

Servicios de valor añadido

Por José M. Román

FiberCli

Somos pura fibra

JOSE MANUEL ROMAN

17 años de experiencia, Mikrotik Certified Consultant and Trainer.
MTCNA, MTCRE, MTCTCE, MTCUME, MTCWE, MTCINE, CISA, CISSP, Master
ITIL

- (2015 – Now) CEO @ WISP Cloud Networking Spain
- (2008 – Now) Security Consultant and Analyst
- ***(2000 – 2007) Profesor de redes, programación, sistemas y Base de datos.***



MADRID / PRAGUE



@MAFIASOLEH



+34 652 241431



Jose.roman@fibercli.com

José Manuel Román para FiberCli





FAJAR NUGROHO

Network Engineer by Job and Troublemaker by Act, currently focusing on MikroTik, Juniper, Arista, UBNT, Vmware Virtualization, Linux/Unix (Debian & FreeBSD). CCNA, MTCNA, MTCRE, MTCTCE, JNCIA, JNCIS-ENT, JNCIS-SP, JNCIP-SP, MikroTik Certified Trainer.

- (2015 – 2016) Infrastructure (*System, Network & Security*) Engineer. @ [Technology and Information Department of Jakarta Capital City](#) and [Jakarta SmartCity](#)
- (2012 – Now) Freelancer @ SMB to Enterprise customers
- (2008 – 2012) Helpdesk, NOC (*Network Operator Center*). @ [Wireless Internet Service Provider](#) and [Triple Play \(CaTV, VoIP and Internet\) Service Provider](#)



