X-PACK
MONITORING

MONITORING

Componente que facilita un control de recursos y estadísticas del ELK Stack.

Salud y rendimiento de Elasticsearch, Logstash y Kibana en tiempo real para analizar rendimientos.

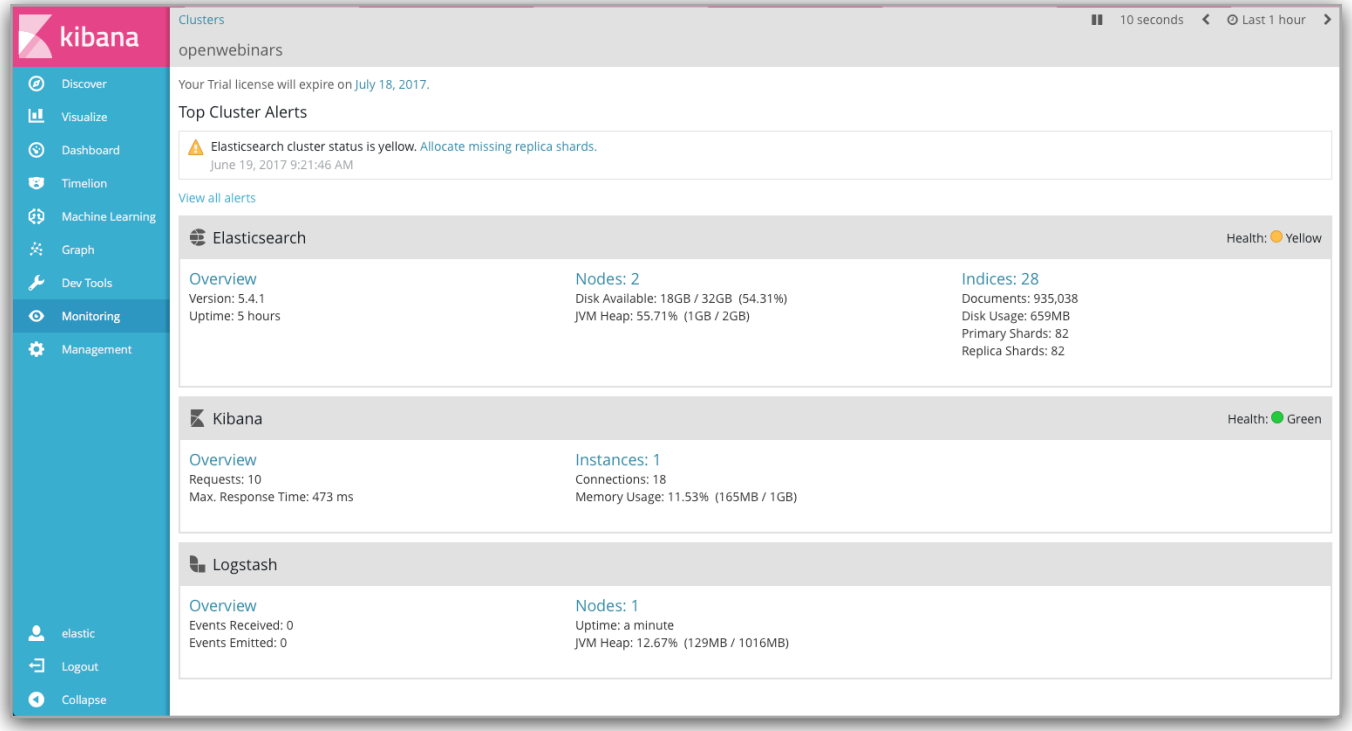
1.

INTRODUCCIÓN

INTRODUCCIÓN

- *Monitoring* activado por defecto con la instalación de X-pack.
- Debe instalarse en todos los nodos del clúster Elasticsearch, Kibana y Logstash.
- Ayuda a controlar la falta de recursos y a comprobar cómo afectan los cambios aplicados en cualquier punto del clúster al estado del mismo.

INTRODUCCIÓN



2.

