OSSEC Server and Agent Installation

Install OSSEC HIDS on Rocky 9 / CentOS 9

Install OSSEC Server

Provide a computer name to the server

```
sudo  hostnamectl  set-hostname  ossec-server
```

disable selinux.

```
sudo  vi  /etc/selinux/config
```

In this file look for the setting **SELINUX=enforcing**

Change this setting to
SELINUX=disabled

Save the file.

```
sudo setenforce 0
```

Install required software.

```
sudo yum install zlib-devel pcre2-devel make gcc sqlite-devel openssl-devel libevent-devel systemd-devel automake autoconf epel-release  wget tar unzip -y
```

```
sudo yum install -y https://rpms.remirepo.net/enterprise/remi-release-9.rpm
```

```
sudo yum module list php
```

```
sudo yum module enable php:remi-7.4  -y
```

```
sudo yum install -y php php-cli php-common php-fpm
```

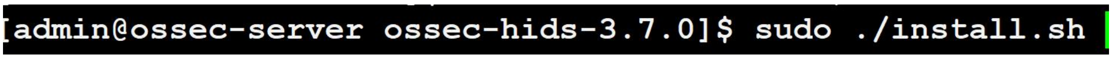
Download OSSEC, extract and then install

```
wget https://github.com/ossec/ossec-hids/archive/3.7.0.tar.gz
```

```
tar xvzf 3.7.0.tar.gz
```

```
cd ossec-hids-3.7.0
```

```
sudo  ./install.sh
```

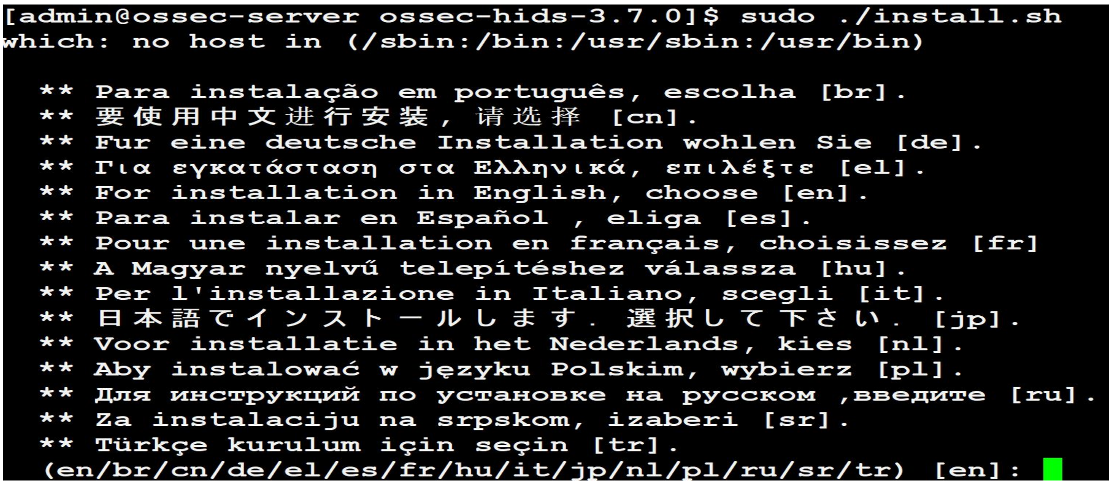


```
[admin@ossec-server ossec-hids-3.7.0]$ sudo ./install.sh
```

Answer the questions asked.

First the script will ask for the language for the OSSEC installation. Default is en for english.

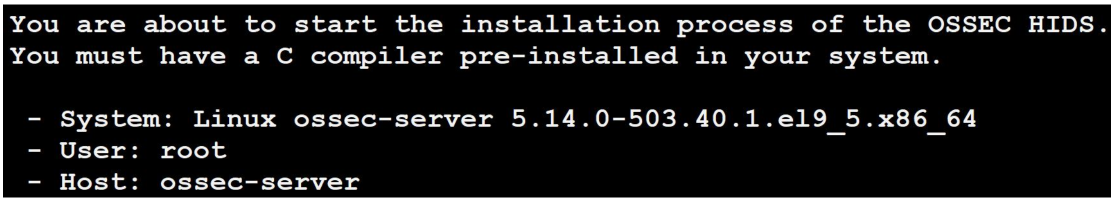
This is shown in the below image.



```
[admin@ossec-server ossec-hids-3.7.0]$ sudo ./install.sh
which: no host in (/sbin:/bin:/usr/sbin:/usr/bin)

  ** 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]:
```

Press Enter to continue with English language.

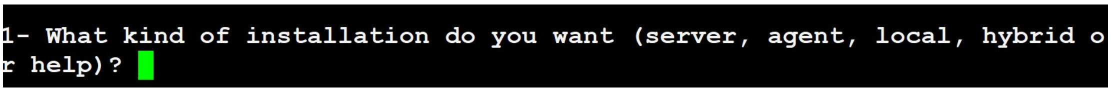
Next it displays the Kernel version, Username and Hostname.



```
 You are about to start the installation process of the OSSEC HIDS.
 You must have a C compiler pre-installed in your system.

  - System: Linux ossec-server 5.14.0-503.40.1.el9_5.x86_64
  - User: root
  - Host: ossec-server
```

Press Enter to continue.

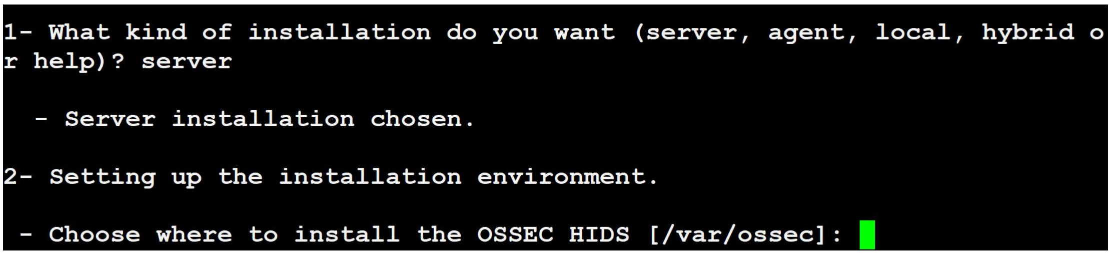
Next it will ask you what type of OSSEC installation you want?



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

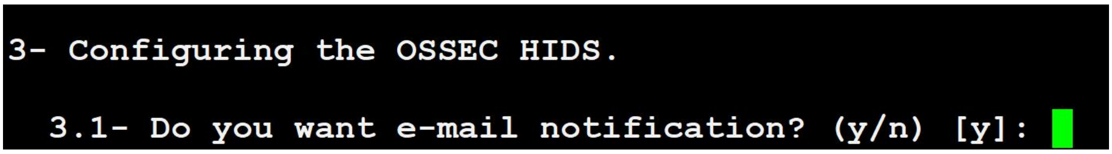
For a standalone computer select local option.

But here we are going to install **server**. Thus type server and press Enter.



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

  - Server installation chosen.

2- Setting up the installation environment.

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

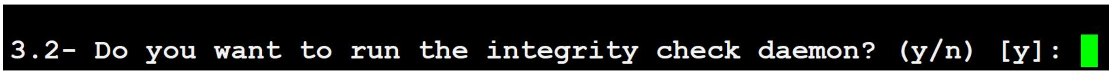
Next it will ask for the OSSEC installation directory. The default is /var/ossec. We will use this default directory.
Press Enter.



```
3- Configuring the OSSEC HIDS.

  3.1- Do you want e-mail notification? (y/n) [y]:
```

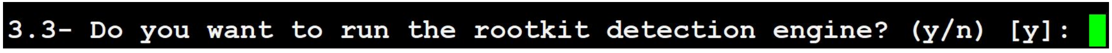
Next it will ask for e-mail notification. Type **n** here.

Next it will prompt for integrity check. This will check for any modifications in the files and generate an alert. Type y here.



