Análisis de archivos de logs con Wazuh

Mediante el uso de un script personalizado, Se realizará la copia línea por línea de los archivos recibidos hacia un archivo monitorizado por Wazuh, simulando así el comportamiento del agente que recibe los logs en tiempo real.

Siguiendo estos pasos se podrán gestionar y analizar los datos de manera más eficiente, por que se filtraran las alertas por nivel de criticidad en el dashboard y no tendremos que analizar los logs que tienen criticidad nula o no tienen que ver con la investigación, para lograrlo realizaremos los siguientes pasos:

Edición del archivo de configuración.

Abrimos el archivo de configuración del agente o manager de Wazuh ***ossec.conf*** posteriormente agregamos la configuración para monitorear el archivo de logs.

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

Configuración de ejemplo:

```
<localfile>
  <log_format>syslog</log_format>
  <location>/ruta/al/archivo/authlog.log</location>
</localfile>
```

Se debe verificar el formato del archivo de los registros para que sea decodificado de manera correcta y posteriormente analizado.

Una vez realizada la edición del archivo se debe reiniciar el agente o el manager donde se haya realizado la configuración.

```
systemctl restart wazuh-agent
systemctl restart wazuh-manager
```

Automatización.

Este script leerá el archivo de logs línea por línea y lo copiará a un archivo que será monitorizado por Wazuh.

```
#!/bin/bash
# Archivo de entrada (registros proporcionados)
input_file="authlog.log"
# Archivo de salida (Archivo monitorizado por wazuh)
output_file="archivoauthlog.log"
# Verifica si el archivo de salida existe y, si es así, lo elimina
if [ -f "$output_file" ]; then
    rm "$output_file"
fi
# Lee el archivo línea por línea
while IFS= read -r line
do
    # Simula la recepción de logs añadiendo un retraso de 200 ms
    sleep 0.2
    # Escribe la línea en el archivo de salida
    echo "$line" >> "$output_file"
    echo "Log añadido: $line"
done < "$input_file"
echo "El archivo ha sido copiado línea por línea a $output_file"
```

```
chmod +x /ruta/al/script.sh
```

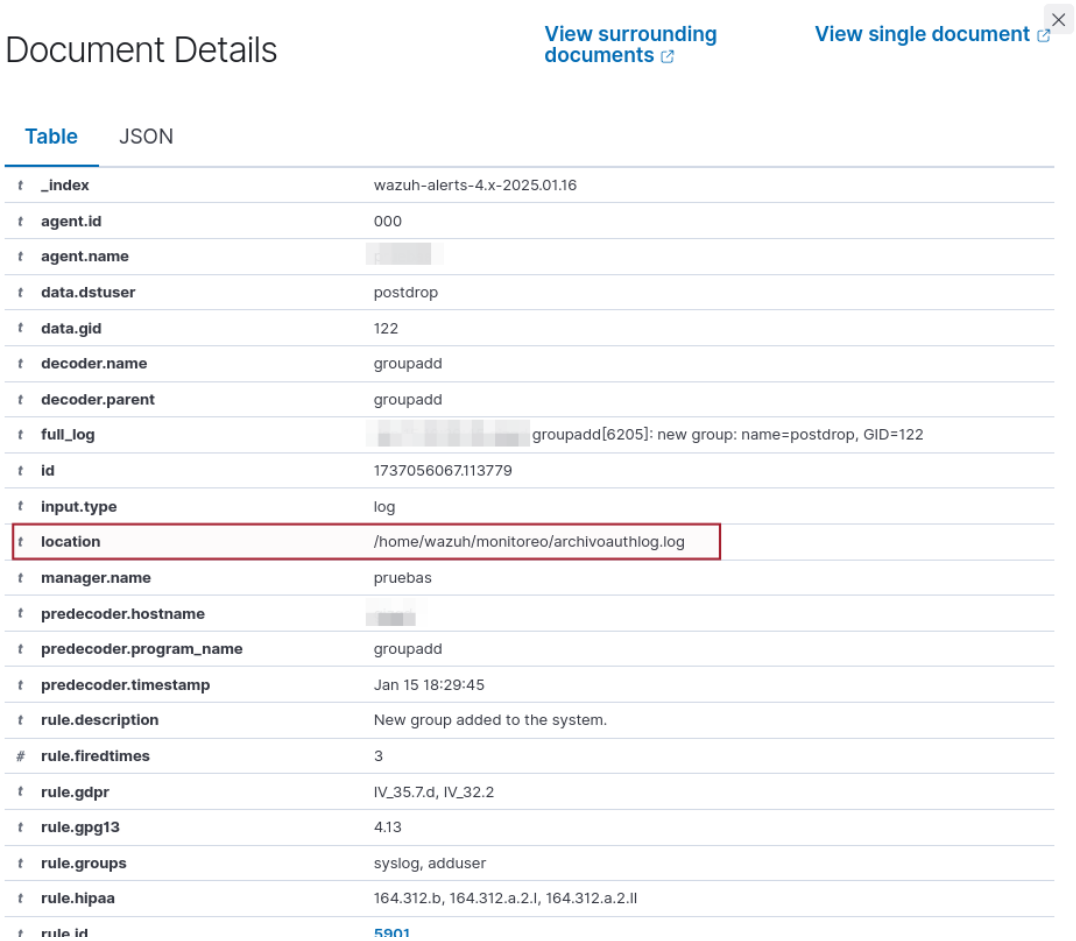
Verificación la Configuración.

Acceder al panel de Wazuh Manager y verificar que los logs estén siendo recibidos y analizados correctamente.

	Jan 16, 2025 @ 15:34:27.526	pruebas	Successful sudo to ROOT executed.	3	5402
	Jan 16, 2025 @ 15:34:27.526	pruebas	Successful sudo to ROOT executed.	3	5402
	Jan 16, 2025 @ 15:34:27.526	pruebas	PAM: Login session opened.	3	5501
	Jan 16, 2025 @ 15:34:25.524	pruebas	New user added to the system.	8	5902
	Jan 16, 2025 @ 15:34:25.523	pruebas	New group added to the system.	8	5901
	Jan 16, 2025 @ 15:34:25.523	pruebas	New group added to the system.	8	5901
	Jan 16, 2025 @ 15:34:23.521	pruebas	PAM: Login session opened.	3	5501
	Jan 16, 2025 @ 15:34:23.521	pruebas	First time user executed sudo.	4	5403
	Jan 16, 2025 @ 15:34:23.521	pruebas	Successful sudo to ROOT executed.	3	5402
	Jan 16, 2025 @ 15:34:23.521	pruebas	PAM: Login session closed.	3	5502

Rows per page: 100 ‹ 1 2 3 4 ›

Para comprobar que se trata del archivo analizado inspeccionamos el elemento deseado y verificamos que se trata del archivo de logs escogido.



Revision #3
Created 16 enero 2025 17:05:13 by Ricardo Chavez
Updated 3 abril 2025 12:30:23 by Ricardo Chavez