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, programaación, sistemas y Base de datos.***

MADRID / PRAGUE

+34 652 241431

@MAFIASOLEH

Jose.roman@fibercli.com

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) Infrastucture *(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

+62 813 1777 1455

@MAFIASOLEH

fajar@fibercli.com

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 busqueda que almacena datos de una forma estructurada, que va a facilitar la labor de busqueda y que nos va a dar muchas alegrias

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.

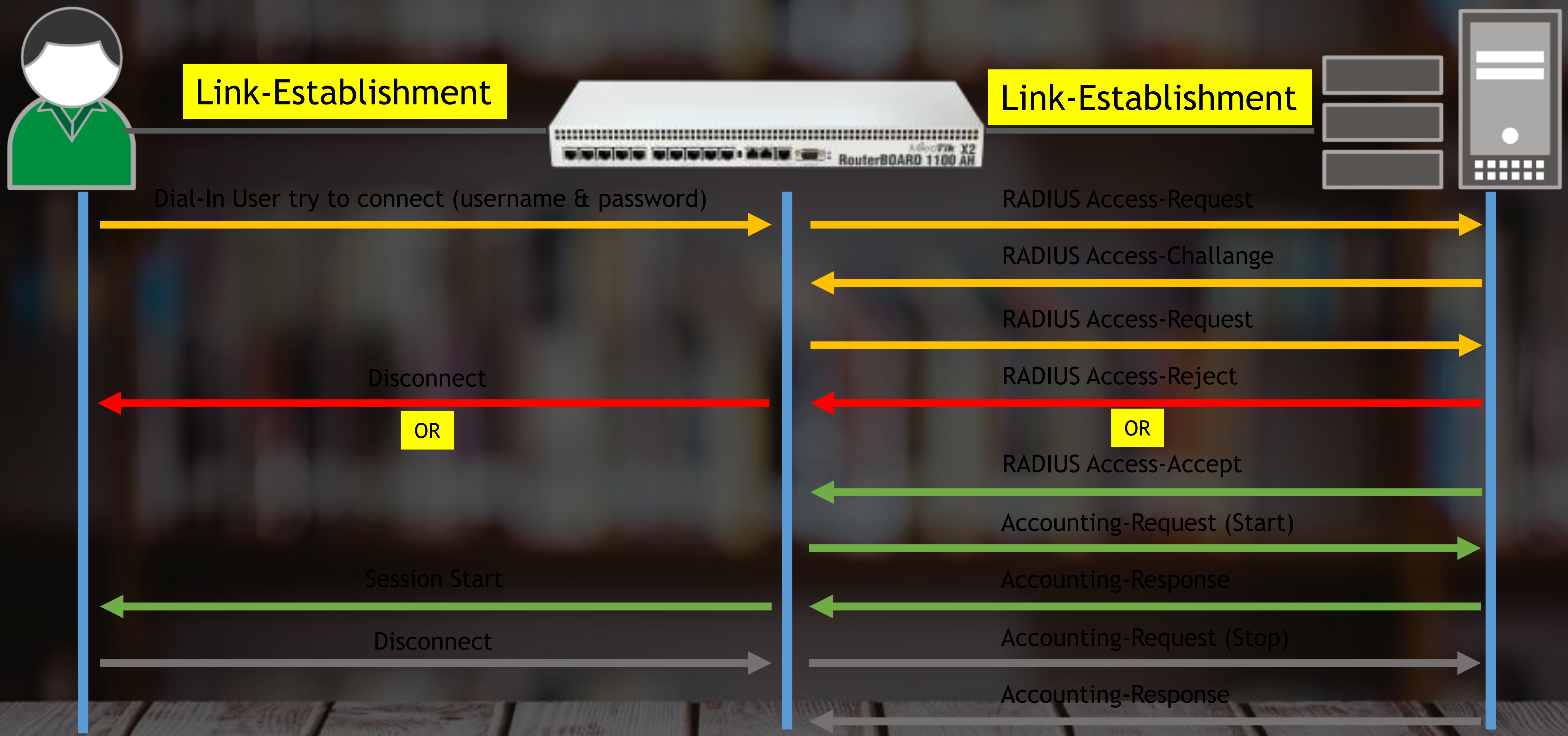

Powered by
MikroTik
FreeRADIUS
The world's most popular RADIUS Server
elastic
kibana
ZABBIX
rsyslog
NetFlow