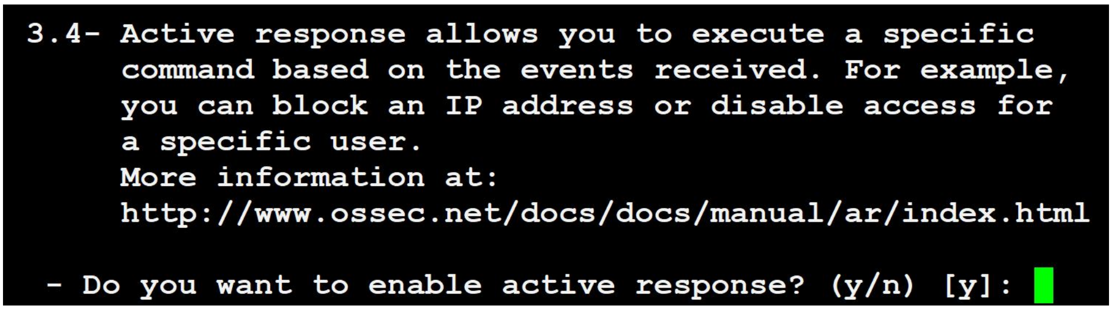
```
3.2- Do you want to run the integrity check daemon? (y/n) [y]:
```

Next it will ask for the rootkit detection. Type y to enable rootkit detection.



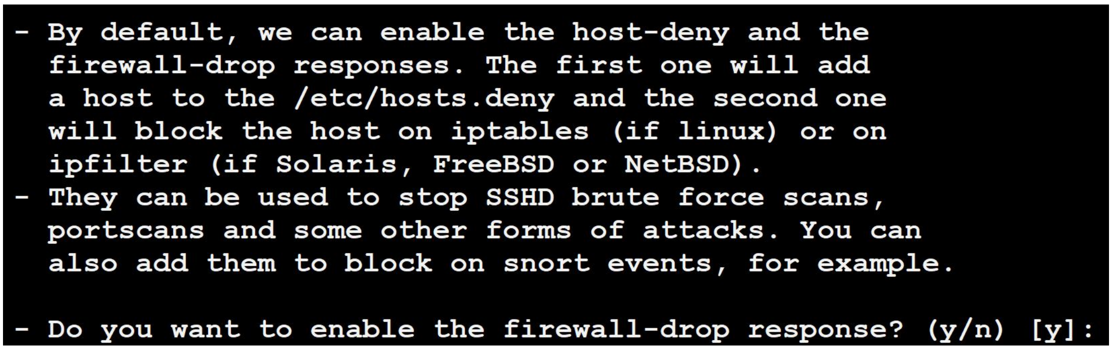
```
3.3- Do you want to run the rootkit detection engine? (y/n) [y]:
```

Next it will prompt for active response. Type Y here.



```
 3.4- Active response allows you to execute a specific
      command based on the events received. For example,
      you can block an IP address or disable access for
      a specific user.
      More information at:
      http://www.ossec.net/docs/docs/manual/ar/index.html

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

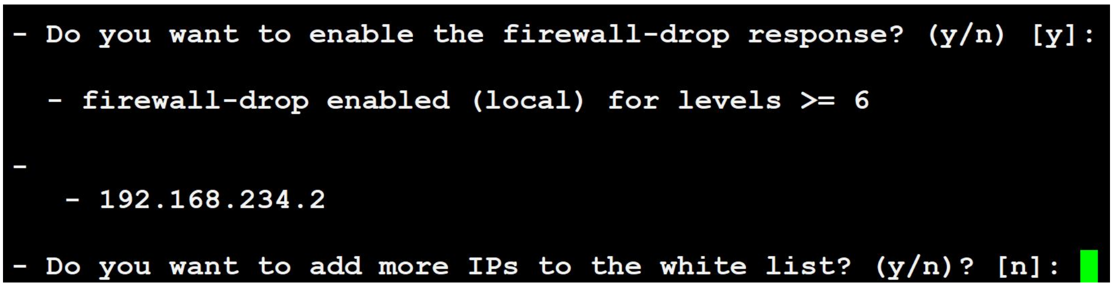
Next it ask to enable firewall drop response.



```
- By default, we can enable the host-deny and the
  firewall-drop responses. The first one will add
  a host to the /etc/hosts.deny and the second one
  will block the host on iptables (if linux) or on
  ipfilter (if Solaris, FreeBSD or NetBSD).
- They can be used to stop SSHD brute force scans,
  portscans and some other forms of attacks. You can
  also add them to block on snort events, for example.

- Do you want to enable the firewall-drop response? (y/n) [y]:
```

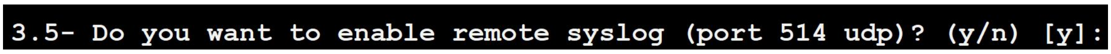
Type y if you want to enable it else type n. Press Enter.

It will add the default gateway IP address into the whitelist. Also it will prompt you to add additional IP addresses to whitelist.



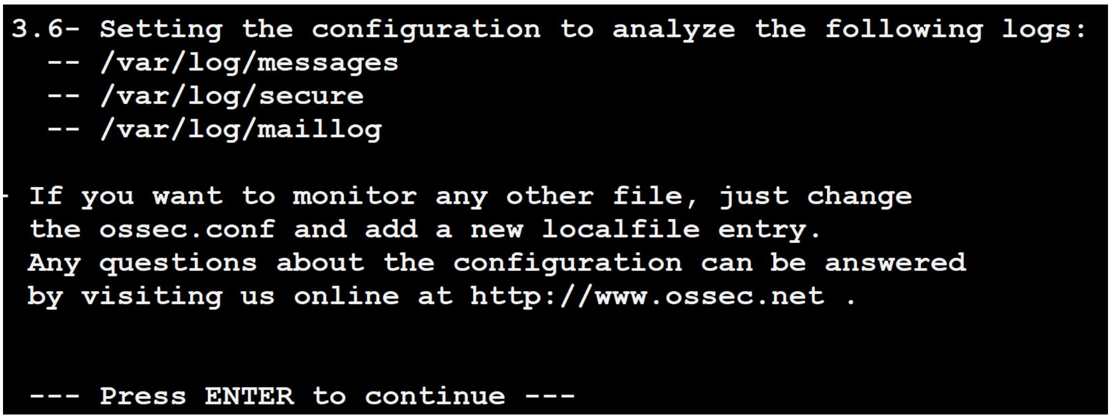
```
- Do you want to enable the firewall-drop response? (y/n) [y]:

  - firewall-drop enabled (local) for levels >= 6

-
   - 192.168.234.2

- Do you want to add more IPs to the white list? (y/n)? [n]:
```

Press Enter as we do not want to whitelist any other IP address.
Next it will ask you to enable remote syslog server. Type n here and press Enter.



```
3.5- Do you want to enable remote syslog (port 514 udp)? (y/n) [y]:
```

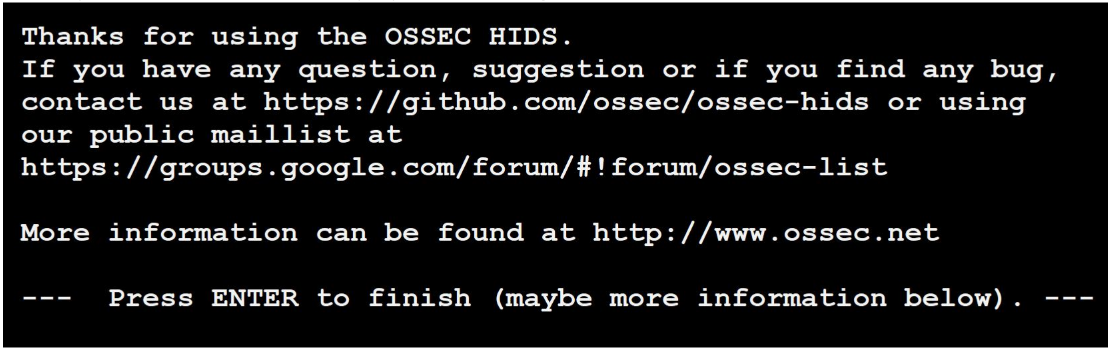
Finally it will display the following screen.



```
3.6- Setting the configuration to analyze the following logs:
  -- /var/log/messages
  -- /var/log/secure
  -- /var/log/maillog

 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 ---
```

Once you press Enter, it will compile and install OSSEC server.

As the process finishes, it will display the following screen.

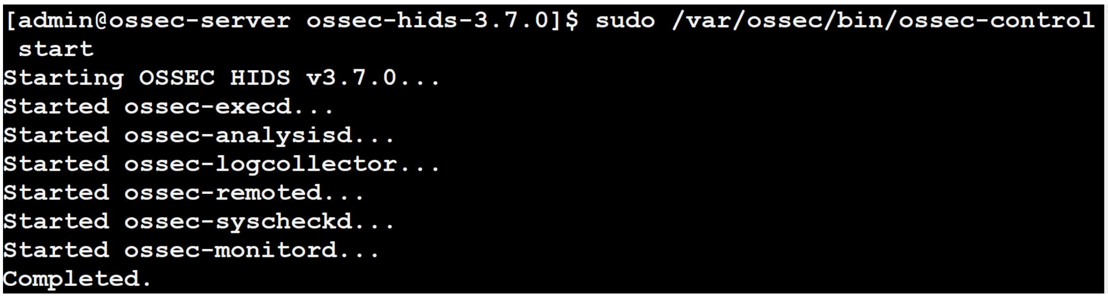


```
 Thanks for using the OSSEC HIDS.
 If you have any question, suggestion or if you find any bug,
 contact us at https://github.com/ossec/ossec-hids or using
 our public maillist at
 https://groups.google.com/forum/#!forum/ossec-list

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

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

Press Enter.
The OSSEC Server installation is finished.

