PRACTICA EMPRESARIAL TELEFÓNICA - MOVISTAR

Proyecto: Monitoreo de plataformas por medio de Bmc ProactiveNet

CARLOS MAURICIO MÁRQUEZ LOZANO

UNIVERSIDAD PONTIFICIA BOLIVARIANA

FACULTAD INGENIERIA ELECTRÓNICA

FLORIDABLANCA

2014

PRACTICA EMPRESARIAL TELEFÓNICA - MOVISTAR

Proyecto: Monitoreo de plataformas por medio de Bmc ProactiveNet

Presentado por:

CARLOS MAURICIO MÁRQUEZ LOZANO

I.D: 000-126155

Monografía para optar por el Título de Ingeniero Electrónico

Dirigido Por:

Ph.D. Jhon Jairo Padilla Aguilar

UNIVERSIDAD PONTIFICIA BOLIVARIANA

FACULTAD INGENIERIA ELECTRÓNICA

FLORIDABLANCA

2014

PÁGINA DE ACEPTACIÓN

El documento **PRACTICA EMPRESARIAL TELEFÓNICA – MOVISTAR (Proyecto: *Monitoreo de plataformas por medio de Bmc ProactiveNet)***, elaborado por **CARLOS MAURICIO MÁRQUEZ LOZANO**, ha sido aprobado para optar al título de Ingeniero Electrónico, de acuerdo con lo estipulado por la Facultad de Ingeniería Electrónica de la Universidad Pontificia Bolivariana – Seccional Bucaramanga.

_____

_____

_____

_____

_____

_____

_____

_____

Firma Ph.D. Jhon Jairo Padilla Aguilar

Tutor Asignado

_____

Fecha

ADVERTENCIA

Por políticas de seguridad de TELEFÓNICA - MOVISTAR, en el presente documento no se revelará información de clientes, presupuesto, direcciones, IP’s, nombres de servidores, comandos ejecutados u otro tipo de información que afecte la integridad del negocio de la empresa.

DESCRIPCIÓN DE LA EMPRESA TELEFÓNICA – MOVISTAR

Telefónica, es uno de los operadores integrados de telecomunicaciones líderes a nivel mundial en la provisión de servicios y soluciones de comunicación, información y entretenimiento, con presencia en más de 25 países y cuenta con una base de clientes que supera los 320,3 millones a septiembre de 2013.

Telefónica es una empresa totalmente privada, con más de 1,5 millones de accionistas directos y cotiza en el mercado continuo en las bolsas españolas (Madrid, Barcelona, Bilbao y Valencia) y en las de Londres, Nueva York, Lima y Buenos Aires.
En Latinoamérica, el grupo Telefónica se posiciona como operador líder en países como Brasil, Argentina, Chile y Perú, y cuenta con una participación relevante en Colombia, Cosa Rica, Ecuador, El Salvador, Guatemala, México, Nicaragua, Panamá, Puerto Rico, Uruguay y Venezuela.
En Europa, la compañía tiene presencia, además de en España, en el Reino Unido, Irlanda, Alemania, República Checa y Eslovaquia, dando servicio a más de 101,9 millones de clientes al cierre de septiembre de 2013.

En Colombia, Telefónica tiene presencia desde el 2004, año en el cual empezó a actuar sobre el mercado móvil con la adquisición del operador Bellsouth. En el año 2006, Telefónica adquirió el control y la gestión de Colombia Telecom. Posteriormente, en abril de 2012 llegó a un acuerdo con el gobierno nacional para reestructurar la organización y los negocios de telefonía fija y móvil que contemplaba la fusión de Colombia Telecomunicaciones y Telefónica Móviles Colombia. Dicha fusión significó la creación del segundo mayor operador integrado del país.

A Junio de 2012, Telefónica Móviles maneja aproximadamente el 84% de la base de clientes del grupo Telefónica en Colombia, lo cual convierte la telefonía móvil en un sector de negocio importante para la organización.

Telefónica Móviles Colombia cuenta con 16 Direcciones que se encuentran bajo la gestión del Presidente Ejecutivo y el CEO. Entre estas Direcciones se encuentra la dirección Comercial, TI, Mercadeo, Empresas y Redes, entre otras.
El área de *Plataformas VAS y Tasadores* es una gerencia que se deriva de la Dirección de Redes. Esta área es la encargada de gestionar y mantener en óptimo funcionamiento diversas plataformas de servicios de voz móvil de Telefónica Móviles Colombia y a su vez de realizar la tasación de los servicios y el tráfico generado por los abonados de la red en servicios de voz y de valor agregado.

GLOSARIO

Abonado: Cualquier persona física o jurídica que haya celebrado un contrato con un proveedor de servicios de comunicaciones electrónicas disponibles para el público, para la prestación de dichos servicios.

