

Wazuh és un programari de monitorització per detectar amenaces.

Funciona sobre una màquina Ubuntu, per exemple, i amb el programari Elasticsearch i Kibana.

Wazuh manager

El Wazuh manager és el sistema que analitza les dades rebudes dels agents registrats i provoca alertes quan un event coincideix amb alguna regla com per exemple: deteccions d'intrusió, modificació de fitxers, configuracions estranyes o altres. A més a més, el manager pot redirigir les alertes que provoca a *syslogs* o *emails*.

Per instal·lar-lo sobre una màquina Ubuntu segueix el següent tutorial:

<https://documentation.wazuh.com/current/installation-guide/open-distro/all-in-one-deployment/all-in-one.html>

Nota: Si esculls la instal·lació pas a pas amb APT, hi ha passos on amb la comanda *sudo* no n'hi ha prou i demana igualment permisos d'administrador. Per tant, cal seguir el tutorial amb la sessió de *root* (*sudo -i*).

El directori on s'instal·la és */var/ossec*

I el fitxer de configuració és */var/ossec/etc/ossec.conf*

Problema: a l'instal·lar els nous certificats, diu que no troba el fixer.

Això ha passat perquè s'ha instal·lat amb l'usuari normal i la comanda *sudo*. Quan alguna comanda no m'ha acceptat la comanda *sudo* per falta de privilegis, he continuat amb *root* mitjançant la comanda *sudo -i*.

Solució: Per crear els nous certificats, com que ho faig amb l'usuari *root*, he d'estar situat al directori */root* i des d'allà executar: *bash ~/wazuh-cert-tool.sh*

Wazuh agent a Windows

L'agent Wazuh és el programari que s'executa a la màquina client a monitoritzar, recull informació i l'envia al Wazuh manager.




El tutorial d'instal·lació de l'agent Wazuh per Windows està a:

<https://documentation.wazuh.com/current/installation-guide/wazuh-agent/wazuh-agent-package-windows.html>

Descarrega't l'instal·lador (*wazuh-agent-4.2.5-1.msi*) i des de l'interpret de comandes escriu:

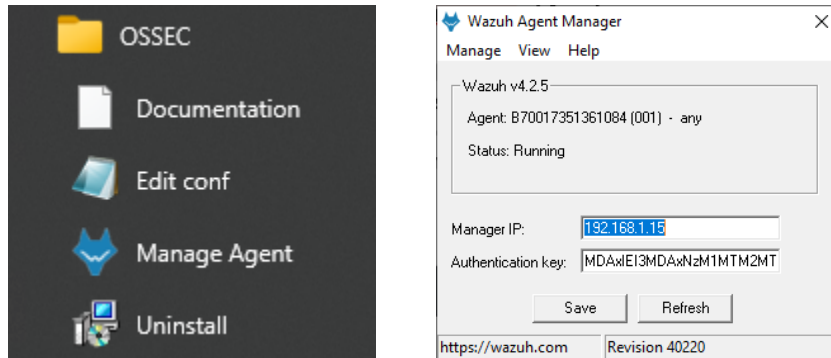
wazuh-agent-4.2.5-1.msi /q WAZUH_MANAGER="IP_servidor" WAZUH_REGISTRATION_SERVER="IP_servidor"

Comprova que està funcionant com a servei de Windows:

	Waves Audio Universal Serv...	Waves Audi...	En ejecu...	Automático	Sistema local
	Wazuh	Wazuh Win...	En ejecu...	Automático	Sistema local
	Windows Backup	Provides Wi...		Manual	Sistema local

La carpeta d'instal·lació és: *C:\Program Files (x86)\ossec-agent*
En aquesta carpeta hi podem trobar el fitxer de configuració: *ossec.conf*

També ens queda instal·lat l'agent Wazuh en mode gràfic:

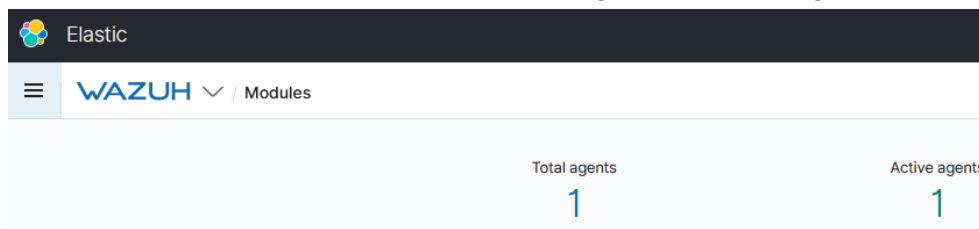


Comprova si funciona

Per accedir al servidor escriu: https://IP_servidor

Et demanarà identificar-te, l'usuari per defecte és `admin@admin`, o bé `wazuh@wazuh`.

Un cop dins, has de veure la teva màquina registrada com a agent:



Aquest agent s'identifica amb el nom de la màquina, en el meu cas: B70017351361084

Wazuh agent a Ubuntu Desktop

El tutorial d'instal·lació per a Linux està a:

<https://documentation.wazuh.com/current/installation-guide/wazuh-agent/wazuh-agent-package-linux.html>

L'agent Wazuh queda instal·lat al directori `/var/ossec` i el fitxer de configuració és `/var/ossec/etc/ossec.conf`