Start OSSEC using following command.

sudo /var/ossec/bin/ossec-control   start



```
[admin@ossec-server ossec-hids-3.7.0]$ sudo /var/ossec/bin/ossec-control
 start
Starting OSSEC HIDS v3.7.0...
Started ossec-execd...
Started ossec-analysisd...
Started ossec-logcollector...
Started ossec-remoted...
Started ossec-syscheckd...
Started ossec-monitord...
Completed.
```

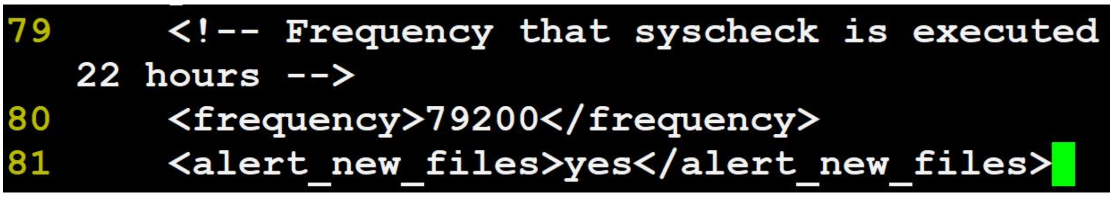
Configure OSSEC

sudo vi /var/ossec/etc/ossec.conf

add a line to report new file addition to the server.

This on line number 81 as shown in the below image.

```
<syscheck>
   <!-- Frequency that syscheck is executed - default to every 22 hours -->
   <frequency>79200</frequency>
   <alert_new_files>yes</alert_new_files>
```



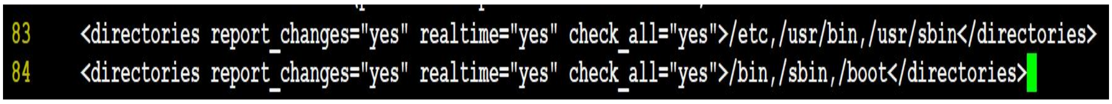
```
      <!-- Frequency that syscheck is executed
   22 hours -->
      <frequency>79200</frequency>
      <alert_new_files>yes</alert_new_files>
```

Also change following lines

```
<directories check_all="yes">/etc,/usr/bin,/usr/sbin</directories>
<directories check_all="yes">/bin,/sbin</directories>
```

to as below.

```
<directories report_changes="yes" realtime="yes" Check_all="yes" >etc,/usr/bin,/usr/sbin
</directories>
<directories report_changes="yes" realtime="yes" Check_all="yes" > /var/www,/bin,/sbin
</directories>
```



```
    <directories report_changes="yes" realtime="yes" check_all="yes">/etc,/usr/bin,/usr/sbin</directories>
    <directories report_changes="yes" realtime="yes" check_all="yes">/bin,/sbin,/boot</directories>
```

Save the file.

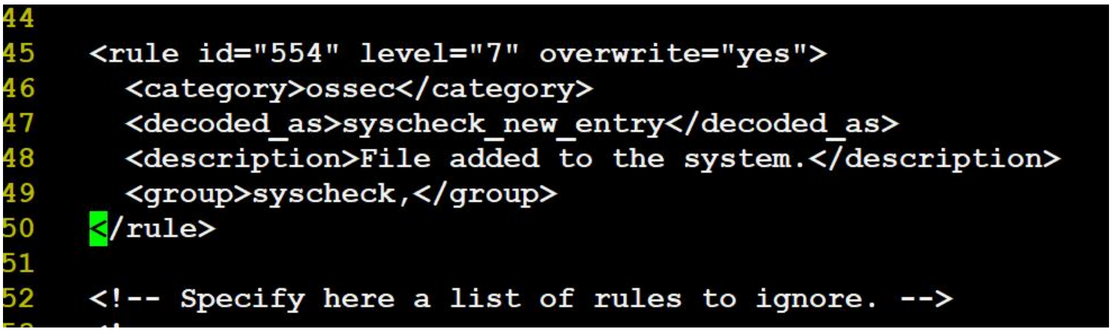
Now edit the local_rules.xml file.

sudo vi /var/ossec/rules/local_rules.xml

Add following lines

```
<rule id="554" level="7" overwrite="yes">
   <category>ossec</category>
   <decoded_as>syscheck_new_entry</decoded_as>
   <description>File added to the system.</description>
   <group>syscheck,</group>
</rule>
```

This is shown in the following image. Make sure you add these lines before the line “Specify here a list of rules to ignore”

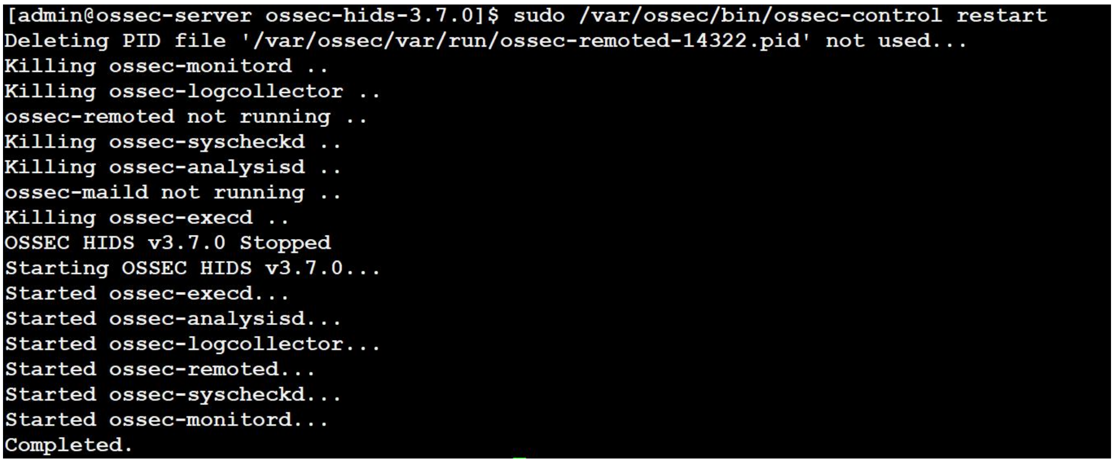


```

  <rule id="554" level="7" overwrite="yes">
    <category>ossec</category>
    <decoded_as>syscheck_new_entry</decoded_as>
    <description>File added to the system.</description>
    <group>syscheck,</group>
  </rule>

  <!-- Specify here a list of rules to ignore. -->
```

save the file.

Restart the OSSEC

sudo /var/ossec/bin/ossec-control restart



```
[admin@ossec-server ossec-hids-3.7.0]$ sudo /var/ossec/bin/ossec-control restart
Deleting PID file '/var/ossec/var/run/ossec-remoted-14322.pid' not used...
Killing ossec-monitord ..
Killing ossec-logcollector ..
ossec-remoted not running ..
Killing ossec-syscheckd ..
Killing ossec-analysisd ..
ossec-maild not running ..
Killing ossec-execd ..
OSSEC HIDS v3.7.0 Stopped
Starting OSSEC HIDS v3.7.0...
Started ossec-execd...
Started ossec-analysisd...
Started ossec-logcollector...
Started ossec-remoted...
Started ossec-syscheckd...
Started ossec-monitord...
Completed.
```

Install OSSEC web user interface.

