

System integration and analysis

By José M. Román

FiberCli

We are pure fiber

JOSE MANUEL ROMAN

17 years experience, Mikrotik Certified Consultant and Trainer. MTCNA, MTCRE, MTCTCE, MTCUME, MTCWE, MTCINE, CISA, CISSP, Master ITIL

- (Now) CEO at Fibercli
- (2015 – Now) CEO @ WISP Cloud Networking Spain
- (2008 – Now) Security Consultant and Analyst
- ***(2000 – 2007) Networking, security and itil teacher.***



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

Fiber optic key projects
Level 3 support 24 x 7 for ISP's
Mikrotik certifications
System and software integration



20% Discount for MUM assistant



Problem

Multiple events on the network as a system administrator or network administrator we don't know locate the source.



Symptom

Multiple incidents that are not managed.
Feeling of lack of control over the network.



Solution

Centralized system to collect, normalize,
visualization and analysis



AGENDA

- Intro
- Architecture
- ELK (ElasticSearch, Logstash, Kibana)
- Mkt + AAA+ with Freeradius and DB centralized
- Mkt + Centralized Log and ELK
- Mkt + Monitoring and ELK
- Mkt + Netflow and ELK
- Q and A

¿What is? **ELK**



Elasticsearch

Elasticsearch is a search engine based on Lucene. It provides a distributed, multitenant-capable full-text search engine with an HTTP web interface and schema-free JSON documents.



Elasticsearch

Elasticsearch is developed in Java and is released as open source under the terms of the Apache License



Elasticsearch

- Distributed, scalable, and highly available
 - Real-time search and analytics capabilities
 - Sophisticated RESTful API
-
- <https://www.elastic.co/products/elasticsearch>



Elasticsearch

- **Schema-free, REST & JSON based distributed search engine**
- **Open Source: Apache License 2.0**
- **Easy to understand, yet very powerful query language**

Full text search (phrase, fuzzy)

Numeric search (support ranges, dates, ipv4 addresses)

Highlighting

Aggregations

Suggestions



Logstash

Logstash is a tool to collect, process, and forward events and log messages. Collection is accomplished via configurable input plugins including raw socket/packet communication, file tailing, and several message bus clients.



Logstash

- Centralize data processing of all types
 - Normalize varying schema and formats
 - Quickly extend to custom log formats
 - Easily add plugins for custom data sources
-
- <https://wikitech.wikimedia.org/wiki/Logstash>



Logstash

- 
- **Inputs:** collect data from variety of sources
 - **Filters:** parse, process and enrich data
 - **Outputs:** push data to a variety of destinations

