UNIVERSIDAD TECNOLÓGICA DE PANAMÁ

FACULTAD DE INGENIERÍA EN SISTEMAS COMPUTACIONALES

PROYECTO FINAL:

IMPLEMENTACION DE SEGURIDAD XDR Y SIEM CON WAZUH.

INTEGRANTES:

NEFTHALY ABREGO 4-806-103

DEYBI MOJICA 8-930-2000

ASESOR

MGTR. LEANDRO ESPINOZA

REPÚBLICA DE PANAMÁ

AÑO

2024

INTRODUCCION

El vertiginoso cambio tecnológico trae consigo grandes retos de seguridad informática a nivel empresarial involucrando tiempo, dinero, y recursos, esto provoca la necesidad de implementar mecanismos potentes para la identificación, detección, análisis, monitoreo en tiempo real de las amenazas que atentan contra los activos e infraestructura. El aumento del cibercrimen obliga a las empresas a invertir en seguridad informática para combatir las amenazas y mitigar los riesgos. El objetivo es proteger las computadoras, redes, bases de datos y aplicando correcciones de seguridad a vulnerabilidades encontradas que pueden ser explotadas por ciberdelincuentes.

La cantidad masiva de datos generados por los dispositivos en las comunicaciones en red y operaciones diarias complican la tarea del monitoreo y análisis de registros para la generación de alertas, es por ello por lo que la recopilación de datos e identificación rápida de eventos permite actuar de forma oportuna en la aplicación de las correcciones que salvaguarden los equipos informáticos que soportan los procesos del negocio, así como la información almacenada.[1]

Las tecnologías emergentes llamadas XDR abordan esta difícil tarea integrando componentes para detectar, analizar y responder a las amenazas desde múltiples dispositivos finales. Los sistemas de información de seguridad y gestión de eventos (SIEM) centraliza la telemetría para recolectar datos de diferentes dispositivos en la red (firewalls, IDS, servidores y aplicaciones) para analizar en tiempo real el cumplimiento y las brechas de seguridad; esta potente tecnología permite conocer rápidamente el estado de la seguridad informática.[2]

En este proyecto se realiza la implementación de las funcionalidades de Wazuh Server y distintos clientes en sistemas operativos Windows y Linux.

ÍNDICE GENERAL

TABLA DE CONTENIDO

INTRODUCCION 3
Índice General 4
Índice de Figuras 5
Índice de Tablas 6
Marco teórico 13
1.1 XDR y SIEM 13
1.1.1 XDR 13
1.1.2 SIEM 14
1.2 Wazuh 15
1.2.1 Generalidades de la arquitectura de Wazuh 15
1.3 Características y módulos de Wazuh 16
1.3.1 Endpoint Security 16
1.3.2 Threat Intelligence 17
1.3.3 Security Operations 18
1.3.4 Cloud Security 19
Proceso de implementación y configuración 21
1.4 Requirementos de Wazuh 21
1.4.1 Sistemas operativos recomendados Wazuh 21
1.5 Descarga de sistema operative Ubuntu 22
1.6 Configuraciones máquina virtual 22
1.7 Procedimiento de instalación de Wazuh Server en All in One Deployment. 34
1.8 Proceso de instalación el servidor wazuh 34
1.9 Procedimiento de instalación de agentes 43
1.9.1 Proceso de instalación y configuración de Windows 44

1.9.2 Proceso de instalación de agente y configuración de Ubuntu 56
1.10 Escenario de ataque con Kali 56
1.11 Resultados de comportamiento de servicios de Wuazuh 56
Conclusiones 58
Recomendaciones 58
Referencias bibliográficas 58
Anexos 61

ÍNDICE DE FIGURAS

Ilustración 1: Indicar el título de la figura..... ***¡Error! Marcador no definido.***

ÍNDICE DE TABLAS

No se encontraron entradas de tabla de contenido.

MARCO TEÓRICO

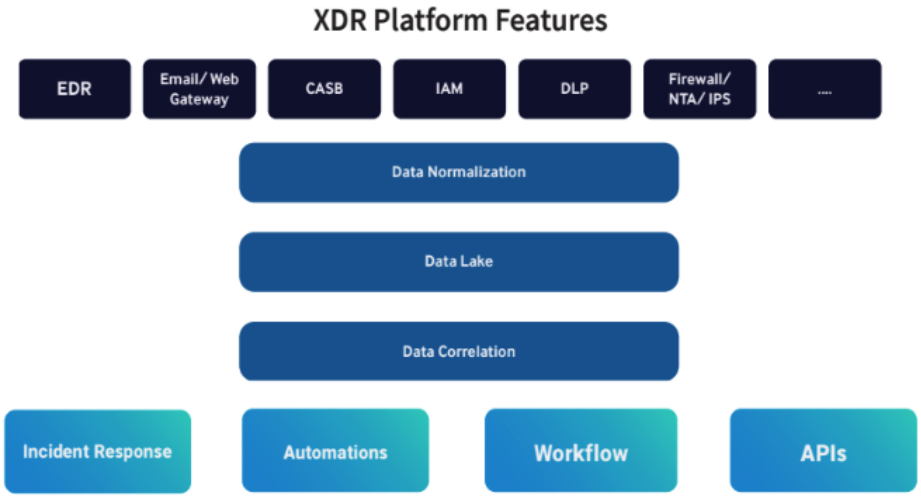
1.1 XDR y SIEM

Los XDR (detección y respuesta extendida) y SIEM (información y gestión de eventos) son soluciones de ciberseguridad, estos tienen diferentes alcances e integración con los datos de seguridad. El SIEM tienen un enfoque de gestión de registros de eventos, análisis histórico e informes de cumplimiento de seguridad basándose en los datos de los puntos finales, el tráfico de red y los entornos basados en la nube. El XDR se consideran una extensión de EDR (Detección y respuesta de endpoint) unifica la seguridad en una organización permitiendo la detección y respuesta ante amenazas con el proceso de recopilación de varias fuentes de datos de la infraestructura. Las dos soluciones pueden unificarse para obtener una experiencia de extremo a extremo mejorando el proceso de prevenir, detectar y responder a las amenazas en los distintos puntos finales como aplicaciones, endpoint, correos electrónicos, IoT, plataformas en la nube entre otras.[3][4]

Esta plataforma de código abierto con licencia publica general 2.0 (GNU) y licencia apache 2.0 (ALv2).

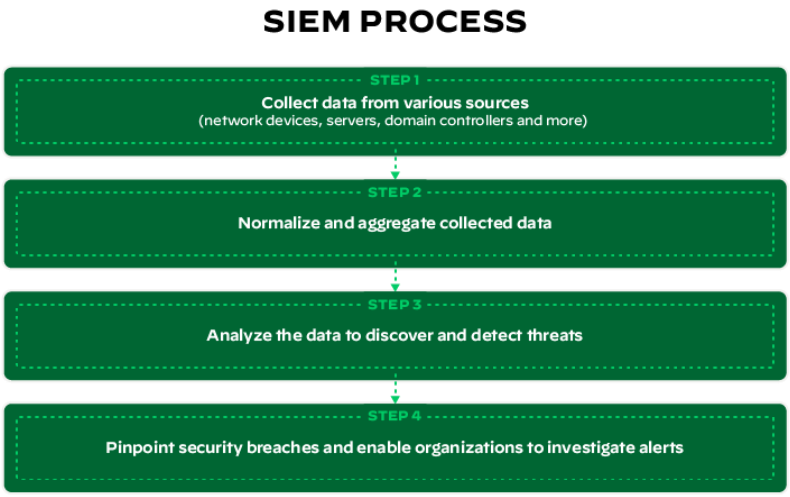
1.1.1 XDR

Características de XDR,

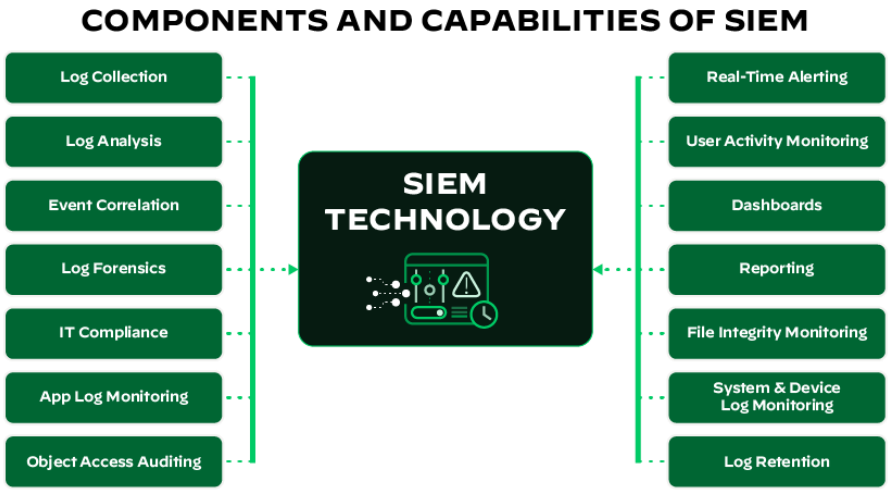


1.1.2 SIEM

Proceso de SIEM



Componentes de SIEM



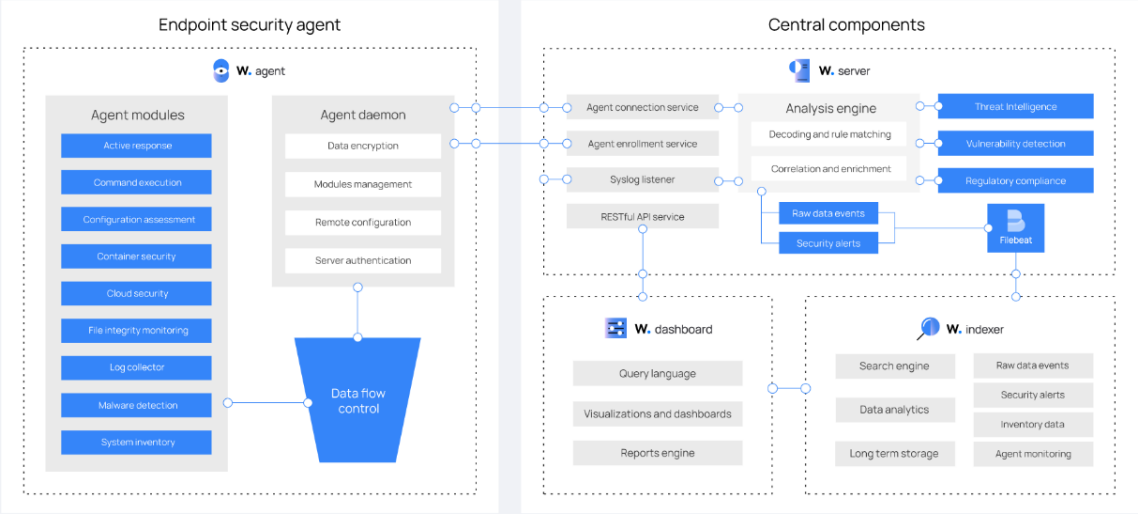
1.2 Wazuh

Es una Plataforma de seguridad que permite que las organizaciones protejan sus activos informáticos de amenazas de seguridad informática. Esta solución permite proteger las cargas de trabajo en infraestructuras locales, virtualizadas, en contenedores y basadas en la nube.

1.2.1 Generalidades de la arquitectura de Wazuh

La Plataforma de seguridad con protección XDR y SIEM para endpoints y cargas de trabajo en la nube. Esta plataforma actúa como un componente único, un agente universal con tres componentes centrales los cuales son el **servidor de Wazuh, el indexador de Wazuh y el centro o panel de control de Wazuh.**

Componentes de la arquitectura de Wazuh.



Wazuh Indexer

El indexador es el motor de búsqueda y análisis de cadenas de texto completo y escalable. Se encarga de indexar y almacenar las alertas generadas por el servidor de Wazuh.

Wazuh Server

El servidor de Wazuh analiza los datos recibidos de los agentes a través de reglas y decodificadores utilizando inteligencia de amenazas para buscar indicadores de compromiso (IOC) conocidos. Este es el núcleo que procesa y permite gestionar los cientos de miles de agentes, configurándolos y actualizando de forma remota cuando sea necesario.

Wazuh dashboard

El panel de control de Wazuh es la parte frontal del usuario web para visualizar y representar los análisis de datos. Estos son paneles de control listos para visualizar los eventos de seguridad, monitorear el cumplimiento normativo (HIPAA, NIST 800-53, GDPR, CIS, PCI DSS), vulnerabilidades en aplicaciones detectadas, monitoreo de integridad de archivos, evaluaciones de configuración, eventos que permiten monitorear la infraestructura en la nube, así como configuraciones propias de Wazuh que permiten monitorear su estado.

Wazuh Agent

Los agentes de Wazuh son los endpoints que se instalan en portátiles, ordenadores de mesa, servidores, instancias en la nube o máquinas virtuales, esta permite capacidades de prevención detección y respuesta a amenazas. Compatible con Linux, Windows, MacOS, Solaris, AIX y HP-UX. Otras capacidades de monitoreo incluyen dispositivos sin agentes es decir firewalls, conmutadores, enrutadores o IDS de red, entre otras soluciones que son desplegadas en la infraestructura tecnológica, esto por medio de recopilación de Syslog como datos de registros que son monitoreados a través de rastreos periódicos de los datos a través de SSH o APIs.[5]

1.3 Características y módulos de Wazuh

1.3.1 Endpoint Security

Configuration Assessment

Wazuh permite evaluación de la configuración de seguridad de los sistemas, esto permite garantizar el cumplimiento de las mejores prácticas y estándares de seguridad. El módulo SCA identifica errores de configuración y vulnerabilidades en los endpoint monitoreados. La evaluación de la configuración de seguridad ayuda a la comprobación de exposiciones y errores de configuraciones en los endpoints. Esto se trae consigo los beneficios de la detección de vulnerabilidades, fortalecimiento del sistema, mejora en la gestión del cumplimiento, aseguramiento de los sistemas, monitoreo continuo, verificaciones exhaustivas de configuraciones, así como la generación de informes y análisis detallados.[6]

Malware Detection

Esta característica permite aplicar estrategas a través de sus módulos para la detección de amenazas de malware como Ransomware, rootkits, spyware, troyanos, adware, virus y gusanos. Las capacidades incluidas son la de detección de malware. Esto da las ventajas de una protección en tiempo para la visualización centralizada de amenazas y otras integraciones extensibles permitiendo a los expertos ejecutar planes de mitigación oportunamente.[7]

File Integrity Monitoring

Este módulo (FIM) permite supervisar y alertar sobre cambios en archivos y directorios críticos permitiendo que las organizaciones detectar rápidamente archivos que sean comprometidos a ataques cibernéticos. Permite el monitoreo en tiempo real, aseguramiento del cumplimiento normativo interno y una gestión centralizada. El seguimiento de cambios en los atributos, la propiedad y el contenido es un método altamente efectivo para reducir las amenazas internas en los agentes. Este módulo se integra con múltiples plataformas Windows, Linux y MacOS.[8]

1.3.2 Threat Intelligence

Threat Hunting

Las búsquedas avanzadas integradas en Wazuh permite detectar y prevenir ataques persistentes. Esta permite una visibilidad completa de todos los componentes de una infraestructura de TI como registros del sistema operativo, las aplicaciones, bases de datos y mucho más. Estos análisis de los registros generados en los agentes permiten una gran cantidad de datos que son indexados y consultados en el tiempo para facilitar la identificación de problemas. [9]

Además, el mapeo MITRE AT&CK para mitigar las amenazas a través de la inteligencia de amenazas, la respuesta de incidentes y evaluaciones de seguridad permite tener un lenguaje común centralizado con tácticas y técnicas. Las fases de MITRE ATT&CK son el reconocimiento, entrada, expansión, explotación, persistencia, comando y control, movimiento lateral, exfiltración al

conocerlas permite una mejor cobertura ante incidentes de seguridad informática.[10]

Log Data Analysis

El log implica la revisión de todos los registros generados por los equipos en la red, los endpoints y las aplicaciones. Estos registros son una amplia fuente de datos para el análisis de datos que permiten detectar patrones que apoyan los procesos de ciberseguridad (Identificar, Proteger, Detectar, Responder y recuperar) todo esto lo hace en tiempo real, almacenando los registros. La ventaja que proporciona Wazuh con integraciones de terceros amplia los casos de uso para mayor cobertura de la infraestructura. [11]

Vulnerability Detection

Las capacidades anteriores proporcionan una amplia fuente de datos para detectar vulnerabilidades que nos permiten proteger la infraestructura de TI de amenazas cibernéticas. Wazuh utiliza el enfoque basado en riesgo para ayudar al equipo en la priorización de amenazas más críticas, categorizando las amenazas por nivel de severidad. Esta capacidad de detección de vulnerabilidades permite identificar y remediar las vulnerabilidades de forma proactiva de tal forma que se mitigan los riesgos.[12]

1.3.3 Security Operations

Incident Response

La respuesta a incidentes son el conjunto de acciones y procesos que apoyan a las organizaciones para abordar las amenazas detectadas en la infraestructura desde el proceso de detección hasta la metida que aborda la amenaza para eliminarla o mitigarla. Esta permite que los equipos respondan de manera eficaz a los incidentes de seguridad. En Wazuh se pueden configurar respuestas automatizadas a estos, se pueden optimizar las operaciones de seguridad, integrarse con terceros y reducir los tiempos. Esta respuesta incluye bloqueos de peticiones de red sospechosas, eliminación de archivos maliciosos, puesta en cuarentena de terminales entre otras. La optimización se realiza por medio de la centralización de la supervisión, la generación de alertas y análisis de

todos los registros y eventos en tiempo real. La integración con terceros permite orquestar con Wazuh server otras herramientas de inteligencia y detección, así como herramientas de alertas y comunicación.[13]

Regulatory Compliance

El cumplimiento normativo involucra hacer cumplir las obligaciones, políticas, estándares, procedimientos, normas y entorno a la seguridad informática. Esto permite abordar la complejidad de alinear a la empresa al cumplimiento de los requisitos específicos de altos estándares reglamentarios como PCI DSS, HIPPA, GDPR, NIST 800-53 y TSC entre otras de cada país. Además, simplifica la auditoria de la infraestructura notificando incumplimiento, optimización de las actividades relacionadas a hacer cumplir los mecanismos de control interno. Es posible crear políticas personalizadas a través del módulo FIM esto para adaptar los controles internos. [14]

IT Hygiene

Esta característica permite tener las mejores prácticas y medidas para mantener la seguridad, la disponibilidad y mayor eficiencia de la infraestructura. Cuando una organización no cuenta con una adecuada gestión de tecnología los atacantes aprovechan las brechas. Implementar Wazuh permite obtener una visibilidad completa del inventario informático, desde los datos, sistemas operativos, aplicaciones, interfaces de red y afrontar las amenazas aplicando el proceso de ciberseguridad.[15]

1.3.4 Cloud Security

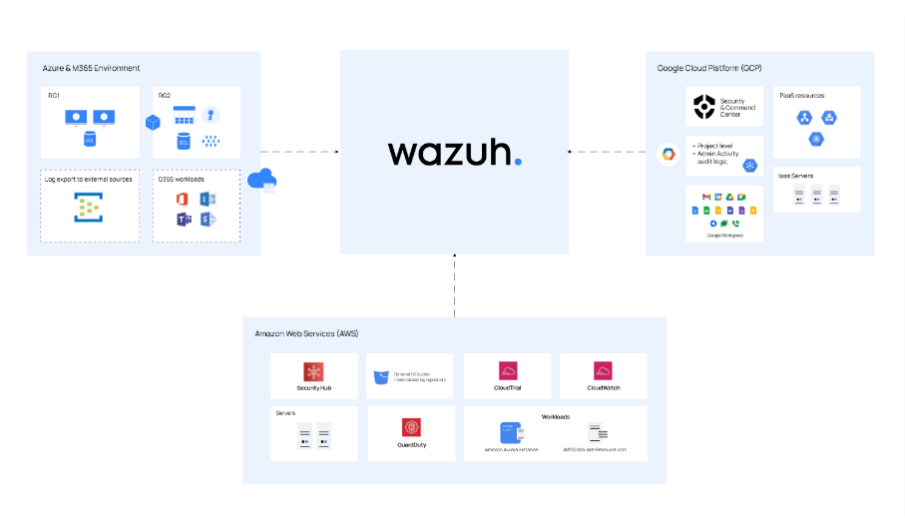
Container Security

La seguridad en los contenedores implica medidas de seguridad para proteger este entorno de virtualización, así como la infraestructura subyacente de las amenazas a lo largo del ciclo de vida de estos. Esto a través de la detección de amenazas, auditoria a las plataformas de orquestación e inventario de los contenedores, supervisión de los estados de los contenedores y su supervisión de ejecución.[16]

Posture Management

El crecimiento del uso de los servicios en la nube requiere de una postura que nos permita evaluar, mejorar y mantener esta seguridad en la nube. Las cargas de trabajo en entornos en la nube involucran identificar riesgos de seguridad y garantizar el cumplimiento en este entorno. La integración con los proveedores en la nube es altamente soportada en Wazuh permitiendo integraciones con AWS, Azure entre otras. Esto permite evaluar las configuraciones de seguridad en este entorno detectando errores de configuración, puertos sin restricciones, usuarios con privilegios excesivos entre otros.[17]

Cloud Workload Protection



La protección de cargas de trabajo en la nube en sus implementaciones hibridas garantizan que todos los recursos en la nube sean supervisados y protegidos. Wazuh permite proteger estas cargas de las plataformas adoptadas en la nube como AWS, GOOGLE CLOUD y AZURE. Esto incluye la captura y análisis de los registros de estos entornos, la detección de las amenazas y la respuesta, la gestión de vulnerabilidades y la supervisión de los archivos.[18]

Proceso de implementación y configuración

1.4 Requerimientos de Wazuh

Los requisitos de hardware dependen en gran medida del número de puntos de conexión protegidos y de la cantidad de cargas de trabajo en la nube. Este número nos ayuda a estimar cuantos datos se procesan y analizan además de la cantidad de alertas de seguridad que se almacenan e indexan.

