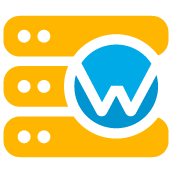
**Tutorial Wazuh Manager**



Daniel Escaño Hernández CET Ciberseguridad

# **1. Índice:**

[**1. Índice:**](#_lmwzrhyaxgtw) **1**

[**2. Instalación de Requisitos y Wazuh Manager**](#_g59i8ewd3ed3) **2**

[2.1 Configuración previa](#_ykezcd8mw12i) 2

[2.2 Stack ELK y Wazuh Manager](#_sffnnaov3efl) 2

[2.3 Comprobación](#_b4y9kw10647m) 3

[**3. Instalación Wazuh Agent en Windows**](#_9kam67hzat2s) **4**

[3.1 Configuración e instalación](#_7r4o3dc4ku8v) 4

[3.2 Comprobación](#_h96fubhqa8rg) 5

[**4. Monitorización con Wazuh Manager**](#_2nlq8xq3soqm) **6**

[4.1 Configuración acceso remoto](#_yqwefbnm4otd) 6

[4.2 Ataque simulado con diccionario a la máquina Windows 10](#_llovw68rb2rf) 7

[4.3 Comprobación](#_9d9ne1o6i7nr) 7

[**5. Reglas de alerta en Wazuh Manager**](#_fazv3zhptrv8) **10**

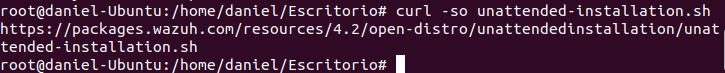
[**6. Instalación Wazuh Agent en Linux**](#_yg0l72pdreaj) **12**

[**7. Generación de Estadísticas e Informes en Wazuh**](#_qg0g18okyxfp) **15**

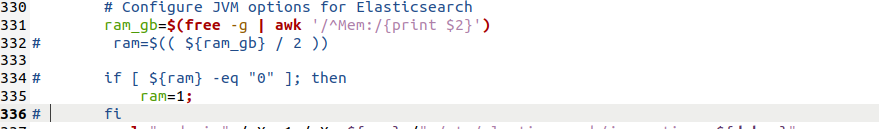
# **2. Instalación de Requisitos y Wazuh Manager**

### **2.1 Configuración previa**

Instalamos dependencias previas requeridas y descargamos el instalador:

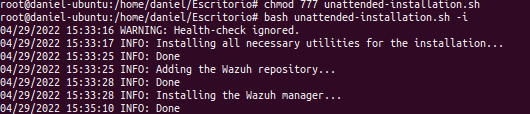


Debemos comentar estas 3 líneas en el archivo instalador:

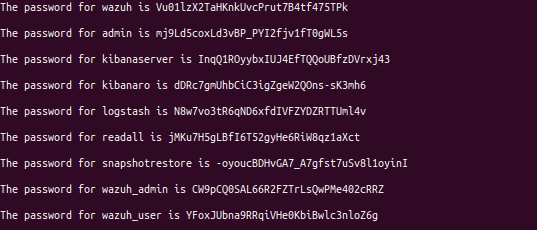


### **2.2 Stack ELK y Wazuh Manager**

Procedemos a ejecutarlo.

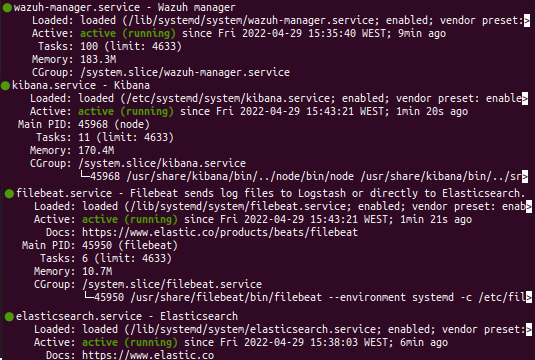


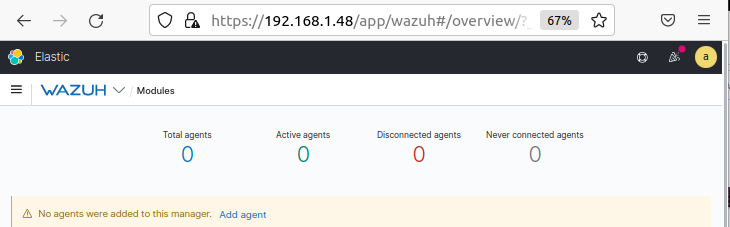
Estas son todas nuestras contraseñas generadas.



### **2.3 Comprobación**

Comprobamos el correcto funcionamiento de todos los módulos:

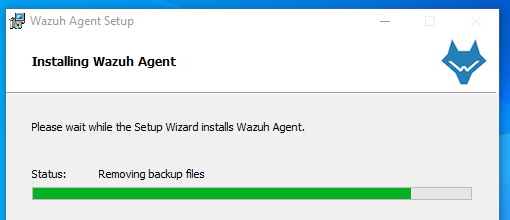




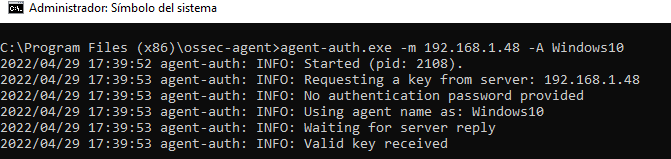
# **3. Instalación Wazuh Agent en Windows**

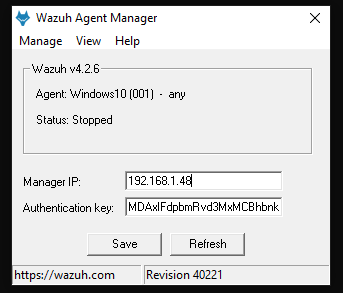
### **3.1 Configuración e instalación**

Continuamos instalando un agente en una máquina virtual Windows 10.

