

CATÉGORIE GLPI · JP CONSULTING

Playbook Serveurs et services

Les runbooks de la catégorie GLPI Serveurs et services

Jean-Philippe Rebischung

Sommaire

Ce playbook regroupe les runbooks de la catégorie GLPI **Serveurs et services**. Un runbook par sous-catégorie ; chaque runbook décrit, cas par cas, la conduite à tenir pour un incident ou une demande.

Annuaire et GPO 3

Incident · Les lecteurs réseau ont disparu (GPO refusée ou absente) 4

Applications métier 9

Incident · L'inventaire d'une machine est refusé par GLPI (403) 10

Certificats 13

Changement · Le certificat de GLPI arrive à échéance 14

Mises à jour 19

Incident · Un serveur ne se met plus à jour 20

Stockage et partages 25

Incident · Le volume des partages est presque plein 26

Virtualisation et matériel 35

Incident · Des machines virtuelles tombent en écran bleu (0x124) 36

Index par symptôme

Ce que je reçois	Runbook	Page
Un utilisateur : « je n'ai plus mes lecteurs P: et I: »	Annuaire et GPO	4
L'agent GLPI : « 403 Forbidden » à l'envoi de l'inventaire	Applications métier	10
Une alerte Zabbix : le certificat de GLPI expire dans moins de 30 jours	Certificats	14
Un constat : les mises à jour d'un serveur échouent (0x80240438, 0x800736b3)	Mises à jour	20
Une alerte Zabbix : espace libre faible sur le volume des partages (E:)	Stockage et partages	26
Un constat : plusieurs VM ont redémarré seules en même temps (écran bleu 0x124)	Virtualisation et matériel	36

> **Les champs à remplacer**
>
> Dans les commandes et les messages, un texte entre chevrons, comme **`<N°_TICKET>`** ou **`<NOM_DU_DOSSIER>`**, est **à remplacer par la valeur de ton cas, chevrons compris**. Exemple : **`E:\Restauration-<N°_TICKET>`** devient **`E:\Restauration-21`**.
>
> Avant de valider une commande, relis-la : s'il reste un chevron, elle n'est pas prête.

RUNBOOK · PLAYBOOK SERVEURS ET SERVICES

Annuaire et GPO

L'annuaire Active Directory et les stratégies de groupe.

Cas traités dans ce runbook

INCIDENT Les lecteurs réseau ont disparu (GPO refusée ou absente).....4

Statut : non validé

INCIDENT · ANNUAIRE ET GPO

Les lecteurs réseau ont disparu (GPO refusée ou absente)

Niveau	N1 (gpresult, constat) puis N2 (console GPO).
Où	le poste de l'utilisateur (sa session) et **`SRV-DC01`** (console Gestion de stratégie de groupe), compte **`JPCONSULTING\admin.domaine`**.
GLPI	type Incident · catégorie : Serveurs et services › Annuaire et GPO.
	Statut : non validé

Ce que tu reçois et ce qu'on attend de toi

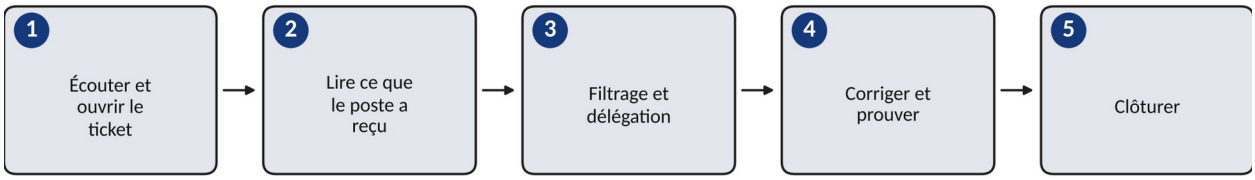
Les lecteurs réseau (**`P:`** Commun, **`I:`** Informatique) sont donnés par la GPO *Utilisateurs - Mappage lecteurs*. Quand ils disparaissent, la question est : **qu'est-ce que le poste a réellement reçu ?** La GPO est appliquée, refusée, ou absente.

Ton travail : lire ce que le poste a reçu, trouver pourquoi une GPO est refusée ou absente, corriger le bon réglage, prouver par la session de l'utilisateur.

Ce que tu reçois, par exemple : « Je n'ai plus mes lecteurs P: et I: depuis ce matin. »

Regle d'or

`gpresult` d'abord, la console ensuite : on lit ce qui est **arrivé** sur le poste avant de modifier une GPO.



Les étapes de ce cas.

1 Écouter et ouvrir le ticket

- Quels lecteurs manquent ? Tous, ou seulement **`I:`** (réservé au groupe **`DL_Informatique_M`**) ?
- Depuis quand ? Un collègue est-il touché ?
- A-t-on modifié une GPO ou un groupe récemment ?

Ticket : **Incident**, catégorie **Serveurs et services › Annuaire et GPO** (corrigée à la clôture selon la cause réelle).

2 Lire ce que le poste a reçu

Machine : Le poste de l'utilisateur | **Compte :** l'utilisateur (sa propre session) | **Outil :** Invite de commandes (sans élévation)

```
gpresult /r /scope user
```

Lire la commande

`/scope user` : la partie **utilisateur** des GPO, qui n'existe que dans la session de l'utilisateur. Lance-la donc dans **sa** session, pas en administrateur.

La GPO est…	Ce que ça veut dire	Suite
dans les **appliquées**	La consigne est arrivée ; ce sont ses **paramètres** qui posent problème	`net use`, chemins de la GPO
dans les **refusées**, raison inconnue	Signature du correctif **MS16-072*** : l'ordinateur ne peut pas lire la GPO	Étape 3
dans **aucune** liste	La GPO n'atteint pas l'utilisateur (compte hors de `JP Consulting`, lien désactivé)	UO du compte, liens de la GPO

3 Filtrage et délégation

Console **Gestion de stratégie de groupe** → *Utilisateurs - Mappage lecteurs*. Onglet **Étendue**, cadre *Filtrage de sécurité* : *Utilisateurs authentifiés* est-il présent ? Onglet **Délégation** : une ligne donne-t-elle la **Lecture** à **Ordinateurs du domaine** (ou à *Utilisateurs authentifiés*) ?

Pourquoi

Depuis 2016, la partie utilisateur d'une GPO est lue **avec l'identité de l'ordinateur**. Si l'on restreint le filtrage à un groupe d'utilisateurs en retirant *Utilisateurs authentifiés*, l'ordinateur perd la lecture : la GPO est refusée pour tout le monde.

