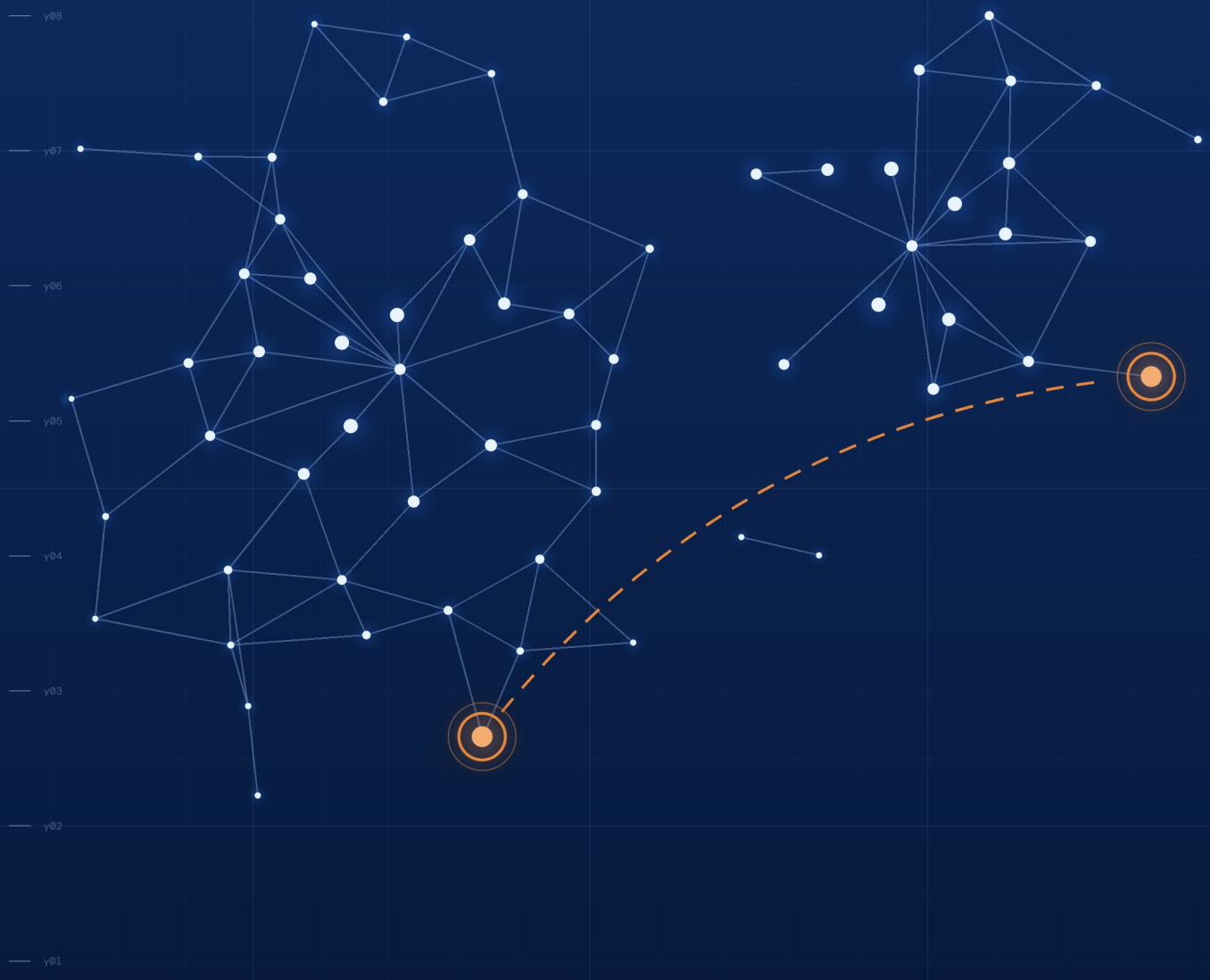


DOCUMENTATION DU LAB · JP CONSULTING

Plan de reprise d'activité

Remettre le lab en route après un sinistre

Jean-Philippe Rebischung

Plan de reprise d'activité

Que faire après une panne ou un sinistre dans le lab JP Consulting, et ce qui a vraiment été testé

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

OBJET DU DOCUMENT

Ce plan décrit comment remettre le lab en état après une perte : un fichier, un compte, une machine virtuelle, GLPI, un pare-feu, le contrôleur de domaine. Il donne les délais **mesurés** lors des tests réels, les délais **visés** pour le reste, l'ordre de redémarrage et la procédure de chaque scénario. Il dit aussi, sans détour, ce qu'il ne couvre pas. Il décrit le lab **tel qu'il est au 01/11/2026** et s'appuie sur le DAT-01 pour l'architecture et sur le DEX-01 pour les tâches courantes.

