Mode Opératoire

Exploitation de Wazuh
SIEM de l'infrastructure BTS SIO

Code :	MO-SEC-001
Version :	1.0
Date :	27 mars 2026
Auteur :	Cédric LEGRAND
Classification :	USAGE INTERNE — Équipe BTS SIO

Historique des révisions

Version	Date	Modifications
1.0	27/03/2026	Création initiale

1 Objet

Ce mode opératoire décrit les procédures d'exploitation quotidienne de **Wazuh**, la solution SIEM (*Security Information and Event Management*) open-source déployée sur l'infrastructure BTS SIO du Lycée Jean Lurçat.

Il couvre le démarrage et l'arrêt du conteneur, l'accès au tableau de bord, la consultation des alertes de sécurité, la gestion des agents et le déploiement de nouveaux agents sur les postes et serveurs supervisés.

Wazuh assure la détection d'intrusion (HIDS), l'analyse des journaux système, le contrôle d'intégrité des fichiers et la vérification de conformité réglementaire sur l'ensemble de l'infrastructure pédagogique.

2 Champ d'application

Public concerné	Enseignants de l'équipe BTS SIO, administrateurs de l'infrastructure pédagogique
Systèmes	Wazuh (CT 103 sur ProxMox), agents déployés sur les serveurs et postes de travail
Durée estimée	10 minutes (consultation), 15–20 minutes (déploiement d'un agent)

3 Prérequis

Prérequis

— Accès SSH à l'hyperviseur ProxMox (`10.0.112.200`) ou accès à l'interface web (port 8006)
— Connexion au réseau BTS SIO (câble RJ45 ou tunnel VPN WireGuard)
— Navigateur web récent (Firefox, Chrome ou Edge) pour le tableau de bord Wazuh
— Identifiants ProxMox et Wazuh (voir le gestionnaire de mots de passe de l'équipe)

4 Architecture Wazuh

Wazuh est déployé dans le conteneur LXC **CT 103** sur l'hyperviseur ProxMox. Il intègre trois composants principaux :

— **wazuh-manager** : collecte et analyse les événements transmis par les agents installés sur les machines supervisées. Il déclenche les alertes selon les règles de détection configurées.
— **wazuh-indexer** : moteur d'indexation basé sur OpenSearch. Il stocke l'ensemble des alertes et permet les recherches avancées.
— **wazuh-dashboard** : interface web basée sur OpenSearch Dashboards. Elle fournit les tableaux de bord, les visualisations et les outils de recherche.

Ressources allouées au CT 103

Le conteneur dispose de 8 cœurs, 8 Go de RAM et 100 Go d'espace disque. Ces ressources sont dimensionnées pour l'infrastructure pédagogique actuelle (quelques dizaines d'agents au maximum).

Port	Protocole	Rôle
443	TCP	Tableau de bord Wazuh (HTTPS)
1514	TCP	Communication agents → manager (événements)
1515	TCP	Enrôlement (*enrollment*) des nouveaux agents
9200	TCP	API OpenSearch (indexer, usage interne)
55000	TCP	API REST Wazuh (administration programmatique)

5 Procédure

5.1 Démarrage et arrêt du CT Wazuh

Étape 1 — Se connecter à ProxMox

Deux méthodes sont possibles :

— **Interface web** : ouvrir `https://10.0.112.200:8006` et se connecter avec les identifiants ProxMox (compte `root@pam`, mot de passe dans le gestionnaire de mots de passe).

— **SSH** : ouvrir un terminal et exécuter :

```
ssh root@10.0.112.200
```

Étape 2 — Démarrer le conteneur CT 103

Depuis la ligne de commande ProxMox :

```
# Verifier l'etat du conteneur
pct status 103

# Demarrer le conteneur (si arrete)
pct start 103

# Verifier que le conteneur est bien lance
pct status 103
```

Depuis l'interface web : sélectionner **CT 103 (wazuh)** dans le panneau de gauche, puis cliquer sur **Démarrer** dans la barre d'actions.