4 Corriger et prouver

Onglet **Délégation** → **Ajouter…** → `Ordinateurs du domaine` → **OK** → droit **Lecture** (et non *Lire, Appliquer*). Puis, sur le poste, dans la session de l'utilisateur :

Machine : Le poste de l'utilisateur | **Compte :** l'utilisateur | **Outil :** Invite de commandes

```
gpupdate /force
```

Fermer la session et la rouvrir (les lecteurs se connectent à l'ouverture), puis :

Machine : Le poste de l'utilisateur | **Compte :** l'utilisateur | **Outil :** Invite de commandes

```
net use
```

Je dois voir

`P:` connecté (et `I:` pour un membre de `GG_Informatique`). `gpresult /r /scope user` range la GPO dans les **appliquées**.

Contre-épreuve : un utilisateur hors de `GG_Informatique` n'a toujours **pas** `I:` : le ciblage fonctionne encore.

5 Clôturer

Texte de la tâche (GLPI)

Lecteurs <LECTEURS> absents pour <PRÉNOM> sur <POSTE> depuis <HEURE>. `gpresult` : GPO *Utilisateurs - Mappage lecteurs* <APPLIQUÉE/REFUSÉE/ABSENTE>. Cause : <CAUSE> (filtrage : <CONSTAT> ; délégation : <CONSTAT>). Correction : <ACTION> à <HEURE>. Preuve : `net use` après reconnexion, contre-épreuve <RÉSULTAT>.

Texte de la solution (GLPI), lisible par l'utilisateur

Bonjour <PRÉNOM>,

Vos lecteurs réseau sont de nouveau disponibles : un réglage de la stratégie qui les distribue empêchait votre poste de la lire. Il a été corrigé ; les lecteurs reviennent à chaque ouverture de session.

Cordialement,

Lexique

Les mots marqués d'un astérisque (*) dans ce runbook.

GPO (stratégie de groupe)

Ensemble de réglages appliqués automatiquement aux ordinateurs ou aux utilisateurs d'une UO.

MS16-072

Correctif de juin 2016 : la partie utilisateur d'une GPO est lue avec le compte de l'ordinateur, qui doit donc avoir le droit de lecture sur la GPO.

Notes

RUNBOOK · PLAYBOOK SERVEURS ET SERVICES

Applications métier

GLPI et les applications du lab.

Cas traités dans ce runbook

INCIDENT L'inventaire d'une machine est refusé par GLPI (403).....10

Statut : non validé

L'inventaire d'une machine est refusé par GLPI (403)

Niveau	N2.
Où	la machine inventoriée (**`SRV-DC01`**, compte **`JPCONSULTING\admin.domaine`**) et **`SRV-GLPI01`** (SSH depuis le PC hôte, compte **`admin.linux`**).
GLPI	type Incident · catégorie : Serveurs et services › Applications métier. *Statut : non validé*

Ce que tu reçois et ce qu'on attend de toi

L'agent GLPI d'une machine envoie son inventaire au serveur GLPI. Un **403*** veut dire : « j'ai compris ta demande, et je la refuse ». Ce n'est donc **ni le réseau, ni le certificat** : le serveur est joignable, mais un réglage lui interdit d'accepter les inventaires.

Ton travail : lire l'erreur exacte, écarter le réseau, prouver la valeur du réglage **à la source** (la base), corriger, vérifier.

Ce que tu reçois : la fiche d'une machine n'est plus à jour dans GLPI, ou un inventaire forcé échoue.

Regle d'or

Affiché n'est pas enregistré : une case cochée à l'écran ne prouve rien tant que la valeur n'est pas relue en base.



Les étapes de ce cas.

1 Lire l'erreur de l'agent

Machine : SRV-DC01 | **Compte :** JPCONSULTING\admin.domaine | **Outil :** PowerShell (administrateur)

```
Get-Content "C:\Program Files\GLPI-Agent\logs\glpi-agent.log" -Tail 30
```

Je dois voir

Une ligne d'échec avec **403** (*Forbidden*). Aucune ligne récente : force un inventaire depuis **`http://localhost:62354`** sur la machine, puis relis le journal.

Sur ce lab, seul le DC a l'agent GLPI (service **`glpi-agent`**).

Ticket : **Incident**, catégorie **Serveurs et services › Applications métier**.

2 Écarter le réseau

Machine : SRV-DC01 | **Compte :** JPCONSULTING\admin.domaine | **Outil :** PowerShell (administrateur)

```
Test-NetConnection SRV-GLPI01.jpconsulting.lan -Port 443
```

Je dois voir

`TcpTestSucceeded : True`. De toute façon, un 403 **prouve** que la connexion et le chiffrement ont abouti : ne cherche pas de ce côté.

3 Lire le réglage en base

Machine : SRV-GLPI01 (192.168.20.60) | **Compte :** compte sudo (admin.linux) | **Outil :** SSH depuis le PC hôte

```
sudo mysql -e "SELECT context, name, value FROM glpi.glpi_configs WHERE name =
'enabled_inventory';"
```

Je dois voir

`value` = `0` : la réception des inventaires est **désactivée** en base, quelle que soit la case affichée. `1` : le réglage est actif, cherche ailleurs (droits, entité).

4 Corriger et vérifier

GLPI : **Administration → Inventaire**, coche **Activer l'inventaire**, puis **Sauvegarder** (bandeau de confirmation). Relis la valeur en base (même commande) : `1`. Force un inventaire depuis `http://localhost:62354` sur la machine.

Je dois voir

Plus de 403 dans `glpi-agent.log` ; la fiche de la machine est à jour dans **Parc → Ordinateurs** (date du dernier inventaire).

5 Clôturer

Texte de la tâche (GLPI)

Inventaire forcé de <MACHINE> à <HEURE> : 403 Forbidden (journal de l'agent). Réseau et certificat écartés (connexion aboutie). `enabled_inventory` = 0 en base. Réglage sauvegardé dans Administration → Inventaire ; valeur relue à 1. Nouvel inventaire à <HEURE> : accepté, fiche à jour.

Texte de la solution (GLPI)

L'inventaire de <MACHINE> est de nouveau accepté par GLPI : la réception des inventaires n'avait jamais été enregistrée. C'est corrigé et vérifié.

Lexique

Les mots marqués d'un astérisque (*) dans ce runbook.

403 Forbidden

Réponse d'un serveur web qui a compris la demande et la refuse par configuration. À distinguer d'un délai dépassé (réseau) ou d'une erreur de certificat.

Agent GLPI

Programme installé sur une machine, qui envoie son inventaire (matériel, logiciels) au serveur GLPI.

RUNBOOK · PLAYBOOK SERVEURS ET SERVICES

Certificats

Les certificats des interfaces d'administration, signés par l'autorité JPConsulting-RootCA.