CONFIGURACIÓN DE MONITORIZACIÓN

CONFIGURACIÓN DE MONITORIZACIÓN

Monitorizar elasticsearch

- Necesario tener instalado X-Pack
- Kibana debe apuntar al clúster ES en el *kibana.yml*:
  elasticsearch.url: “http://es-mon-1:9200"
- Se puede cifrar la información entre ES y Kibana:
  server.ssl.key: /path/to/your/server.key
  server.ssl.cert: /path/to/your/server.crt
- Si SSL está activado añadir la CA:
  elasticsearch.ssl.ca: “/path/to/ca/file"

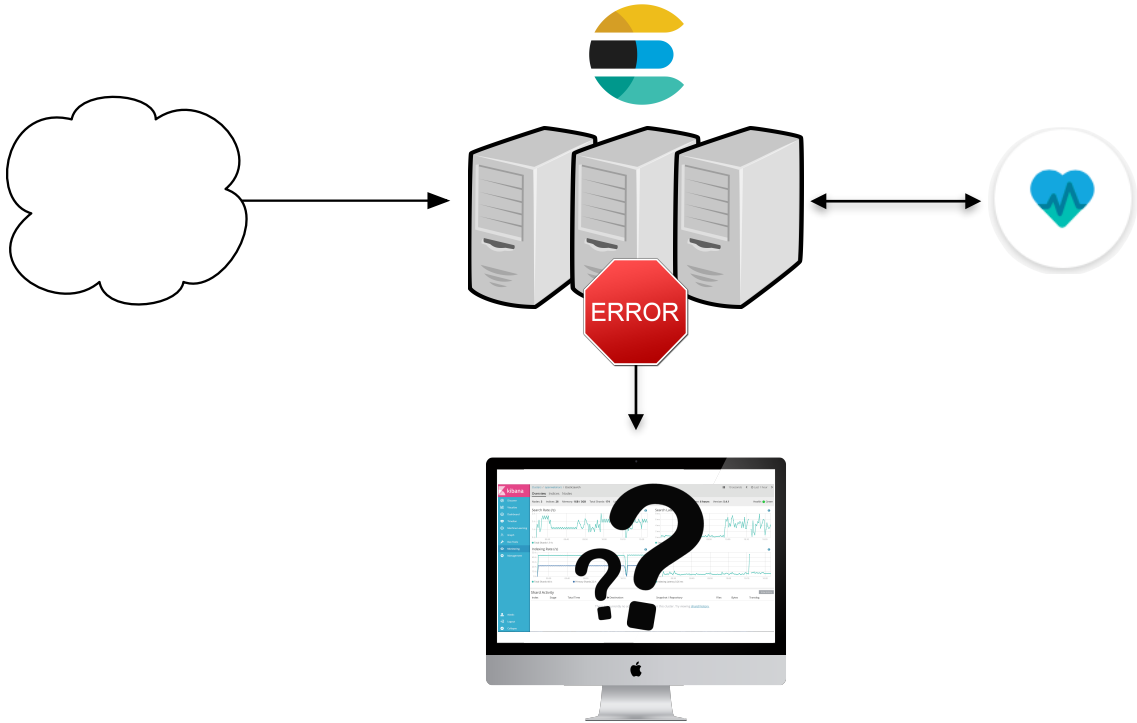
CONFIGURACIÓN DE MONITORIZACIÓN

Exportar a clúster de monitorización

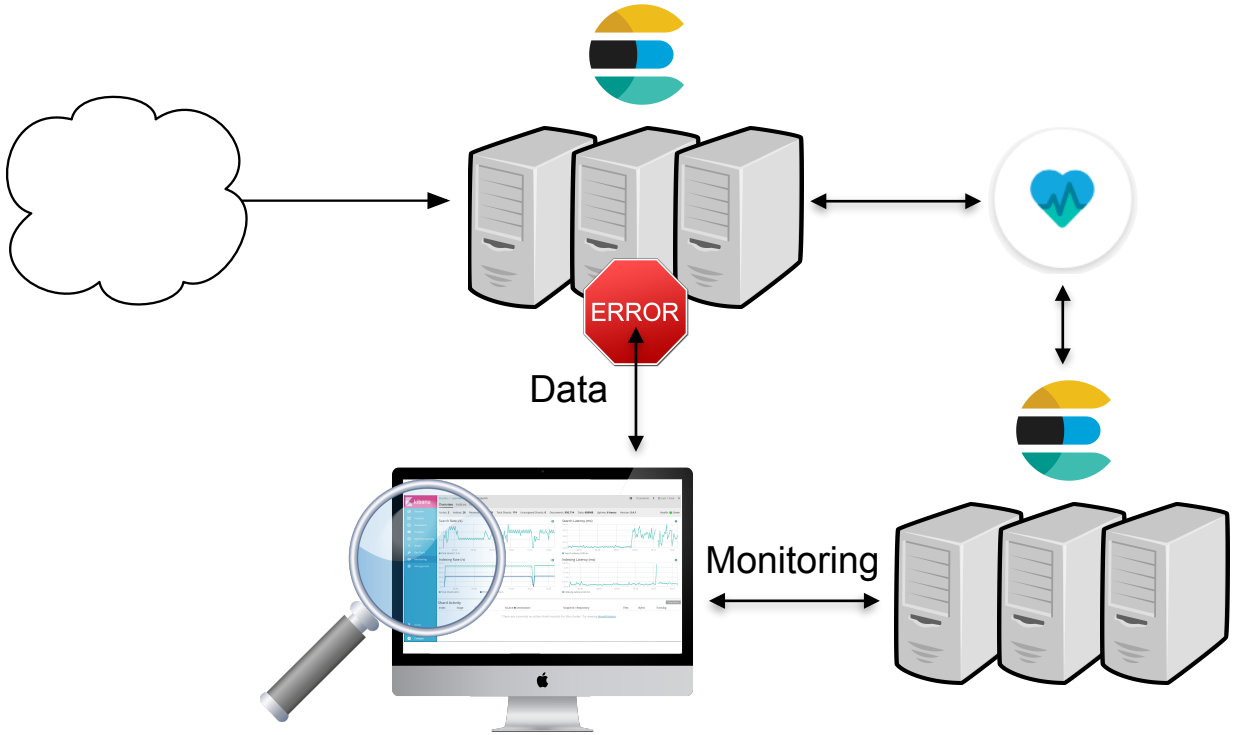
- **¡Buena práctica!**
- Reenvío de logs a otro clúster:

```
xpack.monitoring.exporters:
    id1:
        type: http
        host: ["http://es-mon-1:9200", "http://es-mon2:9200"]
        auth.username: remote_monitor
        auth.password: changeme
```

CONFIGURACIÓN DE MONITORIZACIÓN



CONFIGURACIÓN DE MONITORIZACIÓN



CONFIGURACIÓN DE MONITORIZACIÓN

Monitorizar Kibana

- Necesario tener instalado X-Pack
- Elasticsearch por defecto envía sus métricas al Elasticsearch apuntado por el parámetro *elasticsearch.url* en el *kibana.yml.*
- Importante, para usar Kibana para acceder a los 2 clúster, usar el parámetro:
  xpack.monitoring.elasticsearch.url

CONFIGURACIÓN DE MONITORIZACIÓN

Monitorizar Logstash

- Necesario tener instalado X-Pack
- IP y autenticación para indexar los datos de monitorización:

xpack.monitoring.elasticsearch.url: ["http://es-prod-node-1:9200", "http://es-prod-node-2:9200"]
xpack.monitoring.elasticsearch.username: "logstash_system"
xpack.monitoring.elasticsearch.password: "changeme"
xpack.monitoring.elasticsearch.ssl.ca: ["/path/to/ca.crt"]

3.

MÉTRICAS DE MONITORIZACIÓN

MÉTRICAS DE MONITORIZACIÓN

Alertas de clúster

- Verde (shards correctos), amarillo (falta alguna réplica) o rojo (falta al menos un primario).
- *Versión de Elasticsearch no coincide*. Aparece cuando hay diferentes versiones de ES en el mismo clúster.
- *Versión de Kibana no coincide*. Instancia de Kibana con diferente versión que el clúster de ES.

