Módulo 2. Despliegue Base de SIEM

CÓRDOBA CREA FUTURO

1. Wazuh

2. Graylog / ELK

Referencias

1. Wazuh

En los entornos de monitoreo de seguridad, la capacidad de analizar registros provenientes de múltiples sistemas depende no solo de la generación de logs, sino también de la existencia de plataformas que permitan recolectar, procesar y visualizar esos datos de forma estructurada. En el módulo anterior se abordaron los fundamentos de los registros de eventos, incluyendo sus fuentes, formatos, mecanismos de normalización y criterios de organización. Sobre esta base conceptual se construyen las plataformas de gestión de eventos de seguridad, conocidas como sistemas SIEM (Security Information and Event Management).

Los sistemas SIEM permiten centralizar registros generados por distintos componentes de una infraestructura tecnológica, como servidores, aplicaciones, dispositivos de red y herramientas de seguridad. Una vez recolectados, estos eventos pueden ser procesados para identificar patrones de actividad, generar alertas y facilitar el análisis del comportamiento de los sistemas. La implementación de estas plataformas constituye una práctica utilizada por organizaciones que necesitan supervisar entornos tecnológicos complejos y mantener visibilidad sobre las actividades que ocurren dentro de su infraestructura.

En este contexto surgen preguntas operativas que orientan el despliegue inicial de estas herramientas: ¿cómo se instala una plataforma de monitoreo de eventos en una infraestructura tecnológica? ¿de qué manera se integran los sistemas que generan registros con el sistema central de análisis? ¿cómo se organizan las reglas que permiten interpretar los eventos recolectados?

Asimismo, una vez que los registros han sido procesados, resulta necesario contar con mecanismos que permitan visualizar y explorar la información, facilitando su interpretación por parte de los equipos responsables del monitoreo.

La plataforma Wazuh constituye una de las soluciones utilizadas para implementar sistemas de monitoreo de seguridad basados en logs. Esta herramienta permite recolectar eventos generados por distintos sistemas mediante agentes, procesar los registros utilizando reglas de análisis y visualizar la información a través de paneles de monitoreo. Estas capacidades permiten construir una infraestructura de observabilidad orientada al análisis de eventos de seguridad.

En esta unidad se abordarán los componentes principales que intervienen en el despliegue inicial de Wazuh, incluyendo el proceso de instalación base del sistema, el registro de agentes que recolectan eventos, la utilización de reglas para interpretar los logs y el uso de *dashboards* para visualizar la información generada por la plataforma. Estos elementos permiten comprender cómo se implementa una plataforma de monitoreo de seguridad y cómo se integran los registros generados por los sistemas dentro de un entorno de análisis centralizado.

Instalación base

El despliegue de una plataforma de monitoreo de seguridad comienza con la instalación de los componentes que permiten recolectar, procesar y visualizar los registros generados por los sistemas. En el caso de Wazuh, la instalación base establece la infraestructura inicial sobre la cual se apoyan los procesos de análisis de eventos, gestión de agentes y visualización de datos. Esta etapa constituye el primer paso para construir un entorno de monitoreo capaz de integrar registros provenientes de distintos sistemas dentro de una misma plataforma.

La arquitectura de Wazuh se organiza a partir de varios componentes que trabajan de forma coordinada. Entre los elementos principales se encuentran el servidor Wazuh, responsable de procesar los eventos recibidos; el indexador, que permite almacenar e indexar los datos; y el dashboard, que proporciona una interfaz para explorar y visualizar la información registrada. Estos componentes conforman la base del sistema y permiten transformar los registros generados por los sistemas en información que puede analizarse dentro de la plataforma.

La guía de instalación de Wazuh describe un proceso de despliegue que permite instalar estos componentes de forma integrada mediante un procedimiento simplificado. Este proceso de instalación automatiza la configuración inicial del sistema y facilita la puesta en funcionamiento de la plataforma en entornos de prueba o en implementaciones iniciales de monitoreo (Wazuh, s. f.).

Durante la instalación base, el sistema configura los servicios necesarios para que los distintos componentes de la plataforma puedan comunicarse entre sí. El servidor se encarga de recibir los eventos enviados por los agentes, mientras que el indexador organiza la información para que pueda consultarse posteriormente. El *dashboard* permite acceder a los datos mediante paneles que facilitan la exploración de los registros y la observación del estado de la infraestructura.

Una vez finalizado el proceso de instalación, la plataforma se encuentra preparada para comenzar a recibir registros de eventos provenientes de distintos sistemas. Sin embargo, para que esto ocurra es necesario desplegar agentes en los equipos que generarán los logs. Estos agentes se encargan de recolectar los registros del sistema y enviarlos al servidor de Wazuh para su procesamiento.

