Integración de herramientas Open Source para la Monitorización del Sistema Informático

Open Source Tools Integration to monitor the Computer System Infrastructure

Mª Isabel Belijar Lisón, Ángel L. Mateo Martínez, Fco. Javier García Ros, Francisco Yepes Candel, Miguel Á. García Lax

Resumen

En organizaciones donde existe una gran infraestructura informática y es necesario garantizar la accesibilidad y disponibilidad de los servicios a los usuarios, se hace necesario la implantación de un sistema de monitorización. Éste sirve de gran ayuda a los administradores para prevenir y localizar posibles fallos en los equipos y servicios. Utilizando herramientas Open Source de monitorización, se configurará un portal centralizado compuesto por diferentes herramientas que ofrecen distintas representaciones de estado para los servicios (estado en tiempo real, estadísticas gráficas, vista jerárquica y mapas de estado), en función del perfil del usuario.

En este artículo se presentará la solución de monitorización implantada en el servicio de informática de la Universidad de Murcia.

Palabras clave: Herramienta Open Source, monitorización, servicios, equipos, dependencia, Nagios.

Summary

When corporations have a large computer system infrastructure and need to garantee services disponibility and accesibility to their users, a system monitoring software becomes necessary. So that, system administrators can prevent and detect potencial system and services failures. Using different Open Source monitoring tools, we are going to configure a central portal based on some tools which offer different status services representations (real time status, graph statistics, tree views and status maps), depending on the user profile.

This article shows the monitoring solution deployed in the IT Department at the University of Murcia.

Keywords: Open Source tool, monitoring, services, hosts, dependency, Nagios.

Utilizando herramientas Open Source de monitorización, se configurará un portal centralizado

1. Introducción

Se deben tomar medidas para reducir el riesgo y el efecto de potenciales fallos de los servicios

Hoy día, cualquier organización, pública o privada, utiliza los **sistemas informáticos** para dar soporte a sus operaciones diarias. Uno de los objetivos fundamentales para las organizaciones es **garantizar la disponibilidad y la continuidad de los servicios** que ofrece, por lo que los sistemas informáticos se convierten en un elemento crítico e imprescindible para éstas.

La necesidad de aumentar la eficiencia y productividad de los sistemas informáticos implica incorporar nuevos elementos hardware (servidores, discos, switches,...) y software (bases de datos, servidores web,...), que llevan asociados unos riesgos tecnológicos: no están exentos de fallos y/o errores imprevistos que pueden tener un impacto negativo sobre el desarrollo de la actividad.

Dado que es difícil evitar paradas imprevistas de un servicio informático, se deben tomar medidas para reducir el riesgo y el efecto de dichas paradas o potenciales fallos de los servicios. Dos de las **soluciones utilizadas** habitualmente son:

1. Montar los servicios como **clusters de servicios,** de forma que se garantice la alta disponibilidad mediante la redundancia en varios nodos.

2. Implantar un **sistema de monitorización** que permita, entre otras cosas, anticiparse a los posibles errores que pueden ocurrir en el sistema informático.

La primera solución se plantea como un recurso **proactivo,** pues se garantiza que ante posibles fallos y/o caídas del sistema, el servicio seguirá estando accesible al existir alta disponibilidad. En cuanto a la segunda solución, se propone como recurso **proactivo,** ya que posibilita la detección de anomalías en el funcionamiento de los equipos y servicios por parte de los responsables, y les ayuda a prevenir que uno o más servicios se degraden completamente. Y también como recurso **reactivo,** ya que si hay una caída o fallo general imprevisible, esta medida permite localizar los elementos que están fallando y los que se han recuperado.

En cualquier entorno, el sistema de monitorización no es imprescindible, pero sí un elemento complementario y recomendable. Además de alertar de los problemas acontecidos en el sistema informático, ofrece generación de estadísticas, permite realizar un seguimiento exhaustivo para conocer los períodos de no disponibilidad de los servicios, así como el uso de los recursos informáticos y su evolución en el tiempo.

2. Motivación y objetivos

Desde el Servicio de Informática de la Universidad de Murcia **(Área de Tecnologías de la Información y las Comunicaciones Aplicadas - ATICA)**, se ofrece variedad de servicios destinados a la comunidad universitaria (web, correo, campus virtual, directorio corporativo, etc.) que requieren una gran infraestructura informática para garantizar la alta disponibilidad y continuidad de los servicios.

