

Ansinnelli Yohann - Ralite Justin - Mathéo Balazuc

WAZUH Déploiement

I/ Wazuh Indexer

Pour installer le serveur Wazuh, on va dans un premier temps faire l'installation du wazuh indexer, il existe deux méthodes pour l'installer, soit faire l'installation step by step ou sinon faire l'installation à l'aide d'assistant. Dans notre cas on fera l'installation avec l'assistant pour une installation plus rapide :

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

Configuration du fichier ./config.yml

```
nodes:
# Wazuh indexer nodes
indexer:
  - name: index_wazuh
    ip: "10.202.0.66"
  #- 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: "10.202.0.66"
  # 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: "10.202.0.66"
```

On lance l'assistant générer les clés de répartition :

```
root@WAZUH:/home/test# bash wazuh-install.sh --generate-config-files -i
29/11/2023 09:51:18 INFO: Starting Wazuh installation assistant. Wazuh version: 4.7.0
29/11/2023 09:51:18 INFO: Verbose logging redirected to /var/log/wazuh-install.log
29/11/2023 09:51:22 WARNING: Hardware and system checks ignored.
29/11/2023 09:51:22 INFO: --- Configuration files ---
29/11/2023 09:51:22 INFO: Generating configuration files.
29/11/2023 09:51:23 INFO: Created wazuh-install-files.tar. It contains the Wazuh cluster key, certificates, and passwords necessary for installation.
```

Téléchargement de l'assistant Wazuh :

```
curl -sO https://packages.wazuh.com/4.7/wazuh-install.sh
```

On lance l'assistant cette fois-ci pour installer l'indexer :

```
bash wazuh-install.sh --wazuh-indexer node-1
```

```
root@WAZUH:/home/test# bash wazuh-install.sh --wazuh-indexer index_waz -i
29/11/2023 10:12:03 INFO: Starting Wazuh installation assistant. Wazuh version: 4.7.0
29/11/2023 10:12:03 INFO: Verbose logging redirected to /var/log/wazuh-install.log
29/11/2023 10:12:08 WARNING: Hardware and system checks ignored.
29/11/2023 10:12:11 INFO: Wazuh repository added.
29/11/2023 10:12:12 INFO: --- Wazuh indexer ---
29/11/2023 10:12:12 INFO: Starting Wazuh indexer installation.
29/11/2023 10:13:47 INFO: Wazuh indexer installation finished.
29/11/2023 10:13:47 INFO: Wazuh indexer post-install configuration finished.
29/11/2023 10:13:47 INFO: Starting service wazuh-indexer.
29/11/2023 10:13:59 INFO: wazuh-indexer service started.
29/11/2023 10:13:59 INFO: Initializing Wazuh indexer cluster security settings.
29/11/2023 10:14:00 INFO: Wazuh indexer cluster initialized.
29/11/2023 10:14:00 INFO: Installation finished.
```

La dernière étape consiste à lancer le script de sécurité admin.

```
root@WAZUH:/home/test# bash wazuh-install.sh --start-cluster -i
29/11/2023 10:15:15 INFO: Starting Wazuh installation assistant. Wazuh version: 4.7.0
29/11/2023 10:15:15 INFO: Verbose logging redirected to /var/log/wazuh-install.log
29/11/2023 10:15:19 WARNING: Hardware and system checks ignored.
29/11/2023 10:15:28 INFO: Wazuh indexer cluster security configuration initialized.
29/11/2023 10:16:00 INFO: Wazuh indexer cluster started.
```

Obtentions des informations admin :

```
root@WAZUH:/home/test# tar -axf wazuh-install-files.tar wazuh-install-files/wazuh-passwords.txt -O | grep -P '\admin\' -A 1
indexer_username: 'admin'
indexer_password: '7WLeK92Q54In8?Vz0pP0420*a5R?*abQ'
```

On regarde si l'installation est un succès :

```
root@WAZUH:/home/test# curl -k -u admin:7WLeK92Q54In8?Vz0pP0420*a5R?*abQ https://10.202.0.66:9200
{
  "name" : "index_waz",
  "cluster_name" : "wazuh-indexer-cluster",
  "cluster_uuid" : "SEvXtZ-0Q40okXo88WK5KQ",
  "version" : {
    "number" : "7.10.2",
    "build_type" : "rpm",
    "build_hash" : "db90a415ff2fd428b4f7b3f800a51dc229287cb4",
    "build_date" : "2023-06-03T06:24:25.112415503Z",
    "build_snapshot" : false,
    "lucene_version" : "9.6.0",
    "minimum_wire_compatibility_version" : "7.10.0",
    "minimum_index_compatibility_version" : "7.0.0"
  },
  "tagline" : "The OpenSearch Project: https://opensearch.org/"
}
```

