

QUÉ HACE TU ASTERISK CUANDO NO MIRAS

Elio Rojano

VOIP2DAY
2016



Quién Soy...

- **Elio Rojano**  @hellc2
- Linuxero y defensor del Software Libre
- Más de 12 años trabajando diariamente con VoIP y Asterisk
- Creador de la web sinologic.net
- Co-creador de la comunidad **Asterisk-ES**
- Consultor y desarrollador de software
- Lector de libros sobre gatitos, perritos y cerditos desde hace 2 años

Introducción



AsteriskTM

Introducción

Por desgracia, existen ciertas razones por las que no podemos estar siempre del CLI controlando qué ocurre en nuestro Asterisk...



eat



sleep

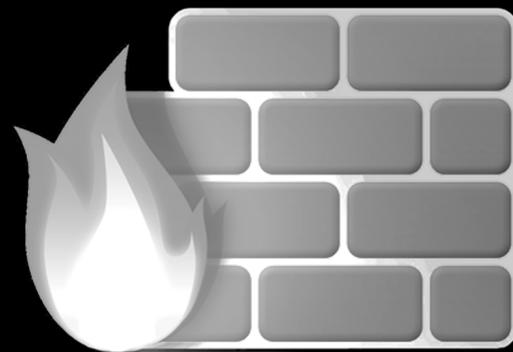


code

Además de que existen otras herramientas que no tienen CLI y que también tenemos que controlar...



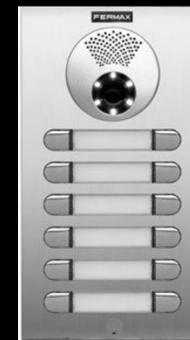
Otras herramientas de comunicaciones



Seguridad



Tráfico de red



Accesos



Gestión de colas Agentes y llamadas



Cuándo se pulsa un botón

Guardando lo que ocurre cuando no estamos:

La importancia de los LOGS

Logs

Un archivo de *LOG* debe guardar cualquier información que pueda ser relevante para que el usuario pueda conocer qué ha hecho la aplicación en todo momento.

Si analizamos los *logs*, veremos que estos siempre deben llevar el **tiempo** (día, mes, año, hora, minuto y segundo) en el que se realizó la acción, la **categoría** del mensaje, y el **mensaje** en sí.

```
[Nov  6 13:00:24] NOTICE[1327][C-003834d0] chan_sip.c: Call from  
' (82.163.211.145:5074) to extension '019448422882040' rejected  
because extension not found in context 'public'.
```

```
[Nov  6 13:00:27] NOTICE[1327][C-003834d1] chan_sip.c: Call from  
' (82.163.211.145:5074) to extension '019448422882040' rejected  
because extension not found in context 'public'.
```

```
[Nov  6 13:00:29] NOTICE[1327][C-003834d2] chan_sip.c: Call from
```

Logs



— /etc/asterisk

— /usr/sbin/asterisk

— /usr/lib/asterisk

— /var/lib/asterisk

— /var/spool/asterisk

/var/log/asterisk



/etc/asterisk/logger.conf

```
[logfiles]
```

```
;; hundreds of comments about how this file works..
```

```
;debug => debug
```

```
console => notice,warning,error
```

```
;console => notice,warning,error,debug
```

```
messages => notice,warning,error,security
```

```
;full => notice,warning,error,debug,verbose,dtmf,fax
```

```
;syslog.local10 => notice,warning,error
```

```
/var/log/asterisk/messages  
/var/log/asterisk/full
```

Logs

Por esta regla de tres, si cada aplicación guarda su archivo de log, tendremos un directorio `/var/log` con cientos de archivos, cada uno de una aplicación diferente.

Para evitar esto, se utiliza una herramienta/protocolo llamado **syslog**



Logs

-“Disponer de **demasiada información** oculta lo verdaderamente importante.”

Logs

Analizando los logs, podemos...

- **Ver qué ha ocurrido en un momento determinado...**
- **Programar alertas para que nos avise en momentos críticos...**
- **Procesarlos para generar informes estadísticos interesantes...**



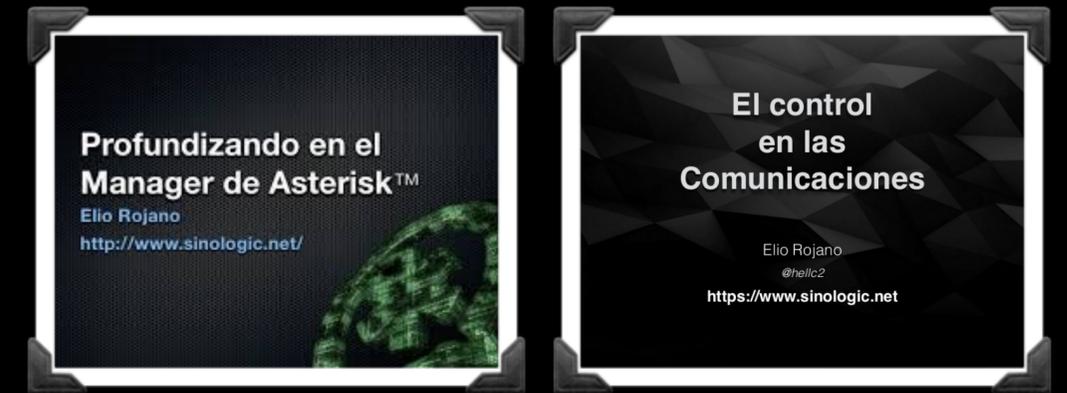
Logs

Asterisk, además de logs, dispone de otros métodos para reportar qué hace en cada momento:

AMI (Asterisk Manager Interface)

ARI (Asterisk Rest Interface)

CLI (Console Line Interface)



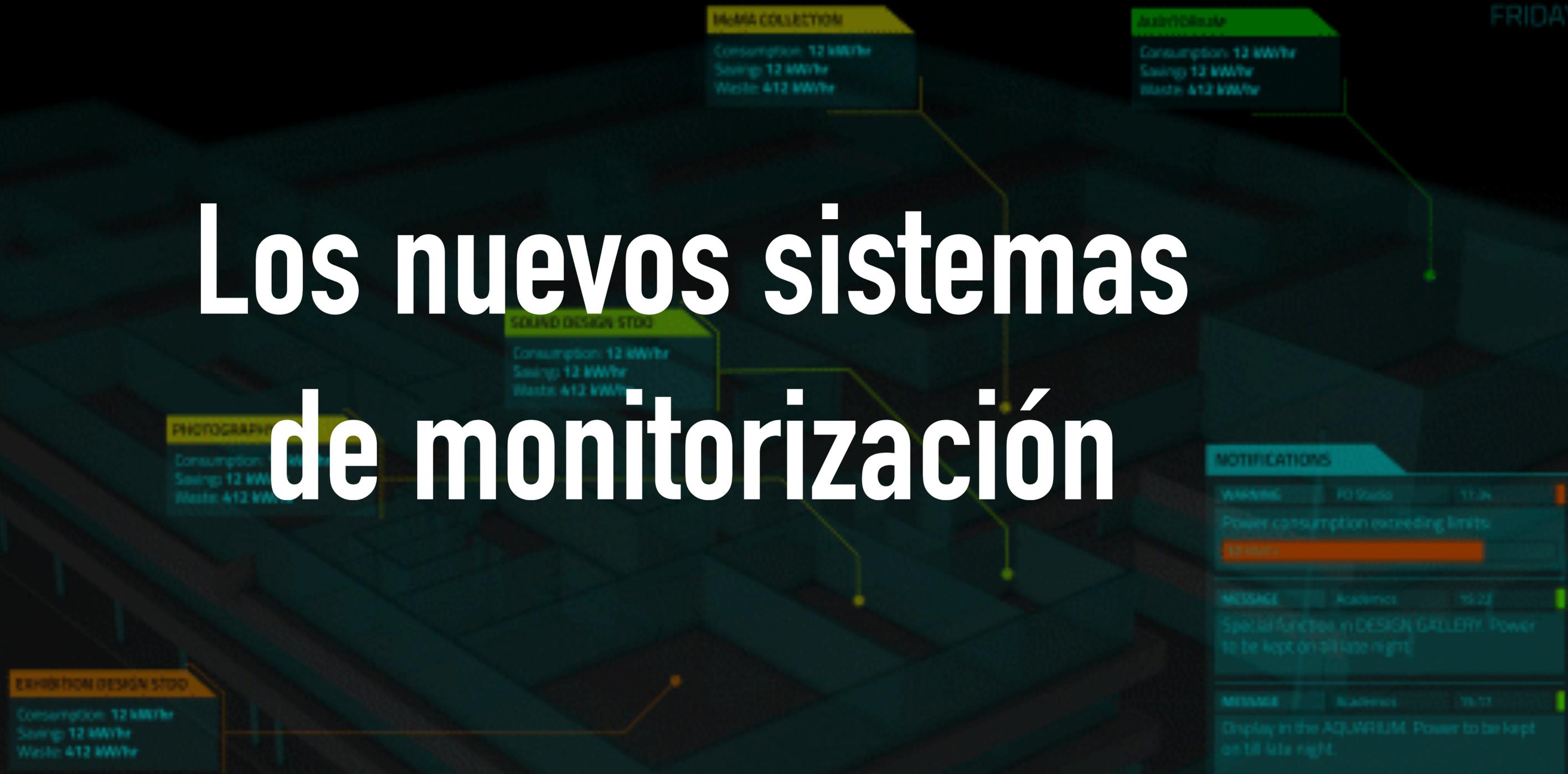
<http://www.slideshare.net/hellc2>

Pero también incorpora algunas características nuevas...

