Introducción

“ELK” es la sigla para tres proyectos open source: Elasticsearch, Logstash y Kibana.
Elasticsearch es un motor de búsqueda y analítica. Logstash es un pipeline de procesamiento de datos del lado del servidor que ingesta datos de una multitud de fuentes simultáneamente, los transforma y luego los envía a un "escondite", como Elasticsearch.
Kibana permite a los usuarios visualizar los datos en cuadros y gráficos con Elasticsearch.

El Elastic Stack es la próxima evolución en el ELK Stack.

Comenzó con Elasticsearch…
El motor de búsqueda open source, distribuido, RESTful basado en JSON. Fácil de usar, escalable y flexible, ganó hiperpopularidad entre los usuarios y una empresa se formó a su alrededor, ya sabes, para búsquedas.

Y creció con Logstash y Kibana.
Un motor de búsqueda en esencia, los usuarios empezar a usar Elasticsearch para logs y querían ingestar y visualizarlos fácilmente. Y allí llegaron Logstash, la poderosa pipeline de ingesta, y Kibana, la herramienta de visualización flexible.

Ya sea que fuera para buscar los mejores resultados de N en una jungla de documentos basados en texto, analizar eventos de seguridad o dividir métricas libremente, la comunidad mundial seguía presionando los límites con ELK.

En 2015, introdujimos una familia de agentes de datos de propósito único y livianos en la ecuación del ELK Stack. Los llamamos Beats.

Hace su entrada, el Elastic Stack

Los mismos productos open source que los usuarios conocen y aman, pero mejor integrados, más poderosos, más fáciles de empezar a usar y repletos de posibilidades.

Partes

Elasticsearch

Elasticsearch es un motor de analítica y análisis distribuido y open source para todos los tipos de datos, incluidos textuales, numéricos, geoespaciales, estructurados y desestructurados. Elasticsearch está desarrollado en Apache Lucene y fue presentado por primera vez en 2010 por Elasticsearch N.V. (ahora conocido como Elastic). Conocido por sus API REST simples, naturaleza distribuida, velocidad y escalabilidad, Elasticsearch es el componente principal del Elastic Stack, un conjunto de herramientas open source para la ingesta, el enriquecimiento, el almacenamiento, el análisis y la visualización de datos. Comúnmente referido como el ELK Stack (por Elasticsearch, Logstash y Kibana), el Elastic Stack ahora incluye una gran colección de agentes de envío conocidos como Beats para enviar los datos a Elasticsearch.

https://www.elastic.co/es/webinars/getting-started-elasticsearch?elektra=what-is-elasticsearch&storm=hero-banner-cta&rogue=gs-with-elasticsearch-webinar

¿Para qué se usa Elasticsearch?

La velocidad y escalabilidad de Elasticsearch y su capacidad de indexar muchos tipos de contenido significan que puede usarse para una variedad de casos de uso:

- Búsqueda de aplicaciones
- Búsqueda de sitio web
- Búsqueda Empresarial
- Logging y analíticas de log
- Métricas de infraestructura y monitoreo de contenedores
- Monitoreo de rendimiento de aplicaciones
- Análisis y visualización de datos geoespaciales
- Analítica de Seguridad
- Analítica de Negocios

¿Cómo funciona Elasticsearch?

Los datos sin procesar fluyen hacia Elasticsearch desde una variedad de fuentes, incluidos logs, métricas de sistema y aplicaciones web. La ingesta de datos es el proceso mediante el cual estos datos son parseados, normalizados y enriquecidos antes de su indexación en Elasticsearch. Una vez indexados en Elasticsearch, los usuarios pueden ejecutar consultas complejas sobre sus datos y usar agregaciones para recuperar resúmenes complejos de sus datos. Desde Kibana, los usuarios crean visualizaciones poderosas de sus datos, comparten dashboards y gestionan el Elastic Stack.

¿Qué es un índice de Elasticsearch?

Un índice de Elasticsearch es una colección de documentos relacionados entre sí.
Elasticsearch almacena datos como documentos JSON. Cada documento correlaciona un conjunto de claves (nombres de campos o propiedades) con sus valores correspondientes (textos, números, Booleanos, fechas, variedades de valores, geolocalizaciones u otros tipos de datos).
Elasticsearch usar una estructura de datos llamada índice invertido, que está diseñado para permitir búsquedas de texto completo muy rápidas. Un índice invertido hace una lista de cada palabra única que aparece en cualquier documento e identifica todos los documentos en que ocurre cada palabra.
Durante el proceso de indexación, Elasticsearch almacena documentos y construye un índice invertido para poder buscar datos en el documento casi en tiempo real. La indexación comienza con la API de índice, a través de la cual puedes agregar o actualizar un documento JSON en un índice específico.

