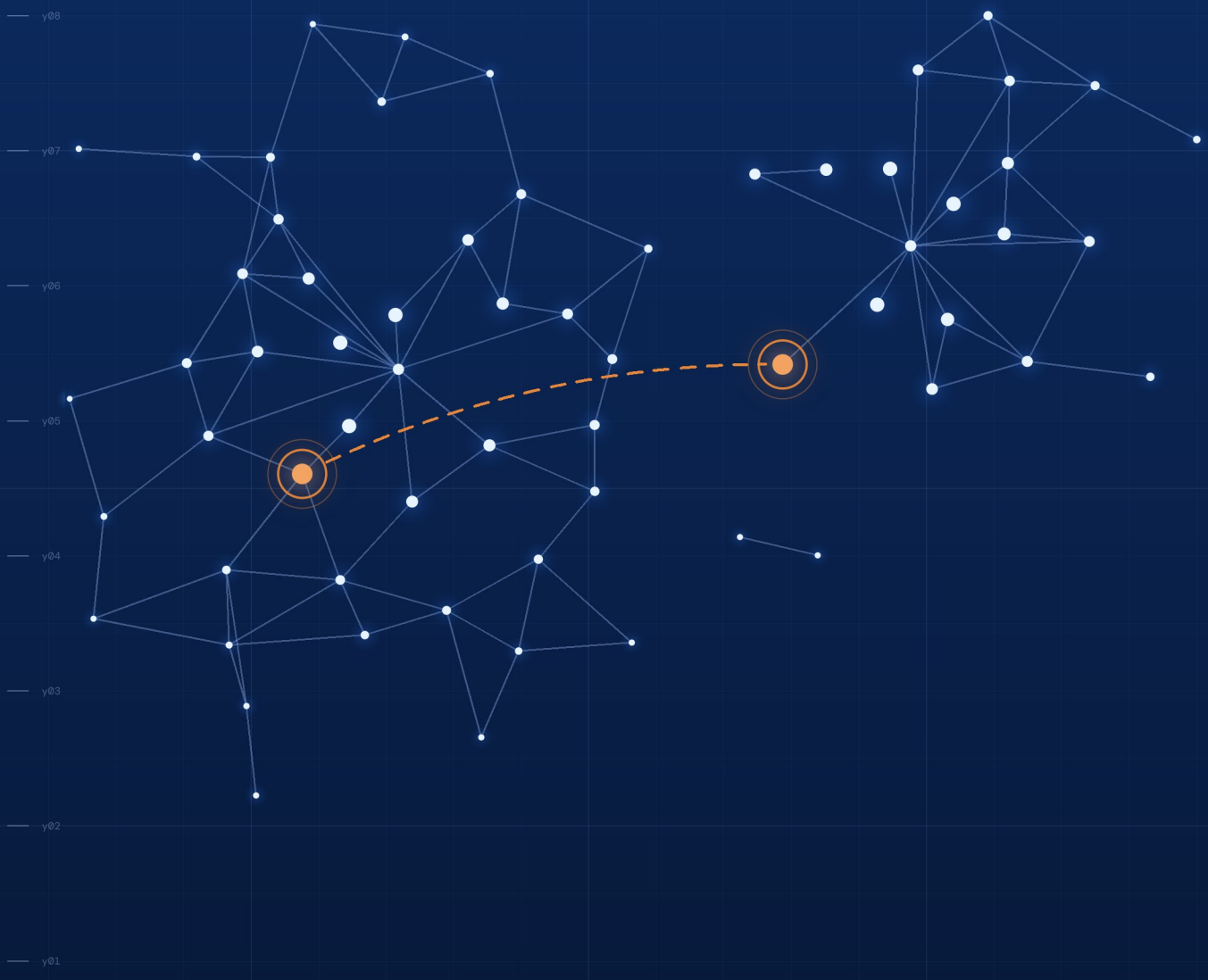


CATÉGORIE GLPI · JP CONSULTING

Playbook Exploitation

Les runbooks de la catégorie GLPI Exploitation

Jean-Philippe Rebischung

Sommaire

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

Sauvegarde et restauration **3**

Demande · Un dossier du partage a été supprimé par erreur 4

Supervision et journaux **11**

Incident · Un serveur Linux ne remonte plus dans Zabbix 12

Index par symptôme

Ce que je reçois	Runbook	Page
Un utilisateur : « j'ai supprimé un dossier du partage par erreur »	Sauvegarde et restauration	4
Une alerte Zabbix : « Zabbix agent is not available » sur un serveur Linux	Supervision et journaux	12

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 EXPLOITATION

Sauvegarde et restauration

Les sauvegardes du lab et la récupération de fichiers ou de dossiers perdus : copies instantanées et Sauvegarde Windows Server.