Los nuevos sistemas de monitorización

CONSUMPTION

Total consumption:
1018 kW/hr
Current cost:
Rs. 32,435



NOTIFICATIONS

WARNING | PO Studio | 18:06
Power consumption exceeding limits
12 kW/hr

MESSAGE | Academics | 18:21
Special function in DESIGN GALLERY. Power to be kept on till late night.

MESSAGE | Academics | 18:11
Display in the AQUARIUM. Power to be kept on till late night.

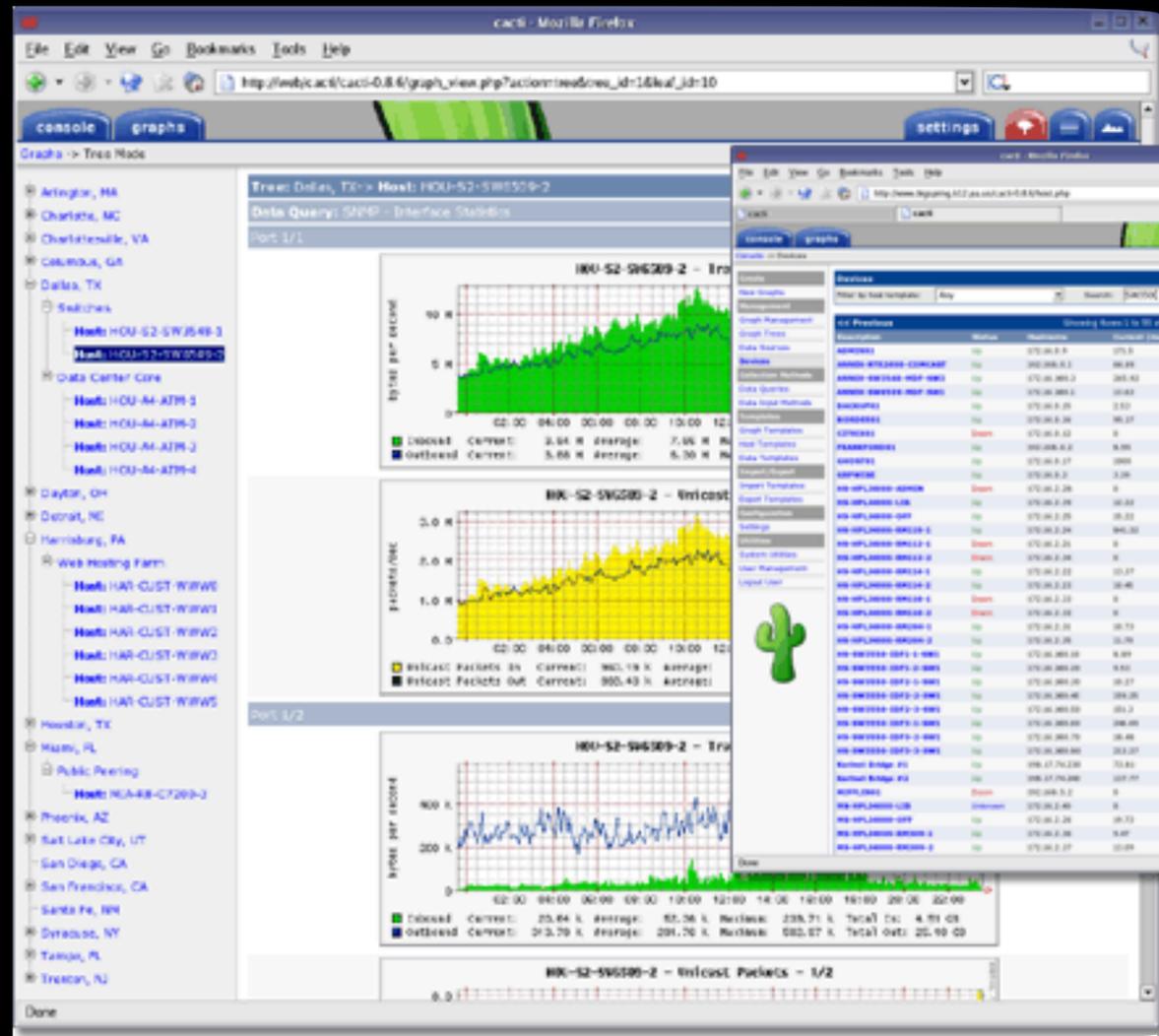
Visión Global

Antiguamente se utilizaba lo siguiente:

