour où les fichiers déménageront, il faudra modifier la GPO.
>
> La GPO des imprimantes vise un serveur souvent éteint : l'ouverture de session peut en être ralentie (hypothèse non encore testée).

6.4 Partages de fichiers

Les données vivent sur le disque E: du contrôleur (100 Go, volume « Partages »). Deux dossiers existent : **Commun** (lecture pour tous, écriture pour l'Administration et la Direction) et **Informatique** (écriture pour le service Informatique). Ils sont partagés largement et restreints par les droits NTFS, avec énumération basée sur l'accès (**ABE**) : un utilisateur ne voit que ce qui lui est ouvert. L'espace de noms DFS \\jpconsulting.lan\Partages les présente sous un seul nom.

Sujet	Réglage
Quotas et filtres (FSRM)	Informatique limité à 5 Go (quota strict) ; filtre des fichiers audio et vidéo. Commun n'a pas de quota
Copies instantanées	Sur E:, à 12 h et à 17 h ; si la machine est éteinte à l'heure dite, la copie est rattrapée au démarrage. Les utilisateurs et techniciens les lisent par l'onglet *Versions précédentes*
À venir	Quatre partages de service (Direction, Administration, Commercial, Production) : ils n'existent pas encore

6.5 FreeIPA et l'approbation entre les deux domaines

Le domaine Linux jpconsulting-linux.lan est géré par FreeIPA sur SRV-FREEIPA01. Les clients Linux s'y joignent comme les postes Windows se joignent à l'AD. Entre les deux domaines existe une **approbation de forêt** à sens unique : FreeIPA fait confiance à l'AD. Un utilisateur Windows peut donc ouvrir une session sur une machine Linux, avec un identifiant Linux calculé à partir de son identifiant Windows.

Élément	Détail
Sens	Unidirectionnel : le domaine Linux fait confiance au domaine Windows, pas l'inverse
Résolution de noms	Redirecteurs DNS conditionnels dans les deux sens ; exclusion de la validation DNSSEC pour le domaine Windows
Droits administrateur Linux	Le compte admin.linux obtient sudo complet par un rôle LDAP (admin-linux-total)
Ports ouverts pour l'approbation	88, 464, 389, 139, 445 entre les deux réseaux, autorisés dans les deux pare-feux
Point ouvert	Le bouton de validation de l'approbation, côté Windows, échoue ; la validation côté FreeIPA réussit. L'enquête est ouverte

6.6 Comptes d'administration

Compte	Où	Usage
admin.domaine	Domaine Windows, UO Comptes-Privilegies	Administrateur du domaine, pour le travail d'administration. Retiré des groupes *Administrateurs du schéma* et *de l'entreprise*. Le mot de passe n'expire pas (choix assumé, compensé par une phrase de passe longue)
Administrateur	Domaine Windows	Compte intégré. Seul membre des groupes du schéma et de l'entreprise : réservé aux opérations exceptionnelles
admin.local	Domaine Windows	Compte de secours (« bris de glace ») du domaine
adm-sarah.fraichit	Domaine Windows, UO Comptes-Privilegies	Compte restreint de sarah.fraichit (N1) : administrateur local des postes, rien d'autre
adm-ray.boot	Domaine Windows, UO Comptes-Privilegies	Compte restreint de ray.boot (N2) : administrateur local des postes, plus le droit délégué de réinitialiser un compte ordinateur (pour réparer une relation d'approbation). Cette délégation n'a pas encore été exercée en réel
svc.glpi-ldap	Domaine Windows, UO Comptes-Services	Compte de liaison de GLPI avec l'annuaire : lecture seule, aucun droit en plus. Son mot de passe n'expire pas ; il est à changer à la main une fois par an, dans l'AD **et** dans GLPI
adm.secours	Local à WinTech01	Compte administrateur local du poste technicien, porte de secours
admin.linux	FreeIPA	Administrateur Linux, sudo par rôle. Un compte local du même nom existe sur SRV-SYSLOG01, SRV-ZABBIX01 et SRV-GLPI01 : c'est lui qu'utilise Ansible
secours	Machines Linux	Compte local de secours, si l'annuaire est injoignable
Compte DSRM	SRV-DC01	Compte local du mode de restauration de l'annuaire

6.7 Niveaux d'intervention et moindre privilège

Trois niveaux de technicien se partagent le travail. Chacun n'a que les droits dont il a besoin, et chaque niveau a ses comptes.

