

# RedBorder logstash documentation

redborder

Version 0.0.1

# Índice

Capítulo 1: Introducción a Logstash.....	1
RedBorder Vault.....	1
Logstash.....	1
Arquitectura en RedBorder Vault .....	1

# Capítulo 1: Introducción a Logstash

En este capítulo introduciremos el servicio de Logstash y su integración dentro de la arquitectura de redBorder.

## RedBorder Vault

Cuando se depende de varios servicios para la operatividad de un producto o infraestructura es necesario disponer de un sistema que nos permita una rápida y simple gestión de los múltiples logs que se generan. Es aquí donde entra en juego RedBorder Vault.

RedBorder Vault es nuestro módulo de análisis de logs y eventos del sistema que permite la monitorización de logs así como su integración con el CEP para la correlación de eventos. Para llevar a cabo todo el tratamiento de datos se hace uso del conocido servicio Logstash.

## Logstash

Logstash es una herramienta open source que permite el procesamiento de datos. El procesamiento se hace a través de la definición de un pipeline que permite la ingesta de datos desde múltiples fuentes, los transforma a través de uno o varios filtros y finalmente los envía a distintos silos de almacenamiento.

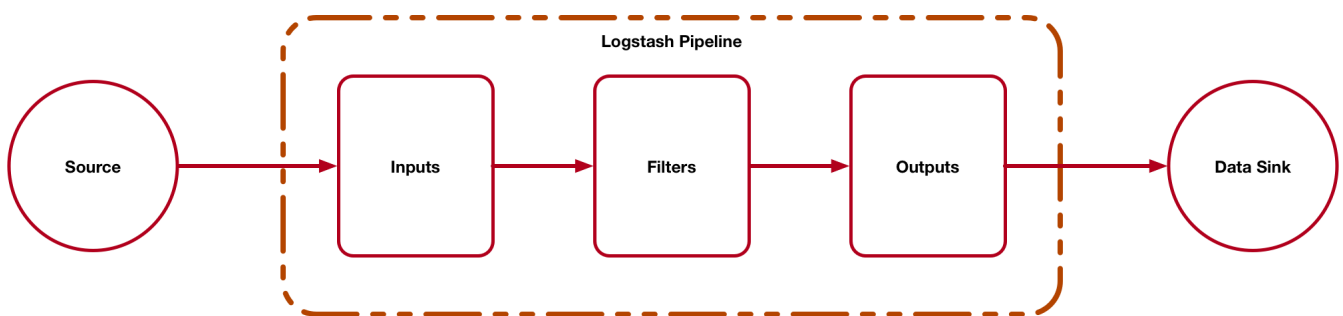


Figure 1. Logstash Pipeline

Además, Logstash cuenta con una comunidad muy activa que está en continuo crecimiento ofreciendo una gran variedad de plugins y filtros.

## Arquitectura en RedBorder Vault

Gracias a la combinación de Logstash y Kafka podemos ofrecer un servicio realmente potente y escalable para la monitorización de logs de múltiples servicios.

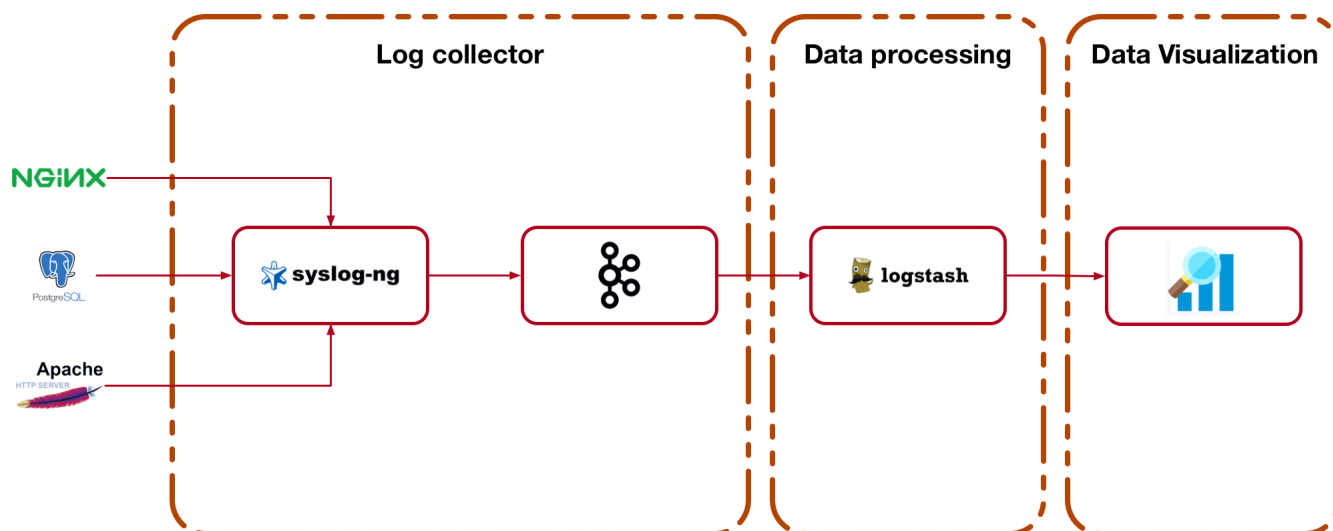


Figure 2. Arquitectura RedBorder Vault

Con una interfaz sencilla y muy intuitiva podrá visualizar todos los eventos de su entorno para asegurarse de que tiene la mejor respuesta en cada uno de los servicios.