

# DOCUMENTATION

Fonctionnelle  
&  
Technique

**Documents installation [WAZUH](#)**

## Table des matières

<b>1. Procédure installation Wazuh .....</b>	<b>3</b>
1.1 Étape 1: Prérequis.....	3
1.2 Étape 2: Installation du Wazuh Manager .....	3
1.2.1 Ajout du dépôt Wazuh .....	3
1.2.1 Installation du Wazuh Manager .....	4
1.2.2 Vérification de l'état du service .....	5
1.3 Étape 3: Installation de Wazuh Agent.....	6
1.3.1 Installation sur un système Linux .....	6
1.3.2 Configuration de l'agent.....	6
1.3.3 Démarrage de l'agent .....	7
1.4 Étape 4: Installation de Wazuh Kibana plugin.....	7
1.4.1 Installation d'Elasticsearch .....	7
1.4.2 Installation de Kibana .....	7
1.4.3 Installation du plugin Wazuh pour Kibana .....	7
1.4.4 Redémarrage de Kibana .....	8
1.5 Étape 5: Validation de l'installation .....	8

## 1. PROCEDURE INSTALLATION WAZUH

---

Documentation détaillée sur l'installation de Wazuh, une plateforme de sécurité open source pour la détection des menaces, la surveillance de l'intégrité, et la réponse aux incidents. Voici les grandes étapes à suivre, basées sur la [documentation officielle de Wazuh](#).

### 1.1 Étape 1: Prérequis

Avant de commencer l'installation, assurez-vous que votre système répond aux prérequis nécessaires. Vous aurez besoin de :

Un système d'exploitation compatible (Linux/Windows/MacOS).

Une connexion internet stable pour télécharger les paquets nécessaires.

Les droits administrateur ou sudo sur le système.

### 1.2 Étape 2: Installation du Wazuh Manager

Le "Wazuh Manager" est le cœur de la plateforme, traitant les données de sécurité recueillies par les agents.

#### 1.2.1 Ajout du dépôt Wazuh

Sur un système basé sur Debian/Ubuntu, vous pouvez ajouter le dépôt comme suit :

```
1 curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | gpg --dearmor > /usr/share/keyrings/wazuh-archive-keyring.gpg
2 echo "deb [signed-by=/usr/share/keyrings/wazuh-archive-keyring.gpg] https://packages.wazuh.com/4.x/apt/ stable main" | sudo tee /etc/apt/sources.list.d/wazuh.list
3
```

Sur CentOS/RHEL :

```
1 sudo rpm --import https://packages.wazuh.com/key/GPG-KEY-WAZUH
2 sudo tee /etc/yum.repos.d/wazuh.repo<<EOF
3 [wazuh_repo]
4 name=Wazuh repository
5 gpgcheck=1
6 gpgkey=https://packages.wazuh.com/key/GPG-KEY-WAZUH
7 enabled=1
8 baseurl=https://packages.wazuh.com/4.x/yum/
9 protect=1
10 EOF
```

### 1.2.1 Installation du Wazuh Manager

Sur Debian/Ubuntu :

```
1 sudo apt-get update
2 sudo apt-get install wazuh-manager
3
```

Sur CentOS/RHEL :



```
1 sudo yum install wazuh-manager
```

```
2
```

### 1.2.2 Vérification de l'état du service

Vous pouvez vérifier si le service Wazuh Manager fonctionne correctement avec :



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

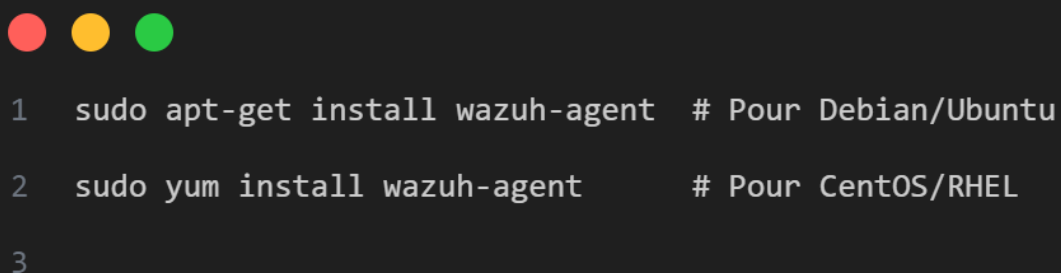
```
2
```

### 1.3 Étape 3: Installation de Wazuh Agent

Les agents Wazuh sont installés sur les machines que vous souhaitez surveiller, envoyant les données collectées au manager.

