Certificación
avanzada en

DevOps

Telemetría de Backend

UNC FCEFyN mundosE PEOPLE & BUSINESS SCHOOL

¿Qué vamos a ver hoy?

- Introducción
- De que vamos a hablar?
- Monitorizando con Elasticsearch. Logstash, Kibana, Grafana
- ¿Qué es Elasticsearch?
- ¿Qué es Logstash?
- ¿Qué es Grafana?
- ¿Qué hace Grafana?
- ¿Qué es Kibana?
- ¿Para qué se usa Kibana?
- ¿Por qué usar Kibana?

Telemetría de Backend / Monitorizando con:

Telemetría de Backend / Monitorizando con:

Es la base de datos, es un gestor de datos y almacéndistribuido.

Telemetría de Backend / Monitorizando con:

Es el gestor de logs, nos procesará la información que recopile y lo almacenará en Elasticsearch

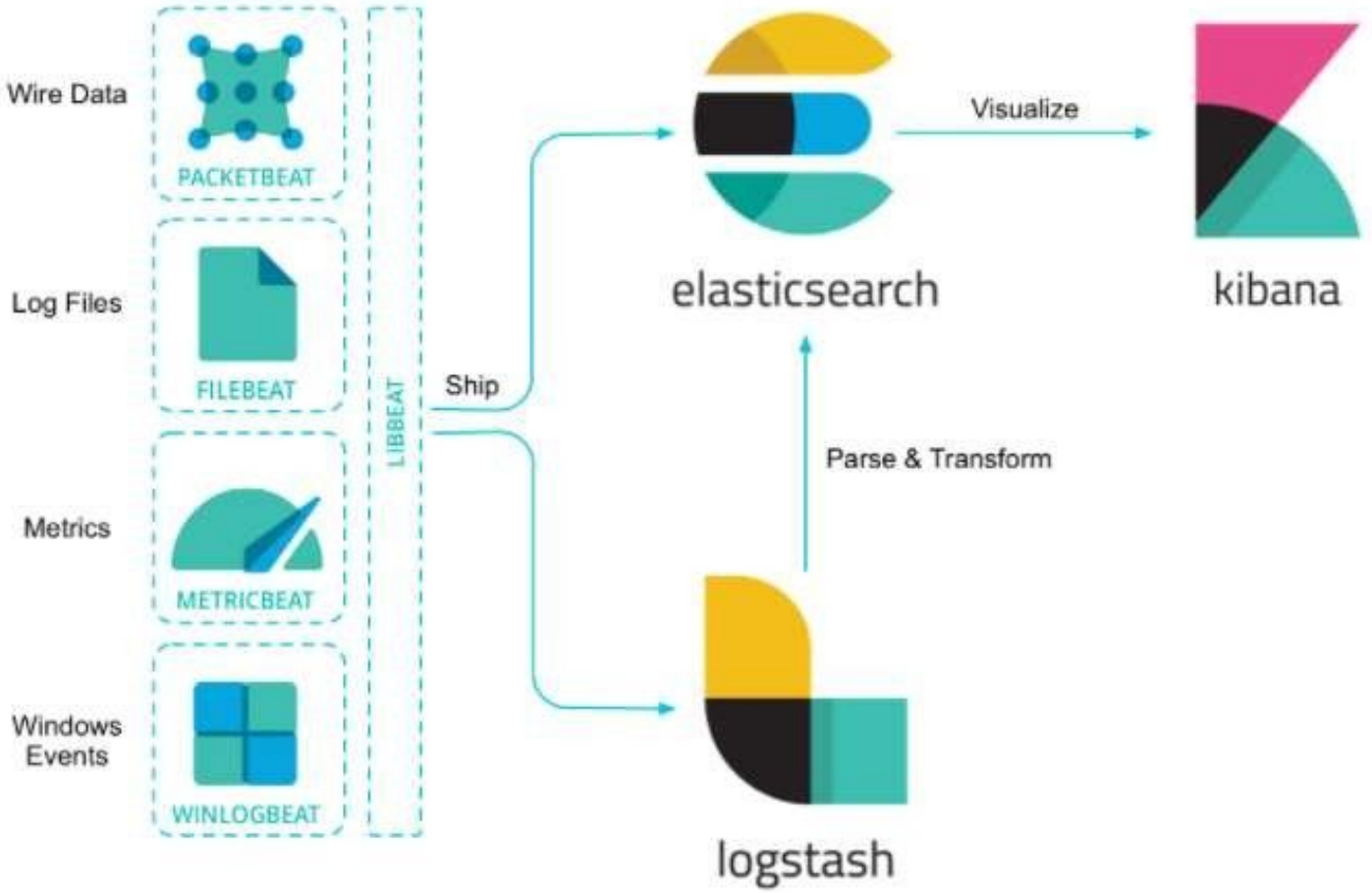
Telemetría de Backend / Monitorizando con:

Nos servirá para visualizar e interpretar los datos de Elasticsearch de una manera gráfica.

