Supervisión proactiva de Infraestructuras TIC mediante Zabbix

Proactive supervision of ICT infrastructures using Zabbix

Víctor Manuel Armas Hidalgo

Resumen

La monitorización de equipos, servicios y recursos del sistema operativo es una parte fundamental de la administración de infraestructuras TIC. La proliferación de servicios prestados de forma continua (24x7) hace que ya no sólo baste con una monitorización que nos alerte de la existencia de fallos en el servicio. Se hace cada vez más necesario un sistema que incluya cierto nivel de proactividad y de autocorrección de problemas, para que las incidencias ocurridas fuera del horario laboral no impliquen parada de servicio para los usuarios de nuestros servicios. Y ya no sólo debemos asegurar que el servicio esté activo, sino que su funcionamiento esté dentro de unos parámetros de calidad estipulados.

Paralelamente, es deseable que los resultados de todos los testeos de calidad sean almacenados para su posterior estudio y representación gráfica, incluso pudiendo proporcionar a directivos de perfil no técnico una visión sencilla del estado de nuestras infraestructuras.

En esta ponencia expondremos cómo hemos implementado en la Universidad de Las Palmas de Gran Canaria (ULPGC) un sistema de monitorización proactiva utilizando la herramienta open-source Zabbix.

Palabras clave: monitorización, Zabbix, ULPGC.

Summary

The monitoring of operating system equipment, services and resources is a fundamental part of the administration of ICT infrastructures. The proliferation of 24/7 services means that it is no longer enough to carry out monitoring that alerts us to the existence of faults in the system. Increasingly, a system is required that includes a certain level of proactive input and the auto-correction of problems, so that incidents that occur outside working hours do not disrupt the service for our service users. We must not only ensure that the service is active, but also that it is operating within the stipulated quality parameters.

At the same time, it is desirable that the results of all the quality tests are stored for subsequent analysis and graphic representation, including being able to provide nontechnical profile managers with a simple overview of the status of our infrastructures. In this paper we explain how, in the University of Las Palmas, Gran Canaria (ULPGC), we have implemented a proactive monitoring system using the open-source Zabbix tool.

Keywords: monitor, Zabbix, ULPGC.

Se hace cada vez más necesario un sistema que incluya cierto nivel de proactividad y de autocorreción de problemas

Antes de la implementación del Zabbix, en la ULPGC se usaba Nagios como herramienta de monitorización

1. Introducción

Con anterioridad a la implementación del Zabbix, en la ULPGC usamos Nagios como herramienta de monitorización. Esta herramienta nos era suficiente para alertarnos de paradas en el servicio, pero a medida que iban aumentando los niveles de calidad y disponibilidad de los servicios que prestábamos a la comunidad universitaria, fue haciéndose evidente que Nagios no era el entorno ideal para nuestras necesidades.

Por una parte, necesitábamos obtener algún tipo de representación gráfica de los valores numéricos de los testeos realizados. Ya no nos era suficiente con saber si, por ejemplo, el número de procesos de un servidor había pasado un valor límite. Necesitábamos saber cómo había sido la evolución de ese parámetro, si había subido repentinamente o de forma continuada en el tiempo.

Adicionalmente, necesitábamos disponer de una herramienta con un interfaz web realmente único e integrado. No nos era práctico tener una interfaz para la visualización de la monitorización, otra para la

configuración de los test, y otra para la representación gráfica de valores (Nagios, Nagat, MRTG-RRDTools-Cacti).

Con la aparición de servicios en cluster, prestados simultáneamente por diferentes máquinas, necesitábamos realizar comprobaciones que no sólo se basaran en los datos de un servidor, sino que combinaran los valores obtenidos de varios sistemas. También se hizo necesario aumentar la complejidad de los testeos realizados, y de las condiciones de activación de las alertas. E incluso simular la experiencia real de nuestros usuarios simulando interactuar con nuestros servicios web, comprobando que la información sea entregada en un tiempo razonable para nuestros parámetros de calidad.

Zabbix tiene una serie de funcionalidades que nos permitía implementar todas estas mejoras, y gracias a las cuales tenemos hoy un completo sistema de monitorización que satisface todas nuestras necesidades.

2. Características destacables de Zabbix

Con Zabbix tenemos un completo sistema de monitorización que satisface todas nuestras necesidades

A continuación expondremos sucintamente algunas funcionalidades más destacadas de Zabbix, y algunos casos prácticos de uso en la ULPGC.