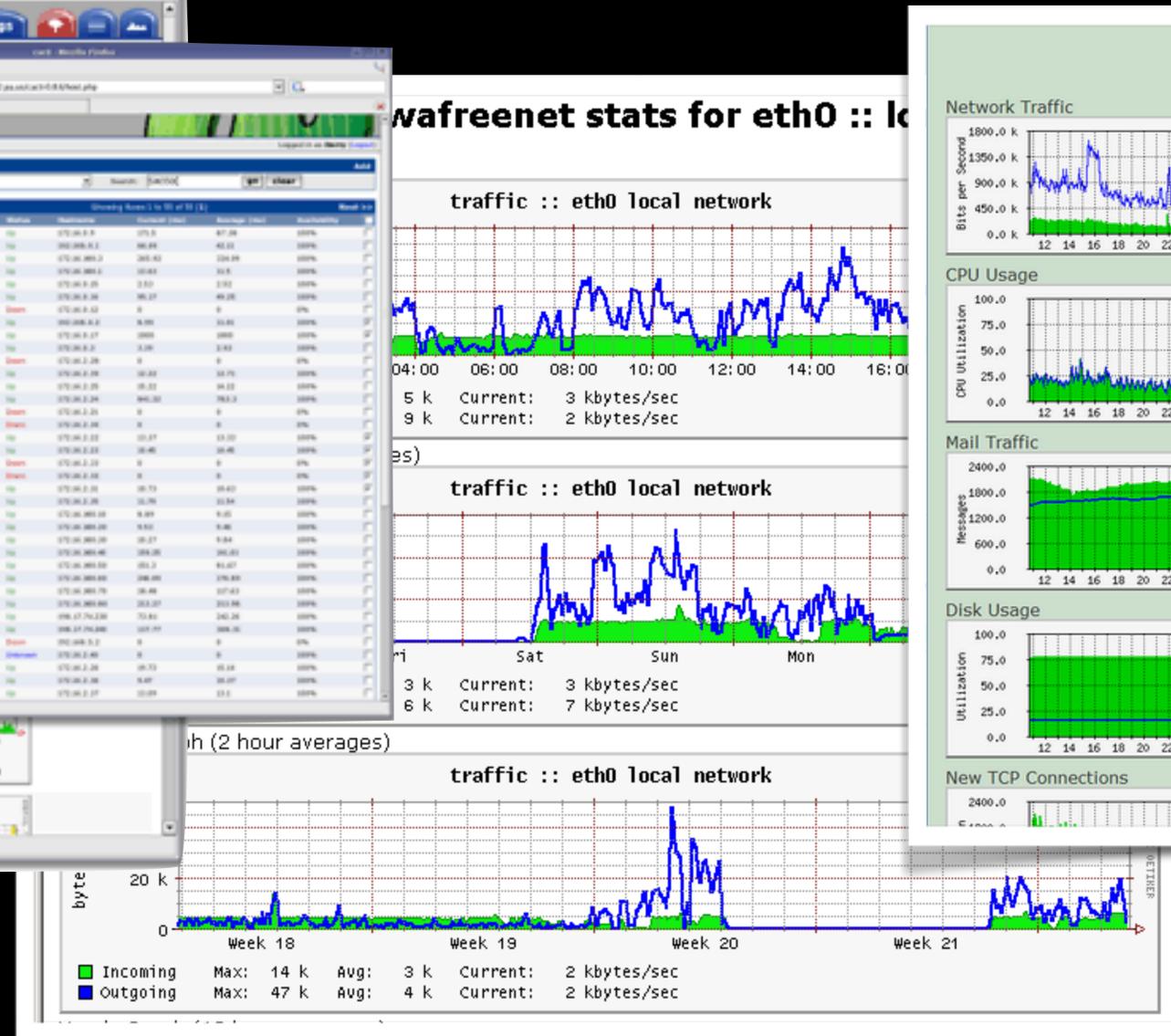


Visión Global

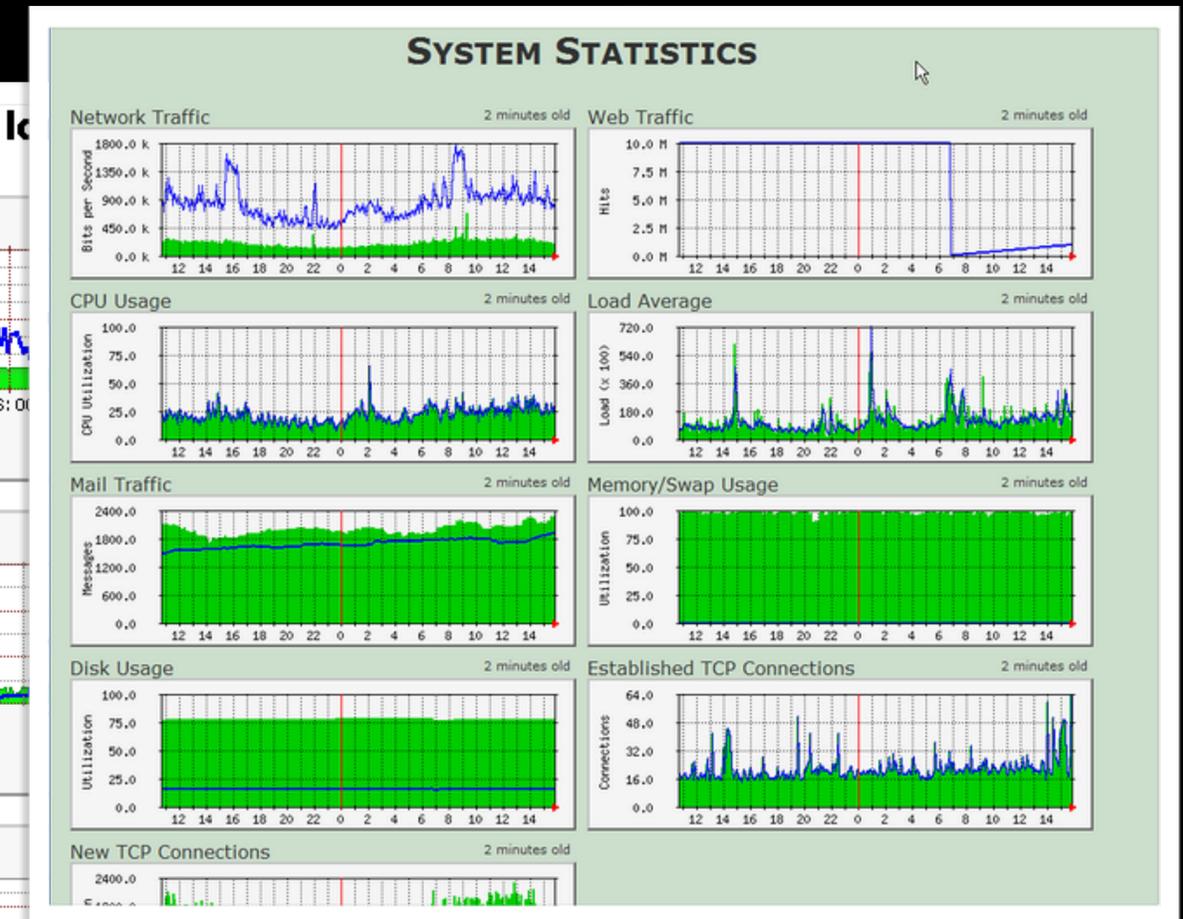
Y se obtenían algunas páginas y gráficas muy interesantes:



CACTI



MRTG



RRDTOOL

Sistemas de Monitorización

ELK

Graphite

InfluxData

Mostrar



Kibana

Graphite-web

Chronograf

Almacenar



ElasticSearch

Whisper

InfluxDB

Capturar



Logstash

Carbon

Telegraf

Sistemas de Monitorización

Mostrar

Servicios



Almacenar

Sistema Operativo



Capturar

Hardware



Sistemas de Monitorización

SNMP

Simple Network Management Protocol

Un protocolo muy útil y práctico aunque poco intuitivo

Mostrar

Almacenar

Capturar

Qué demonios es

1.3.6.1.4.868.2.4.1.2.1.1.1.3.3562.3 !?

Iso(1)
 org(3)
 dod(6)
 internet(1)
 private(4)
 transition(868)
 products(2)
 chassis(4)

...

Sistemas de Monitorización

Mostrar

Almacenar

Capturar

StatsD

<https://github.com/etsy/statsd>



...

Sistemas de Monitorización

Mostrar

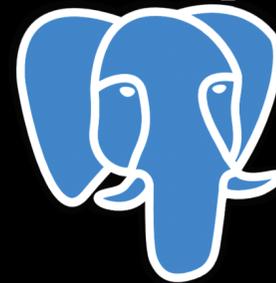
Almacenar

Capturar

CollectD

<https://collectd.org/>

SNMP



MySQL®



...

