<!--

Wazuh - Manager - Default configuration for debian 11

More info at: https://documentation.wazuh.com

Mailing list: https://groups.google.com/forum/#!forum/wazuh

-->

<ossec\_config>

<global>

<jsonout\_output>yes</jsonout\_output>

<alerts\_log>yes</alerts\_log>

<logall>no</logall>

<logall\_json>no</logall\_json>

<email\_notification>no</email\_notification>

<smtp\_server>smtp.example.wazuh.com</smtp\_server>

<email\_from>wazuh@example.wazuh.com</email\_from>

<email\_to>recipient@example.wazuh.com</email\_to>

<email\_maxperhour>12</email\_maxperhour>

<email\_log\_source>alerts.log</email\_log\_source>

<agents\_disconnection\_time>10m</agents\_disconnection\_time>

<agents\_disconnection\_alert\_time>0</agents\_disconnection\_alert\_time>

</global>

<alerts>

<log\_alert\_level>3</log\_alert\_level>

<email\_alert\_level>12</email\_alert\_level>

</alerts>

<!-- Choose between "plain", "json", or "plain,json" for the format of internal logs -->

<logging>

<log\_format>plain</log\_format>

</logging>

<remote>

<connection>secure</connection>

<port>1514</port>

<protocol>tcp</protocol>

<queue\_size>131072</queue\_size>

</remote>

<!-- Policy monitoring -->

<rootcheck>

<disabled>no</disabled>

<check\_files>yes</check\_files>

<check\_trojans>yes</check\_trojans>

<check\_dev>yes</check\_dev>

<check\_sys>yes</check\_sys>

<check\_pids>yes</check\_pids>

<check\_ports>yes</check\_ports>

<check\_if>yes</check\_if>

<!-- Frequency that rootcheck is executed - every 12 hours -->

<frequency>43200</frequency>

<rootkit\_files>etc/rootcheck/rootkit\_files.txt</rootkit\_files>

<rootkit\_trojans>etc/rootcheck/rootkit\_trojans.txt</rootkit\_trojans>

<skip\_nfs>yes</skip\_nfs>

</rootcheck>

<wodle name="cis-cat">

<disabled>yes</disabled>

<timeout>1800</timeout>

<interval>1d</interval>

<scan-on-start>yes</scan-on-start>

<java\_path>wodles/java</java\_path>

<ciscat\_path>wodles/ciscat</ciscat\_path>

</wodle>

<!-- Osquery integration -->

<wodle name="osquery">

<disabled>yes</disabled>

<run\_daemon>yes</run\_daemon>

<log\_path>/var/log/osquery/osqueryd.results.log</log\_path>

<config\_path>/etc/osquery/osquery.conf</config\_path>

<add\_labels>yes</add\_labels>

</wodle>

<!-- System inventory -->

<wodle name="syscollector">

<disabled>no</disabled>

<interval>1h</interval>

<scan\_on\_start>yes</scan\_on\_start>

<hardware>yes</hardware>

<os>yes</os>

<network>yes</network>

<packages>yes</packages>

<ports all="no">yes</ports>

<processes>yes</processes>

<!-- Database synchronization settings -->

<synchronization>

<max\_eps>10</max\_eps>

</synchronization>

</wodle>

<sca>

<enabled>yes</enabled>

<scan\_on\_start>yes</scan\_on\_start>

<interval>12h</interval>

<skip\_nfs>yes</skip\_nfs>

</sca>

<vulnerability-detector>

<enabled>no</enabled>

<interval>5m</interval>

<min\_full\_scan\_interval>6h</min\_full\_scan\_interval>

<run\_on\_start>yes</run\_on\_start>

<!-- Ubuntu OS vulnerabilities -->

<provider name="canonical">

<enabled>no</enabled>

<os>trusty</os>

<os>xenial</os>

<os>bionic</os>

<os>focal</os>

<os>jammy</os>

<update\_interval>1h</update\_interval>

</provider>

<!-- Debian OS vulnerabilities -->

<provider name="debian">

<enabled>no</enabled>

<os>stretch</os>

<os>buster</os>

<os>bullseye</os>