SOMMAIRE

1. L'essentiel
2. Périmètre et sauvegardes existantes
3. Objectifs de reprise : RTO et RPO
4. Scénarios retenus
5. Ordre de redémarrage
6. Procédures de reprise
7. Résultats des tests réels
8. Ce qui reste à couvrir
9. Exercices pour compléter le plan
10. Lexique

1. L'essentiel

En clair

Un plan de reprise répond à une question : « Si ça casse, comment je remets en route, dans quel ordre, en combien de temps, et avec quelles données ? ». Il se prépare **avant** la panne, et il ne vaut que s'il a été essayé.

Avec les mots du métier

Un **PRA** (plan de reprise d'activité) organise le redémarrage après un sinistre. Deux mesures le cadrent : le **RTO** (*Recovery Time Objective*), durée d'interruption acceptable, et le **RPO** (*Recovery Point Objective*), quantité de données qu'on accepte de perdre, mesurée en temps depuis la dernière copie.

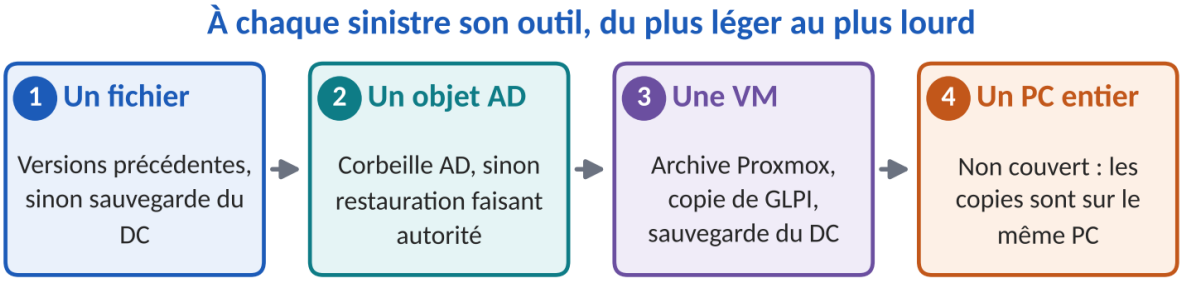


Figure 1 — les quatre niveaux de perte et l'outil de reprise qui correspond à chacun

Question	Réponse courte
Qu'est-ce qui est vraiment protégé ?	Le contrôleur de domaine (copie quotidienne), les partages (versions précédentes deux fois par jour), GLPI (copie quotidienne, doublée sur une seconde machine), les VM du site B (une archive sur disque externe), la configuration des pare-feux (exports chiffrés).
Qu'est-ce qui a été restauré pour de vrai ?	Un fichier, un dossier par les versions précédentes, un compte par la Corbeille AD, une UO par restauration faisant autorité, une VM FreeIPA, la base de GLPI.
Qu'est-ce qui reste à tester ?	La reconstruction complète du contrôleur sur une machine vide, la restauration d'un pare-feu, la perte d'un PC hôte.
Quel est le plus gros risque ?	Les copies du site A (sauf GLPI) sont sur le même PC que les machines : la perte du PC emporte tout.

Le cadre du lab

Ce plan décrit un **lab** : deux PC de bureau, des VM, aucun utilisateur réel. **Aucune VM ne tourne la nuit** : un sinistre se découvre à l'allumage ou pendant une séance. Les délais sont ceux d'un technicien qui suit sa propre procédure, pas ceux d'une équipe d'astreinte.

Les valeurs « visées » de ce document sont des **hypothèses de travail**, à discuter. Seules les valeurs « mesurées » ont été constatées.

2. Périmètre et sauvegardes existantes

Le périmètre couvre les deux sites décrits dans le DAT-01. Le tableau dit, pour chaque élément, **ce qui existe comme copie**, où elle se trouve et ce qui la rend fragile.

