Rapport Wazuh

Installation et configuration

Céréna HOSTAINS

2024-04-04

Table des matières

1 Serveur 1: Wazuh

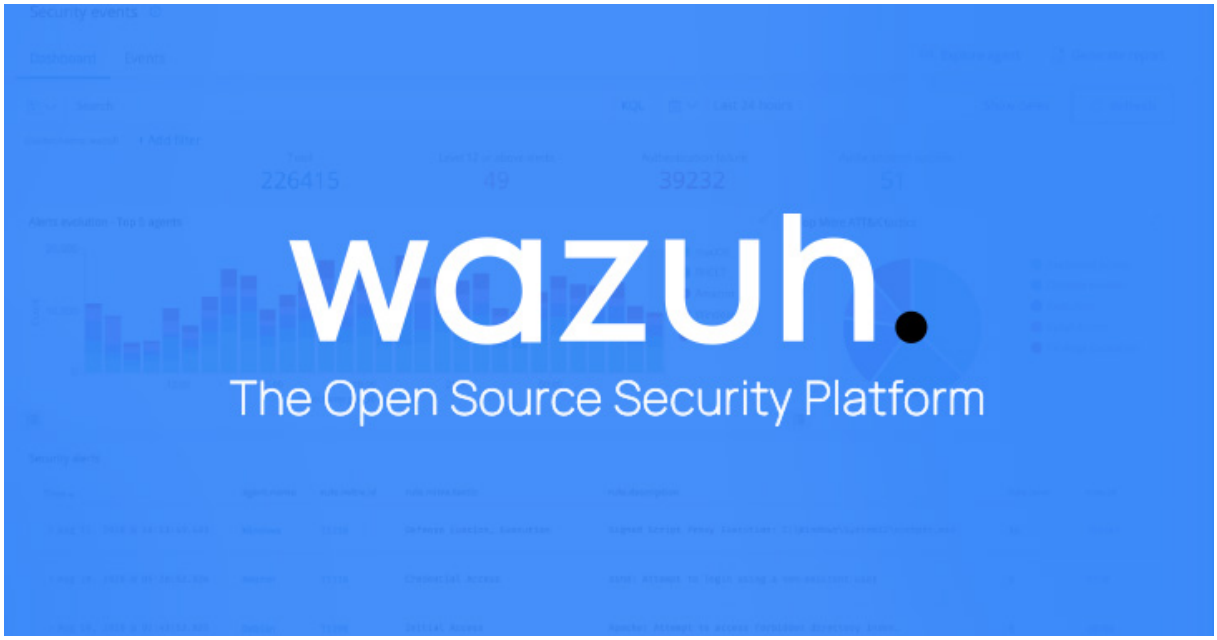

Figure 1.1: logoWazuh

Licence GNU General Public License

1.1 Caractéristiques matérielles pour 1 à 25 agents

- Processeurs: 4 vCPU
- Mémoire: 8 Gio RAM
- Stockage: 50 Go
- Système d'exploitation: Amazon Linux 2 / CentOS 7, 8 / Red Hat Enterprise Linux 7, 8, 9 / Ubuntu 16.04, 18.04, 20.04, 22.04
- Compatibilité du navigateur: Chrome 95 ou version ultérieure, Firefox 93 ou version ultérieure, Safari 13.7 ou version ultérieure

