.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

.Tuenti

OBJETIVOS

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

.Tuenti

01 HERRAMIENTAS

.Tuenti

NUESTRA RED

- 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

.Tuenti

.Tuenti

FILOSOFÍA

- 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

.Tuenti

.Tuenti

Prometheus

/Captura y almacenamiento de métricas

- snmp-exporter

/PromQL

- Procesado de métricas
- Generación de alarmas

/Alarmas:

- Baja gravedad: Slack
- Alta gravedad: PagerDuty

.Tuenti

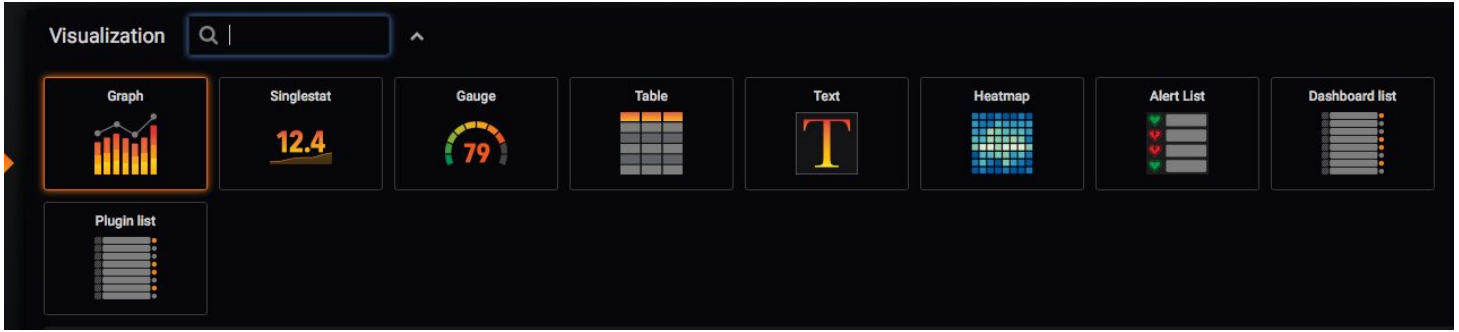
.Tuenti

Grafana

Representación gráfica

- Múltiples tipos de gráfico

Integración con Prometheus de fábrica



.Tuenti

.Tuenti

Alarmas

/Multiples tipos de alarmas

- Correo
- Slack
- PagerDuty
- Pushover
- OpsGenie

/Alarmas:

- Baja gravedad: Slack
- Alta gravedad: PagerDuty

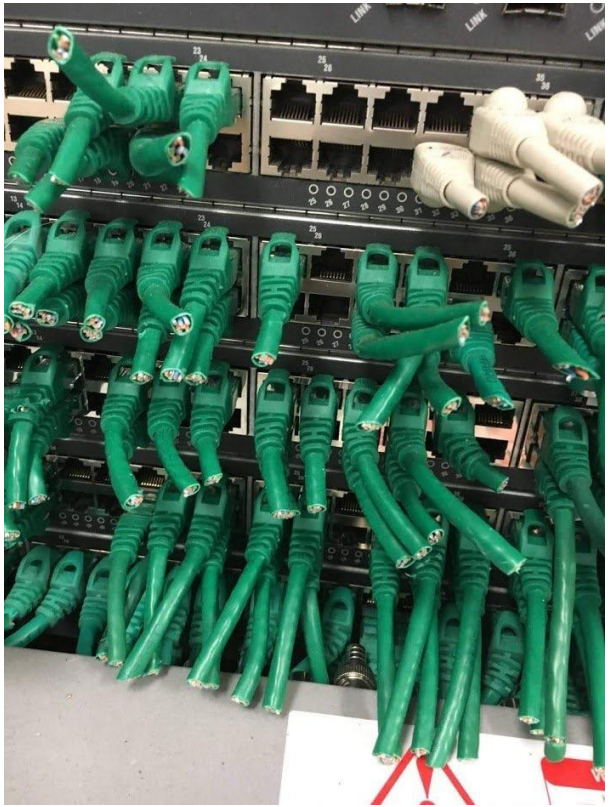
.Tuenti

02 QUE MONITORIZAR

.Tuenti

Switches: lo obvio

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



.Tuenti

.Tuenti

Switches: no tan obvio

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

.Tuenti

.Tuenti

Switches: molaría

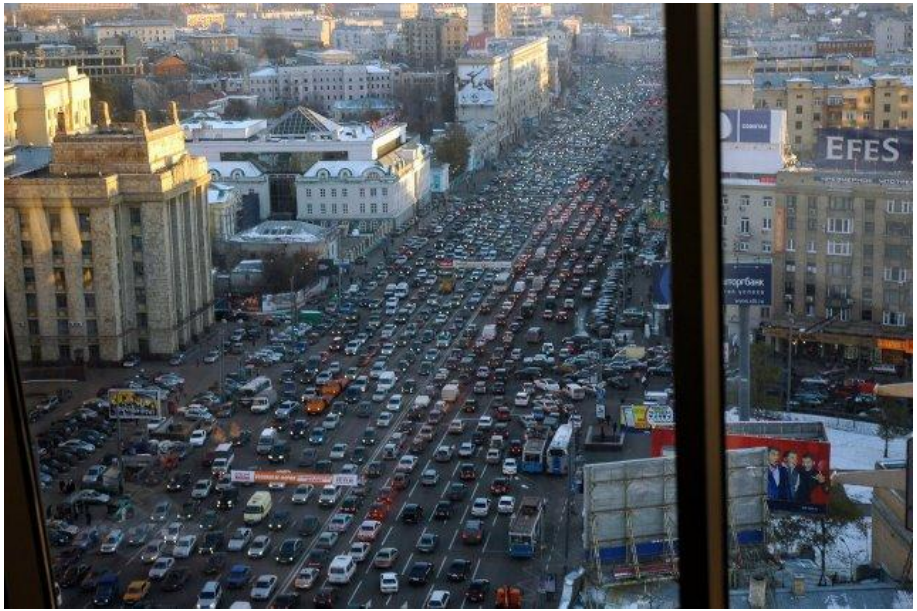
- Flapping de una interfaz
  - No hay MIB para eso
- Tráfico cero
  - Puede ser en interfaces de backup o gestión
- Incrementos o descensos bruscos de tráfico
  - Si tráfico cero, cualquier cosa es brusca

.Tuenti

.Tuenti

Routers: lo obvio

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

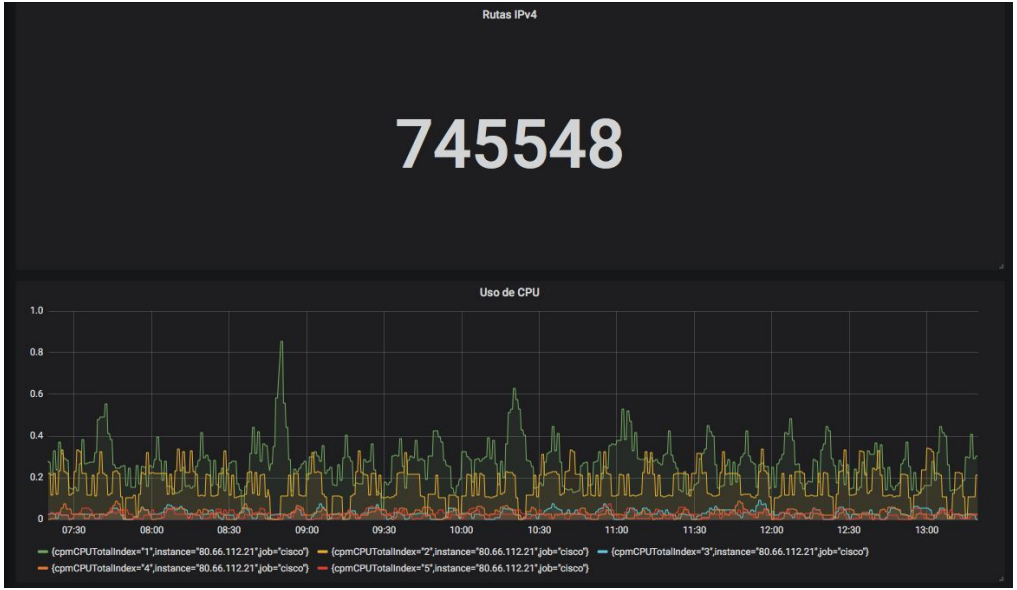


.Tuenti

.Tuenti

Routers: no tan obvio

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



.Tuenti

.Tuenti

Routers: molaría

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

.Tuenti

.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**

.Tuenti

.Tuenti

Instala prometheus

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

.Tuenti

.Tuenti

Instala snmp_exporter

- Paquete precompilado
- https://github.com/prometheus/snmp_exporter
- Enlace con Prometheus
  - Una línea

