

Documentation Wazuh



Wazuh est un fork libre permettant de détecter les intrusions.

Pour installer et configurer Wazuh, il faut dans un premier temps installer les packages qui seront nécessaires à son installation.

La commande étant nécessaire pour installer tous ces packages est la suivante :

```
apt install curl apt-transport-https unzip wget libcap2-bin software-properties-common lsb-release gnupg
```

Après avoir installé les packages il faut maintenant installer la clé GPG.

La clé GPG permet de vérifier la viabilité de Wazuh.

Pour installer la clé GPG, il faut utiliser la commande suivante :

```
curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | apt-key add -
```

```
root@Wazuh:~# curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | apt-key add -  
Warning: apt-key is deprecated. Manage keyring files in trusted.gpg.d instead (see apt-key(8)).  
OK
```

Une fois la clé GPG installé, il suffit d'ajouter le dépôt de référence avec la commande qui va avec :

```
"deb https://packages.wazuh.com/4.x/apt/ stable main" | tee -a /etc/apt/sources.list.d/wazuh.list
```

Une fois le dépôt de référence ajouté, il faut mettre à jour les informations du package.

La commande a utilisé afin de les mettre à jour est :

```
apt-get update
```

Une fois avoir mis les informations de package à jour, il nous faut installer le package du gestionnaire de Wazuh.

La commande étant nécessaire à son installation est :

`apt-get install wazuh-manager -y`

```
ist.d/wazuh.list:1 et /etc/apt/sources.list.d/wazuh.list:3
W: La cible Translations (main/i18n/Translation-fr_FR) est spécifiée plusieurs fois dans /etc/apt/sources.list.d/wazuh.list:1 et /etc/apt/sources.list.d/wazuh.list:3
W: La cible Translations (main/i18n/Translation-fr) est spécifiée plusieurs fois dans /etc/apt/sources.list.d/wazuh.list:1 et /etc/apt/sources.list.d/wazuh.list:3
W: La cible Translations (main/i18n/Translation-en) est spécifiée plusieurs fois dans /etc/apt/sources.list.d/wazuh.list:1 et /etc/apt/sources.list.d/wazuh.list:3
W: La cible Packages (main/binary-amd64/Packages) est spécifiée plusieurs fois dans /etc/apt/sources.list.d/wazuh.list:1 et /etc/apt/sources.list.d/wazuh.list:4
W: La cible Packages (main/binary-all/Packages) est spécifiée plusieurs fois dans /etc/apt/sources.list.d/wazuh.list:1 et /etc/apt/sources.list.d/wazuh.list:4
W: La cible Translations (main/i18n/Translation-fr_FR) est spécifiée plusieurs fois dans /etc/apt/sources.list.d/wazuh.list:1 et /etc/apt/sources.list.d/wazuh.list:4
W: La cible Translations (main/i18n/Translation-fr) est spécifiée plusieurs fois dans /etc/apt/sources.list.d/wazuh.list:1 et /etc/apt/sources.list.d/wazuh.list:4
W: La cible Translations (main/i18n/Translation-en) est spécifiée plusieurs fois dans /etc/apt/sources.list.d/wazuh.list:1 et /etc/apt/sources.list.d/wazuh.list:4
root@Wazuh:~# apt-get install wazuh-manager -y
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Paquets suggérés :
  expect
Les NOUVEAUX paquets suivants seront installés :
  wazuh-manager
0 mis à jour, 1 nouvellement installés, 0 à enlever et 2 non mis à jour.
Il est nécessaire de prendre 120 Mo dans les archives.
Après cette opération, 460 Mo d'espace disque supplémentaires seront utilisés.
Réception de :1 https://packages.wazuh.com/4.x/apt/stable/main amd64 wazuh-manager amd64 4.3.10-1 [120 MB]
120 Mo réceptionnés en 7s (17,6 Mo/s)
Sélection du paquet wazuh-manager précédemment désélectionné.
(Lecture de la base de données... 26875 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../wazuh-manager_4.3.10-1_amd64.deb ...
Dépaquetage de wazuh-manager (4.3.10-1) ...
Paramétrage de wazuh-manager (4.3.10-1) ...
root@Wazuh:~# apt-get install wazuh-manager -y
```

Une fois le package de gestionnaire de Wazuh installé, il est nécessaire de l'activer ainsi que de le démarrer.

