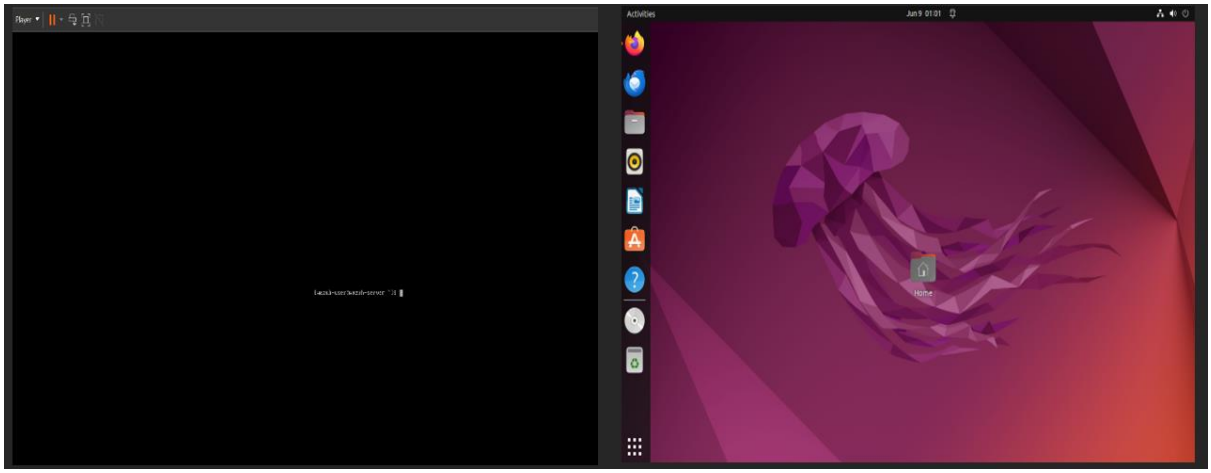
File integrity monitoring

File Integrity Monitoring (FIM) helps in auditing sensitive files and meeting regulatory compliance requirements. Wazuh has an inbuilt FIM module that monitors file system changes to detect the creation, modification, and deletion of files.

This use case uses the Wazuh FIM module to detect changes in monitored directories on Ubuntu and Windows endpoints. The Wazuh FIM module enriches alert data by fetching information about the user and process that made the changes using who-data audit.

In this lab, I am going to test the file integrity in Linux Instance.

