

FICHE 2 – SIEM WAZUH – INSTALLATION

Liens :

- Lien officiel de l'installation : <https://documentation.wazuh.com/current/installation-guide/index.html>
- Liens directs pour le dépannage :
 - Wazuh-dashboard : <https://documentation.wazuh.com/current/user-manual/wazuh-dashboard/troubleshooting.html>
 - Wazuh-agent : <https://documentation.wazuh.com/current/user-manual/agent/agent-enrollment/troubleshooting.html>

Les exigences matérielles dépendent fortement du nombre de terminaux protégés et de charges de travail cloud. Ce nombre permet d'estimer la quantité de données à analyser et le nombre d'alertes de sécurité à stocker et indexer :

Agents	CPU	RAM	Storage (90 days)
1-25	4 vCPU	8 GiB	50 GB
25-50	8 vCPU	8 GiB	100 GB
50-100	8 vCPU	8 GiB	200 GB

L'interface de Wazuh est en anglais. il a été parfois utilisé un traducteur automatique du navigateur lors des copies d'écran.

SOMMAIRE

A. Installation de Wazuh	2
A.1 Installation rapide avec un seul script	2
A.2 Installation des composants de Wazuh	3
A.2.1 Prérequis pour l'installation de l'indexeur	3
A.2.2 Installation de l'indexeur	5
A.2.3 Installation de Wazuh-manager	6
A.2.4 Installation de Filebeat	6
A.2.5 Installation du dashboard Wazuh	8
A.3 Installation avec docker compose	8
B. Déploiement des agents Wazuh	9
B.1 Création d'un groupe d'agents (facultatif)	9
B.2 L'agent Wazuh	9
B.2.1 L'agent Wazuh pour Windows	9
B.2.2 L'agent Wazuh pour Linux	10
B.3 Ajout ou suppression d'un agent à un groupe	13
C. Mise à jour du serveur wazuh et des agents	13
C.1 Mise à jour du serveur Wazuh	13
C.2 Mise à jour des agents Wazuh	15
C.2.1 Mise à jour des agents sur Ubuntu/Debian	15
C.2.2 Mise à jour des agents sur Windows	16

Pour bien comprendre l'installation des composants de Wazuh, il est nécessaire de s'appuyer sur la fiche n° 1 : SIEM WAZUH – Architecture.

A. INSTALLATION DE WAZUH

A.1 INSTALLATION RAPIDE AVEC UN SEUL SCRIPT

Étape 1 : Téléchargez et exécutez l'assistant d'installation Wazuh

Pour s'assurer d'installer la dernière version disponible, copier/coller la commande proposée par Wazuh via ce lien : <https://documentation.wazuh.com/current/quickstart.html>.

Par exemple :

```
curl -sO https://packages.wazuh.com/4.11/wazuh-install.sh && sudo bash ./wazuh-install.sh -a
```

ATTENTION : Patience, le script met un certain temps avant de finaliser le déploiement de l'ensemble des composants.

Une fois l'assistant terminé l'installation, le produit indique les identifiants d'accès et un message qui confirme que l'installation a réussi.

```
INFO: --- Summary ---
INFO: You can access the web interface https://<wazuh-dashboard-ip>
      User: admin
      Password: <ADMIN_PASSWORD>
INFO: Installation finished.
```

Permettre au service wazuh-indexer de redémarrer automatiquement après un redémarrage du système.

```
systemctl enable wazuh-indexer.service
```

Étape 2 : Accéder à l'interface web Wazuh avec <https://<wazuh-dashboard-ip>> et vos identifiants :

- Nom d'utilisateur : **admin**
- Mot de passe : **<ADMIN_PASSWORD>**

Si jamais l'interface web Wazuh n'est pas accessible, essayer de redémarrer les composants de Wazuh avec les commandes ci-après

```
systemctl restart wazuh-dashboard
systemctl restart wazuh-indexer
systemctl restart wazuh-manager
```

Vous pourrez également être amené à redémarrer le module filebeat (Elastic) :

```
systemctl restart filebeat
```



Vous pouvez trouver les mots de passe pour tous les utilisateurs d'indexation Wazuh et Wazuh API dans le **wazuh-passwords.txt** Dossier à l'intérieur **wazuh-install-files.tar**. Pour les afficher, exécutez la commande suivante :

```
sudo tar -O -xvf wazuh-install-files.tar wazuh-install-files/wazuh-passwords.txt
```

NB : Désinstaller les composants de Wazuh

Vous pouvez désinstaller tous les composants centraux Wazuh en utilisant l'assistant d'installation de Wazuh.