Cas traités dans ce runbook

CHANGEMENT Le certificat de GLPI arrive à échéance.....14

Statut : non validé

Le certificat de GLPI arrive à échéance

Niveau	N2, validation N3.
Où	**`SRV-GLPI01`** (SSH depuis le PC hôte, compte **`admin.linux`**), le PC hôte (transferts), **`SRV-DC01`** (signature, compte **`JPCONSULTING\admin.domaine`**).
GLPI	type Changement · catégorie : Serveurs et services › Certificats. *Statut : non validé*

Ce que tu reçois et ce qu'on attend de toi

Les interfaces d'administration du lab présentent un **certificat*** signé par l'autorité **`JPConsulting-RootCA`**. Un certificat a une date de fin : après, les navigateurs et les outils refusent la connexion. Zabbix surveille celui de GLPI et prévient **30 jours** avant.

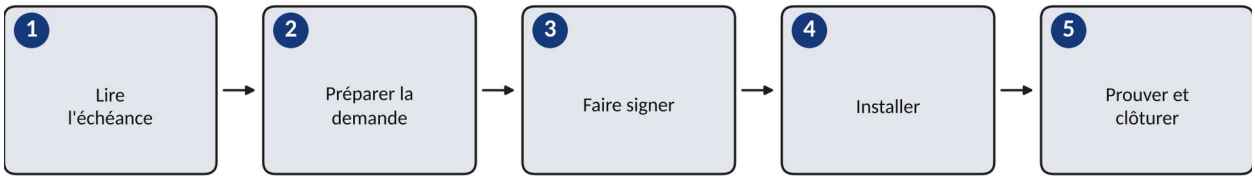
Ton travail : vérifier l'échéance, préparer un nouveau certificat (la clé naît sur la machine et n'en sort pas), le faire signer, l'installer, prouver.

Ce que tu reçois : une alerte Zabbix sur l'hôte **`Certificat - GLPI`** : le certificat expire dans moins de 30 jours.

Regle d'or

La **clé privée*** ne quitte jamais la machine qui la porte : seule la demande de signature voyage.

On remplace un certificat **avant** l'échéance, sur **demande de changement** : l'interface sera coupée quelques secondes.



Les étapes de ce cas.

1 Lire l'échéance

Machine : SRV-GLPI01 (192.168.20.60) | **Compte :** compte sudo (admin.linux) | **Outil :** SSH depuis le PC hôte

```
grep -E 'SSLCertificate(Key)?File' /etc/apache2/sites-available/glpi-ssl.conf
```

Je dois voir

Deux lignes : le fichier du certificat (**`SSLCertificateFile`**) et celui de la clé (**`SSLCertificateKeyFile`**, dans **`/etc/ssl/private/`**). Note les deux chemins.

Machine : SRV-GLPI01 | **Compte :** compte sudo (admin.linux) | **Outil :** Bash

```
openssl x509 -noout -subject -enddate -ext subjectAltName -in <CHEMIN_DU_CERTIFICAT>
```

Je dois voir

`notAfter=` : la date de fin. Le SAN* (**`DNS:SRV-GLPI01.jpconsulting.lan`** et l'adresse) est à reprendre à l'identique dans le nouveau certificat.

Ticket : **Changement** (ou Incident si l'échéance est passée), catégorie **Serveurs et services › Certificats**.

2 Préparer la demande

- **`SRV-ADCS01` allumée** : elle porte l'autorité ; éteinte, la signature échoue en **`0x800706ba`** (« Le serveur RPC n'est pas disponible »).
- **`SRV-WSUS01` allumée** si l'on veut vérifier la révocation en HTTP.
- Validation du changement par le N3, avec l'heure de la courte coupure de GLPI.

Machine : SRV-GLPI01 | **Compte :** compte sudo (admin.linux) | **Outil :** Bash

```
sudo openssl req -new -newkey rsa:3072 -nodes -keyout
/etc/ssl/private/<NOM_DE_LA_CLÉ>.key -out /tmp/glpi.csr -subj "/CN=SRV-
GLPI01.jpconsulting.lan" -addext "subjectAltName=DNS:SRV-
GLPI01.jpconsulting.lan,IP:192.168.20.60"
```

Lire la commande

`-newkey rsa:3072 -nodes` : crée une nouvelle clé RSA de 3072 bits, sans phrase secrète (Apache doit la lire seul au démarrage).

`-keyout` : la clé, rangée dans **`/etc/ssl/private/`** ; donne-lui un **nouveau nom** pour garder l'ancienne en cas de retour arrière. **`-out`** : la demande de signature (CSR*).

`-subj` et **`-addext subjectAltName=…`** : le nom et le SAN, identiques à ceux du certificat actuel.

3 Faire signer

La demande passe par le PC hôte, seul poste qui ouvre une session SSH sur GLPI et sur le DC : copie **`/tmp/glpi.csr`** vers le PC hôte, puis vers **`C:\Outils\Certificats\`** sur le DC (**`scp`**).

Machine : SRV-DC01 | **Compte :** JPCONSULTING\admin.domaine | **Outil :** PowerShell (administrateur)

```
certreq -submit -attrib "CertificateTemplate:WebServer" -config "SRV-
ADCS01.jpconsulting.lan\JPConsulting-RootCA" C:\Outils\Certificats\glpi.csr C:\Outils\
Certificats\glpi-<ANNÉE>.cer
```

Je dois voir

Un numéro de demande et le message de certificat délivré ; le fichier **`.cer`** est créé. **`0x800706ba`** : **`SRV-ADCS01`** est éteinte.

4 Installer

Rapporte le **`.cer`** sur GLPI par le même chemin. Copie-le à côté de l'ancien certificat sous un **nouveau nom**, puis, dans **`glpi-ssl.conf`**, fais pointer **`SSLCertificateFile`** et **`SSLCertificateKeyFile`** vers les nouveaux fichiers (garde une copie du fichier de configuration avant de le modifier).

Machine : SRV-GLPI01 | **Compte :** compte sudo (admin.linux) | **Outil :** Bash

```
sudo apachectl configtest && sudo systemctl reload apache2
```

Lire la commande

`configtest` vérifie la configuration ; `&&` ne lance le rechargement que si le test répond `Syntax OK`. Un rechargement ne coupe pas les sessions en cours.

5 Prouver et clôturer

Machine : HOTE-VMWARE (PC hôte, 192.168.20.70) | **Compte :** session Windows de l'hôte | **Outil :** navigateur, puis Zabbix

Ouvre `https://SRV-GLPI01.jpconsulting.lan` : aucun avertissement, et le cadenas montre la **nouvelle date de fin**. Dans Zabbix, le problème de l'hôte `Certificat - GLPI` passe en **Résolu**.

Texte de la tâche (GLPI)

Alerte Zabbix du <DATE> : certificat GLPI échéance <DATE>. Changement validé par <N3>. Nouvelle clé RSA 3072 générée sur GLPI (<CHEMIN>), CSR signée sur le DC (modèle WebServer, demande n° <N>), certificat installé, `glpi-ssl.conf` mis à jour (copie conservée), Apache rechargé à <HEURE>. Preuve : nouvelle échéance <DATE> lue dans le navigateur, alerte Zabbix résolue. Ancienne clé et ancien certificat conservés jusqu'au <DATE>.

