Documentation d'Installation et Configuration Wazuh

Guide complet d'installation d'une VM Wazuh Server et configuration d'agent Windows

Date: Mars 2026
Version: Wazuh 4.14 LTS
Système: Debian 12 / Ubuntu 24.04
Serveur Windows surveillé: 172.20.0.14

Introduction

Ce document présente la procédure complète d'installation et de configuration d'une machine virtuelle Wazuh Server ainsi que la configuration d'un agent Wazuh sur un serveur Windows pour permettre la détection des menaces, l'analyse de sécurité et la conformité[1].

Wazuh est une plateforme de sécurité open-source unifiée qui offre des capacités de détection des menaces, de surveillance de l'intégrité, de réponse aux incidents et de conformité réglementaire (PCI DSS, HIPAA, GDPR)[2].

Objectifs de cette documentation

- Déployer une VM Wazuh Server complète (Indexer + Manager + Dashboard)
- Configurer les certificats SSL/TLS pour les communications sécurisées
- Déployer l'agent Wazuh sur le serveur Windows (172.20.0.14)
- Établir la supervision et détection de menaces sur le serveur Windows
- Configurer les règles de détection et alertes

Architecture Wazuh

Wazuh est composé de trois composants principaux[31]:

- **Wazuh Indexer**: Stocke et indexe les données de sécurité (basé sur OpenSearch)
- **Wazuh Manager**: Collecte et analyse les données des agents, déclenche les alertes
- **Wazuh Dashboard**: Interface web pour visualisation et gestion (port 443)

Prérequis

Configuration matérielle recommandée

Composant	Spécification minimale
CPU	4 vCPU (2 minimum)
RAM	8 Go (4 Go minimum)
Disque dur	50 Go (données de sécurité volumineuses)
Réseau	Interface réseau configurée

Table 1: Configuration recommandée pour VM Wazuh

Logiciels requis

- Hyperviseur: VMware, VirtualBox, Hyper-V ou KVM
- ISO Debian 12 ou Ubuntu 24.04 LTS
- Accès administrateur sur le serveur Windows (172.20.0.14)
- Connexion Internet pour téléchargement des packages
- 16 Go de RAM recommandés pour environnement de production

Informations réseau

- Serveur Windows cible: **172.20.0.14**
- Port agent Wazuh: **1514** (TCP, pour enrôlement)
- Port agent Wazuh: **1515** (TCP, communication agent-manager)
- Port Dashboard Wazuh: **443** (HTTPS)
- Port Wazuh API: **55000** (TCP)
- Port Wazuh Indexer: **9200** (TCP)

Partie 1: Installation du Serveur Wazuh (All-in-One)

Étape 1: Préparation de la VM

1.1 Créer la machine virtuelle

1. Créer une nouvelle VM dans votre hyperviseur
2. Allouer les ressources (4 vCPU, 8 Go RAM, 50 Go disque)
3. Monter l'ISO Debian 12 ou Ubuntu 24.04
4. Démarrer l'installation de l'OS
5. Configurer un utilisateur avec privilèges sudo

1.2 Configuration réseau de base

Après installation de l'OS, configurez une IP statique pour la VM Wazuh:

Exemple pour Debian/Ubuntu avec netplan

sudo nano /etc/netplan/00-installer-config.yaml

Configuration réseau:

network:
version: 2
ethernets:
ens33:
addresses:
- 172.20.0.10/24
gateway4: 172.20.0.1
nameservers:
addresses: [8.8.8.8, 1.1.1.1]

Appliquer la configuration:

sudo netplan apply

1.3 Mise à jour du système

Mettre à jour le système

sudo apt update && sudo apt upgrade -y

Installer les dépendances nécessaires

sudo apt install curl apt-transport-https unzip wget gnupg -y

Étape 2: Installation automatique avec Wazuh Installation Assistant

Wazuh fournit un assistant d'installation automatique qui déploie tous les composants en une seule commande[35].