Sistema AAA

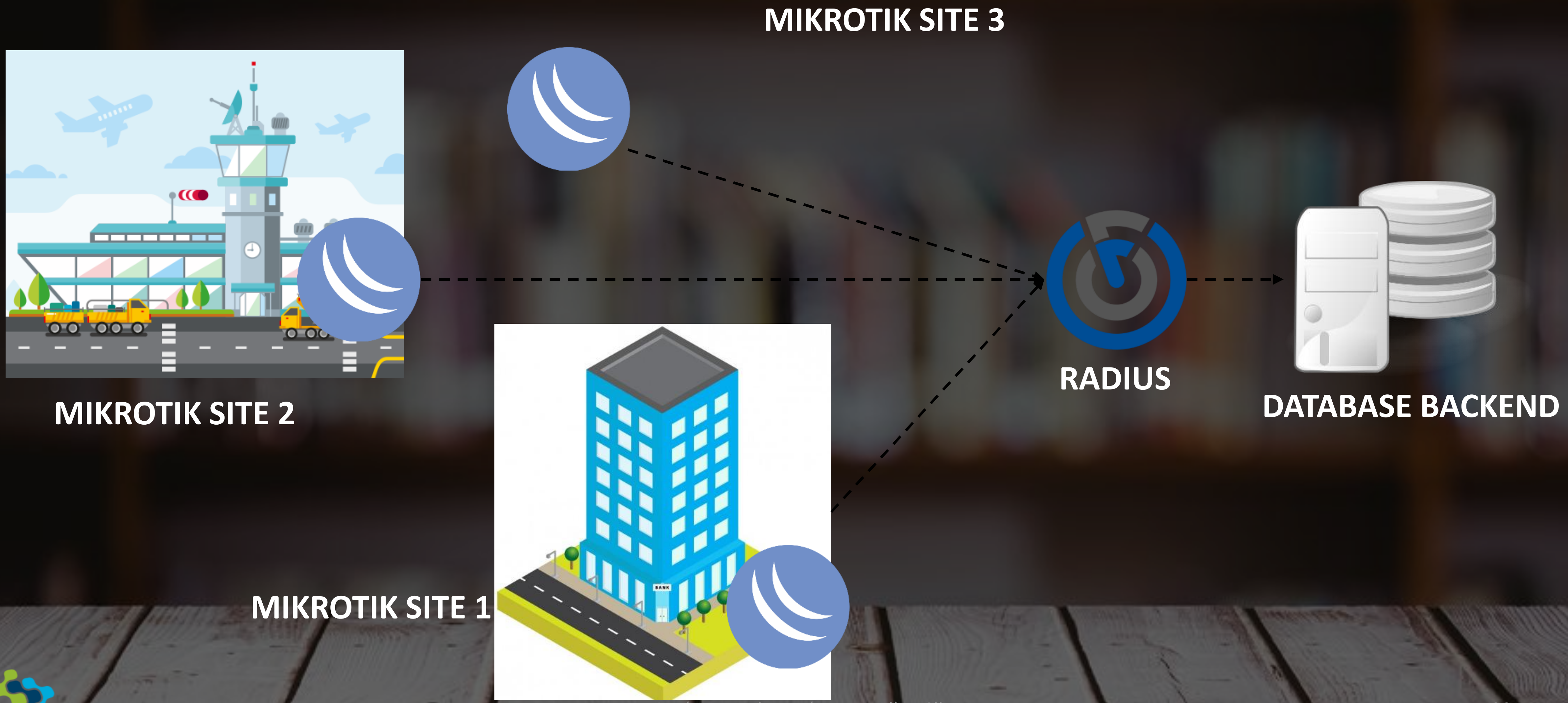
Radius

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

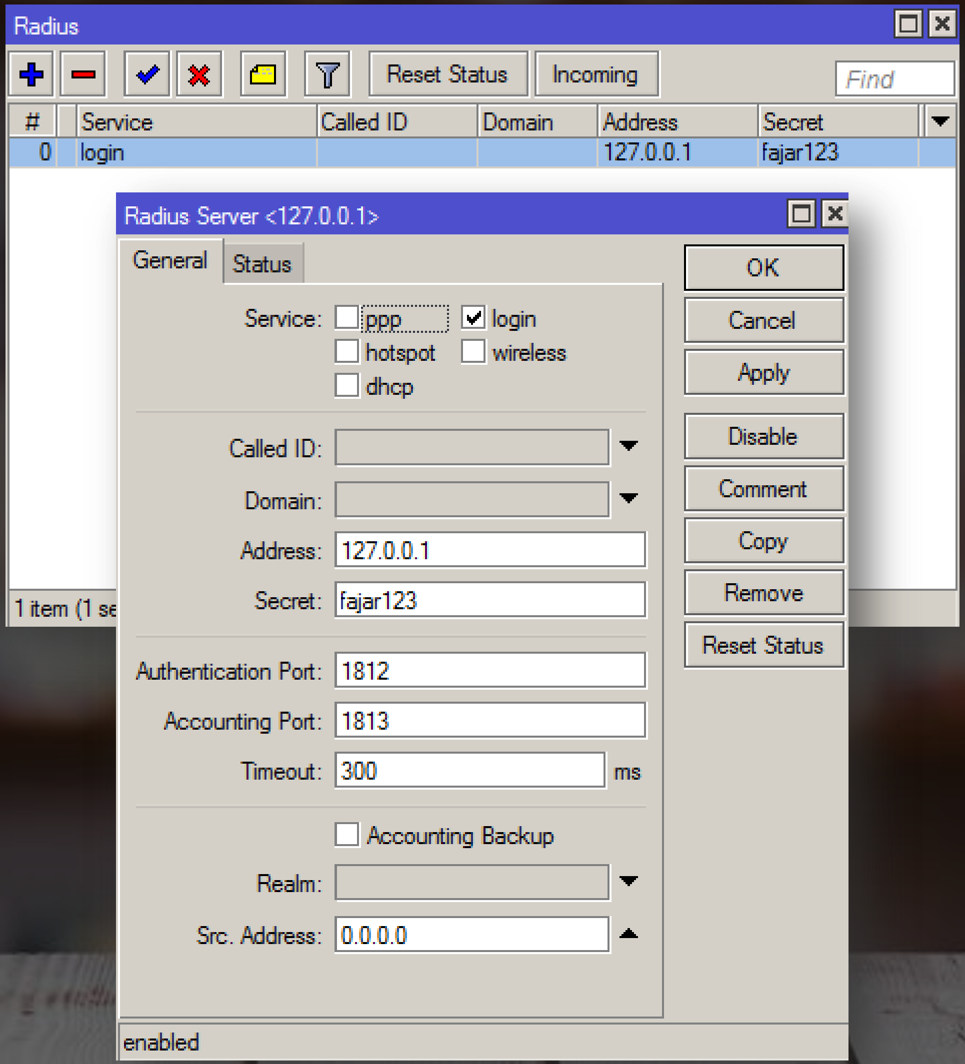
Está definido en el RFC 2865.


Link-Establishment
Link-Establishment
RouterBOARD 1100 AH
Dial-In User try to connect (username & password)
RADIUS Access-Request
RADIUS Access-Challange
RADIUS Access-Request
Disconnect
RADIUS Access-Reject
OR
OR
RADIUS Access-Accept
Accounting-Request (Start)
Session Start
Accounting-Response
Disconnect
Accounting-Request (Stop)
Accounting-Response

Topología


MIKROTIK SITE 3
MIKROTIK SITE 2
RADIUS
DATABASE BACKEND
MIKROTIK SITE 1

Configuración en Mikrotik


Radius
Reset Status
Incoming
Find
#
Service
Called ID
Domain
Address
Secret
0
login
127.0.0.1
fajar123
1 item (1 se
Radius Server <127.0.0.1>
General
Status
OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Status
Service:
ppp
login
hotspot
wireless
dhcp
Called ID:
Domain:
Address:
127.0.0.1
Secret:
fajar123
Authentication Port:
1812
Accounting Port:
1813
Timeout:
300
ms
Accounting Backup
Realm:
Src. Address:
0.0.0.0
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

