IES GONZALO NAZARENO

Alejandro Montes Delgado

Despliegue y funcionamiento de Wazuh

1. ¿Qué es Wazuh?

Wazuh es una plataforma Open-Source que unifica las capacidades de XDR (detección y respuesta extendidas) y SIEM (gestión de información y eventos de seguridad), y está integrado con Elastic Stack, utilizada para la prevención, detección y respuesta a las amenazas, es capaz de proteger cargas de trabajos en entornos locales, virtualizados, en contenedores y en la nube.

La solución Wazuh consta de agentes de seguridad desplegado en los sistemas supervisados, y un servidor que recoge y analiza los datos recopilados por los agentes.

1.1. Servicios de Wazuh

- **Análisis de seguridad**: Wazuh es utilizado para recolectar, agregar, indexar y analizar información de seguridad, ayudando a las organizaciones a detectar intrusos, amenazas y anomalías de comportamiento.
- **Detección de intrusos**: Los agentes de Wazuh monitorizan los sistemas buscando malware, rootkits y anomalías sospechosas.
- **Análisis de logs**: Los agentes de Wazuh leen el SO y los logs de las aplicaciones, y los envían de manera segura al administrador central para ser analizados y almacenados.
- **Monitorización de la integridad de los Archivos**: Wazuh monitorea el sistema de archivos, identificando cambios en el contenido, permisos, propiedad, y los atributos que necesitas mantener bajo control.
- **Detección de vulnerabilidades**: Los agentes de Wazuh envían información referida al servidor, donde es correlacionada con la base de datos de actualizaciones continuas de CVE, para identificar las vulnerabilidades de software conocidas
- **Configuración de Evaluación**: Wazuh monitorea los ajustes de configuración del sistema y las aplicaciones para asegurar que se alinean con las políticas de seguridad.

1.1. Servicios de Wazuh

- **Respuesta ante incidentes**: Wazuh provee respuestas activas para accionar varias contra medidas para la dirección de amenazas activas, como bloquear acceso al sistema para las fuentes de amenazas cuando ciertos criterios son cumplidos.
- **Cumplimiento Normativo**: Wazuh provee algunos de los controles de seguridad necesarios para cumplir con los estándares y regulaciones de la industria.
- **Seguridad en la nube**: Wazuh ayuda a monitorear infraestructuras en la nube a un nivel API, usando integración de módulos que son capaces de enviar datos de manera segura desde proveedores de servicios en la nube bien conocidos, como Amazon AWS, Azure o Google Cloud.
- **Seguridad en contenedores**: Wazuh provee seguridad en los host y contenedores Docker, monitorizando su comportamiento y detectando amenazas y anomalías.