TOLEDO / JAKARTA




@MAFIASOLEH
José Manuel Román para FiberCli



+62 813 1777 1455

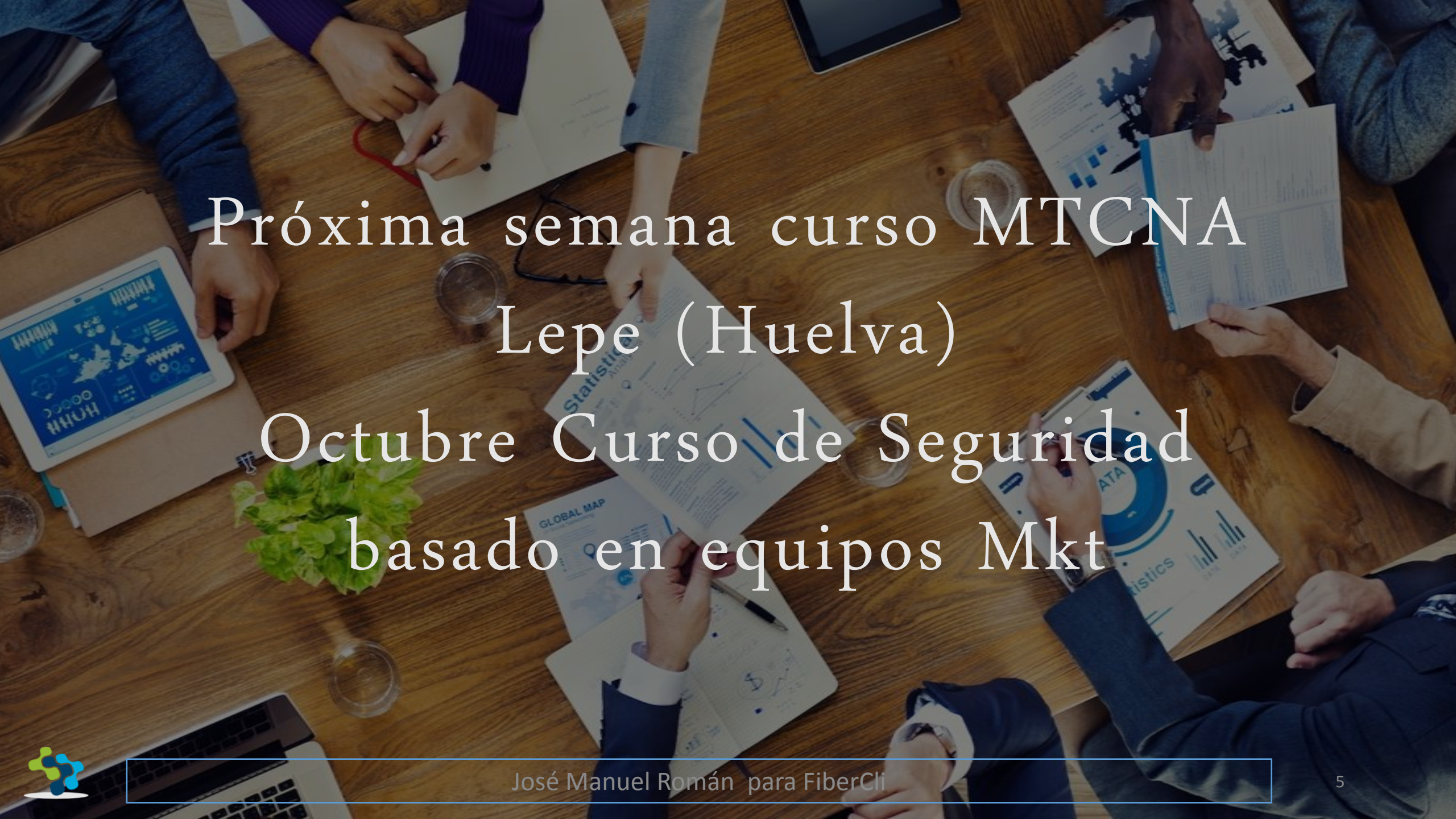


fajar@fibercli.com

A top-down view of a meeting table with people's hands, papers, a laptop, and a tablet. The text is overlaid on the image.

Llave en mano fibra óptica Soporte 24 x 7 Formación en Mikrotik y Seguridad





Próxima semana curso MTCNA
Lepe (Huelva)
Octubre Curso de Seguridad
basado en equipos Mkt





20% Descuento Asistentes al MUM



Problema

Múltiples eventos en la red que como administrador de sistemas o red no sabemos localizar el origen.



Síntomas

Multiples incidentes que no son recogidos en ninguna parte.

Sensación de descontrol en la red.



Solución

Arquitectura de red con Sistema Centralizado de Recopilación,
Normalización, Visualización y Análisis



AGENDA

- Introduction
- Arquitectura Centralizada
- ELK (ElasticSearch, Logstash, Kibana)
- Mkt + AAA+ con Freeradius y Bases de datos centralizadas
- Mkt + Log centralizado y ELK
- Mkt + Monitorización y ELK
- Mkt + Netflow y ELK
- Q and A

¿Qué es? **ELK**



Elasticsearch

Es un motor de búsqueda que almacena datos de una forma estructurada, que va a facilitar la labor de búsqueda y que nos va a dar muchas alegrías



Elasticsearch

- Escrito en Java
- Puede indexar datos heterogeneos
- Posibilita busquedas potentes en tiempo real
- Tiene api con REST y salida JSON



Logstash

Es un motor de recolección de datos que nos va permitir unificar y normalizar



Logstash

Consta de tres partes:

Input: Convierte los logs para ser procesados a un formato adecuado.

Filter: Condiciones para llevar a cabo una acción en caso que se produzca un evento.

Output: Toma de decisiones para los eventos procesados.



Kibana

Es una plataforma de visualización y análisis que nos va a poner guapos nuestros datos.





rsyslog



Sistema AAA



Radius

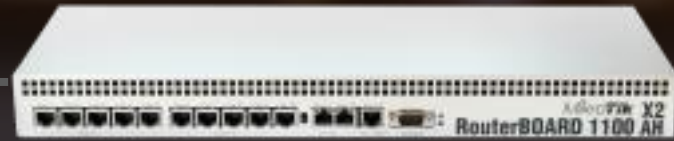
RADIUS es un protocolo de nivel de aplicación que proporciona autenticación, autorización y accounting (AAA).

Está definido en el RFC 2865.





