ELK + Grafana
Conferencia sobre gestión de logs en servicios fundamentales.

¿Que es Elasticsearch?

Elasticsearch es un servidor de búsqueda basado en Lucene. Provee un motor de búsqueda de texto completo, distribuido y con capacidad de multi-tenencia con una interfaz web RESTful y con documentos JSON. Elasticsearch está desarrollado en Java y está publicado como código abierto bajo las condiciones de la licencia Apache.

¿Qué es Logstash?

Logstash es una herramienta para la administración de logs. Todo tipo de logs. Logs de sistema, de servidor, de errores, de aplicación. Básicamente es capaz de leer todo lo que le eches.

Se encarga de recolectar, parsear y filtrar los logs para posteriormente darles alguna salida como, almacenarlos en MongoDB, enviarlos por correo electrónico o, como en nuestro caso guardarlos en Elasticsearch.

Estos logs le pueden llegar a Losgstash desde el mismo servidor o desde un servidor externo, por lo que podríamos tener un servidor exclusivo para el stack ELK.

La aplicación se encuentra basada en jRuby y requiere de Java Virtual Machine para correr.

¿Qué es Kibana?

Kibana es una herramienta analítica open source (licencia Apache) que nos va a permitir interactuar con la información almacenada (por Logstash) en Elasticsearch y monitorizarla.

¿Cómo funciona el stack ELK?

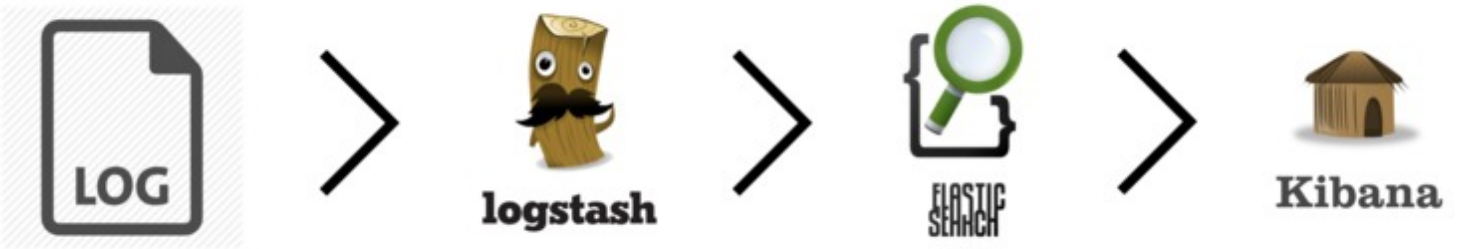
El flujo de información/funcionamiento del stack es el siguiente:

1- Logstash: Es realmente el protagonista de todo esto. Él se va a encargar de la recolección de logs, parsearlos y almacenarlos en Elasticsearch.

2- Elasticsearch: Encargado de almacenar de forma estructurada e indexada toda la información enviada por Logstash.

3- Kibana: Que leerá los datos almacenados por Logstash en Elasticsearch para posteriormente monitorizarlos.

Ilustrando un poco



¿Que es grafana?

Grafana: Es una herramienta para consultar y visualizar series de datos de forma “bonita”. Es una herramienta muy potente, con un editor de consultas muy elaborado que te permite elegir entre las métricas que tengas registradas y realizar con ellas todo el tratamiento que necesites. Como origen de datos también tiene gran variedad, pudiendo elegir entre CloudWatch, ElasticSearch, Graphite, InfluxDB, OpenTSDB o Prometheus.

Ejemplos practicos de logs procesados con estas herramientas

Logs de Correos (Externo a ERMPCFG)

Zoom Out | Last 12 hours

Dominio Origen: All | Dirección de Origen: All | Direccion Destino: All | Intervalo de tiempo: 12h

Hora Actual
2017-10-12
3:45:43 PM

Tráfico entrante

Last 12 hours

Tráfico 79.2 MB

Usuario que más recibe correo

Last 12 hours

Usuario que más recibe correo: maritza@mpcfg.co.cu

Dominio del que más se recibe correo

Last 12 hours

Dominio del que más se recibe correo: uermp.cu

Origen de mensajes de correos

Last 12 hours

Cantidad origen

Last 12 hours

from_domain	Count
uermp.cu	170
gmail.com	44
dpcf.cc.bandec.cu	40
alerts.bounces.google.com	20
yahoo.es	12
feedburner.bounces.google.com	11
cuvenpetrol.cu	9
yahoo.com	7
twoomail.com	7
jovenclub.cu	7
hotmail.com	7
nl.telesurtv.net	6
nauta.cu	6
explore.pinterest.com	6
cfg.jovenclub.cu	6
acinoxtunas.co.cu	6
google.com	5

