Wazuh Agent installieren auf Proxmox (PVE, PBS und evtl. PMR)

Die aktuellen Proxmox Versionen nutzen Debian 12 (Stand 04/2024). Diese sollten normalerweise unterstützt werden - jedoch lassen sie diese nicht so einfach installieren, bzw. in Betrieb nehmen.

Ich hatte beispielsweise das Problem, das sich der Agent zwar installieren aber nicht starten ließ (z.B. fehlte der User Wazuh, was man in der /etc/passwd sehen konnte - aber es fehlen auch noch andere Dinge, die Wazuh benötigt.

Sollte eine zuvor versuchte Installation noch vorhanden sein, dann diese wieder entfernen:

```
apt remove --purge wazuh-agent
```

Danach müssen wir dann den Client erst mal runterladen (aktuelle Übersicht der Downloadadressen findet ihr hier: https://documentation.wazuh.com/current/installation-guide/packages-list.html - hier könnt ihr mit der rechten Maustaste auf den Link gehen und dann die Adresse kopieren), z.B.

```
 wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.7.3-1_amd64.deb
```

Anschließend dann die Vorraussetzungen erfüllen und folgende Komponenten laden:

```
apt install lsb-base lsb-release
```

Danach dann die benötigen Variablen laden, die der Agent bei der Installation verwendet (bitte verwendet natürlich eure eigenen Daten:

```
WAZUH_MANAGER='192.168.1.1'
WAZUH_AGENT_GROUP='default,LINUX,SERVER,PROXMOX'
```

Danach könnt ihr dann auch schon den Agent installieren mit:

```
dpkg -i wazuh-agent_4.7.3-1_amd64.deb
```

Anschließend den Dienst registrieren und starten:

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

Sollte der Start einen Fehler ausgeben, dann könnt ihr den wie folgt kontrollieren:

```
systemctl status wazuh-agent
```

Sollte dort angegeben werden, das der Manager nicht gefunden wurde, dann hat das Setup die Daten die variablen nicht richtig übernommen, kontrolliert bitte ob in der Daten /var/ossec/etc/ossec.conf die Adresse verwendet wird und nicht der Name MANAGER_IP - ihr könnt auch direkt die Gruppen und das Debian Profil kontrollieren - es sollte ungefähr so aussehen:

```
<ossec_config>
  <client>
    <server>
      <address>192.168.1.1</address>
      <port>1514</port>
      <protocol>tcp</protocol>
    </server>
    <config-profile>debian, debian12</config-profile>
    <notify_time>10</notify_time>
    <time-reconnect>60</time-reconnect>
    <auto_restart>yes</auto_restart>
    <crypto_method>aes</crypto_method>
    <enrollment>
      <enabled>yes</enabled>
      <groups>default,PROXMOX,LINUX,SERVERS</groups>
      <authorization_pass_path>etc/authd.pass</authorization_pass_path>
    </enrollment>
  </client>
```

Wenn ihr dies geändert habt, dann könnt ihr wieder den Agent erneut starten und kontrollieren ob er gestartet wurde:

```
systemctl start wazuh-agent
systemctl status wazuh-agent
```

Der Agent sollte nun nach kurzer Zeit in eurer Wazuh Agent Übersicht auftauchen.

Noch ein wenig schneller geht es, wenn ihr den Teil mit den Variablen laden überspringt - während das bei fast allen Linux Systemen funktioniert, scheint es bei den Proxmox Systemen nicht zu funktionieren) und auch bevor ihr den Dienst registriert/startetn schon vorher die ossec.conf kontrolliert und ggf. anpasst. So sollte dann jeder Agent in ca. 3 Minuten installiert sein.

Revision #3
Created 2024-04-14 11:32:25 UTC by Peter Leibling
Updated 2024-04-14 12:05:50 UTC by Peter Leibling