

## ApiaMonitor

### Monitor de Infraestructura BPMS

Por: Ing. Manuel Cabanelas – Product Manager de Apia

[Manuel.Cabanelas@statum.biz](mailto:Manuel.Cabanelas@statum.biz)

<http://www.statum.biz> – <http://www.statum.info> – <http://www.statum.org>

### Abstract

A la hora de monitorear la ejecución de un sistema en producción implementado utilizando un BPMS, existen dos grupos de usuarios con necesidades y responsabilidades claramente diferentes. Los responsables del negocio y los responsables de la infraestructura.

Los responsables de negocio requieren de herramientas que les permitan consultar acerca de la situación actual en la que se encuentran sus procesos ya sea en forma individual o agrupada, y la evolución de los mismos hasta llegar a la situación actual. En este sentido las herramientas de Business Intelligence brindan un soporte adecuado para satisfacer dichas necesidades, mediante la definición y uso de cubos multidimensionales, indicadores, paneles de control y reportes.

Los responsables de infraestructura están más preocupados en que los procesos funcionen sin interrupciones, y con una performance adecuada a las necesidades del negocio.

Este artículo describe las características de la herramienta provista por Apia para el monitoreo de la infraestructura tecnológica utilizada.

### Factores Motivantes

Las soluciones basadas en productos BPMS, generalmente son implementaciones complejas que atraviesan horizontalmente a toda la organización, e involucran la integración de diversas aplicaciones, y bases de datos, excediendo en algunos casos la frontera de la propia organización. Este panorama hace extremadamente dificultosa la labor del personal de TI, quien

debe garantizar el correcto funcionamiento de dicha infraestructura. Para ello se torna necesario contar con herramientas que permitan:

- Determinar en tiempo real problemas en la ejecución del sistema.
- Contar con un análisis histórico de la ejecución del sistema que permita de forma pro-activa identificar futuros problemas.
- Tomar acciones en tiempo real para solucionar o evitar problemas en la ejecución del sistema.
- Permitir definir políticas de niveles de servicios (SLA), y contar con mecanismos de notificación automáticos ante la violación de dichos acuerdos.

### Arquitectura de la solución

La herramienta para el monitoreo de la infraestructura de TI provista por Apia, consiste en:

- Un Servidor Central de Monitoreo, el cual recibe información acerca de los eventos monitoreados de diferentes agentes instalados en las aplicaciones y servidores que serán monitoreados. Este servidor es el encargado de:
  - Registrar los eventos obtenidos por los agentes.
  - Controlar los niveles de servicio (SLA), ejecutando acciones que pueden estar pre-determinadas.
  - Brindar la información a las diferentes consolas de administración del sistema (Clientes de Monitoreo).
- Un Cliente de Monitoreo, el cual permite a los usuarios configurar los datos del Servidor Central de Monitoreo, y visualizar la información asociada a los distintos eventos.
- Agentes de Monitoreo, encargados de comunicar los eventos al Servidor Central de Monitoreo. Cada aplicación/servidor a ser monitoreado debe tener un Agente de Monitoreo configurado de forma adecuada para poder recabar la información de monitoreo que sea necesaria. Dentro de

los elementos de una instalación que típicamente son monitoreados, se encuentran:

- El Servidor de Aplicaciones ejecutando el BPMS. En instalaciones de gran porte, existen varios servidores configurados en cluster para soportar altos volúmenes de usuarios concurrentes.
- El Servidor de Base de Datos utilizado por el BPMS, para persistir y consultar la información asociada al mismo.
- El Servidor de Business Intelligence utilizado para realizar consultas analíticas sobre la ejecución de los procesos, tareas, usuarios y grupos de trabajo.
- El File Server utilizado por el BPMS para el almacenamiento de documentos.
- Otros servidores de Aplicaciones o de Bases de Datos que pueden estar siendo utilizados por los procesos definidos en el BPMS, ya sea a través de reglas de negocio, consultas o interfaces.