Élément	Copie existante	Où	Fragilité
SRV-DC01 (annuaire, DNS, DHCP, fichiers)	Sauvegarde Windows Server : système complet et volume E:, tous les jours à 13 h ; plus de quinze versions conservées, réussie chaque jour	Disque virtuel dédié de 150 Go, sur le PC hôte	Même PC que la machine sauvegardée ; pas de copie si la VM est éteinte à 13 h
Partages (E:)	Copies instantanées à 12 h et 17 h (versions précédentes), avec rattrapage	Volume E: de SRV-DC01	Même disque que les données : protège d'une erreur, pas d'une panne
GLPI	Script local (base et fichiers) à 13 h 30, 14 copies ; copie tirée toutes les 2 h par SRV-FREEIPA01, 60 jours	SRV-GLPI01 et **seconde machine physique** (site B)	Fraîcheur non supervisée ; clé glpicrypt.key à garder avec la base
VM du site B (FreeIPA, clients, PFSENSE02, poste d'audit)	Archives Proxmox (vzdump, mode instantané, zstd), 42,4 Go	Disque SSD externe, **une seule copie**	Une archive, à renouveler ; pas de planification ; seule la VM FreeIPA a été restaurée
PFSENSE01, PFSENSE02	Export XML **chiffré** de la configuration ; les deux exports sont à jour	Disque externe et disque D: du PC hôte	Jamais réimporté ; à refaire après toute modification
GPO du domaine	Sauvegarde et rapport HTML ; **sauvegarde planifiée à programmer**	C:\Outils du contrôleur et PC hôte	Le jeu de GPO a changé depuis le dernier export : à refaire, puis à planifier
Autres VM du site A (WSUS, AD CS, Zabbix, collecteur, clients, poste technicien)	Aucune sauvegarde planifiée ; un instantané éphémère avant un exercice, supprimé après	Sur le PC hôte	Un instantané n'est pas une sauvegarde ; il n'en existe aucun aujourd'hui
Configuration du PC hôte	AOMEI Backupper, espace de destination limité	Disque E: de l'hôte	Non comptée parmi les sauvegardes fiables

> **À retenir**
>
> **Un instantané de VM n'est pas une sauvegarde** : il vit sur le même disque que la VM. Et restaurer un vieil instantané d'un contrôleur de domaine casse l'annuaire (numéros de version de réplication en retard). Le lab a connu un contrôleur chargé de cinq instantanés de quatre mois, tous supprimés depuis.

3. Objectifs de reprise : RTO et RPO

Le **RPO** découle de la fréquence des copies : si la copie date de 13 h et que la panne survient à 12 h le lendemain, on perd 23 heures de modifications. Le **RTO** se mesure en chronométrant une restauration réelle. Dans le lab, les VM sont éteintes la nuit : le RPO ne compte donc que si la machine était **allumée à l'heure de la copie**.

Composant	RPO réel (fréquence)	RTO visé	RTO mesuré
Un fichier de partage	Au plus 19 h (copies à 12 h et 17 h) ; 24 h par la sauvegarde	30 min	Réussi (dossier et fichier) ; non chronométré
SRV-DC01, un objet de l'annuaire	Immédiat par la Corbeille ; 24 h par la sauvegarde	2 h	**1 h 45** au total pour une UO (restauration faisant autorité, dont 27 min de restauration)
GLPI, base et fichiers	24 h (copie de 13 h 30), seconde copie au plus 2 h plus tard	1 h	Base restaurée dans une base de test ; non chronométré
SRV-DC01, perte complète de la VM	24 h	4 h	**Non mesuré : à tester**
Une VM du site B	Date de la dernière archive (**aucune planification**)	1 h	**111 secondes pour FreeIPA, hors** vérifications
Un pare-feu	Date du dernier export	1 h	**Non mesuré**
Un PC hôte	—	Non défini	**À couvrir**

Comment lire le tableau

Les colonnes « RTO visé » sont des choix de ce document, à valider ; aucun besoin métier ne les impose.

Le RPO de 24 h du contrôleur est cohérent pour un lab ; il serait trop long pour une entreprise qui modifie son annuaire toute la journée.

Le RPO des VM du site B est celui d'une **archive unique, non planifiée** : tout ce qui a changé depuis son établissement serait perdu.

4. Scénarios retenus

N°	Sinistre	Reprise	Essayé ?
S1	Un fichier ou un dossier de partage est supprimé ou écrasé	Versions précédentes ; sinon sauvegarde du contrôleur	**Oui (sauvegarde et versions précédentes)**
S2	Un compte, un groupe ou un ordinateur est supprimé	Corbeille Active Directory	**Oui**
S3	Une UO entière est supprimée, Corbeille non utilisable	Restauration faisant autorité, mode DSRM	**Oui (une fois)**
S4	Une VM du site B est perdue ou abîmée	Restauration de l'archive Proxmox	**Oui, pour FreeIPA seulement**
S5	Un pare-feu perd sa configuration	Réimport de l'export XML chiffré	**Non**
S6	La VM SRV-DC01 est perdue	Restauration de l'état du système sur une VM neuve	**Non**
S7	Le PC d'un site tombe en panne ou est perdu	Reconstruction du site	**À couvrir**
S8	GLPI est perdu ou sa base est corrompue	Restauration de la copie la plus récente	**Oui, pour la base (base de test)**
S9	Un disque du PC hôte du site A lâche (cf. incident NVMe)	Selon le disque : déplacer ou restaurer les VM touchées	**Non** ; le motif d'arrêt a été diagnostiqué, la reprise reste à jouer

Comment le lire

Lire ce tableau comme une carte de confiance : S1 à S4 et S8 ont été prouvés par un test (S8 : la base seulement), S5 et S6 sont des procédures écrites, à tester, S7 et S9 n'ont pas de réponse complète aujourd'hui.

