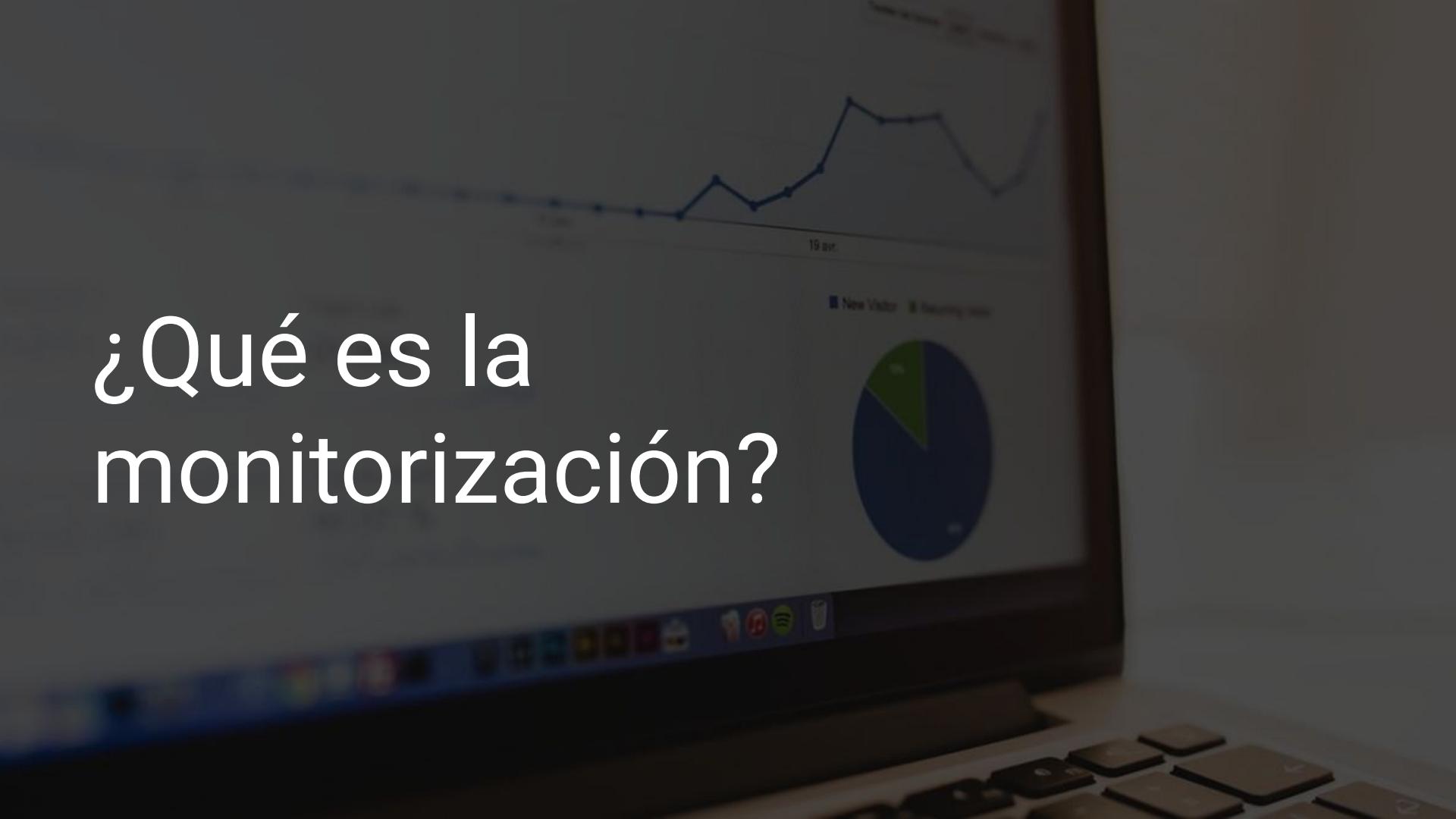




Evaristo R. Rivieccio Vega

¿Qué es la monitorización?

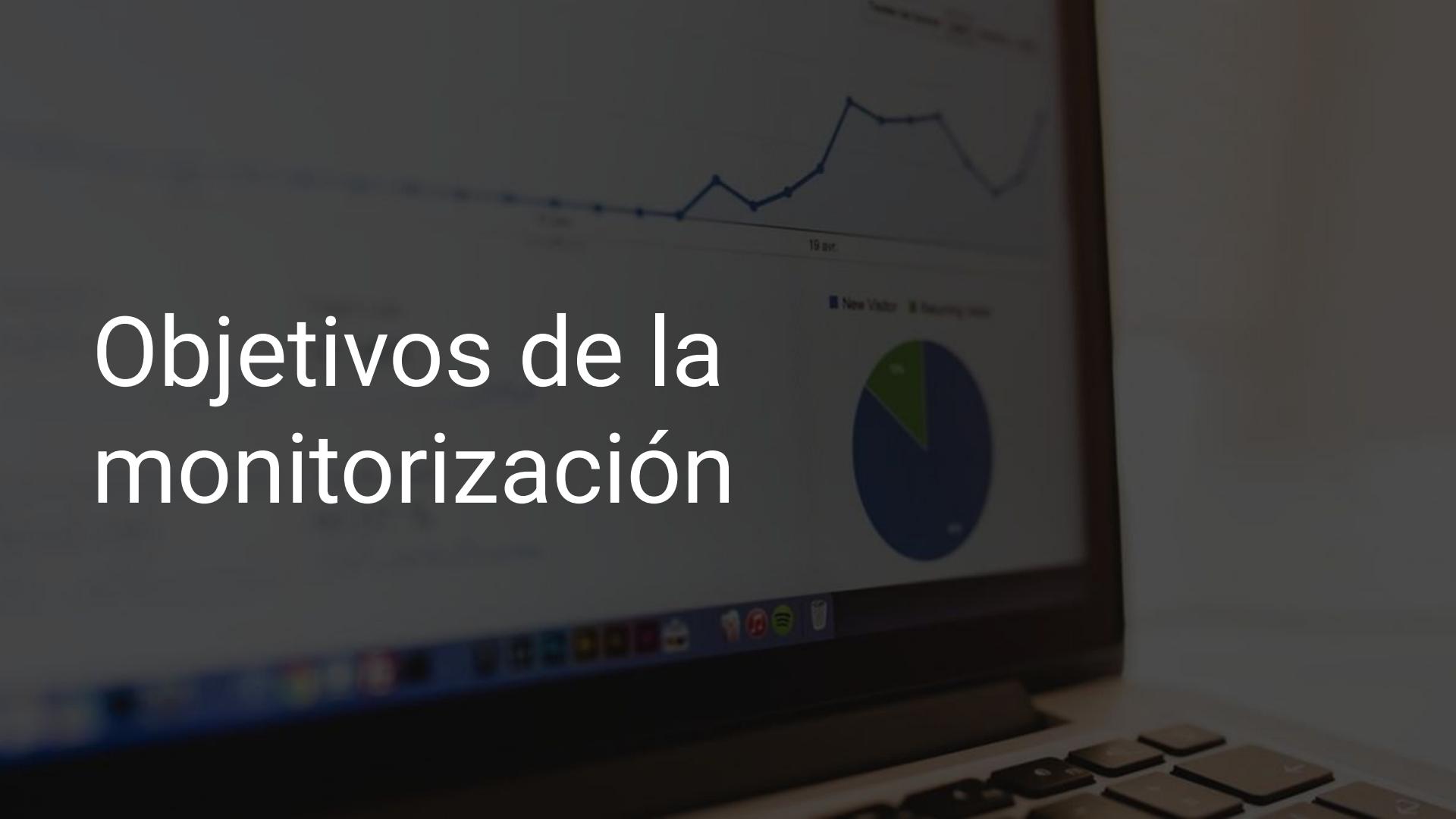


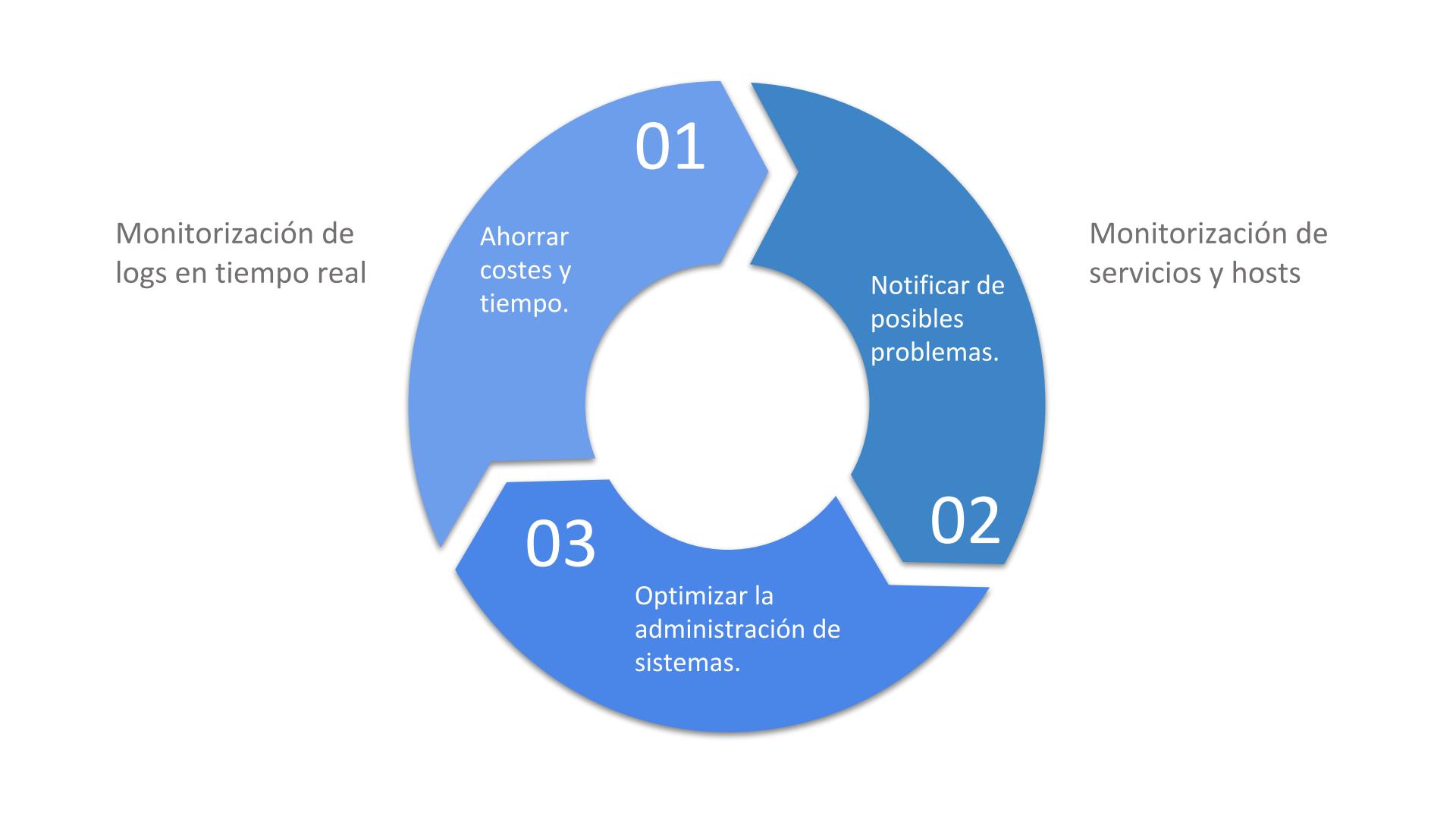
¿Qué es la monitorización?

Monitorización o monitoreo generalmente significa **ser consciente del estado de un sistema, para observar una situación de cambios que se pueda producir con el tiempo.**



Objetivos de la monitorización





Monitorización de logs en tiempo real

01

Ahorrar costes y tiempo.

Notificar de posibles problemas.

02

Optimizar la administración de sistemas.

03

Monitorización de servicios y hosts

Evolución y tendencias de las herramientas de monitorización



1.^a Generación

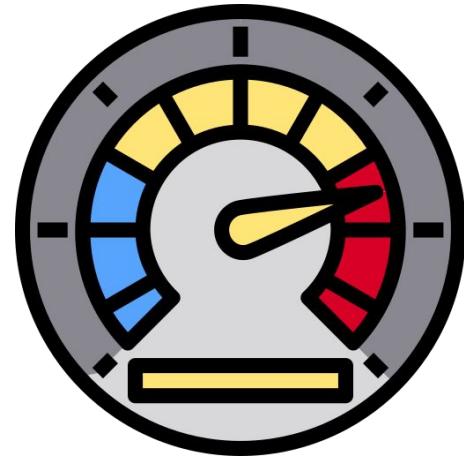
Aplicaciones para monitorizar dispositivos activos o inactivos.



2.^a Generación

Aplicaciones de análisis de métricas.

Análisis para poder evaluar los estados de los componentes dentro de los dispositivos (CPU, memoria, espacio de almacenamiento, paquetes enviados y recibidos...)

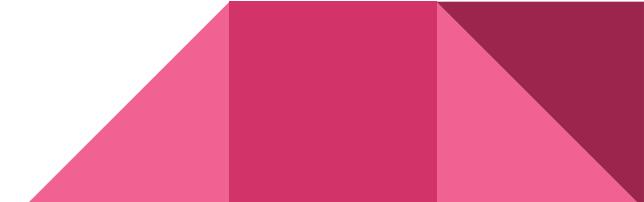


3.^a Generación

Aplicaciones de análisis optimizado.