2.1 Téléchargement de l'assistant d'installation

Télécharger l'assistant d'installation

curl -sO https://packages.wazuh.com/4.14/wazuh-install.sh

Télécharger le fichier de configuration

curl -sO https://packages.wazuh.com/4.14/config.yml

2.2 Configuration du fichier config.yml

Éditer le fichier de configuration[36]:

sudo nano config.yml

Contenu du fichier (installation All-in-One sur un seul nœud):

nodes:

Wazuh indexer nodes

indexer:
- name: node-1
ip: "172.20.0.10"

Wazuh server nodes

server:
- name: wazuh-1
ip: "172.20.0.10"

Wazuh dashboard nodes

dashboard:
- name: dashboard
ip: "172.20.0.10"

Note importante: Les trois composants utilisent la même IP (172.20.0.10) car ils sont installés sur la même VM.

2.3 Génération des certificats SSL/TLS

Générer les certificats pour communications sécurisées

sudo bash wazuh-install.sh --generate-config-files

Les certificats sont créés dans wazuh-install-files.tar

2.4 Installation complète automatique

Installation All-in-One (Indexer + Manager + Dashboard)

sudo bash wazuh-install.sh --all-in-one

Cette commande installe et configure automatiquement[38]:

- Wazuh Indexer (stockage et indexation des données)
- Wazuh Manager (analyse et traitement)
- Filebeat (transfert sécurisé des données)
- Wazuh Dashboard (interface web)
- Configuration des certificats SSL/TLS
- Démarrage automatique de tous les services

 Durée d'installation: Environ 10-15 minutes selon la connexion Internet.

2.5 Récupération des identifiants

À la fin de l'installation, l'assistant affiche les identifiants du Dashboard[42]:

INFO: --- Summary ---
INFO: You can access the web interface https://172.20.0.10:443
User: admin
Password: <MOT_DE_PASSE_GENERE>

IMPORTANT: Notez immédiatement ce mot de passe, il ne sera plus affiché.

Étape 3: Vérification de l'installation

3.1 Vérification des services

Vérifier le statut du Wazuh Manager

sudo systemctl status wazuh-manager

Vérifier le statut du Wazuh Indexer

sudo systemctl status wazuh-indexer

Vérifier le statut du Wazuh Dashboard

sudo systemctl status wazuh-dashboard

Vérifier le statut de Filebeat

sudo systemctl status filebeat

Tous les services doivent être **active (running)**.

3.2 Vérification des ports

Vérifier les ports en écoute

sudo netstat -tlnp | grep -E '443|9200|55000|1514|1515'

Ports attendus:

- **443**: Wazuh Dashboard (HTTPS)
- **9200**: Wazuh Indexer (API)

- **55000**: Wazuh Manager API
- **1514**: Wazuh Manager (enrôlement agent)
- **1515**: Wazuh Manager (communication agent)

Étape 4: Accès au Dashboard Wazuh

4.1 Connexion à l'interface web

Ouvrir un navigateur et accéder à:

https://172.20.0.10

Note: Le certificat SSL est auto-signé, vous devrez accepter l'avertissement de sécurité du navigateur.

4.2 Connexion initiale

Identifiants[40]:

- Username: **admin**
- Password: **<mot de passe généré à l'étape 2.5>**

4.3 Changement du mot de passe administrateur

IMPORTANT: Changez immédiatement le mot de passe par défaut:

1. Cliquer sur l'icône utilisateur (en haut à droite)
2. Aller dans **Security** > **Users**
3. Sélectionner l'utilisateur **admin**
4. Cliquer sur **Edit user**
5. Définir un nouveau mot de passe fort
6. Sauvegarder

Partie 2: Installation de l'agent Wazuh sur Windows

Étape 5: Téléchargement de l'agent Windows

5.1 Obtenir le package MSI

Deux méthodes possibles:

Méthode 1: Depuis le Dashboard Wazuh

1. Se connecter au Dashboard: https://172.20.0.10
2. Aller dans **Agents** > **Deploy new agent**
3. Sélectionner **Windows**
4. Copier la commande d'installation générée

Méthode 2: Téléchargement direct

Se rendre sur: https://packages.wazuh.com/4.x/windows/

Télécharger: `wazuh-agent-4.14.3-1.msi`

Étape 6: Installation de l'agent sur Windows (172.20.0.14)

6.1 Installation en ligne de commande (Recommandée)

Ouvrir PowerShell en tant qu'Administrateur sur le serveur Windows (172.20.0.14)[40]:

Télécharger l'agent (si pas déjà fait)

Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.14.3-1.msi -OutFile $env:TEMP\wazuh-agent.msi