La administración de los equipos se basa en virtualización de servidores y servicios montados en clusters. El funcionamiento de cada servicio lleva asociado un conjunto de dependencias desde cada aplicación de alto nivel que percibe el usuario hacia los servidores (bases de datos, sistemas de ficheros, etc.) y hardware con los que realmente opera, incluyendo los elementos de red que permiten la comunicación (routers, firewalls, balanceadores, etc.). Es decir, existen más de 200 elementos (equipos y dispositivos de red) que soportan la actividad corporativa.

La administración de los equipos se basa en virtualización de servidores y servicios montados en clusters

De ahí la necesidad de un **Sistema de Monitorización** que modele las dependencias de los equipos y servicios, desde el nivel más bajo, las comunicaciones de red, hasta el nivel más alto, las aplicaciones y servicios de usuarios. Y así, determinar los fallos que tienen implicación en otros elementos de la cadena de dependencias.

Los objetivos establecidos en este proyecto son:

Uno de los objetivos del proyecto es facilitar la detección de fallos a los administradores

1. **Modelar los equipos y servicios que ofrece ATICA,** así como la cadena de dependencias asociada a cada servicio, para facilitar la detección de fallos a los administradores.

2. **Representar la información de estado de los servicios de alto nivel o aplicaciones de usuario (metaservicios)** para que los usuarios finales conozcan la disponibilidad de los mismos.

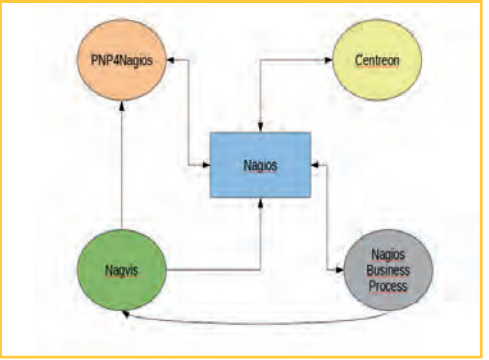
3. **Integrar todas esas herramientas en un portal centralizado,** en el que distintos usuarios con determinados perfiles (administrador, operador y público) tengan información de monitorización con diferente nivel de abstracción.

3. Selección de herramientas Open Source

Actualmente existe una gran variedad de herramientas libres y propietarias para realizar la gestión de la monitorización de los elementos de red y de servicios. En nuestro caso, optamos por utilizar herramientas Open Source por la extensibilidad, integración y personalización que ofrecen.

Hemos evaluado las características y prestaciones de herramientas de monitorización como *Zenoss*[1], *Zabbix*[2], *Centreon*[3] y *Nagios*[4]. En general, todas ellas ofrecen información de estado de los equipos y servicios en tiempo real, notificaciones vía email a los responsables, estadísticas gráficas de comportamiento e histórico de incidencias. Las diferencias que hemos encontrado son en cuanto al nivel de detalle de la información que manejan, la flexibilidad para usar plugins o módulos de terceros y la capacidad de poder ampliar algunas funcionalidades.

FIGURA 1. RELACIÓN DE LAS HERRAMIENTAS



Se optó por Nagios como núcleo de la monitorización por su sencillez, madurez y extensiones disponibles

Finalmente, se optó por Nagios como núcleo de la monitorización por su sencillez, madurez y extensiones disponibles. Para complementar su funcionalidad, hemos adaptado un conjunto de herramientas (ver **figura 1**) que pueden interaccionar con Nagios y facilitan la representación de la información de estado. En particular, nuestro sistema de monitorización está basado en un conjunto de herramientas Open Source, que podemos agrupar en las siguientes categorías:

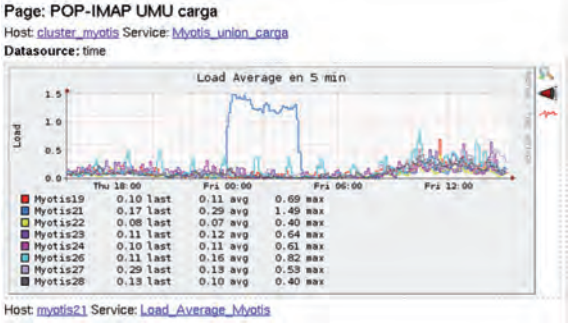
- **Núcleo de la monitorización: Nagios**
  Se utiliza Nagios para realizar las consultas de estado hacia los equipos y servicios. Para ello, se utilizan plugins (comandos) disponibles en el repositorio de Nagios y algunos propios creados para nuestro entorno.

- **Configuración de los objetos de monitorización: Centreon**
  Utilizamos el módulo de configuración de Centreon para gestionar los objetos que forman parte de la monitorización. Mediante él, se definen todos los equipos, servicios, grupos de hosts, grupos de servicios, contactos, comandos y períodos de tiempo, y además, se invoca al proceso que exporta la configuración al formato de los ficheros Nagios.