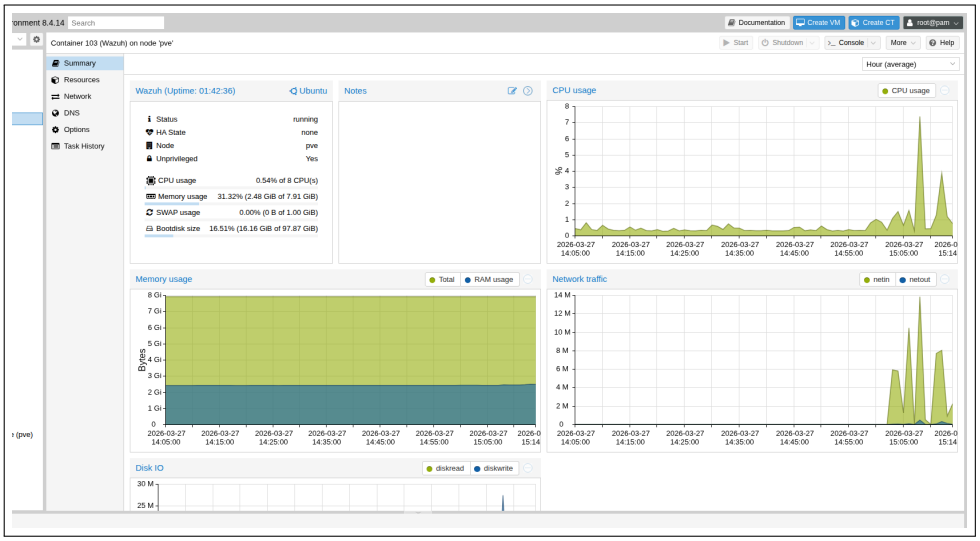

Figure 1 – Statut du CT 103 dans l'interface ProxMox

Étape 3 — Vérifier l'état des services Wazuh

Se connecter au conteneur, puis vérifier que les trois services sont actifs :

```
# Entrer dans le conteneur
pct enter 103

# Verifier les trois services
systemctl status wazuh-manager
systemctl status wazuh-indexer
systemctl status wazuh-dashboard
```

Chaque service doit afficher `active (running)` en vert. Si un service n'est pas démarré, consulter la section 7.

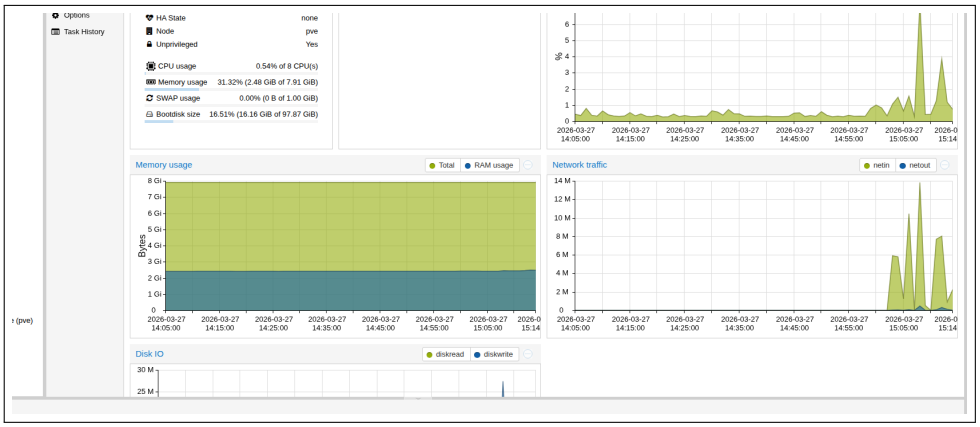

Figure 2 – Consommation de ressources du CT 103

Démarrage automatique

Le CT 103 est configuré avec `onboot=1` : il démarre automatiquement avec l'hyperviseur ProxMox. En fonctionnement normal, il n'y a pas besoin de le démarrer manuellement.