As shown below, I have launched both my Wazuh and Linux instances up and alive

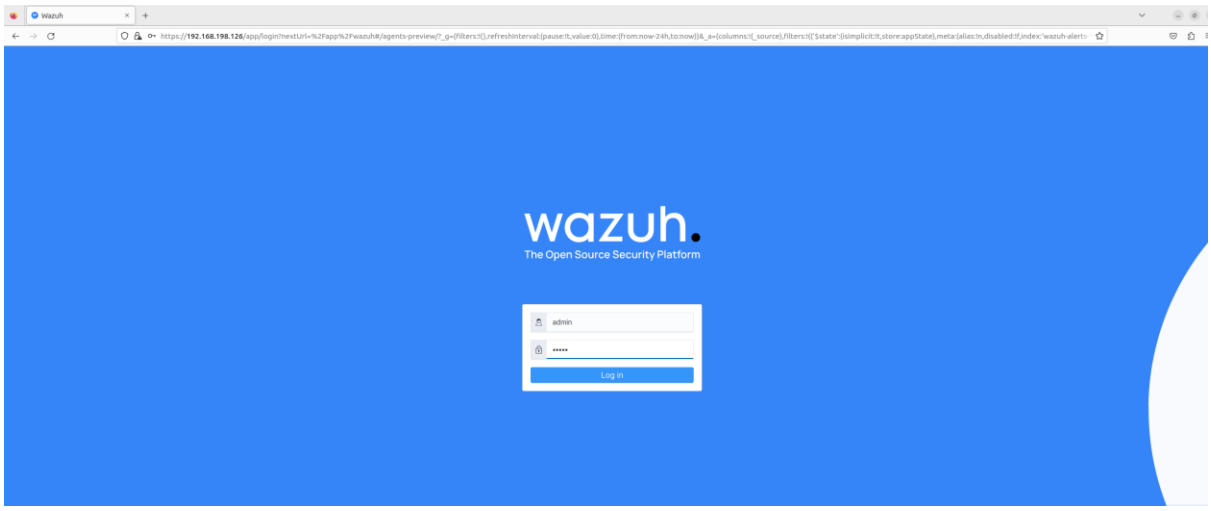


I have logged into the dashboard in LInux instance

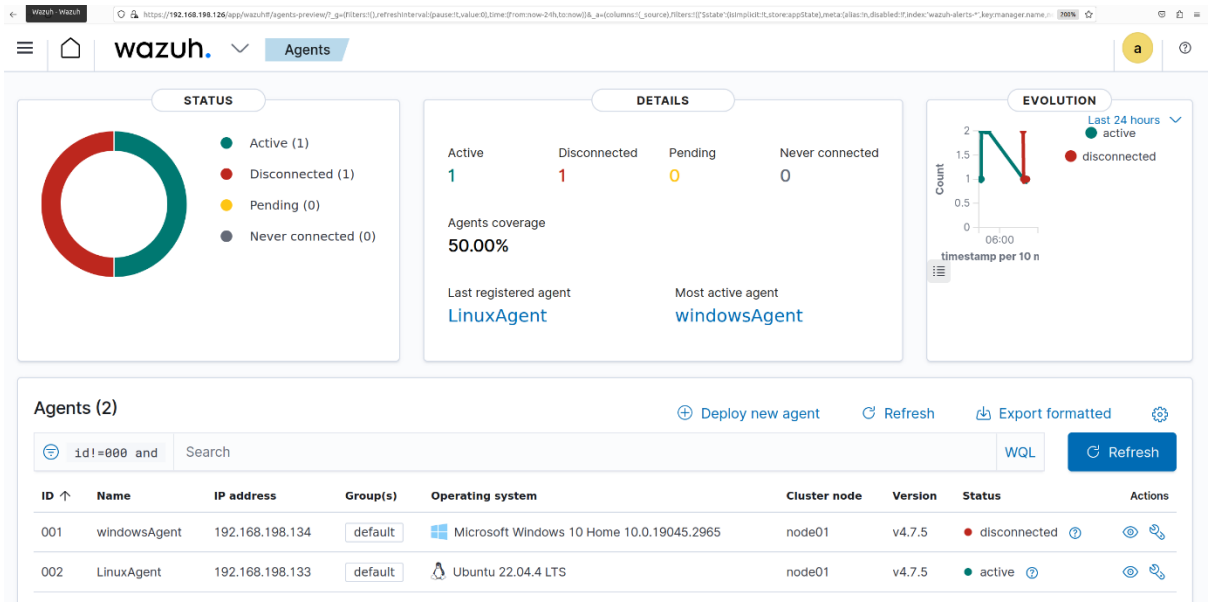
https://your-wazuh-IP

paste this URL in any web browser

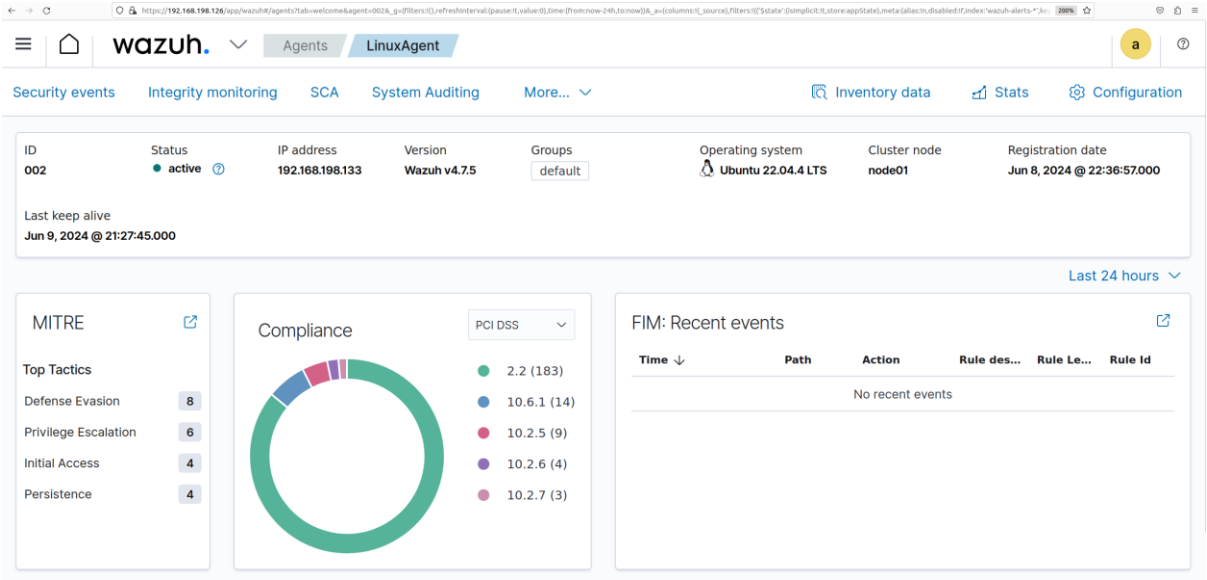
You can see, in my case, I have two Agents already been registered. Since, I have booted only my Linux instance, its showing Active agents as “1”.



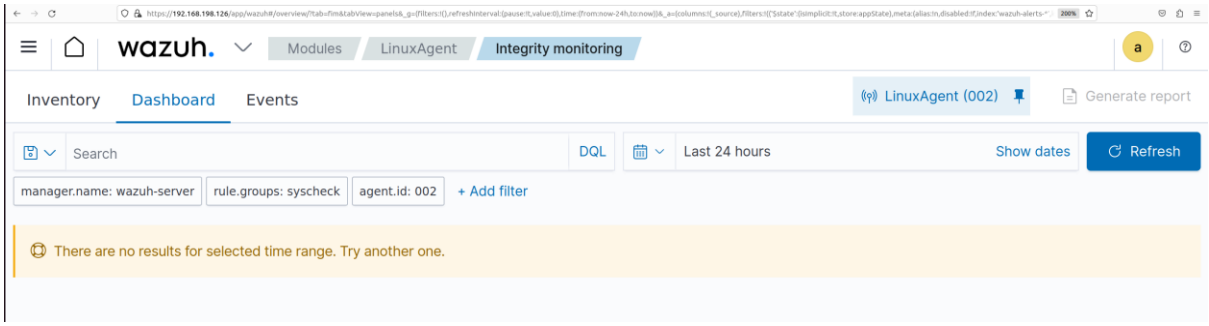
Now, click on “Agents”



Next click on the instance that is being shown. in my case its “LinuxAgent”



Then, click on “integrity monitoring”. Now, you can see that there were no data found.
in order to configure it



Go, to root mode and follow this path.

cd /var/ossec/etc/

```
root@project01-virtual-machine:/# cd var
root@project01-virtual-machine:/var# ls
backups  cache  crash  lib  local  lock  log  mail  metrics  opt  ossec  run  snap  spool  tmp
root@project01-virtual-machine:/var# cd ossec
root@project01-virtual-machine:/var/ossec# cd etc
root@project01-virtual-machine:/var/ossec/etc# ls
client.keys  internal_options.conf  local_internal_options.conf  localtime  ossec.conf  shared  wpk_root.pem
root@project01-virtual-machine:/var/ossec/etc# nano ossec.conf
```

nano ossec.conf, after opening that file, search for File Integrity monitoring section,

```
 GNU nano 6.2                                    ossec.conf

<!-- 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>

  <!-- 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>

^G Help          ^O Write Out     ^W Where Is      ^K Cut           ^T Execute       ^C Location      M-U Undo
^X Exit          ^R Read File     ^\ Replace       ^U Paste         ^J Justify       ^/ Go To Line    M-E Redo
```