Panel Title

Last 12 hours

Show 10 entries Search:

@timestamp	from	to	Count
2017-10-12 15:44:45	suc4571@dpcf.cc.bandec.cu	bmaguada@mpcfg.co.cu	1
2017-10-12 15:44:10	suc4871@dpcf.cc.bandec.cu	bmabreus@mpcfg.co.cu	1
2017-10-12 15:43:52	suc4871@dpcf.cc.bandec.cu	bmabreus@mpcfg.co.cu	1
2017-10-12 15:32:59	cristinauribe@uermp.cu	carmen@mpcfg.co.cu	1
2017-10-12 15:32:59	cristinauribe@uermp.cu	maritza@mpcfg.co.cu	1
2017-10-12 15:31:50	suc4711@dpcf.cc.bandec.cu	bmcruces@mpcfg.co.cu	1
2017-10-12 15:06:19	piloto@cfg.emgef.une.cu	cecilia@mpcfg.co.cu	1
2017-10-12 14:57:07	laura@uermp.cu	carmen@mpcfg.co.cu	1
2017-10-12 14:54:02	olgasosa2010@hotmail.com	oladys@mpcfg.co.cu	1
2017-10-12 14:49:17	cgcartaya@esicf.azcuba.cu	ybarmax@mpcfg.co.cu	1

Showing 1 to 10 of 435 entries First Previous 1 2 3 4 5 ... 44 Next Last

Usuarios que más reciben correos

Last 12 hours

to	Count
maritza@mpcfg.co.cu	71
ybarmax@mpcfg.co.cu	34
cecilia@mpcfg.co.cu	34
marilis@mpcfg.co.cu	29
onelva@mpcfg.co.cu	25
omar@mpcfg.co.cu	24
jesus@mpcfg.co.cu	22
islenia@mpcfg.co.cu	20
sadys@mpcfg.co.cu	19
diana@mpcfg.co.cu	19

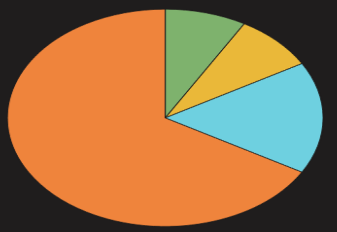
Alertas Detalladas

Last 12 hours

@timestamp	from	to
12/10/17 2:14:39 pm	edting022@yahoo.com	mailmp
12/10/17 2:14:29 pm	sales@p113.yzvip.shop	mailmp
12/10/17 2:14:16 pm	comercial@ersucav.co.cu	odaly@m