Sistemas de Monitorización

Mostrar



Logstash

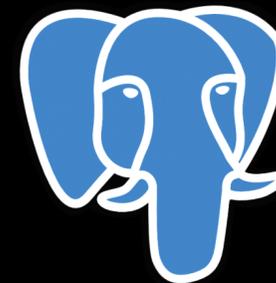


Graylog

Almacenar

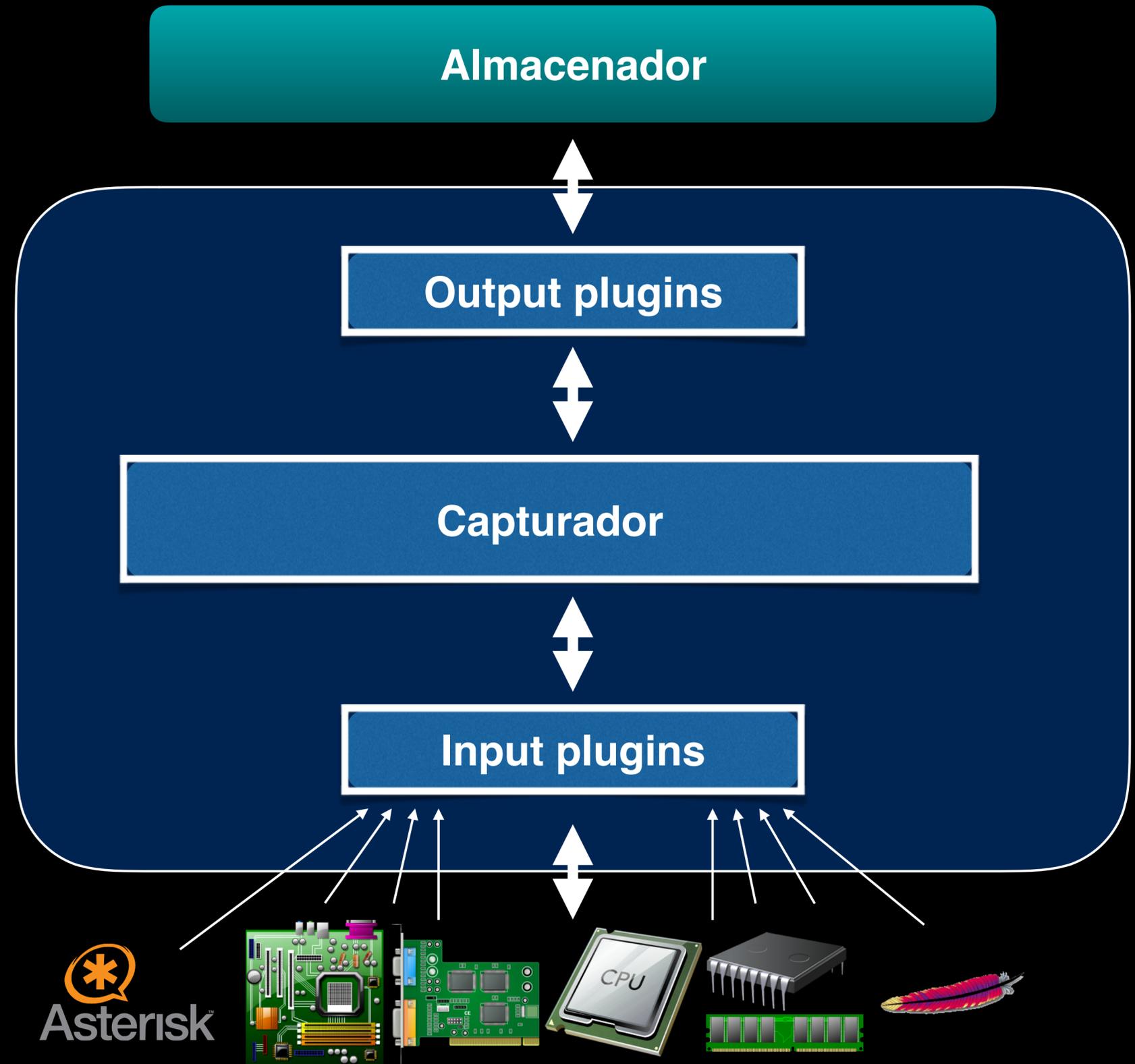
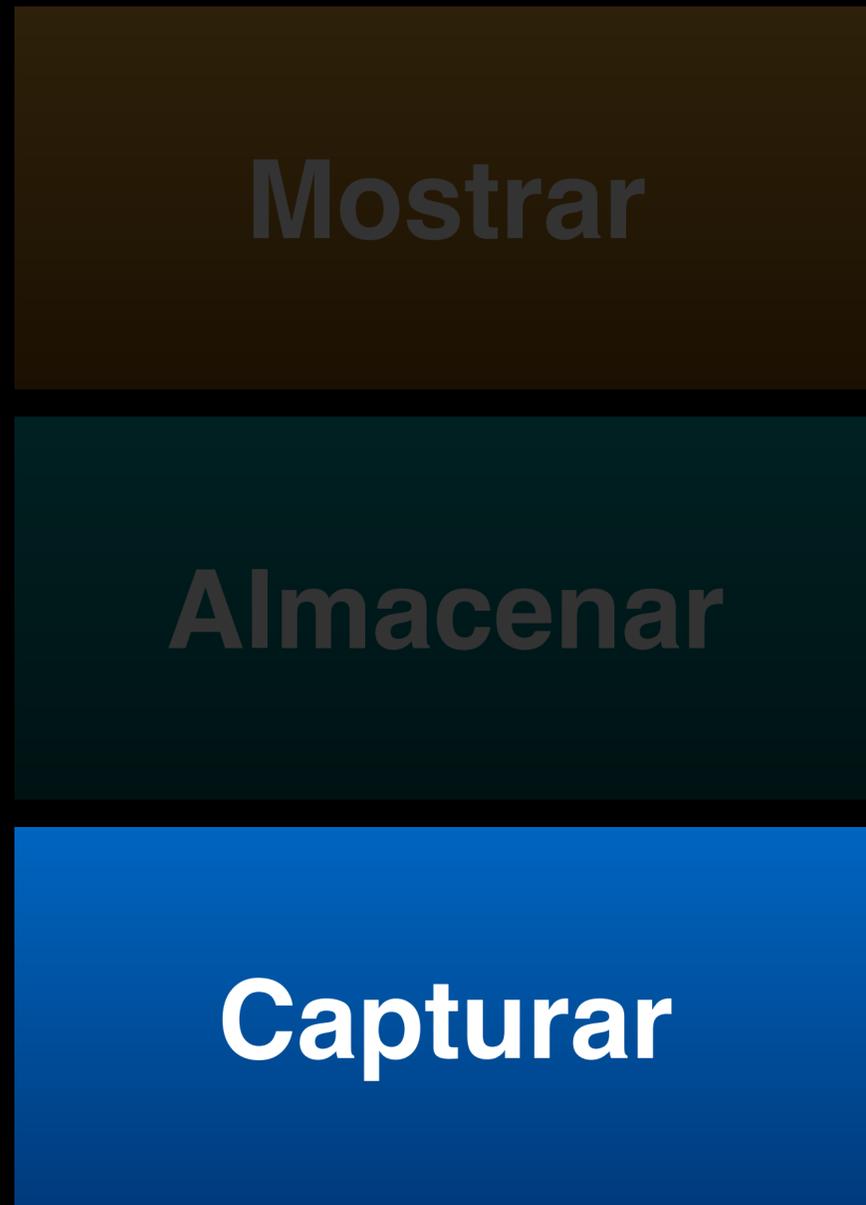


Capturar



mongoDB®

Sistemas de Monitorización



Sistemas de Monitorización

Bases de datos especiales

Rápidas pero orientadas a almacenar valores y tiempos

Mostrar

Almacenar

Capturar

Asistentes a la conferencia	
<i>Time</i>	<i>Value</i>
2016-11-16 12:24:31	25
2016-11-16 12:24:32	26
2016-11-16 12:24:33	26
2016-11-16 12:24:34	25



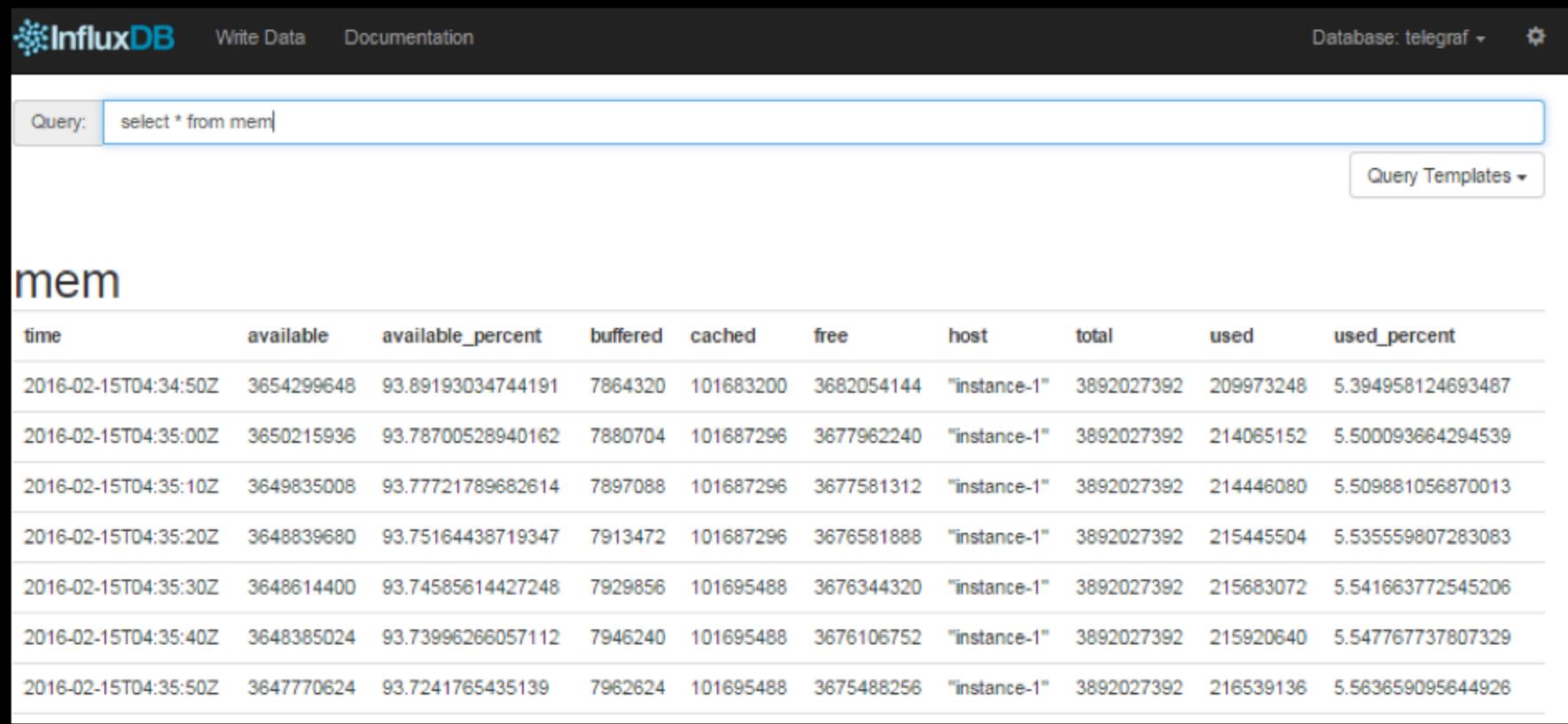
Sistemas de Monitorización

Mostrar

Almacenar

Capturar

- Bases de datos no relacionales
- Basados en SQL, pero bastante limitadas
- Para ser rápidos, se sacrifican funcionalidades
- Almacenan valores simples (decimales, enteros, ...)
- La gestión se suele hacer vía JSON o interfaz web