La implementación rápida de Wazuh implica desplegar el servidor de Wazuh, el indexador y el panel de control en un mismo host.

Agentes	CPU	RAM	Almacenamiento (90 días)
1–25	4 vCPU	8 GiB	50 GB
25–50	8 vCPU	8 GiB	100 GB
50–100	8 vCPU	8 GiB	200 GB

1.4.1 Sistemas operativos recomendados Wazuh

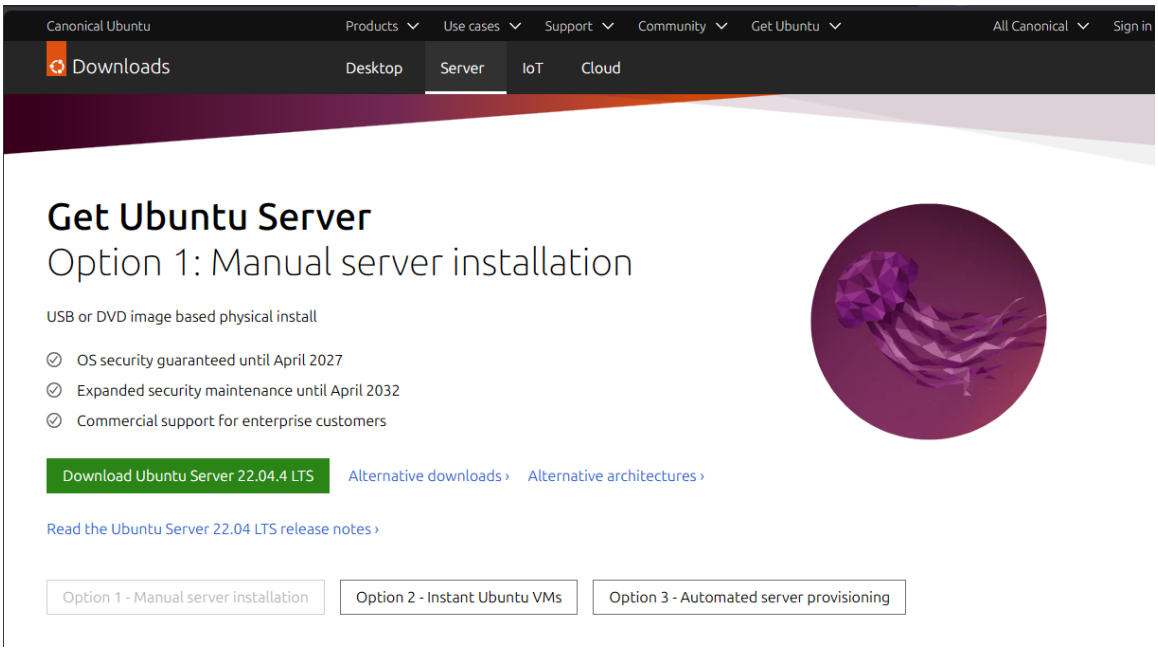
Los componentes CORE de Wazuh se pueden instalar en sistemas operativos Linux de 64 bits. Wazuh este recomendado para los siguientes sistemas operativos:

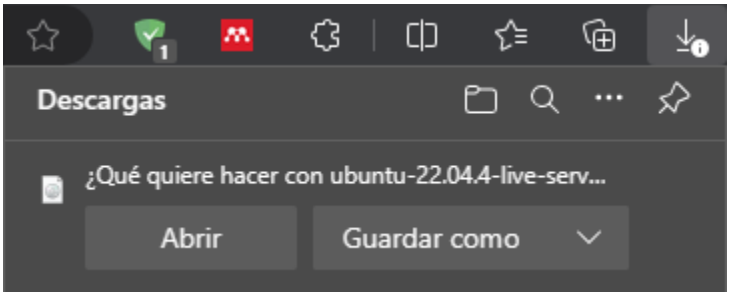
Amazon Linux 2	CentOS 7, 8
Red Hat Enterprise Linux 7, 8, 9	Ubuntu 16.04, 18.04, 20.04, 22.04

Los navegadores web compatibles para gestionar la interfaz de panel de control son: Chromium, Chrome 95, Firefox 93 y Safari 13.7 o versiones posteriores a estas.

1.5 Descarga de sistema operative Ubuntu

Desde la página oficial de Ubuntu descargamos el sistema operativo Ubuntu Server 22.04 https://ubuntu.com/download/server .

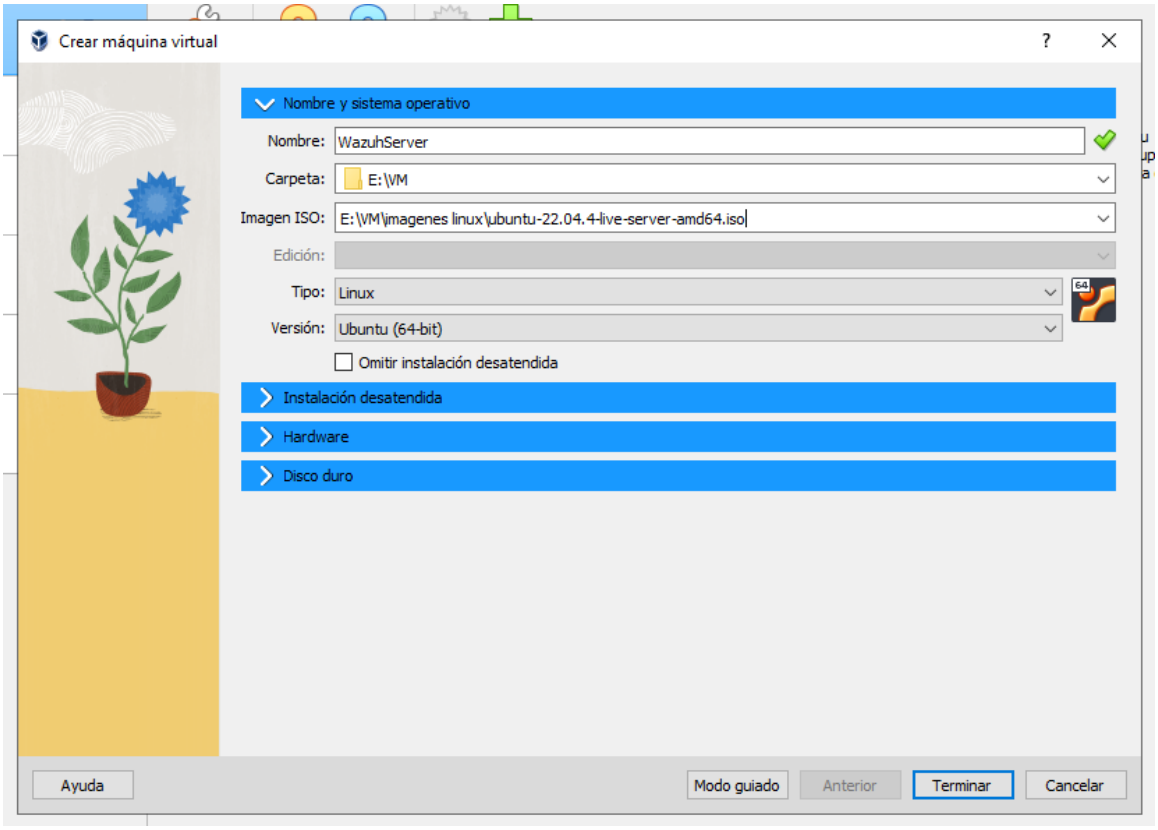




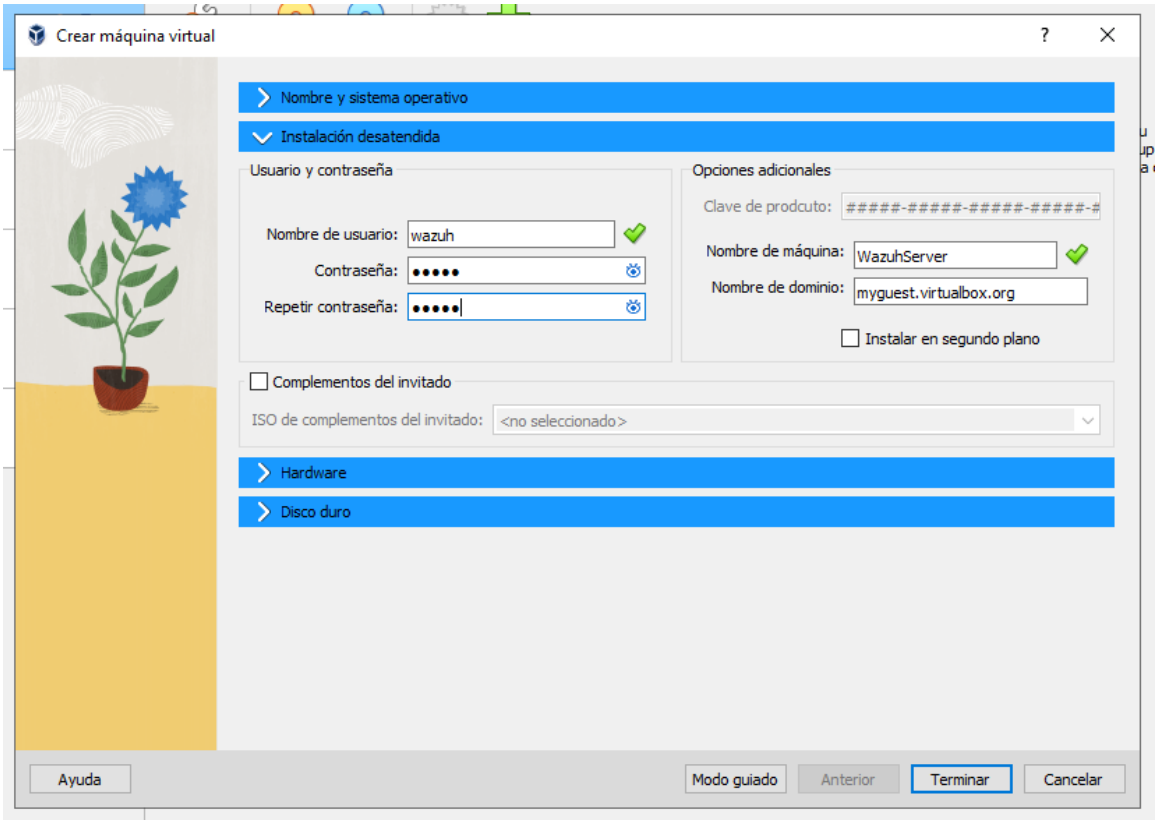
Una vez descargado creamos una máquina virtual con VirtualBox configurando la máquina virtual a los requerimientos mínimos del servidor de Wazuh.

1.6 Configuraciones máquina virtual

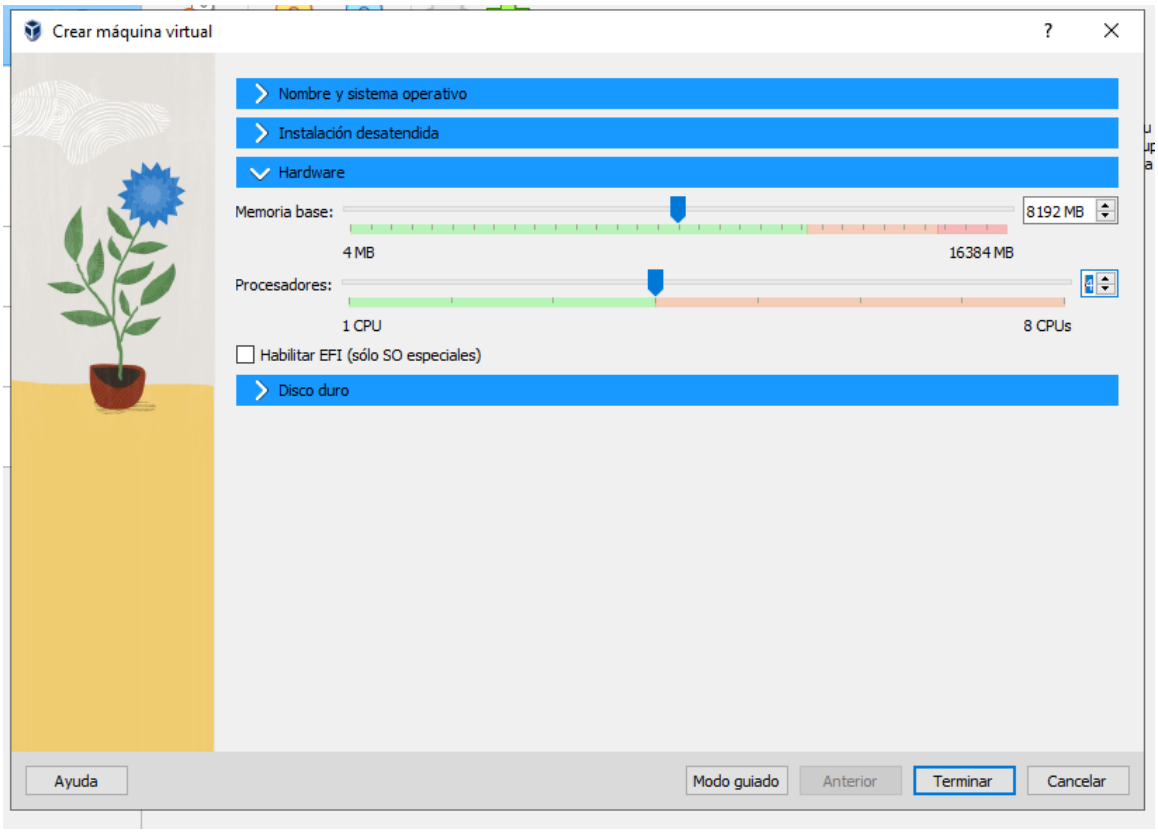
Asignación del nombre y ubicación de la máquina virtual.



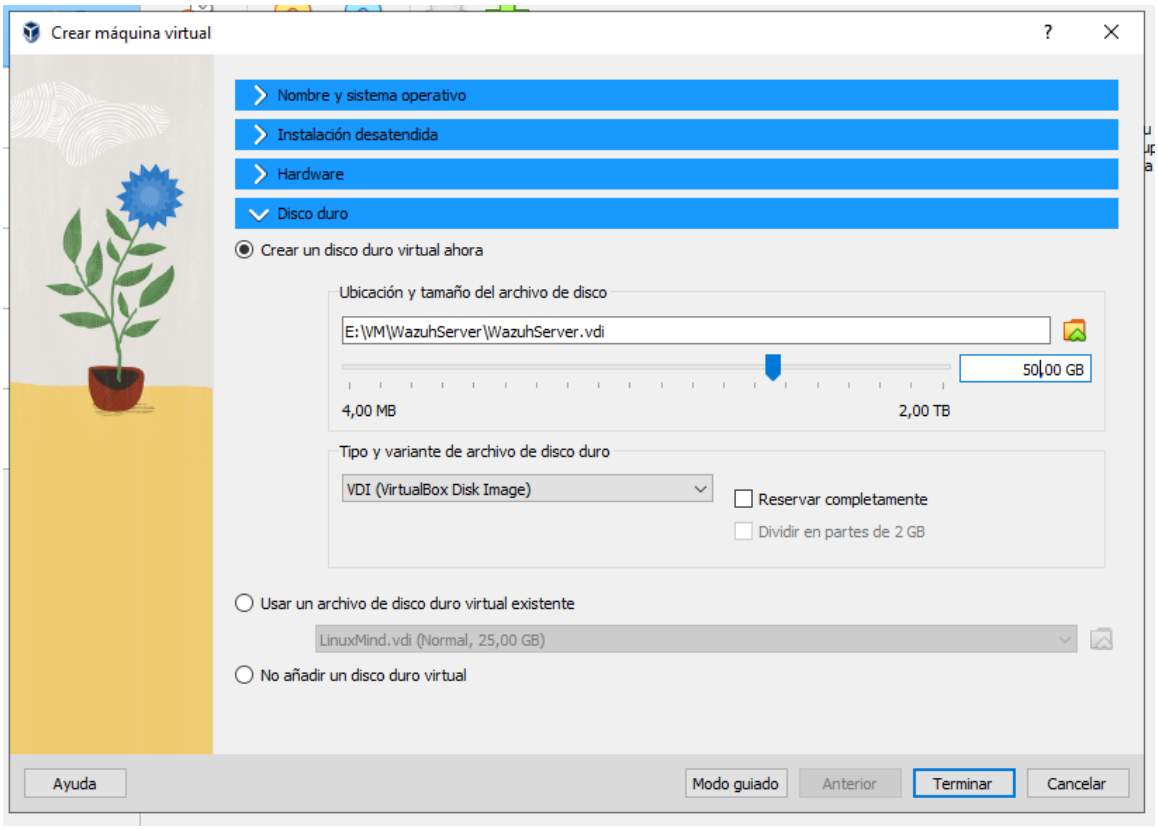
Creación de nombre de usuario y contraseña



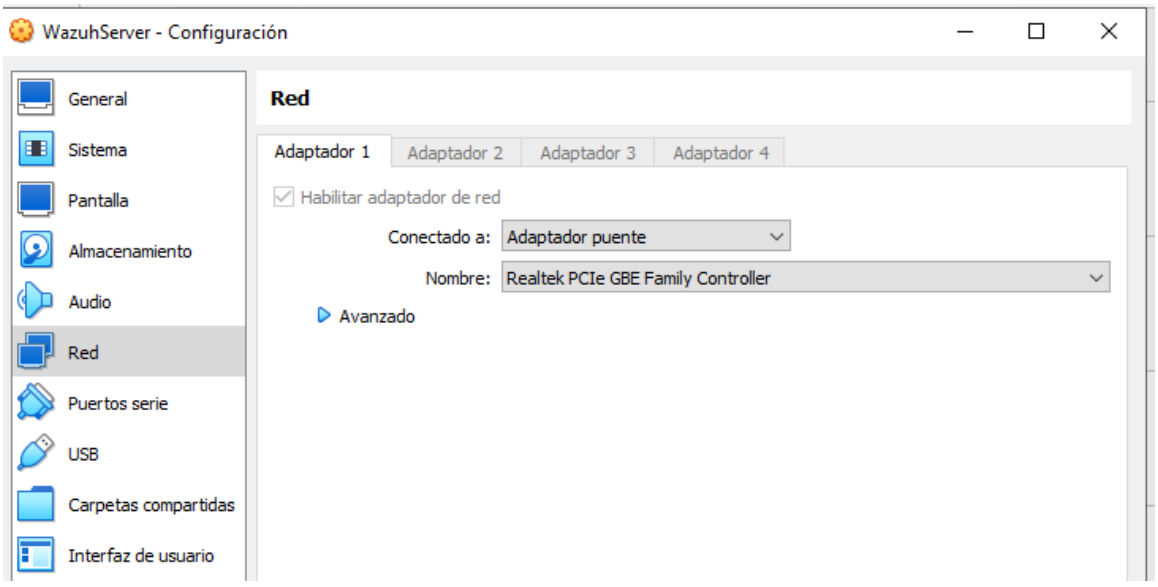
Configuración de hardware de máquina virtual Ubuntu Server