¿Para qué se usa Logstash?

Logstash, uno de los productos principales del Elastic Stack, se usa para agregar y procesar datos y enviarlos a Elasticsearch. Logstash es una pipeline de procesamiento de datos open source y del lado del servidor que te permite ingestar datos de múltiples fuentes simultáneamente y enriquecerlos y transformarlos antes de que se indexen en Elasticsearch.

¿Para qué se usa Kibana?

Kibana es una herramienta de visualización y gestión de datos para Elasticsearch que brinda histogramas en tiempo real, gráficos circulares y mapas. Kibana también incluye aplicaciones avanzadas, como Canvas, que permite a los usuarios crear infografías dinámicas personalizadas con base en sus datos, y Elastic Maps para visualizar los datos geoespaciales.

¿Por qué usar Elasticsearch?

Elasticsearch es rápido. Como Elasticsearch está desarrollado sobre Lucene, es excelente en la búsqueda de texto completo. Elasticsearch también es una plataforma de búsqueda en casi tiempo real, lo que implica que la latencia entre el momento en que se indexa un documento hasta el momento en que se puede buscar en él es muy breve: típicamente, un segundo. Como resultado, Elasticsearch está bien preparado para casos de uso con restricciones de tiempo como analítica de seguridad y monitoreo de infraestructura.

Elasticsearch es distribuido por naturaleza. Los documentos almacenados en Elasticsearch se distribuyen en distintos contenedores conocidos como shards, que están duplicados para brindar copias redundantes de los datos en caso de que falle el hardware. La naturaleza distribuida de Elasticsearch le permite escalar horizontalmente a cientos (o incluso miles) de servidores y gestionar petabytes de datos.

Elasticsearch viene con un amplio conjunto de características. Además de su velocidad, la escalabilidad y la resistencia, Elasticsearch tiene una cantidad de características integradas poderosas que contribuyen a que el almacenamiento y la búsqueda de datos sean incluso más eficientes, como data rollup y gestión de ciclo de vida del índice.

El Elastic Stack simplifica la ingesta de datos, la visualización y el reporte. La integración con Beats y Logstash facilita el proceso de datos antes de indexarlos en Elasticsearch. Y Kibana provee visualización en tiempo real de los datos de Elasticsearch así como UI para acceder rápidamente al monitoreo de rendimiento de aplicaciones (APM), los logs y los datos de métricas de infraestructura.

¿Qué lenguajes de programación soporta Elasticsearch?

Elasticsearch soporta una variedad de lenguajes y hay clientes oficiales para los siguientes:

- Java
- JavaScript (Node.js)
- Go
- .NET (C#)
- PHP
- Perl
- Python
- Ruby

Repositorio Github
https://github.com/elastic

Primeros pasos
https://www.elastic.co/es/webinars/logging-observability-with-elasticsearch-service?baymax=rtp&storm=default1&elektra=products-log-monitoring&iesrc=ctr

Kibana

Kibana es una aplicación de frontend open source que se encuentra sobre el Elastic Stack y proporciona capacidades de visualización de datos y de búsqueda para los datos indexados en Elasticsearch. Comúnmente conocido como la herramienta de representación para el Elastic Stack (anteriormente llamado ELK Stack por Elasticsearch, Logstash y Kibana), Kibana también actúa como la interfaz de usuario para monitorear, administrar y asegurar un cluster del Elastic Stack; además de como concentrador centralizado de las soluciones integradas desarrolladas en el Elastic Stack. Desarrollado en 2013 en la comunidad de Elasticsearch, Kibana ha llegado a ser la ventana al propio Elastic Stack ofreciendo un portal para los usuarios y las empresas.

Para qué se usa Kibana?

La estrecha integración de Kibana con Elasticsearch y el más amplio Elastic Stack, lo convierten en la herramienta ideal para soportar lo siguiente:

1. Buscar, ver y visualizar datos indexados en Elasticsearch y analizar los datos a través de la creación de gráficos de barras, gráficos circulares, tablas, histogramas y mapas. Una vista de dashboard combina estos elementos visuales para luego compartirlos a través del navegador y brindar vistas analíticas en tiempo real de grandes volúmenes de datos para dar soporte a casos de uso como los siguientes:
    - Logging y analíticas de log
    - Métricas de infraestructura y monitoreo de contenedores
    - Monitoreo de rendimiento de aplicaciones (APM)
    - Análisis y visualización de datos geoespaciales
    - Analítica de Seguridad
    - Analítica de Negocios
2. Monitorear, administrar y asegurar una instancia del Elastic Stack a través de interfaz web
3. Centralizar el acceso para soluciones integradas desarrolladas en el Elastic Stack para aplicaciones de observabilidad, seguridad y búsqueda empresarial

Cómo funciona la búsqueda y visualización de datos en Kibana?