Link-Establishment



Link-Establishment



Dial-In User try to connect (username & password)



RADIUS Access-Request



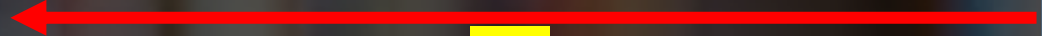
RADIUS Access-Challenge



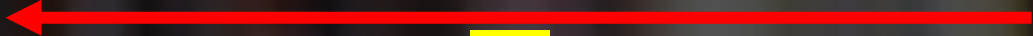
RADIUS Access-Request



RADIUS Access-Reject



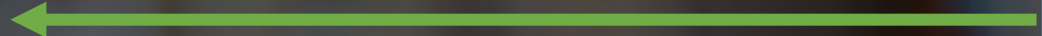
Disconnect



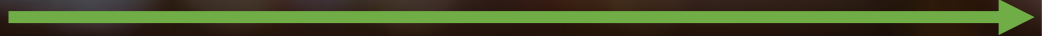
OR

OR

RADIUS Access-Accept



Accounting-Request (Start)



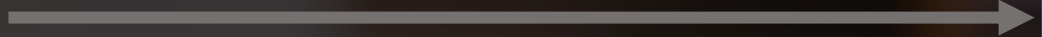
Accounting-Response



Session Start



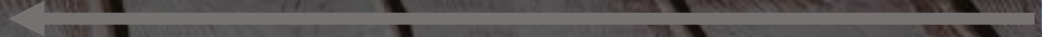
Accounting-Request (Stop)



Disconnect



Accounting-Response



Topología

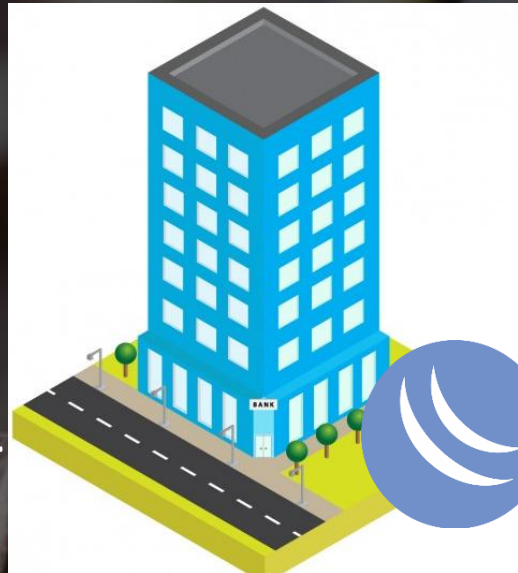




MIKROTIK SITE 2



MIKROTIK SITE 3



MIKROTIK SITE 1



RADIUS



DATABASE BACKEND



Configuración en Mikrotik



Radius

#	Service	Called ID	Domain	Address	Secret
0	login			127.0.0.1	fajar123

1 item (1 selected)

Radius Server <127.0.0.1>

General | Status

Service: ppp login
 hotspot wireless
 dhcp

Called ID:

Domain:

Address:

Secret:

Authentication Port:

Accounting Port:

Timeout: ms

Accounting Backup

Realm:

Src. Address:

enabled



Freeradius produce una serie de logs que podemos procesar dentro de logstash

<http://code.metager.de/source/xref/freeradius/server/doc/schemas/logstash/>



Log centralizado



RSYSLOG

RSYSLOG stand for "the rocket-fast system for log processing" is an open-source software utility used on UNIX and Unix-like computer systems for forwarding log messages in an IP network. It implements the basic syslog protocol, extends it with content-based filtering, rich filtering capabilities, flexible configuration options and adds features such as using TCP for transport

<http://www.rsyslog.com/rsyslog-8-19-0-v8-stable-released/>



RSYSLOG

Rsyslog nos ofrece:

Marca de tiempo ISO 8601 timestamp con granularidad de milisegundos

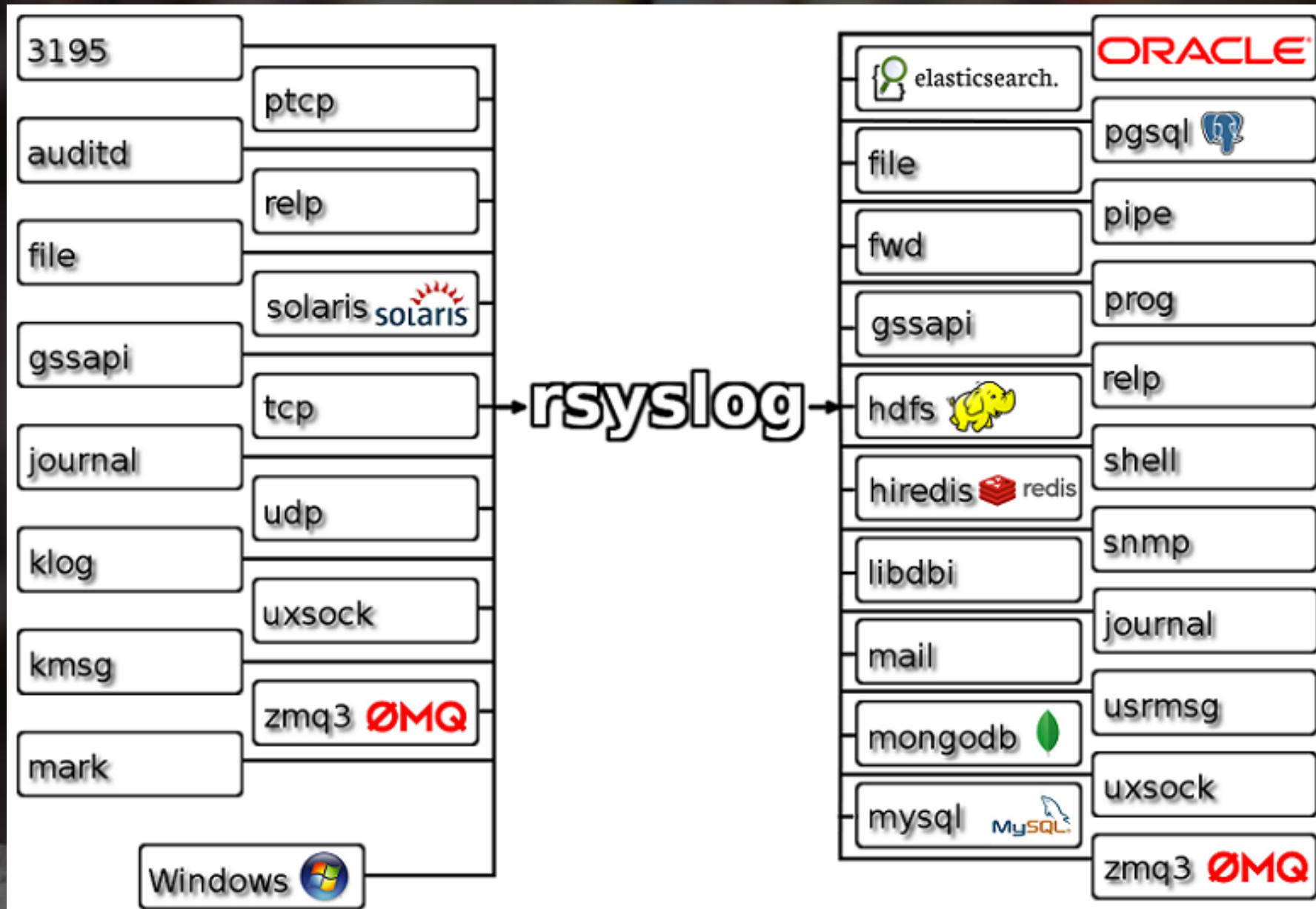
Transporte utilizando tcp y soporte de TLS