⚠ Arrêt du SIEM

Arrêter le CT 103 désactive **toute la chaîne de détection d'intrusion** sur l'infrastructure. Les agents continuent de collecter localement les événements, mais ceux-ci ne sont ni analysés ni indexés tant que le manager est arrêté. Ne procéder à un arrêt qu'en cas de maintenance planifiée et pour une durée limitée.

5.2 Accéder au tableau de bord Wazuh

Étape 4 — Ouvrir le tableau de bord

Dans un navigateur, accéder à :

`https://10.0.232.33`

Le navigateur affiche un avertissement de certificat auto-signé : accepter l'exception de sécurité pour continuer.

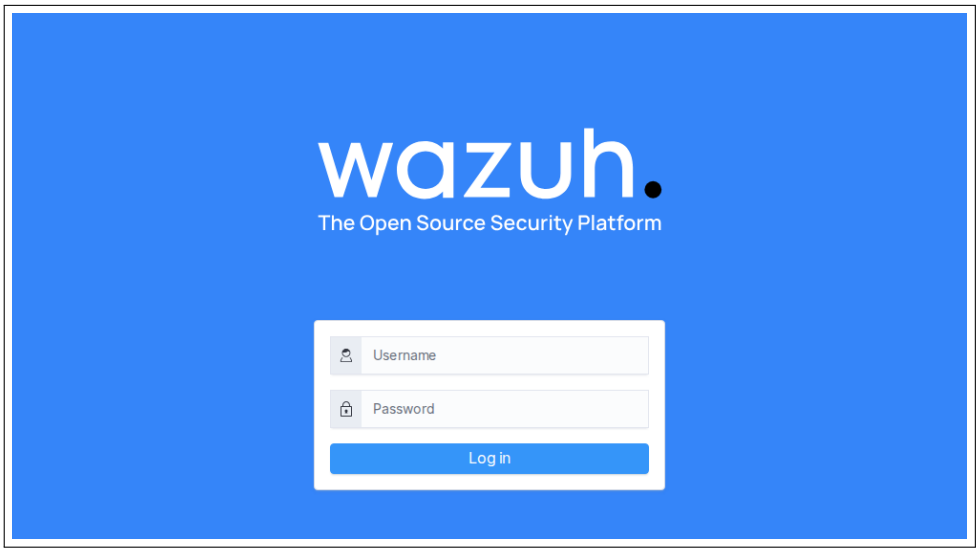

Figure 3 – Page de connexion du tableau de bord Wazuh

Étape 5 — Se connecter au tableau de bord

Saisir les identifiants :

— *Username* : `admin`

— *Password* : le mot de passe communiqué par l'administrateur (voir le gestionnaire de mots de passe)

Cliquer sur **Log in**.

