Gestión de Logs

ELK

Introducción

¿Qué son los logs?

En informática, se usa el término registro, log o historial de log para referirse a la grabación secuencial en un archivo o en una base de datos de todos los acontecimientos (eventos o acciones) que afectan a un proceso particular (aplicación, actividad de una red informática, etc.). De esta forma constituye una evidencia del comportamiento del sistema.

```
2016-02-26 15:26:07.652737 I [1917:Puma 001] [127.0.0.1] [jbloggs] Rails — Started GET "/groups" for 127.0.0.1 at 2016-02-26 15:26:07 +0000
2016-02-26 15:26:07.830436 I [1917:Puma 001] [127.0.0.1] [jbloggs] GroupsController — Processing #index
2016-02-26 15:26:08.089099 I [1917:Puma 001] [127.0.0.1] [jbloggs] ActionView::Base —   Rendered cascading_gals/_groups_select.html.haml (28.4ms)
2016-02-26 15:26:08.104141 I [1917:Puma 001] [127.0.0.1] [jbloggs] ActionView::Base —   Rendered search/_search_form.html.haml (74.3ms)
2016-02-26 15:26:08.204800 I [1917:Puma 001] [127.0.0.1] [jbloggs] ActionView::Base —   Rendered action_links/_crud.html.haml (11.8ms)
2016-02-26 15:26:08.205121 I [1917:Puma 001] [127.0.0.1] [jbloggs] ActionView::Base —   Rendered groups/_group.html.haml (39.3ms)
2016-02-26 15:26:08.213000 I [1917:Puma 001] [127.0.0.1] [jbloggs] ActionView::Base —   Rendered groups/index.html.haml within layouts/application (212.3ms)
2016-02-26 15:26:08.573078 I [1917:Puma 001] [127.0.0.1] [jbloggs] ActionView::Base —   Rendered layouts/_ie_conditional.html.haml (116.2ms)
2016-02-26 15:26:08.700857 I [1917:Puma 001] [127.0.0.1] [jbloggs] ActionView::Base —   Rendered layouts/_menu.html.haml (125.9ms)
```

ELK

1. Un **agente de recogida de logs** en nuestras aplicaciones.

   Logstash.
2. Una **base de datos** donde almacenar, indexar y buscar los eventos de log de las aplicaciones.

   Elasticsearch.
3. Una **aplicación frontend** donde los usuarios puedan consultar los eventos más interesantes y estar informados de cualquier incidencia.

   Kibana.

¿Cómo vemos lo logs?

grep

tail

cat/less/more

vim/notepad

Desafíos en el manejo de logs

Generalmente tenemos muchas aplicaciones funcionando en paralelo y reportando sus logs. (servidores, app, sistema)

Pasar de un manejo de logs a un análisis de los logs

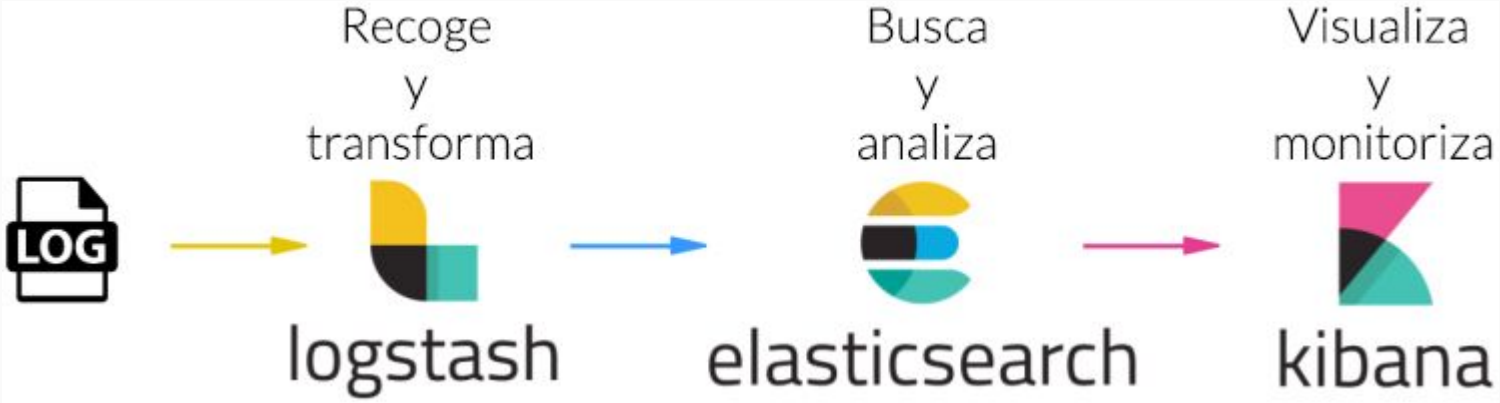
¿Cómo hacemos para conectar logs de distintas fuentes?