Niveau	Qui	Ce qu'il fait	Ce qu'il ne fait pas
N1	sarah.fraichit	Déverrouiller un compte, réinitialiser un mot de passe, dépanner un poste, lire Zabbix, ouvrir et escalader un ticket	Aucun accès aux serveurs
N2	ray.boot	Tout le N1, plus créer ou désactiver un compte, gérer les groupes, diagnostiquer les partages, restaurer par *Versions précédentes*	Ne modifie pas le serveur ; ne se connecte pas au contrôleur de domaine (un compte administrateur est utilisé, limite du lab)
N3	admin.domaine	FSRM, sauvegarde et restauration anciennes, DHCP, GPO, agrandir un volume, sur demande de changement	—

Système	Ce qui est en place	Ce qui reste à faire
Active Directory	Comptes restreints, groupes GG_AdminPostes et GG_ReparationPostes, droit de réparation du compte ordinateur	Délégations par niveau de support, lecture déléguée des mots de passe LAPS
GLPI	Groupes Support N1 et Exploitation N2, profil Technician avec le droit d'assigner, droit de valider pour les responsables	—
Zabbix	Comptes de lecture seule pour le N1 et le N2, groupe Support - Lecture seule	—

À retenir

Qui décide n'est pas qui exécute. Une demande de droit sur des données est validée dans le ticket par le responsable des données ; le technicien N2 exécute, et seulement après cette validation. Le N3 ne fait que clore.

7. Matrice de flux

Un **flux** est une communication autorisée : qui parle à qui, sur quel port, pour quoi faire. Tout ce qui n'est pas listé est refusé par les pare-feux ou par les pare-feux locaux des machines.

7.1 Flux à l'intérieur du site A

De	Vers	Protocole, port	Raison
Clients Windows	SRV-DC01	DNS 53, Kerberos 88, LDAP 389, SMB 445	Résolution, ouverture de session, partages
Clients Windows	SRV-DC01	DHCP (UDP 67/68)	Obtenir une adresse
SRV-GLPI01	SRV-DC01	LDAPS 636	Authentification des utilisateurs de GLPI par l'AD (même réseau, sans passer par le pare-feu)
Clients et serveurs	SRV-WSUS01	HTTPS 8531	Mises à jour
Clients et serveurs	SRV-WSUS01	HTTP 80 (IIS)	Récupérer la liste de révocation des certificats
Équipements d'accès	SRV-WSUS01	RADIUS 1812	Authentification réseau (NPS)
SRV-DC01 et clients	SRV-GLPI01	HTTPS 443	Inventaire par l'agent GLPI, tickets
PC hôte et WinTech01	SRV-ZABBIX01	HTTPS 443	Interface web de Zabbix (les deux adresses seulement)
SRV-ZABBIX01	SRV-DC01, HOTE-VMWARE, SRV-SYSLOG01	Agent Zabbix 10050	Supervision en mode passif
Agents actifs	SRV-ZABBIX01	10051	Supervision en mode actif
SRV-ZABBIX01	PFSENSE01, PFSENSE02	SNMP 161	Supervision des pare-feux
Serveurs Windows	SRV-SYSLOG01	TLS 6514	Journaux Windows (NXLog)
PFSENSE01 et PFSENSE02	SRV-SYSLOG01	UDP 514	Journaux des pare-feux et alertes Suricata
Machines Linux	SRV-SYSLOG01	RELP sur TLS 20514	Journaux Linux
PC hôte	Serveurs Windows et Linux	SSH 22	Administration (le PC hôte seul est autorisé)