Texte de la solution (GLPI)

Le certificat de l'interface GLPI a été renouvelé ; il est valable jusqu'au <DATE>. Aucune action n'est nécessaire de votre côté.

Lexique

Les mots marqués d'un astérisque (*) dans ce runbook.

Certificat
Carte d'identité numérique d'un serveur, signée par une autorité ; il a une date de fin.

Clé privée
Secret associé au certificat ; elle ne doit jamais quitter la machine qui la porte.

CSR / SAN
CSR : demande de signature (contient la clé publique). SAN : noms et adresses pour lesquels le certificat est valable.

Notes

RUNBOOK · PLAYBOOK SERVEURS ET SERVICES

Mises à jour

Les mises à jour des serveurs et des postes, distribuées par WSUS.

Cas traités dans ce runbook

INCIDENT Un serveur ne se met plus à jour.....20

Statut : non validé

Un serveur ne se met plus à jour

Niveau	N2. Source locale, remplacement d'un serveur : N3.
Où	**`SRV-DC01`** (le contrôleur de domaine), compte **`JPCONSULTING\admin.domaine`**, PowerShell ouvert **en administrateur**. Sur ce lab, le technicien N2 ne peut pas se connecter au contrôleur de domaine : on utilise un compte administrateur.
GLPI	type Incident · catégorie : Serveurs et services › Mises à jour. *Statut : non validé*

Ce que tu reçois et ce qu'on attend de toi

Windows garde une **réserve de pièces détachées** (le **magasin de composants***) pour s'installer et se mettre à jour. Quand une pièce manque, la mise à jour échoue (**`0x800736b3`**). Avant cela, une cause plus simple est fréquente sur ce lab : le serveur **WSUS** est éteint (**`0x80240438`**).

Ton travail : lire le code, écarter WSUS, réparer le magasin (DISM puis SFC), et décider quand remplacer plutôt qu'insister.

Ce que tu reçois : un constat, par exemple « le DC n'a plus installé de mise à jour depuis un mois, l'historique montre des échecs ».

Regle d'or

DISM d'abord, SFC ensuite : SFC répare les fichiers en service à partir du magasin que DISM répare.

On n'éteint jamais un DC défaillant : s'il faut le remplacer, on ajoute un nouveau DC d'abord (PROC-30).



Les étapes de ce cas.

1 Lire le code d'erreur

Machine : SRV-DC01 | **Compte :** JPCONSULTING\admin.domaine | **Outil :** PowerShell (administrateur)

```
Get-WinEvent -LogName Microsoft-Windows-WindowsUpdateClient/Operational -MaxEvents 30
| Where-Object LevelDisplayName -eq 'Erreur' | Format-List TimeCreated, Message
```

Je dois voir

Le code d'erreur dans le message : **`0x80240438`** → étape 2 ; **`0x800736b3`** ou **`0x800f0915`** → étape 3.

Ticket : **Incident**, catégorie **Serveurs et services › Mises à jour**.

2 Écarter WSUS

Machine : SRV-DC01 | **Compte :** JPCONSULTING\admin.domaine | **Outil :** PowerShell (administrateur)

```
Test-NetConnection SRV-WSUS01.jpconsulting.lan -Port 8531
```

Je dois voir

`True` : WSUS répond. **`False`** : la VM **`SRV-WSUS01`** est éteinte ou injoignable : démarre-la, relance la recherche de mises à jour ; c'était peut-être toute la panne.

3 Réparer le magasin

Machine : SRV-DC01 | **Compte :** JPCONSULTING\admin.domaine | **Outil :** PowerShell (administrateur)

```
DISM /Online /Cleanup-Image /RestoreHealth
```

Je dois voir

« L'opération de restauration s'est terminée correctement ». Un palier long vers 62 % est normal (10 à 20 minutes sur une VM) : n'interromps pas.

Échec en **`0x800f0915`** : DISM ne trouve pas de quoi réparer ; il faut une source locale (image d'installation de la **même version**) : escalade N3.

Machine : SRV-DC01 | **Compte :** JPCONSULTING\admin.domaine | **Outil :** PowerShell (administrateur)

```
sfc /scannow
```

Je dois voir

« n'a trouvé aucune violation d'intégrité » : les fichiers en service sont sains.

4 Vérifier

Relance une mise à jour réelle (*Paramètres → Windows Update → Rechercher des mises à jour*, ou depuis la console WSUS). Pour un DC, vérifie aussi l'annuaire :

Machine : SRV-DC01 | **Compte :** JPCONSULTING\admin.domaine | **Outil :** PowerShell (administrateur)

```
dcdiag /q
```

Je dois voir

La mise à jour s'installe. **`dcdiag /q`** n'affiche rien : aucun test en échec.

Attention

Cas vécu (STAR 33) : l'ancien DC échouait encore après réparation avec une source locale (composants plus récents que l'image). Décision : le **remplacer** par un nouveau DC (PROC-30) plutôt qu'insister. Cette décision appartient au N3.

5 Clôturer

Texte de la tâche (GLPI)

Serveur <NOM> : échecs de mises à jour depuis le <DATE>, code <CODE>. WSUS (8531) : <JOIGNABLE/ÉTEINT>. DISM /RestoreHealth : <RÉSULTAT>. SFC : <RÉSULTAT>. Mise à jour <KB> installée à <HEURE>. dcdiag /q : <RÉSULTAT>.

Texte de la solution (GLPI)

Le serveur <NOM> installe de nouveau ses mises à jour : <CAUSE_EN_MOTS_SIMPLES>.

Lexique

Les mots marqués d'un astérisque (*) dans ce runbook.

Magasin de composants (WinSxS)
Réserve de fichiers dont Windows se sert pour s'installer, se mettre à jour et se réparer.

DISM / SFC
DISM répare le magasin de composants ; SFC vérifie et répare les fichiers système en service à partir de ce magasin.

WSUS
Serveur qui distribue les mises à jour Microsoft aux machines du domaine ; ici **`SRV-WSUS01`**, port HTTPS 8531.

Notes

RUNBOOK · PLAYBOOK SERVEURS ET SERVICES

Stockage et partages

Les volumes et les dossiers partagés du serveur de fichiers : espace disque, quotas, accès aux partages.