Les commandes ci-dessous nous permettra de l'activer et de le démarrer :

```
root@Wazuh:~# systemctl daemon-reload
root@Wazuh:~# systemctl enable wazuh-manager
Synchronizing state of wazuh-manager.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable wazuh-manager
Created symlink /etc/systemd/system/multi-user.target.wants/wazuh-manager.service → /lib/systemd/system/wazuh-manager.service.
root@Wazuh:~# systemctl start wazuh-manager
root@Wazuh:~# _
```

Une fois activer et démarrer, vérifier le statut du gestionnaire.

Commande a utilisé ci-contre :

```
root@Wazuh:~# systemctl status wazuh-manager
● wazuh-manager.service - Wazuh manager
   Loaded: loaded (/lib/systemd/system/wazuh-manager.service; enabled; vendor preset: enabled)
   Active: active (running) since Wed 2023-02-08 11:21:45 CET; 10min ago
     Process: 39982 ExecStart=/usr/bin/env /var/ossec/bin/wazuh-control start (code=exited, status=0)
    Tasks: 104 (limit: 2294)
   Memory: 405.8M
      CPU: 30.976s
   CGroup: /system.slice/wazuh-manager.service
           └─40035 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh-apid.py
             └─40076 /var/ossec/bin/wazuh-authd
               └─40091 /var/ossec/bin/wazuh-db
                 └─40104 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh-apid.py
                   └─40107 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh-apid.py
                     └─40121 /var/ossec/bin/wazuh-execd
                       └─40134 /var/ossec/bin/wazuh-analysisd
                         └─40146 /var/ossec/bin/wazuh-syscheckd
                           └─40184 /var/ossec/bin/wazuh-remoted
                             └─40215 /var/ossec/bin/wazuh-logcollector
                               └─40235 /var/ossec/bin/wazuh-monitord
                                 └─40257 /var/ossec/bin/wazuh-modulesd

févr. 08 11:21:35 Wazuh env[39982]: Started wazuh-db...
févr. 08 11:21:36 Wazuh env[39982]: Started wazuh-execd...
févr. 08 11:21:37 Wazuh env[39982]: Started wazuh-analysisd...
févr. 08 11:21:38 Wazuh env[39982]: Started wazuh-syscheckd...
févr. 08 11:21:39 Wazuh env[39982]: Started wazuh-remoted...
févr. 08 11:21:40 Wazuh env[39982]: Started wazuh-logcollector...
févr. 08 11:21:41 Wazuh env[39982]: Started wazuh-monitord...
févr. 08 11:21:43 Wazuh env[39982]: Started wazuh-modulesd...
févr. 08 11:21:45 Wazuh env[39982]: Completed.
févr. 08 11:21:45 Wazuh systemd[1]: Started Wazuh manager.
```

Après avoir vérifié le statut du gestionnaire de Wazuh, installer Elasticsearch.

Elasticsearch est un logiciel utilisant Lucene pour l'indexation et la recherche de données.

La commande nécessaire à son installation est :

```
apt install elasticsearch-oss opendistroforelasticsearch
```

Une fois cela fait, il suffit de télécharger le fichier de configuration d'Elastic search.

Une commande est nécessaire à son téléchargement :

```
curl -so /etc/elasticsearch/elasticsearch.yml https://packages.wazuh.com/resources/4.2/opendistro/elasticsearch/7.x/elasticsearch_all_in_one.yml
```

Après avoir terminé le téléchargement du fichier de configuration, il est nécessaire d'ajouter des utilisateurs ainsi que des rôles.

