BTS SIO — Option SISR — Fiche de Réalisation Professionnelle n°2

Suivi de migration inter-sites d'un poste client

Traçabilité GLPI & Supervision Zabbix au travers du tunnel IPsec

CL-WIN11-01 — Site A (10.11.3.x) → Site B (10.11.4.x) — SioSisr — sio.local

Contexte métier — Scénario de migration

L'entreprise `SioSisr` déplace physiquement le poste **CL-WIN11-01** du siège (`Site A — LAN 10.11.3.16/28`) vers l'agence distante (`Site B — LAN 10.11.4.16/28`). En tant qu'administrateur systèmes et réseaux, vous devez gérer ce changement **de bout en bout** : détecter la déconnexion, tracer la nouvelle configuration réseau, et rétablir la supervision.

Enjeu technique : Le poste rejoint un réseau distant — les outils d'administration (GLPI, Zabbix) ne peuvent atteindre ce nouveau sous-réseau que via le **tunnel IPsec IKEv2** interconnectant les deux sites. La procédure démontre la robustesse de cette architecture.

I. Objectif

Objectif principal : Démontrer que l'infrastructure d'administration de la PME SioSisr gère de manière cohérente la migration physique d'un poste client d'un site à l'autre, en s'appuyant sur le tunnel IPsec comme vecteur d'administration unifié.

Trois preuves attendues

① **Preuve de rupture :** Zabbix génère une alerte critique `unreachable` détectant l'absence du poste — surveillance active.

② **Preuve de traçabilité :** GLPI met à jour automatiquement la fiche du poste avec sa nouvelle adresse IP `10.11.4.x` — inventaire dynamique via le tunnel.

③ **Preuve de rétablissement :** Zabbix retrouve le poste après mise à jour de l'IP et affiche un statut `Resolved` — administration centralisée opérationnelle.

II. Prérequis

- **Tunnel IPsec IKEv2** opérationnel entre pfSense-01 (`10.10.101.3`) et pfSense-02 (`10.10.101.4`) — état **Established** visible dans `Status > IPsec`
- **Agent GLPI** installé sur `CL-WIN11-01` via GPO `DEPLOY-GLPI` — remontée vers `http://10.11.3.22/glpi`
- **Agent Zabbix** installé sur `CL-WIN11-01` — service actif, port `TCP 10050` ouvert, hôte déclaré dans Zabbix
- Adresse IP actuelle de `CL-WIN11-01` : `10.11.3.23` — Masque `/28` — Passerelle `10.11.3.17`
- **SRV-AD-02** (10.11.4.18) opérationnel au Site B — DHCP scope `10.11.4.23-10.11.4.30` actif
- Compte `Admin` Zabbix et `admin` GLPI disponibles
- Agent GLPI préconfiguré avec l'adresse du Proxy Squid (http://10.11.3.2:3127) via le registre/GPO pour autoriser la sortie web.

Vérification préalable du tunnel IPsec

Depuis `SRV-AD-01`, exécuter pour confirmer la connectivité inter-sites :

```
# Test de connectivité inter-sites via tunnel IPsec
ping 10.11.4.18 -n 4

# Résultat attendu : Reply from 10.11.4.18: bytes=32 time<5ms TTL=127
# Vérification DNS inter-sites
nslookup srv-ad-02.sio.local 10.11.3.18
```

III. Procédure — Les trois phases

PHASE 1

Alerte de déconnexion — Zabbix détecte la rupture

Phase 1 — Simulation du débranchement et constat Zabbix

1.1 — Simulation du débranchement réseau

Pour reproduire le scénario de migration, on simule la déconnexion physique du poste en désactivant l'interface réseau depuis `CL-WIN11-01`. Cette action prive Zabbix de sa capacité à interroger l'agent, déclenchant l'alerte `unreachable`.