Cas traités dans ce runbook

INCIDENT Le volume des partages est presque plein.....26

Statut : non validé

Le volume des partages est presque plein

Niveau	N2 (mesurer et informer). Quota et agrandissement du volume : N3.
Où	**`SRV-DC01`** (le serveur de fichiers), compte **`JPCONSULTING\admin.domaine`**, PowerShell ouvert **en administrateur**. Sur ce lab, le technicien N2 ne peut pas se connecter au serveur de fichiers (c'est aussi le contrôleur de domaine) : on utilise un compte administrateur.
GLPI	type Incident (proactif) · catégorie : Serveurs et services › Stockage et partages. *Statut : non validé*

Ce que tu reçois et ce qu'on attend de toi

Un disque plein, c'est la panne : plus personne ne peut enregistrer. Cette alerte te prévient **avant**.

Ton travail : dire combien il reste de place et où elle est partie, puis **informer la personne qui décide**. C'est elle qui décide ce qu'on garde. Tu mesures et tu informes ; tu ne supprimes rien de toi-même.

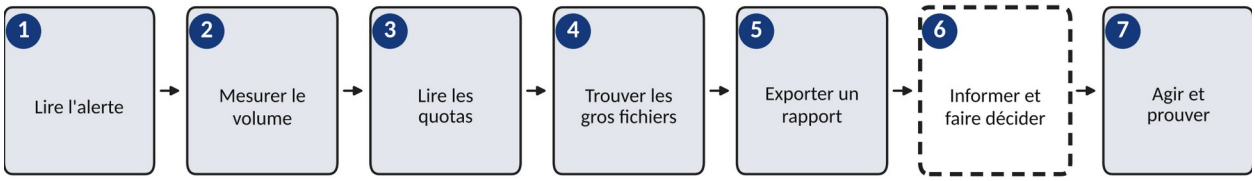
Ce que tu reçois : une alerte Zabbix sur le serveur de fichiers, gravité Moyen. Aucun utilisateur ne se plaint encore. Texte de l'alerte :

```
Windows FS [Partages(E:)]: Space is critically low (used>90%, total 100.0GB)
```

Lecture : le volume **`E:`** (étiquette Partages, 100 Go) est occupé à plus de 90 %.

Regle d'or

On ne supprime jamais un fichier d'un partage sans décision écrite de la personne qui décide. Un fichier supprimé à travers le réseau ne passe **pas** par la Corbeille de Windows : il est perdu, sauf copie de sauvegarde*.



Les sept étapes de ce cas. À l'étape 6, c'est la personne responsable des données qui décide.

1 Lire l'alerte

Sur le PC hôte, dans Zabbix : **Surveillance → Problèmes**. Note l'hôte, le volume, le pourcentage et l'**heure de début**.

Ouvre tout de suite le ticket dans GLPI. **Titre** : « Espace libre faible sur le volume Partages (E:) ». **Description** : le texte exact de l'alerte et son heure. Mets l'**urgence* à Moyenne** pour l'instant et l'**impact* à Haut** : si le volume se remplit, tous les utilisateurs des partages sont touchés.

Pourquoi

L'urgence dépend du **délai** avant la panne. Tu ne le connaîtras qu'à l'étape 6 : tu reverras alors l'urgence. L'impact dépend du **nombre de personnes** touchées, pas de la gravité technique.

2 Mesurer le volume

Interface graphique : **Explorateur de fichiers → Ce PC → clic droit sur le disque E: (Partages) → Propriétés**. Le camembert donne l'espace utilisé, libre et la capacité. Puis la même mesure en PowerShell, qui s'écrit et se garde dans le ticket :

Machine : SRV-DC01 | **Compte :** JPCONSULTING\admin.domaine | **Outil :** PowerShell (administrateur)

```
Get-Volume -DriveLetter E | Select-Object DriveLetter, FileSystemLabel,
@{n='TailleGo';e={[math]::Round($_.Size/1GB,1)}},
@{n='LibreGo';e={[math]::Round($_.SizeRemaining/1GB,1)}},
@{n='PctLibre';e={[math]::Round(100*$_.SizeRemaining/$_.Size,1)}}
```

Lire la commande

`Get-Volume` : une commande s'écrit **Verbe-Nom**, ici « obtenir les volumes ». `-DriveLetter E` : seulement le volume E.

`|` (le **tube**) : le résultat de gauche est envoyé à la commande de droite. `Select-Object` : choisit les colonnes à afficher.

`@{n='LibreGo';e={...}}` : une colonne inventée. `n` = son nom, `e` = le calcul (octets divisés par `1GB`, arrondi à 1 décimale).

Je dois voir

Une ligne : `E Partages TailleGo LibreGo PctLibre`. Exemple : 100 / 8,8 / 8,8 = il reste 8,8 Go libres, soit 8,8 % (le volume est occupé à 91,2 %).

Aucune ligne : la lettre n'existe pas (disque absent). Regarde **Gestionnaire de serveur → Outils → Gestion de l'ordinateur → Gestion des disques**.

Attention

Un pourcentage seul ne dit pas l'urgence : 5 % de 100 Go = 5 Go, mais 5 % de 20 To = 1 To. Note la **valeur en Go** et l'**heure** de la mesure : l'évolution compte autant que la valeur.

3 Lire les quotas

Un **quota*** limite la taille d'un **dossier**, pas du disque. Un dossier peut donc refuser d'écrire alors que le disque a de la place. Tu vérifies si un quota explique l'alerte. Graphique : **Gestionnaire de serveur → Outils → Gestionnaire de ressources du serveur de fichiers → Gestion de quota → Quotas**, colonne Utilisation. En PowerShell :

Machine : SRV-DC01 | **Compte :** JPCONSULTING\admin.domaine | **Outil :** PowerShell (administrateur)

```
Get-FsrmQuota | Select-Object Path, @{n='LimiteGo';e={[math]::Round($_.Size/1GB,2)}},
@{n='UtiliseGo';e={[math]::Round($_.Usage/1GB,2)}}, SoftLimit
```

Je dois voir

Une ligne par quota : le dossier, sa limite, ce qu'il utilise. `SoftLimit False` = quota **inconditionnel*** : au-delà de la limite, l'écriture est refusée.

Si `UtiliseGo` est proche de `LimiteGo` : ce dossier va refuser les écritures même si le volume a de la place. Note-le dans le ticket.

Attention

Un quota qui n'est pas plein **n'explique pas** la saturation du volume, et l'absence de quota ne dit rien sur l'endroit où l'espace est parti. L'étape 4 sert à le trouver.

4 Trouver les gros fichiers

Premier essai à la main : les 10 plus gros fichiers du volume, avec leur **propriétaire*** et leurs dates.

Machine : SRV-DC01 | **Compte :** JPCONSULTING\admin.domaine | **Outil :** PowerShell (administrateur)

```
Get-ChildItem E:\ -Recurse -File -ErrorAction SilentlyContinue | Sort-Object Length -
Descending | Select-Object -First 10 | Select-Object FullName,
@{n='TailleMo';e={[math]::Round($_.Length/1MB)}}, @{n='Proprietaire';e={(Get-Acl -
LiteralPath $_.FullName).Owner}}, LastWriteTime, CreationTime
```

Lire la commande

`Get-ChildItem E:\ -Recurse -File` : liste **tous les fichiers** (`-File`) de E: et de ses sous-dossiers (`-Recurse`).