Cas traités dans ce runbook

DEMANDE Un dossier du partage a été supprimé par erreur.....4

Statut : non validé

DEMANDE · SAUVEGARDE ET RESTAURATION

Un dossier du partage a été supprimé par erreur

Niveau	N2. Lecture des copies par le N2 ; sauvegarde ancienne : 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 Demande · catégorie : Exploitation › Sauvegarde et restauration. *Statut : non validé*

Ce qui se passe et ce qu'on attend de toi

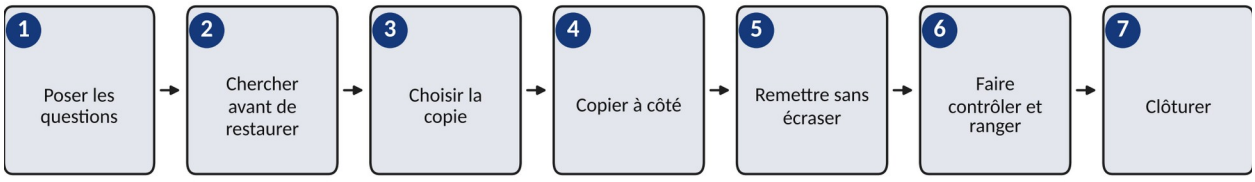
Un fichier supprimé sur un partage n'est pas dans la Corbeille du poste de l'utilisateur. Il reste pourtant des **copies du passé** : les copies instantanées* (onglet **Versions précédentes**) et la sauvegarde*. Chacune est une photo du disque à une heure précise. Tu récupères le dossier **tel qu'il était à cette heure**, jamais ce qui a été fait après.

Danger : pendant ce temps, des collègues ont pu continuer à travailler dans le même dossier, ou le recréer. On ne remet donc rien **par-dessus**.

Ce que tu reçois, par exemple : « Bonjour, j'ai supprimé par erreur un dossier du partage hier, pouvez-vous le récupérer ? » Le message ne dit ni le chemin exact, ni l'heure, ni si d'autres travaillent dedans : c'est à toi de le demander.

Regle d'or

On restaure **à côté**, jamais par-dessus. On copie ensuite dans le partage **seulement ce qui manque**. Le bouton « Restaurer » de l'onglet Versions précédentes remplace tout le dossier par l'ancienne version : on ne l'utilise pas.



Les sept étapes de ce cas.

1 Poser les questions

- Quel dossier, dans quel partage ? Le chemin exact, tel qu'il le voit (lecteur réseau et nom).
- Quand l'a-t-il supprimé (jour, heure approximative) ?
- Quels fichiers contenait-il, et lesquels avaient été créés ou modifiés **le jour même** ? Depuis quand le dossier existait-il ?
- D'autres personnes travaillent-elles dedans ? Y ont-elles ajouté des fichiers depuis ? Quelqu'un a-t-il recréé un dossier du même nom ?
- Est-il sûr de l'avoir **supprimé**, et pas déplacé par erreur dans un dossier voisin ?

Note les réponses dans le ticket : elles servent de **référence** aux étapes 2 et 3 (ce que le dossier devait contenir).

Ouvre le ticket (type Demande). **Urgence** : selon son échéance. **Impact** : le nombre de personnes qui travaillent dans ce dossier.

> **Attention**
>
> Ne promets rien encore. Tu ne sais pas si une copie existe, ni de quelle heure. Dis seulement : « Je regarde ce qui peut être récupéré et je reviens vers vous ».