Next, add this line at the end of that section

Command :

<directories check_all="yes" whodata="yes">path-to-your-directory-where-you-store-files </directories>

```
<!-- 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>

  <!-- Directories to check  (perform all possible verifications) -->
  <directories>/etc,/usr/bin,/usr/sbin</directories>
  <directories>/bin,/sbin,/boot</directories>
  <directories check_all="yes" whodata="yes">/home/project-01/Downloads</directories>
```

In my case, I have given my downloads path {/home/project-01/Downloads}

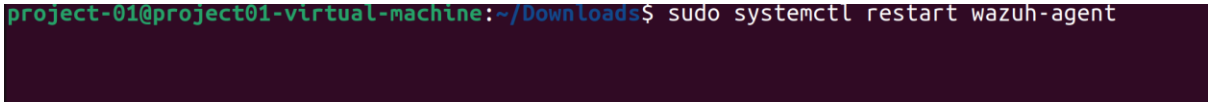
To know your path, go to your command line

```
project-01@project01-virtual-machine:~/Downloads$ pwd
/home/project-01/Downloads
project-01@project01-virtual-machine:~/Downloads$
```

After making changes, don’t forget to restart your Wazuh agent, for that you can use the command

Command:

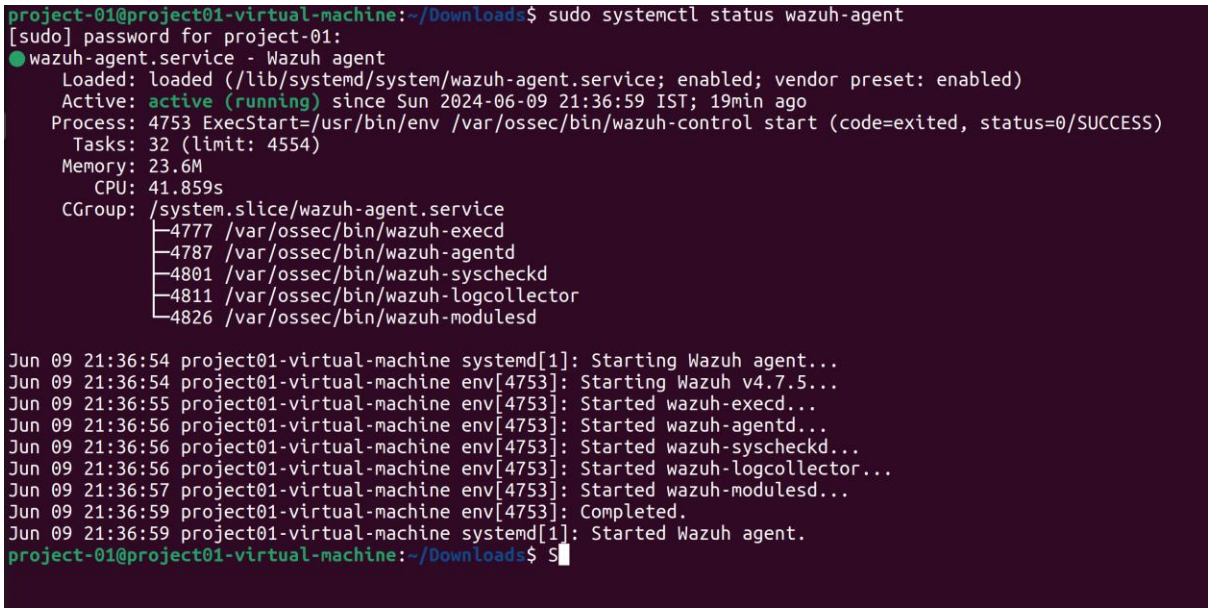
sudo systemctl restart Wazuh-agent



Now, check your Wazuh-agent status, by following this command

Command:

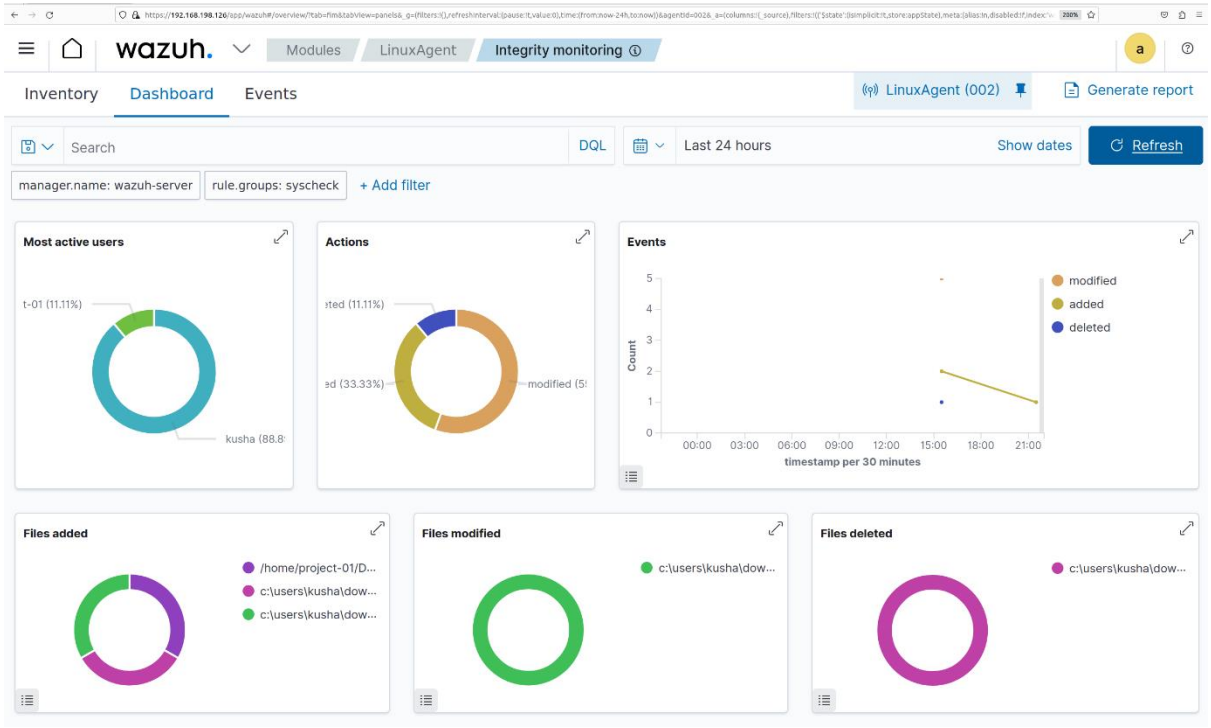
Sudo systemctl status Wazuh-agent



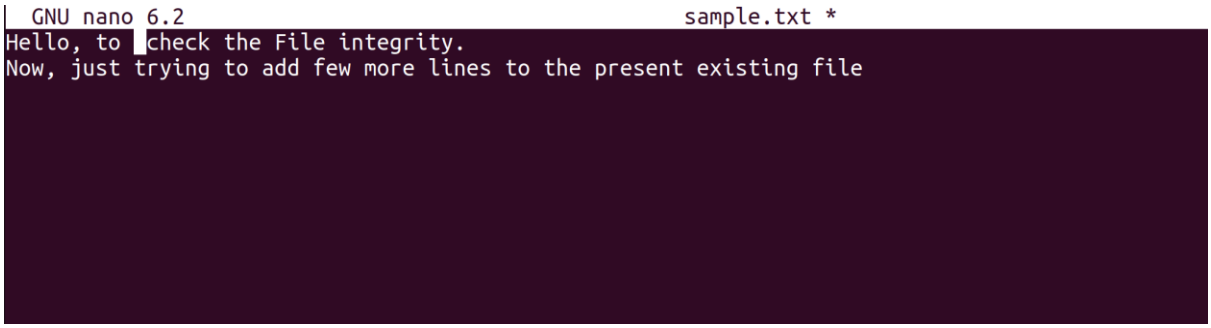
Since, its active, then everything is good to go.

Now, try to create a .txt file in