<update\_interval>1h</update\_interval>

</provider>

<!-- RedHat OS vulnerabilities -->

<provider name="redhat">

<enabled>no</enabled>

<os>5</os>

<os>6</os>

<os>7</os>

<os>8</os>

<os>9</os>

<update\_interval>1h</update\_interval>

</provider>

<!-- Amazon Linux OS vulnerabilities -->

<provider name="alas">

<enabled>no</enabled>

<os>amazon-linux</os>

<os>amazon-linux-2</os>

<update\_interval>1h</update\_interval>

</provider>

<!-- Arch OS vulnerabilities -->

<provider name="arch">

<enabled>no</enabled>

<update\_interval>1h</update\_interval>

</provider>

<!-- Windows OS vulnerabilities -->

<provider name="msu">

<enabled>yes</enabled>

<update\_interval>1h</update\_interval>

</provider>

<!-- Aggregate vulnerabilities -->

<provider name="nvd">

<enabled>yes</enabled>

<update\_from\_year>2010</update\_from\_year>

<update\_interval>1h</update\_interval>

</provider>

</vulnerability-detector>

<!-- File integrity monitoring -->

<syscheck>

<disabled>no</disabled>

<!-- Frequency that syscheck is executed default every 12 hours -->

<frequency>43200</frequency>

<scan\_on\_start>yes</scan\_on\_start>

<!-- Generate alert when new file detected -->

<alert\_new\_files>yes</alert\_new\_files>

<!-- Don't ignore files that change more than 'frequency' times -->

<auto\_ignore frequency="10" timeframe="3600">no</auto\_ignore>

<!-- Directories to check (perform all possible verifications) -->

<directories>/etc,/usr/bin,/usr/sbin</directories>

<directories>/bin,/sbin,/boot</directories>

<!-- Files/directories to ignore -->

<ignore>/etc/mtab</ignore>

<ignore>/etc/hosts.deny</ignore>

<ignore>/etc/mail/statistics</ignore>

<ignore>/etc/random-seed</ignore>

<ignore>/etc/random.seed</ignore>

<ignore>/etc/adjtime</ignore>

<ignore>/etc/httpd/logs</ignore>

<ignore>/etc/utmpx</ignore>

<ignore>/etc/wtmpx</ignore>

<ignore>/etc/cups/certs</ignore>

<ignore>/etc/dumpdates</ignore>

<ignore>/etc/svc/volatile</ignore>

<!-- File types to ignore -->

<ignore type="sregex">.log$|.swp$</ignore>

<!-- Check the file, but never compute the diff -->

<nodiff>/etc/ssl/private.key</nodiff>

<skip\_nfs>yes</skip\_nfs>

<skip\_dev>yes</skip\_dev>

<skip\_proc>yes</skip\_proc>

<skip\_sys>yes</skip\_sys>

<!-- Nice value for Syscheck process -->

<process\_priority>10</process\_priority>

<!-- Maximum output throughput -->

<max\_eps>100</max\_eps>

<!-- Database synchronization settings -->

<synchronization>

<enabled>yes</enabled>

<interval>5m</interval>

<max\_interval>1h</max\_interval>

<max\_eps>10</max\_eps>

</synchronization>

</syscheck>

<!-- Active response -->

<global>

<white\_list>127.0.0.1</white\_list>

<white\_list>^localhost.localdomain$</white\_list>

<white\_list>37.17.118.136</white\_list>

<white\_list>37.17.118.152</white\_list>

</global>

<command>

<name>disable-account</name>

<executable>disable-account</executable>

<timeout\_allowed>yes</timeout\_allowed>

</command>

<command>

<name>restart-wazuh</name>

<executable>restart-wazuh</executable>

</command>

<command>

<name>firewall-drop</name>

<executable>firewall-drop</executable>

<timeout\_allowed>yes</timeout\_allowed>

</command>

<command>

<name>host-deny</name>

<executable>host-deny</executable>

<timeout\_allowed>yes</timeout\_allowed>

</command>

<command>