1.2 Schéma réseau

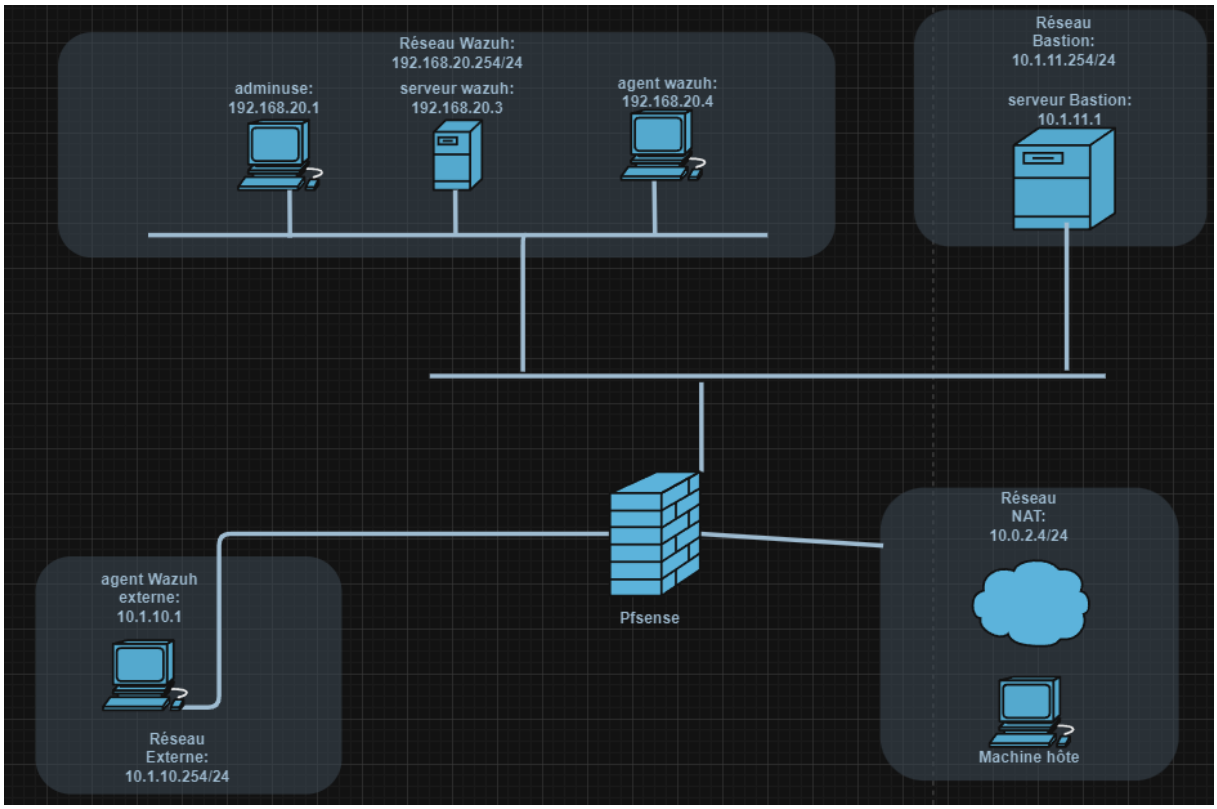

Figure 1.2: Infrastructure Wazuh

1.3 Prérequis

- Installez les dépendances.
- Téléchargez et exécutez l'assistant d'installation de Wazuh (*téléchargement dockerisé*):

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

- Exécutez la commande suivante pour obtenir les certificats souhaités:

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

Les certificats se trouvent dans le répertoire config/wazuh_indexer_ssl_certs.

- Démarrez le déploiement Wazuh en utilisant docker-compose: `docker-compose up` ou `docker-compose up -d`, selon le type de détails souhaités.

1.4 Configurations à apporter

- Dans wazuh-docker/single-node, il faut modifier le fichier **docker-compose.yaml** et remplacer **https:// :9200** par **https:// l'adresse du serveur Wazuh:9200**.

1.5 Configuration firewall

- Ouvrir les ports:

Ports	Protocoles	Besoins
1514	TCP	connexion du service Wazuh agent
1515	TCP	service d'inscription de l'agent
514	UDP	collecte les logs des agents Wazuh
55000	TCP	API RESTful serveur*
9200	TCP	visualisation client de l'interface Wazuh
443	TCP	interface web Wazuh utilisateur

*Cette API fournit une interface web permettant d'interagir avec le serveur Wazuh, notamment pour effectuer des opérations de gestion et de surveillance, comme la visualisation des journaux, la gestion des règles de détection, la configuration du système, etc.

1.6 Paramétrage Wazuh

1.6.1 Seuil d'alerte

Chaque événement collecté par l'agent Wazuh est transmis au gestionnaire Wazuh. Le gestionnaire attribuera à l'événement un niveau de gravité en fonction des règles qu'il correspond à partir du jeu de règles. Par défaut, il enregistre uniquement les alertes avec un niveau de gravité de 3 ou plus. Le seuil de niveau d'alerte est configuré dans le `config/wazuh_cluster/wazuh_manager.conf`, qui utilise la balise XML `<alert>`.

```
<ossec_config>
  <alerts>
      <log_alert_level>6</log_alert_level>
  </alerts>
</ossec_config>
```

Ceci est le niveau de gravité minimum qui déclenchera les alertes stockées dans le `alerts.log`.