Exécuter l'assistant avec l'option -u ou --uninstall comme suit :

```
sudo bash wazuh-install.sh --uninstall
```

Cela supprimera l'**indexeur Wazuh**, le **serveur Wazuh** et le **tableau de bord Wazuh**.

A.2 INSTALLATION DES COMPOSANTS DE WAZUH

Trois composants doivent être installés :

- l'**indexeur** pour collecter les données de sécurité ;
- le **serveur** pour analyser et détecter les menaces ;
- le **tableau de bord** pour visualiser et gérer les alertes générées.

A.2.1 Prérequis pour l'installation de l'indexeur

a. Installation des certificats

Télécharger un script pour créer les certificats et le fichier de configuration.

```
curl -sO https://packages.wazuh.com/4.9/wazuh-certs-tool.sh
curl -sO https://packages.wazuh.com/4.9/config.yml
```

Le fichier de configuration **config.yml** doit être modifié en ajoutant l'adresse IP de notre serveur Wazuh :

```
nodes:
  # Wazuh indexer nodes
  indexer:
    - name: node-1
      ip: "192.168.2.1"
    #- name: node-2
    # ip: "<indexer-node-ip>"
    #- name: node-3
    # ip: "<indexer-node-ip>"
  # Wazuh server nodes
  # If there is more than one Wazuh server
  # node, each one must have a node_type
  server:
    - name: wazuh-1
      ip: "192.168.2.1"
    # node_type: master
    #- name: wazuh-2
    # ip: "<wazuh-manager-ip>"
    # node_type: worker
    #- name: wazuh-3
    # ip: "<wazuh-manager-ip>"
    # node_type: worker
  # Wazuh dashboard nodes
  dashboard:
    - name: dashboard
      ip: "192.168.2.1"
```

Exécuter le script bash pour la création des certificats :

```
bash ./wazuh-certs-tool.sh -A
```

Compresser le dossier comprenant les certificats générés :

```
tar -cvf ./wazuh-certificates.tar -C ./wazuh-certificates/ .
```

b. Installation des dépôts et des paquets nécessaires à la suite de l'installation

- Paquets nécessaires à l'installation de la solution WAZUH : **debconf adduser procps gnupg** et **apt-transport-https** :

```
apt-get install debconf adduser procps
```

debconf est un système de configuration centralisé utilisé par les paquets Debian pour gérer leurs paramètres de configuration de manière standardisée.

Le paquet **adduser** fournit un script simplifié pour créer et gérer les utilisateurs sur un système Linux.

procps est un paquet qui regroupe divers outils permettant de surveiller et gérer les processus et l'état du système.

```
apt-get install gnupg apt-transport-https
```

Installation de l'outil **GnuPG** (GNU Privacy Guard), qui est une implémentation open source du standard OpenPGP. GnuPG est utilisé pour gérer les clés publiques permettant de vérifier les signatures numériques des paquets et des dépôts APT.

Installation de **apt-transport-https** pour ajouter la prise en charge du protocole HTTPS pour les dépôts APT. Par défaut, APT n'est configuré que pour le protocole HTTP.

```
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
```

curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH

Télécharge la clé GPG publique du dépôt Wazuh à partir de son URL.

La clé GPG est utilisée pour vérifier l'authenticité et l'intégrité des paquets provenant du dépôt Wazuh. Si un fichier est altéré ou non signé par cette clé, il sera rejeté par APT.

-s : Active le mode silencieux de curl, supprimant les messages inutiles pour rendre la commande plus propre.

| gpg --no-default-keyring --keyring gnupg-ring:/usr/share/keyrings/wazuh.gpg --import

--no-default-keyring : Empêche l'utilisation des trousseaux de clés (*keyrings*) GPG par défaut, garantissant que cette clé est ajoutée uniquement au fichier spécifié.

--keyring gnupg-ring:/usr/share/keyrings/wazuh.gpg :

Indique que la clé doit être importée dans un trousseau de clés spécifique, ici : /usr/share/keyrings/wazuh.gpg.

Cette pratique est recommandée pour isoler les clés des dépôts dans des fichiers distincts, évitant toute interférence ou confusion.

--import : Ajoute la clé téléchargée au trousseau de clés spécifié.