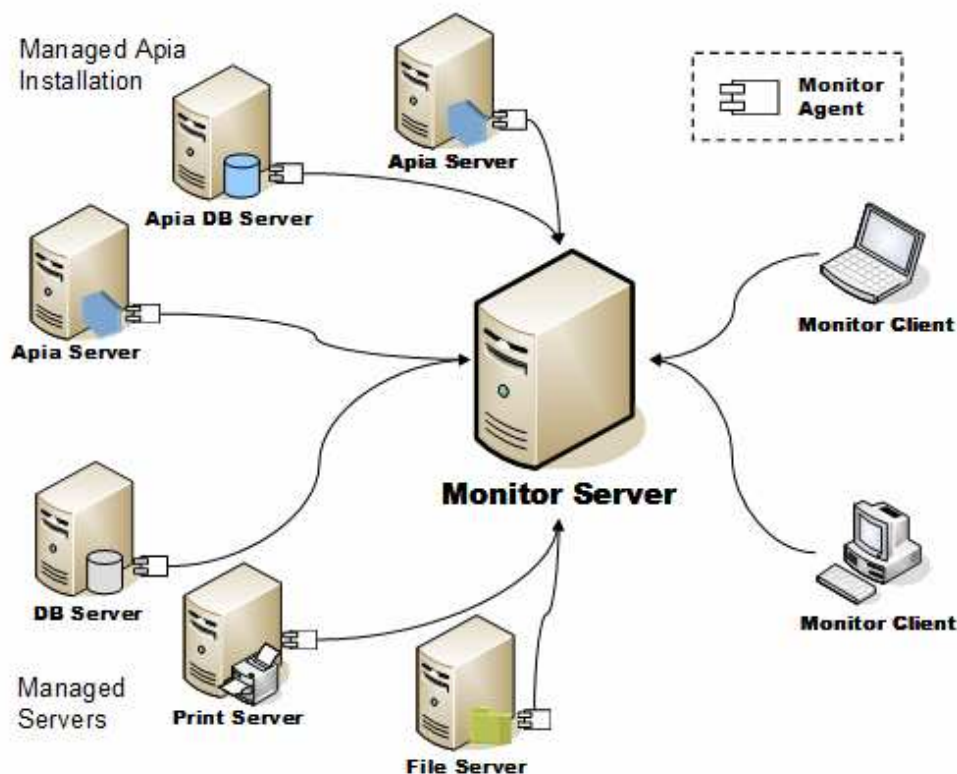


Ilustración 1: Arquitectura de la Solución

### Eventos de Monitoreo

Se le denomina evento de monitoreo a cualquier evento que deba ser comunicado a través de un Agente al Servidor Central de Monitoreo, de forma de que este último pueda aplicar las reglas de SLA y generar la información de ejecución necesaria para realizar el monitoreo de un sistema.

Los eventos de monitoreo pueden ser agrupados dentro de alguna de las siguientes tres categorías:

- **Single Event.** Evento sistémico y puntual generado por algún sistema. Un ejemplo de este tipo de evento es el reporte de un error de sistema y una descripción de la falla. Dentro de la información enviada por estos eventos encontramos:
  - El código asociado al evento (por ejemplo el nombre de una exception).

- El nivel o gravedad del evento (critical, error, warning, etc.)
  - Descripción. Detalles sobre el evento (por ejemplo el stack trace de una exception).
- Timed Event. Evento sistémico que sucede en dos tiempos, teniéndose un evento de comienzo y uno de final bien marcados. Para este evento es tan importante el tiempo de ejecución del evento total, como el resultado de la ejecución ya que el indicador de fin de evento puede nunca llegar. Estos eventos son utilizados para obtener indicadores de tiempos de ejecución de elementos de sistemas (como por ejemplo una consulta a una base de datos, la invocación a un Web Service, el inicio de un proceso, la completitud de una tarea, etc.). Los atributos más relevantes de estos eventos son:
    - El código asociado al evento (por ejemplo el nombre de un Web Service accionado).
    - El estado del evento (en ejecución, finalizado, finalizado con error, finalizado por timeout, etc.).
    - El tiempo de ejecución del evento.
    - El identificador del proceso asociado al evento. Esta información será utilizada para tomar acciones sobre el sistema (por ejemplo finalizar la ejecución del proceso, si el mismo permanece en ejecución durante un tiempo excesivo).
- Sampling Event. Es un evento temporizado lanzado desde un Agente de Monitoreo, que toma alguna medida del servidor y/o aplicación. Ejemplos de este tipo de eventos son: el porcentaje de uso de CPU o memoria del Servidor de Aplicaciones o Base de Datos, la cantidad de espacio libre en disco, la cantidad de usuarios conectados al sistema, etc.. Como atributos de estos eventos encontramos:
    - El código asociado al evento (por ejemplo porcentaje de CPU utilizado).
    - El valor asociado a la muestra tomada.