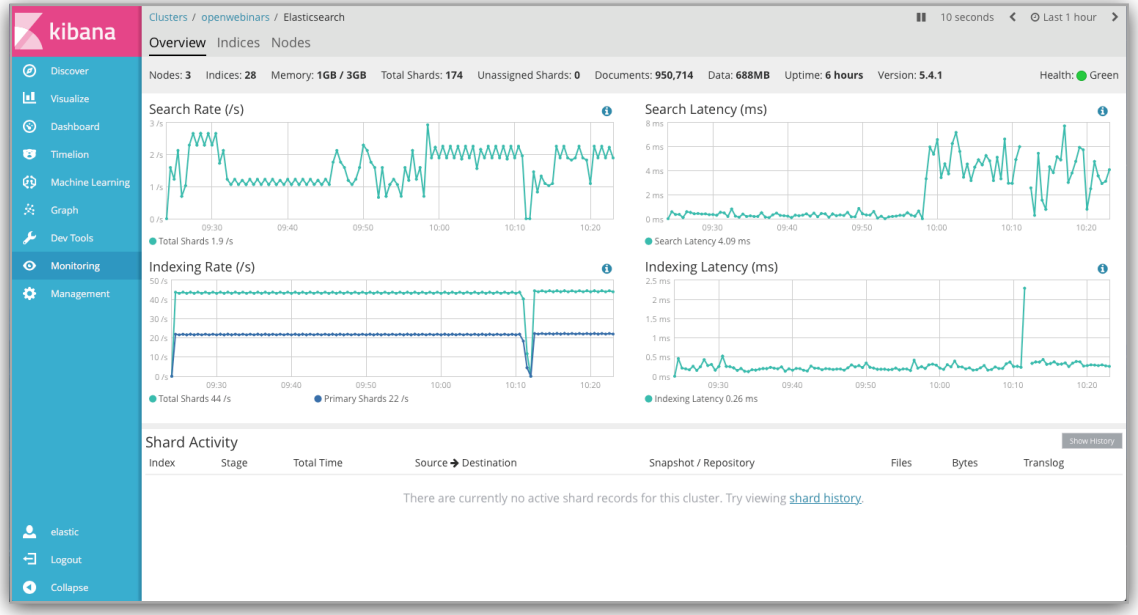
MÉTRICAS DE MONITORIZACIÓN

Elasticsearch: Vista Clúster

- *Resumen de variables del clúster y estado*. Nodos que forman el clúster, índices, RAM, Shards…
- *Estadísticas de búsqueda*. Ratio de búsqueda en *eventos/seg* y la latencia de estas búsquedas en *ms*.
- *Estadísticas de indexado*. Ratio de indexado en *eventos/seg* y la latencia de estos indexados en *ms*.
- *Actividad de shards*. Reindexados o movimientos entre nodos quedan aquí registrados.