&& chmod 644 /usr/share/keyrings/wazuh.gpg

Définit les permissions du fichier wazuh.gpg pour qu'il soit lisible par tous les utilisateurs (lecture seule pour les autres et le groupe). Cela garantit que les processus système, y compris APT, peuvent accéder à cette clé pour vérifier les paquets téléchargés depuis le dépôt Wazuh.

Ajout du dépôt Wazuh à APT pour lui permettre de télécharger les paquets depuis le dépôt officiel de Wazuh.

```
echo "deb [signed-by=/usr/share/keyrings/wazuh.gpg]  
https://packages.wazuh.com/4.x/apt/ stable main" | tee -a  
/etc/apt/sources.list.d/wazuh.list  
apt update
```

A.2.2 Installation de l'indexeur

Installation du binaire de l'indexeur

```
apt -y install wazuh-indexer
```

Configuration de l'indexeur

```
nano /etc/wazuh-indexer/opensearch.yml
```

Préciser à la ligne suivante l'adresse IP de notre serveur Wazuh :

```
network.host: "192.168.2.1"
```

Créer une variable d'environnement pour déployer le certificat de l'indexeur. La valeur **node-1** est la même que vous avez renseigné dans votre fichier **config.yml**

```
NODE_NAME=node-1
```

Créer un répertoire dédié à la gestion des certificats pour Wazuh Indexer.

```
mkdir /etc/wazuh-indexer/certs
```

Extrait les certificats nécessaires du fichier archive **wazuh-certificates.tar** vers le répertoire **/etc/wazuh-indexer/certs/**.

```
tar -xf ./wazuh-certificates.tar -C /etc/wazuh-indexer/certs/  
./$NODE_NAME.pem ./$NODE_NAME-key.pem ./admin.pem ./admin-key.pem ./root-ca.pem
```

Extrait les certificats nécessaires du fichier archive **wazuh-certificates.tar** vers le répertoire **/etc/wazuh-indexer/certs/**.

Fichiers extraits :

\$NODE_NAME.pem : Certificat public pour le nœud Indexer.

\$NODE_NAME-key.pem : Clé privée correspondante pour le certificat du nœud.

admin.pem et admin-key.pem : Certificat et clé privée pour les connexions administratives.

root-ca.pem : Certificat d'autorité racine utilisé pour vérifier les autres certificats.

```
mv -n /etc/wazuh-indexer/certs/$NODE_NAME.pem  
/etc/wazuh-indexer/certs/indexer.pem  
mv -n /etc/wazuh-indexer/certs/$NODE_NAME-key.pem  
/etc/wazuh-indexer/certs/indexer-key.pem
```

Renommer les fichiers extraits en noms standard pour simplifier leur identification par le système Wazuh.

indexer.pem : Certificat du serveur Indexer.

indexer-key.pem : Clé privée associée.

Configurer les permissions de sécurité pour protéger les certificats

```
chmod 500 /etc/wazuh-indexer/certs  
chmod 400 /etc/wazuh-indexer/certs/*  
chown -R wazuh-indexer:wazuh-indexer /etc/wazuh-indexer/certs
```

Redémarrer les services

```
systemctl daemon-reload  
systemctl enable wazuh-indexer  
systemctl start wazuh-indexer
```

Exécuter le script qui permet de charger les certificats et de démarrer le cluster

```
/usr/share/wazuh-indexer/bin/indexer-security-init.sh
```

Réaliser un test pour vérifier que l'indexeur est opérationnel

```
curl -k -u admin:admin https://192.168.2.1:9200
```

```
{
  "name" : "node-1",
  "cluster_name" : "wazuh-cluster",
  "cluster_uuid" : "BlcLbEe3TiqUvw9vrG_YKw",
  "version" : {
    "number" : "7.10.2",
    "build_type" : "deb",
    "build_hash" : "7149046c7c9c64aa43e437826af0b8b0dcabd730",
    "build_date" : "2025-01-15T11:04:30.997631Z",
    "build_snapshot" : false,
    "lucene_version" : "9.11.1",
    "minimum_wire_compatibility_version" : "7.10.0",
    "minimum_index_compatibility_version" : "7.0.0"
  },
  "tagline" : "The OpenSearch Project: https://opensearch.org/"
}
```

A.2.3 Installation de Wazuh-manager

Installation du binaire du serveur Wazuh

```
apt-get -y install wazuh-manager
```

Redémarrer les services

```
systemctl daemon-reload
systemctl enable wazuh-manager
systemctl start wazuh-manager
```

Vérifier que le service est bien actif

```
systemctl status wazuh-manager
```

A.2.4 Installation de Filebeat

Filebeat est un outil léger de la suite **Elastic** utilisé pour collecter et transférer des journaux. Dans l'écosystème Wazuh, **Filebeat** joue un rôle important pour intégrer Wazuh avec la pile **Elastic Stack (Elasticsearch, Logstash, Kibana)**. Voici une explication de son rôle et de son utilité.