`-ErrorAction SilentlyContinue` : n'affiche pas les erreurs. Un dossier illisible n'est alors **pas compté** : note-le.

`Sort-Object Length -Descending` : trie du plus gros au plus petit. `Select-Object -First 10` : garde les 10 premiers.

`Get-Acl ... .Owner` : lit le propriétaire du fichier. `LastWriteTime` : date de dernière **modification** ; `CreationTime` : date de **création**.

Je dois voir

Dix lignes, de la plus grosse à la plus petite. **Additionne** les tailles des fichiers qui se ressemblent (même dossier, même nom, même date) : c'est ce total, pas un fichier seul, qui explique l'espace perdu. Exemple du lab : 9 fichiers de 10 240 Mo = 92 160 Mo, soit environ 90 Go.

Attention

Le propriétaire n'est pas forcément la personne qui a déposé le fichier : une copie réseau appartient souvent à celui qui l'a copiée, un fichier restauré à l'administrateur. Présente-le comme une **indication**, jamais comme une preuve.

`TailleMo` vaut 0 pour un très petit fichier (moins de 0,5 Mo) : ce n'est pas une erreur. Une date ou un chemin coupé dans la console reste complet dans le CSV de l'étape 5.

5 Exporter un rapport

Taper une commande prouve que tu as regardé. Un **script*** refait la même chose à l'identique et laisse deux fichiers **CSV*** datés à joindre au ticket. Celui-ci est en **lecture seule : il lit et exporte, il ne supprime et ne modifie rien.** Il suit quatre temps : paramètres, vérifications, traitement, export et message de fin.

Lire la commande

Il produit deux CSV dans **`C:\Outils\Rapports`** : **`gros-fichiers-...csv`** (les plus gros fichiers, avec taille, propriétaire, dates) et **`tailles-dossiers-...csv`** (la taille de chaque dossier de premier niveau).

Trois paramètres, tous facultatifs : **`-Racine`** (où chercher, **`E:\`** par défaut), **`-Nombre`** (combien de gros fichiers, 30 par défaut), **`-Sortie`** (où écrire les CSV).

Ouvre ce script en le lisant : tu dois pouvoir dire, avant de le lancer, ce que fait chaque bloc.

Ouvre le Bloc-notes, colle le script, puis **Fichier → Enregistrer sous…** : dossier **`C:\Outils`**, nom **`Rapport-Espace-Partage.ps1`**, type **Tous les fichiers**.

```
# Rapport-Espace-Partage.ps1 - LECTURE SEULE : ne supprime rien
# Exporte les plus gros fichiers et la taille des dossiers de premier niveau.
param(
    [string]$Racine = 'E:\',
    [int]$Nombre = 30,
    [string]$Sortie = 'C:\Outils\Rapports'
)
# 1. Verifications
if (-not (Test-Path -LiteralPath $Racine)) {
    Write-Error "Racine introuvable : $Racine"
    exit 1
}
New-Item -ItemType Directory -Path $Sortie -Force | Out-Null
$h = Get-Date -Format 'yyyyMMdd-HHmm'
$ea = 'SilentlyContinue'
# 2. Traitement : les plus gros fichiers
$fichiers = Get-ChildItem -LiteralPath $Racine -Recurse -File -ErrorAction $ea |
    Sort-Object Length -Descending |
    Select-Object -First $Nombre |
    ForEach-Object {
        [pscustomobject]@{
            Chemin       = $_.FullName
            TailleMo     = [math]::Round($_.Length / 1MB, 1)
            Proprietaire = (Get-Acl -LiteralPath $_.FullName -ErrorAction $ea).Owner
            Modifie      = $_.LastWriteTime
            Cree         = $_.CreationTime
        }
    }
# 3. Traitement : taille de chaque dossier de premier niveau
$dossiers = Get-ChildItem -LiteralPath $Racine -Directory -ErrorAction $ea |
    ForEach-Object {
        $sous = Get-ChildItem -LiteralPath $_.FullName -Recurse -File -ErrorAction $ea
        $somme = ($sous | Measure-Object Length -Sum).Sum
        [pscustomobject]@{
            Dossier  = $_.FullName
            TailleMo = [math]::Round($somme / 1MB, 1)
        }
    } |
    Sort-Object TailleMo -Descending
# 4. Export et message de fin
$f1 = Join-Path $Sortie "gros-fichiers-$h.csv"
$f2 = Join-Path $Sortie "tailles-dossiers-$h.csv"
$fichiers | Export-Csv -Path $f1 -NoTypeInformation -Encoding UTF8 -Delimiter ';'
$dossiers | Export-Csv -Path $f2 -NoTypeInformation -Encoding UTF8 -Delimiter ';'
Write-Output "Rapports : $f1 et $f2"
```

On teste toujours sur un petit dossier d'abord. Puis, en PowerShell administrateur :

Machine : SRV-DC01 | **Compte :** JPCONSULTING\admin.domaine | **Outil :** PowerShell (administrateur)

```
C:\Outils\Rapport-Espace-Partage.ps1 -Racine E:\Commun -Nombre 5
```

Je dois voir

Une ligne : `Rapports : C:\Outils\Rapports\gros-fichiers-AAAAMMJJ-HHMM.csv et C:\Outils\Rapports\tailles-dossiers-AAAAMMJJ-HHMM.csv` (ici AAAAMMJJ-HHMM est la date et l'heure du lancement, écrites par le script : rien à remplacer).

Ouvre les deux fichiers dans `C:\Outils\Rapports` (Excel, ou le Bloc-notes s'il n'y en a pas) : une ligne par fichier ou par dossier, tailles cohérentes avec l'Explorateur.

Quand c'est bon, relance **sans** les options : `C:\Outils\Rapport-Espace-Partage.ps1` (tout le volume E:).

Attention

PowerShell refuse de lancer le script (**stratégie d'exécution***) : lis le message et ne change aucun réglage. Colle plutôt le script directement dans la console.

`Racine introuvable` : chemin faux. Un CSV vide : droits insuffisants, relance en administrateur.

Les CSV sont sur le serveur. Pour les joindre au ticket GLPI, il faut d'abord les **transférer** sur le poste depuis lequel tu ouvres GLPI : dans la console VMware du serveur, **glisse-dépose** le fichier sur le Bureau du poste (VMware Tools). Vérifie que l'extension est bien `.csv`.

