Wazuh 4.11.2

Installation distribuée sur Ubuntu 24.04

Déploiement des agents Windows & Linux

Architecture : Distribuée (3 VMs Proxmox)
Indexer : 10.0.0.10 | Manager : 10.0.0.11 | Dashboard : 10.0.0.12
Domaine : mvgroup.local | Agents : Windows 11 + Ubuntu 24.04

Rédigé par : Samuel — Avril 2026

1. Introduction & Architecture

Wazuh est une plateforme SIEM/XDR open source qui permet de surveiller la sécurité des endpoints, détecter les intrusions, analyser les logs et assurer la conformité. Ce document décrit l'installation complète de Wazuh 4.11.2 en architecture distribuée sur 3 VMs Ubuntu 24.04 hébergées sur Proxmox.

1.1 Composants Wazuh

Composant	Rôle	VM	IP
Wazuh Indexer	Stockage et indexation des logs (OpenSearch)	WAZUH-INDEXER-SAM	10.0.0.10
Wazuh Manager	Analyse, corrélation des alertes, gestion des agents	WAZUH-MANAGER-SAM	10.0.0.11
Wazuh Dashboard	Interface web de visualisation	WAZUH-DASHBOARD-SAM	10.0.0.12

1.2 Spécifications des VMs

VM	CPU	RAM	Disque	OS
WAZUH-INDEXER-SAM	4 cœurs	4 GB	40 GB	Ubuntu 24.04 LTS
WAZUH-MANAGER-SAM	4 cœurs	4 GB	40 GB	Ubuntu 24.04 LTS
WAZUH-DASHBOARD-SAM	4 cœurs	4 GB	40 GB	Ubuntu 24.04 LTS

1.3 Agents déployés

Machine	OS	IP	Nom agent
Client Windows 11	Windows 11 Pro	10.0.100.1	W11-CLIENT1-SAM
Client Ubuntu	Ubuntu 24.04.4 LTS	10.0.100.2	UBUNTU-CLIENT2-SAM

2. Préparation des VMs

Cette étape est identique pour les 3 VMs. Effectuez ces opérations sur chacune d'elles.

2.1 Configuration réseau IP statique

Sur chaque VM, configurez une IP statique via systemd-networkd et Netplan :

```
sudo -i

# Désactiver NetworkManager et activer systemd-networkd
systemctl disable NetworkManager
systemctl stop NetworkManager
systemctl enable systemd-networkd

# Supprimer les fichiers Netplan existants
rm -f /etc/netplan/01-network-manager-all.yaml
rm -f /etc/netplan/50-cloud-init.yaml

# Créer le fichier de configuration Netplan
nano /etc/netplan/00-installer-config.yaml
```

Contenu du fichier (adaptez l'IP selon la VM) :

```
network:
  version: 2
  renderer: networkd
  ethernets:
    ens18:
      dhcp4: no
      addresses:
        - 10.0.0.10/16   # 10.0.0.11 pour Manager, 10.0.0.12 pour
Dashboard
      routes:
        - to: default
          via: 10.0.0.1
      nameservers:
        addresses:
          - 10.0.200.2
          - 8.8.8.8
```

Appliquer la configuration :

```
chmod 600 /etc/netplan/00-installer-config.yaml
```

```
netplan apply
ip a
```

2.2 Désactiver le DHCP cloud-init

Si le fichier 50-cloud-init.yaml existe, supprimez-le pour éviter les conflits :

```
rm /etc/netplan/50-cloud-init.yaml
echo "network: {config: disabled}" > /etc/cloud/cloud.cfg.d/99-disable-
network-config.cfg
```

2.3 Installer SSH et curl

```
apt-get update
apt-get install -y openssh-server curl
systemctl enable ssh
```

2.4 Configurer /etc/hosts sur chaque VM

```
nano /etc/hosts

# Ajouter à la fin :
10.0.0.10   WAZUH-INDEXER-SAM
10.0.0.11   WAZUH-MANAGER-SAM
10.0.0.12   WAZUH-DASHBOARD-SAM
```

3. Génération des certificats

La génération des certificats s'effectue une seule fois sur la VM WAZUH-INDEXER-SAM. Les certificats générés sont ensuite distribués sur les autres VMs.