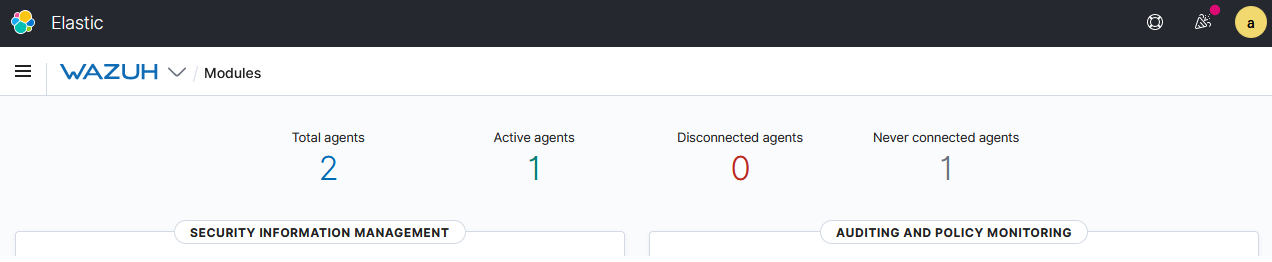


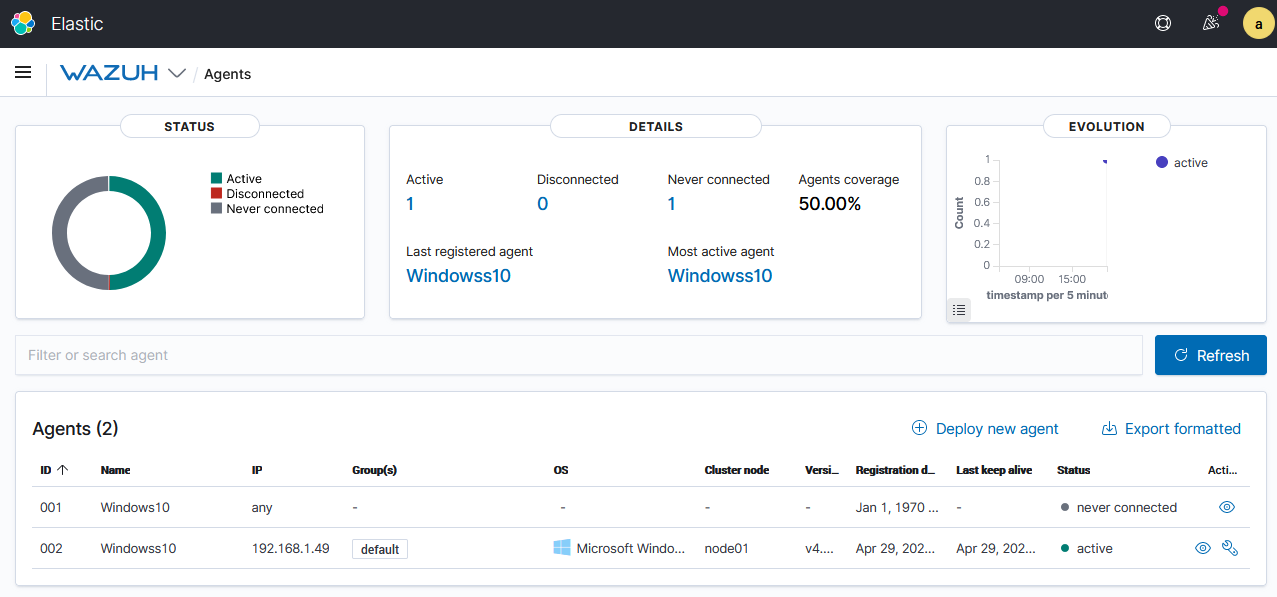
Necesitamos ejecutar este comando como administrador y concluimos añadiendo la ip de Wazuh Manager.





### **3.2 Comprobación**

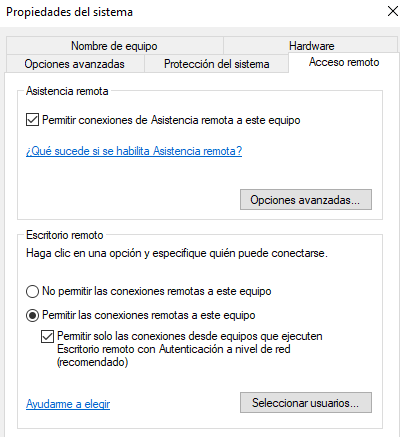




# **4. Monitorización con Wazuh Manager**

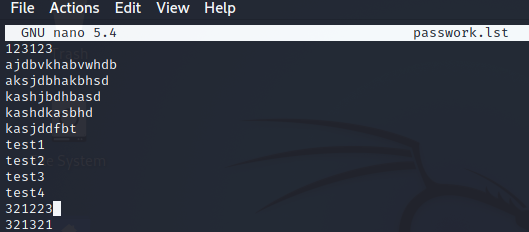
### **4.1 Configuración acceso remoto**

Para realizar este test requerimos de la correcta configuración de la herramienta de acceso remoto, debemos permitir este acceso.

