

Wazuh - Journal De Bord

Sommaire

Wazuh Indexer

- Démarches :
 - Ajout des certificats :
 - Configuration du fichier config.yml
 - Installation du service
 - Configuration de l'indexer
 - Déploiement des certificats
- Redimensionnement de la partition /dev/sda3 car les logs arrivent sur le serveur et non pas sur l'indexeur ./

Wazuh Server

- Installation du service
 - Création d'un utilisateur par défaut admin | admin
 - Déploiement des certificats

Wazuh Dashboard

- Installation du service
 - Déploiement des certificats
 - Démarrage du service

Debuggage

- Erreur de chargement de l'API
- Données figées pendant un long moment sur l'interface

Déploiement certificats *.crous-nantes.fr

- Wazuh-Dashboard
- Wazuh-Server

Déploiement agents

- Windows
- Linux

Ports à ouvrir

- Wazuh-Dashboard
- Wazuh-Indexer
- Wazuh-Server
- Wazuh-Agent

Changement mot de passe administrateur

Configuration

- Activation du scan des vulnérabilités sur les hôtes
- Activation de l'active response

Déplacement du dossier logs sur wazuh-server

Wazuh Indexer

Spécificités de la machine Wazuh-Indexer :

- 16Go de RAM
- 8 Coeurs
- 500Go de stockage pour les logs
- 192.168.11.2/24, Gateway 192.168.11.254
- Dans Vlan DMZ_PRIV

Démarches :

apt-get update
apt-get install curl

Ajout des certificats :

mkdir /etc/wazuh && cd /etc/wazuh
curl -sO https://packages.wazuh.com/4.7/wazuh-certs-tool.sh

```
curl -sO https://packages.wazuh.com/4.7/config.yml
```

Configuration du fichier config.yml

```
nodes:
  # Wazuh indexer nodes
  indexer:
    - name: node-1
      ip: "192.168.11.2"
    #- name: node-2
    # ip: "<indexer-node-ip>"
    #- name: node-3
    # ip: "<indexer-node-ip>"
  # Wazuh server nodes
  # If there is more than one Wazuh server
  # node, each one must have a node_type
  server:
    - name: wazuh-1
      ip: "192.168.11.3"
    # node_type: master
    #- name: wazuh-2
    # ip: "<wazuh-manager-ip>"
    # node_type: worker
    #- name: wazuh-3
    # ip: "<wazuh-manager-ip>"
    # node_type: worker
  # Wazuh dashboard nodes
  dashboard:
    - name: dashboard
      ip: "192.168.11.1"
```

```
chmod +rwx wazuh-certs-tool.sh
./wazuh-certs-tool.sh
```

Les certificats créés vont servir pour créer les deux autres serveurs de Wazuh donc on les compresse pour les copier sur les autres machines.

```
tar -cvf ./wazuh-certificates.tar -C ./wazuh-certificates/ .
scp ./wazuh-certificates.tar crous@192.168.11.1:/home/crous
scp ./wazuh-certificates.tar crous@192.168.11.3:/home/crous
```

Installation du service

```
apt-get install debconf adduser procps
apt-get install gnupg apt-transport-https
curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | gpg --no-default-keyring --keyring gnupg-ring:/usr/share/keyrings/wazuh.gpg --import && chmod 644 /usr/share/keyrings/wazuh.gpg
echo "deb [signed-by=/usr/share/keyrings/wazuh.gpg] https://packages.wazuh.com/4.x/apt/ stable main" | tee -a /etc/apt/sources.list.d/wazuh.list
apt-get update
apt-get -y install wazuh-indexer
```

Configuration de l'indexer

```
Fichier /etc/wazuh-indexer/opensearch.yml :
-network.host : 192.168.11.2
node.name : node-1
```

Pour le reste j'ai pas touché pour l'instant.