Esta generación captura “flujos” de tráfico e identifica cuellos de botella y latencias a lo largo de las conexiones.

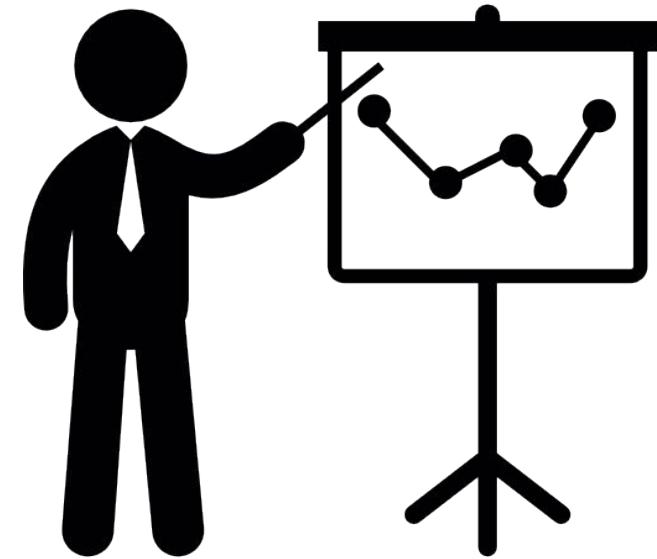
Se logra conectar todas las partes de manera eficiente, evitando así una sobrecarga de información



4.^a Generación

Debido a los requerimientos de las organizaciones de hoy, llegamos a las vistas de “dashboard”.

Indicadores que el cliente puede crear y personalizar para apoyarse en la **toma de decisiones**.



Tipos de monitorización



Monitorización predictiva

- Ayuda a anticiparnos al problema.
- Ofrece datos reales de la plataforma.
- Permite tomar decisiones.
- Posibilita un trabajo de revisión continuada.

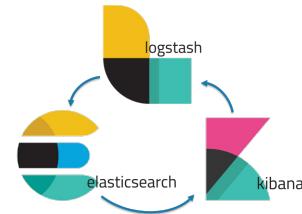
Monitorización proactiva

- Detecta los problemas.
- Soluciona los problemas.
- Dar respuestas al día a día.
- Suplir los problemas por falta de personal.

Herramientas de monitorización.



Nagios®





GPL(GNU)

(Creado por Ethan Galstad)
Estándar de la industria de
la monitorización desde
1999.

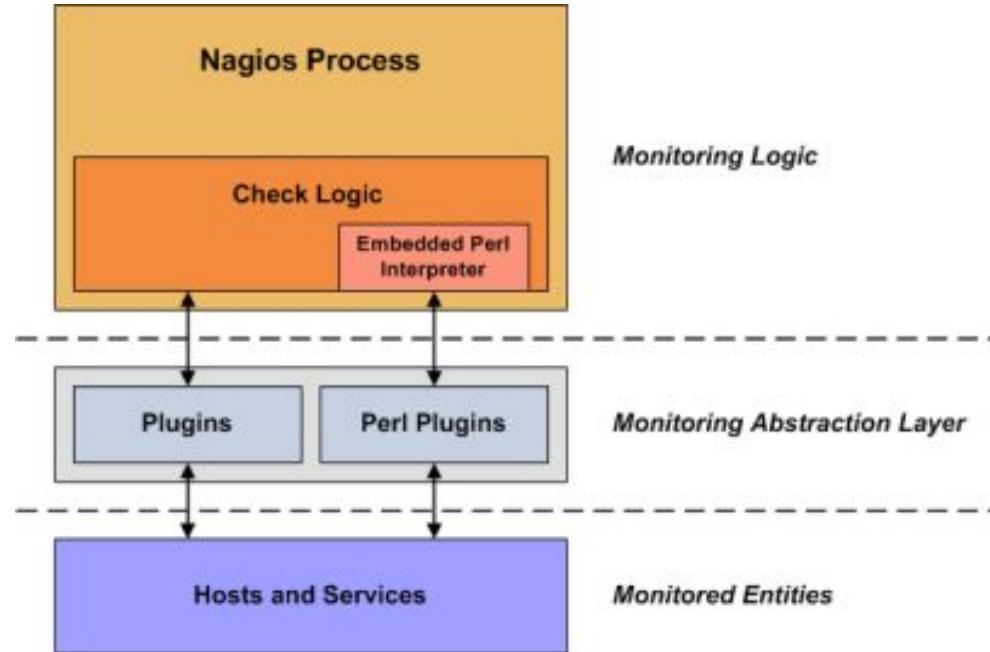
Monitorización de servicios
de red y de los recursos de
sistemas hardware.

Nagios

- General
 - Home
 - Documentation
- Monitoring
 - Tactical Overview
 - Service Detail
 - Host Detail
 - Status Overview
 - Status Summary
 - Status Grid
 - 3-D Status Map
 - Service Problems
 - Host Problems
 - Network Outages
 - Comments
 - Downtime
- Process Info
- Performance Info
- Scheduling Queue
- Reporting
 - Trends
 - Availability
 - Alert Histogram
 - Alert History
 - Alert Summary
 - Notifications
 - Event Log
- Configuration
 - View Config

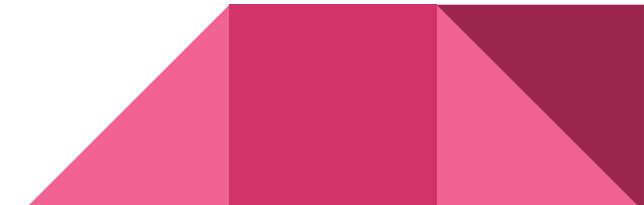
Monitoring						
webprod03	Check_Users	OK	01-26-2007 14:58:59	0d 0h 53m 23s	1/4	USERS OK - 1 users currently logged in
	Current Load	OK	01-26-2007 14:59:54	0d 0h 53m 23s	1/4	OK - load average: 0.21, 0.08, 0.05
	Memory Usage	OK	01-26-2007 14:55:29	0d 0h 53m 23s	1/4	OK: Memory Usage 56% - Total: 511 MB, Used: 287 MB, Free: 224 MB
	PING	OK	01-26-2007 14:56:14	0d 0h 50m 23s	1/4	PING OK - Packet loss = 0%, RTA = 0.16 ms
	Root Partition	OK	01-26-2007 14:57:09	0d 0h 50m 33s	1/4	DISK OK [243816 kB (5%) free on /dev/sda2]
	SWAP Usage	OK	01-26-2007 14:57:44	0d 0h 50m 33s	1/4	Swap ok - (null) 0% (0 out of 16386)
	Total Processes	OK	01-26-2007 14:58:29	0d 0h 50m 33s	1/4	OK - 95 processes running
	Xen Virtual Machine Monitor	CRITICAL	01-26-2007 14:59:04	0d 0h 44m 34s	1/4	Critical Xen VMs Usage - Total NB: 0 - detected VMs:
webprod04	Check_Users	OK	01-26-2007 14:59:54	0d 0h 15m 33s	1/4	USERS OK - 2 users currently logged in
	Current Load	OK	01-26-2007 14:55:34	0d 0h 14m 53s	1/4	OK - load average: 0.30, 0.60, 0.44
	Memory Usage	OK	01-26-2007 14:56:19	0d 0h 14m 13s	1/4	OK: Memory Usage 37% - Total: 511 MB, Used: 190 MB, Free: 321 MB
	PING	OK	01-26-2007 14:57:10	0d 0h 13m 23s	1/4	PING OK - Packet loss = 0%, RTA = 0.27 ms
	Root Partition	OK	01-26-2007 14:57:49	0d 0h 12m 34s	1/4	DISK OK [3948940 kB (94%) free on /dev/sda2]
	SWAP Usage	OK	01-26-2007 14:58:34	0d 0h 11m 53s	1/4	Swap ok - (null) 0% (0 out of 16386)
	Total Processes	OK	01-26-2007 14:59:09	0d 0h 16m 22s	1/4	OK - 250 processes running
	Xen Virtual Machine Monitor	WARNING	01-26-2007 14:58:54	0d 0h 1m 33s	1/4	Warning: Xen VMs Usage - Total NB: 1 - detected VMs: migrating-xen-vm4
webprod05	PING	OK	01-26-2007 14:55:39	0d 0h 24m 58s	1/4	PING OK - Packet loss = 0%, RTA = 0.25 ms
	Xen Virtual Machine Monitor	OK	01-26-2007 14:59:54	0d 0h 0m 33s	1/4	OK: Xen Hypervisor "webprod05" is running 4 Xen VMs: xen-vm1 xen-vm2 xen-vm3 xen-vm4
xen-vm1	Check_Users	OK	01-26-2007 14:58:09	0d 0h 17m 23s	1/4	USERS OK - 1 users currently logged in
	Current Load	OK	01-26-2007 14:57:54	0d 0h 16m 21s	1/4	OK - load average: 1.54, 1.09, 0.48
	Memory Usage	OK	01-26-2007 14:58:39	0d 0h 15m 41s	1/4	OK: Memory Usage 8% - Total: 8195 MB, Used: 676 MB, Free: 7519 MB
	PING	OK	01-26-2007 14:59:15	0d 0h 15m 21s	1/4	PING OK - Packet loss = 0%, RTA = 0.49 ms
	Root Partition	OK	01-26-2007 14:59:59	0d 0h 14m 51s	1/4	DISK OK [4196280 kB (99%) free on udev]
	SWAP Usage	OK	01-26-2007 14:55:44	0d 0h 14m 1s	1/4	Swap ok - (null) 0% (0 out of 2055)
	Total Processes	OK	01-26-2007 14:57:29	0d 0h 18m 3s	1/4	OK - 86 processes running
xen-vm2	Check_Users	OK	01-26-2007 14:57:15	0d 0h 3h 7m 41s	1/4	USERS OK - 0 users currently logged in
	Current Load	OK	01-26-2007 14:57:59	0d 0h 3h 7m 1s	1/4	OK - load average: 0.00, 0.00, 0.00
	Memory Usage	OK	01-26-2007 14:58:44	0d 0h 6m 21s	1/4	OK: Memory Usage 6% - Total: 1023 MB, Used: 64 MB, Free: 958 MB
	PING	OK	01-26-2007 14:59:19	0d 0h 48m 14s	1/4	PING OK - Packet loss = 0%, RTA = 0.43 ms
	Root Partition	OK	01-26-2007 15:00:05	0d 0h 15m 4s	1/4	DISK OK [524220 kB (99%) free on udev]
	SWAP Usage	OK	01-26-2007 14:55:49	0d 0h 9m 41s	1/4	Swap ok - (null) 0% (0 out of 2055)
	Total Processes	OK	01-26-2007 14:56:34	0d 0h 9m 1s	1/4	OK - 52 processes running

Nagios®



Nagios[®]

- Nagios base está extremadamente limitado en funcionalidades de serie.
- Su configuración es estática, engorrosa. La escalabilidad no es el punto fuerte de Nagios.





GPL(GNU)

Zabbix (creado por Alexei Vladishev) Surge en 2001 y se comenta que en muchos casos hace la sombra a Nagios.

Es un desarrollo completo, no un fork de Nagios.

The screenshot shows the Zabbix web interface with the following sections:

- Top Navigation:** ZABBIX, Monitoring, Inventory, Reports, Configuration, Administration.
- Header:** Dashboard, Overview, Web, Latest data, Triggers, Events, Graphs, Screens, Maps, Discovery, IT services.
- Left Sidebar:** Favourite maps, Local network, Maps; Favourite graphs, New host: CPU load, Zabbix server, Graphs; Favourite screens, Zabbix server, Screens, Slide shows; System, Host inventory, Latest data, Triggers, Graphs, Data, Host screens.
- Central Content:**
 - Last 20 issues:** A table showing issues with columns: HOST, ISSUE, LAST CHANGE, AGE, INFO, ACK, ACTIONS. One issue is highlighted: "New host: Zabbix agent on New host is unreachable for 5 minutes" (2016-01-12 01:50:00).
 - SCRIPTS:** Detect operating system, Ping, Traceroute.
 - Host status:** A table showing host status by group: WITHOUT PROBLEMS, WITH PROBLEMS, TOTAL. For "Clouds", there is 1 host without problems and 0 with problems, totaling 1.
- Right Sidebar:** Status of Zabbix table, Discovery status table, Web monitoring table.



GPL(GNU)

Visión más holística de la monitorización, cubriendo rendimiento, no solo estados (Una de las carencias más significativas de Nagios)

ZABBIX Monitoring Inventory Reports Configuration Administration

Dashboard Overview Web Latest data Triggers Events Graphs Screens Maps Discovery IT services

Last 20 issues

HOST	ISSUE	LAST CHANGE	AGE	INFO	ACK	ACTIONS
New host	Zabbix agent on New host is unreachable for 5 minutes	2016-01-12 01:50:00	17m 17s	No	1	
Zabbix server	Zabbix discoverer processes	2016-01-12 01:23:39	43m 34s	No	1	

Favourite maps

Favourite graphs

Favourite screens

Syst

Host inventory

Latest data

Triggers

Graphs

Host screens

Discovered hosts

JB applications

Linux servers

Network devices

SNMP hosts

Virtual machines

Web servers

Windows servers

Zabbix servers

Host status

HOST GROUP

WITHOUT PROBLEMS

WITH PROBLEMS

TOTAL

Clouds

1 0 1

Status of Zabbix

PARAMETER	VALUE	DETAILS
Zabbix server is running	Yes	localhost:10051
Number of hosts (enabled/disabled/templates)	54	11 / 0 / 43
Number of items (enabled/disabled/not supported)	356	350 / 0 / 6
Number of triggers (enabled/disabled/problem/ok)	95	93 / 2 / 3 / 90
Number of users (online)	3	2
Required server performance: new values per second	4.79	

Discovery status

DISCOVERY RULE

UP DOWN

Local network2

0 0

Web monitoring

HOST GROUP

OK FAILED UNKNOWN

Discovered hosts

1 0 0

Zabbix servers

1 0 0

Updated: 02:08:13

Updated: 02:08:12

Updated: 02:08:12

Updated: 02:08:13

Debug



- Degradación del rendimiento a partir de 1000 nodos.
- Zabbix no tiene informes en tiempo real.
- Configuración, aunque intuitiva, requiere de muchos clics para completarla.



