



Primeros pasos con Logstash y Beats

Enrique V. Kortright

10 de febrero de 2021

<https://github.com/evkortright/primeros-pasos-con-logstash-y-beats>

Meetup del grupo de usuarios de Elastic (EUG) de Costa Rica

Conéctese con la comunidad de Elastic

Existen User Groups en Costa Rica,
Mexico, Colombia, Argentina y Uruguay -
encuentra el tuyo:



<https://community.elastic.co/>

User Group Virtual:

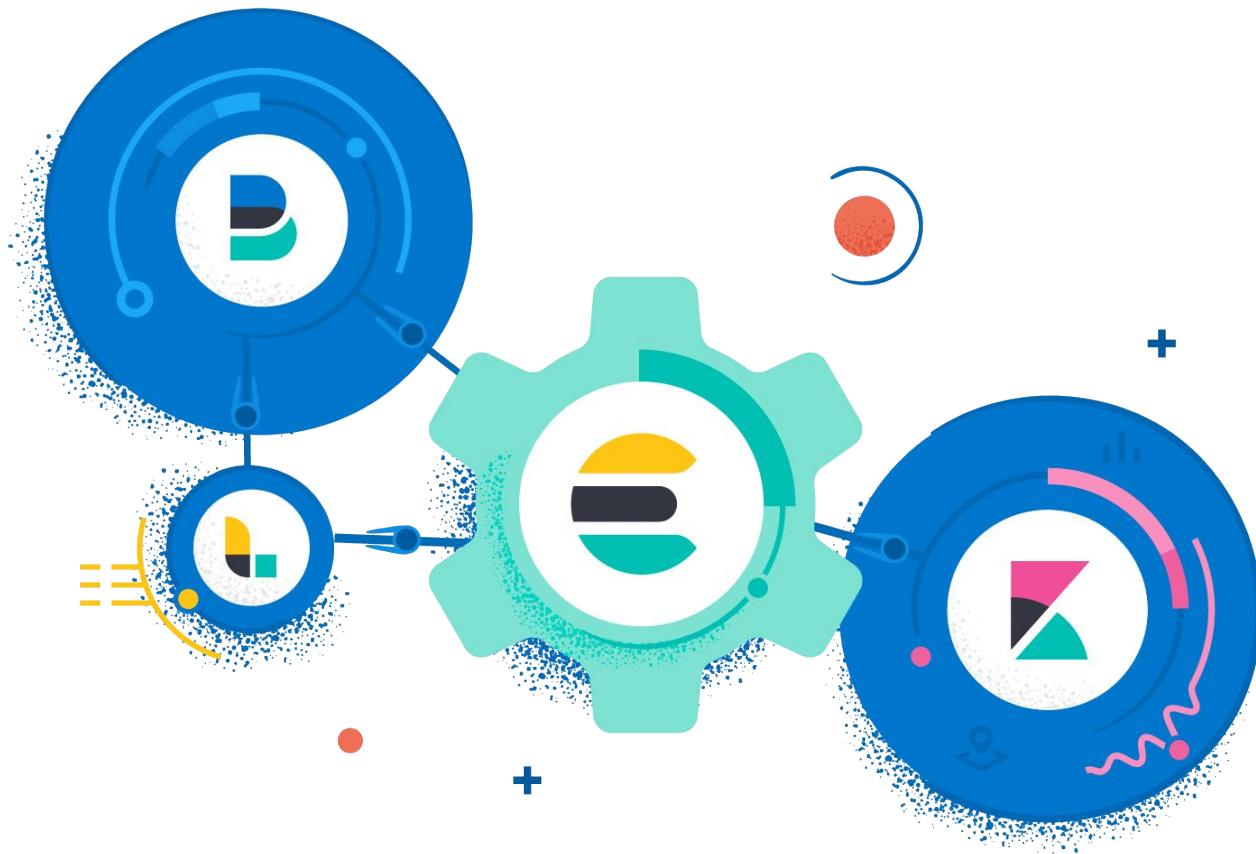


<https://community.elastic.co/amèr-virtual/>

Agenda

- Repaso del Elastic Stack
- Logstash
- Beats
 - Heartbeat, Filebeat, Metricbeat, el servidor APM y sus agents
- Ejercicio con Beats, Logstash y Elasticsearch
- Arquitectura genérica y específica para caso de uso
- Preguntas y respuestas
- Recursos y el camino a seguir

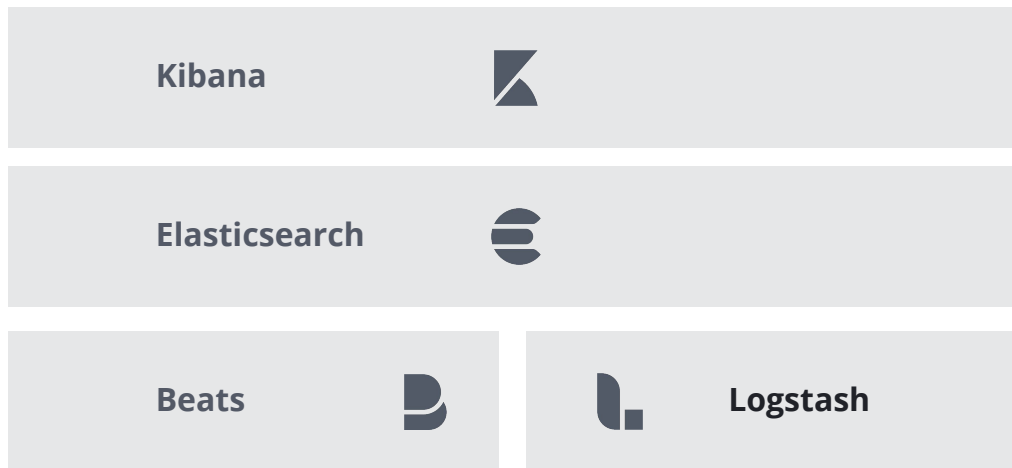
Elasticsearch es parte del Elastic Stack



