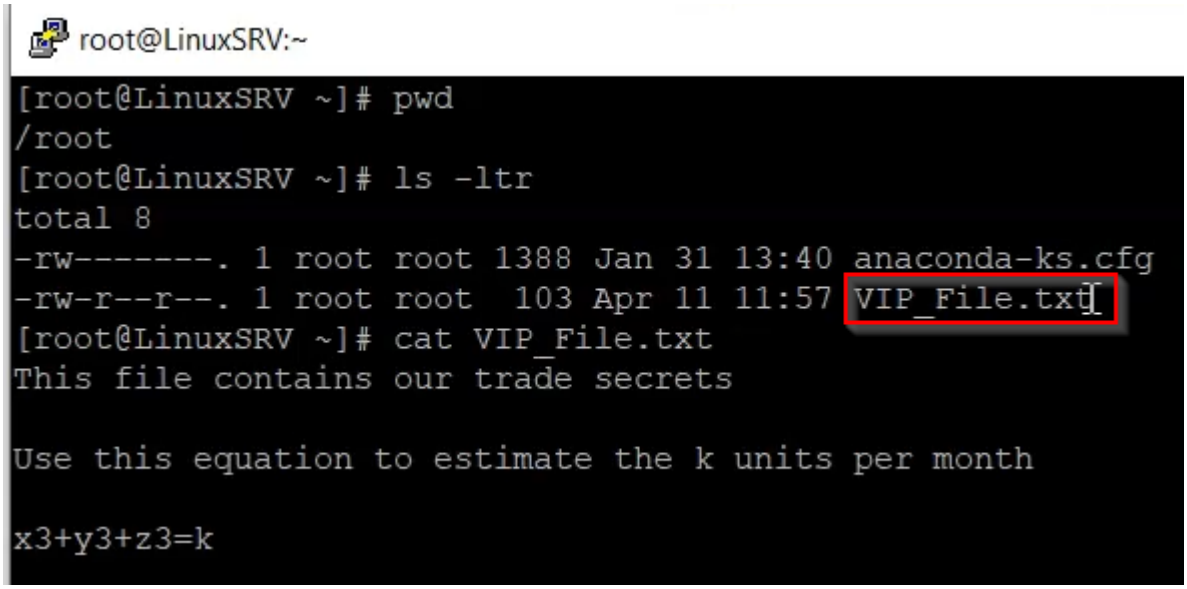
- let's do some attack simulation against some file that contains important information (let's say, it is stored in the linux server)



- lets assume `VIP_File.txt` file contains some trade secret for one company
- so basically we need to have a way or some capability to detect if the file has been tampered with
- previously we have installed windows agent, here we will do the linux agent installation, this will allow us to enable FIM (File Integrity Monitoring) capability where we can detect such attack.
- thanks to FortiSIEM which comes with built in rules that can detect or check for events coming from the FortiSIEM agent where some files has been tampered with or some attributes has been changed in some file system.
- first thing is to install the FortiSIEM linux agent on linux server

Linux Agent Installation

```
Prerequisites
_____________
1/ OS supported: CentOS/RHEL>7.4 and other linux flavors
2/ curl>7.19.7 & nss>3.36.0 otherwise >> yum update -y nss curl lib curl
3/ validate rsyslog >> systemctl status rsyslog.service >> if not
running >> systemctl start rsyslog.service
4/ Make sure timzone is ok on the Linux machine >> timedatectl set-
timezone Asia/Qatar
```

5/ The following packages must be installed (yum install <package_name>) before FortiSIEM Linux Agents can run on CentOS/RHEL:

libcap
audit
audispd-plugins
rsyslog
logrotate
If SELinux is enabled (sestatus), then the following packages also must be installed:
policycoreutils
libselinux-utils
setools-console

Install/Start/Configure the Agent

1/ Download the Linux installation script from Fortinet Support website support.fortinet.com and upload it using WinSCP
2/ chmod +x fortisiem-linux-agent-installer-6.6.0.1633.sh
3/ Run the command: bash fortisiem-linux-agent-installer—<VERSION>.sh -s <SUPER_IP> -i <ORG_ID> -o <ORG_NAME> -u <AGENT_USER> -p <AGENT_PWD> -n <HOST_NAME>
bash fortisiem-linux-agent-installer-6.6.0.1633.sh -s 192.168.100.155 -i 1 -o super -u lnxusr -p P@ssword@123 -n LinuxSRV
4/ Start the agent: /usr/bin/sh -c /opt/fortinet/fortisiem/linux-agent/bin/phLinuxAgent &
5/ Define the template and assign to host
6/ If File Integrity monitoring is chosen, validate the SElinux context
ls -Z >> validate SE context is var_log_t >> or change >> chcon system_u:object_r:var_log_t:s0 VIP_File.txt

Log Rotation

https://docs.fortinet.com/document/fortisiem/6.6.3/linux-agent-installation-guide/201446/fortisiem-linux-agent#Log_Rotating__var_log_messages_to_Prevent_Filling_Up_the_Root_Disk