Telemetría de Backend / Monitorizando con:

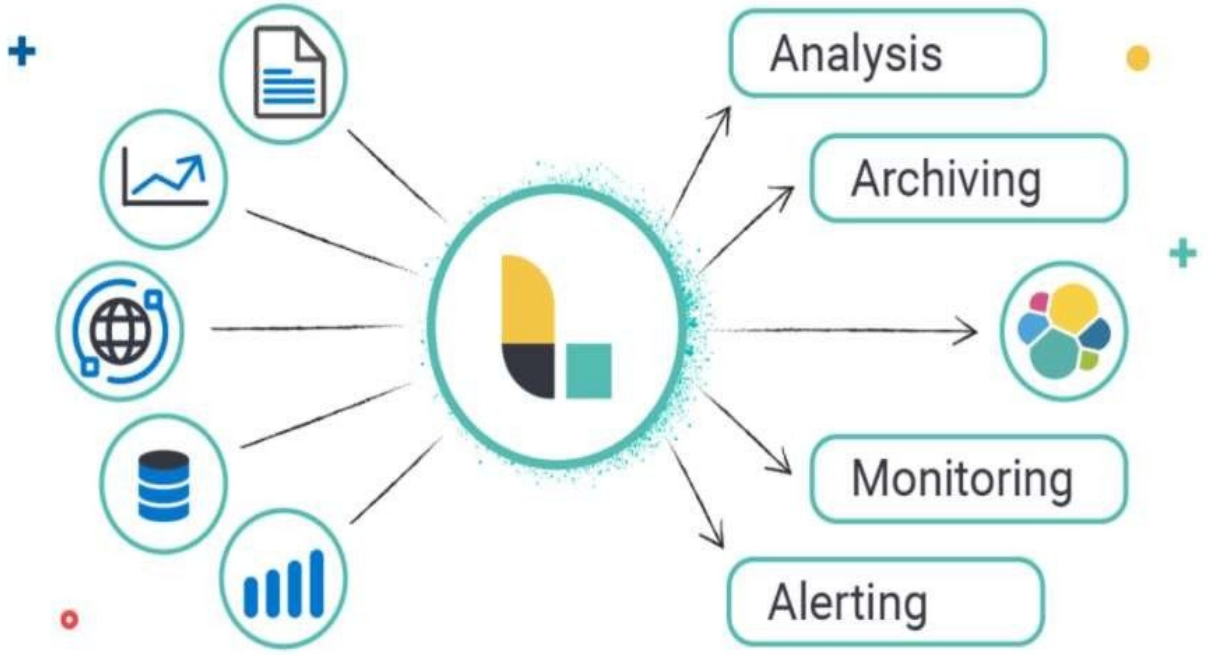
Al igual que Kibana, Grafana es visualizador de datos. Será este pues, por el que personalmente me decante a la hora de mostraros los posts.

Telemetría de Backend / Monitorizando con:



Telemetría de Backend / ¿Qué es Lonstash?

Cómo acabamos de introducir, Logstash es parte del ElasticStack. Es una herramienta Open Source que nos permite centralizar la recolección de información, normalizarla y redistribuirla. Originalmente Logstash fue pensado para la recolección de logs



Telemetría de Backend / ¿Qué es ELK?

Es un conjunto de herramientas de gran potencial de código abierto que se combinan para crear una herramienta de administración de registros permitiendo la monitorización, consolidación y análisis de logs generados en múltiples servidores, estas herramientas son: ElasticSearch, Logstash y Kibana.También pueden ser utilizadas como herramientas independientes, pero la unión de todasellas hace una combinación perfecta para la gestión de registros.

Telemetría de Backend / ¿Qué es ELK?

¿Qué busca realmente Elasticsearch?

Lo que se consigue con ELK es coger toda esta información, procesarla y almacenarla de forma distribuida. Así se va a poder escalar en Big Data y obtener buenos rendimientos con grandes cantidades de información, y transformarla en visualizaciones, con las que poder identificar anomalías, comportamientos, eventos, picos, etc., de forma gráfica y visual, como en la diapositiva mostrada.

ELK / ¿Qué hace?

- Recolecta logs de eventos y de aplicaciones.
- Procesa dicha información y la pone a disposición de las personas que la necesitan: Tiene módulos de seguridad para implementar que cada usuario accede a la información que realmente pueda administrar, evitando que un usuario acceda a información que no le pertenece.
- Formatea los campos y los convierte en opciones de búsqueda y filtrado: Hay logs que tienen formatos irregulares, ya sean de aplicaciones propias o de servicios que no sigan ningún formato. Dichos logs son prácticamente cadenas de texto muy complicadas de entender. Con Logstach trabajaremos con dichos logs convertidos en distintos campos, que después podremos utilizar después para el filtrado.
- Presenta esa información y esos campos en visualizaciones, donde podremos realizar búsquedas, filtrados, agregaciones y ver la información mucho mejor que módulos de texto.