2 Chercher avant de restaurer

Un dossier « supprimé » est parfois seulement glissé dans un dossier voisin. Cherche son nom dans tout le partage (remplace le nom ET le dossier de départ par ceux de la demande) :

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

```
Get-ChildItem E:\Commun -Recurse -Directory -Filter '*<NOM_DU_DOSSIER>*' -ErrorAction SilentlyContinue | Select-Object FullName
```

> **Je dois voir**
>
> **Aucun résultat** : le dossier n'existe plus. Passe à l'étape 3.
>
> **Un chemin affiché** : un dossier de ce nom existe. Cela ne prouve pas que ce soit le bon : quelqu'un a pu le **recréer** après la suppression. Regarde son **contenu** (commande ci-dessous) et compare-le avec ce que l'utilisateur t'a dit qu'il contenait (étape 1).

```
Get-ChildItem -LiteralPath '<CHEMIN_TROUVÉ>' -Recurse -File | Select-Object FullName, Length, LastWriteTime
```

> **Je dois voir**
>
> Le contenu d'origine est là (mêmes fichiers, mêmes dates) : le dossier a seulement changé de place. Dis-le à l'utilisateur : fin de ce runbook.
>
> Le dossier est vide, ou ne contient que des fichiers récents que l'utilisateur ne connaît pas : c'est un dossier recréé, **le travail de quelqu'un d'autre**. Ne touche à rien et passe à l'étape 3 : on ne restaurera pas par-dessus.

3 Choisir la copie

Deux sources de copies existent. Commence par les copies instantanées, plus rapides à lire :

Source	Quand elle est prise	À utiliser quand
Copie instantanée* de E: (Versions précédentes)	12:00 et 17:00, les jours où le serveur est allumé	La suppression est récente
Sauvegarde* Windows Server	À heure fixe planifiée (à relever avec `wbadmin get versions`)	Aucune copie instantanée ne convient. N3 : voir le bas de cette page

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

```
vssadmin list shadows /for=E:
```

Je dois voir

Une liste de copies. Pour chacune : l'**heure de création** (heure locale) et un chemin qui contient **`@GMT-AAAA.MM.JJ-HH.MM.SS`**.

Le chemin **`@GMT`** est en **temps universel*** (UTC) : **1 h de moins** que l'heure locale en heure d'hiver (depuis le changement d'heure d'octobre), **2 h de moins** en heure d'été. Exemple : une copie créée à 16:29:13 en heure locale d'hiver a pour chemin **`@GMT-2026.10.29-15.29.13`**. Recopie le chemin tel quel.

Pourquoi

Quelle copie choisir ? Il faut qu'elle ait été prise **après** la création des fichiers qu'on veut récupérer (sinon ils n'y sont pas) et **avant** la suppression (sinon le dossier n'y est plus). Parmi celles-ci, prends la plus récente. Ce qui a été fait entre cette copie et la suppression est **perdu** : dis-le à l'utilisateur maintenant.

Pour vérifier le contenu de la copie choisie (remplace la date par celle de ta copie, puis compare avec ce que l'utilisateur t'a décrit) :

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

```
Get-ChildItem '\\localhost\E$\@GMT-<AAAA.MM.JJ-HH.MM.SS>\Commun\<NOM_DU_DOSSIER>' -
Recurse -File | Select-Object FullName, Length, LastWriteTime
```

Je dois voir

Les fichiers que l'utilisateur t'a décrits sont là, **et pas ceux ajoutés après la copie**. Compare avec la liste de l'étape 1 et avec le dossier actuel (étape 2).

Attention

Utilise **PowerShell en administrateur**, pas l'Explorateur : sur le serveur, l'Explorateur normal se voit refuser l'accès à l'intérieur d'une copie (contrôle de compte d'utilisateur). Si une fenêtre propose « Continuer » pour obtenir un accès permanent, **ne clique pas** : elle ajoute ton compte aux droits du dossier.

Sur l'onglet **Versions précédentes** de l'Explorateur, les boutons sont **Ouvrir ▾** et **Restaurer ▾**. Pour ce runbook, n'utilise pas **Restaurer ▾** : il remplace le dossier.

Aucune copie ne convient ? Passe par la sauvegarde. Sur le serveur, **Gestionnaire de serveur › Outils › Sauvegarde Windows Server**, clique sur **Sauvegarde locale**, puis sur **Récupérer...** dans le volet **Actions**. L'**Assistant Récupération** déroule : **Mise en route** (**Ce serveur**) › **Sélectionner une date de sauvegarde** (jours en gras = sauvegardes disponibles ; le champ nommé **Durée** est l'heure) › **Sélectionner le type de récupération** (**Fichiers et dossiers**) › **Sélectionner les éléments à récupérer** (**Partages (E:)**, puis le dossier ; **Suivant** reste grisé tant qu'aucun élément n'est choisi) › **Spécifier les options de récupération** › **Confirmation**, puis **Récupérer**.