The screenshot shows the InfluxDB web interface. At the top, there are links for 'Write Data' and 'Documentation', and a dropdown menu for 'Database: telegraf'. A query input field contains 'select * from mem'. Below the query, the results are displayed in a table with the following columns: time, available, available_percent, buffered, cached, free, host, total, used, and used_percent. The table contains seven rows of data representing memory usage over time.

time	available	available_percent	buffered	cached	free	host	total	used	used_percent
2016-02-15T04:34:50Z	3654299648	93.89193034744191	7864320	101683200	3682054144	"instance-1"	3892027392	209973248	5.394958124693487
2016-02-15T04:35:00Z	3650215936	93.78700528940162	7880704	101687296	3677962240	"instance-1"	3892027392	214065152	5.500093664294539
2016-02-15T04:35:10Z	3649835008	93.77721789682614	7897088	101687296	3677581312	"instance-1"	3892027392	214446080	5.509881056870013
2016-02-15T04:35:20Z	3648839680	93.75164438719347	7913472	101687296	3676581888	"instance-1"	3892027392	215445504	5.535559807283083
2016-02-15T04:35:30Z	3648614400	93.74585614427248	7929856	101695488	3676344320	"instance-1"	3892027392	215683072	5.541663772545206
2016-02-15T04:35:40Z	3648385024	93.73996266057112	7946240	101695488	3676106752	"instance-1"	3892027392	215920640	5.547767737807329
2016-02-15T04:35:50Z	3647770624	93.7241765435139	7962624	101695488	3675488256	"instance-1"	3892027392	216539136	5.563659095644926

Sistemas de Monitorización

Mostrar

Almacenar

Capturar

 influxDB

MQTT

 Graylog

 Elasticsearch

 Librato

Kinesis

 Kafka

Datadog

Graphite

Sistemas de Monitorización

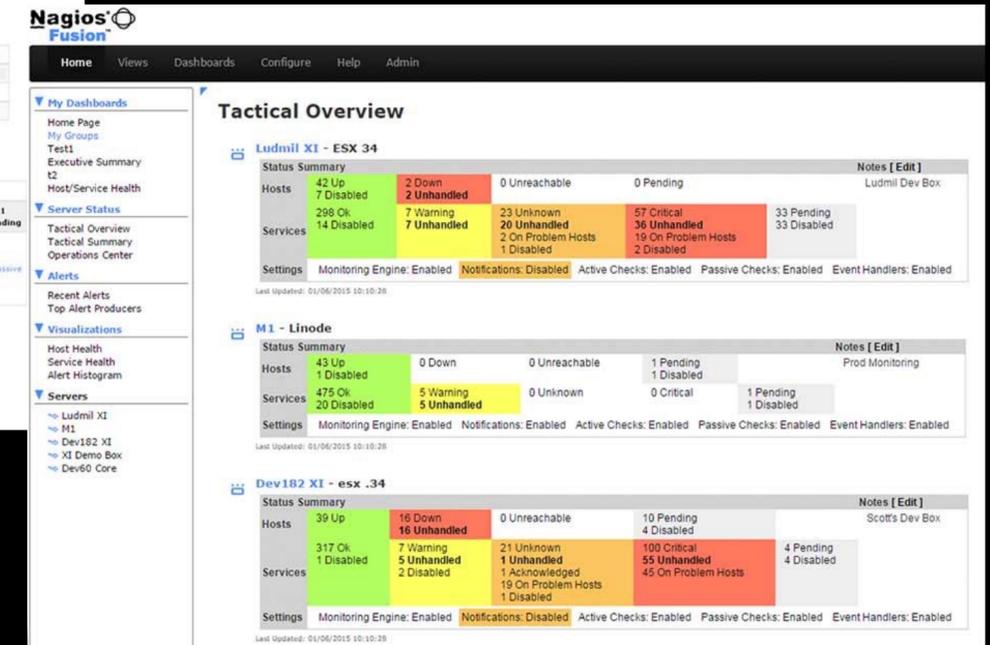
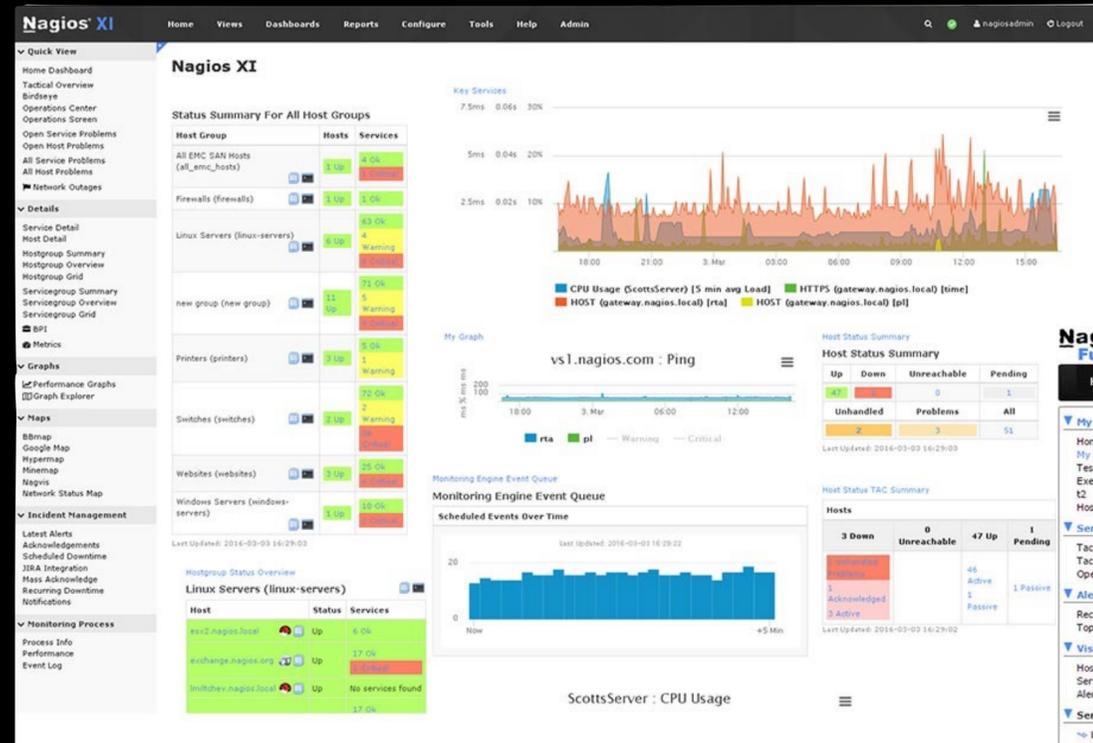
Gráficas, gráficas y más gráficas

Mostrar

También incluye la parte de avisos y alarmas

Almacenar

Capturar



Sistemas de Monitorización

Mostrar

Almacenar

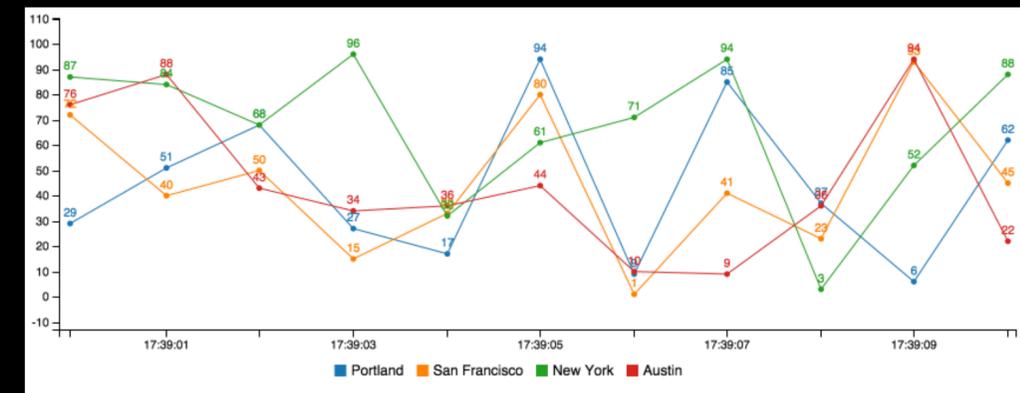
Capturar

Conceptos triviales...

