

# .Tuenti

## Monitorización de red en Tuenti

Fernando García Fernández

16/05/19

**.Tuenti**

- Ingeniero, se cayó el servidor.
- Pues reinícielo.
- Ehh, bueno, cómo le explico...



**.Tuenti**

- / Planificar el crecimiento de la red
- / Reaccionar rápidamente ante incidencias
- / Proactividad ante futuros problemas

01

# HERRAMIENTAS

/ No somos el típico telco

/ 3 centros de datos (Miami,  
Londres, Madrid)

/ Equipamiento de red

Switching de red (multiproveedor)

Routing BGP a internet

Firewalls

Balanceadores

/ Herramienta única para todo: sistemas, aplicaciones, red

/ Modular: mayor adaptabilidad

/ Funcionalidades:

- Recopilar información con SNMP
- Graficar la información relevante
- Generar alertas y alarmas
  - Sin molestia: baja prioridad
  - Con molestia: alta prioridad

### /Captura y almacenamiento de métricas

- snmp-exporter

### /PromQL

- Procesado de métricas
- Generación de alarmas

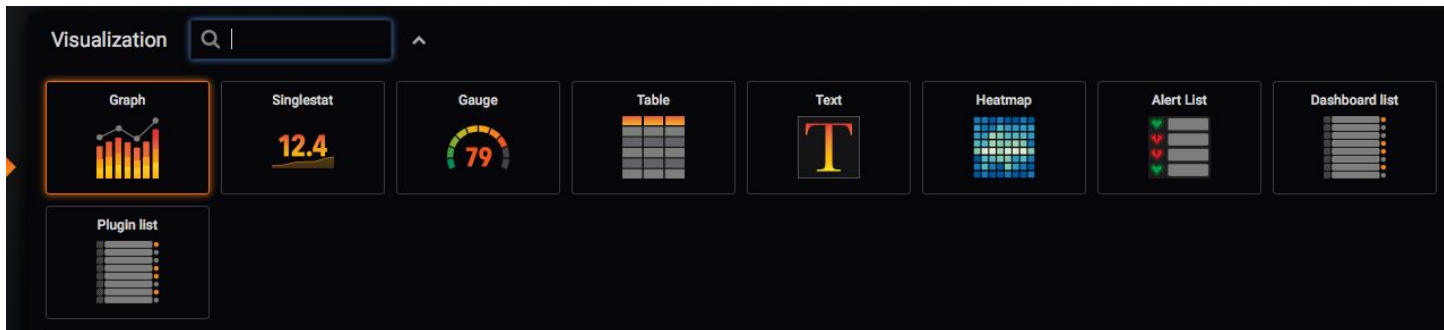
### /Alarmas:

- Baja gravedad: Slack
- Alta gravedad: PagerDuty

Representación gráfica

- Múltiples tipos de gráfico

Integración con Prometheus de fábrica





### / Múltiples tipos de alarmas

- Correo
- Slack
- PagerDuty
- Pushover
- OpsGenie

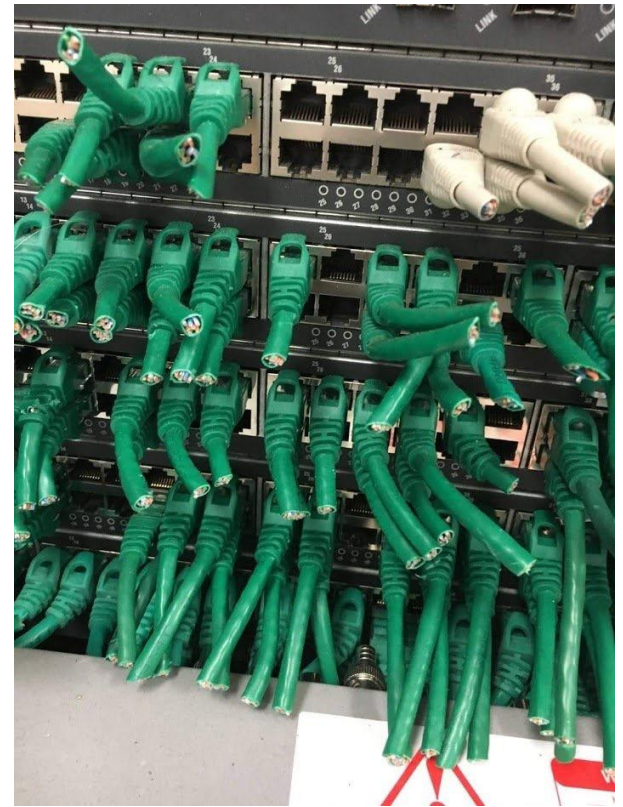
### / Alarmas:

