

DOCUMENTATION

Fonctionnelle
&
Technique

Documents installation [WAZUH](#)

Table des matières

1. Procédure installation Wazuh	3
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.....	5
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
1.6 Étape 6: Configuration des notifications par e-mail.....	9
1.6.1 Modification du fichier de configuration	9
1.6.2 Configurer les règles pour envoyer des alertes.....	10
1.6.3 Installer un serveur SMTP si nécessaire	10
1.6.4 Tester l'envoi d'e-mails	11
1.6.5 Redémarrer Wazuh Manager	11
1.7 Étape 7: Vérification des notifications	12

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
```

Sur CentOS/RHEL :



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

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
```

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
```

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.



```
1 <ossec_config>
2   <client>
3     <manager_hostname>MANAGER_IP</manager_hostname>
4   </client>
5 </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
```

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.

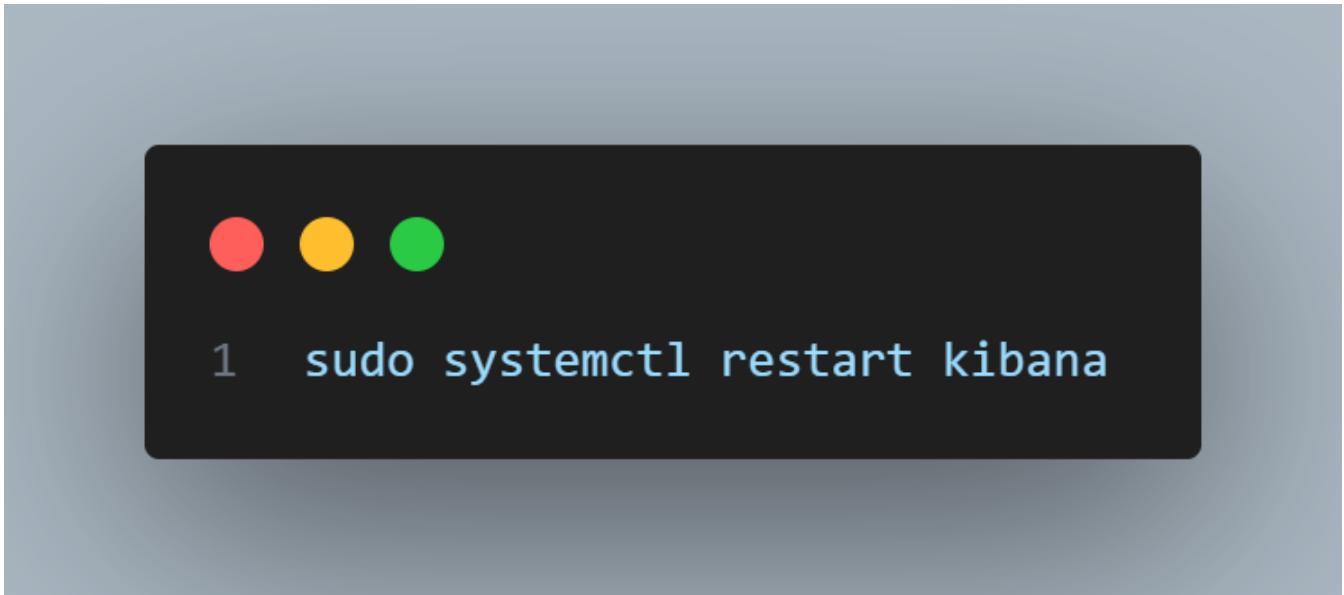
1.4.3 Installation du plugin Wazuh pour Kibana



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

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.

The screenshot shows the Wazuh web interface running on a Windows 10 desktop. The taskbar at the bottom includes icons for File Explorer, Edge browser, Google Chrome, and FileZilla. The system tray shows the date as 18/04/2024 and the time as 11:38.

The main dashboard displays the following agent statistics:

Total agents	Active agents	Disconnected agents	Pending agents	Never connected agents
6	3	3	0	0

The interface is divided into two main sections: SECURITY INFORMATION MANAGEMENT and AUDITING AND POLICY MONITORING, each containing three cards:

- SECURITY INFORMATION MANAGEMENT:**
 - Security events:** Browse through your security alerts, identifying issues and threats in your environment.
 - Integrity monitoring:** Alerts related to file changes, including permissions, content, ownership and attributes.
 - Security configuration assessment:** Scan your assets as part of a configuration assessment audit.
- AUDITING AND POLICY MONITORING:**
 - Policy monitoring:** Verify that your systems are configured according to your security policies baseline.
 - System auditing:** Audit users behavior, monitoring command execution and alerting on access to critical files.
 - File monitoring:** Monitor file integrity and detect changes in real-time.

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](#).

1.6 Étape 6: Configuration des notifications par e-mail

L'activation des notifications et des alertes par e-mail est une fonctionnalité importante de Wazuh pour être informé en temps réel des menaces et des anomalies détectées. Voici comment vous pouvez configurer les alertes par e-mail dans Wazuh.

Pour configurer les notifications par e-mail, vous devrez modifier la configuration de Wazuh pour utiliser un serveur SMTP local ou externe pour l'envoi d'e-mails.

Configuration de l'agent de notification (Intégration)

1.6.1 Modification du fichier de configuration

Editez le fichier de configuration de Wazuh pour activer et configurer l'intégration e-mail. Ce fichier est typiquement situé à `/var/ossec/etc/ossec.conf`. Ajoutez la section suivante dans la configuration globale (`<global>` tag):