Gauges (indicador)



Counter (contadores)



Sistemas de Monitorización

Mostrar

Almacenar

Capturar

1.- Configuramos la fuente de datos

influxDB Instrumental Kinesis
Elastixsearch Datadog Librato
Kafka graphite grayLog

2.- Seleccionamos los datos que queremos ver

3.- Configuramos el aspecto del dashboard

4.- Configuramos los valores críticos para alertas

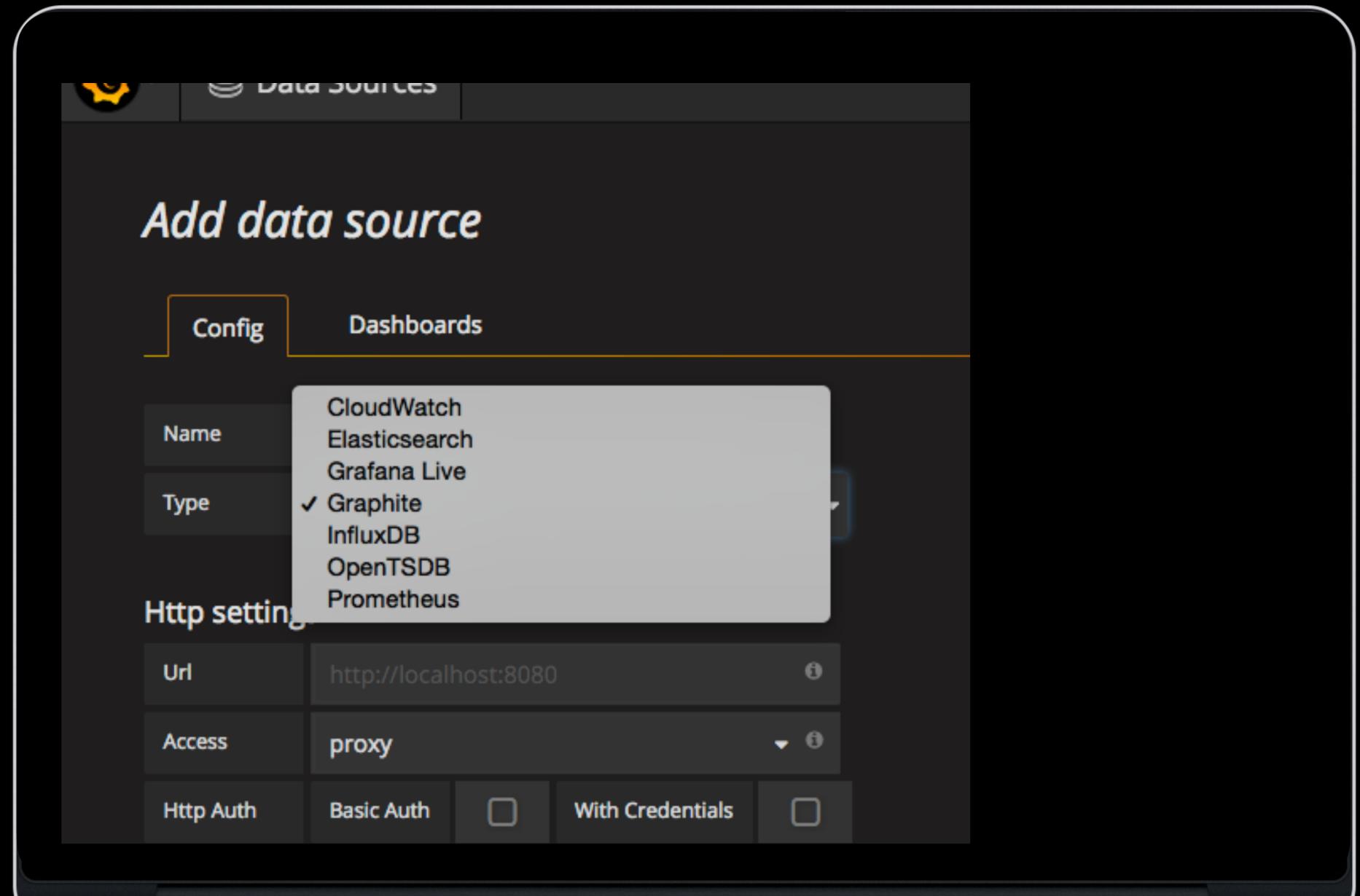
Sistemas de Monitorización

Son tan flexibles que trabajan con casi todos los sistemas de almacenamiento que hemos hablado antes.

Mostrar

Almacenar

Capturar



Sistemas de Monitorización

Aplicaciones web con editores de estilo para personalizar los datos y gráficas que queremos ver.

Mostrar

Almacenar

Capturar



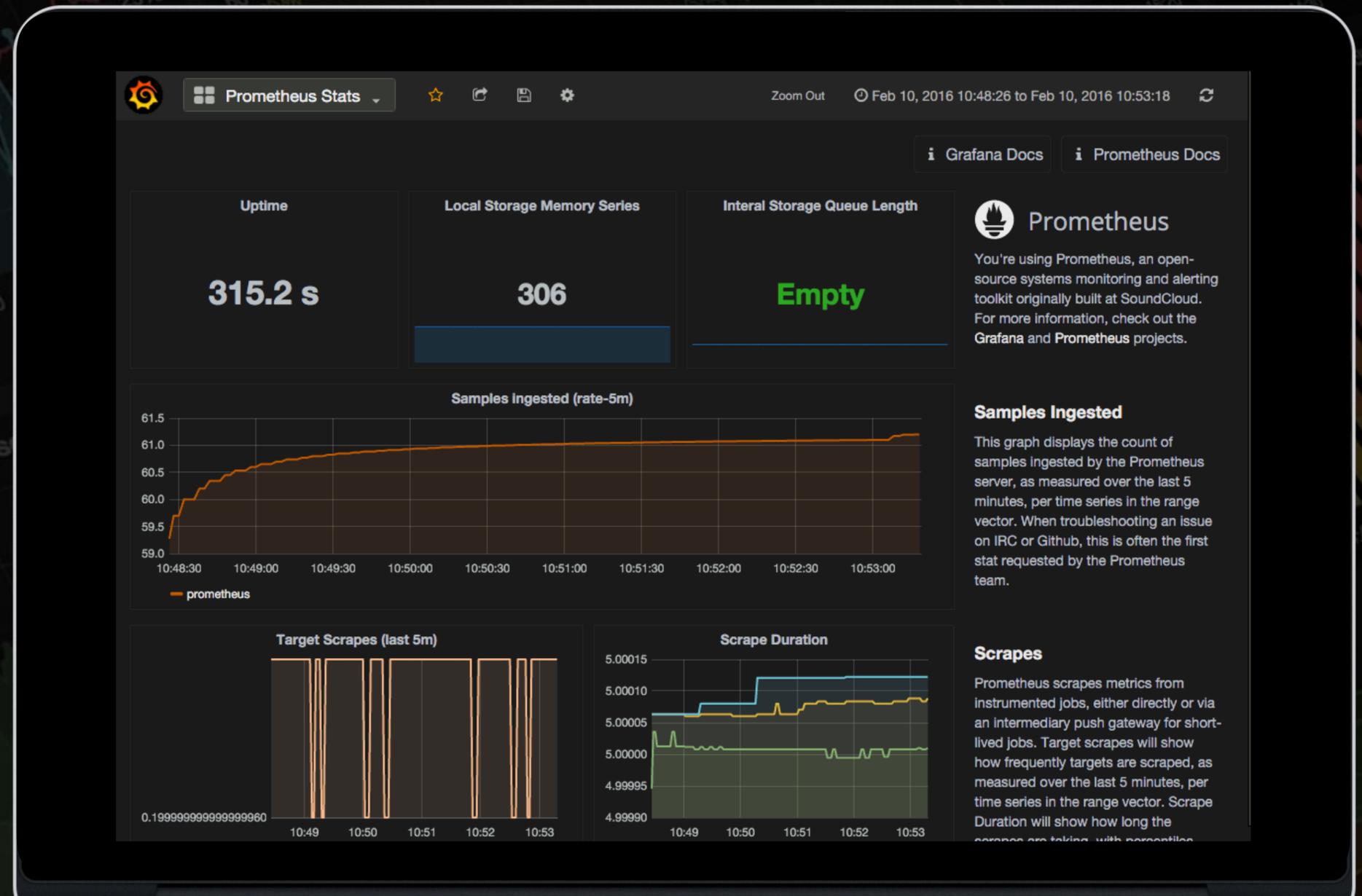
Sistemas de Monitorización

Aplicaciones web con editores de estilo para personalizar los datos y gráficas que queremos ver.

Mostrar

Almacenar

Capturar



Sistemas de Monitorización

Aplicaciones web con editores de estilo para personalizar los datos y gráficas que queremos ver.

Mostrar

Almacenar

Capturar



Grafana

Sistemas de Monitorización

Aplicaciones web con editores de estilo para personalizar los datos y gráficas que queremos ver.