Dans le ticket GLPI : **Répondre**, texte explicatif, zone **Fichier(s)** (**Sélect. fichiers** ou glisser-déposer, 20 Mio maximum), puis **Ajouter**. Le fichier apparaît sous le suivi.

6 Informer et faire décider

Informer sans inventer. Donne les faits mesurés : espace libre, dossier concerné, total des fichiers en cause. Pour annoncer un **délai avant saturation***, il faut un rythme **mesuré** : espace libre ÷ espace consommé par jour. Pour le mesurer, refais la mesure de l'étape 2 plus tard, ou compare les dates de création des gros fichiers.

Attention

Si les gros fichiers portent **la même date**, il n'y a **pas de rythme mesurable** : n'annonce aucun délai. Écris-le tel quel (« pas de rythme mesurable : les fichiers ont tous été créés le même jour ») et propose de refaire la mesure le lendemain. Un délai deviné est pire que pas de délai.

Qui décide ? Celui qui est responsable des données du dossier concerné :

Dossier qui occupe la place	Qui décide
`E:\Commun`	sam.plante
`E:\Informatique`	ray.boot
Tout autre dossier (hors Commun et Informatique)	N3 ou administrateur : tu lui transmets le dossier, les faits et les CSV

Dans le ticket, dans cet ordre : **Répondre → Ajouter un document** (les deux CSV, une fois transférés), puis **Demander une validation** à la personne qui décide, puis **Mettre en attente**.

Message à la personne qui décide (validation GLPI)

Bonjour <PRÉNOM>,

Le <DATE> à <HEURE>, le volume des partages (E:) était occupé à <X> % : il reste <X> Go libres sur 100 Go.

Le dossier <NOM_DU_DOSSIER> occupe <X> Go, dont <N> fichiers de même nature (<NOM_DES_FICHIERS>, <X> Go au total). <PHRASE_SUR_LE_RYTHME : un rythme mesuré, ou « pas de rythme mesurable »>.

Les deux rapports sont joints à ce ticket. Nous ne supprimons rien sans votre accord écrit.

Pouvez-vous nous indiquer, pour chaque fichier : à garder, à archiver ailleurs, ou à supprimer ?

Cordialement,

7 Agir et prouver

1. Vérifie qu'une sauvegarde* existe. C'est elle qui dit si la suppression sera réversible :

Machine : SRV-DC01 | **Compte :** JPCONSULTING\admin.domaine | **Outil :** PowerShell (administrateur)

```
wbadmin get versions
```

Je dois voir

Une ou plusieurs versions, avec leur date et heure en **temps universel*** (UTC : recopie-les telles quelles) et une ligne « Sauvegardable(s) » qui **contient** le volume E:.

Compare l'heure de la **dernière version** avec l'heure de **création** des fichiers à supprimer (étape 4, `CreationTime`, en heure locale : convertis avant de comparer).

Pourquoi

Si la dernière version est **antérieure** à la création des fichiers, aucune sauvegarde ne les contient : leur suppression est **irréversible**. Dans ce cas, l'accord écrit de la personne qui décide est la seule garantie : vérifie-le avant d'agir.

Si une version est postérieure à leur création, ils sont récupérables (playbook Exploitation, runbook Sauvegarde et restauration) : dis-le à la personne qui décide.

2. Supprime seulement ce que la décision écrite autorise. D'abord une **simulation** : `-WhatIf` affiche ce qui serait supprimé et ne supprime **rien**.

Machine : SRV-DC01 | **Compte :** JPCONSULTING\admin.domaine | **Outil :** PowerShell (administrateur)

```
Remove-Item -LiteralPath '<CHEMIN_DU_FICHIER>' -WhatIf
```

Plusieurs fichiers numérotés (exemple du lab : `export_2.bak` à `export_9.bak` dans `E:\Temp_Migration`, `export_1.bak` conservé) :

```
2..9 | ForEach-Object { Remove-Item -LiteralPath "E:\Temp_Migration\export_$_.bak" -WhatIf }
```

Lire la commande

`Remove-Item` : supprimer. `-LiteralPath` : le chemin est pris **tel quel**, sans joker : on ne peut pas supprimer par erreur plus que ce qu'on a écrit.

`2..9` : les nombres de 2 à 9. `ForEach-Object { ... }` : refait la commande pour chacun, `$_` valant tour à tour 2, 3, 4…

`-WhatIf` : « que se passerait-il si ». Rien n'est supprimé.

Je dois voir

La liste des fichiers prévus à la suppression. Elle doit être **identique, fichier pour fichier,** à la décision écrite. Un fichier en trop (ou un fichier à conserver dans la liste) : **stop**.

Si la liste est conforme, **même commande sans `-WhatIf`**. Puis prouve le résultat :

```
Get-Volume -DriveLetter E | Select-Object DriveLetter,
@{n='LibreGo';e={[math]::Round($_.SizeRemaining/1GB,1)}}
```

L'espace libre doit être remonté de la taille des fichiers supprimés (exemple du lab : 8,8 Go → 88,8 Go, soit +80 Go = 8 × 10 Go). L'alerte Zabbix passe en **Résolu** après son prochain relevé.

3. Dans GLPI, dans cet ordre. D'abord une **tâche** (le détail technique), puis la **solution**. Le demandeur approuve la solution ; dans ce lab, le N3 ne peut que clore.

Texte de la tâche (GLPI)

Tâche (pour le N3, avec les commandes) : `Get-Volume` avant : <X> Go libres. `wbadmin get versions` : dernière version <DATE_HEURE_UTC>, antérieure ou postérieure à la création des fichiers. Simulation `-WhatIf` conforme à la décision du <DATE>. Suppression de <LISTE>. `Get-Volume` après : <X> Go libres. <Fichier conservé et jusqu'à quand>.

Texte de la solution (GLPI), lisible par le demandeur

Bonjour <PRÉNOM>,

Suite à votre accord du <DATE>, nous avons supprimé <DESCRIPTION_EN_MOTS_SIMPLES>. Le volume des partages a maintenant <X> Go libres (il en avait <X>) et l'alerte est résolue.

<CE_QUI_EST_CONSERVÉ_ET_JUSQU'À_QUAND>. Merci de nous confirmer que tout est en ordre.

Lexique

Les mots marqués d'un astérisque (*) dans ce runbook.

Urgence / impact

L'urgence dit **dans quel délai** il faut agir ; l'impact dit **combien de personnes** sont touchées. Les deux donnent la priorité.

Quota (FSRM)

Limite de taille posée sur un dossier. **FSRM** (File Server Resource Manager) est l'outil de Windows Server qui gère quotas et filtres.

Quota inconditionnel

L'écriture est **refusée** au-delà de la limite. Conditionnel : elle passe, on est seulement prévenu.

Propriétaire

Le compte propriétaire du fichier (droits NTFS). Une indication de qui l'a créé ou copié, pas une preuve.