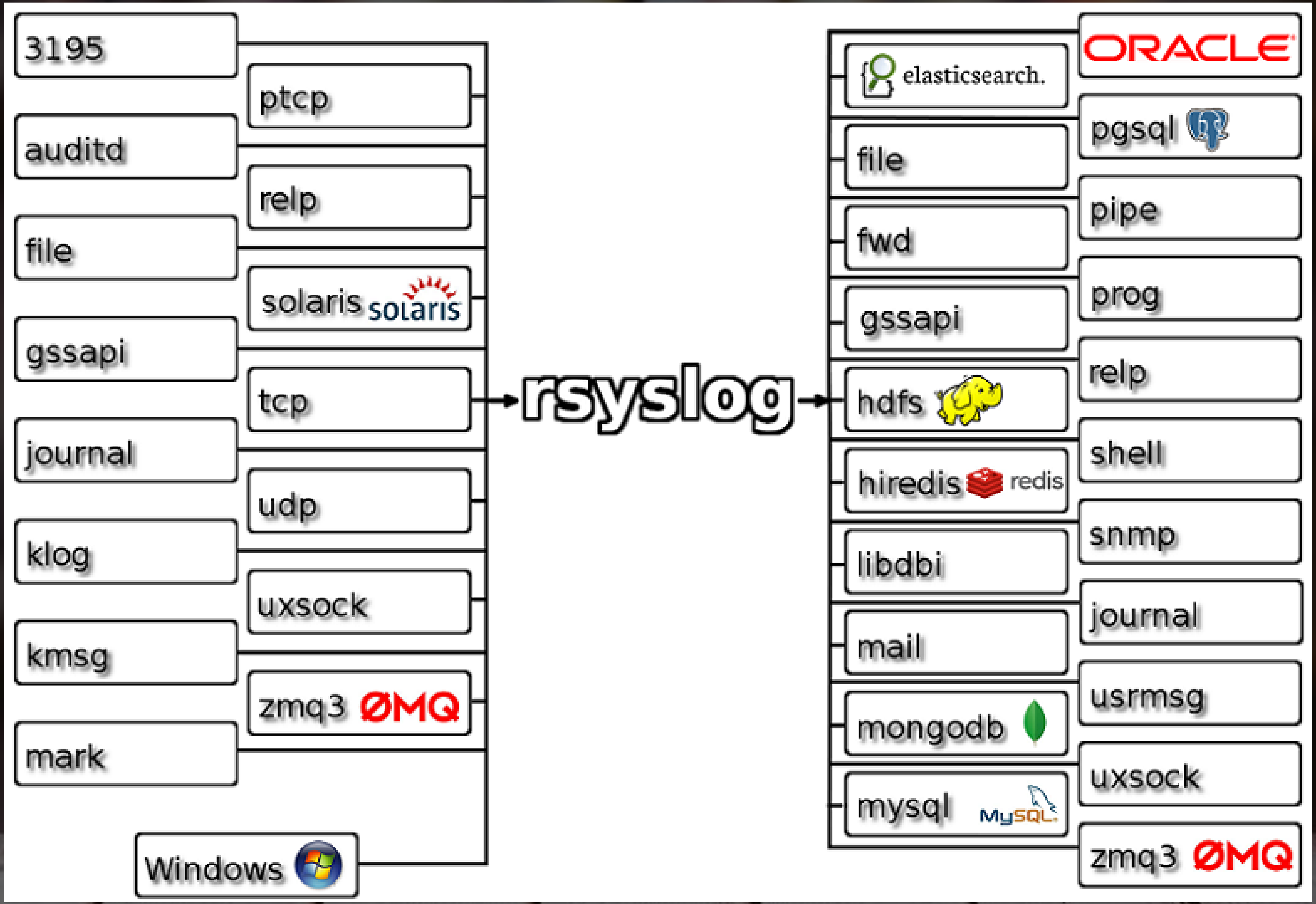
Rsyslog nos ofrece:

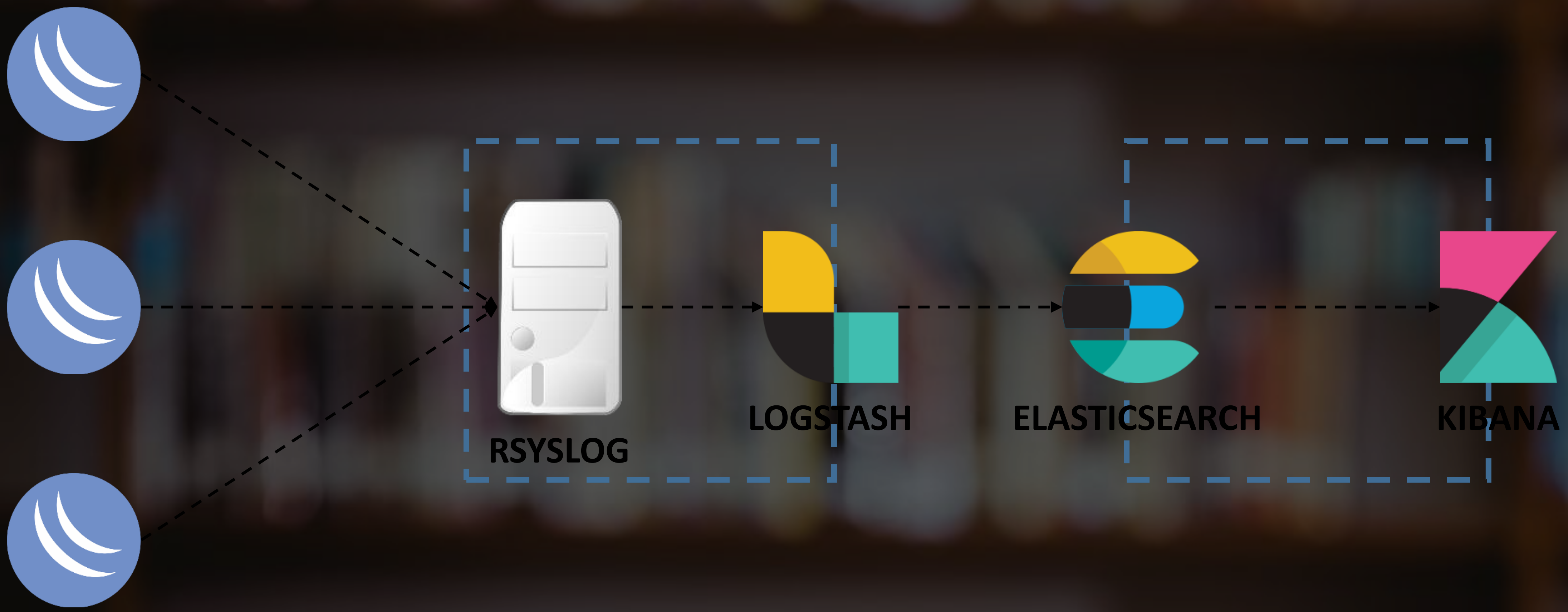
Marca de tiempo ISO 8601 timestamp con granularidad de milisegundos