7.2 Flux entre les deux sites, dans le tunnel IPsec

De	Vers	Protocole, port	Raison
Site B (Linux)	SRV-SYSLOG01	RELP sur TLS 20514	Journaux des machines Linux du site B
SRV-FREEIPA01	SRV-DC01	88, 464, 389, 139, 445	Approbation de forêt
SRV-DC01	SRV-FREEIPA01	88, 464, 389, 139, 445	Approbation de forêt, sens inverse
Clients Linux	SRV-DC01	DNS 53	Résolution des noms Windows
Site A	Site B	SSH 22, HTTPS 443, DNS 53, ICMP	Administration et supervision
SRV-FREEIPA01	Réseau .20	SSH 22	Ansible vers les serveurs du site A
SRV-FREEIPA01	SRV-GLPI01	SSH 22 (rsync en lecture seule)	Copie des sauvegardes de GLPI, toutes les deux heures, par un compte limité à cet usage
Agents du site B	SRV-ZABBIX01	10051	Supervision active
PFSENSE02	PFSENSE01	UDP 514, SNMP 161	Journaux et supervision du second pare-feu
PFSENSE01	Site B	Chaque flux ci-dessus	Chaque flux est **autorisé deux fois** : à l'entrée et à la sortie du tunnel

7.3 Ce qui est interdit

Interdit	Pourquoi
LAN_40 vers le pare-feu lui-même et vers tout réseau privé	Le réseau est isolé : Internet seulement, pour limiter ce qu'un poste « compromis » peut atteindre
Site B vers le réseau de la box ou vers HOTE-VMWARE	Le site Linux n'a pas à atteindre le poste qui héberge le lab
VPN vers le lab	Le VPN ne donne accès qu'à un seul poste d'administration, depuis une adresse source précise
Entrée depuis Internet sauf VPN	Seul l'accès VPN est ouvert sur le WAN de PFSENSE01

> **Source de vérité**
> Cette matrice est rédigée d'après les règles relevées sur les pare-feux. En cas de doute sur un flux, la règle affichée dans pfSense fait foi, pas ce tableau.

8. Sécurité

8.1 Les couches de protection

Couche	Ce qui est en place
Réseau	Deux pare-feux avec règles par réseau et alias de ports ; réseau isolé LAN_40 ; filtrage entre sites
Accès distant	OpenVPN : un certificat par appareil, une seule route poussée, deux connexions maximum
Chiffrement des liaisons	IPsec entre sites ; TLS mutuel pour les journaux Linux et Windows ; HTTPS sur GLPI, Zabbix, les deux pare-feux, Proxmox et WSUS ; LDAPS entre GLPI et l'annuaire
Identité et droits	Modèle AGDLP ; verrouillage des comptes après 5 essais ; comptes d'administration distincts des comptes courants et restreints par niveau ; LAPS ; sudo par rôle LDAP ; liaison GLPI par un compte en lecture seule
Postes et serveurs	Pare-feux locaux, accès SSH durci, fail2ban, fichiers de configuration pilotés par Ansible
Détection	Suricata sur le réseau Windows (PFSENSE01) et le réseau Linux (PFSENSE02) : jeu de règles ET Open, alertes seules. LAN_40 n'est pas couvert
Sauvegarde	Sauvegarde quotidienne du contrôleur de domaine, copies instantanées des partages, sauvegarde de GLPI en trois couches, exports chiffrés des pare-feux, sauvegardes des VM du site B

8.2 Autorité de certification interne

L'autorité **JPConsulting-RootCA** (AD CS, sur SRV-ADCS01) est une racine d'entreprise à un seul niveau, clé RSA 4096, SHA-256, validité 10 ans. Elle signe les certificats HTTPS de six services : GLPI, Zabbix, les deux pare-feux, Proxmox et WSUS (modèle serveur web, 2 ans). Chaque clé est créée sur la machine qui demande le certificat ; la signature se fait à la main avec certreq. Le contrôleur de domaine reçoit lui, automatiquement, un certificat de modèle *Contrôleur de domaine* (un an) : c'est lui qui permet la liaison LDAPS de GLPI. Les machines Linux qui doivent lui faire confiance installent le certificat de l'autorité. Les listes de révocation sont publiées en HTTP par IIS sur SRV-WSUS01, sous l'alias pki. La révocation a été testée.