Script / CSV

Un script est une suite de commandes enregistrée dans un fichier. Un CSV est un tableau en texte, qui s'ouvre dans Excel.

Stratégie d'exécution

Le réglage de PowerShell qui décide quels scripts il accepte de lancer.

Saturation

Le moment où le disque est plein et refuse toute écriture.

Sauvegarde

Copie de secours prise à heure fixe, planifiée : elle permet de revenir en arrière après une suppression, mais seulement pour ce qui existait au moment de la copie.

Temps universel (UTC)

L'heure de référence mondiale. Elle diffère de l'heure locale de 1 h (hiver) ou 2 h (été).

Notes

RUNBOOK · PLAYBOOK SERVEURS ET SERVICES

Virtualisation et matériel

Les hyperviseurs (VMware Workstation, Proxmox) et le matériel qui les porte.

Cas traités dans ce runbook

INCIDENT Des machines virtuelles tombent en écran bleu (0x124).....36

Statut : non validé

INCIDENT · VIRTUALISATION ET MATÉRIEL

Des machines virtuelles tombent en écran bleu (0x124)

Niveau	N2. Matériel de l'hôte défaillant : N3.
Où	la VM touchée (compte **`JPCONSULTING\admin.domaine`**) et le PC hôte **`HOTE-VMWARE`** (administrateur de l'hôte, VMware Workstation).
GLPI	type Incident · catégorie : Serveurs et services › Virtualisation et matériel. *Statut : non validé*

Ce que tu reçois et ce qu'on attend de toi

Une ou plusieurs VM Windows s'arrêtent d'un coup et redémarrent, avec un code **0x124***. Dans une VM, le matériel est simulé : le coupable le plus fréquent est le **disque de l'hôte**, trop lent à répondre sous charge.

Ton travail : confirmer l'arrêt brutal, lire le code, chercher le point commun entre les VM tombées, corriger le stockage, et vérifier **sur plusieurs jours**.

Ce que tu reçois : « Le DC et la VM WSUS ont redémarré seuls cette nuit, en même temps. »

Regle d'or

Une correction n'est prouvée que par la **disparition du symptôme sur plusieurs jours**, sous charge, pas par une heure sans plantage.



Les étapes de ce cas.

1 Confirmer l'arrêt brutal

Machine : La VM touchée | **Compte :** JPCONSULTING\admin.domaine | **Outil :** PowerShell (administrateur)

```
Get-WinEvent -FilterHashtable @{LogName='System'; Id=41,6008,1074,1001} -MaxEvents 20
| Format-Table TimeCreated, Id, ProviderName -AutoSize
```

Lire la commande

41 : redémarrage sans arrêt propre. **6008** : arrêt précédent inattendu. **1074** : arrêt demandé (mise à jour, administrateur). **1001** : code de l'écran bleu.

Je dois voir

41 et 6008 **sans** 1074, puis un 1001 avec **`0x00000124`** : arrêt brutal confirmé. Note le **premier paramètre** du 1001 : **`0x10`** = erreur remontée par un pilote ; **`0x0`** = processeur (escalade).

Ticket : **Incident**, catégorie **Serveurs et services › Virtualisation et matériel**, priorité **Haute** si le DC est touché.

2 Chercher le point commun

Machine : HOTE-VMWARE (PC hôte, 192.168.20.70) | **Compte :** administrateur de l'hôte | **Outil :** PowerShell (administrateur)

```
Get-PhysicalDisk | Select-Object FriendlyName, MediaType, BusType, HealthStatus, Size
```

Je dois voir

L'état de santé des disques de l'hôte, et leur type. Croise avec l'emplacement des VM tombées : sont-elles toutes sur le **même disque** ?

Pourquoi

Cas vécu (STAR 46) : le DC, la VM WSUS et le client 1 étaient sur le disque `D:` de l'hôte, un **SSD SATA sans cache** rempli à 71 %. PFSENSE01, resté stable, avait un disque virtuel d'un autre type. Le vidage mémoire (WinDbg, `!analyze -v`) montrait le pilote `stornvme` : le contrôleur NVMe virtuel n'avait plus répondu.

3 Mesurer le disque de l'hôte

Machine : HOTE-VMWARE (PC hôte, 192.168.20.70) | **Compte :** administrateur de l'hôte | **Outil :** PowerShell

```
Get-Volume | Where-Object DriveLetter | Select-Object DriveLetter, FileSystemLabel,
@{n='LibreGo';e={[math]::Round($_.SizeRemaining/1GB)}},
@{n='TotalGo';e={[math]::Round($_.Size/1GB)}}
```

Je dois voir

Règle du lab : garder **au moins 20 à 25 % libres sur `D:`**. En dessous, un SSD sans cache ralentit fortement sous charge.

4 Corriger le stockage

- **Un seul changement à la fois**, puis on observe.
- Libérer de la place sur le disque de l'hôte (archiver les VM inutilisées sur un autre disque), supprimer les instantanés inutiles.
- Déplacer la VM critique (le DC d'abord) vers le disque NVMe, VM éteinte ; au démarrage, répondre **I Moved It** (pas *I Copied It*, qui change l'identité et l'adresse MAC).

Attention

Ne modifie jamais les lignes `encryption.*` du fichier `.vmx` : la VM a un TPM virtuel, ces lignes protègent sa clé.

5 Vérifier sur plusieurs jours

Quand	Vérifier
Tout de suite	les VM démarrent ; pour le DC : `dcdiag /q`
Sous charge	relancer l'opération lourde qui précédait les pannes : aucun arrêt
Chaque jour pendant une semaine	`Get-WinEvent -FilterHashtable @{LogName='System'; Id=1001} -MaxEvents 5` : rien de nouveau

Texte de la tâche (GLPI)

Arrêts brutaux de <VM> le <DATE> (41 + 6008 sans 1074 ; 1001 code 0x124, paramètre 1 = <VALEUR>). Point commun : disque <DISQUE> de l'hôte, <X> % libres. Correction : <ACTION> le <DATE>. Suivi : aucun 1001 du <DATE> au <DATE>, y compris sous charge.

Texte de la solution (GLPI)

Les redémarrages inattendus des serveurs venaient d'un disque de l'hyperviseur saturé et trop lent. Le stockage a été corrigé ; aucun nouvel arrêt n'a été constaté depuis le <DATE>.

Lexique

Les mots marqués d'un astérisque (*) dans ce runbook.

0x124 (WHEA_UNCORRECTABLE_ERROR)

Écran bleu « erreur matérielle ». Dans une VM, il vient souvent d'un disque de l'hôte qui ne répond plus à temps.

Vidage mémoire

Copie de la mémoire écrite au moment du plantage (`C:\Windows\MEMORY.DMP`), lue avec WinDbg pour trouver le pilote en cause.

Notes