```
1 <global>
2   <smtp_server>smtp.example.com</smtp_server>
3   <email_from>wazuh@example.com</email_from>
4   <email_to>your-email@example.com</email_to>
5   <email_notification>yes</email_notification>
6 </global>
```

Remplacez `smtp.example.com`, `wazuh@example.com`, et `your-email@example.com` avec vos informations réelles.

1.6.2 Configurer les règles pour envoyer des alertes

Vous pouvez configurer les alertes pour qu'elles envoient un e-mail basé sur certaines règles. Trouvez ou ajoutez des règles dans **/var/ossec/etc/rules/local_rules.xml** et assurez-vous qu'elles ont l'action d'envoyer un e-mail :

```
1 <rule id="100001" level="12">
2   <decoded_as>json</decoded_as>
3   <field name="agent.id">001</field>
4   <description>Exemple d'alerte par e-mail pour l'agent 001.</description>
5   <group>syslog,access_control,</group>
6   <options>alert_by_email</options>
7 </rule>
```

Cette règle envoie un e-mail si elle est déclenchée (ici configurée pour l'agent avec l'ID 001).

Configuration du serveur de messagerie

1.6.3 Installer un serveur SMTP si nécessaire

Si vous n'avez pas de serveur SMTP, vous pouvez installer Postfix ou un autre serveur de messagerie sur le serveur Wazuh Manager :

```
1 sudo apt-get install postfix
```

Pendant l'installation, sélectionnez "Site Internet" et configurez le nom de domaine approprié.

1.6.4 Tester l'envoi d'e-mails

Vous pouvez tester l'envoi d'e-mails directement depuis la ligne de commande pour vous assurer que votre configuration SMTP fonctionne :

```
● ● ●  
1 echo "Test email from Wazuh" | mail -s "Test Mail" your-email@example.com
```

Remplacez **your-email@example.com** avec votre adresse e-mail réelle.

Redémarrage de Wazuh Manager

1.6.5 Redémarrer Wazuh Manager

Après avoir configuré les notifications par e-mail, redémarrez le service Wazuh Manager pour appliquer les changements :

```
● ● ●  
1 sudo systemctl restart wazuh-manager
```

1.7 Étape 7: Vérification des notifications

Pour vérifier que les notifications par e-mail fonctionnent :

Déclenchez une règle qui envoie un e-mail (cela peut être fait par un test ou une configuration spécifique).

Vérifiez votre boîte de réception pour l'e-mail de notification d'alerte.

Ces étapes complètent la configuration de base des notifications par e-mail dans Wazuh. Il est recommandé de surveiller activement la fonctionnalité pour s'assurer qu'elle fonctionne comme prévu et

d'ajuster les niveaux d'alerte et les règles en fonction des besoins de votre environnement. Pour une personnalisation plus avancée, consultez [la documentation officielle de Wazuh](#) sur les notifications.

Fait à MULHOUSE, le 25/04/2024

Signature des responsables du projet :

Anthony SCHULTZ / Joshua TRUTTMANN / Audrey SCHLAEFLIN