La instalación base también establece los servicios que permiten gestionar la seguridad del sistema. El proceso de despliegue incluye la configuración de certificados y mecanismos de autenticación que protegen la comunicación entre los distintos componentes de la plataforma. Esto permite garantizar que los datos de eventos se transmitan de forma segura dentro de la infraestructura de monitoreo.

En los entornos de monitoreo de seguridad, la instalación inicial de la plataforma constituye una etapa que requiere verificar distintos aspectos técnicos antes de comenzar a integrar fuentes de logs. Para facilitar esta revisión, es posible utilizar una checklist que permita confirmar que los componentes principales del sistema se encuentran correctamente configurados.

Checklist de verificación para instalación base de Wazuh

- [ ] El servidor Wazuh se encuentra instalado y en ejecución.
- [ ] El indexador está configurado y operativo para almacenar eventos.
- [ ] El dashboard se encuentra accesible desde el navegador.
- [ ] Los servicios principales del sistema se encuentran activos.
- [ ] La comunicación entre los componentes del sistema funciona correctamente.
- [ ] Los certificados y mecanismos de autenticación se encuentran configurados.
- [ ] La plataforma se encuentra preparada para registrar agentes.

La verificación de estos elementos permite confirmar que la infraestructura básica del sistema se encuentra operativa antes de comenzar a integrar fuentes de eventos. Una vez que la instalación base ha sido completada y verificada, el siguiente paso consiste en desplegar los agentes que permitirán recolectar los registros generados por los sistemas dentro de la infraestructura tecnológica.

Este proceso será analizado en el siguiente apartado, donde se abordará el registro de agentes y la recolección de eventos dentro de la plataforma Wazuh.

Agentes y registro

Una vez que la plataforma Wazuh ha sido instalada y los componentes principales del sistema se encuentran operativos, el siguiente paso consiste en integrar los sistemas que generarán los registros de eventos. Este proceso se realiza mediante el despliegue de **agentes**, que son componentes de software instalados en los equipos que se desea monitorear. Los agentes permiten recolectar información del sistema y enviarla al servidor Wazuh para su procesamiento y análisis.

Los agentes constituyen uno de los elementos centrales en la arquitectura de Wazuh, ya que permiten extender la capacidad de monitoreo de la plataforma hacia diferentes sistemas dentro de una infraestructura tecnológica. Cada agente se instala en un equipo específico —como servidores, estaciones de trabajo o sistemas virtualizados— y se encarga de recopilar eventos relacionados con la actividad del sistema operativo, los archivos del sistema y otros elementos relevantes para el monitoreo de seguridad.

Una vez instalado, el agente establece comunicación con el servidor Wazuh para registrar el sistema dentro de la plataforma. Este proceso se conoce como registro de agentes o agent enrollment. Durante esta etapa, el agente obtiene las credenciales necesarias para identificarse ante el servidor y poder enviar los registros que recolecta del sistema. Este mecanismo permite que el servidor reconozca los equipos monitoreados y gestione de forma centralizada los eventos que generan.

La documentación técnica de Wazuh describe que el registro de agentes permite establecer una relación entre el sistema monitoreado y el servidor de análisis, de modo que los eventos generados por el agente puedan ser procesados por el motor de análisis del sistema (Wazuh, s. f.). A partir de este proceso, los registros generados por los sistemas comienzan a formar parte del flujo de datos que la plataforma utiliza para construir su base de eventos.

Los agentes pueden recolectar distintos tipos de información según la configuración establecida. Entre los datos que pueden registrar se incluyen eventos del sistema operativo, modificaciones en archivos críticos, actividad de procesos y otros registros relevantes para el análisis de seguridad. Esta información se envía periódicamente al servidor, donde es procesada por los mecanismos de análisis del sistema.

El proceso de recolección de eventos se basa en la transmisión de los registros desde los agentes hacia el servidor Wazuh mediante canales de comunicación seguros. Este mecanismo permite centralizar la información generada por múltiples sistemas dentro de un único entorno de análisis. A partir de esta centralización, la plataforma puede organizar los eventos, aplicar reglas de análisis y presentar los resultados dentro de los paneles de monitoreo.

La gestión de agentes también permite administrar los sistemas monitoreados desde una interfaz centralizada. A través del panel de administración de Wazuh es posible visualizar los agentes registrados, verificar su estado de conexión y gestionar su configuración. Esta capacidad facilita el control de los sistemas que forman parte de la infraestructura de monitoreo y permite identificar rápidamente si alguno de los agentes deja de enviar eventos.

En entornos donde múltiples sistemas generan registros de eventos, el uso de agentes permite construir una red de recolección de datos que alimenta continuamente la plataforma de monitoreo. Esta infraestructura de agentes

constituye la base sobre la cual se desarrollan posteriormente los procesos de análisis de eventos y detección de comportamientos relevantes dentro del sistema.