À la page des options : destination **Autre emplacement** (bouton **Parcourir**, vers le dossier de travail de l'étape 4), choix **Créer des copies pour avoir les deux versions**, case **Restaurer les autorisations de la liste contrôle d'accès...** cochée. Aucun réglage n'est appliqué avant le clic sur **Récupérer** : **Annuler** ferme l'assistant sans rien restaurer.

4 Copier à côté

Crée un dossier de travail **hors des partages** (remplace **`<N°_TICKET>`** par le numéro du ticket), puis copie-y le dossier depuis la copie :

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

```
New-Item -ItemType Directory -Path E:\Restauration-<N°_TICKET>
```

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

```
robocopy '\\localhost\E$\@GMT-<AAAA.MM.JJ-HH.MM.SS>\Commun\<NOM_DU_DOSSIER>' 'E:\
Restauration-<N°_TICKET>\<NOM_DU_DOSSIER>' /E /COPY:DAT
```

Lire la commande

`robocopy source destination` : copie un dossier. **`/E`** : avec tous ses sous-dossiers. **`/COPY:DAT`** : copie les données (**D**), les attributs (**A**) et les dates (**T**).

Les droits de la destination viennent du dossier parent (héritage*) : c'est ce qu'on veut, on les contrôlera à l'étape 6.

Je dois voir

Un tableau de synthèse à la fin : lignes **Répertoires** et **Fichiers**, colonnes **Total, Copiés, Ignorés, Non concordance, ÉCHEC, Extras**. La colonne **ÉCHEC** doit être à **0** sur les deux lignes.

Ouvre **`E:\Restauration-<N°_TICKET>\<NOM_DU_DOSSIER>`** dans l'Explorateur : les fichiers sont là, avec les dates d'origine.

5 Remettre sans écraser

D'abord un **essai à blanc** : **`/L`** liste ce qui serait copié et ne copie **rien**. Les options **`/XC /XN /XO`** excluent tout fichier qui existe déjà avec une différence : seuls les fichiers **manquants** seront copiés.

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

```
robocopy 'E:\Restauration-<N°_TICKET>\<NOM_DU_DOSSIER>' 'E:\Commun\
<NOM_DU_DOSSIER>' /E /XC /XN /XO /L
```

Je dois voir

Les lignes **Nouveau fichier** : ce sont les fichiers qui manquent dans le partage. Ce sont eux, et eux seuls, qui seront copiés.

Un fichier du partage qui n'existe pas dans ta copie (celui d'un collègue) est signalé **Fichier SUPPL.** et compté dans la colonne **Extras** : il n'est pas touché. C'est normal.

Si un fichier d'un collègue apparaît en **Nouveau fichier** ou en copie à écraser : **stop**, demande à l'utilisateur.

Si la liste est conforme, **même commande sans `/L`** :

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

```
robocopy 'E:\Restauration-<N°_TICKET>\<NOM_DU_DOSSIER>' 'E:\Commun\
<NOM_DU_DOSSIER>' /E /XC /XN /XO
```

6 Faire contrôler et ranger

Pourquoi contrôler les droits ? Un fichier remis dans un dossier reprend les droits de ce dossier (héritage*). Si le dossier n'a pas les bons droits, son équipe ne verra pas ses fichiers. Le test : **les droits du dossier remis doivent être les mêmes que ceux de son dossier parent.** Deux commandes, une sur chacun :

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

```
icacls 'E:\Commun'
```

```
icacls 'E:\Commun\<NOM_DU_DOSSIER>'
```

Lire la commande

`icacls` affiche les droits d'un dossier : une ligne par groupe ou compte, avec une lettre. **`F`** = contrôle total, **`M`** = modification, **`RX`** = lecture et exécution.

`DL_` : groupe **de ressource** du modèle AGDLP (domain local). Les utilisateurs sont dans des groupes **`GG_`**, et ce sont les groupes **`DL_`** qui reçoivent les droits sur le dossier. Ici **`DL_Commun_L`** = lecture, **`DL_Commun_M`** = modification.

`(I)` = droit **hérité** du dossier parent. **`(OI)(CI)`** = le droit s'applique aux fichiers et sous-dossiers.