Kibana habilita el análisis visual de los datos de un índice de Elasticsearch o varios índices. Los índices se crean cuando Logstash (un ingestador a gran escala) o Beats (una recopilación de agentes de datos de propósito único) ingesta datos no estructurados de archivos de log y otras fuentes, y los convierte a un formato estructurado para las funcionalidades de búsqueda y almacenamiento de Elasticsearch.

La interfaz de Kibana permite a los usuarios buscar datos en índices de Elasticsearch y luego visualizar los resultados a través de opciones de gráficos estándar o apps integradas como Lens, Canvas y Maps. Los usuarios pueden elegir entre diferentes tipos de gráficos, cambiar las agregaciones de números y filtrar segmentos específicos de datos.

¿Qué es un dashboard de Kibana?

Un **dashboard de Kibana** es una recopilación de gráficos, grafos, métricas, búsquedas y mapas que se recopilaron en un solo panel. Los dashboards permiten obtener información de un vistazo sobre datos de varias perspectivas y permiten a los usuarios explorar los detalles.

¿Cómo creo dashboards en Kibana?

Para crear un dashboard en Kibana, los usuarios deben tener datos indexados en Elasticsearch y deben tener creada una búsqueda, visualización o mapa. Desde Kibana, haz clic en Dashboard en el panel de navegación lateral. Cuando se abre la interfaz de Dashboard, se muestra una visión general de los dashboards existentes. Si no hay dashboards, se pueden agregar **conjuntos de datos de muestra**, que incluyen dashboards prediseñados.
Para crear un dashboard, los usuarios pueden seguir estos pasos:

1. En el panel de navegación lateral, haz clic en **Dashboard**.
2. Luego en **Create new dashboard** (Crear nuevo dashboard).
3. Haz clic en **Add** (Agregar).
4. Usa **Add Panels** (Agregar paneles) para agregar visualizaciones y búsquedas guardadas al dashboard. Si hay una gran cantidad de visualizaciones, las listas se pueden filtrar.

Si en el encabezado hay un ícono de solo lectura, esto indica que un usuario no tiene permisos suficientes para crear, editar o guardar dashboards. Los administradores de Kibana pueden cambiar esta configuración de permisos de forma individual o grupal.

Ejemplos de dashboards de Kibana

Elastic ofrece un **sitio de demostración** diseñado para explorar Kibana. El entorno de demostración proporciona muchos ejemplos de dashboards que te permiten explorar gráficos y visualizaciones de Kibana con un set de datos de muestra.

- **Datos de Logs de muestra**
- **Vuelos globales**
- **Ingresos de comercio electrónico**

Kibana Lens

Kibana Lens es una herramienta integrada diseñada para permitir un acceso más rápido a información sobre los datos tanto para usuarios experimentados como novatos. Lens tiene una interfaz que permite arrastrar y soltar para simplificar el proceso de explorar los datos de Elasticsearch y crear elementos visuales. Lens ayuda en la creación de gráficos con sugerencias inteligentes que proporcionan formas alternativas de visualizar datos basadas en patrones de uso común y mejores prácticas de análisis de datos.
Con Kibana Lens, un usuario puede hacer lo siguiente:

- Explorar datos en un índice de Elasticsearch con una mínima interacción con el programa
- Arrastrar y soltar campos de datos para crear varias visualizaciones
- Buscar simultáneamente en varios índices de Elasticsearch para compararlos en la misma visualización
- Personalizar visualizaciones de datos cambiando los tipos de gráficos y las agregaciones en tiempo real
- Crear visualizaciones de datos interactivas sin código ni experiencia previa con Kibana

Kibana Canvas

Canvas es una aplicación de visualización y presentación de datos en Kibana. Con Canvas, los datos en vivo se pueden extraer directamente de Elasticsearch y combinarse con colores, imágenes, texto y otras opciones personalizadas para crear pantallas dinámicas de varias páginas.