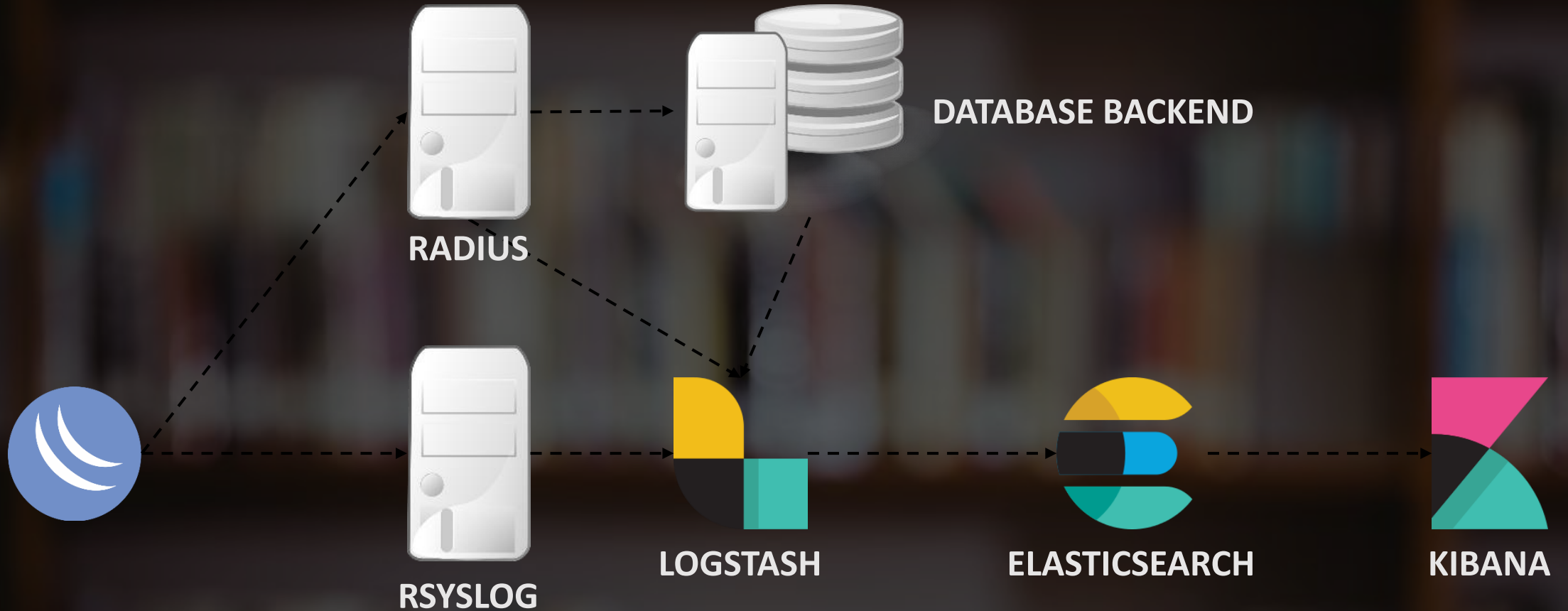


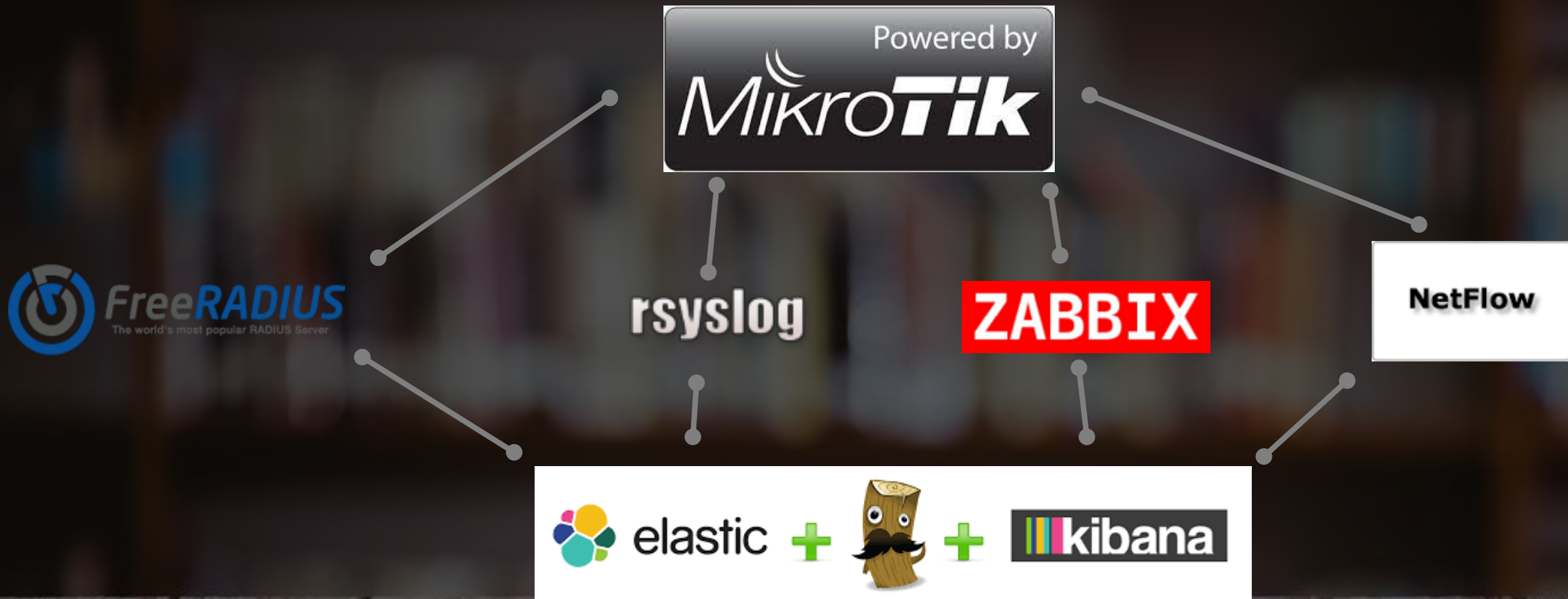
Kibana



- Execute queries on your data & visualize results
- Add/remove widgets
- Share/Save/Load dashboards
- Open Source: Apache License 2.0

Big Picture





AAA System



Radius

RADIUS is an application level protocol that carries Authentication, Authorization and Accounting (AAA) configuration information between a Network Access Server (NAS) and a Shared Authentication Server. Radius defined in RFC 2865



Radius

In MikroTik RouterOS itself support RADIUS for Hotspot, PPP, DHCP, Wireless and Login. RADIUS using transport protocol UDP.

UDP Port 1812 – Authentication

UDP Port 1813 – Accounting



Radius

RADIUS operation typically split into three type :

- Dial-In User : User who requesting for login and password
- Network Access Server (NAS) / RADIUS Client : Device who accept the request from dial-in user and
: Forward into RADIUS Server.
- Shared Authentication Server / RADIUS Server : Device who make a decision for request (Accept, Reject or Challenge)





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)