Je dois voir

Sur le dossier parent comme sur le dossier remis, les mêmes entrées : le système et les administrateurs en contrôle total (**`F`**), **`DL_Commun_L`** en **`RX`**, **`DL_Commun_M`** en **`M`**. Sur le dossier remis, chaque ligne est précédée de **`(I)`** : c'est l'héritage qui a fait son travail.

Une entrée en plus sur le parent (par exemple un compte administrateur nominatif) n'est pas un problème tant qu'elle est aussi sur le dossier remis.

Une entrée sans **`(I)`** ou un groupe **`DL_`** absent sur le dossier remis : droits différents du parent, **ne rends pas le dossier** et escalade au N3.

Puis l'utilisateur **ouvre** ses fichiers : contenu et date corrects, pas seulement le nom. Un collègue confirme que son travail est intact. Après sa **confirmation écrite**, supprime le dossier de travail : d'abord la simulation, puis la suppression (relis le chemin avant d'appuyer sur Entrée).

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

```
Remove-Item -LiteralPath 'E:\Restauration-<N°_TICKET>' -Recurse -WhatIf

Remove-Item -LiteralPath 'E:\Restauration-<N°_TICKET>' -Recurse

Test-Path -LiteralPath 'E:\Restauration-<N°_TICKET>'
```

Je dois voir

`-WhatIf` : le dossier de travail, et lui seul, est annoncé comme supprimé. Après la vraie suppression, **`Test-Path`** répond **False**.

7 Clôturer

Dans GLPI, dans cet ordre : d'abord une **tâche** (le détail technique), puis la **solution**, courte et lisible par l'utilisateur. Le demandeur approuve la solution ; dans ce lab, le N3 ne peut que clore.

Texte de la tâche (GLPI)

Dossier **`<CHEMIN_DU_DOSSIER>`** supprimé le <DATE> vers <HEURE>. Copie utilisée : **`<CHEMIN_GMT_RECOPIÉ_TEL_QUEL>`**. Dossier de travail : **`E:\Restauration-<N°_TICKET>`**.

Commandes : **`vssadmin list shadows /for=E:`**, contrôle du contenu de la copie, **`robocopy … /E /COPY:DAT`**, essai à blanc **`robocopy … /L`**, **`robocopy …`**, **`icacls`** (parent et dossier remis), **`Remove-Item`** du dossier de travail.

Fichiers remis : <LISTE>. Fichiers non récupérables : <LISTE ou « aucun »>. Fichiers du collègue : intacts. Droits identiques au parent. Durée réelle : <DURÉE>.

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

Bonjour <PRÉNOM>,

Votre dossier <NOM_DU_DOSSIER> a été remis à sa place à partir de la copie du <JOUR> à <HEURE>. Les <N> fichiers sont revenus ; le travail ajouté depuis par vos collègues est intact. Ce qui a été fait entre <HEURE> et la suppression n'a pas pu être récupéré.

Merci de vérifier le contenu et de nous confirmer que tout est en ordre.

Lexique

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

Copie instantanée (Versions précédentes)

Photo du disque prise à heure fixe par Windows. L'onglet **Versions précédentes** de l'Explorateur la montre à l'utilisateur.

Sauvegarde

Copie de secours planifiée : plus lourde à lire, elle sert quand aucune copie instantanée ne convient.

Temps universel (UTC / GMT)

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

Héritage

Un dossier reprend les droits de son dossier parent. Un dossier recopié au bon endroit retrouve donc les droits du partage.

AGDLP / groupe DL_

Méthode de gestion des droits : les comptes (**A**) vont dans des groupes globaux (**G**), qui vont dans des groupes de domaine local (**DL**), qui reçoivent les permissions (**P**). Les groupes `DL_` sont ceux qu'on voit dans `icacls`.

robocopy

Commande Windows de copie de dossiers : elle sait ne copier que ce qui manque.

RUNBOOK · PLAYBOOK EXPLOITATION

Supervision et journaux

Les alertes de Zabbix et la collecte des journaux : un hôte muet, des données qui n'arrivent plus.