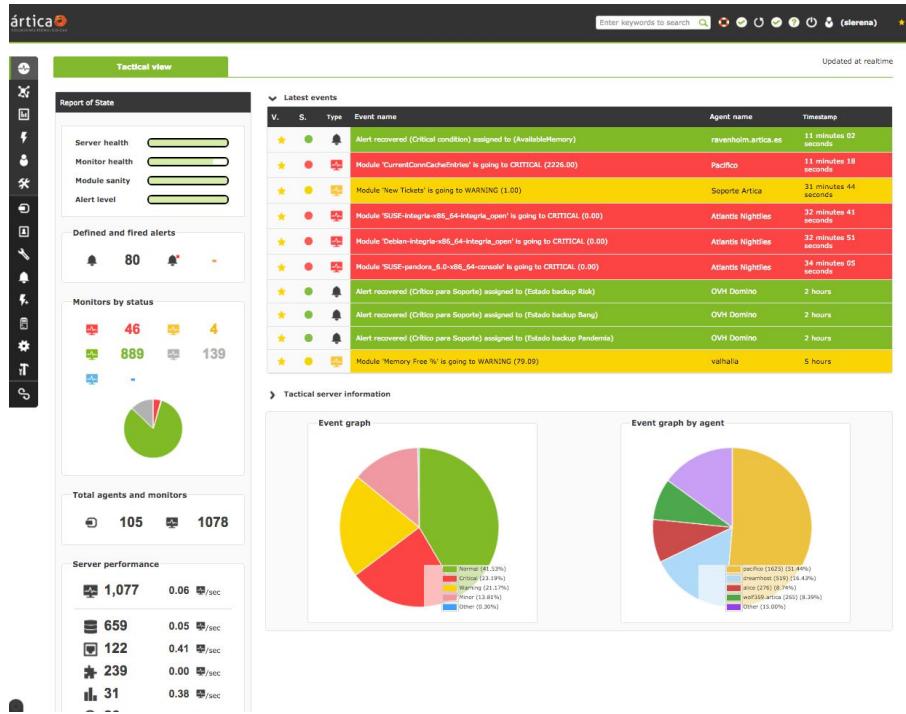


PANDORA**FMS**

GPL(GNU) y Enterprise

Pandora FMS tiene su origen en el año 2004 de la mano de Ártica ST.

Similar a Zabbix pero renovado y más “amigable”





La versión de la comunidad, a diferencia de la Enterprise está muy limitada.

- Incapacidad de recolectar logs.
- Ausencia de autenticación LDAP.
- ...
 - <https://pandorafms.com/es/precios-de-pandora-fms/#pricing%7C1>





CHECK_MK

Das Monitoring

GPL(GNU) y Enterprise

- Plugin de Nagios, creado por Mathias Kettner que aportaba más funcionalidad y rendimiento.
- Llegó a tener tal popularidad, que pasó a ser una herramienta independiente.

Main Overview

cmkadmin (admin) 13:42

TACTICAL OVERVIEW

Hosts	Problems	Unhandled	State
769	7	2	0
Services	Problems	Unhandled	State
31156	74	12	5
Events	Problems	Unhandled	State
8	8	4	0

HOST STATISTICS

Up: 762
Down: 7
Unreachable: 0
In Downtime: 0

SERVICE STATISTICS

OK: 31082
In Downtime: 0
On Down host: 0
Warning: 57
Unknown: 0
Critical: 17

HOST PROBLEMS (UNHANDLED)

STATE	ALIAS	ICONS	AGE	STATUS DETAIL
DOWN	carsv0142ldap	≡	4 m	No IP packet received for 15.847799 s (deadline is 15.000000 s)
DOWN	mucap0213san	≡	38.4 s	No IP packet received for 15.998454 s (deadline is 15.000000 s)

EVENTS OF RECENT 4 HOURS

TIME	ALIAS	SERVICE	OUTPUT
4 m	lyosv0887sql	ASM Diskgroup DATA_MUCORA11	WARN - 80.3% used (1.57 of 1.95 TB), trend: 0.00 B / 24 hours, extern redundancy
4 m	lyosv0887sql	ASM Diskgroup DATA_MUCORA11	WARN - 80.3% used (1.57 of 1.95 TB), trend: 0.00 B / 24 hours, extern redundancy
4 m	lyosv0413jvm	JVM LOGSERVER Threads	WARN - ThreadRate: 0.00, ThreadCount: 92 CRIT (Levels at 80/100), DaemonThreadCount: 90, PeakThreadCount: 129, TotalStartedThreadCount: 6047
4 m	lyosv0413jvm	JVM LOGSERVER Threads	WARN - ThreadRate: 0.00, ThreadCount: 92 WARN (Levels at 80/100), DaemonThreadCount: 90, PeakThreadCount: 129, TotalStartedThreadCount: 6047
4 m	lyosv0413jvm	JVM CBF Threads	CRIT - ThreadRate: 0.00, ThreadCount: 103 CRIT (Levels at 80/100), DaemonThreadCount: 64, PeakThreadCount: 111, TotalStartedThreadCount: 798
4 m	mucsv01228lic	Citrix_terminal_srv_licensing	WARN - Remote Desktop Licensing: stopped (start type is auto)
4 m	lyosv0413jvm	JVM CBF Threads	WARN - ThreadRate: 0.00, ThreadCount: 103 CRIT (Levels at 80/100), DaemonThreadCount: 64, PeakThreadCount: 111, TotalStartedThreadCount: 798
5 m	mucsv01228lic	Citrix_terminal_srv_licensing	WARN - Remote Desktop Licensing: stopped (start type is auto)
5 m	mucsv01228lic	Citrix_terminal_srv_licensing	WARN - Remote Desktop Licensing: stopped (start type is auto)

WATO - QUICKACCESS

MATHIAS KETTNER



CHECK_MK

Das Monitoring

GPL(GNU) y Enterprise

- Los agentes no hacen una llamada por cada comprobación.
- En cada llamada que les hace a ellos Check_MK, éstos envían todo lo que saben sobre su anfitrión.

TACTICAL OVERVIEW

Hosts	Problems	Unhandled	State
769	7	2	0

DASHBOARDS

- Host & Services Problems
- Main Overview
- Network Topology

VIEWS

- Overview
- Hosts
- Host Groups
- Services
- Service Groups
- Metrics
- Business Intelligence
- Problems
- Event Console
- Inventory
- Other

WATO - QUICKACCESS

... 4 CHANGES

MATHIAS KETTNER

Main Overview

Managed: 1,589

cmkadmin (admin) 13:42

HOST STATISTICS

Up: 762
Down: 7
Unreachable: 0
In Downtime: 0

Total: 769

SERVICE STATISTICS

OK: 31082
In Downtime: 0
On/Off host: 0
Warning: 0
Unknown: 57
Critical: 17

Total: 31156

HOST PROBLEMS (UNHANDLED)

STATE	ALIAS	ICONS	AGE	STATUS DETAIL
DOWN	carsv0142ldap	≡	4 m	No IP packet received for 15.847799 s (deadline is 15.000000 s)
DOWN	mucap0213san	≡	38.4 s	No IP packet received for 15.998454 s (deadline is 15.000000 s)

EVENTS OF RECENT 4 HOURS

TIME	ALIAS	SERVICE	OUTPUT
4 m	lyosv0887sql	ASM Diskgroup DATA_MUCORAII	WARN - 80.3% used (1.57 of 1.95 TB), trend: 0.00 B / 24 hours, extern redundancy
4 m	lyosv0887sql	ASM Diskgroup DATA_MUCORAII	WARN - 80.3% used (1.57 of 1.95 TB), trend: 0.00 B / 24 hours, extern redundancy
4 m	lyosv0413jvm	JVM LOGSERVER Threads	WARN - ThreadRate: 0.00, ThreadCount: 92 WARN (Levels at 80/100), DaemonThreadCount: 90, PeakThreadCount: 129, TotalStartedThreadCount: 6047
4 m	lyosv0413jvm	JVM LOGSERVER Threads	WARN - ThreadRate: 0.00, ThreadCount: 92 WARN (Levels at 80/100), DaemonThreadCount: 90, PeakThreadCount: 129, TotalStartedThreadCount: 6047
4 m	lyosv0413jvm	JVM CBF Threads	CRIT - ThreadRate: 0.00, ThreadCount: 103 CRIT (Levels at 80/100), DaemonThreadCount: 64, PeakThreadCount: 111, TotalStartedThreadCount: 798
4 m	lyosv0413jvm	JVM CBF Threads	CRIT - ThreadRate: 0.00, ThreadCount: 103 CRIT (Levels at 80/100), DaemonThreadCount: 64, PeakThreadCount: 111, TotalStartedThreadCount: 798
4 m	mucsv1228lic	Citrix_terminal_srv_licensing	WARN - Remote Desktop Licensing: stopped (start type is auto)
4 m	lyosv0413jvm	JVM CBF Threads	WARN - ThreadRate: 0.00, ThreadCount: 92 WARN (Levels at 80/100), DaemonThreadCount: 64, PeakThreadCount: 111, TotalStartedThreadCount: 798
5 m	mucsv1228lic	Citrix_terminal_srv_licensing	WARN - Remote Desktop Licensing: stopped (start type is auto)
5 m	mucsv1228lic	Citrix_terminal_srv_licensing	WARN - Remote Desktop Licensing: stopped (start type is auto)



CHECK_MK

Das Monitoring

GPL(GNU) y Enterprise

Ofrece una versión Enterprise con varias mejoras y comodidades, como exportación de gráficos, y un núcleo más optimizado aún, pero la versión gratuita es 100% funcional.

Main Overview

cmkadmin (admin) 13:42

TACTICAL OVERVIEW

Hosts	Problems	Unhandled	State
769	7	2	0
Services	Problems	Unhandled	State
31156	74	12	5
Events	Problems	Unhandled	State
8	8	4	0

QUICKSEARCH

DASHBOARDS

- Host & Services Problems
- Main Overview
- Network Topology

VIEWS

- Overview
- Hosts
- Host Groups
- Services
- Service Groups
- Metrics
- Business Intelligence
- Problems
- Event Console
- Inventory
- Other

WATO - QUICKACCESS

... 4 CHANGES

MATHIAS KETTNER

HOST STATISTICS

Up: 769
Down: 0
Unreachable: 0
In Downtime: 0

Total: 769

SERVICE STATISTICS

OK: 31082
In Downtime: 0
On Down host: 0
Warning: 0
Unknown: 57
Critical: 17
Total: 31156

HOST PROBLEMS (UNHANDLED)

STATE	ALIAS	ICONS	AGE	STATUS DETAIL
DOWN	carsy0142ldap	≡	4 m	No IP packet received for 15.847799 s (deadline is 15.000000 s)
DOWN	mucap0213san	≡	38.4 s	No IP packet received for 15.998454 s (deadline is 15.000000 s)

