Vectra FIM - How to add agents

Document classification: Confidential

Requirements

UDP/1514 needs to be allowed both ways between endpoint and FIM (OSSEC Manager) host.

Agent installation on Windows Endpoint

0. Send agent authentication key to the client.

1.. Run ossec-agent-win32-3.7.0-24343.exe as administrator.

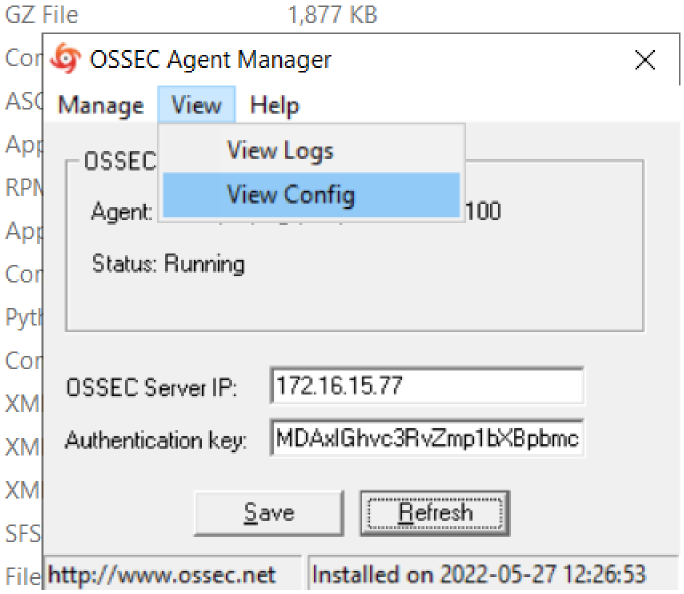
2.. Run C:\Program Files (x86)\ossec-agent\os_win32ui.exe to open the agent UI.

3.. Manage > Stop OSSEC

4.. Set the OSSEC Server IP to be the IP of the OSSEC Manager (FIM host).

5.. Set the Authentication key to the value indicated by Vectra (see below). Each host/agent has a unique authentication key.

6.. Overwrite configuration file to remove unnecessary feature -> Copy the contents from the osseca-agent.conf file. On the AgentUI go to, View >> View Config, a text file will open up. Select all and remove the current configuration and then paste in the content. Save and close.