UnInstall the Agent

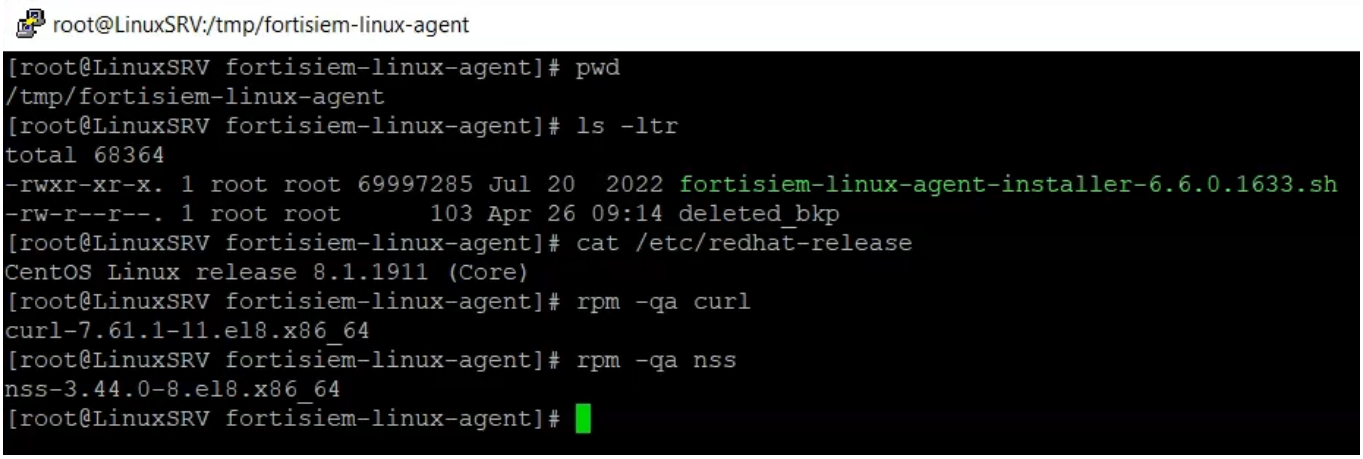
/opt/fortinet/fortisiem/linux-agent/bin/fortisiem-linux-agent-uninstall.sh

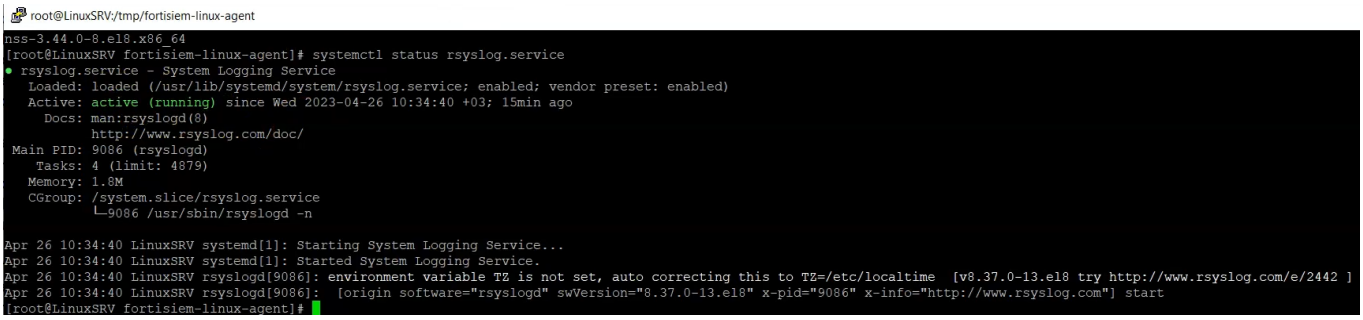
Sources

https://docs.fortinet.com/document/fortisiem/6.7.3/linux-agent-

installation-guide/201446/fortisiem-linux-agent
https://help.fortinet.com/fsiem/6-6-0/Online-Help/HTML5_Help/Configuring_Linux_Agent.htm
https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/selinux_users_and_administrators_guide/sect-security-enhanced_linux-working_with_selinux-selinux_contexts_labeling_files
https://unix.stackexchange.com/questions/79311/configuring-selinux-to-allow-logging-to-a-file-thats-outside-var-log
https://docs.fortinet.com/document/fortisiem/6.6.3/linux-agent-installation-guide/201446/fortisiem-linux-agent#Managing

- check the prerequisites





- also check if SELinux is enabled (sestatus)

```
[root@LinuxSRV fortisiem-linux-agent]# sestatus
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             targeted
Current mode:                   enforcing
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Memory protection checking:     actual (secure)
Max kernel policy version:      31
[root@LinuxSRV fortisiem-linux-agent]#
```

- while installing the linux agent, we need to create the agent user in the `FortiSIEM` > `CMDB > Users > New`
  - make sure `System Admin` checkbox is checked and inside that select `Agent Admin` and put username and password
- retrieve server name from the linux server and then install