Déploiement des certificats

```
#NODE_NAME=node-1
```

```
mkdir /etc/wazuh-indexer/certs

tar -xf /etc/wazuh/wazuh-certificates.tar -C /etc/wazuh-indexer/certs/ ./${NODE_NAME}.pem ./${NODE_NAME}-key.pem ./admin.pem ./admin-key.pem ./root-ca.pem

mv -n /etc/wazuh-indexer/certs/${NODE_NAME}.pem /etc/wazuh-indexer/certs/indexer.pem

mv -n /etc/wazuh-indexer/certs/${NODE_NAME}-key.pem /etc/wazuh-indexer/certs/indexer-key.pem

chmod 500 /etc/wazuh-indexer/certs

chmod 400 /etc/wazuh-indexer/certs/*

chown -R wazuh-indexer:wazuh-indexer /etc/wazuh-indexer/certs

bash /usr/share/wazuh-indexer/bin/indexer-security-init.sh
```

Redimensionnement de la partition /dev/sda3 car les logs arrivent sur le serveur et non pas sur l'indexeur :/

Dans Vcenter :

--> ISO GpartEd ([VIRT - Guide d'extension de disque de VM — Wikicrous \(crous-nantes.fr\)](https://www.wikicrous.fr/guide/extension-disque-vm))

Wazuh Server

Installation du service

```
apt-get install gnupg apt-transport-https

apt-get install curl

curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | gpg --no-default-keyring --keyring gnupg-ring:/usr/share/keyrings/wazuh.gpg --import && chmod 644 /usr/share/keyrings/wazuh.gpg

echo "deb [signed-by=/usr/share/keyrings/wazuh.gpg] https://packages.wazuh.com/4.x/apt/ stable main" | tee -a /etc/apt/sources.list.d/wazuh.list

apt-get update

apt-get install wazuh-manager

systemctl daemon-reload

systemctl enable wazuh-manager

systemctl start wazuh-manager

apt-get install filebeat

curl -so /etc/filebeat/filebeat.yml https://packages.wazuh.com/4.7/tpl/wazuh/filebeat/filebeat.yml

Dans /etc/filebeat/filebeat.yml --> hosts: ["192.168.11.2:9200"]

filebeat keystore create
```

Création d'un utilisateur par défaut admin | admin

```
echo admin | filebeat keystore add username --stdin --force

echo admin | filebeat keystore add password --stdin --force

curl -so /etc/filebeat/wazuh-template.json https://raw.githubusercontent.com/wazuh/wazuh/v4.7.2/extensions/elasticsearch/7.x/wazuh-template.json

chmod go+r /etc/filebeat/wazuh-template.json

curl -s https://packages.wazuh.com/4.x/filebeat/wazuh-filebeat-0.3.tar.gz | tar -xvz -C /usr/share/filebeat/module
```

Déploiement des certificats

```
#NODE_NAME=wazuh-1

mkdir /etc/filebeat/certs

tar -xf ./wazuh-certificates.tar -C /etc/filebeat/certs/ ./${NODE_NAME}.pem ./${NODE_NAME}-key.pem ./root-ca.pem

mv -n /etc/filebeat/certs/${NODE_NAME}.pem /etc/filebeat/certs/filebeat.pem

mv -n /etc/filebeat/certs/${NODE_NAME}-key.pem /etc/filebeat/certs/filebeat-key.pem
```

```
chmod 500 /etc/filebeat/certs
```

```
chmod 400 /etc/filebeat/certs/*
```

```
chown -R root:root /etc/filebeat/certs
```

```
systemctl daemon-reload
```

```
systemctl enable filebeat
```

```
systemctl start filebeat
```

filebeat test output

Si erreur comme ça :

```
root@Wazuh-Server:/etc/filebeat/certs# filebeat test output
elasticsearch: https://192.168.11.2:9200...
  parse url... OK
  connection...
    parse host... OK
    dns lookup... OK
    addresses: 192.168.11.2
    dial up... OK
  TLS...
    security: server's certificate chain verification is enabled
    handshake... OK
    TLS version: TLSv1.3
    dial up... OK
  talk to server... ERROR 503 Service Unavailable: OpenSearch Security not initialized.
```

