

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

The screenshot displays the Kibana Clusters monitoring interface. The left sidebar contains navigation links: Discover, Visualize, Dashboard, Timelion, Machine Learning, Graph, Dev Tools, Monitoring (selected), and Management. The main content area shows the 'openwebinars' cluster. A notification states: 'Your Trial license will expire on July 18, 2017.' Below this, 'Top Cluster Alerts' shows a warning: 'Elasticsearch cluster status is yellow. Allocate missing replica shards.' dated June 19, 2017 9:21:46 AM. A link 'View all alerts' is provided. The main section lists three components: Elasticsearch (Health: Yellow), Kibana (Health: Green), and Logstash. Each component has an 'Overview' section with various metrics.

Component	Health	Overview
Elasticsearch	Yellow	Overview Version: 5.4.1 Uptime: 5 hours Nodes: 2 Disk Available: 18GB / 32GB (54.31%) JVM Heap: 55.71% (1GB / 2GB) Indices: 28 Documents: 935,038 Disk Usage: 659MB Primary Shards: 82 Replica Shards: 82
Kibana	Green	Overview Requests: 10 Max. Response Time: 473 ms Instances: 1 Connections: 18 Memory Usage: 11.53% (165MB / 1GB)
Logstash		Overview Events Received: 0 Events Emitted: 0 Nodes: 1 Uptime: a minute JVM Heap: 12.67% (129MB / 1016MB)



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:
```

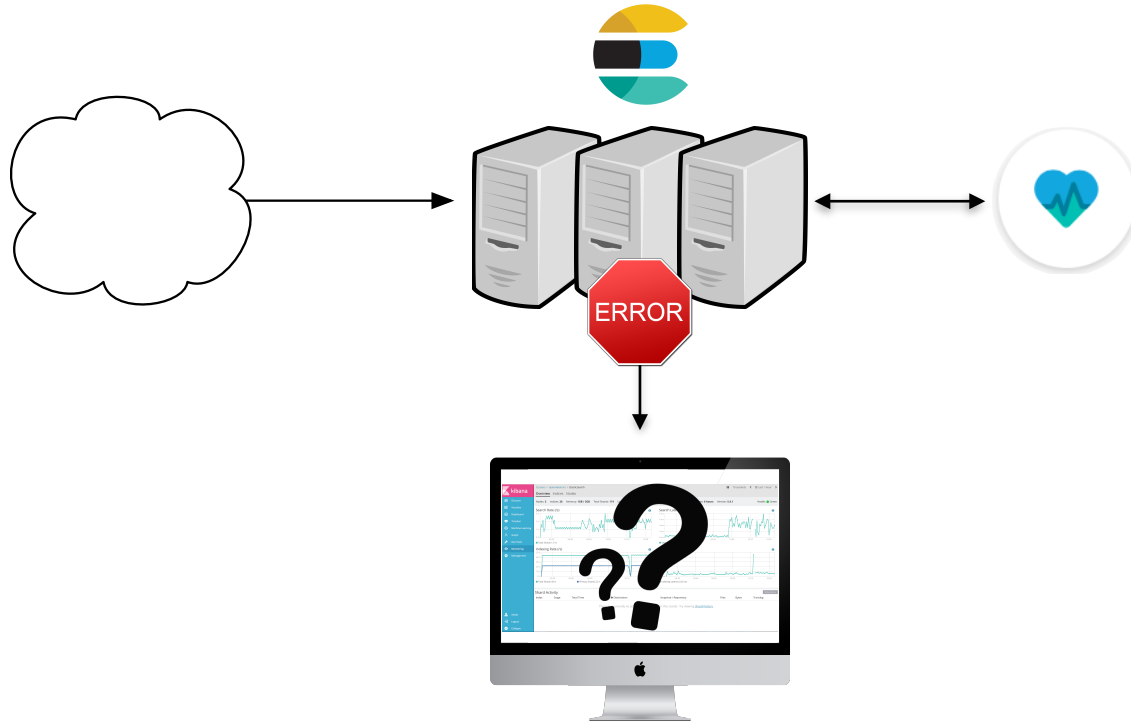
```
type: http
```