Quand une valeur est modifiée dans le fichier `wazuh_manager.conf`, le service doit être redémarré avant que les modifications ne prennent effet.

```
systemctl restart wazuh-manager
```

1.6.2 Activation des archives Wazuh

Pour stocker et conserver les journaux, les alertes et d'autres données liées à la sécurité collectées sur le serveur Wazuh, il faut activer les archives Wazuh. Pour cela, il faut se déplacer dans le fichier ossec.conf et remplacer les champs en surbrillance ci-dessous sur `yes`:

```
<ossec_config>
  <global>
    <jsonout_output>yes</jsonout_output>
    <alerts_log>yes</alerts_log>
    <logall>yes</logall>
    <logall_json>yes</logall_json>
</ossec_config>
```

`<logall>` est une option qui active ou qui désactive l'archivage de tous les messages du journal. Lorsqu'il est activé, le serveur Wazuh stocke les journaux au format syslog. `<logall_json>` est une option qui active ou qui désactive la journalisation des événements. Lorsqu'il est activé, le serveur Wazuh stocke les événements au format JSON.

Redémarrez le gestionnaire Wazuh pour appliquer les modifications de configuration.

1.6.3 Visualisation des événements sur le tableau de bord

Pour créer les indices et les afficher dans le tableau de bord Wazuh, il faut:

- Modifier le fichier de configuration Filebeat `/wazuh-docker/build-docker-images/wazuh-manager/config/filebeat.yml` et changer la valeur false en true:

```
archives:
enabled: true
```

- Redémarrez Filebeat pour appliquer les modifications de configuration
- Cliquez sur l'icône du menu supérieur gauche et accédez à Stack management > Index patterns > Create index pattern. Utilisez `wazuh-archives-*` comme nom du modèle d'index, et définissez `timestamp` dans Time field dans la liste déroulante.
- Pour afficher les événements sur le tableau de bord, cliquez sur l'icône du menu supérieur gauche et accédez à Discover. Modifiez le modèle d'index pour `wazuh-archives-*`.

1.6.4 Modification du mot de passe des utilisateurs Wazuh

- Tout d'abord, arrêtez le déploiement si le docker est en cours d'exécution avec `docker-compose down`
- Exécutez cette commande pour générer le hachage de votre nouveau mot de passe. Une fois le conteneur lancé, entrez le nouveau mot de passe et appuyez sur Entrée:

```
docker run --rm -ti wazuh/wazuh-indexer:4.7.3 bash
↪ /usr/share/wazuh-indexer/plugins/opensearch-security/tools/hash.sh
```

- Copiez le hachage généré.
- Ouvrez le fichier `config/wazuh_indexer/internal_users.yml`. Localisez le bloc pour l'utilisateur pour lequel vous modifiez le mot de passe. Et remplacez le hachage.
- Pour définir le nouveau mot de passe: Ouvrez le fichier docker-compose.yml. Modifiez toutes les occurrences de l'ancien mot de passe par le nouveau.
- Appliquer les changements: Démarrez la pile de déploiement: `docker-compose up -d`

Vous ne pouvez changer qu'un mot de passe à la fois.

1.6.5 Définir un modèle d'index

- Accédez à Management > Stack Management et cliquez sur Index Patterns dans le menu du tableau de bord Wazuh en haut à gauche.
- Cliquez sur Create index pattern.
- Dans Index pattern name, saisissez un nom de modèle d'index comme wazuh-*. Cela permettra de définir le modèle d'index pour visualiser les événements transférés et indexés.
- Cliquez sur Next step.
- Séléctionnez Timestamp dans le menu déroulant Time field.
- Cliquez sur Create index pattern.
- Pour afficher le modèle créé, cliquez sur Discover dans le menu supérieur gauche.
- Séléctionnez le modèle d'index créé pour visualiser les événements.

1.6.6 Les indices wazuh-statistics-*

Le tableau de bord Wazuh utilise les indices wazuh-statistics-* pour afficher des statistiques sur l'utilisation et les performances du serveur Wazuh. Les informations affichées incluent le nombre d'événements décodés, le volume d'octets reçus et le nombre de sessions TCP.

Ces indices stockent les statistiques du serveur Wazuh toutes les 5 minutes par défaut.

- Pour visualiser ces informations dans le tableau de bord Wazuh, accédez à Management > Statistics.

Si l'erreur **Wazuh API error** apparaît cela signifie qu'il faut activer le mode cluster pour visualiser l'ensemble des informations.

- Pour activer le mode cluster, dirigez-vous dans le fichier config/wazuh_cluster/wazuh_manager.conf.