¿Cómo hacemos para referencias y correlacionar esta información?

Necesidades para hacer análisis de logs

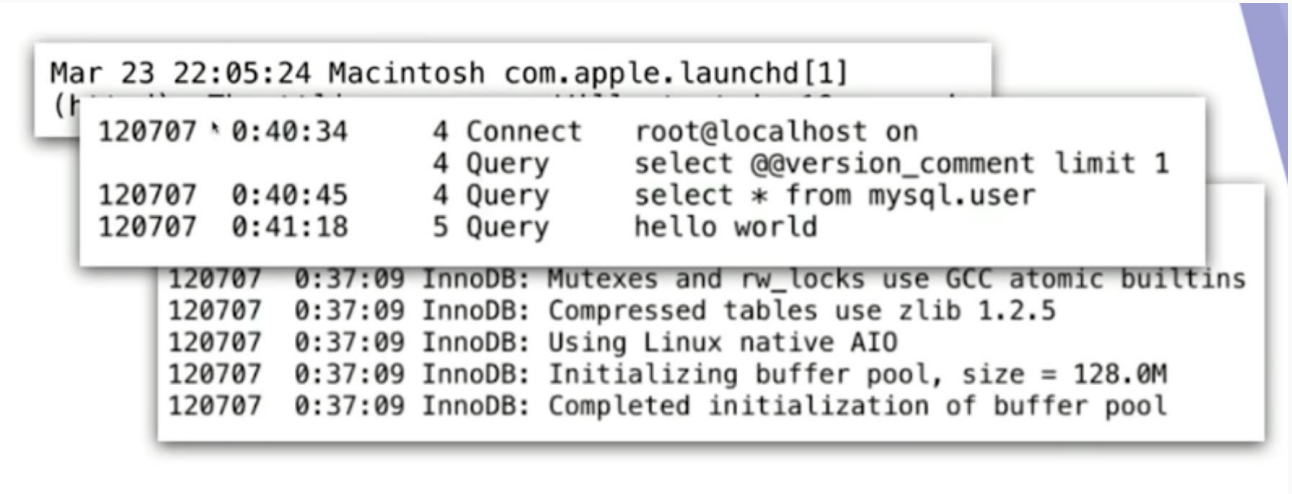
- Poder fácilmente conectar distintas fuentes de logs
- Correlacionarlos y referenciarlos
- Buscar, filtrar e identificar
- Visualizar lo que está pasando (por ejemplo ctos logs x segundo está generando una determinada aplicación)
- Detección de anomalías y alertas
- ¿Cómo hacemos una retención de los logs sensibles?

Proceso


LOG
Recoge
y
transforma
logstash
Busca
y
analiza
elasticsearch
Visualiza
y
monitoriza
kibana

