Utilisation de l'espace disque

L'utilisation de l'espace disque est cruciale pour garantir des performances optimales et éviter les pannes système. Avec **Wazuh**, on peut surveiller l'espace disque sur les systèmes Windows et Linux pour s'assurer que les partitions ne dépassent pas les limites définies.

Voici comment procéder :

I - Surveiller l'espace disque sur le point de terminaison Windows

1. Configuration du point de terminaison Windows :

- Pour activer l'exécution de commandes à distance, on ajoute les paramètres suivants au fichier **C:\Program Files (x86)\ossec-agent\local_internal_options.conf** :

```
logcollector.remote_commands=1
```

- Ensuite, on redémarre l'agent **Wazuh** pour appliquer les modifications (**PowerShell** ou **Gestionnaire des Tâches**) :

```
Restart-Service -Name WazuhSvc
```

2. Configuration du Serveur Wazuh :

- On ajoute la configuration suivante au fichier **/var/ossec/etc/shared/default/agent.conf** sur le serveur **Wazuh** :

```
<agent_config os="Windows">
    <localfile>
        <log_format>command</log_format>
        <command>Powershell -c "Get-Volume -DriveLetter C | Select-Object -Property @{ 'Name' = '% Free';
Expression = {'{0:P}' -f ($_.SizeRemaining / $_.Size) }}"</command>
        <alias>check_win_disk_space</alias>
    </localfile>
</agent_config>
```

- Ensuite, on ajoute les règles spécifiques au fichier **/var/ossec/etc/rules/local_rules.xml** :

```
<group name="disk_space_utilization">
  <rule id="100014" level="7">
    <if_sid>530</if_sid>
    <match>^ossec: output: 'check_win_disk_space': </match>
    <regex type="pcre2">[0-1]\d.\d+%$</regex>
    <description>C: Drive free space less than 20%.</description>
  </rule>
</group>
```

- Enfin, on redémarre le gestionnaire **Wazuh** pour appliquer les modifications :

```
sudo systemctl restart wazuh-manager
```

3. Visualisation des alertes :

- Pour visualiser l'alerte générée lorsque l'espace disque libre est inférieur à 20%, on accède à l'onglet « **Modules** » > « **Security Events** » sur le tableau de bord **Wazuh**.

Utilisation de l'espace disque

II - Surveiller l'espace disque sur le point de terminaison Linux

1. Configuration du point de terminaison Linux :

- Pour activer l'exécution de commandes à distance, on ajoute les paramètres suivants au fichier **/var/ossec/etc/local_internal_options.conf** :

```
wazuh_command.remote_commands=1
```

- Ensuite, on redémarre l'agent **Wazuh** pour appliquer les modifications :

```
sudo systemctl restart wazuh-agent
```

2. Configuration du Serveur Wazuh :

- On crée un script bash nommé **disk-usage.sh** dans le répertoire **/var/ossec/etc/shared/default** sur le serveur **Wazuh** avec le contenu suivant :

```
#!/bin/bash
df -h | while IFS= read -r line;
do
  echo "disk-usage: "$line
done
```

- Ensuite, on ajoute la configuration suivante au fichier **/var/ossec/etc/shared/default/agent.conf** sur le serveur **Wazuh** :

```
<agent_config os="Linux">
  <wodle name="command">
    <disabled>no</disabled>
    <tag>disk-usage</tag>
    <command>/bin/bash /var/ossec/etc/shared/disk-usage.sh</command>
    <interval>2m</interval>
    <run_on_start>yes</run_on_start>
    <timeout>10</timeout>
    <verify_md5><MD5_HASH></verify_md5>
    <verify_sha1><SHA1_HASH></verify_sha1>
    <verify_sha256><SHA256_HASH></verify_sha256>
  </wodle>
</agent_config>
```

On remplace **<MD5_HASH>**, **<SHA1_HASH>** et **<SHA256_HASH>** par les hachages appropriés du binaire **/bin/bash** sur les points de terminaison Linux.

Le bloc ci-contre est à répéter autant de fois qu'il y a de points de terminaison Linux.

Commandes pour avoir le hache de /bin/bash :

```
md5sum /bin/bash
md5sum /bin/bash
md5sum /bin/bash
```

- On ajoute également le décodeur au fichier **/var/ossec/etc/decoders/local_decoder.xml** :

```
<decoder name="disk-usage">
  <prematch>^disk-usage: </prematch>
  <regex offset="after_prematch">(\S+)\s*(\S+)\s*(\S+)\s*(\S+)\s*(\S+)%\s*(\S+)</regex>
  <order>filesystem, size, used, available, usage, mnt</order>
</decoder>
```

- et les règles spécifiques fichiers **/var/ossec/etc/rules/local_rules.xml** :

```
<group name="disk_space_utilization,">
  <rule id="100015" level="7">
    <decoded_as>disk-usage</decoded_as>
    <field name="filesystem">^/dev/</field>
    <field name="usage">^9\d|^8\d</field>
    <description>Usage $(usage)% of $(filesystem) partition exceeded 80%.</description>
  </rule>
</group>
```

3. Redémarrage du Gestionnaire Wazuh :

- Enfin, on redémarre le gestionnaire **Wazuh** pour appliquer les modifications :

```
sudo systemctl restart wazuh-manager
```