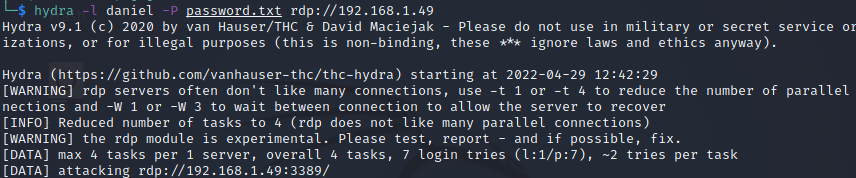


### **4.2 Ataque simulado con diccionario a la máquina Windows 10**

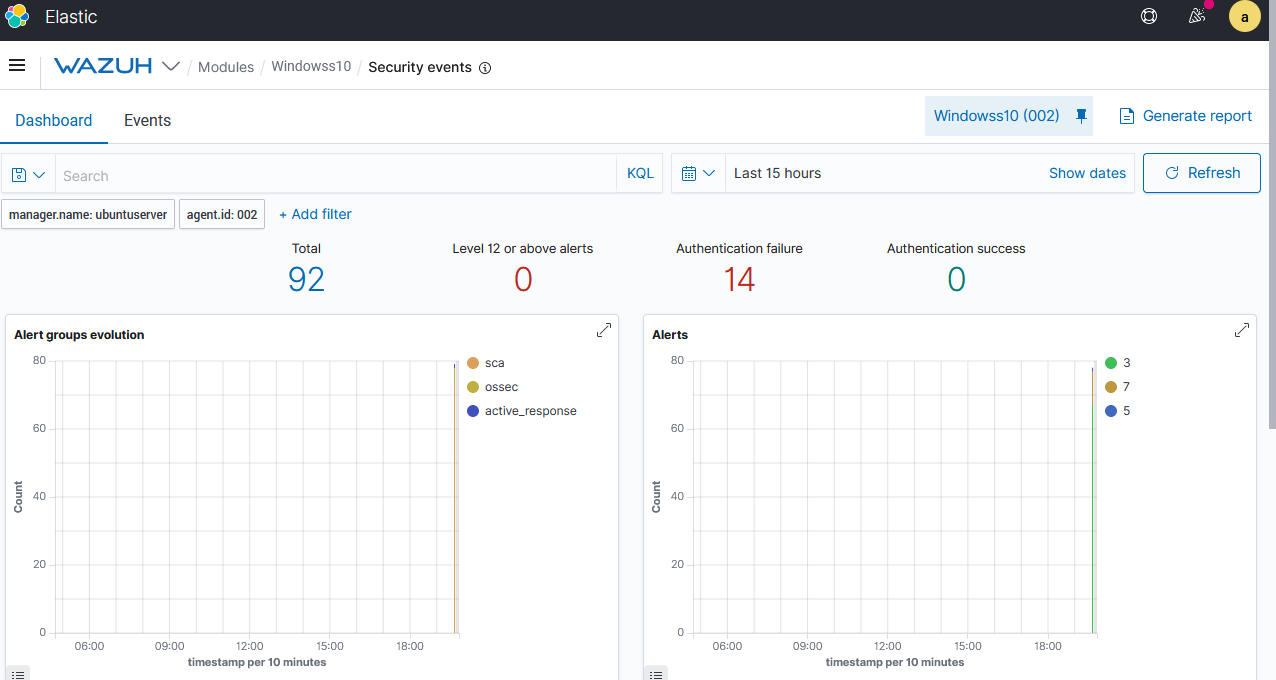
Creamos el diccionario que utilizaremos.