1. Sur `CL-WIN11-01`, ouvrir une invite de commandes en tant qu'Administrateur
2. Identifier le nom de l'interface réseau :

```
# Lister les interfaces réseau
ipconfig /all

# Identifier le nom de l'adaptateur (ex: 'Ethernet0' ou 'Local Area
Connection')
```

3. Désactiver l'interface réseau (simulation débranchement câble) :

```
# Désactiver l'adaptateur réseau — remplacer 'Ethernet0' par le nom réel
netsh interface set interface "Ethernet0" admin=disabled

# Vérification : l'interface doit afficher 'Disconnected'
ipconfig /all
```

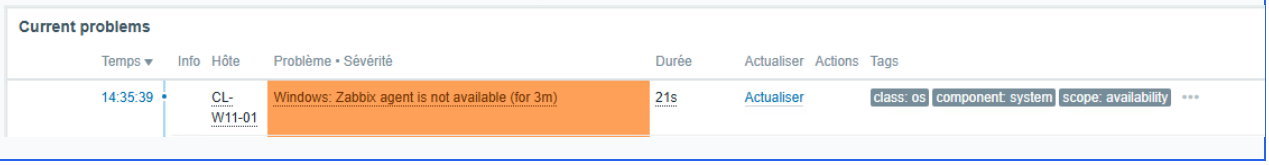
1.2 — Constat dans Zabbix de l'alerte critique

Navigation : `Monitoring > Problems (ou Dashboard > Problem hosts)`

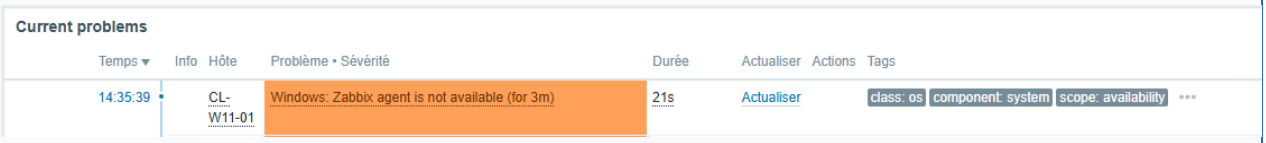
Après **5 à 10 minutes** (délai de détection Zabbix configurable), l'agent devient injoignable et Zabbix génère automatiquement un problème de sévérité **High / Average**.

4. Dans Zabbix, naviguer dans `Monitoring > Problems`
5. Observer l'apparition du problème `Zabbix agent on CL-WIN11-01 is unreachable` avec :
   - **Sévérité :** Average ou High (selon la configuration du template)
   - **Hôte :** `CL-WIN11-01`
   - **Statut :** `PROBLEM` affiché en rouge
   - **Durée :** temps écoulé depuis la détection
6. Naviguer dans `Monitoring > Latest data` pour `CL-WIN11-01` — les items affichent **No data** ou la dernière valeur avec un horodatage ancien

CAPTURE D'ÉCRAN N°1 — Dashboard ou Monitoring > Problems de Zabbix — L'alerte 'Zabbix agent on CL-WIN11-01 is unreachable' apparaît en rouge/orange. La colonne 'Duration' montre le temps depuis la déconnexion.



CAPTURE D'ÉCRAN N°2 — Zabbix — Monitoring > Problem hosts — CL-WIN11-01 apparaît avec un indicateur rouge. Preuve que la supervision détecte la déconnexion physique en moins de 10 minutes.



Analyse technique

Zabbix utilise le mode **Pull (Passif)** par défaut : le serveur Zabbix interroge activement l'agent sur le port `TCP 10050` toutes les `60 secondes`. Dès que l'agent ne répond plus à 3 tentatives consécutives, le trigger `Zabbix agent unreachable` se déclenche — délai total : environ 3 minutes.

PHASE 2

Reconnexion et inventaire dynamique — GLPI trace la nouvelle IP

Phase 2 — Reconnexion sur Site B et mise à jour GLPI

2.1 — Reconnexion du poste sur le réseau Site B

Le poste est physiquement rebranché sur le switch du Site B. Il obtient une adresse IP du scope DHCP de `SRV-AD-02` (`10.11.4.18`) et communique avec les serveurs d'administration **exclusivement via le tunnel IPsec**.