Pour l'ajout des utilisateurs ainsi que des rôles, les commandes sont les suivante :

```

root@Wazuh:~# curl -so /usr/share/elasticsearch/plugins/opendistro_security/securityconfig/roles.yml
https://packages.wazuh.com/ressources/4.2/open-distro/elasticsearch/roles/roles.yml
root@Wazuh:~# curl -so /usr/share/elasticsearch/plugins/opendistro_security/securityconfig/roles.yml
https://packages.wazuh.com/ressources/4.2/open-distro/elasticsearch/roles/roles_mapping.yml
root@Wazuh:~# curl -so /usr/share/elasticsearch/plugins/opendistro_security/securityconfig/roles.yml
https://packages.wazuh.com/ressources/4.2/open-distro/elasticsearch/roles/internal_users.yml
root@Wazuh:~#

```

Une fois l'ajout des utilisateurs et des rôles terminés, il faut supprimer les certificats de démonstration.

Afin de supprimer les certificats de démonstrations, utiliser la commande ci-contre :

```

root@Wazuh:~# rm /etc/elasticsearch/esnode-key.pem /etc/elasticsearch/esnode.pem /etc/elasticsearch/
kirk-key.pem /etc/elasticsearch/kirk.pem /etc/elasticsearch/root-ca.pem -f
root@Wazuh:~# _

```

Après la suppression des certificats de démonstration, il faut télécharger les certificats Wazuh.

Deux commandes sont nécessaire à leurs téléchargements :

```

root@Wazuh:~# curl -so ~/wazuh-cert-tool.sh https://packages.wazuh.com/ressources/4.2/open-distro/to
ols/certificate-utility/wazuh-cert-tool.sh
root@Wazuh:~# curl -so ~/instances.yml https://packages.wazuh.com/ressources/4.2/open-distro/tools/c
ertificate-utility/instance_aio.yml
root@Wazuh:~#

```

Une fois les certificats Wazuh téléchargés, il faut effectuer l'exécution de Wazuh afin de créer les certificats.

Avec la commande ci-contre :

```
~/wazuh-cert-tool.sh
```

Une fois les fichiers créés, déplacer les certificats vers leurs emplacement correspondant.

Toutes les commandes suivantes la commande mkdir il faut les effectuer sur l'ESXI.

Les commandes à utiliser sont les suivantes :

```

mkdir etc/elasticsearch/certs/
mv ~/certs/elasticsearch* etc/elasticsearch/certs
mv ~/certs/admin* etc/elasticsearch/certs
cp ~/certs/root-ca* etc/elasticsearch/certs

```

Une fois ces commandes effectuées il nous faut activer et démarrer elasticsearch.

Pour activer et démarrer elasticsearch les commandes à utiliser sont les suivantes :

```
systemctl daemon-reload
```

```
systemctl enable elasticsearch
```

```
systemctl start elasticsearch
```

Une fois activer et démarrer, vérifier le statut d'Elasticsearch avec la commande :

```
systemctl status elasticsearch
```

Une fois le statut vérifié, exécuter le script securityadmin et afin de charger les nouvelles informations.

```
export JAVA_HOME=/usr/share/elasticsearch/jdk/ &&  
/usr/share/elasticsearch/plugins/opendistro_security/tools/securityadmin.sh -cd  
/usr/share/elasticsearch/plugins/opendistro_security/securityconfig/ -nhnv -cacert  
/etc/elasticsearch/certs/root-ca.pem -cert /etc/elasticsearch/certs/admin.pem -key  
/etc/elasticsearch/certs/admin-key.pem
```

Une fois le script d'Elasticsearch terminé de charger les nouvelles informations, installer le Filebeat.