II/ Wazuh Server

Pour faire l'installation du serveur on va dans un premier temps télécharger l'assistant puis ensuite le lancer avec les deux commandes suivantes :

```
curl -sO https://packages.wazuh.com/4.7/wazuh-install.sh
bash wazuh-install.sh --wazuh-server wazuh-1
```

```
root@WAZUH:/home/test# bash wazuh-install.sh --wazuh-server wazuh-1 -i
29/11/2023 10:25:21 INFO: Starting Wazuh installation assistant. Wazuh version: 4.7.0
29/11/2023 10:25:21 INFO: Verbose logging redirected to /var/log/wazuh-install.log
29/11/2023 10:25:34 WARNING: Hardware and system checks ignored.
29/11/2023 10:25:46 INFO: Wazuh repository added.
29/11/2023 10:25:46 INFO: --- Wazuh server ---
29/11/2023 10:25:46 INFO: Starting the Wazuh manager installation.
29/11/2023 10:26:51 INFO: Wazuh manager installation finished.
29/11/2023 10:26:51 INFO: Starting service wazuh-manager.
29/11/2023 10:27:07 INFO: wazuh-manager service started.
29/11/2023 10:27:07 INFO: Starting Filebeat installation.
29/11/2023 10:27:15 INFO: Filebeat installation finished.
29/11/2023 10:27:15 INFO: Filebeat post-install configuration finished.
29/11/2023 10:27:20 INFO: Starting service filebeat.
29/11/2023 10:27:21 INFO: filebeat service started.
29/11/2023 10:27:21 INFO: Installation finished.
```

III/ Wazuh Dashboard

De même que le serveur, on va venir télécharger l'assistant puis le lancer :

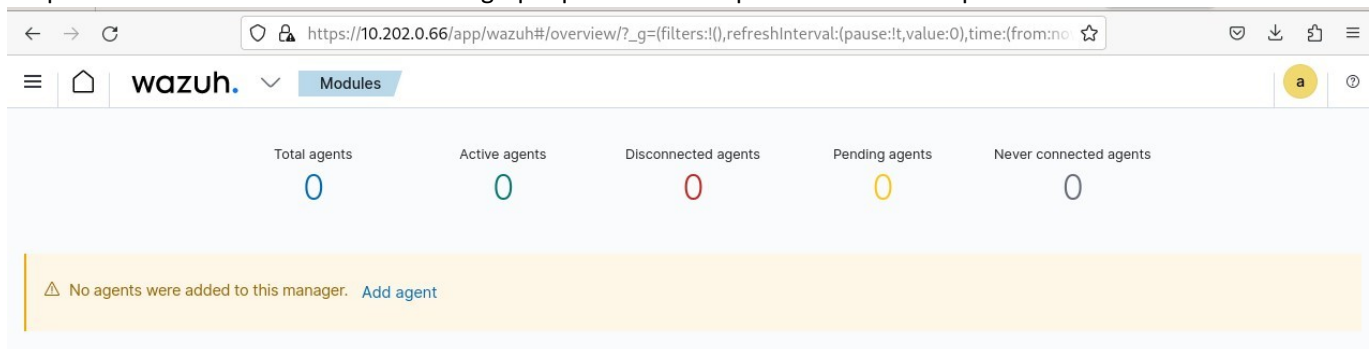
```
curl -sO https://packages.wazuh.com/4.7/wazuh-install.sh
bash wazuh-install.sh --wazuh-dashboard dashboard
```

```

root@WAZUH:/home/test# bash wazuh-install.sh --wazuh-dashboard dashboard -i
29/11/2023 10:30:53 INFO: Starting Wazuh installation assistant. Wazuh version: 4.7.0
29/11/2023 10:30:53 INFO: Verbose logging redirected to /var/log/wazuh-install.log
29/11/2023 10:30:59 WARNING: Hardware and system checks ignored.
29/11/2023 10:30:59 INFO: Wazuh web interface port will be 443.
29/11/2023 10:31:01 INFO: Wazuh repository added.
29/11/2023 10:31:01 INFO: --- Wazuh dashboard ----
29/11/2023 10:31:01 INFO: Starting Wazuh dashboard installation.
29/11/2023 10:33:05 INFO: Wazuh dashboard installation finished.
29/11/2023 10:33:05 INFO: Wazuh dashboard post-install configuration finished.
29/11/2023 10:33:05 INFO: Starting service wazuh-dashboard.
29/11/2023 10:33:06 INFO: wazuh-dashboard service started.
29/11/2023 10:33:19 INFO: Initializing Wazuh dashboard web application.
29/11/2023 10:33:20 INFO: Wazuh dashboard web application initialized.
29/11/2023 10:33:20 INFO: --- Summary ---
29/11/2023 10:33:20 INFO: You can access the web interface https://10.202.0.66:443
    User: admin
    Password: 7WLek92Q54In8?Vz0pP0420*a5R?*abQ
29/11/2023 10:33:20 INFO: Installation finished.