.Tuenti

.Tuenti

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
```

.Tuenti

.Tuenti

Configura los dispositivos (2)

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

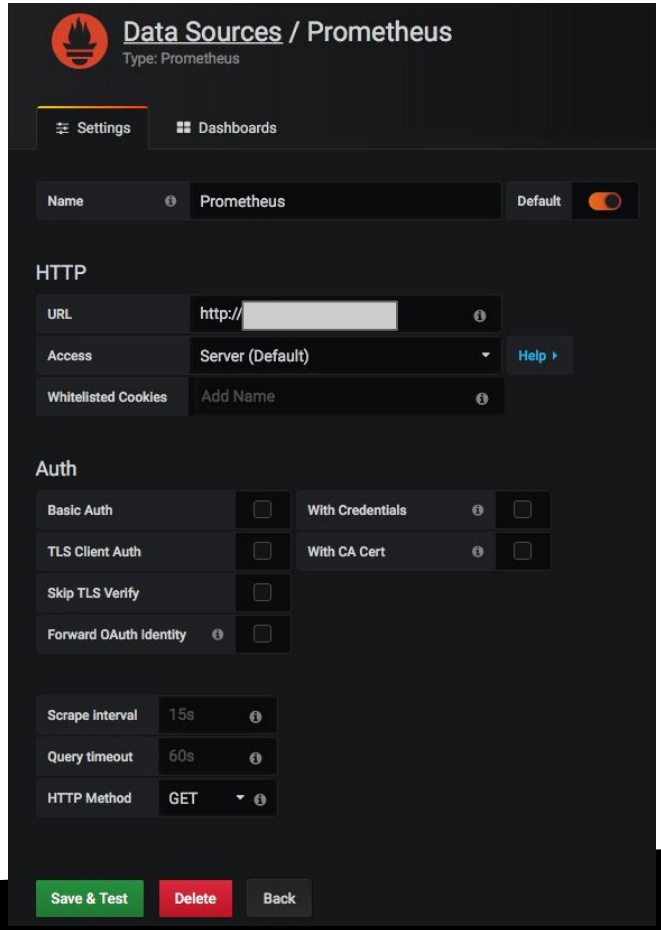
```
- job_name: cisco
  scrape_interval: 60s
  scrape_timeout: 60s
  static_configs:
  - targets:
    - 192.0.2.1
    - 192.0.2.2
    - 192.0.2.11
    - 192.0.2.21
    - 192.0.2.31
    - 192.0.2.41
  metrics_path: /snmp
  params:
    module: [cisco]
  relabel_configs:
  - source_labels: [__address__]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