> **Échéance à surveiller**
> Le certificat du contrôleur de domaine expire le **04/10/2027**. Son renouvellement automatique n'a pas encore été constaté et son échéance n'est pas supervisée. S'il expirait, plus aucun utilisateur ne pourrait se connecter à GLPI avec son compte de domaine ; seuls les comptes locaux de GLPI continueraient de fonctionner.

8.3 Durcissement automatisé

Les réglages de sécurité des serveurs Linux de l'administration (SSH, fail2ban, pare-feu local, MariaDB) sont décrits dans des fichiers Ansible, qui sont la **source unique**. Rejouer le playbook sur une machine conforme ne change rien (changed=0) : c'est la preuve que la conformité est tenue. Règle : on ne pose pas une règle à la main sans la reporter dans Ansible. Une dérive de ce type a déjà été constatée et réparée. La détection d'intrusion se teste avec un User-Agent BlackSun, qui déclenche la règle 2008983.

8.4 Correctifs et vulnérabilités

Les mises à jour des postes et des serveurs Windows passent par WSUS. Les serveurs Linux se mettent à jour par leur gestionnaire de paquets. Quand une faille critique est annoncée, chaque VM concernée est traitée **une à**

une, avec un instantané avant l'action, une vérification de version après, puis la suppression de l'instantané. Exemple : une faille critique du cœur de PHP a été corrigée dans les deux jours sur GLPI, Zabbix et Nagios XI, et vérifiée non concernée sur le serveur FreeIPA.

Pistes d'évolution de la sécurité

Un seul contrôleur de domaine et une seule autorité de certification en ligne : pas de redondance.

UDP 514 (pare-feux) et SNMP v2c ne sont pas chiffrés.

Les clients WinClt2 à WinClt4 sont en 23H2, hors support.

Plusieurs réglages sont faits à la main, hors Ansible : règle de pare-feu et SSH des serveurs Windows, durcissement SSH de Proxmox, réglages de confiance de Zabbix, en-têtes de GLPI, configuration d'envoi des journaux, scripts et minuteurs de sauvegarde de GLPI.

L'autorité n'a pas de service **OCSP** : seule la liste de révocation est consultable.

Le contrôleur de domaine refuse les liaisons LDAP en clair (c'est voulu) : toute application qui lit l'annuaire doit passer par LDAPS.

L'audit des échecs d'ouverture de session n'est pas confirmé au niveau du contrôleur : un échec est journalisé sur le poste (4625) et, selon toute vraisemblance, sous d'autres numéros (4771, 4776) sur le contrôleur.

9. Supervision et journaux

9.1 Supervision (Zabbix)

> **En clair**
> Zabbix **regarde** régulièrement chaque machine importante et prévient quand quelque chose sort de l'ordinaire.

Élément supervisé	Méthode
HOTE-VMWARE	Agent Zabbix ; aussi supervisé par Nagios XI quand celui-ci est allumé
SRV-DC01	Agent classique, mode passif ; espace libre du volume Partages (alerte au-delà de 90 % d'occupation)
SRV-FREEIPA01	Agent, mode actif
SRV-SYSLOG01	Agent, mode passif
Hôte Proxmox	API, compte en lecture seule (rôle PVEAuditor)
PFSENSE01, PFSENSE02	SNMP v2c ; PFSENSE02 via le tunnel
Certificat GLPI	Agent 2, contrôle de la validité (alerte 30 jours avant l'échéance)

L'interface de Zabbix est ouverte en lecture seule aux techniciens N1 et N2, depuis le PC hôte et depuis leur poste. Zabbix affiche en permanence quelques problèmes qui ne sont pas des pannes : machines éteintes par conception, services Windows bénins, déclencheurs DHCP de pfSense. Ce « bruit connu » est à nettoyer ; un technicien doit savoir le reconnaître.