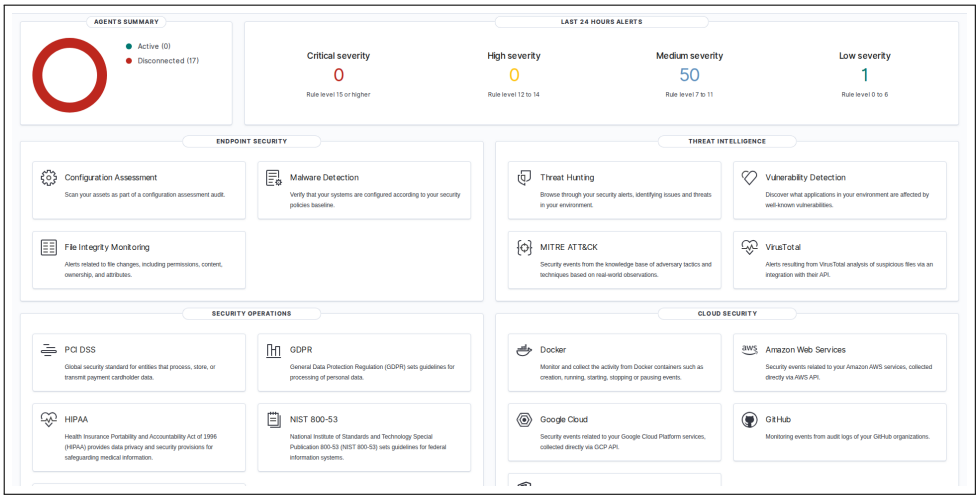

Figure 4 – Vue d'ensemble du tableau de bord Wazuh après connexion

Adresse IP dynamique

Le CT 103 obtient son adresse via DHCP sur le bridge `vmbr0`. L'adresse `10.0.232.33` peut changer après un redémarrage du conteneur ou du serveur DHCP. En cas d'inaccessibilité, vérifier l'adresse IP courante :

```
pct exec 103 -- ip addr show eth0
```

5.3 Consulter les alertes de sécurité

Étape 6 — Accéder aux événements de sécurité

Depuis le tableau de bord, cliquer sur **Security events** dans le menu principal (ou via **Modules** → **Security events**).
La page affiche l'ensemble des alertes détectées par les agents, classées par date et niveau de sévérité.

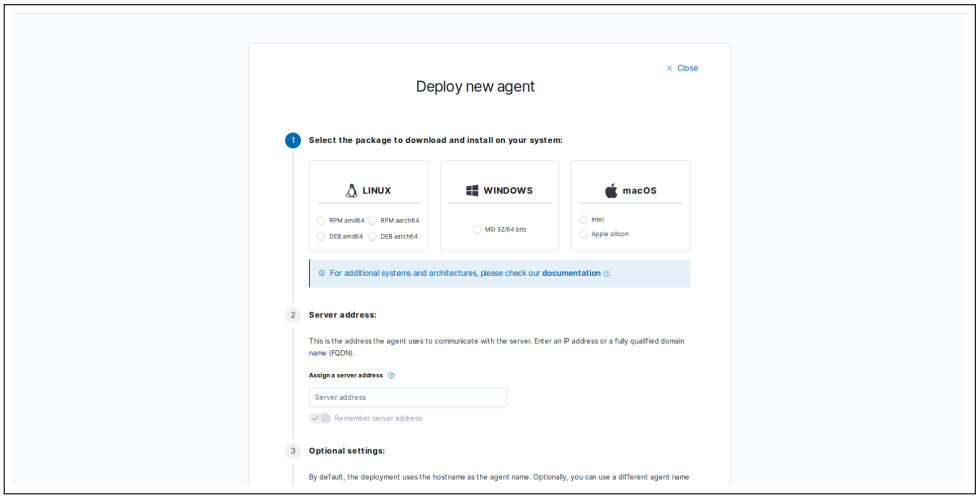

Figure 5 – Vue des événements de sécurité

Les alertes Wazuh sont classées selon une échelle de sévérité de 1 à 15 :

Niveau	Catégorie	Description
1–3	Informationnel	Événements normaux (connexions réussies, mises à jour)
4–7	Avertissement	Activités inhabituelles nécessitant une attention (tentatives échouées répétées)
8–11	Élevé	Événements significatifs (modifications de fichiers critiques, élévation de privilèges)
12–15	Critique	Incidents de sécurité majeurs (intrusion détectée, rootkit, brute force réussie)

Filtrer les alertes efficacement

Utiliser la barre de recherche en haut de la page pour filtrer les événements :

— Par niveau de sévérité : `rule.level >= 10` pour les alertes critiques

— Par agent : `agent.name : DC1` pour cibler un serveur précis

— Par type de règle : `rule.groups : authentication_failed` pour les échecs d'authentification

— Par période : ajuster la plage temporelle via le sélecteur de dates en haut à droite

En cas d'alerte de niveau 12 ou supérieur, une investigation immédiate est recommandée.

5.4 Gérer les agents

Étape 7 — Accéder à la liste des agents

Depuis le tableau de bord, cliquer sur **Agents** dans le menu latéral gauche.
La page affiche la liste de tous les agents enregistrés, avec leur nom, leur adresse IP, leur système d'exploitation et leur statut.