El Stack de Elastic

Casos de uso

Logging	Metrics	APM	Uptime	Security Analytics	FUTURE
App Search	Site Search	Enterprise Search	Maps	Business Analytics	




Visualiza, analiza,
administra y
alerta

Guarda, busca y
procesa

Captura, enriquece,
transforma y carga

SaaS

Elastic Stack

- Elasticsearch
 - es un almacén de documentos de JSON
 - es una máquina de búsqueda de alto rendimiento
 - Maneja y procesa los datos a través de una serie de APIs de REST 
- Kibana
 - es la interfaz de usuario (UI)
 - proporciona operaciones de administración y monitoreo de un cluster de Elasticsearch
 - proporciona funciones de visualización en tiempo casi-real
 - proporciona UIs para trabajos de aprendizaje de máquina
 - proporciona UIs especializadas para áreas que incluyen observabilidad, seguridad, aprendizaje de máquina, visualización de datos geoespaciales, infográficos usando Canvas, grafos de relaciones entre objetos y otras más
- Logstash
 - es la herramienta de transformación, enriquecimiento y carga de datos
 - puede jalar y empujar datos almacenados en fuentes muy diversas como bases de datos
- Beats
 - son agentes ligeros (generalmente) desplegados en el punto de origen de datos
 - se encargan de capturar logs, métricas o trazas y enviarlos a Elasticsearch directamente o a través de Logstash

- API conventions
- cat APIs
- Cluster APIs
- Cross-cluster replication APIs
- Data stream APIs
- Document APIs
- Enrich APIs
- Graph Explore API
- Index APIs
- Index lifecycle management APIs
- Ingest APIs
- Info API
- Licensing APIs
- Machine learning anomaly detection APIs
- Machine learning data frame analytics APIs
- Migration APIs
- Reload Search Analyzers API
- Repositories Metering APIs
- Rollup APIs
- Search APIs
- Searchable snapshots APIs
- Security APIs
- Snapshot and restore APIs
- Snapshot lifecycle management APIs
- Transform APIs
- Usage API
- Watcher APIs

Plan de esta serie de primeros pasos

- En el primer episodio nos enfocamos en **Elasticsearch**
 - Creación, lectura, actualización, y borrado de datos (CRUD) individualmente o a granel
 - El lenguaje de dominio específico (DSL) de Elasticsearch
 - El lenguaje de búsqueda para hacer consultas
 - Diseño de una gran experiencia de búsqueda
- En este segundo episodio exploramos **Kibana**
- En este tercer episodio nos enfocamos en **Logstash y Beats**

Beats y Logstash



Y ahora... **LOS BEATS**



Filebeat

Archivos de log



Metricbeat

Métricas



Packetbeat

Datos de red



Winlogbeat

Logs de eventos de Windows



Auditbeat

Información de auditoría

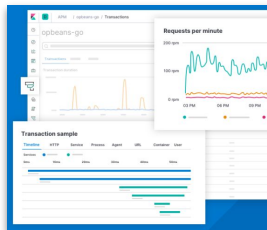


Functionbeat

Agente sin servidor



APM + agentes

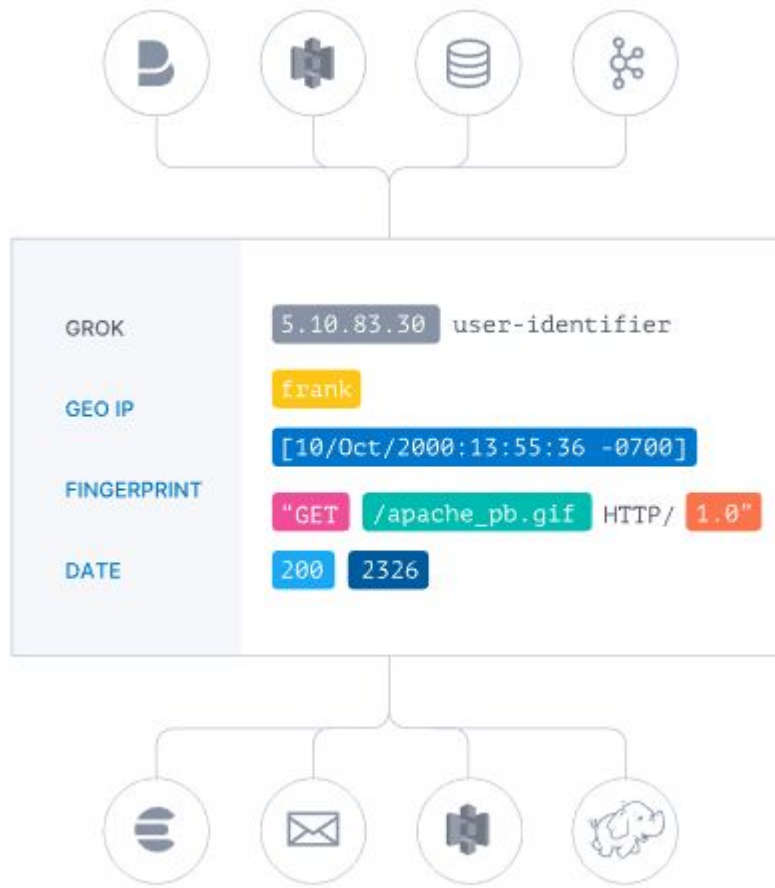


Logstash


INGESTA Y MÁS

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.



Ejercicio on Filebeat, Logstash y Elasticsearch

The slide features a dark blue background with several abstract geometric elements. In the top right, there is a yellow square. Below it, a large teal circle is partially cut off by the right edge, with a smaller blue square overlapping its top right. Three vertical white lines of varying lengths extend downwards from the circle. To the left of the circle, there are three small white dots. In the bottom right, there is a teal rectangle, a blue square, and a white square outline.

