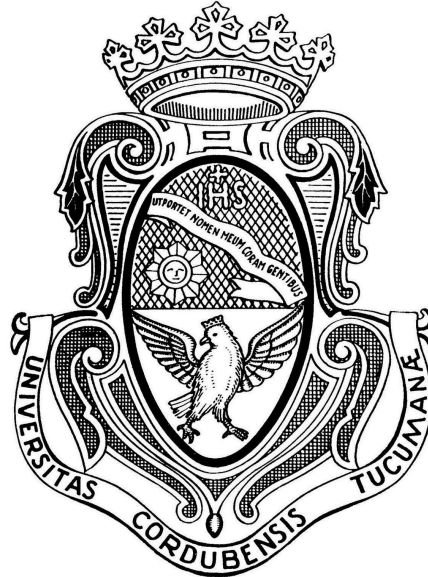


UNIVERSIDAD NACIONAL DE CÓRDOBA
FACULTAD DE CIENCIAS EXACTAS, FÍSICAS Y NATURALES



Criptografía y Seguridad de Redes
Sistemas de Detección de Intrusión basado en Host

Comisión: Única

Docentes: Jorge, Javier; Solinas, Miguel

Apellido	Nombre	Matrícula
GUGLIELMOTTI	Bruno	43474558
RODRÍGUEZ	Franco Aníbal	42994188

¿Qué es Wazuh?

Wazuh es una plataforma de seguridad y monitoreo open-source diseñada para la detección de amenazas, respuesta ante incidentes, cumplimiento normativo y monitoreo de la seguridad de los sistemas y aplicaciones.

Actúa como un sistema de **SIEM** (Security Information and Event Management) e **HIDS** (Host-based Intrusion Detection System), proporcionando visibilidad en tiempo real sobre lo que ocurre en una red o en hosts individuales.

¿Para qué sirve?

Tiene varios propósitos, entre ellos:

1. **Detección de intrusiones:** Monitorea actividades sospechosas o potencialmente maliciosas tanto en sistemas operativos como en aplicaciones. Puede detectar cambios en archivos, análisis de logs, tráfico de red, y más.
2. **Monitoreo de integridad de archivos (FIM):** Realiza un seguimiento de los cambios en los archivos críticos del sistema, como archivos de configuración o binarios, para detectar cualquier manipulación no autorizada.
3. **Cumplimiento normativo:** Wazuh ayuda a cumplir con varios estándares de seguridad, como PCI DSS, GDPR, HIPAA, ISO 27001, y otros. Genera informes que detallan las políticas de seguridad y control implementadas.
4. **Análisis de logs:** Recoge y analiza logs de diversas fuentes, incluyendo sistemas operativos, aplicaciones, dispositivos de red y otros servicios. Esto permite identificar comportamientos anómalos, fallos o indicios de ciberataques.
5. **Monitoreo de vulnerabilidades:** Wazuh puede integrarse con bases de datos de vulnerabilidades para realizar análisis de seguridad sobre el software instalado en los hosts monitoreados, alertando cuando detecta vulnerabilidades conocidas.
6. **Respuesta ante incidentes:** Proporciona mecanismos automáticos para responder a incidentes de seguridad. Esto puede incluir la ejecución de scripts, bloqueo de usuarios, cierre de conexiones no autorizadas, entre otros.

¿Qué se pretende lograr con Wazuh?

El objetivo principal de Wazuh es proporcionar una **plataforma integral de seguridad** que permita a las organizaciones monitorear, detectar y responder ante amenazas en tiempo real. Sus capacidades buscan:

1. **Aumentar la visibilidad y control:** Proveer una visión detallada de todo lo que ocurre en la infraestructura de una organización, desde servidores y aplicaciones hasta dispositivos conectados.

2. **Proteger contra ataques de seguridad:** Detectar actividades maliciosas antes de que puedan comprometer sistemas críticos, ayudando a prevenir incidentes graves de seguridad.
3. **Automatización de la seguridad:** Implementar respuestas automáticas ante amenazas, reduciendo el tiempo de reacción y mitigando posibles daños.
4. **Facilitar el cumplimiento de normativas:** Ayudar a las organizaciones a cumplir con las regulaciones y estándares de seguridad mediante el monitoreo constante y generación de reportes.
5. **Mejorar la capacidad de respuesta ante incidentes:** Permitir que los equipos de seguridad identifiquen, respondan y contengan incidentes de manera rápida y eficiente.