9.2 Journaux centralisés

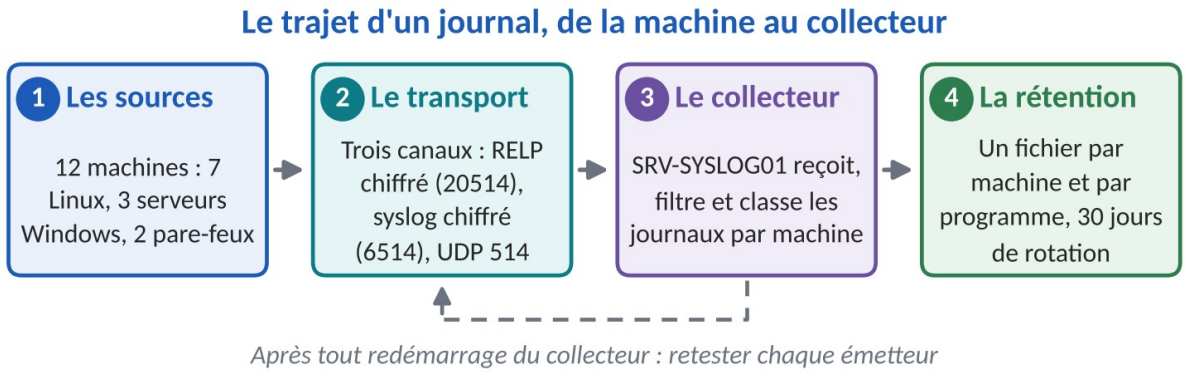


Figure 2 — chemin d'un journal depuis les machines jusqu'au collecteur

Source	Canal	Port
7 machines Linux (FreeIPA, Oracle, Mint, Ubuntu, Kali interne, GLPI, Zabbix)	RELP sur TLS, authentification mutuelle	20514
3 serveurs Windows	Syslog TLS, via NXLog CE ; événements Sysmon (configuration SwiftOnSecurity)	6514
2 pare-feux, dont alertes Suricata	Syslog UDP, format RFC 5424	514

Le collecteur SRV-SYSLOG01 range les journaux sous /var/log/distant/<machine>/<programme>.log. Une rotation quotidienne conserve 30 jours. Côté Linux, l'envoi est filtré : messages d'authentification, ou gravité

inférieure ou égale à 4. Une file de 200 Mo conserve les messages si le collecteur est injoignable. Les certificats de la chaîne de journalisation viennent d'une autorité de certification dédiée aux journaux (OpenSSL), hébergée sur le collecteur.

9.3 Détection d'intrusion (Suricata)

Suricata fonctionne en **IDS** (détection seule, pas de blocage) sur PFSENSE01, pour le réseau Windows, et sur PFSENSE02, avec le jeu de règles ET Open. Le réseau isolé LAN_40 n'est pas couvert. L'option de blocage des sources hostiles est désactivée. La règle 2210044 est désactivée par une liste de gestion des identifiants de règle (disablesid-jp.conf) sur PFSENSE01. Le passage en **IPS** (blocage) est une évolution prévue.

Pistes d'évolution

Le collecteur n'est **pas un SIEM** : il stocke et classe, il ne corrèle pas et n'alerte pas.

Le périmètre supervisé est limité : l'hôte, les deux pare-feux, FreeIPA, le collecteur et le contrôleur de domaine. Les clients, SRV-WSUS01, SRV-ADCS01 et SRV-GLPI01 ne sont pas supervisés par un agent.