MÉTRICAS DE MONITORIZACIÓN

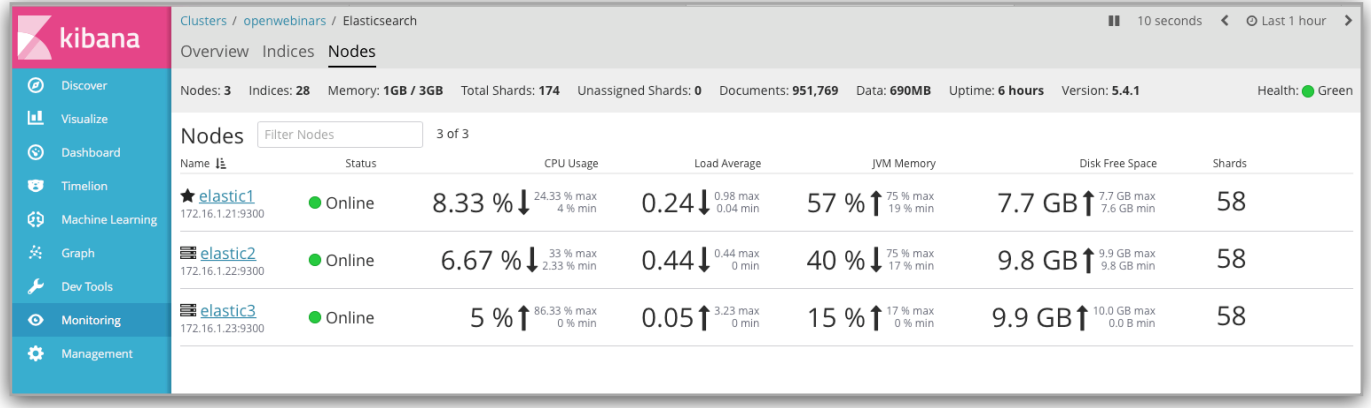
Elasticsearch: Vista Clúster



MÉTRICAS DE MONITORIZACIÓN

Elasticsearch: Nodos

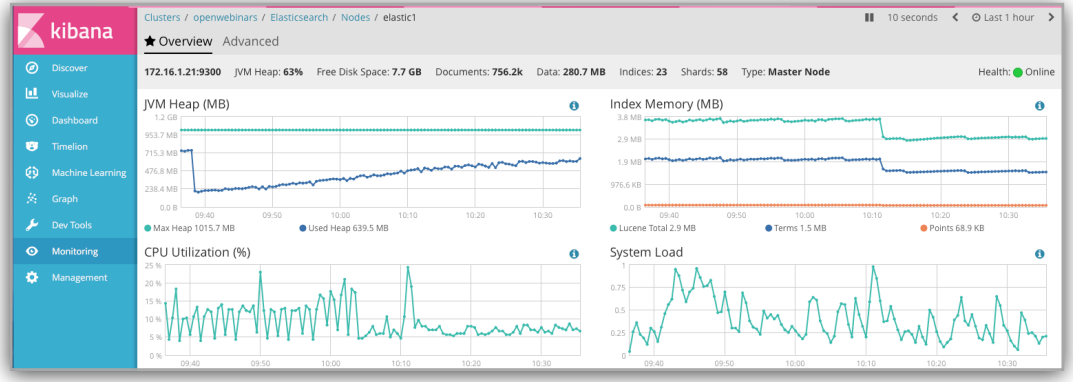
- Métricas de los nodos recursos y shards.



MÉTRICAS DE MONITORIZACIÓN

Elasticsearch: Vista Nodos

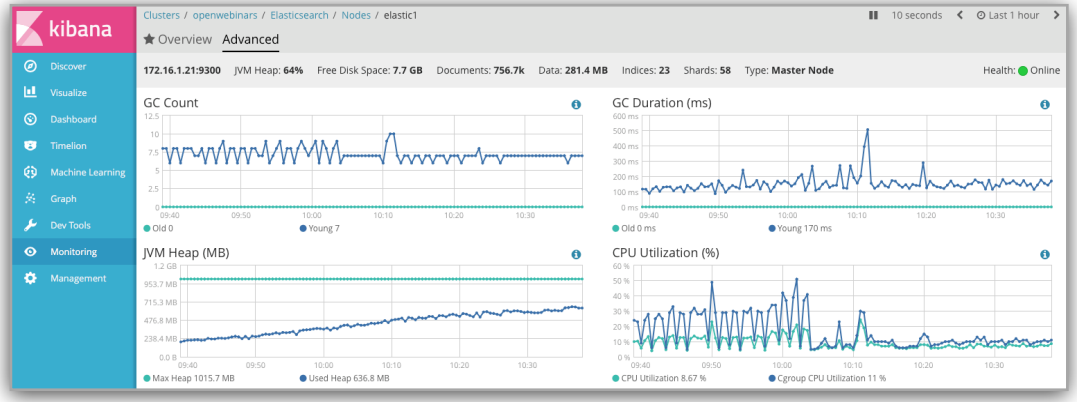
- Uso de JVM, memoria de índice, CPU, Uptime, latencia, número de segmentos.