```
host: ["http://es-mon-1:9200", "http://es-mon2:9200"]
```

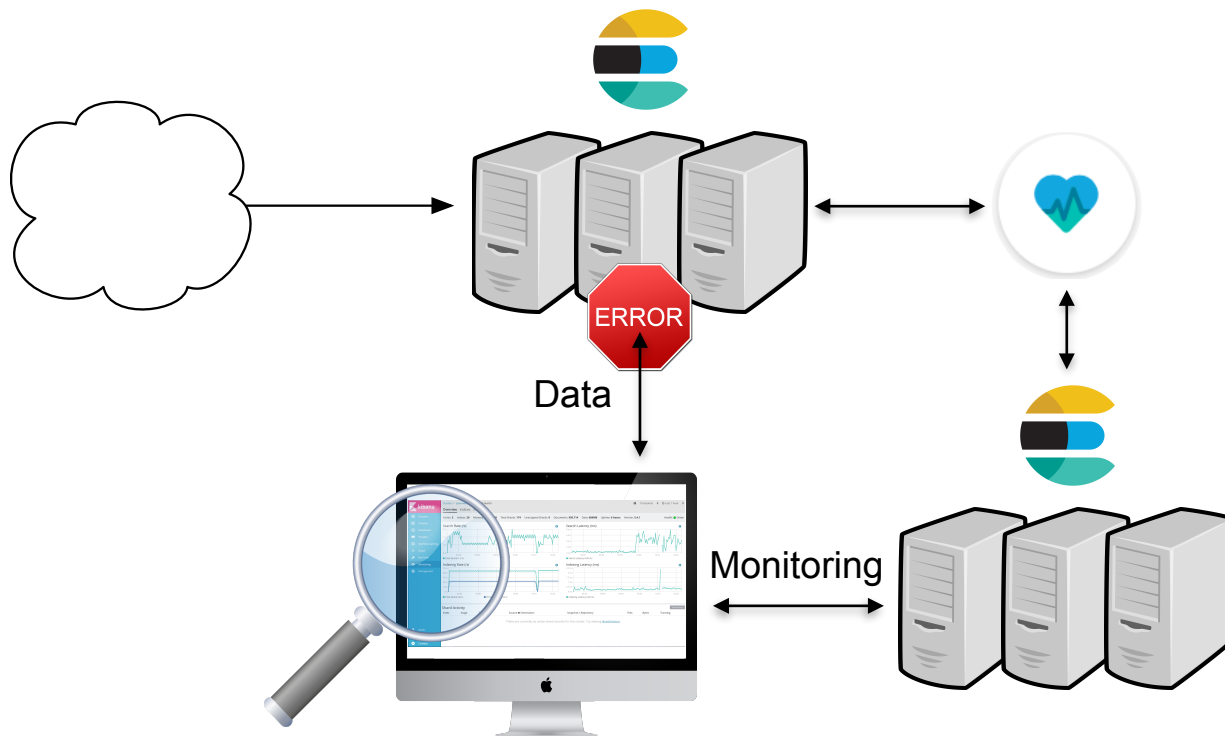
```
auth.username: remote_monitor
```

```
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.