```

On peut maintenant accéder à l'interface graphique à l'adresse ip 10.202.0.66 et au port 443 :



IV/ Wazuh Agent

Une fois sur l'interface graphique on va pouvoir venir installer les agents, pour cela ils existent deux méthodes :

1. Déploiement Manuel

La première méthode va consister à déployer les agents manuellement. On va dans un premier temps venir installer la clé 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

```

Une fois la clé gpg d'installé on va venir déployer l'agent avec les commandes suivantes :

```
WAZUH_MANAGER="10.202.0.66" apt-get install wazuh-agent
```

On lance l'agent wazuh :

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

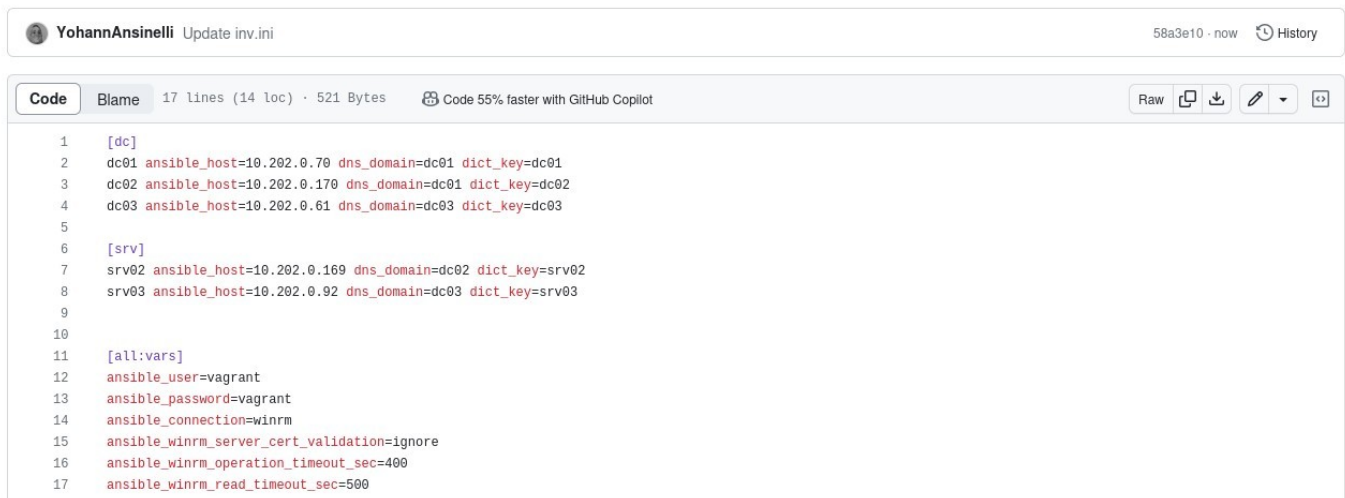
ATTENTION, wazuh recommande de désactiver les mises à jours pour garantir la compatibilité entre le serveur et les agents. Pour désactiver les mises à jours on exécute la commande suivantes :

```
sed -i "s/^deb/#deb/" /etc/apt/sources.list.d/wazuh.list
```

L'agent vient d'être déployé manuellement !

2. Déploiement Automatique

Pour le déploiement automatique des agents wazuh on va pouvoir utiliser **Ansible**. Dans un premier temps on va venir stocker les adresses des machines du GOAD dans un fichier inventaire :



The screenshot shows a GitHub web interface for a repository named 'YohannAnsinelli' with the file 'Update inv.ini'. The file content is an Ansible inventory file with the following structure:

```
1 [dc]
2 dc01 ansible_host=10.202.0.70 dns_domain=dc01 dict_key=dc01
3 dc02 ansible_host=10.202.0.170 dns_domain=dc01 dict_key=dc02
4 dc03 ansible_host=10.202.0.61 dns_domain=dc03 dict_key=dc03
5
6 [srv]
7 srv02 ansible_host=10.202.0.169 dns_domain=dc02 dict_key=srv02
8 srv03 ansible_host=10.202.0.92 dns_domain=dc03 dict_key=srv03
9
10
11 [all:vars]
12 ansible_user=vagrant
13 ansible_password=vagrant
14 ansible_connection=winrm
15 ansible_winrm_server_cert_validation=ignore
16 ansible_winrm_operation_timeout_sec=400
17 ansible_winrm_read_timeout_sec=500
```

Ensuite on va venir faire le script ansible suivant :

RaliteJ Add files via upload9b7c39c · last weekHistory

CodeBlame22 lines (20 loc) · 693 BytesCode 55% faster with GitHub Copilot

RawDownloadEdit

```
1  ---
2  - name: "Installation des Wazuh agents on SRV"
3    hosts: srv, dc
4    gather_facts: false
5    tasks:
6      - name: "Download Wazuh Agent"
7        win_shell: |
8          Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.7.0-1.msi -OutFile ${env:tmp}\wazuh-agent
9          args:
10             executable: powershell.exe
11
12      - name: "Configuration"
13        win_shell: |
14          msixec.exe /i ${env:tmp}\wazuh-agent /q WAZUH_MANAGER='10.202.0.66' WAZUH_AGENT_GROUP='default' WAZUH_REGISTRATION_SERVER='10.202.0.66'
15          args:
16             executable: powershell.exe
17
18      - name: "Lancement de l'agent"
19        win_shell: |
20          NET START WazuhSvc
21          args:
22             executable: powershell.exe
```

Ce script automatise le processus d'installation de l'agent Wazuh sur des machines Windows spécifiques. Il télécharge l'agent, le configure avec des paramètres spécifiques comme l'adresse IP du serveur Wazuh, puis démarre le service de l'agent.

On obtient l'ensemble des agents déployés :

← → ↺https://10.202.0.66/app/wazuh#/agents-preview/?_g=(filters:(),refreshInterval:(pause:!t,value:0),time:(fr)☆

≡🏠wazuh. ▾Agentsa ⓘ

STATUS

- Active (5)
- Disconnected (0)
- Pending (0)
- Never connected (0)

DETAILS

Active5Disconnected0Pending0Never connected0Agents coverage100.00%

Last registered agentkingslanding

Most active agentwinterfell

EVOLUTION

Last 24 hours ▾

No results found

Agents (5)

⊕ Deploy new agent ↺ Refresh 📄 Export formatted ⚙️

🔍 id!=000 and status=activeWQLRefresh

ID ↑	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
001	castelblack	10.202.0.176	default	Microsoft Windows Server 2019 Datacenter Evaluation 10.0.17763.5122	node01	v4.7.0	● active ⓘ	👁️🔗
002	braavos	10.202.0.169	default	Microsoft Windows Server 2016 Standard Evaluation 10.0.14393.2791	node01	v4.7.0	● active ⓘ	👁️🔗
003	winterfell	10.202.0.150	default	Microsoft Windows Server 2019 Datacenter Evaluation 10.0.17763.1935	node01	v4.7.0	● active ⓘ	👁️🔗
004	meereen	10.202.0.137	default	Microsoft Windows Server 2016 Standard Evaluation 10.0.14393.1944	node01	v4.7.0	● active ⓘ	👁️🔗
005	kingslanding	10.202.0.56	default	Microsoft Windows Server 2019 Datacenter Evaluation 10.0.17763.1935	node01	v4.7.0	● active ⓘ	👁️🔗

V/ Sysmon

Pour implémenter sysmon dans wazuh il faudra préalablement installer sysmon sur les machines du GOAD et ensuite on va devoir du côté des agents modifier le fichier "ossec.conf" pour y ajouter :

```
<localfile>
<location>Microsoft-Windows-Sysmon/Operational</location>
<log_format>eventchannel</log_format>
</localfile>
```

6 / 7

Et côté serveur je vais venir modifier le fichier "local_rules.xml" dans le chemin /var/ossec/etc/rules pour y ajouter ceci :

```
<group name="sysmon,">
  <rule id="255000" level="12">
    <if_group>sysmon_event1</if_group>
    <field name="sysmon.image">\\powershell.exe||\\.ps1||\\.ps2</field>
    <description>Sysmon - Event 1: Bad exe: $(sysmon.image)</description>
    <group>sysmon_event1,powershell_execution,</group>
  </rule>
</group>
```

ATTENTION il ne faut pas oublier de redémarrer l'agent et le dashboard pour que les changements soient pris en compte. Voilà notre wazuh peut récupérer les logs sysmon.