- Baja gravedad: Slack
- Alta gravedad: PagerDuty

02

QUE  
MONITORIZAR

- Tráfico interfaces
  - **Avisar de saturación**
- Errores en interfaces
  - **Cualquier cantidad >0**
- Caídas de interfaces
- Equipos que no responden
  - **Really Fer?**



## Switches: no tan obvio

- (CPU)
- (Memoria)
- Tabla de MAC address

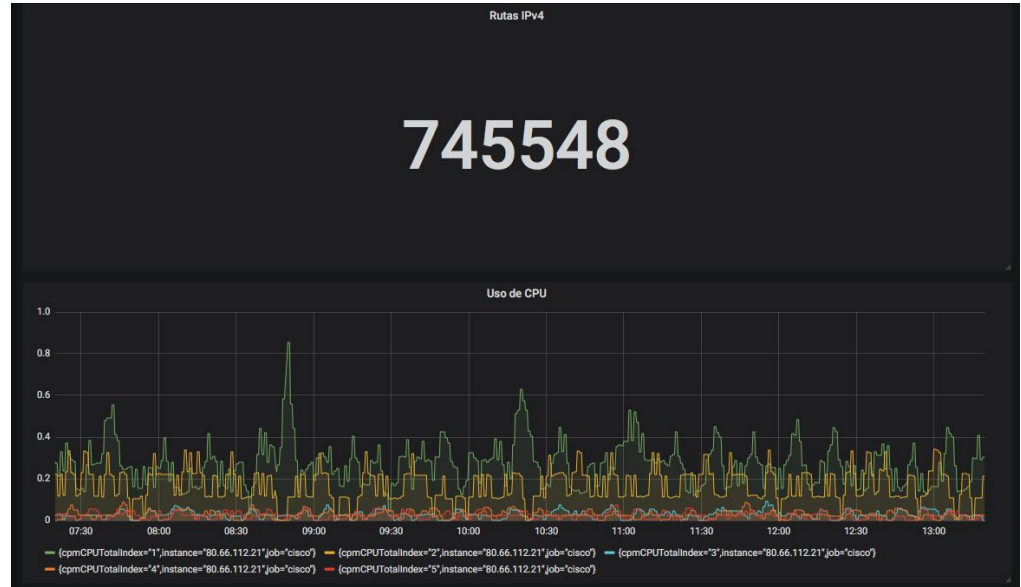
- Flapping de una interfaz
  - No hay MIB para eso
- Tráfico cero
  - Puede ser en interfaces de backup o gestión
- Incrementos o descensos bruscos de tráfico
  - Si tráfico cero, cualquier cosa es brusca

- Tráfico interfaces
- Errores en interfaces
- Caídas de interfaces
- Equipos que no responden



## Routers: no tan obvio

- CPU
- Memoria
- Sesiones BGP (OSPF, IS-IS)
- Tamaño tabla de rutas



- Flapping de una interfaz
- Tráfico cero
- Incrementos o descensos bruscos de tráfico



**.Tuenti**

**¿Pero en todas las interfaces?**

**.Tuenti**

03

Y ASI LO  
HACEMOS

# **.Tuenti** | **Pasos**

- 1. Instala prometheus**
- 2. Instala alertmanager**
  - a. Enlazado con prometheus**
- 3. Instala snmp\_exporter**
  - a. Enlazalo con prometheus**
  - b. Configura los dispositivos**
- 4. Instala Grafana**
  - a. Enlazalo con prometheus**

- Paquete precompilado
  - Mac
  - Linux
  - Windows
- También disponible como Docker
- En el mismo sitio alertmanager
- <https://prometheus.io>

# Instala snmp\_exporter

- Paquete precompilado
- [https://github.com/prometheus/snmp\\_exporter](https://github.com/prometheus/snmp_exporter)
- Enlace con Prometheus
  - Una línea