Instalación

Para poder usar Wazuh debemos tener instalado Docker en nuestro sistema, si ya contamos con eso clonamos el repositorio de wazuh

```
git clone https://github.com/wazuh/wazuh-docker.git -b v4.4.1
```

Una vez clonado debemos entrar dentro de la carpeta **single-node** del repositorio e instalar los certificados correspondientes

```
docker-compose -f generate-indexer-certs.yml run --rm generator
```

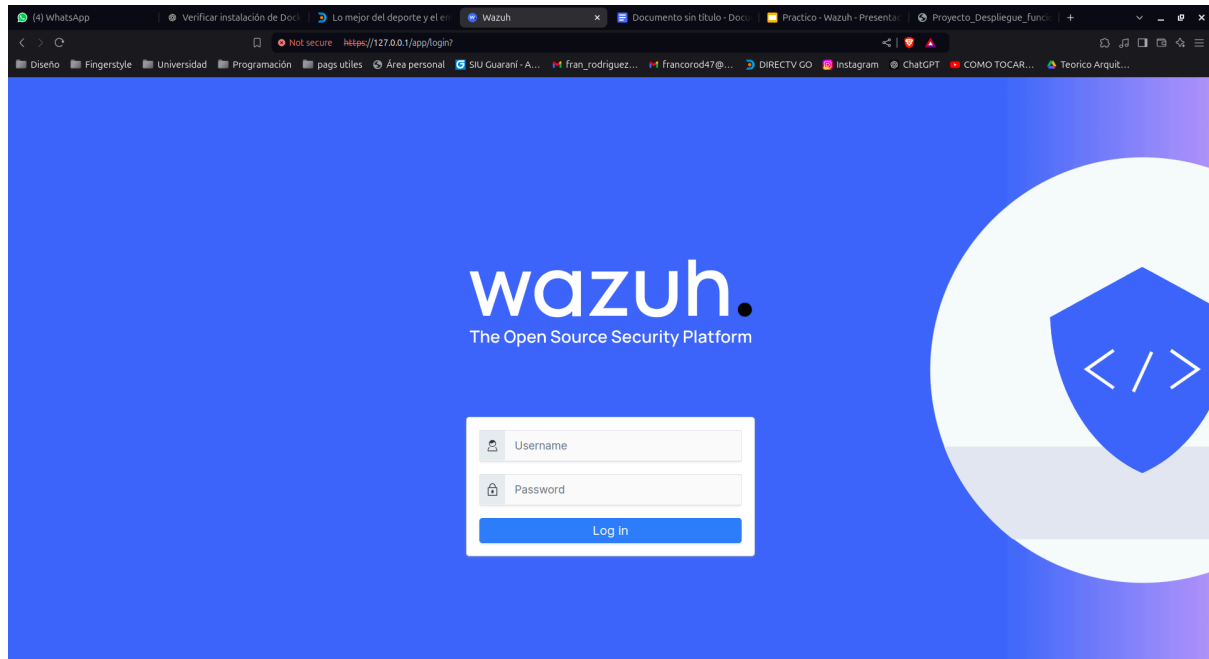
finalmente levantamos el servicio usando el comando **docker-compose up -d**

```

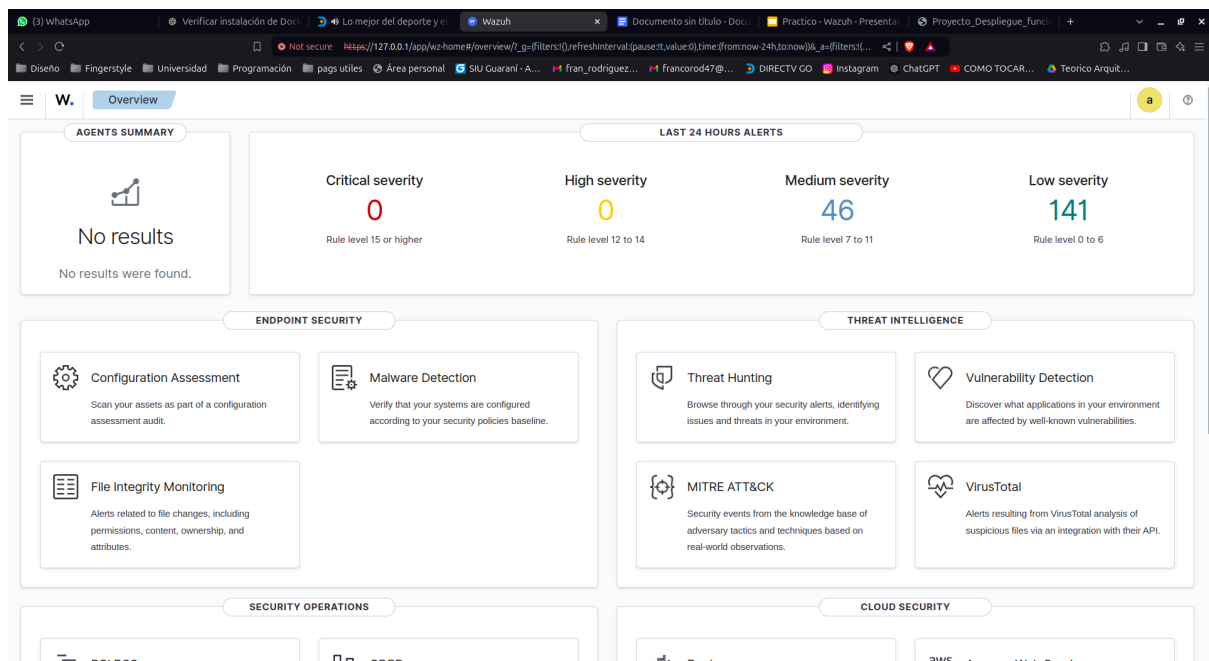
franco@HP-Pavilion-15: ~/wazuh-docker/single-node
4.9.0: Pulling from wazuh/wazuh-indexer
f9dd052e142d: Already exists
2f8354c90bfc: Pull complete
fa249f6889bf: Pull complete
f608eb455c9a: Pull complete
5ef66777e3d3: Pull complete
48a66c1138a6: Pull complete
943c1d0235ee: Pull complete
1d5f05b7a27c: Pull complete
9092330cb249: Pull complete
3946f6b8a01c: Pull complete
6907bd94efad: Pull complete
3641d8f13081: Pull complete