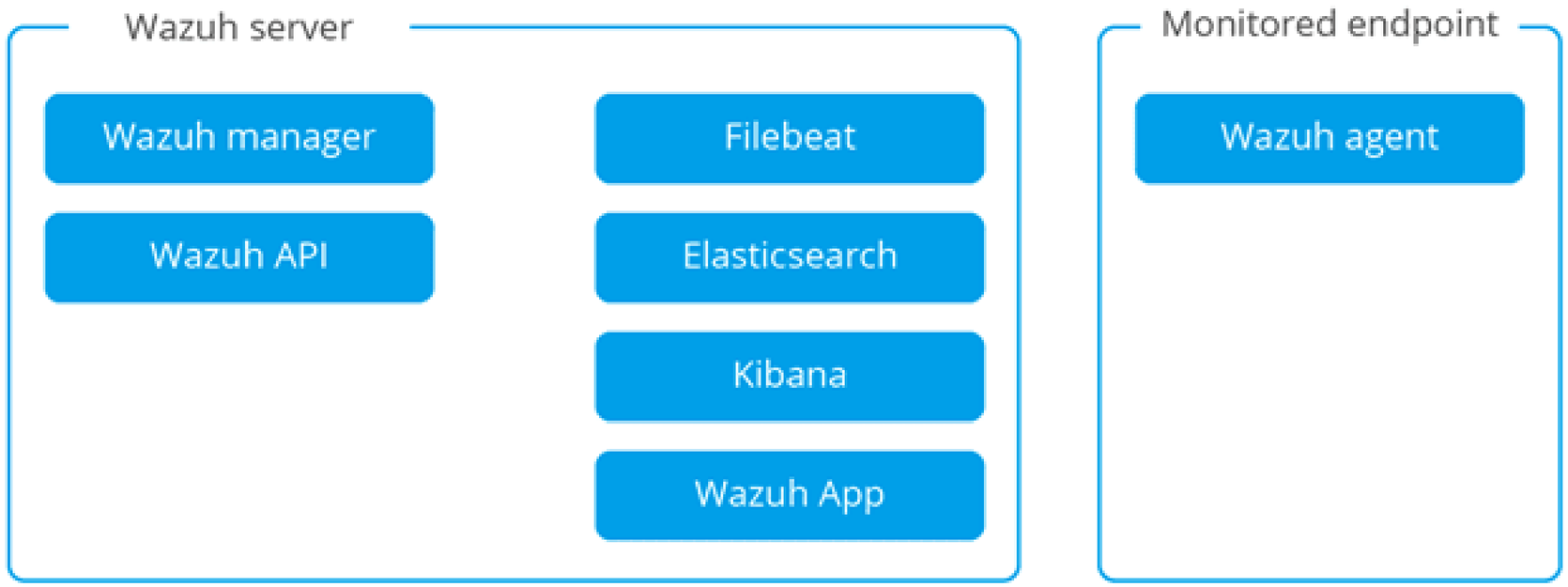
2. Componentes de Wazuh

- **OSSEC HIDS**: Es un sistema de detección de intrusos que es usado para la detección, visibilidad y monitorización del cumplimiento de eventos de seguridad. Está basado en un agente multiplataforma que envía datos del sistema a un gestor central, donde es analizado y procesado, dando como resultado alertas de seguridad. También es un servidor centralizado de logs.
- **OpenSCAP**: Es un intérprete que se usa para chequear las configuraciones del sistema y detectar aplicaciones vulnerables. Es una herramienta diseñada para el cumplimiento de la seguridad y el bastionado de los sistemas en un entorno empresarial.
- **Elastic Stack**: Es un conjunto de software que es usado para recolectar, comparar, almacenar, indexar, buscar y mostrar datos de logs. Proporciona una interfaz web que muestra los datos a través de un dashboard.
- **Agente de Wazuh:** Es un paquete multiplataforma y se ejecuta en los endpoints que el usuario desea supervisar. Se comunica con el servidor Wazuh, enviando datos casi en tiempo real a través de un canal encriptado y autenticado.

3. Arquitectura de Wazuh

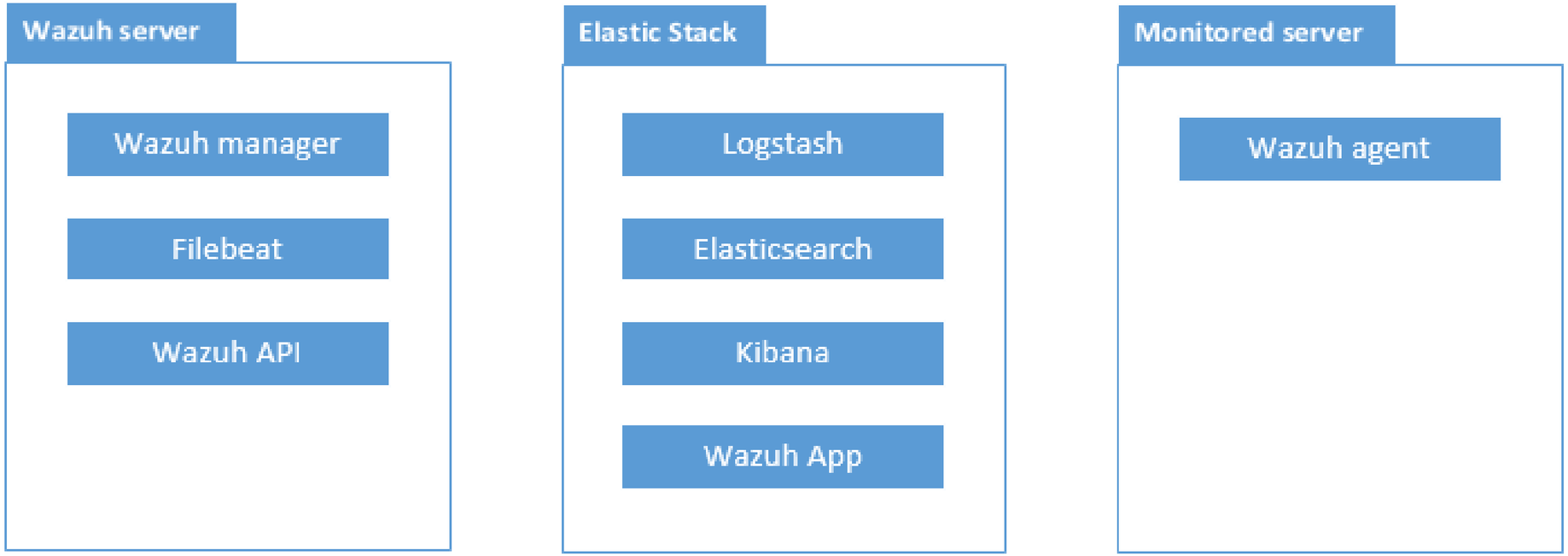
Wazuh tiene dos componentes principales que instalar: Wazuh Manager y Elastic Stack. Hay dos tipos de arquitectura para la instalación de Wazuh:

- **Arquitectura centralizada**: Wazuh y Elastic Stack se ejecutan en el mismo servidor. La siguiente imagen muestra como es este tipo de arquitectura:



3. Arquitectura de Wazuh

- **Arquitectura distribuida**: Wazuh y Elastic Stack se ejecutan en distintos servidores y en uno o varios formando así un clúster. En la siguiente imagen se muestra su arquitectura:



4. Ventajas y desventajas de Wazuh

Ventajas:

- Está basado en OSSEC. Es su predecesor.
- Se pueden monitorizar clouds como AWS o Azure.
- Estándares de cumplimiento normativo como PCI DSS.
- Se puede implementar con Docker, Ansible, Puppet, cheff...
- Permite escaneo de vulnerabilidades.
- Se integra con Splunk para alertas y datos de API.

Desventajas

- Requiere de ELK Stack para su funcionamiento.
- Esto conlleva a un mayor consumo de recursos.
- Limitación de los sistemas operativos compatibles.

Gracias

ALEJANDRO MONTES DELGADO