3.1 Télécharger le script et le fichier de config

```
# Sur WAZUH-INDEXER-SAM
ssh samuel@10.0.0.10
sudo -i

curl -sO https://packages.wazuh.com/4.11/wazuh-install.sh
curl -sO https://packages.wazuh.com/4.11/config.yml
```

3.2 Configurer le fichier config.yml

```
nano config.yml
```

Contenu du fichier :

```
nodes:
  indexer:
    - name: WAZUH-INDEXER-SAM
      ip: 10.0.0.10

  server:
    - name: WAZUH-MANAGER-SAM
      ip: 10.0.0.11

  dashboard:
    - name: WAZUH-DASHBOARD-SAM
      ip: 10.0.0.12
```

3.3 Générer les certificats

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

✅ Le fichier wazuh-install-files.tar est créé dans /root/. Il contient les certificats et mots de passe pour tous les composants.

3.4 Distribuer les certificats sur les autres VMs

```
scp /root/wazuh-install-files.tar samuel@10.0.0.11:/home/samuel/
scp /root/wazuh-install-files.tar samuel@10.0.0.12:/home/samuel/
```

4. Installation du Wazuh Indexer

L'Indexer est basé sur OpenSearch. Il stocke et indexe tous les logs et alertes remontés par les agents.

```
# Sur WAZUH-INDEXER-SAM
bash wazuh-install.sh --wazuh-indexer WAZUH-INDEXER-SAM
```

- ✅ Wazuh indexer installation finished
- ✅ wazuh-indexer service started
- ✅ Wazuh indexer cluster initialized

⚠️ *Ne démarrez pas le cluster maintenant. Installez d'abord le Manager et le Dashboard.*

5. Installation du Wazuh Manager

Le Manager analyse les logs reçus des agents, applique les règles de détection et génère les alertes.

```
# Sur WAZUH-MANAGER-SAM
ssh samuel@10.0.0.11
sudo -i

curl -sO https://packages.wazuh.com/4.11/wazuh-install.sh
mv /home/samuel/wazuh-install-files.tar /root/

bash wazuh-install.sh --wazuh-server WAZUH-MANAGER-SAM
```

- ✅ Wazuh manager installation finished
- ✅ wazuh-manager service started
- ✅ Filebeat installation finished
- ✅ filebeat service started

6. Démarrage du cluster Wazuh Indexer

Avant d'installer le Dashboard, le cluster Indexer doit être démarré. Cette étape initialise la sécurité et les utilisateurs internes.

```
# Retourner sur WAZUH-INDEXER-SAM
ssh samuel@10.0.0.10
sudo -i

bash wazuh-install.sh --start-cluster
```

- ✅ Wazuh indexer cluster security configuration initialized
- ✅ Wazuh indexer cluster started

7. Installation du Wazuh Dashboard

Le Dashboard est l'interface web de Wazuh. Il permet de visualiser les alertes, gérer les agents et explorer les logs.

```
# Sur WAZUH-DASHBOARD-SAM
ssh samuel@10.0.0.12
sudo -i

curl -sO https://packages.wazuh.com/4.11/wazuh-install.sh
mv /home/samuel/wazuh-install-files.tar /root/

bash wazuh-install.sh --wazuh-dashboard WAZUH-DASHBOARD-SAM
```

- ✅ Wazuh dashboard installation finished
- ✅ wazuh-dashboard service started
- ✅ Wazuh dashboard web application initialized

7.1 Identifiants de connexion

⚠️ *Notez précieusement ces identifiants affichés en fin d'installation, ils ne seront plus affichés !*

Champ	Valeur
URL	https://10.0.0.12:443
URL DNS	https://wazuh-dashboard-sam.mvgroup.local
Utilisateur	admin
Mot de passe	Généré automatiquement (affiché en fin d'installation)

ℹ️ *Acceptez l'avertissement de certificat auto-signé dans votre navigateur, c'est normal en environnement lab.*

8. Configuration DNS

Ajoutez les enregistrements DNS pour les 3 serveurs Wazuh dans le gestionnaire DNS Windows Server (10.0.200.2).

