

X-PACK **REPORTING**



REPORTING

X-Pack posibilita la generación de informes que contienen los dashboards, visualizaciones y búsquedas guardadas.

Se exportan en formato PDF.



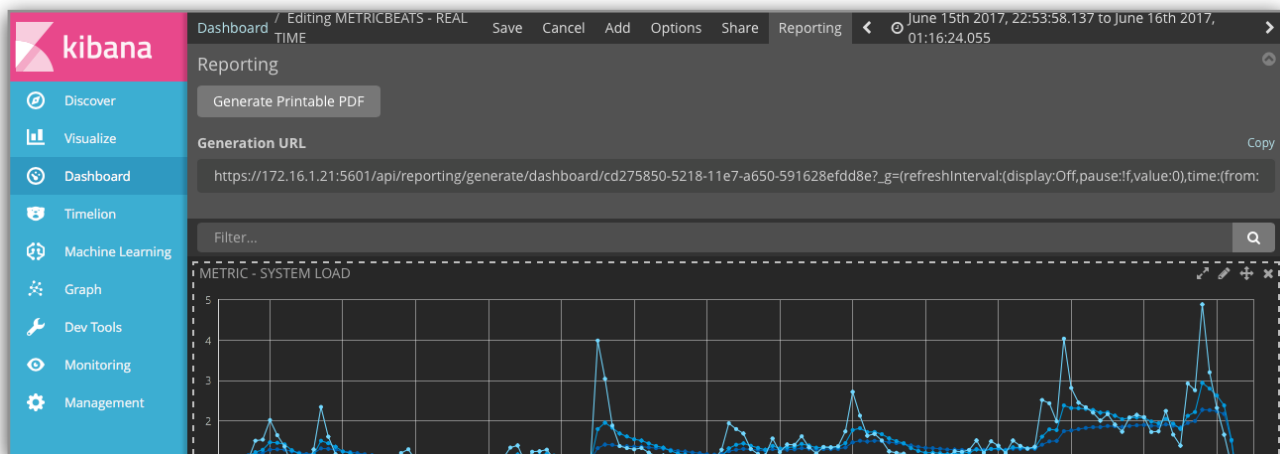


1.

CREACIÓN DE REPORTS

CREACIÓN DE REPORTS

- Una vez instalado X-Pack, el menú *Reporting* se añade en la barra superior.



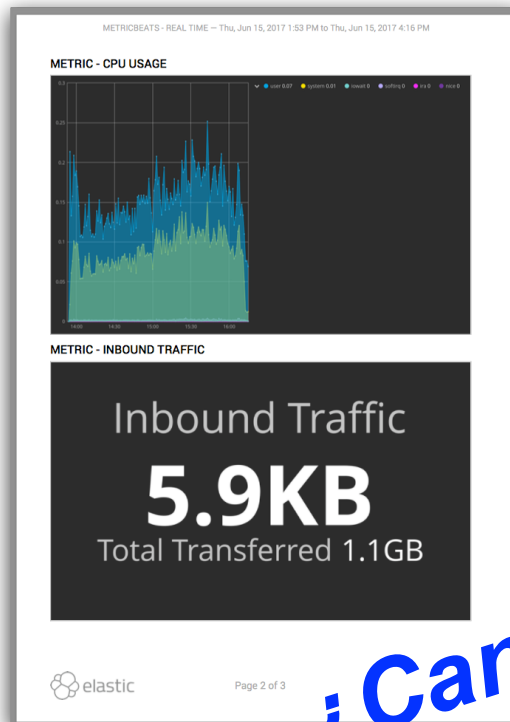
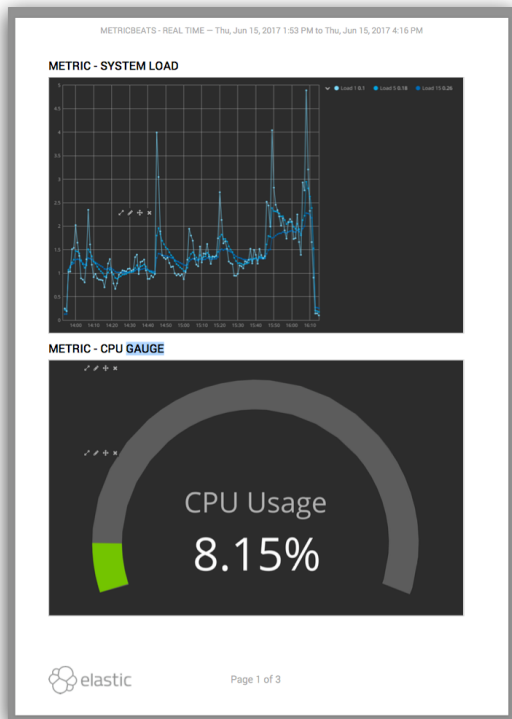
CREACIÓN DE REPORTS