Installer l'agent avec enrôlement automatique

msiexec.exe /i $env:TEMP\wazuh-agent.msi /q WAZUH_MANAGER="172.20.0.10" WAZUH_AGENT_NAME="WIN-SRV-2024"

Paramètres d'installation:

Paramètre	Description
WAZUH_MANAGER	IP du serveur Wazuh (172.20.0.10)
WAZUH_AGENT_NAME	Nom de l'agent (WIN-SRV-2024)
WAZUH_REGISTRATION_SERVER	Serveur d'enrôlement (optionnel)
WAZUH_REGISTRATION_PASSWORD	Mot de passe d'enrôlement (optionnel)

Table 2: Paramètres d'installation de l'agent Windows

6.2 Démarrage du service

Démarrer le service Wazuh

NET START WazuhSvc

Ou avec PowerShell

Start-Service wazuhsvc

Vérifier le statut

Get-Service wazuhsvc

6.3 Installation via GUI (Alternative)

1. Double-cliquer sur le fichier MSI téléchargé
2. Suivre l'assistant d'installation
3. Entrer l'adresse du serveur: **172.20.0.10**
4. Entrer le nom d'agent: **WIN-SRV-2024**
5. Terminer l'installation
6. Démarrer le service via l'interface graphique

Étape 7: Configuration manuelle de l'agent (si nécessaire)

7.1 Éditer le fichier de configuration

L'agent est installé dans:

C:\Program Files (x86)\ossec-agent

Éditer le fichier de configuration[37]:

C:\Program Files (x86)\ossec-agent\ossec.conf

Configuration essentielle:

<ossec_config>
172.20.0.10 1514 tcp

<client_buffer>
no
</client_buffer>
</ossec_config>

7.2 Configuration avancée

Activation de la surveillance des logs Windows:

Application eventchannel Security eventchannel System eventchannel

7.3 Redémarrage du service après modification

Redémarrer le service

Restart-Service wazuhsvc

Vérifier le statut

Get-Service wazuhsvc

Étape 8: Configuration du pare-feu Windows

8.1 Autoriser les ports nécessaires

Ouvrir PowerShell en Administrateur:

Autoriser la communication avec le Wazuh Manager (port 1514)

```
New-NetFirewallRule -DisplayName "Wazuh Agent - Registration" -
Direction Outbound
-Protocol TCP -RemoteAddress 172.20.0.10
-RemotePort 1514 `
-Action Allow
```

Autoriser la communication avec le Wazuh Manager (port 1515)

```
New-NetFirewallRule -DisplayName "Wazuh Agent - Communication"
-Direction Outbound
-Protocol TCP -RemoteAddress 172.20.0.10
-RemotePort 1515 `
-Action Allow
```

8.2 Vérification des règles

1. Ouvrir "Pare-feu Windows Defender avec sécurité avancée"
2. Aller dans "Règles de trafic sortant"
3. Vérifier que les règles "Wazuh Agent" sont activées

Étape 9: Vérification de l'enrôlement de l'agent

9.1 Depuis le Dashboard Wazuh

1. Se connecter au Dashboard: https://172.20.0.10
2. Aller dans **Agents**
3. L'agent "WIN-SRV-2024" doit apparaître avec le statut **Active**
4. Vérifier l'adresse IP: 172.20.0.14

9.2 Depuis le serveur Wazuh (ligne de commande)

Lister tous les agents enrôlés

sudo /var/ossec/bin/agent_control -l

Vérifier le statut d'un agent spécifique

sudo /var/ossec/bin/agent_control -i 001

Sortie attendue:

Wazuh agent_control. Agent information:
Agent ID: 001
Agent Name: WIN-SRV-2024
IP address: 172.20.0.14
Status: Active

9.3 Vérification des logs sur Windows

Consulter les logs de l'agent

Get-Content "C:\Program Files (x86)\ossec-agent\ossec.log" -Tail 50

Messages attendus:

INFO: Connected to the server (172.20.0.10:1514/1515).
INFO: Agent started.