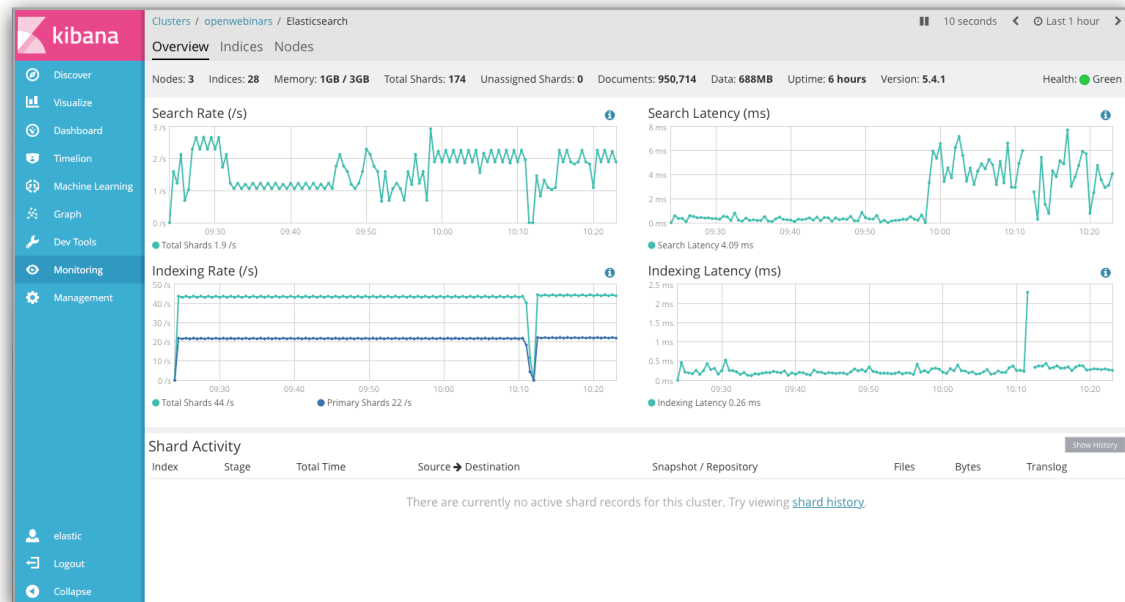
MÉTRICAS DE MONITORIZACIÓN

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.

Clusters / openwebinars / Elasticsearch

Overview Indices **Nodes**

Nodes: 3 Indices: 28 Memory: 1GB / 3GB Total Shards: 174 Unassigned Shards: 0 Documents: 951,769 Data: 690MB Uptime: 6 hours Version: 5.4.1 Health: ● Green

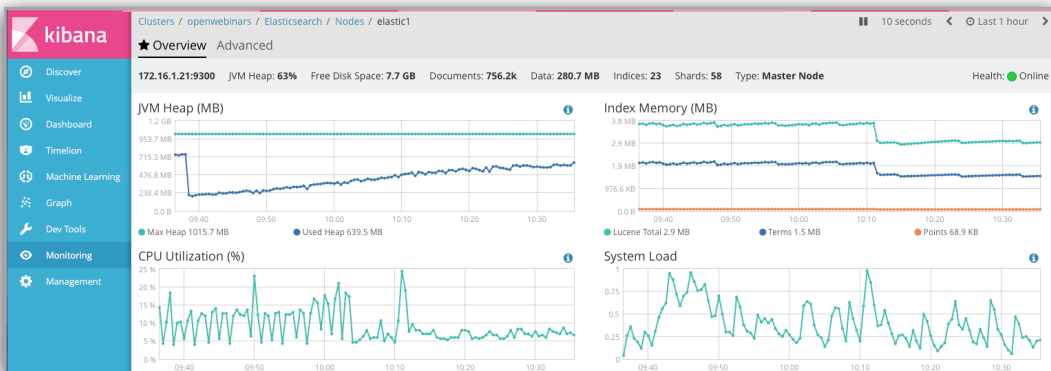
Nodes 3 of 3

Name	Status	CPU Usage	Load Average	JVM Memory	Disk Free Space	Shards
★ elastic1 172.16.1.21:9300	● Online	8.33 % ↓ 24.33 % max 4 % min	0.24 ↓ 0.98 max 0.04 min	57 % ↑ 75 % max 19 % min	7.7 GB ↑ 7.7 GB max 7.6 GB min	58
elastic2 172.16.1.22:9300	● Online	6.67 % ↓ 33 % max 2.33 % min	0.44 ↓ 0.44 max 0 min	40 % ↓ 75 % max 17 % min	9.8 GB ↑ 9.9 GB max 9.8 GB min	58
elastic3 172.16.1.23:9300	● Online	5 % ↑ 86.33 % max 0 % min	0.05 ↑ 3.23 max 0 min	15 % ↑ 17 % max 0 % min	9.9 GB ↑ 10.0 GB max 0.0 B min	58