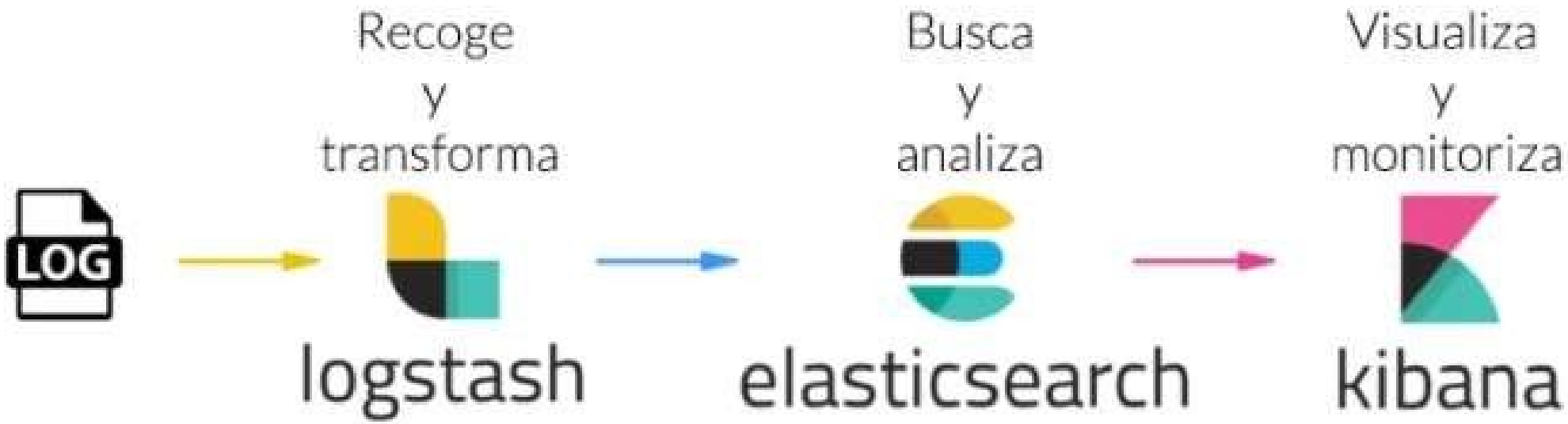
ELK / Componentes

▶ Elasticsearch: Es una base de datos distribuida. Distribuye toda la información en todos los nodos, por tanto es tolerante a fallos y tiene alta disponibilidad. Al igual que distribuye la información, distribuye el procesamiento. Cuando se realiza una consulta o búsqueda y esa información se encuentra distribuida, será cada nodo el que procese dicha información y devuelva los resultados. Por tanto, podemos obtener mejores rendimientos.

▶ Logstach:
çEs la parte de preprocesamiento antes de guardar la información en Elasticsearch que hemos comentado, donde recogemos un input, una entrada, trabajamos los eventos y los sacamos por una salida, antes de almacenarlos en las bases de datos.

▶ KibanaEs el más visual, dónde vamos a generar las visualizaciones sobre la información y dónde vamos a generar los dashboards.

ELK / Componentes



ELK / ¿Qué es Kibana?

Kibana es una aplicación de frontend gratuita y abierta que se encuentra sobre el Elastic Stack y proporciona capacidades de visualización de datos y de búsqueda para los datos indexados en Elasticsearch. Comúnmente conocida 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, gestionar 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.

ELK / ¿Para qué usar Kibana?

La estrecha integración de Kibana con Elasticsearch y el más amplio Elastic Stack, loconvierten en la herramienta ideal para soportar lo siguiente: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 logMétricas de infraestructura y monitoreo de contenedoresMonitoreo de rendimiento de aplicaciones (APM)Análisis y visualización de datos geoespacialesAnalítica de SeguridadAnalítica de NegociosMonitorear, administrar y asegurar una instancia del Elastic Stack a través de interfazweb

ELK / ¿Para qué usar Kibana?

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

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 logMétricas de infraestructura y monitoreo de contenedoresMonitoreo de rendimiento de aplicaciones (APM)Análisis y visualización de datos geoespacialesAnalítica de SeguridadAnalítica de NegociosMonitorear, administrar y asegurar una instancia del Elastic Stack a través de interfazweb

ELK / ¿Qué es grafana?

Grafana es una herramienta de código abierto para el análisis y visualización de métricas. Se utiliza frecuentemente para visualizar de una forma elegante series de datos en el análisis de infraestructuras y aplicaciones.

TAKE A BREAK!

y en 15´volvemos.

UNC FCEFyN mundosE PEOPLE & BUSINESS SCHOOL

¿Preguntas?

MUCHAS GRACIAS!

CONTACTO

UNC

FCEFyN

mundosE
PEOPLE & BUSINESS SCHOOL