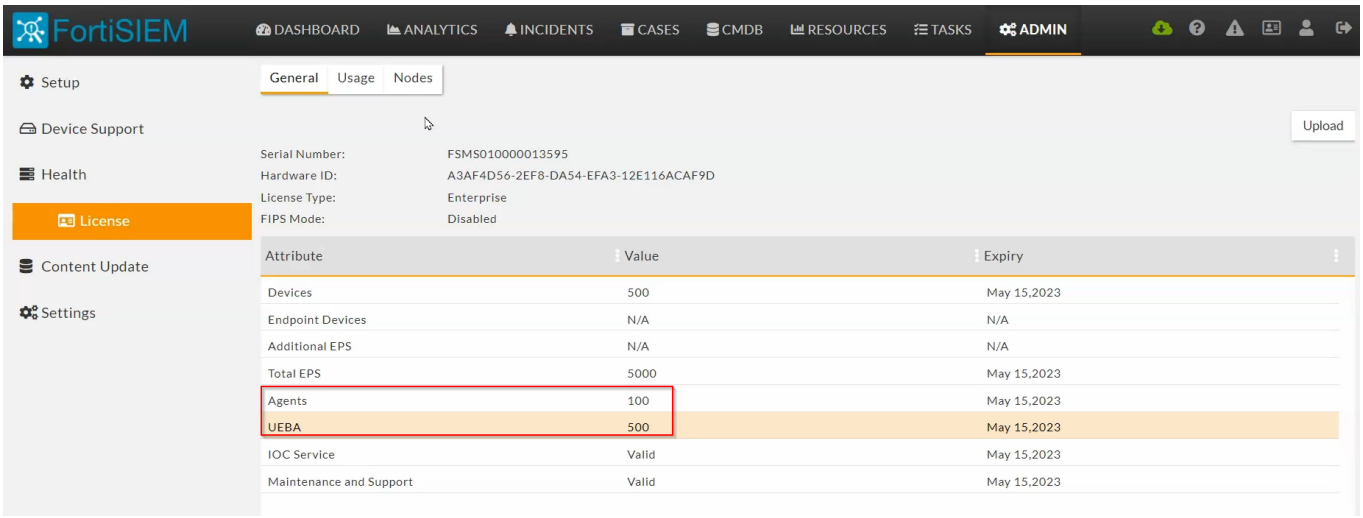
```
[root@LinuxSRV fortisiem-linux-agent]# ls -ltr
total 68364
-rwxr-xr-x. 1 root root 69997285 Jul 20  2022 fortisiem-linux-agent-installer-6.6.0.1633.sh
-rw-r--r--. 1 root root      103 Apr 26 09:14 deleted_bkp
[root@LinuxSRV fortisiem-linux-agent]# bash fortisiem-linux-agent-installer-6.6.0.1633.sh -s 192.168.100.155 -i 1 -o super -u lnxusr -p P@ssword@123 -n LinuxSRV
Checking Connectivity to Server ... 192.168.100.155
Supervisor at 192.168.100.155 is reachable. Continuing with installation...
Agent parameters validated successfully
 SUPER_IP:192.168.100.155
 CUSTOMER_ID:1
 CUSTOMER_NAME:super
 AGENT_REG_USERNAME:lnxusr
 AGENT_REG_PASSWORD:P@ssword@123
 PROXY_SERVER_IP:
 PROXY_SERVER_PORT:
 SSL_VERIFY_PEER:false
 SSL_CA_CERT_FILE:/etc/pki/tls/certs/ca-bundle.crt
 HOST_NAME:LinuxSRV
 SSL_CA_CERT_PATH:
Executing command  systemctl start fortisiem-linux-agent.service
Executing command  systemctl enable fortisiem-linux-agent.service
Created symlink /etc/systemd/system/multi-user.target.wants/fortisiem-linux-agent.service → /etc/systemd/system/fortisiem-linux-agent.service.
Executing command  systemctl daemon-reload
service fortisiem-linux-agent status...
Redirecting to /bin/systemctl status fortisiem-linux-agent.service
● fortisiem-linux-agent.service - FortiSIEM Linux Agent daemon
   Loaded: loaded (/etc/systemd/system/fortisiem-linux-agent.service; enabled; vendor preset: disabled)
   Active: activating (auto-restart) (Result: exit-code) since Wed 2023-04-26 10:56:19 +03; 886ms ago
 Main PID: 10051 (code=exited, status=1/FAILURE)
    Tasks: 0 (limit: 4879)
   Memory: 0B
   CGroup: /system.slice/fortisiem-linux-agent.service
INSTALLATION SUCCESS, but service did not start.
Please check if the agent registration username or password is incorrect
Also please check for errors in the agent log here: /opt/fortinet/fortisiem/linux-agent/log/phoenix.log
[root@LinuxSRV fortisiem-linux-agent]#
```

- to start the service

```
/usr/bin/sh -c /opt/fortinet/fortisiem/linux-agent/bin/phLinuxAgent &
```

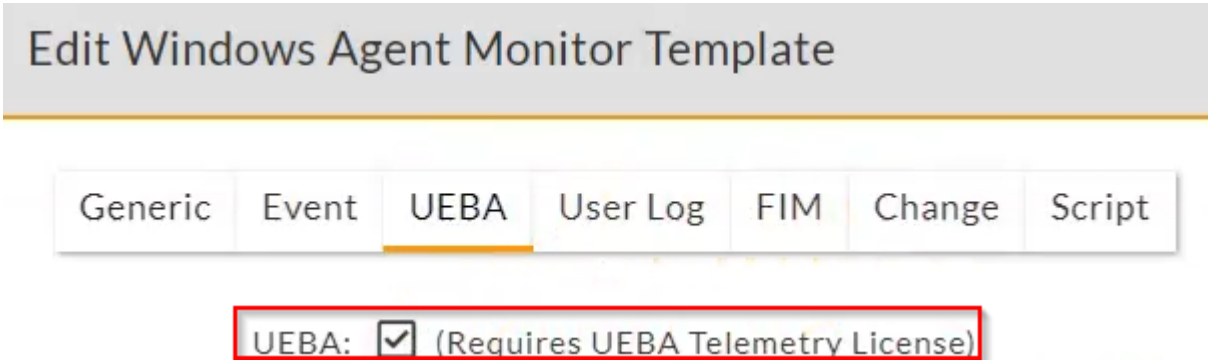
Note: info about license usage and regarding the agents

- you will see separate count for number of `Agents` and number of `UEBA`
- actually `UEBA` is a feature inside the `Agent`
  - it's a kernel level component that is being installed along with the same agent that you install