## Configura los dispositivos (1)

- Crear archivo de generacion SNMP (1 por tipo de dispositivo)
- Ejecutar generator sobre generator.yaml
- Copiar snmp.yaml al directorio de config

```
modules:  
  ciscocatalyst:  
    walk:  
      - sysUpTime  
      - sysDescr  
      - ifType  
      - ifMtu  
      - ifSpeed  
      - ifPhysAddress  
      - ifAdminStatus  
      - ifOperStatus  
      - ifLastChange  
      - ifInDiscards  
    lookups:  
      - source_indexes: [ifIndex]  
        lookup: ifDescr  
        drop_source_indexes: false  
      -source_indexes: [ifIndex]  
        lookup: ifName  
        drop_source_indexes: false  
    auth:  
      community: public
```

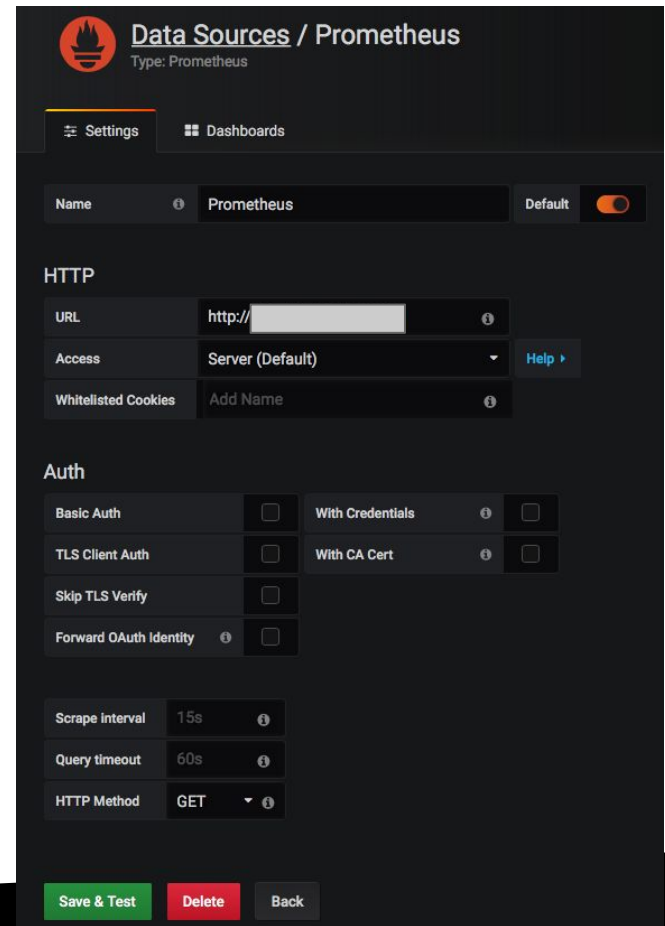
## Configura los dispositivos (2)

- En la configuración de Prometheus
  - Referenciar el modulo snmp.yaml
  - Añadir lista de IPs de equipos

```
- job_name: cisco
  scrape_interval: 60s
  scrape_timeout: 60s
  static_configs:
  - targets:
    - 192.0.2.1
    - 192.0.2.2
    - 192.0.2.11
    - 192.0.2.21
    - 192.0.2.31
    - 192.0.2.41
  metrics_path: /snmp
  params:
    module: [cisco]
  relabel_configs:
  - source_labels: [__address__]
    target_label: __param_target
  - source_labels: [__param_target]
    target_label: instance
  - target_label: __address__
    replacement: 127.0.0.1:9116
```

# .Tuenti | Instala grafana

- Paquete precompilado
- También disponible como Docker
- Una línea de configuración
- Configurar gráficas
  - Definiciones genéricas: una gráfica para todos los routers e interfaces