À compléter dans Zabbix : SNMP v2c non chiffré, pas de sonde du tunnel IPsec, un certificat sur sept surveillé, pas d'alerte par courriel (pas de messagerie), quatre éléments non pris en charge, aucune supervision de la fraîcheur des sauvegardes de GLPI.

Nagios XI supervise le PC hôte, mais il n'est allumé qu'à la demande : il ne donne pas de supervision continue. Deux alertes internes de l'outil restent non traitées.

Après tout redémarrage du collecteur, chaque émetteur doit être retesté : des connexions à moitié ouvertes peuvent subsister.

10. Sauvegarde

Ce qui est sauvegardé	Comment	Fréquence, état
Contrôleur de domaine SRV-DC01 (système complet et disque E:)	Sauvegarde Windows Server, disque dédié de 150 Go	Tous les jours à 13 h, si la machine est allumée ; plus de quinze versions conservées ; réussie chaque jour
Partages de SRV-DC01	Copies instantanées de E:	À 12 h et à 17 h, avec rattrapage au démarrage
GLPI	Script local (base et fichiers) + copie tirée par SRV-FREEIPA01 sur une autre machine physique	Locale chaque jour à 13 h 30, les 14 dernières conservées ; copie toutes les deux heures. Restauration testée
Six VM du site B	Sauvegarde Proxmox (vzdump) sur un disque externe	Une copie, environ 42,4 Go, 19 minutes
Configuration des pare-feux	Exports XML chiffrés, copies sur deux supports hors Proxmox	Export de PFSENSE01 refait après sa dernière modification
Machines du site A	Instantanés VMware, pris machine éteinte	Aucun conservé : un instantané est pris juste avant un exercice, supprimé juste après
PC hôte	AOMEI Backupper	Espace de destination limité : non compté parmi les sauvegardes fiables

10.1 Restaurations réellement testées

Test	Statut	Résultat
Restauration d'un fichier	Réalisé	Réussie
Corbeille Active Directory : suppression puis restauration d'un compte	Réalisé	Réussie
Restauration faisant autorité d'une UO, en mode DSRM	Réalisé	Réussie, environ 1 h 45 au total dont 27 minutes de restauration
Restauration d'une VM du site B (FreeIPA)	Réalisé	Réussie, 111 secondes
Restauration de la base de GLPI dans une base de test	Réalisé	Réussie : les 9 tickets présents au moment de la sauvegarde sont revenus
Récupération d'un dossier supprimé par copie instantanée, sans écraser le travail existant	Réalisé	Réussie, droits vérifiés après remise en place

Pistes d'évolution de la sauvegarde

La règle **3-2-1** (3 copies, 2 supports, 1 hors site) n'est **pas respectée** : les sauvegardes du site A sont sur le même PC que les machines. Seule la sauvegarde de GLPI a une copie sur une autre machine physique.

La récupération complète du contrôleur sur une machine vide (*bare metal*) reste à tester.

Aucun objectif de reprise (RTO, RPO) n'a été défini ni mesuré : voir le PRA.

Un instantané de VM n'est pas une sauvegarde.

Une sauvegarde planifiée n'a lieu que si la machine est allumée à l'heure dite.

11. Choix d'architecture et justification

Chaque choix a une raison et un prix. Le tableau les met face à face ; la dernière colonne dit ce que le choix coûte ou ce qu'une entreprise ferait différemment.