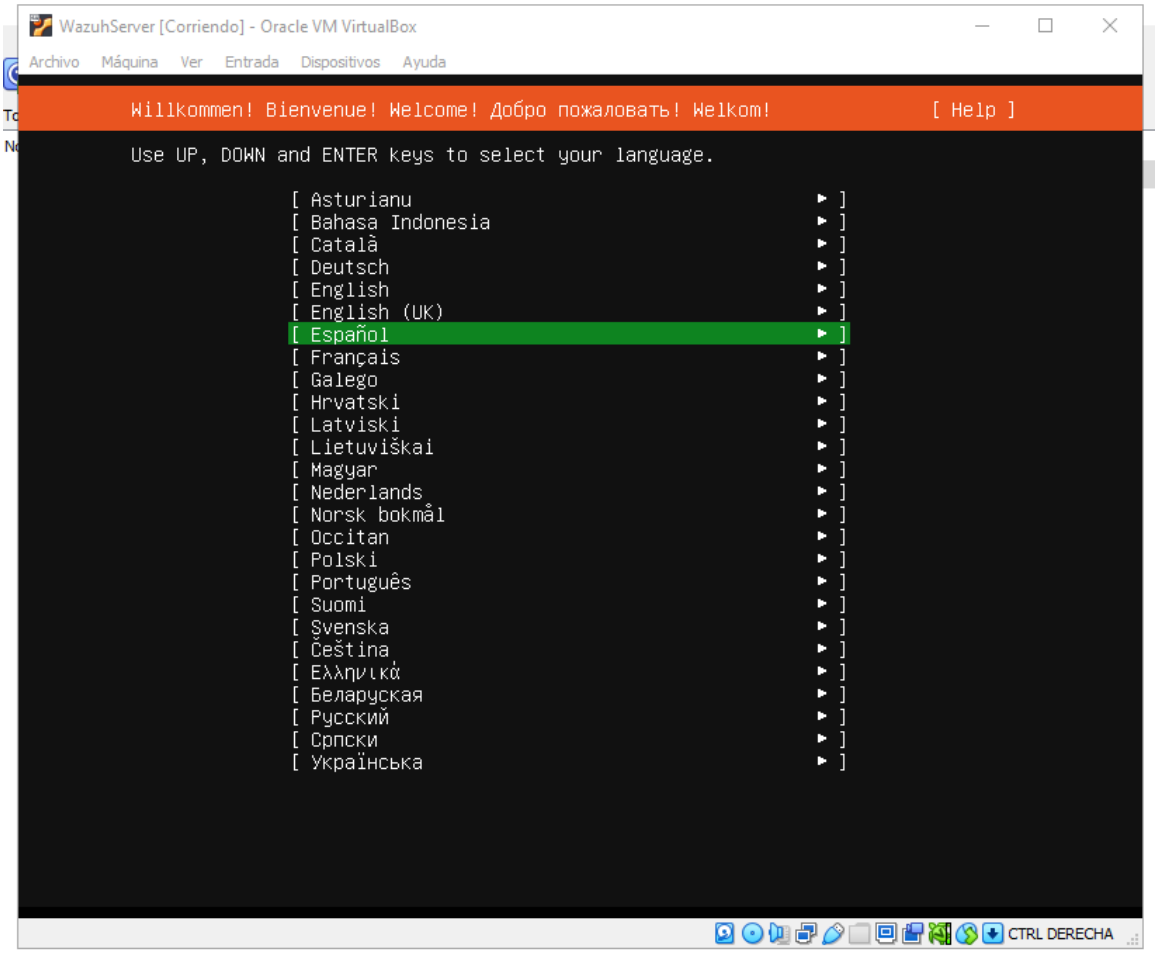
Configuración de disco duro



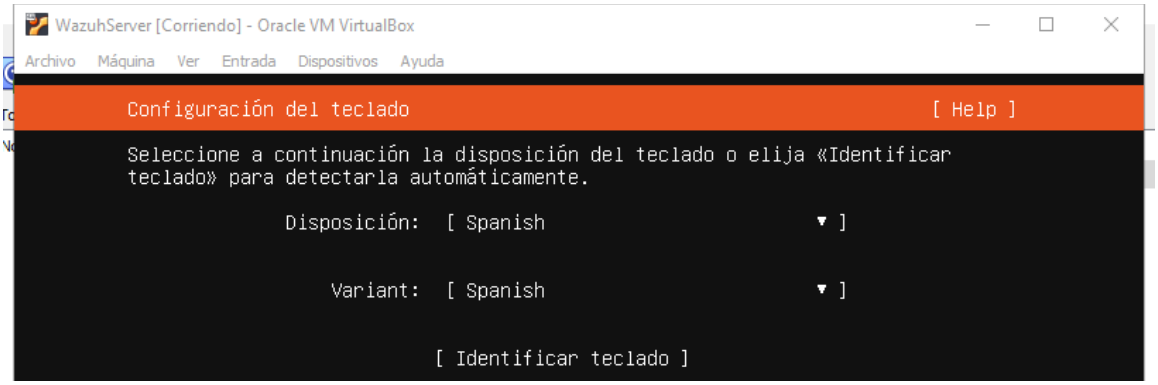
Configuraciones de red



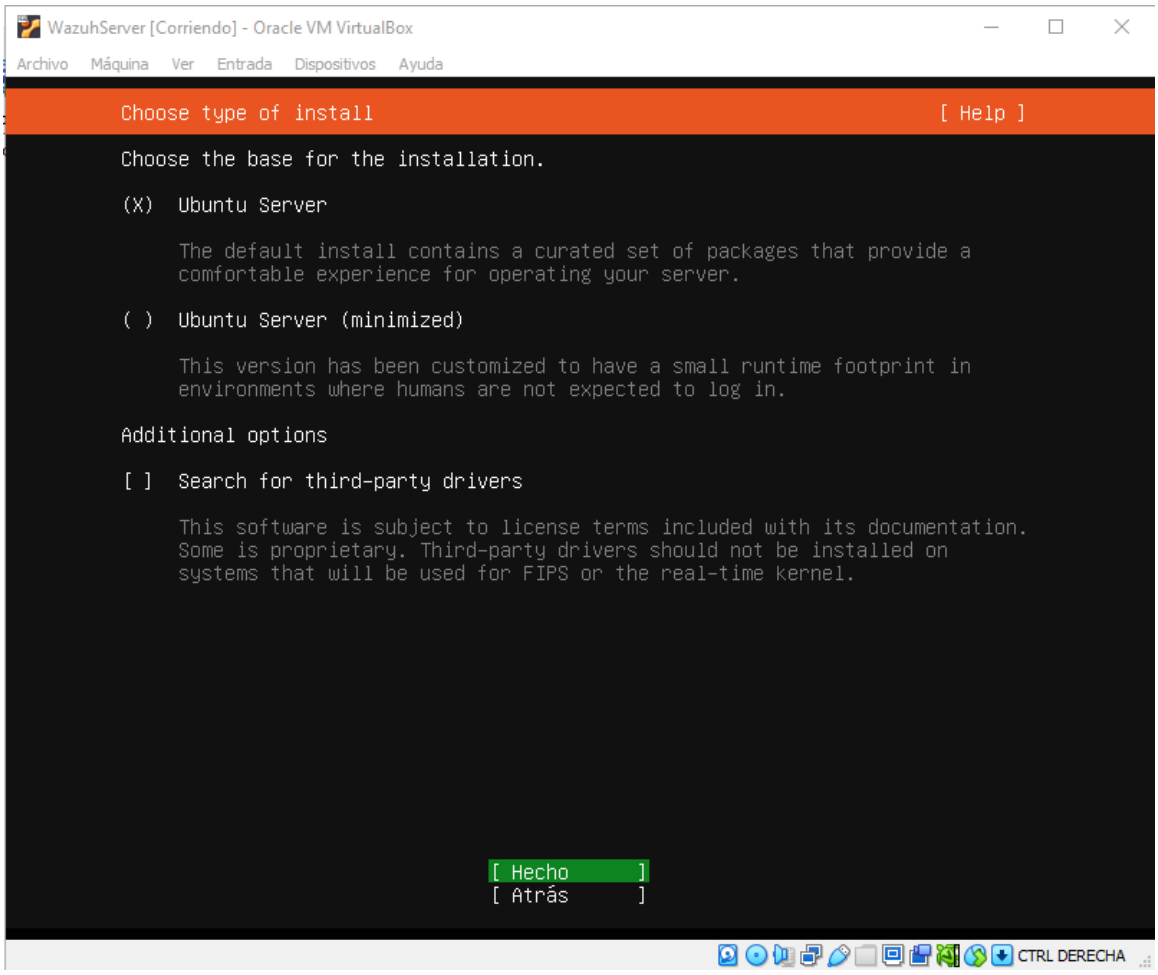
Instalación del sistema operativo



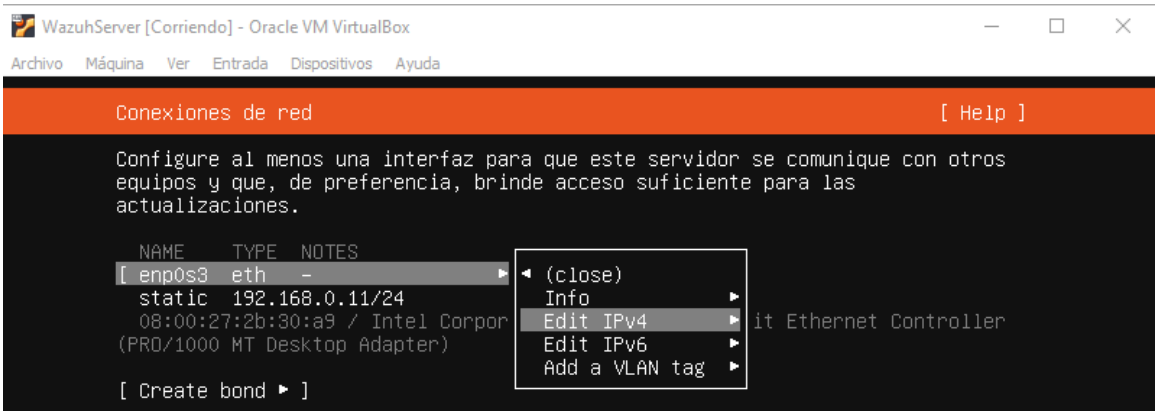
Configuración del teclado

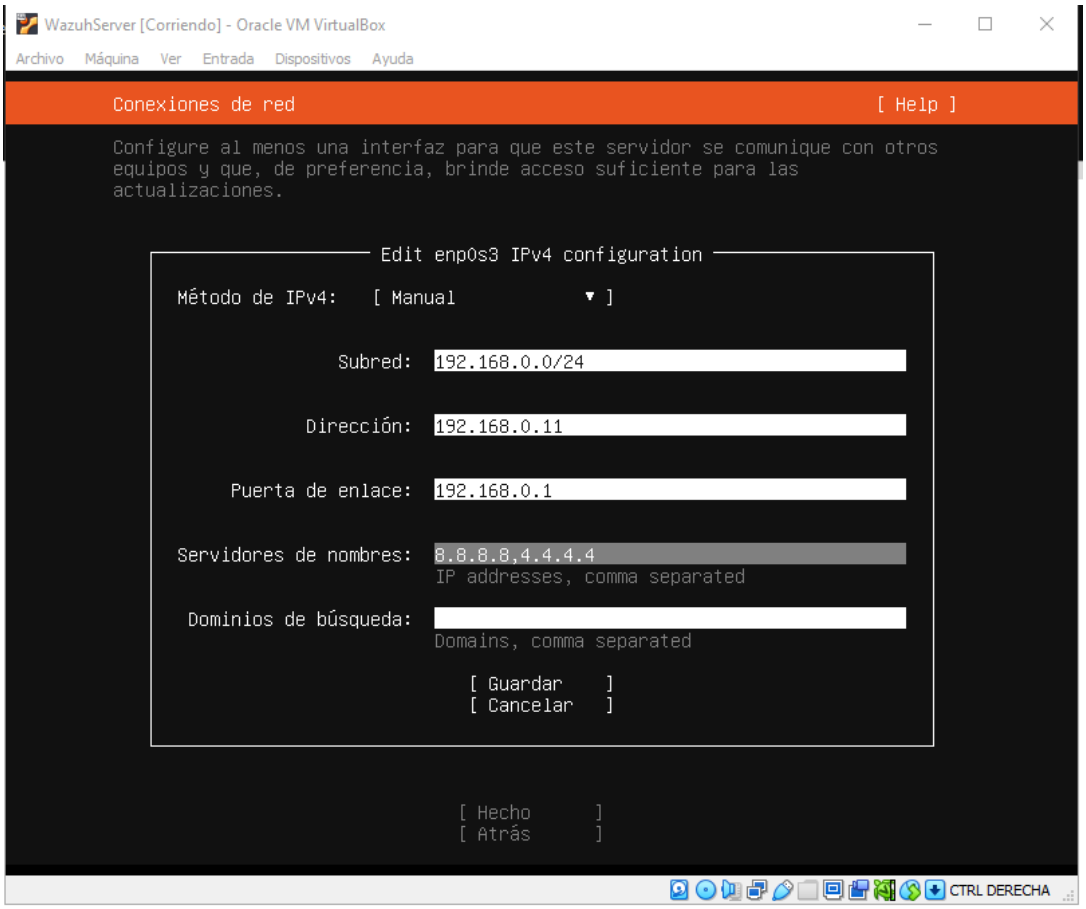


Tipo de instalación

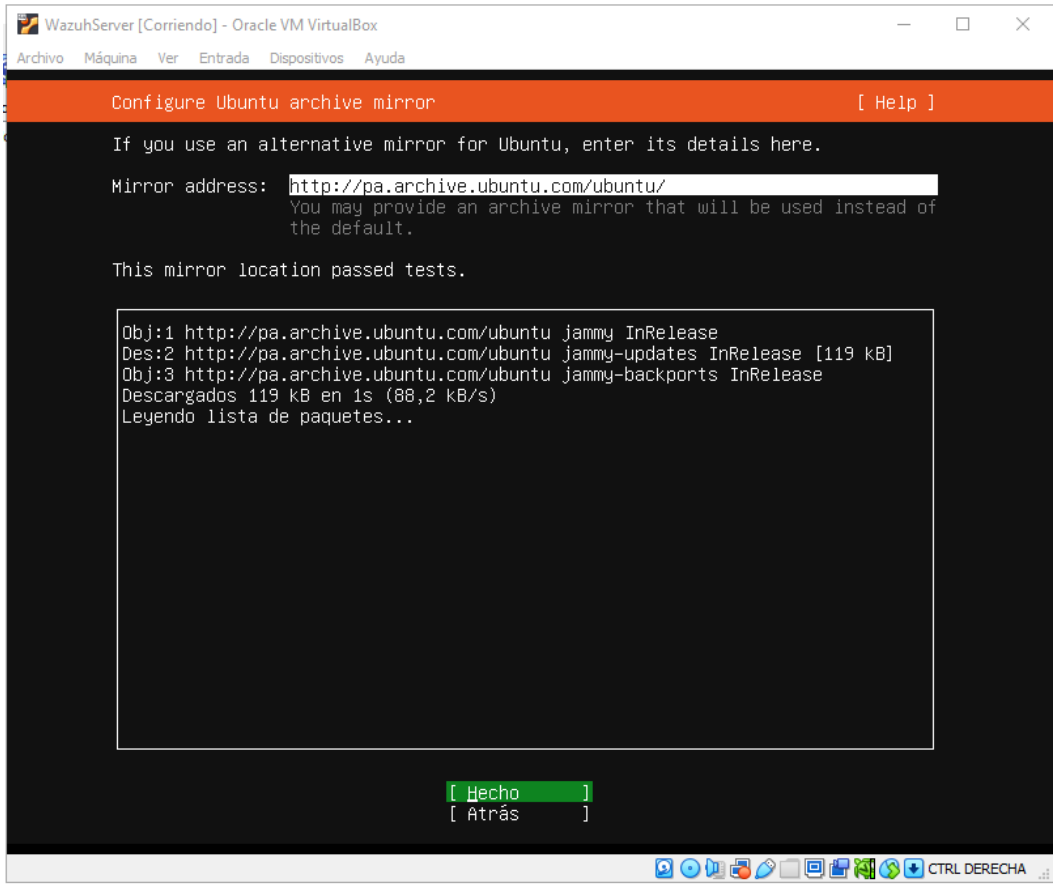


Configuración de red estática

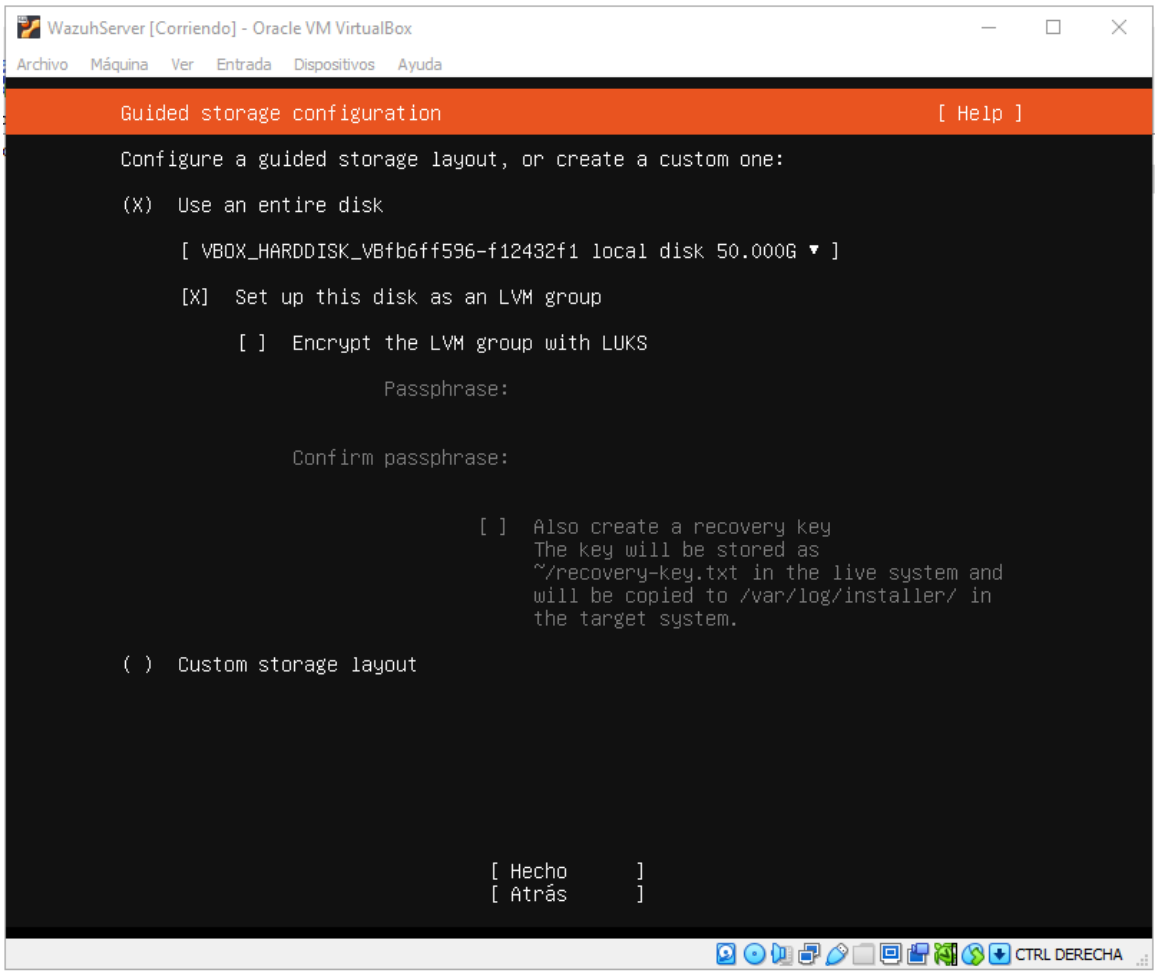


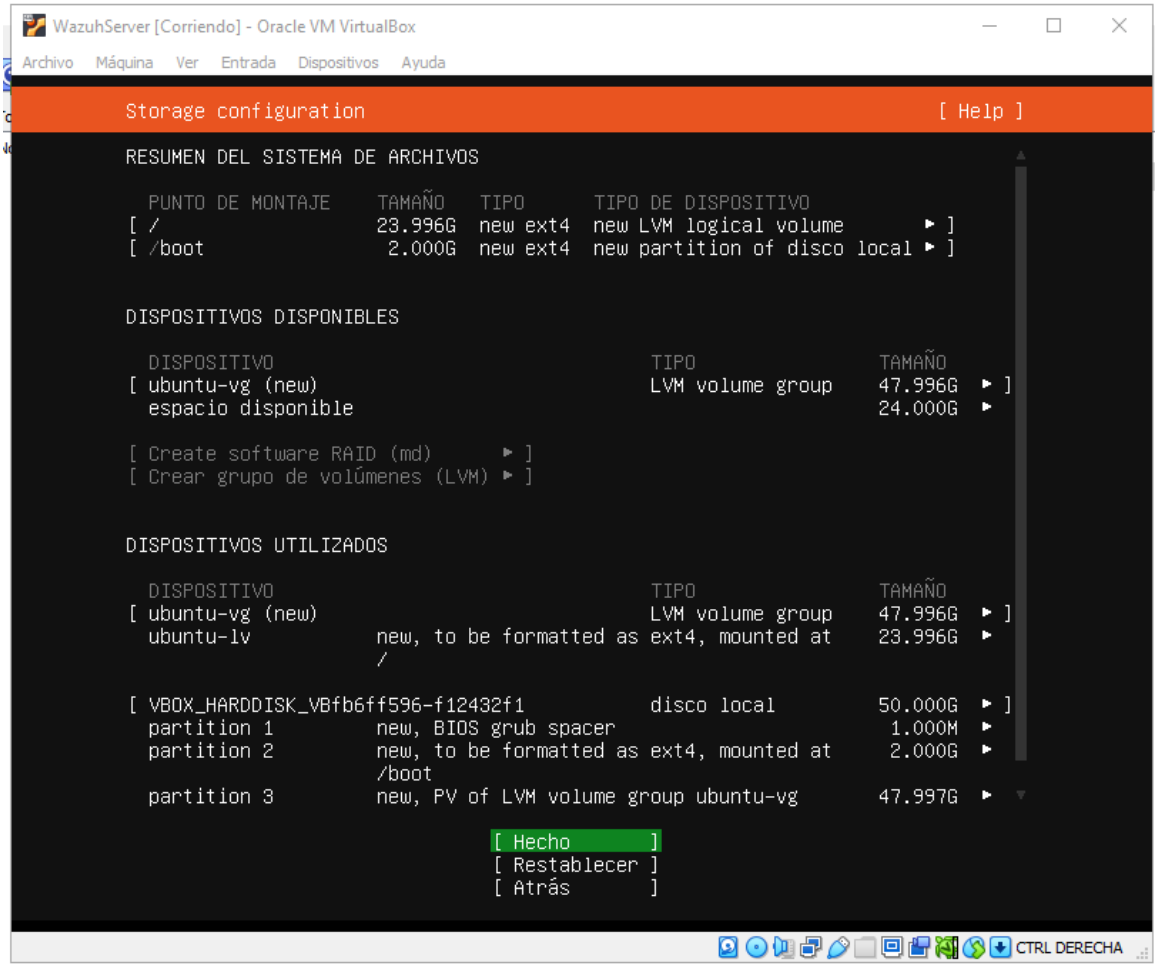


Configuración de mirror

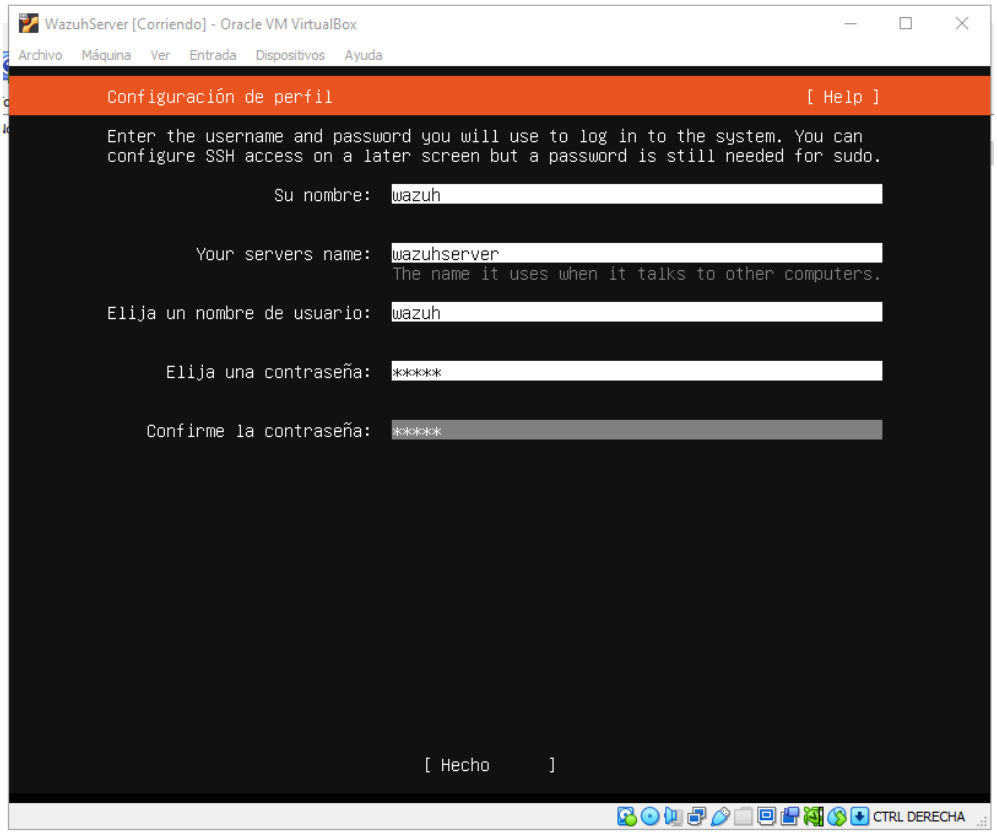


Configuración de discos

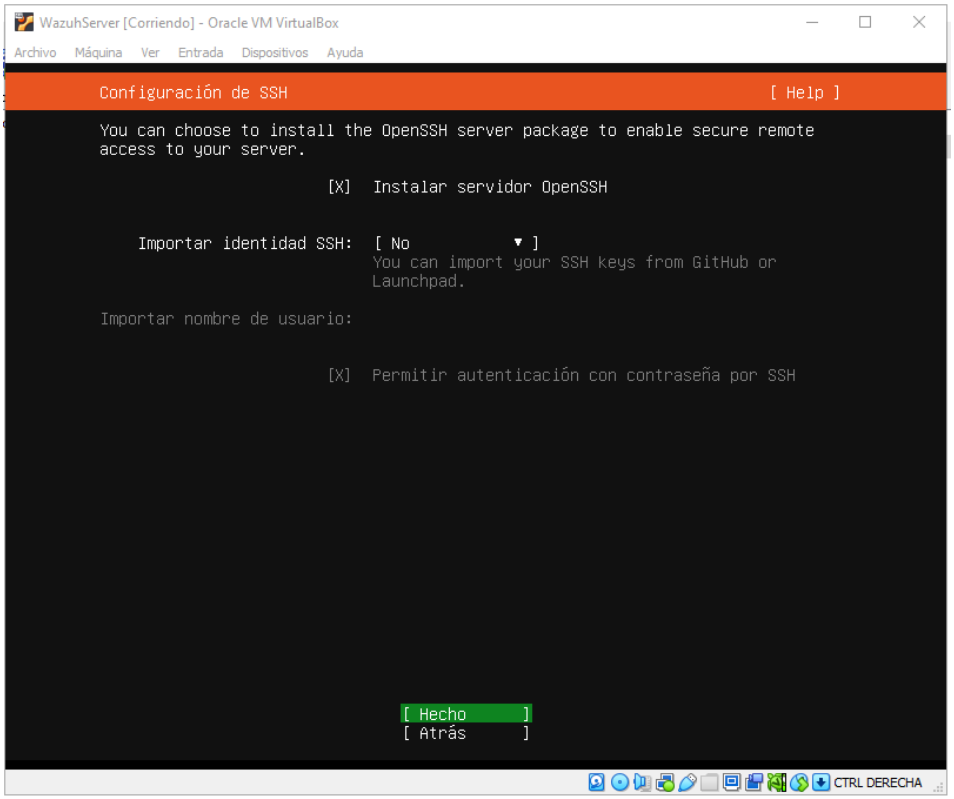

WazuhServer [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Guided storage configuration [Help]
Configure a guided storage layout, or create a custom one:
(X) Use an entire disk
[VBOX_HARDDISK_VBfb6ff596-f12432f1 local disk 50.000G ▾]
[X] Set up this disk as an LVM group
[ ] Encrypt the LVM group with LUKS
Passphrase:
Confirm passphrase:
[ ] Also create a recovery key
The key will be stored as
~/recovery-key.txt in the live system and
will be copied to /var/log/installer/ in
the target system.
( ) Custom storage layout
[Hecho]
[Atrás]
CTRL DERECHA



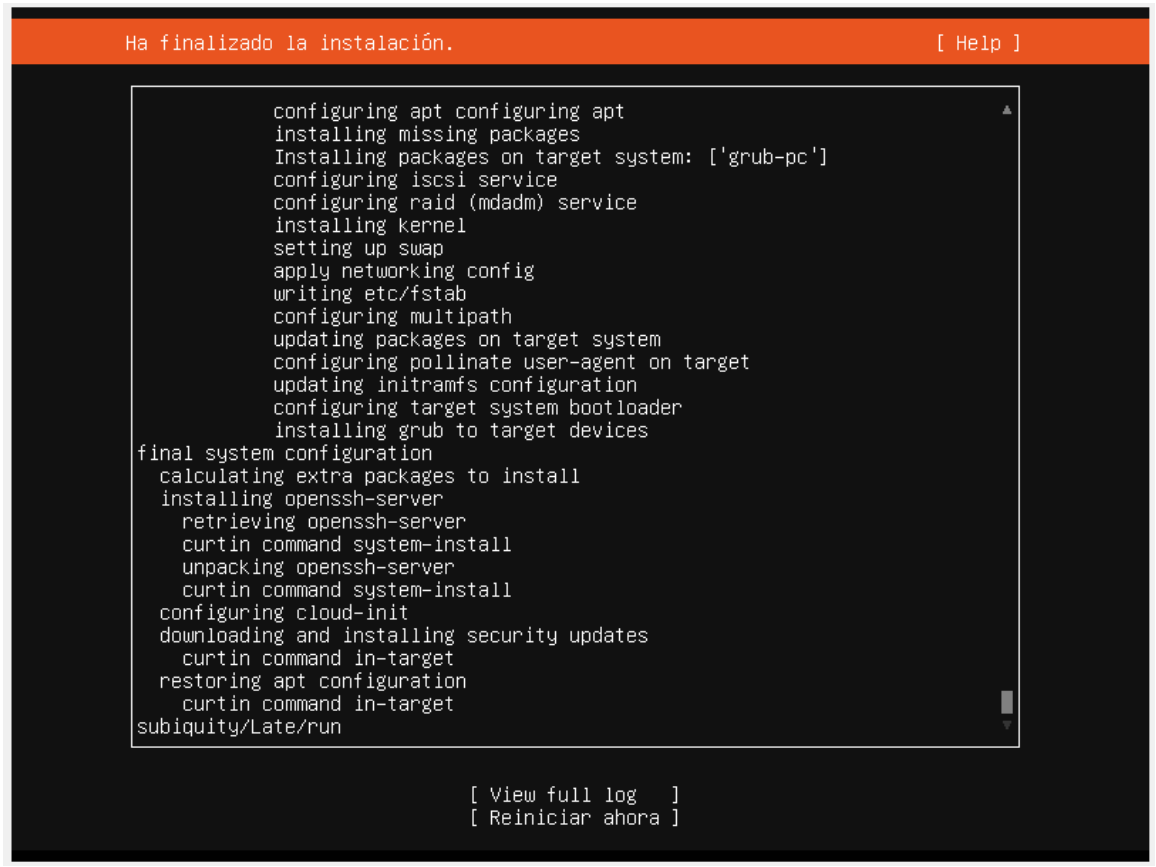
Configuraciones de perfiles de usuario y equipo