- **Completo sistema de monitorización**
  Zabbix tiene un sistema de monitorización completísimo, pudiendo monitorizar cualquier dispositivo conectado a nuestra red. Para obtener datos internos de los servidores hemos de instalar un agente en el mismo. Podemos obtener los datos usando los múltiples monitores predefinidos, o crear un programa que obtenga el monitor que necesitemos. Permite hacer monitorizaciones usando SNMP, tanto en modo "polling" o "trapping". Y permite realizar acciones en base a los valores de los monitores, bien sea la notificación por mail o SMS, o la ejecución de un programa.

- **Interfaz web integrada**
  Zabbix tiene un único interfaz web en la cual se integran la parte de monitorización, representación gráfica de los datos obtenidos, configuración de la monitores y alertas, y administración de los usuarios, permitiendo personalizar las funcionalidades visibles en función del perfil del usuario.

Zabbix tiene un único interfaz web que permite personalizar las funcionalidades visibles en función del perfil de usuario

- **Posibilidad de especificar condiciones complejas de alerta**
  Podemos especificar condiciones de alerta bastante complejas, pudiendo combinar varios monitores, incluso de diferentes servidores, y sobre ellos disparar alertas en base a la suma, media o valores mínimos o máximos en un periodo de tiempo determinado, o en los últimos N valores.

- **Niveles de gravedad de alertas**
  Para todas las monitorizaciones puede definirse la gravedad de la misma (desde informativa hasta crítica), y en base a esa gravedad podemos establecer la acción a tomar (a quién se avisa, el medio utilizado o la acción a realizar).

  Así, en el caso de que la gravedad de la incidencia sea baja, recibimos el aviso por email, mientras que en caso de alertas de gravedad alta los avisos se hacen por SMS.

- **Escalabilidad de acciones**
  Zabbix permite designar una sucesión de escalabilidad de acciones a realizar ante un evento. Por ejemplo, puede ejecutar un script de autocorrección cuando se produce la incidencia por primera

vez, enviar un aviso por correo electrónico si pasado un tiempo no se ha solventado el problema, emitir avisos por SMS si el problema sigue sin resolverse en una tercera comprobación.

Esta utilidad es especialmente útil para la adopción de medidas proactivas en caso de incidencias que pudieran ser solventables de forma automática. Por ejemplo, ante la caída de un servicio web fuera de horario laboral, que como primera medida intente un reinicio del servicio, y que en caso de que esa acción no solvente el problema, realice el aviso al técnico correspondiente. O por ejemplo, que en el caso de una primera incidencia avise el técnico asignado, y si no está resuelta en una segunda comprobación, que avise al resto de técnicos de su grupo, o a su superior, algo que es bastante útil para casos de ausencia por trabajo fuera de despacho o por vacaciones.

- **Autodescubrimiento**
  Podemos especificar un rango de direcciones IP en el que hay equipos que queremos monitorizar, y el propio sistema comienza a testear todas las IPs de ese rango y los puertos abiertos en cada uno de ellos, y es capaz de crear los correspondientes monitores para los equipos detectados.

  Esto es muy útil para por ejemplo monitorizar todos los equipos de un aula de informática, simplemente hay que encender todos los equipos y poner a funcionar la autodetección.

Podemos especificar un rango de direcciones IP en el que hay equipos que queremos monitorizar

- **Plantillas**
  Podemos definir una serie de plantillas sobre las cuales determinamos los monitores y disparadores de alerta correspondientes. Cada vez que demos de alta a un nuevo dispositivo, simplemente le asociamos las plantillas que deseemos usar y ya tenemos la máquina configurada, con sólo especificar nombre, dirección IP y plantillas asociadas.

  Podemos definir plantillas genéricas para un servidor Linux, para servidores web, servidores de correo, UPS, switches, etc. Así, cuando necesitemos monitorizar un servidor Linux que presta servicio de correo IMAP e interfaz web, simplemente damos de alta el nombre de equipo, la IP y le asociamos las tres plantillas correspondientes.

- **Representación gráfica de cualquier monitorización**
  Zabbix almacena los valores obtenidos de cada monitorización en una base de datos MySQL, y a partir de ellos elaborar una gráfica de líneas. No es necesario hacer nada al respecto. Simplemente creando el monitor se crea su gráfica correspondiente, no tenemos que preocuparnos de crearla. Si lo consideramos necesario, podemos especificarle la cantidad de valores que queremos que almacene, por si nos preocupa el posible incremento de la base de datos.