Transporte utilizando tcp y soporte de TLS

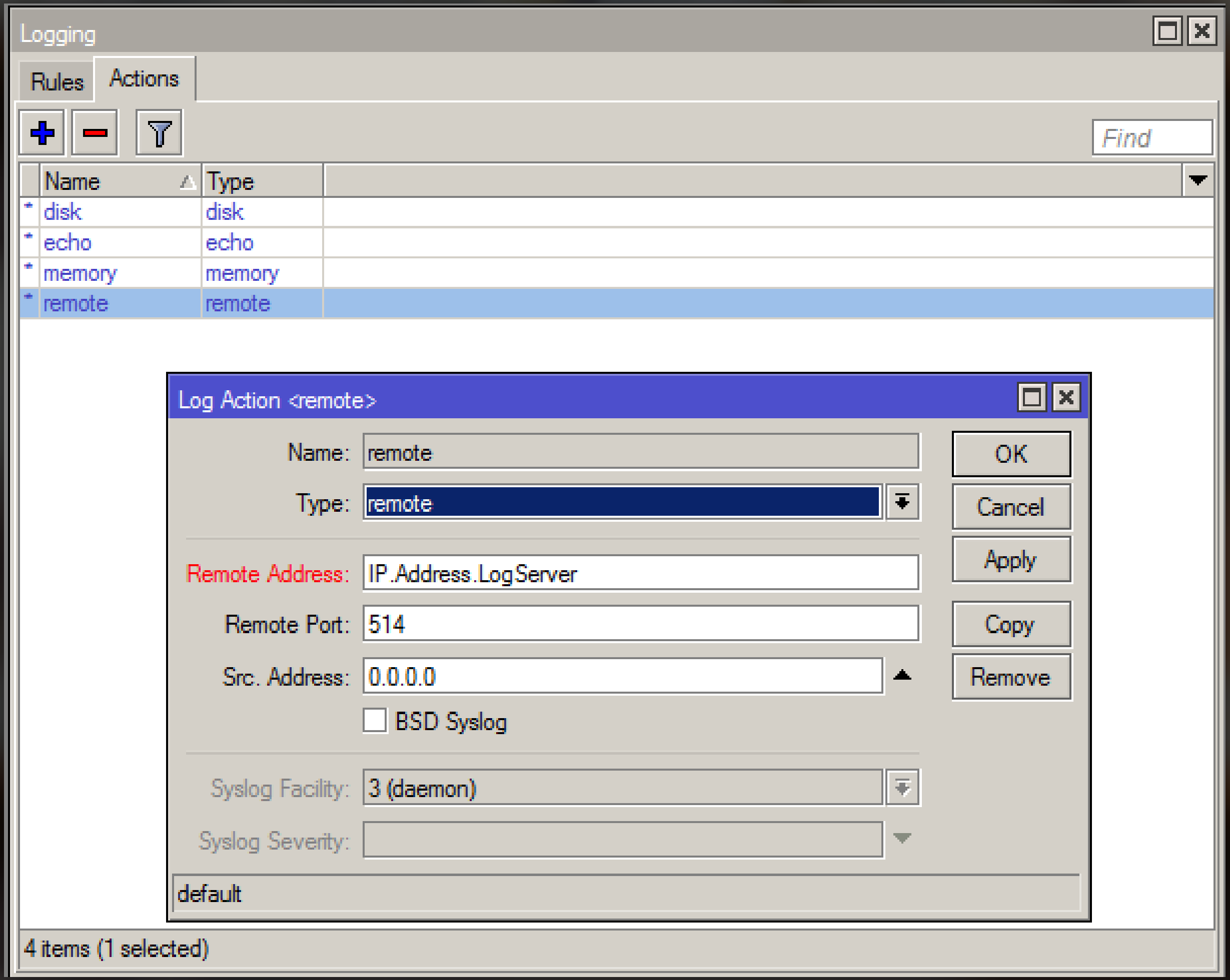
Capacidad de almacenar los logs en diferentes bases de datos.