4f4fb700ef54: Pull complete
005448c3a277: Pull complete
fd952b3f8660: Pull complete
Digest: sha256:a7adcac99648b73e075c4fa8daa5bd552da46ec4a7700d7faccdd579a2c5e7cc2
Status: Downloaded newer image for wazuh/wazuh-indexer:4.9.0
Pulling wazuh.dashboard (wazuh/wazuh-dashboard:4.9.0)...
4.9.0: Pulling from wazuh/wazuh-dashboard
f9dd052e142d: Already exists
d69f1c40cdd2: Pull complete
23db20106b4e: Pull complete
a786ffa9b469: Pull complete
d1e1d6602142: Pull complete
89bb95e67fe9: Pull complete
2a4730cba52e: Pull complete
378daa8a0ede: Pull complete
fea0bf982a0c: Pull complete
3c35d67b26d: Pull complete
79ca90777905: Pull complete
6c3009a0a8d3: Pull complete
4f4fb700ef54: Pull complete
Digest: sha256:9cc37f86a1efac76c0f0ddbc95dda0bdf72517b5067f384d66bcc7d95338a6c
Status: Downloaded newer image for wazuh/wazuh-dashboard:4.9.0
Creating single-node_wazuh.indexer_1 ... done
Creating single-node_wazuh.manager_1 ... done
Creating single-node_wazuh.dashboard_1 ... done
franco@HP-Pavilion-15:~/wazuh-docker/single-node$