Partie 3: Configuration de la supervision

Étape 10: Exploration du Dashboard

10.1 Vue d'ensemble de la sécurité

1. Aller dans **Security Events**
2. Consulter le résumé des alertes en temps réel
3. Vérifier les événements de l'agent WIN-SRV-2024

10.2 Modules de sécurité disponibles

- **Security Events**: Événements de sécurité en temps réel
- **Integrity Monitoring**: Surveillance de l'intégrité des fichiers (FIM)
- **Vulnerability Detection**: Détection de vulnérabilités
- **Configuration Assessment**: Évaluation de la configuration (SCA)
- **Threat Hunting**: Chasse aux menaces
- **Regulatory Compliance**: Conformité (PCI DSS, GDPR, HIPAA)
- **MITRE ATT&CK**: Mapping des tactiques et techniques d'attaque

Étape 11: Configuration de la détection de vulnérabilités

11.1 Activer la détection de vulnérabilités

Éditer la configuration sur le serveur Wazuh:

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

Ajouter ou vérifier la section:

yes 5m yes yes 1h
Redémarrer le manager:

sudo systemctl restart wazuh-manager

11.2 Consulter les vulnérabilités détectées

1. Aller dans **Vulnerability Detection**
2. Filtrer par agent: WIN-SRV-2024
3. Analyser les vulnérabilités critiques et hautes
4. Télécharger le rapport pour remédiation

Étape 12: Configuration de la surveillance d'intégrité (FIM)

12.1 Configuration FIM sur Windows

Éditer le fichier sur Windows:

C:\Program Files (x86)\ossec-agent\ossec.conf

Ajouter la surveillance de répertoires critiques:

no 43200 C:\Windows\System32 C:\Program Files C:\Users\Administrator\Desktop HKEY_LOCAL_MACHINE\Software HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services
Redémarrer l'agent:

Restart-Service wazuhsvc

12.2 Tester la détection FIM

1. Créer un fichier test sur le bureau Windows
2. Attendre quelques minutes
3. Dans le Dashboard: **Integrity Monitoring**
4. Vérifier l'alerte de création de fichier

Étape 13: Configuration des alertes personnalisées

13.1 Créer une règle personnalisée

Éditer le fichier des règles locales sur le serveur Wazuh:

sudo nano /var/ossec/etc/rules/local_rules.xml

Exemple: Alerte pour échecs de connexion Windows:

60122 failed Multiple Windows authentication failures detected T1110
13.2 Activer la règle

Vérifier la syntaxe

sudo /var/ossec/bin/wazuh-logtest

Redémarrer le manager

sudo systemctl restart wazuh-manager

Étape 14: Configuration des notifications email

14.1 Configuration SMTP sur le serveur Wazuh

Éditer la configuration:

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

Ajouter la section email:

yes smtp.votredomaine.com wazuh@votredomaine.com
admin@votredomaine.com 12
<email_alerts>
<email_to>admin@votredomaine.com</email_to>
10 authentication_failed,
<do_not_delay/>
</email_alerts>

14.2 Redémarrer le service

sudo systemctl restart wazuh-manager

14.3 Tester les alertes email

Tester l'envoi d'email

sudo /var/ossec/bin/wazuh-maild -t

Partie 4: Configuration avancée

Étape 15: Évaluation de la configuration (SCA)

15.1 Activer les politiques SCA pour Windows

Les politiques SCA (Security Configuration Assessment) sont activées par défaut[40].

Politiques disponibles pour Windows:

- CIS Benchmark for Windows Server 2016/2019/2022
- CIS Benchmark for Windows 10/11
- PCI DSS compliance checks

15.2 Consulter les résultats SCA

1. Aller dans **Configuration Assessment**
2. Sélectionner l'agent WIN-SRV-2024
3. Analyser les checks passés/échoués
4. Télécharger le rapport de conformité

Étape 16: Réponse active automatique

16.1 Configurer une réponse active

Éditer la configuration sur le serveur:

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

Exemple: Bloquer automatiquement après 5 échecs de connexion:

win_route-null route-null.exe yes no win_route-null local 60122 1800
16.2 Redémarrer le manager

sudo systemctl restart wazuh-manager

Étape 17: Intégration avec MITRE ATT&CK

17.1 Activer le mapping MITRE

1. Aller dans **MITRE ATT&CK**
2. Sélectionner l'agent WIN-SRV-2024
3. Visualiser les tactiques et techniques détectées
4. Identifier les vecteurs d'attaque potentiels

17.2 Analyser les techniques d'attaque

Exemple de techniques détectées:

- T1110 - Brute Force (tentatives de connexion multiples)
- T1078 - Valid Accounts (utilisation de comptes valides)
- T1059 - Command and Scripting Interpreter (exécution PowerShell)
- T1003 - OS Credential Dumping (tentative d'extraction de credentials)

Dépannage

Problèmes courants et solutions

Problème 1: L'agent n'apparaît pas dans le Dashboard

Diagnostic:

Depuis le serveur Wazuh, vérifier les connexions

sudo tail -f /var/ossec/logs/ossec.log | grep -i agent

Sur Windows, vérifier les logs de l'agent

Get-Content "C:\Program Files (x86)\ossec-agent\ossec.log" -Tail 50

Solutions:

- Vérifier la connectivité réseau: ping 172.20.0.10
- Tester la connexion aux ports:
  - Test-NetConnection -ComputerName 172.20.0.10 -Port 1514
  - Test-NetConnection -ComputerName 172.20.0.10 -Port 1515
- Vérifier le pare-feu Windows (autoriser ports 1514 et 1515 sortants)
- Vérifier que le service WazuhSvc est démarré
- Redémarrer l'agent: Restart-Service wazuhsvc

Problème 2: Dashboard inaccessible

Solutions:

- Vérifier que le service est actif: sudo systemctl status wazuh-dashboard
- Vérifier le port 443: sudo netstat -tlnp | grep 443
- Consulter les logs: sudo journalctl -u wazuh-dashboard -f
- Redémarrer le dashboard: sudo systemctl restart wazuh-dashboard
- Vérifier les certificats SSL: ls -la /etc/wazuh-dashboard/certs/

Problème 3: Erreur "Unable to connect to Wazuh API"

Solutions:

- Vérifier que le Wazuh Manager est actif: sudo systemctl status wazuh-manager
- Vérifier l'API: curl -k -u admin:admin https://172.20.0.10:55000/
- Régénérer le mot de passe API si nécessaire
- Vérifier la configuration dans /etc/wazuh-dashboard/opensearch_dashboards.yml

Problème 4: Agent status "Disconnected"

Diagnostic:

Vérifier le statut exact de l'agent

sudo /var/ossec/bin/agent_control -i 001

Solutions:

- Vérifier que l'IP du manager est correcte dans ossec.conf (Windows)
- Vérifier que le service est démarré: Get-Service wazuhsvc
- Consulter les logs Windows pour erreurs de connexion
- Réenrôler l'agent si nécessaire:
  - Supprimer l'agent du Dashboard
  - Supprimer le client.keys sur Windows
  - Réinstaller l'agent

Problème 5: Vulnérabilités non détectées

Solutions:

- Vérifier que le module est activé: grep -A 5 "vulnerability-detector" /var/ossec/etc/ossec.conf
- Forcer une mise à jour: sudo /var/ossec/bin/wazuh-modulesd
- Attendre la première analyse (peut prendre 15-30 minutes)
- Consulter les logs: sudo tail -f /var/ossec/logs/ossec.log | grep -i vulnerability

---

Commandes de référence rapide

Serveur Wazuh (Linux)

Gestion des services

sudo systemctl start wazuh-manager
sudo systemctl stop wazuh-manager
sudo systemctl restart wazuh-manager
sudo systemctl status wazuh-manager

sudo systemctl start wazuh-indexer
sudo systemctl status wazuh-indexer

sudo systemctl start wazuh-dashboard
sudo systemctl status wazuh-dashboard

Gestion des agents

sudo /var/ossec/bin/agent_control -l # Lister tous les agents
sudo /var/ossec/bin/agent_control -i 001 # Info agent ID 001
sudo /var/ossec/bin/manage_agents -l # Lister agents enrôlés
sudo /var/ossec/bin/manage_agents -r 001 # Supprimer agent ID 001

Consultation des logs

sudo tail -f /var/ossec/logs/ossec.log # Logs généraux
sudo tail -f /var/ossec/logs/alerts/alerts.log # Alertes
sudo journalctl -u wazuh-manager -f # Logs systemd

Test de règles

sudo /var/ossec/bin/wazuh-logtest

Vérification de la configuration

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

Agent Windows (PowerShell)

Gestion du service

Get-Service wazuhsvc
Start-Service wazuhsvc
Stop-Service wazuhsvc
Restart-Service wazuhsvc