the Downloads folder and add give some input to it.

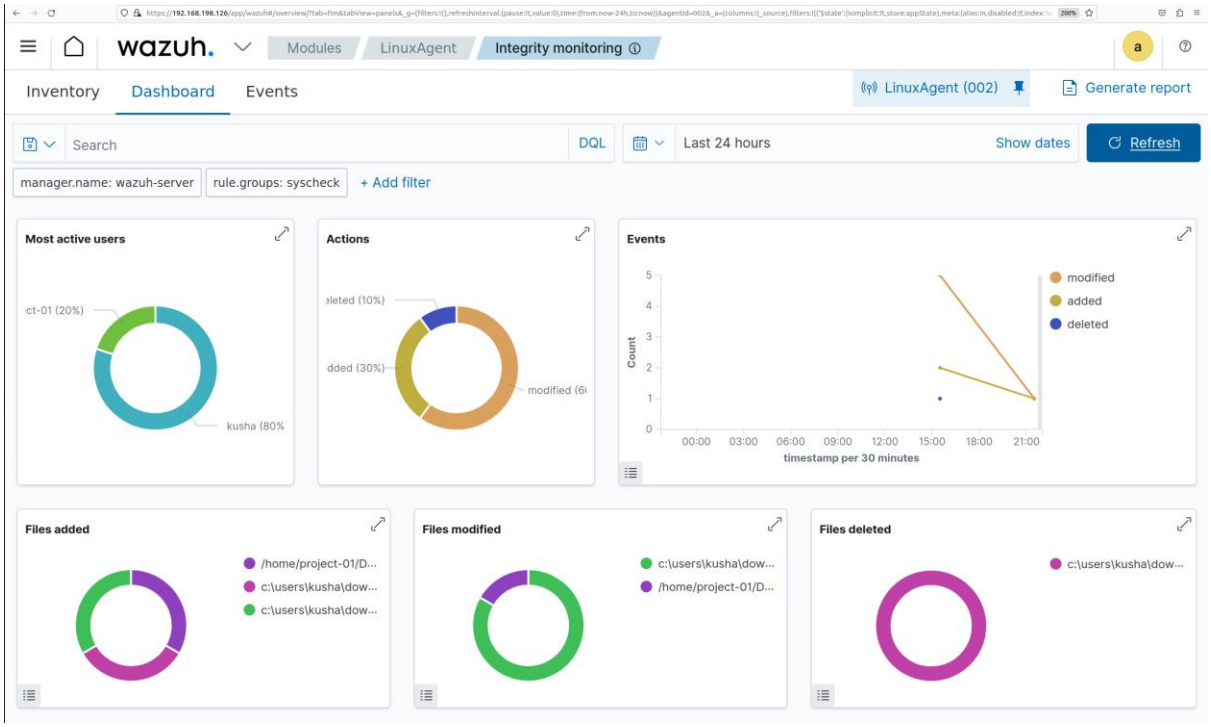
Now, access your Wazuh dashboard and just try to refresh it, you can see that the information has been updated