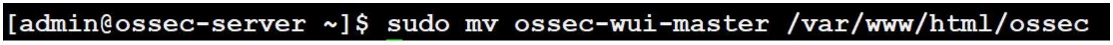
sudo yum install httpd -y

cd

wget https://github.com/ossec/ossec-wui/archive/master.zip

unzip master.zip

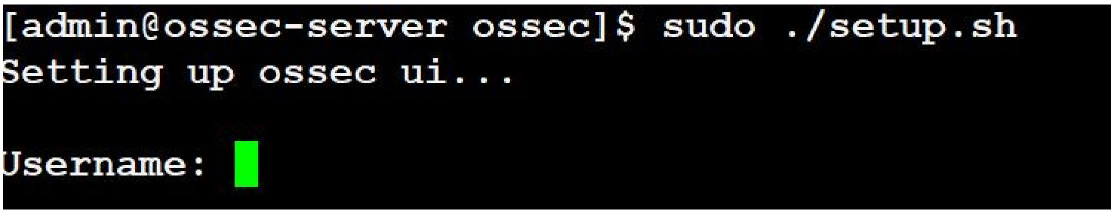
sudo mv ossec-wui-master /var/www/html/ossec



```
[admin@ossec-server ~]$ sudo mv ossec-wui-master /var/www/html/ossec
```

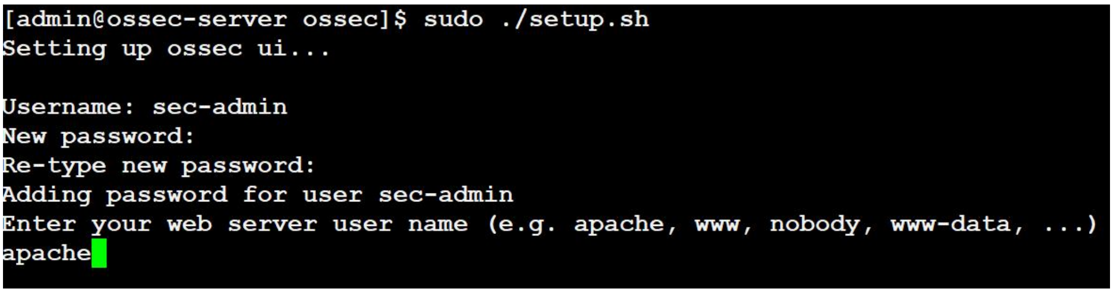
cd /var/www/html/ossec

sudo ./setup.sh



```
[admin@ossec-server ossec]$ sudo ./setup.sh
Setting up ossec ui...

Username:
```

provide username and password. Here username given is sec-admin. You can choose your own username. Provide password for this user. Specify the web server user as apache as shown below.



```
[admin@ossec-server ossec]$ sudo ./setup.sh
Setting up ossec ui...

Username: sec-admin
New password:
Re-type new password:
Adding password for user sec-admin
Enter your web server user name (e.g. apache, www, nobody, www-data, ...)
apache
```

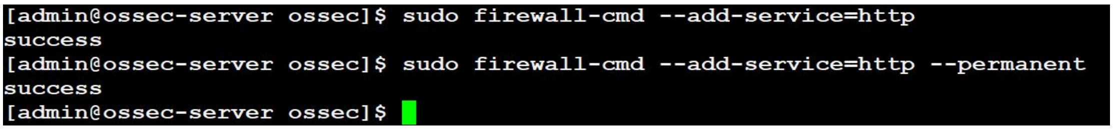
Once the setup is successful, restart the web server.

sudo systemctl restart httpd

sudo systemctl enable httpd

sudo firewall-cmd --add-service=http

sudo firewall-cmd --add-service --permanent



```
[admin@ossec-server ossec]$ sudo firewall-cmd --add-service=http
success
[admin@ossec-server ossec]$ sudo firewall-cmd --add-service=http --permanent
success
[admin@ossec-server ossec]$
```

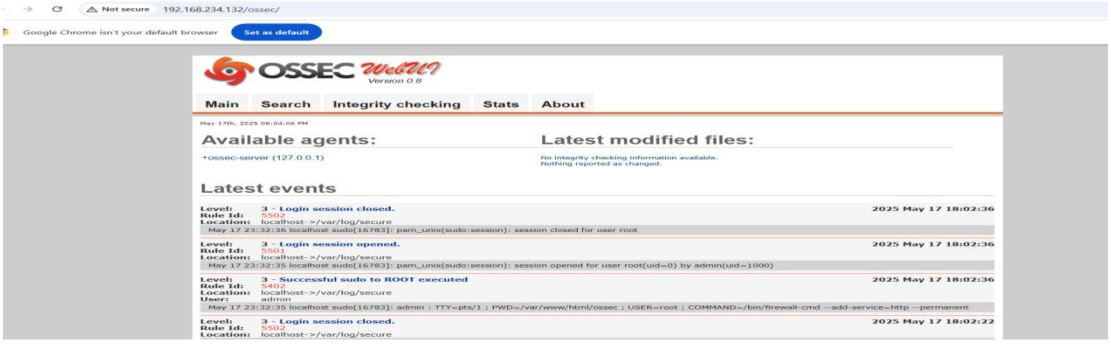
Restart the OSSEC Server

sudo   /var/ossec/bin/ossec-control   restart

Access the OSSEC web user interface.

open browser and go to the following URL. (Replace your IP address)

http://machine-ip/ossec



May 17th, 2025 06:04:06 PM

Available agents:

+ossec-server (127.0.0.1)

Latest modified files:

No integrity checking information available.
Nothing reported as changed.

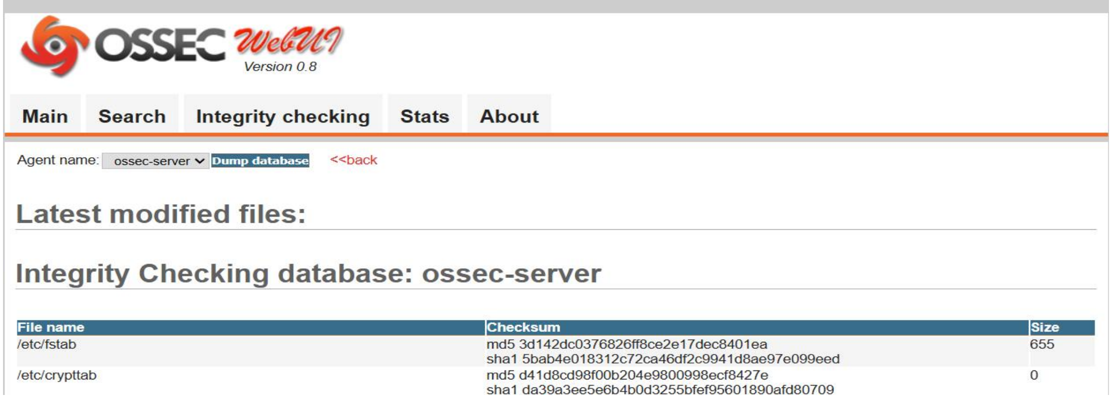
Latest events

```
Level:     3 - Login session closed.                                                  2025 May 17 18:02:36
Rule Id:   5502
Location:  localhost->/var/log/secure
  May 17 23:32:36 localhost sudo[16783]: pam_unix(sudo:session): session closed for user root
Level:     3 - Login session opened.                                                  2025 May 17 18:02:36
Rule Id:   5501
Location:  localhost->/var/log/secure
  May 17 23:32:35 localhost sudo[16783]: pam_unix(sudo:session): session opened for user root(uid=0) by admin(uid=1000)
Level:     3 - Successful sudo to ROOT executed                                       2025 May 17 18:02:36
Rule Id:   5402
Location:  localhost->/var/log/secure
User:      admin
  May 17 23:32:35 localhost sudo[16783]: admin : TTY=pts/1 ; PWD=/var/www/html/ossec ; USER=root ; COMMAND=/bin/firewall-cmd --add-service=http --permanent
Level:     3 - Login session closed.                                                  2025 May 17 18:02:22
Rule Id:   5502
Location:  localhost->/var/log/secure
```

You should be able to get similar interface as shown above.

Test OSSEC.

On the web interface click Integrity Checking tab. On that page Below Integrity Checking Dump Database option (With blue background) is present. Click on that. It will display the file information. The first file is the /etc/fstab. Check the number in the last column.