Mostrar

Almacenar

Capturar



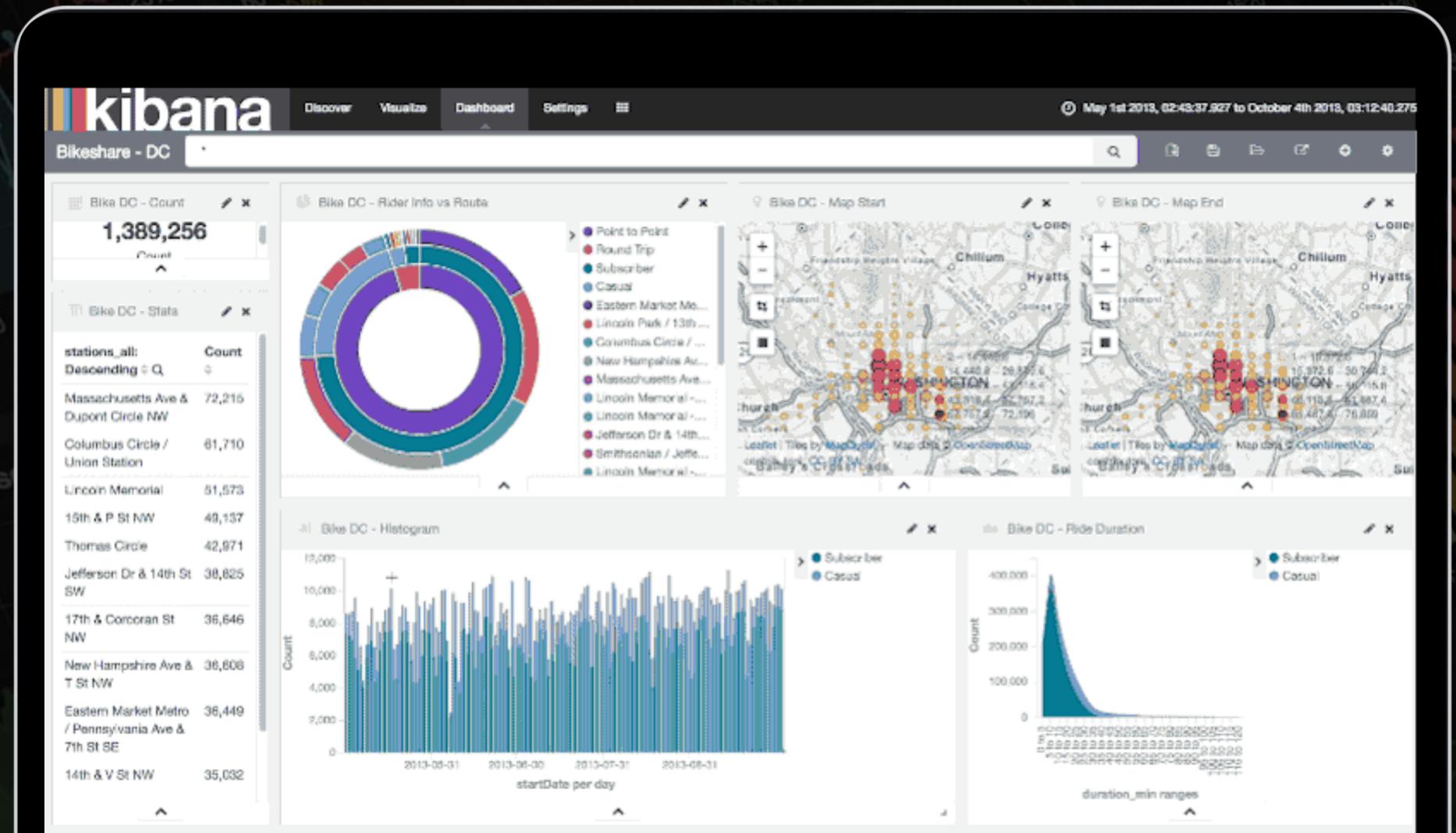
Sistemas de Monitorización

Aplicaciones web con editores de estilo para personalizar los datos y gráficas que queremos ver.

Mostrar

Almacenar

Capturar



Kibana

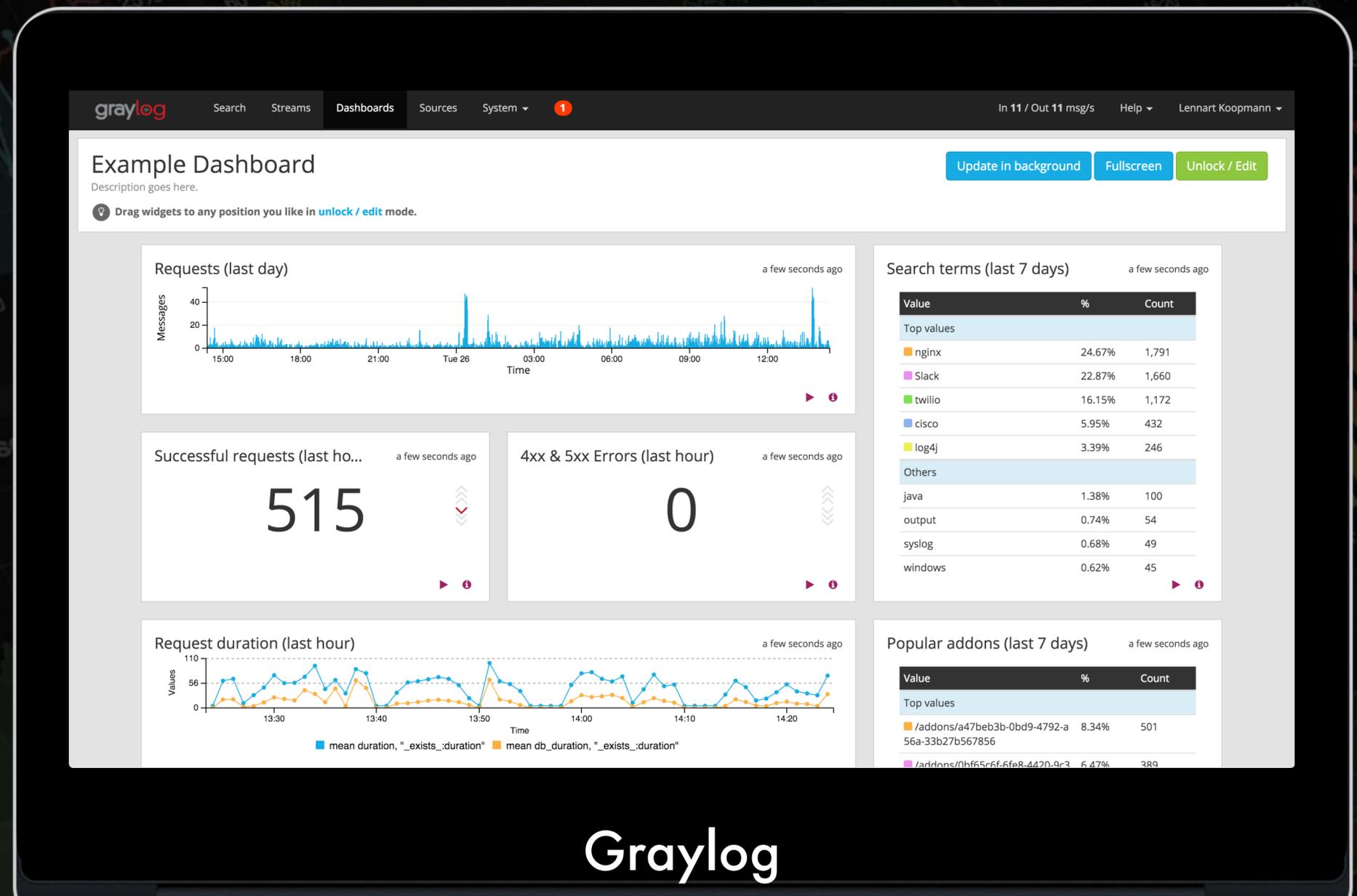
Sistemas de Monitorización

Aplicaciones web con editores de estilo para personalizar los datos y gráficas que queremos ver.