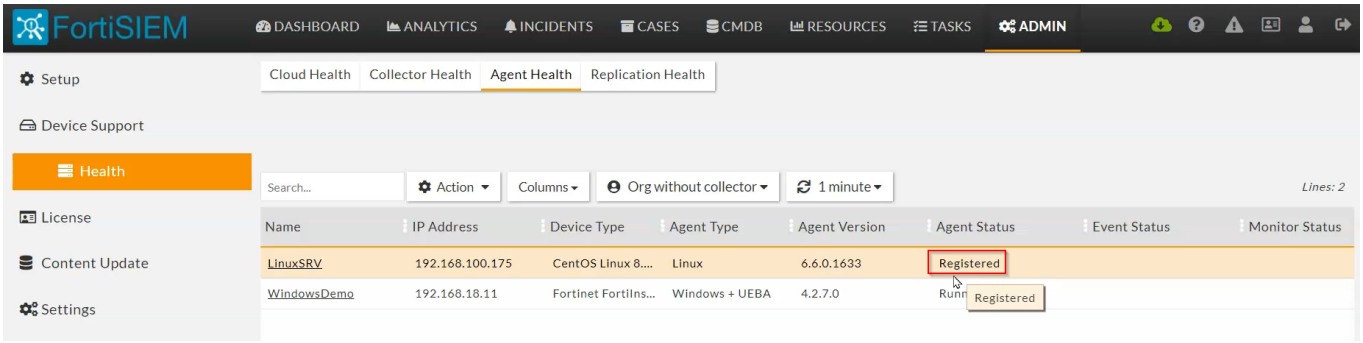


- here we can see the usage.

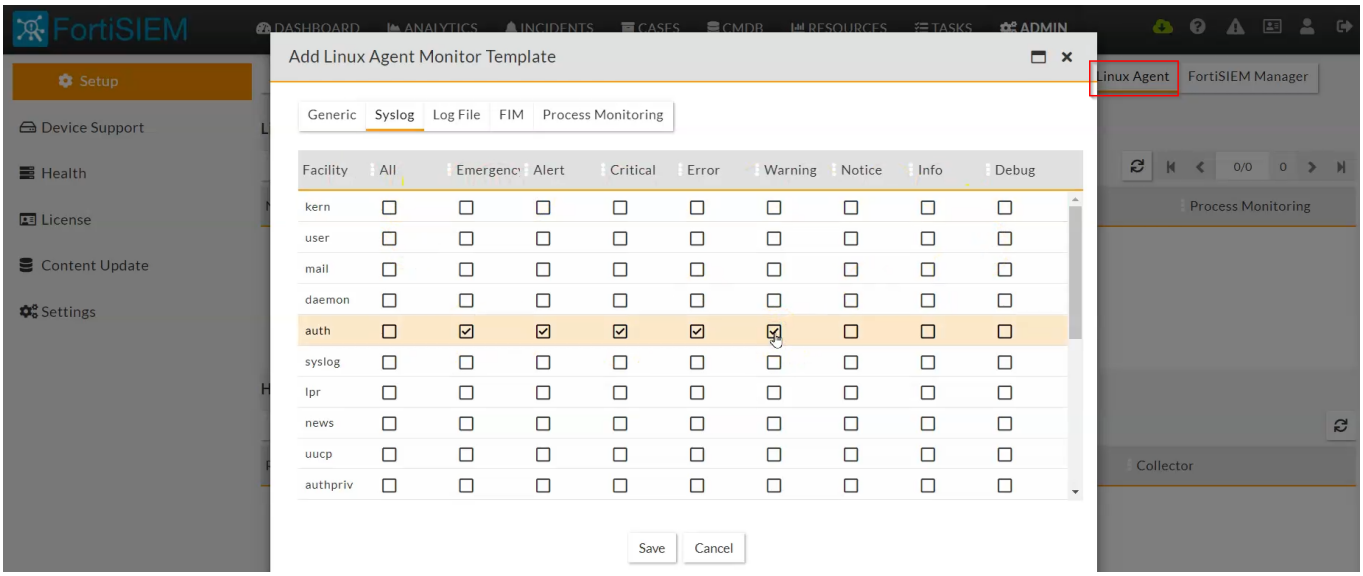
- why we have UEBA because, in the installing the windows agent we have checked the UEBA