Una vez que los agentes se encuentran registrados y comienzan a enviar registros al servidor, la plataforma puede aplicar reglas de análisis para interpretar los eventos recolectados. Estas reglas permiten identificar patrones dentro de los logs y clasificar las actividades registradas por los sistemas. Este mecanismo será abordado en el siguiente apartado dedicado al uso de reglas en Wazuh.

Reglas

Una vez que los agentes comienzan a enviar registros al servidor Wazuh, el sistema debe interpretar la información contenida en esos eventos para identificar actividades relevantes dentro de la infraestructura tecnológica. Este proceso se realiza mediante el uso de **reglas**, que permiten analizar los logs recolectados y clasificar los eventos según el tipo de actividad que representan. Las reglas constituyen uno de los mecanismos principales que utiliza Wazuh para transformar los registros en información que puede ser interpretada dentro del sistema de monitoreo.

Las reglas funcionan como instrucciones que describen cómo debe interpretarse un determinado tipo de evento dentro del sistema. Cada regla establece condiciones que permiten identificar patrones específicos dentro de los registros. Cuando un evento coincide con las condiciones definidas en una

regla, el sistema genera una alerta o clasifica el evento dentro de una categoría determinada.

El conjunto de reglas utilizado por Wazuh se conoce como ruleset, que agrupa múltiples reglas diseñadas para analizar diferentes tipos de eventos. Este conjunto incluye reglas orientadas a interpretar registros provenientes de sistemas operativos, aplicaciones, servicios de red y herramientas de seguridad. Al aplicar estas reglas sobre los logs recolectados, el sistema puede identificar comportamientos que requieren atención dentro del proceso de monitoreo.

Según la documentación de Wazuh, las reglas permiten analizar eventos que han sido previamente interpretados por los mecanismos de procesamiento de logs del sistema (Wazuh, s. f.). Una vez que los registros han sido procesados y sus campos principales han sido identificados, las reglas pueden evaluar la información contenida en esos eventos para determinar si representan una actividad relevante dentro de la infraestructura tecnológica.

Cada regla incluye distintos elementos que permiten describir el evento que se desea detectar. Entre estos elementos se encuentran condiciones relacionadas con los campos del registro, el nivel de severidad asociado al evento y la descripción de la actividad que representa. Estos componentes permiten organizar las alertas generadas por el sistema y facilitar su interpretación dentro de la plataforma de monitoreo.

Las reglas también permiten definir diferentes niveles de severidad para los eventos detectados. Estos niveles ayudan a clasificar las alertas según la importancia de la actividad registrada. Por ejemplo, algunas reglas pueden identificar eventos informativos relacionados con el funcionamiento normal del sistema, mientras que otras pueden señalar actividades que requieren análisis por parte del equipo de monitoreo.

Además del conjunto de reglas incluido en la configuración inicial de Wazuh, la plataforma permite personalizar o crear reglas adicionales según las necesidades de cada entorno tecnológico. Esta capacidad permite adaptar el sistema de monitoreo a las características específicas de la infraestructura que se desea supervisar. De este modo, las organizaciones pueden incorporar reglas diseñadas para detectar actividades relevantes dentro de sus propios sistemas.

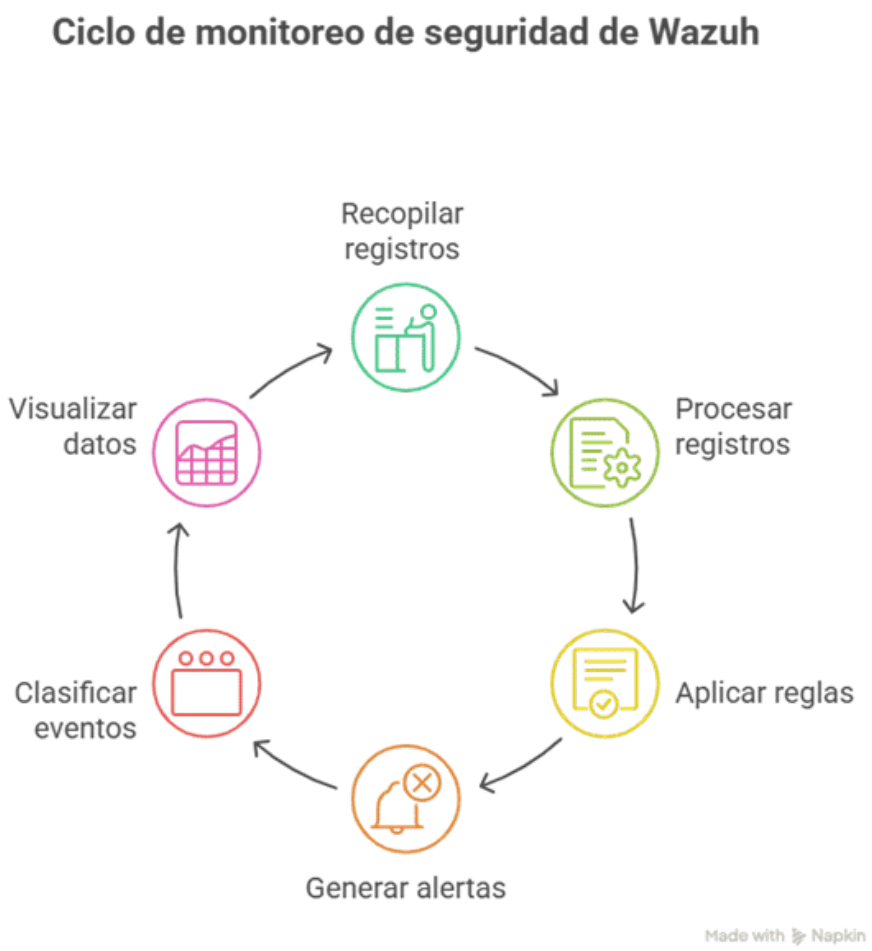
La personalización de reglas constituye una práctica que permite ampliar las capacidades del sistema de monitoreo. Al definir nuevas reglas, los administradores pueden ajustar el comportamiento del sistema para identificar eventos que resulten relevantes dentro de su entorno tecnológico. Este proceso permite adaptar el análisis de logs a diferentes contextos operativos y fortalecer los mecanismos de supervisión de la infraestructura.