Mediante PNP4 Nagios se generan automáticamente las estadísticas gráficas asociadas a los equipos y servicios de Nagios

- **Generación de estadísticas gráficas: PNP4Nagios**
  Mediante PNP4Nagios[5], se generan automáticamente las estadísticas gráficas asociadas a los equipos y servicios de Nagios, una vez que se dan de alta. Utilizando el módulo de **Páginas (Pages),** se pueden agrupar distintas gráficas de diferentes servicios en una misma página. La configuración de las gráficas para servicios agregados (metaservicios) se hace en base a las plantillas PHP que maneja (ver **figura 2**).

FIGURA 2. GRÁFICA CON AGREGADO DE CARGA DE DIFERENTES EQUIPOS



- **Representación de servicios de alto nivel: Nagios Business Process**
  Con Nagios Business Process[6] se pueden mostrar los servicios de alto nivel en árbol jerárquico de dependencias. Además, esta herramienta tiene un módulo de **Análisis de Impacto** (Impact Analisys) que permite simular cambios de estado en los equipos y servicios, para ver la implicación que tendrían sobre los servicios de alto nivel.

Para visualizar estas características, se hará una simulación sobre los servicios de alto nivel definidos en nuestro entorno:

1. Hay definidos cuatro procesos de negocio que dependen de un conjunto de clusters y cada uno de ellos está compuesto de los nodos que ejecutan el mismo servicio. (ver **Dibujo 1**).

DIBUJO 1. PROCESOS DE NEGOCIO

El módulo de Análisis de Impacto permite simular cambios de estado en los equipos y servicios

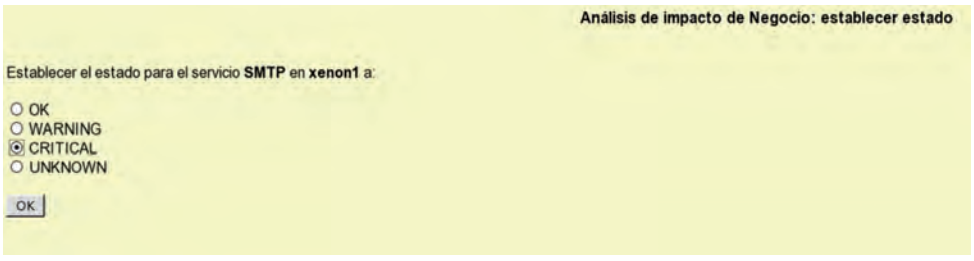
2. Accediendo al proceso de negocio Correo UMU, se ve el listado de equipos y servicios de los que depende (ver **Dibujo 2**).

3. Accediendo sobre un servicio en particular se puede establecer el estado que se pretende simular sobre este servicio (ver **Dibujo 3**).

DIBUJO 2. DEPENDENCIAS DE EQUIPOS Y SERVICIOS.NEGOCIO

El estado simulado del proceso de negocio cambiará según las condiciones definidas para el funcionamiento del servicio

DIBUJO 3. SIMULACIÓN DE CAMBIO DE ESTADO DE UN SERVICIO



DIBUJO 4. SERVICIOS CAMBIADOS DE ESTADO

DIBUJO 5. NUEVO ESTADO DEL PROCESO DE NEGOCIO CORREO

Gráficamente se pueden visualizar los elementos o servicios más representativos del CPD

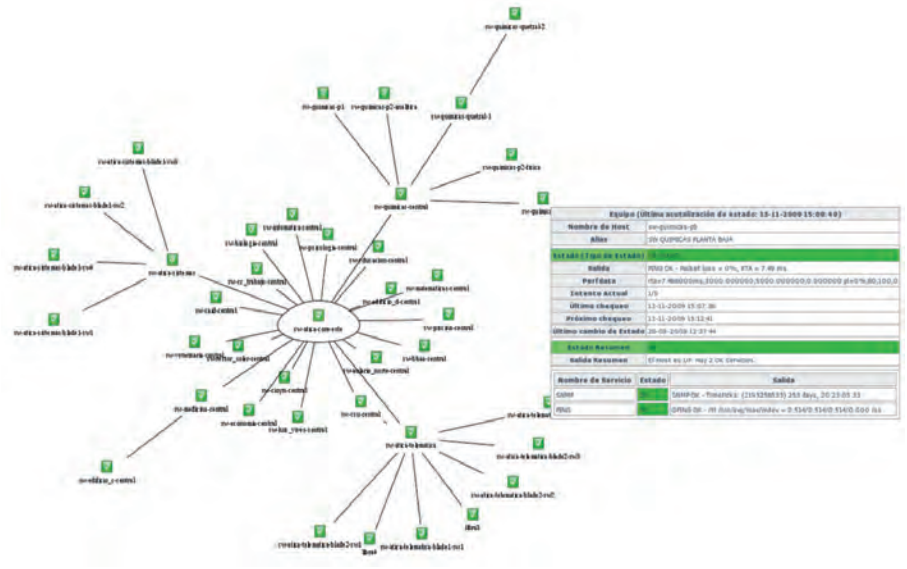
4. Repitiendo el paso 2, cambiamos el estado de dos de los servicios del cluster SMTP a CRITICAL y otro a WARNING (ver **Dibujo 4**).