```

Si entramos a la dirección **localhost** de nuestro navegador o usando **127.0.0.1** entonces veremos lo siguiente



Las credenciales por defecto son **admin** y **SecretPassword**

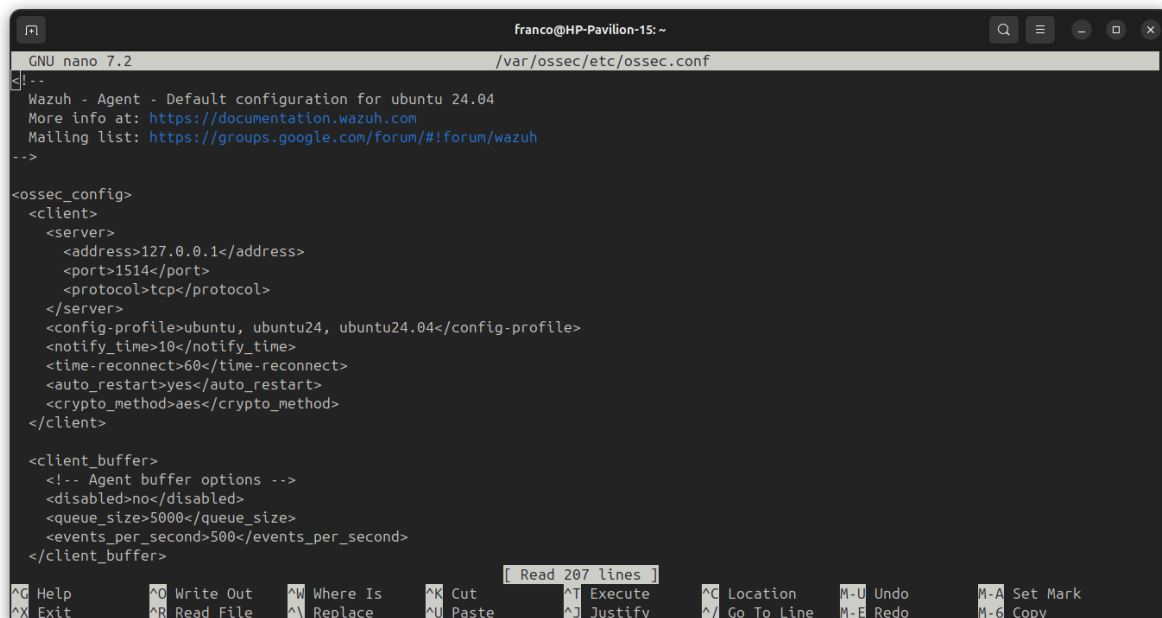


Este **dashboard** nos da mucha información sobre diferentes funciones, pero vemos que no tenemos ningún agente. Para poder utilizar Wazuh debemos instalar su agente mediante su repositorio y su clave GPG

```
curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | sudo apt-key add -  
echo "deb https://packages.wazuh.com/4.x/apt/ stable main" | sudo tee  
/etc/apt/sources.list.d/wazuh.list  
sudo apt update  
sudo apt install wazuh-agent
```

Luego debemos agregar la información de nuestro host al siguiente archivo de configuración que se encuentra en la siguiente ruta

```
sudo nano /var/ossec/etc/ossec.conf
```