MÉTRICAS DE MONITORIZACIÓN

Elasticsearch: Vista avanzada de Nodos

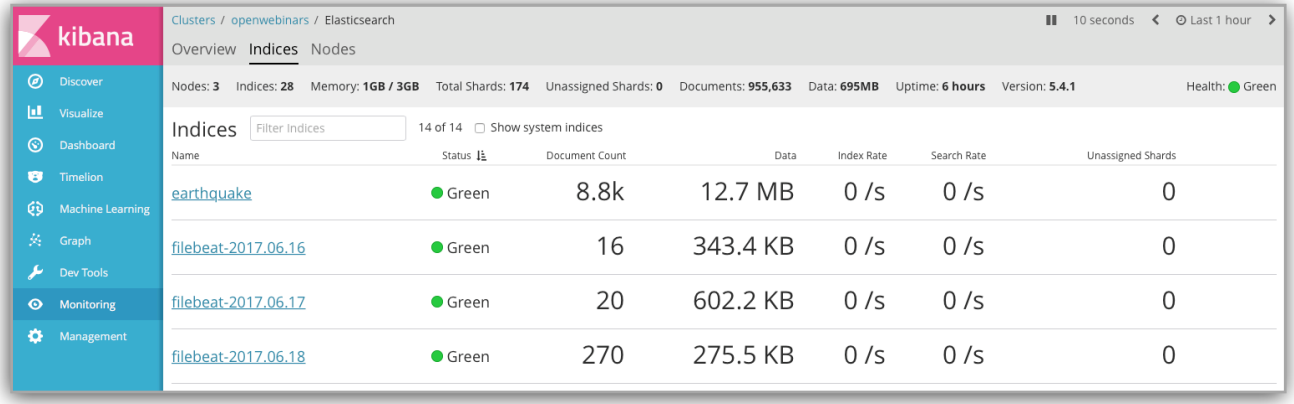
- Uso de Garbage Collector, JVM, memoria usada por Lucene, threats…



MÉTRICAS DE MONITORIZACIÓN

Elasticsearch: Índices

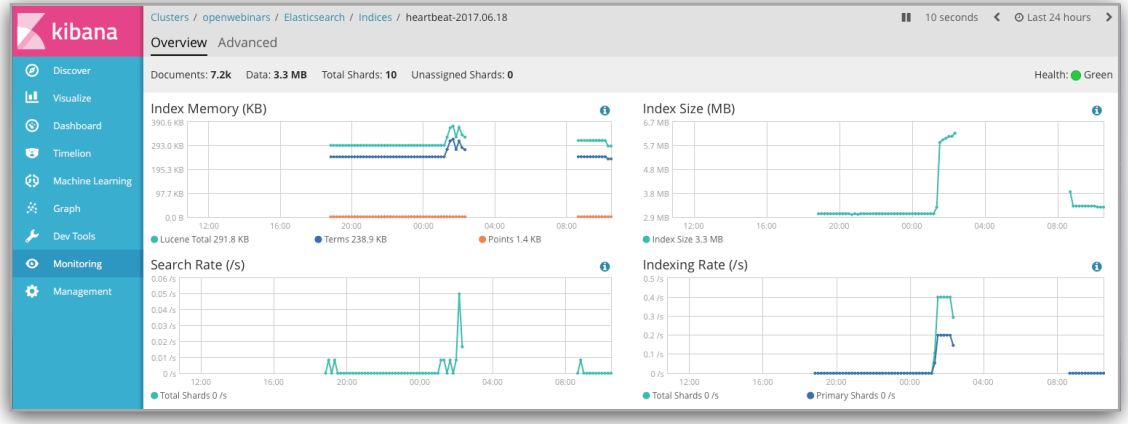
- Métricas de indexado y búsqueda, shards correctos y sin asignar…