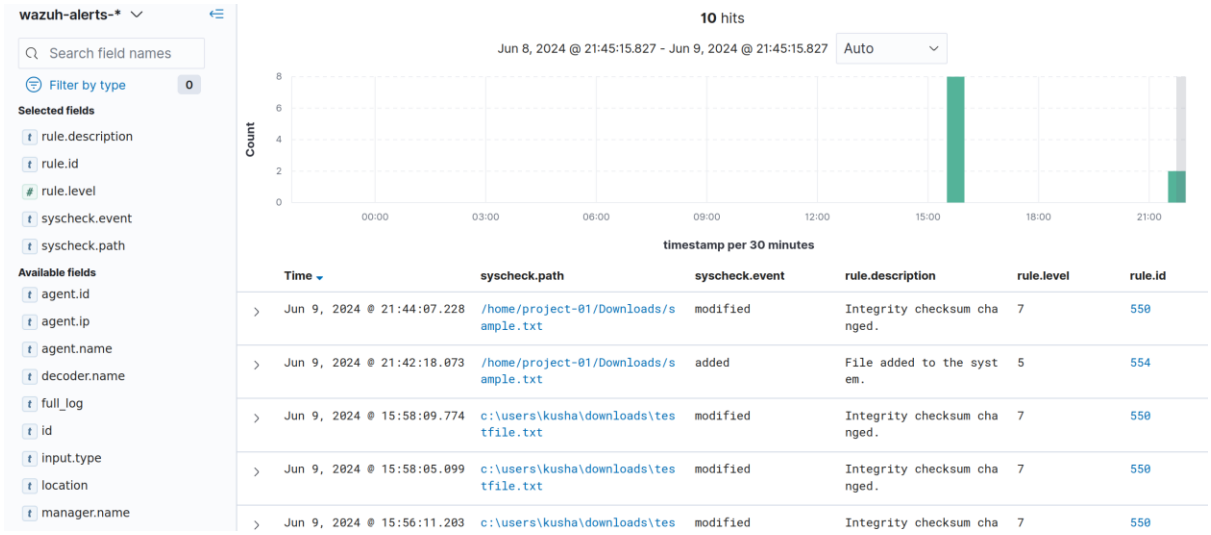


Now, try to modify the information in previous created .txt file



Now, try to access you Wazuh-dashboard and try to refresh it and this time you see a different graphs


wazuh.
Modules
LinuxAgent
Integrity monitoring
Inventory
Dashboard
Events
LinuxAgent (002)
Generate report
Search
DQL
Last 24 hours
Show dates
Refresh
manager.name: wazuh-server
rule.groups: syscheck
+ Add filter
Most active users
kusha (80%
Actions
modified (6
Events
modified
added
deleted
Count
timestamp per 30 minutes
Files added
/home/project-01/D...
c:\users\kusha\dow...
Files modified
Files deleted


wazuh-alerts-*
Search field names
Filter by type
Selected fields
rule.description
rule.id
rule.level
syscheck.event
syscheck.path
Available fields
agent.id
agent.ip
agent.name
decoder.name
full_log
id
input.type
location
manager.name
10 hits
Jun 8, 2024 @ 21:45:15.827 - Jun 9, 2024 @ 21:45:15.827
Auto
Count
timestamp per 30 minutes
Time
syscheck.path
syscheck.event
rule.description
rule.level
rule.id
Jun 9, 2024 @ 21:44:07.228
/home/project-01/Downloads/sample.txt
modified
Integrity checksum changed.
7
550
Jun 9, 2024 @ 21:42:18.073
/home/project-01/Downloads/sample.txt
added
File added to the system.
5
554
Jun 9, 2024 @ 15:58:09.774
c:\users\kusha\downloads\testfile.txt
modified
Integrity checksum changed.
7
550
Jun 9, 2024 @ 15:58:05.099
c:\users\kusha\downloads\testfile.txt
modified
Integrity checksum changed.
7
550
Jun 9, 2024 @ 15:56:11.203
c:\users\kusha\downloads\tes
modified
Integrity checksum cha
7
550