Cas traités dans ce runbook

INCIDENT Un serveur Linux ne remonte plus dans Zabbix.....12

Statut : non validé

Un serveur Linux ne remonte plus dans Zabbix

Niveau	N2. Modification d'Ansible : N3.
Où	**`SRV-ZABBIX01`** (**`192.168.20.62`**) et l'hôte en alerte, en SSH depuis le PC hôte, compte **`admin.linux`** (sudo).
GLPI	type Incident · catégorie : Exploitation › Supervision et journaux.
	Statut : non validé

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

Zabbix interroge les machines à intervalles réguliers. En **mode passif***, c'est le serveur Zabbix qui frappe à la porte de l'agent (port **10050**). Quand personne ne répond, l'hôte passe au rouge : « Zabbix agent is not available ».

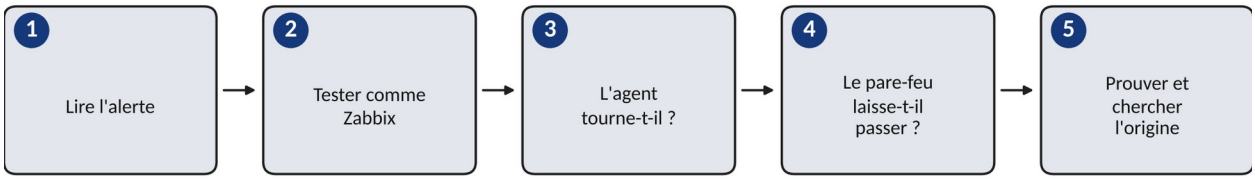
Ton travail : trouver **où** la demande s'arrête (pare-feu du réseau, pare-feu local, agent, SELinux), corriger seulement ce qui est prouvé, et dire pourquoi c'est arrivé.

Ce que tu reçois : une alerte Zabbix, sans utilisateur, par exemple « Linux: Zabbix agent is not available (for 3m) » sur un serveur Linux.

Regle d'or

On ne touche à rien avant de savoir de quel côté ça casse. Une preuve par couche, dans l'ordre.

On n'ouvre jamais un port à tout le monde pour « tester » : la règle se limite à l'adresse du serveur Zabbix.



Les étapes de ce cas.

1 Lire l'alerte

Interface Zabbix (HTTPS, depuis le PC hôte) : **Surveillance → Problèmes**. Relève l'hôte, le message mot pour mot, la gravité et l'**heure de début**. Puis **Collecte de données → Hôtes** : sur la ligne de l'hôte, l'**Interface** **`IP:10050`** et un modèle sans « active » indiquent un agent **passif** ; le badge **ZBX** rouge dit que Zabbix ne le joint plus. Enfin **Surveillance → Dernières données** : la date de la dernière valeur dit quand le silence a commencé.

Attention

La machine est-elle **allumée** ? Les VM du lab ne sont pas permanentes : un hôte éteint donne exactement cette alerte.

Ticket : **Incident**, catégorie **Exploitation › Supervision et journaux**, titre « Agent Zabbix injoignable sur <HÔTE> », description = les faits relevés.

2 Tester comme Zabbix

Machine : SRV-ZABBIX01 (192.168.20.62) | **Compte :** compte sudo (admin.linux) | **Outil :** Bash (SSH depuis le PC hôte)

```
zabbix_get -s <IP_DE_L_HÔTE> -p 10050 -k agent.version
```

Lire la commande

`zabbix_get` interroge l'agent exactement comme le fait le serveur. **`-s`** : l'adresse de l'hôte ; **`-p 10050`** : le port de l'agent ; **`-k agent.version`** : la question posée.

Réponse	Ce que ça veut dire	Suite
`7.4.15` (une version)	L'agent répond : la route est libre	Vérifie l'adresse de l'interface, l'alerte se résout peut-être
`connection timed out`	Silence : la demande est jetée en route, un pare-feu est le premier suspect	Étapes 3 puis 4
`Connection refused`	La machine répond que personne n'écoute : agent arrêté ou autre port	Étape 3

3 L'agent tourne-t-il ?

Machine : L'hôte en alerte | **Compte :** compte sudo (admin.linux) | **Outil :** Bash

```
systemctl list-units 'zabbix*' --all
```

Je dois voir

`zabbix-agent.service loaded active running` : l'agent tourne. Le nom peut être **`zabbix-agent2`** selon l'hôte : utilise le nom affiché ici dans la suite.

`inactive dead` ou **`failed`** : lis le journal (**`sudo journalctl -u zabbix-agent -n 50 --no-pager`**) avant de le relancer.