Mostrar

Almacenar

Capturar



Graylog

Sistemas de Monitorización

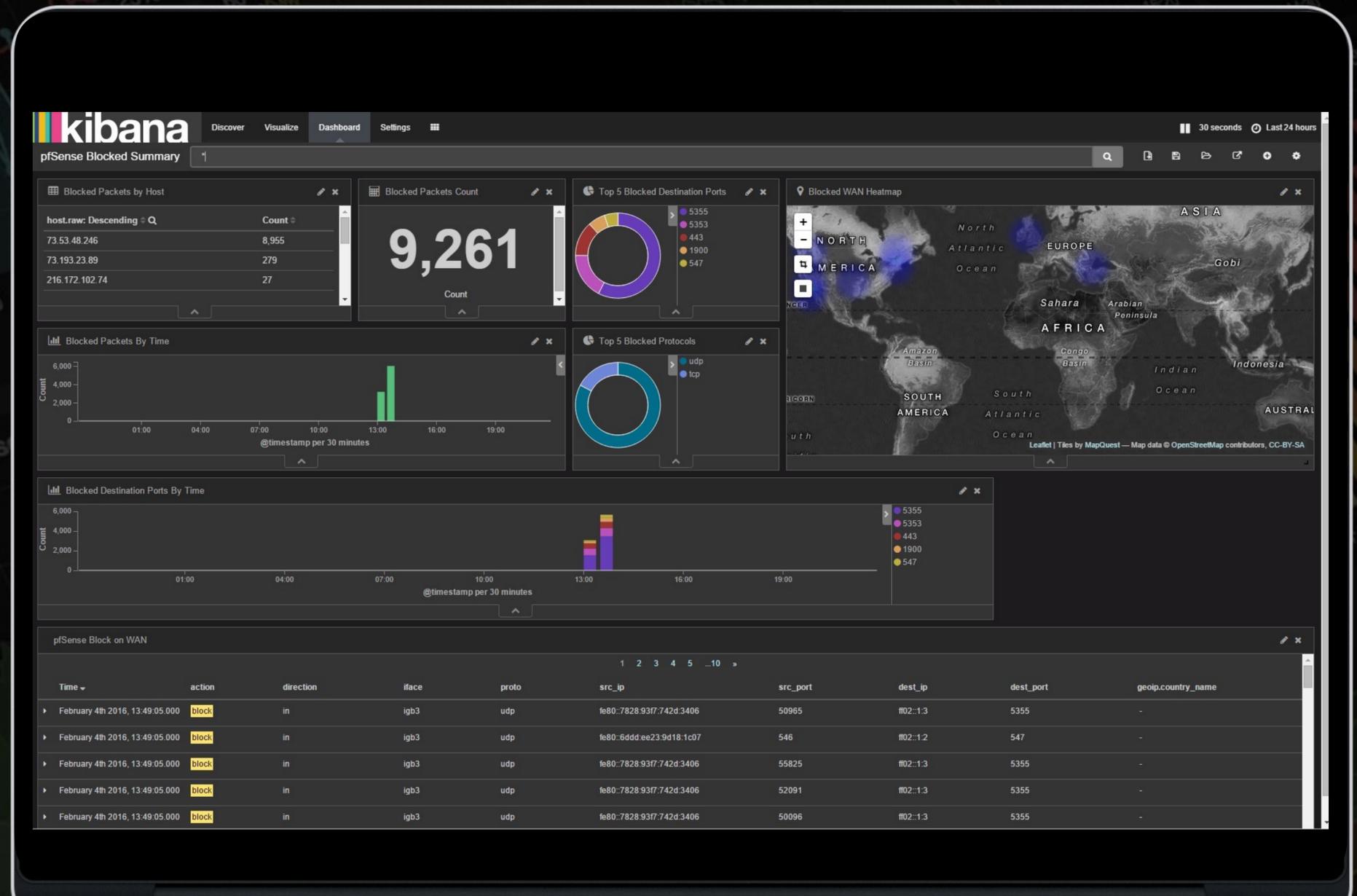


Monitorizando pfSense con ELK...

Mostrar

Almacenar

Capturar



Cómo hacer esto con



AsteriskTM

Utilizando STATSd

<https://github.com/etsy/statsd>

A partir de **Asterisk 14***

Cómo monitorizar Asterisk

Asterisk 13 y 14 incluyen un conector con StatsD que permite a Asterisk hacer de cliente y conectarse a un servidor StatsD para enviarle información sobre llamadas, canales, etc.

Para ello, debemos compilar Asterisk para que lo soporte.

```
[*] app_sms
[ ] app_statsd
[*] app_test

[*] res_snmp
[*] res_statsd
XXX res_timing_queue
```

-- Info about application 'StatsD' --

[Synopsis]

Allow statistics to be passed to the StatsD server from the dialplan.

[Description]

This dialplan application sends statistics to the StatsD server specified inside of 'statsd.conf'.

[Syntax]

StatsD(metric_type,statistic_name,value[,sample_rate])

[Arguments]

metric_type

The metric type to be sent to StatsD. Valid metric types are 'g' for gauge, 'c' for counter, 'ms' for timer, and 's' for sets.

statistic_name

The name of the variable to be sent to StatsD. Statistic names cannot contain the pipe (|) character.

value

The value of the variable to be sent to StatsD. Values must be numeric. Values for gauge and counter metrics can be sent with a '+' or '-' to update a value after the value has been initialized. Only counters can be initialized as negative. Sets can send a string as the value parameter, but the string cannot contain the pipe character.

sample_rate

The value of the sample rate to be sent to StatsD. Sample rates less than or equal to 0 will never be sent and sample rates greater than or equal to 1 will always be sent. Any rate between 1 and 0 will be compared to a randomly generated value, and if it is greater than the random value, it will be sent.

[See Also]

Not available

Con esos dos módulos dispondremos de una aplicación que nos permite enviar valores a StatsD mediante el dialplan.

Cómo monitorizar Asterisk

Una vez tengamos esos módulos, ya podemos usar el código de dialplan para enviar a StatsD nuestros propios valores:

statsd.conf

```
[general]
enabled = yes           ; When set to yes, statsd support is enabled
server = 127.0.0.1     ; server[:port] of statsd server to use.
                       ; If not specified, the port is 8125
;prefix =              ; Prefix to prepend to all metrics
;add_newline = no      ; Append a newline to every event. This is
                       ; useful if you want to run a fake statsd
                       ; server using netcat (nc -lu 8125)
```

extension.conf

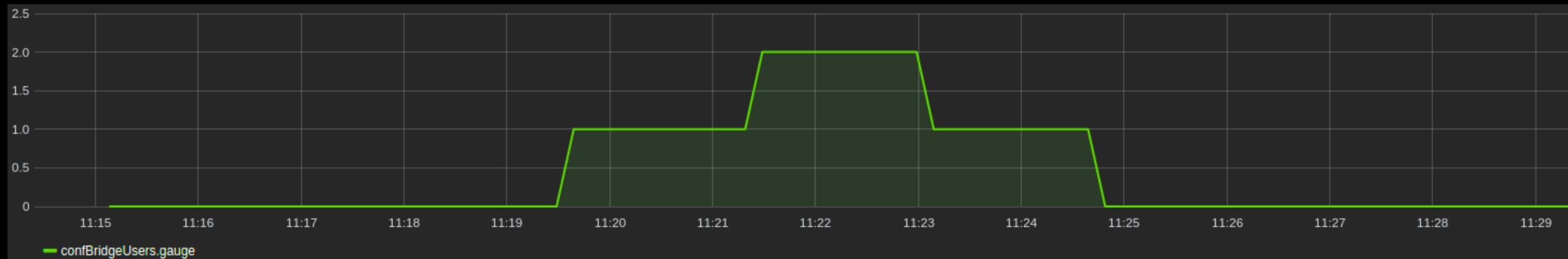
```
[default]

exten => 100,1,NoOp()
    same => n,StatsD(g,confBridgeUsers,+1,1)
    same => n,Set(CHANNEL(hangup_handler_push)=default,200,1);
    same => n,ConfBridge(1000)
    same => n,StatsD(g,confBridgeUsers,-1,1)
    same => n,Hangup()

exten => 200,1,NoOp()
    same => n,StatsD(g,confBridgeUsers,-1,1)
    same => n,Hangup()
```

Más información:

<https://wiki.asterisk.org/wiki/display/AST/Utilizing+the+StatsD+Dialplan+Application>



Conectando Asterisk con todo el sistema



Cómo monitorizar Asterisk

Si tenemos StatsD configurado, **PJSIP** también lo utiliza para exportar datos de registro, llamadas, usuarios, contacts, etc...

Grafana (por ejemplo) nos permite configurar alertas (v.4.0) cuando ocurren determinados valores:



Cómo monitorizar Asterisk

Tanto los “capturadores” como los “almacenadores” disponen de librerías en la mayoría de lenguajes de programación, por lo que podemos realizar integraciones con nuestras propias soluciones y mostrar los valores a nuestro gusto.





¿Preguntas?

Gracias

Agradecimientos a:

- a **Rosa Atienza** y **Pablo** (por su tiempo, paciencia y consejos)
- a **Tomás Sahagún** (por descubrirme ciertos mundos)
- a **Javier Vidal** y **Robert** (por su amistad, apoyo, soporte, ayuda y tantas cosas...)
- a **Avanzada 7** (por organizar el V2D y por muchas cosas más...)
- a vosotros que habéis aguantado todo este rato. ;)
- y un agradecimiento muy especial a **los lectores de sinologic.net**, ya que gracias a ellos...

Hoy **SINOLOGIC.NET** cumple
10 años