Exécuter "bash /usr/share/wazuh-indexer/bin/indexer-security-init.sh" sur Wazuh-Indexer

```
root@Wazuh-Server:/etc/filebeat/certs# filebeat test output
elasticsearch: https://192.168.11.2:9200...
  parse url... OK
  connection...
    parse host... OK
    dns lookup... OK
    addresses: 192.168.11.2
    dial up... OK
  TLS...
    security: server's certificate chain verification is enabled
    handshake... OK
    TLS version: TLSv1.3
    dial up... OK
  talk to server... OK
  version: 7.10.2
```

Wazuh Dashboard

Installation du service

```
apt-get install debhelper tar curl libcap2-bin
```

```
apt-get install gnupg apt-transport-https
```

```
apt-get install curl
```

```
curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | gpg --no-default-keyring --keyring gnupg-ring:/usr/share/keyrings/wazuh.gpg --import && chmod 644 /usr/share/keyrings/wazuh.gpg
```

```
echo "deb [signed-by=/usr/share/keyrings/wazuh.gpg] https://packages.wazuh.com/4.x/apt/ stable main" | tee -a /etc/apt/sources.list.d/wazuh.list
```

```
apt-get update
```

```
apt-get -y install wazuh-dashboard
```

Dans /etc/wazuh-dashboard/opensearch_dashboards.yml

```
--> server.host : 0.0.0.0
```

```
opensearch.hosts : https://192.168.11.2:9200
```

Déploiement des certificats

```
#NODE_NAME=dashboard
```

```
mkdir /etc/wazuh-dashboard/certs
```

```
tar -xf ./wazuh-certificates.tar -C /etc/wazuh-dashboard/certs/ ./${NODE_NAME}.pem ./${NODE_NAME}-key.pem ./root-ca.pem
```

```
mv -n /etc/wazuh-dashboard/certs/${NODE_NAME}.pem /etc/wazuh-dashboard/certs/dashboard.pem
```

```
mv -n /etc/wazuh-dashboard/certs/$NODE_NAME-key.pem /etc/wazuh-dashboard/certs/dashboard-key.pem
```

```
chmod 500 /etc/wazuh-dashboard/certs
```

```
chmod 400 /etc/wazuh-dashboard/certs/*
```

```
chown -R wazuh-dashboard:wazuh-dashboard /etc/wazuh-dashboard/certs
```

Démarrage du service

```
systemctl daemon-reload
```

```
systemctl enable wazuh-dashboard
```

```
systemctl start wazuh-dashboard
```

