Eficiencia en el monitoreo de redes y servidores – Implementación de Xymon en Universidad Nacional de Gral. Sarmiento

Analia Barberio, Damian Natale, Diego Rossi, Enrique Vela, Maximiliano Llosa –
Programa Sistemas y Tecnologías de Información de la
Universidad Nacional de Gral Sarmiento

Resumen. Este artículo resume la estrategia implementada para optimizar los recursos con los que cuenta el sector de TI de la Universidad Nacional de General Sarmiento quien no escapa a una situación común en la mayoría de los departamentos tecnológicos de las Universidades Nacionales de Argentina: áreas con equipos reducidos donde la demanda cotidiana pospone lo importante para atender las urgencias. Ante esta situación se desarrolló un proyecto de implementación de una herramienta de monitoreo de red y servidores.

El presente artículo aborda la problemática de la gestión de los recursos humanos en un área de TI y la estrategia de implementación, junto a una breve descripción de los resultados obtenidos a partir de una reingeniería de procesos en el marco de un Sistema de Gestión de Calidad.

Para ello se seleccionó un software open source que permitió profundizar en la estrategia planteada y lograr el objetivo de optimización de los recursos en el área de redes y tecnologías.

Palabras Claves: Calidad, monitoreo, Xymon, Hobbit, BigBrother, BBwin.

1 Introducción

La Universidad Nacional de Gral. Sarmiento cuenta con un Programa de Sistemas y Tecnologías de Información que presta servicios de manera centralizada a toda la Universidad. El sector dedicado a redes y servidores cuenta con un equipo muy reducido de personal. Resulta difícil ampliar los recursos humanos del equipo por varios motivos, es por ello que se trabajó fuertemente en la implementación de estrategias que permitan reducir el tiempo de tareas operativas para poder aprovecharlo en tareas de desarrollo e innovación tecnológica.

Actualmente el Programa se encuentra implementando un Sistema de Gestión de Calidad, basado en mejora continúa con vistas a lograr la Certificación ISO 9001. En ese contexto se evaluaron distintas herramientas de software libre, se optó por el Xymon. Este artículo realiza una breve reseña del proyecto.

El Xymon es una herramienta para monitorear el estado del tráfico de la red, los dispositivos y los servidores además de las aplicaciones que se ejecutan en ellos. Proporciona una forma sencilla e intuitiva de control a través de un navegador web. En este artículo se describe la herramienta y el proceso de implementación. Es un software de código abierto, licenciado bajo la GPL de GNU.

2 Xymon, herramienta personalizada de monitoreo como estrategia de gestión

2.1 Evolución Tecnológica del Xymon

Xymon fue conocido como "Hobbit" hasta noviembre de 2008, cuando se denominó con el actual nombre. Inicialmente comenzó como una mejora de Gran Hermano llamado "bbgen". Durante un período de 5 años, xymon ha evolucionado desde un pequeño complemento para un sistema de monitoreo con capacidades muy por encima de lo que había en el paquete Big Brother original. Aun sigue manteniendo cierta compatibilidad con el Gran Hermano, por lo que es posible migrar de Gran Hermano a xymon sin demasiados problemas.

2.1.2 Versiones

- La versión 1 de bbgen fue lanzado en noviembre de 2002, y se optimiza la generación de páginas web en los servidores de Gran Hermano.
- La versión 2 de bbgen fue lanzado en abril de 2003, y añadió una herramienta para realizar pruebas de red.
- La versión 3 de bbgen fue lanzado en septiembre de 2004, y se elimina el uso de varias bibliotecas externas para pruebas de red, lo que resulta en una mejora significativa del rendimiento.
- Con la versión 4.0 liberada el 30 de marzo de 2005, el proyecto se desacopla del Gran Hermano, y cambió su nombre a Hobbit. Esta versión fue la primera implementación completa del servidor Hobbit, pero todavía se utilizan los datos recogidos por los clientes de Gran Hermano.
- La versión 4.1 fue lanzado en julio de 2005, incluyó un simple cliente para Unix.
- La versión 4.2 fue lanzado en julio de 2006, e incluye un cliente totalmente funcional para Unix.
- La versión 4.3 fue lanzado en noviembre de 2010, e implementó el cambio de nombre del proyecto a xymon. Este nombre ya se introdujo en 2008 con una

versión del parche de 4.2, pero con la versión 4.3.0 de este cambio de nombre se aplicó en forma total.