Choix	Raison	Contrepartie
Deux sites, deux hyperviseurs	Pratiquer le type 2 et le type 1 ; avoir deux réseaux à relier	Deux PC à faire tourner ; le PC du site A est un point unique de défaillance
Deux domaines reliés par une approbation	Reproduire un parc mixte Windows et Linux	Plus de DNS et de pare-feu à régler ; sens unique seulement
pfSense sur chaque site	Un pare-feu complet, gratuit, avec IPsec, OpenVPN et Suricata	Administration à la main ; pas de haute disponibilité
Passerelle en .254, serveurs en .1	Convention lisible, éviter la confusion avec un réseau domestique	À expliquer à qui découvre le lab
DHCP limité à .100–.200	Garder les plages basses pour des adresses fixes	Impossible de dépasser 101 clients sans changer l'étendue
WSUS avec ciblage côté client	Les GPO rangent chaque machine dans son groupe : rien à faire sur le serveur	WSUS est un produit en fin de vie
Autorité racine à un seul niveau, sur Server Core	Simple à monter ; surface d'attaque réduite par Server Core	Pas de racine hors ligne ; la machine doit être allumée pour signer
Collecteur rsyslog plutôt qu'un SIEM	Centraliser sans coût ni lourdeur ; comprendre le chemin d'un journal	Aucune corrélation, aucune alerte
Suricata en détection seule	Observer les alertes avant de bloquer, pour ne pas couper le lab par erreur	Aucune protection active
VPN limité à un poste	Réduire ce qu'un appareil perdu pourrait atteindre	Pas d'accès direct aux serveurs : il faut passer par l'hôte
Ansible, source unique du durcissement	Rejouable et vérifiable	Encore incomplet : plusieurs réglages à la main
Zabbix comme supervision de référence, Nagios XI en complément	Zabbix est à jour et sait superviser tout ce qui est utile ici ; Nagios XI, vu en formation, garde un rôle pour le PC hôte	Deux outils à maintenir ; Nagios XI n'est allumé qu'à la demande
Un compte courant et un compte d'administration par technicien	Limiter les dégâts si un mot de passe est volé ; tracer qui a fait quoi	Deux comptes à gérer par personne
LDAPS plutôt qu'une liaison LDAP en clair	Le contrôleur refuse les liaisons non protégées ; le mot de passe de liaison ne circule pas en clair	Un certificat de plus à renouveler, dont l'échéance n'est pas supervisée
Rôle fichiers sur le contrôleur de domaine	Un serveur de moins à faire tourner sur un PC de 32 Go	Pratique à éviter en entreprise ; un technicien N2 ne peut pas se connecter au contrôleur

12. Points d'amélioration et évolutions

12.1 Points d'amélioration

Pistes d'évolution	Conséquence
Un seul contrôleur de domaine	Si SRV-DC01 s'arrête, plus d'authentification, y compris vers GLPI ; il ne se rattrape que par restauration
Un seul point matériel par site	Le PC hôte du site A, ou le disque unique de Proxmox, en panne : arrêt du site
Disque SATA du PC hôte sans mémoire cache	A provoqué des écrans bleus ; les VM serveurs sont désormais sur le disque NVMe, avec 20 à 25 % d'espace libre à garder sur le SATA
Mémoire du PC hôte	Environ six VM en même temps : on n'allume que ce que l'exercice demande
Sauvegardes sur la même machine	La règle 3-2-1 n'est pas tenue
Pas de SIEM	Les journaux sont conservés mais non analysés
Pare-feu, switch, serveurs : peu de redondance	Aucun scénario de haute disponibilité n'est testé
Rôle fichiers sur le contrôleur de domaine	Un technicien N2 doit utiliser un compte administrateur pour consulter les partages côté serveur ; les lecteurs dépendent du nom du serveur
Pas de messagerie	GLPI est le seul canal de communication ; les alertes ne partent pas par courriel
Composants non configurés	WDS, intranet IIS, imprimante (fictive)