<name>route-null</name>

<executable>route-null</executable>

<timeout\_allowed>yes</timeout\_allowed>

</command>

<command>

<name>win\_route-null</name>

<executable>route-null.exe</executable>

<timeout\_allowed>yes</timeout\_allowed>

</command>

<command>

<name>netsh</name>

<executable>netsh.exe</executable>

<timeout\_allowed>yes</timeout\_allowed>

</command>

<!--

<active-response>

active-response options here

</active-response>

-->

<!-- Log analysis -->

<localfile>

<log\_format>syslog</log\_format>

<location>/var/ossec/logs/active-responses.log</location>

</localfile>

<localfile>

<log\_format>syslog</log\_format>

<location>/var/log/messages</location>

</localfile>

<localfile>

<log\_format>syslog</log\_format>

<location>/var/log/auth.log</location>

</localfile>

<localfile>

<log\_format>syslog</log\_format>

<location>/var/log/syslog</location>

</localfile>

<localfile>

<log\_format>syslog</log\_format>

<location>/var/log/dpkg.log</location>

</localfile>

<localfile>

<log\_format>syslog</log\_format>

<location>/var/log/kern.log</location>

</localfile>

<localfile>

<log\_format>command</log\_format>

<command>df -P</command>

<frequency>360</frequency>

</localfile>

<localfile>

<log\_format>full\_command</log\_format>

<command>netstat -tulpn | sed 's/\([[:alnum:]]\+\)\ \+[[:digit:]]\+\ \+[[:digit:]]\+\ \+\(.\*\):\([[:digit:]]\*\)\ \+\([0-9\.\:\\*]\+\).\+\ \([[:digit:]]\*\/[[:alnum:]\-]\*\).\*/\1 \2 == \3 == \4 \5/' | sort -k 4 -g | sed 's/ == \(.\*\) ==/:\1/' | sed 1,2d</command>

<alias>netstat listening ports</alias>

<frequency>360</frequency>

</localfile>

<localfile>

<log\_format>full\_command</log\_format>

<command>last -n 20</command>

<frequency>360</frequency>

</localfile>

<ruleset>

<!-- Default ruleset -->

<decoder\_dir>ruleset/decoders</decoder\_dir>

<rule\_dir>ruleset/rules</rule\_dir>

<rule\_exclude>0215-policy\_rules.xml</rule\_exclude>

<list>etc/lists/audit-keys</list>

<list>etc/lists/amazon/aws-eventnames</list>

<list>etc/lists/security-eventchannel</list>

<!-- User-defined ruleset -->

<decoder\_dir>etc/decoders</decoder\_dir>

<rule\_dir>etc/rules</rule\_dir>

</ruleset>

<rule\_test>

<enabled>yes</enabled>

<threads>1</threads>

<max\_sessions>64</max\_sessions>

<session\_timeout>15m</session\_timeout>

</rule\_test>

<!-- Configuration for wazuh-authd -->

<auth>

<disabled>no</disabled>

<port>1515</port>

<use\_source\_ip>no</use\_source\_ip>

<purge>yes</purge>

<use\_password>no</use\_password>

<ciphers>HIGH:!ADH:!EXP:!MD5:!RC4:!3DES:!CAMELLIA:@STRENGTH</ciphers>

<!-- <ssl\_agent\_ca></ssl\_agent\_ca> -->

<ssl\_verify\_host>no</ssl\_verify\_host>

<ssl\_manager\_cert>etc/sslmanager.cert</ssl\_manager\_cert>

<ssl\_manager\_key>etc/sslmanager.key</ssl\_manager\_key>

<ssl\_auto\_negotiate>no</ssl\_auto\_negotiate>

</auth>

<cluster>

<name>wazuh</name>

<node\_name>node01</node\_name>

<node\_type>master</node\_type>

<key></key>

<port>1516</port>

<bind\_addr>0.0.0.0</bind\_addr>

<nodes>

<node>NODE\_IP</node>

</nodes>

<hidden>no</hidden>

<disabled>yes</disabled>

</cluster>

<database\_output>

<hostname>127.0.0.1</hostname>

<username>MySQLadmin</username>

<password>Wazuhmysql123%.!</password>

<database>Alerts\_DB</database>

<type>mysql</type>

</database\_output>

</ossec\_config>