Topología

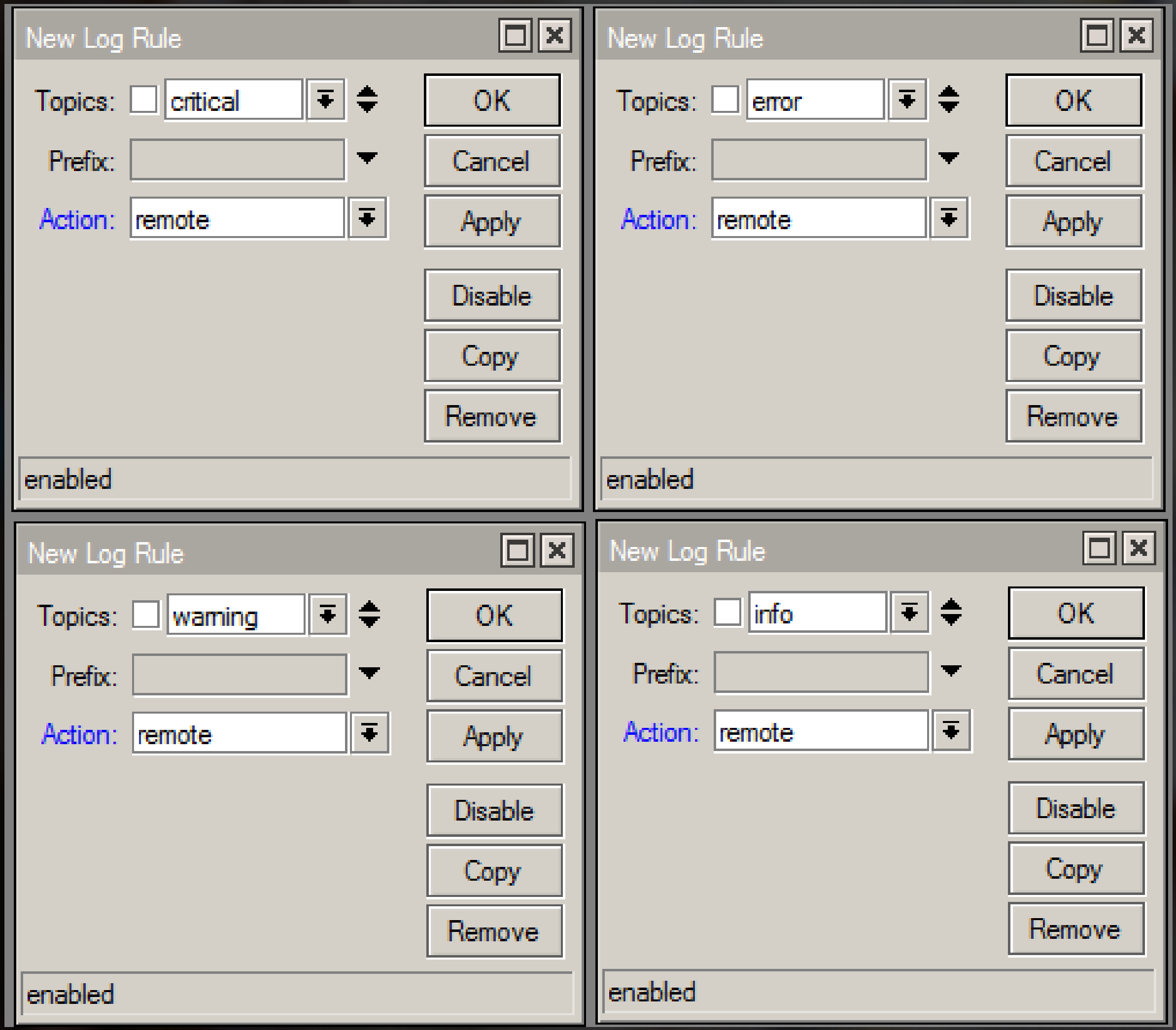

3195
ptcp
auditd
relp
file
solaris
gssapi
tcp
journal
udp
klog
uxsock
kmsg
zmq3 ØMQ
mark
Windows
rsyslog
elasticsearch.
ORACLE
file
pgsql
fwd
pipe
gssapi
prog
hdfs
relp
hiredis redis
shell
libdbi
snmp
mail
journal
mongodb
usrmsg
mysql MySQL
uxsock
zmq3 ØMQ


