

Création de règles personnalisées

Dans ce guide, l'agent **Wazuh** est configuré pour collecter des journaux et des événements contenant des informations spécifiques sur les points de terminaison surveillés. Il est possible de créer un ensemble de règles personnalisé pour extraire les informations pertinentes des journaux collectés.

I - Configuration du Serveur Wazuh

1. **Activation des Archives Wazuh** : On modifie le fichier de configuration `/var/ossec/etc/ossec.conf` en définissant la valeur de `<logall>` et `<logall_json>` à **yes** dans le bloc `<global>` pour activer les archives Wazuh.

```
<logall>yes</logall>
<logall_json>yes</logall_json>
```

2. **Redémarrage du Gestionnaire Wazuh** : On redémarre le gestionnaire **Wazuh** pour appliquer les modifications de configuration :

```
systemctl restart wazuh-manager
```

II - Configuration du point de terminaison Linux

1. **Ajout de la Configuration du Module de Commande** : On ajoute la configuration du module de commande dans le fichier `/var/ossec/etc/ossec.conf` :

```
<wodle name="command">
  <disabled>no</disabled>
  <tag>unused_memory</tag>
  <command>grep MemFree /proc/meminfo</command>
  <interval>5m</interval>
  <ignore_output>no</ignore_output>
  <run_on_start>yes</run_on_start>
  <timeout>0</timeout>
</wodle>
```

2. **Redémarrage de l'Agent Wazuh** : On redémarre l'agent **Wazuh** pour appliquer les modifications de configuration :

```
systemctl restart wazuh-agent
```

III – Traitement des Journaux

1. **Vérification des Journaux Reçus** : On exécute la commande suivante pour obtenir le journal reçu du point de terminaison **Linux** surveillé :

```
grep "unused_memory" /var/ossec/logs/archives/archives.json
```

Résultat attendu :

```
{ "timestamp": "2023-07-26T09:06:08.947+0000", "agent": { "id": "002", "name": "Ubuntu-22-LTS", "ip": "10.0.2.15" }, "manager": { "name": "wazuh-server", "id": "1690362368.662599", "full_log": "MemFree: 90008 kB", "decoder": {}, "location": "command_unused_memory" }
```

2. **Décodage des Journaux** : On utilise le programme **wazuh-logtest** pour décoder les journaux et vérifier les informations extraites :

```
/var/ossec/bin/wazuh-logtest
```

Résultat attendu :

```
#!/var/ossec/bin/wazuh-logtest
Starting wazuh-logtest v4.7.3
Type one log per line
MemFree:      90008 kB
**Phase 1: Completed pre-decoding.
    full event: 'MemFree:      90008 kB'
**Phase 2: Completed decoding.
    No decoder matched.
```

Remarque : Aucun décodeur n'est disponible pour décoder le journal comme indiqué. On crée un décodeur pour extraire les informations du journal.

3. Création d'un Décodeur Personnalisé : On ajoute le décodeur personnalisé dans le fichier `/var/ossec/etc/decoders/local_decoder.xml` pour extraire les informations du journal :

```
<decoder name="unused-memory">
  <prematch>^MemFree: </prematch>
  <regex offset="after_prematch">\t*(\S+)\s(\S+)</regex>
  <order>free_memory, unit_of_measurment</order>
</decoder>
```

Étape 4: Création de Règles Personnalisées :

1. Ajout de Règles Personnalisées : On ajoute une règle personnalisée dans le fichier `/var/ossec/etc/rules/local_rules.xml` pour générer une alerte lorsque le module de commande exécute la commande :

```
<group name="unused_memory">
  <rule id="100003" level="5">
    <decoded_as>unused-memory</decoded_as>
    <description>The system's free memory is $(free_memory) $(unit_of_measurment).</description>
  </rule>
</group>
```

2. Redémarrage du Gestionnaire Wazuh : On redémarre le gestionnaire **Wazuh** pour appliquer les modifications de configuration :

```
systemctl restart wazuh-manager
```

V - Visualisation des Alertes

1. Vérification des Alertes Générées : On exécute la commande suivante pour voir l'alerte **JSON** générée lorsque le module de commande exécute la commande :

```
grep "unused_memory" /var/ossec/logs/alerts/alerts.json | /var/ossec/framework/python/bin/python3 -mjson.tool
```

2. Accès au Tableau de Bord Wazuh : On accède au tableau de bord **Wazuh**, on sélectionne le point de terminaison Linux surveillé, puis on se rend à l'onglet « **Security Events** » pour afficher les alertes générées.

```
> 26 mars 2024 à 15:48:09.848 La mémoire libre du système est de 68 904 Ko. 5 100003
```