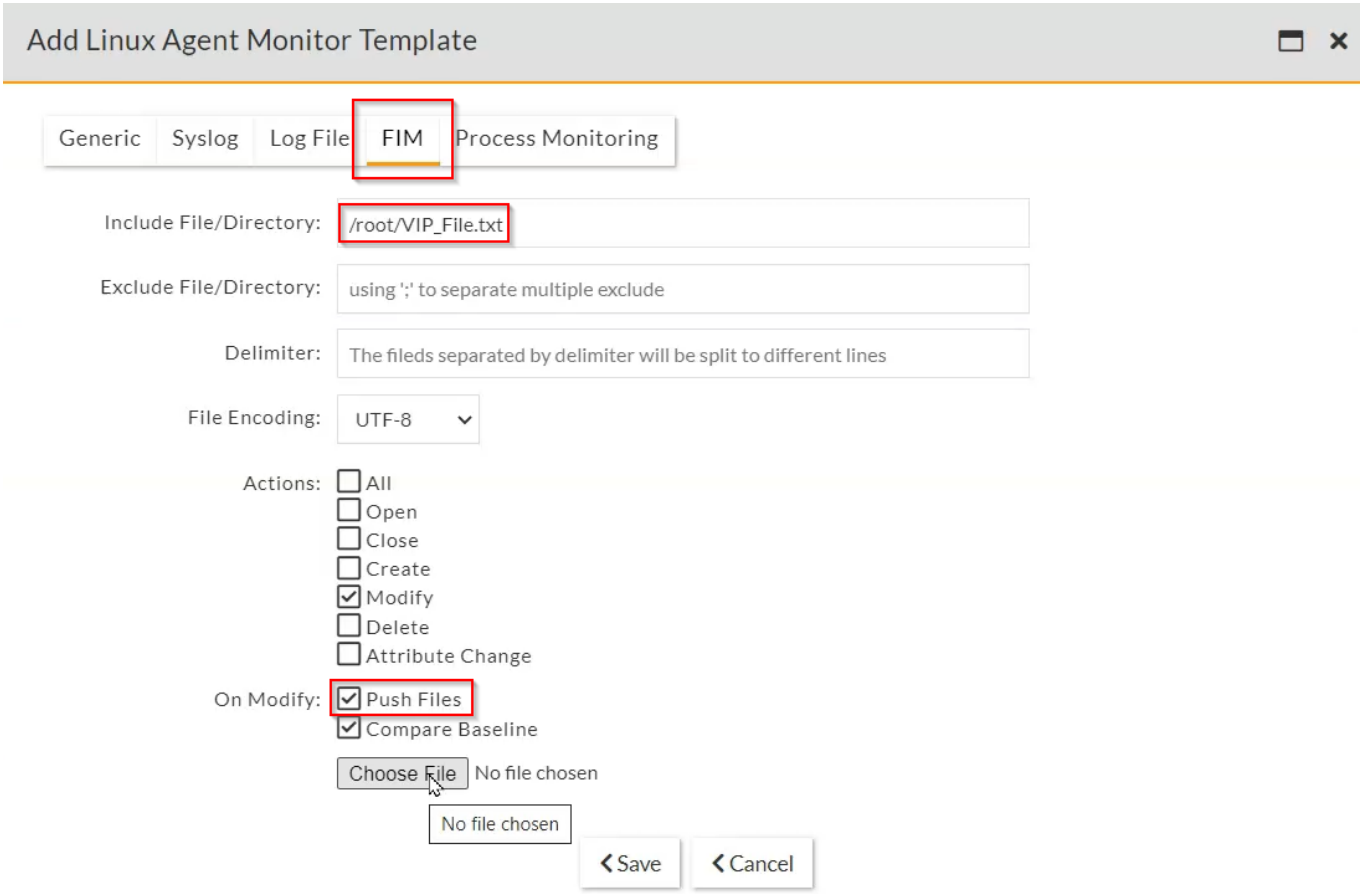
- this is how you can track your license usage
- now after successful installation of linux agent, its showing as `Registered`



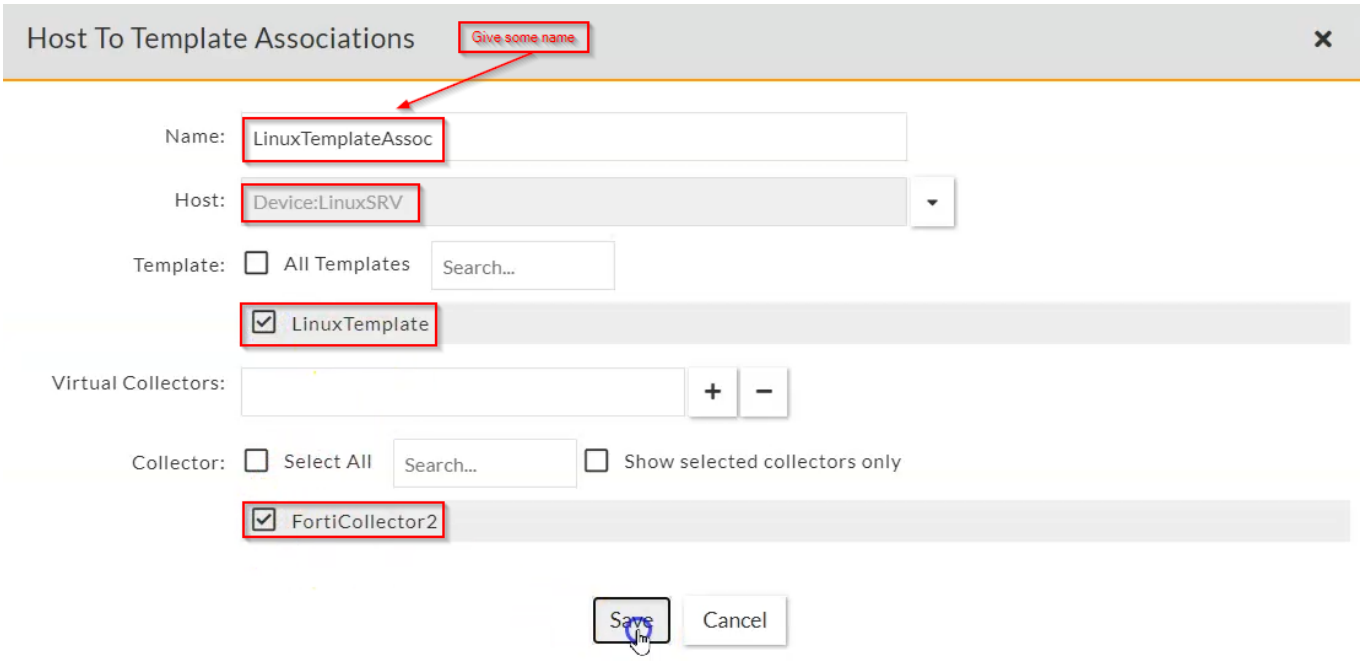
- to make it active (`Running Active`), we need to define the template