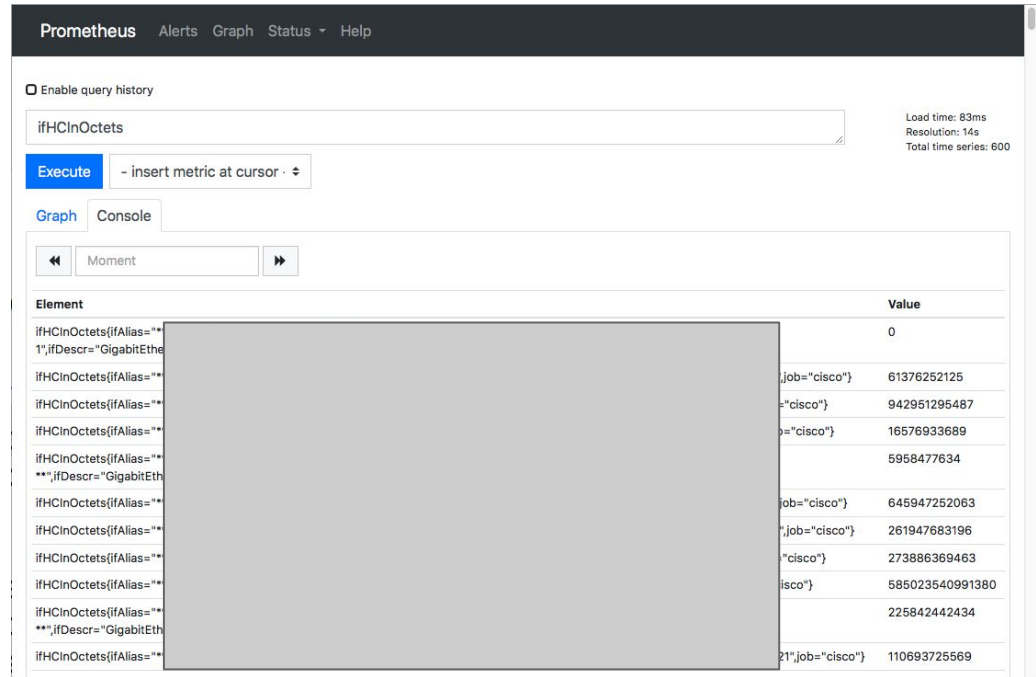


The screenshot shows the Grafana configuration interface for a Prometheus data source. At the top, there is a logo and the title "Data Sources / Prometheus" with the subtitle "Type: Prometheus". Below this, there are tabs for "Settings" and "Dashboards". The main configuration area includes a "Name" field set to "Prometheus" and a "Default" toggle switch that is turned on. Under the "HTTP" section, there is a "URL" field with a placeholder "http://", an "Access" dropdown menu set to "Server (Default)", and a "Whitelisted Cookies" section with an "Add Name" button. The "Auth" section contains several options: "Basic Auth" with a checkbox and "With Credentials" with a checkbox; "TLS Client Auth" with a checkbox and "With CA Cert" with a checkbox; "Skip TLS Verify" with a checkbox; and "Forward OAuth Identity" with a checkbox. At the bottom of the configuration area, there are three input fields: "Scrape interval" set to "15s", "Query timeout" set to "60s", and "HTTP Method" set to "GET". At the very bottom, there are three buttons: "Save & Test" (green), "Delete" (red), and "Back" (grey).



