

Documentation Wazuh

wazuh.

Lucas MAIGNE

12/05/24

	E4 Documentation E4	Lucas MAIGNE
	E4-Wazuh-Doc	Date : 12/05/2024

Développement :

Table des matières

Wazuh.....	2
Présentation.....	2
Installation.....	3
Agents.....	3
Modification mot de passe.....	6
Sources.....	7

Wazuh

Présentation

Lucas Maigne @L.maigne · 1 week ago

Author Developer 😊 ↩️ ✎ ⋮

Présentation

Wazuh est une plateforme open source utilisée pour la prévention, la détection et la réponse aux menaces. On dit alors que WAZUH est une plateforme open source unifiée XDR (Extended Detection and Response) et SIEM.

Elle sécurise les environnements de travail sur site, virtualisés, conteneurisés et en cloud. Wazuh est largement utilisée par des milliers d'organisations à travers le monde, de la petite entreprise à la grande entreprise.

Wazuh se compose de plusieurs agents de sécurité, déployés sur les systèmes surveillés, et d'un serveur de gestion, qui collecte et analyse les données recueillies par les agents.

Les fonctionnalités

- Analyse de la sécurité
- Détection d'intrusion
- Analyse des données du journal
- Contrôle de l'intégrité des fichiers
- Détection de la vulnérabilité
- Evaluation de configuration
- Réponse aux incidents
- La sécurité cloud
- Sécurité des conteneurs
- Conformité réglementaire
- Détection et réponse aux points terminaux (EDR)

	E4 Documentation E4	Lucas MAIGNE
	E4-Wazuh-Doc	Date : 12/05/2024

Installation

Mise en place de Wazuh

Prérequis

- Avoir une machine Debian 12
- Docker & Docker-compose sont déjà installés (voir [Installation Docker](#))

Installation

Tout d'abord, mettre à jour les dépôts

```
sudo apt update
sudo apt upgrade
```

Pour la suite il faut se diriger vers le site de [Wazuh](#) pour récupérer la commande git permettant de récupérer la dernière version des scripts docker. Sur la machine, cloner le dépôt :

```
git clone https://github.com/wazuh/wazuh-docker.git -b v4.7.3
```

On se déplace ensuite dans le dossier contenant les scripts d'installation en mode single node :

```
cd wazuh-docker/single-node/
```

Dans un premier temps on va exécuter cette commande docker-compose pour générer les certificats nécessaires à l'installation :

```
sudo docker-compose -f generate-indexer-certs.yml run --rm generator
```

Puis on lance la commande permettant de mettre en place WAZUH via docker-compose :

```
sudo docker-compose up -d
```

Une fois l'ensemble des conteneurs mis en place on peut consulter leur consommation de ressources via la commande suivante :

```
sudo docker stats
```

Attendre alors que l'usage CPU devienne de façon stable en dessous des 10%. Vous pouvez maintenant vous connecter à l'interface de WAZUH via l'IP de votre Debian (<https>)

Login/MotDePasse par défaut : admin/SecretPassword

Agents

Afin d'utiliser Wazuh correctement, il faut ajouter des agents, cela va permettre à surveiller et protéger les systèmes en collectant des données de sécurité et en détectant les menaces potentielles. Voici comment **ajouter des agents** :

Lucas Maigne @Lmaigne · 1 week ago

Author Developer

Wazuh Agent

L'agent Wazuh est multi-plateforme et s'exécute sur les points de terminaison que l'utilisateur souhaite surveiller. Il communique avec le serveur Wazuh, envoyant des données en temps quasi réel via un canal crypté et authentifié.

Pour déployer un nouvel agent en suivant les instructions du tableau de bord Wazuh. Allez sur la page Wazuh > Agents, et cliquez sur Déployer un nouvel agent :



Sélectionnez votre système d'exploitation :

Close

Deploy new agent

1 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.

Entrez l'adresse de votre serveur Wazuh :

2 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:

Server address

Assignez un nom unique à l'agent et vous pouvez également l'associer à un groupe :

3 Optional settings:

By default, the deployment uses the hostname as the agent name. Optionally, you can use a different agent name in the field below.

Assign an agent name:

Agent name

The agent name must be unique. It can't be changed once the agent has been enrolled.