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

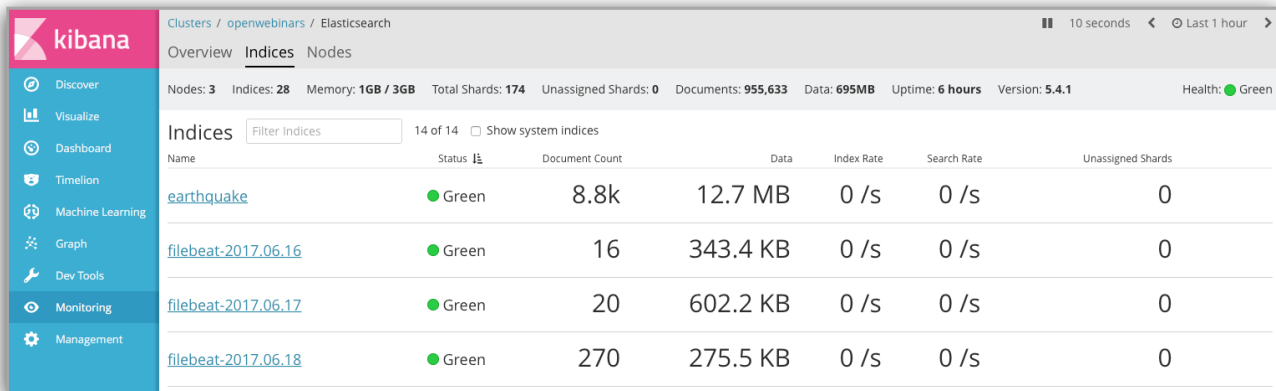
- Uso de Garbage Collector, JVM, memoria usada por Lucene, threats...



MÉTRICAS DE MONITORIZACIÓN

Elasticsearch: Índices

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



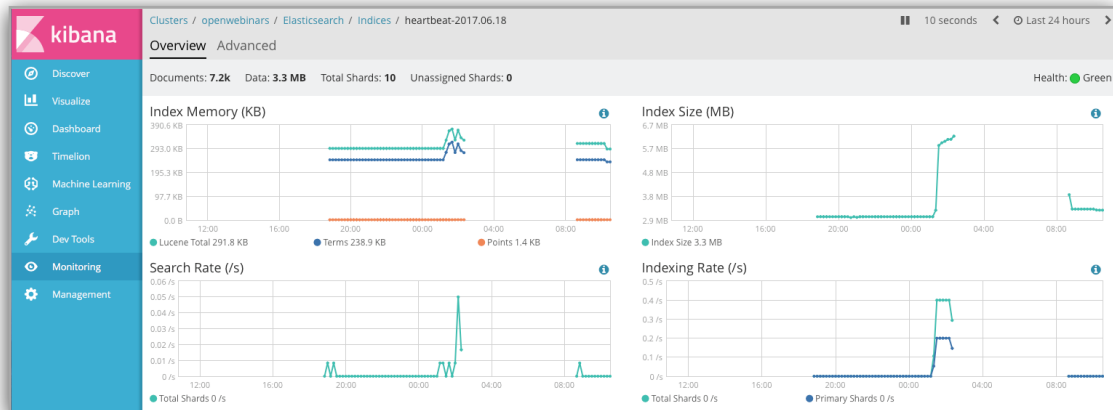
The screenshot shows the Kibana interface for monitoring Elasticsearch indices. The top navigation bar includes the Kibana logo and a sidebar with menu items: Discover, Visualize, Dashboard, Timeline, Machine Learning, Graph, Dev Tools, Monitoring (selected), and Management. The main content area displays the 'Indices' page for the 'openwebinars' cluster. It shows a summary of cluster health and metrics: 3 nodes, 28 indices, 1GB/3GB memory, 174 total shards, 0 unassigned shards, 955,633 documents, 695MB data, 6 hours uptime, and version 5.4.1. Below this, a table lists the first four indices: 'earthquake', 'filebeat-2017.06.16', 'filebeat-2017.06.17', and 'filebeat-2017.06.18'. Each row shows the index name, status (Green), document count, data size, index rate, search rate, and unassigned shards.