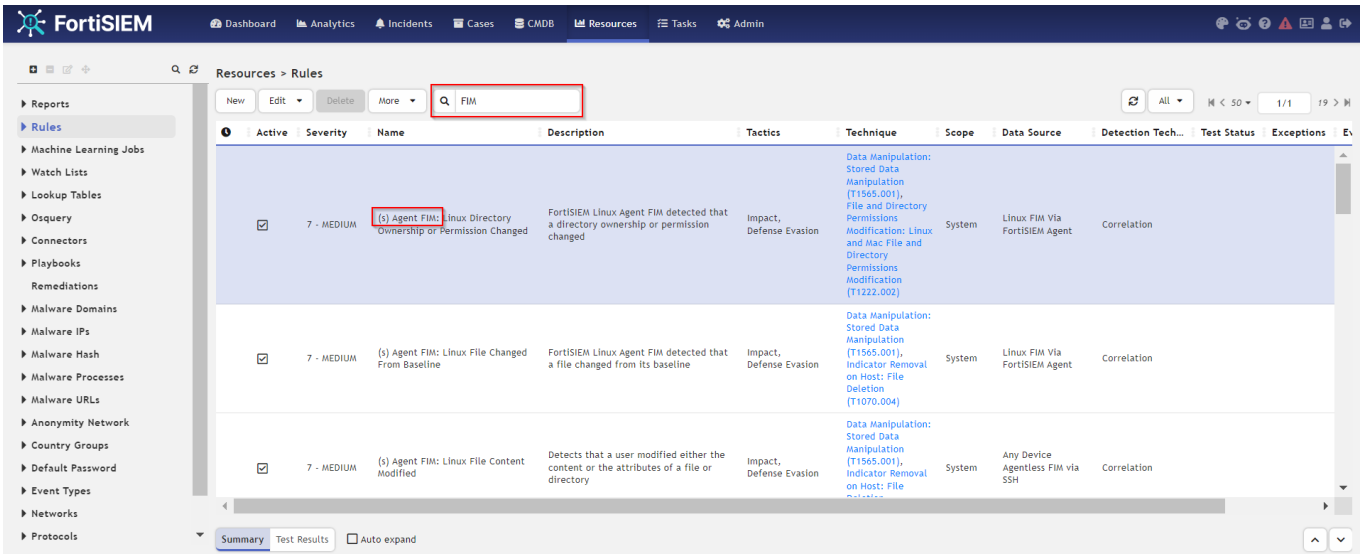
- in our case, we need to monitor important file (e.g., `VIP_File.txt`), include this in FIM
  - `Push Files` will push the metadata into FortiSIEM (actually stored in SVN database)



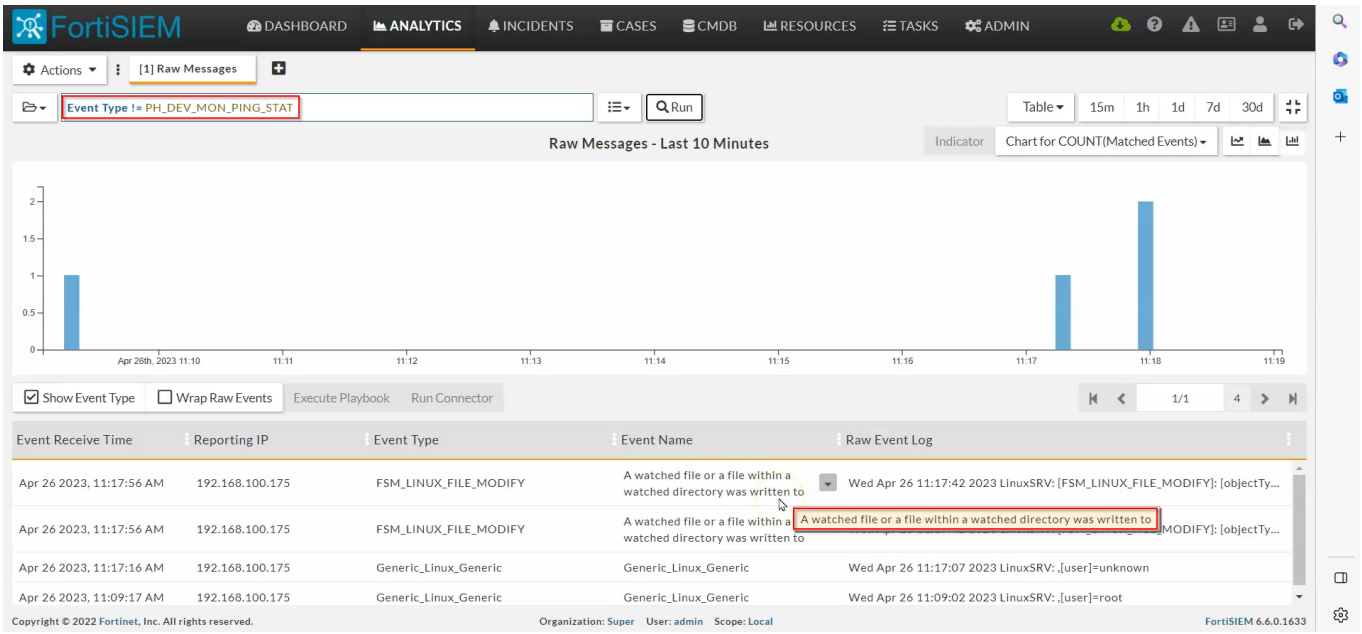
- then we need to associate this template into some host