Select one or more existing groups:

Default

Exécutez sur votre agent les commandes suivantes pour installer puis démarrer l'agent Wazuh :

4

Run the following commands to download and install the agent:

```
wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.7.3-1_amd64.deb &&  
sudo WAZUH_MANAGER='242.test' dpkg -i ./wazuh-agent_4.7.3-1_amd64.deb
```

④ Requirements

- You will need administrator privileges to perform this installation.
- Shell Bash is required.

Keep in mind you need to run this command in a Shell Bash terminal.

5

Start the agent:

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

	E4 Documentation E4	Lucas MAIGNE
	E4-Wazuh-Doc	Date : 12/05/2024

Modification mot de passe

Lucas Maigne @lmaigne · 1 week ago

Author Developer ✓ 😊 ↩ ✎ ⋮

Modifier le mot de passe des utilisateurs Wazuh

1. Stoppez le conteneur si il est déjà en fonctionnement

```
docker-compose down
```

2. Exécutez cette commande pour générer le hachage de votre nouveau mot de passe.

```
docker run --rm -ti wazuh/wazuh-indexer:4.7.3 bash /usr/share/wazuh-indexer/plugins/opensearch-security
```

3. Copiez le hachage généré.

4. Ouvrez le fichier `config/wazuh_indexer/internal_users.yml`. Remplacez le hachage de l'utilisateur souhaité.

```
...
admin:
  hash: "$2y$12$K/~"
  reserved: true
  backend_roles:
    - "admin"
  description: "Demo admin user"
...
```

5. Ouvrez le fichier `docker-compose.yml`. Remplacez toutes les occurrences de l'ancien mot de passe par le nouveau :

```
services:
  wazuh.manager:
    ...
    environment:
      - INDEXER_URL=https://wazuh.indexer:9200
      - INDEXER_USERNAME=admin
      - INDEXER_PASSWORD=SecretPassword
      - FILEBEAT_SSL_VERIFICATION_MODE=full
      - SSL_CERTIFICATE_AUTHORITIES=/etc/ssl/root-ca.pem
      - SSL_CERTIFICATE=/etc/ssl/filebeat.pem
      - SSL_KEY=/etc/ssl/filebeat.key
      - API_USERNAME=wazuh-wui
      - API_PASSWORD=MyS3cr37P450r.*-
    ...
  wazuh.dashboard:
    ...
    environment:
      - INDEXER_USERNAME=admin
      - INDEXER_PASSWORD=SecretPassword
      - WAZUH_API_URL=https://wazuh.manager
      - DASHBOARD_USERNAME=kibanaserver
      - DASHBOARD_PASSWORD=kibanaserver
      - API_USERNAME=wazuh-wui
      - API_PASSWORD=MyS3cr37P450r.*-
    ...
```

	E4 Documentation E4	Lucas MAIGNE
	E4-Wazuh-Doc	Date : 12/05/2024

6. Démarrez le conteneur :

```
docker-compose up -d
```

7. Exécutez `docker exec -it <WAZUH_INDEXER_CONTAINER_NAME> bash` pour entrer dans le conteneur. Par exemple :

```
docker exec -it single-node_wazuh.indexer_1 bash
```

8. Définissez les variables suivantes :

```
export INSTALLATION_DIR=/usr/share/wazuh-indexer
CACERT=$INSTALLATION_DIR/certs/root-ca.pem
KEY=$INSTALLATION_DIR/certs/admin-key.pem
CERT=$INSTALLATION_DIR/certs/admin.pem
export JAVA_HOME=/usr/share/wazuh-indexer/jdk
```

8. Attendez que l'indexeur Wazuh s'initialise correctement. Le temps d'attente peut varier de deux à cinq minutes. Ensuite, exécutez le script `securityadmin.sh` pour appliquer toutes les modifications :

```
bash /usr/share/wazuh-indexer/plugins/opensearch-security/tools/securityadmin.sh -cd /usr/share/wazuh-i
```

9. Quittez le conteneur de l'indexeur Wazuh et connectez vous avec le nouveau mot de passe.

Edited 1 week ago by Lucas Maigne

Sources

Documentations issues de GitLab que j'ai réalisées durant mon stage au sein de l'entreprise Ackwa.