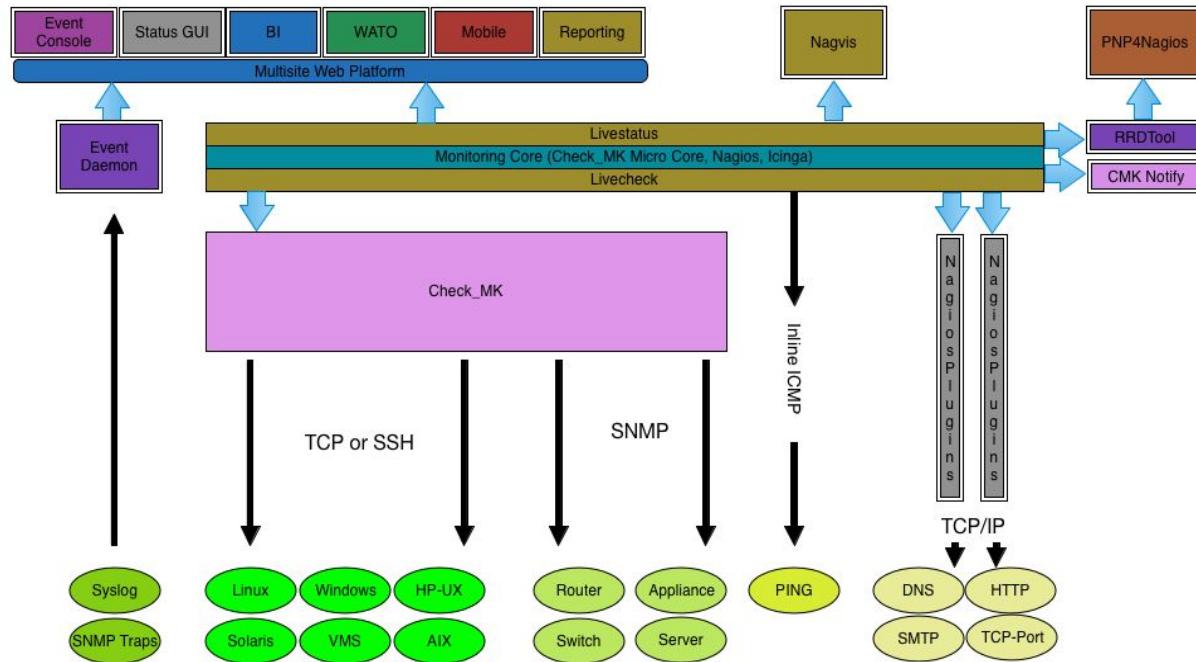
EVENTS OF RECENT 4 HOURS

TIME	ALIAS	SERVICE	OUTPUT
4 m	lyosv0887sql	ASM Diskgroup DATA_MUCORAII	WARN - 80.3% used (1.57 of 1.95 TB), trend: 0.00 B / 24 hours, extern redundancy
4 m	lyosv0887sql	ASM Diskgroup DATA_MUCORAII	WARN - 80.3% used (1.57 of 1.95 TB), trend: 0.00 B / 24 hours, extern redundancy
4 m	lyosv0413jvm	JVM LOGSERVER Threads	WARN - ThreadRate: 0.00, ThreadCount: 92 [WARN] (Levels at 80/100), DaemonThreadCount: 90, PeakThreadCount: 129, TotalStartedThreadCount: 6047
4 m	lyosv0413jvm	JVM LOGSERVER Threads	WARN - ThreadRate: 0.00, ThreadCount: 92 [WARN] (Levels at 80/100), DaemonThreadCount: 90, PeakThreadCount: 129, TotalStartedThreadCount: 6047
4 m	lyosv0413jvm	JVM CBF Threads	CRIT - ThreadRate: 0.00, ThreadCount: 103 [CRIT] (Levels at 80/100), DaemonThreadCount: 64, PeakThreadCount: 111, TotalStartedThreadCount: 798
4 m	lyosv0413jvm	JVM CBF Threads	CRIT - ThreadRate: 0.00, ThreadCount: 103 [CRIT] (Levels at 80/100), DaemonThreadCount: 64, PeakThreadCount: 111, TotalStartedThreadCount: 798
4 m	mucsv1228lic	Citrix_terminal_srv_licensing	WARN - Remote Desktop Licensing: stopped (start type is auto)
4 m	lyosv0413jvm	JVM CBF Threads	WARN - ThreadRate: 0.00, ThreadCount: 103 [CRIT] (Levels at 80/100), DaemonThreadCount: 64, PeakThreadCount: 111, TotalStartedThreadCount: 798
5 m	mucsv1228lic	Citrix_terminal_srv_licensing	WARN - Remote Desktop Licensing: stopped (start type is auto)
5 m	mucsv1228lic	Citrix_terminal_srv_licensing	WARN - Remote Desktop Licensing: stopped (start type is auto)



CHECK_MK

Das Monitoring



Check_MK mejora a Zabbix en:

- Configuración de ficheros planos.
 - Facilidad para implementar scripts y/o agentes personalizados escritos en Python, en los cuales dependiendo de la salida del script (0,1,2) manejaremos los: **OK**, **CRITICAL** o **WARNING**.



Check_MK destaca por:

- Detección de “Flapping” suspendiendo inmediatamente las alertas para no saturar con “ruido” la bandeja de entrada de incidencias.
- Agentes muy ligeros.
- Documentación muy detallada.

Pero, ¿Y los logs?

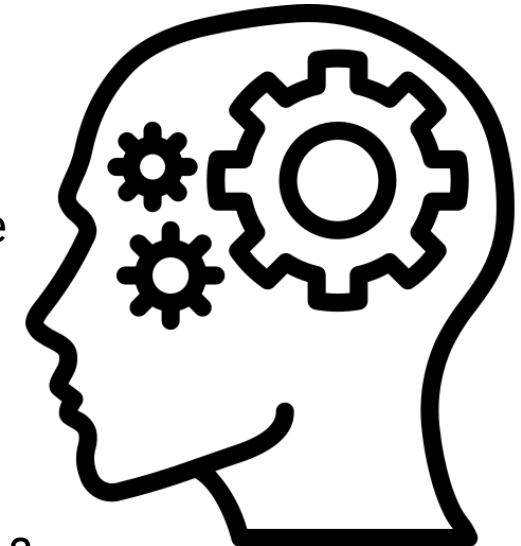
- Plugin “mk_logwatch”
 - Definimos qué eventos van a ser considerados como “Critical” o “Warning”

```
/var/log/auth.log
W sshd.*Corrupted MAC on input
```

```
/var/log/syslog
I i915.*registered panic notifier
I drm.*registered panic notifier
I Command line: .* panic=
I Modules linked in.*pvpanic
C panic
C Oops
W Killed process
W generic protection rip
W .*Unrecovered read error - auto reallocate failed
```

¿Entonces cómo...?

- ¿En qué horas hay mayores conexiones de alumnos?
- ¿Qué alumnos se han conectado, en qué equipo y a que hora?
- ¿Por dónde están navegando los alumnos?
- ¿Qué procesos están en ejecución en los equipos y cuántos recursos consumen?
- ¿Es la CPU o es la RAM lo que más limita a los alumnos?
- ¿Docker o en Máquinas Virtuales?



~~Nagios®~~

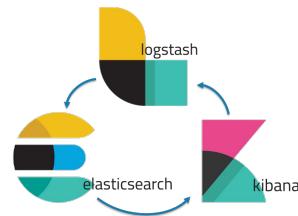


~~CHECK_MK~~
Das Monitoring

Grafana

Prometheus

splunk>



x-pack

Open Distro
for Elasticsearch

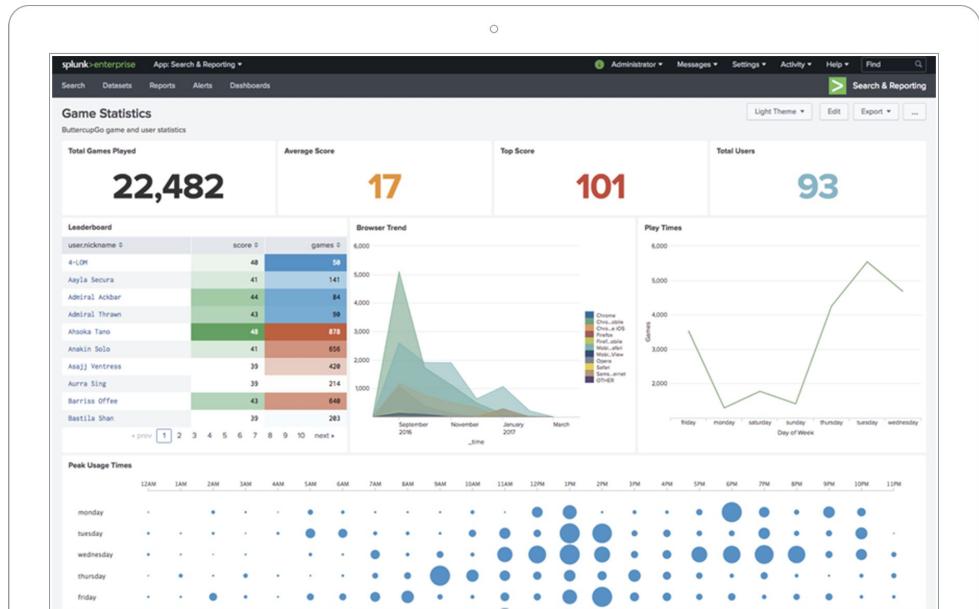




splunk®

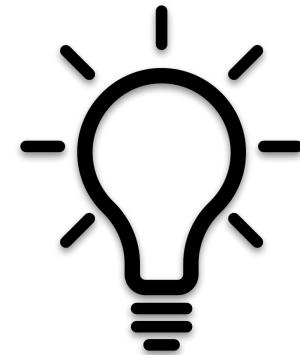
Enterprise

- Una de las primeras compañías en lidiar con los problemas inherentes al registro y los datos de la máquina, incluso antes de que se acuñara el término big data.
 - Fundada en 2003 (Michael Baum, Rob Das y Erik Swan)

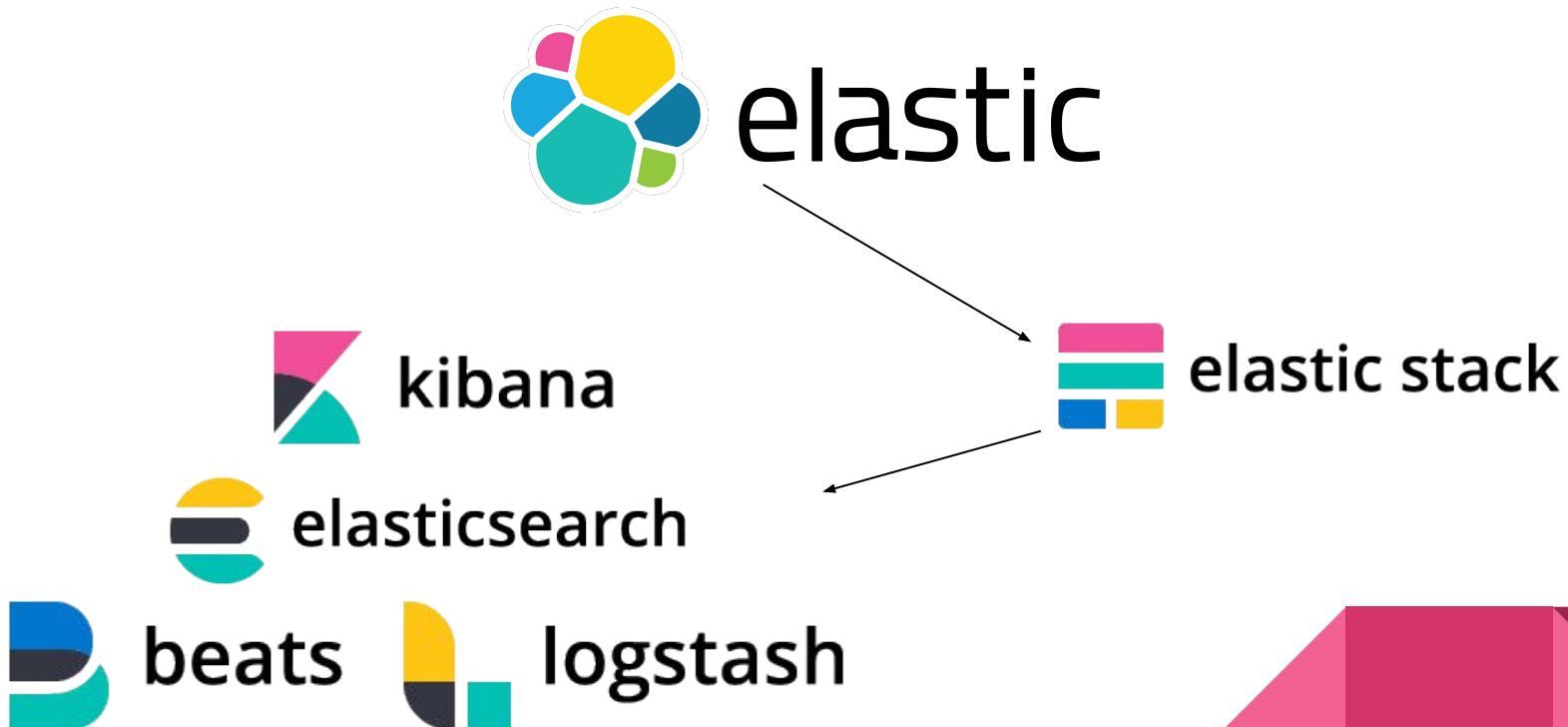




- No es de código abierto.
- “La otra cara de la moneda” es **ElasticSearch**, que sí era de código abierto, y que fue lanzada por Shay Banon en 2010.