Debuggage

Problème avec le lancement : systemctl ne peut pas le lancer car il manque de permission pour ouvrir le fichier de configuration :

```

janv. 31 15:19:42 Wazuh-Dashboard.restau.crousntes.fr systemd[1]: Started wazuh-dashboard.
janv. 31 15:19:42 Wazuh-Dashboard.restau.crousntes.fr opensearch-dashboards[22387]: vi6.20.0
janv. 31 15:19:42 Wazuh-Dashboard.restau.crousntes.fr opensearch-dashboards[22387]: node:internal/fs/utils:347
janv. 31 15:19:42 Wazuh-Dashboard.restau.crousntes.fr opensearch-dashboards[22387]:   throw err;
janv. 31 15:19:42 Wazuh-Dashboard.restau.crousntes.fr opensearch-dashboards[22387]:
janv. 31 15:19:42 Wazuh-Dashboard.restau.crousntes.fr opensearch-dashboards[22387]: Error: EACCES: permission denied, open '/etc/wazuh-dashboard/opensearch_dashboards.yml'
janv. 31 15:19:42 Wazuh-Dashboard.restau.crousntes.fr opensearch-dashboards[22387]:   at Object.openSync (node:fs:550:3)
janv. 31 15:19:42 Wazuh-Dashboard.restau.crousntes.fr opensearch-dashboards[22387]:   at Object.readFileSync (node:fs:456:35)
janv. 31 15:19:42 Wazuh-Dashboard.restau.crousntes.fr opensearch-dashboards[22387]:   at readYaml (/usr/share/wazuh-dashboard/node_modules/@oad/apm-config-loader/target/utils/read_config.js:33:18)
janv. 31 15:19:42 Wazuh-Dashboard.restau.crousntes.fr opensearch-dashboards[22387]:   at Object.exports.getConfigFromFiles (/usr/share/wazuh-dashboard/node_modules/@oad/apm-config-loader/target/utils/read_config.js:44:18)
janv. 31 15:19:42 Wazuh-Dashboard.restau.crousntes.fr opensearch-dashboards[22387]:   at exports.loadConfiguration (/usr/share/wazuh-dashboard/node_modules/@oad/apm-config-loader/target/utils/read_config.js:55:15)
janv. 31 15:19:42 Wazuh-Dashboard.restau.crousntes.fr opensearch-dashboards[22387]:   at module.exports (/usr/share/wazuh-dashboard/src/apm.js:55:15)
janv. 31 15:19:42 Wazuh-Dashboard.restau.crousntes.fr opensearch-dashboards[22387]:   at Object.<anonymous> (/usr/share/wazuh-dashboard/src/cli/dist.js:32:18)
janv. 31 15:19:42 Wazuh-Dashboard.restau.crousntes.fr opensearch-dashboards[22387]:   at Module.compile (node:internal/modules/cjs/loader:1196:14)
janv. 31 15:19:42 Wazuh-Dashboard.restau.crousntes.fr opensearch-dashboards[22387]:   at Object.Module._extensions..js (node:internal/modules/cjs/loader:1250:10)
janv. 31 15:19:42 Wazuh-Dashboard.restau.crousntes.fr opensearch-dashboards[22387]:   at Module.load (node:internal/modules/cjs/loader:1074:32) {
janv. 31 15:19:42 Wazuh-Dashboard.restau.crousntes.fr opensearch-dashboards[22387]:     errno: -13,
janv. 31 15:19:42 Wazuh-Dashboard.restau.crousntes.fr opensearch-dashboards[22387]:     syscall: 'open',
janv. 31 15:19:42 Wazuh-Dashboard.restau.crousntes.fr opensearch-dashboards[22387]:     code: 'EACCES',
janv. 31 15:19:42 Wazuh-Dashboard.restau.crousntes.fr opensearch-dashboards[22387]:     path: '/etc/wazuh-dashboard/opensearch_dashboards.yml'
janv. 31 15:19:42 Wazuh-Dashboard.restau.crousntes.fr opensearch-dashboards[22387]: }
janv. 31 15:19:42 Wazuh-Dashboard.restau.crousntes.fr systemd[1]: wazuh-dashboard.service: Main process exited, code=exited, status=1/FAILURE
janv. 31 15:19:42 Wazuh-Dashboard.restau.crousntes.fr systemd[1]: wazuh-dashboard.service: Failed with result 'exit-code'.

```

En revanche en exécutant le lancement à la main avec :

```
sudo /usr/share/wazuh-dashboard/bin/opensearch-dashboards --allow-root -c "/etc/wazuh-dashboard/opensearch_dashboards.yml"
```

