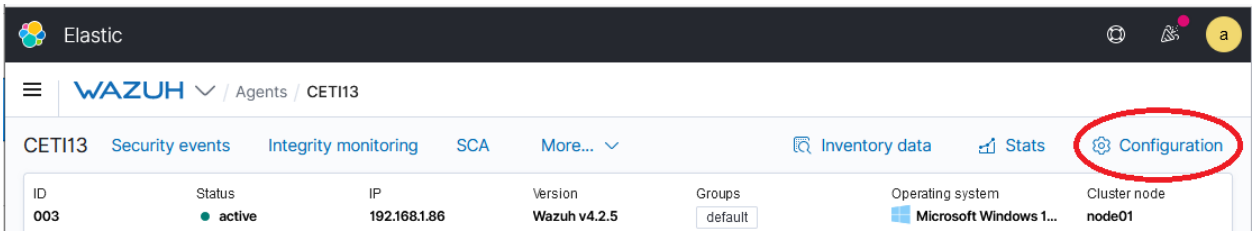
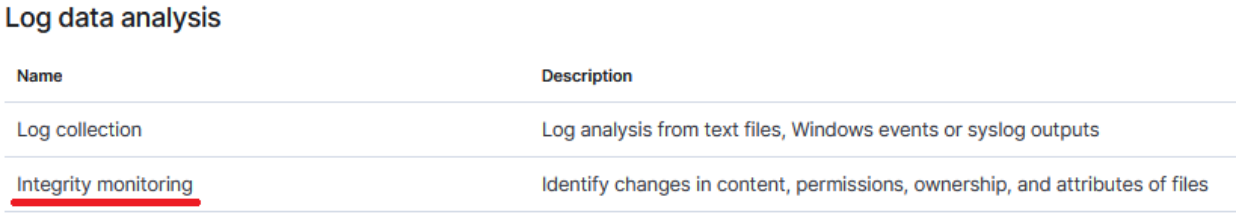
Wazuh FIM (File Integrity Monitoring)
Aquest sistema vigila alguns fitxers, el registre de sistema a Windows, i alerta si es modifiquen. El component Syscheck emmagatzema un *checksum* criptogràfic i altres atributs dels fitxers, i periòdicament els compara amb els actuals que està utilitzant el sistema buscant canvis.

Visualitzar
Per comprovar els fitxers que estas seguint selecciona la màquina, ves a la configuració i selecciona *Integrity monitoring*.





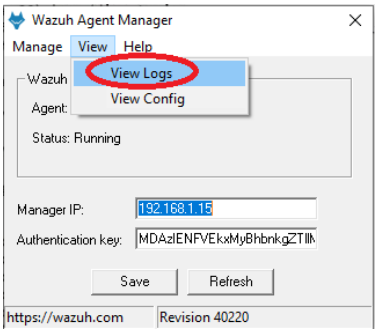
Per defecte està programat que comprovi la integritat dels fitxers cada 12 hores (43200 segons) però es pot configurar per fer-ho un dia concret de la setmana.

Posa ara un valor més petit per fer proves. Recorda que ho pots canviar de dues maneres:
- Des de la màquina client al fitxer de configuració de l'agent: *ossec.conf*
- Des del Wazuh manager i administració de grups.

Per saber quan es posa en marxa, pots fer un seguiment del fitxer *c:\Archivos de programa (x86)\ossec-agent\ossec.log*

```
2022/02/10 20:02:17 wazuh-agent: INFO: (6008): File integrity monitoring scan started.
2022/02/10 20:02:27 wazuh-agent: INFO: (6009): File integrity monitoring scan ended.
```

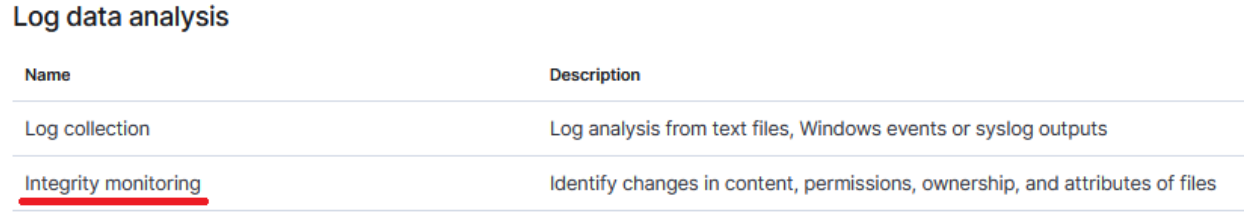
Que també pots visualitzar a través de la barra de menús del Wazuh *agent manager*:



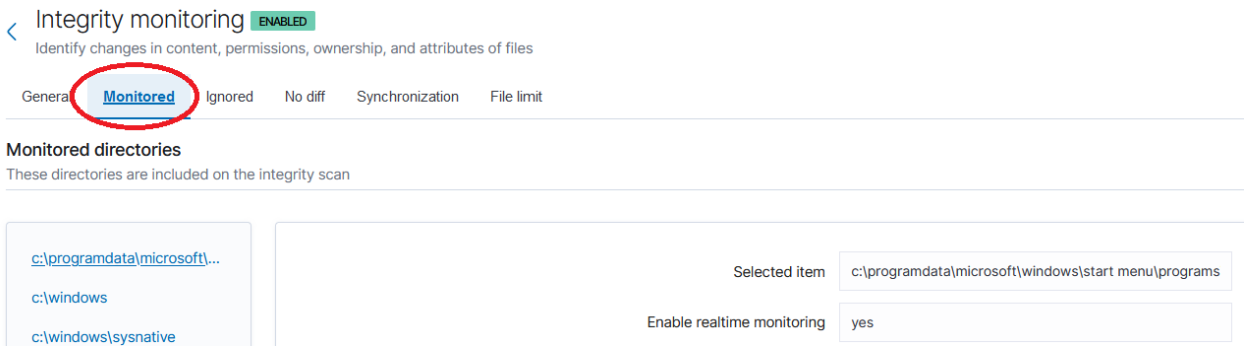
Veiem un exemple de canvis al registre de sistema a Windows:
Al connectar-se l'ordinador a una altra Wifi es produeixen canvis al registre de sistema que provoquen notificacions a *Integrity monitoring*:

Feb 1, 2022 @ 10:13:01.186	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Dnscache\Parameters\DnsActiveIfs\MiFibra-A752_3	deleted	Registry Value Entry Deleted.	5	751
Feb 1, 2022 @ 10:13:01.186	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Dnscache\Parameters\DnsActiveIfs\MiFibra-A752_3	deleted	Registry Value Entry Deleted.	5	751
Feb 1, 2022 @ 10:13:01.182	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Dnscache\Parameters\DnsActiveIfs\MiFibra-A752_3	deleted	Registry Key Entry Deleted.	5	597

Veiem ara canvis en el sistema de fitxers de Windows:
Torna a l'apartat de comprovació de la configuració de *Integrity monitoring*:



Selecciona ara la pestanya *Monitored*:



Aquí pots veure les carpetes monitoritzades i els apartats del registre de sistema que comprova.

Provoca unes alertes:

- Modifica el fitxer C:\Windows\win.ini
- Modifica el fitxer C:\Windows\System32\drivers\etc\hosts
- Afegeix un fitxer a la carpeta C:\Windows\System32\drivers\etc\

I després d'executar-se l'anàlisi d'integritat, comprova que hagis rebut les alertes.

Feb 10, 2022 @ 20:02:17.665	c:\windows\sysnative\drivers\etc\prova1etc.txt	added
Feb 10, 2022 @ 20:02:17.664	c:\windows\sysnative\drivers\etc\hosts	modified
Feb 10, 2022 @ 20:02:17.664	c:\windows\win.ini	modified

També pots monitoritzar la integritat d'una nova carpeta en temps real. Per a això, afegeix la següent directriu al fitxer ossec.conf de l'agent:

```
<!-- File integrity monitoring -->
 <syscheck>
        …
        <directories check_all="yes" realtime="yes" report_changes="yes" > c:\carpeta_nova </directories>
        …
 </syscheck>
```

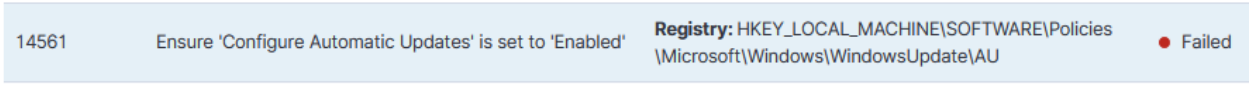
Wazuh SCA (Security Configuration Assessment)

Aquest mòdul monitoritza les configuracions de les màquines clients tant Windows, com Linux, com macOS. La configuració es limita a les següents directrius:

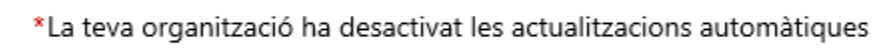
```
<sca>
   <enabled>yes</enabled>
   <scan_on_start>yes</scan_on_start>
   <interval>12h</interval>
   <skip_nfs>yes</skip_nfs>
</sca>
```

La part que trobo molt interessant és que a part de dir-te quines configuracions pots millorar, te les explica i et diu com ho has de fer.

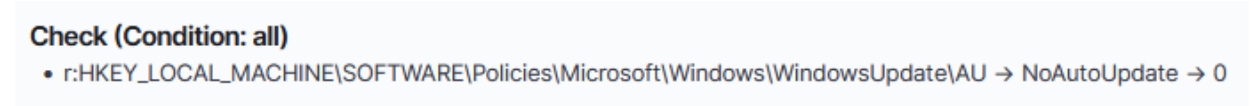
Per exemple:



Em diu que no tinc activat les actualitzacions automàtiques. I efectivament, si vaig a la configuració em diu:



A més a més, el Wazuh *manager* em diu com activar-la:



Com que des del panell de control de Windows no em deixa canviar la configuració de les actualitzacions, ho faig directament al registre de sistema tal com m'indica l'SCA.

A la pròxima comprovació de configuracions ja tindré una incidència menys.

Cerca les possibles millores de configuració de la teva màquina i canvia'n alguna.