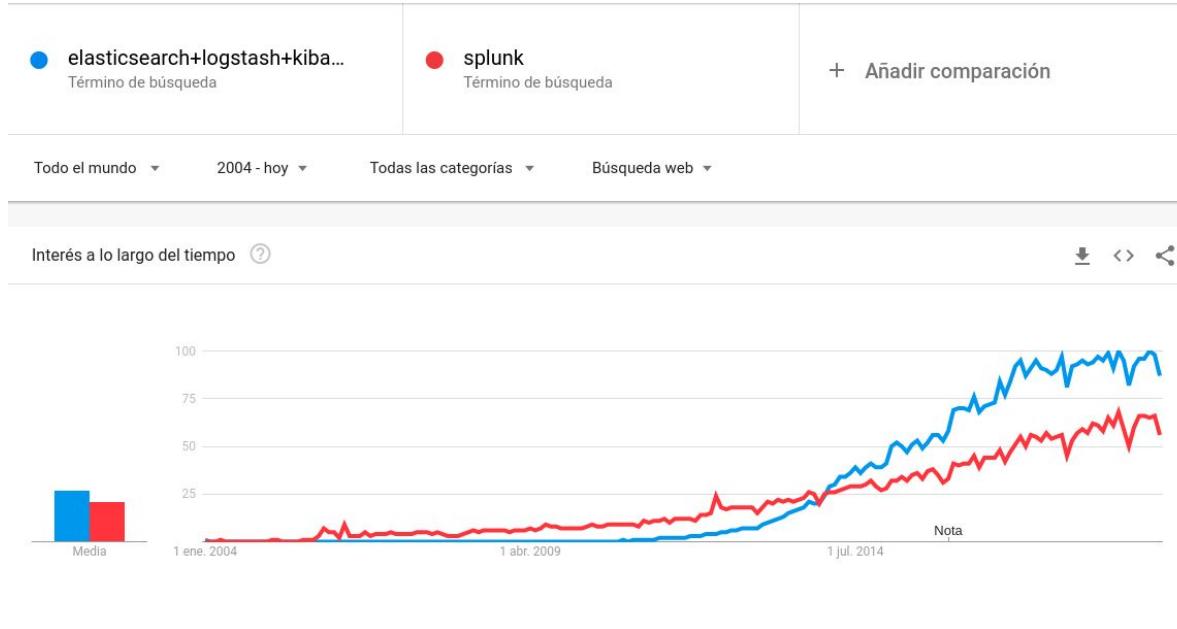
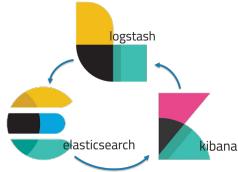


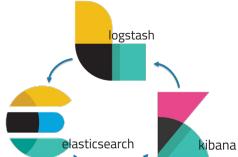
En base a Elasticsearch, se fundó:





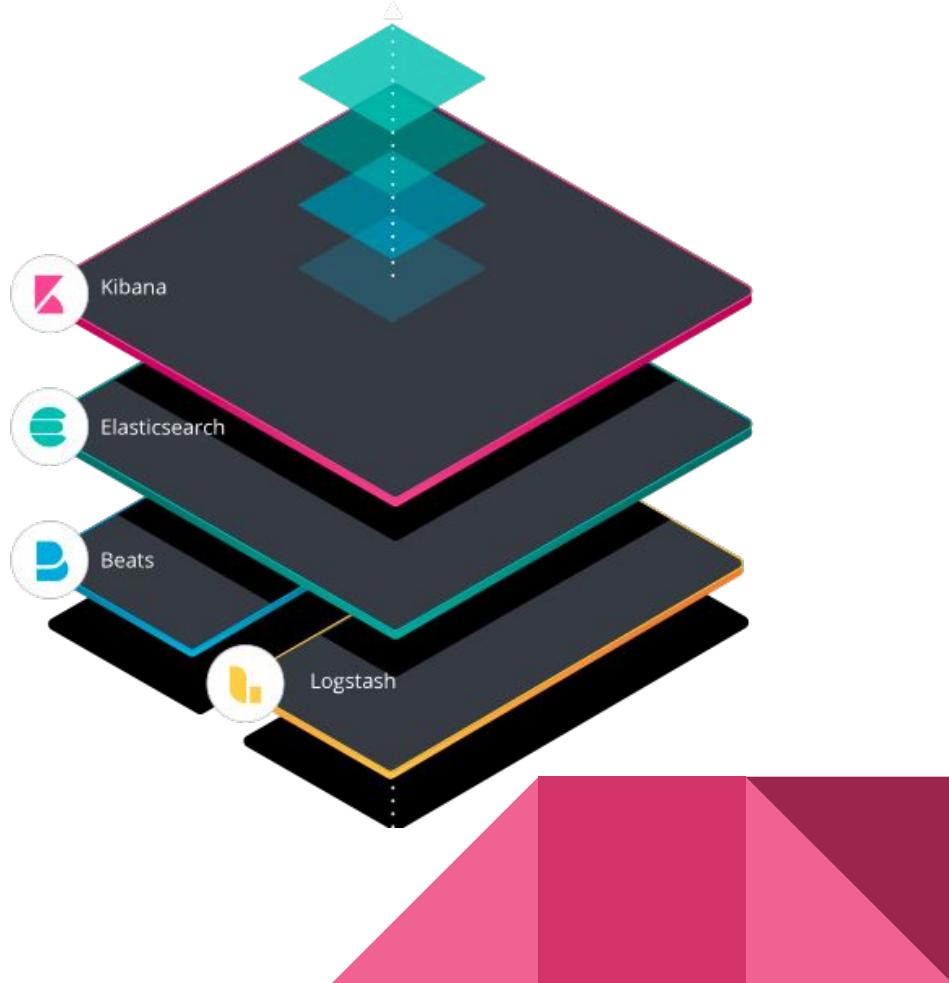
V/S





Licencia Apache

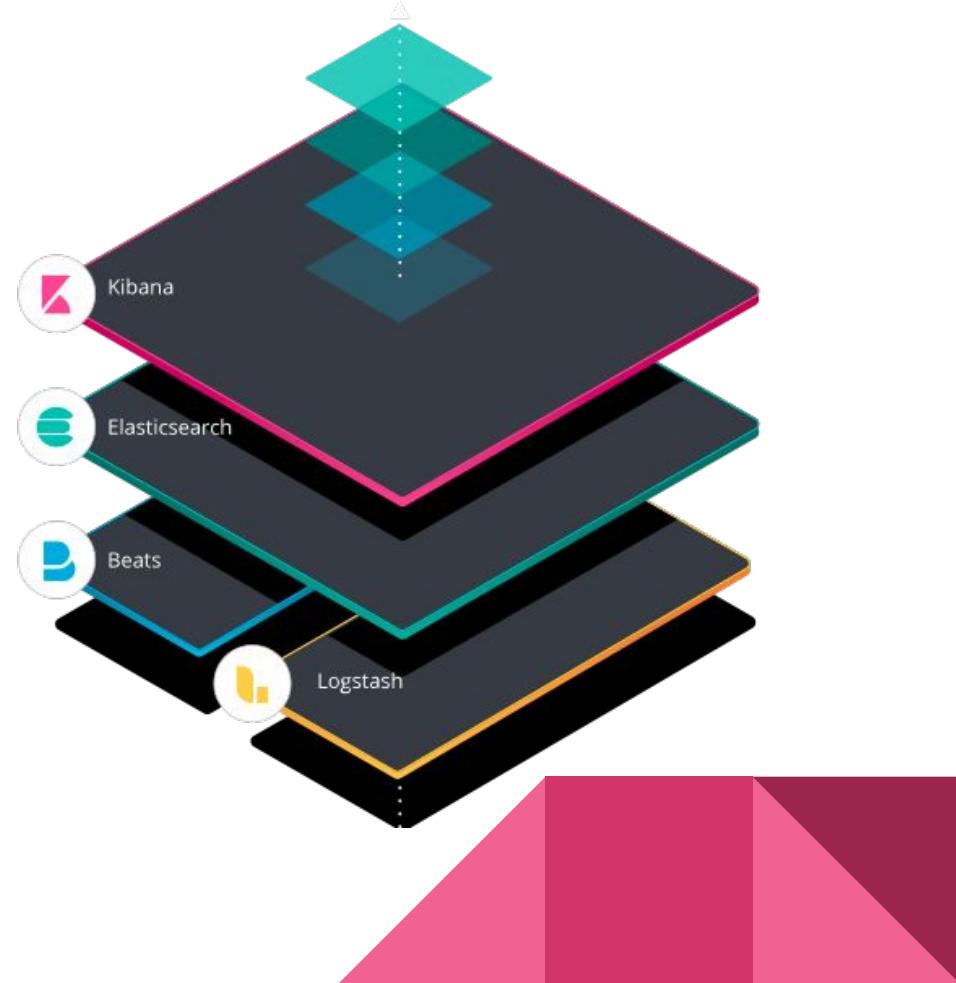
ELK Stack es un conjunto de herramientas de gran potencial de código abierto (Licencia Apache) que se combinan permitiendo la monitorización, consolidación y análisis de logs generados en múltiples servidores.





Licencia Apache

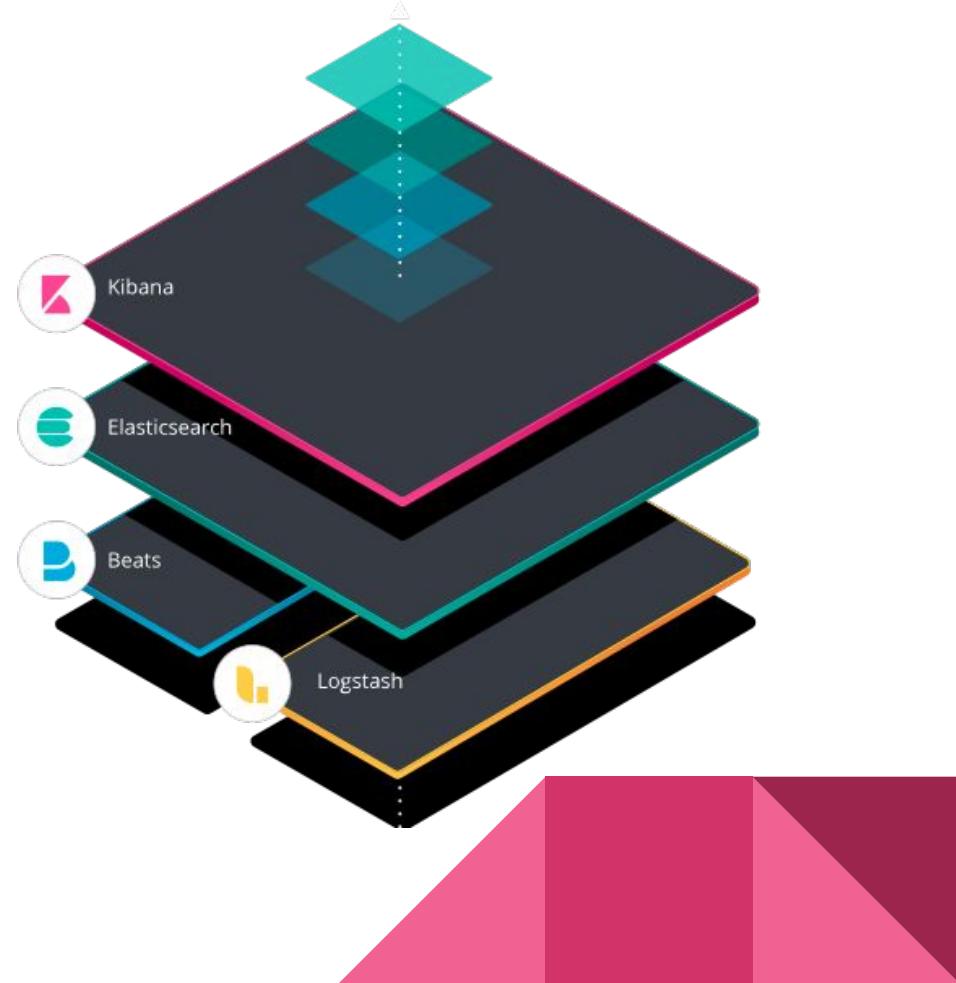
- Elasticsearch es un motor de búsqueda y análisis RESTful distribuido.
- Permite realizar y combinar muchos tipos de búsquedas: estructuradas, no estructuradas...





Licencia Apache

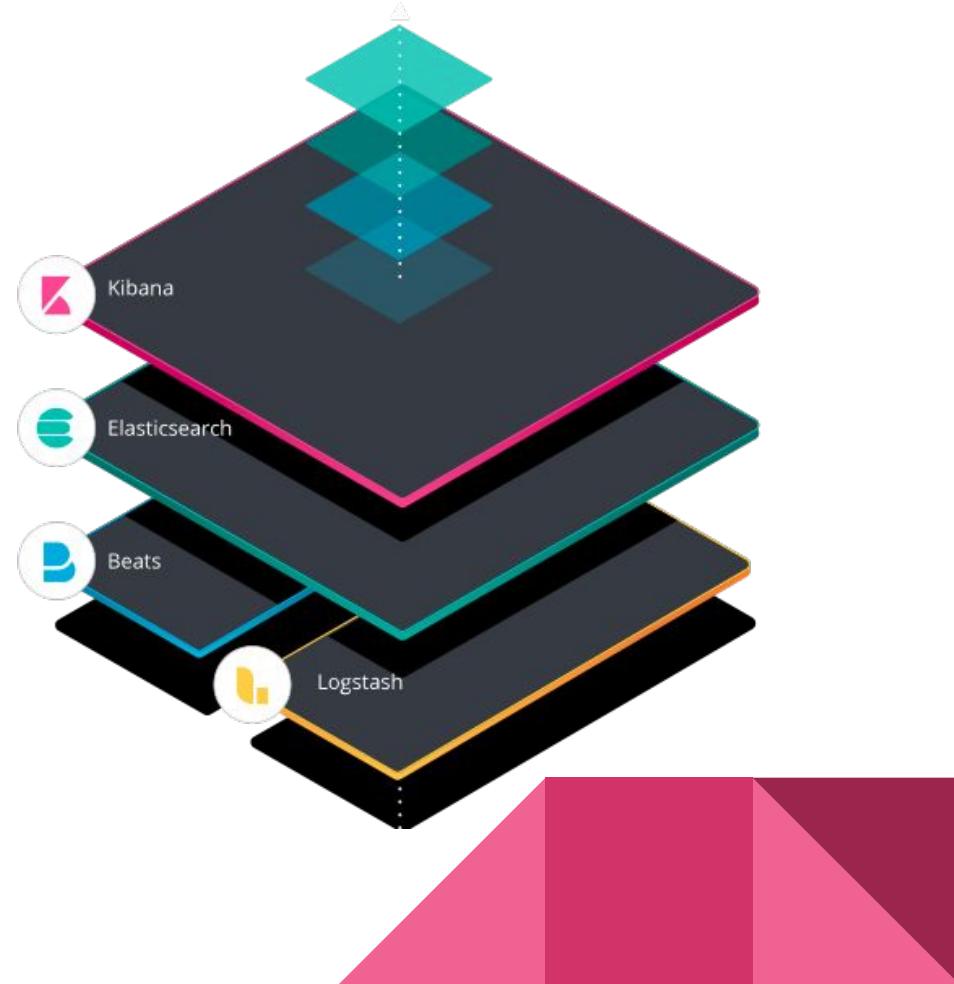
- Logstash es una fuente de procesamiento de datos del lado del servidor.
- Ingiere datos de una multitud de fuentes simultáneamente, la transforma y luego la envía.