Instala Filebeat

- Crea un folder `filebeat`
- Baja y descomprime Filebeat para tu OS en tu nuevo folder

```
wget https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-7.10.2-darwin-x86_64.tar.gz
tar xvf filebeat-7.10.2-darwin-x86_64.tar.gz
mv filebeat-7.10.2-darwin-x86_64 filebeat
cd filebeat
mkdir logs
cd logs
```

- Baja y descomprime los logs de demostración

```
wget https://download.elastic.co/demos/logstash/gettingstarted/logstash-tutorial.log.gz
gunzip logstash-tutorial.log.gz
cd ..
```

Filebeat => consola

- Crea la siguiente configuración `filebeat_1.yml`

```
filebeat.inputs:  
- type: log  
  paths:  
    -  
    logs/logstash-tutorial.log  
  
output.console:  
  pretty: true
```

- Verifica la configuración
`./filebeat test config -c filebeat_1.yml`
- Corre Filebeat con esta configuración
`./filebeat -c filebeat_1.yml`
- Filebeat simplemente lee cada línea del archivo de logs, la convierte a *JSON*, añade información del sistema y los envía a la consola
- Borra el *registry* de Filebeat para poder usar los logs otra vez
`rm -r data/registry/`

Filebeat => console a través del modulo de apache

- Use ^C para detener Filebeat. Crea la configuración `filebeat_2.yml` y verifícala

```
filebeat.config.modules:  
  path: ${path.config}/modules.d/*.yaml  
  reload.enabled: false  
  
output.console:  
  pretty: true
```

- Habilita el módulo de apache
`./filebeat modules enable apache -c filebeat_2.yml`
- Configura el module de apache `modules.d/apache.yml`

```
- module: apache  
  access:  
    enabled: true  
    var.paths: ["logs/logstash-tutorial.log"]  
  
  error:  
    enabled: false
```

- Corre filebeat -- ahora Filebeat lee los logs a través del módulo de apache

Filebeat => Logstash

- Dirige la salida a Logstash con la configuración `filebeat_3.yml`

```
filebeat.config.modules:  
  path: ${path.config}/modules.d/*.yaml  
  reload.enabled: false  
  
output.logstash:  
  hosts: ["localhost:5044"]
```

- No podemos correr Filebeat todavía porque no hemos creado un nodo de Logstash

Instala y configura Logstash

- Crea un folder `logstash`
- Baja y descomprime Logstash para tu OS en tu nuevo folder

```
wget https://artifacts.elastic.co/downloads/logstash/logstash-7.10.2-darwin-x86_64.tar.gz
tar xvf logstash-7.10.2-darwin-x86_64.tar.gz
mv logstash-7.10.2 logstash
cd logstash
```


Filebeat => Logstash => consola

- Crea la siguiente configuración `pipeline_1.conf`

```
input {
  beats {
    port => "5044"
  }
}

output {
  stdout { }
}
```

- Corre Logstash con esta configuración

```
./bin/logstash -f pipeline_1.conf
```

- Verifica, prueba y corre Filebeat con la configuración `filebeat_3.yml`

```
./filebeat test config -c filebeat_3.yml
```

```
./filebeat test output -c filebeat_3.yml
```

```
rm -r data/registry/
```

```
./filebeat -c filebeat_3.yml
```

Filebeat => Logstash (=> grok => geoip) => consola

- Crea una la configuración `pipeline_2.conf` añadiendo filtros a la tubería de Logstash para parsear el mensaje de cada log y procesar el IP presente en el campo `clientip`

```
input {
  beats {
    port => "5044"
  }
}

filter {
  grok {
    match => { "message" => "%{COMBINEDAPACHELOG}" }
  }
  geoip {
    source => "clientip"
  }
}

output {
  stdout { }
}
```

- Corre Logstash con esta configuración -- corre Filebeat de nuevo

Filebeat => Logstash => Elasticsearch

- Crea la configuración `pipeline_3.conf` que dirige la salida a un cluster de Elasticsearch
- Corre Logstash con esta configuración
- Corre Filebeat de nuevo

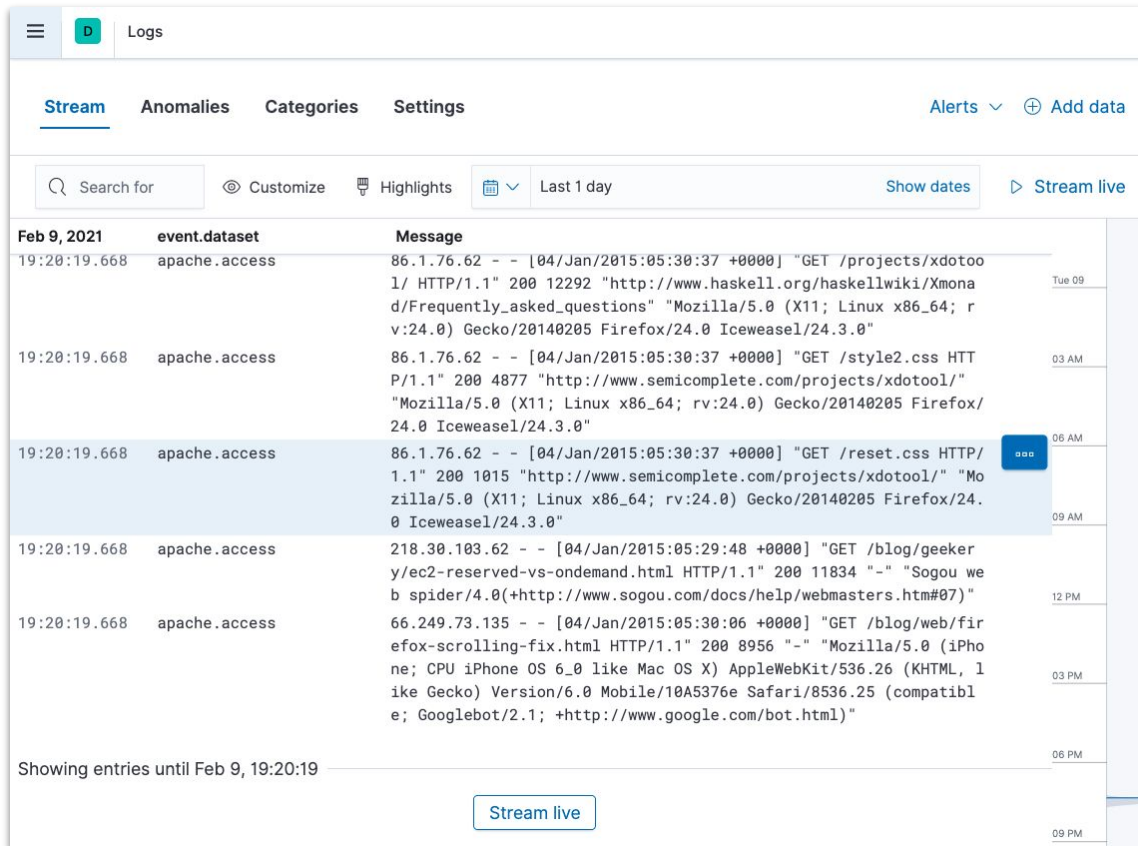
```
input {
  beats {
    port => "5044"
  }
}

filter {
  grok {
    match => { "message" => "%{COMBINEDAPACHELOG}" }
  }
  geoip {
    source => "clientip"
  }
}

output {
  elasticsearch {
    hosts => [ "localhost:9200" ]
    index => "%{[@metadata][beat]}-%{[@metadata][version]}"
    user => "elastic"
    password => "changeme"
    ecs_compatibility => disabled
  }
}
```