.Tuenti

.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

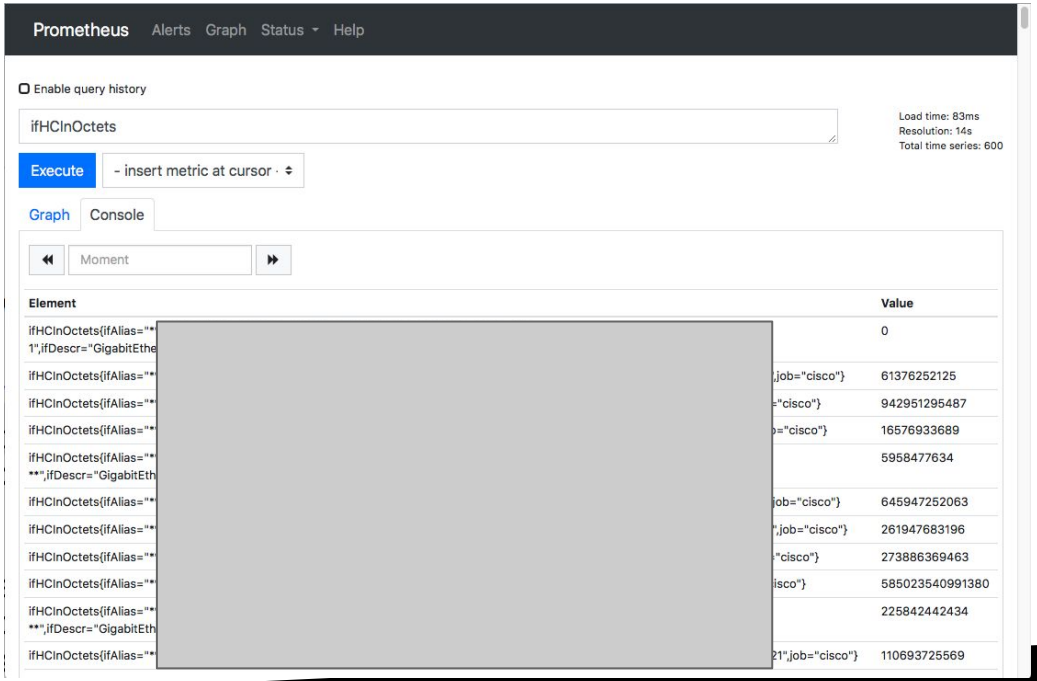


.Tuenti

.Tuenti

Queries

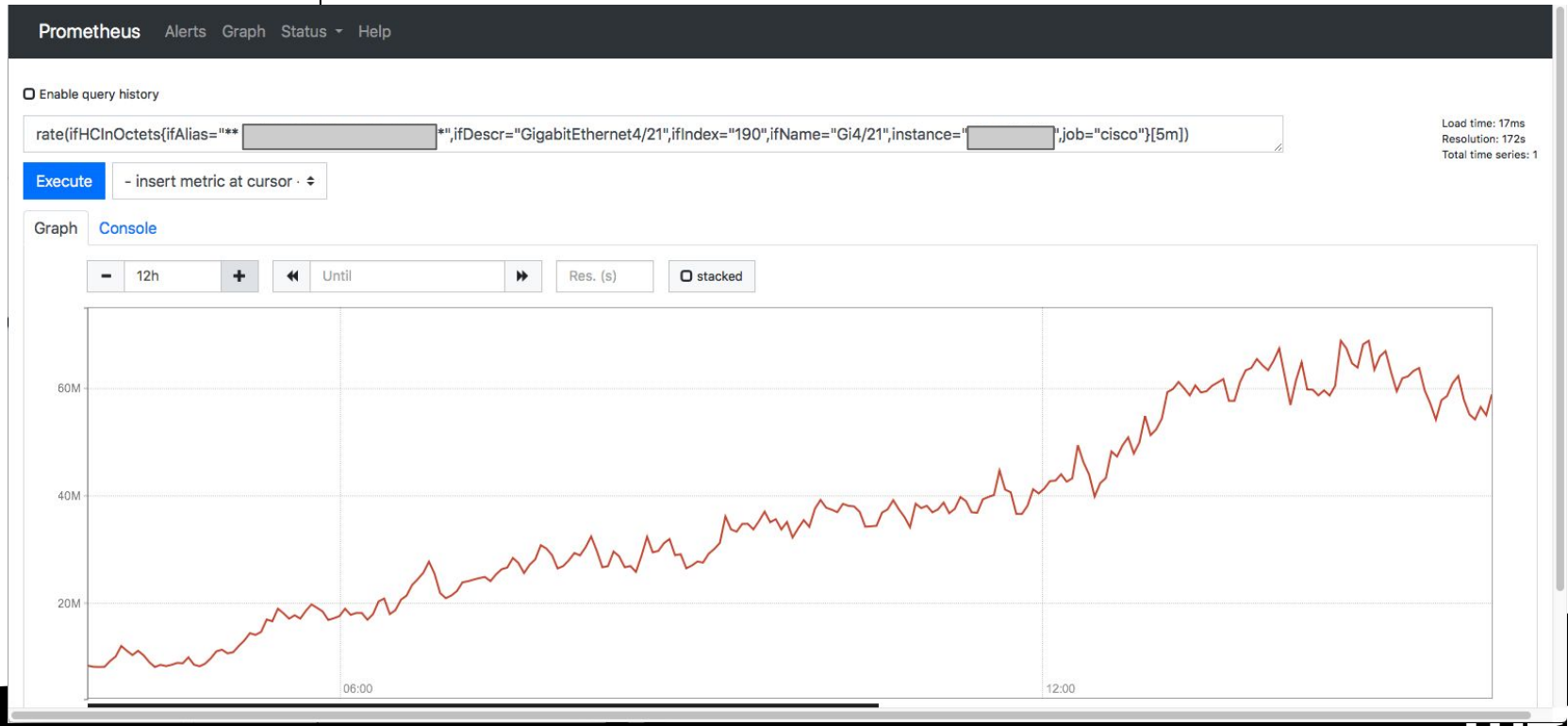
- Navegador integrado
- Peticiones con PromQL