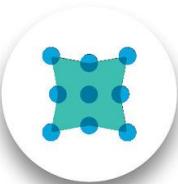
Licencia Apache

- Beats es una familia de agentes muy ligeros que recolectan datos de los hosts y los envían a Elasticsearch o Logstash.
- Amplia familia de Beats (Logs, Métricas, y + de 40 beats de la comunidad)





The Beats family



Packetbeat

Network data



Metricbeat

Metrics



Winlogbeat

Windows Event Logs



Auditbeat

Audit data



Filebeat

Log files



Heartbeat

Uptime monitoring

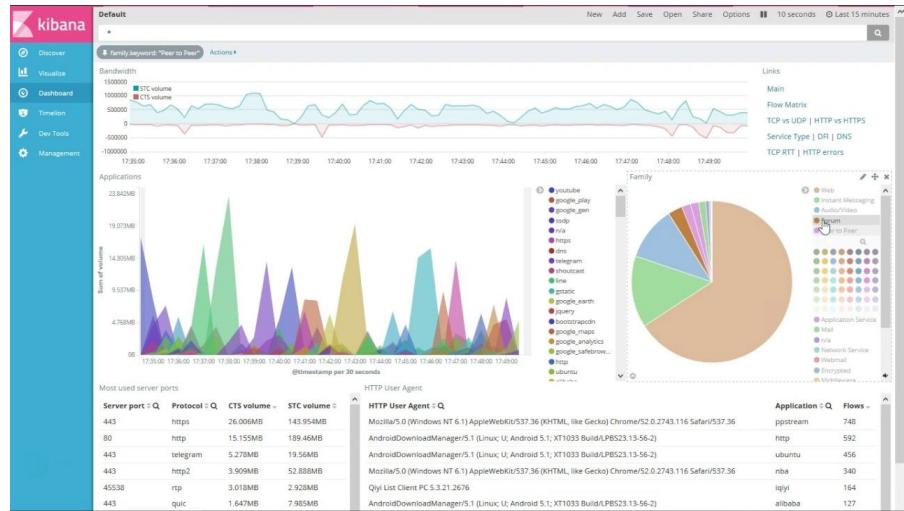
+40 de la
comunidad



Functionbeat

Serverless Shipper

- Kibana es una plataforma de análisis y visualización, diseñada para trabajar con Elasticsearch.
- Análisis y visualización de datos avanzados.





kibana

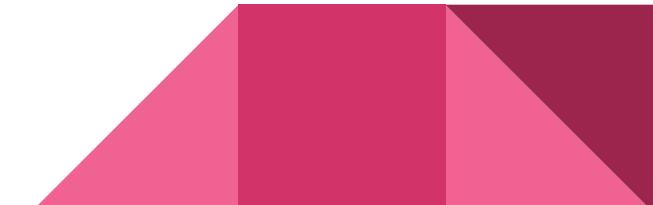
v/s



Grafana

Durante el transcurso de la investigación sobre Kibana, fue constante el encontrarse menciones a Grafana.

¿Pero qué es Grafana?



- Herramienta de visualización que se puede usar sobre una variedad de diferentes almacenes de datos, como: Graphite, InfluxDB, y también Elasticsearch.





kibana

v/s



Grafana

La diferencia clave entre las dos herramientas de visualización proviene de su **propósito**:

- Grafana está diseñado para analizar y visualizar métricas como la CPU del sistema, la memoria, el disco y la utilización de E / S.
- Grafana no permite consultas de datos de texto completo.



kibana

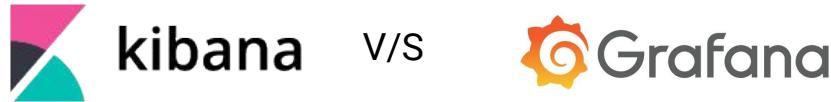
v/s



Grafana

Diferencias en fuentes de datos:

- Grafana funciona con múltiples almacenes de datos de series de tiempo, incluyendo integraciones integradas con Graphite, Prometheus, InfluxDB, MySQL, PostgreSQL y Elasticsearch...
- Kibana, por otro lado, está diseñado para funcionar solo con Elasticsearch



Diferencias en “Consultas”:

- Consultar y buscar registros es una de las funciones más potentes de Kibana. (Lucene, DSL Elasticsearch Query, Kuery experimental...)
- Con Grafana, los usuarios utilizan un Editor de consultas para realizar consultas. Cada fuente de datos tiene una sintaxis diferente.

- Prometheus es una BD de series de tiempo y un sistema de monitoreo y alertas.
- Su origen se remonta al 2012 en la compañía SoundCloud.
- Es una potente y ligera herramienta para recopilar y procesar métricas.
- Es muy común conectarlo con Grafana, para mejorar la experiencia gráfica.





Licencia Apache

- Es una herramienta orientada a métricas, y como bien indican en el FAQ de Prometheus:

"Prometheus es un sistema para recopilar y procesar métricas, no un sistema de registro de eventos. "Usa algo como ELK Stack en su lugar."



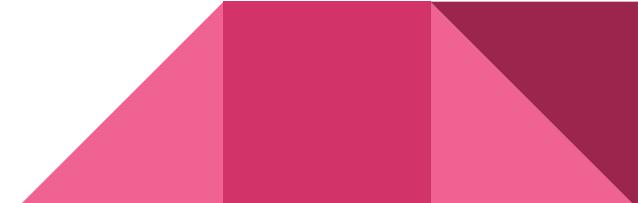




x-pack <6.3 privado. > 6.3 “código abierto (No OSI)”

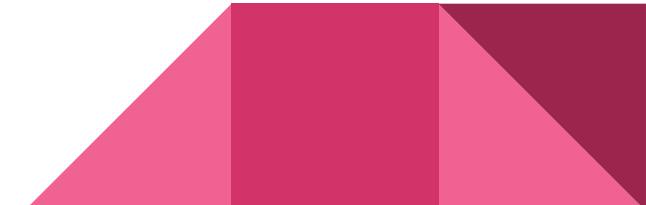
- **Seguridad y privacidad de la información.**
- Monitorización del clúster.
- Sistema de alertas.
- Reportes gráficos sobre la conectividad.
- Machine learning.



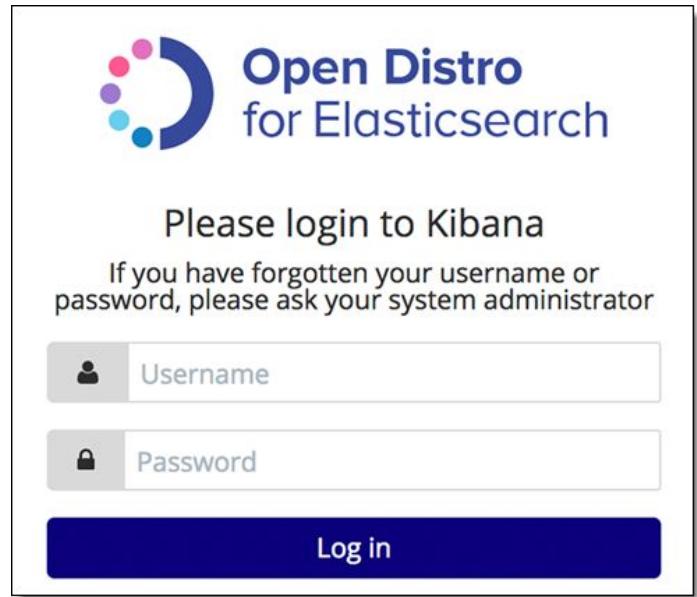


 +  +  =  Open Distro
for Elasticsearch

- Lanzado el 11 de marzo de 2019.
- Sustituto de X-Pack, 100% de código abierto y gratis.



- **Seguridad**
 - OpenSSL y TLS 1.2
 - LDAP, SAML, Kerberos...
 - Roles
- Alertas
 - Webhooks, SMTP(próximamente) y Slack.
- SQL
- Performance Analyzer





Eche un vistazo a las próximas características de Amazon Elasticsearch Service

Obtenga más información sobre la nueva Open Distro para Elasticsearch, una distribución de código abierto 100 % impulsada por la comunidad de Elasticsearch

[Más información](#)



Amazon Elasticsearch Service

Amazon Elasticsearch Service (Amazon ES) le permite configurar, utilizar y escalar fácilmente un clúster de Elasticsearch en la nube.

[Crear un nuevo dominio](#)

[Comprar una instancia reservada](#)

[Guía de introducción](#)



Lanzar un clúster de Elasticsearch

[Crear clústeres de Elasticsearch en la nube](#)



Administrar y monitorear

[Administración del clúster y monitoreo del tráfico](#)



Cargar y consultar datos

[Utilice las herramientas más populares para...](#)



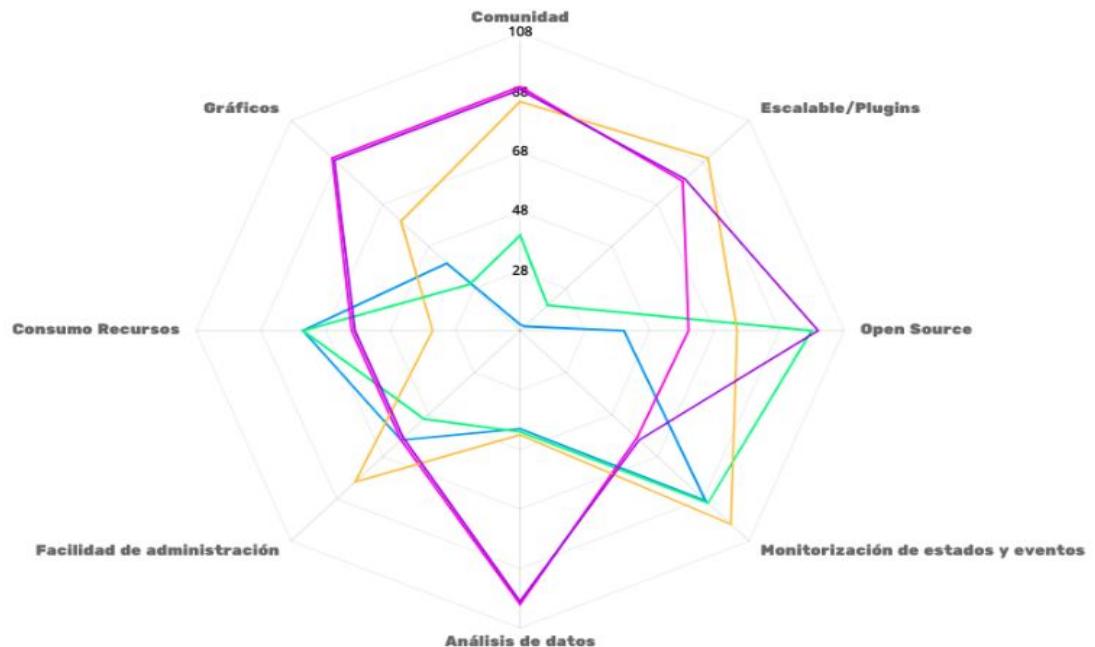
Compra de instancias reservadas

[Get significant cost savings by reserving...](#)



Version history

Open Distro for Elasticsearch version	Release highlights	Release date	Elasticsearch version
0.9.0	Bumps Elasticsearch version.	1 May 2019	6.7.1
0.8.0	Bumps Elasticsearch version.	5 April 2019	6.6.2
0.7.1	Fixes Kibana multitenancy.	29 March 2019	6.5.4
0.7.0	Initial release.	11 March 2019	6.5.4