5. Ordre de redémarrage

Après une coupure générale, ou une reconstruction, on remet les machines en route **dans l'ordre des dépendances** : un service qui a besoin d'un autre tombe avec lui. Démarrer tout en même temps donne des erreurs trompeuses (le DHCP qui démarre avant l'annuaire, par exemple : c'est pourquoi son démarrage est différé).

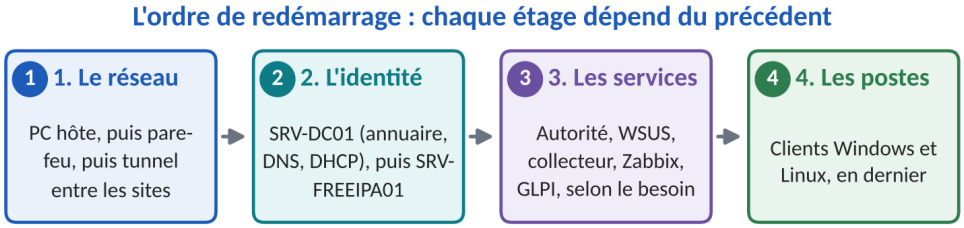


Figure 2 — les quatre étages de redémarrage ; on ne passe à l'étage suivant que quand le précédent est vérifié

Ordre	Machine	Pourquoi à cette place	Comment vérifier
1	PC hôte du site A, puis **PFSENSE01**	Rien ne communique sans le pare-feu	Interface web joignable ; WAN actif
2	PC hôte du site B (Proxmox), qui relance seul **PFSENSE02** et **SRV-FREEIPA01**	Même raison côté site B	Console Proxmox ; interface de PFSENSE02
3	**Tunnel IPsec**	L'approbation et les journaux du site B en dépendent	État *Established* dans pfSense ; ping de B vers A
4	**SRV-DC01**	Annuaire, DNS et DHCP : tout le reste en dépend	dcdiag /q ; seule l'erreur du journal système au démarrage est tolérée
5	**SRV-FREEIPA01**	Annuaire Linux, DNS du domaine Linux	ipactl status : tous les services *RUNNING*
6	**SRV-ADCS01**	L'autorité doit être **allumée pour signer**	Console de l'autorité ; sinon erreur 0x800706ba
7	**SRV-WSUS01**	Publie aussi les listes de révocation (IIS)	Page de la liste de révocation en HTTP
8	**SRV-SYSLOG01**	Les émetteurs s'y connectent ; le démarrer avant eux évite des pertes	ss -tulnp : ports 20514, 6514, 514 en écoute
9	**SRV-ZABBIX01**, **SRV-GLPI01**	Supervision et tickets ; GLPI a besoin du contrôleur pour l'authentification	Interface web en HTTPS ; connexion avec un compte du domaine
10	Postes clients, poste technicien	Dépendent de l'annuaire et du DHCP	Ouverture de session ; adresse reçue

Pièges vécus. Au redémarrage de PFSENSE02, la configuration IPsec n'était pas chargée seule : le tunnel est resté tombé (incident vécu). Une garde planifiée recharge désormais la configuration ; après tout redémarrage de PFSENSE02, **vérifier que le tunnel est monté** avant de chercher ailleurs. Après tout redémarrage du collecteur, **retester chaque émetteur** (logger -p auth.warning test) : des connexions à moitié ouvertes peuvent subsister. Arrêter les VM **avant** de fermer VMware Workstation : le fermer en laissant le contrôleur « en arrière-plan » l'a déjà rendu non pilotable.

6. Procédures de reprise

Chaque scénario suit le même fil : où on tape, avec quel compte, ce qu'on doit voir, quoi faire sinon. Les noms de machines sont ceux du DAT-01. Le compte d'administration du domaine est admin.domaine. **Avant toute restauration lourde**, prendre un instantané VM éteinte ; le supprimer une fois la reprise vérifiée.

