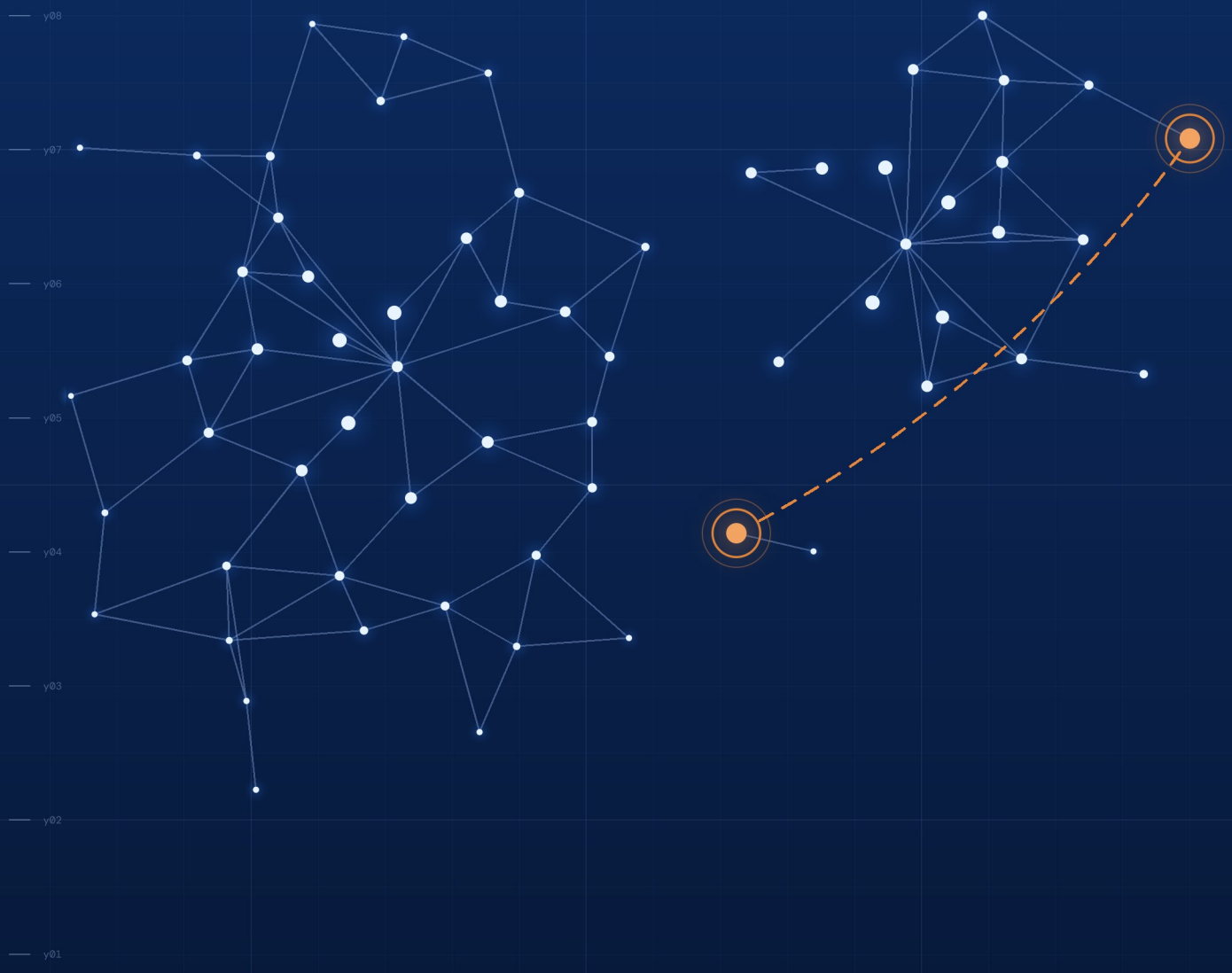


CATÉGORIE GLPI · JP CONSULTING

Playbook Sécurité

Les runbooks de la catégorie GLPI Sécurité

Jean-Philippe Rebischung

Sommaire

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

Durcissement **3**

Changement · Rendre visibles les échecs d'authentification sur le DC 4

Incident de sécurité **9**

Incident · Un balayage venant d'un poste interne 10

Index par symptôme

Ce que je reçois	Runbook	Page
Un constat : les mots de passe ratés n'apparaissent pas dans les journaux du DC	Durcissement	4
Le journal du pare-feu : blocages en rafale depuis 192.168.40.103	Incident de sécurité	10

> **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 SÉCURITÉ

Durcissement

Les réglages qui réduisent la surface d'attaque et rendent les attaques visibles.