12.2 Évolutions envisagées

Évolution	Intérêt
Mettre en service SRV-FILES01 (serveur de fichiers séparé)	Sortir les données du contrôleur ; régler les lecteurs qui dépendent du nom du serveur ; permettre au N2 de travailler sans compte administrateur du domaine
Mettre en service SRV-DC02, avec basculement DHCP	Supprimer le point unique de défaillance de l'annuaire, du DNS, du DHCP et de la connexion à GLPI
Créer les quatre partages de service et leurs quotas	Donner à chaque service un espace conforme à l'organisation décrite au chapitre 6
Poser les délégations de support N1 et N2 et la lecture déléguée de LAPS	Terminer le moindre privilège : aujourd'hui les droits du N2 passent surtout par ses comptes restreints
Sauvegarde hors du PC hôte	Se rapprocher de la règle 3-2-1
Tester la récupération complète du contrôleur	Mesurer un vrai délai de reprise
Passer Suricata en IPS	Bloquer et pas seulement détecter
Étendre Ansible aux réglages restants et aux sauvegardes de GLPI	Tout rejouer, tout vérifier
Superviser les clients, les sondes IPsec, l'échéance du certificat du contrôleur, la fraîcheur des sauvegardes	Combler les trous de la supervision
Déplacer une VM peu couplée vers le site B	Soulager le PC hôte ; à mesurer d'abord, car une VM déplacée change de réseau, d'adresses et de règles
Pistes d'architecture à étudier : VLAN, proxy inverse devant GLPI et Zabbix, zone démilitarisée	Rapprocher le lab d'une architecture d'entreprise ; sans échéance
Configurer WDS	Déploiement de postes par le réseau

13. Lexique

Terme	En clair
AD DS	*Active Directory Domain Services* : l'annuaire des comptes et des ordinateurs d'un domaine Windows.
AGDLP	Méthode de rangement des droits : comptes → groupes globaux → groupes de domaine local → permissions.
ABE	*Access-Based Enumeration* : on ne voit que les dossiers auxquels on a droit.
Approbation de forêt	Lien de confiance entre deux domaines : l'un accepte les comptes de l'autre.
Copie instantanée	Photo d'un volume à un instant donné : permet de retrouver une ancienne version d'un fichier (onglet *Versions précédentes*).
DAT	Dossier d'architecture technique : ce document.
DHCP	Service qui attribue automatiquement une adresse IP aux machines.
DNS	Service qui traduit un nom de machine en adresse IP.
DSRM	Mode de démarrage d'un contrôleur de domaine sans annuaire, pour le restaurer.
FSMO	Les cinq rôles qu'un seul contrôleur du domaine doit tenir à la fois.
FSRM	Outil de gestion des quotas et des filtres de fichiers sur un serveur.
GPO	Stratégie de groupe : réglages poussés automatiquement aux machines et aux utilisateurs.
Hyperviseur	Logiciel qui fait tourner des machines virtuelles ; type 1 posé sur le matériel, type 2 posé sur un système.
IDS / IPS	Système de détection (IDS) ou de détection et blocage (IPS) d'intrusions.
IPsec	Protocole qui chiffre le trafic entre deux réseaux ; IKEv2 en gère les clés.

Terme	En clair
LAPS	Mot de passe administrateur local différent et renouvelé sur chaque machine.
LDAPS	Interrogation d'un annuaire par le protocole LDAP, dans un canal chiffré (port 636).
Moindre privilège	Donner à chacun seulement les droits dont il a besoin pour sa tâche.
NPS	Serveur RADIUS de Windows : authentifie les accès réseau.
OCSP	Service qui répond en direct à « ce certificat est-il révoqué ? ».
PKI	Infrastructure à clés publiques : l'ensemble qui crée et gère les certificats.
Playbook	Document regroupant, pour une catégorie du service de tickets, les fiches de traitement des incidents et des demandes.
PRA	Plan de reprise d'activité : que faire après un sinistre.
RELP	Protocole d'envoi de journaux plus fiable que le syslog classique.
RTO, RPO	Délai de reprise accepté ; quantité de données qu'on accepte de perdre.
SIEM	Outil qui rassemble les journaux, les corrèle et lève des alertes.
SNMP	Protocole de supervision des équipements réseau.
Server Core	Windows Server sans interface graphique, avec moins de surface d'attaque.
WSUS	Serveur qui distribue les mises à jour Windows dans l'entreprise.