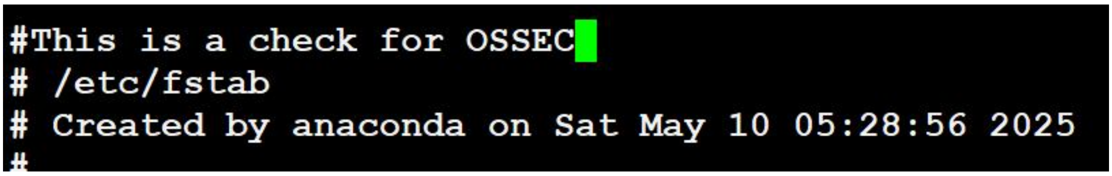
Agent name: ossec-server

Latest modified files:

Integrity Checking database: ossec-server

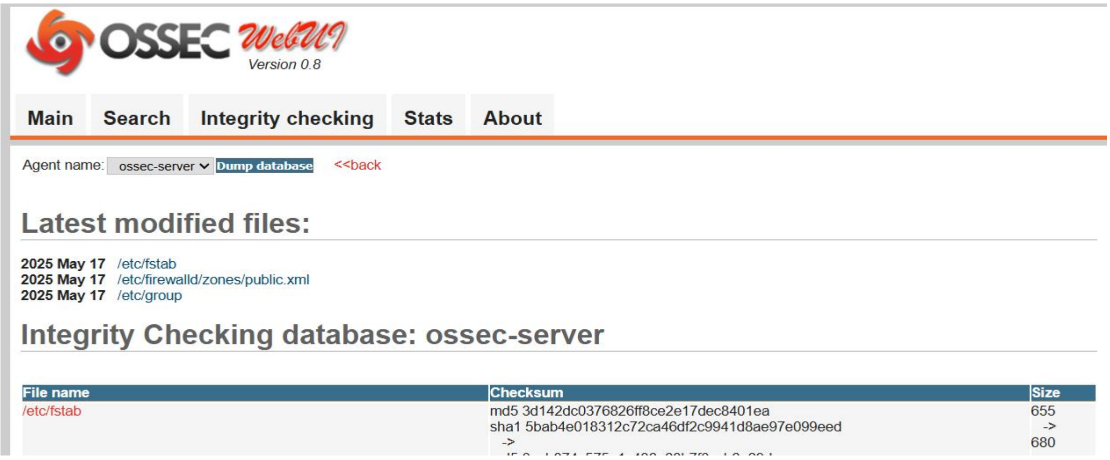
File name	Checksum	Size
/etc/fstab	md5 3d142dc0376826ff8ce2e17dec8401ea sha1 5bab4e018312c72ca46df2c9941d8ae97e099eed	655
/etc/crypttab	md5 d41d8cd98f00b204e9800998ecf8427e sha1 da39a3ee5e6b4b0d3255bfef95601890afd80709	0

Modify the /etc/fstab by adding a # this is check for OSSEC line.



```
#This is a check for OSSEC
# /etc/fstab
# Created by anaconda on Sat May 10 05:28:56 2025
#
```

Check the logs on Web UI. Click Back button and Dump database again. You should be able to get following output.



Agent name: ossec-server

Latest modified files:

2025 May 17 /etc/fstab
2025 May 17 /etc/firewalld/zones/public.xml
2025 May 17 /etc/group

Integrity Checking database: ossec-server

File name	Checksum	Size
/etc/fstab	md5 3d142dc0376826ff8ce2e17dec8401ea sha1 5bab4e018312c72ca46df2c9941d8ae97e099eed ->	655 -> 680

The /etc/fstab file name is shown in the red colour. Also the number in the last column is changed.

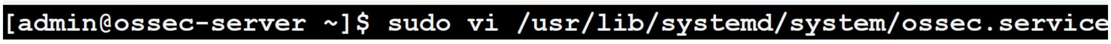
The OSSEC logs are in the /var/ossec/logs/alerts/alerts.log file.

Configure OSSEC as a Service.

You have to make sure that the OSSEC server services should be running even after a restart of the system. Thus you need to add OSSEC as a service so that using systemctl command you can enable the service for auto start and also start and stop it.

For this, create a file in the /usr/lib/systemd/system directory by the name of the service. The extension of the file should be .service.

sudo vi /usr/lib/systemd/system/ossec.service



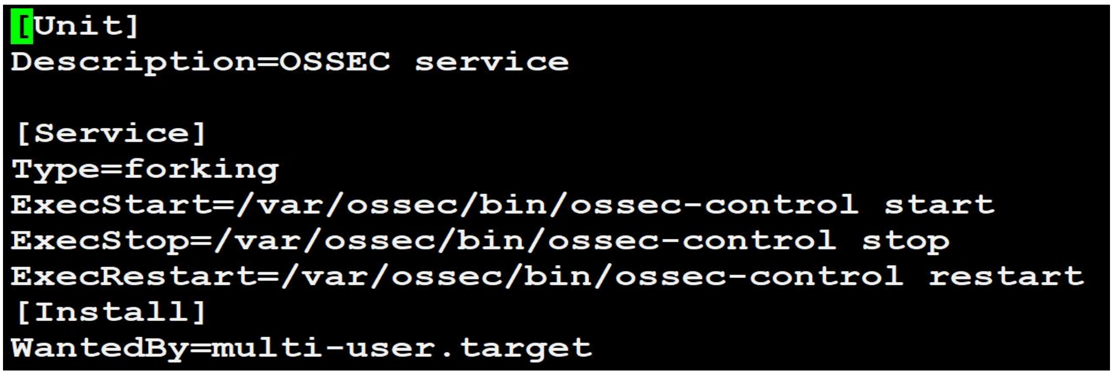
```
[admin@ossec-server ~]$ sudo vi /usr/lib/systemd/system/ossec.service
```

Type following in the file.

[Unit]
Description=OSSEC service

[Service]
Type=forking
ExecStart=/var/ossec/bin/ossec-control start
ExecStop=/var/ossec/bin/ossec-control stop
ExecRestart=/var/ossec/bin/ossec-control restart
[Install]
WantedBy=multi-user.target

This will look as shown below.



```
[Unit]
Description=OSSEC service

 [Service]
Type=forking
ExecStart=/var/ossec/bin/ossec-control start
ExecStop=/var/ossec/bin/ossec-control stop
ExecRestart=/var/ossec/bin/ossec-control restart
 [Install]
WantedBy=multi-user.target
```

Save the file.

Now stop the OSSEC service.

sudo /var/ossec/bin/ossec-control stop

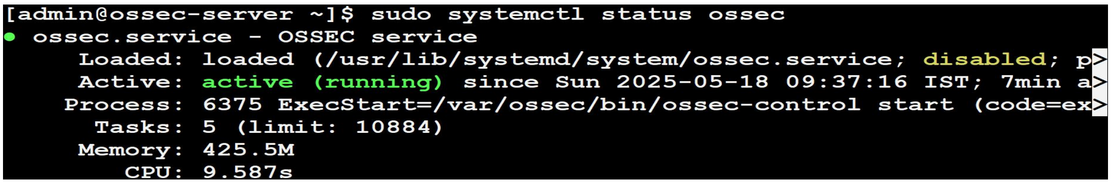
Now start the service using systemctl command.

sudo systemctl start ossec

If you get any error, please check the syntax and spelling mistakes in the above file.

If there is no error then check the service status.

sudo systemctl status ossec

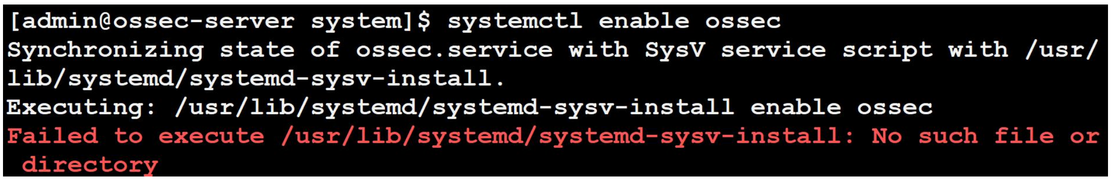


```
[admin@ossec-server ~]$ sudo systemctl status ossec
● ossec.service - OSSEC service
     Loaded: loaded (/usr/lib/systemd/system/ossec.service; disabled; p>
     Active: active (running) since Sun 2025-05-18 09:37:16 IST; 7min a>
    Process: 6375 ExecStart=/var/ossec/bin/ossec-control start (code=ex>
      Tasks: 5 (limit: 10884)
     Memory: 425.5M
        CPU: 9.587s
```

Enable the OSSEC service for auto start.

sudo systemctl enable ossec

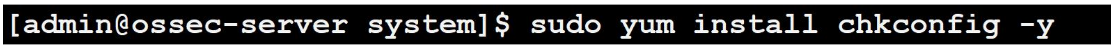
However on RedHat9/Rocky9/CentOS9 you will get following error.



```
[admin@ossec-server system]$ systemctl enable ossec
Synchronizing state of ossec.service with SysV service script with /usr/
lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable ossec
Failed to execute /usr/lib/systemd/systemd-sysv-install: No such file or
 directory
```

This is due to systemd-sysv-install is removed in these distributions. It is optional as most of the services do not require it. However certain services like OSSEC, grafana may require it.
For this you need to install the chkconfig package.

sudo yum install chkconfig -y

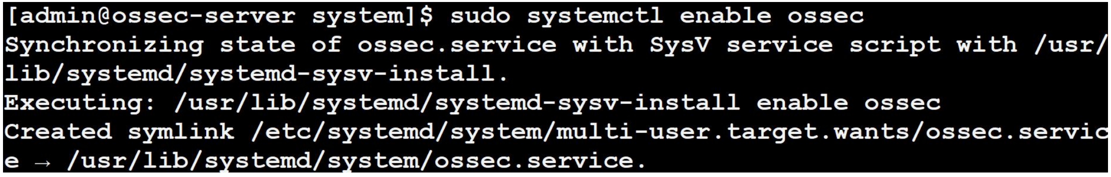


```
[admin@ossec-server system]$ sudo yum install chkconfig -y
```

Once this package is installed, enable the ossec service.

sudo systemctl enable ossec

This time there will not be any error.