- Se pueden descargar los informes y ver su estado desde su correspondiente menú.

Generated Reports			
Filter Reports: ☒ Only show my reports			
Document	Added	Status	Actions
METRICBEATS - REAL TIME dashboard	2017-06-21 @ 12:23 AM elastic	processing 2017-06-21 @ 12:23 AM	

Document	Added	Status	Actions
METRICBEATS - REAL TIME dashboard	2017-06-21 @ 12:23 AM elastic	completed 2017-06-21 @ 12:23 AM	

CREACIÓN DE REPORTS



¿Canvas?



2.

AUTOMATIZACIÓN DE REPORTS

AUTOMATIZACIÓN DE REPORTS

Se pueden crear informes desde un *Watch* haciendo uso de la API.

Dashboards:

/api/reporting/generate/dashboard/<dashboard-id>

Visualizations:

/api/reporting/generate/visualization/<visualization-id>

Saved Search:

/api/reporting/generate/search/<saved-search-id>

AUTOMATIZACIÓN DE REPORTS

- Ejemplo:

```
"actions" : {  
  "email_admin" : { ❶  
    "email": {  
      "to": "'Recipient Name <recipient@example.com>'",  
      "subject": "Error Monitoring Report",  
      "attachments" : {  
        "error_report.pdf" : {  
          "reporting" : {  
            "url": "http://0.0.0.0:5601/api/reporting/generate/dashboard/Error-Monitoring?  
_g=(time:(from:now-1d%2Fd,mode:quick,to:now))", ❷  
            "retries":6, ❸  
            "interval":"1s", ❹  
          }  
        }  
      }  
    }  
  }  
}
```

X-PACK

MACHINE LEARNING



MACHINE LEARNING

Módulo (beta) que automatiza el análisis de time-series creando un patrón de comportamiento normal e identificando anomalías en dichos datos.

Datos recogidos de ES y mostrados en su correspondiente plugin de Kibana.





3.

FUNCIONAMIENTO M.LEARNING

FUNCIONAMIENTO M.LEARNING

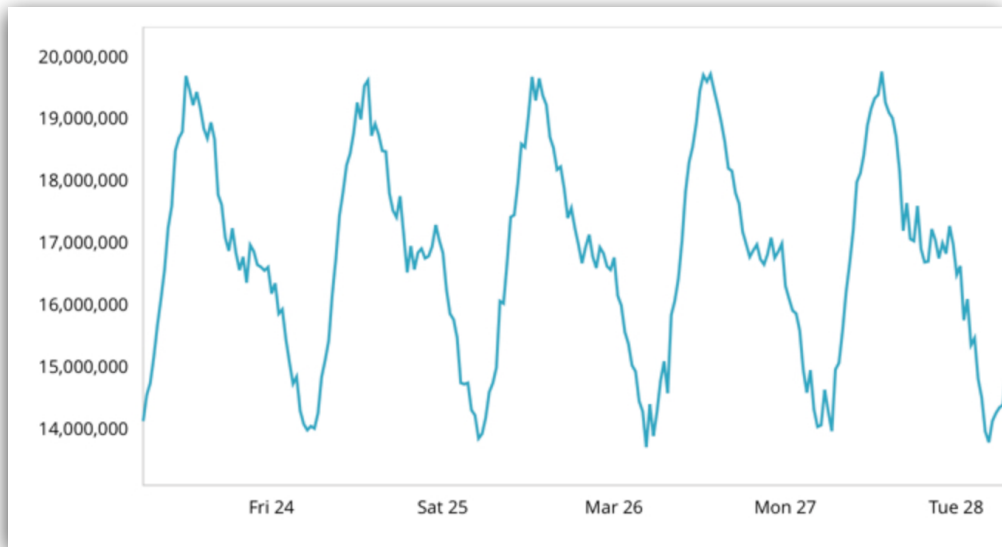
Algoritmos capaces de detectar:

- Anomalías relacionadas con la desviación en tiempo, contabilizados, frecuencias...
- Rarezas estadísticas.
- Comportamiento inusual de un miembro perteneciente a una población.

Transparente para el usuario final (abstracción de algoritmos, modelos, configuraciones...).

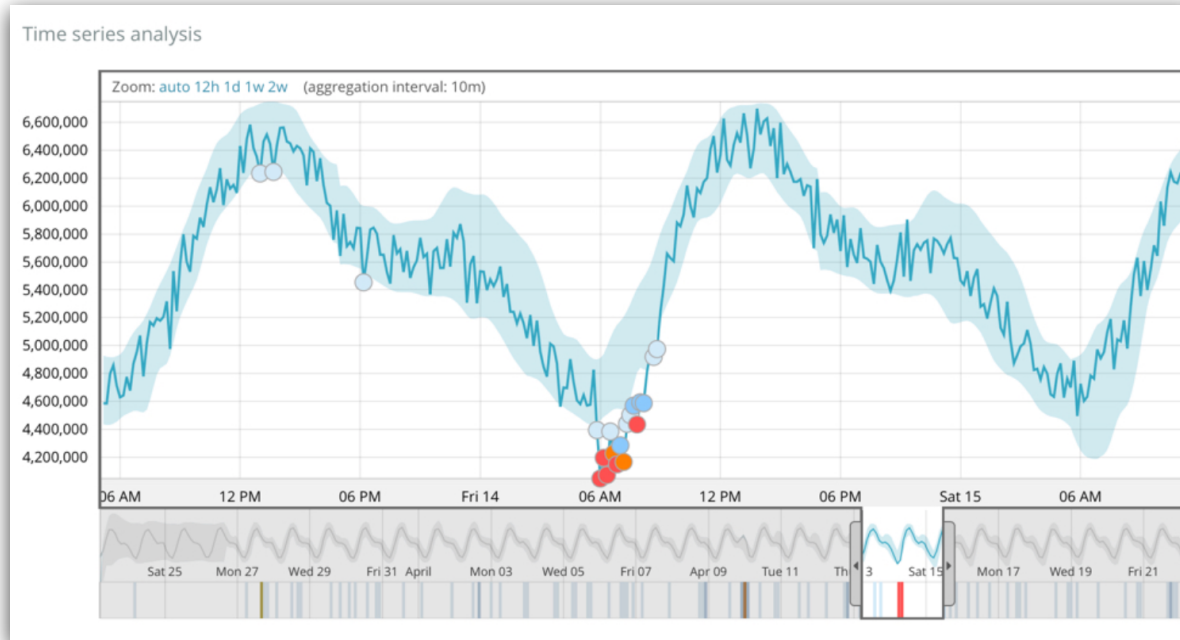
FUNCIONAMIENTO M.LEARNING

- Ingesta de datos



FUNCIONAMIENTO M.LEARNING

- Búsqueda de anomalías



FUNCIONAMIENTO M.LEARNING

- Detalles

Anomalies

Severity threshold: ▲ warning ▼ Interval: Auto ▼

time ⚙	max severity ⚙	detector ⚙	actual ⚙	typical ⚙	description ⚙	job ID ⚙
▼ April 14th 2017, 06:00	▲ 96	sum(total)	4045220	4698040	↓ 1.2x lower	total-requests

Description:
critical anomaly in sum(total)

Details on highest severity anomaly:

time:	April 14th 2017, 06:00:00 to April 14th 2017, 06:10:00
function:	sum
fieldName:	total
actual:	4045220
typical:	4698040
job ID:	total-requests
probability:	3.12169e-10

FUNCIONAMIENTO M.LEARNING

- Detección de ataques de fuerza bruta