7. Réactiver l'interface réseau sur `CL-WIN11-01` (maintenant connectée au Site B) :

```
# Réactiver l'adaptateur réseau
netsh interface set interface "Ethernet0" admin=enabled

# Forcer le renouvellement DHCP — obtenir une IP du scope Site B
ipconfig /release
ipconfig /renew

# Vérifier la nouvelle adresse obtenue (doit être en 10.11.4.x)
ipconfig /all
```

8. Vérifier que le poste a obtenu une adresse dans la plage `10.11.4.23–10.11.4.30` avec :
   - **Passerelle :** `10.11.4.17` (pfSense-02)
   - **DNS primaire :** `10.11.4.18` (SRV-AD-02)
   - **DNS secondaire :** `10.11.3.18` (SRV-AD-01 via IPsec)

CAPTURE D'ÉCRAN N°3 — **Terminal CL-WIN11-01 — résultat de 'ipconfig /all' montrant la nouvelle adresse IP en 10.11.4.x, la passerelle 10.11.4.17 et les serveurs DNS. Preuve du changement de site réseau.**

```
C:\Users\Administrateur>ipconfig /all

Configuration IP de Windows

   Nom de l'hôte . . . . . . . . . . . : CL-W11-01
   Suffixe DNS principal . . . . . . . : sio.local
   Type de noeud. . . . . . . . . . . . : Hybride
   Routage IP activé . . . . . . . . . : Non
   Proxy WINS activé . . . . . . . . . : Non
   Liste de recherche du suffixe DNS.: sio.local

Carte Ethernet Ethernet0 :

   Suffixe DNS propre à la connexion. . . :
   Description. . . . . . . . . . . . . . : Intel(R) 82574L Gigabit Network Connection
   Adresse physique . . . . . . . . . . . : 00-50-56-95-68-9C
   DHCP activé. . . . . . . . . . . . . . : Non
   Configuration automatique activée. . . : Oui
   Adresse IPv4. . . . . . . . . . . . . .: 10.11.4.23(préféré)
   Masque de sous-réseau. . . . . . . . . : 255.255.255.240
   Passerelle par défaut. . . . . . . . . : 10.11.4.17
   Serveurs DNS. . .  . . . . . . . . . . : 10.11.4.18
                                 10.11.3.18
   NetBIOS sur Tcpip. . . . . . . . . . . : Activé

C:\Users\Administrateur>
```

2.2 — Forçage de l'inventaire GLPI

Par défaut, l'agent GLPI s'exécute à l'intervalle défini par la GPO (généralement au démarrage). Pour démontrer la mise à jour en temps réel pendant la procédure, on force manuellement l'inventaire.

1. Sur `CL-WIN11-01`, ouvrir PowerShell en tant qu'Administrateur et exécuter :

```
# Forcer l'inventaire GLPI immédiat vers le serveur SRV-GLPI
# L'agent contacte SRV-GLPI (10.11.3.22) via le tunnel IPsec
& 'C:\Program Files\GLPI-Agent\glpi-agent.exe' --server
http://10.11.3.22/glpi --force

# Résultat attendu dans la console :
# [info] Running inventory task
# [info] Inventory sent to http://10.11.3.22/glpi
```

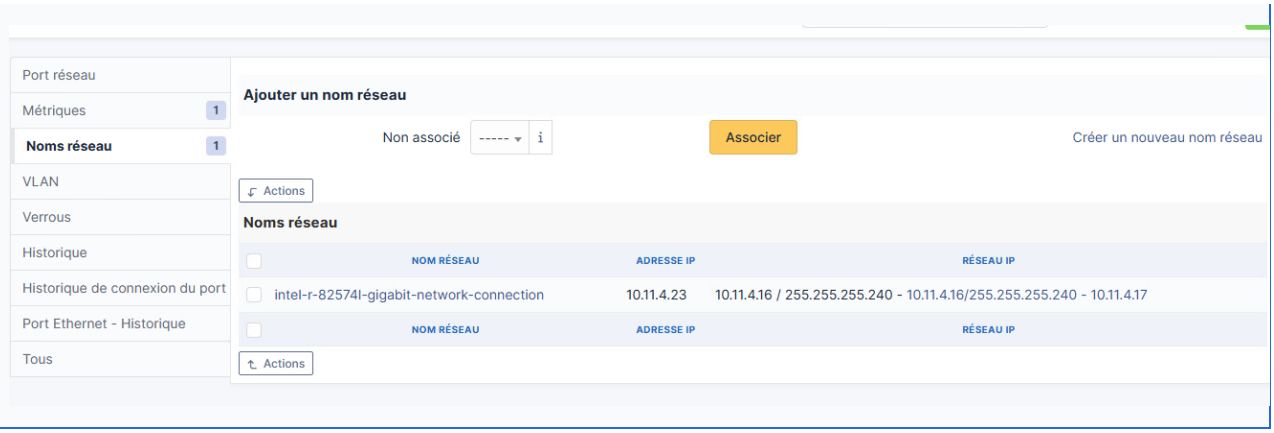
> **Rôle du tunnel IPsec dans cette étape**
> Le serveur GLPI (`10.11.3.22`) est sur le réseau du Site A. Le poste `CL-WIN11-01` est maintenant sur le Site B (`10.11.4.x`). La communication entre le poste et GLPI transite **intégralement par le tunnel IPsec** pfSense-02 → pfSense-01. Sans ce tunnel, l'agent ne pourrait pas atteindre son serveur d'inventaire.