El uso de reglas permite transformar los registros recolectados por los agentes en **alertas y eventos clasificados**, lo que facilita su interpretación dentro del sistema de monitoreo. Una vez que los eventos han sido procesados por las

reglas, los resultados pueden visualizarse dentro de los paneles de monitoreo que proporciona la plataforma.

En el siguiente apartado se abordará el uso de **dashboards**, que permiten visualizar la información generada por el sistema de monitoreo y explorar los eventos detectados por la plataforma Wazuh.

Figura 1. Ciclo de monitoreo de seguridad de Wazuh



Fuente: elaboración propia.

Dashboards

Una vez que los registros de eventos han sido recolectados por los agentes y procesados por el motor de análisis del sistema, resulta necesario contar con herramientas que permitan visualizar e interpretar la información generada por la plataforma de monitoreo. En el caso de Wazuh, esta función se realiza mediante el Wazuh *Dashboard*, una interfaz que permite explorar los datos recolectados, observar el estado de los sistemas monitoreados y analizar los eventos detectados por la plataforma.

El *dashboard* constituye el punto de acceso principal para interactuar con la información generada por el sistema de monitoreo. A través de esta interfaz, los usuarios pueden consultar registros de eventos, examinar alertas generadas por las reglas del sistema y observar distintos indicadores relacionados con la actividad de la infraestructura tecnológica. Este entorno permite transformar los datos almacenados por el sistema en representaciones visuales que facilitan su interpretación.

Según la documentación de Wazuh, el *dashboard* permite acceder a distintas vistas que organizan la información del sistema en paneles de visualización (Wazuh, s. f.). Estos paneles pueden incluir gráficos, tablas y representaciones agregadas de los eventos recolectados por la plataforma. De esta forma, los usuarios pueden observar tendencias dentro de los registros y analizar la actividad registrada por los distintos sistemas monitoreados.

El uso de paneles de visualización permite examinar la información desde diferentes perspectivas. Algunos dashboards muestran el estado general del sistema, incluyendo el número de agentes conectados o la cantidad de eventos registrados en un período

determinado. Otros paneles permiten explorar alertas específicas generadas por las reglas del sistema o examinar registros relacionados con determinadas categorías de eventos.

La visualización de datos constituye un elemento importante dentro de los sistemas de monitoreo, ya que permite comprender de forma más clara el comportamiento de la infraestructura tecnológica. A través de gráficos y representaciones visuales, los equipos responsables del monitoreo pueden identificar patrones de actividad, examinar eventos relevantes y comprender cómo se relacionan distintos registros dentro del sistema.

El *dashboard* también permite realizar consultas sobre los registros almacenados por la plataforma. Los usuarios pueden filtrar eventos según distintos criterios, como el sistema que generó el registro, el tipo de evento detectado o el momento en que ocurrió la actividad. Esta capacidad permite explorar grandes volúmenes de datos de forma estructurada y facilita el análisis de los registros generados por la infraestructura.

Además de visualizar los eventos recolectados, el *dashboard* permite gestionar distintos aspectos del sistema de monitoreo. Desde esta interfaz es posible revisar el estado de los agentes registrados, observar la actividad del sistema y acceder a distintas herramientas de análisis que permiten examinar los registros de eventos.