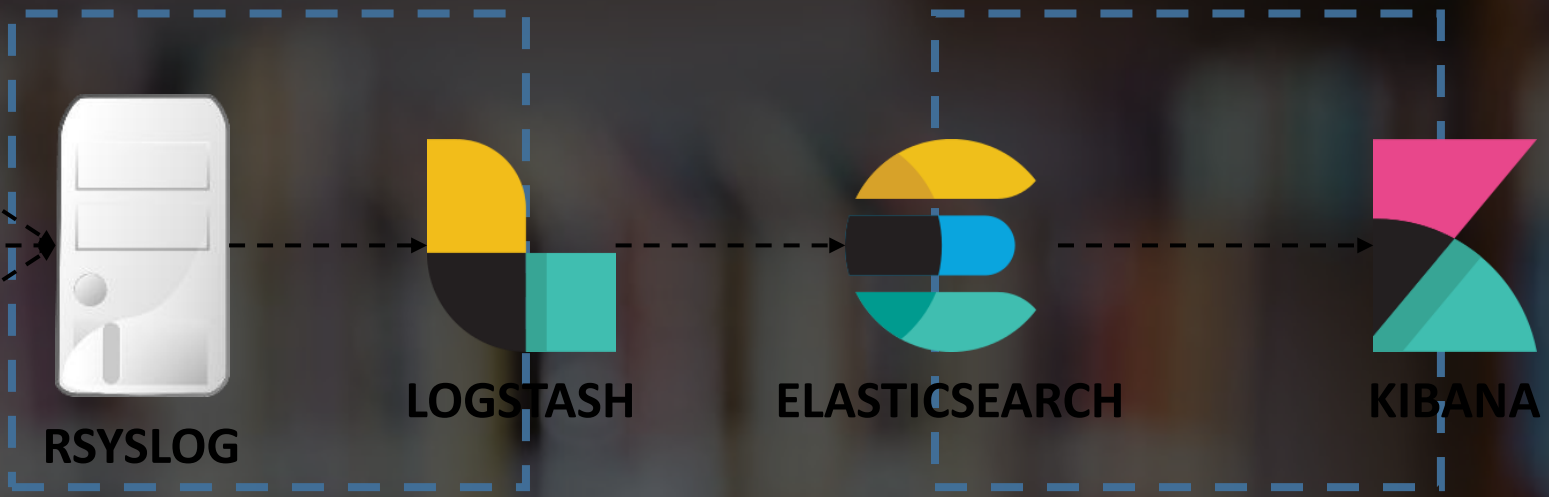
Capacidad de almacenar los logs en diferentes bases de datos.



Topología







MikroTik log Configuration



Logging

Rules Actions

+ - Filter Find

Name	Type
* disk	disk
* echo	echo
* memory	memory
* remote	remote

Log Action <remote>

Name: remote

Type: remote

Remote Address: IP.Address.LogServer

Remote Port: 514

Src. Address: 0.0.0.0

BSD Syslog

Syslog Facility: 3 (daemon)

Syslog Severity:

default

OK Cancel Apply Copy Remove

4 items (1 selected)

```
system logging action set remote remote=ip.address.log.server
```



New Log Rule

Topics: critical

Prefix:

Action: remote

enabled

New Log Rule

Topics: error

Prefix:

Action: remote

enabled

New Log Rule

Topics: warning

Prefix:

Action: remote

enabled

New Log Rule

Topics: info

Prefix:

Action: remote






enabled




```
/system logging
add action=remote topics=critical
add action=remote topics=error
add action=remote topics=info
add action=remote topics=warning
```



Logging

Rules Actions

Action  contains  remote 

Topics	Prefix	Action	
critical		remote	
error		remote	
info		remote	
waming		remote	

4 items out of 8 (1 selected)



Monitorización



```
/snmp set enabled=yes contact="jose.roman@fibercli.com" location="Mum Madrid" trap-community=public trap-version=2
```



Host Templates IPMI Macros Host inventory Encryption

Host name

Visible name

Groups

In groups

- Discovered hosts
- Zabbix servers

Other groups

- Database servers
- Hypervisors
- JB applications
- Linux servers
- Network devices
- SNMP hosts
- Templates
- UPS devices
- Virtual machines
- Web servers
- Windows servers

New group

Agent interfaces

IP ADDRESS	DNS NAME	CONNECT TO	PORT	DEFAULT
<input type="text" value="192.168.3.239"/>	<input type="text"/>	<input type="button" value="IP"/>	<input type="text" value="10050"/>	<input checked="" type="radio"/> Remove

[Add](#)

SNMP interfaces

<input type="text" value="127.0.0.1"/>	<input type="text"/>	<input type="button" value="IP"/>	<input type="text" value="161"/>	<input checked="" type="radio"/> Remove
--	----------------------	-----------------------------------	----------------------------------	---

Use bulk requests

[Add](#)

JMX interfaces [Add](#)

IPMI interfaces [Add](#)

Description

Monitored by proxy

Enabled



Existen clientes para exportar historicos de datos desde zabbix a bases de datos de series temporales.

<https://github.com/jojobhappy/zabbix-relay>



Podemos integrar los eventos de zabbix como entrada a logstash, con el objetivo de tener una monitorizacion desacoplada.