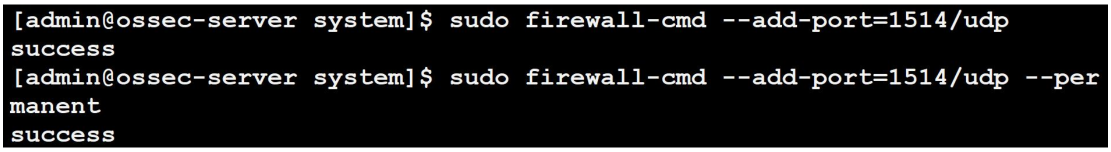


```
[admin@ossec-server system]$ sudo systemctl enable ossec
Synchronizing state of ossec.service with SysV service script with /usr/
lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable ossec
Created symlink /etc/systemd/system/multi-user.target.wants/ossec.servic
e → /usr/lib/systemd/system/ossec.service.
```

Now open the port used by the OSSEC service in the firewall. This will allow agents to communicate with the server.
OSSEC uses UDP port 1514.

sudo   firewall-cmd --add-port=1514/udp

sudo firewall-cmd --add-port=1514/udp --permanent



```
[admin@ossec-server system]$ sudo firewall-cmd --add-port=1514/udp
success
[admin@ossec-server system]$ sudo firewall-cmd --add-port=1514/udp --per
manent
success
```

<u>This is how the OSSEC server is installed successfully.</u>

Install and add agent to the OSSEC server for monitoring.

This is another computer. Login to this computer with sudo permissions.

Provide a computer name to the server

sudo hostnamectl set-hostname client1

disable selinux.

sudo vi /etc/selinux/config

In this file look for the setting **SELINUX=enforcing**

Change this setting to
SELINUX=disabled

Save the file.

sudo setenforce 0

Install required software.

sudo yum install zlib-devel pcre2-devel make gcc sqlite-devel openssl-devel libevent-devel systemd-devel automake autoconf epel-release wget tar unzip -y

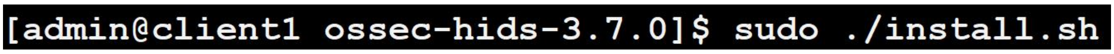
Download OSSEC, extract and then install

wget https://github.com/ossec/ossec-hids/archive/3.7.0.tar.gz

tar xvzf 3.7.0.tar.gz

cd ossec-hids-3.7.0

sudo ./install.sh

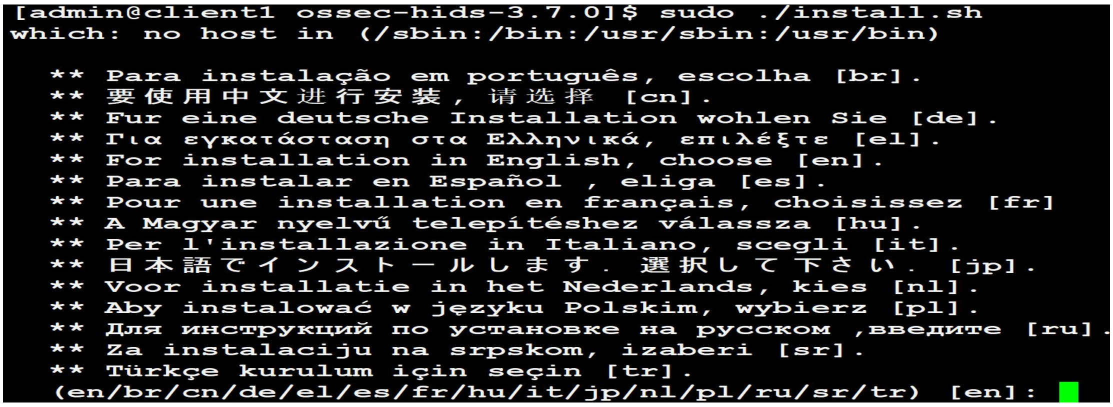


```
[admin@client1 ossec-hids-3.7.0]$ sudo ./install.sh
```

Answer the questions asked.

First the script will ask for the language for the OSSEC installation. Default is en for english.

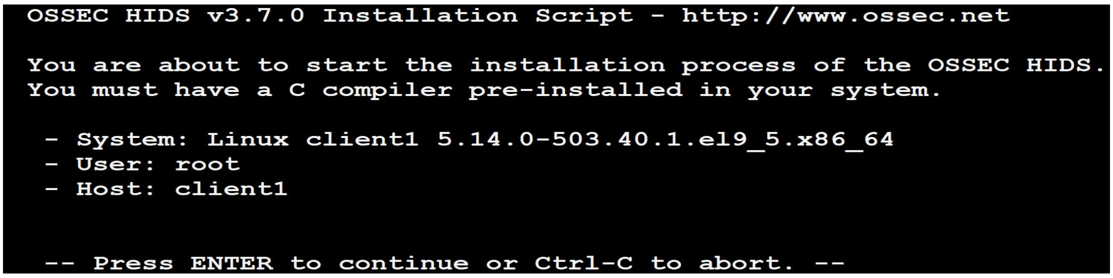
This is shown in the below image.



```
 [admin@client1 ossec-hids-3.7.0]$ sudo ./install.sh
which: no host in (/sbin:/bin:/usr/sbin:/usr/bin)

  ** 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]:
```

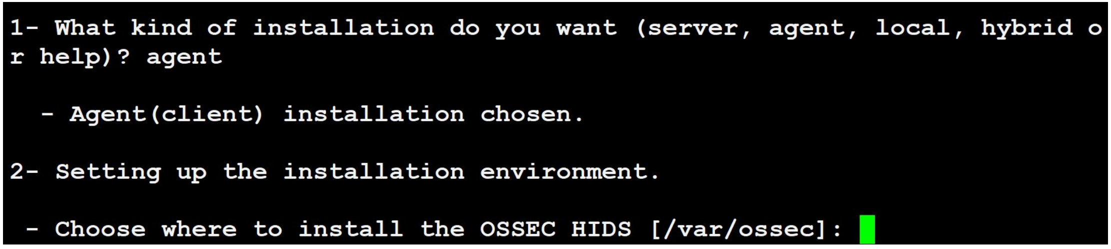
Press Enter to continue with English language.

Next it displays the Kernel version, Username and Hostname.



```
 OSSEC HIDS v3.7.0 Installation Script - http://www.ossec.net

 You are about to start the installation process of the OSSEC HIDS.
 You must have a C compiler pre-installed in your system.

  - System: Linux client1 5.14.0-503.40.1.el9_5.x86_64
  - User: root
  - Host: client1


  -- Press ENTER to continue or Ctrl-C to abort. --
```

Press Enter to continue.
Next it will ask you what type of OSSEC installation you want?

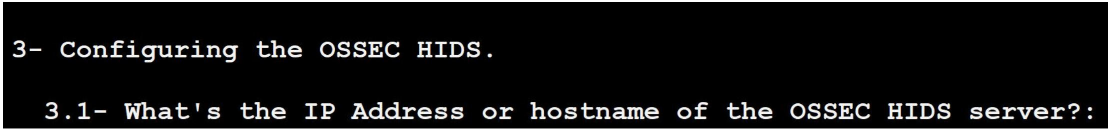


```
1- What kind of installation do you want (server, agent, local, hybrid o
r help)? agent

  - Agent(client) installation chosen.

2- Setting up the installation environment.

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

As we are installing agent here, type agent at the prompt. Press Enter.

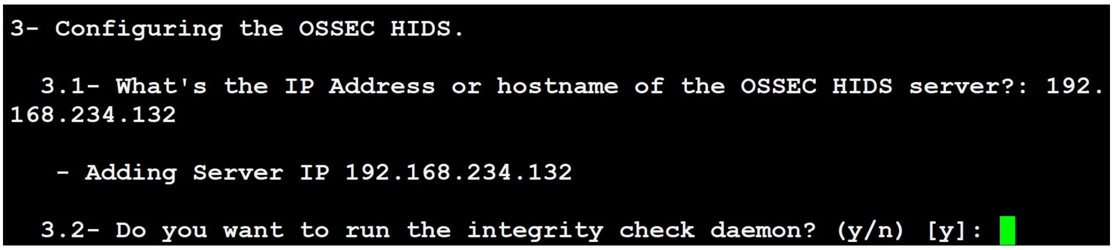
Press Enter to select the default installation directory /var/ossec.

Next it will prompt for the OSSEC server IP address as shown below.



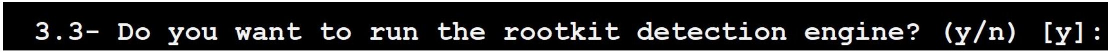
```
3- Configuring the OSSEC HIDS.