La capacidad de visualizar los datos recolectados constituye un componente esencial dentro de la

operación de una plataforma SIEM. A través de los dashboards, los registros procesados por el sistema se transforman en información que puede ser interpretada por los equipos de monitoreo. Este proceso permite comprender la actividad de los sistemas monitoreados y facilita la identificación de eventos que requieren análisis adicional.

Una vez que los registros pueden visualizarse y explorarse dentro de la plataforma, el sistema de monitoreo se encuentra preparado para integrar otras herramientas de análisis y procesamiento de datos. En la siguiente unidad se abordará una introducción a plataformas como Graylog y ELK, que también permiten recolectar, organizar y analizar registros de eventos dentro de infraestructuras de monitoreo.

CONTINUAR

2. Graylog / ELK

En el módulo anterior se abordaron los fundamentos de los registros de eventos y los mecanismos utilizados para organizar y analizar logs dentro de entornos de monitoreo. Sobre esa base conceptual, en la unidad anterior se analizó el despliegue inicial de Wazuh, incluyendo su instalación, la incorporación de agentes, el uso de reglas de análisis y la visualización de eventos mediante dashboards. Estos componentes permiten construir una infraestructura inicial de monitoreo basada en la recolección y análisis de registros provenientes de distintos sistemas.

Sin embargo, las plataformas de monitoreo de eventos suelen integrarse con otras herramientas que amplían las capacidades de análisis y gestión de logs dentro de una infraestructura tecnológica. En este contexto, soluciones como Graylog y el conjunto de herramientas conocido como ELK (Elasticsearch, Logstash y Kibana) permiten recolectar, almacenar, explorar y visualizar grandes volúmenes de registros generados por múltiples sistemas. Estas plataformas se utilizan en distintos entornos de monitoreo para facilitar la exploración de datos, la búsqueda de eventos y la generación de alertas basadas en la actividad registrada.

En infraestructuras tecnológicas modernas, los sistemas pueden generar grandes cantidades de eventos en períodos de tiempo reducidos. Este volumen de información requiere herramientas que permitan organizar los datos, realizar búsquedas eficientes dentro de los registros y generar mecanismos de alerta que ayuden a identificar actividades relevantes dentro del sistema. Las

plataformas de gestión de logs ofrecen mecanismos que permiten estructurar esta información y facilitar su interpretación dentro de entornos de monitoreo.

En este contexto surgen preguntas relevantes para comprender el funcionamiento de estas herramientas: ¿cómo ingresan los registros generados por los sistemas dentro de una plataforma de análisis de logs? ¿de qué manera se organizan los eventos para facilitar su exploración dentro del sistema? ¿cómo se realizan búsquedas dentro de grandes volúmenes de registros? Asimismo, una vez que los eventos han sido procesados y organizados, resulta necesario contar con mecanismos que permitan generar alertas y reportes que faciliten el seguimiento de la actividad dentro de la infraestructura tecnológica.

En esta unidad se presentará una introducción a Graylog y al ecosistema ELK, analizando algunos de los componentes que intervienen en el procesamiento y análisis de registros de eventos. En particular, se abordarán los conceptos de entradas y streams para la organización de logs, los mecanismos de búsqueda dentro de los registros, la configuración de alertas básicas y la generación de reportes a partir de la información recolectada por estas plataformas. Estos elementos permiten comprender cómo se organizan y exploran los registros dentro de sistemas de gestión de logs utilizados en entornos de monitoreo.

Entradas / *streams*

En las plataformas de gestión de logs, el análisis de eventos comienza con el proceso de ingreso de datos al sistema. Para que los registros generados por los distintos sistemas puedan ser analizados, primero deben ser recibidos por la plataforma que centraliza la información. En el caso de Graylog, este proceso se realiza mediante componentes conocidos como inputs, que permiten recibir los logs enviados por servidores, aplicaciones, dispositivos de red u otras herramientas de monitoreo.

Los inputs constituyen los puntos de entrada a través de los cuales los registros ingresan al sistema de análisis. Cada input se configura para recibir datos utilizando determinados protocolos o formatos de transmisión. Por ejemplo, los logs pueden enviarse utilizando mecanismos como Syslog, GELF u otros métodos de transporte compatibles con la plataforma. Una vez configurado un input, los sistemas que generan registros pueden enviar sus eventos hacia Graylog, donde los datos comenzarán a formar parte del flujo de procesamiento del sistema.

Según la documentación de Graylog, los inputs permiten que la plataforma reciba datos provenientes de múltiples fuentes dentro de una infraestructura tecnológica (Graylog, s. f.). Esta capacidad permite centralizar los registros generados por distintos sistemas dentro de un entorno común de análisis, lo que facilita la exploración de los eventos y el seguimiento de la actividad registrada en la infraestructura.

Una vez que los registros ingresan al sistema, Graylog permite organizarlos mediante mecanismos conocidos como streams. Los streams funcionan como canales de clasificación que agrupan los eventos según determinadas condiciones definidas por el sistema.