Instalación de SSH

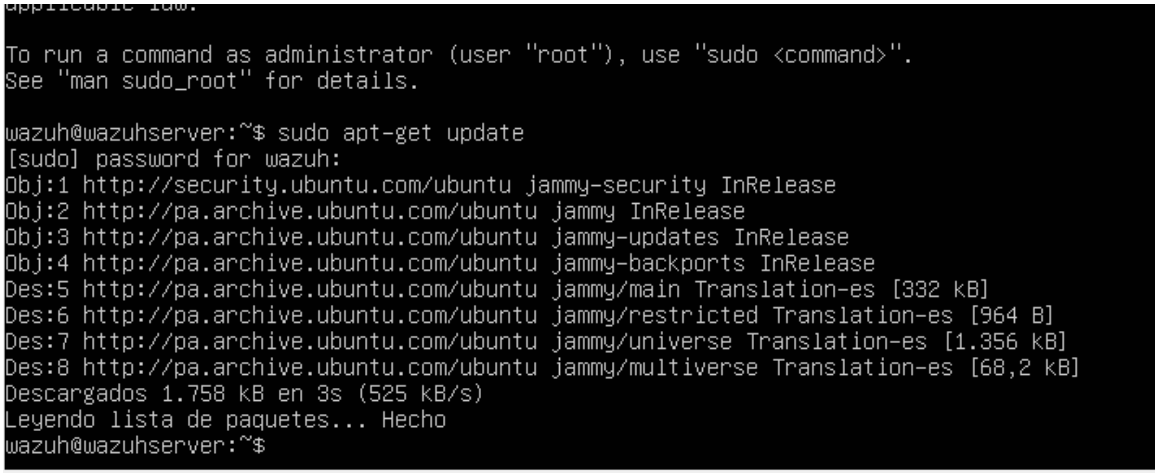


Proceso de instalación del sistema



Actualización del servidor Ubuntu

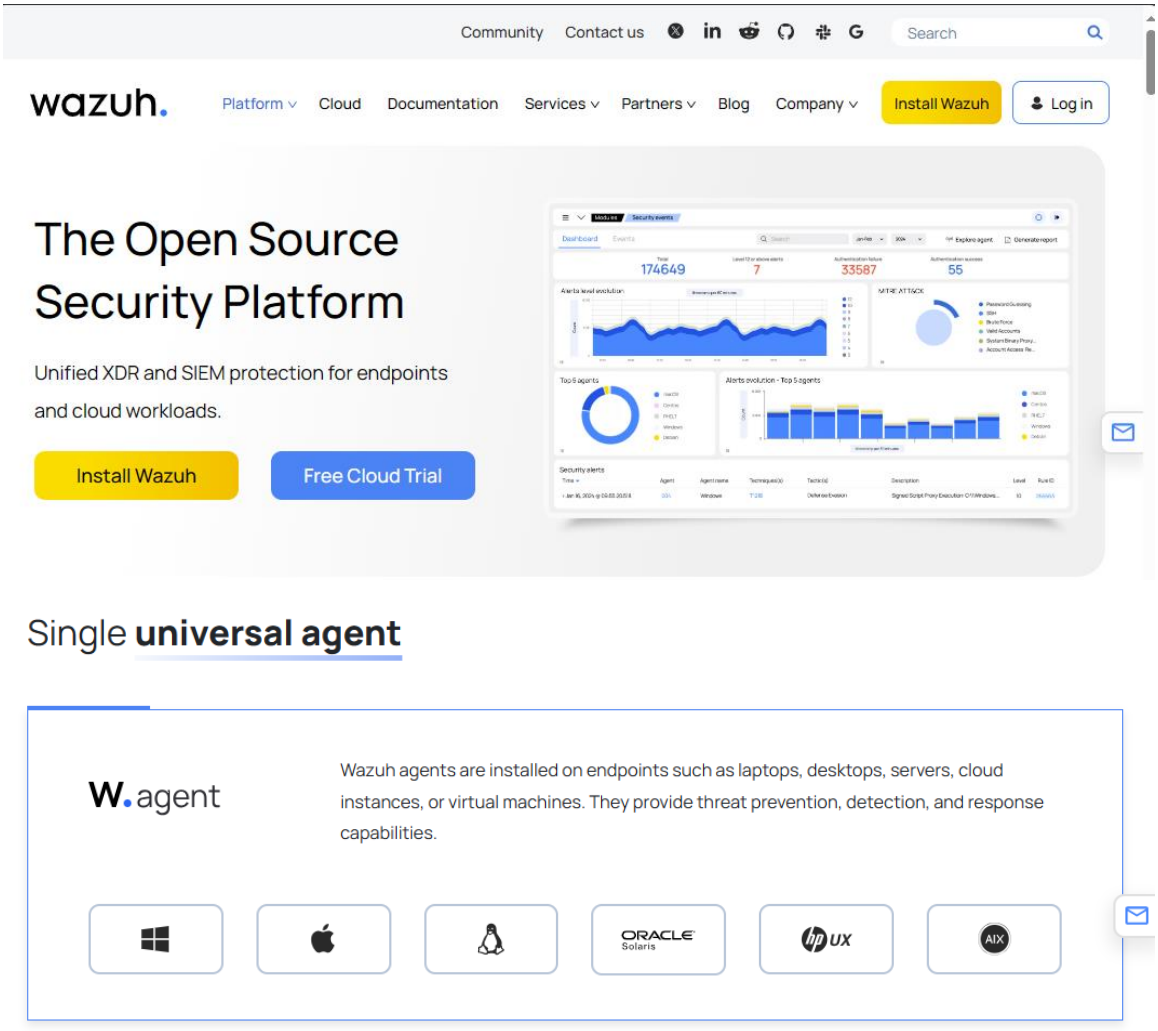
Comando: sudo apt-get update, sudo apt-get upgrade



```
wazuh@wazuhserver:~$ sudo apt-get upgrade
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Calculando la actualización... Hecho
Se actualizarán los siguientes paquetes:
  cloud-init tcpdump
2 actualizados, 0 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
Se necesita descargar 1.053 kB de archivos.
Se utilizarán 61,4 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] S_
```

1.7 Instalación de Wazuh Server.

En la página oficial de Wazuh buscamos los procesos de instalación para Linux, realizamos el proceso de instalación en modalidad All in One Deployment utilizando el asistente de instalación.

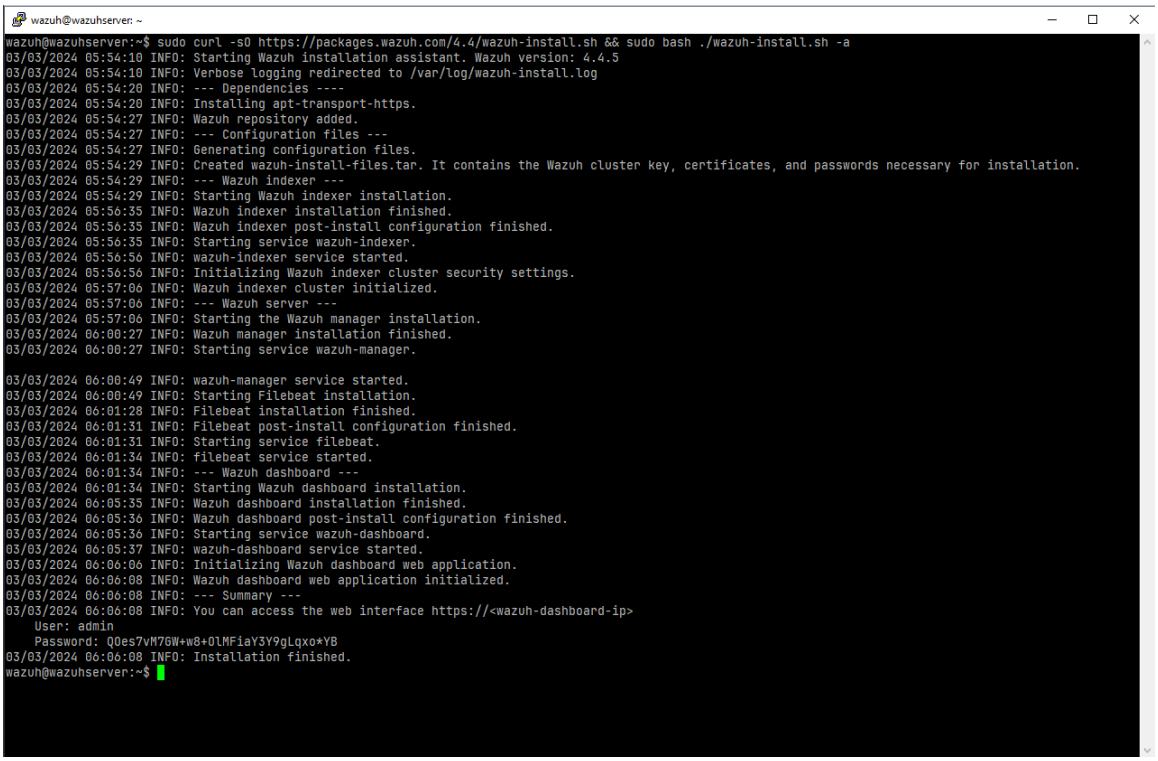


1.8 Proceso de instalación el servidor Wazuh

Descargue y ejecute el asistente de instalación de Wazuh.

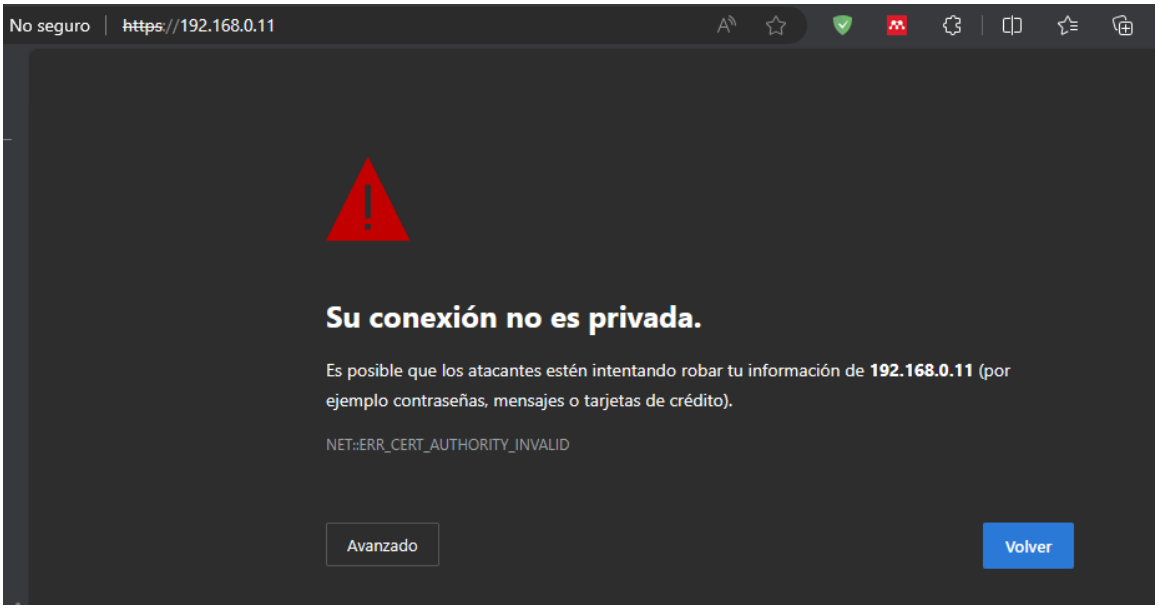
curl -sO https://packages.wazuh.com/4.7/wazuh-install.sh && sudo bash ./wazuh-install.sh -a

Una vez que el asistente finaliza la instalación, el resultado muestra las credenciales de acceso y un mensaje que confirma que la instalación se realizó correctamente.