6.1 S1 — Récupérer un fichier ou un dossier supprimé

Objectif	Remettre un fichier ou un dossier de partage perdu, sans écraser le travail existant.
Machine	Poste de l'utilisateur ou SRV-DC01
Compte	Compte autorisé sur le partage (ou admin.domaine)
Outil	Explorateur de fichiers, onglet *Versions précédentes*

Voie 1 — versions précédentes (la plus rapide, copies de 12 h et 17 h).

1. Clic droit sur le dossier **parent** de l'élément perdu, puis *Propriétés*, onglet *Versions précédentes*.
2. Choisir la version datée d'**avant la perte**, puis *Ouvrir* pour vérifier le contenu.
   → Le dossier ou le fichier perdu s'y trouve.
3. Utiliser *Copier…* vers un emplacement de travail (et non *Restaurer*, qui écraserait l'existant), puis remettre l'élément en place.
4. Vérifier les droits de l'élément remis en place, puis **ouvrir le fichier**.

Voie 2 — sauvegarde du contrôleur, si aucune version précédente ne convient (perte plus ancienne, volume E: abîmé).

1. Sur SRV-DC01, menu *Outils*, ouvrir *Sauvegarde Windows Server*, puis *Sauvegarde locale* et *Récupérer…*.
2. *Ce serveur*, puis choisir la date : les jours avec sauvegarde sont en gras. Prendre une version **postérieure à la création** du fichier et **antérieure à sa perte**.
3. *Type de récupération* : *Fichiers et dossiers*, sélectionner l'élément.
4. *Destination* : emplacement d'origine ; cocher *Restaurer les autorisations de la liste de contrôle d'accès*.
5. Lancer, attendre *Opération réussie*, puis **ouvrir le fichier** pour vérifier son contenu.
   → Le contenu est identique à l'original.

> **Résultat attendu**
> L'élément est présent, ouvert, avec le contenu d'avant la perte et ses droits.

> **Si ce n'est pas le cas**
> Si l'élément est absent de la liste, la version choisie est antérieure à sa création : en prendre une plus récente. Si on lit une copie en ligne de commande par son chemin de type @GMT, l'heure est celle du temps universel : **heure locale moins 1 h** (moins 2 h en heure d'été).

6.2 S2 — Récupérer un compte, un groupe ou un ordinateur

Objectif	Annuler une suppression d'objet de l'annuaire sans arrêter le serveur.
Machine	SRV-DC01
Compte	admin.domaine
Outil	*Centre d'administration Active Directory*

La Corbeille Active Directory est active ; elle garde les objets supprimés **180 jours**, avec leurs attributs et leurs groupes. Elle ne protège que ce qui est supprimé **après** son activation.

1. Ouvrir le *Centre d'administration Active Directory*, le domaine, puis double-clic sur *Deleted Objects*.
   → La liste des objets supprimés s'affiche.
2. Repérer l'objet ; la colonne *Dernier parent connu* indique son UO d'origine.
3. Clic droit sur l'objet, puis *Restaurer*.
   → L'objet retourne dans son UO.
4. Vérifier que l'objet est entier : attributs et appartenance aux groupes.

Machine : SRV-DC01 · Compte : admin.domaine · exemple avec un compte témoin ; remplacer par le compte restauré

```
Get-ADUser -Identity test.corbeille -Properties MemberOf, Description | Select-Object Name, Description, MemberOf
```

Résultat attendu

Le compte, sa description et ses groupes sont revenus.

Si ce n'est pas le cas

Si l'objet est introuvable dans *Deleted Objects*, il a été supprimé avant l'activation de la Corbeille ou depuis plus de 180 jours : passer à S3.

6.3 S3 — Restauration faisant autorité d'une UO

Objectif	Récupérer une UO entière supprimée, que la Corbeille ne sait pas rendre.
Machine	SRV-DC01
Compte	Compte local du mode DSRM
Outil	wbadmin, ntdsutil, msconfig

En clair

On redémarre le contrôleur sans son annuaire, on y remet la copie d'hier, puis on dit à l'annuaire : « pour ces objets, ma version est la bonne ». Sans ce dernier geste, un autre contrôleur ferait disparaître à nouveau l'objet récupéré.

Avec les mots du métier

La restauration **faisant autorité** (*authoritative restore*) incrémente de 100 000 le numéro de version des objets restaurés pour qu'ils l'emportent sur la réplication. **DSRM** (*Directory Services Restore Mode*) est le mode de démarrage sans annuaire qui permet de restaurer la base.