Accounting-Response

Disconnect



Topology

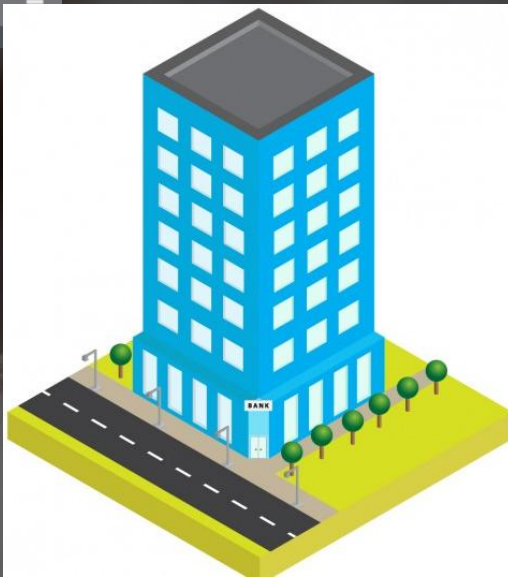




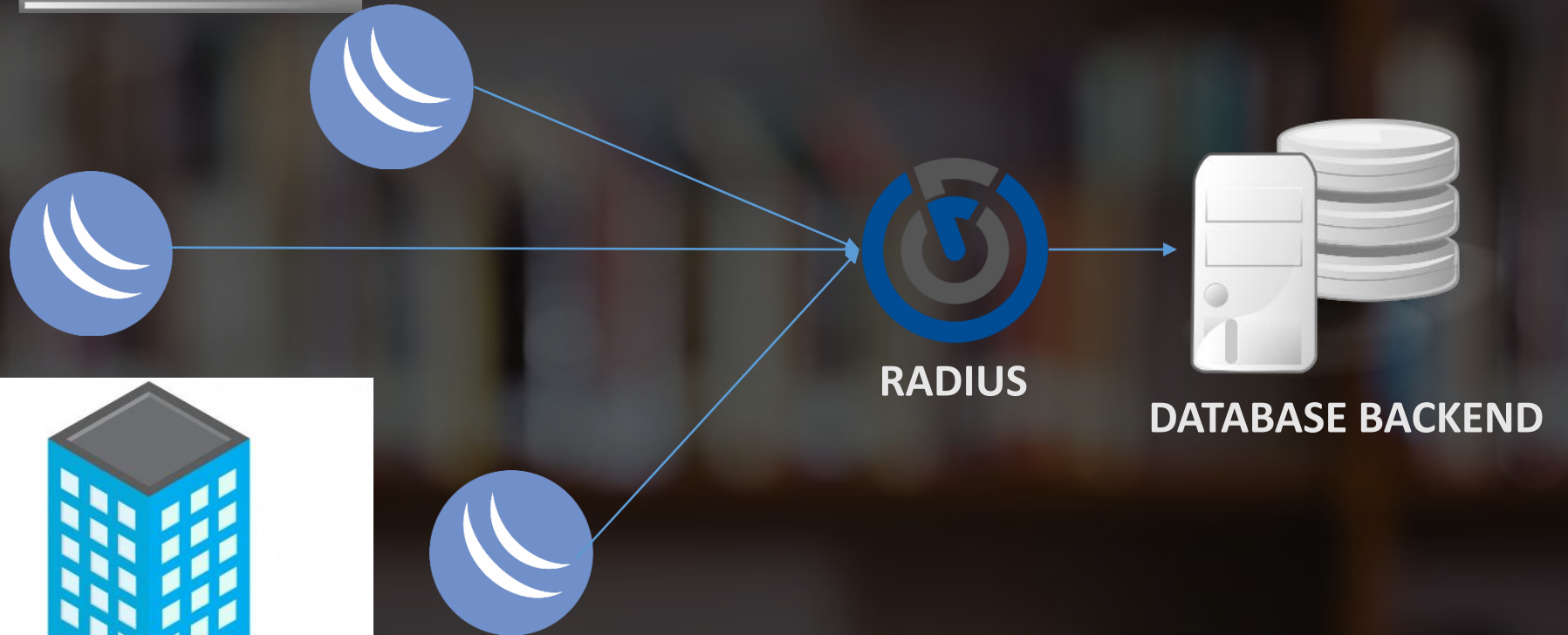
MIKROTIK SITE 2



MIKROTIK SITE 3



MIKROTIK SITE 1



Radius

Buttons: +, -, ✓, ✗, 📁, 🔍, Reset Status, Incoming, Find

#	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: 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

Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove, Reset Status



service (ppp|login|hotspot|wireless|dhcp; Default:)

- *hotspot* - HotSpot authentication service
- *login* - router's local user authentication
- *ppp* - Point-to-Point clients authentication
- *wireless* - wireless client
- *dhcp* - DHCP protocol client authentication

Address (IPv4/IPv6 address; Default: 0.0.0.0) IPv4 or IPv6 address of RADIUS server.

Secret (string; Default:) Shared secret used to access the RADIUS server.



Freeradius produces several logs that we can process with logstash

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




```
# Tue Mar 10 15:32:24 2015
12# Packet-Type = Access-Request
13# User-Name = "test@example.com"
14# Calling-Station-Id = "01-02-03-04-05-06"
15# Called-Station-Id = "aa-bb-cc-dd-ee-ff:myssid"
16# NAS-Port = 10
17# NAS-IP-Address = 10.9.0.4
18# NAS-Identifier = "Wireless-Controller-1"
19# Service-Type = Framed-User
20# NAS-Port-Type = Wireless-802.11
21#
```

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



```
26input {  
27  stdin {  
28    type => radiusdetail  
29  }  
30}
```