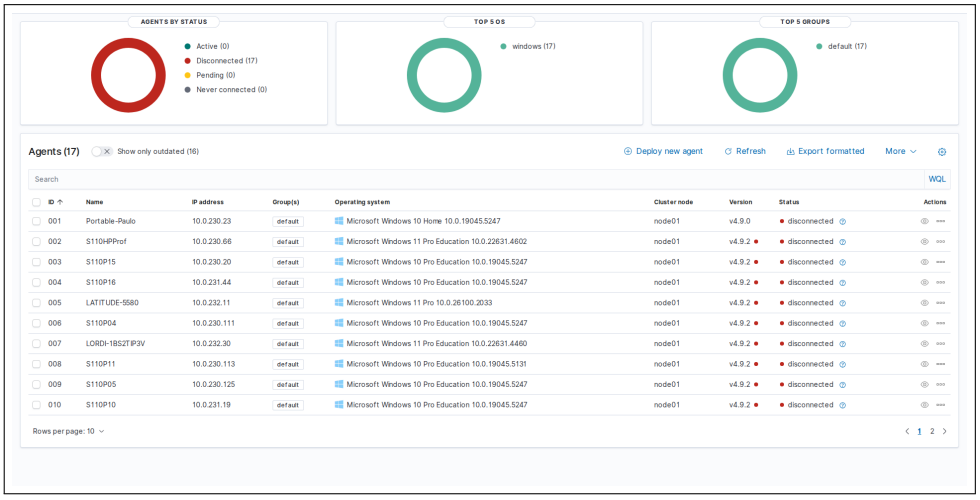

Figure 6 – Liste des agents Wazuh enregistrés

Trois états sont possibles pour un agent :

— **Active** (vert) : l'agent communique normalement avec le manager. Situation attendue

en fonctionnement normal.

— **Disconnected** (rouge) : l'agent ne communique plus. Causes possibles : machine éteinte, service arrêté, problème réseau, pare-feu bloquant le port 1514.

— **Never connected** (gris) : l'agent a été enregistré mais ne s'est jamais connecté au manager. Vérifier l'installation et la configuration de l'agent.

Note

Cliquer sur le nom d'un agent permet d'accéder à son tableau de bord détaillé : événements récents, contrôle d'intégrité, vulnérabilités détectées, conformité et informations système.

5.5 Déployer un nouvel agent

Étape 8 — Accéder à l'assistant de déploiement

Depuis le tableau de bord, naviguer vers **Agents** puis cliquer sur Deploy new agent.

L'assistant propose les commandes d'installation adaptées au système d'exploitation cible.

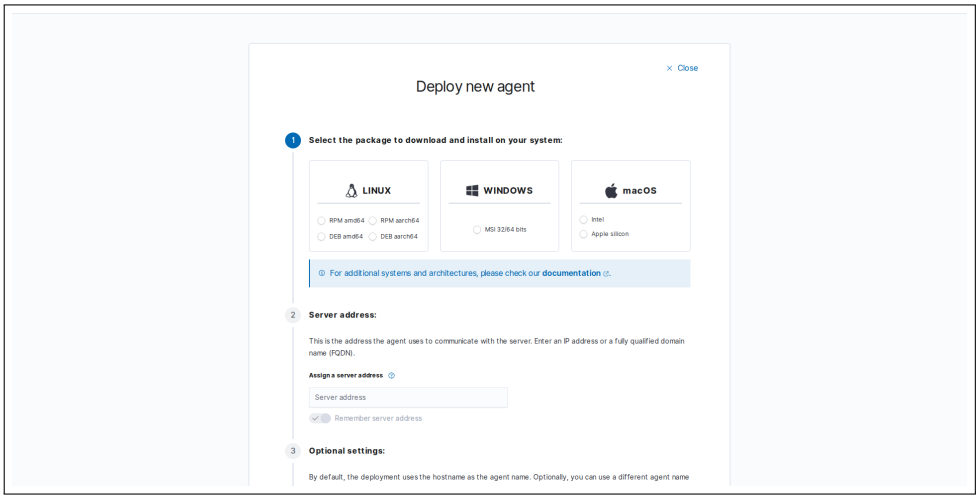

Figure 7 – Assistant de déploiement d'un nouvel agent

Déploiement sur Windows (DC1, DC2, postes)

Les contrôleurs de domaine et les postes Windows constituent la majorité de l'infrastructure BTS SIO. La procédure ci-dessous utilise PowerShell en mode administrateur.