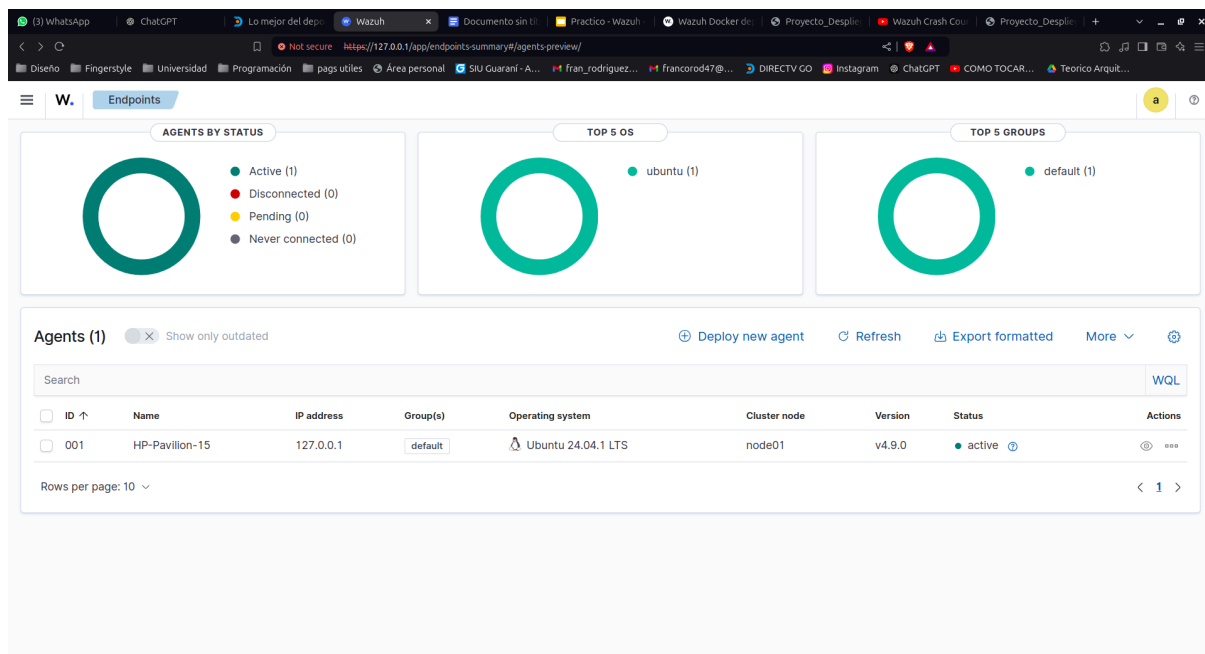
```
GNU nano 7.2 /var/ossec/etc/ossec.conf
--
Wazuh - Agent - Default configuration for ubuntu 24.04
More info at: https://documentation.wazuh.com
Mailing list: https://groups.google.com/forum/#!forum/wazuh
-->

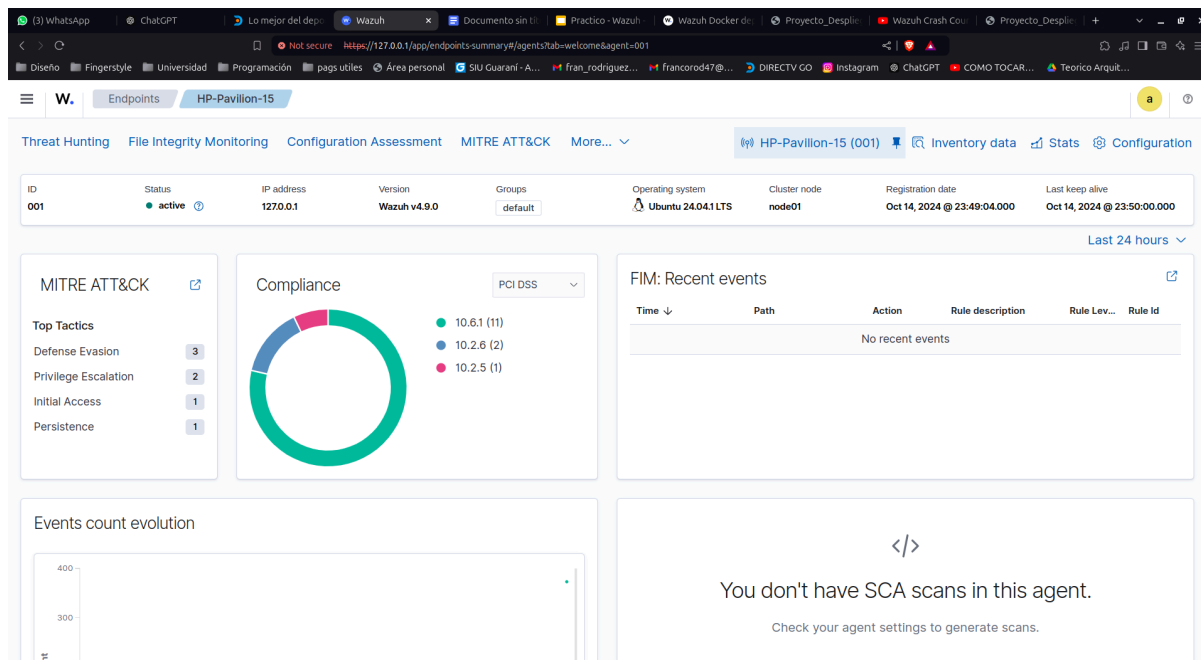
<ossec_config>
  <client>
    <server>
      <address>127.0.0.1</address>
      <port>1514</port>
      <protocol>tcp</protocol>
    </server>
    <config-profile>ubuntu, ubuntu24, ubuntu24.04</config-profile>
    <notify_time>10</notify_time>
    <time-reconnect>60</time-reconnect>
    <auto_restart>yes</auto_restart>
    <crypto_method>aes</crypto_method>
  </client>

  <client_buffer>
    <!-- Agent buffer options -->
    <disabled>no</disabled>
    <queue_size>5000</queue_size>
    <events_per_second>500</events_per_second>
  </client_buffer>

[ Read 207 lines ]
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^G Location   M-U Undo      M-A Set Mark
^X Exit      ^R Read File  ^_ Replace    ^U Paste      ^J Justify    ^_ Go To Line M-E Redo      M-G Copy
```