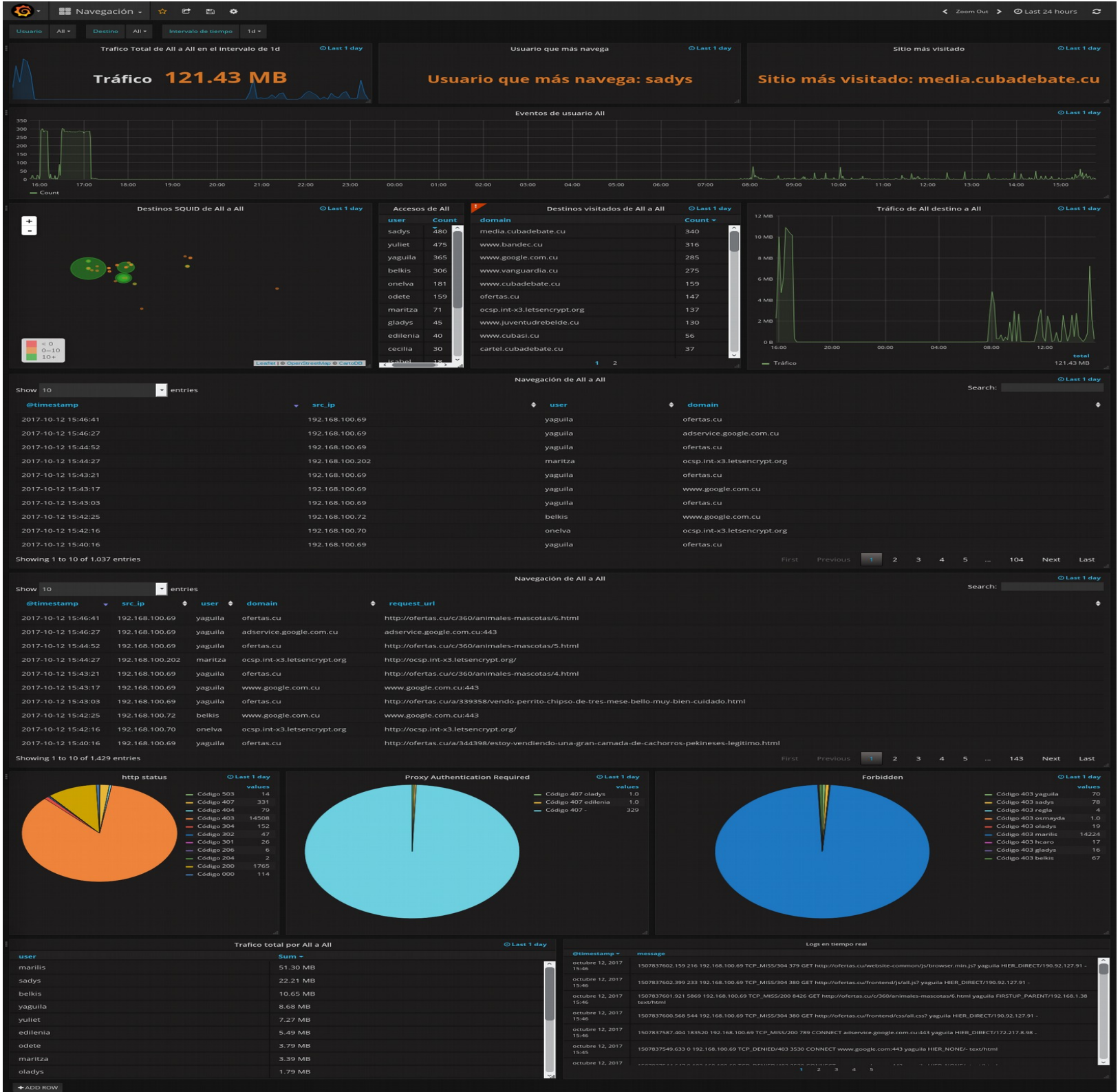
Alertas

Last 12 hours



	values
Alerta: Sender address rejected: Solo correo nacional	1.0
Alerta: Sender address rejected: Correo Internacional Limitado	1.0
Alerta: Relay access denied	2
Alerta: Recipient address rejected: mpcfg.co.cu	8