1. **Éteindre** la VM et prendre un instantané, puis la rallumer.
   → Retour arrière possible.
2. Lancer wbadmin get versions et noter l'**identificateur de la version** voulue.
   → Format américain, heure **UTC** : l'identifiant s'écrit MM/JJ/AAAA-HH:MM ; ajouter 1 h en hiver, 2 h en été pour retrouver l'heure locale.
3. Passer en mode DSRM : msconfig, onglet *Démarrer*, *Démarrage sécurisé*, *Réparer Active Directory*. Redémarrer.
   → Au retour, AD DS et DNS apparaissent en rouge dans le Gestionnaire de serveur : c'est la signature du mode.
4. Ouvrir la session avec .\Administrateur et le mot de passe DSRM fixé à la promotion.

5. Restaurer l'état du système (commande 1). Confirmer trois fois. **Ne pas redémarrer** à la fin.
   → Environ 27 minutes.
6. Dans une seconde console, lancer ntdsutil (commande 2) et marquer l'UO.
   → Trois entrées mises à jour.
7. Retirer le mode DSRM (commande 3), puis redémarrer.
   → Le contrôleur démarre normalement.

Machine : SRV-DC01 (DSRM) · Compte : Administrateur local · commande 1 — restaure l'état du système et SYSVOL

```
wbadmin start systemstaterecovery -version:<identificateur> -authsysvol
```

Machine : SRV-DC01 (DSRM) · Compte : Administrateur local · commande 2 — l'UO et son contenu l'emportent sur toute réplication

```
ntdsutil
activate instance ntds
authoritative restore
restore subtree "OU=<nom de l'UO>,DC=jpconsulting,DC=lan"
quit
quit
```

Machine : SRV-DC01 (DSRM) · Compte : Administrateur local · commande 3 — sans elle, le serveur redémarre en DSRM à chaque fois

```
bcdedit /deletevalue safeboot
```

Résultat attendu

L'UO et son contenu sont revenus dans la console.

dcdiag /q ne signale que l'erreur habituelle du journal système au démarrage.

Un utilisateur du domaine Windows reste reconnu depuis une machine Linux (l'approbation a été revérifiée après le test).

Si ce n'est pas le cas

Si le serveur redémarre en DSRM sans fin, la commande 3 n'a pas été passée. Si wbadmin ne trouve aucune version, le disque de sauvegarde n'est pas visible (voir Get-Disk) ou l'identificateur est mal recopié (UTC, format américain).

Pistes d'évolution

Domaine à **un seul contrôleur** : l'effet de l'autorité sur un partenaire de réplication n'a pas été observé. La procédure a été faite une fois.

6.4 S4 — Restaurer une VM du site B

Objectif	Remettre en service une VM Proxmox à partir de son archive.
Machine	HOTE-PROXMOX
Compte	root
Outil	qmrestore, qm

1. Brancher le disque externe et le monter provisoirement (il n'est pas déclaré comme stockage).
2. Repérer l'archive de la VM dans le dossier des sauvegardes.
3. Si la VM d'origine existe encore, restaurer d'abord **à côté**, sous un autre numéro, **réseau coupé**, pour ne pas dupliquer une adresse IP.
   → La copie démarre sans carte réseau active.

4. Démarrer la copie et contrôler : interface réseau, services, comptes.
   → Pour FreeIPA : ipactl status tout *RUNNING*, kinit admin, ipa user-find.
5. Si la copie est saine : arrêter et supprimer la VM abîmée, restaurer sous son numéro d'origine, réseau branché.

Machine : HOTE-PROXMOX · Compte : root · l'option unique 1 génère une nouvelle adresse MAC ; la copie d'essai se coupe du réseau avant démarrage

```
qmrestore <archive>.vma.zst <numéro> --storage local-lvm --unique 1
```

Machine : HOTE-PROXMOX · Compte : root · supprime la copie d'essai ou la VM abîmée

```
qm destroy <numéro> --purge
```

Résultat attendu

FreeIPA restaurée : 111 secondes ; mêmes comptes qu'avant, aucun service en échec.

Si ce n'est pas le cas

Si le disque externe n'est pas détecté, vérifier le port USB : un port USB 2.0 l'a déjà fait passer inaperçu (dmesg montrait une liaison *full-speed* et des erreurs). Changer de port.

Pistes d'évolution

Les archives ne contiennent pas la garde IPsec ni la tâche planifiée posée sur PFSENSE02 après la sauvegarde de cette VM : l'export XML plus récent les contient.

