installation

Ossec is used
Ossec has an agent for the clients and a server that gets logs from the agents

Download from the following link
https://github.com/ossec/ossec-hids/archive/3.6.0.zip

Extract the contents to obtain the following files

```
:/opt/ossec/ossec-hids-3.6.0$ ls
active-response  CONFIG        doc      install.sh  src
BUGS             contrib       etc      LICENSE     SUPPORT.md
CHANGELOG.md     CONTRIBUTORS  INSTALL  README.md
```

Run the install script as root

```
:/opt/ossec/ossec-hids-3.6.0$ sudo ./install.sh

** Para instalação em português, escolha [br].
** 要使用中文进行安装，请选择 [cn].
** Fur eine deutsche Installation wohlen Sie [de].
** Για εγκατάσταση στα Ελληνικά, επιλέξτε [el].
** For installation in English, choose [en].
** Para instalar en Español , eliga [es].
** Pour une installation en français, choisissez [fr]
** A Magyar nyelvű telepítéshez válassza [hu].
** Per l'installazione in Italiano, scegli [it].
** 日本語でインストールします．選択して下さい．[jp].
** Voor installatie in het Nederlands, kies [nl].
** Aby instalować w języku Polskim, wybierz [pl].
** Для инструкций по установке на русском ,введите [ru].
** Za instalaciju na srpskom, izaberi [sr].
** Türkçe kurulum için seçin [tr].
(en/br/cn/de/el/es/fr/hu/it/jp/nl/pl/ru/sr/tr) [en]:


OSSEC HIDS v3.6.0 Installation Script - http://www.ossec.net

You are about to start the installation process of the OSSEC HIDS.
```

```
1- What kind of installation do you want (server, agent, local, hybrid or help)?
agent

  - Agent(client) installation chosen.
```

```
2- Setting up the installation environment.

 - Choose where to install the OSSEC HIDS [/var/ossec]:

    - Installation will be made at  /var/ossec .
```

```
3- Configuring the OSSEC HIDS.

  3.1- What's the IP Address or hostname of the OSSEC HIDS server?: 172.168.7.2

   - Adding Server IP 172.168.7.2

  3.2- Do you want to run the integrity check daemon? (y/n) [y]:

   - Running syscheck (integrity check daemon).

  3.3- Do you want to run the rootkit detection engine? (y/n) [y]:

   - Running rootcheck (rootkit detection).

  3.4 - Do you want to enable active response? (y/n) [y]:


  3.5- Setting the configuration to analyze the following logs:
    -- /var/log/auth.log
    -- /var/log/syslog
    -- /var/log/dpkg.log

 - If you want to monitor any other file, just change
   the ossec.conf and add a new localfile entry.
   Any questions about the configuration can be answered
   by visiting us online at http://www.ossec.net .


   --- Press ENTER to continue ---
```

```
root@        :/opt/ossec/ossec-hids-3.6.0# apt install libpcre2-dev zlib1g-dev
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  fonts-font-awesome geoipupdate libjs-bootstrap libjs-d3 libjs-jquery-form
  libjs-jquery-metadata libjs-jquery-tablesorter libjs-rickshaw libllvm9
  libndpi5
Use 'apt autoremove' to remove them.
The following additional packages will be installed:
  libpcre2-16-0 libpcre2-32-0 libpcre2-posix0
The following NEW packages will be installed:
  libpcre2-16-0 libpcre2-32-0 libpcre2-dev libpcre2-posix0 zlib1g-dev
0 upgraded, 5 newly installed, 0 to remove and 22 not upgraded.
Need to get 1,137 kB of archives.
```

```
Done building agent

./init/adduser.sh ossec ossecm ossecr ossec /var/ossec
Wait for success...
success
install -m 0550 -o root -g ossec -d /var/ossec/
install -m 0750 -o ossec -g ossec -d /var/ossec/logs
install -m 0660 -o ossec -g ossec /dev/null /var/ossec/logs/ossec.log
install -m 0550 -o root -g 0 -d /var/ossec/bin
install -m 0550 -o root -g 0 ossec-logcollector /var/ossec/bin
install -m 0550 -o root -g 0 ossec-syscheckd /var/ossec/bin
install -m 0550 -o root -g 0 ossec-execd /var/ossec/bin
install -m 0550 -o root -g 0 manage_agents /var/ossec/bin
install -m 0550 -o root -g 0 ../contrib/util.sh /var/ossec/bin/
install -m 0550 -o root -g 0 ./init/ossec-client.sh /var/ossec/bin/ossec-control
install -m 0550 -o root -g ossec -d /var/ossec/queue
install -m 0770 -o ossec -g ossec -d /var/ossec/queue/alerts
install -m 0750 -o ossec -g ossec -d /var/ossec/queue/ossec
install -m 0750 -o ossec -g ossec -d /var/ossec/queue/syscheck
install -m 0750 -o ossec -g ossec -d /var/ossec/queue/diff
install -m 0550 -o root -g ossec -d /var/ossec/etc
install -m 0440 -o root -g ossec /etc/localtime /var/ossec/etc
install -m 0440 -o root -g ossec /etc/resolv.conf /var/ossec/etc
install -m 1550 -o root -g ossec -d /var/ossec/tmp
install -m 0640 -o root -g ossec -b ../etc/internal_options.conf /var/ossec/etc/
install -m 0640 -o root -g ossec ../etc/local_internal_options.conf /var/ossec/e
tc/local_internal_options.conf
```

```
- System is Debian (Ubuntu or derivative).
- Init script modified to start OSSEC HIDS during boot.

- Configuration finished properly.

- To start OSSEC HIDS:
    /var/ossec/bin/ossec-control start

- To stop OSSEC HIDS:
    /var/ossec/bin/ossec-control stop

- The configuration can be viewed or modified at /var/ossec/etc/ossec.conf


   Thanks for using the OSSEC HIDS.
   If you have any question, suggestion or if you find any bug,
   contact us at https://github.com/ossec/ossec-hids or using
   our public maillist at
   https://groups.google.com/forum/#!forum/ossec-list

   More information can be found at http://www.ossec.net

   ---  Press ENTER to finish (maybe more information below). ---
```