Luego de reiniciar el servicio ya tenemos disponible nuestro agente en el dashboard





Configuración del monitor de seguridad

Para esta parte debemos ir a la misma configuración dónde fuimos para añadir el agente

```
sudo nano /var/ossec/etc/ossec.conf
```

y buscar la zona que menciona al **syscheck** agregar la línea

"<directories check_all="yes" report_changes="yes" realtime="yes">/root</directories>"

que generará muchas alertas innecesarias pero permitirá poder ver todo lo que sucede

```
franco@HP-Pavilion-15: ~
GNU nano 7.2 /var/ossec/etc/ossec.conf
<syscheck>
  <disabled>no</disabled>

  <!-- Frequency that syscheck is executed default every 12 hours -->
  <frequency>43200</frequency>

  <scan_on_start>yes</scan_on_start>

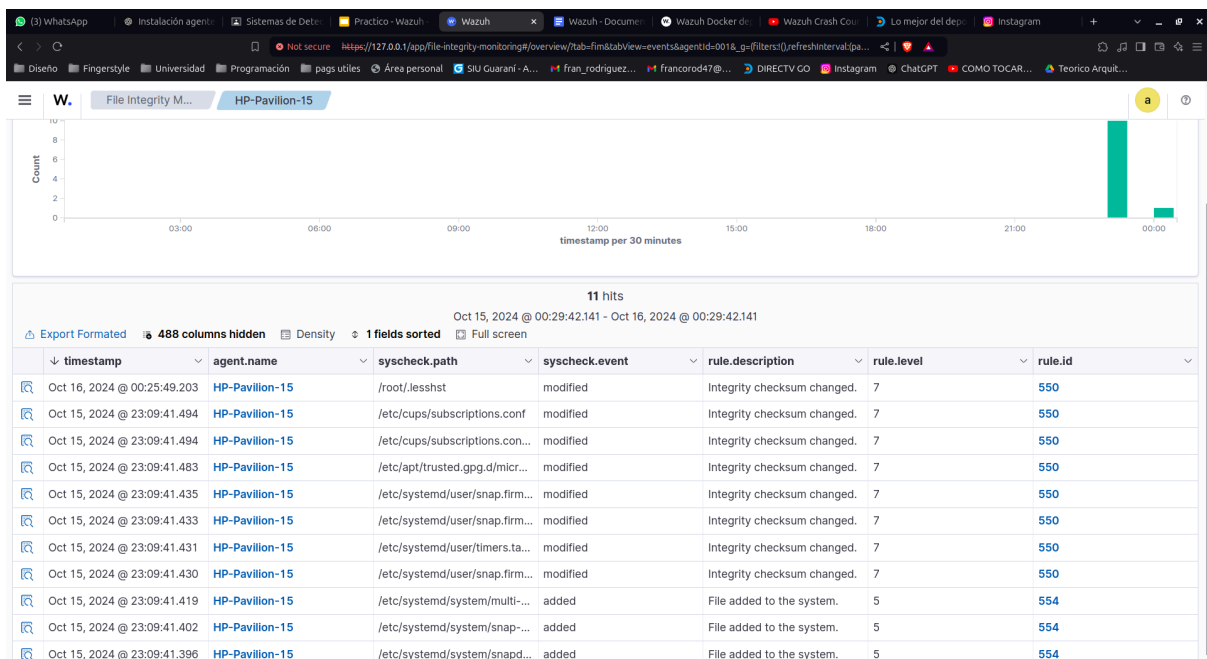
  <!-- Directories to check (perform all possible verifications) -->
  <directories>/etc,/usr/bin,/usr/sbin</directories>
  <directories>/bin,/sbin,/boot</directories>
  <directories check_all="yes" report_changes="yes" realtime="yes">/root</directories>

  <!-- 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>
```