Filebeat agit comme un agent qui collecte les journaux générés par le Wazuh Manager ou les systèmes intégrés (comme les agents Wazuh) et les envoie vers **Elasticsearch** pour l'analyse et la visualisation.

Kibana, couplé à **Elasticsearch**, permet de visualiser ces alertes dans une interface utilisateur. Les tableaux de bord Wazuh disponibles dans **Kibana** exploitent ces données pour offrir une vue d'ensemble des menaces et des événements.

Installation du binaire de filebeat

```
apt-get -y install filebeat
```

Éditer le fichier de configuration

```
curl -so /etc/filebeat/filebeat.yml
https://packages.wazuh.com/4.7/tpl/wazuh/filebeat/filebeat.yml
nano /etc/filebeat/filebeat.yml Modifier la ligne suivante pour prendre en
compte l'adresse IP de notre serveur
hosts: ["192.168.2.1:9200"]
```

Filebeat utilise un magasin de clés sécurisé (*keystore*) pour stocker en toute sécurité des informations sensibles comme des mots de passe, des clés API, ou des jetons d'authentification.

Ce magasin de clés sécurisé permet de séparer les informations sensibles des fichiers de configuration, garantissant qu'elles ne soient pas stockées en texte clair dans des fichiers comme **filebeat.yml**.

Cette commande stocke le mot de passe "admin" dans le keystore sous la clé password. Comme pour le nom d'utilisateur, ce mot de passe sera utilisé par Filebeat pour se connecter à un serveur Elasticsearch ou Logstash.

```
filebeat keystore create
echo admin | filebeat keystore add username --stdin --force
echo admin | filebeat keystore add password --stdin --force
```

Télécharger le template de wazuh qui contient les alertes pour l'indexeur.

Cette commande permet d'obtenir le modèle de configuration JSON nécessaire pour Elasticsearch afin de s'assurer que les données de Wazuh sont indexées correctement dans Elasticsearch.

```
curl -so /etc/filebeat/wazuh-template.json
https://raw.githubusercontent.com/wazuh/wazuh/v4.7.3/extensions/elasticsearch/
7.x/wazuh-template.json
chmod go+r /etc/filebeat/wazuh-template.json
```

Télécharger et installer un module spécifique pour Filebeat afin de permettre à Filebeat de collecter et envoyer les journaux de Wazuh vers Elasticsearch (ou un autre stockage centralisé).

```
curl -s https://packages.wazuh.com/4.x/filebeat/wazuh-filebeat-0.3.tar.gz | tar
-xvz -C /usr/share/filebeat/module
```

Déployer les certificats pour Filebeat

Ces commandes sont utilisées pour gérer des certificats SSL/TLS pour Filebeat dans le cadre de l'intégration sécurisée avec Wazuh et Elasticsearch (ou un autre système centralisé de logs). Elles concernent l'extraction, la gestion des permissions, et la mise en place des certificats dans le répertoire de Filebeat.

```
NODE_NAME=wazuh-1
mkdir /etc/filebeat/certs
tar -xf ./wazuh-certificates.tar -C /etc/filebeat/certs/ ./${NODE_NAME}.pem
./${NODE_NAME}-key.pem ./root-ca.pem
mv -n /etc/filebeat/certs/${NODE_NAME}.pem /etc/filebeat/certs/filebeat.pem
mv -n /etc/filebeat/certs/${NODE_NAME}-key.pem /etc/filebeat/certs/filebeat-
key.pem
chmod 500 /etc/filebeat/certs
chmod 400 /etc/filebeat/certs/*
chown -R root:root /etc/filebeat/certs
```

Redémarrer les services

```
systemctl daemon-reload
systemctl enable filebeat
systemctl start filebeat
```

Tester filebeat pour vérifier qu'il n'y a aucune erreur

```
filebeat test output
```

A.2.5 Installation du dashboard Wazuh

Installation du binaire du dashboard

```
apt-get install debhelper tar curl libcap2-bin #debhelper version 9 or later
apt-get -y install wazuh-dashboard
```

Modifier le fichier de configuration du dashboard pour indiquer l'adresse IP du serveur

```
nano /etc/wazuh-dashboard/opensearch_dashboards.yml
```