6.5 S5 — Reconfigurer un pare-feu (procédure écrite, à tester)

Objectif	Remettre la configuration d'un pare-feu pfSense à partir de son export.
Machine	PFSENSE01 ou PFSENSE02
Compte	admin
Outil	Interface web, menu *Diagnostics*, *Backup & Restore*

1. Réinstaller pfSense si la machine est vide et lui donner une adresse d'administration.
2. Ouvrir *Diagnostics*, *Backup & Restore*, section *Restore Backup*.
3. Choisir le fichier d'export, saisir le mot de passe de chiffrement, lancer la restauration.
   → La machine redémarre.
4. Vérifier les interfaces, le tunnel IPsec, les règles, puis les alertes Suricata.

À vérifier

Cette procédure n'a pas été essayée dans le lab : le menu exact et le comportement du tunnel au redémarrage sont à confirmer. Les exports des deux pare-feux sont à jour ; refaire l'export après toute modification.

6.6 S6 — La VM SRV-DC01 est perdue (procédure écrite, à tester)

Objectif	Reconstruire le contrôleur de domaine sur une VM vide à partir de la sauvegarde.
Machine	VM neuve sur HOTE-VMWARE
Compte	Compte local
Outil	Support d'installation de Windows Server, console *Sauvegarde Windows Server*

En clair

On crée une VM vide aussi grande que l'ancienne, on la démarre sur le support d'installation, et on lui remet l'image complète prise la veille.

1. Créer une VM de même firmware (UEFI), avec des disques **au moins aussi grands** que ceux d'origine, sans la brancher au réseau.
2. Rattacher le disque de sauvegarde de 150 Go à la nouvelle VM.
3. Démarrer sur le support d'installation, choisir *Réparer l'ordinateur*, puis *Récupération de l'image système*.
4. Choisir la version la plus récente, restaurer, laisser la machine redémarrer.
5. Au premier démarrage, **contrôler avant de rebrancher le réseau** : dcdiag /q, partages, DNS, DHCP.
6. Rebrancher le réseau, vérifier l'approbation avec le domaine Linux, puis le reste du site A dans l'ordre du chapitre 5. GLPI ne permettra la connexion par l'annuaire qu'une fois le contrôleur et son certificat de nouveau valides.

À savoir

Pas encore testée. Le délai de 4 heures est une estimation.

Le disque de sauvegarde étant sur le même PC, cette procédure ne couvre que la perte de **la VM**, pas celle du PC (S7).

Ne jamais rallumer l'ancienne VM du contrôleur à côté de la nouvelle : deux contrôleurs avec les mêmes rôles faussent l'annuaire.

6.7 S8 — Restaurer GLPI

Objectif	Remettre GLPI en état (tickets, inventaire) à partir de la copie la plus récente.
Machine	SRV-GLPI01
Compte	Compte d'administration Linux
Outil	Terminal, navigateur

1. Repérer la copie la plus récente : sur SRV-GLPI01 (14 dernières, tous les jours à 13 h 30) ou, si la VM est perdue, sur la seconde machine (SRV-FREEIPA01, 60 jours).
2. Si la VM est détruite, en refaire une avec le même système, la même version de GLPI et le même PHP, avant de recharger quoi que ce soit.
3. Recharger la **base** et les **fichiers** de la même copie, **avec la clé glpicrypt.key** (droits 640).
   → Sans la clé, les secrets stockés sont illisibles.
4. Contrôler dans le navigateur : connexion locale, connexion avec un compte du domaine, nombre de tickets, un ticket ouvert, l'inventaire.
   → Les 9 tickets de la copie testée étaient revenus.

Pistes d'évolution

Seule la **base** a été restaurée en vrai, dans une base de test. La reconstruction d'une VM GLPI complète n'a pas été jouée ; les commandes exactes sont à consigner au premier exercice chronométré.

7. Résultats des tests réels

Statut	Test	Résultat	Ce que cela prouve
Réalisé	Archive des six VM du site B (vzdump), vérification des archives	Environ 19 min pour 42,4 Go ; intégrité de chaque archive contrôlée	Les archives sont lisibles
Réalisé	Restauration de FreeIPA sous un autre numéro, réseau coupé	111 s ; services démarrés, comptes intacts, aucune adresse dupliquée	Cette archive-là est utilisable
Réalisé	Restauration d'un fichier, contenu contrôlé	Réussie	La sauvegarde du contrôleur contient les données
Réalisé	Suppression et restauration d'un compte par la Corbeille	Réussie	La Corbeille est active et fonctionne
Réalisé	Suppression d'une UO, puis restauration faisant autorité en DSRM	Réussie ; environ 1 h 45 au total, dont 27 min de restauration ; approbation Linux revérifiée	La sauvegarde de l'état du système est exploitable
Réalisé	Restauration de la base de GLPI dans une base de test	Réussie : les 9 tickets sont revenus	La copie de GLPI est lisible et complète
Réalisé	Récupération d'un dossier supprimé par les versions précédentes, sans écraser le travail existant	Réussie ; droits vérifiés après remise en place	Les copies instantanées protègent les partages

À retenir

Une sauvegarde n'est prouvée que par une restauration. Les archives des cinq autres VM du site B n'ont été vérifiées que par leur intégrité, pas par un démarrage ; la VM GLPI complète reste à reconstruire.