Explora logs con el ap Logs de Kibana

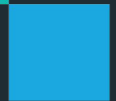
- En Kibana abre el ap de Logs y explora los datos enviados por Filebeat a través de Logstash
- En este ap podemos ver logs llegar a Elasticsearch en tiempo real
- Podemos también crear alertas



The screenshot displays the Kibana Logs application interface. At the top, there's a navigation bar with a menu icon, a 'D' icon, and the word 'Logs'. Below this is a sub-navigation bar with tabs for 'Stream' (selected), 'Anomalies', 'Categories', and 'Settings'. On the right of this bar are links for 'Alerts' and 'Add data'. A search bar with the placeholder 'Search for' is on the left, followed by 'Customize', 'Highlights', and a time range selector set to 'Last 1 day'. A 'Show dates' link and a 'Stream live' button are on the right. The main area shows a table of log entries. The table has three columns: 'Time' (e.g., Feb 9, 2021), 'event.dataset' (e.g., apache.access), and 'Message' (HTTP log details). The entries are sorted by time, with the most recent at the top. A vertical scrollbar is on the right. At the bottom, it says 'Showing entries until Feb 9, 19:20:19' and has a 'Stream live' button.

Time	event.dataset	Message
Feb 9, 2021	apache.access	86.1.76.62 - - [04/Jan/2015:05:30:37 +0000] "GET /projects/xdotoo1/ HTTP/1.1" 200 12292 "http://www.haskell.org/haskellwiki/Xmonad/Frequently_asked_questions" "Mozilla/5.0 (X11; Linux x86_64; rv:24.0) Gecko/20140205 Firefox/24.0 Iceweasel/24.3.0"
19:20:19.668	apache.access	86.1.76.62 - - [04/Jan/2015:05:30:37 +0000] "GET /style2.css HTTP/1.1" 200 4877 "http://www.semicomplete.com/projects/xdotoo1/" "Mozilla/5.0 (X11; Linux x86_64; rv:24.0) Gecko/20140205 Firefox/24.0 Iceweasel/24.3.0"
19:20:19.668	apache.access	86.1.76.62 - - [04/Jan/2015:05:30:37 +0000] "GET /reset.css HTTP/1.1" 200 1015 "http://www.semicomplete.com/projects/xdotoo1/" "Mozilla/5.0 (X11; Linux x86_64; rv:24.0) Gecko/20140205 Firefox/24.0 Iceweasel/24.3.0"
19:20:19.668	apache.access	218.30.103.62 - - [04/Jan/2015:05:29:48 +0000] "GET /blog/geekery/ec2-reserved-vs-ondemand.html HTTP/1.1" 200 11834 "-" "Sogou web spider/4.0(+http://www.sogou.com/docs/help/webmasters.htm#07)"
19:20:19.668	apache.access	66.249.73.135 - - [04/Jan/2015:05:30:06 +0000] "GET /blog/web/firefox-scrolling-fix.html HTTP/1.1" 200 8956 "-" "Mozilla/5.0 (iPhone; CPU iPhone OS 6_0 like Mac OS X) AppleWebKit/536.26 (KHTML, like Gecko) Version/6.0 Mobile/10A5376e Safari/8536.25 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"

Demostración: Jalando datos de mysql usando Logstash



Jalando datos con Logstash

- Además de recibir datos, Logstash puede jalar datos de una gran variedad de fuentes, incluyendo bases de datos como mysql y muchas otras fuentes

Input plugins

An input plugin enables a specific source of events to be read by Logstash.

The following input plugins are available below. For a list of Elastic supported plugins, please consult the [Support Matrix](#).

Plugin	Description	Github repository
azure_event_hubs	Receives events from Azure Event Hubs	azure_event_hubs
beats	Receives events from the Elastic Beats framework	logstash-input-beats
cloudwatch	Pulls events from the Amazon Web Services CloudWatch API	logstash-input-cloudwatch
couchdb_changes	Streams events from CouchDB's _changes URI	logstash-input-couchdb_changes
dead_letter_queue	read events from Logstash's dead letter queue	logstash-input-dead_letter_queue
elasticsearch	Reads query results from an Elasticsearch cluster	logstash-input-elasticsearch
exec	Captures the output of a shell command as an event	logstash-input-exec
file	Streams events from files	logstash-input-file
ganglia	Reads Ganglia packets over UDP	logstash-input-ganglia
gelf	Reads GELF-format messages from Graylog2 as events	logstash-input-gelf
generator	Generates random log events for test purposes	logstash-input-generator
github	Reads events from a GitHub webhook	logstash-input-github

mysql => Logstash => Elasticsearch

- La siguiente configuración lee datos cada minuto de la tabla amigos de la base de datos db_example

```
input {
  jdbc {
    jdbc_driver_library => "/mysql-connector-java-5.1.36-bin.jar"
    jdbc_driver_class => "com.mysql.jdbc.Driver"
    jdbc_connection_string => "jdbc:mysql://localhost:3306/db_example"
    jdbc_user => "springuser"
    jdbc_password => "ThePassword"
    schedule => "* * * * *"
    statement => "SELECT * from amigos where fecha > :sql_last_value"
  }
}

output {
  stdout { codec => "dots" }
  elasticsearch {
    hosts => [ "localhost:9200" ]
    index => "amigos"
    user => "elastic"
    password => "changeme"
    ecs_compatibility => disabled
  }
}
```