## Niveles de Servicio

A través del Cliente de Monitoreo pueden ser definidos en el Servidor Central de monitoreo, niveles de servicio para diferentes operaciones del sistema. Estos niveles de servicio son implementados mediante la definición de reglas sobre los eventos recibidos por el Servidor de Monitoreo, y controlados en tiempo real por el mismo.

Asociado a dichos SLA es posible definir acciones, a ser ejecutadas al superar los umbrales definidos para dichos niveles de servicio. Estas acciones pueden ser informativas (envío de e-mail o SMS para advertir de un problema) o correctivas (intentar matar un proceso bloqueado, aumentar el tamaño de un pool de conexiones, etc.).

Una regla de SLA tiene tres partes principales:

- Un filtro que indica para que eventos será aplicada la regla de SLA. Generalmente el filtro indicará el tipo de evento, el código y el origen del evento a ser estudiado.
- Una condición que indica cuando un evento genera un incumplimiento de un nivel de servicio.
- Una acción a ejecutarse ante el incumplimiento de una regla.

Algunos ejemplos de posibles reglas son:

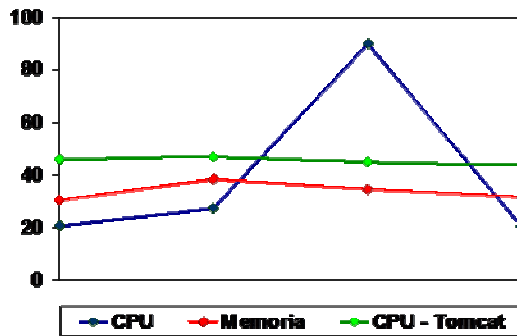
- Para los Sampling Event “% de uso de CPU”, del servidor “serverName” que superen el valor de 80%, enviar un SMS al administrador del sistema.
- Para los Timed Events asociados a la ejecución del Web Service “webServiceName”, cuya ejecución exceda el minuto, cancelar el proceso asociado.
- Para todos los Single Events de nivel “critical” enviar un e-mail al administrador del sistema.

El siguiente gráfico presenta un ejemplo del tipo de información mostrada a través del cliente de monitoreo.

--- Agent Status ---

Agent	Server	Connection
Apia_1	SVR_01	OK
Apia_2	SVR_02	OK
Apia_3	SVR_01	OK
DB_1	DB_SVR_01	NOK

--- Latest Samples ---



--- Latest SLA Violations ---

Agent	Time	Violation
Apia_1	3 sec. ago	Wen Service WS_1 execution > 1m.
Apia_2	1 hour ago	Complete Task TSK_1 > 30s.
Apia_1	2 days ago	% CPU > 75%
DB_1	6 days ago	Connection pool empty

--- Unclosed Events ---

Agent	Time	Description
Apia_1	3 sec. ago	Exec. SQL: select * from ...
Apia_2	3 sec. ago	Exec. SQL: insert into ...
Apia_2	4 sec. ago	Exec. Rule: getTotalInvoice
Apia_2	5 sec. ago	Exec. WS: WS_2

--- Latest Events ---

Agent	Time	Description
Apia_1	30 min. ago	FATAL - ApiaException
Apia_2	2 hrs. ago	WARNING - Apia DB Pool empty

Ilustración 2 Información de Monitoreo

En la siguiente pantalla se puede observar la interfaz gráfica del cliente de Monitoreo.