Vérification des logs

Get-Content "C:\Program Files (x86)\ossec-agent\ossec.log" -Tail 50

Test de connectivité

Test-NetConnection -ComputerName 172.20.0.10 -Port 1514
Test-NetConnection -ComputerName 172.20.0.10 -Port 1515

Vérification des règles pare-feu

Get-NetFirewallRule | Where-Object {$_.DisplayName -like "*Wazuh*"}

Forcer un scan FIM

Restart-Service wazuhsvc

API Wazuh

Authentification et token

curl -u admin:admin -k -X GET "https://172.20.0.10:55000/security/user/authenticate?raw=true"

Lister les agents (avec token)

curl -k -X GET "https://172.20.0.10:55000/agents" -H "Authorization: Bearer $TOKEN"

Obtenir les alertes

curl -k -X GET "https://172.20.0.10:55000/alerts" -H "Authorization: Bearer $TOKEN"

Maintenance et bonnes pratiques

Sauvegarde régulière

Base de données Wazuh Indexer

Créer un snapshot du Wazuh Indexer

curl -XPUT "https://172.20.0.10:9200/*snapshot/my_backup/snapshot*$(date +%Y%m%d)"
-H 'Content-Type: application/json'
-u admin:admin -k

Sauvegarder les configurations

sudo tar -czf /backup/wazuh-config-$(date +%Y%m%d).tar.gz
/var/ossec/etc/
/etc/filebeat/
/etc/wazuh-dashboard/

Fichiers de configuration Windows

Sauvegarder la configuration de l'agent

Copy-Item "C:\Program Files (x86)\ossec-agent\ossec.conf" `
-Destination "C:\Backup\ossec.conf.$(Get-Date -Format 'yyyyMMdd')"

Mises à jour

Mise à jour du serveur Wazuh

Vérifier la version actuelle

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

Mettre à jour (avec l'assistant)

curl -sO https://packages.wazuh.com/4.x/wazuh-upgrade.sh
sudo bash wazuh-upgrade.sh

Ou mise à jour manuelle

sudo apt update
sudo apt upgrade wazuh-manager wazuh-indexer wazuh-dashboard

Mise à jour de l'agent Windows

1. Télécharger la nouvelle version MSI
2. Arrêter le service: Stop-Service wazuhsvc
3. Exécuter le nouvel installateur (écrase l'ancienne version)
4. La configuration est automatiquement préservée
5. Démarrer le service: Start-Service wazuhsvc

Optimisation des performances

Serveur Wazuh

- Ajuster le niveau de log pour réduire le volume de données
- Configurer la rotation des logs
- Limiter la fréquence des scans FIM (frequency dans syscheck)
- Utiliser des filtres pour ignorer les événements non pertinents
- Monitorer l'utilisation CPU/RAM/Disque du serveur

Configuration de rotation des logs

sudo nano /etc/logrotate.d/wazuh

/var/ossec/logs/ossec.log {
daily
rotate 7
compress

missingok
notifempty
postrotate
/var/ossec/bin/wazuh-control restart > /dev/null 2>&1 || true
endscript
}

Surveillance du serveur Wazuh

Auto-surveillance (Wazuh monitor himself)

Le serveur Wazuh peut se surveiller lui-même:

1. Installer l'agent Wazuh localement sur le serveur
2. L'enrôler comme agent
3. Surveiller les métriques: CPU, RAM, disque, services

Politique de rétention des données

Configurer la rétention des indices dans le Wazuh Indexer:

Configuration de la rétention (30 jours par défaut)

curl -XPUT "https://172.20.0.10:9200/_cluster/settings"
-H 'Content-Type: application/json'
-u admin:admin -k
-d '{
"persistent": {
"indices.lifecycle.rollover.max_age": "30d"
}
}'

Cas d'usage avancés

Cas 1: Détection d'attaque par force brute

Configuration automatique:

- Règle 60122: Détection d'échecs d'authentification Windows
- Niveau 10: Alerte critique après 5 échecs
- Réponse active: Blocage automatique de l'IP source
- Email d'alerte envoyé à l'administrateur

Cas 2: Surveillance de conformité PCI DSS

1. Activer les politiques SCA pour PCI DSS
2. Configurer la surveillance FIM sur les fichiers sensibles (cardholder data)
3. Activer les logs d'accès aux bases de données
4. Générer des rapports de conformité mensuels

Cas 3: Chasse aux menaces (Threat Hunting)