Con Canvas, un usuario puede hacer lo siguiente:

- Crear y personalizar un espacio de trabajo con fondos, bordes, colores, fuentes y más
- Personalizar paneles de trabajo con visualizaciones personalizadas, como imágenes y texto
- Personalizar datos extrayéndolos directamente de Elasticsearch
- Mostrar datos con gráficos, grafos, monitores de progreso y más
- Enfocarse en los datos deseados para mostrarlos con filtros

¿Por qué usar Kibana?

Kibana es la interfaz oficial de Elasticsearch. Los usuarios de Elasticsearch encontrarán que Kibana es la interfaz más efectiva para descubrir información sobre los datos y realizar una administración activa del estado de su Elastic Stack.

Kibana aborda muchos casos de uso. Elastic ha hecho una gran inversión para innovar la interfaz de visualización. Los usuarios aprovechan las características integradas de Kibana para casos de uso como APM, Analítica de Seguridad, Analítica de Negocios, monitoreo de tiempo de actividad, analíticas geoespaciales y más.

Kibana tiene un gran apoyo de la comunidad. Como interfaz open source, Kibana se adoptó ampliamente y tiene un gran aporte de la comunidad. Los niveles de experiencia de los usuarios de Kibana varían enormemente; la documentación, la instrucción y el soporte de la comunidad reflejan este amplio espectro de experiencia. Elastic también ofrece capacitación y soporte individual para ayudar a los usuarios a ponerlo en marcha.

Características de Kibana

Las características integradas y de acceso con suscripción ayudan a los usuarios a descubrir y mostrar su información sobre los datos. Kibana tiene docenas de características para la exploración, visualización, monitoreo y administración de los datos. Ve la lista completa de características de Kibana.

Seguridad de Kibana

Kibana proporciona seguridad a nivel de los campos y los documentos, encripción, Control de Acceso basado en roles (RBAC), inicio de sesión único (SSO), API de seguridad y más. Los controles de seguridad personalizados se pueden configurar en Kibana.

¿Cómo visualizo los datos en Kibana?
En la **app Visualize** en Kibana, se puede dar formato a los datos con una variedad de gráficos, tablas, mapas y más. En la documentación de Kibana se proporcionan los pasos sobre cómo **agregar visualizaciones a un dashboard**.
Desde el panel de navegación izquierdo de Kibana, las apps **Visualize**, **Canvas** y **Maps** permitirán a los usuarios visualizar datos de Elasticsearch. La app Visualize proporciona acceso a gráficos y grafos estándar, al igual que Kibana Lens. Canvas permite a los usuarios crear reportes con estilo de infografías y presentaciones respaldadas con datos en vivo, e incluye la capacidad de usar más opciones de formato detallado como elementos de CSS personalizados. Elastic Maps permite a los usuarios graficar sus datos geoespaciales usando índices de Elasticsearch como capas únicas en una sola vista.

Video
https://www.elastic.co/es/webinars/getting-started-kibana?baymax=rtp&storm=sub2&rogue=default&elektra=home&iesrc=ctr

Repositorio GitHub
https://github.com/elastic/kibana

Tutorial kibana
https://www.elastic.co/guide/en/kibana/current/getting-started.html

Kibana
https://www.elastic.co/es/kibana

Primeros pasos
https://www.elastic.co/es/webinars/getting-started-kibana?elektra=home&storm=sub2

Logtash

Centraliza, transforma y almacena tus datos
Logstash es un pipeline de procesamiento de datos de open source del lado del servidor que ingesta datos de una multitud de fuentes simultáneamente, los transforma y luego los envía a tu "escondite" favorito.

Entradas, filtros y salidas
Logstash ingesta, transforma y envía de forma dinámica tus datos independientemente de su formato o complejidad. Deriva estructura a partir de datos no estructurados con grok, descifra las coordenadas geográficas de las direcciones IP, anonimiza o excluye los campos sensibles y facilita el procesamiento general.

Ingesta datos de todas las formas, tamaños y fuentes
Los datos a menudo se encuentran repartidos o en silos en muchos sistemas en diversos formatos. Logstash admite **una variedad de entradas** que extraen eventos de una multitud de fuentes comunes, todo al mismo tiempo. Ingesta fácilmente desde tus logs, métricas, aplicaciones web, almacenes de datos y varios servicios de AWS, todo de una manera de transmisión continua.

FILTROS

Parsea y transforma tus datos sobre la marcha

A medida que los datos viajan de la fuente al almacén, los filtros Logstash parsean cada evento, identifican los campos con nombre para crear la estructura y los transforman para que terminen en un formato común para un análisis y un valor comercial más potente.
Logstash transforma y prepara de forma dinámica tus datos independientemente de su formato o complejidad:

- Deriva estructura a partir de datos no estructurados con grok
- Descifra las coordenadas geográficas a partir de las direcciones IP
- Anonimiza datos PII y excluye campos sensibles por completo
- Facilita el procesamiento general, independientemente de la fuente de datos, el formato o el esquema.