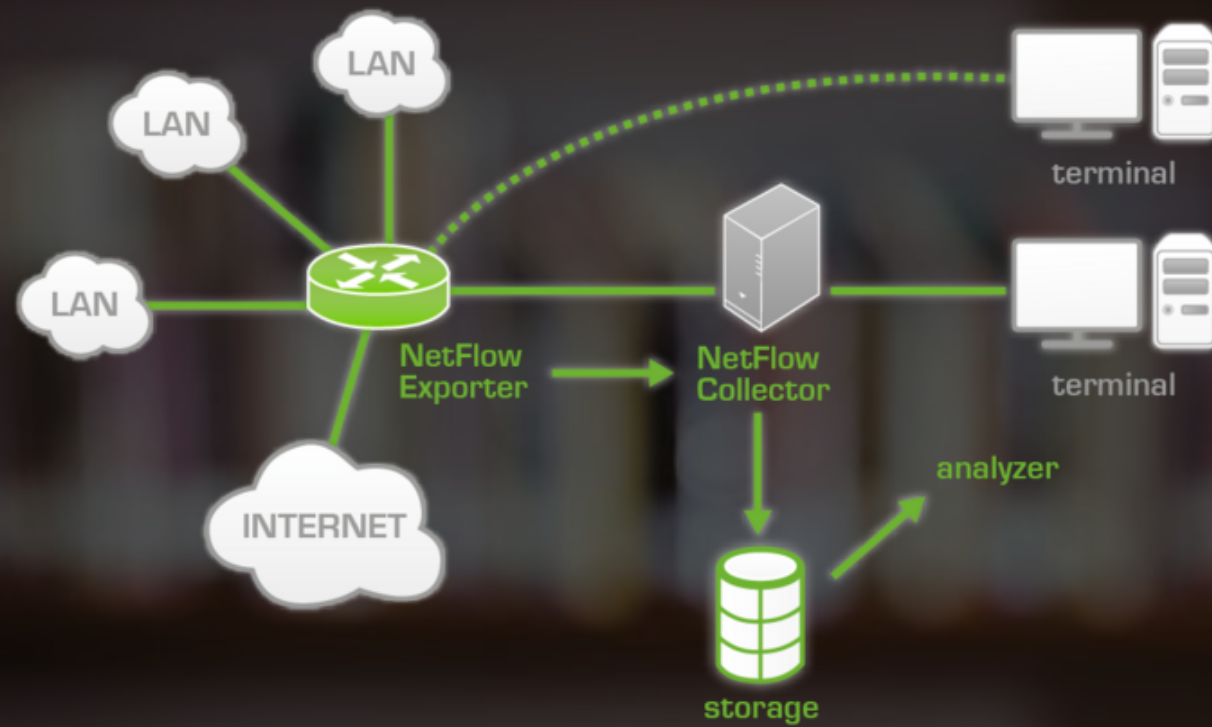


Netflow



NetFlow es un [protocolo de red](#) desarrollado por [Cisco Systems](#) para recolectar información sobre tráfico [IP](#).





```
/ip traffic-flow set active-flow-timeout=30m cache-entries=1M  
\enabled=yes inactive-flow-timeout=15s interfaces=all
```



```
/ip traffic-flow target add dst-address=ip.server port=5055 disabled=no  
\v9-template-refresh=20 v9-template-timeout=30m version=9
```