.Tuenti

.Tuenti

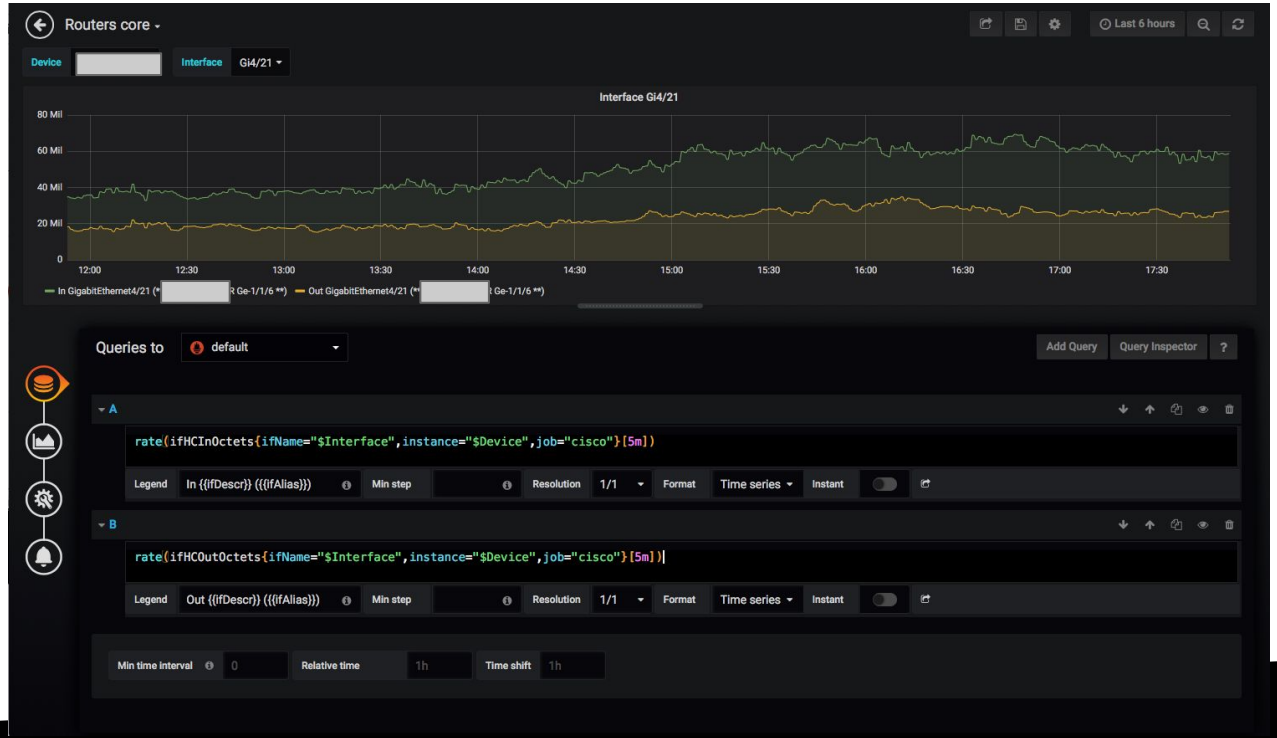
Queries



.Tuenti

.Tuenti

Queries to Grafana



.Tuenti

.Tuenti

Alarmas en Slack

AlertManager APP 23:15

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

Alerts Firing:
- [WARNING]: Cisco Nexus switch nex[redacted]om has unsaved configuration changes for more than 2 hours.
- [WARNING]: Cisco Nexus switch nex[redacted]om has unsaved configuration changes for more than 2 hours.
- [WARNING]: Cisco Nexus switch nex[redacted]com has unsaved configuration changes for more than 2 hours.

Ayer

AlertManager APP 00:40

[RESOLVED] CiscoNxosUnsavedConfig (Unsaved configuration in Cisco Nexus swith)

Alerts Resolved:
- Cisco Nexus switch nex[redacted]m has unsaved configuration changes for more than 2 hours.
- Cisco Nexus switch nex[redacted].com has unsaved configuration changes for more than 2 hours.
- Cisco Nexus switch ne[redacted].com has unsaved configuration changes for more than 2 hours.