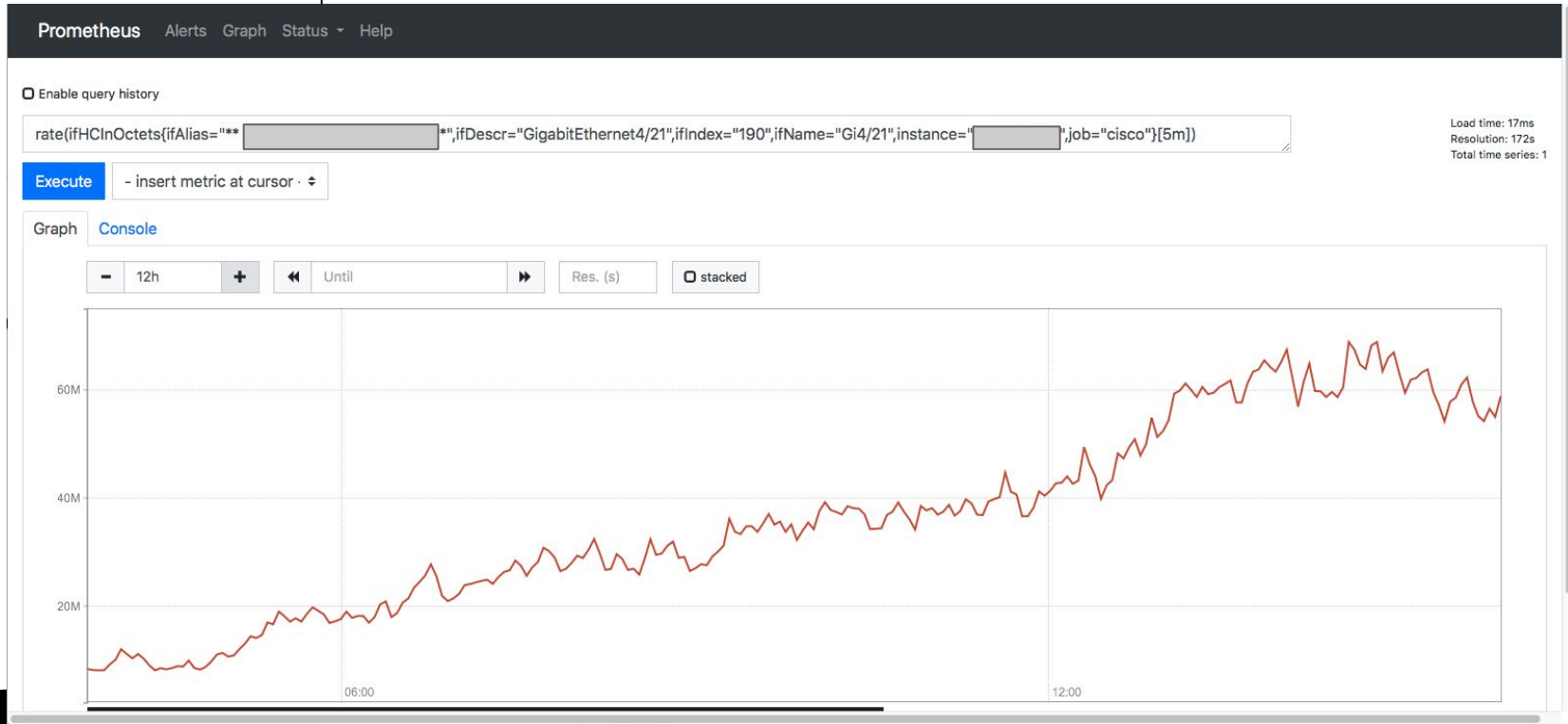
# .Tuenti | Queries

- Navegador integrado
- Peticiones con PromQL

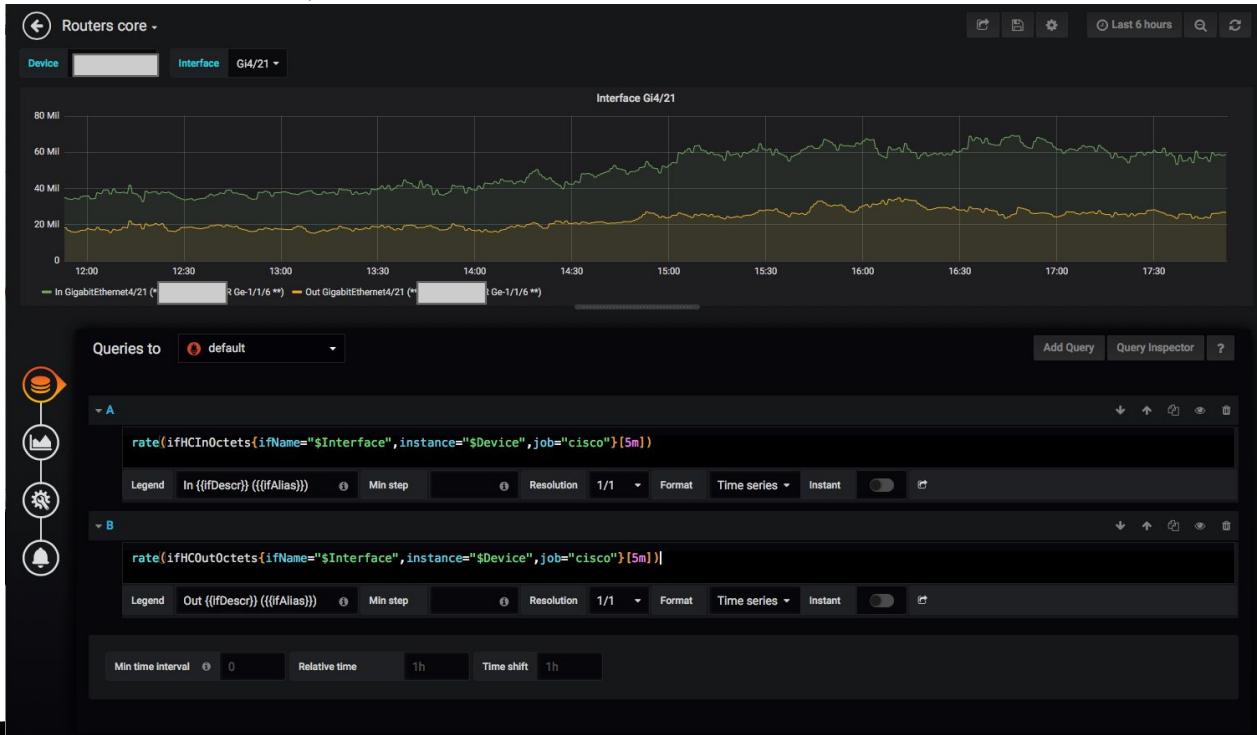


The screenshot shows the Prometheus web interface. At the top, there is a navigation bar with 'Prometheus', 'Alerts', 'Graph', 'Status', and 'Help'. Below this, there is a search bar containing the query 'ifHCInOctets'. To the right of the search bar, it displays 'Load time: 83ms', 'Resolution: 14s', and 'Total time series: 600'. Below the search bar is an 'Execute' button and a dropdown menu set to '- insert metric at cursor'. There are two tabs: 'Graph' and 'Console'. Below the tabs is a time range selector set to 'Moment'. The main content area shows a table with two columns: 'Element' and 'Value'. The table contains 12 rows of data, with the first row having a value of 0 and the others having various numerical values.

Element	Value
ifHCInOctets{ifAlias="1",ifDescr="GigabitEth	0
ifHCInOctets{ifAlias="1",ifDescr="GigabitEth	61376252125