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




```
filter {
34
35   if [type] == "radiusdetail" {
36
37       # join all lines of a record together
38       multiline {
39           pattern => "^[^\\t]"
40           negate => true
41           what => "previous"
42       }
43
44       # pull off the timestamp
45       grok {
46           match => [ "message", "%{?timestamp>[^\n\\t]+}[\\n\\t]" ]
47       }
48
49       # create the timestamp field
50       date {
51           match => [ "timestamp", "%EEE MMM dd HH:mm:ss yyyy",
52                   "%EEE MMM d HH:mm:ss yyyy" ]
53       }
54
55       # split the attributes and values into fields
56       kv {
57           field_split => "\\n"
58           source => "message"
59           trim => "\\ "
60           trimkey => "\\t "
61       }
62   }
63}
```

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



```
65output {  
66  if [type] == "radiusdetail" {  
67    elasticsearch {  
68      host => localhost  
69      protocol => http  
70      cluster => elasticsearch  
71      index_type => "detail"  
72      index => "radius-%{+YYYY.MM.dd}"  
73      flush_size => 1000  
74    }  
75  }  
76}
```

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



Centralize Log



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

- Protocol supported by rsyslog are:
- ISO 8601 timestamp with millisecond granularity and timezone information
- The addition of the name of relays in the host fields to make it possible to track the path a given message has traversed
- Reliable transport using TCP
- Support GSS-API and TLS