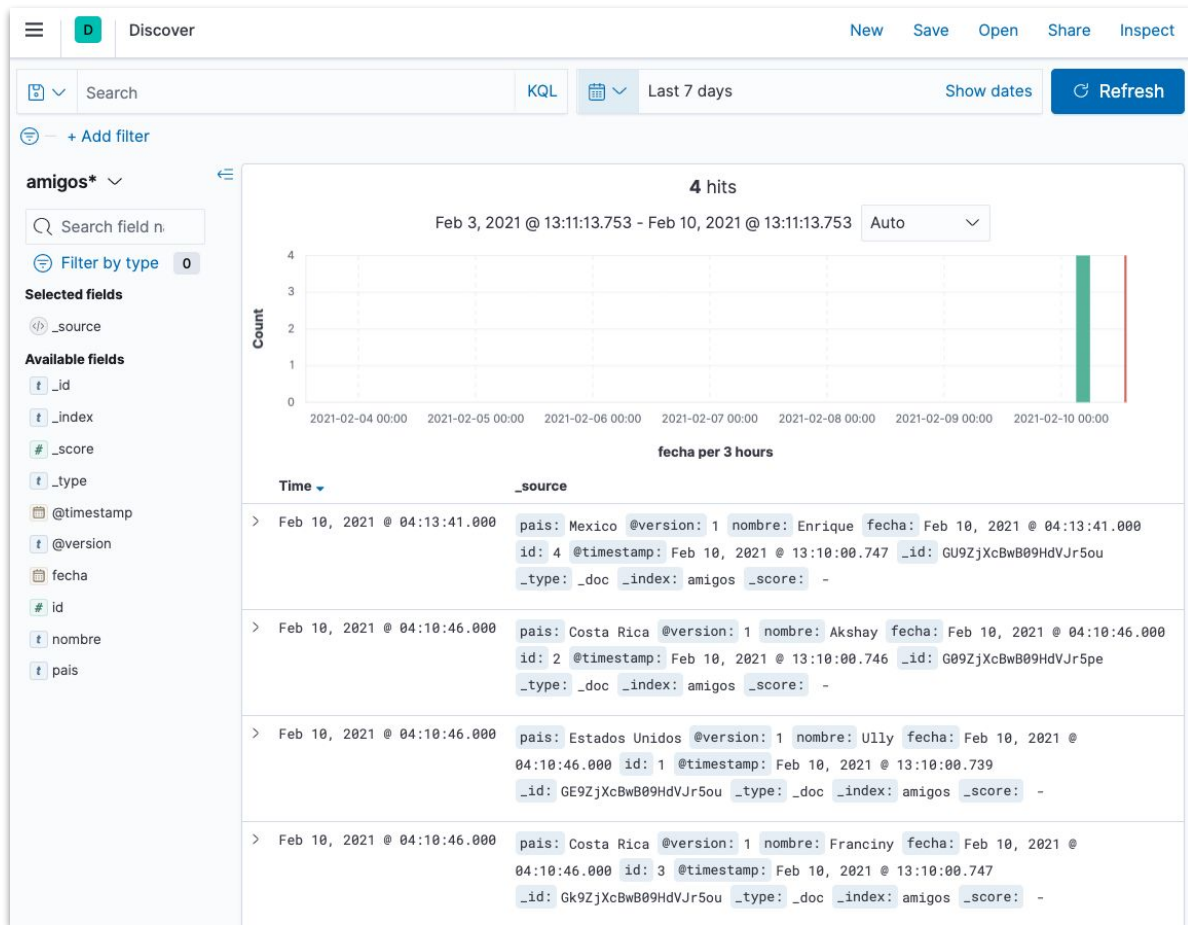
```
DROP TABLE IF EXISTS `amigos`;
CREATE TABLE `amigos` (
  `id` BIGINT(20) UNSIGNED NOT NULL AUTO_INCREMENT,
  `nombre` VARCHAR(32) NOT NULL,
  `pais` VARCHAR(500) NOT NULL,
  `fecha` TIMESTAMP NOT NULL DEFAULT CURRENT_TIMESTAMP,
  PRIMARY KEY (`id`)
) ENGINE=INNODB AUTO_INCREMENT=1 DEFAULT CHARSET=utf8;

INSERT INTO amigos (nombre, pais) VALUES ('Uly', 'Estados Unidos');
INSERT INTO amigos (nombre, pais) VALUES ('Akshay', 'Costa Rica');
INSERT INTO amigos (nombre, pais) VALUES ('Franciny', 'Costa Rica');
INSERT INTO amigos (nombre, pais) VALUES ('Enrique', 'Mexico');
```

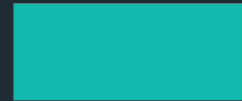
- Inicializa el punto de ultima consulta de jdbc y corre Logstash

```
rm ~/.logstash_jdbc_last_run
./bin/logstash -f pipeline_mysql_1.conf
```

Explora tus amigos con Discover en Kibana



Demostración: Monitoreo basico con Heartbeat



Monitoreo basico con Heartbeat

- Heartbeat usa pings de protocolos *icmp*, *tcp* y *http* para monitorear las componentes y microservicios de un sistema
- Usa la configuración `heartbeat_1.yml` para monitorear **elasticsearch**, **kibana**, **logstash**, y **mysql**