Agente PATROL: Es una aplicación de máquina virtual, la cual, se instala en cada computadora. La función principal de esta aplicación es el monitoreo y la administración de recursos de operación, tales como CPU, memoria, aplicaciones, y bases de datos, usando KMs.

Base de datos: Conjunto de datos que se encuentran organizados y relacionados entre sí, con el fin de satisfaces tratamientos de información implicados en las actividades de una empresa.

Backup: Es una copia que se realiza de los datos originales presentes en una base de datos o en cualquier dispositivo de almacenamiento, con el fin de disponer de un medio de recuperarlos en caso de pérdida.

BMC ProactiveNet: Es una plataforma de integración, la cual combina el manejo de eventos, la gestión de alarmas y el análisis de datos de las diferentes plataformas monitoreadas.

Crontab: Es un archivo de GNU Linux donde se guardan las distintas tareas programadas de los usuarios.

Filesystem: Componente del sistema operativo encargado de administrar y facilitar el uso de las memorias periféricas. Sus principales funciones son la asignación de espacio a los archivos, la administración del espacio libre, y la administración del acceso a los datos resguardados.

Hardware Sentry: es un modulo de conocimiento (KM) destinado para un agente PATROL; y por tal motivo, debe ser instalado en cada máquina a monitorear con su respectivo agente.

KMs: La base de conocimiento entera de un agente y su funcionalidad, se define como KM, Knowledge module/ modulo de conocimiento.

Log: Es un registro oficial de eventos durante un rango de tiempo en particular.

OSS: Sistemas de información directamente vinculados a la red de telecomunicaciones para el mantenimiento, supervisión, configuración de elementos de red y gestión de fallas.

Servicio de telecomunicaciones: Es un servicio ofrecido a uno o más clientes por parte de un proveedor de telecomunicaciones para hacer posible la transmisión y recepción de información en forma electrónica.

Servidor: equipo informático en el cual se aloja un servicio de telecomunicaciones. Se encarga de recibir peticiones de servicio y enviar respuestas a los clientes.

Tarea programada: Es una orden o un conjunto de órdenes que se ejecutan de manera planeada por medio de la configuración disponible en el sistema operativo. En Linux, las tareas programadas se administran a través de crontab.

TNES:
Traffica Network Element Server.

TRAFFICA: Es un sistema de monitoreo en tiempo real de la red. Este sistema monitorea la calidad del servicio en tiempo real, el trafico en los elementos de red, gestiona alarmas, recopila datos, etc.

XYMON: Xymon es una herramienta para monitorear servidores, aplicaciones y redes. Este colecta información sobre la salud de los computadores, las aplicaciones que estos ejecutan y las conexiones de red entre ellos.

RESUMEN GENERAL DE TRABAJO DE GRADO

TITULO: PRACTICA EMPRESARIAL TELEFÓNICA – MOVISTAR

AUTOR(ES): Carlos Mauricio Márquez Lozano.

FACULTAD: Facultad de Ingenier&#65533;a Electr&#65533;nica

DIRECTOR(A): Ph.D. Jhon Jairo Padilla Aguilar.

RESUMEN

Partiendo de la necesidad de brindar y garantizar una serie de servicios constantes y confiables a todos los usuarios externos e internos de la compañía, es fundamental realizar un seguimiento a cada uno de los procesos que se presentan en los sistemas a cargo de la Jefatura Plataformas VAS, ya sean procesos de sistema operativo, bases de datos, hardware, conectividad, o servicios, entre otros. Teniendo en mente esta premisa, el principal objetivo en el desarrollo de la práctica empresarial y del proyecto Monitoreo de plataformas por medio de BMC ProactiveNet, es la integración de las diferentes plataformas en un sistema de supervisión confiable, exacto, eficiente y claro, el cual, permita: ⎫ Integrar las plataformas a cargo de la Jefatura, en un único y centralizado sistema de monitoreo. ⎫ Realizar el monitoreo de los diferentes componentes hardware y software de cada plataforma. ⎫ Detectar anormalidades, interrupciones o posibles fallas en los sistemas. ⎫ Efectuar una detección de problemas inmediata, de forma que sea posible efectuar una solución proactiva de los inconvenientes que se presenten. ⎫ Generar reportes, notificaciones y alarmas ante errores presentes en los sistemas por medio de correo electrónico y/o mensaje de texto. Para lograr estos objetivos, se implementa BMC ProactiveNet, como una herramienta que combina la gestión de eventos y el análisis de datos (líneas de base, detección de anomalías y algoritmos analíticos) en una sencilla e integrada solución. La gestión de eventos proporciona la detección proactiva y la resolución de problemas de TI en tiempo real. Además, el análisis de datos busca proporcionar un centro de investigación, el cual permita detectar anomalías, predecir interrupciones y proporcionar diagnósticos detallados a partir de la información recopilada en cada sistema.