Lancé comme ça, le serveur web fonctionne et est accessible via <https://192.168.11.1>

```

root@Wazuh-Dashboard:/etc/wazuh-dashboard# /usr/share/wazuh-dashboard/bin/opensearch-dashboards --allow-root -c "/etc/wazuh-dashboard/opensearch_dashboards.yml"
vi6.20.0
log [14:32:23.533] [info] [plugins-service] Plugin "dataSourceManagement" has been disabled since the following direct or transitive dependencies are missing or disabled: [dataSource]
log [14:32:23.539] [info] [plugins-service] Plugin "dataSource" is disabled.
log [14:32:23.539] [info] [plugins-service] Plugin "visTypeKy" is disabled.
log [14:32:23.539] [info] [plugins-service] Plugin "mlCommonDashboards" is disabled.
log [14:32:23.737] [info] [plugins-system] Setting up [44] plugins: [alertingDashboards, usageCollection, opensearchDashboardsUsageCollection, opensearchDashboardsLegacy, mapsLegacy, share, opensearchUIShared,
home, data, home, console, apmOss, management, indexPatternManagement, advancedSettings, savedObjects, reportsDashboards, indexManagementDashboards, dashboard, visualizations, visTypeVega, visTypeTable, visTypeTimeline, vis
regionMap, customImportMapDashboards, inputControlVis, ganttChartDashboards, visualize, notificationsDashboards, charts, visTypeVislib, visTypeTimeSeries, visTypeTagcloud, visTypeMetric, discover, savedObjectManagement]
log [14:32:24.053] [info] [savedObjects-service] Waiting until all OpenSearch nodes are compatible with OpenSearch Dashboards before starting saved objects migrations...
log [14:32:24.128] [info] [savedObjects-service] Starting saved objects migrations
log [14:32:24.255] [info] [plugins-system] Starting [44] plugins: [alertingDashboards, usageCollection, opensearchDashboardsUsageCollection, opensearchDashboardsLegacy, mapsLegacy, share, opensearchUIShared,
home, data, home, console, apmOss, management, indexPatternManagement, advancedSettings, savedObjects, reportsDashboards, indexManagementDashboards, dashboard, visualizations, visTypeVega, visTypeTable, visTypeTimeline, vis
regionMap, customImportMapDashboards, inputControlVis, ganttChartDashboards, visualize, notificationsDashboards, charts, visTypeVislib, visTypeTimeSeries, visTypeTagcloud, visTypeMetric, discover, savedObjectManagement]
log [14:32:24.499] [info] [httpdmain] Server running at https://0.0.0.0:443
log [14:32:24.663] [info] [OpenSearchDashboards] [http] http server running at https://0.0.0.0:443

```

Possible solution fonctionnelle sur <https://github.com/wazuh/wazuh/discussions/19560>

En fait non, pas le même problème.

```
--> chmod -R 755 /etc/wazuh-dashboard
```

Erreur de chargement de l'API

```
--> Pas assez de permission sur les fichiers
```

```
Réglé avec chown -R wazuh-dashboard:wazuh-dashboard /usr/share/wazuh-dashboard
```

Données figées pendant un long moment sur l'interface

Checker mot de passe Filebeat dans /etc/filebeat/filebeat.yml, il doit correspondre au mot de passe défini pour admin

```
echo "<nouveau-mot-de-passe>" | filebeat keystore add password --stdin --force
```

Déploiement certificats *.crous-nantes.fr

Wazuh-Dashboard

Déplacement des fichiers créés par Certbot dans /etc/wazuh-dashboard/certs/

Dans /etc/wazuh-dashboard/opensearch-dashboards.yml :

server.ssl.key: "/etc/wazuh-dashboard/certs/privkey.pem"

server.ssl.certificate: "/etc/wazuh-dashboard/certs/fullchain.pem"

Wazuh-Server

Même chose mais dans /etc/filebeat/certs/

Fichier : /etc/filebeat/filebeat.yml

Déploiement agents

Les agents doivent envoyer leurs informations au serveur/manager wazuh, à savoir wazuh-serveur.crous-nantes.fr