Agent: 100

Status: Running

OSSEC Server IP: 172.16.15.77

Authentication key: MDAxlGhvc3RvZmp1bXBpbmc

http://www.ossec.net

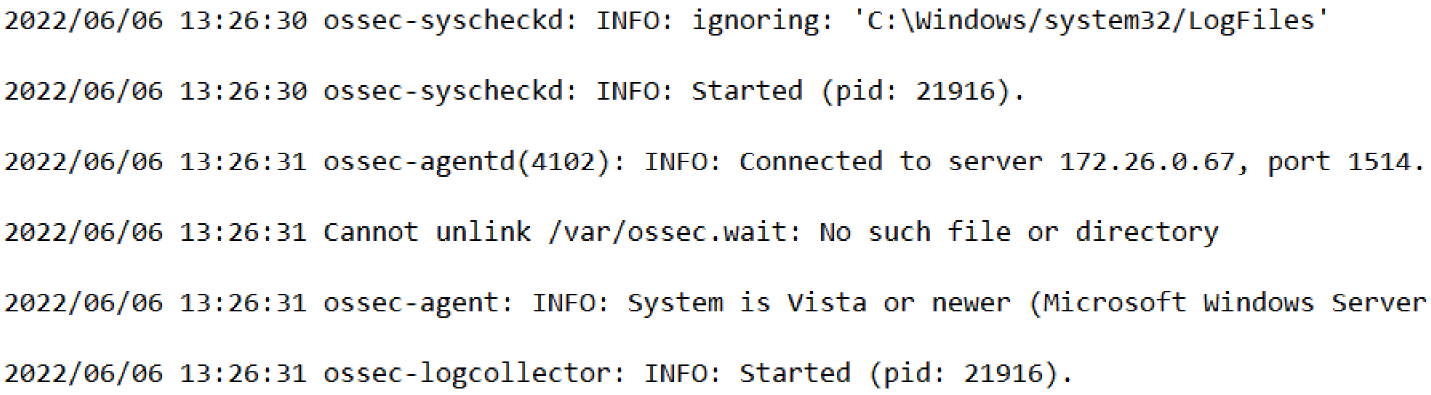
Installed on 2022-05-27 12:26:53

7.. Copy and paste the agent.conf here, C:\Program Files (x86)\ossec-agent\

8.. Manage > Start OSSEC

Note: the Server IP and Auth key may be required again after changing the configuration. Enter the Syslog server's IP and the authentication key.

9.. If everything was properly configured, the ossec.log file will show the agent is connected to the OSSEC Manager (FIM) as shown below. To check the log file on the WinUI.exe go to View>> ViewLogs , should look something like this,



```
2022/06/06 13:26:30 ossec-syscheckd: INFO: ignoring: 'C:\Windows/system32/LogFiles'

2022/06/06 13:26:30 ossec-syscheckd: INFO: Started (pid: 21916).

2022/06/06 13:26:31 ossec-agentd(4102): INFO: Connected to server 172.26.0.67, port 1514.

2022/06/06 13:26:31 Cannot unlink /var/ossec.wait: No such file or directory

2022/06/06 13:26:31 ossec-agent: INFO: System is Vista or newer (Microsoft Windows Server

2022/06/06 13:26:31 ossec-logcollector: INFO: Started (pid: 21916).
```

Limitations

Newly installed agents have OSSEC's ossec.conf file, which needs to be manually overwritten for each host. The agent.conf file that is propagated from the manager doesn't overwrite local ossec.conf file. That is, local ossec.conf file has precedence over agent.conf, that's why local ossec.conf needs to be modified on each agent.

Agent installation on Linux Endpoint

0.. Send agent authentication key to the client.

1.. wget -q -O - http://www.atomicorp.com/installers/atomic | sh {This is to add the atomic repository on linux agents, which works for all, so binaries would be downloaded automatically during step 2 and the current version is 3.7.0) OR For anything other than CentOS use wget -q -O - http://www.atomicorp.com/installers/atomic | sudo bash

→ sudo yum update OR sudo apt-get update

2.. The package manager may differ on various unix systems, (This will map all the dependencies as well)

- For CentOS yum install ossec-hids-agent
- For others apt-get install ossec-hids-agent

3.. If steps 1 and 2 don't work copy the binaries and install them.

- Wget https://github.com/ossec/ossec-hids/archive/3.7.0.tar.gz
- sudo yum group install "Development Tools"
- yum install zlib-devel
- yum install yum install pcre2-devel
- tar -xzf 3.7.0.tar.gz
- cd 3.7.0
- ./install