1.6.7 Configuration de sortie Syslog

La sortie Syslog est configurée dans le fichier `wazuh_manager.conf`.

```
<ossec_config>
  <syslog_output>
    <level>à_compléter</level>
    <server>à_compléter</server>
  </syslog_output>

  <syslog_output>
    <server>à_compléter</server>
  </syslog_output>
</ossec_config>
```

La configuration ci-dessus enverra des alertes au serveur en question et, si le niveau d'alerte est supérieur au numéro compléter, alors les alertes sont également envoyées à l'autre serveur en question. Pour appliquer les modifications, redémarrez Wazuh

1.6.8 Configuration des alertes e-mail

Wazuh peut être configuré pour envoyer des alertes par e-mail à une ou plusieurs adresses e-mail lorsque certaines règles sont déclenchées ou pour des rapports d'événements quotidiens.

Afin de configurer Wazuh pour envoyer des alertes par e-mail, les paramètres de messagerie doivent être configurés dans le `<global>` du fichier `wazuh_manager.conf`:

```
<ossec_config>
    <global>
        <email_notification>yes</email_notification>
        <email_to>me@test.com</email_to>
```

```
        <smtp_server>mail.test.com</smtp_server>
        <email_from>wazuh@test.com</email_from>
    </global>
</ossec_config>
```

Une fois que ce qui précède a été configuré, le email_alert_level doit être défini sur le niveau d'alerte minimum qui déclenchera un e-mail.

```
<ossec_config>
  <alerts>
      <email_alert_level>10</email_alert_level>
  </alerts>
</ossec_config>
```

Après que le `alert_level` a été configuré, Wazuh doit être redémarré pour que la modification prenne effet.

1.6.9 Fichier `wazuh_manager.conf`

Dans le fichier `wazuh_manager.conf`, il est important d'activer le `CIS-CAT`, le `Osquery integration`, le `System inventory`, le `vulnerability-detector`, les `OS vulnerabilities` et le SCA.

1.6.10 Résolution du problème Check alerts index pattern

Lors du Healthcheck, une erreur apparaît sur le check alert index pattern, nous indiquant qu'il manque un template. Pour régler ce problème, nous devons procéder étape par étape:

- Dans `wazuh-docker`, téléchargez le modèle Wazuh et enregistrez-le dans un fichier (par exemple, template.json'):

```
curl -so template.json
↪  https://raw.githubusercontent.com/wazuh/wazuh/4.7/extensions/elasticsearch/7.x/wazuh-
↪  template.json
```

- Enregistrez les modifications et insérez le nouveau modèle dans l'indexeur Wazuh:

```
curl -XPUT -k -u admin:SecretPassword 'https://<adresse_serveur>:9200/_template/wazuh' -H
↪  'Content-Type: application/json' -d @template.json
```

- Dès que le message `{"acknowledged":true}` apparaît, cela signifie que le problème est résolu.
- Depuis l'interface Wazuh, nous pouvons interroger les informations d'index à l'aide de l'API de l'indexeur Wazuh: dirigez-vous sur le menu > Management > Dev Tools:

```
GET /_cat/indices/wazuh-*?v
```

- Rechargez la page est relancez le Healthcheck.

L'utilisateur kibanaserver avec le mot de passe kibanaserver à également les droits.

1.6.11 Changement du logo Wazuh

Pour utiliser nos propre logos sur l'interface Wazuh, il suffit de cliquer sur le logo avec le menu défilant de l'application et d'aller dans Settings > Configuration. Dans la page qui apparaît, allez au niveau de Custom branding et configurez les propriétés suivantes:

- App main logo: Ce logo est utilisé dans le menu principal de l'application, dans le coin supérieur gauche.
- Healthcheck logo: Ce logo est affiché lors de la routine Healthcheck de l'application.
- PDF reports logo: Ce logo est utilisé dans les rapports PDF générés par l'application. Il est placé dans le coin supérieur gauche de chaque page pdf.
- Navigation drawer logo: Il s'agit du logo que l'application doit afficher dans la navigation de la plateforme, c'est-à-dire, au niveau du menu défilant.

2 Agent Wazuh

2.1 Installation

- Pour déployer un nouvel agent, il faut suivre les instructions du tableau de bord Wazuh. Accédez à Wazuh > Agents, et cliquez sur Deploy new agent.
- Ensuite, suivez les étapes pour compléter le déploiement du nouvel agent.