Problema 1 – Predicción, detección y notificación de comportamiento anómalo al monitorizar una red

Introducción

El problema de recolectar, almacenar y visualizar información de un servicio de red usando series de tiempo se puede solucionar usando el software RRDtool.

Administrar un servicio de red en tiempo real no es una tarea trivial. Cada variable es monitorizada, ya sea el tráfico en bytes en una interfaz de un switch, la carga del CPU en un host, o las peticiones atendidas por un demonio, generan series de tiempo. Todas esas series reflejan una parte de la salud del servicio de red.

El primer desafío, por lo tanto, es recopilar, almacenar y proporcionar acceso en tiempo real a esta vasta y diversa información. El software de código abierto RRDtool cumple con este primer desafío. Es probable que un técnico de red esté interesado en un comportamiento aberrante; es decir, cambios en el comportamiento a corto plazo de una serie temporal (del orden de minutos u horas) que son inconsistentes con el historial pasado. Las tendencias a largo plazo (del orden de semanas o meses) no son de interés desde la perspectiva del monitoreo del servicio porque se espera que una serie temporal evolucione en un entorno dinámico.

El comportamiento aberrante puede indicar un cuello de botella de rendimiento, una falla en el componente de la aplicación o un tiempo de inactividad del sistema. En algunos casos, se puede anticipar un comportamiento aberrante.

El segundo desafío del monitoreo de red es identificar automáticamente un comportamiento aberrante en medio de miles de series de tiempo de servicios de red. Una vez que se identifica ese comportamiento, se puede activar una alerta para llamar la atención del técnico sobre el problema potencial. Las herramientas de software existentes proporcionan parte de esta funcionalidad, pero estas soluciones generalmente se basan en reglas o umbrales simples (es decir, la utilización de la memoria debe ser inferior al 80%). Estas reglas y umbrales son suficientes para muchas aplicaciones, pero no pueden detectar cambios más sutiles en el comportamiento y aplican un criterio estático para detectar comportamientos aberrantes en lugar de dinámicos.

Para informar un comportamiento anómalo es necesario implementar un algoritmo de predicción y tendencia. El algoritmo de predicción permite conocer cuando extrapolan la carga de la red y el punto de interrupción definido. RRDtool permite proporcionar el análisis de datos (a través del algoritmo de predicción de

Holt-Winters), umbrales definidos y el comportamiento anómalo en la serie temporal del conjunto de datos.La detección de comportamiento anómalo es descompuesta en tres partes, cada una se construye sobre su predecesor:

- Un algoritmo para predecir los valores de una serie temporal en un valor esperado.
- Una medida de desviación entre los valores esperados y los valores observados.
- Un mecanismo para decidir si un valor observado o una secuencia de valores observados son “demasiado desviados” de los valores esperados

Haciendo predicción de la tendencia y análisis,el módulo es capaz de “predecir” dónde y cuándo un determinado valor se producirá en cierta fecha con un grado de certeza.

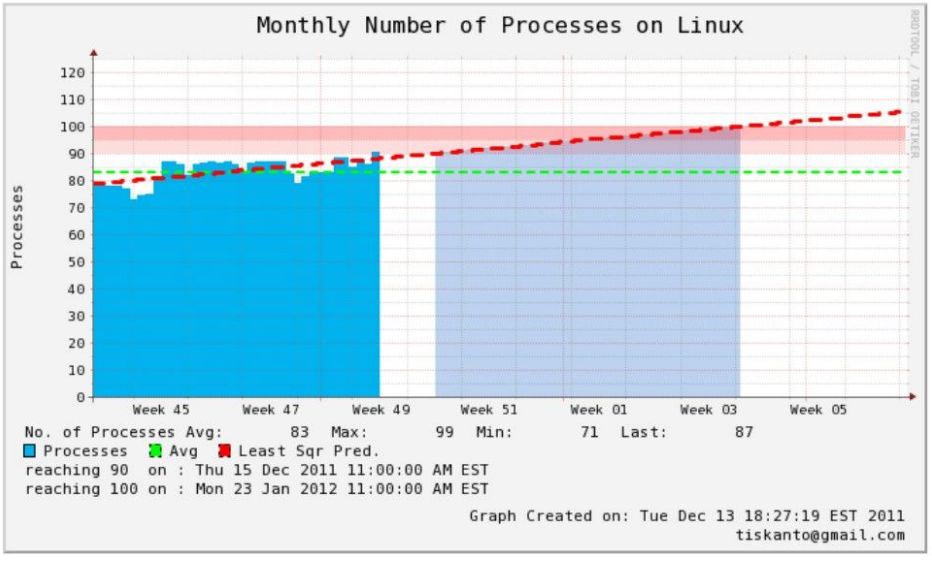
Desarrollo

Tarea 1 - Predicción de la tendencia de series temporales lineales

Para analizar una serie temporal con comportamiento lineal se usará el método de mínimos cuadrados para encontrar la línea del mejor ajuste al comportamiento de una variable monitorizada. Dicho método cumple la siguiente función:

$$y = a(x) + b$$

Donde ‘a’ denota la pendiente y ‘b’ es el valor de la constante de la ecuación (intercepción en y). Usando el método de mínimos cuadrados se puede predecir cuándo el procesamiento alcanzará el 90 y el 100%.



El alumno deberá monitorizar la carga del CPU de un agente y, usando mínimos cuadrados, predecir cuándo la carga alcanzará el 90 %. La predicción se debe introducir en la gráfica.

Tarea 2 - Predicción de la tendencia de series temporales no lineales

Para la predicción de valores de un conjunto de datos no lineales se usa el algoritmo de Holt Winters que está definido en RRDtool.
https://oss.oetiker.ch/rrdtool/doc/rrdcreate.en.html

Tarea 3 - Detección y notificación de comportamiento anómalo

Un desafío del monitoreo de red es identificar automáticamente un comportamiento aberrante en medio de miles de series de tiempo de servicios de red. Una vez que se identifica ese comportamiento, se puede activar una alerta para llamar la atención del técnico sobre el problema potencial. El alumno debe detectar un comportamiento anormal y notificar vía email adjuntando una imagen como la siguiente