8. Ce qui reste à couvrir

Risque	Conséquence aujourd'hui	Amélioration envisagée
Panne ou perte du PC hôte du site A	Les VM **et** leurs sauvegardes disparaissent ensemble (sauf la copie de GLPI)	Copier la sauvegarde du contrôleur sur un support extérieur au PC (règle 3-2-1)
Panne d'un disque du PC hôte du site A	Les VM de ce disque tombent (cf. incident NVMe) ; reprise à jouer	Répéter l'exercice : déplacer ou restaurer une VM sur un autre disque
Panne du PC du site B ou de son disque unique	Les archives sont sur le disque externe : reconstruction possible, à jouer	Seconde copie des archives ; test sur une machine vide
Un seul contrôleur de domaine	Pas d'authentification pendant la reprise ; la reprise est une restauration	Second contrôleur : la plupart des pertes deviennent des bascules
Reconstruction sur machine vide non testée	Aucun RTO réel pour S6	Exercice de reconstruction chronométré
Archives du site B non planifiées	RPO de plusieurs semaines	Planifier la sauvegarde Proxmox
Zabbix, collecteur, WSUS, AD CS sans sauvegarde planifiée	Reconstruction à partir de zéro	Sauvegardes applicatives hors machine
Copie au même endroit	Les exports des pare-feux sont sur des supports du même bureau	Un exemplaire hors site

Prochaines étapes

La règle **3-2-1** (3 copies, 2 supports, 1 hors site) n'est **pas respectée**. Seule la copie de GLPI sort du PC.

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

Aucun RTO/RPO n'a été validé par un besoin métier : ce sont des hypothèses.

Ce plan n'est pas un plan de **continuité** : rien ne permet de poursuivre l'activité pendant la panne.

9. Exercices pour compléter le plan

Exercice	Ce qu'il apporte	Difficulté
Reconstruire SRV-DC01 sur une VM vide, chronomètre en main	Un vrai RTO pour S6 ; confirme que la sauvegarde complète est exploitable	Moyenne
Copier la sauvegarde du contrôleur sur un support extérieur	Premier pas vers la règle 3-2-1	Facile
Réimporter l'export XML d'un pare-feu sur une VM pfSense de test	Valide S5	Facile
Restaurer une seconde VM du site B (un client Linux)	Passe de « une VM prouvée » à « deux »	Facile
Refaire une archive des VM du site B, puis planifier la sauvegarde Proxmox	Renouvelle l'archive et donne un RPO réel au site B	Moyenne
Programmer la sauvegarde des GPO (tâche planifiée)	Une copie à jour sans y penser	Facile
Reconstruire une VM GLPI complète et chronométrer	Un RTO réel pour S8 ; consigne les commandes exactes	Moyenne
Superviser la fraîcheur de la copie de GLPI dans Zabbix	Une copie ancienne ne passerait plus inaperçue	Facile

10. Lexique

Terme	En clair
Bare metal	Restauration complète sur une machine vide, sans système installé.
Corbeille AD	Fonction de l'annuaire qui garde les objets supprimés pendant 180 jours.
DSRM	Mode de démarrage d'un contrôleur de domaine sans annuaire, pour le restaurer.
État du système	Annuaire, SYSVOL et registre d'un contrôleur ; indispensable pour le restaurer.
Faisant autorité	Marquage qui force des objets restaurés à l'emporter sur la réplication.
Instantané	Photo de l'état d'une VM, sur le même disque ; pas une sauvegarde.
Versions précédentes	Copies d'un partage gardées par le serveur à heure fixe ; protègent d'une erreur, pas d'une panne de disque.

Terme	En clair
PRA / PCA	Plan de reprise (repartir après) / de continuité (continuer pendant).
RPO	Perte de données acceptée, en temps depuis la dernière copie.
RTO	Durée d'interruption acceptée.
Règle 3-2-1	Trois copies, deux supports, une copie hors site.
vzdump	Outil de sauvegarde des VM de Proxmox.
wbadmin	Commande de la Sauvegarde Windows Server.