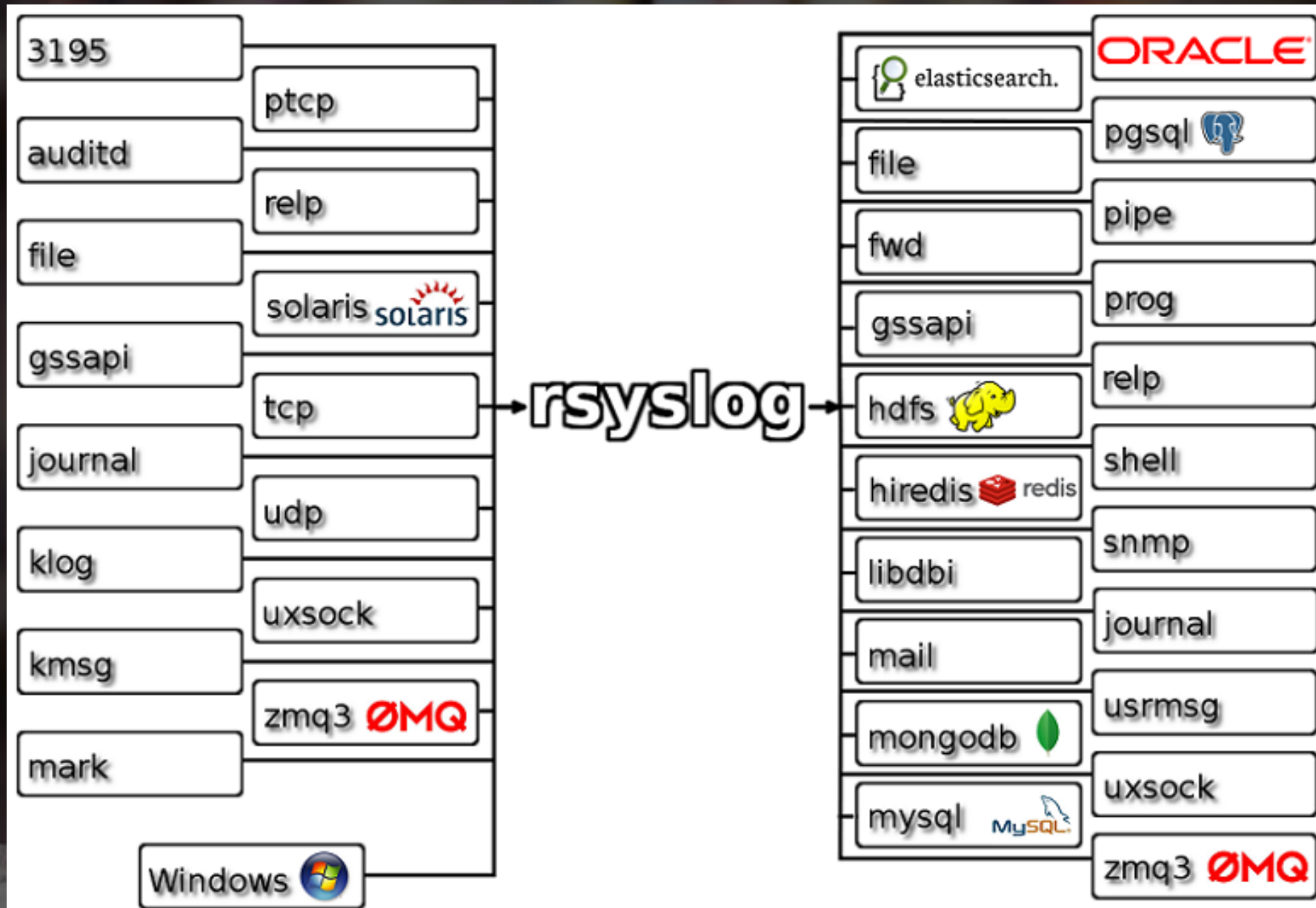
RSYSLOG

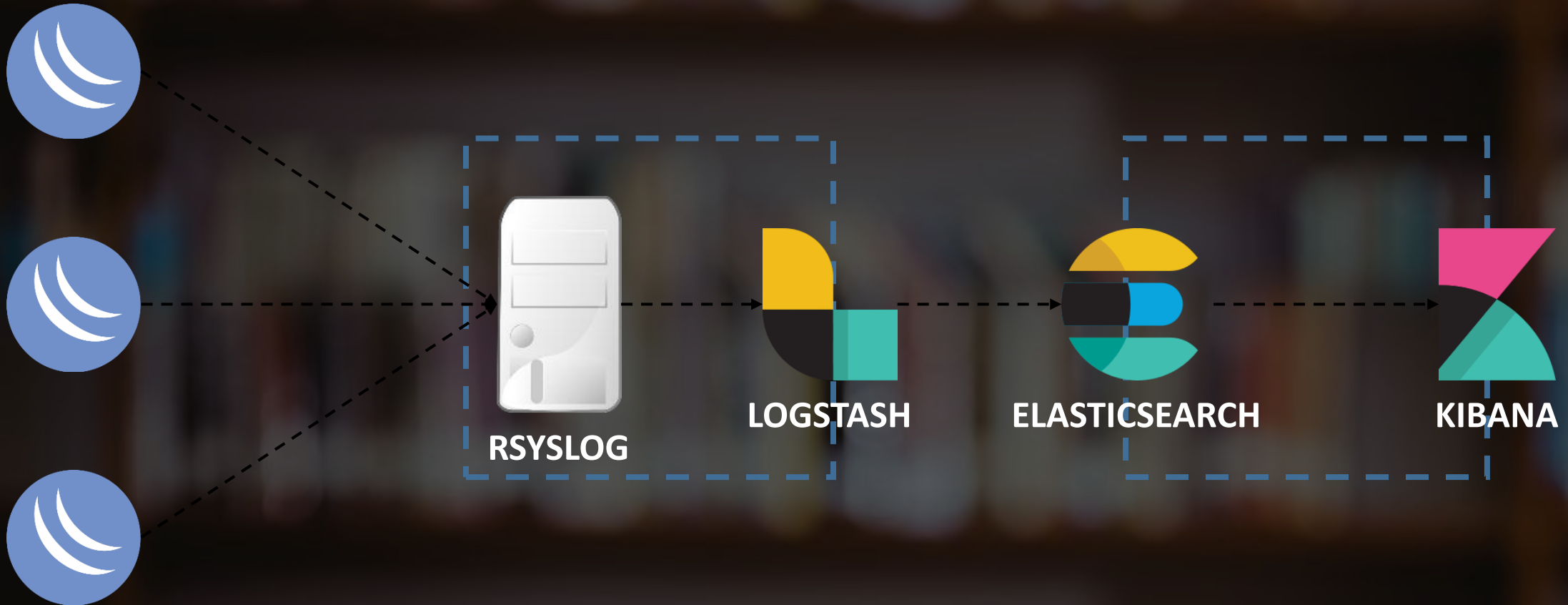
- Logging directly into various database engines.
- Support for RFC 5424, RFC 5425, RFC 5426
- Complete input/output support for systemd journal



Topology







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:

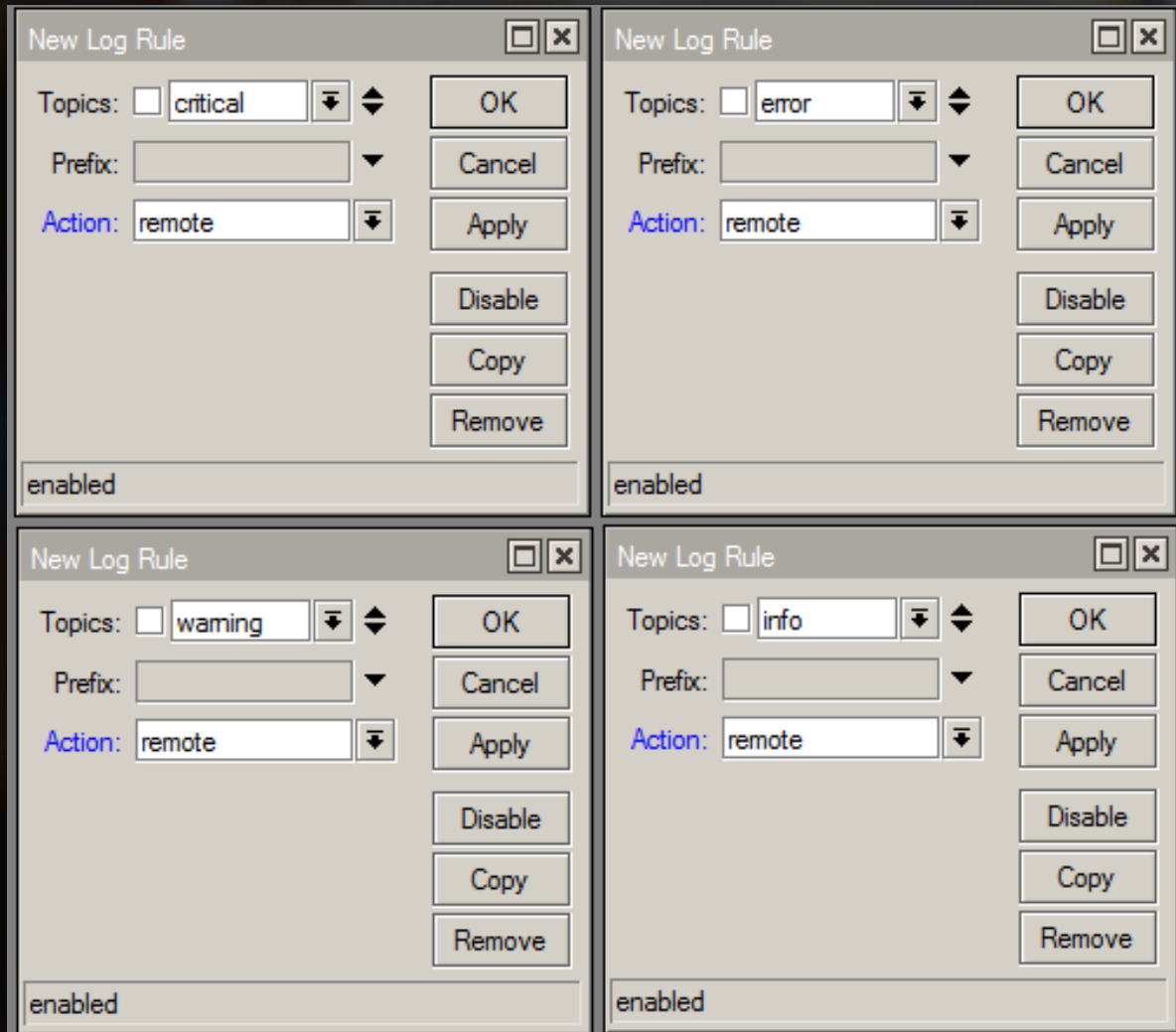
default

OK Cancel Apply Copy Remove

4 items (1 selected)

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





The image displays four instances of the 'New Log Rule' dialog box, arranged in a 2x2 grid. Each dialog box has a title bar with a close button (X) and a checkbox. The main area contains three input fields: 'Topics' (with a dropdown arrow), 'Prefix' (with a dropdown arrow), and 'Action' (with a dropdown arrow). Below these fields are five buttons: 'OK', 'Cancel', 'Apply', 'Disable', and 'Copy'. At the bottom of each dialog is a 'Remove' button. The status bar at the bottom of each dialog shows 'enabled'.

- Top-left dialog: Topics: ☐ critical
- Top-right dialog: Topics: ☐ error
- Bottom-left dialog: Topics: ☐ warning
- Bottom-right dialog: Topics: ☐ info

In all four dialogs, the 'Prefix' field is empty and the 'Action' field is set to 'remote'.

```
/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)



Monitoring




```
/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
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

Monitored by proxy

Enabled ☒



There are clients to export data to databases like fluentdb.

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



We can integrate Zabbix events as input in Logstash, with the goal to have a decoupled monitorization.