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

Type the IP address of your OSSEC server and press enter as shown below.



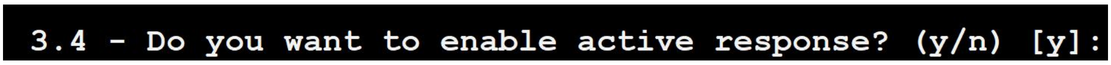
```
3- Configuring the OSSEC HIDS.

  3.1- What's the IP Address or hostname of the OSSEC HIDS server?: 192.
168.234.132

   - Adding Server IP 192.168.234.132

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

To enable Integrity Check press Enter.
Next to enable rootkit detection press Enter.



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

On next prompt press Enter to enable active response.



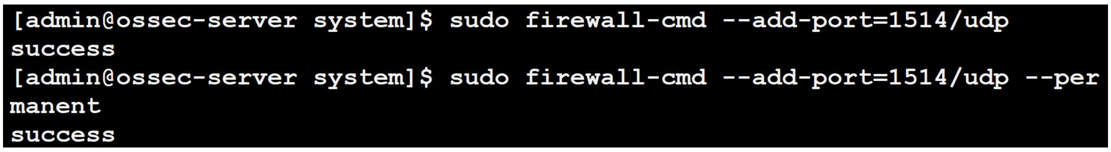
```
  3.4 - Do you want to enable active response? (y/n) [y]:
```

Press Enter to continue installation.
Finally press Enter to finish the installation.

Now open the port used by the OSSEC service in the firewall. This will allow agents to communicate with the server.
OSSEC uses UDP port 1514.

sudo   firewall-cmd --add-port=1514/udp

sudo firewall-cmd --add-port=1514/udp --permanent

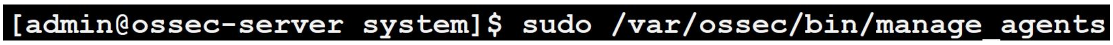


```
[admin@ossec-server system]$ sudo firewall-cmd --add-port=1514/udp
success
[admin@ossec-server system]$ sudo firewall-cmd --add-port=1514/udp --per
manent
success
```

Add agent to Server

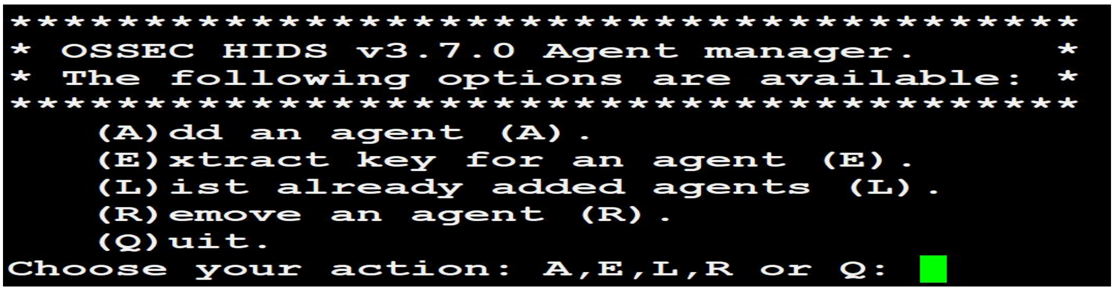
Go to the OSSEC Server and run following command

sudo   /var/ossec/bin/manage_agents



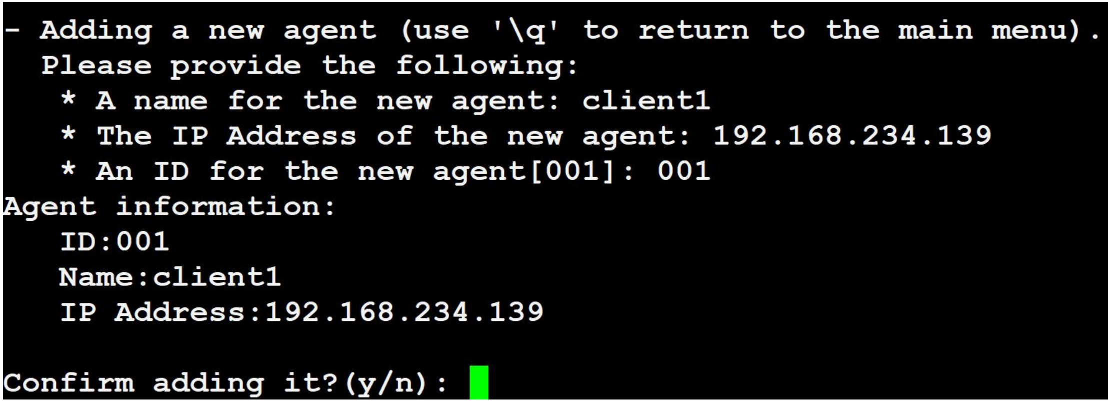
```
[admin@ossec-server system]$ sudo /var/ossec/bin/manage_agents
```

This will display following screen.



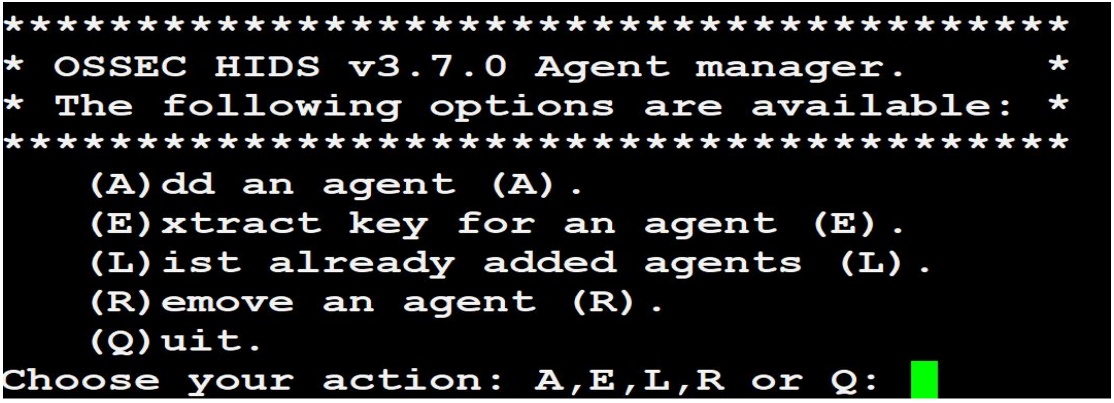
```
****************************************
* OSSEC HIDS v3.7.0 Agent manager.     *
* The following options are available: *
****************************************
   (A)dd an agent (A).
   (E)xtract key for an agent (E).
   (L)ist already added agents (L).
   (R)emove an agent (R).
   (Q)uit.
Choose your action: A,E,L,R or Q:
```

Type A as you want to add an agent. It will prompt to enter a name for the new agent. Type the name. Then it will ask the IP address of the client. Type IP address if client IP address is fixed. Else you can type any. Next you need to provide an ID for the agent. Each agent needs to get a unique ID. As this is the first agent we assign 001. This is as shown below.



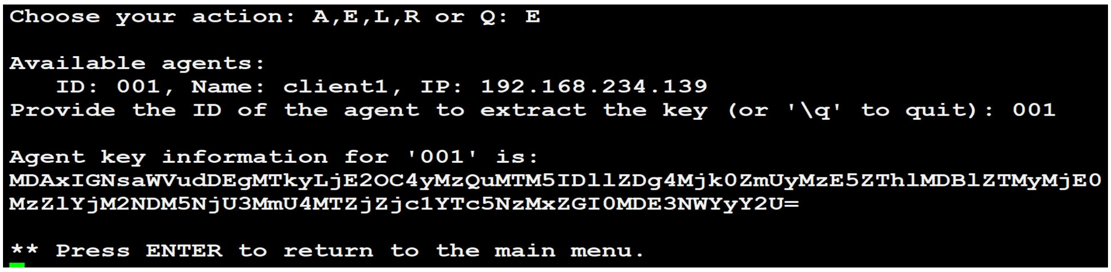
```
- Adding a new agent (use '\q' to return to the main menu).
  Please provide the following:
   * A name for the new agent: client1
   * The IP Address of the new agent: 192.168.234.139
   * An ID for the new agent[001]: 001
Agent information:
   ID:001
   Name:client1
   IP Address:192.168.234.139

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

Type y to confirm the agent addtion.
Again following screen is displayed.



```
****************************************
* OSSEC HIDS v3.7.0 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:
```

Now you need a key which you have to give to the client so that it can connect to the OSSEC server. Thus type E to Extract key for an agent. It will display agents added to the server. Type ID of the agent for which you want to extract the key. Here we have only one agent with ID 001.