2.2 Características

- **Monitoreo de hosts y redes:** Xymon recoge información sobre los sistemas de dos maneras diferentes: desde una consulta a los servicios de red (Web, LDAP, DNS, correo, etc), o desde secuencias de comandos que se ejecutan en el servidor de xymon o en los sistemas que supervisan. El paquete incluye un cliente xymon que se puede instalar en los servidores que controlan, el cual recopila datos acerca del CPU, discos, utilización de la memoria, logs, puertos de red en uso, archivos, directorios de información y mucho más. Toda la información se almacena dentro del servidor xymon, así también como definir las condiciones que dan lugar a las alertas, por ejemplo, si un servicio de red deja de responder, o un disco se llena.
- **Front-end web simple, intuitivo y personalizado:**"El verde es bueno, el rojo es malo". La utilización de las páginas web xymon es tan simple como eso. Los hosts se pueden agrupar de una manera fácil de leer según la infraestructura local y se presentan en una estructura de árbol. Las páginas web utilizan muchas técnicas para transmitir información acerca de los sistemas de seguimiento, por ejemplo, diferentes iconos se puede utilizar para estados recientemente cambiaron; enlaces a subpáginas se pueden enumerar en varias columnas; diferentes iconos se puede utilizar para conexiones de red. Se pueden quitar columnas para eliminar información no deseada, o siempre incluir cierta información, se pueden mostrar nombres de hosts personalizados independientemente de su verdadero nombre de host. Se puede tener enlaces automáticos a la documentación en línea, por lo que la información sobre los sistemas críticos está a sólo un clic de distancia.

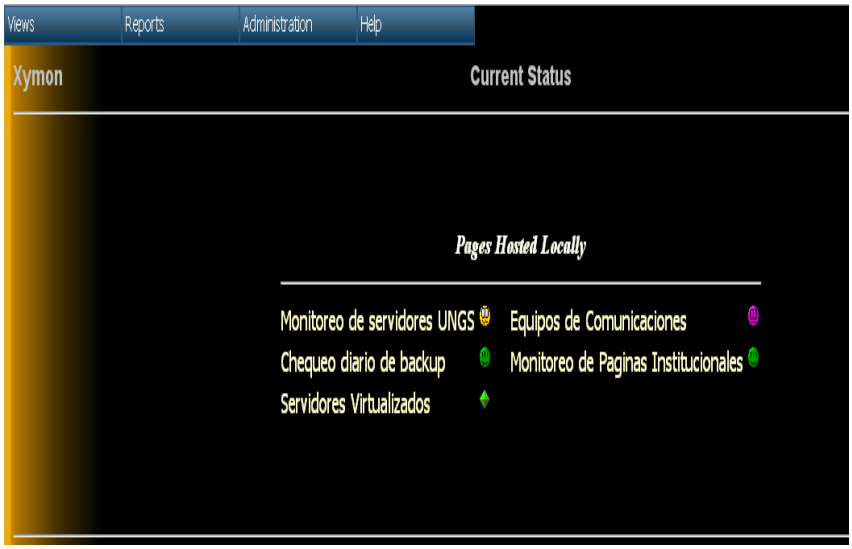

Fig. 1. Página web de visualización de recursos de la Universidad Nacional de General Sarmiento (Xymon 4.3.7)