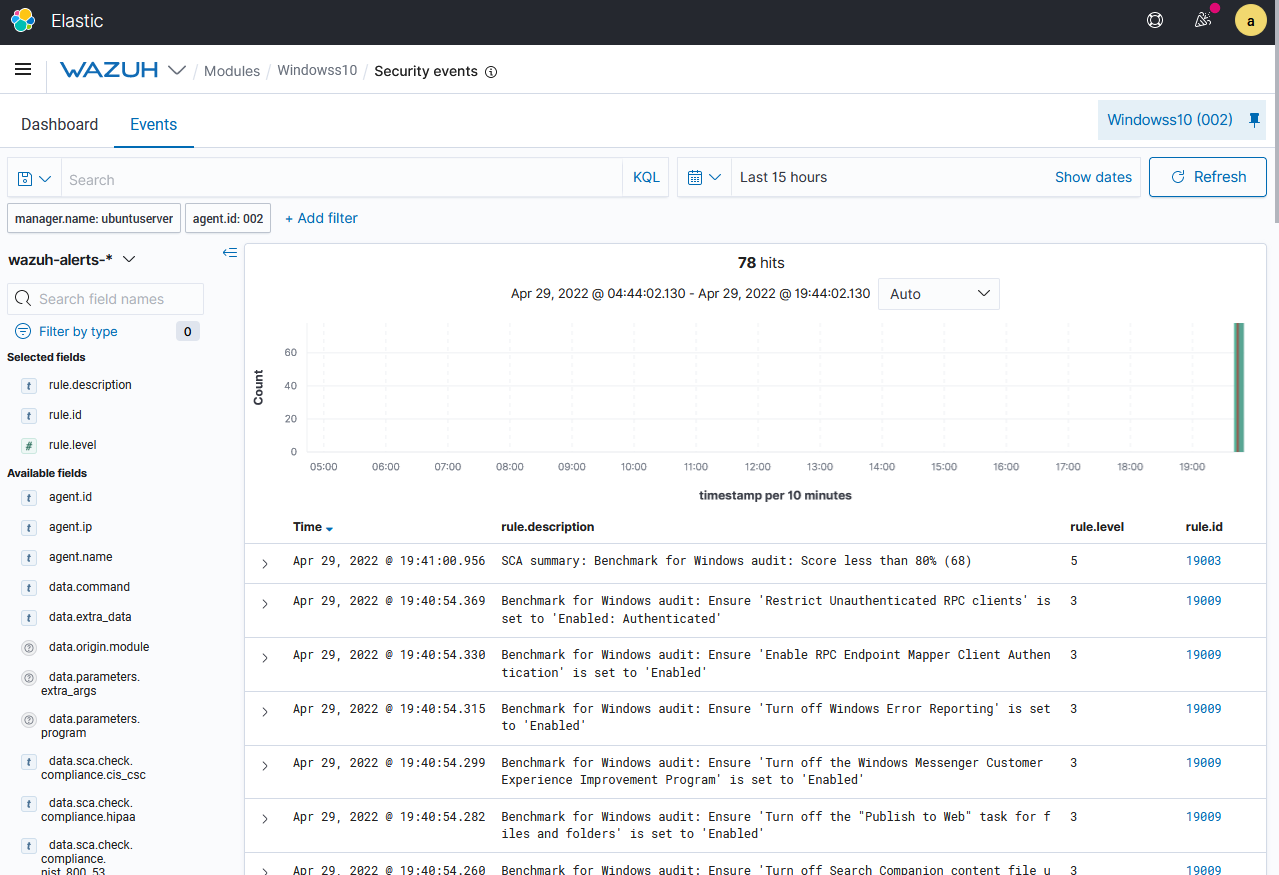


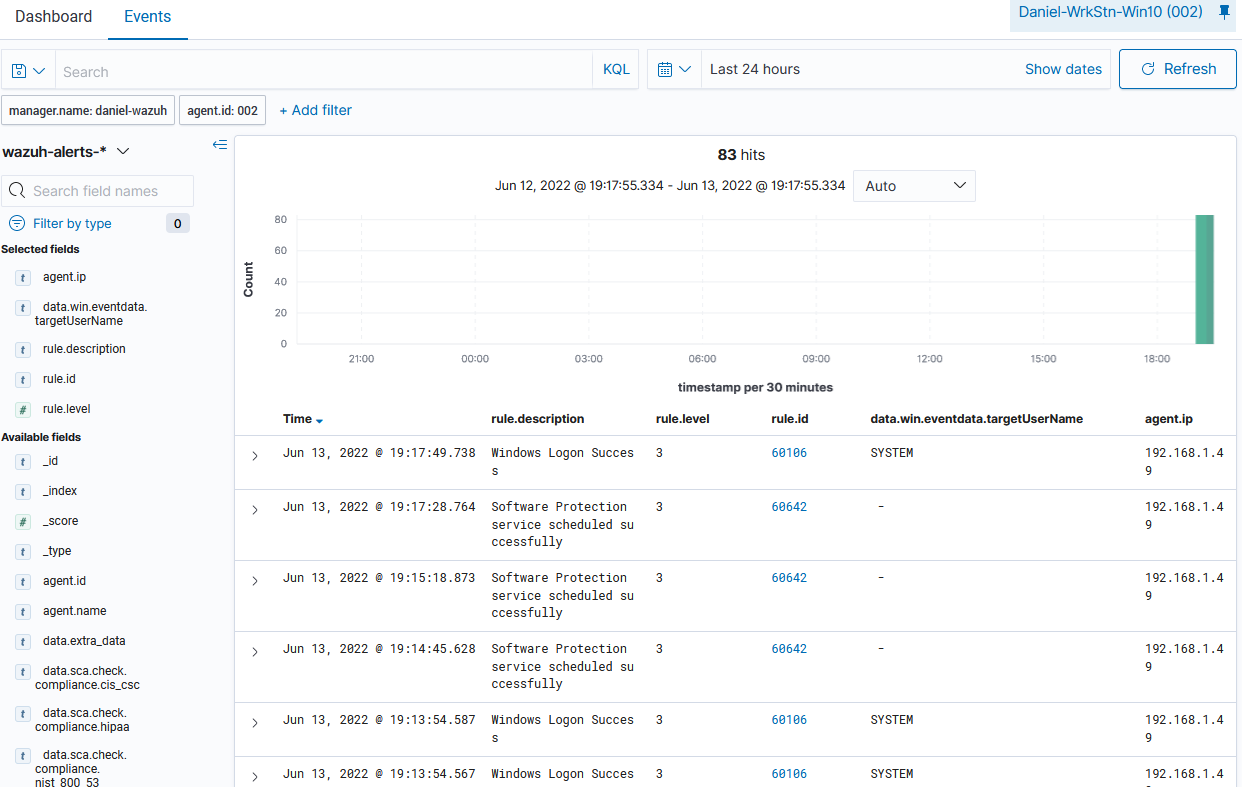
Finalmente lanzamos el ataque:

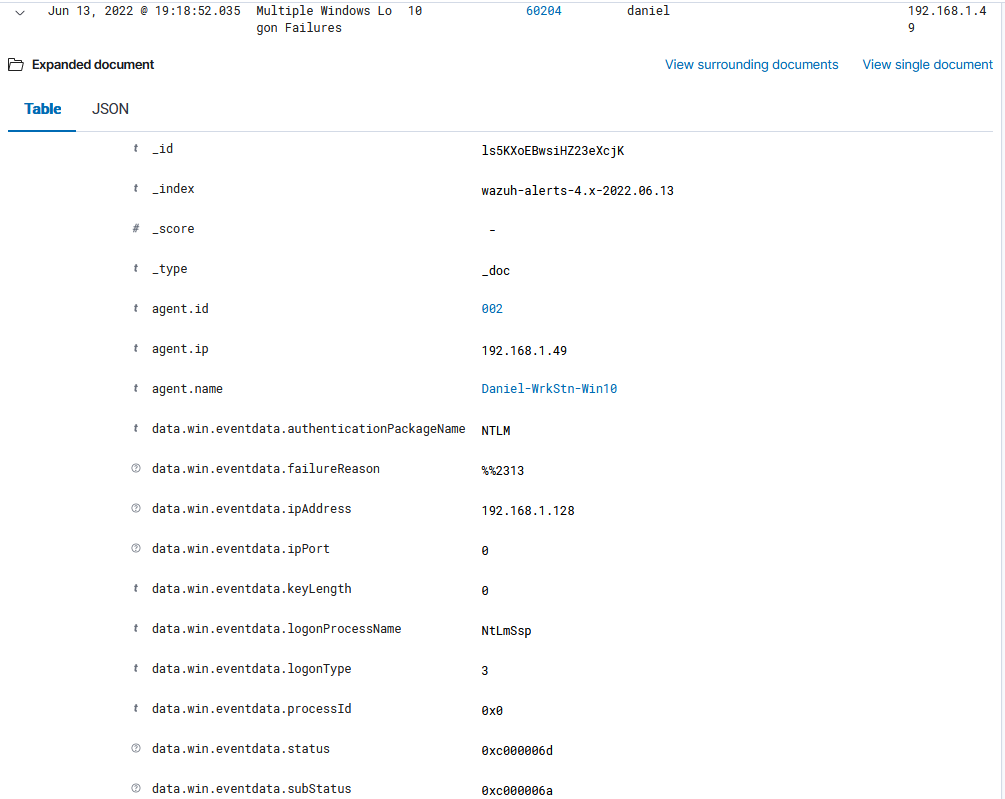


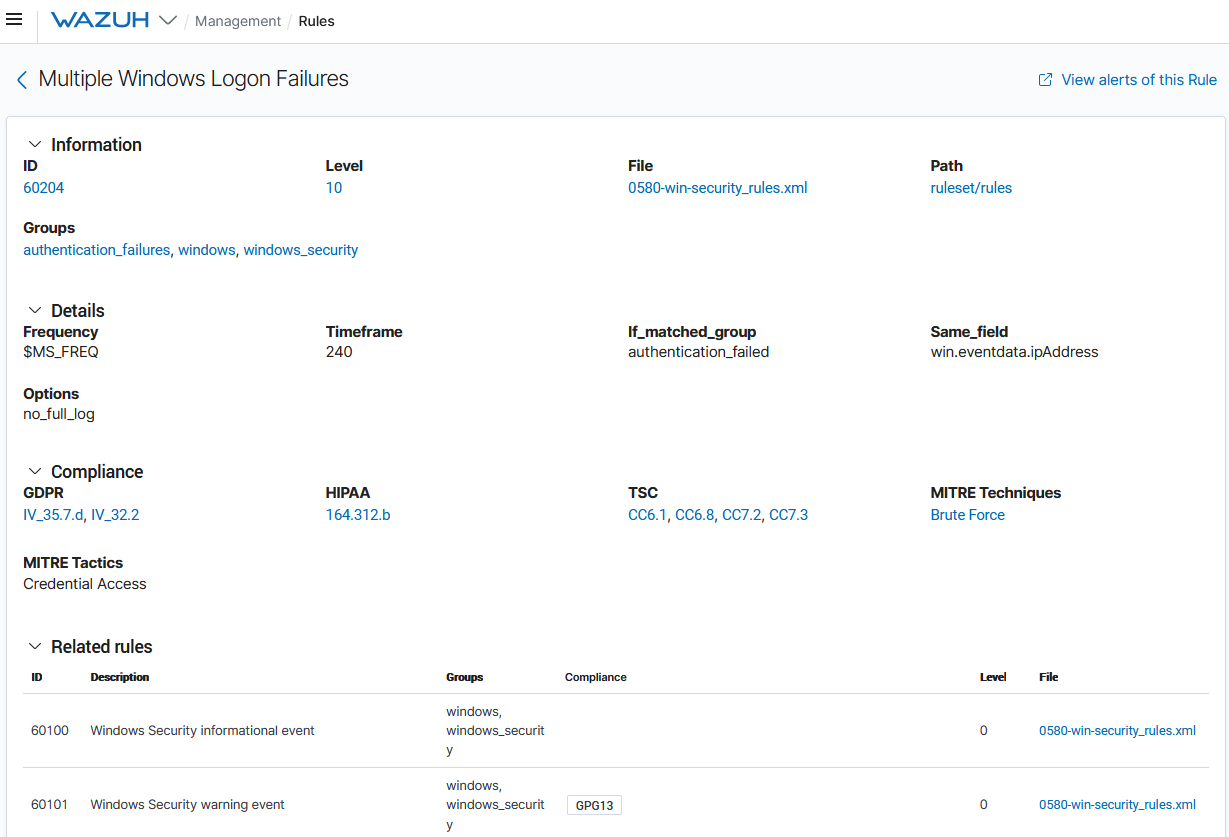
### **4.3 Comprobación**







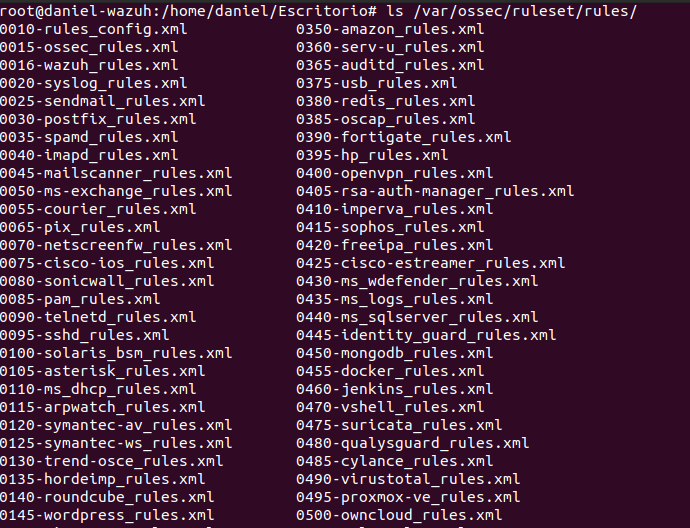


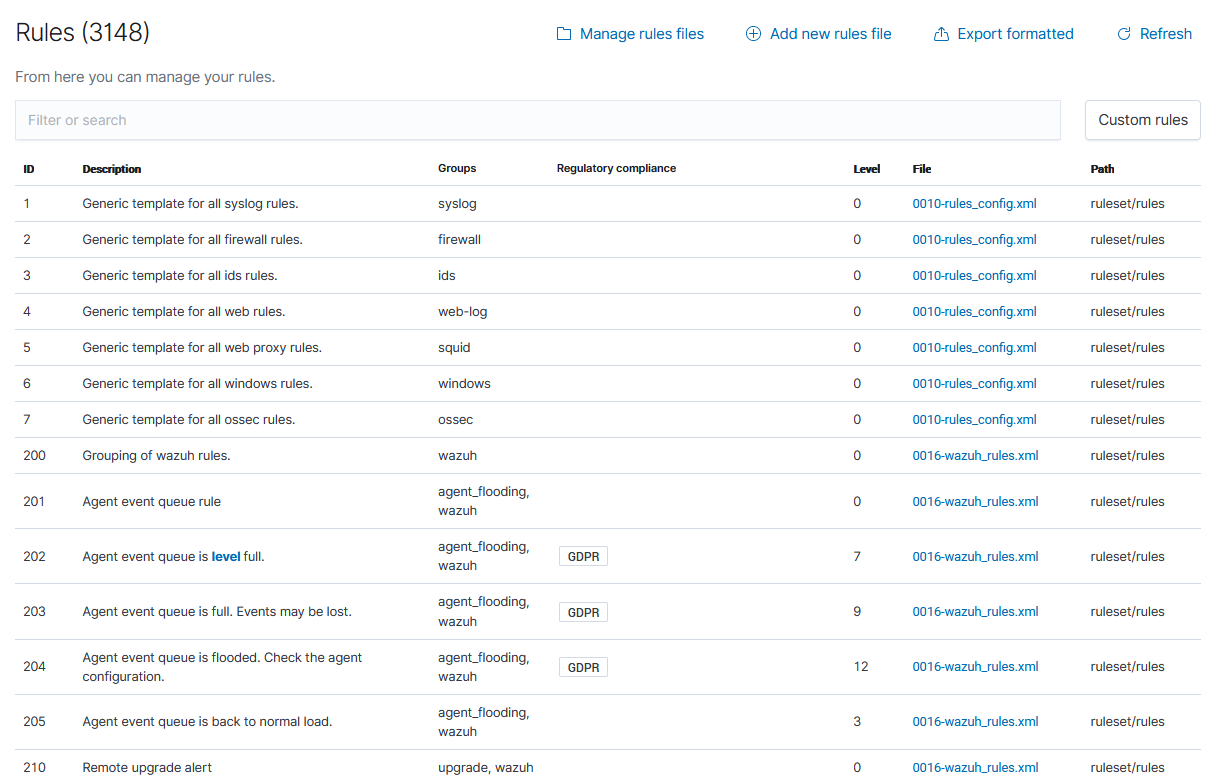