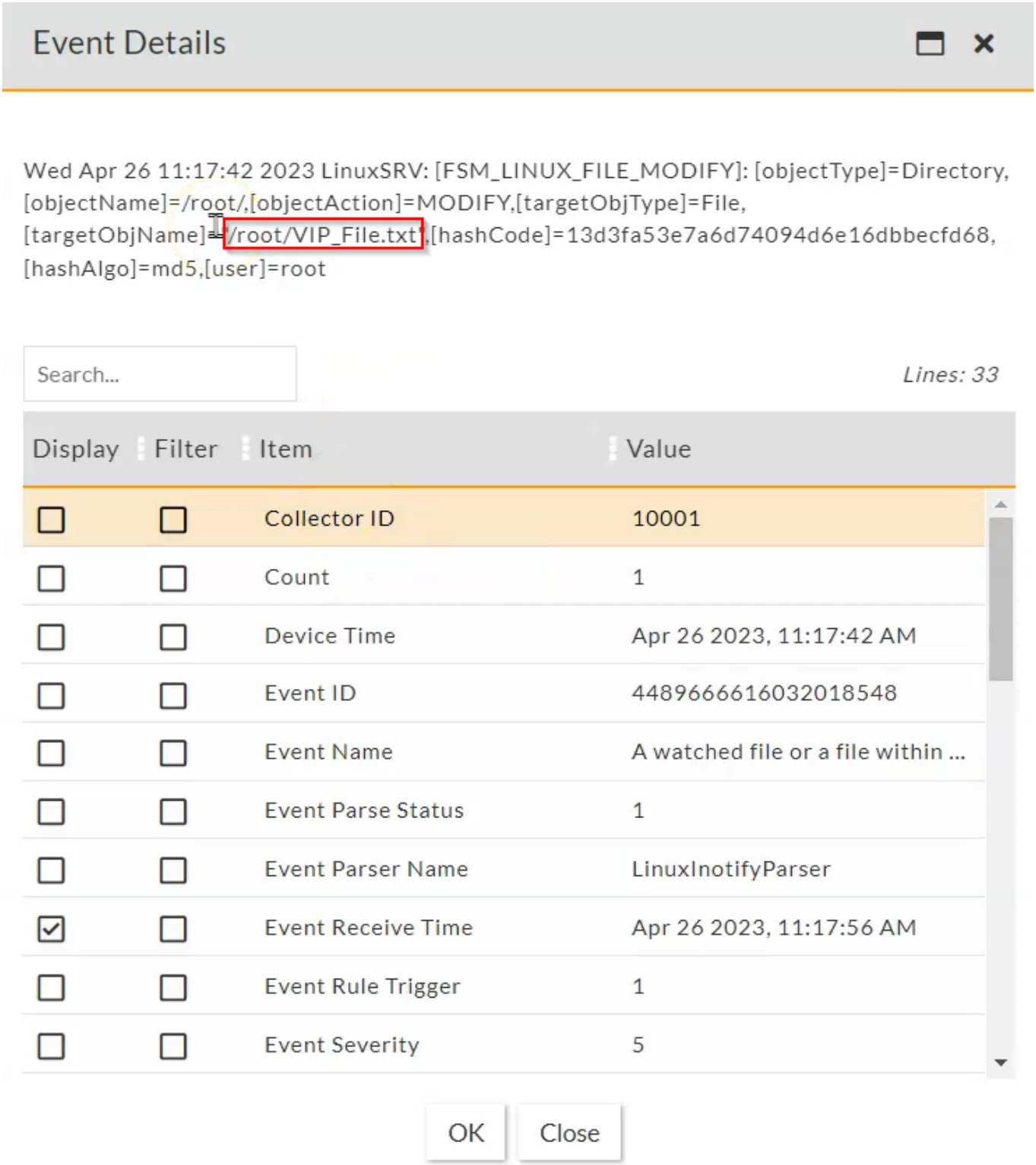
- and then apply, and then you can see `Running Active` in Health section in ADMIN panel
- let's check what are the built-in rules that can be useful to detect the modification attempt



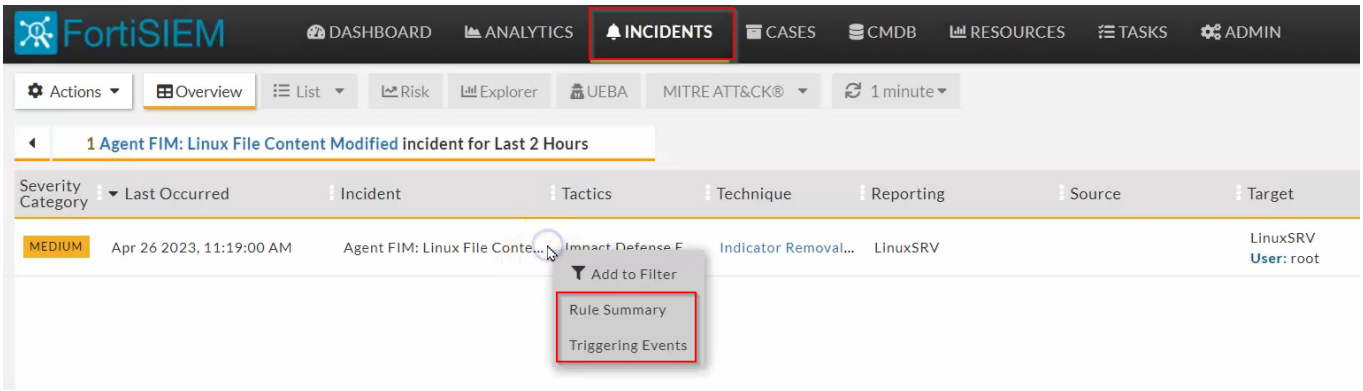
- let's see what exact rule will be triggered when we try to modify the file