Cas traités dans ce runbook

CHANGEMENT Rendre visibles les échecs d'authentification sur le DC.....4

Statut : non validé

CHANGEMENT · DURCISSEMENT

Rendre visibles les échecs d'authentification sur le DC

Niveau	N2 (préparer, appliquer), validation 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 Changement (ou Demande) · catégorie : Sécurité › Durcissement. *Statut : non validé*

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

Sur ce lab, des mots de passe ratés tapés sur un poste n'apparaissent pas en **4625** sur le contrôleur de domaine (constat fait lors d'un exercice). C'est normal en partie : un échec d'ouverture de session sur un poste est noté **sur le poste** (4625) ; le contrôleur de domaine, lui, note l'échec d'**authentification Kerberos*** (**4771**) ou NTLM (**4776**), à condition que l'**audit*** correspondant soit activé.

Ton travail : relever ce qui est audité, faire valider un **changement**, l'appliquer par GPO après sauvegarde, et prouver qu'un échec devient visible.

Ce que tu reçois : une demande du N3 : « On ne voit pas les échecs de connexion sur le DC. Peux-tu vérifier l'audit et proposer la correction ? »

Regle d'or

Une GPO de contrôleur de domaine ne se modifie qu'**après sauvegarde** et sur **demande de changement validée**.



Les étapes de ce cas. À l'étape 2, le N3 valide le changement.

1 Relever l'audit en place

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

```
auditpol /get /category:*
```

Lire la commande

Affiche, pour chaque sous-catégorie d'audit, ce qui est noté : **Succès**, **Échec**, les deux, ou **Pas d'audit**. Les noms sont en français.

Je dois voir

À relever dans le ticket : *Ouverture de session*, *Validation des informations d'identification*, *Service d'authentification Kerberos*. Un échec n'est journalisé que si la ligne contient **Échec**.

Pour mémoire, *Gestion des comptes d'utilisateur* est en **Succès** sur ce lab : c'est ce qui produit le 4740 (verrouillage).

2 Faire valider

Ticket de type **Changement**, catégorie **Sécurité › Durcissement**. Décris le constat, le réglage proposé, l'effet attendu (journal Sécurité un peu plus volumineux), le retour arrière (restauration de la GPO), puis **Demander une validation** au N3.

Pourquoi

Le réglage porte sur la *Default Domain Controllers Policy* : une erreur touche le seul contrôleur du lab. La sauvegarde et la validation sont le prix de ce risque.

3 Sauvegarder la GPO

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

```
Backup-GPO -Name 'Default Domain Controllers Policy' -Path C:\Sauvegardes\GPO
```

Je dois voir

Une sortie avec un `Id` de sauvegarde et l'heure : note-les dans le ticket (retour arrière : `Restore-GPO`).

4 Appliquer

Console **Gestion de stratégie de groupe** → *Default Domain Controllers Policy* → **Modifier**. Puis : **Configuration ordinateur → Stratégies → Paramètres Windows → Paramètres de sécurité → Configuration avancée de la stratégie d'audit → Stratégies d'audit**. Dans **Connexion de compte**, *Auditer la validation des informations d'identification* et *Auditer le service d'authentification Kerberos* : **Succès** et **Échec**. Dans **Ouverture/Fermeture de session**, *Auditer l'ouverture de session* : **Succès** et **Échec**.

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

```
gpupdate /force
```

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

```
auditpol /get /category:*
```

Je dois voir

Les trois sous-catégories affichent **Succès et échec**.