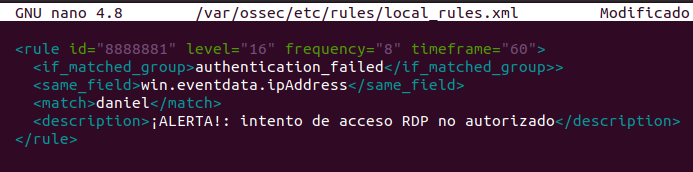


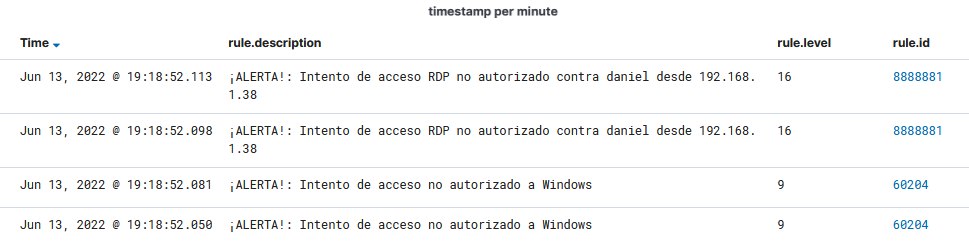


# **5. Reglas de alerta en Wazuh Manager**

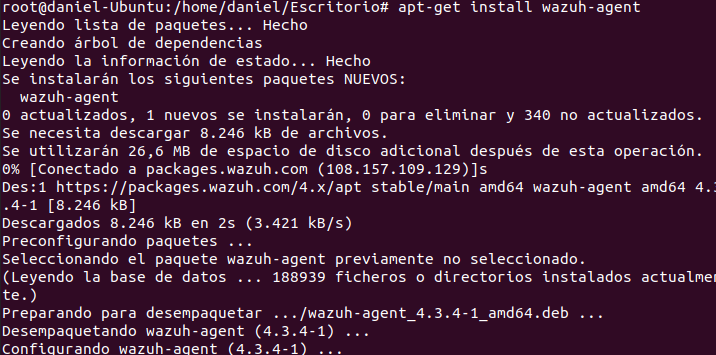