Las posibilidades son infinitas con nuestra completa **biblioteca de filtros** y el **Elastic Common Schema**.

SALIDAS

Elige tu escondite, transporta tus datos

Si bien Elasticsearch es nuestro producto de referencia que abre un mundo de posibilidades de búsqueda y analítica, no es el único disponible.
Logstash tiene **una variedad de salidas** que te permiten enrutar los datos donde lo desees, lo que te brinda la flexibilidad de desbloquear una gran cantidad de casos de uso posteriores.

EXTENSIBILIDAD

Crea y configura tu pipeline a tu manera

Logstash tiene un marco de trabajo conectable con más de 200 plugins. Mezcla, combina y orquesta diferentes entradas, filtros y salidas para trabajar en armonía con el pipeline. ¿Ingestas desde una aplicación personalizada? ¿No ves el plugin que necesitas? Los plugins de Logstash son fáciles de crear. Tenemos una API fantástica para el desarrollo de plugins y un generador de plugin para ayudarte a comenzar y compartir tus creaciones.

DURABILIDAD Y SEGURIDAD

Confía en un pipeline creado para entregar resultados

Si los nodos de Logstash fallan, Logstash garantiza al menos una vez la entrega de tus eventos en proceso con su cola persistente. Los eventos que no se procesan correctamente se pueden derivar a una cola de mensajes fallidos para su introspección y reproducción. Con la capacidad de absorber el rendimiento, Logstash escala a través de picos de ingesta sin tener que usar una capa de cola externa. Además, hemos hecho posible que asegures completamente tus pipelines de ingesta.

MONITORING

Obtén visibilidad completa de tus despliegues

Los pipelines de Logstash a menudo son multipropósito y pueden volverse sofisticados, lo que hace que una comprensión sólida del rendimiento del pipeline, la disponibilidad y los cuellos de botella sean invaluables. Con las características de monitoreo y visualizador de pipeline, puedes observar y estudiar fácilmente un nodo Logstash activo o un despliegue completo.

Beats

Beats es la plataforma para los agentes de datos con un solo propósito. Envían datos de cientos o miles de máquinas y sistemas a Logstash o Elasticsearch.

AGENTES DE DATOS

Envía desde la fuente. Simple y sencillo.
Los Beats son excelentes para recopilar datos. Se quedan en tus servidores, con tus contenedores, o se despliegan como funciones, y luego centralizan los datos en Elasticsearch. Los Beats envían datos que cumplen con **Elastic Common Schema (ECS)**, y si deseas una mayor potencia de procesamiento, pueden enviarlos a Logstash para las tareas de transformación y parseo.

PLUG AND PLAY

Acelera la experiencia de datos a visualización con módulos
Filebeat y **Metricbeat** incluyen módulos que simplifican la recopilación, el parseo y la visualización de la información de fuentes de datos clave, como sistemas, contenedores y plataformas cloud, y tecnologías de red. Ejecuta un solo comando y explora más allá.

INFORMACIÓN DE LOS ENTORNOS

Seguimiento del linaje de datos
Beats reúne los logs y las métricas de tus entornos únicos y los documenta con metadatos esenciales de hosts, plataformas de contenedores como Docker y Kubernetes y proveedores Cloud antes de enviarlos al Elastic Stack. Desde el **monitoreo de contenedores** hasta el envío de datos desde **arquitecturas sin servidor**, nos aseguramos de que tengas el contexto que necesitas.

EXTENSIBLE

¿Te falta un Beat? Que no te falte ninguno. Crea el tuyo y compártelo.
La pieza clave de cada Beat de open source es libbeat, la biblioteca común para reenviar datos. ¿Tienes un protocolo especializado que necesitas monitorear? Créalo. Te proporcionamos los elementos esenciales que necesitas. Y nuestra **lista de Beats comunitarios** sigue creciendo.

ELASTICSEARCH HOSPEDADO

Los Beats también envían a Elastic Cloud
¿Ejecutas Elasticsearch hospedado? Estos agentes ligeros también son una excelente manera de enviar datos a **Elastic Cloud**.

Canvas

Muestra tus datos, en vivo y con píxeles perfectos
Has llegado a tu espacio creativo para datos de Elasticsearch en vivo. Juega con las paletas de colores, agrega tus propios elementos de CSS, arrastra y suelta recursos, y convierte tus presentaciones y reportes en obras de arte dinámicas y con estilo de infografía.