2.3 — Vérification dans l'interface GLPI

> **Navigation : `Parc` > `Ordinateurs` > `CL-WIN11-01` > `Onglet Réseau`**

2. Se connecter à GLPI : `http://10.11.3.22` — Login `admin` / `Mewo123`
3. Naviguer dans `Parc > Ordinateurs` et ouvrir la fiche de `CL-WIN11-01`
4. Cliquer sur l'onglet **« Réseau »** (ou « Composants réseau »)
5. Vérifier les informations mises à jour :
   - **Adresse IP :** doit afficher la nouvelle IP en **10.11.4.x**
   - **Passerelle :** `10.11.4.17`
   - **Date du dernier inventaire :** horodatage correspondant à l'heure du forçage
6. Dans l'onglet **« Inventaire »**, vérifier que le champ **Dernière mise à jour** correspond à l'heure de la commande précédente

> **CAPTURE D'ÉCRAN N°4** — **Fiche GLPI de CL-WIN11-01 — Onglet Réseau montrant la nouvelle adresse IP en 10.11.4.x, la passerelle 10.11.4.17 et la date de dernier inventaire récente. Preuve de la mise à jour dynamique via le tunnel IPsec.**



CAPTURE D'ÉCRAN N°5 — GLPI — Onglet Inventaire de CL-WIN11-01 — Champ 'Dernière mise à jour' avec l'horodatage du forçage. Prouve que GLPI fonctionne en mode Push automatique.