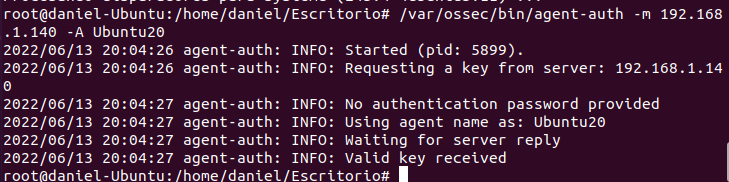


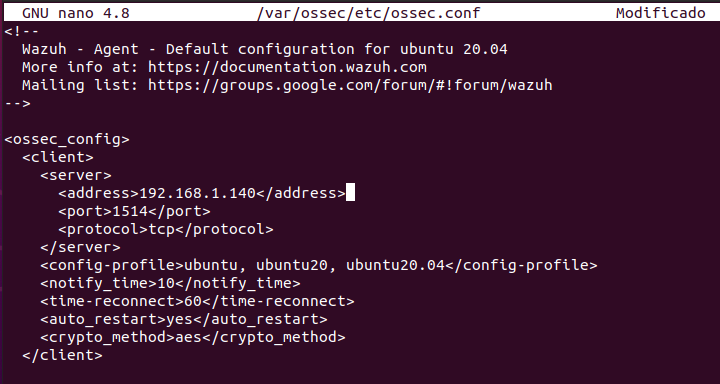


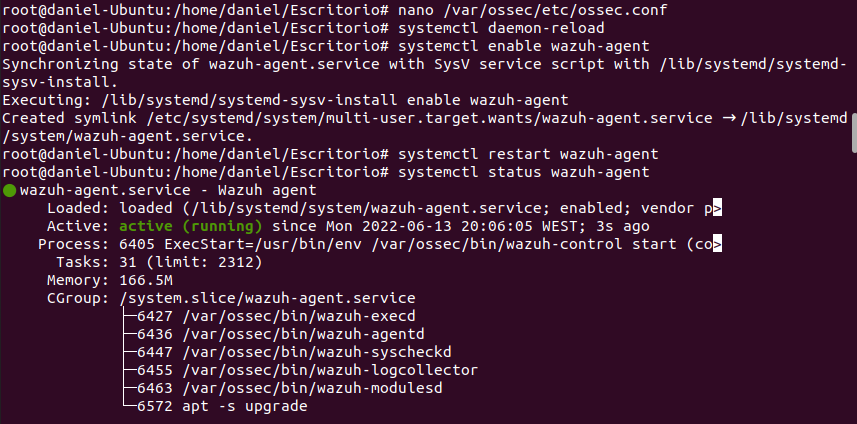


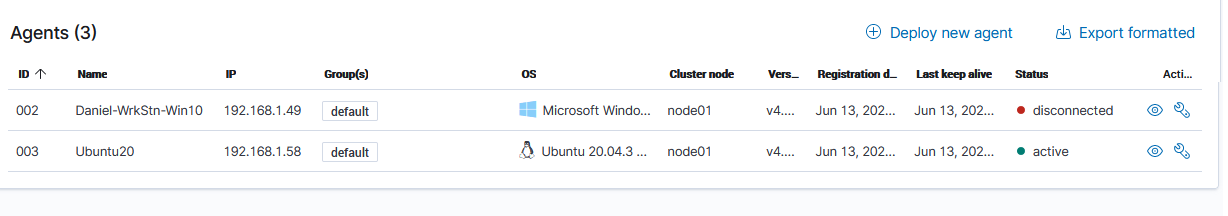
# **6. Instalación Wazuh Agent en Linux**