PERSONALIZA

Expresa tus datos, a tu manera
Convierte tus datos en dashboards únicos y dinámicos con los logos, los colores y los elementos de diseño que definen **tu** marca. Ya sea que estés trabajando con logs de infraestructura, eventos de seguridad, métricas de aplicación o datos de tu proyecto Arduino de hobby, Elastic Canvas te da control creativo. De simple a estilizado, de dos tonos a tecnicolor, observa cómo tus datos toman forma de una manera que te conmueve.

INSPIRA

De lo normal a lo inesperado
La vida no sigue una plantilla. Canvas es flexible, por lo que puedes salir de la rigidez de una cuadrícula y darle vida a las cosas encantadoras que importan. Piensa en submarinos amarillos, lluvia púrpura, mirlos… o lo que sea que te inspire. Todo es un dato.

PRESENTA

Grandes ideas en la pantalla grande
Presenta los datos de Elasticsearch de forma tal que cuenten la historia de tu empresa, ya sea presentar estadísticas de vuelo en un quiosco de aeropuerto o revisar logs de autenticación en una sala de conferencias. Mantén a tu equipo comprometido con presentaciones atractivas y en tiempo real que muestren analíticas sociales, participación de los usuarios, analíticas operativas, KPI o, en realidad, cualquier dato. Además, lleva las visualizaciones fuera de Kibana; las visualizaciones compartibles de Canvas te permiten incorporar paneles de trabajo estáticos directamente en sitios HTML.

REPORTA

Usa tu marca, automatiza, celebra
¿Están empezando a confundirse los gráficos genéricos en tus correos electrónicos semanales? Crea reportes por marca con elementos personalizados que tu equipo estará encantado de abrir. Arma tus reportes una vez y observa cómo se envían automáticamente con los datos semanales, mensuales o anuales más recientes. Adiós a las acciones copiar y pegar.

SQL

Simplemente usa SELECT
Canvas tiene soporte completo para sintaxis de búsqueda de **Elasticsearch SQL** para que puedas disfrutar la emoción de escribir SELECT y ver cómo sucede la magia. Usa Elasticsearch SQL para desarrollar agregaciones y dar forma a tus datos dentro de Canvas. Luego, usa esa sintaxis familiar para las métricas, las visualizaciones de series de tiempo, las infografías y mucho más.

EXTIENDE

Más que una cara bonita

Lo nuestro no es la belleza superficial. ¿Qué le da a Canvas su profundidad? Para comenzar, un lenguaje de expresión con muchas funciones y basado en pipeline con Monaco como editor de expresión. Con características como diseño en modo oscuro, resaltado de sintaxis y ayuda sensible al contexto al pasar el mouse, tu experiencia con Canvas es hermosa desde adentro hacia afuera. Agrega nuestro marco de trabajo con plugin sin JavaScript a la combinación y tendrás opciones de personalización ilimitadas. Extender Canvas con plugins es posible para todos, desde codificadores copiar-pegar hasta los desarrolladores extremos.

OBSERVA

Los datos de Elasticsearch cobran vida

Transmitiendo datos a Elasticsearch desde una pista de carreras en riel, Rashid demuestra la manera simple en que las expresiones SQL pueden ayudar a crear visualizaciones en vivo en Canvas.

Primeros pasos
https://www.elastic.co/es/start

Elastic logs

Monitoreo de log open source
El Elastic Stack (también conocido como el ELK Stack) es la plataforma de logging open source más popular.

https://www.elastic.co/es/webinars/logging-observability-with-elasticsearch-service?baymax=rtp&storm=default1&elektra=products-log-monitoring&iesrc=ctr

Comienza con los logs que necesites

Con el soporte listo para usar para fuentes de datos comunes y además tableros predeterminados, el Elastic Stack se trata de una experiencia que simplemente funciona. Envía registros desde Kubernetes, MySQL y más. Indexa tus datos en Elasticsearch y visualiza todo en Kibana en minutos. **Continúa para comenzar con los logs de Elastic**. (Y si no ves el **módulo** que necesitas, créalo o aprovecha la comunidad. ¡Open source es genial!)

Muestra el final de un archivo directamente en la UI

Mantente al tanto de todos los logs que fluyen desde tus servidores, máquinas virtuales y **contenedores** en una visión centralizada creada para operaciones de infraestructura. Marca campos estructurados como IP o tipo de evento, y explora logs relacionados sin salir de tu pantalla actual. Accede a más información sobre la app de Logs en Kibana para una experiencia de estilo consola en todos tus logs, con transmisión en tiempo real.