PALABRAS CLAVES:

Agente PATROL, Hardware Sentry, KM, TRAFFICA, OSS, servidor.

V° B° DIRECTOR DE TRABAJO DE GRADO

GENERAL SUMMARY OF WORK OF GRADE

TITLE: PRACTICA EMPRESARIAL TELEFÓNICA – MOVISTAR

AUTHOR(S): Carlos Mauricio Márquez Lozano.

FACULTY: Facultad de Ingenier﷿a Electr﷿nica

DIRECTOR: Ph.D. Jhon Jairo Padilla Aguilar.

ABSTRACT

Based on the need to provide and ensure consistent and reliable services for all the external and internal users of the company, it is essential to monitor each of the processes that occur in the systems maintained by the Jefatura Plataformas VAS, whether these are operating system processes, database, hardware, connectivity, or services, among others. Having this premise in mind, the main objective of the internship and the project “Monitoreo de Plataformas por medio de BMC ProactiveNet”, is the integration of different platforms in a reliable, accurate, efficient and clear monitoring system, which allows: ⎪ Integration of platforms in a single and centralized monitoring system. ⎪ Monitoring hardware and software components of every platform. ⎪ Detection of abnormalities, possible interruptions or system failures. ⎪ Immediate detection of problems. Generation of proactive solutions to the problems that rise. ⎪ Generation of reports, notifications and alarms via email and SMS containing the errors present in the systems. To achieve these objectives, BMC ProactiveNet is implemented as a tool that combines event management and data analysis (baseline, anomaly detection and analytical algorithms) in a single integrated solution. Event management provides proactive detection and resolution of IT problems in real time. In addition, the data analytics provide a research facility, to better detect abnormalities, predict interruptions and provide detailed diagnostics from the information collected in each system. This has the ultimate goal of preventing an impact on critical systems and ensures the continuity and proper functioning of each of the services provided by TELEFÓNICA – MOVISTAR.

KEYWORDS:

PATROL Agent, Hardware Sentry, KM, TRAFFICA, OSS, server.

V° B° DIRECTOR OF GRADUATE WORK

1. INTRODUCCIÓN

La práctica empresarial elaborada en ***TELEFÓNICA MOVISTAR,*** le permite al estudiante afianzar los conocimientos en redes y en telecomunicaciones, teniendo como base de desarrollo una serie de actividades de monitoreo y soporte de los servicios que ofrece la compañía, junto con la realización de un proyecto principal, vinculado a la labor diaria del estudiante y a las necesidades presentes en el día a día para la ***Jefatura Plataformas VAS***.

Dentro de las actividades diarias del estudiante se encuentran:

- ✓ Soporte on-call de la *Jefatura Desarrollo OSS*: Consiste en la atención telefónica de las alarmas y los inconvenientes que se presenten con los sistemas, plataformas, aplicativos y reportes a cargo de la *Jefatura de Desarrollo OSS*.

- ✓ Verificación de estadísticas de la red: Monitoreo, revisión y gestión del tráfico de datos presente en los elementos de red GSM, UMTS y LTE pertenecientes a la compañía.

- ✓ Verificación del proceso GIE – Información en bases de datos: Revisión, monitoreo, gestión y manejo de la carga de datos de tráfico de los elementos de red GSM, UMTS y LTE en las diferentes bases de datos de la compañía.

- ✓ Reportes GSM – UMTS – LTE: Generación y validación de reportes GSM, UMTS y LTE utilizados por la compañía para el monitoreo del comportamiento de la red.

- ✓ Revisión de servidores: Revisión física de los servidores que componen los sistemas de la *Jefatura Plataformas VAS*. Esta actividad también incluye la revisión de filesystems, espacio disponible en disco, uso de CPU, uso de memoria en cada servidor, etc.

- ✓ Manejo de backups: Manejo y supervisión de la correcta generación de backups realizados en las plataformas de la Jefatura (OSS Ericsson 3G – OSS Ericsson 4G – OSS Huawei – OSS Nokia).

- ✓ Monitoreo de alarmas: Revisión continúa de las alarmas presentes en las plataformas de la Jefatura. Estas alarmas son procesadas por diferentes aplicativos, para ser observadas por el administrador de la red

por medio de correo electrónico, mensajes de texto, interfaces gráficas, y sistemas de gestión (*Xymon - BEM)*.

- ✓ Prueba de servicios: Realización de pruebas de los servicios que ofrece la compañía, con el fin de garantizar su correcto funcionamiento. Algunos de estos servicios son:

    - Voice mail.
    - Llamada.
    - Mensaje de texto.
    - Spinvox.
    - Internet prepago.
    - Revisión de saldo.
    - Realización de recargas.
    - Número preferidos.
    - Correo corporativo.