5 Tester et clôturer

Test : sur un poste du domaine, tente une ouverture de session avec un compte de test et un **mauvais** mot de passe (une seule fois, pour ne pas le verrouiller). Puis :

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

```
Get-WinEvent -FilterHashtable @{LogName='Security'; Id=4771,4776,4625} -MaxEvents 10 |
Format-List TimeCreated, Id, Message
```

Je dois voir

Un événement **4771** (ou 4776) à l'heure du test, avec le compte et l'adresse du poste. Un 4771 avec le code **`0x18`** = mauvais mot de passe.

Texte de la tâche (GLPI)

Constat : <SOUS-CATÉGORIES ET VALEURS AVANT>. Changement validé par <N3> le <DATE>. Sauvegarde GPO : Id <ID>, <HEURE>. Réglage : validation des informations d'identification, service d'authentification Kerberos, ouverture de session en Succès et Échec. Preuve : **`auditpol`** après ; test d'échec à <HEURE> → événement <4771/4776> visible. Retour arrière : **`Restore-GPO`** avec l'Id ci-dessus.

Texte de la solution (GLPI)

Les échecs d'authentification sont désormais journalisés sur le contrôleur de domaine. Le changement a été testé ; la sauvegarde de la stratégie permet de revenir en arrière.

Lexique

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

Audit
Réglage qui décide quels événements de sécurité Windows écrit dans le journal Sécurité (succès, échecs).

Kerberos
Protocole d'authentification du domaine : le contrôleur délivre des tickets. Un mauvais mot de passe saisi sur un poste donne un 4771 sur le contrôleur.

Notes

RUNBOOK · PLAYBOOK SÉCURITÉ

Incident de sécurité

La détection, la qualification et la réponse à une activité suspecte.

Cas traités dans ce runbook

INCIDENT Un balayage venant d'un poste interne.....10

Statut : non validé

Un balayage venant d'un poste interne

Niveau	N2 (qualifier, conserver, isoler sur accord), N3 (décider de la suite).
Où	PFSENSE01 (interface web depuis le PC hôte), **`SRV-SYSLOG01`** (collecteur, SSH, compte **`admin.linux`**), VMware sur le PC hôte.
GLPI	type Incident · catégorie : Sécurité › Incident de sécurité.
	Statut : non validé

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

Le pare-feu note en rafale des connexions refusées venant d'une même adresse, vers beaucoup de ports ou de machines : c'est la signature d'un **balayage*** (reconnaissance avant une attaque). Sur ce lab, la machine **`192.168.40.103`** (**`KaliAudit2`**) joue le **poste interne compromis**.

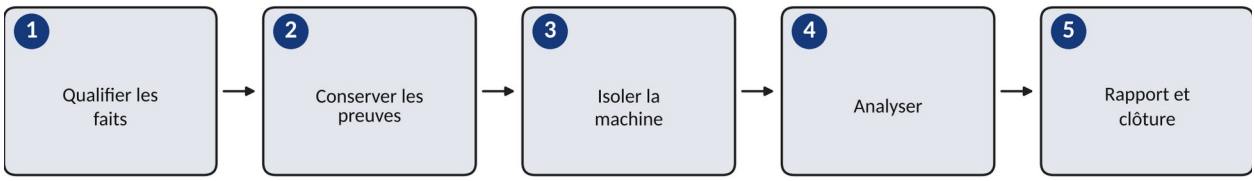
Ton travail : qualifier les faits, **conserver les preuves**, contenir (isoler la machine), informer le N3, et écrire un rapport factuel.

Ce que tu reçois : un constat en lisant le journal du pare-feu, ou une demande du N3 : « Beaucoup de blocages venant du LAN_40 ce matin, peux-tu regarder ? »

Regle d'or

On **conserve les preuves avant d'agir** : un journal effacé ou une machine éteinte trop tôt ne se rattrapent pas.

On n'attaque pas en retour et on n'éteint pas la machine : on l'**isole** du réseau.



Les étapes de ce cas.

