INTRODUCCIÓN & INSTALACIÓN LOGSTASH

LOGSTASH

Servicio para procesar/transformar información recolectada de distintas fuentes y enviarla a múltiples tipos de salidas.

Compuesto por: *entrada*, *filtrado* y *salida*.

1.

INTRODUCCIÓN

UTILIDADES: LIMPIEZA DE DATOS

- Eventos con gran cantidad de campos.
- ¿Todos necesarios? -> Campos realmente útiles.
- Arreglo de campos mal formados

Por ejemplo:

Campos A,D y G innecesarios: *Se eliminan*

Campo F -> *192.168.1.1:80:eth1:domain.com*

F_ip: ***192.168.1.1*** *F_port:* ***80***

F_iface: ***eth1*** *F_domain:* ***domain.com***

UTILIDADES: ENRIQUECIMIENTO DE DATOS

- Crear nuevos campos
- Añadir información a campos existentes
- Geolocalización

Por ejemplo:

Si el campo A:80 -> Se crea campo “proto:HTTP”

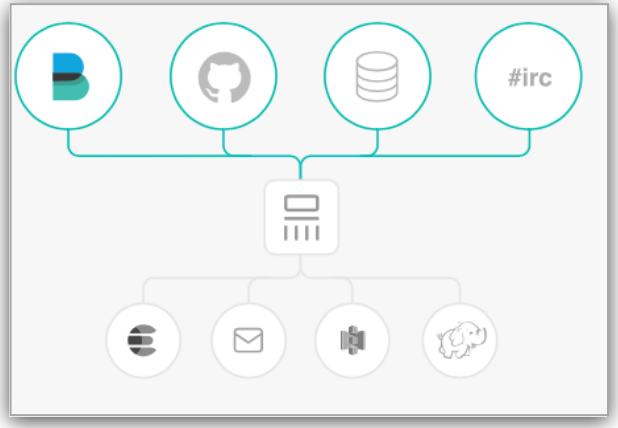
Campo F -> 25.26.27.28 (IP pública)

*Consulta de **Latitud** y **Longitud** de la misma*

Posibilidad de representar en un mapa.

CARACTERÍSTICAS DE LOGSTASH

Ingesta de datos de todas las formas, tamaños y fuentes.
Soporta distintos formatos de entrada permitiendo entrada de datos simultánea de logs, métricas, aplicaciones web, bases de datos, servicios AWS…

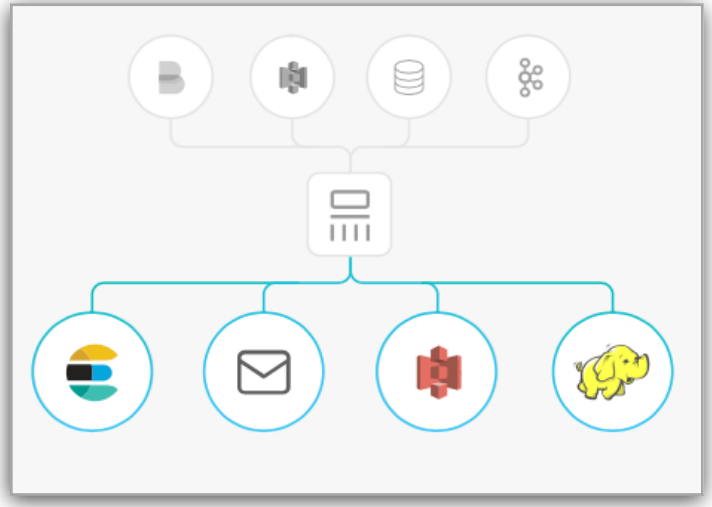


CARACTERÍSTICAS DE LOGSTASH

Transformaciones al vuelo identificando los campos y transformándolos. Estructura datos, añade geolocalización, trabaja con fingerprints y reconoce fechas.

CARACTERÍSTICAS DE LOGSTASH

Distintas salidas disponibles encaminando la información hacia ellas aportando flexibilidad para distintos casos de uso.



CARACTERÍSTICAS DE LOGSTASH

Extensibilidad: Más de 200 plugins y posibilidad de desarrollar plugins propios.
Durabilidad: Ofrece la posibilidad de usar una “cola” de almacenamiento temporal ante errores.
Monitorización: Visibilidad de recursos de las máquinas y estadísticas del servicio.
Seguridad: Información cifrada en la comunicación con los servicios, tanto de entrada como de salida.

2.

INSTALACIÓN

LOGSTASH

NOTA: necesario Java 8 (9 no soportado aún)

- Importar Elasticsearch PGP Key

  $ wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -

- Necesario el paquete *apt-transport-https*

  $ sudo apt-get install apt-transport-https

LOGSTASH

- Almacenar el repositorio en “*/etc/apt/sources.list.d/elastic-5.x.list*” :

  $ echo "deb https://artifacts.elastic.co/packages/5.x/apt stable main" | sudo tee -a /etc/apt/sources.list.d/elastic-5.x.list

- Instalación:

  $ sudo apt-get update && sudo apt-get install logstash

LOGSTASH (*Paths*)

Las **principales rutas** del servicio Logstash son:

- *home:* */usr/share/logstash*
- *bin:* */usr/share/logstash/bin*
- *conf:* */etc/logstash*
- *env:* */etc/default/logstash*
- *data:* */var/lib/logstash*
- *logs:* */var/log/logstash*
- *plugins:* */usr/share/logstash/plugins*

3.

PRIMER PROCESADO

PRIMER PIPELINE

Input, *Output* (obligatorios) y *Filter* (opcional).

- Procesamiento simple:

```
bin/logstash -e 'input { stdin { } } output { stdout {} }'
```

El parámetro *"-e"* permite especificar la configuración directamente en la línea de comandos.

Nota: *Tiempo* e *IP* añadidas automáticamente.