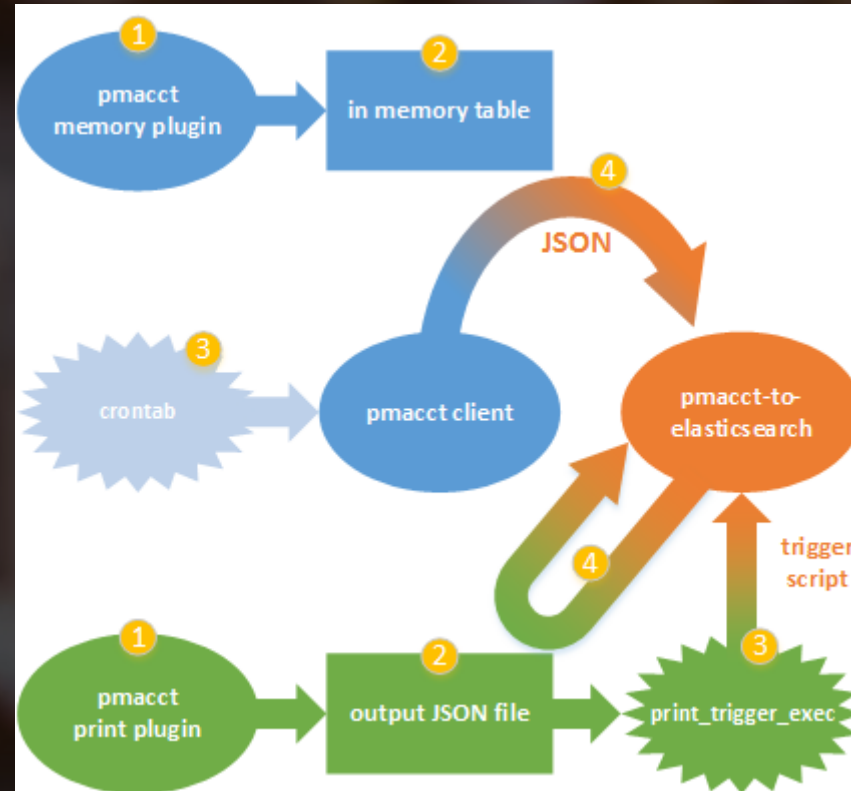
Para recoger esta salida necesitamos un colector de netflow que va a recoger los paquetes enviados por la sonda, como por ejemplo pmacct.



Una vez que recogemos los logs con pmacct vamos a enviar las salida a en formato json a ElasticSearch.