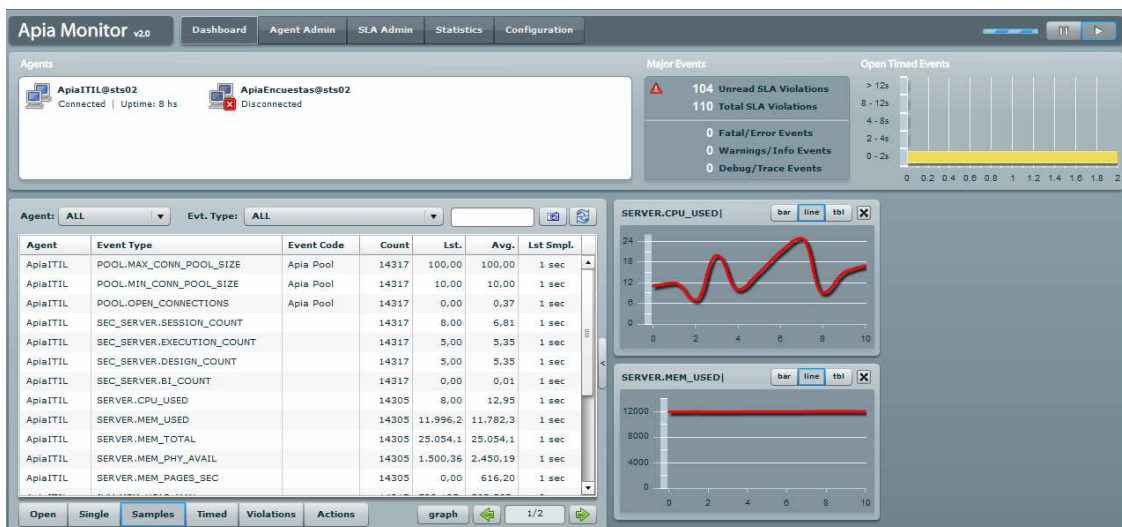


Ilustración 3 Cliente de Monitoreo

Estadísticas

A través del cliente de monitoreo pueden ser obtenidos reportes estadísticos de la información recibida por los agentes. A modo de ejemplo, puede ser obtenida información agrupada en forma diaria, semanal o mensual acerca de: las consultas mas ejecutadas, las que más demoran, los máximos, mínimos y promedios de demora, la cantidad de violaciones de SLA registradas, la

cantidad máxima, mínima y promedio de usuarios conectados por franja horaria, los picos de consumo de memoria y CPU por franja horaria, etc.

En el siguiente gráfico se puede observar las cantidades máxima, mínima y promedio de usuarios conectados a la aplicación por franja horaria, para la semana actual.

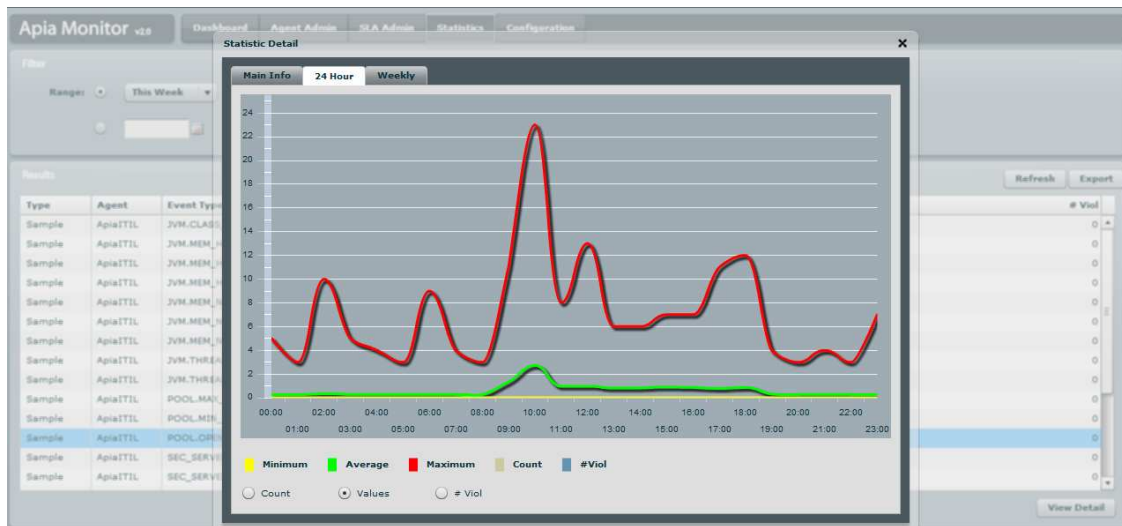


Ilustración 4 Estadísticas

## Conclusiones

El uso de ApiaMonitor trae aparejados una gran cantidad de beneficios, entre ellos destacamos:

- Alcanzar niveles de disponibilidad de los procesos implementados en el BPMS del orden de 99,9%.
- Anticipar y planificar las necesidades de ampliación en el hardware y Software utilizado por el BPMS.
- Detectar en forma automática errores del sistema, facilitando la labor de depurado de los componentes de software desarrollados.
- Optimizar la performance del sistema, mediante la detección de los componentes de software más utilizados y que presentan plazos de ejecución más altos.