server

sudo docker pull atomicorp/ossec-docker

```
[redacted]:/opt/ossec/ossec-hids-3.6.0$ sudo docker pull atomicorp/ossec-docker
Using default tag: latest
latest: Pulling from atomicorp/ossec-docker
ab5ef0e58194: Pull complete
c5fe32e1fe7c: Pull complete
c7aeecc4fa5e: Pull complete
bbb357a31414: Pull complete
f10766aaa55a: Pull complete
8e45908f78d3: Pull complete
8b90fcedecda: Pull complete
Digest: sha256:480d5b0b220e64832a8f61c3dc89cdacb840c2c462cd2dad0daa23314d6862c4
Status: Downloaded newer image for atomicorp/ossec-docker:latest
docker.io/atomicorp/ossec-docker:latest
```

```
[root@c6a85374a505 /]# /var/ossec/bin/manage_agents


****************************************
* OSSEC HIDS v3.6.0 Agent manager.     *
* The following options are available: *
****************************************
   (A)dd an agent (A).
   (E)xtract key for an agent (E).
   (L)ist already added agents (L).
   (R)emove an agent (R).
   (Q)uit.
Choose your action: A,E,L,R or Q: A

- Adding a new agent (use '\q' to return to the main menu).
  Please provide the following:
   * A name for the new agent: my_agent
   * The IP Address of the new agent: 172.17.0.1
   * An ID for the new agent[002]:
Agent information:
   ID:002
   Name:my_agent
   IP Address:172.17.0.1
```

```
Choose your action: A,E,L,R or Q: E

Available agents:
   ID: 001, Name: DEFAULT LOCAL AGENT, IP: 127.0.0.1
   ID: 002, Name: my_agent, IP: 172.17.0.1
Provide the ID of the agent to extract the key (or '\q' to quit): 002

Agent key information for '002' is:
MDAyIG15X2FnZW50IDE3Mi4xNy4wLjEgYThlM2RkMjY4YTRjMGY2M2U3MGE5YzE3ODg2YWFjOTZhYzYxNTk0YmJlMzQ5YTRjZTU4ZGFjODExZGRlZTY2
ZA==

** Press ENTER to return to the main menu.
```

```
root@esphagio:/var/ossec/queue/rids# /var/ossec/bin/manage_agents


****************************************
* OSSEC HIDS v3.6.0 Agent manager.     *
* The following options are available: *
****************************************
   (I)mport key from the server (I).
   (Q)uit.
Choose your action: I or Q: I

* Provide the Key generated by the server.
* The best approach is to cut and paste it.
*** OBS: Do not include spaces or new lines.

Paste it here (or '\q' to quit): MDAyIG15X2FnZW50IDE3Mi4xNy4wLjEgYThlM2RkMjY4YTRjMGY2M2U3MGE5YzE3ODg2YWFjOTZhYzYxNTk
0YmJlMzQ5YTRjZTU4ZGFjODExZGRlZTY2ZA==

Agent information:
   ID:002
   Name:my_agent
   IP Address:172.17.0.1

Confirm adding it?(y/n): y
```

Restart client

```
root@          :/var/ossec# service ossec restart
root@          :/var/ossec# service ossec status
● ossec.service - LSB: Start and stop OSSEC HIDS
   Loaded: loaded (/etc/init.d/ossec; generated)
   Active: active (running) since Tue 2020-11-24 22:46:01 EAT; 21s ago
     Docs: man:systemd-sysv-generator(8)
  Process: 18036 ExecStart=/etc/init.d/ossec start (code=exited, status=0/SUCCESS)
    Tasks: 4 (limit: 4915)
   CGroup: /system.slice/ossec.service
           ├─18074 /var/ossec/bin/ossec-agentd
           ├─18076 /var/ossec/bin/ossec-agentd
           ├─18080 /var/ossec/bin/ossec-logcollector
           └─18085 /var/ossec/bin/ossec-syscheckd
```