ifHCInOctets{ifAlias="1",ifDescr="GigabitEth	942951295487
ifHCInOctets{ifAlias="1",ifDescr="GigabitEth	16576933689
ifHCInOctets{ifAlias="1",ifDescr="GigabitEth	5958477634
ifHCInOctets{ifAlias="1",ifDescr="GigabitEth	645947252063
ifHCInOctets{ifAlias="1",ifDescr="GigabitEth	261947683196
ifHCInOctets{ifAlias="1",ifDescr="GigabitEth	273886369463
ifHCInOctets{ifAlias="1",ifDescr="GigabitEth	585023540991380
ifHCInOctets{ifAlias="1",ifDescr="GigabitEth	225842442434
ifHCInOctets{ifAlias="1",ifDescr="GigabitEth	110693725569



# .Tuenti | Queries to Grafana



## Alarmas en Slack



AlertManager APP 23:15

### [FIRING:3] CiscoNxosUnsavedConfig (Unsaved configuration in Cisco Nexus switch)

#### Alerts Firing:

- [WARNING]: Cisco Nexus switch nex10... has unsaved configuration changes for more than 2 hours.
- [WARNING]: Cisco Nexus switch nex... has unsaved configuration changes for more than 2 hours.
- [WARNING]: Cisco Nexus switch nex... has unsaved configuration changes for more than 2 hours.