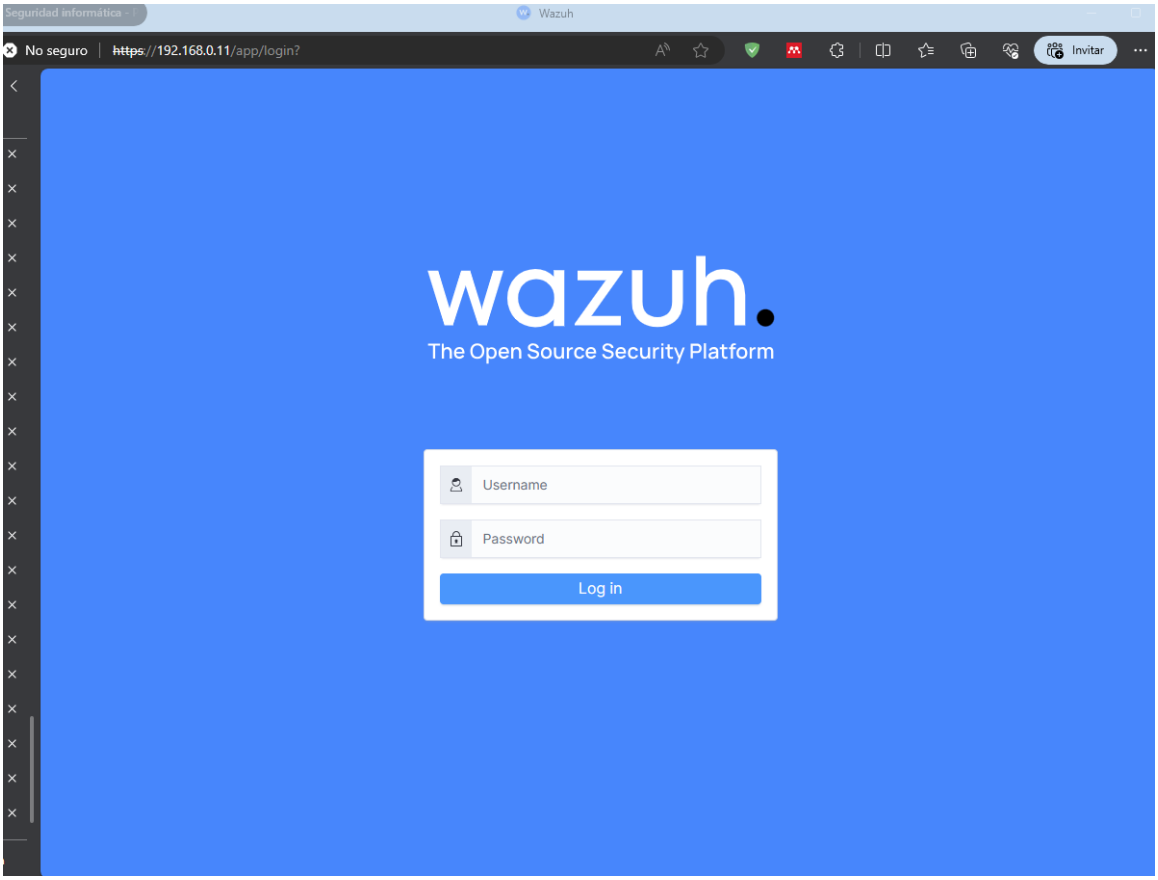


User: admin

Password: QOes7vM7GW+w8+OlMFiaY3Y9gLqxo*YB



Cuando accede al panel de control de Wazuh por primera vez, el navegador muestra un mensaje de advertencia que indica que el certificado no fue emitido por una autoridad de confianza. Esto es lo esperado y el usuario tiene la opción de aceptar el certificado como una excepción o, alternativamente, configurar el sistema para usar un certificado de una autoridad de confianza.[19]



Las contraseñas de todos los usuarios del indexador de Wazuh y de la API de Wazuh en el archivo dentro del archivo txt para imprimirlos, ejecute el siguiente comando:

sudo tar -O -xvf wazuh-install-files.tar wazuh-install-files/wazuh-passwords.txt.

wazuh@wazuhserver:~$ sudo tar -O -xvf wazuh-install-files.tar wazuh-install-files/wazuh-passwords.txt

[sudo] password for wazuh:

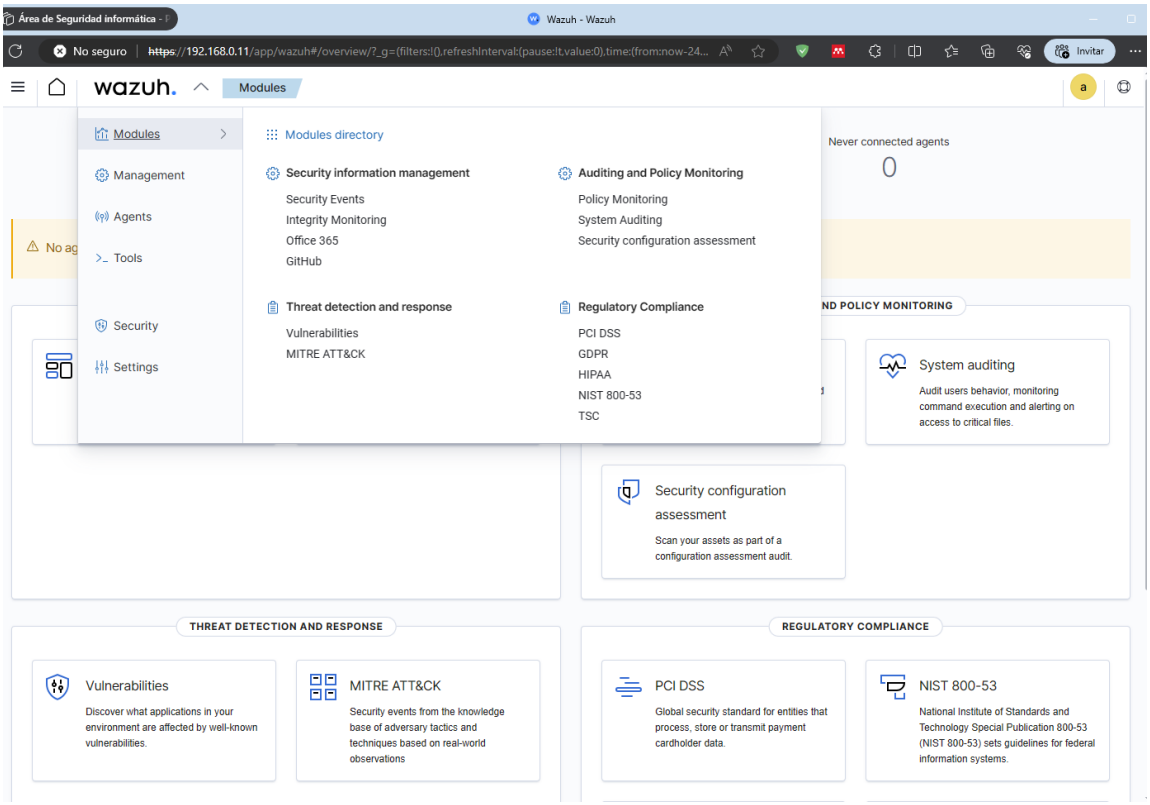
wazuh-install-files/wazuh-passwords.txt

```
# Admin user for the web user interface and Wazuh indexer. Use this user to log in to Wazuh dashboard
  indexer_username: 'admin'
  indexer_password: 'QOes7vM7GW+w8+OlMFiaY3Y9gLqxo*YB'

# Wazuh dashboard user for establishing the connection with Wazuh indexer
  indexer_username: 'kibanaserver'
  indexer_password: 'T8tXYyjv7c.O.h?hJxXNHPWW.r*Rv4dt'

# Regular Dashboard user, only has read permissions to all indices and all permissions on the .kibana index
  indexer_username: 'kibanaro'
  indexer_password: 'UsqTNX5B5n*4eDOf.t.q?4EpDPXAIDsO'

# Filebeat user for CRUD operations on Wazuh indices
  indexer_username: 'logstash'
  indexer_password: 'r0*wqfYLH9qrZ*QWDUGMhVGLiuLqhjRj'

# User with READ access to all indices
  indexer_username: 'readall'
  indexer_password: 'JT3+DV06?vjDa6+ijvn1gK4*76*9Tt8i'

# User with permissions to perform snapshot and restore operations
  indexer_username: 'snapshotrestore'
  indexer_password: 'ai75A3IDS89e4.DjUcnq2SslzJ9akJZP'

# Password for wazuh API user
  api_username: 'wazuh'
  api_password: 'fN.0hMKk3n8?LCrpmlehx7xgCZl*d7yT'
# Password for wazuh-wui API user
  api_username: 'wazuh-wui'
```

api_password: 'gE17dO.M1ysiPoIUmzp1rSD8ewLvHjkH'

Ahora que la instalación de Wazuh está lista, procedemos a implementar los agente de Wazuh. Esto se puede usar para proteger computadoras portátiles, computadoras de escritorio, servidores, instancias en la nube, contenedores o máquinas virtuales.

El agente es liviano y polivalente, lo que proporciona una variedad de capacidades de seguridad.



Wazuh | Part 1 : Components and Capabilities – Igor_sec's Blog (igorsec.blog)

Wazuh | Part 2 : Installing Wazuh and Configuring the Server – Igor_sec's Blog (igorsec.blog)

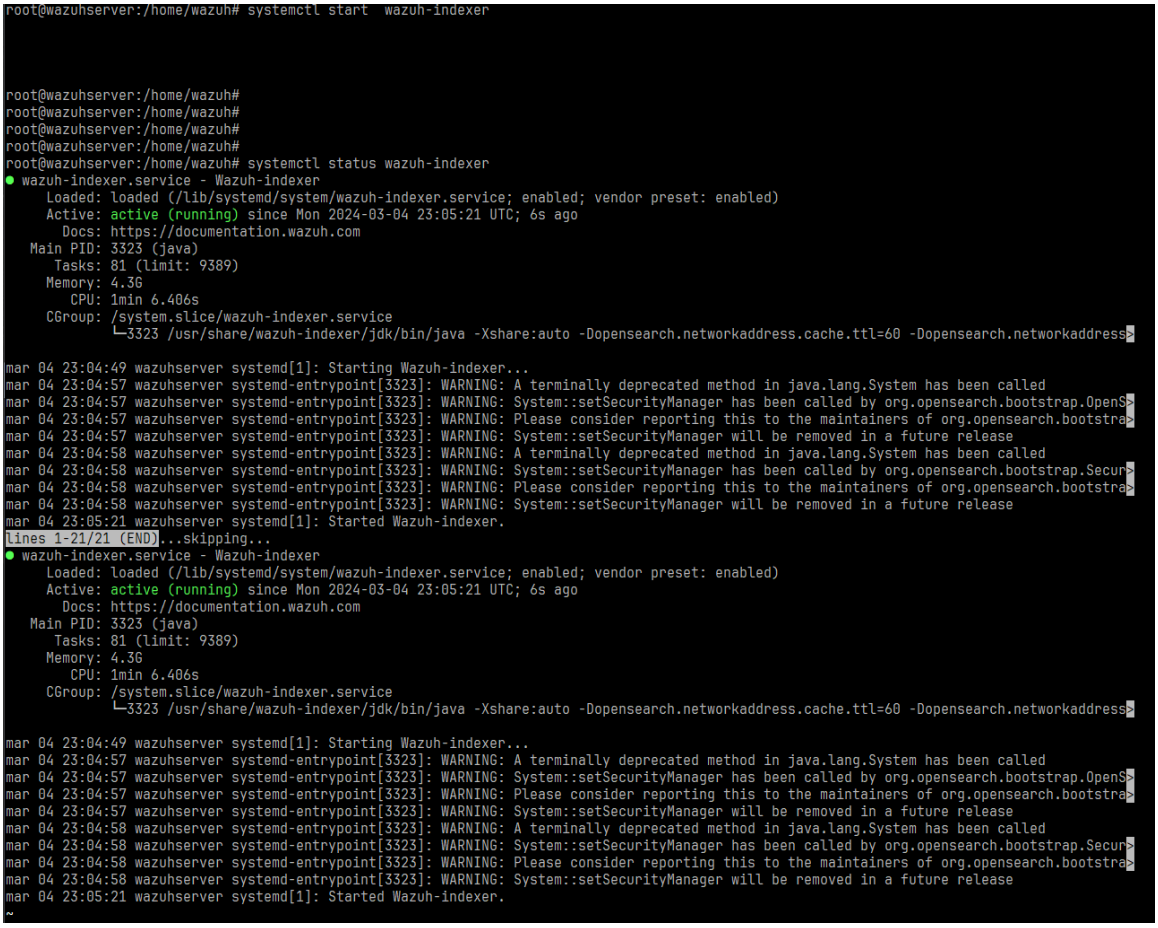
Solución problema Wazuh dashboard server is not ready yet.

El mensaje "El servidor del panel de control de Wazuh aún no está listo" indica un problema que impide que el panel de control de Wazuh acceda a los recursos necesarios. Estos son algunos pasos para solucionar el problema:

1. Comprobación del servicio Wazuh Indexer:

```
root@wazuhserver:/home/wazuh# systemctl status wazuh-indexer
× wazuh-indexer.service - Wazuh-indexer
     Loaded: loaded (/lib/systemd/system/wazuh-indexer.service; enabled; vendor preset: enabled)
     Active: failed (Result: timeout) since Mon 2024-03-04 21:57:18 UTC; 1h 7min ago
       Docs: https://documentation.wazuh.com
    Process: 702 ExecStart=/usr/share/wazuh-indexer/bin/systemd-entrypoint -p ${PID_DIR}/wazuh-indexer.pid --quiet (code=exited, status=143)
   Main PID: 702 (code=exited, status=143)
        CPU: 38.908s

mar 04 21:55:26 wazuhserver systemd-entrypoint[702]: WARNING: Please consider reporting this to the maintainers of org.opensearch.bootstrap>
mar 04 21:55:26 wazuhserver systemd-entrypoint[702]: WARNING: System::setSecurityManager will be removed in a future release
mar 04 21:55:33 wazuhserver systemd-entrypoint[702]: WARNING: A terminally deprecated method in java.lang.System has been called
mar 04 21:55:33 wazuhserver systemd-entrypoint[702]: WARNING: System::setSecurityManager has been called by org.opensearch.bootstrap.Securi>
mar 04 21:55:33 wazuhserver systemd-entrypoint[702]: WARNING: Please consider reporting this to the maintainers of org.opensearch.bootstrap>
mar 04 21:55:33 wazuhserver systemd-entrypoint[702]: WARNING: System::setSecurityManager will be removed in a future release
mar 04 21:57:18 wazuhserver systemd[1]: wazuh-indexer.service: start operation timed out. Terminating.
mar 04 21:57:18 wazuhserver systemd[1]: wazuh-indexer.service: Failed with result 'timeout'.
mar 04 21:57:18 wazuhserver systemd[1]: Failed to start Wazuh-indexer.
mar 04 21:57:18 wazuhserver systemd[1]: wazuh-indexer.service: Consumed 38.908s CPU time.
...skipping...
× wazuh-indexer.service - Wazuh-indexer
     Loaded: loaded (/lib/systemd/system/wazuh-indexer.service; enabled; vendor preset: enabled)
     Active: failed (Result: timeout) since Mon 2024-03-04 21:57:18 UTC; 1h 7min ago
       Docs: https://documentation.wazuh.com
    Process: 702 ExecStart=/usr/share/wazuh-indexer/bin/systemd-entrypoint -p ${PID_DIR}/wazuh-indexer.pid --quiet (code=exited, status=143)
   Main PID: 702 (code=exited, status=143)
        CPU: 38.908s

mar 04 21:55:26 wazuhserver systemd-entrypoint[702]: WARNING: Please consider reporting this to the maintainers of org.opensearch.bootstrap>
mar 04 21:55:26 wazuhserver systemd-entrypoint[702]: WARNING: System::setSecurityManager will be removed in a future release
mar 04 21:55:33 wazuhserver systemd-entrypoint[702]: WARNING: A terminally deprecated method in java.lang.System has been called
mar 04 21:55:33 wazuhserver systemd-entrypoint[702]: WARNING: System::setSecurityManager has been called by org.opensearch.bootstrap.Securi>
mar 04 21:55:33 wazuhserver systemd-entrypoint[702]: WARNING: Please consider reporting this to the maintainers of org.opensearch.bootstrap>
mar 04 21:55:33 wazuhserver systemd-entrypoint[702]: WARNING: System::setSecurityManager will be removed in a future release
mar 04 21:57:18 wazuhserver systemd[1]: wazuh-indexer.service: start operation timed out. Terminating.
mar 04 21:57:18 wazuhserver systemd[1]: wazuh-indexer.service: Failed with result 'timeout'.
mar 04 21:57:18 wazuhserver systemd[1]: Failed to start Wazuh-indexer.
mar 04 21:57:18 wazuhserver systemd[1]: wazuh-indexer.service: Consumed 38.908s CPU time.
~
```

Como el servicio está en estado failed se procede a iniciar nuevamente el servicio.



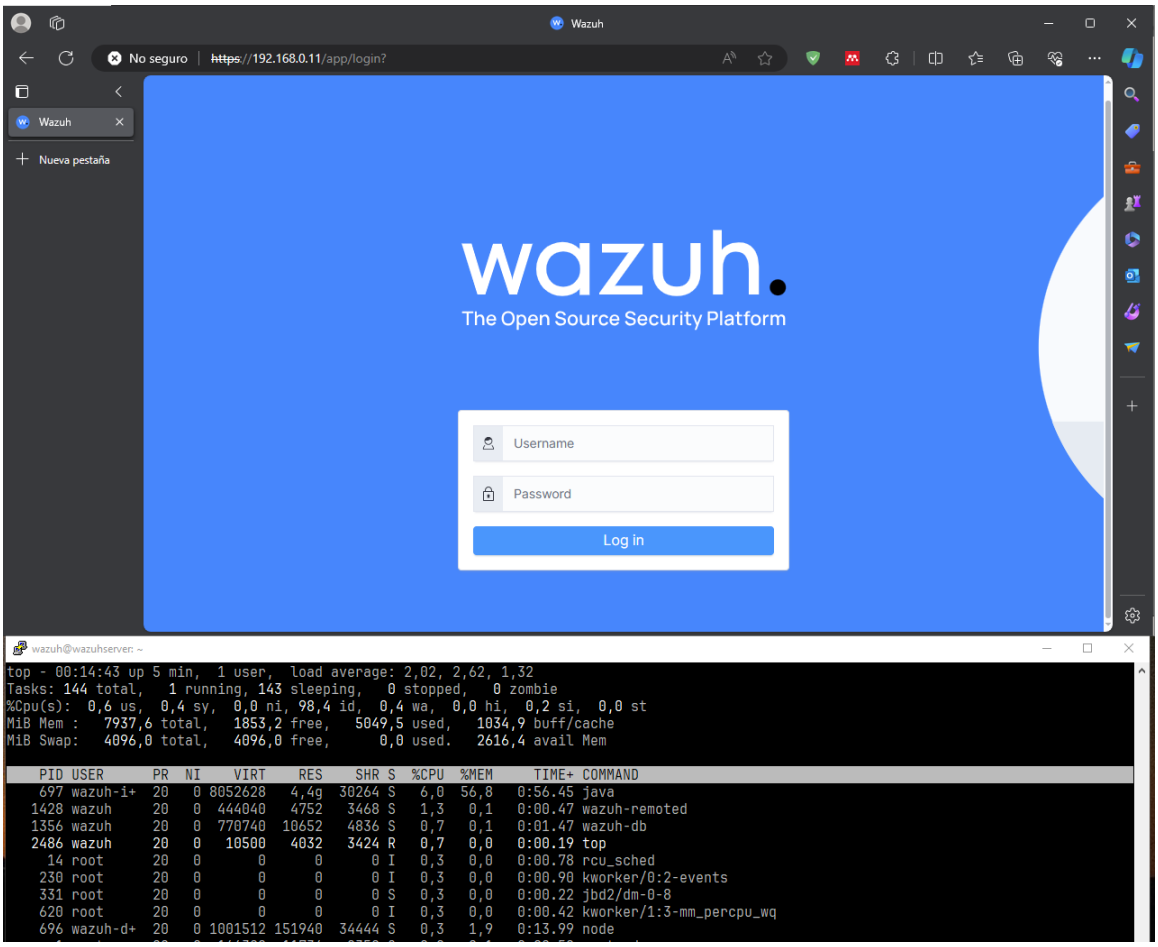
Cada vez que se reinicia la máquina virtual del servidor de wazuh el servicio de wazuh indexer no es levantado en el sistema. Para ello procedemos a configurar un mayor tiempo de espera para levantar el servicio. Los pasos para aumentar el tiempo de espera de wazuh-indexer.service se realizan a continuación:

Se realiza una búsqueda en el directorio **systemd** para encontrar la ubicación del servicio indexer. Se procede a editar como administrador el archivo de configuración del servicio con el editor **nano**, luego incrementamos el tiempo en el parámetro TimeoutStartSec=180 como valor predeterminado a TimeoutStartSec=360. Luego procedemos a guardar y recargar la configuración de Systemd con el comando systemctl daemon-reload y posteriormente reiniciamos el servicio Wazuh Indexer con el comando systemctl restart wazuh-indexer.

```
root@wazuhserver: /home/wazuh
wazuh@wazuhserver:~$ nano /etc/systemd/system/multi-user.target.wants/wazuh-indexer.service
wazuh@wazuhserver:~$ sudo su
[sudo] password for wazuh:
root@wazuhserver:/home/wazuh# nano /etc/systemd/system/multi-user.target.wants/wazuh-indexer.service
  GNU nano 6.2                 /etc/systemd/system/multi-user.target.wants/wazuh-indexer.service
WorkingDirectory=/usr/share/wazuh-indexer

User=wazuh-indexer
Group=wazuh-indexer

ExecStart=/usr/share/wazuh-indexer/bin/systemd-entrypoint -p ${PID_DIR}/wazuh-indexer.pid --quiet

# StandardOutput is configured to redirect to journalctl since
# some error messages may be logged in standard output before
# wazuh-indexer logging system is initialized. Elasticsearch
# stores its logs in /var/log/wazuh-indexer and does not use
# journalctl by default. If you also want to enable journalctl
# logging, you can simply remove the "quiet" option from ExecStart.
StandardOutput=journal
StandardError=inherit

# Specifies the maximum file descriptor number that can be opened by this process
LimitNOFILE=65535

# Specifies the maximum number of processes
LimitNPROC=4096

# Specifies the maximum size of virtual memory
LimitAS=infinity

# Specifies the maximum file size
LimitFSIZE=infinity

# Disable timeout logic and wait until process is stopped
TimeoutStopSec=0

# SIGTERM signal is used to stop the Java process
KillSignal=SIGTERM

# Send the signal only to the JVM rather than its control group
KillMode=process

# Java process is never killed
SendSIGKILL=no

# When a JVM receives a SIGTERM signal it exits with code 143
SuccessExitStatus=143

# Allow a slow startup before the systemd notifier module kicks in to extend the timeout
TimeoutStartSec=180

[Install]
WantedBy=multi-user.target
```

```
root@wazuhserver: /home/wazuh
root@wazuhserver:/home/wazuh# systemctl daemon-reload
root@wazuhserver:/home/wazuh# systemctl restart wazuh-indexer
root@wazuhserver:/home/wazuh#
```

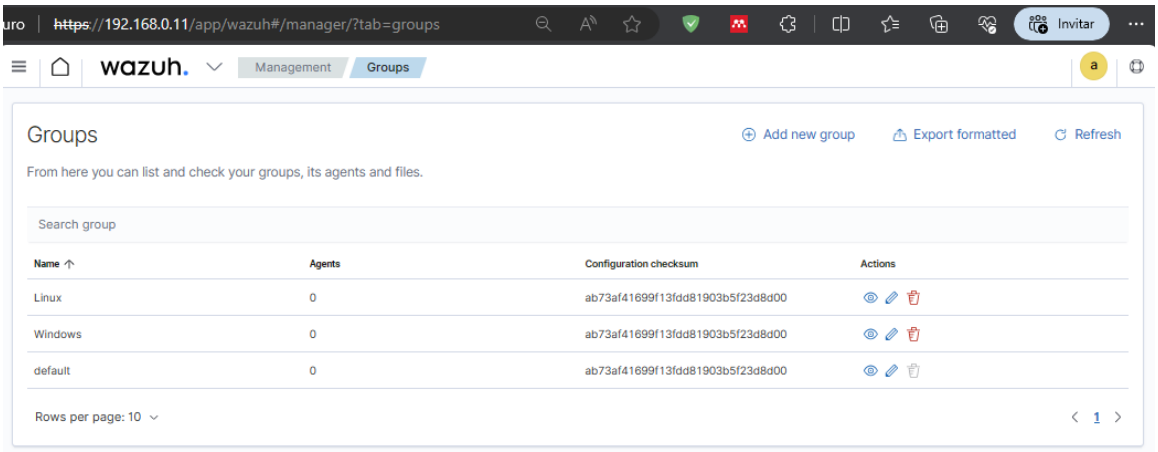
Como resultado al iniciar nuevamente la máquina virtual el servicio de wazuh indexer permanece iniciado.



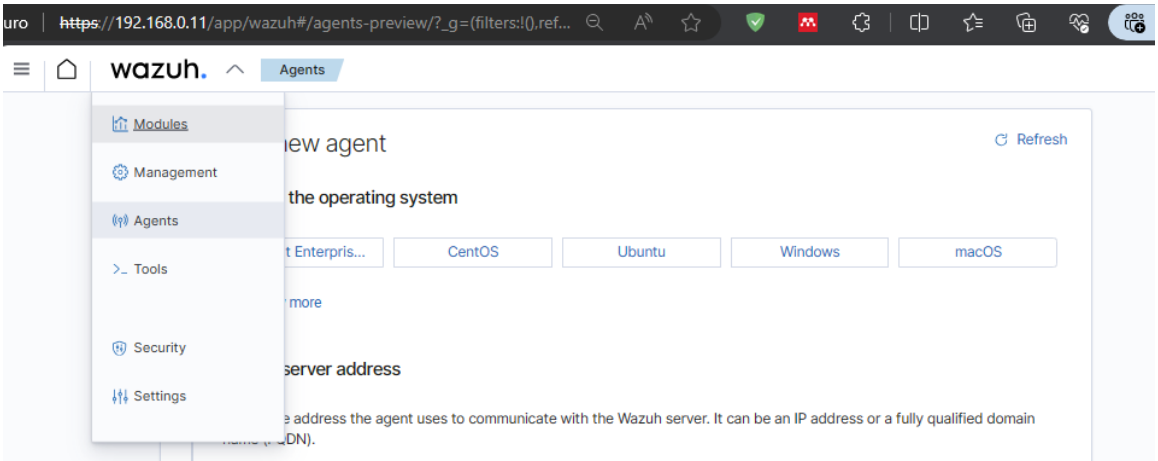
1.9 Procedimiento de instalación de agentes

Los agentes proporcionan las funciones clave para la seguridad, se ejecutan en los endpoints desplegados en la red, estos portátiles, servidores, equipos de mesa, servidores desplegados en la nube como maquinas virtuales. Estos pueden estar ejecutando cualquier sistema operativo, Wazuh permite enlazar o inscribir estos agentes para permitir la comunicación y ejecución de las capacidades integradas con los componentes del servidor de wazuh, estos agentes se instalan sobre los endpoints para la supervisión, requiere 35MB de RAM promedio.

Primero creamos dos grupos para gestionar en categorías los agentes.



Para desplegar los agentes en Wazuh esto se hace de forma rápida con la guía asistida en la sección Wazuh-Agents y seleccionando el tipo de agente a desplegar.[20]



1.9.1 Proceso de instalación y configuración de Windows

Estos links contienen el procedimiento paso a paso de alguien que implemento, solo seguir el procedimiento y parafrasear, hay que ver que se pide configurar, que módulos.

Uno de este link realiza una configuración de Docker en Wazuh, lo podemos usar para un capítulo en la monografía, pero antes montar el entorno de la parte práctica de Docker, hacer una parte práctica de ataque y evaluar el comportamiento con wazuh. Es una idea para tener lista la idea de lo que va la monografía.

Wazuh | Part 3 : Wazuh Agents installation – Igor_sec's Blog (igorsec.blog)

Wazuh | Part 4 : Proof of Concept – Ubuntu Endpoint Part 1 of 3 – Igor_sec's Blog (igorsec.blog)

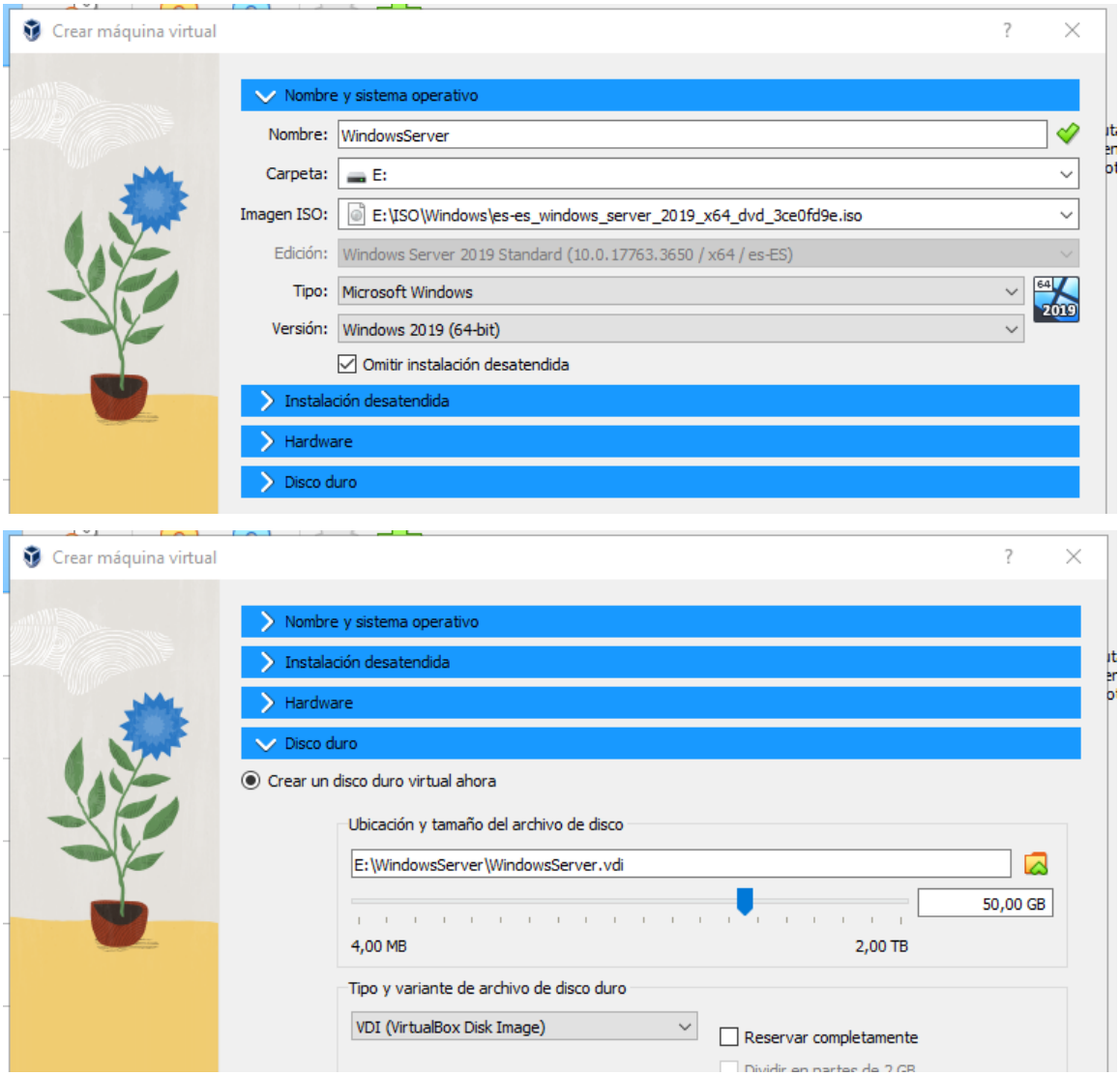
Wazuh | Part 4 : Proof of Concept – Ubuntu Endpoint Part 2 of 3 – Igor_sec's Blog (igorsec.blog)

Wazuh | Part 4 : Proof of Concept – Ubuntu Endpoint Part 3 of 3 – Igor_sec's Blog (igorsec.blog)

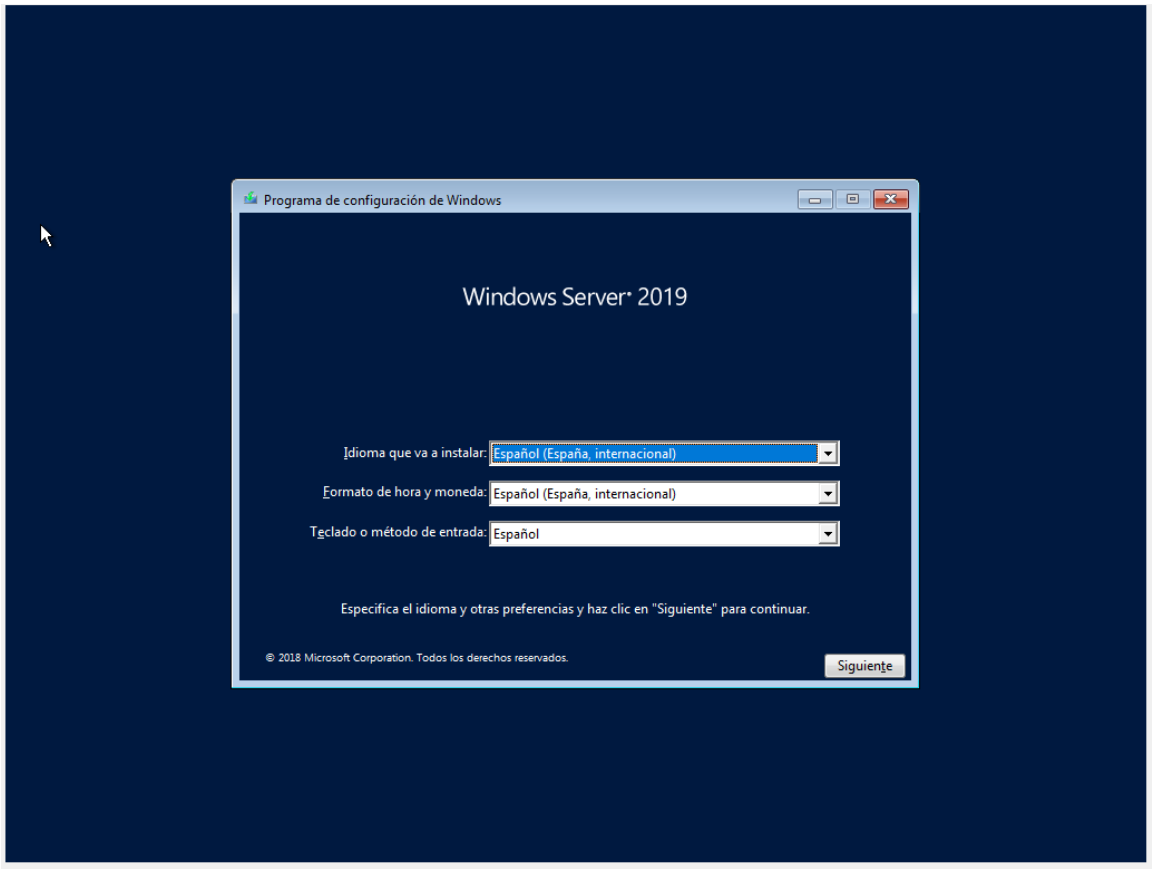
Wazuh | Part 4 : Proof of Concept—Windows Endpoint Part 1 of 2 – Igor_sec's Blog (igorsec.blog)

Wazuh | Part 4 : Proof of Concept—Windows Endpoint Part 2 of 2 – Igor_sec's Blog (igorsec.blog)

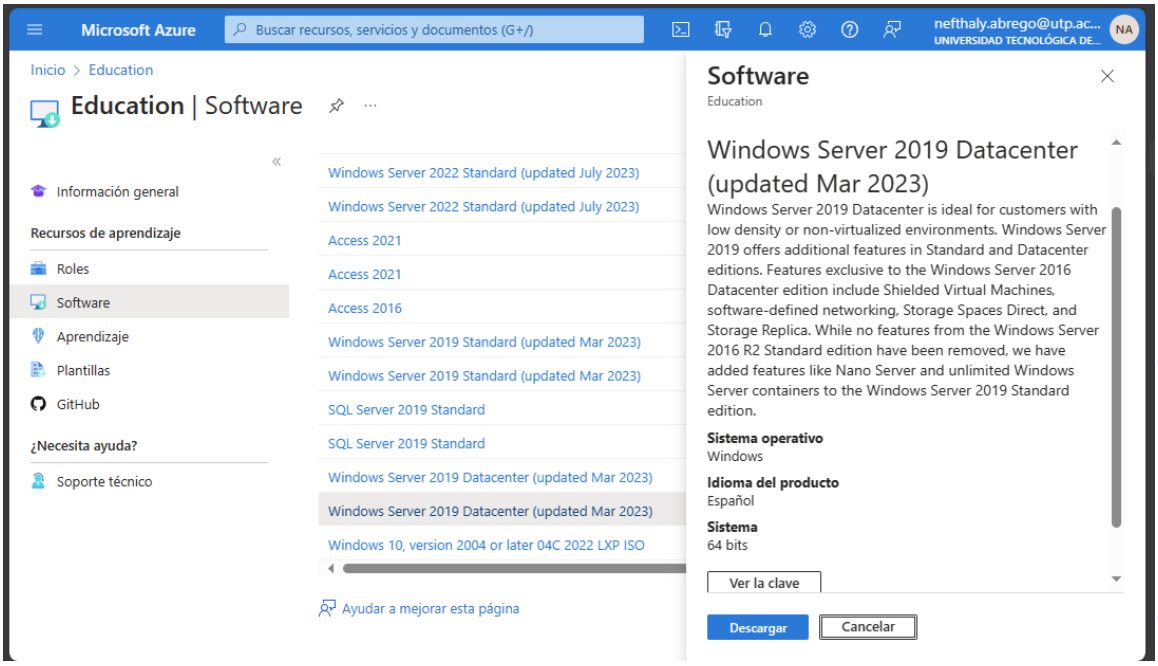
Proceso de creación de maquina virtual de creación de agente windows



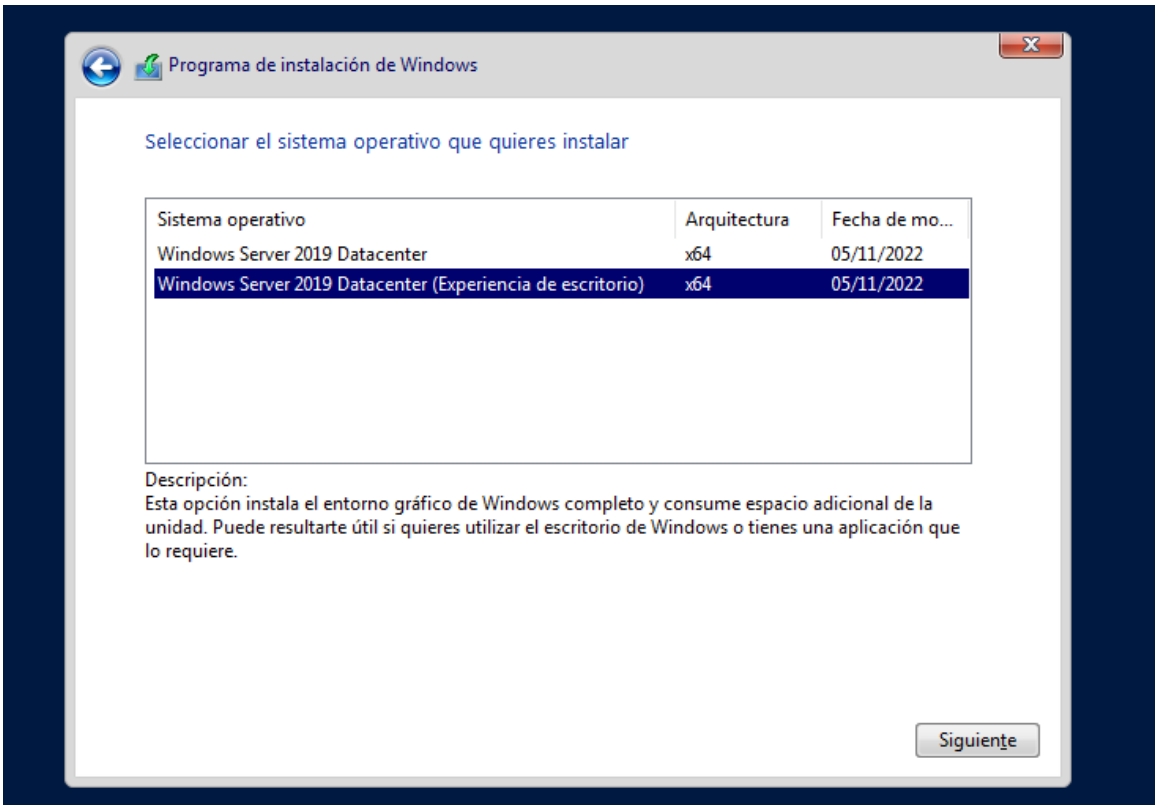
Proceso de instalación de Máquina virtual Windows