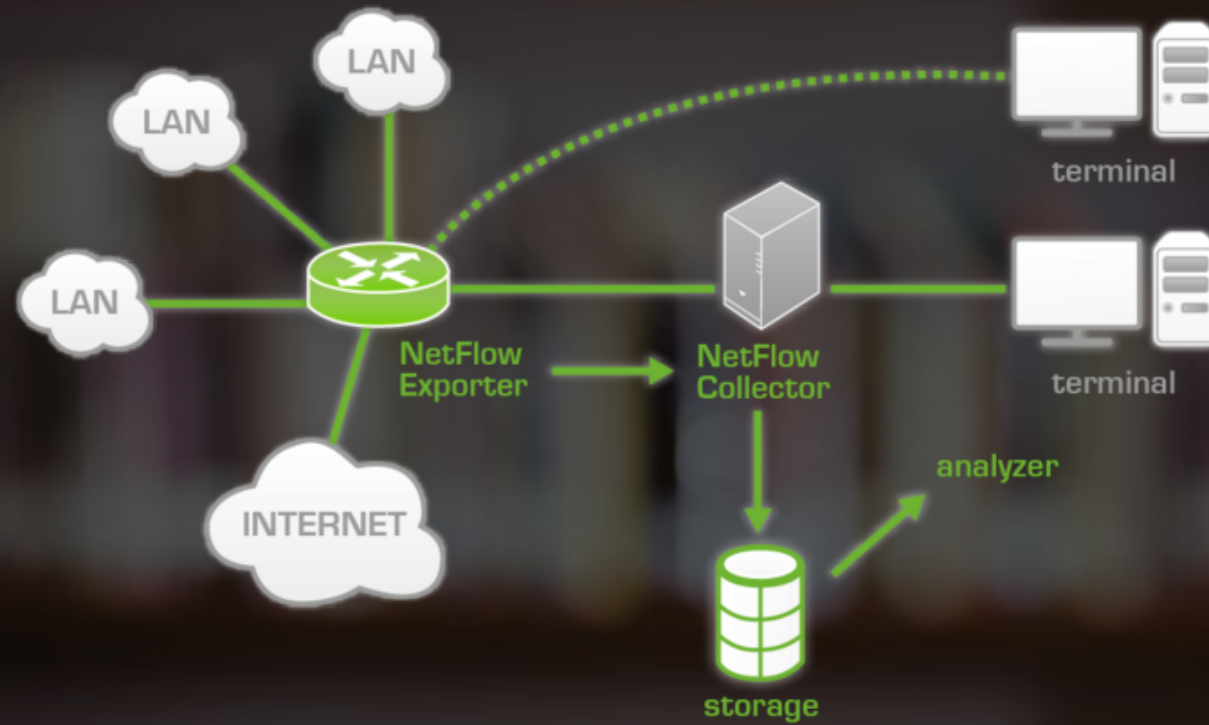


Netflow



NetFlow is a network protocol created by [Cisco Systems](#) to collect information about ip traffic.





```
/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
```



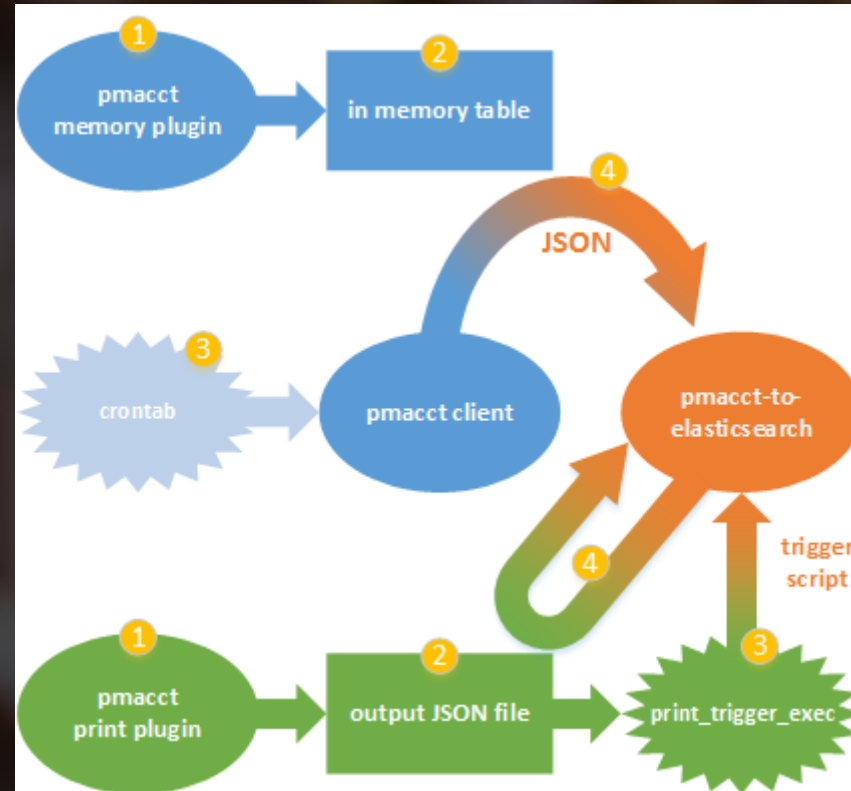
To collect the output we need a netflow collector, for example pmacctsonda.



When we collect the logs with pmacct we'll send the output in json format to ElasticSearch.