Reseteamos el servicio y verificamos que todo esté andando en orden

```
franco@HP-Pavilion-15: ~  
franco@HP-Pavilion-15:~$ sudo systemctl status wazuh-agent.service  
● wazuh-agent.service - Wazuh agent  
   Loaded: loaded (/usr/lib/systemd/system/wazuh-agent.service; enabled; preset: enabled)  
   Active: active (running) since Wed 2024-10-16 00:25:36 -03; 12s ago  
     Process: 32637 ExecStart=/usr/bin/env /var/ossec/bin/wazuh-control start (code=exited, status=0/SUCCESS)  
    Tasks: 39 (limit: 18952)  
   Memory: 77.6M (peak: 80.6M)  
      CPU: 22.431s  
   CGroup: /system.slice/wazuh-agent.service  
           └─32659 /var/ossec/bin/wazuh-execd  
             └─32670 /var/ossec/bin/wazuh-agentd  
               └─32685 /var/ossec/bin/wazuh-syscheckd  
                 └─32695 /var/ossec/bin/wazuh-logcollector  
                   └─32712 /var/ossec/bin/wazuh-modulesd  
  
Oct 16 00:25:29 HP-Pavilion-15 systemd[1]: Starting wazuh-agent.service - Wazuh agent...  
Oct 16 00:25:29 HP-Pavilion-15 env[32637]: Starting Wazuh v4.9.0...  
Oct 16 00:25:30 HP-Pavilion-15 env[32637]: Started wazuh-execd...  
Oct 16 00:25:32 HP-Pavilion-15 env[32637]: Started wazuh-agentd...  
Oct 16 00:25:32 HP-Pavilion-15 env[32637]: Started wazuh-syscheckd...  
Oct 16 00:25:33 HP-Pavilion-15 env[32637]: Started wazuh-logcollector...  
Oct 16 00:25:34 HP-Pavilion-15 env[32637]: Started wazuh-modulesd...  
Oct 16 00:25:36 HP-Pavilion-15 env[32637]: Completed.  
Oct 16 00:25:36 HP-Pavilion-15 systemd[1]: Started wazuh-agent.service - Wazuh agent.  
franco@HP-Pavilion-15:~$
```

Ahora si vamos a **wazuh > agents > hp-pavilion-15 > file integrity monitoring > events** se nos mostrará todos los cambios hechos



Ahora creamos un archivo de prueba para verificar si el monitor funciona

```
franco@HP-Pavilion-15:~$ sudo touch /root/prueba.txt  
franco@HP-Pavilion-15:~$ ls /root  
ls: cannot open directory '/root': Permission denied  
franco@HP-Pavilion-15:~$ sudo ls /root  
Desktop  prueba.txt  snap  
franco@HP-Pavilion-15:~$
```

Y vemos como nos da los detalles del cambio

W.

File Integrity M...

HP-Pavillon-15

DashboardInventoryEvents

Search

manager.name: wazuh.manager rule.groups: syscheck agent.id: 001 + Add filter

Count

03:0006:0009:0012:00

timestamp

Export Formatted488 columns hiddenDensity1 fields sortedFull screen

Oct 15, 2024 @ 00:32:51.380

timestampagent.namesyscheck.pathsyscheck.e

Oct 16, 2024 @ 00:31:53.451HP-Pavillon-15/root/prueba.txtadded

Oct 16, 2024 @ 00:25:49.203HP-Pavillon-15/root/jesshtmodified

Oct 15, 2024 @ 23:09:41.494HP-Pavillon-15/etc/cups/subscriptions.con...modified

Oct 15, 2024 @ 23:09:41.494HP-Pavillon-15/etc/cups/subscriptions.confmodified

Oct 15, 2024 @ 23:09:41.463HP-Pavillon-15/etc/apt/trusted.gpg.d/micro...modified

Document Details

View surrounding documents

View single document

TableJSON

index

wazuh-alerts-4.x-2024.10.16

agent.id

001

agent.ip

127.0.0.1

agent.name

HP-Pavillon-15

decoder.name

syscheck_new_entry

full_log

File '/root/prueba.txt' added Mode: realtime

id

1729049513.24779

input.type

log

location

syscheck

manager.name

wazuh.manager

rule.description

File added to the system.

rule.firetimes

1

rule.gdpr

II_5.1.f

rule.gpg13

4.11

rule.groups

ossec, syscheck, syscheck_entry_added, syscheck_file

rule.hipaa

164.312.c.1 164.312.c.2

7