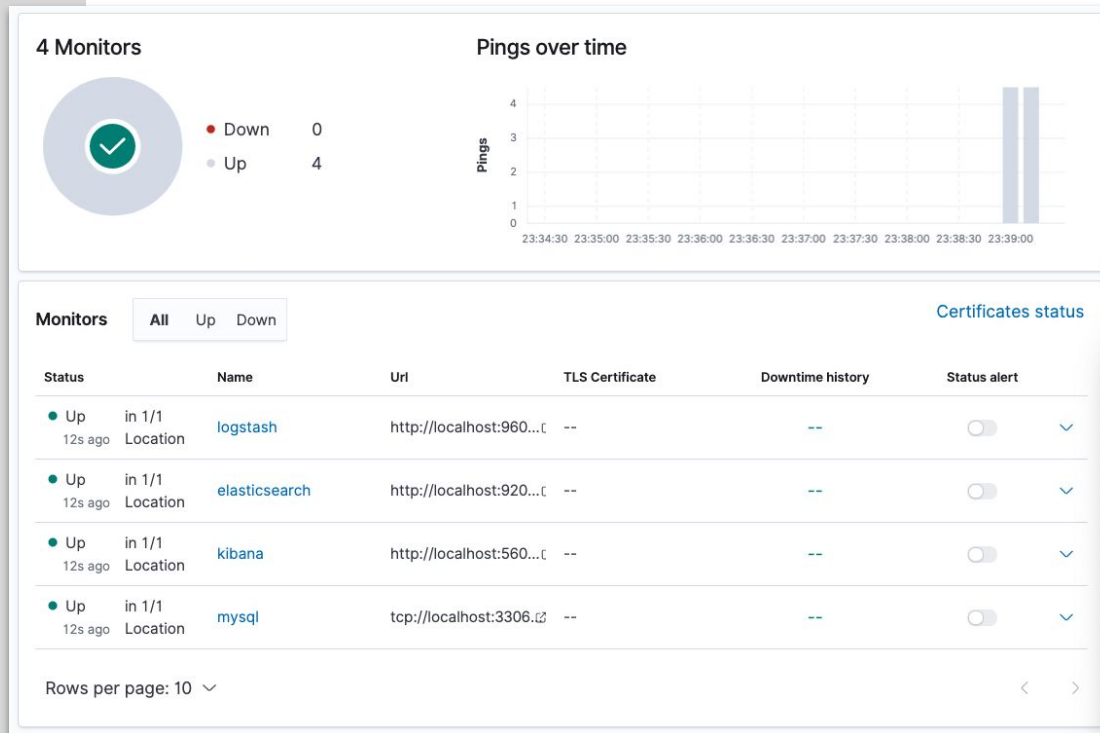
```
heartbeat.monitors:  
- type: http  
  name: elasticsearch  
  enabled: true  
  schedule: '@every 10s'  
  urls: ["http://localhost:9200"]  
  ipv4: true  
  ipv6: true  
  mode: any  
  timeout: 5s  
  username: "elastic"  
  password: "changeme"  
  check.request:  
    method: "GET"  
  check.response:  
    status: 200
```

```
- type: http  
  name: kibana  
  enabled: true  
  schedule: '@every 10s'  
  urls: ["localhost:5601"]  
  ipv4: true  
  ipv6: true  
  mode: any  
  timeout: 5s
```

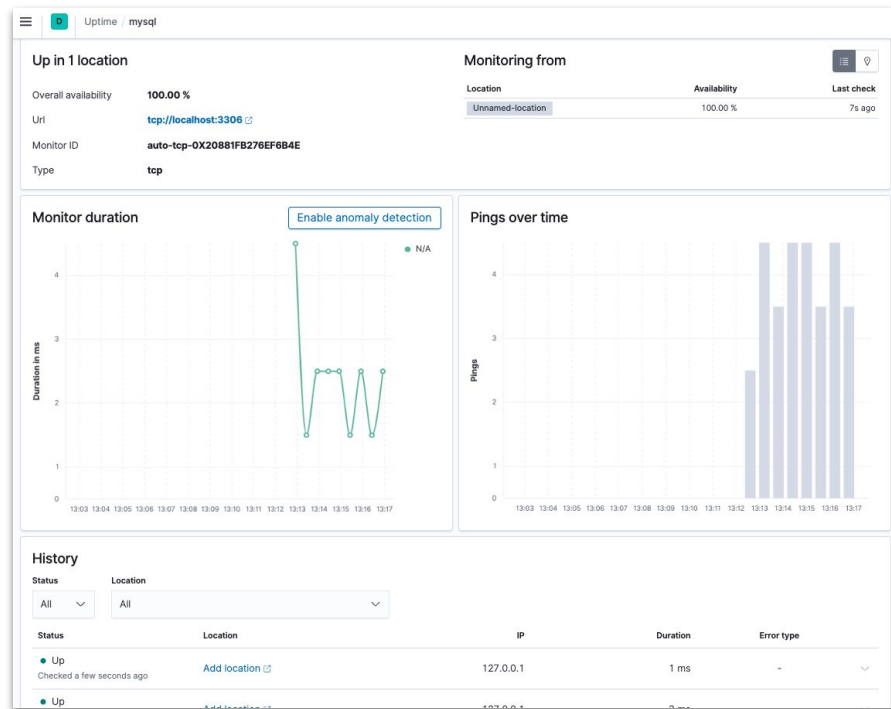
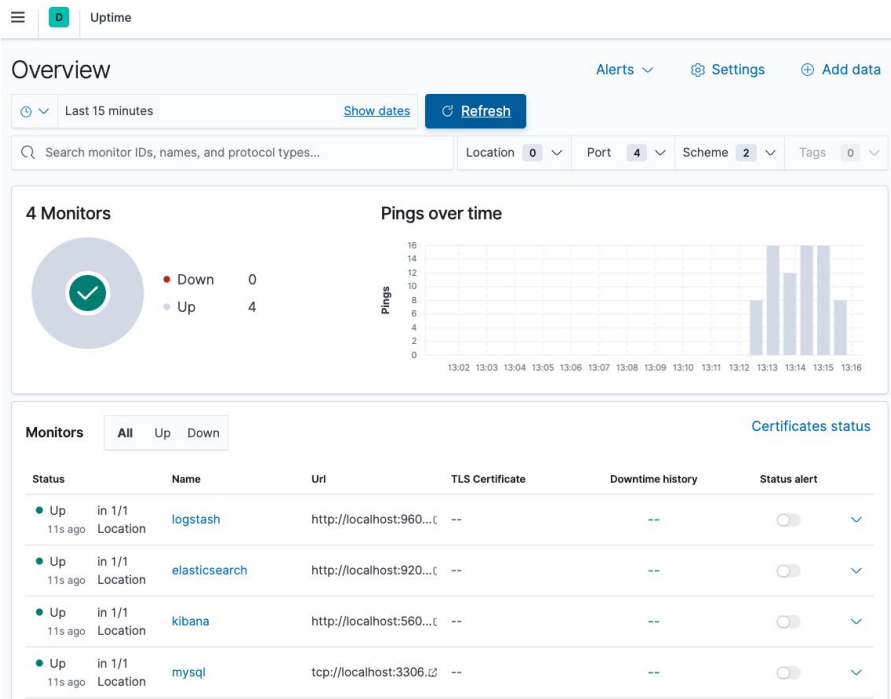
```
- type: http  
  name: logstash  
  enabled: true  
  schedule: '@every 10s'  
  urls: ["http://localhost:9600"]  
  ipv4: true  
  ipv6: true  
  mode: any  
  timeout: 5s  
  check.request:  
    method: "GET"  
  check.response:  
    status: 200
```

```
- type: tcp  
  name: mysql  
  enabled: true  
  schedule: '@every 10s'  
  hosts: ["tcp://localhost:3306"]
```

```
output.elasticsearch:  
  hosts: ["http://localhost:9200"]  
  username: "elastic"  
  password: "changeme"  
  logging_to_files: false
```