RSYSLOG
LOGSTASH
ELASTICSEARCH
KIBANA

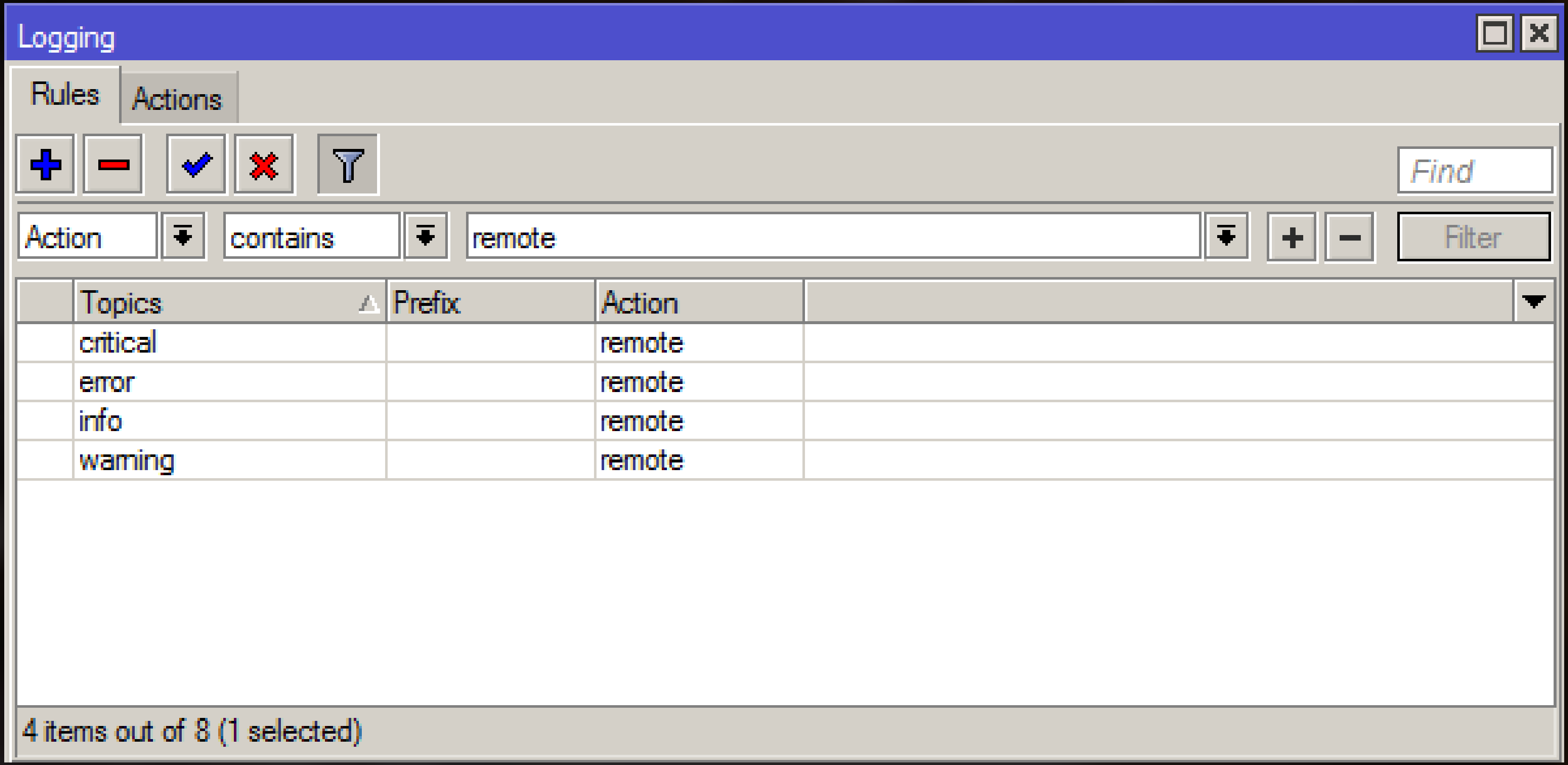
MikroTik log Configuration




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

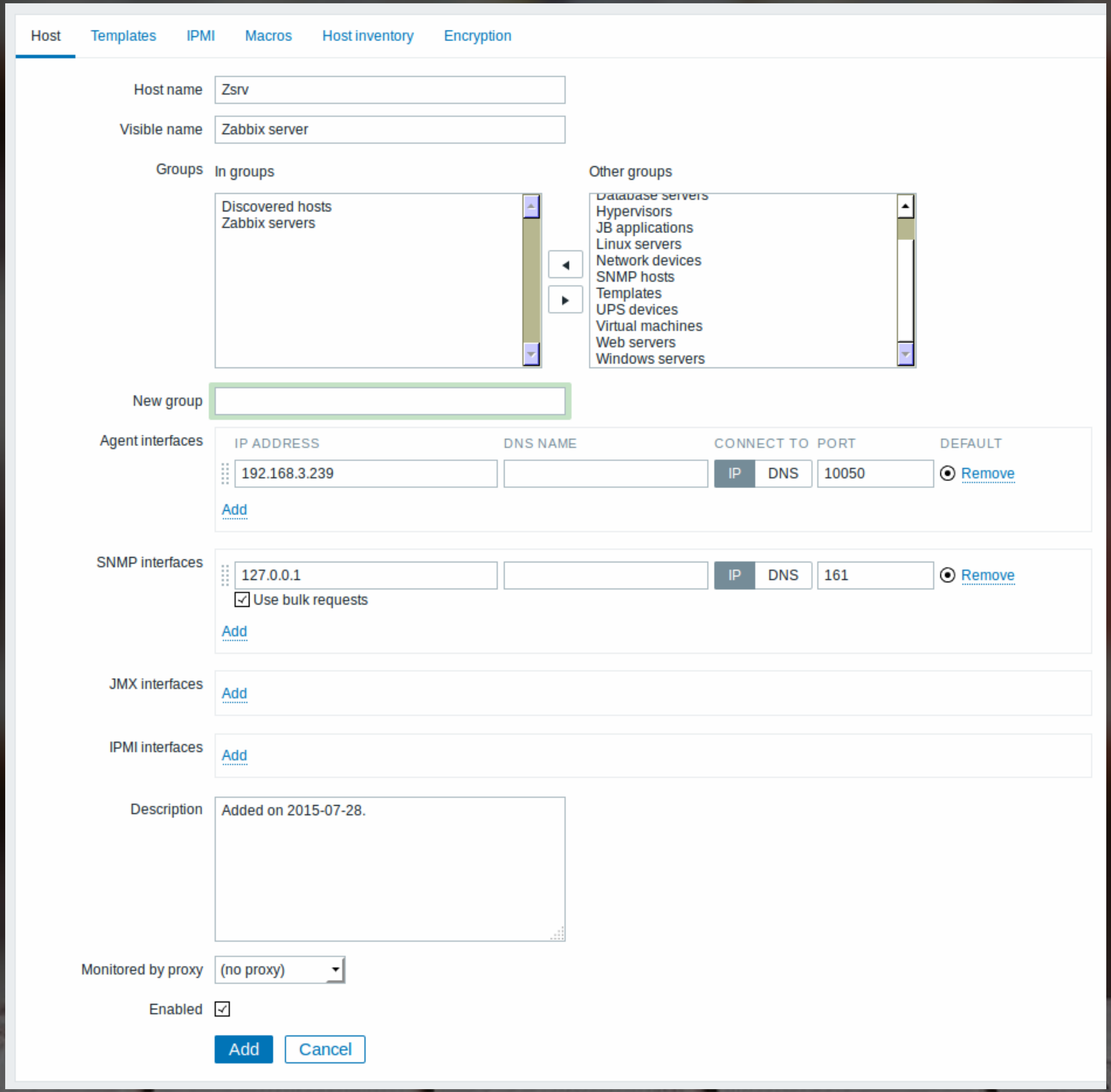



```
/system logging
add action=remote topics=critical
add action=remote topics=error
add action=remote topics=info
add action=remote topics=warning
```


Logging
Rules
Actions
Find
Action
contains
remote
Filter
Topics
Prefix
Action
critical
remote
error
remote
info
remote
warning