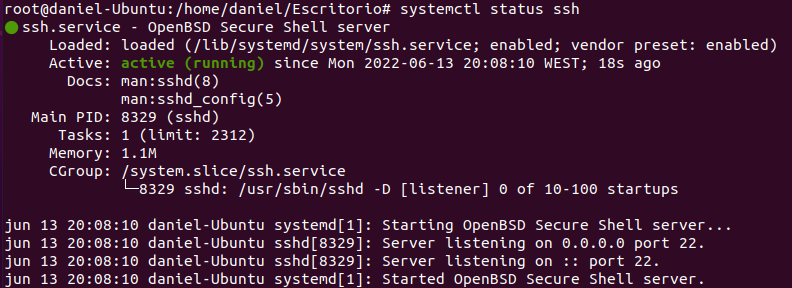


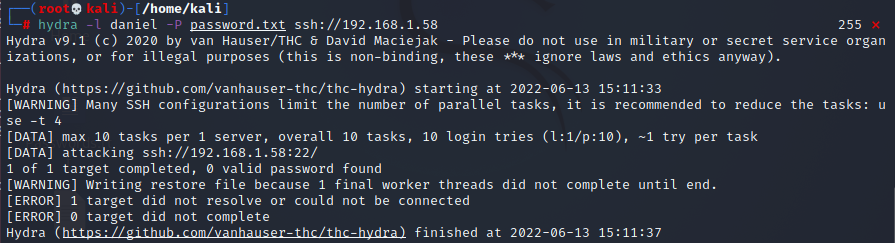


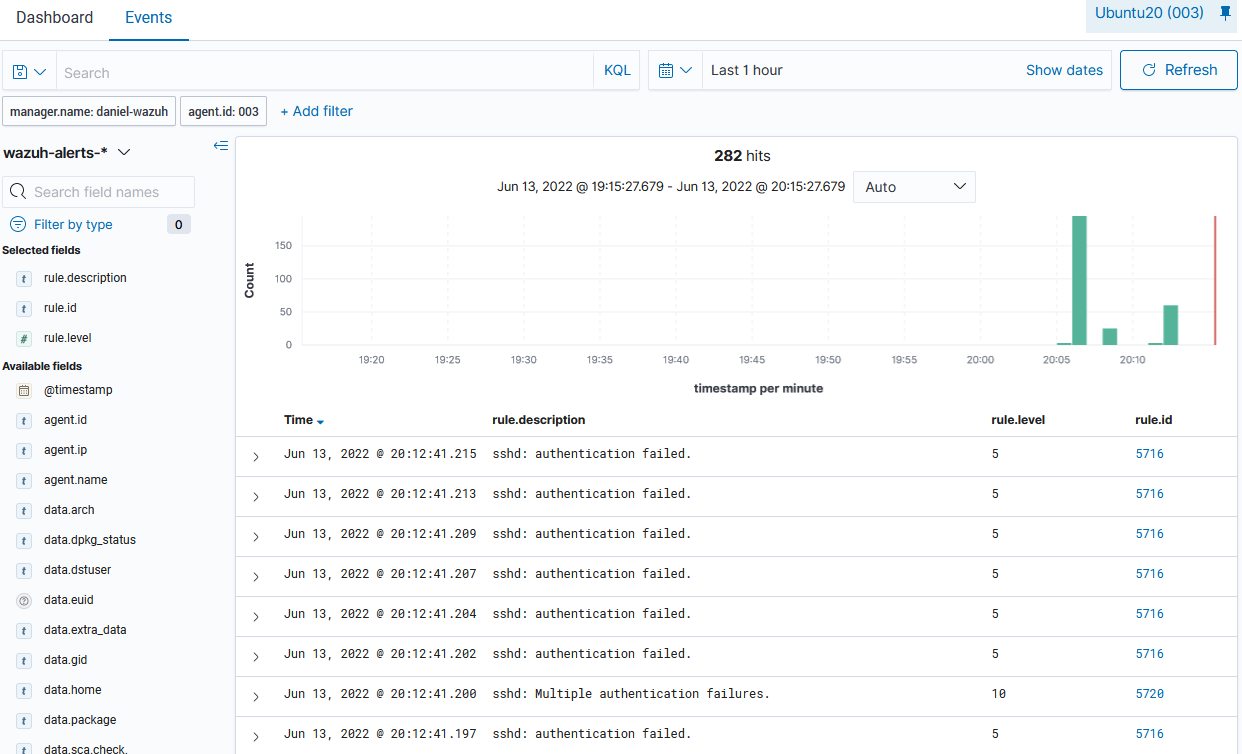












# **7. Generación de Estadísticas e Informes en Wazuh**