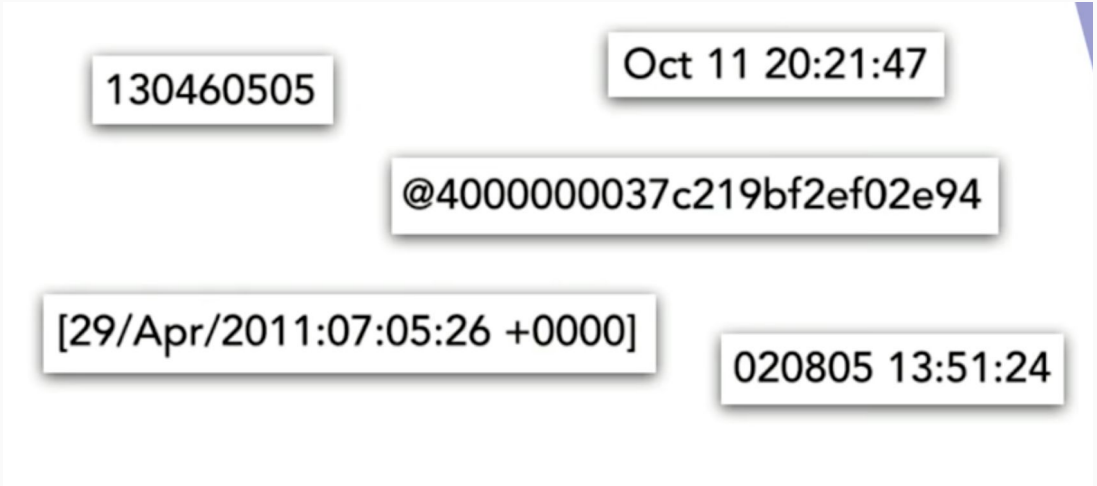
¿Qué resuelve Logstash?

Falta de consistencia: puedo estar recolectando logs con distintos formatos y cantidad de información

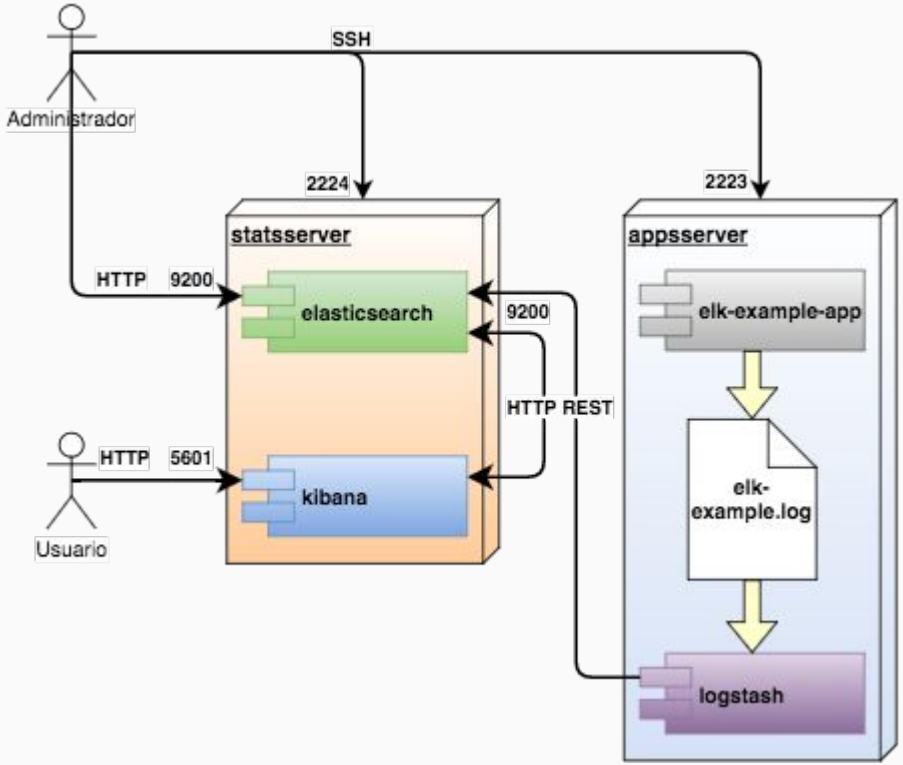


¿Qué resuelve Logstash?

Formato de tiempo: los formatos no siempre coinciden y el tiempo suele ser fundamental para analizar un proceso.



Una arquitectura posible



Comandos

1. sudo docker pull sebp/elk
2. sudo docker run -p 5601:5601 -p 9200:9200 -p 5044:5044 -it --name elk sebp/elk

- 5601 (Kibana web interface).
- 9200 (Elasticsearch JSON interface).
- 5044 (Logstash Beats interface

1ro Tenemos que enviar los logs al almacén

En el mundo Elastic existe un agente llamado filebeat

Este tiene módulos para configurarlo, pero también se puede configurar a mano