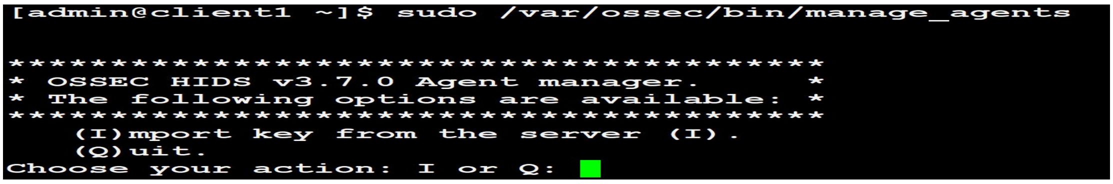
```
Choose your action: A,E,L,R or Q: E

Available agents:
   ID: 001, Name: client1, IP: 192.168.234.139
Provide the ID of the agent to extract the key (or '\q' to quit): 001

Agent key information for '001' is:
MDAxIGNsaWVudDEgMTkyLjE2OC4yMzQuMTM5IDllZDg4Mjk0ZmUyMzE5ZThlMDBlZTMyMjE0
MzZlYjM2NDM5NjU3MmU4MTZjZjc1YTc5NzMxZGI0MDE3NWYyY2U=

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

Press Enter. Then type Q to quit the utility.

Copy the key Displayed.

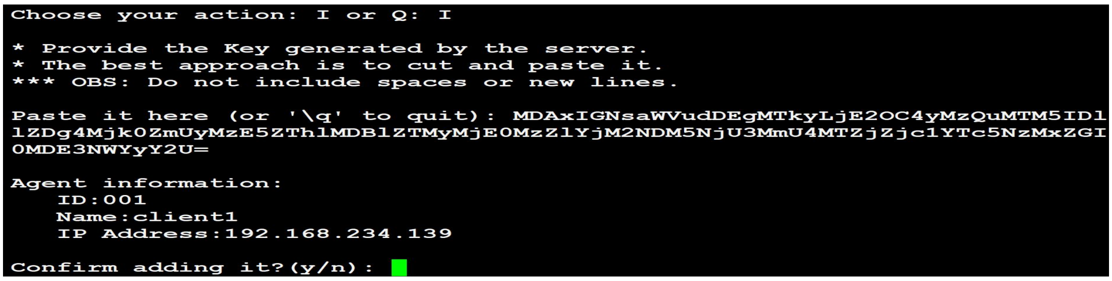
No go to the client1 computer.
Run the same above command.

sudo /var/ossec/bin/manage_agents



```
[admin@client1 ~]$ sudo /var/ossec/bin/manage_agents

****************************************
* OSSEC HIDS v3.7.0 Agent manager.     *
* The following options are available: *
****************************************
   (I)mport key from the server (I).
   (Q)uit.
Choose your action: I or Q: 
```

The above screen is displayed. Press I to Import key from server. Then paste the key generated on the server.
The following screen will be displayed.

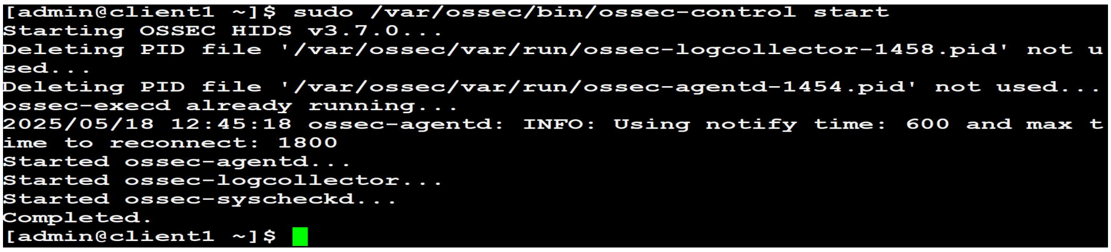


```
Choose your action: I or Q: I

* 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): MDAxIGNsaWVudDEgMTkyLjE2OC4yMzQuMTM5IDl
lZDg4Mjk0ZmUyMzE5ZThlMDBlZTMyMjE0MzZlYjM2NDM5NjU3MmU4MTZjZjc1YTc5NzMxZGI
0MDE3NWYyY2U=

Agent information:
   ID:001
   Name:client1
   IP Address:192.168.234.139

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

Type y to confirm. Press Enter to continue. Type Q to quit the utility.

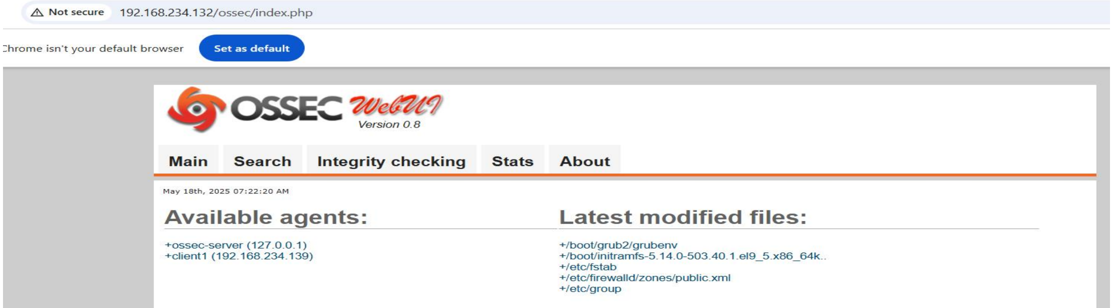
Now start the OSSEC Service.

sudo /var/ossec/bin/ossec-control start



```
[admin@client1 ~]$ sudo /var/ossec/bin/ossec-control start
Starting OSSEC HIDS v3.7.0...
Deleting PID file '/var/ossec/var/run/ossec-logcollector-1458.pid' not u
sed...
Deleting PID file '/var/ossec/var/run/ossec-agentd-1454.pid' not used...
ossec-execd already running...
2025/05/18 12:45:18 ossec-agentd: INFO: Using notify time: 600 and max t
ime to reconnect: 1800
Started ossec-agentd...
Started ossec-logcollector...
Started ossec-syscheckd...
Completed.
[admin@client1 ~]$ 
```

Wait for 2 to 3 minutes. Now go to the OSSEC Server web interface. Refresh the page if it is already open. The client should be shown as below.



May 18th, 2025 07:22:20 AM

Available agents:

+ossec-server (127.0.0.1)
+client1 (192.168.234.139)

Latest modified files:

+/boot/grub2/grubenv
+/boot/initramfs-5.14.0-503.40.1.el9_5.x86_64k..
+/etc/fstab
+/etc/firewalld/zones/public.xml
+/etc/group

If the client is not displayed then restart the OSSEC service on the server using

sudo systemctl restart ossec.

Configure OSSEC as a Service on the client.

For this, create a file in the /usr/lib/systemd/system directory by the name of the service. The extension of the file should be .service.

```
sudo  vi  /usr/lib/systemd/system/ossec.service
```

Type following in the file.

```
[Unit]
Description=OSSEC service

[Service]
Type=forking
ExecStart=/var/ossec/bin/ossec-control start
ExecStop=/var/ossec/bin/ossec-control stop
ExecRestart=/var/ossec/bin/ossec-control restart
[Install]
WantedBy=multi-user.target
```

Save the file.

```
sudo  yum install chkconfig   -y
```

Stop the OSSEC service.

```
sudo   /var/ossec/bin/ossec-control stop
```

Now start the service with

```
sudo systemctl  start ossec
```

Enable the service for the auto start.

```
sudo  systemctl  enable  ossec
```

This is how you have installed the OSSEC server and added an agent to it. Follow the same procedure to add other agents.