#### 1.3.1 Installation sur un système Linux

Ajoutez le dépôt comme montré précédemment, puis installez l'agent :



```
1 sudo apt-get install wazuh-agent # Pour Debian/Ubuntu
2 sudo yum install wazuh-agent    # Pour CentOS/RHEL
3
```

#### 1.3.2 Configuration de l'agent

Éditez le fichier de configuration (/var/ossec/etc/ossec.conf) pour ajouter l'adresse IP de votre manager.



```
<ossec_config>
  <client>
    <manager_hostname>MANAGER_IP</manager_hostname>
  </client>
</ossec_config>
```

### 1.3.3 Démarrage de l'agent



```
1 sudo systemctl daemon-reload
2 sudo systemctl enable wazuh-agent
3 sudo systemctl start wazuh-agent
4
```

## 1.4 Étape 4: Installation de Wazuh Kibana plugin

Wazuh peut être intégré avec Elastic Stack pour visualiser et analyser les données de manière efficace.

### 1.4.1 Installation d'Elasticsearch

Suivez les instructions de la documentation officielle pour installer Elasticsearch.

### 1.4.2 Installation de Kibana

Installez Kibana et configurez-le pour qu'il se connecte à votre instance Elasticsearch.

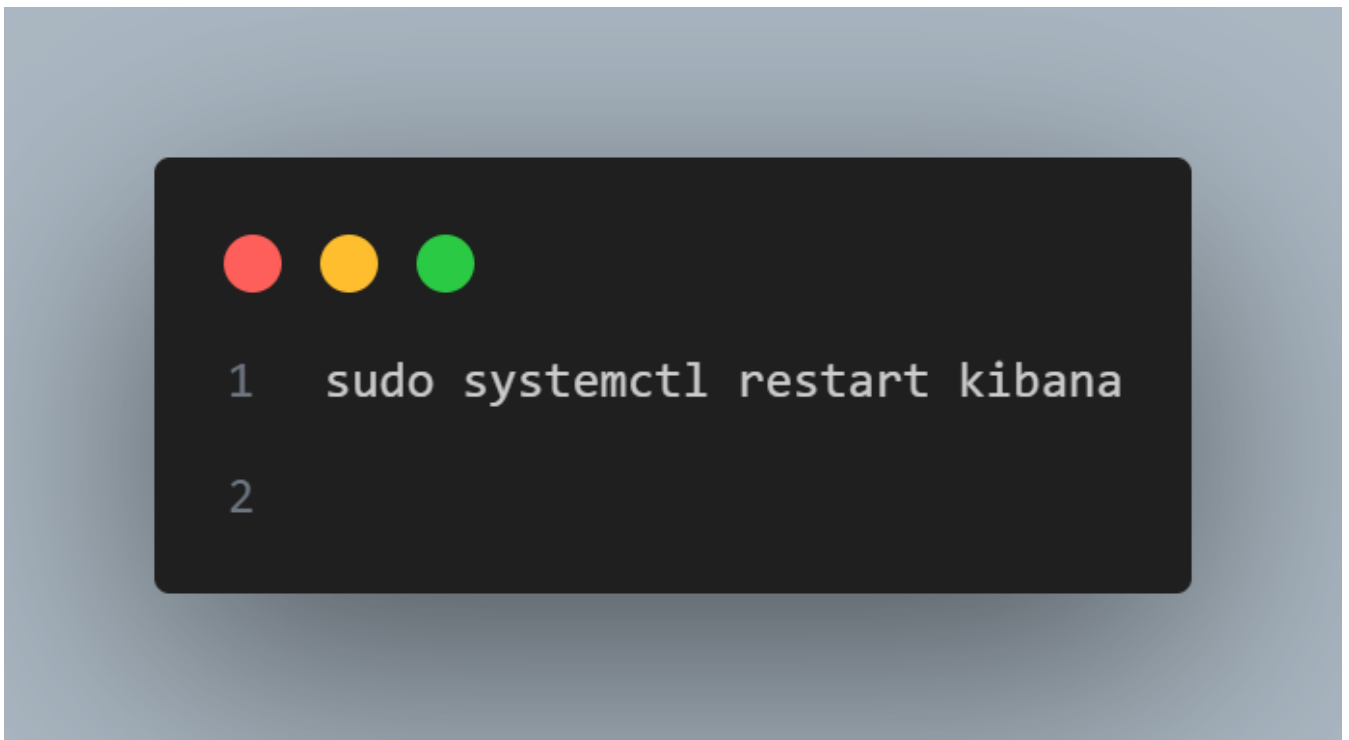
### 1.4.3 Installation du plugin Wazuh pour Kibana



```
1 sudo -u kibana /usr/share/kibana/bin/kibana-plugin install https://packages.wazuh.com/4.x/ui/kibana/wazuh_kibana-.zip
2
```