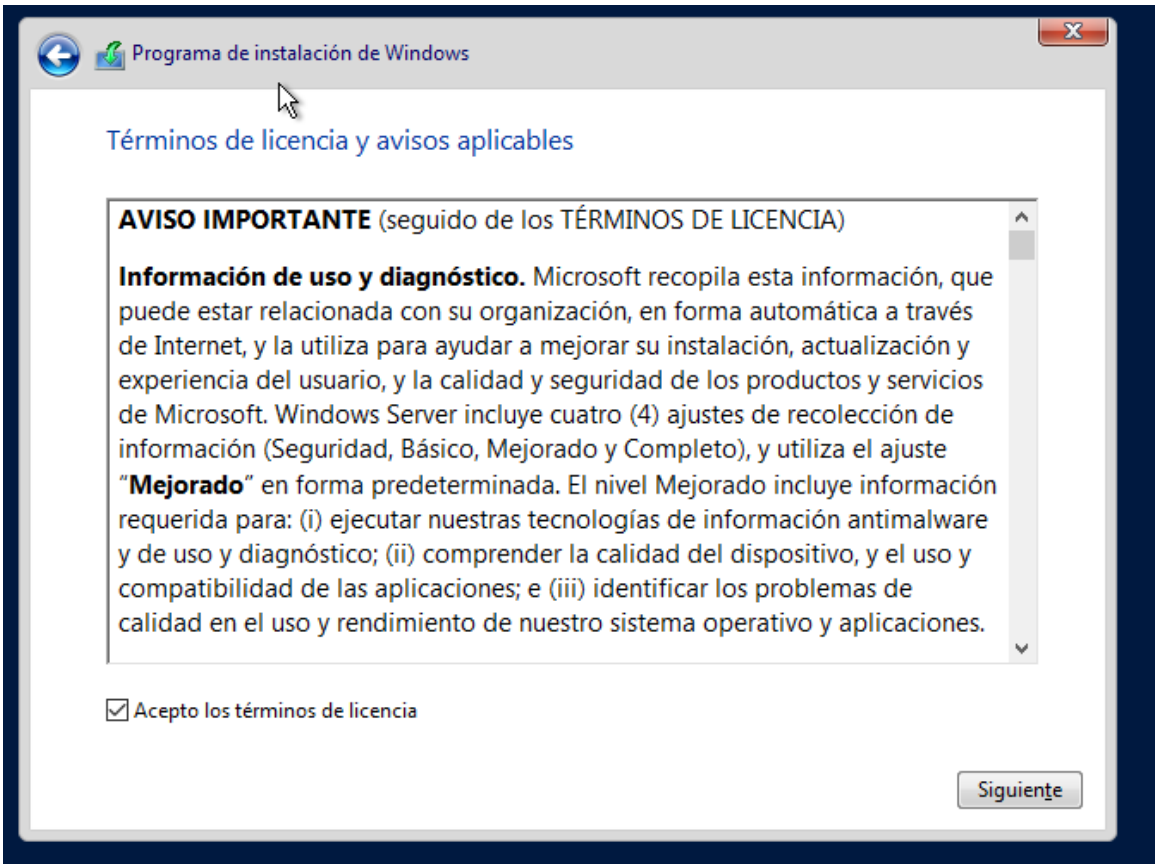


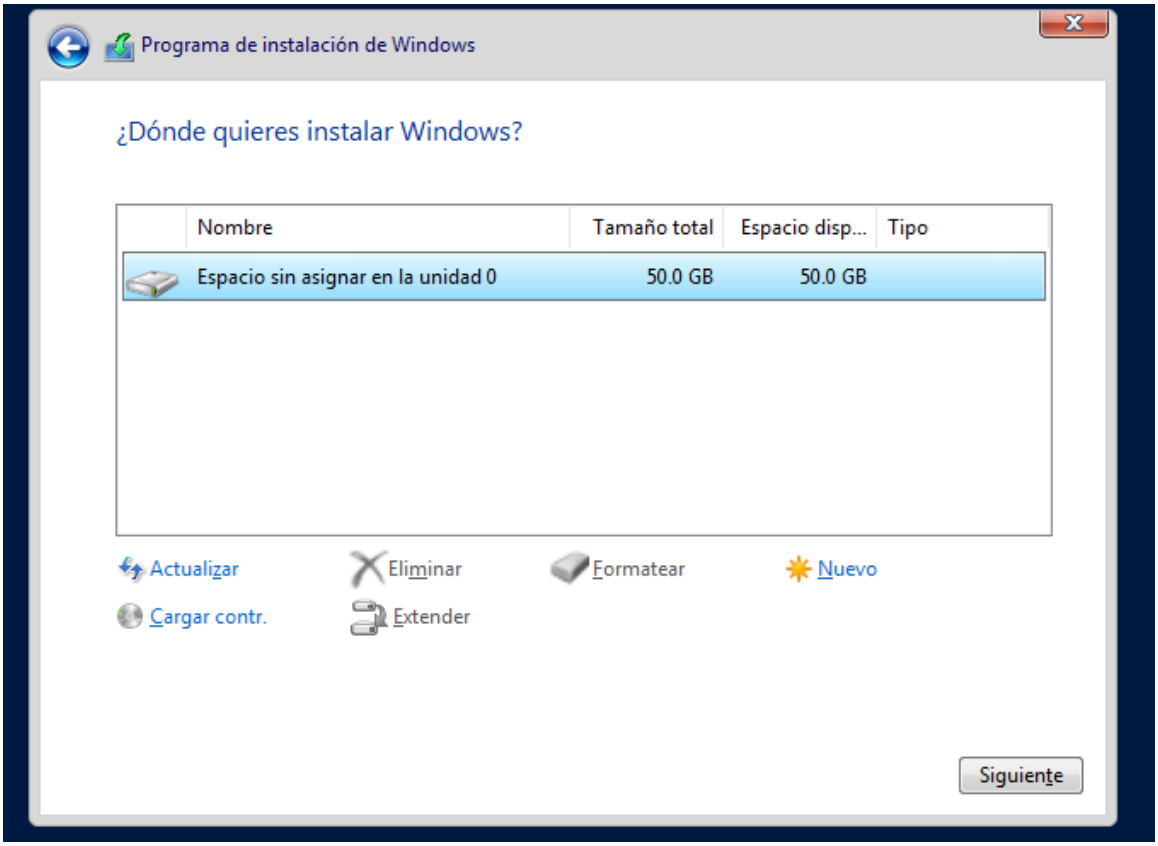
Instalación de clave de licencia



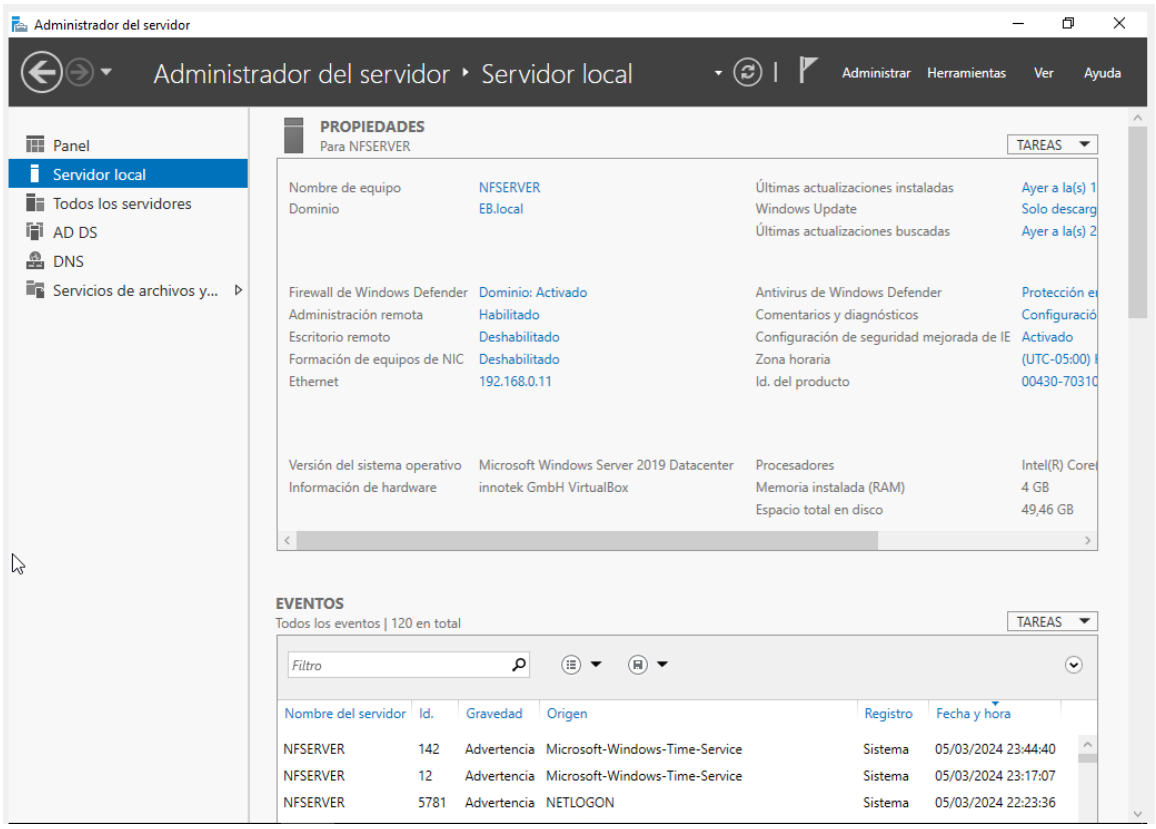
Selección de sistema operativo


Programa de instalación de Windows
Seleccionar el sistema operativo que quieres instalar
Sistema operativo
Arquitectura
Fecha de mo...
Windows Server 2019 Datacenter
x64
05/11/2022
Windows Server 2019 Datacenter (Experiencia de escritorio)
x64
05/11/2022
Descripción:
Esta opción instala el entorno gráfico de Windows completo y consume espacio adicional de la unidad. Puede resultarte útil si quieres utilizar el escritorio de Windows o tienes una aplicación que lo requiere.
Siguiente


Programa de instalación de Windows
Términos de licencia y avisos aplicables
AVISO IMPORTANTE (seguido de los TÉRMINOS DE LICENCIA)
Información de uso y diagnóstico. Microsoft recopila esta información, que puede estar relacionada con su organización, en forma automática a través de Internet, y la utiliza para ayudar a mejorar su instalación, actualización y experiencia del usuario, y la calidad y seguridad de los productos y servicios de Microsoft. Windows Server incluye cuatro (4) ajustes de recolección de información (Seguridad, Básico, Mejorado y Completo), y utiliza el ajuste "Mejorado" en forma predeterminada. El nivel Mejorado incluye información requerida para: (i) ejecutar nuestras tecnologías de información antimalware y de uso y diagnóstico; (ii) comprender la calidad del dispositivo, y el uso y compatibilidad de las aplicaciones; e (iii) identificar los problemas de calidad en el uso y rendimiento de nuestro sistema operativo y aplicaciones.
Acepto los términos de licencia
Siguiente



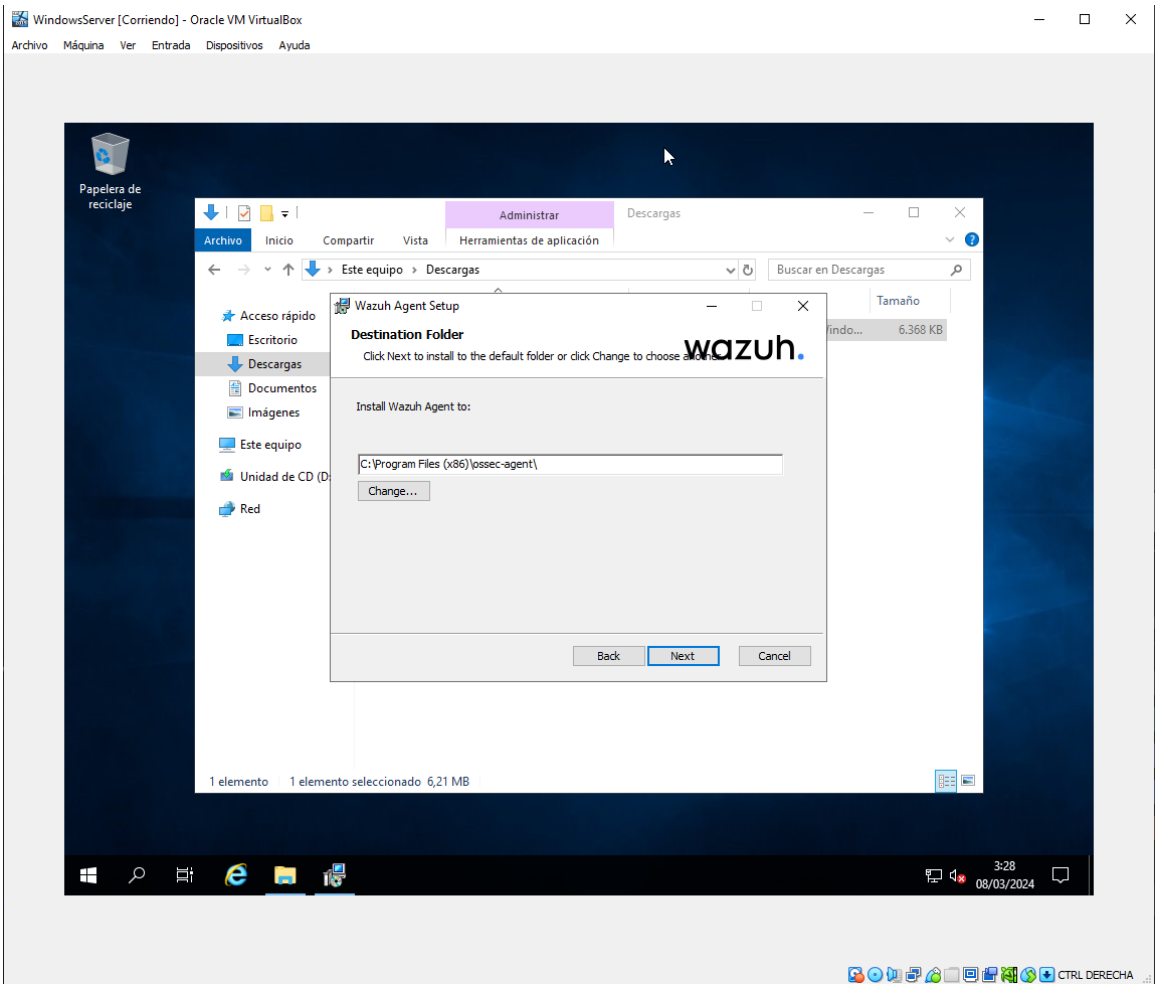
Maquina windows preparada para instalación de agente

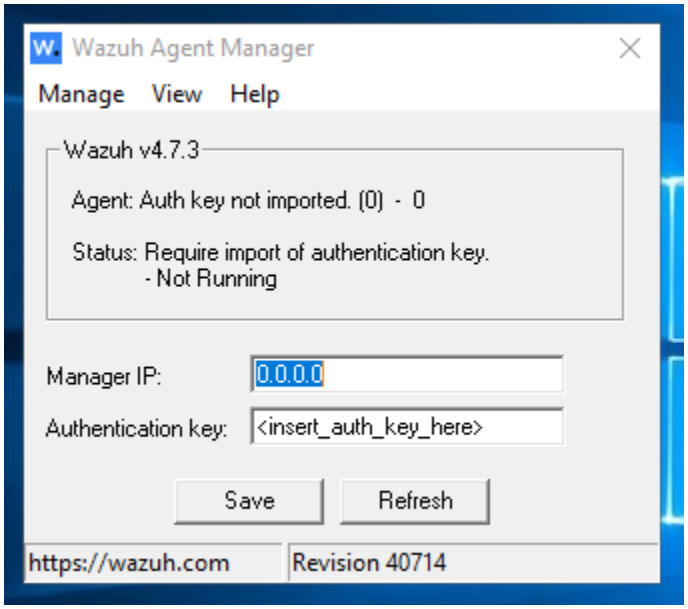


Proceso de instalación de agente Windows Server 2019

El agente se instala en Windows Server 2019 para permitir la comunicación con el servidor de Wazuh, este permite enviar datos en tiempo real a través de un canal cifrado y autenticado.

Para iniciar el proceso de instalación, descargue el instalador de Windows.


WindowsServer [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Papelera de reciclaje
Administrar
Descargas
Archivo Inicio Compartir Vista Herramientas de aplicación
Este equipo › Descargas
Buscar en Descargas
Acceso rápido
Escritorio
Descargas
Documentos
Imágenes
Este equipo
Unidad de CD (D:
Red
Tamaño
6.368 KB
Wazuh Agent Setup
Destination Folder
Click Next to install to the default folder or click Change to choose another.
wazuh.
Install Wazuh Agent to:
C:\Program Files (x86)\ossec-agent\
Change...
Back
Next
Cancel
1 elemento
1 elemento seleccionado 6,21 MB
3:28
08/03/2024
CTRL DERECHA


Wazuh Agent Manager
Manage View Help
Wazuh v4.7.3
Agent: Auth key not imported. (0) - 0
Status: Require import of authentication key.
- Not Running
Manager IP:
0.0.0.0
Authentication key:
<insert_auth_key_here>
Save
Refresh
https://wazuh.com
Revision 40714

Luego realizamos la inscripción del agente como miembro autorizado esto se realiza para asegurar la identidad de los agentes que se comunican con el gestor.

Para insertar el agente y permitir la comunicación con el servidor lo podemos hacer de varias maneras, a través de la configuración del agente estableciendo la ip del servidor el agente puede solicitar la clave e importarla. Para este se ingresa la IP del administrador de Wazuh

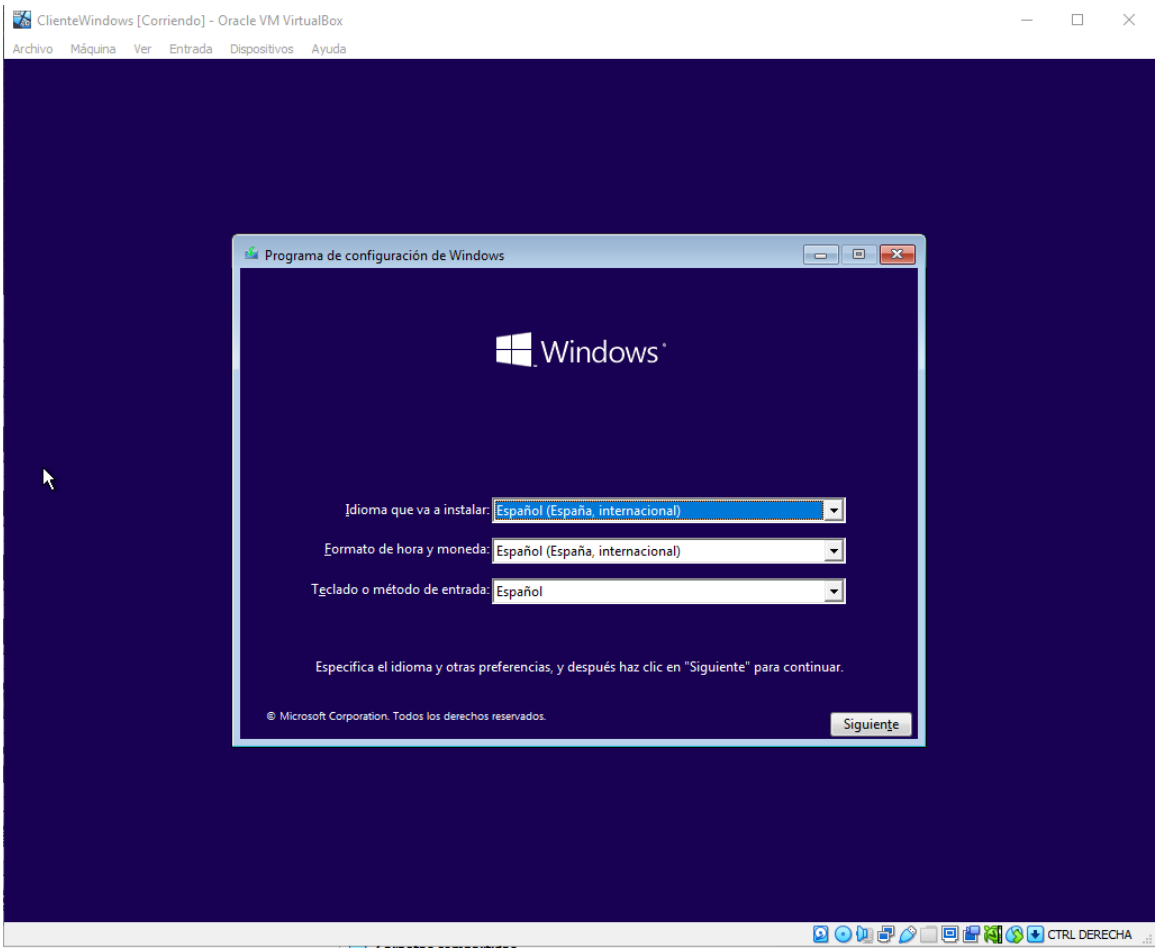
Se puede registrar un agente mediante la API del administrador en donde el usuario solicita una API de administrador y a continuación la importa al agente manualmente.