8.1 Zone de recherche directe (mvgroup.local)

Pour chaque serveur, créez un enregistrement A en cochant Créer un enregistrement PTR associé :

Nom d'hôte	IP	PTR associé
WAZUH-INDEXER-SAM	10.0.0.10	Coché
WAZUH-MANAGER-SAM	10.0.0.11	Coché
WAZUH-DASHBOARD-SAM	10.0.0.12	Coché

8.2 Zone de recherche inversée (0.0.10.in-addr.arpa)

Numéro IP	Pointe vers
10	WAZUH-INDEXER-SAM.mvgroup.local
11	WAZUH-MANAGER-SAM.mvgroup.local
12	WAZUH-DASHBOARD-SAM.mvgroup.local

8.3 Vérification DNS

```
# Résolution directe
nslookup WAZUH-INDEXER-SAM.mvgroup.local
nslookup WAZUH-MANAGER-SAM.mvgroup.local
nslookup WAZUH-DASHBOARD-SAM.mvgroup.local

# Résolution inverse
nslookup 10.0.0.10
nslookup 10.0.0.11
nslookup 10.0.0.12
```

9. Déploiement de l'agent — Windows 11

L'agent Wazuh collecte les logs et événements de sécurité sur les endpoints et les envoie au Manager pour analyse.

9.1 Générer la commande depuis le Dashboard

1. Accéder à https://10.0.0.12 → Deploy new agent
2. Sélectionner : WINDOWS → MSI 32/64 bits
3. Server address : 10.0.0.11
4. Agent name : W11-CLIENT1-SAM
5. Group : default
6. Copier la commande PowerShell générée

9.2 Installer l'agent sur Windows 11

Ouvrir PowerShell en administrateur et exécuter :

```
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.11.2-1.msi `
  -OutFile $env:tmp\wazuh-agent; `
  msiexec.exe /i $env:tmp\wazuh-agent /q `
  WAZUH_MANAGER='10.0.0.11' `
  WAZUH_AGENT_NAME='W11-CLIENT1-SAM'
```

Démarrer le service Wazuh :

```
NET START WazuhSvc
```

✅ Le service Wazuh démarre et W11-CLIENT1-SAM apparaît dans le Dashboard avec le statut active.

10. Déploiement de l'agent — Ubuntu 24.04

10.1 Générer la commande depuis le Dashboard

7. Accéder à https://10.0.0.12 → Deploy new agent
8. Sélectionner : LINUX → DEB amd64
9. Server address : 10.0.0.11
10. Agent name : UBUNTU-CLIENT2-SAM
11. Group : default
12. Copier la commande générée

10.2 Installer l'agent sur Ubuntu

```
# Se connecter sur UBUNTU-CLIENT2-SAM
ssh samuel@10.0.100.2
sudo -i

# Télécharger et installer l'agent
wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.11.2-1_amd64.deb \
  && WAZUH_MANAGER='10.0.0.11' \
  WAZUH_AGENT_NAME='UBUNTU-CLIENT2-SAM' \
  dpkg -i ./wazuh-agent_4.11.2-1_amd64.deb
```

Démarrer et activer le service :

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

✅ UBUNTU-CLIENT2-SAM apparaît dans le Dashboard avec le statut active.

11. Récapitulatif

11.1 État final des composants

Composant	VM	IP	DNS	Statut
Wazuh Indexer	WAZUH-INDEXER-SAM	10.0.0.10	WAZUH-INDEXER-SAM.mvgroup.local	✅ Actif
Wazuh Manager	WAZUH-MANAGER-SAM	10.0.0.11	WAZUH-MANAGER-SAM.mvgroup.local	✅ Actif
Wazuh Dashboard	WAZUH-DASHBOARD-SAM	10.0.0.12	WAZUH-DASHBOARD-SAM.mvgroup.local	✅ Actif

11.2 État des agents

Agent	OS	IP	Statut
W11-CLIENT1-SAM	Windows 11 Pro	10.0.100.1	✅ Active
UBUNTU-CLIENT2-SAM	Ubuntu 24.04.4 LTS	10.0.100.2	✅ Active

11.3 Checklist finale

- VM WAZUH-INDEXER-SAM : IP statique, SSH, /etc/hosts configurés
- VM WAZUH-MANAGER-SAM : IP statique, SSH, /etc/hosts configurés
- VM WAZUH-DASHBOARD-SAM : IP statique, SSH, /etc/hosts configurés
- Certificats générés et distribués sur les 3 VMs
- Wazuh Indexer installé et cluster démarré
- Wazuh Manager + Filebeat installés
- Wazuh Dashboard installé et accessible via https://10.0.0.12
- Enregistrements DNS A + PTR créés pour les 3 serveurs
- Agent déployé sur Windows 11 (W11-CLIENT1-SAM) — status active
- Agent déployé sur Ubuntu 24.04 (UBUNTU-CLIENT2-SAM) — status active