Windows

Le script désinstalle la version déjà installée de l'agent s'il est installé, puis installe la bonne version et lance le service. (Peut-être fonctionnel)

```
If (Test-Path "C:\Program Files (x86)\ossec-agent\wazuh-agent.exe"){
Invoke-RestMethod -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.7.2-1.msi -OutFile ${env:tmp}\wazuh-agent.msi; msixec.exe /q /n /x ${env:tmp}\wazuh-agent.msi
/norestart -Wait
}

[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.7.2-1.msi -OutFile ${env:tmp}\wazuh-agent.msi; msixec.exe /i ${env:tmp}\wazuh-agent.msi /q
WAZUH_MANAGER='wazuh-serveur.crous-nantes.fr' WAZUH_AGENT_NAME="${env:COMPUTERNAME}" WAZUH_REGISTRATION_SERVER='wazuh-serveur.crous-nantes.fr' -Wait
NET START WazuhSvc
```

Linux

```
#!/bin/bash
bash /usr/local/bin/no-iptables.sh
apt-get update
apt-get install curl gpg
curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | gpg --no-default-keyring --keyring gnupg-ring:/usr/share/keyrings/wazuh.gpg --import && chmod 644
/usr/share/keyrings/wazuh.gpg
echo "deb [signed-by=/usr/share/keyrings/wazuh.gpg] https://packages.wazuh.com/4.x/apt/ stable main" | tee -a /etc/apt/sources.list.d/wazuh.list
apt-get update
WAZUH_MANAGER="wazuh-serveur.crous-nantes.fr" apt-get install wazuh-agent
echo "$IPTABLES -A OUTPUT -p TCP --match multiport --dports 1514,1515 -j ACCEPT" >> /usr/local/bin/iptables.rules
bash /usr/local/bin/iptables.sh
systemctl daemon-reload
systemctl enable wazuh-agent
systemctl start wazuh-agent
```

Ports à ouvrir

Wazuh-Dashboard

```
## INBOUND
$IPTABLES -A INPUT -p TCP --dport 443 -j ACCEPT #HTTPS

## OUTBOUND
$IPTABLES -A OUTPUT -p TCP --dport 443 -j ACCEPT # HTTPS
$IPTABLES -A OUTPUT -p TCP --dport 9200 -d 192.168.11.2 -j ACCEPT #Communication avec Indexer
$IPTABLES -A OUTPUT -p TCP --dport 1515 -d wazuh-serveur.crous-nantes.fr -j ACCEPT #Communication avec Server
$IPTABLES -A OUTPUT -p TCP --dport 55000 -d wazuh-serveur.crous-nantes.fr -j ACCEPT #API de Server
```

Wazuh-Indexer

```
## INBOUND
$IPTABLES -A INPUT -p TCP --dport 9200 -j ACCEPT

## OUTBOUND
$IPTABLES -A OUTPUT -p TCP --dport 9200 -j ACCEPT
```

Wazuh-Server

```
## INBOUND
$IPTABLES -A INPUT -p TCP --dport 55000 -j ACCEPT
$IPTABLES -A INPUT -p TCP --dport 1514 -j ACCEPT
$IPTABLES -A INPUT -p TCP --dport 1515 -j ACCEPT
$IPTABLES -A INPUT -p TCP --dport 1516 -j ACCEPT
```

Wazuh-Agent

```
## OUTBOUND
$IPTABLES -A OUTPUT -p TCP --match multiport --dports 1514,1515 -j ACCEPT
```