Machine : L'hôte en alerte | **Compte :** compte sudo (admin.linux) | **Outil :** Bash

```
sudo ss -tlnp | grep 10050
```

Je dois voir

Deux lignes **`LISTEN`** sur **`0.0.0.0:10050`** et **`[::]:10050`** : l'agent attend bien sur le port 10050.

Aucune ligne : rien n'écoute (agent arrêté, ou autre port dans sa configuration).

Attention

`ss` voit l'intérieur de la machine seulement. Deux lignes **`LISTEN`** ne prouvent pas que le pare-feu laisse entrer.

4 Le pare-feu laisse-t-il passer ?

Machine : L'hôte en alerte (Debian) | **Compte :** compte sudo (admin.linux) | **Outil :** Bash

```
sudo ufw status
```

Je dois voir

Attendu : une ligne **`10050/tcp ALLOW 192.168.20.62`**. Aucune ligne pour le port 10050 depuis cette adresse : **`ufw`** jette la demande, d'où le *timed out*.

Sur AlmaLinux ou Rocky : **`sudo firewall-cmd --list-all`** (règle riche autorisant **`192.168.20.62`** vers 10050), puis **`getenforce`** et **`sudo ausearch -m avc -ts recent`** pour SELinux.

Correction, seulement si l'absence de règle est prouvée :

Machine : L'hôte en alerte (Debian) | **Compte :** compte sudo (admin.linux) | **Outil :** Bash

```
sudo ufw allow from 192.168.20.62 to any port 10050 proto tcp comment 'Zabbix agent passif'
```

Pourquoi

Sur **`SRV-SYSLOG01`**, **`SRV-ZABBIX01`** et GLPI, les règles de pare-feu sont décrites dans **Ansible** (**`durcissement.yml`**, exécuté depuis SRV-FREEIPA01). Une règle ajoutée à la main sera effacée au prochain passage si elle n'est pas aussi ajoutée dans les variables d'Ansible : signale-le au N3 dans le ticket.

5 Prouver et chercher l'origine

Machine : SRV-ZABBIX01 | **Compte :** compte sudo (admin.linux) | **Outil :** Bash

```
zabbix_get -s <IP_DE_L_HÔTE> -p 10050 -k agent.version
```

Je dois voir

La version revient. Une ou deux minutes après : badge **ZBX** vert, problème **Résolu** dans Surveillance → Problèmes, valeur récente dans Dernières données.

Cherche aussi **pourquoi** la règle avait disparu : une personne (journal des commandes **`sudo`**), Ansible, une réinitialisation.

Machine : L'hôte en alerte | **Compte :** compte sudo (admin.linux) | **Outil :** Bash

```
sudo journalctl _COMM=sudo --since today
```

Lire la commande

Chaque ligne donne l'heure, le compte et la commande lancée avec **`sudo`**. Une ligne **`COMMAND=/usr/bin/bash`** signale un shell administrateur ouvert : les commandes tapées dedans ne sont pas listées une à une.

Texte de la tâche (GLPI)

Alerte « <MESSAGE> » sur <HÔTE> à <HEURE>. **`zabbix_get`** : <RÉSULTAT>. Service : <ÉTAT>. **`ss`** : écoute sur 10050 <OUI/NON>. Pare-feu local : <CONSTAT>. Correction : <RÈGLE_AJOUTÉE> à <HEURE>. Preuve : **`zabbix_get`** rend <VERSION>, badge ZBX vert à <HEURE>. Origine de la suppression : <CONSTAT_JOURNAL_SUDO>. À reporter dans Ansible : <OUI/NON>.

Texte de la solution (GLPI)

L'agent de supervision de <HÔTE> n'était plus joignable : <CAUSE_EN_MOTS_SIMPLES>. La règle a été rétablie ; le serveur remonte de nouveau dans Zabbix depuis <HEURE>.

Lexique

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

Mode passif / actif

En passif, le serveur Zabbix interroge l'agent (port 10050 de la machine) ; en actif, l'agent envoie ses valeurs au serveur (port 10051 du serveur).

ufw / firewalld

Pare-feu local d'une machine Linux : `ufw` sur Debian et Ubuntu, `firewalld` sur AlmaLinux et Rocky. `ufw` jette en silence ce qui n'est pas autorisé.

SELinux

Contrôle d'accès de Red Hat, AlmaLinux et Rocky : il peut bloquer un programme même quand le pare-feu laisse passer.

Notes