Name	Status	Document Count	Data	Index Rate	Search Rate	Unassigned Shards
earthquake	Green	8.8k	12.7 MB	0 /s	0 /s	0
filebeat-2017.06.16	Green	16	343.4 KB	0 /s	0 /s	0
filebeat-2017.06.17	Green	20	602.2 KB	0 /s	0 /s	0
filebeat-2017.06.18	Green	270	275.5 KB	0 /s	0 /s	0

MÉTRICAS DE MONITORIZACIÓN

Elasticsearch: Estadísticas de índices

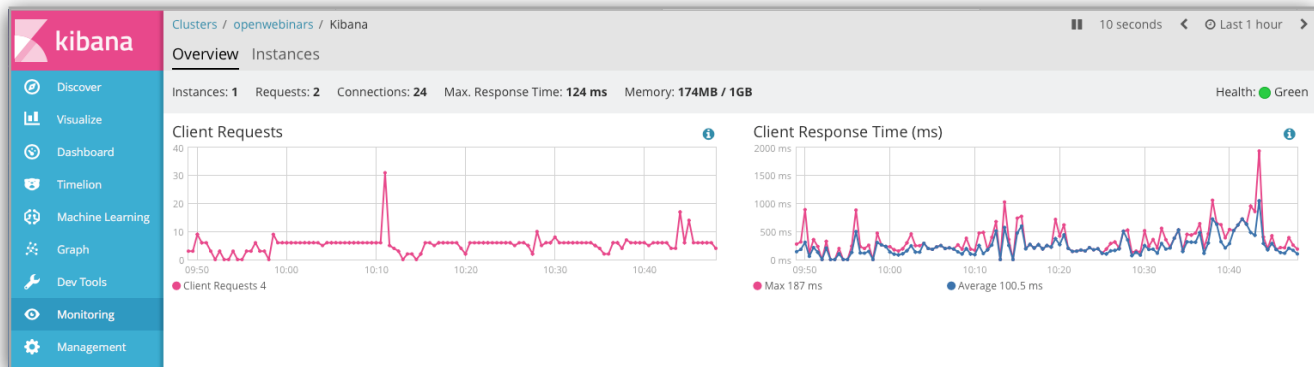
- Información más detallada de un índice, ratios, número de segmentos, números de documentos...



MÉTRICAS DE MONITORIZACIÓN

Kibana: Vista general

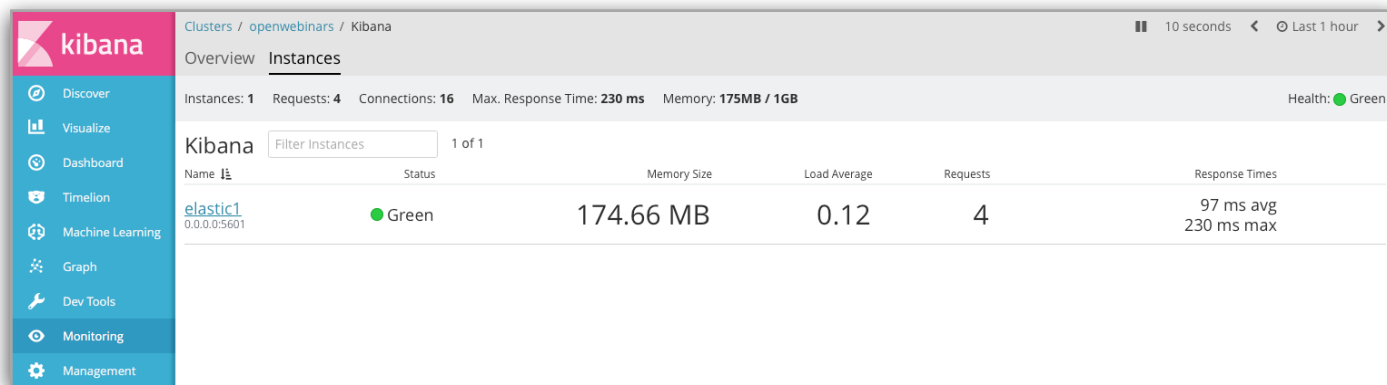
- Información más detallada de un índice, ratios, número de segmentos, números de documentos...