Análisis de tendencias con logs categorizados

¿Buscas patrones en tus datos de eventos? En lugar de desplazarte e identificar manualmente logs similares, ve tendencias instantáneamente en la vista de categorización de logs en la UI. Analiza eventos que se han agrupado según sus mensajes y formatos para poder tomar medidas más rápido.

Procesamiento de transmisión de datos flexible
Preparar tus logs para una búsqueda rápida y centralizada es fácil con Elastic, sin importar el tipo o la cantidad de fuentes. **Beats** envía logs de tus sistemas directamente a Elasticsearch, para que puedas comenzar a analizarlos de inmediato en un solo lugar. Usa módulos de Filebeat con pipelines de **nodos de ingestión** para tipos de log comunes para procesar previamente los documentos antes de indexarlos.
Y si buscas incluso más fuerza para procesar, **Logstash** puede servir como una capa de procesamiento de transmisión de datos dedicada mediante ingesta, parseo y transformación incluso de tus datos más complejos.

Una búsqueda poderosa que escala contigo
La experiencia que tienes en una computadora portátil es la misma que tendrás en cientos de nodos con petabytes de datos. Puedes evitar los dolores de cabeza que trae volver a crear la arquitectura. Y no te preocupes por priorizar tipos o fuentes de datos (lo cual te obliga a dejar atrás datos valiosos). Ingesta e indexa todo lo que sea importante para ti.
El modelado uniforme de datos con el **Elastic Common Schema (ECS)** significa que puedes definir un conjunto común de campos de documentos y analizar de forma centralizada datos de diversas fuentes.

Ve cómo todo se despliega en tiempo real
Con Elasticsearch en el centro del Elastic Stack, puedes beneficiarte de los tiempos de respuesta rápidos, incluso a escala. Haz una pregunta y obtén una respuesta rápidamente. Lava. Enjuaga. Repite. No te quedes esperando... que los dashboards... se... carguen…

Agrega Machine Learning para una detección de anomalías automática
No deberías tener que encargarte de cada mensaje o transacción de log, sino solo de los que sean importantes o que valgan la pena.
Las características de Machine Learning de Elastic extienden el Elastic Stack para modelar automáticamente el comportamiento de tus datos de Elasticsearch y alertarte sobre los problemas en tiempo real.

https://www.elastic.co/es/log-monitoring

Grafana

¿Qué es Grafana?
Grafana es una herramienta hecha en software libre, específicamente con licencia Apache 2.0, ideada por Torkel Ödegaard (quien todavía está al frente de su desarrollo y mantenimiento) y creada en enero de 2014. Este desarrollador sueco comenzó su carrera en el ambiente **.NET** y en 2012 (hasta la fecha) sigue ofreciendo servicios de desarrollo y consultoría en esta popular plataforma privativa, de forma paralela con el desarrollo de software libre.

Grafana está escrita en **Lenguaje Go** (creado por Google) y **Node.js LTS** y con una fuerte Interfaz de Programación de Aplicaciones (API); es una aplicación que ha venido escalando posiciones, con una comunidad entusiasta de más de 600 colaboradores bien integrados (son 7 desarrolladores líderes -Torkel a la cabeza- y 5 a tiempo parcial para poder coordinar tal grupo de personas). Su código fuente está publicado, cómo no, en GitHub.

Es una herramienta para visualizar datos de serie temporales.
A partir de una serie de datos recolectados obtendremos un panorama gráfico de la situación de una empresa u organización. Del dicho al hecho: Wikidata, la enorme base de datos de conocimientos, editada en colaboración y que progresivamente va estructurando los artículos en la enciclopedia en línea Wikipedia, utiliza a grafana.wikimedia.org de manera pública para mostrar las ediciones realizadas (en nuestro caso personal lo hacemos regularmente) hechas por los colaboradores -y máquinas- con las «páginas» creadas (o mejor dicho, fichas de datos creadas) y editadas en determinado periodo de tiempo.