Utiliser le module Threat Hunting:

1. Aller dans **Threat Hunting**
2. Rechercher des indicateurs de compromission (IOC)
3. Analyser les processus suspects (PowerShell encodé, cmd.exe inhabituel)
4. Corréler les événements sur la timeline
5. Exporter les résultats pour analyse forensique

Cas 4: Détection de malware et ransomware

Configuration:

- Surveillance FIM sur répertoires critiques (realtime="yes")
- Détection de modifications massives de fichiers (indicateur ransomware)
- Surveillance de création de fichiers .encrypted, .locked, etc.
- Alerte immédiate et réponse active (isolation de l'endpoint)

Conclusion

Vous avez maintenant une installation complète et opérationnelle de Wazuh comprenant:

- Un serveur Wazuh complet (Indexer + Manager + Dashboard)
- Des certificats SSL/TLS configurés pour communications sécurisées
- Un agent Wazuh déployé sur le serveur Windows (172.20.0.14)
- Détection des menaces en temps réel
- Détection de vulnérabilités automatique
- Surveillance de l'intégrité des fichiers (FIM)
- Évaluation de la configuration de sécurité (SCA)
- Conformité réglementaire (PCI DSS, GDPR, HIPAA)
- Mapping MITRE ATT&CK
- Réponses actives automatiques

Cette infrastructure vous permet de:

- Détecter les menaces et anomalies de sécurité en temps réel
- Surveiller la conformité réglementaire
- Analyser les vulnérabilités du système
- Répondre automatiquement aux incidents
- Générer des rapports d'audit détaillés
- Effectuer de la chasse aux menaces proactive

Prochaines étapes recommandées

1. Déployer des agents sur d'autres serveurs et endpoints
2. Configurer des alertes personnalisées selon vos besoins
3. Intégrer Wazuh avec un SIEM externe (Splunk, ELK)
4. Configurer l'intégration avec des services tiers (Slack, PagerDuty)
5. Implémenter une architecture haute disponibilité (multi-nœuds)
6. Former les équipes SOC à l'utilisation du Dashboard
7. Créer des playbooks de réponse aux incidents
8. Automatiser la génération de rapports de conformité
9. Configurer la surveillance des applications critiques (IIS, SQL Server, AD)
10. Explorer les intégrations cloud (AWS, Azure, GCP)

Ressources complémentaires

- Documentation officielle Wazuh: https://documentation.wazuh.com
- Wazuh GitHub: https://github.com/wazuh/wazuh
- Forum communautaire: https://groups.google.com/g/wazuh
- Ruleset officiel: https://github.com/wazuh/wazuh-ruleset
- Blog Wazuh: https://wazuh.com/blog/

Références

[1] Wazuh Documentation. (2026). Installation guide. https://documentation.wazuh.com/current/installation-guide/index.html

[2] Wazuh. (2026). Install Wazuh - Start protecting your system. https://wazuh.com/install/

[31] Wazuh Documentation. (2026). Installing the Wazuh server step by step. https://documentation.wazuh.com/current/installation-guide/wazuh-server/step-by-step.html

[35] GitHub - Wazuh. (2023). Wazuh Installation Assistant. https://github.com/wazuh/wazuh-installation-assistant

[36] IT-ADMIN. (2024). Installer Wazuh sous Linux (Debian 12, Ubuntu, Mint). https://it-admin.tg/installer-wazuh-sous-linux-debianubuntumint/

[37] Wazuh Documentation. (2026). Windows - Enrollment via agent configuration. https://documentation.wazuh.com/current/user-manual/agent/agent-enrollment/enrollment-methods/via-agent-configuration/windows-endpoint.html

[38] OneUptime. (2026). How to Set Up Wazuh Security Platform on Ubuntu. https://oneuptime.com/blog/post/2026-01-15-setup-wazuh-security-platform-ubuntu/view

[40] Wazuh Documentation. (2026). Deploying Wazuh agents on Windows endpoints. https://documentation.wazuh.com/current/installation-guide/wazuh-agent/wazuh-agent-package-windows.html

[42] Sweat Digital. (2025). Step-by-Step Guide to Install Wazuh on Ubuntu/CentOS and Deploy Agents. https://www.sweat-digital.com/step-by-step-guide-to-install-wazuh-on-ubuntu-centos-and-deploy-agents-windows-linux/