<https://github.com/pierky/pmacct-to-elasticsearch/blob/master/CONFIGURATION.md>

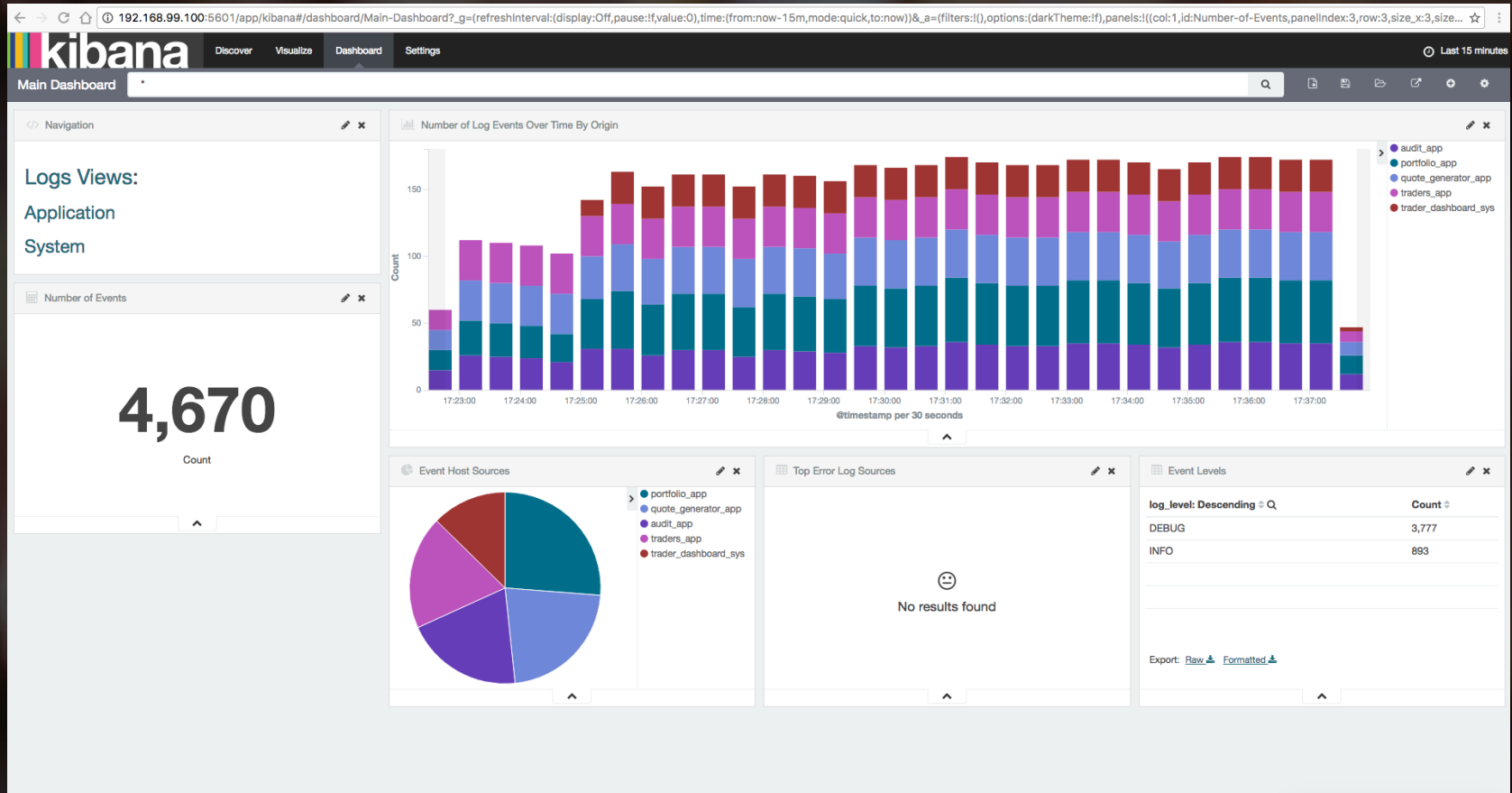




<https://github.com/pierky/pmacct-to-elasticsearch/blob/master/CONFIGURATION.md>







Recursos adicionales



Grafana

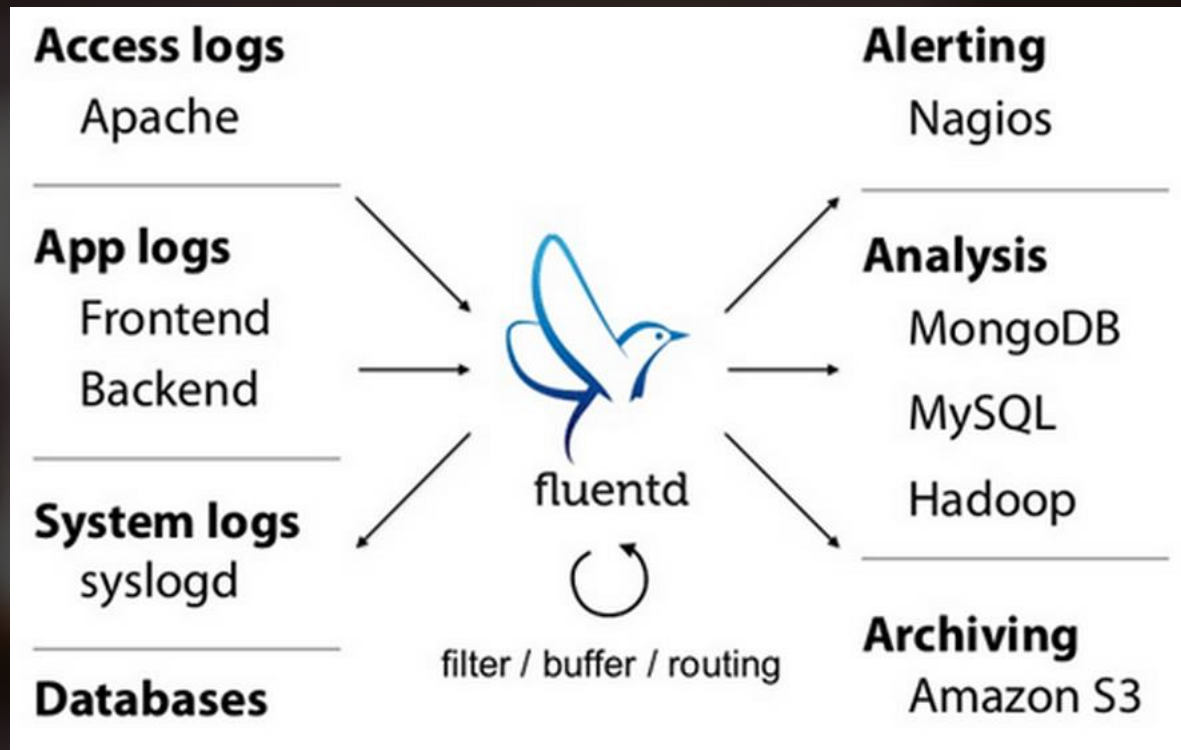


Influxdb



Fluentd





Muchas gracias