Para la Wikipedia y/o Wikidata? Es apenas una vía o manera de representar datos estadísticos de una manera rápida y pública, utilizando siempre código abierto y/o software libre. Otros entes que utilizan Grafana regularmente son:

- Organización Europea para la Investigación Nuclear (CERN)
- DigitalOcean, un servicio de alojamiento de máquinas virtuales basadas por entero en software libre.
- Laboratorio Nacional Fermi (FermiLab).
- ¡Y muchas otras empresas privadas!
-

¿Qué ventajas tiene Grafana?
Puede correr en modo TV (un particular eufemismo para el modo kiosko) de manera tal que, cada cierto tiempo prefijado, puede mostrar diferentes paneles de control que hayamos guardado en listas de reproducción. Esto busca solucionar dos detalles: si no podemos visualizar todo de un solo golpe en una pantalla, pues dividirlo en partes y mostrarlo de manera automática y periódica; el otro detalle es combatir la estática, para nosotros los seres humanos, de ver la misma pantalla -con valores que cambian, claro está- pero que atrae nuestra atención -y la del público, dado el caso- al hacer la transición gráfica. Para salir del modo kiosko solo debemos presionar las teclas «d» más «k», lo cual nos lleva al siguiente punto.
Grafana ama el uso del teclado. ¿Qué es Grafana sin un atajo de teclado? Es como una flor sin aroma, poéticamente hablando; para los desarrolladores este es un punto de honor: el poder trabajar sin el uso de un dispositivo apuntador tal como un ratón. De nuevo, en nuestro caso personal, valoramos mucho esta característica, no solo en este software sino en cualquier otro.

https://play.grafana.org/

Ecosistema de Grafana
Como dijimos, sirve para visualizar información, la cual es recolectada y/o procesada por aplicaciones de terceros. El **único objetivo de Grafana** es presentar los datos de monitoreo de una manera más fácil de usar y agradable. En este punto debemos hacer una aclaratoria: puede recopilar de **forma nativa** datos de Cloudwatch, Graphite, Elasticsearch, OpenTSDB, Prometheus, Hosted Metrics e InfluxDB.

Existe una versión Enterprise (grafana.com) que usa complementos para más fuentes de datos, pero no hay razón para que esos otros complementos de fuentes de datos no puedan crearse como fuente abierta, ya que el ecosistema de complementos de Grafana ya ofrece muchas otras fuentes de datos; para febrero de 2018:

- 37 complementos de fuentes de datos.
- 28 complementos para el panel.
- 15 complementos de aplicaciones.
- Más de 600 paneles de control creados para aplicaciones populares.

Recientemente le agregaron una opción para enviar, de manera manual, una alerta a donde se desee con solo ampliar la gráfica y llamar a un menú emergente. Si bien es una adición bienvenida que no necesariamente reemplazará una plataforma de alerta, ciertamente puede ayudar, al proporcionar una perspectiva diferente sobre los criterios de alerta (evidentemente, para usos y criterio masivo para cientos de dispositivos es inviable).
Grafana en el campo de la monitorización
Elasticsearch es una de las fuentes de datos para las que Grafana ofrece apoyo nativo; esto no ha de sorprendernos, considerando que Grafana inicialmente era un componente dentro de Kibana, de la cual se bifurcó. La plataforma ELK significa la combinación de Elasticsearch, Logstash y Kibana; los dos primeros componentes son utilizados por Pandora FMS desde la versión 712 (más detalles acerca de su implementación en este enlace) para la recolección de logs.

Pandora FMS tiene una poderosa consola web y la Metaconsola para unificarlas; puede correr en modo kiosko y provee poderosas herramientas asociadas a la monitorización en su conjunto. Este artículo sobre Grafana es solo una muestra de la extraordinaria flexibilidad de Pandora FMS, y no significa un endoso o respaldo público a la información aquí presentada.
El tiempo es un factor importante a la hora de la búsqueda y visualización de registros o «logs». La palabra o palabras claves serán el otro factor determinante, pero, ¿quién proporciona esta palabra clave? Para ello imaginamos escenarios no rutinarios: uno o varios ejecutivos que tengan a su disposición un programador que construya los tableros necesarios para representar la más variada información, o tal vez un administrador de red que desee tomar la información de determinado desarrollo que esté aplicando a un sistema de producción. En realidad son muchísimos los usos que podremos dar a Grafana, además de que ofrece una autenticación de usuarios a nivel de usuario que se pudiera compartir con Pandora FMS si se utiliza en ambos LDAP. Sin embargo, hallamos más útil la posibilidad de que Grafana conecte por autenticación con GitHub para que nuestros programadores puedan ellos mismos buscar su propia información de los logs sin afectar para nada el (los) sistema(s) a los cuales esté conectado Grafana. ¿Qué es Grafana para los programadores? Es la oportunidad de indagar -y revisar- el resultado, en producción- de sus propias aplicaciones, ¡sin mayor esfuerzo que el de crear los tableros y/o tableros personalizados necesarios!

Repositorio Github
https://github.com/grafana/grafana