Éditer le fichier de configuration et modifier les lignes suivantes :

```
server.host: 192.168.2.1
opensearch.hosts: https://192.168.2.1:9200
```


Installer les certificats pour le dashboard

```
NODE_NAME=dashboard
mkdir /etc/wazuh-dashboard/certs
tar -xf ./wazuh-certificates.tar -C /etc/wazuh-dashboard/certs/
./$NODE_NAME.pem ./$NODE_NAME-key.pem ./root-ca.pem
mv -n /etc/wazuh-dashboard/certs/$NODE_NAME.pem
/etc/wazuh-dashboard/certs/dashboard.pem
mv -n /etc/wazuh-dashboard/certs/$NODE_NAME-key.pem
/etc/wazuh-dashboard/certs/dashboard-key.pem
chmod 500 /etc/wazuh-dashboard/certs
chmod 400 /etc/wazuh-dashboard/certs/*
chown -R wazuh-dashboard:wazuh-dashboard /etc/wazuh-dashboard/certs
```

Redémarrer les services

```
systemctl daemon-reload
systemctl enable wazuh-dashboard
systemctl start wazuh-dashboard
```

A.3 INSTALLATION AVEC DOCKER COMPOSE

 **Attention** : suivre la procédure d'installation de Docker compose préconisée par Wazuh (<https://docs.docker.com/compose/install/>) pour télécharger un docker compose « autonome » : <https://documentation.wazuh.com/current/deployment-options/docker/docker-installation.html>

1. Clonez le dépôt git Wazuh sur votre système

```
git clone https://github.com/wazuh/wazuh-docker.git -b v4.10.1
```

Puis entrez dans le « single-node » un répertoire pour exécuter toutes les commandes décrites ci-après à l'intérieur de ce répertoire.

2. Générer les certificats pour les 3 composants (ici en conteneurs) de Wazuh

Exécuter la commande suivante pour obtenir les certificats souhaités :

```
docker-compose -f generate-indexer-certs.yml run --rm generator
```

Cela permet d'enregistrer les certificats dans le « config/wazuh_indexer_ssl_certs ».

3. Commencez le déploiement de Wazuh en utilisant docker-compose

```
docker-compose up -d
```

Cela permet d'enregistrer les certificats dans le « config/wazuh_indexer_ssl_certs ».

Le nom d'utilisateur et le mot de passe par défaut pour le tableau de bord Wazuh sont « **admin** » et « **SecretPassword** ». Pour plus de sécurité, vous pouvez changer le mot de passe par défaut pour l'utilisateur administrateur de l'indexeur Wazuh.

ATTENTION : Il faut attendre quelques minutes que l'ensemble des conteneurs démarre.

B. DÉPLOIEMENT DES AGENTS WAZUH

B.1 CRÉATION D'UN GROUPE D'AGENTS (FACULTATIF)

Aller dans le menu « Server management / Endpoint Groups / Add New group ».

Ajouter un nouveau groupe.

B.2 L'AGENT WAZUH

L'agent Wazuh est multi-plateforme et fonctionne sur les points d'extrémité que l'utilisateur souhaite surveiller. Il communique avec le serveur Wazuh, envoyant des données en temps quasi réel via un canal crypté et authentifié.



La compatibilité entre l'agent Wazuh et le gestionnaire Wazuh est garantie lorsque la version du gestionnaire de Wazuh est postérieure ou égale à celle de l'agent Wazuh.

Vous pouvez déployer un nouvel agent en suivant les instructions du tableau de bord de Wazuh. Allez dans Agents Management / Endpoints Summary, et cliquez sur « Deploy new agent ».

Il est nécessaire ensuite de saisir les informations, variables selon le système sur lequel l'agent va être installé, de manière à ce que Wazuh génère la commande adéquate.

B.2.1 L'agent Wazuh pour Windows

Prescriptions

- Vous aurez besoin de privilèges d'administrateur pour effectuer cette installation.
- PowerShell 3.0 ou plus est nécessaire.

Exécuter cette commande générée par Wazuh dans un terminal Windows Power Shell du point d'extrémité (en adaptant si nécessaire en fonction de la commande générée par Wazuh) :

```
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.11.1-1.msi -OutFile $env:tmp\wazuh-agent; msixexec.exe /i $env:tmp\wazuh-agent /q WAZUH_MANAGER='192.168.2.1' WAZUH_AGENT_GROUP='serveurs' WAZUH_AGENT_NAME='CubAD'
```

Démarrer l'agent :

```
NET START WazuhSvc
```

Si vous rencontrez un problème sur l'agent Windows, vous pouvez trouver le fichier journal dans C:\Program Files (x86)\ossec-agent\ossec.log (afficher les extensions).