Étape 9 — Télécharger et installer l'agent Windows

Sur la machine Windows cible, ouvrir **PowerShell en tant qu'administrateur** et exécuter :

```
# Telecharger l'installeur MSI (adapter la version)
Invoke-WebRequest -Uri
    https://packages.wazuh.com/4.x/windows/wazuh-agent-4.7.2-1.msi
    -OutFile $env:TEMP\wazuh-agent.msi

# Installer avec l'IP du manager
msiexec.exe /i $env:TEMP\wazuh-agent.msi /q WAZUH_MANAGER="10.0.232.33"
    WAZUH_REGISTRATION_SERVER="10.0.232.33"
```

L'adresse IP du manager (`10.0.232.33`) doit correspondre à l'adresse courante du CT 103.

Étape 10 — Démarrer le service agent Windows

Toujours dans PowerShell en mode administrateur :

```
# Demarrer le service
NET START Wazuh

# Verifier le statut
Get-Service WazuhSvc
```

Le service doit afficher le statut `Running`.

Déploiement sur Linux (serveurs, conteneurs)

Étape 11 — Ajouter le dépôt et installer l'agent Linux

Sur la machine Linux cible, exécuter en tant que `root` :

```
# Importer la cle GPG Wazuh
curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | gpg
    --no-default-keyring --keyring
    gnupg-ring:/usr/share/keyrings/wazuh.gpg --import && chmod 644
    /usr/share/keyrings/wazuh.gpg

# Ajouter le depot (Debian/Ubuntu)
echo "deb [signed-by=/usr/share/keyrings/wazuh.gpg]
    https://packages.wazuh.com/4.x/apt/ stable main" | tee
    /etc/apt/sources.list.d/wazuh.list

# Installer l'agent
apt-get update && apt-get install -y wazuh-agent
```

Étape 12 — Configurer et démarrer l'agent Linux

Éditer le fichier de configuration pour renseigner l'adresse du manager :

```
# Editer la configuration de l'agent
nano /var/ossec/etc/ossec.conf
```

Localiser la section `<client>` et remplacer l'adresse du manager :

```
<client>
  <server>
    <address>10.0.232.33</address>
    <port>1514</port>
    <protocol>tcp</protocol>
  </server>
</client>
```

Puis démarrer et activer le service :

```
systemctl daemon-reload
systemctl enable wazuh-agent
systemctl start wazuh-agent
systemctl status wazuh-agent
```

⚠ Pare-feu et ports réseau

Les machines hébergeant un agent doivent pouvoir joindre le CT 103 sur les ports **1514/TCP** (communication) et **1515/TCP** (enrôlement initial). Vérifier que les règles de pare-feu du réseau pédagogique autorisent ce trafic.

En cas de doute, tester la connectivité depuis la machine agent :

```
# Test de connectivite vers le manager
nc -zv 10.0.232.33 1514
nc -zv 10.0.232.33 1515
```

5.6 Maintenance

Étape 13 — Redémarrer les services Wazuh

En cas de dysfonctionnement, redémarrer les services dans l'ordre suivant depuis le CT 103 :

```
# Entrer dans le conteneur
pct enter 103

# Redemarrer dans l'ordre : indexer, manager, dashboard
systemctl restart wazuh-indexer
systemctl restart wazuh-manager
systemctl restart wazuh-dashboard

# Verifier l'etat de chaque service
systemctl status wazuh-indexer wazuh-manager wazuh-dashboard
```

L'ordre est important : l'indexer doit être opérationnel avant que le manager et le dashboard ne démarrent correctement.

