Aujourd'hui, nous allons installer un SIEM.
Un SIEM est une solution permettant d'aider à la détection, à l'analyse et à la détection des menaces informatiques.

Pourquoi installer un SIEM ?

- Vue d'ensemble des menaces potentielles
- Identification et réponses aux menaces
- Audit de vulnérabilité

I. Installation

Concernant l'installation de wazuh je vais passer par un conteneur docker depuis une vm archlinux. C'est un choix personnel d'utiliser docker. Je trouve l'installation bien moins contraignante que les autres méthodes d'installation proposer (script tout en un/ manuelle).

Commande pour augmenter les zones mémoire :

```
sysctl -w vm.max_map_count=262144
```

Ici, je configure wazuh pour un seul noeud :

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

Génération des certificats :

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

Changement du mot de passe par défaut pour la connexion au dashboard :

```
sudo vim config/wazuh_dashboard/wazuh.yml
```

```
hosts:
  - 1513629884013:
      url: "https://wazuh.manager"
      port: 55000
      username: wazuh-wui
      password: "                    "
      run_as: false
```

Changement du mot de passe par défaut de kibana :

```
docker run --rm -ti wazuh/wazuh-indexer:4.11.0 bash /usr/share/wazuh-
indexer/plugins/opensearch-security/tools/hash.sh
```

```
[localadm@template single-node]$ sudo docker run --rm -ti wazuh/wazuh-indexer:4.11.0 bash /usr/share/wa
zuh-indexer/plugins/opensearch-security/tools/hash.sh
************************************************************************
** This tool will be deprecated in the next major release of OpenSearch **
** https://github.com/opensearch-project/security/issues/1755           **
************************************************************************
[Password:]
$2y$
```

Changement dans le fichier internal_user :

```
admin:
  hash: "$2y$
  reserved: true
  backend_roles:
  - "admin"
  description: "Demo admin user"

kibanaserver:
  hash: "$2y
  reserved: true
  description: "Demo kibanaserver user"
```

On redémarre le dockerfile :

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

Export de variable suivante :

```
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
```

démarrer le script pour appliquer les changements :

```
bash /usr/share/wazuh-indexer/plugins/opensearch-
security/tools/securityadmin.sh -cd /usr/share/wazuh-indexer/opensearch-
security/ -nhnv -cacert  $CACERT -cert $CERT -key $KEY -p 9200 -icl
```

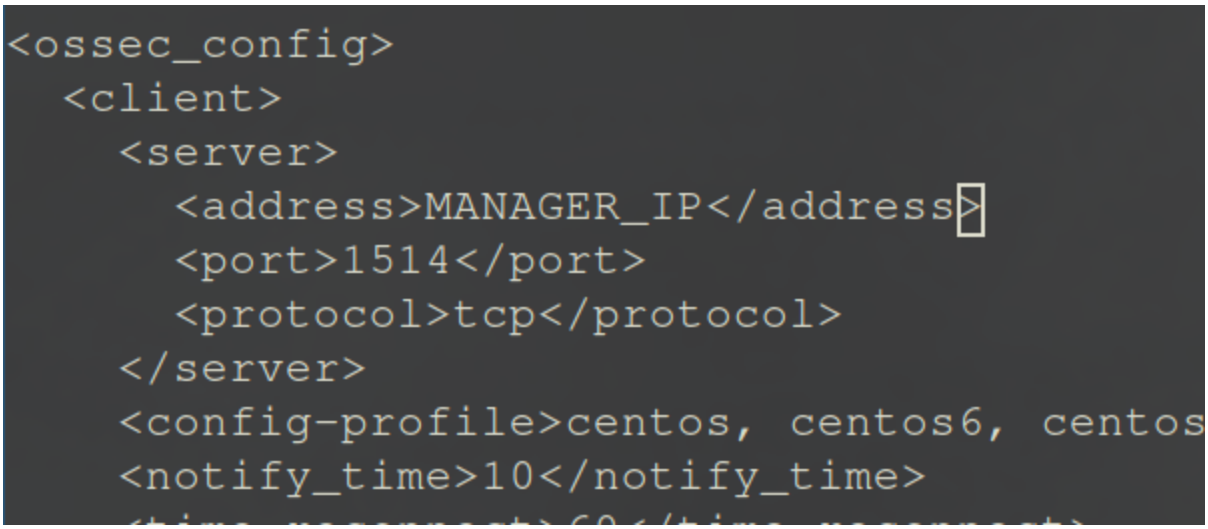
Vous pouvez maintenant accéder à WAZUH depuis son interface web.

Installation d'un agent

Installation depuis un système archlinux :

```
git clone https://aur.archlinux.org/wazuh-agent.git
cd wazuh-agent
makepkg -si
```

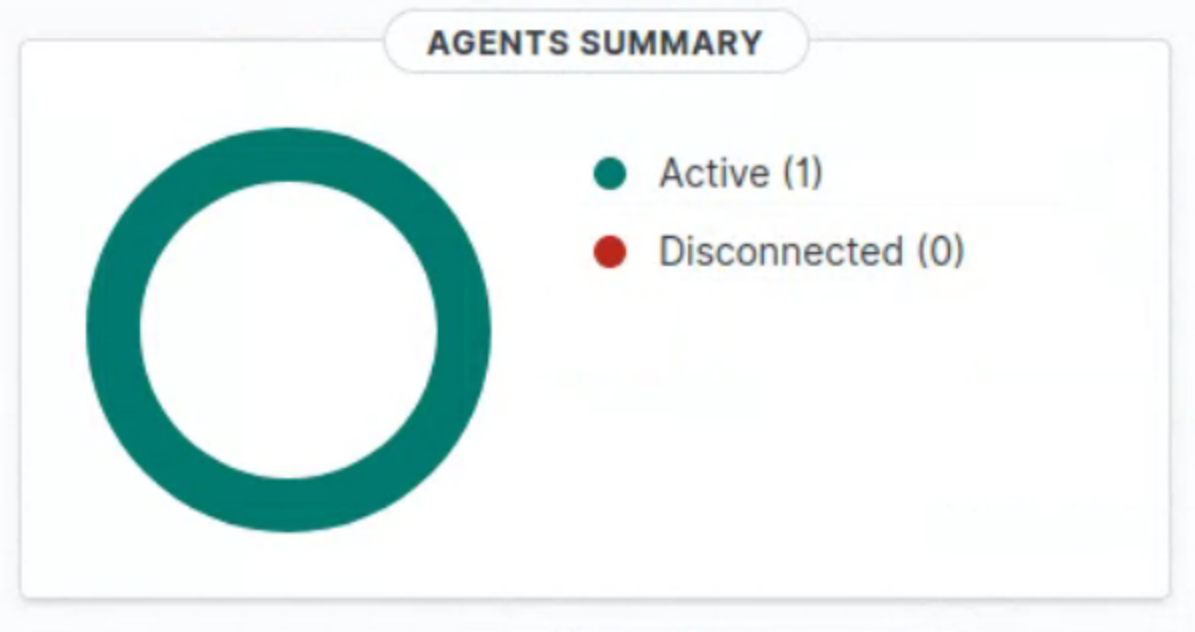
Changement de l'ip dans /var/ossec/etc/ossec.conf:



On démarre ensuite le service :

```
sudo systemctl enable --now wazuh-agent
```

Notre agent a bien été détecté :



Vous pouvez maintenant installer des agents sur toutes vos VM/conteneurs.