5. El estado simulado del proceso de negocio cambiará según las condiciones definidas para el funcionamiento del servicio (ver **Dibujo 5**).

- **Representación de mapas gráficos: Nagvis**
  Utilizando Nagvis[7] se pueden representar diseños personalizados de mapas gráficos para mostrar elestado de los equipos, servicios, grupos de equipos y grupos de servicios. Gráficamente se pueden visualizar los elementos o servicios más representativos del CPD. Además, tiene la funcionalidad de **automap**, que consiste en mostrar las dependencias de equipos definidas en Nagios, dinámicamente, partiendo de un nodo raíz. La información de estado de los elementos que se representan se puede ampliar usando desplegables (hover), que aportan más detalles (último y próximo chequeo, último cambio de estado, gráfica asociada a un servicio, servicios asociados a un equipo, equipos asociados a un grupo de equipos, etc.) (ver **figura 3**).

Para facilitar el acceso conjunto de herramientas que componen el sistema de monitorización, se ha configurado el Portal MONITORUM

FIGURA 3. AUTOMAP CON LAS DEPENDENCIAS DE UN SWITCH E INFORMACIÓN DESPLEGABLE



4. Integración de las herramientas en un portal centralizado

Para facilitar el acceso al conjunto de herramientas que componen el sistema de monitorización, hemos configurado un portal unificado, al que hemos denominado **Portal MONITORUM,** que permite:

- **Acceso centralizado.** La entrada al portal se realiza con la autenticación de usuarios contra el LDAP corporativo, y permite dar acceso a todas las herramientas que componen el sistema de monitorización a través de una única plataforma.

- **Gestión de usuarios.** Hemos establecido unos perfiles y grupos de usuarios (administrador, operador y público) que en conjunción con el proceso de autenticación, permite filtrar las vistas de páginas y de los elementos de monitorización a mostrar. De esta manera, un usuario sólo verá aquellos elementos para los que esté autorizado.

- **Flexibilidad de contenidos.** Se puede configurar qué herramientas formarán parte de este portal y los contenidos que se muestran a los usuarios. Debido al gran dinamismo que se da en el software libre, la idea es que si aparecen nuevas herramientas de monitorización que aportan nuevas funcionalidades o mejoran las ya existentes, sean fácilmente integrables dentro de este portal.

Con TYPO3 tenemos dos entornos de visualización de contenidos: el backend y el frontend

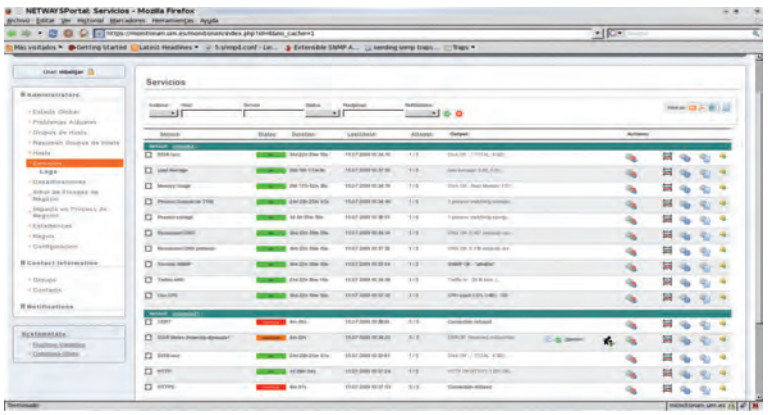
Este portal está construido utilizando como pilar otra herramienta Open Source: **NETWAYS Portal[8]**. Esta herramienta está desarrollada como extensión del gestor de contenidos TYPO3[9] en base a plantillas XML. Tiene un esquema MVC (Modelo, Vista, Controlador) donde se diferencian: la disposición de los elementos en la página web, los elementos lógicos que se van a representar (campos a mostrar), las acciones a realizar (funciones) y la interacción con la base de datos.