- you can view detailed event in `Event Details`

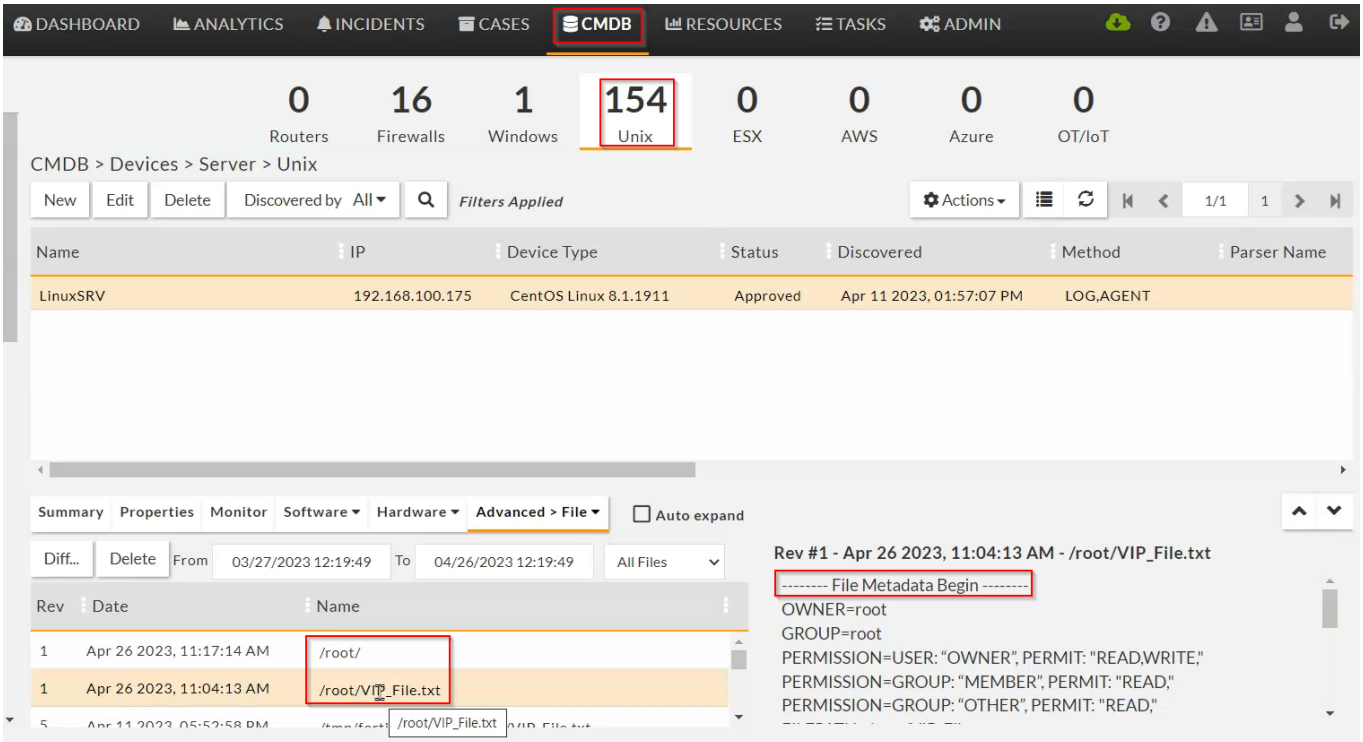


- you can also view details in `INCIDENTS` page in overview section



Note:

- One important capability of monitoring is that the ability to see the differences between the files being modified
- metadata of the files being modified is updated or uploaded to the SVN databases of the supervisors. so you can have the multiple revisions of the same file and you can compare between these revisions and pinpoint the changes that have occurred.
- you can also compare the metadata of the modified file against a master image. so you can also know what has been changed. to check this you have to check the record created of the host inside the CMDB database, from here you can check the file being modified in that host



- here we can see the modification in metadata. first we tried with file itself, the the file path
- you can select both and see the difference (useful when comparing two same files)

File Diff

	Rev #1 Apr 26 2023, 11:04:13 AM /root/VIP_File.txt		Rev #2 Apr 26 2023, 12:25:29 PM /root/VIP_File.txt
1	-------- File Metadata Begin --------	1	-------- File Metadata Begin --------
2	OWNER=root	2	OWNER=root
3	GROUP=root	3	GROUP=root
4	PERMISSION=USER: “OWNER”, PERMIT: "READ,WRITE,"	4	PERMISSION=USER: “OWNER”, PERMIT: "READ,WRITE,"
5	PERMISSION=GROUP: “MEMBER”, PERMIT: "READ,"	5	PERMISSION=GROUP: “MEMBER”, PERMIT: "READ,"
6	PERMISSION=GROUP: “OTHER”, PERMIT: "READ,"	6	PERMISSION=GROUP: “OTHER”, PERMIT: "READ,"
7	FILEPATH=/root/VIP_File.txt	7	FILEPATH=/root/VIP_File.txt
8	HASHCODE=80ce168f9b01063ff310cb20605efc3a	8	HASHCODE=5fb690dc2c9497534401d7605db1135c
9	HASHALGO=MD5	9	HASHALGO=MD5
10	MODIFIED_TIME=2023-04-26T08:04:10Z	10	MODIFIED_TIME=2023-04-26T09:25:20Z
11	-------- File Metadata End --------	11	-------- File Metadata End --------
12	This file contains our trade secrets	12	This file contains our trade secrets
13		13	
14	Use this equation to estimate the k units per month	14	Use this equation to estimate the k units per month
15		15	
16	x3+y3+z3=k	16	4*x3+3*y3+2*z3=k
17		17	
18		18	
19		19	

Top Bottom Previous Next Close

- this is the importance of FIM (File Integrity Monitoring)