Filebeat transfère les données en UDP, il est composé de plusieurs modules de sources de données simplifiant la collecte, l'analyse et les vues des formats de journaux d'entrées

Pour installer Filebeat une commande est nécessaire et on la trouveras ci-dessous :

```
apt-get install filebeat
```

Après l'installation de Filebeat, télécharger le fichier de configuration transmettant les alertes avec la commande suivante :

```
root@Wazuh:~# curl -sO /etc/filebeat/filebeat.yml https://packages.wazuh.com/ressources/4.2/open-dis  
tro/filebeat/7.x/filebeat_all_in_one.yml
```

Une fois le fichier transmettant les alertes, télécharger le modèle des alertes avec la commande suivante :

```
root@Wazuh:~# curl -sO /etc/filebeat/wazuh-template.json https://raw.githubusercontent.com/wazuh/waz  
uh/4.2/extensions/elasticsearch/7.x/wazuh-template.json chmod go+r /etc/filebeat/wazuh-template.json
```

Le modèle des alertes est installé, télécharger le module de Wazuh pour Filebeat.

La commande suivante est nécessaire :

```
curl -s https://packages.wazuh.com/4.x/filebeat/wazuh-filebeat-0.1.tar.gz
```

Après avoir téléchargé le module Wazuh pour Filebeat, faire une copie des certificats d'Elasticsearch.

Trois commandes sont nécessaire à cette copie :

```
mkdir etc/filebeat/certs/
```

```
cp ~/certs/root-ca.pem etc/filebeat/certs/
```

```
mv ~/certs/filebeat* etc/filebeat/certs/
```

Une fois la copie des certificats d'Elasticsearch, activer et démarrer le service Filebeat.

Des commandes sont nécessaire à son activation et à son démarrage :

```
systemctl daemon-reload
```

```
systemctl enable filebeat
```

```
systemctl start filebeat
```

Une fois activer et démarrer, vérifier le statut du service Filebeat.

La commande est la suivante :

```
systemctl status filebeat
```

Après avoir vérifié le statut du service filebeat, installer le service kibana.

Kibana est un greffon de visualisation de données pour Elasticsearch.

Voici les commandes nécessaire à cet installation :

```
apt-get install opendistroforelasticsearch-kibana -y
```

```
curl -so etc/kibana.yml https://packages.wazuh.com/ressources/4.2/open-distro/kibana/7.x/kibana_all_in_one.yml
```

```
mkdir /usr/share/kibana/data
```

```
chown -R kibana:kibana /usr/share/kibana/data
```

Une fois le service kibana téléchargé, il faut l'installer.

La commande étant nécessaire à son installation est la suivante :

```
root@Wazuh:~# cd /usr/share/kibana /usr/kibana/bin/kibana-plugin install https://packages.wazuh.com/4.x/ui/kibana/wazuh-kibana-4.2.5_7.10.2-1.zip --allow-root
```

Après l'avoir installé, il faut de nouveau copier les certificats d'Elasticsearch.

Voici les commandes à utiliser :

```
mkdir /etc/kibana/certs  
cp ~/certs/root-ca.pem /etc/kibana/certs/  
mv ~/certs/kibana* /etc/kibana/certs/  
chown kibana:kibana /etc/kibana/certs/*
```

Une fois les certificats copiés, relier le socket kibana au port 443 .

La commande à utiliser est la suivante :

```
/sbin/setcap 'cap_net_bind_service=+ep' /usr/share/kibana/node/bin/node
```

Après avoir relié le socket kibana au port 443, activer et démarrer le système kibana.

Les commandes à utiliser sont les suivantes :

```
root@Wazuh:~# systemctl daemon-reload  
root@Wazuh:~# systemctl enable kibana  
Synchronizing state of kibana.service with SysV service script with /lib/systemd/systemd-sysv-install.  
Executing: /lib/systemd/systemd-sysv-install enable kibana  
Created symlink /etc/systemd/system/multi-user.target.wants/kibana.service → /etc/systemd/system/kibana.service.  
root@Wazuh:~# systemctl start kibana
```

Une fois activer et démarrer, vérifier le statut du service kibana.