PHASE 3

Rétablissement de la supervision — Zabbix retrouve le poste

Phase 3 — Mise à jour Zabbix et résolution de l'alerte

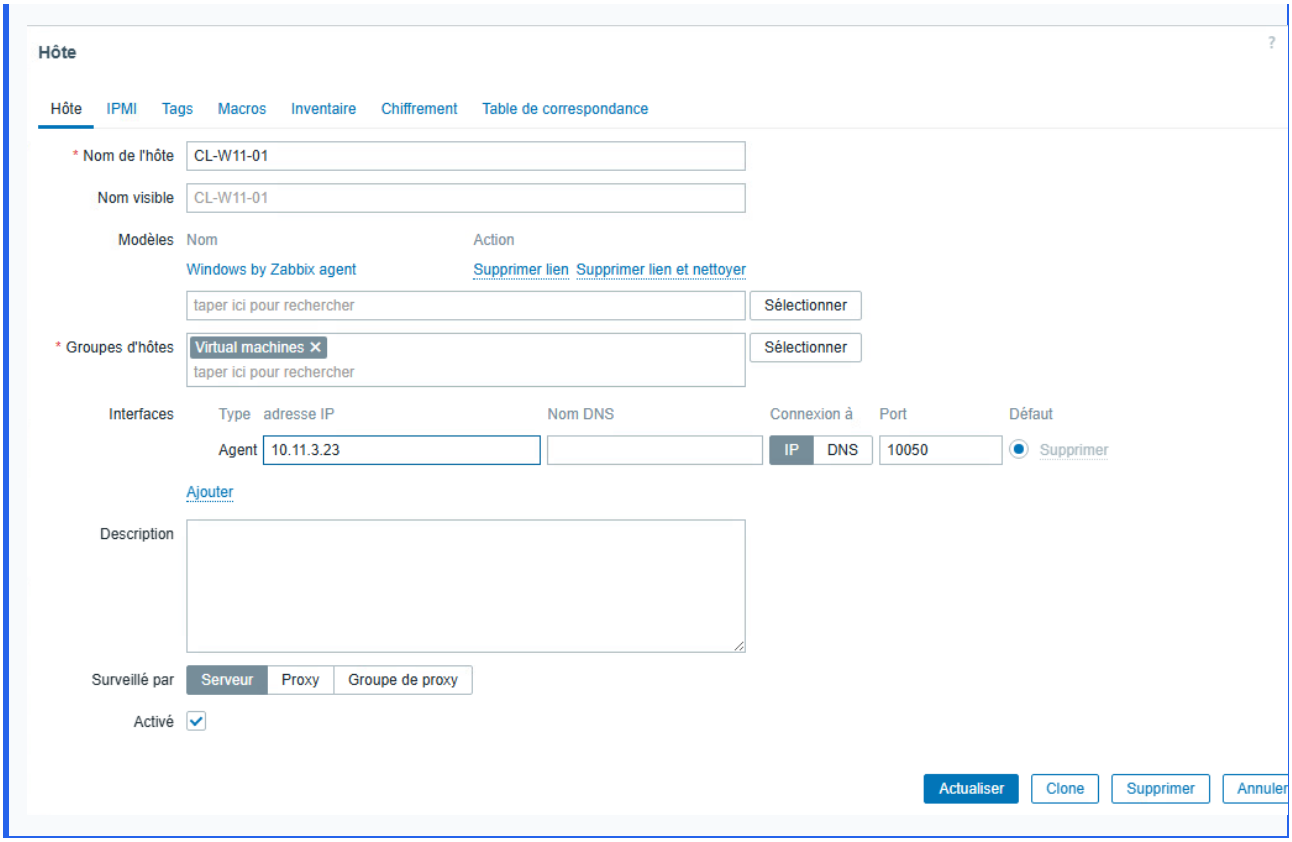
3.1 — Modification de l'adresse IP dans Zabbix

Navigation : `Configuration` > `Hosts` > `CL-WIN11-01` > `Interfaces`

Contrairement à GLPI qui est en mode **Push**, Zabbix fonctionne en mode **Pull** : il a besoin de connaître **explicitement** la nouvelle adresse IP du poste pour aller interroger son agent. Cette mise à jour est manuelle (ou automatisable via l'API Zabbix en production).

7. Dans Zabbix, naviguer dans `Configuration > Hosts`
8. Localiser `CL-WIN11-01` dans la liste (hôte en état **Problem**)
9. Cliquer sur le nom `CL-WIN11-01` pour ouvrir la configuration de l'hôte
10. Dans l'onglet **« Host »**, localiser la section **Interfaces**
11. Sur la ligne **Agent**, modifier le champ **IP address** :
    - **Ancienne IP :** `10.11.3.23` (Site A)
    - **Nouvelle IP :** `10.11.4.2X` (valeur obtenue à l'étape 2.1 — ex: 10.11.4.24)
12. Vérifier que le port reste `10050` et que DNS est vide (utilisation de l'IP directe)
13. Cliquer sur **« Update »** pour sauvegarder la modification

CAPTURE D'ÉCRAN N°6 — Formulaire de configuration de l'hôte CL-WIN11-01 dans Zabbix — Section Interfaces avec le champ 'IP address' modifié à la nouvelle valeur 10.11.4.x. Avant clic sur 'Update'.



3.2 — Constat de la résolution de l'alerte

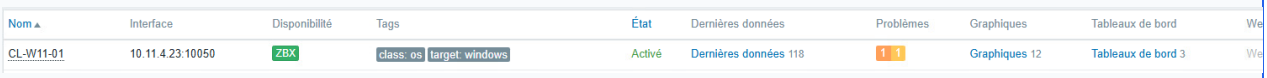
> **Navigation :** `Monitoring > Problems (attendre la prochaine collecte Zabbix)`

Dès le prochain cycle de collecte Zabbix (**60 secondes** par défaut), le serveur interroge l'agent sur la nouvelle IP. Si l'agent répond, le trigger `unreachable` passe en état **Resolved** et disparaît de la liste des problèmes actifs.

