

due to time constraints, scripts in there have not been checked if they actually work

TLS

Server TLS Generation

```
cd /var/ossec/etc

# Create a root CA
openssl req -x509 -new -nodes -newkey rsa:4096 \
-keyout rootCA.key -out rootCA.pem -days 3650 \
-subj "/C=US/ST=WA/0=WazuhCA"

# Create server key and CSR
openssl req -new -nodes -newkey rsa:4096 \
-keyout server.key -out server.csr \
-subj "/C=US/ST=WA/0=WazuhServer"

# Sign server certificate with CA
openssl x509 -req -in server.csr -CA rootCA.pem -CAkey rootCA.key \
-CAcreateserial -out server.pem -days 3650
```

Configure Server

```
<remote>
  <connection>
    <secure>yes</secure>
    <port>1514</port>
    <protocol>tcp</protocol>
    <ssl>
      <ca>/var/ossec/etc/rootCA.pem</ca>
      <certificate>/var/ossec/etc/server.pem</certificate>
      <key>/var/ossec/etc/server.key</key>
    </ssl>
  </connection>
</remote>
```

Agent TLS Generation

```
# Agent key and CSR
openssl req -new -nodes -newkey rsa:4096 \
-keyout agent.key -out agent.csr \
-subj "/C=US/ST=WA/O=WazuhAgent/CN=Agent-Name"

# Sign agent cert
openssl x509 -req -in agent.csr -CA rootCA.pem -CAkey rootCA.key \
-CAcreateserial -out agent.pem -days 3650
```

Configure Agent

```
<client>
  <server>
    <address>WAZUH_SERVER_IP</address>
    <port>1514</port>
    <protocol>tcp</protocol>
    <ssl>
      <ca>/var/ossec/etc/rootCA.pem</ca>
      <certificate>/var/ossec/etc/agent.pem</certificate>
      <key>/var/ossec/etc/agent.key</key>
    </ssl>
  </server>
</client>
```