Ayer



AlertManager APP 00:40

### [RESOLVED] CiscoNxosUnsavedConfig (Unsaved configuration in Cisco Nexus switch)

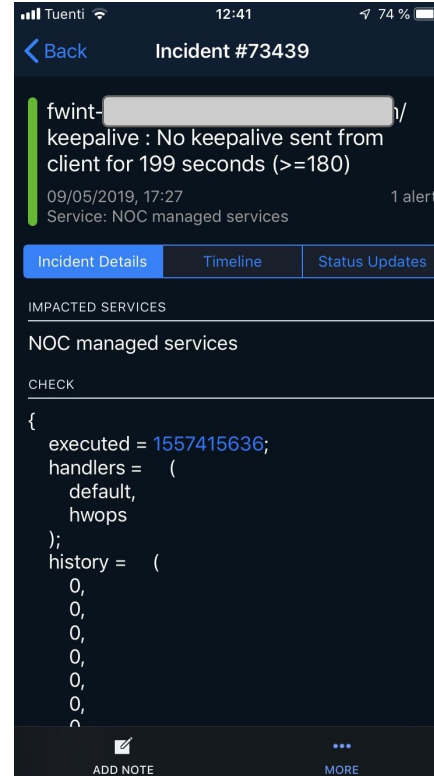
#### Alerts Resolved:

- Cisco Nexus switch nex... has unsaved configuration changes for more than 2 hours.
- Cisco Nexus switch nex... has unsaved configuration changes for more than 2 hours.
- Cisco Nexus switch nex... has unsaved configuration changes for more than 2 hours.

## Ejemplo de alarma

### Servicio de alarmas

- Escalado de alarmas
- Escalado del equipo

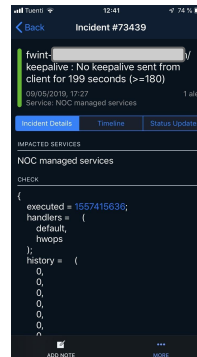
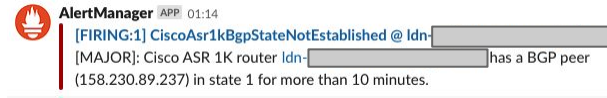


### Caída de sesión

- >10 min: Major

### CPU elevada

- >80% 15 min: Major
- >95% 15 min: Critical



- MAJOR: avisa por Slack
- CRITICAL: Avisa por PagerDuty
- Misma alarma, dos niveles:
  - Interfaz caido 10 minutos: Mayor
  - Interfaz caido 30 minutos: Critical
- Tipo de interfaz

# Configuración alertmanager

```
global:
  smtp_from: 'Alertmanager <alarmas@tuenti.com>'
route:
  receiver: oncall
receivers:
- name: oncall
  email_configs:
  - to: fgarcia@tuenti.com'
    from: 'alarmas@tuenti.com'
    smarthost: "smtp.gmail.com:587"
    auth_username: "alarmas@tuenti.com"
    auth_identity: ""
    auth_password: "xxxxxxxxxxxxxxxx"
    require_tls: true
```



description #T:CORE#S:1#U:BGP to Telefonica#

CORE  
PROD  
PRE  
MGMT  
TEST  
FREE

0= shutdown  
1= no shutdown

Description

```
- alert: CiscoIfInTraffic
  expr: rate(ifHCInOctets{ifAlias=~".*#T:CORE#.*|.*#T:PROD#.*",job="cisco"}[5m]) / (ifHighSpeed * 1250) > 95
  for: 10m
  labels:
    severity: critical
  annotations:
    summary: Cisco router interface input traffic
    description: "Cisco Router {{ $labels.instance }} interface {{ $labels.ifDescr }} ({{ $labels.ifAlias }}) input traffic was over 95% of total interface capacity for more than 10 minutes"
```

04

RECURSOS

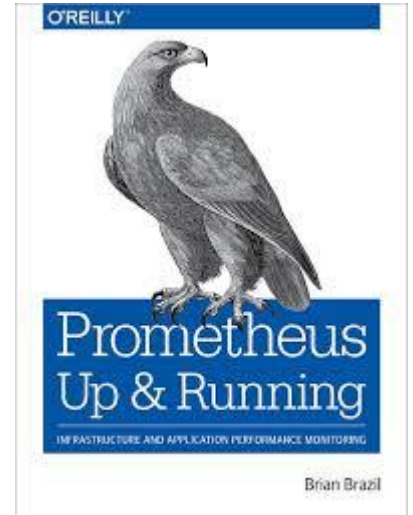
# .Tuenti

Prometheus: <https://prometheus.io>

snmp\_exporter: [https://github.com/prometheus/snmp\\_exporter](https://github.com/prometheus/snmp_exporter)

Graphana: <https://grafana.com>

Y este libro:



**.Tuenti**