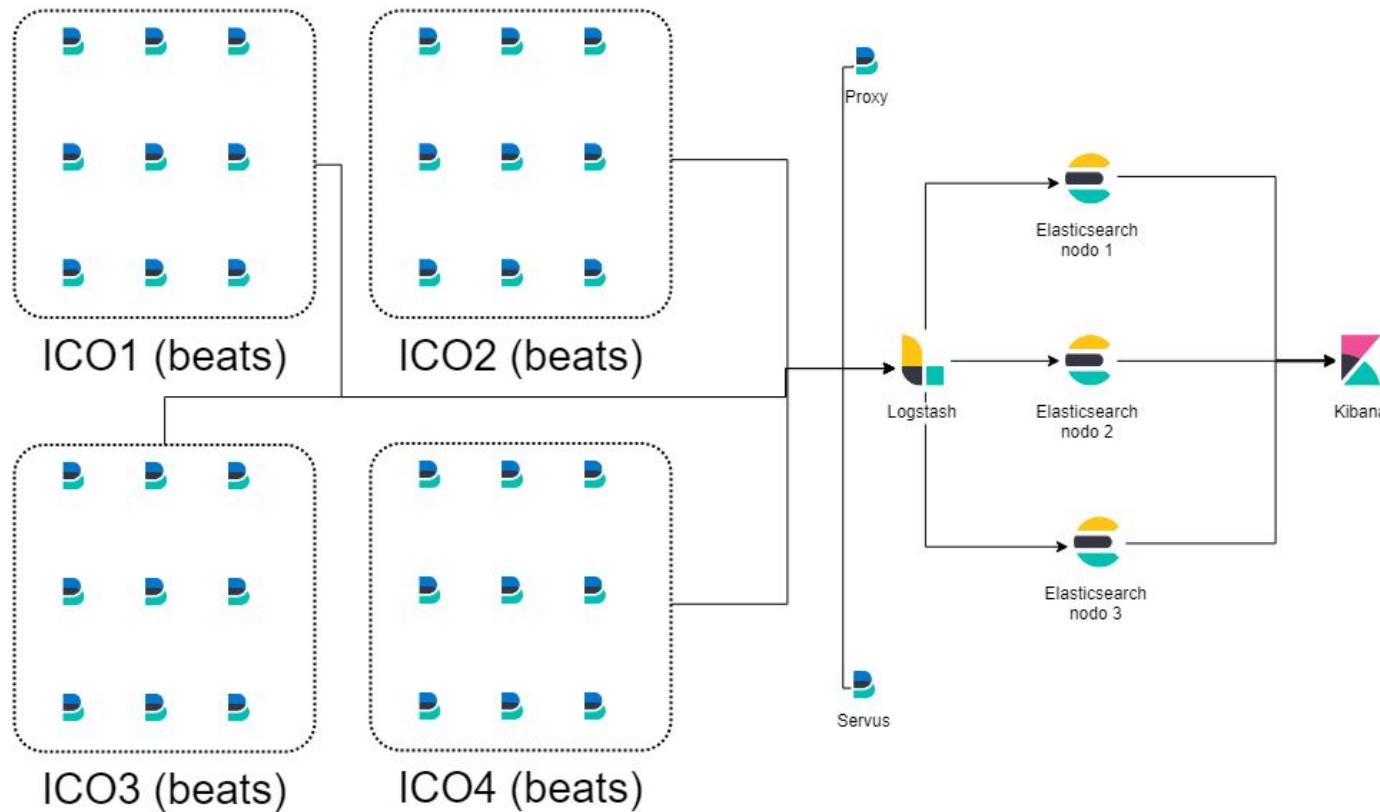
Pandora
Check_MK

Zabbix
Open Distro for Elasticsearch

ELK

Solución + Recursos

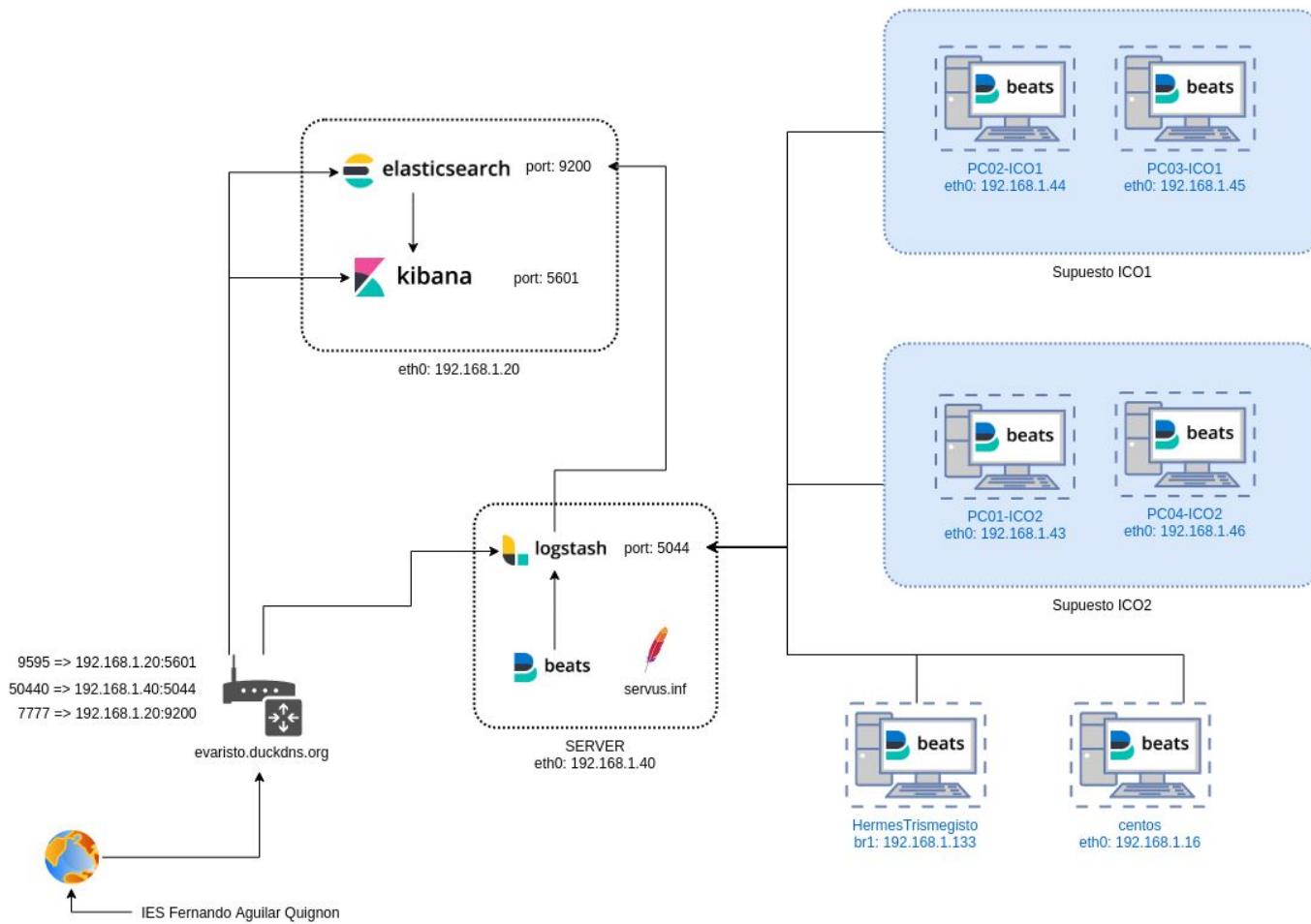




IES Fernando Aguilar Quignon



Evaristo R. Rivieccio Vega

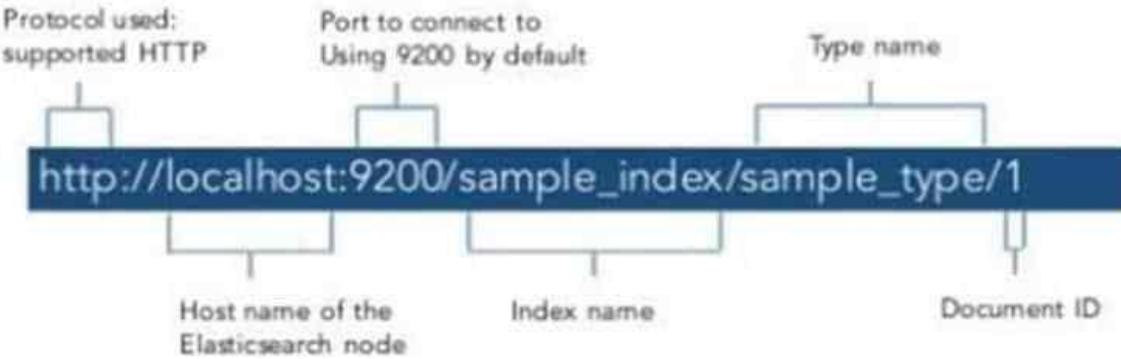


Arquitectura de Elasticsearch



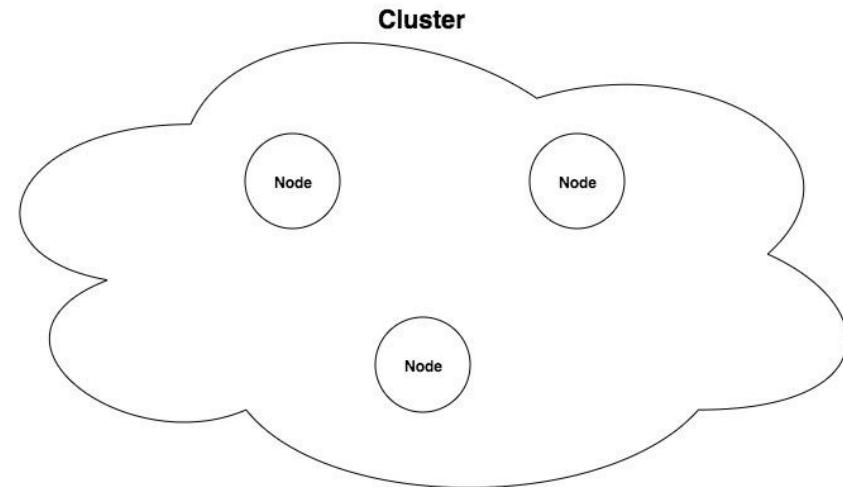
Características de Elasticsearch

- Escalabilidad horizontal
- Respuestas próximas al tiempo real
- Tolerante a fallos en los nodos
- Funciones de búsqueda en texto completo (se considera todo el contenido de los documentos para la búsqueda)
- Orientado a documentos JSON
- Sin esquemas
- APIs sencillas



Características de Elasticsearch

Los clústeres son una colección de nodos que se comunican entre sí para leer y escribir en un índice.



Tipos de nodos de Elasticsearch

- Nodo maestro:
 - Controla el clúster Elasticsearch.
- Nodo de datos:
 - Contiene los datos y el índice invertido.
- Nodo cliente:
 - Actúa como un equilibrador de carga.
- Nodo coordinador:
 - Encamina las solicitudes del cliente al fragmento apropiado en el clúster.

¿Cómo funciona el almacenamiento?

- Almacena documentos (JSON) en índices, que son la unidad principal.
- Los índices se dividen en shards (fragmentos primarios y réplicas)
- Cada fragmento puede ubicarse en un nodo diferente del clúster.
- Las escrituras se realizan sobre shards primarios, los cuales luego son replicados.
- Las lecturas se pueden realizar tanto sobre shards primarios como sobre las réplicas, con lo cual mejora la capacidad de lectura.

- Ejemplo: índice dividido en 2 shards (P0 y P1). 3 nodos y 2 réplicas por shard

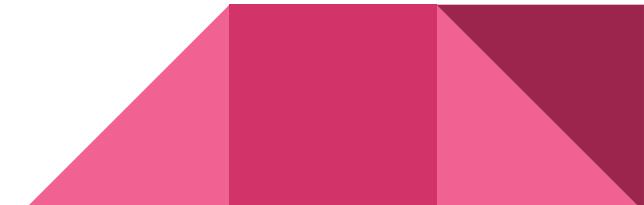


- Si falla un nodo: réplicas pasan a ser primarias.



Lucene

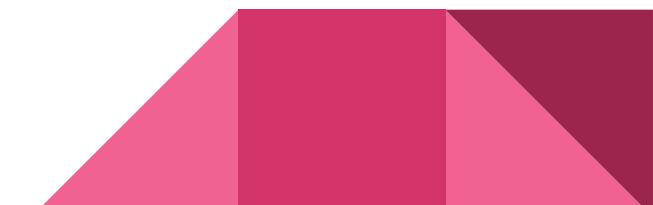
- Lucene es el nombre del motor de búsqueda que alimenta a Elasticsearch.
- Internamente usa una estructura de datos llamada índice invertido.
 - Al tokenizar los términos en el documento, crea una lista ordenada de todos los términos únicos, asociando una lista de documentos con el lugar donde se pueden encontrar las palabras.