Étape 14 — Consulter les journaux

Les journaux du manager sont la première source d'information en cas de problème :

```
# Journal principal du manager
tail -100 /var/ossec/logs/ossec.log

# Journal des alertes
tail -50 /var/ossec/logs/alerts/alerts.json

# Journal de l'indexer
journalctl -u wazuh-indexer --since "1 hour ago"

# Journal du dashboard
journalctl -u wazuh-dashboard --since "1 hour ago"
```

Étape 15 — Vérifier la santé de l'indexer

L'état de l'indexer OpenSearch peut être interrogé via son API locale :

```
# Sante du cluster (doit retourner "green" ou "yellow")
curl -k -u admin:MOTDEPASSE \
  https://127.0.0.1:9200/_cluster/health?pretty

# Espace disque utilise par les indices
curl -k -u admin:MOTDEPASSE \
  https://127.0.0.1:9200/_cat/indices?v
```

Remplacer `MOTDEPASSE` par le mot de passe de l'indexer (voir le gestionnaire de mots de passe).
Un état `green` signifie que tous les index sont sains. L'état `yellow` indique une réplication incomplète (normal en déploiement mono-nœud). L'état `red` requiert une investigation immédiate.

Surveiller l'espace disque

Le CT 103 dispose de 100 Go d'espace disque. Les index Wazuh grandissent avec le volume d'alertes. Vérifier régulièrement l'occupation :

```
df -h /var/ossec /var/lib/wazuh-indexer
```

Si l'espace utilisé dépasse 80 %, configurer une politique de rétention dans **Index Management** → **Index Policies** du dashboard pour supprimer automatiquement les anciens index (par exemple, conserver 90 jours).

6 Vérification

Vérification

Après avoir effectué les opérations de ce mode opératoire, vérifier les points suivants :

- ☐ Le CT 103 est en état `running` dans ProxMox
- ☐ Les trois services sont actifs : `wazuh-manager`, `wazuh-indexer`, `wazuh-dashboard`
- ☐ Le tableau de bord est accessible via `https://10.0.232.33`
- ☐ La connexion au tableau de bord avec le compte `admin` fonctionne
- ☐ Aucune alerte critique (niveau ≥ 12) n'est en attente de traitement
- ☐ Le port 1514 est joignable depuis les machines agents

7 Dépannage

Problème	Solution
Tableau de bord inaccessible	Vérifier que le CT 103 est démarré (`pct status 103`). Contrôler l'adresse IP du conteneur (`pct exec 103 - ip a`) : le DHCP peut avoir attribué une nouvelle adresse. Vérifier enfin que le service `wazuh-dashboard` est actif.
Un service ne démarre pas	Consulter les journaux (`journalctl -u <service> -n 50`). Vérifier la mémoire disponible (`free -h`) : l'indexer nécessite au minimum 4 Go de RAM. Redémarrer les services dans l'ordre indiqué en section 5.6.
Agent non connecté	Vérifier la connectivité vers le port 1514 du manager (`nc -zv 10.0.232.33 1514`). Contrôler l'adresse du manager dans la configuration de l'agent (`/var/ossec/etc/ossec.conf` sous Linux, clé de registre sous Windows). Redémarrer le service agent.
Espace disque insuffisant	Vérifier la taille des index (`curl -k -u admin:MDP https://127.0.0.1:9200/_cat/indices?v`). Configurer une politique de rétention ou supprimer manuellement les index anciens : `curl -k -u admin:MDP -X DELETE https://127.0.0.1:9200/wazuh-alerts-*-YYYY.MM`.
Mot de passe oublié	Utiliser l'outil de gestion des mots de passe Wazuh depuis le CT 103 : `/usr/share/wazuh-indexer/plugins/opensearch-security/tools/w` Consulter la documentation Wazuh pour les paramètres.