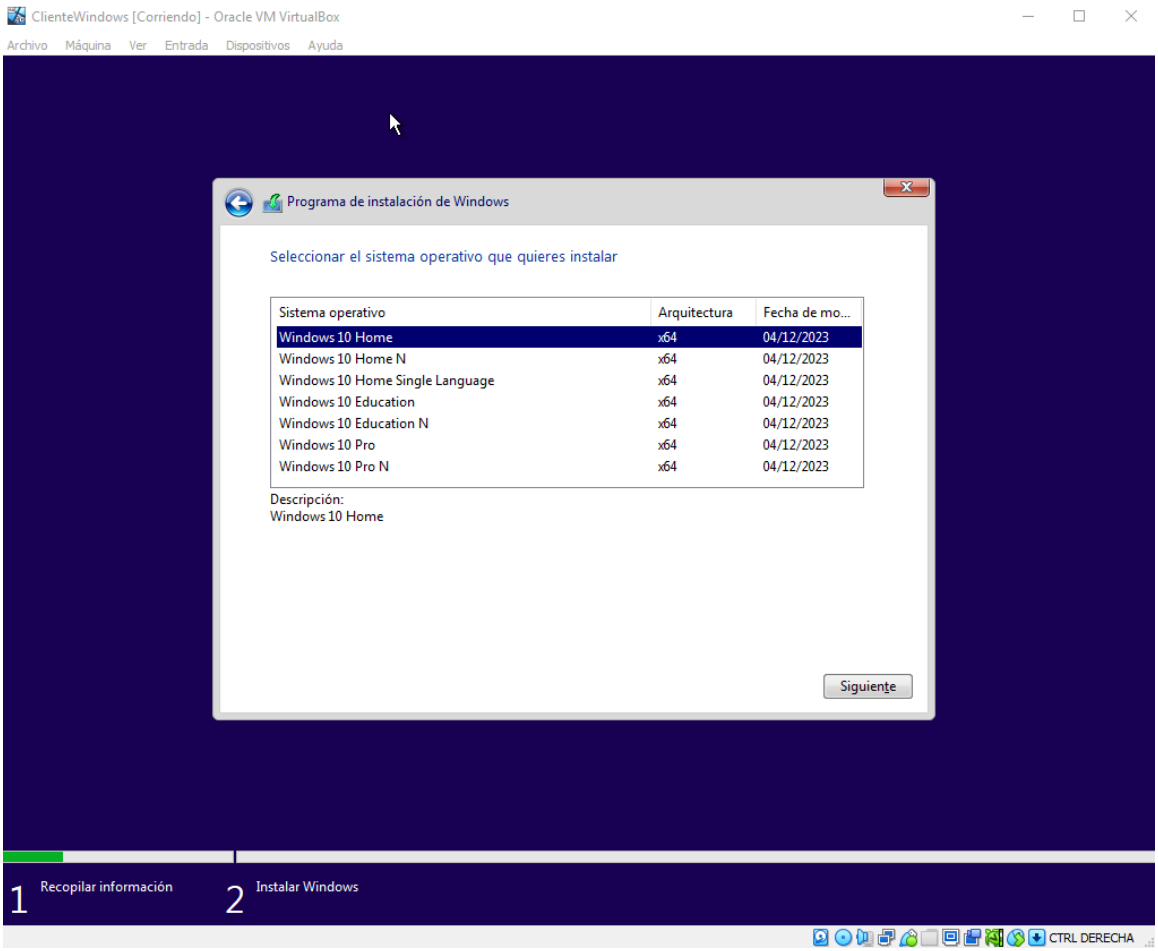
Es necesaria la conexión de wazuh y el conocimiento de los siguientes puertos importantes.

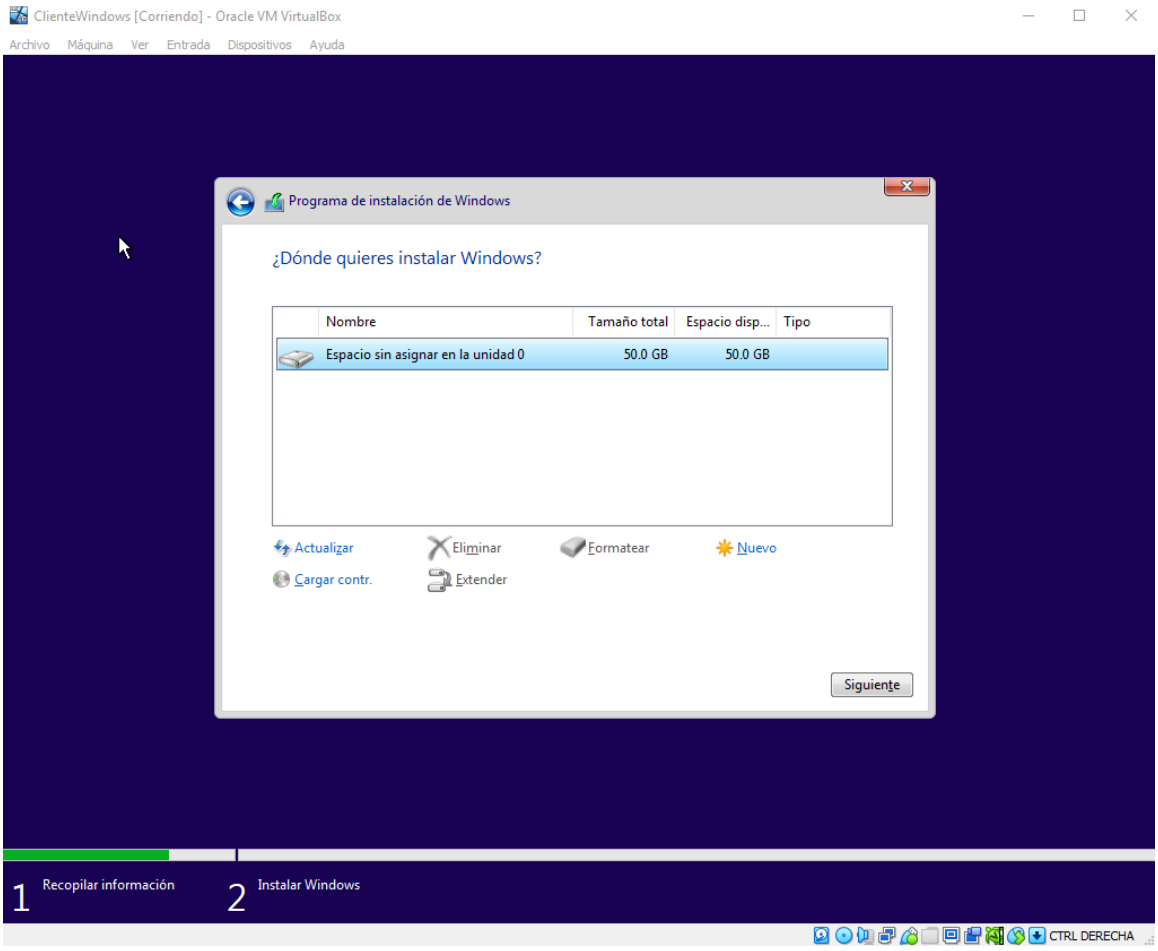
- 1514/TCP para la comunicación con los agentes.
- 1515/TCP para la inscripción a través de la solicitud automática del agente.
- 55000/TCP para la inscripción a través de la API del administrador.

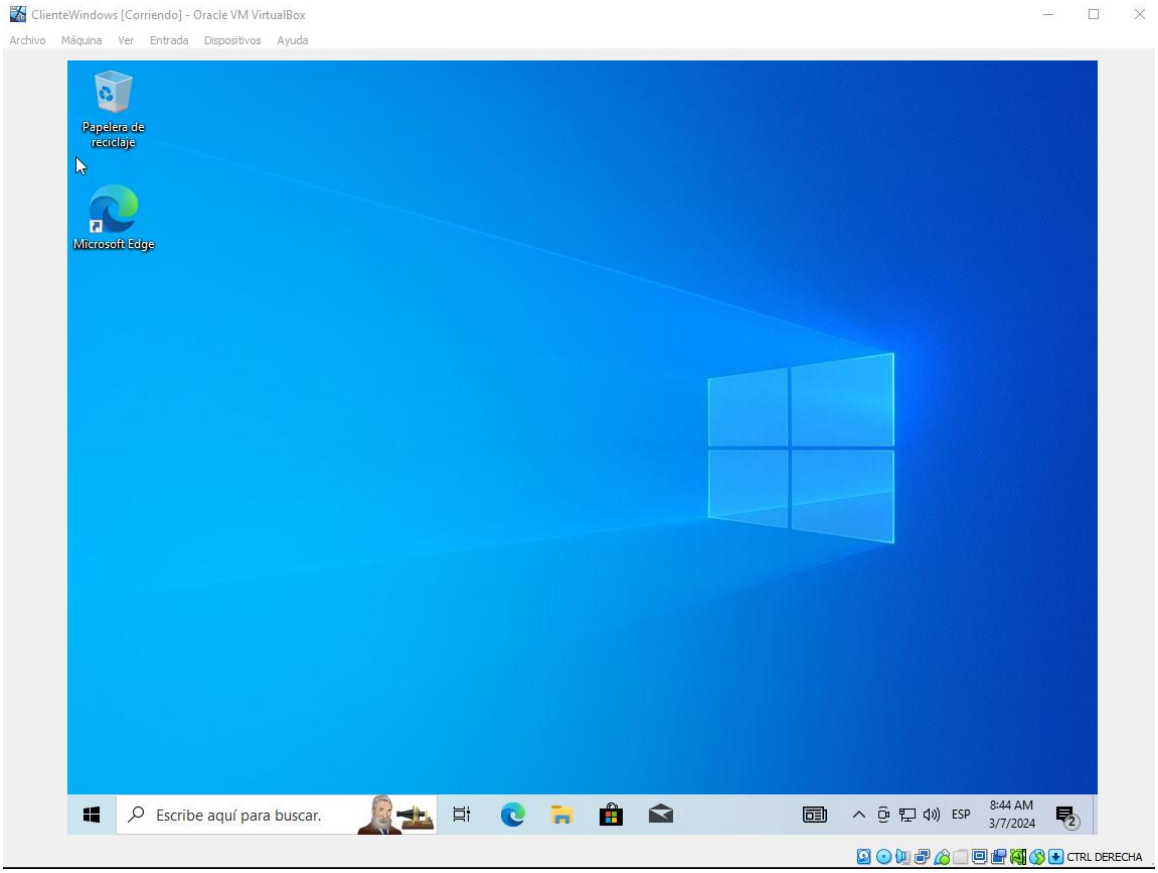
Seleccione el método de instalación que desea seguir: interfaz de línea de comandos (CLI) o interfaz gráfica de usuario (GUI).

Proceso de instalación de cliente Windows server 2019

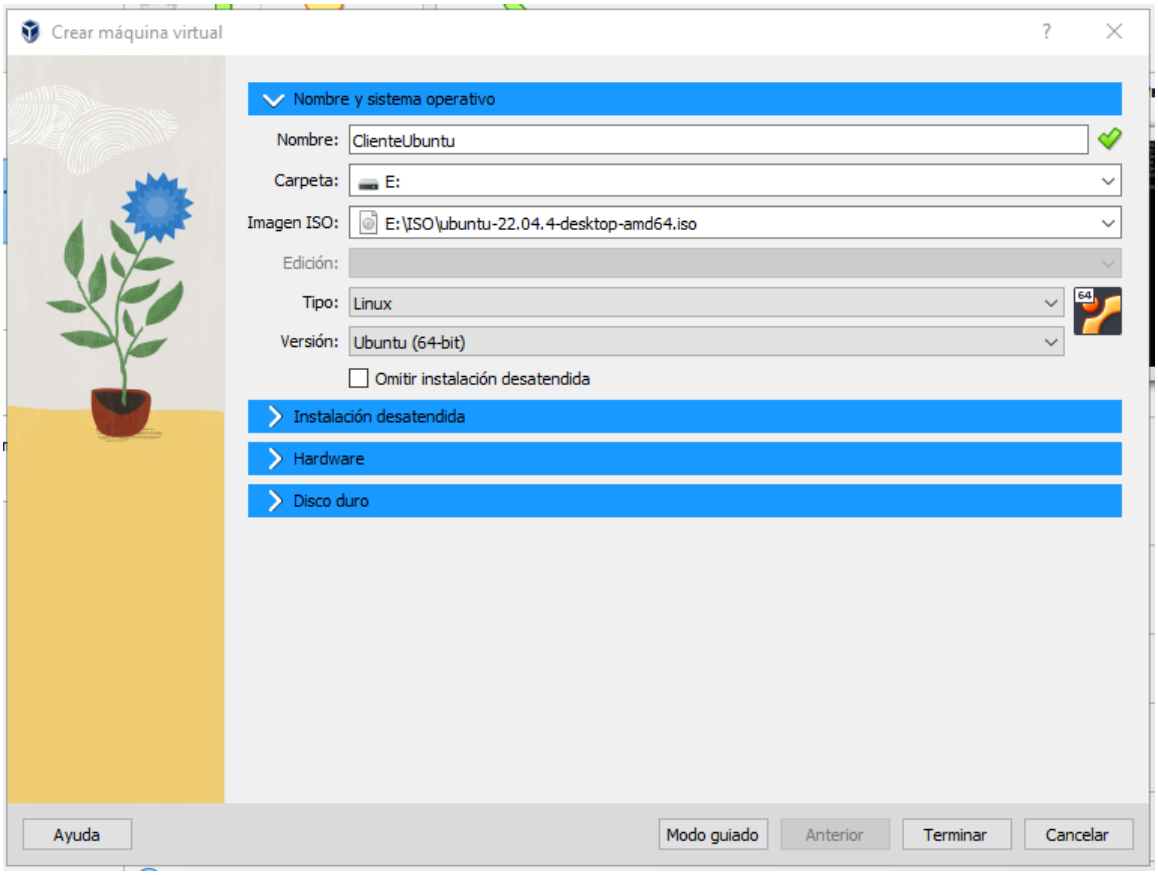

ClienteWindows [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Programa de configuración de Windows
Windows
Idioma que va a instalar: Español (España, internacional)
Formato de hora y moneda: Español (España, internacional)
Teclado o método de entrada: Español
Especifica el idioma y otras preferencias, y después haz clic en "Siguiente" para continuar.
© Microsoft Corporation. Todos los derechos reservados.
Siguiente
CTRL DERECHA


ClienteWindows [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Programa de instalación de Windows
Seleccionar el sistema operativo que quieres instalar
Sistema operativo
Arquitectura
Fecha de mo...
Windows 10 Home
x64
04/12/2023
Windows 10 Home N
x64
04/12/2023
Windows 10 Home Single Language
x64
04/12/2023
Windows 10 Education
x64
04/12/2023
Windows 10 Education N
x64
04/12/2023
Windows 10 Pro
x64
04/12/2023
Windows 10 Pro N
x64
04/12/2023
Descripción:
Windows 10 Home
Siguiente
1 Recopilar información
2 Instalar Windows
CTRL DERECHA


ClienteWindows [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Programa de instalación de Windows
¿Dónde quieres instalar Windows?
Nombre
Tamaño total
Espacio disp...
Tipo
Espacio sin asignar en la unidad 0
50.0 GB
50.0 GB
Actualizar
Eliminar
Formatear
Nuevo
Cargar contr.
Extender
Siguiente
1 Recopilar información
2 Instalar Windows
CTRL DERECHA


ClienteWindows [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Papelera de reciclaje
Microsoft Edge
Escribe aquí para buscar.
ESP
8:44 AM
3/7/2024
CTRL DERECHA

1.9.2 Proceso de instalación de agente y configuración de Ubuntu



Instalación de agente Linux

1.10 Escenario de ataque con Kali

1.11 Resultados de comportamiento de cada uno de los servicios de Wazuh

1. Análisis de Información de los Logs
2. Monitoreo de Integridad de Archivos
3. Detección de vulnerabilidades
4. Configuración de evaluación
5. Respuesta ante incidentes
6. Cumplimiento Normativo
7. Seguridad en la nube
8. Seguridad en contenedores

9. Arquitectura de Wazuh

Log collector	Command execution
File integrity monitoring (FIM)	Security configuration assessment (SCA)
System inventory	Malware detection
Active response	Container security
Cloud security	

Instalar:

- Virtual Box
- Wazuh
- Ubuntu Server
- Windows
- Linux

Presentar en Wazuh en los sistemas operativos Linux o Windows instalar el agente y desde Kali Linux atacar y ver el comportamiento, en todos los servicios mencionados de Wazuh.

CONCLUSIONES

RECOMENDACIONES

REFERENCIAS BIBLIOGRÁFICAS

[1] G. Rawat, P. Kanti, M. Memoria, R. Kumar, and T. Choudhury, “Ace of Cyber Security and it’s Emerging Trends on Latest Technologies,” pp. 1–6, Dec. 2023, doi: 10.1109/CISCT57197.2023.10351359.

[2] “What Is Security Information and Event Management (SIEM)? - Palo Alto Networks.” Accessed: Feb. 05, 2024. [Online]. Available: https://www.paloaltonetworks.com/cyberpedia/what-is-security-information-and-event-management-SIEM

[3] “How the combination of XDR and SIEM can improve SOC operations | CSO Online.” Accessed: Feb. 05, 2024. [Online]. Available: https://www.csoonline.com/article/575477/how-the-combination-of-xdr-and-siem-can-improve-soc-operations.html

[4] “XDR vs SIEM vs SOAR: Choosing The Best Security Solution.” Accessed: Feb. 05, 2024. [Online]. Available: https://swimlane.com/blog/xdr-vs-siem-vs-soar/

[5] Wazuh, “Components - Getting started with Wazuh · Wazuh documentation.” Accessed: Feb. 15, 2024. [Online]. Available: https://documentation.wazuh.com/current/getting-started/components/index.html

[6] Wazuh, “Open Source Security Configuration Assessment | Wazuh.” Accessed: Feb. 16, 2024. [Online]. Available: https://wazuh.com/use-cases/security-configuration-assessment/

[7] Wazuh, “Open Source Malware Detection | Wazuh.” Accessed: Feb. 16, 2024. [Online]. Available: https://wazuh.com/use-cases/malware-detection/

[8] Wazuh, “Open Source File Integrity Monitoring | Wazuh.” Accessed: Feb. 16, 2024. [Online]. Available: https://wazuh.com/use-cases/file-integrity-monitoring/

[9] Wazuh, “Open Source Threat Hunting | Wazuh.” Accessed: Feb. 16, 2024. [Online]. Available: https://wazuh.com/use-cases/threat-hunting/

[10] S. Hernández, “¿Qué es el marco MITRE ATT&CK? ¿Para qué se usa?” Accessed: Feb. 16, 2024. [Online]. Available: https://www.globalsuitesolutions.com/es/que-es-marco-mitre-att-ck/

[11] Wazuh, “Open Source Log Data Analysis | Wazuh.” Accessed: Feb. 16, 2024. [Online]. Available: https://wazuh.com/use-cases/log-data-analysis/

[12] Wazuh, “Open Source Vulnerability Detection | Wazuh.” Accessed: Feb. 16, 2024. [Online]. Available: https://wazuh.com/use-cases/vulnerability-detection/

[13] Wazuh, “Open Source Incident Response | Wazuh.” Accessed: Feb. 16, 2024. [Online]. Available: https://wazuh.com/use-cases/incident-response/

[14] Wazuh, “Open Source Regulatory Compliance | Wazuh.” Accessed: Feb. 16, 2024. [Online]. Available: https://wazuh.com/use-cases/regulatory-compliance/

[15] Wazuh, “Open Source IT Hygiene | Wazuh.” Accessed: Feb. 16, 2024. [Online]. Available: https://wazuh.com/use-cases/it-hygiene/

[16] Wazuh, “Open Source Container Security | Wazuh.” Accessed: Feb. 16, 2024. [Online]. Available: https://wazuh.com/use-cases/container-security/

[17] Wazuh, “Open Source Posture Management | Wazuh.” Accessed: Feb. 16, 2024. [Online]. Available: https://wazuh.com/use-cases/posture-management/

[18] Wazuh, “Open Source Cloud Workload Protection | Wazuh.” Accessed: Feb. 16, 2024. [Online]. Available: https://wazuh.com/use-cases/cloud-workload-protection/

[19] Wazuh, “Quickstart · Wazuh documentation.” Accessed: Mar. 01, 2024. [Online]. Available: https://documentation.wazuh.com/current/quickstart.html

[20] Wazuh, “Wazuh agent - Installation guide · Wazuh documentation.” Accessed: Mar. 07, 2024. [Online]. Available: https://documentation.wazuh.com/current/installation-guide/wazuh-agent/index.html

ANEXOS