Estas condiciones pueden basarse en diferentes atributos del registro, como el tipo de evento, el origen del sistema o la categoría de actividad registrada.

La utilización de streams permite organizar los registros de forma estructurada dentro de la plataforma. En lugar de analizar todos los eventos dentro de un único flujo de datos, los usuarios pueden crear streams que agrupen eventos relacionados con determinadas fuentes o tipos de actividad. Este mecanismo facilita el análisis de los registros y permite examinar conjuntos específicos de eventos dentro del sistema.

Los streams también pueden utilizarse como base para otros procesos dentro de la plataforma. Por ejemplo, los eventos agrupados en un stream específico pueden utilizarse para generar alertas o aplicar reglas de procesamiento adicionales. De este modo, los streams no solo organizan los datos dentro del sistema, sino que también contribuyen a estructurar el análisis de los registros.

La combinación de inputs y streams permite construir un flujo de procesamiento de logs dentro de la plataforma de análisis. Los inputs reciben los registros enviados por los sistemas, mientras que los streams organizan esos eventos dentro de categorías que facilitan su exploración y análisis. Este modelo permite gestionar grandes volúmenes de registros y mantener una estructura que facilite la interpretación de los eventos.

En los entornos de monitoreo de seguridad, la correcta configuración de inputs y streams permite establecer una base organizada para el análisis de logs. Al definir cómo ingresan los registros al sistema y cómo se clasifican dentro de la plataforma, se crea una estructura que facilita la exploración de los eventos y el seguimiento de la actividad dentro de la infraestructura tecnológica.

Una vez que los registros han sido ingresados y organizados dentro del sistema, resulta necesario contar con herramientas que permitan explorar y consultar los datos almacenados. Este proceso se realiza mediante los mecanismos de búsqueda que ofrecen las plataformas de análisis de logs. En el siguiente apartado se abordará el funcionamiento de las búsquedas dentro de los registros, utilizando herramientas de análisis basadas en Elasticsearch.

Búsqueda

Una vez que los registros han sido recolectados y organizados dentro de una plataforma de gestión de logs, resulta necesario contar con mecanismos que permitan explorar y consultar la información almacenada. En los sistemas de análisis de eventos, la búsqueda constituye una herramienta que permite examinar grandes volúmenes de registros y localizar eventos específicos dentro del conjunto de datos recolectados.

Las plataformas de gestión de logs utilizan motores de búsqueda diseñados para procesar grandes cantidades de información. En el ecosistema de herramientas utilizadas para el análisis de registros, Elasticsearch cumple un papel relevante al permitir indexar los eventos y facilitar su consulta mediante distintos criterios de búsqueda. Este motor organiza los datos de manera que

puedan explorarse de forma eficiente, incluso cuando el sistema almacena millones de registros (Elastic, s. f.).

La capacidad de búsqueda permite a los usuarios examinar los registros almacenados utilizando distintos atributos del evento. Por ejemplo, es posible buscar eventos asociados a un determinado usuario, identificar registros provenientes de una dirección IP específica o consultar actividades que ocurrieron dentro de un intervalo temporal determinado. Este tipo de consultas permite explorar la información registrada por el sistema y comprender mejor el comportamiento de la infraestructura tecnológica.

Los motores de búsqueda utilizados en plataformas de análisis de logs suelen ofrecer diferentes formas de consulta. Algunas búsquedas se basan en coincidencias directas dentro de los campos del registro, mientras que otras permiten utilizar expresiones más complejas para combinar múltiples criterios de análisis. Estas capacidades permiten realizar exploraciones detalladas dentro del conjunto de registros almacenados por la plataforma.

Además de localizar eventos específicos, la búsqueda también permite identificar patrones dentro de los registros. Al examinar los resultados de una consulta, los usuarios pueden observar tendencias relacionadas con la actividad de los sistemas, identificar comportamientos repetitivos o examinar eventos que comparten características similares. Este proceso facilita la interpretación de los datos generados por la infraestructura tecnológica.

En los entornos de monitoreo de seguridad, las búsquedas constituyen una herramienta utilizada para investigar actividades registradas por el sistema. Cuando ocurre un evento que requiere análisis adicional, los equipos de monitoreo pueden utilizar consultas para reconstruir la secuencia de actividades relacionadas con ese evento. Esta capacidad permite comprender el contexto en el que ocurrió una actividad y examinar los registros asociados.

Para utilizar eficazmente las herramientas de búsqueda dentro de una plataforma de análisis de logs, resulta útil revisar algunos criterios que permiten estructurar las consultas y mejorar la exploración de los registros. A continuación, se presenta una checklist que resume algunos aspectos que pueden considerarse al realizar búsquedas dentro de sistemas de gestión de logs.