Le fichier de configuration à éventuellement modifier est dans le même dossier et s'appelle « ossec.conf ». Si vous n'arrivez pas à éditer directement ce fichier avec le bloc note via un clic droit puis Ouvrir, lancez au préalable le bloc note et allez chercher le fichier.

Le principe est :

- d'arrêter le service ;
- de modifier le fichier de configuration ;
- de démarrer le service.

Une méthode plus radicale consiste à réinstaller l'agent. Pour cela :

- Télécharger le msi qui a permis de l'installer

```
invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.10.1-1.msi -OutFile $env:tmp\wazuh-agent
```

- Supprimer l'agent :

```
msiexec.exe /x $env:tmp\wazuh-agent /qn
```

- Supprimer le dossier C:\Program Files (x86)\ossec-agent\

B.2.2 L'agent Wazuh pour Linux

Prescriptions :

Vous avez besoin de privilèges d'utilisateur root pour exécuter toutes les commandes décrites ci-dessous.

Si les locales sont positionnées sur la langue française, Wazuh va remonter des faux positifs concernant l'installation des paquets, car les messages seront alors délivrés dans cette langue. Il est conseillé de garder les messages en Anglais :

- Ajout dans /etc/default/locale de LC_MESSAGES=en_US.UTF-8
- Déconnexion et reconnexion

Installation des paquets éventuellement manquants

- Vérification au préalable que les paquets suivants soient bien installés : sudo lsb-release, auditd et audispd-plugins
- Installation des paquets manquants.

Exécuter cette commande dans un terminal (en adaptant si nécessaire en fonction de la commande générée par Wazuh) :

```
wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.10.1-1_amd64.deb && sudo WAZUH_MANAGER='192.168.2.1' WAZUH_AGENT_GROUP='serveurs' WAZUH_AGENT_NAME='CubDHCP' dpkg -i ./wazuh-agent_4.10.1-1_amd64.deb
```

Démarrer l'agent :

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

Si vous rencontrez un problème sur l'agent Linux

Voici les étapes pour diagnostiquer et résoudre les problèmes

1. Vérifiez les journaux

Consultez les journaux sur l'agent et sur le manager pour identifier des messages d'erreur plus détaillés.

Journaux de l'agent

Sur la machine de l'agent, exécutez :

```
sudo tail -f /var/ossec/logs/ossec.log
```

Journaux du manager

Sur la machine du manager, exécutez :

```
sudo tail -f /var/ossec/logs/ossec.log
```

Recherchez des erreurs liées à SSL, des clés incompatibles ou d'autres problèmes réseau.

2. Vérifiez le service du manager Wazuh

Assurez-vous que le service Wazuh manager fonctionne correctement :

```
sudo systemctl status wazuh-manager
```

S'il n'est pas actif, redémarrez-le et recherchez les erreurs :

```
sudo systemctl restart wazuh-manager
```

```
sudo journalctl -xe | grep wazuh ou sudo journalctl -xeu wazuh-agent.service
```



À noter que l'erreur `SSL error: connection refused by the manager` dans Wazuh indique généralement un problème de connexion entre l'agent Wazuh et le manager Wazuh.

3. Vérifiez le nom d'hôte ou l'adresse IP du manager

Assurez-vous que l'agent Wazuh pointe vers le bon nom d'hôte ou la bonne adresse IP du manager Wazuh. Vérifiez le champ `address` dans la configuration de l'agent :

```
sudo nano /var/ossec/etc/ossec.conf.
```

Recherchez la section `<server>` :

```
xml
<server>
  <address>IP_OU_NOM_HOTE_DU_MANAGER</address>
  <port>1514</port> <!-- Port par défaut pour TCP -->
</server>
```

Assurez-vous que le champ `<address>` est correct et qu'il est accessible depuis la machine de l'agent. Testez la connectivité avec :

```
ping IP_OU_NOM_HOTE_DU_MANAGER
```

4. Vérifiez le port

Le port par défaut du manager Wazuh pour la communication des agents est 1514 (TCP) pour les connexions sécurisées. Assurez-vous que le port spécifié dans le champ `<port>` de `ossec.conf` est correct.