Changement mot de passe administrateur

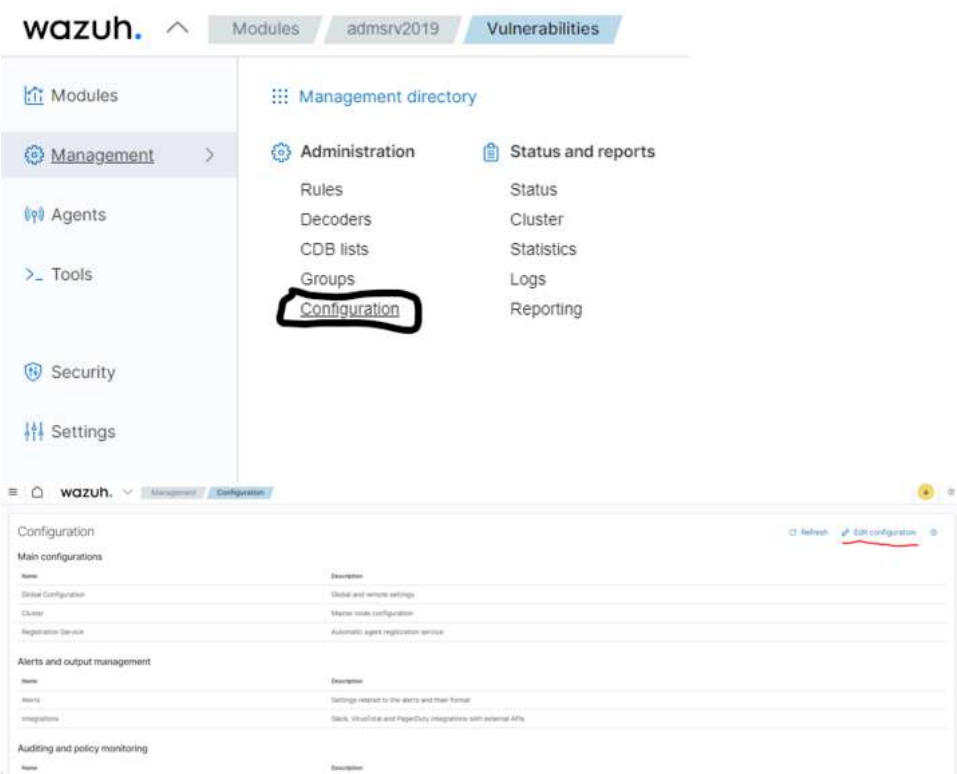
Sur Wazuh-Indexer :

```
cd /usr/share/wazuh-indexer/plugins/opensearch-security/tools/
bash wazuh-passwords-tool.sh -u admin -p <Mot-De-Passe>
```

Puis redémarrer Filebeat et Wazuh-manager sur Wazuh-Server et redémarrer Wazuh-Dashboard.

Configuration

Activation du scan des vulnérabilités sur les hôtes



Chercher la ligne ci-dessous, et passer la directive "enabled" à "yes".

```
<vulnerability-detector>
<enabled>yes</enabled>
<interval>5m</interval>
<min_full_scan_interval>6h</min_full_scan_interval>
<run_on_start>yes</run_on_start>
```

Activation de l'active response

Même endroit.

Suivre la syntaxe suivante pour ajouter une réponse active.

Active response - Capabilities · Wazuh documentation (<https://documentation.wazuh.com/current/user-manual/capabilities/active-response/index.html>)

```
<active-response>
  active-response options her
</active-response>
```

Déplacement du dossier logs sur wazuh-server

Ajout d'un disque de 100Go avec GPartEd puis montage de la partition sur sdb1 --> /stock_ext dans fstab : #echo "/dev/sdb1 /stock_ext xfs defaults, o o" >> /etc/fstab

J'avais créé un lien symbolique entre /var/ossec/logs/alerts et /stock_ext/alerts mais cela ne fonctionnait pas

Déplacement des fichiers : `mv -Rf /var/ossec/logs/* /stock_ext/logs/`

Donc j'ai monté un lien direct dans fstab entre /stock_ext/logs et /var/ossec/logs --> `#echo "/stock_ext/logs /var/ossec/logs/ none defaults,bind o o" >> /etc/fstab`

=> Problème avec centreon donc dans fstab:

`/dev/sdb1 /var/ossec/logs xfs defaults, o o`

=> Montage du disque directement à l'endroit où wazuh écrit les logs.

Récupérée de « https://wiki.crous-nantes.fr/index.php?title=Wazuh_-_Journal_De_Bord&oldid=45905 »

La dernière modification de cette page a été faite le 11 mars 2024 à 15:21.