Podemos simular la "experiencia de usuario" a la hora de navegar por nuestras páginas web

- **Creación de gráficas personalizada (multimonitor y multiservidor)**
  A partir de los valores obtenidos a través de los monitores, podemos realizar gráficas que impliquen diferentes monitores, que pueden además ser de diferentes servidores.

  Con esta utilidad podemos crear gráficas para comparar de un vistazo el tamaño de las colas de los diferentes servidores SMTP, o el espacio ocupado en las diferentes particiones de un mismo servidor.

- **Monitorización Web**
  Podemos simular la "experiencia de usuario" a la hora de navegar por nuestras páginas web, almacenando el tiempo de respuesta y la velocidad de transferencia de datos. Podemos especificar los valores a rellenar en un formulario web, y simular la sucesión de descargas de varias páginas.

Gracias a esta utilidad, podemos simular la experiencia de un usuario del campus virtual, haciendo que la utilidad se autentique en la página web institucional, acceda a la plataforma del campus virtual, entre en un curso determinado y en un foro concreto, y publique un mensaje en respuesta a uno ya publicado.

- **Mapas, pantallas y slideshows**
  Podemos condensar toda la información recopilada en tres posibles representaciones visuales, en pantallas, mapas y slideshows. En un mapa podemos representar sobre un dibujo de fondo (en muchas ocasiones un mapa de localización) el estado de diferentes dispositivos y de las interconexiones que tengan. En una pantalla podemos incluir diferentes gráficas, tablas, mapas, y páginas web, permitiendo tener una completa visualización del estado de nuestras infraestructuras, y en un slideshow podemos diseñar una presentación con una sucesión de pantallas.

  Esto nos permite diseñar unas pantallas para que técnicos no directamente implicados en el control de los sistemas monitorizados (por ejemplo, técnicos de soporte y ayuda al usuario final), directivos de perfil no técnico, o incluso usuarios finales de nuestros servicios, puedan obtener de una forma clara y condensada datos sobre el estado de nuestras infraestructuras TIC.

Podemos crear monitores e iniciadores de un nuevo equipo, clonando otro servidor similar

- **Clonado de equipos**
  Otra posibilidad bastante práctica es la utilidad de clonado de equipos. Con ella podemos crear los monitores e iniciadores de un nuevo equipo, simplemente clonando otro servidor similar.

  Aprovechando esta funcionalidad, y especialmente tras la proliferación de entornos de virtualización en los que es común la existencia de múltiples servidores en cluster que prestan los mismos servicios, y el despliegue rápido de nuevos servidores virtuales, podemos realizar también un despliegue rápido de nuevas alertas con la utilidad de clonado.

- **Monitorización distribuida. Agentes Proxy**
  El Agente proxy es un proceso ligero que recolecta los datos monitorizados en lugar del servidor centralizado, descargando a este último de parte del proceso de recolección de datos. El agente proxy le pasa los datos obtenidos de manera concentrada al servidor central. También se suele utilizar para recolectar los datos de ubicaciones remotas, optimizando la comunicación de datos.

  Aprovechamos esta funcionalidad para recolectar los datos de los centros ubicados en otras islas.

Disponemos de un sistema de monitorización potente, flexible y sencillo de configurar

3. Conclusiones

Nuestra experiencia en la implantación de un sistema de supervisión de infraestructuras TIC basada en la herramienta open-source Zabbix ha sido altamente satisfactoria. Disponemos de un sistema de monitorización potente, flexible y sencillo de configurar, permitiéndonos diseñar un sistema de medidas proactivas para evitar caídas de servicio, con soporte multiusuario y un importante paquete de representaciones gráficas de la información obtenida.

Consideramos que este sistema puede ser igualmente válido para la gran mayoría de instituciones que trabajen con servicios TIC.

Referencias

[1] Página web de Zabbix: *http://www.zabbix.com/*

[2] Manual oficial de Zabbix. *http://www.zabbix.com/documentation*

[3] Página oficial Nagios. *http://www.nagios.org/*

[4] Zenoss: *http://www.zenoss.com/*

Víctor Manuel Armas Hidalgo
(varmas@pas.ulpgc.es)
Universidad de Las Palmas de Gran Canaria