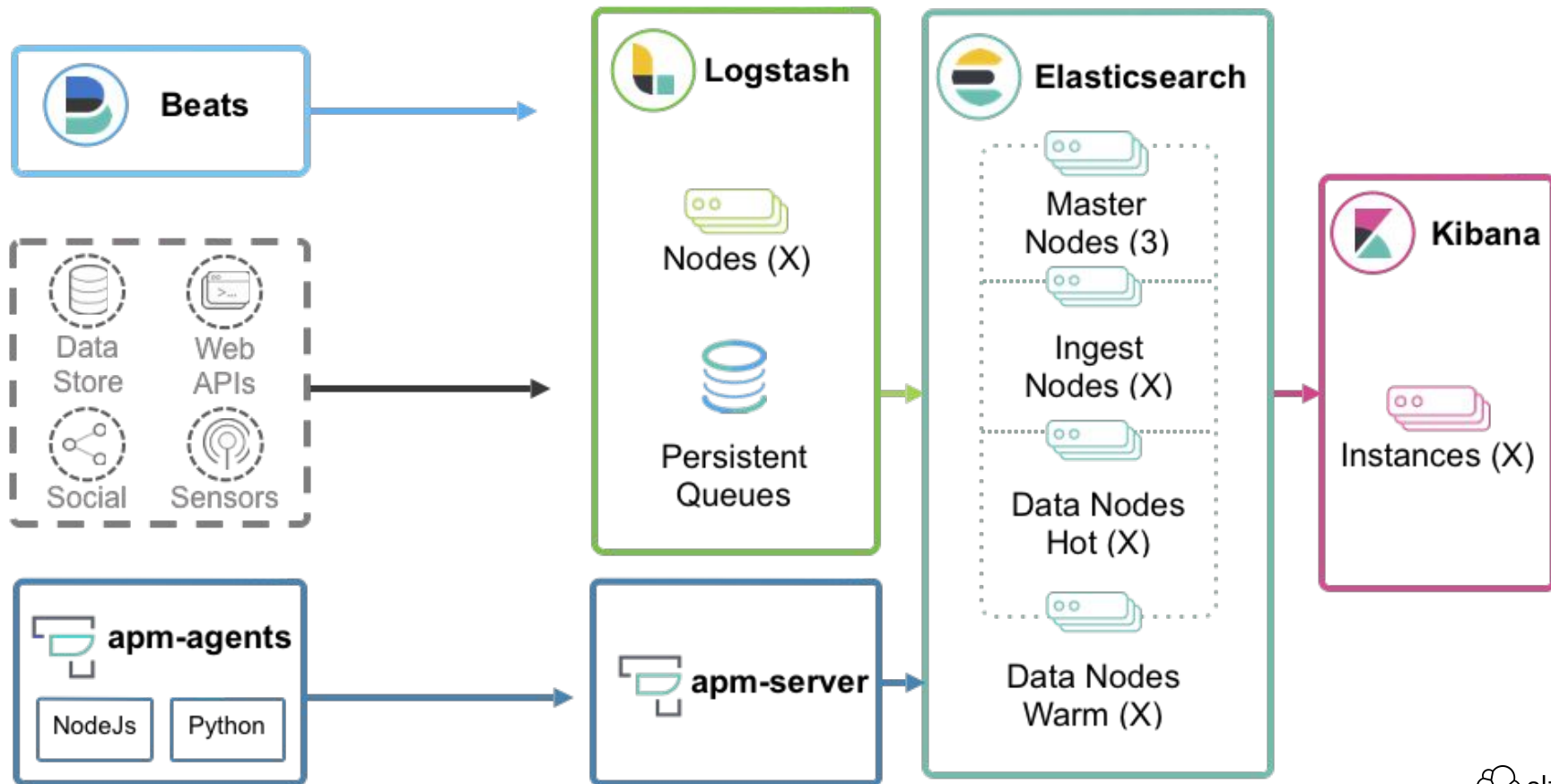
Observa tu sistema con Uptime de Kibana



Arquitecturas con el Elastic Stack



Arquitectura genérica usando el Elastic Stack



Arquitecturas para casos de uso específicos

- Observabilidad
- Negocios
- Seguridad
- Búsqueda
- Juegos

Diseño de una arquitectura de observabilidad

- Monitoreo basico con Heartbeat
- Captura de logs con Filebeat
- Captura de métricas con Metricbeat
- Captura de trazas de microservicios de aplicación con APM Server y sus agentes
- Kibana ofrece aps para cada tipo de observaciones
- El cluster de observación es independiente de otros clusters
- Se puede añadir un cluster adicional de recuperación ante desastres

Sigue aprendiendo



Cursos gratuitos

Free training

Whether you're just getting started or exploring new features, learning Elastic has never been easier with our free introductory training offerings.