Voici la commande à utiliser :

```
root@Wazuh:~# systemctl status kibana  
• kibana.service - Kibana  
   Loaded: loaded (/etc/systemd/system/kibana.service; enabled; vendor preset: enabled)  
   Active: active (running) since Mon 2023-02-13 11:27:30 CET; 18s ago  
     Main PID: 4432 (node)  
       Tasks: 11 (limit: 2294)  
      Memory: 113.8M  
         CPU: 16.853s  
      CGroup: /system.slice/kibana.service  
              └─4432 /usr/share/kibana/bin/./node/bin/node /usr/share/kibana/bin/./src/cli/dist -c  
  
févr. 13 11:27:30 Wazuh systemd[1]: Started Kibana.  
lines 1-11/11 (END)
```

Kibana : interface web

Pour mettre à jour Wazuh-manager sur CentOS, il faut taper la commande suivante :

```
yum update
```

Une fois CentOS à jour, il nous faut installer le système d'apache avec la commande suivante:

```
yum install httpd
```

Il faut maintenant le démarrer et le lancer de manière automatique :

```
systemctl start httpd  
systemctl enable httpd
```

Ouvrir le port 80 du firewall:

```
firewall-cmd --zone=public --add-port=80/tcp --permanent  
firewall-cmd --reload
```

Installer le service php:

```
yum install php
```

Une fois le service php installé, installer mariadb:

```
yum install mariadb-server
```

Il faut maintenant l'activer et lancer de manière automatique:

```
systemctl start mariadb  
systemctl enable mariadb
```

Il faut désormais sécuriser MariaDB:

```
mysql_secure_installation
```

Il faut dès maintenant créer un utilisateur administrateur dans mariaDB:

```
mysql -u root -p  
CREATE USER newuser@localhost IDENTIFIED BY 'password';  
GRANT ALL PRIVILEGES ON * . * TO newuser@localhost WITH GRANT OPTION;  
quit
```

Après cela il faut le supprimer de mariaDB:

```
mysql -u root -p
DROP USER newuser@localhost;
quit
```

Une fois le compte utilisateurs supprimé, installer EPEL afin de pouvoir télécharger phpMyAdmin:

```
yum install epel-release
```

Maintenant installer phpMyAdmin:

```
yum install phpmyadmin
```

Une fois tout cela installer, recharger le système apache:

```
systemctl reload httpd
```

Utilisation de Wazuh :

Afin de savoir utiliser Wazuh,

pour cela il faut

Se connecter identifier : admin et le mdp admin

Deploy new agent



Select the package to download and install on your system:



LINUX

- ☐ RPM amd64 ☐ RPM aarch64
- ☐ DEB amd64 ☐ DEB aarch64



WINDOWS

- ☒ MSI 32/64 bits



macOS

- ☐ Intel
- ☐ Apple silicon

 For additional systems and architectures, please check our documentation [🔗](#).



Server address:

This is the address the agent uses to communicate with the server. Enter an IP address or a fully qualified domain name (FQDN).

Assign a server address: 

172.20.0.10

Assign an agent name: ?

DC

① The agent name must be unique. It can't be changed once the agent has been enrolled. [?](#)

Select one or more existing groups: ?

Default

Run the following commands to download and install the agent:

```
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.7.2-1.msi -  
OutFile $(env:tmp)\wazuh-agent; msexec /s /q $(env:tmp)\wazuh-agent /q  
WAZUH_MANAGER='172.20.0.10' WAZUH_AGENT_NAME='DC' WAZUH_REGISTRATION_SERVER='172.20.0.10'
```

① Requirements

- You will need administrator privileges to perform this installation.
- PowerShell 3.0 or greater is required.

Keep in mind you need to run this command in a Windows PowerShell terminal.

Start the agent:

```
NET START WazuhSvc
```