- **Configuración centralizada:** Toda la configuración de xymon se realiza en el servidor. Aunque se controlen cientos o miles de ordenadores, puede controlar su configuración de forma centralizada en el servidor xymon – por lo que no hay necesidad de acceder a un sistema que se acaba de modificar.
- **Pruebas reales de servicios de red:** Las herramientas de prueba de red ponen a prueba los protocolos más comúnmente utilizados, incluyendo HTTP, SMTP, IMAP, POP3, DNS, LDAP (servicios de directorio), y muchos más. Al comprobar sitios web, no solo comprueba si el servidor web está respondiendo, sino también que la respuesta sea correcta, haciendo coincidir la respuesta contra un patrón predefinido o una suma de comprobación. Los protocolos que utilizan cifrado SSL como HTTPS son sitios web totalmente compatibles, y al comprobar dichos servicios el probador de red se ejecutará automáticamente una comprobación de la validez del certificado del servidor SSL, y generara un alerta acerca de los certificados que están a punto de expirar.

Fig. 2. Página web de visualización de páginas institucionales de la Universidad Nacional de General Sarmiento (Xymon 4.3.7)

- **Resulta sencillo adaptar a las propias necesidades:** Incluye una gran cantidad de tests en el paquete principal, pero además permite realizar de forma muy fácil los tests que no se encuentren en los mismos. Permite escribir scripts de prueba en diferentes lenguajes (bash, python, php, etc.) y que los resultados se muestren como columnas de estado regulares en el front-end web. Se puede activar alertas de éstos, e incluso generar gráficos con la información de manera simple.

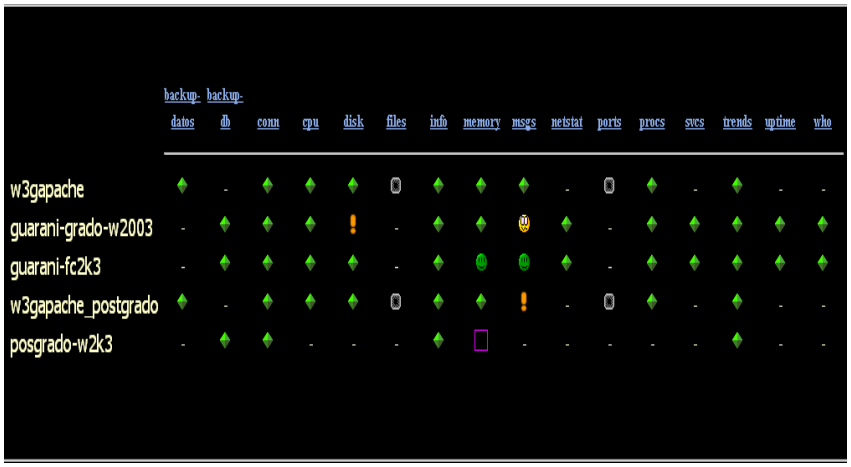

Fig. 3. Página web de visualización de los servidores Guaraní de la Universidad Nacional de General Sarmiento (Xymon 4.3.7)

- **Análisis de tendencias, datos históricos e informes:**Almacena tendencias y la información acerca de todo lo controla. Si se necesita ver cómo se comportan los sistemas con el tiempo, xymon tiene toda la información que se necesita. Ejemplo: Los tiempos de respuesta de una página web durante las horas pico, la utilización de CPU durante las últimas 4 semanas, o la disponibilidad de un servicio. Todas las mediciones pueden ser puestas a disposición en gráficos o archivos exportables.
  Cuando se necesita profundizar en los acontecimientos que han ocurrido, xymon proporciona una poderosa herramienta para visualizar el historial de eventos para cada estado de registro, con una visión general de los problemas que han ocurrido en el pasado y fácil de usar en el evento. En los informes, se puede configurar el tiempo de inactividad planificado, de acuerdo nivel de disponibilidad del servicio, el tiempo de disponibilidad del servicio y generar informes de disponibilidad que muestran directamente la disponibilidad real. Los informes de disponibilidad de servicio se pueden generar sobre la marcha, o por ejemplo, pre-generados para el reporte mensual.
- **Vista de roles:**Se puede tener distintas vistas de un mismo hosts para diferentes partes de la universidad, por ejemplo, una visión para el grupo de hardware, y otra vista para los webmasters.
- **Alertas configurables:** Permite configurar el envío de alertas por diferentes vías. Además de otras opciones muy útiles como el envío en un alerta una única vez y así evitar recibir varios mensajes que informen del mismo error.
- **Cliente multiplataforma:** El cliente xymon funciona en todos los sistemas de tipo Unix, incluyendo Linux, Solaris, FreeBSD, AIX, HP-UX, Microsoft Windows (por medio del cliente BBWin) y otros.