Checklist para realizar búsquedas en plataformas de análisis de logs

- [ ] Se identificó el intervalo temporal que se desea analizar.
- [ ] Se definieron los campos relevantes que se utilizarán en la búsqueda.
- [ ] Se aplicaron filtros para limitar los resultados a eventos relevantes.
- [ ] Se revisó la fuente del registro para comprender el origen del evento.
- [ ] Se examinaron eventos relacionados que puedan formar parte de la misma actividad.

- [ ] Se ajustaron los criterios de búsqueda para refinar los resultados obtenidos.

La utilización de mecanismos de búsqueda permite transformar los registros almacenados en información accesible para el análisis. Al estructurar adecuadamente las consultas, los usuarios pueden explorar los eventos generados por los sistemas y comprender cómo se relacionan distintos registros dentro de la infraestructura tecnológica.

Una vez que los registros pueden explorarse mediante consultas, las plataformas de gestión de logs permiten incorporar mecanismos adicionales que ayudan a identificar eventos relevantes dentro del sistema. Entre estos mecanismos se encuentran las alertas, que permiten detectar actividades específicas dentro de los registros y generar notificaciones cuando se cumplen determinadas condiciones. Este aspecto será abordado en el siguiente apartado dedicado a las alertas básicas dentro de plataformas de análisis de logs.

Alertas básicas

En las plataformas de gestión de logs, el análisis de registros permite examinar la actividad de los sistemas y explorar eventos almacenados dentro de la infraestructura de monitoreo. Sin embargo, en muchos entornos tecnológicos resulta necesario contar con mecanismos que permitan identificar automáticamente determinadas actividades dentro de los registros. Para este propósito, las plataformas de análisis de logs incorporan sistemas de alertas, que permiten detectar eventos específicos y generar notificaciones cuando se cumplen ciertas condiciones dentro de los datos.

Las alertas constituyen un mecanismo que permite transformar los registros almacenados por el sistema en señales que indican la ocurrencia de una actividad relevante. Este proceso se basa en la definición de condiciones que el

sistema evalúa sobre los eventos registrados. Cuando un evento o un conjunto de eventos coincide con esas condiciones, la plataforma genera una alerta que puede ser visualizada dentro del sistema o enviada mediante distintos canales de notificación.

En plataformas como Graylog, las alertas se construyen a partir de reglas que analizan los eventos almacenados dentro del sistema. Estas reglas permiten definir criterios que describen el tipo de actividad que se desea detectar. Por ejemplo, una alerta puede generarse cuando se registra un número elevado de intentos fallidos de autenticación dentro de un intervalo temporal determinado o cuando se detecta actividad proveniente de una fuente específica dentro de la red.

Según la documentación de Graylog, las alertas permiten supervisar continuamente los registros almacenados en el sistema y generar notificaciones cuando se detectan eventos que cumplen determinadas condiciones (Graylog, s. f.). Este mecanismo permite automatizar parte del proceso de monitoreo y facilita la identificación de situaciones que requieren atención dentro de la infraestructura tecnológica.

Las alertas suelen configurarse a partir de diferentes componentes dentro del sistema de monitoreo. En primer lugar, se define la condición que el sistema debe evaluar sobre los registros. Esta condición puede basarse en distintos atributos del evento, como el tipo de actividad registrada, el número de eventos

ocurridos dentro de un intervalo de tiempo o la aparición de determinados valores dentro de los campos del registro.

Una vez definida la condición de alerta, el sistema puede generar notificaciones cuando se detecta la actividad definida en la regla. Estas notificaciones pueden presentarse dentro de la interfaz de la plataforma o enviarse mediante diferentes mecanismos de comunicación, como correo electrónico u otros sistemas de mensajería utilizados dentro de la infraestructura tecnológica.

Las alertas básicas constituyen un primer nivel de automatización dentro de los sistemas de monitoreo de logs. A través de estas configuraciones, la plataforma puede supervisar continuamente los registros generados por los sistemas y advertir cuando se detectan patrones de actividad que requieren análisis adicional. Este mecanismo permite reducir la necesidad de revisar manualmente grandes volúmenes de registros y facilita la identificación de eventos relevantes dentro del sistema.

En los entornos de monitoreo de seguridad, la configuración de alertas permite establecer criterios que ayudan a supervisar actividades específicas dentro de la infraestructura. Estas alertas pueden utilizarse para detectar comportamientos inusuales, supervisar eventos relacionados con la seguridad o identificar situaciones que requieren análisis por parte del equipo de monitoreo.

Una vez que los eventos pueden generar alertas dentro del sistema, las plataformas de gestión de logs también ofrecen mecanismos que permiten organizar y presentar la información recolectada en forma de reportes. Estos reportes permiten resumir la actividad registrada por el sistema y presentar la información de forma estructurada para su revisión o distribución. Este aspecto será abordado en el siguiente apartado dedicado a los reportes dentro de plataformas de análisis de logs.