5. Paramètres du pare-feu

Assurez-vous que le pare-feu du manager autorise le trafic sur le port (par défaut : 1514) :

```
sudo ufw allow 1514/tcp
```

De même, assurez-vous que le pare-feu de la machine de l'agent autorise le trafic sortant vers le manager sur ce port.

6. Configuration SSL

Le message d'erreur indique un problème lié à SSL. Vérifiez les éléments suivants :

a. Certificats sur le manager

Assurez-vous que le manager dispose de certificats valides. Sur le manager, vérifiez les fichiers suivants :

```
sudo ls /var/ossec/etc/sslmanager.key
```

```
sudo ls /var/ossec/etc/sslmanager.cert
```

b. Certificats sur l'agent

Assurez-vous que l'agent possède la clé publique correcte du manager :

```
sudo ls /var/ossec/etc/client.keys
```

```
...
```

Si le fichier `client.keys` est manquant ou corrompu, il peut être nécessaire de réenregistrer l'agent avec le manager.

7. Réenregistrez l'agent

Pour vous assurer que l'agent est correctement enregistré auprès du manager, supprimez-le et ajoutez-le à nouveau. Sur le manager, exécutez :

```
sudo /var/ossec/bin/manage_agents
```

1. Choisissez ****Add Agent**** et suivez les instructions.

2. Sur l'agent, récupérez la clé d'enregistrement depuis le manager, puis utilisez-la pour enregistrer l'agent :

```
sudo /var/ossec/bin/agent-auth -m IP_OU_NOM_HOTE_DU_MANAGER
```

```
...
```

8. Testez la connectivité réseau

Sur la machine de l'agent, testez la connectivité vers le port du manager :

```
nc -zv IP_OU_NOM_HOTE_DU_MANAGER 1514
```

Si la connexion échoue, le problème vient probablement du réseau ou d'une mauvaise configuration du pare-feu.

9. Mettez à jour l'agent et le manager

Assurez-vous que l'agent et le manager Wazuh utilisent des versions compatibles :

```
sudo /var/ossec/bin/wazuh-control info
```

Mettez-les à jour si nécessaire.

Résumé des étapes :

1. Vérifiez que l'adresse et le port dans `ossec.conf` sont corrects.
2. Assurez-vous que les certificats SSL sont valides et bien configurés.
3. Vérifiez les pare-feux et la connectivité réseau.
4. Réenregistrez l'agent si nécessaire.
5. Mettez à jour vos versions Wazuh pour éviter tout problème de compatibilité.

B.3 AJOUT OU SUPPRESSION D'UN AGENT À UN GROUPE

Il est possible d'affecter un agent à un groupe à l'aide de l'outil `/var/ossec/bin/agent_groups` présent sur le serveur Wazuh. Par exemple, Pour affecter un agent Wazuh avec un ID 001 (l'ID est repéré sur le serveur) au groupe préalablement créé, par exemple, « Serveurs_Linux » :

```
/var/ossec/bin/agent_groups -q -a -i 001 -g Serveurs_Linux
```

Notes :

- Le groupe doit être créé et configuré avant d'attribuer des agents. Vous pouvez créer des groupes d'agents à l'aide de l'outil `/var/ossec/bin/agent_groups`. Le nom du groupe ne peut contenir que des lettres majuscules/minuscules, des chiffres, des points, des traits de soulignement et des tirets.
- L'option « -q » (pour « quiet ») permet de ne demander aucune confirmation.

Pour supprimer un agent d'un groupe, il faut utiliser l'option « -r ». Par exemple :

```
/var/ossec/bin/agent_groups -q -r -i 001 -g default
```

C. MISE À JOUR DU SERVEUR WAZUH ET DES AGENTS

La mise à jour de Wazuh et de ses agents est essentielle pour maintenir la sécurité et la performance de votre infrastructure. Voici un guide détaillé pour effectuer la mise à jour.

C.1 MISE À JOUR DU SERVEUR WAZUH

- Vérifier la version actuelle du serveur Wazuh :

```
# /var/ossec/bin/wazuh-control info
WAZUH_VERSION="v4.10.1"
WAZUH_REVISION="41011"
WAZUH_TYPE="server"
```

- Mettre à jour les dépôts :

```
sudo apt-get update
```

- Mettre à jour les paquets :

```
sudo apt-get full-upgrade
```

 Cette commande met tous les paquets à jour et redémarre tous les services.

Il est conseillé de vérifier que les composants ont correctement redémarré.