MÉTRICAS DE MONITORIZACIÓN

Kibana: Información de las instancias

- Máquinas Kibana levantadas y resumen de recursos.



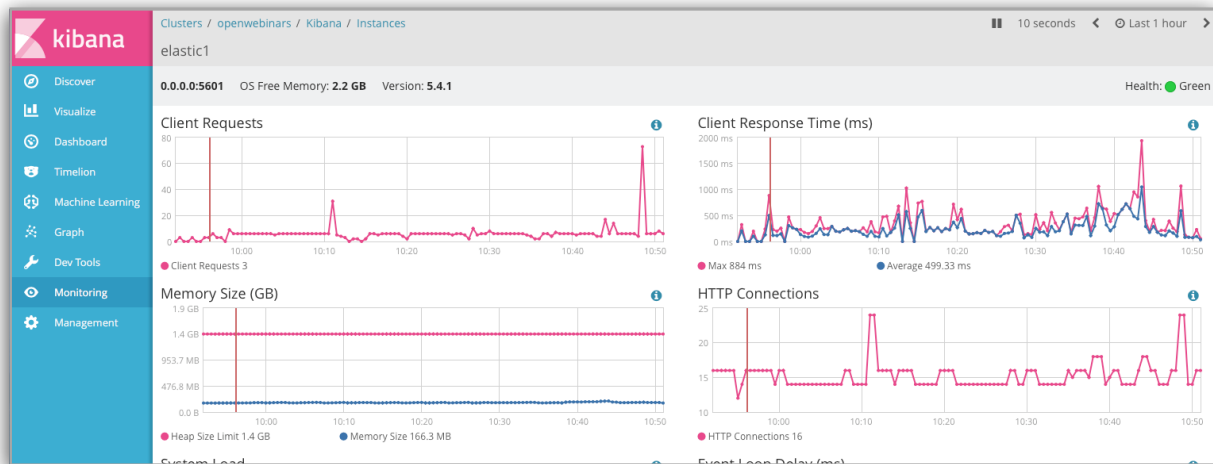
The screenshot displays the Kibana Monitoring interface. The left sidebar contains navigation links: Discover, Visualize, Dashboard, Timelion, Machine Learning, Graph, Dev Tools, Monitoring (selected), and Management. The main content area shows the 'Instances' tab for the 'Kibana' cluster. At the top, summary statistics are provided: 1 instance, 4 requests, 16 connections, a maximum response time of 230 ms, and 175 MB of memory usage. The health status is 'Green'. Below this, a table lists the instance details for 'elastic1' (version 0.0.0.0:5601).

Name	Status	Memory Size	Load Average	Requests	Response Times
elastic1 0.0.0.0:5601	Green	174.66 MB	0.12	4	97 ms avg 230 ms max