Reportes

En las plataformas de gestión de logs, el análisis de registros permite examinar eventos individuales y explorar la actividad de los sistemas dentro de una infraestructura tecnológica. Sin embargo, en muchos contextos resulta útil contar con mecanismos que permitan organizar la información recolectada y presentarla de forma estructurada. Para este propósito, las herramientas de análisis de logs incorporan funciones de generación de reportes, que permiten resumir los datos almacenados por el sistema y presentarlos en formatos que facilitan su revisión.

Los reportes constituyen representaciones organizadas de la información registrada por la plataforma de monitoreo. A partir de los datos recolectados por el sistema, los usuarios pueden generar documentos o visualizaciones que sintetizan la actividad observada dentro de la infraestructura tecnológica. Estos reportes pueden incluir gráficos, tablas y paneles que muestran tendencias o indicadores relacionados con los eventos registrados.

En el ecosistema de herramientas utilizadas para el análisis de logs, Kibana ofrece funciones que permiten generar reportes a partir de los datos almacenados en Elasticsearch. Según la documentación de Elastic, estas capacidades permiten crear representaciones visuales de los datos y exportar la información en distintos formatos para su revisión o distribución (Elastic, s. f.).

La generación de reportes suele basarse en los paneles de visualización previamente configurados dentro de la plataforma. Los dashboards permiten organizar la información en gráficos o tablas que muestran distintos aspectos de la actividad registrada por el sistema. A partir de estos paneles, los usuarios pueden generar

reportes que capturan el estado de los datos en un momento determinado.

Los reportes pueden utilizarse para distintos propósitos dentro de los entornos de monitoreo. En algunos casos permiten documentar la actividad del sistema durante un período específico, mientras que en otros sirven para presentar información resumida sobre eventos detectados por la plataforma. Esta capacidad facilita la revisión de los datos y permite compartir los resultados del análisis con otros miembros del equipo o con áreas responsables de la gestión de la infraestructura tecnológica.

La utilización de reportes también permite mantener un registro de la actividad observada por los sistemas de monitoreo. Al generar informes periódicos sobre los eventos detectados, las organizaciones pueden construir una visión histórica de la actividad registrada dentro de su infraestructura tecnológica. Esta información puede resultar útil para analizar tendencias, evaluar el comportamiento de los sistemas o documentar la evolución de determinados eventos.

Además de facilitar la revisión de la información, los reportes permiten presentar los resultados del análisis de logs de forma accesible. Las representaciones visuales de los datos ayudan a comprender con mayor claridad los patrones observados dentro de los registros y facilitan la interpretación de la actividad registrada por los sistemas monitoreados.

En los entornos de monitoreo de seguridad, la generación de reportes complementa los procesos de

búsqueda y alerta dentro de las plataformas de análisis de logs. Mientras que las búsquedas permiten explorar eventos específicos y las alertas ayudan a detectar actividades relevantes, los reportes permiten sintetizar la información registrada y presentarla de manera organizada.

A lo largo de esta unidad se han analizado distintos componentes utilizados en plataformas de gestión de logs, incluyendo los mecanismos de ingreso de registros mediante inputs, la organización de eventos mediante streams, la exploración de datos mediante búsquedas, la configuración de alertas básicas y la generación de reportes. Estos elementos permiten comprender cómo las plataformas de análisis de logs organizan la información registrada por los sistemas y facilitan su interpretación dentro de entornos de monitoreo.

CONTINUAR

Referencias

Elastic. (s. f.). *Search your data*. https://www.elastic.co/guide/en/elasticsearch/reference/current/search-your-data.html

Elastic. (s. f.). *Reporting and sharing dashboards*. https://www.elastic.co/guide/en/kibana/current/reporting-getting-started.html

Graylog. (s. f.). *What is Graylog?* https://go2docs.graylog.org/current/what_is_graylog/what_is_graylog.htm

Graylog. (s. f.). *Inputs*. https://go2docs.graylog.org/current/getting_in_log_data/inputs.htm

Graylog. (s. f.). *Streams*. https://go2docs.graylog.org/current/making_sense_of_your_log_data/streams.html

Graylog. (s. f.). *Alerts and notifications*. https://go2docs.graylog.org/current/interacting_with_your_log_data/alerts.html

Wazuh. (s. f.). *Installation guide*. https://documentation.wazuh.com/current/installation-guide/index.html

Wazuh. (s. f.). *Agent enrollment*. https://documentation.wazuh.com/current/user-manual/agent-enrollment/index.html

Wazuh. (s. f.). *Ruleset and rule customization*. https://documentation.wazuh.com/current/user-manual/ruleset/index.html

Wazuh. (s. f.). *Wazuh dashboard*. https://documentation.wazuh.com/current/user-manual/wazuh-dashboard/index.html

CONTINUAR