Ejemplo Índice invertido

- **Doc 1:** Programa Insight
Data Engineering Fellows
- **Doc 2:** Programa Insight
Data Science Fellows

Token	Documents
data	Doc 1, Doc 2
engineering	Doc 1
fellows	Doc 1, Doc 2
insight	Doc 1, Doc 2
program	Doc 1, Doc 2
science	Doc 2



Terms

brown

dog

fat

fox

jump

lazi

over

quick

Document

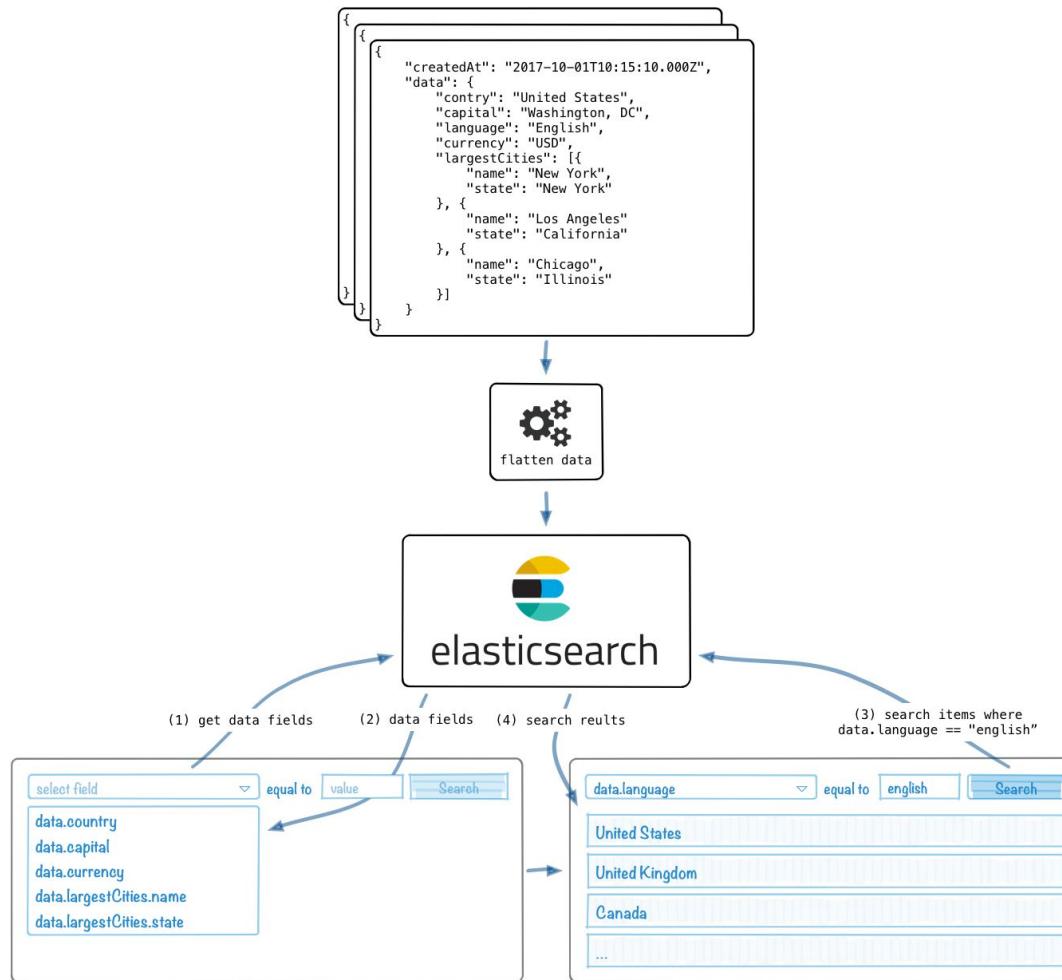
```
{  
  "_id": 1  
  "phrase": "the  
quick brown fox jumps  
over the lazy dog"
```

```
{  
  "_id": 2  
  "phrase": "The fat  
brown dog"  
}
```

Con precisión...

- Cada índice de Elasticsearch (conjunto de documentos) se divide en fragmentos.
- Los fragmentos son la división de un índice.
- Cada fragmento de Elasticsearch es un índice de Lucene.
- El número máximo de documentos que puede tener en un índice de Lucene es de 2.147.483.519.
- El índice de Lucene se divide en archivos más pequeños llamados segmentos.
- Un segmento es un pequeño índice de Lucene. Lucene busca en todos los segmentos secuencialmente.

Elasticsearch Index

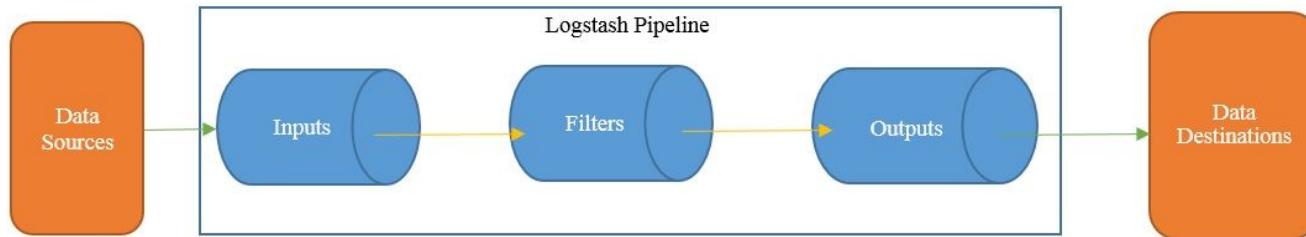


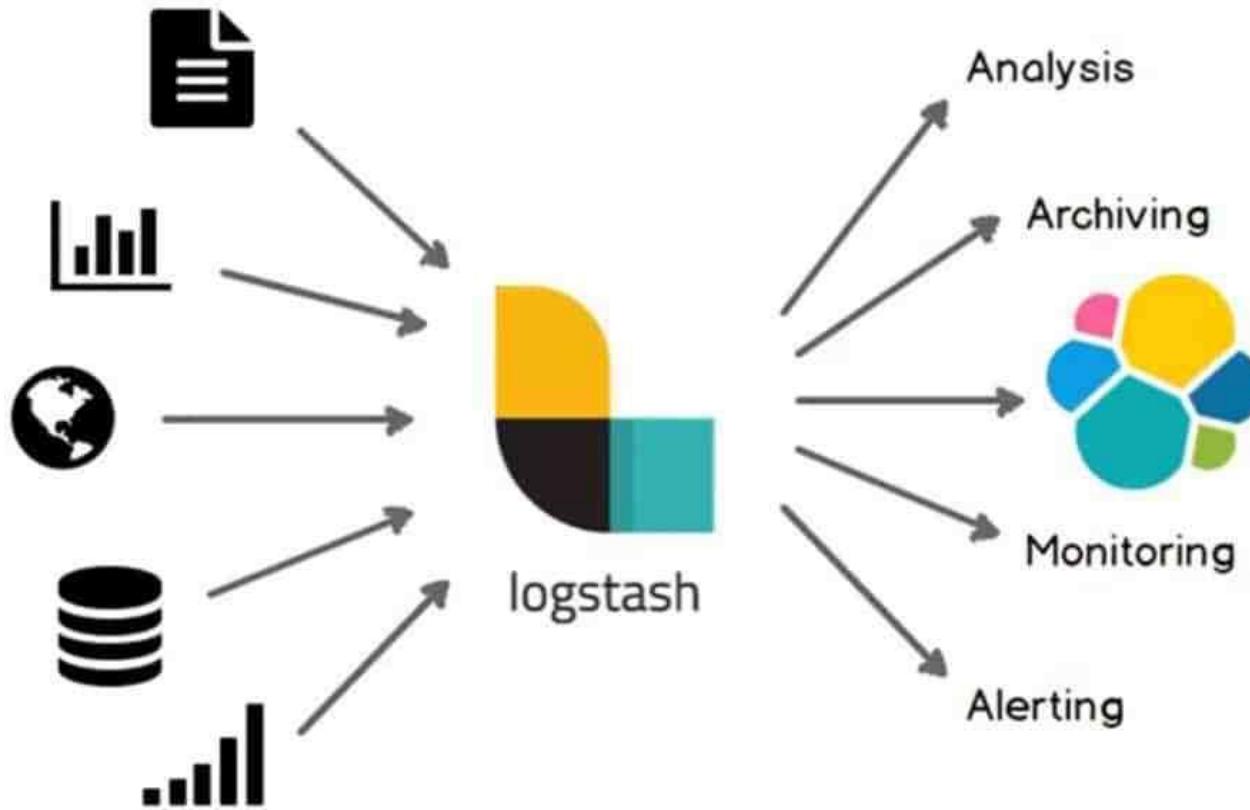
Arquitectura de Logstash



Logstash

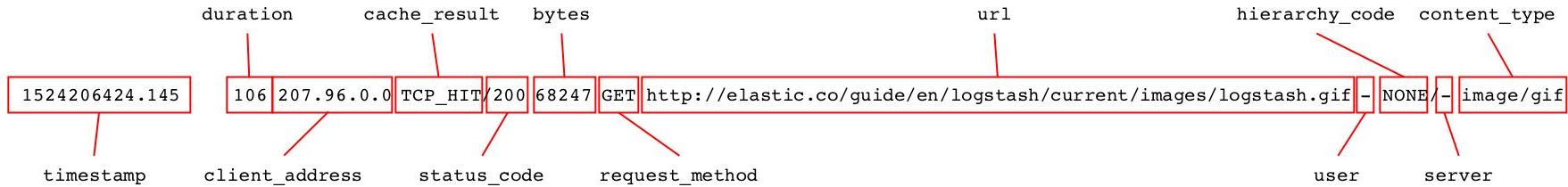
- Extrae y recibe de datos de varios sistemas.
- Los transforma en un conjunto significativo de campos.
- Los transmite a un destino definido para su almacenamiento.





Logstash - Filter (más frecuentes)

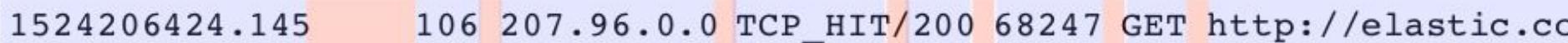
- **dissect:**
 - analiza registros de acuerdo con delimitadores.
- **grok:**
 - funciona de acuerdo con la coincidencia de expresiones regulares.



Grok es generalmente más potente y puede manejar una mayor variedad de datos.

Grok

- Grok usa patrones de expresiones regulares para hacer coincidir campos y delimitadores.

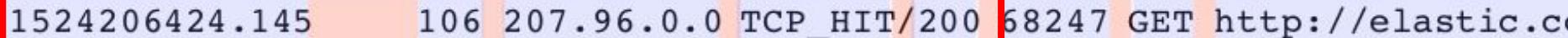


1524206424.145 106 207.96.0.0 TCP_HIT/200 68247 GET http://elastic.co

- Grok viene con una gran variedad de patrones listos para usar.

Grok

- Grok usa patrones de expresiones regulares para hacer coincidir campos y delimitadores.



```
1524206424.145 106 207.96.0.0 TCP_HIT/200 68247 GET http://elastic.c...
```

- SQUID3

```
%{NUMBER:timestamp}\s+ %{NUMBER:duration}\s%{IP:client_address}\s
%{WORD:cache_result}/%{POSINT:status_code}\s%{NUMBER:bytes}\s
%{WORD:request_method}\s%{NOTSPACE:url}\s(%{NOTSPACE:user}|-)\s%
{WORD:hierarchy_code}/%{IPORHOST:server}\s%{NOTSPACE:content_typ
e}
```

https://github.com/evaristorivi/Proyecto_final-ELK-Stack-Opendistro/blob/master/etc/logstash/conf.d/10squid.conf

Grok

- WORD (palabra):
 - patrón que hace coincidir una sola palabra.
- NUMBER (número):
 - patrón que hace coincidir un entero positivo o negativo o un número de punto flotante.
- POSINT:
 - patrón que hace coincidir un entero positivo..
- IP:
 - patrón que hace coincidir una dirección IP IPv4 o IPv6.
- NOTSPACE:
 - patrón que hace coincidir cualquier cosa que no sea un espacio.
- GREEDYDATA:
 - patrón que hace coincidir todos los datos restantes.

<http://grokdebug.herokuapp.com/>

Grok Debugger

Debugger

Discover

Patterns

May 30 09:07:12 pc16-t1 systemd: pam_unix(systemd-user:session): session closed for user antonioroga by (uid=0)

%{SYSLOGTIMESTAMP} %{SYSLOGHOST} systemd: pam_unix\\$(systemd-user:session\): session %{WORD:estado} for user %
{USERNAME:username} by \\$(uid=%{INT:uid:int}\\$)

Add custom patterns Keep Empty Captures Named Captures Only Singles

Autocomplete

Go

```
"SYSLOGTIMESTAMP": [
  [
    "May 30 09:07:12"
  ]
],
"MONTH": [
  [
    "May"
  ]
],
"MONTHDAY": [
  [
    "30"
  ]
]
```

Arquitectura de Beats



Beats - Lumberjack

- Lumberjack se desarrolló inicialmente como un experimento para subcontratar la tarea de extracción de datos y estaba destinado a ser utilizado como un cargador ligero para recopilar registros antes de enviarlos para su procesamiento en otra plataforma.

Lumberjack > Logstash-Forwarder > Beats

protocolo de red

Lumberjack-protocol (El protocolo del leñador)

- El protocolo de leñador está activamente en desarrollo en Elastic.
- Aunque aún no se han documentado los cambios entre los protocolos v1 y v2, las necesidades que conducen a este protocolo son:
 - Encriptación y autenticación para proteger.
 - La compresión debe usarse para reducir el ancho de banda.
 - La latencia de ida y vuelta no debe dañar el rendimiento
 - Reconocimiento de mensajes a nivel de aplicación
- El comportamiento de secuencia y acuse de recibo (incluida la ventana deslizante, etc.) es similar a TCP, pero en lugar de bytes, los mensajes son la unidad base.

Filebeat

- Filebeat consta de dos componentes principales:
 - inputs.
 - fuentes de lectura.
 - recolectores.
 - Se inicia un recolector para cada fichero.
 - Son responsables de abrir y cerrar el fichero.
 - Mantiene el estado de cada fichero.
 - ID únicos.

Filebeat

- en caso de problemas de red o interrupciones en las transmisiones, Filebeat recordará dónde se quedó cuando se restableció la conexión.
- Si hay un problema de ingestión con la salida, Logstash o Elasticsearch, Filebeat ralentizará la lectura de los ficheros.

Cuando se inicia Filebeat...

- Se inician una o más entradas que buscan en las ubicaciones que se han especificado para los datos de registro.
- Para cada registro que Filebeat localiza, Filebeat inicia un recolector.
- Cada recolector lee un registro único para el nuevo contenido y envía los nuevos datos de registro al framework libbeat, que agrega los eventos y envía los datos agregados a la salida que se ha configurado para Filebeat.

Propuestas de Actualización



Propuestas de Actualización

- Beat “Journalbeat”
- Dockerización
- Monitorización de portátiles mediante los logs de DHCP.