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
Zsrv
Visible name
Zabbix server
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
192.168.3.239
IP
DNS
10050
Remove
Add
SNMP interfaces
127.0.0.1
IP
DNS
161
Remove
Use bulk requests
Add
JMX interfaces
Add
IPMI interfaces
Add
Description
Added on 2015-07-28.
Monitored by proxy
(no proxy)
Enabled
Add
Cancel

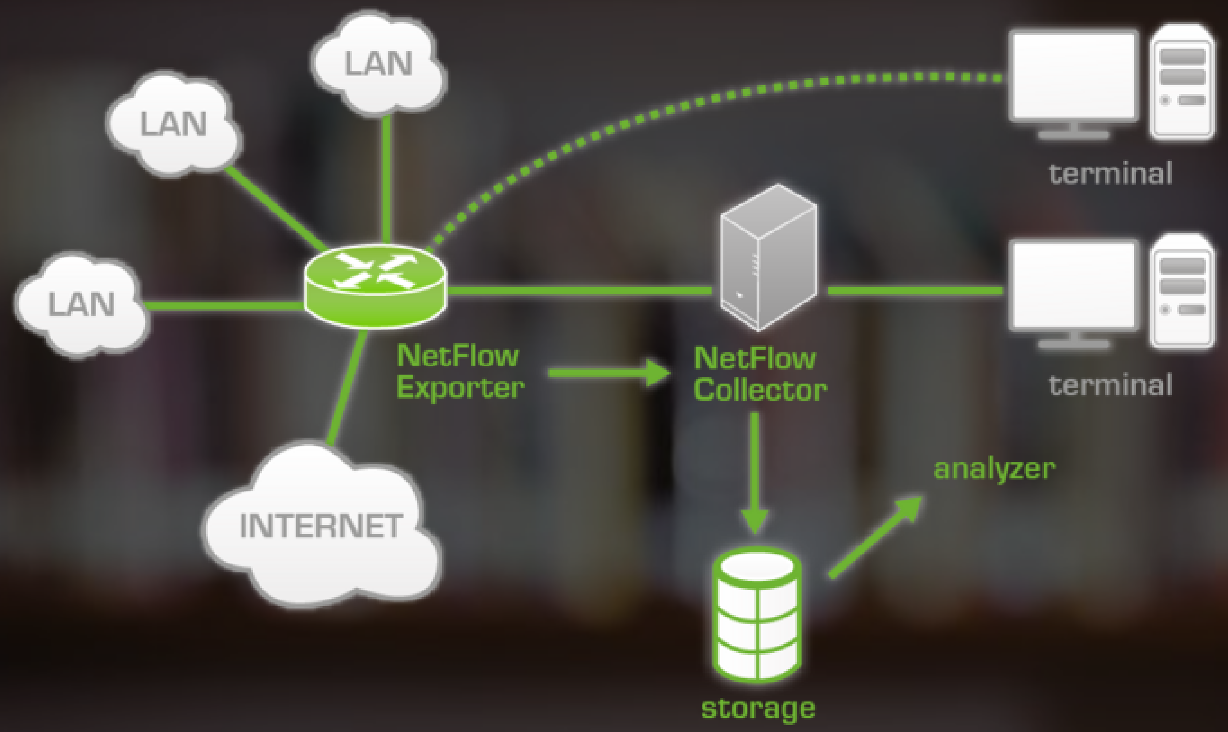
Existen clientes para exportar historicos de datos desde zabbix a bases de datos de series temporales.