MÉTRICAS DE MONITORIZACIÓN

Elasticsearch: Estadísticas de índices

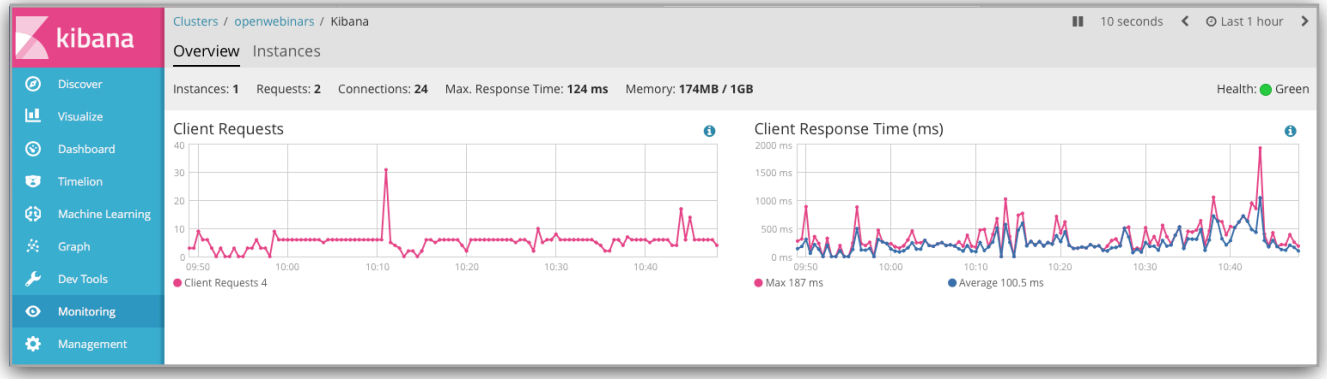
- Información más detallada de un índice, ratios, número de segmentos, números de documentos…



MÉTRICAS DE MONITORIZACIÓN

Kibana: Vista general

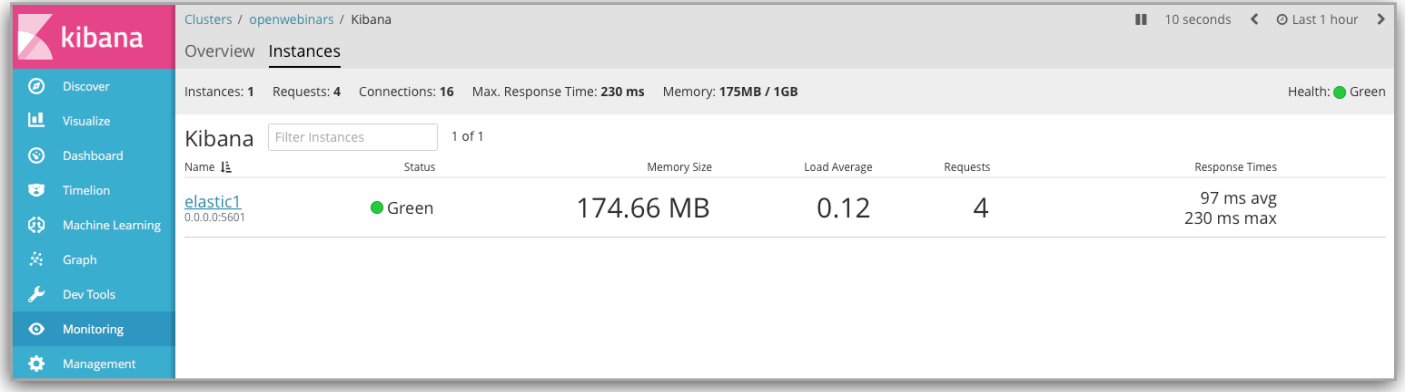
- Información más detallada de un índice, ratios, número de segmentos, números de documentos…