Quick Starts

Start your Elastic journey with these bite-sized modules focused on logging, metrics, APM, Workplace Search, and App Search.

[View Quick Starts →](#)



Fundamentals training

Build your observability, security, and Elastic Stack skills anytime, anywhere with these on-demand courses.

[View Fundamentals courses →](#)

Planes de estudio de certificación

Paths to Elastic certification

The demand for Elasticsearch and Kibana experts increases every day. Our certifications let everyone know that you're just what they're looking for.



Elasticsearch engineers

From spinning up your first cluster to mastering advanced management techniques, the Elastic Certified Engineer path will make you an Elasticsearch expert.

- [Elasticsearch Engineer I >](#)
- [Elasticsearch Engineer II >](#)
- [Elastic Certified Engineer >](#)



Data analysts

Enter training a Kibana novice and leave ready to put your data visualization and advanced analytics skills to the test in our Kibana certification.

- [Data Analysis with Kibana >](#)
- [Elastic Certified Analyst >](#)



Observability engineers

Learn to unify your observability data — logs, metrics, APM — with the Elastic Stack. Then make it operational with dashboards, alerting, and machine learning.

- [Elastic Observability Engineer >](#)
- [Elastic Certified Observability Engineer >](#)

Especializaciones

- Búsqueda avanzada
- Ciencia de datos
- Logging
- Analíticos de seguridad
- Métricas
- Monitoreo de aplicaciones
- Administración del Stack de Elastic

Elasticsearch Advanced Search

Search is the heart of Elasticsearch. It's also about understanding how to use it. It's about understanding how to use it to find what you need. It's about understanding how to use it to find what you need. It's about understanding how to use it to find what you need.

[Get the Elasticsearch Advanced Search Guide](#)

[Elasticsearch Advanced Search](#)

[Elasticsearch Advanced Search](#)

[Elasticsearch Advanced Search](#)

[Elasticsearch Advanced Search](#)



Data Science

Use Elasticsearch to store and search your data. It's about understanding how to use it to find what you need. It's about understanding how to use it to find what you need. It's about understanding how to use it to find what you need.

[Get the Elasticsearch Data Science Guide](#)

[Elasticsearch Data Science](#)

[Elasticsearch Data Science](#)

[Elasticsearch Data Science](#)

[Elasticsearch Data Science](#)



Logging

Use Elasticsearch to store and search your logs. It's about understanding how to use it to find what you need. It's about understanding how to use it to find what you need. It's about understanding how to use it to find what you need.

[Get the Elasticsearch Logging Guide](#)

[Elasticsearch Logging](#)

[Elasticsearch Logging](#)

[Elasticsearch Logging](#)

[Elasticsearch Logging](#)



Security Analytics

Use Elasticsearch to store and search your security data. It's about understanding how to use it to find what you need. It's about understanding how to use it to find what you need. It's about understanding how to use it to find what you need.

[Get the Elasticsearch Security Analytics Guide](#)

[Elasticsearch Security Analytics](#)

[Elasticsearch Security Analytics](#)

[Elasticsearch Security Analytics](#)

[Elasticsearch Security Analytics](#)

Metrics

Use Elasticsearch to store and search your metrics. It's about understanding how to use it to find what you need. It's about understanding how to use it to find what you need. It's about understanding how to use it to find what you need.

[Get the Elasticsearch Metrics Guide](#)

[Elasticsearch Metrics](#)

[Elasticsearch Metrics](#)

[Elasticsearch Metrics](#)

[Elasticsearch Metrics](#)



APM

Use Elasticsearch to store and search your APM data. It's about understanding how to use it to find what you need. It's about understanding how to use it to find what you need. It's about understanding how to use it to find what you need.

[Get the Elasticsearch APM Guide](#)

[Elasticsearch APM](#)

[Elasticsearch APM](#)

[Elasticsearch APM](#)

[Elasticsearch APM](#)

Elastic Stack Management

Use Elasticsearch to store and search your Elastic Stack management data. It's about understanding how to use it to find what you need. It's about understanding how to use it to find what you need. It's about understanding how to use it to find what you need.

[Get the Elasticsearch Elastic Stack Management Guide](#)

[Elastic Stack Management](#)

[Elastic Stack Management](#)

[Elastic Stack Management](#)

[Elastic Stack Management](#)



Preguntas y respuestas



Recursos



Recursos adicionales

- <https://github.com/evkortright/pagina-de-búsqueda>
- <https://github.com/evkortright/primeros-pasos-con-kibana.git>
- enrique.kortright@elastic.co
- <https://www.linkedin.com/in/enrique-kortright-b182ba/>
- <https://discuss.elastic.co/>

Así termina nuestra serie de primeros pasos con el Elastic Stack

- Únete a la comunidad de Elastic en Costa Rica y sigue aprendiendo y conectándote con otros profesionales de Elastic!
- Y, por supuesto, continúa con la **PURA VIDA!**



Conéctate con la comunidad de Elastic

Existen User Groups en Costa Rica,
Mexico, Colombia, Argentina y Uruguay -
encuentra el tuyo:



User Group Virtual:



<https://community.elastic.co/>
<https://community.elastic.co/amer-virtual/>