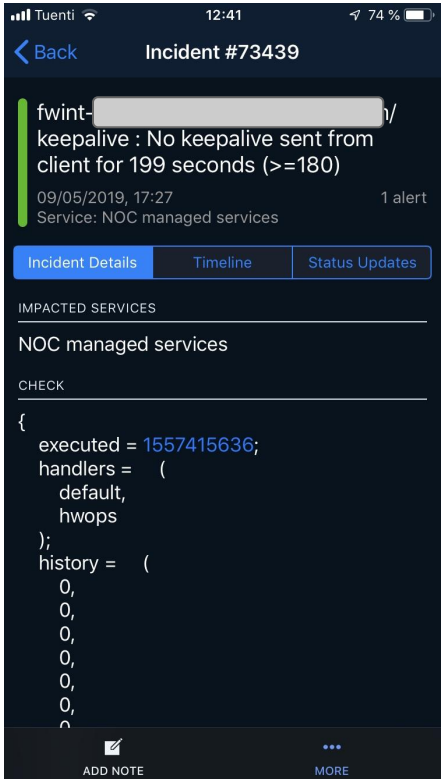
.Tuenti

.Tuenti

Ejemplo de alarma

Servicio de alarmas

- Escalado de alarmas
- Escalado del equipo



.Tuenti

.Tuenti

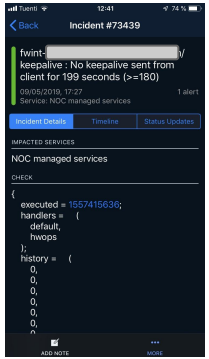
Ejemplos de escalado

Caída de sesión

- >10 min: Major

CPU elevada

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



.Tuenti

.Tuenti

Dos niveles de alarmas

- 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

.Tuenti

.Tuenti

Configuración alertmanager

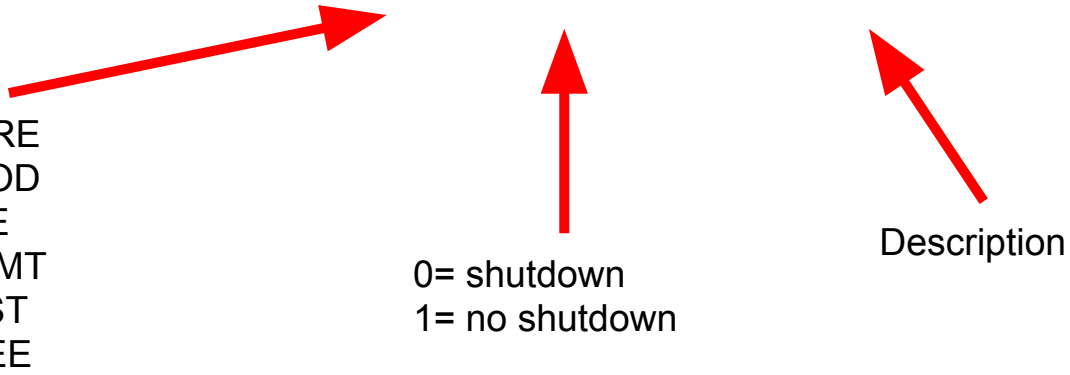
```
global:
   smtp_from: 'Alertmanager <alarmas@tuenti.com>'
route:
  receiver: oncall
receivers:
  - name: oncall
    email_configs:
      - to: fgarcia@tuenti.com'
        from: 'alarmas@tuenti.com'
        smarthost: "smtp.gmail.com:587"
        auth_username: "alarmas@tuenti.com"
        auth_identity: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

.Tuenti

.Tuenti

Clasificacion interfaces

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



.Tuenti

.Tuenti

Alertas

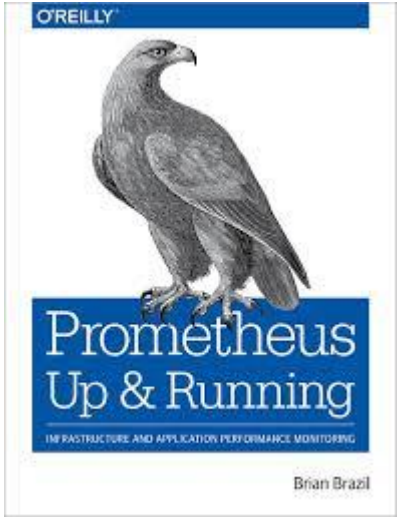
```
  - alert: CiscoIfInTraffic
    expr: rate(ifHCInOctets{ifAlias=~".*#T:CORE#.*|.*#T:PROD#.*",job="cisco"}[5m]) / (ifHighSpeed * 1250) > 95
    for: 10m
    labels:
      severity: critical
    annotations:
      summary: Cisco router interface input traffic
      description: "Cisco Router {{ $labels.instance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

.Tuenti

04 RECURSOS

.Tuenti

Prometheus: https://prometheus.io
snmp_exporter:https://github.com/prometheus/snmp_exporter
Graphana: https://grafana.com
Y este libro:



.Tuenti