MÉTRICAS DE MONITORIZACIÓN

Kibana: Información de las instancias

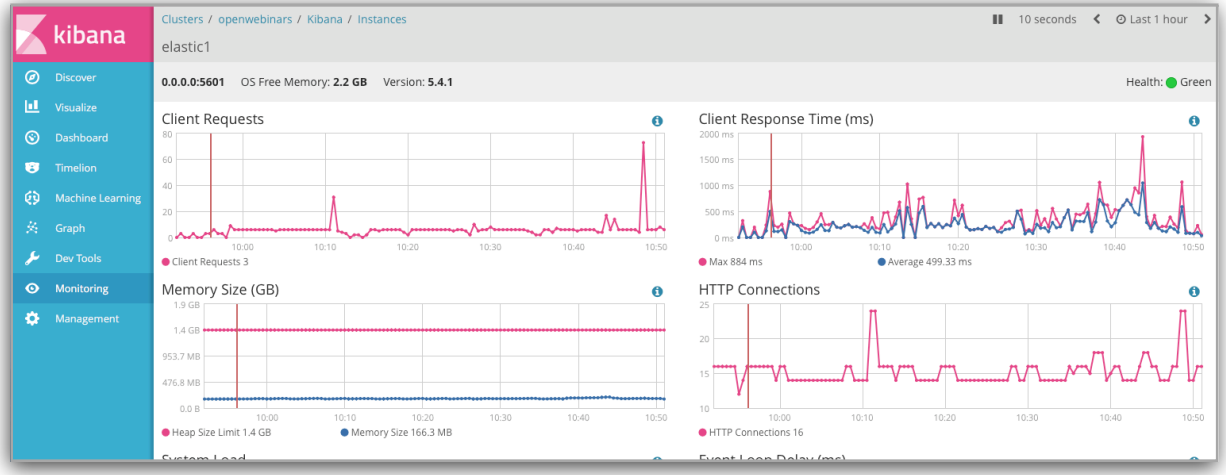
- Máquinas Kibana levantadas y resumen de recursos.



MÉTRICAS DE MONITORIZACIÓN

Kibana: Información detallada de la instancia

- Peticiones, tiempos de respuesta, conexiones HTTP…



MÉTRICAS DE MONITORIZACIÓN

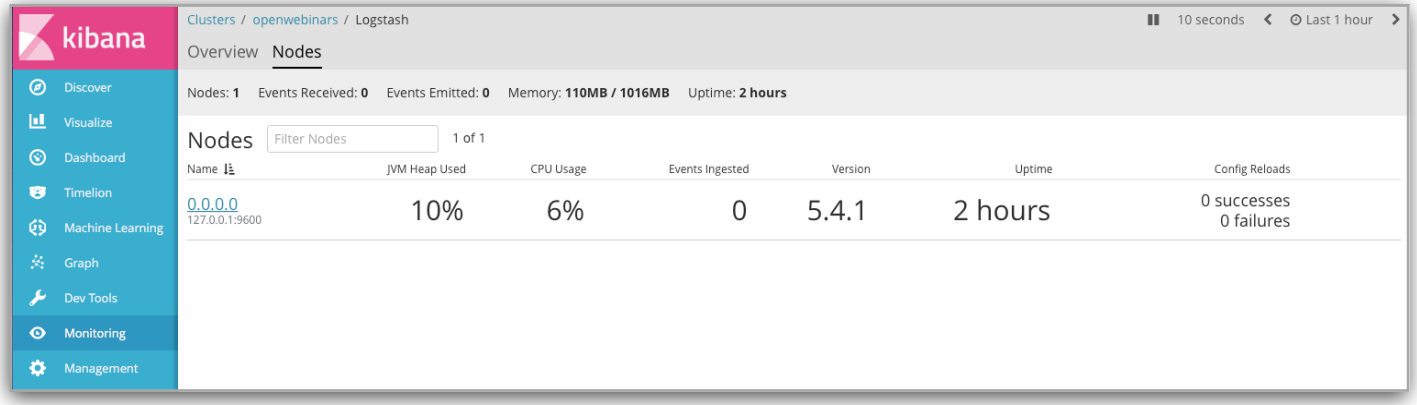
Logstash: Vista general

- Información más detallada de un índice, ratios, número de segmentos, números de documentos…

MÉTRICAS DE MONITORIZACIÓN

Logstash: Información de las instancias

- Máquinas Logstash levantadas y resumen de recursos.



MÉTRICAS DE MONITORIZACIÓN

Logstash: Información detallada de la instancia

- Eventos recibidos/emitidos, JVM, CPU, Load…