2.3 Seguridad

Todas las herramientas del xymon deben ejecutarse bajo una cuenta de usuario sin privilegios. Al instalar el cliente en Linux Debian desde el repositorio oficial se general el usuario denominado "hobbit" sin privilegios (se recomienda anular el intérprete de comandos para este usuario).

Las comunicaciones entre el servidor y los clientes utilizan el puerto TCP 1984 (BigBrother). Si el servidor se encuentra detrás de un firewall, debe permitir conexiones entrantes a dicho puerto. Normalmente, los clientes xymon - es decir, los servidores que se están supervisando - deben permitir conectar con el servidor xymon en este puerto.

Las páginas web xymon se generan dinámicamente a través de programas CGI. El acceso a las páginas web xymon se controla a través de los controles de acceso del servidor web, por ejemplo, puede requerir un inicio de sesión a través de alguna forma de autenticación HTTP.

2.4 Características del hardware utilizado

En el caso de la UNGS el software de monitoreo está instalado en un servidor virtualizado con Vmware ESXI 5.1. Se le asigno las siguientes características:

- 1 socket virtual de un core (Intel Xeon E5405 2.00 GHz)
- 512 MB de memoria RAM
- 1 disco rígido de 80 GB

2.5 Características del software utilizado

- Sistema operativo (GNU/Linux Debian 6.0)
- Servidor WEB (apache2)
- Monitoreo de trafico de red (mrtg)
- Chequeo de servicios SSL (openssl)
- Chequeo del servicio LDAP (openldap)
- Creación de Gráficos (rrdtool)
- Comunicación por medio del protocolo SNMP (snmp)
- Servidor de monitoreo (xymon)
- Chequeo de los servicios del servidor donde se instalo la herramienta de monitoreo (xymon-client)

2.6 Diseño Funcional

Los controles se agruparon en: Monitoreo de servidores UNGS, Chequeo diario de backup, Servidores Virtualizados, Equipos de Comunicaciones y Monitoreo de páginas institucionales. Dentro de cada sección se desagregan los distintos test definidos para monitorear el estado del hardware, del software y de la conectividad.

En cuanto a la información estadística y de registro, se desarrollaron distintos reportes que permiten automatizar la medición de métricas que abastecen el sistema de gestión de calidad. Esto redunda en una facilitación del mantenimiento de los registros del sistema de calidad.

3 Conclusiones

La implementación del Xymon permitió reducir en un 80 % la carga horaria dedicada a los controles de estado de la red.

La integración con el Sistema de Gestión de Calidad a partir de la automatización de la generación de las métricas permitió asegurar la actualización continua de nuestros registros para evaluar la alineación con los objetivos estratégicos del área.

El personal del sector se encuentra motivado, ya que puede dedicar su tiempo a tareas de desarrollo e innovación y esto redunda en un crecimiento exponencial del estado del servicio que brindamos por la incorporación de innumerables mejoras a la red que si bien estaban previstas y detectadas históricamente, la demanda diaria impedía avanzar sobre ellas.

Referencias

1. Página oficial de xymon, http://www.xymon.org
2. Foro de xymon, http:/lists.xymon.com/mailman/listinfo/xymon
3. Página oficial de Linux Debian, http://www.debian.org
4. Página oficial de BBWin, http://bbwin.sourceforge.net/
5. Página oficial de descarga de paquetes Linux Debian, http://www.debian.org/distrib/packages
6. Página oficial de GNU, http://www.gnu.org/
7. Página oficial de Universidad Nacional de General Sarmiento, http://www.ungs.edu.ar/