+ ADD ROW


Navegación
Zoom Out
Last 24 hours
Usuario
All
Destino
All
Intervalo de tiempo
1d
Trafico Total de All a All en el intervalo de 1d
Last 1 day
Tráfico 121.43 MB
Usuario que más navega
Usuario que más navega: sadys
Sitio más visitado
Sitio más visitado: media.cubadebate.cu
Eventos de usuario All
Count
Destinos SQUID de All a All
Leaflet | © OpenStreetMap © CartoDB
Accesos de All
user Count
sadys 480
yuliet 475
yaguila 365
belkis 306
onelva 181
odete 159
maritza 71
gladys 45
edilenia 40
cecilia 30
Destinos visitados de All a All
domain Count
media.cubadebate.cu 340
www.bandec.cu 316
www.google.com.cu 285
www.vanguardia.cu 275
www.cubadebate.cu 159
ofertas.cu 147
ocsp.int-x3.letsencrypt.org 137
www.juventudrebelde.cu 130
www.cubasi.cu 56
cartel.cubadebate.cu 37
Tráfico de All destino a All
Tráfico
total
121.43 MB
Navegación de All a All
Show 10 entries
Search:
@timestamp src_ip user domain
2017-10-12 15:46:41 192.168.100.69 yaguila ofertas.cu
2017-10-12 15:46:27 192.168.100.69 yaguila adservice.google.com.cu
2017-10-12 15:44:52 192.168.100.69 yaguila ofertas.cu
2017-10-12 15:44:27 192.168.100.202 maritza ocsp.int-x3.letsencrypt.org
2017-10-12 15:43:21 192.168.100.69 yaguila ofertas.cu
2017-10-12 15:43:17 192.168.100.69 yaguila www.google.com.cu
2017-10-12 15:43:03 192.168.100.69 yaguila ofertas.cu
2017-10-12 15:42:25 192.168.100.72 belkis www.google.com.cu
2017-10-12 15:42:16 192.168.100.70 onelva ocsp.int-x3.letsencrypt.org
2017-10-12 15:40:16 192.168.100.69 yaguila ofertas.cu
Showing 1 to 10 of 1.037 entries
First Previous 1 2 3 4 5 ... 104 Next Last
Navegación de All a All
Show 10 entries
Search:
@timestamp src_ip user domain request_url
2017-10-12 15:46:41 192.168.100.69 yaguila ofertas.cu http://ofertas.cu/c/360/animales-mascotas/6.html
2017-10-12 15:46:27 192.168.100.69 yaguila adservice.google.com.cu adservice.google.com.cu:443
2017-10-12 15:44:52 192.168.100.69 yaguila ofertas.cu http://ofertas.cu/c/360/animales-mascotas/5.html
2017-10-12 15:44:27 192.168.100.202 maritza ocsp.int-x3.letsencrypt.org http://ocsp.int-x3.letsencrypt.org/
2017-10-12 15:43:21 192.168.100.69 yaguila ofertas.cu http://ofertas.cu/c/360/animales-mascotas/4.html
2017-10-12 15:43:17 192.168.100.69 yaguila www.google.com.cu www.google.com.cu:443
2017-10-12 15:43:03 192.168.100.69 yaguila ofertas.cu http://ofertas.cu/a/339358/vendo-perrito-chipso-de-tres-mese-bello-muy-bien-cuidado.html
2017-10-12 15:42:25 192.168.100.72 belkis www.google.com.cu www.google.com.cu:443
2017-10-12 15:42:16 192.168.100.70 onelva ocsp.int-x3.letsencrypt.org http://ocsp.int-x3.letsencrypt.org/
2017-10-12 15:40:16 192.168.100.69 yaguila ofertas.cu http://ofertas.cu/a/344398/estoy-vendiendo-una-gran-camada-de-cachorros-pekineses-legitimo.html
Showing 1 to 10 of 1.429 entries
First Previous 1 2 3 4 5 ... 143 Next Last
http status
values
Código 503 14
Código 407 331
Código 404 79
Código 403 14508
Código 304 152
Código 302 47
Código 301 26
Código 206 6
Código 204 2
Código 200 1765
Código 000 114
Proxy Authentication Required
values
Código 407 oladys 1.0
Código 407 edilenia 1.0
Código 407 - 329
Forbidden
values
Código 403 yaguila 70
Código 403 sadys 78
Código 403 regla 4
Código 403 osmayda 1.0
Código 403 oladys 19
Código 403 marilis 14224
Código 403 hcaro 17
Código 403 gladys 16
Código 403 belkis 67
Trafico total por All a All
user Sum
marilis 51.30 MB
sadys 22.21 MB
belkis 10.65 MB
yaguila 8.68 MB
yuliet 7.27 MB
edilenia 5.49 MB
odete 3.79 MB
maritza 3.39 MB
oladys 1.79 MB
Logs en tiempo real
@timestamp message
octubre 12, 2017 15:46 1507837602.159 216 192.168.100.69 TCP_MISS/304 379 GET http://ofertas.cu/website-common/js/browser.min.js? yaguila HIER_DIRECT/190.92.127.91 -
octubre 12, 2017 15:46 1507837602.399 233 192.168.100.69 TCP_MISS/304 380 GET http://ofertas.cu/frontend/js/all.js? yaguila HIER_DIRECT/190.92.127.91 -
octubre 12, 2017 15:46 1507837601.921 5869 192.168.100.69 TCP_MISS/200 8426 GET http://ofertas.cu/c/360/animales-mascotas/6.html yaguila FIRSTUP_PARENT/192.168.1.38 text/html
octubre 12, 2017 15:46 1507837600.568 544 192.168.100.69 TCP_MISS/304 380 GET http://ofertas.cu/frontend/css/all.css? yaguila HIER_DIRECT/190.92.127.91 -
octubre 12, 2017 15:46 1507837587.404 183520 192.168.100.69 TCP_MISS/200 789 CONNECT adservice.google.com.cu:443 yaguila HIER_DIRECT/172.217.8.98 -
octubre 12, 2017 15:45 1507837549.633 0 192.168.100.69 TCP_DENIED/403 3530 CONNECT www.google.com:443 yaguila HIER_NONE/- text/html
octubre 12, 2017
ADD ROW