https://github.com/jojohappy/zabbix-relay

Podemos integrar los eventos de zabbix como entrada a logstach, 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.


LAN
LAN
LAN
INTERNET
NetFlow Exporter
NetFlow Collector
terminal
terminal
analyzer
storage

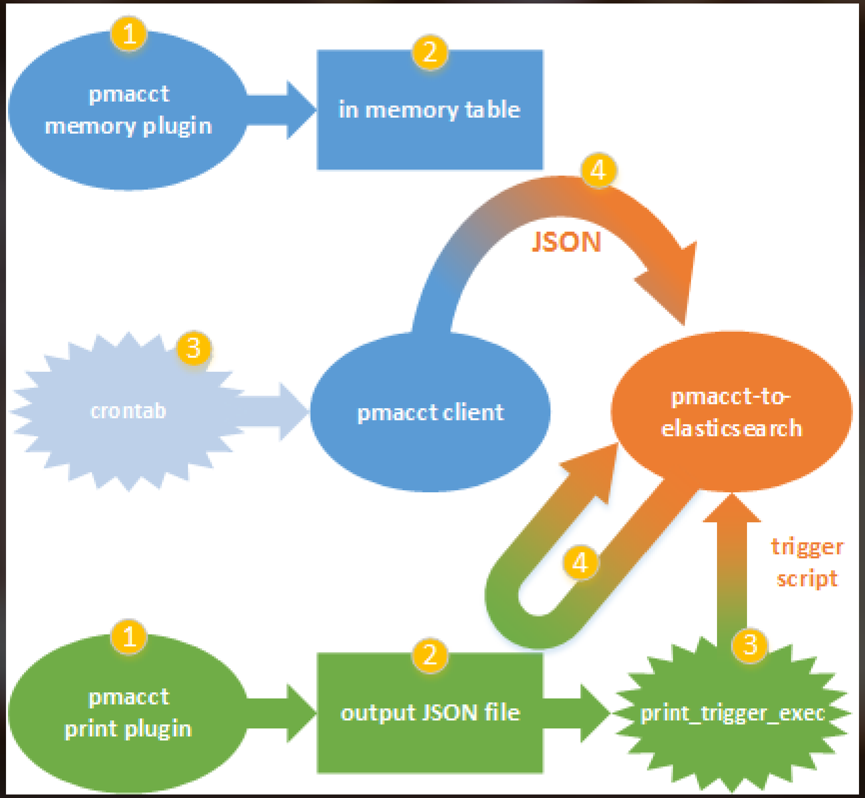
/ip traffic-flow set active-flow-timeout=30m cache-entries=1M \enabled=yes inactive-flow-timeout=15s interfaces=all

```
/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.

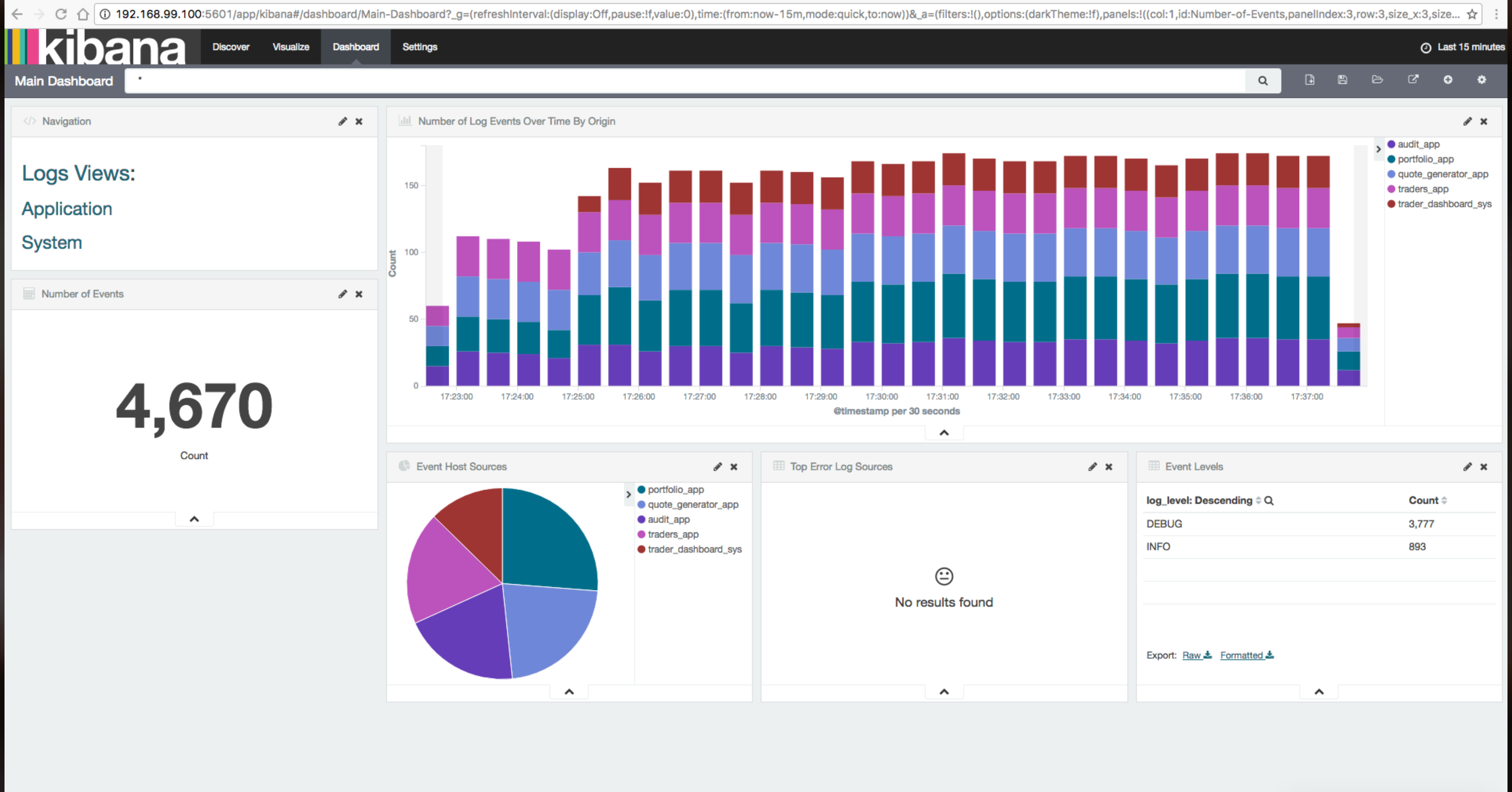
Una vez que recogemos los logs con pcmacct vamos a enviar las salida a en formato json a ElasticSearch.

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



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


kibana
Discover
Visualize
Dashboard
Settings
1 minute
Last 24 hours
silicon - Firewall Events
Blocked - By GeoIP
Packets Blocked - IPv6
679
Count
Packets Blocked - IPv4
10,494
Count
Blocked - By Country
Count
United States
United Kingdom
China
Taiwan
Netherlands
France
Germany
Russian Federation
India
Argentina
Brazil
Malaysia
Hong Kong
Korea, Republic of
Poland
Turkey
Italy
Moldova, Republic of
Ukraine
Canada
geoip.country_name.raw: Descending
Leaflet | Tiles by MapQuest — Map data © OpenStreetMap contributors, CC-BY-SA
Firewall - Events by Time
Count
@timestamp per 30 minutes
Blocked - By Protocol
Legend
TCP
UDP
Blocked - By Interface
Legend
em0 - LAN
em1 - MGMT
em5 - W.WiFi
em6 - Guest
em7 - WAN
Blocked - By IP Version
Legend
IPv4
IPv6
Blocked - By Port
Legend
443
137
80
389
138
993

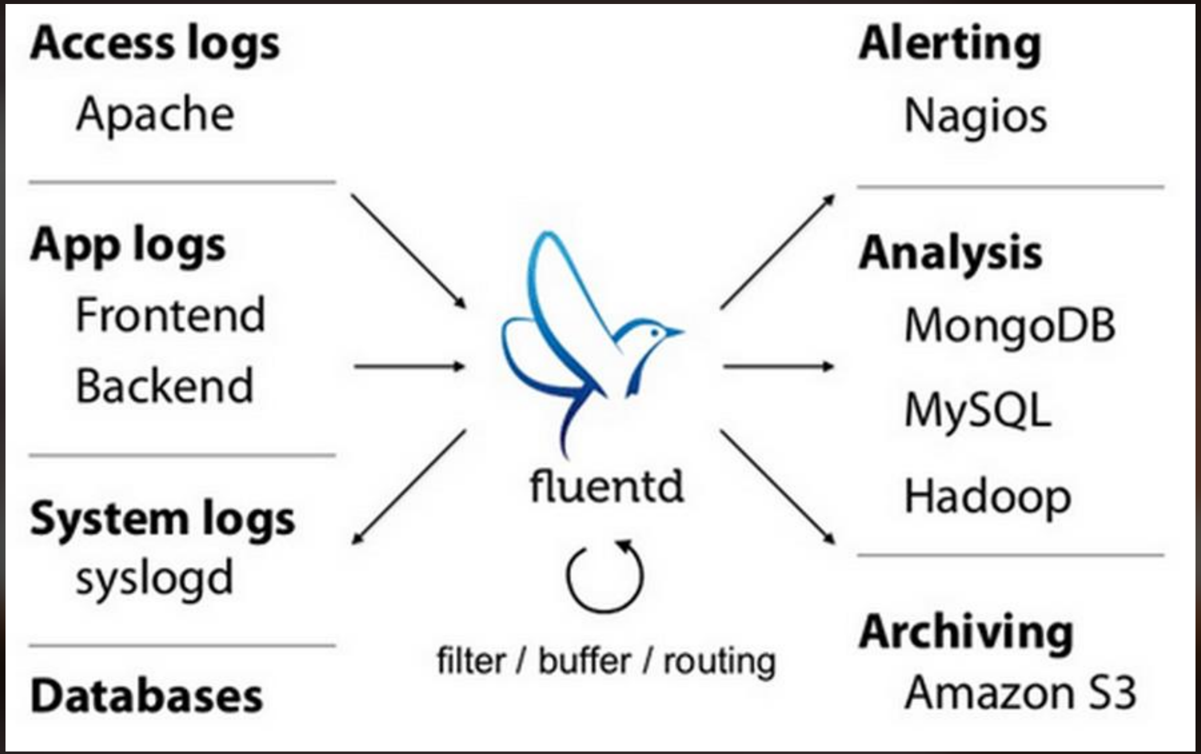

kibana
Discover
Visualize
Dashboard
Settings
Last 15 minutes
Main Dashboard
Navigation
Logs Views:
Application
System
Number of Events
4,670
Count
Number of Log Events Over Time By Origin
Count
@timestamp per 30 seconds
audit_app
portfolio_app
quote_generator_app
traders_app
trader_dashboard_sys
Event Host Sources
Top Error Log Sources
No results found
Event Levels
log_level: Descending
Count
DEBUG
3,777
INFO
893
Export: Raw Formatted

Recursos adicionales

Grafana

Influxdb

Fluentd


Access logs
Apache
App logs
Frontend
Backend
System logs
syslogd
Databases
fluentd
filter / buffer / routing
Alerting
Nagios
Analysis
MongoDB
MySQL
Hadoop
Archiving
Amazon S3

Muchas gracias