1 Qualifier les faits

PFSENSE01 : **État → Journaux système → Pare-feu**, filtre *Adresse IP source* = **`192.168.40.103`**. Relève l'heure de début, les destinations, les ports, le nombre de lignes.

Je dois voir

Des dizaines de blocages en quelques secondes, vers des ports différents d'une même cible (ou un même port sur plusieurs cibles) : balayage probable.

Quelques blocages isolés vers un même service : plutôt une erreur de configuration (voir le runbook Pare-feu du playbook Réseau).

Pourquoi

Suricata, sur PFSENSE01, surveille le **LAN Windows** seulement, pas le LAN_40 : un trafic bloqué à l'entrée du LAN_40 n'y arrive jamais. Ici, la preuve est dans le **journal du pare-feu**, pas dans les alertes Suricata.

Ticket : **Incident**, catégorie **Sécurité › Incident de sécurité**, priorité **Haute**. Préviens le N3 dès ce constat.

2 Conserver les preuves

Les journaux des pare-feux sont copiés sur le collecteur **`SRV-SYSLOG01`** (**`192.168.20.63`**), un dossier par machine sous **`/var/log/distant/`**.

Machine : SRV-SYSLOG01 (192.168.20.63) | **Compte :** compte sudo (admin.linux) | **Outil :** SSH depuis le PC hôte

```
sudo grep -rl '192.168.40.103' /var/log/distant/
```

Je dois voir

La liste des fichiers qui citent l'adresse : celui de PFSENSE01 en premier. Note le chemin.

Machine : SRV-SYSLOG01 | **Compte :** compte sudo (admin.linux) | **Outil :** Bash

```
sudo grep -h '192.168.40.103' <FICHIER_DU_PARE-FEU> > ~/preuve-scan-<N°_TICKET>.log ;
wc -l ~/preuve-scan-<N°_TICKET>.log
```

Lire la commande

Copie les lignes concernées dans un fichier de preuve, dans ton dossier personnel, sans toucher au journal d'origine ; **`wc -l`** compte les lignes.

3 Isoler la machine

Avec l'accord du N3 : dans VMware, **VM → Settings → Network Adapter**, décoche **Connected**. La machine reste allumée (sa mémoire peut servir à l'analyse) mais ne parle plus au réseau.

Attention

N'éteins pas la machine et ne la nettoie pas toi-même : ce serait détruire des traces. La suite (analyse du poste) est une décision du N3.

4 Analyser

- Fenêtre de temps : première et dernière ligne du fichier de preuve.
- Cibles et ports visés : quels services l'attaquant cherchait (22, 445, 3389…).
- Un flux a-t-il été **autorisé** ? Sur ce lab, le LAN_40 n'a le droit de joindre que le DNS du DC, le collecteur (20514) et Internet : tout autre essai vers le LAN Windows est refusé.
- Les comptes : des verrouillages (4740) ou des échecs (4771) au même moment sur le DC ?

5 Rapport et clôture

Texte de la tâche (GLPI) — rapport factuel

Constat le <DATE> à <HEURE> : <N> blocages en <DURÉE> depuis 192.168.40.103 (KaliAudit2, LAN_40) vers <CIBLES>:<PORTS>. Preuve conservée : **`~/preuve-scan-<N°_TICKET>.log`** sur SRV-SYSLOG01 (<N> lignes). Isolement réseau à <HEURE>, accord de <N3>. Aucun flux autorisé constaté hors règles prévues. Comptes : <CONSTAT_4740_4771>. Suite décidée par le N3 : <DÉCISION>.

Texte de la solution (GLPI)

Une activité de reconnaissance venant d'un poste du réseau de test a été bloquée par le pare-feu. Le poste a été isolé ; aucune intrusion n'a été constatée.

Lexique

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

Balayage (scan)

Série rapide de tentatives de connexion vers de nombreux ports ou machines, pour découvrir les services ouverts. Première étape d'une attaque.

Collecteur de journaux

Serveur qui reçoit et conserve les journaux des autres machines (ici **`SRV-SYSLOG01`**). Ce n'est pas un SIEM : rien n'y est corrélé automatiquement.

Notes