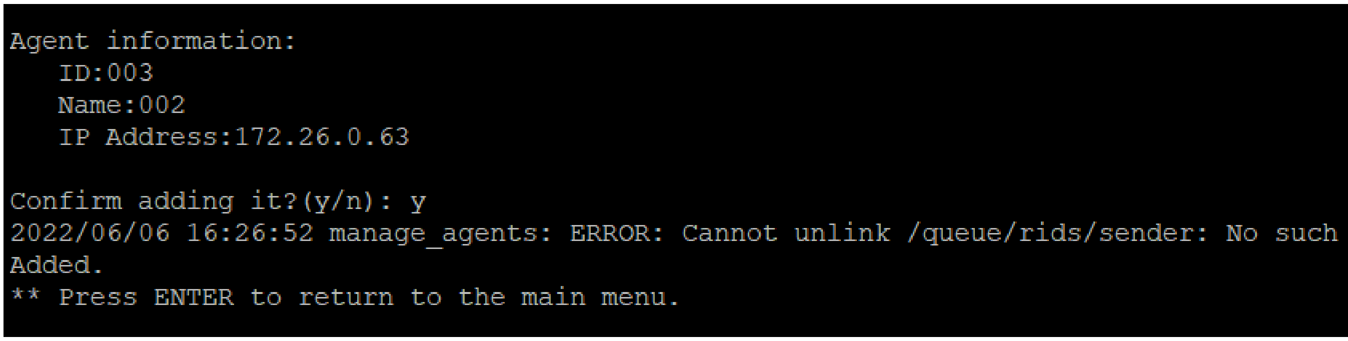
4.. Run the following /var/ossec/bin/ossec-configure

```
1- What kind of installation do you want (server, agent, local, hybrid or help)?
Agent
2- Setting up the installation environment. /var/ossec
3- Configuring the OSSEC HIDS.
3.1- Do you want e-mail notification? (y/n) [y]: NO
3.2- Do you want to run the integrity check daemon? (y/n) [y]: YES
3.3- Do you want to run the rootkit detection engine? (y/n) [y]: NO
3.4- Do you want to enable active response? (y/n) [y]: YES
3.4.1- Do you want to enable the firewall-drop response? (y/n) [y]: NO
3.4.2- Do you want to add more IPs to the white list? (y/n)? [n]: NO
3.5- Do you want to enable remote syslog (port 514 udp)? (y/n) [y]: NO
```

5..Run /var/ossec/bin/manage_agent

6.. Select the option to I to insert the key, copy paste the client key and quit

- If it gives an error like this,



```
Agent information:
   ID:003
   Name:002
   IP Address:172.26.0.63

Confirm adding it?(y/n): y
2022/06/06 16:26:52 manage_agents: ERROR: Cannot unlink /queue/rids/sender: No such
Added.
** Press ENTER to return to the main menu.
```

Use **touch /var/ossec/queue/rids/sender**

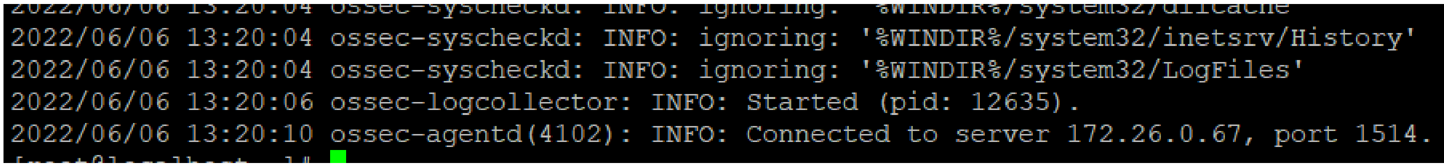
Repeat step 6.

7.. Overwrite the contents of the /var/ossec/etc/ossec.conf with the configuration file that has been supplied for linux agents (ossec.conf). Make changes to the server IP, change it to the Ip of the syslog server where the manager is installed. Save changes.

8.. Copy the agent.conf file to /var/ossc/etc/shared/

9.. Run /var/ossec/bin/ossec-agentd start | /var/ossec/bin/ossec-control restart

10.. if everything is configure properly Check /var/ossec/logs/ossec.log for logs and this should be populated.



```
2022/06/06 13:20:04 ossec-syscheckd: INFO: ignoring: '%WINDIR%/system32/dllcache'
2022/06/06 13:20:04 ossec-syscheckd: INFO: ignoring: '%WINDIR%/system32/inetsrv/History'
2022/06/06 13:20:04 ossec-syscheckd: INFO: ignoring: '%WINDIR%/system32/LogFiles'
2022/06/06 13:20:06 ossec-logcollector: INFO: Started (pid: 12635).
2022/06/06 13:20:10 ossec-agentd(4102): INFO: Connected to server 172.26.0.67, port 1514.
[root@localhost ~]#
```

Limitations

Newly installed agents have OSSEC's ossec.conf file, which needs to be manually overwritten for each host. The agent.conf file that is propagated from the manager doesn't overwrite local ossec.conf file. That is, local ossec.conf file has precedence over agent.conf, that's why local ossec.conf needs to be modified on each agent.