Con TYPO3 tenemos dos entornos de visualización de contenidos: el backend, para realizar la gestión de usuarios y administración de los contenidos (plantillas, herramientas, enlaces, etc.), y el frontend, como portal de monitorización que manejan los usuarios.

En este portal hemos definido vistas de estado simplificadas de los servicios de Nagios, con el objetivo de mostrar al usuario una interfaz sencilla. Esto ha sido posible gracias a la flexibilidad de crear plantillas y adaptar las ya existentes para personalizar la información a mostrar. Además, al basarse en un gestor de contenidos, hemos podido extender la funcionalidad añadiendo aplicaciones de terceros y conectarlas entre sí. (ver **figura 4**).

El portal muestra al usuario una interfaz sencilla

FIGURA 4. PORTAL CENTRALIZADO QUE DA ACCESO A LAS HERRAMIENTAS DE MONITORIZACIÓN



Como toda herramienta de gestión de contenidos, *TYPO3* posee un amplio repositorio de extensiones que permite ampliar la funcionalidad de los entornos que se crean bajo éste. En nuestro caso, hemos utilizado las siguientes extensiones:

- **eu_ldap:** para realizar la autenticación basada en LDAP corporativo.
- **net_sproxy:** actúa como proxy para las aplicaciones externas que, se pretende, sean accedidas internamente desde el portal. Con esta extensión se consigue que la mayoría de herramientas se integren como contenido (frame central) en el portal (ver **figura 5**).
- **net_nagioscmd:** actúa como intérprete de comandos hacia los host y servicios monitorizados. Los comandos que ofrece son: habilitar y deshabilitar chequeos, notificaciones, planificación de paradas voluntarias, añadir comentarios, etc.
- **net_dbdata:** conecta la aplicación de NETWAYS Portal con la base de datos (*NDOUtils*[10]) que utiliza Nagios para almacenar información de estado.

Con el Portal MONITORUM obtenemos variedad de vistas y funcionalidades gracias a la diversidad de aplicaciones utilizadas

FIGURA 5. ACCESO A PNP4Nagios DESDE EL PORTAL

Con el *Portal MONITORUM,* tenemos un acceso centralizado al conjunto de herramientas que forman parte del sistema de monitorización y obtenemos variedad de vistas y funcionalidades gracias a la diversidad de aplicaciones utilizadas.

Las organizaciones, utilizando un Sistema de Monitorización, podrán garantizar una buena prestación de sus servicios a los usuarios

5. Conclusiones

Las organizaciones, utilizando un Sistema de Monitorización que les permita realizar un seguimiento exhaustivo del funcionamiento de los sistemas informáticos, podrán garantizar una buena prestación de sus servicios a los usuarios. En general, mediante la gestión y control que nos ofrece, podemos prevenir y detectar las incidencias de nuestros sistemas, disminuyendo los tiempos de re-establecimiento de los servicios.

El uso de herramientas Open Source nos permite:

- Adaptar y extender herramientas de monitorización que aportan diversas funcionalidades a un entorno concreto.
- Una buena gestión del mantenimiento de las herramientas que componen nuestro sistema de monitorización actual y una evolución funcional hacia otras que aporten nuevas características.

Referencias

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

[2] Zabbix: *http://www.zabbix.com/*

[3] Cenreon: *http://www.centreon.com/*

[4] Nagios: *http://www.nagios.org/*

[5] PNP4Nagios: *http://www.pnp4nagios.org/pnp/start*

[6] Nagios Business Process: *http://nagiosbp.projects.nagiosforge.org/*

[7] Nagvis: *http://www.nagvis.org/*

[8] NETWAYS Portal: *http://www.netways.de/en/de/produkte/nagios/*

[9] TYPO3: *http://typo3.org/extensions/repository/*

[10] NDOUtils: *http://prdownloads.sourceforge.net/sourceforge/nagios/ndoutils-1.4b9.tar.gz*

María Isabel Belijar Lisón
(mbelijar@um.es)
Ángel Luis Mateo Martínez
(amateo@um.es)
Francisco Javier García Ros
(jgarcia@um.es)
Francisco Yepes Candel
(pacoy@um.es)
Miguel Ángel García Lax
(glax@um.es)
Sección de Telemática
Área de Tecnologías de la Información y las Comunicaciones Aplicadas (ATICA)
Universidad de Murcia