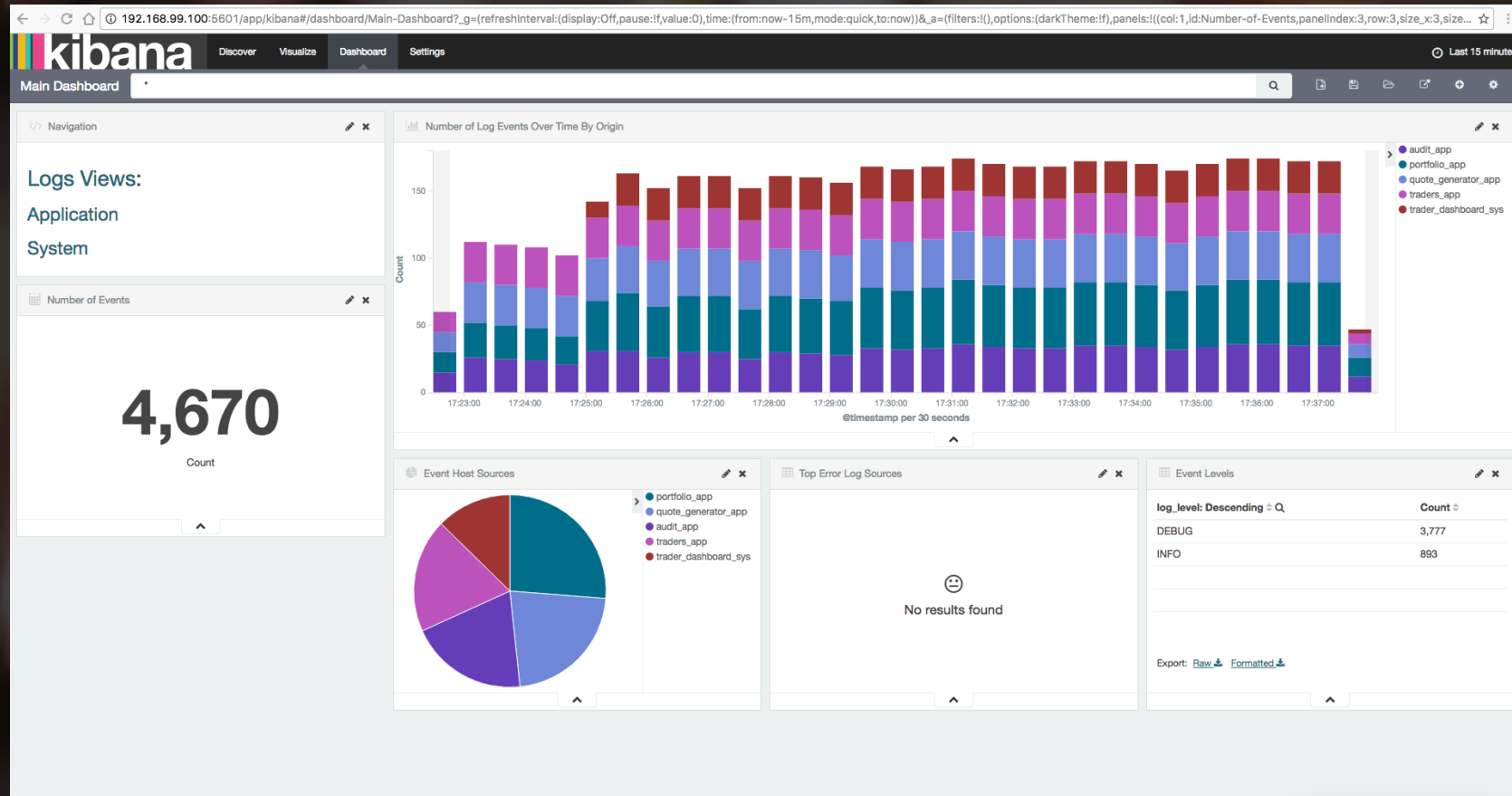
<https://github.com/pierky/pmacct-to-elasticsearch/blob/master/CONFIGURATION.md>





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





Additional resources



Grafana

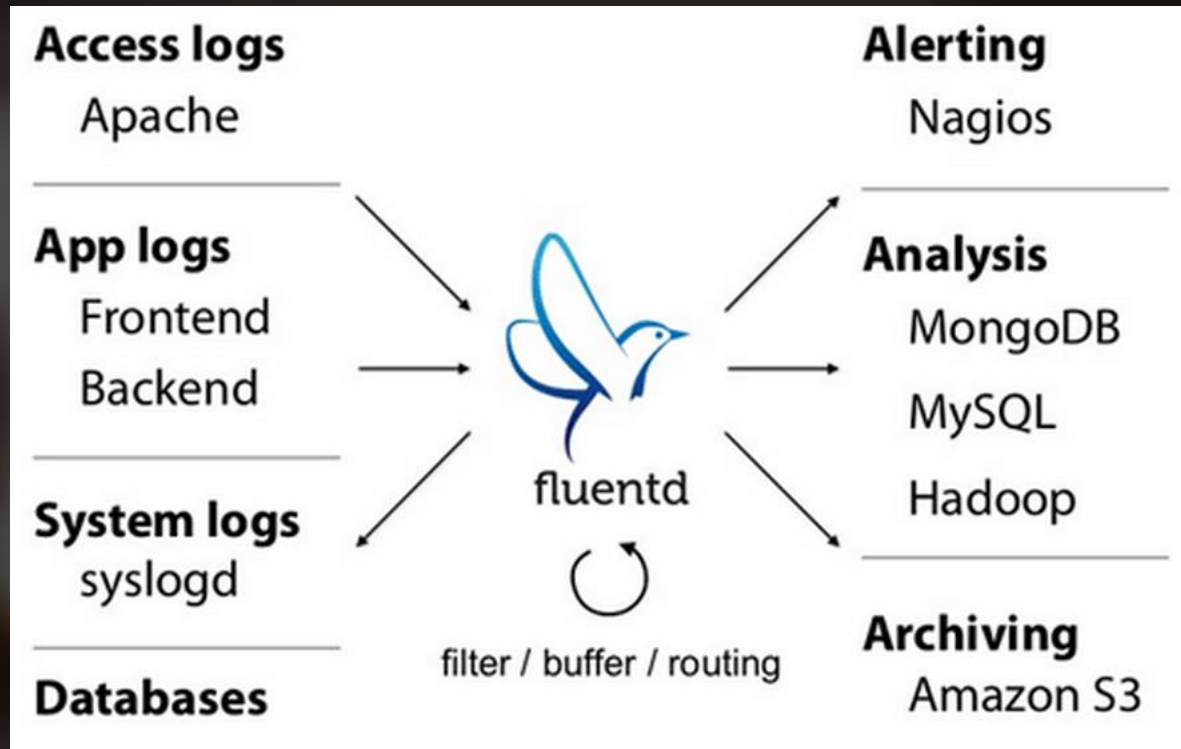


Influxdb



Fluentd





Thank you



jose.roman@fibercli.com

www.fibercli.com