14. Patienter **1 à 3 minutes** après la mise à jour de l'IP dans Zabbix
15. Dans `Monitoring > Problems`, vérifier que l'alerte `CL-WIN11-01 is unreachable` n'apparaît plus
16. Naviguer dans `Monitoring > Latest data` pour `CL-WIN11-01` — les métriques doivent afficher des valeurs récentes (CPU, RAM, disque)
17. Dans `Monitoring > Hosts`, vérifier que `CL-WIN11-01` affiche à nouveau un rond **vert ZBX**

> **CAPTURE D'ÉCRAN N°7** — **Zabbix — Monitoring > Problems — L'alerte 'CL-WIN11-01 is unreachable' a disparu. Le tableau des problèmes actifs est vide ou ne contient plus d'alerte pour ce poste.**

CAPTURE D'ÉCRAN N°8 — Zabbix — Monitoring > Hosts — CL-WIN11-01 affiche un rond vert 'ZBX' dans la colonne Availability. Monitoring > Latest data montre des valeurs CPU/RAM récentes avec un horodatage actuel. Preuve du rétablissement total.



Validation complète — Bilan des trois phases

☑ **Phase 1 :** Zabbix a détecté la déconnexion et généré une alerte critique — surveillance proactive opérationnelle

☑ **Phase 2 :** GLPI a mis à jour automatiquement la fiche réseau avec la nouvelle IP 10.11.4.x — traçabilité via le tunnel IPsec confirmée

☑ **Phase 3 :** Zabbix a retrouvé le poste après mise à jour de l'IP — supervision rétablie, alerte résolue

IV. Argumentaire pour l'oral — Architecture d'administration unifiée

Concept clé : Push (GLPI) vs Pull (Zabbix)

La différence fondamentale entre GLPI et Zabbix réside dans leur **modèle de communication**, révélée par cet exercice de migration :

Caractéristique	GLPI — Mode Push (Actif)	Zabbix — Mode Pull (Passif)
Initiateur	L'agent (le poste)	Le serveur (Zabbix)
Direction du flux	Poste → Serveur GLPI	Serveur Zabbix → Poste
Connaissance IP requise	Non — l'agent contacte le serveur	Oui — le serveur doit connaître l'IP
Adaptation au changement IP	Automatique à la prochaine collecte	Manuelle (ou via API Zabbix)
Port requis	TCP 80/443 (sortant du poste)	TCP 10050 (entrant sur le poste)
Comportement migration	Transparent — GLPI suit le poste	Alerte unreachable → MàJ manuelle
Avantage	Zéro configuration IP côté serveur	Monitoring actif, détection instantanée

Rôle vital du tunnel IPsec — L'épine dorsale de l'administration

> *"Sans le tunnel IPsec IKEv2 interconnectant les deux sites, cette procédure serait impossible. L'agent GLPI du poste `CL-WIN11-01` ne pourrait pas atteindre le serveur `SRV-GLPI (10.11.3.22)` situé sur un autre réseau privé. Zabbix ne pourrait pas interroger l'agent sur le port `TCP 10050` depuis `SRV-ZABBIX (10.11.3.19)`.*
>
> *Le tunnel IPsec agit comme une **extension transparente du réseau LAN** : du point de vue applicatif, `10.11.3.x` et `10.11.4.x` appartiennent au même espace d'adressage logique. C'est ce qui permet d'administrer deux sites géographiquement distincts depuis un seul point de contrôle centralisé — sans VPN client, sans exposition publique des outils d'administration."*

Synthèse des bénéfices démontrés

Résilience de l'inventaire : GLPI maintient une base de données cohérente même lors d'une migration physique — aucune intervention manuelle requise sur la fiche CMDB

Détection proactive : Zabbix alerte en moins de 5 minutes lors d'une déconnexion non planifiée — distingue une migration d'une panne

Administration centralisée : Un seul point de contrôle pour les deux sites via IPsec — pas de déplacement physique requis pour administrer le parc du Site B

Traçabilité ITIL : L'historique GLPI conserve l'ancienne IP, la date de migration et la nouvelle configuration — conformité aux bonnes pratiques de gestion des changements (ITIL Change Management)