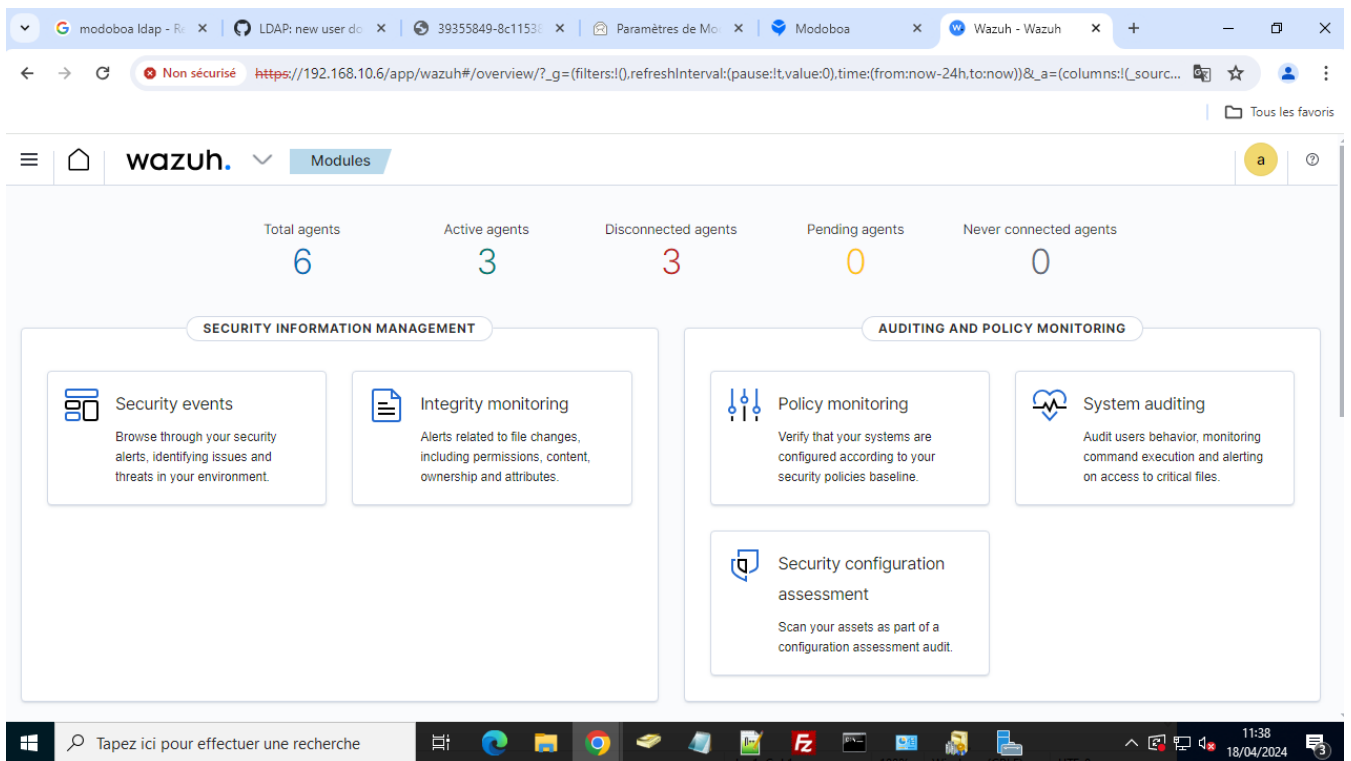
Remplacez <version> par la version compatible de Kibana.

#### 1.4.4 Redémarrage de Kibana



#### 1.5 Étape 5: Validation de l'installation

Vérifiez que tout fonctionne correctement en accédant à l'interface utilisateur de Kibana et en vérifiant que les données des agents sont visibles et correctement traitées.





N'oubliez pas de régulièrement mettre à jour vos systèmes et logiciels pour bénéficier des dernières fonctionnalités et corrections de sécurité. Pour des informations plus spécifiques ou des configurations avancées, référez-vous toujours à la [documentation officielle de Wazuh](#).