MÉTRICAS DE MONITORIZACIÓN

Kibana: Información detallada de la instancia

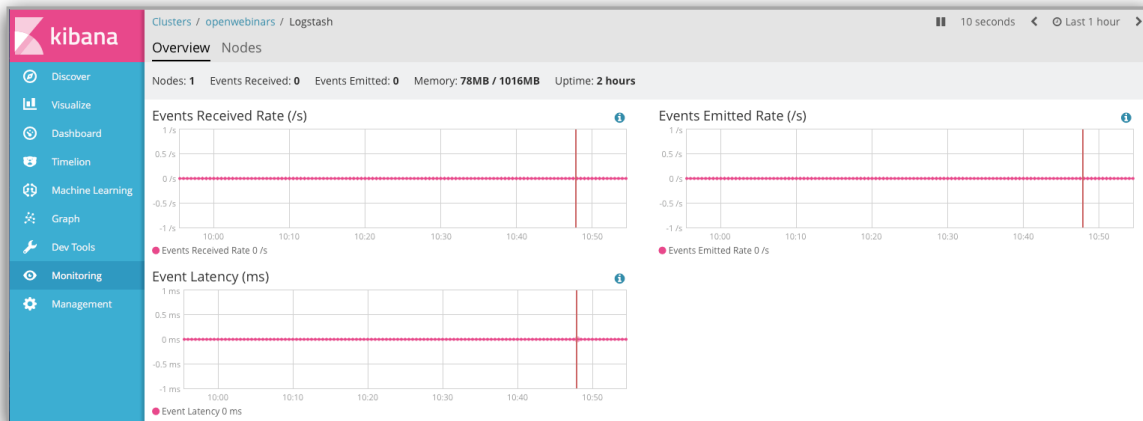
- Peticiones, tiempos de respuesta, conexiones HTTP...



MÉTRICAS DE MONITORIZACIÓN

Logstash: Vista general

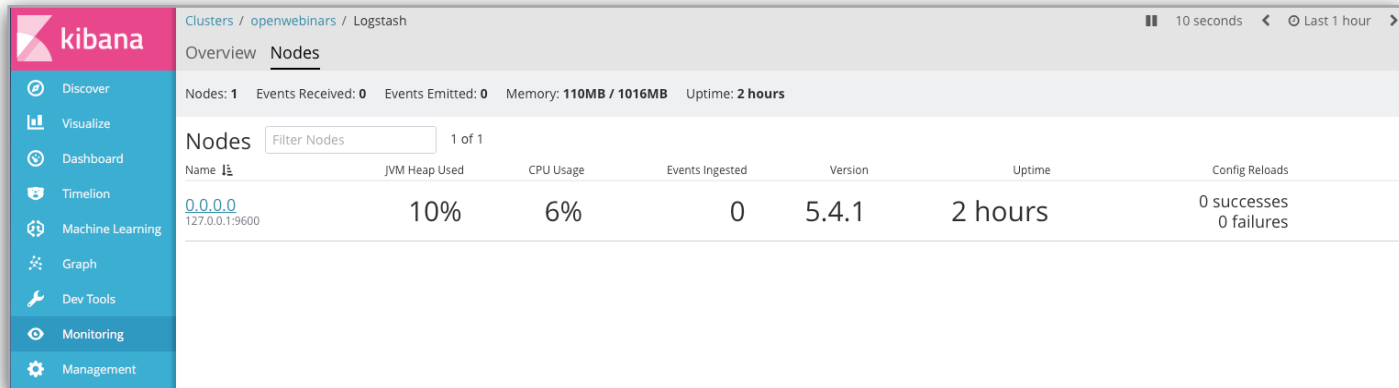
- Información más detallada de un índice, ratios, número de segmentos, números de documentos...



MÉTRICAS DE MONITORIZACIÓN

Logstash: Información de las instancias

- Máquinas Logstash levantadas y resumen de recursos.



The screenshot displays the Kibana interface for monitoring Logstash nodes. The left sidebar contains navigation links: Discover, Visualize, Dashboard, Timeline, Machine Learning, Graph, Dev Tools, Monitoring (selected), and Management. The main content area shows the 'Logstash' cluster overview with tabs for Overview and Nodes. The Nodes tab is active, displaying a table of node metrics. The table has columns for Name, JVM Heap Used, CPU Usage, Events Ingested, Version, Uptime, and Config Reloads. A single node is listed with the following details:

Name	JVM Heap Used	CPU Usage	Events Ingested	Version	Uptime	Config Reloads
0.0.0.0 127.0.0.1:9600	10%	6%	0	5.4.1	2 hours	0 successes 0 failures

MÉTRICAS DE MONITORIZACIÓN

Logstash: Información detallada de la instancia

- Eventos recibidos/emitados, JVM, CPU, Load...