- Vérifier le statut du **service Indexer** :

```
# systemctl status wazuh-indexer
● wazuh-indexer.service - wazuh-indexer
   Loaded: loaded (/lib/systemd/system/wazuh-indexer.service; enabled; vendor preset: enabled)
   Active: active (running) since Sun 2025-03-16 10:52:15 CET; 10min ago
     Docs: https://documentation.wazuh.com
   Main PID: 17392 (java)
    Tasks: 81 (limit: 9439)
   Memory: 1.3G
      CPU: 1min 14.098s
   CGroup: /system.slice/wazuh-indexer.service
           └─17392 /usr/share/wazuh-indexer/jdk/bin/java -Xshare:auto
-Dopensearch.networkaddress.cache.ttl=60
-Dopensearch.networkaddress.cache.negative.ttl=10 ->
mars 16 10:51:56 siem systemd-entrypoint[17392]: WARNING:
System::setSecurityManager has been called by
org.opensearch.bootstrap.OpenSearch (file:/usr/share/wazuh-i>
```

- Vérifier le statut du **service Dashboard** :

```
# systemctl status wazuh-dashboard
● wazuh-dashboard.service - wazuh-dashboard
   Loaded: loaded (/etc/systemd/system/wazuh-dashboard.service; enabled; vendor preset: enabled)
   Active: active (running) since Sun 2025-03-16 13:47:46 CET; 6s ago
   Main PID: 65179 (node)
    Tasks: 11 (limit: 9439)
   Memory: 218.9M
      CPU: 6.370s
   CGroup: /system.slice/wazuh-dashboard.service
           └─65179 /usr/share/wazuh-dashboard/node/bin/node --no-warnings --max-http-header-size=65536 --unhandled-re>
mars 16 13:47:51 siem opensearch-dashboards[65179]: [agentkeepalive:deprecated] options.freeSocketKeepAliveTimeout is d>
```

- Vérifier la version de Wazuh et des agents sur Wazuh :

```
# /var/ossec/bin/wazuh-control info
WAZUH_VERSION="v4.11.1"
WAZUH_REVISION="41112"
WAZUH_TYPE="server"
```

The screenshot shows the Wazuh dashboard with the following components:

- Agents par statut:** A donut chart showing 2 active agents, 0 disconnected, 0 suspended, and 0 never connected.
- TOP 5 OS:** A donut chart showing 1 Windows and 1 Ubuntu.
- Cinq groupes les plus...**: A donut chart showing the top 5 groups.
- Agents 2:** A table listing the agents with columns for ID, Nom, Adresse IP, Groupe(s), Système d'exploitation, Noeud de cluster, Version, État d'avancement, and Actions.

ID	Nom	Adresse IP	Groupe(s)	Système d'exploitation	Noeud de cluster	Version	État d'avancement	Actions
001	CubAD	192.168.1.134	par défaut	Microsoft Windows Server 2022 Standard	nod01	v4.10.1	actif	🔍 ⋮
002	CubDHCP	192.168.1.189	par défaut	Ubuntu 22.04.2 LTS	nod01	v4.10.1	actif	🔍 ⋮

C.2 MISE À JOUR DES AGENTS WAZUH

C.2.1 Mise à jour des agents sur Ubuntu/Debian

- Vérifier la version actuelle de l'agent sur le serveur wazuh :

```
# /var/ossec/bin/wazuh-agentlessd -V
```

Wazuh v4.11.1 - Wazuh Inc.

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License (version 2) as published by the Free Software Foundation. For more details, go to <https://www.gnu.org/licenses/gpl.html>

- Mettre à jour les agents sur le client Ubuntu/Debian (commande générée depuis l'ajout d'un agent sur l'interface du serveur Wazuh) :

```
# wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.11.1-1_amd64.deb && sudo WAZUH_MANAGER='192.168.1.139' dpkg -i ./wazuh-agent_4.11.1-1_amd64.deb
```

- Redémarrer l'agent après la mise à jour :

```
sudo systemctl daemon-reload  
sudo systemctl restart wazuh-agent
```

C.2.2 Mise à jour des agents sur Windows

- Vérifier la version installée en powershell :

```
notepad.exe "C:\Program Files (x86)\ossec-agent\VERSION"
```

- Télécharger et installer la dernière version de l'agent Wazuh.

```
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.11.1-1.msi -OutFile $env:tmp\wazuh-agent; msixexec.exe /i $env:tmp\wazuh-agent /q WAZUH_MANAGER='192.168.1.139'
```