Junto con la realización de las actividades diarias, se desarrolla el proyecto ***Monitoreo de Plataformas por medio de BMC ProactiveNet***, el cual, busca la integración de las diferentes plataformas a cargo de la ***Jefatura Plataformas VAS***, en un sistema de monitoreo confiable, exacto, eficiente y claro, el cual, permita realizar la supervisión de diferentes componentes hardware y software de cada plataforma.

Dentro de los parámetros, procesos y dispositivos a supervisar se encuentran:

- ✓ Conectividad de puertos.
- ✓ Tamaño disponible en discos lógicos y físicos.
- ✓ Estado de discos lógicos y físicos.
- ✓ Tamaño disponible en memoria.
- ✓ Consumo de potencia.
- ✓ Estado de las fuentes de energía.
- ✓ Estado de fans (Ventiladores de enfriamiento).
- ✓ Estado de módulos de memoria.
- ✓ Procesadores.
- ✓ Temperatura.

Por medio del monitoreo de estos parámetros es posible detectar anomalías, predecir interrupciones, generar diagnósticos y enviar notificaciones y alarmas, las cuales, garanticen la continuidad y el correcto funcionamiento de cada uno de los servicios prestados por *TELEFÓNICA – MOVISTAR, y* eviten algún posible impacto en los sistemas críticos a cargo de la Jefatura.

1.1 PLANTEAMIENTO DEL PROBLEMA

Debido a las intermitencias que algunas veces presentan los servicios ofrecidos a los usuarios de la compañía, la presencia de fallas en el hardware o el software de los equipos que componen las plataformas, y la necesidad de brindar y garantizar una serie de servicios constantes y confiables a todos los usuarios externos e internos de la compañía, es fundamental realizar un seguimiento a cada uno de los procesos que se presentan en los sistemas a cargo de la ***Jefatura Plataformas VAS***.

1.2 JUSTIFICACIÓN

En un área como la ***Jefatura Plataformas VAS***, en donde a diario se debe hacer seguimiento de múltiples alarmas de distintas índoles, ya sea de sistema operativo, bases de datos, hardware, conectividad, servicios, o procesos propios de las plataformas, se hace necesaria una herramienta de fácil detección y prevención de fallas.

De acuerdo a esto, El proyecto ***Monitoreo de Plataformas por medio de BMC ProactiveNet***, se plantea como una herramienta central, integrada y de fácil manejo, la cual, combina la supervisión de eventos, el análisis de datos y la gestión de alarmas para cada plataforma en donde se encuentre presente, con el fin de evitar un impacto en los sistemas críticos a cargo de la Jefatura y garantizar la continuidad y el correcto funcionamiento de cada uno de los servicios prestados por *TELEFÓNICA – MOVISTAR.*

2. OBJETIVOS

2.1 Objetivos Generales:

Conocer y manejar de manera eficiente y correcta, las herramientas de supervisión y monitoreo de los sistemas y servicios de la Jefatura de plataformas VAS con el fin de interpretar e identificar de manera proactiva las posibles fallas presentes en la red para darles una solución pertinente a estas.

Integrar los diferentes sistemas a cargo de la *Jefatura Plataformas VAS*, en un sistema de monitoreo confiable, exacto, eficiente y claro, el cual, permita realizar la supervisión de los componentes hardware, software, conectividad y servicios de cada plataforma.

2.2 Objetivos Específicos:

- ✓ Conocer las plataformas TRAFFICA – IAS – HUAWEI – NOKIA y ERICSSON a cargo de la *Jefatura Plataformas VAS*.
- ✓ Estudiar y comprender los diferentes sistemas de monitoreo de redes y servicios disponibles en el mercado.
- ✓ Supervisar las plataformas a cargo de la *Jefatura Plataformas VAS* en una interfaz centralizada (BMC Proactive Net).
- ✓ Supervisar y reportar las posibles fallas presentes en las plataformas por medio del sistema de monitorio y otros medios; entre los cuales se presentan el correo electrónico y el mensaje de texto (SMS).
- ✓ Generar y enviar alarmas ante eventos de *Degradación (Warnings*) en las plataformas por medio del sistema de monitoreo, correo electrónico y mensaje de texto (SMS) hacia el personal encargado de la Jefatura.
- ✓ Generar y enviar alarmas ante fallas o daños en las plataformas monitoreadas (*Salud de discos, fans, temperatura máquinas, fuentes de poder, módulos de memoria, etc.*) hacia el personal encargado de la Jefatura.

3. PLAN DE TRABAJO PROPUESTO

Durante el desarrollo de la práctica Empresarial, se plantean diferentes actividades a realizar y se establecen metas a cumplir. Dentro de las actividades, se deben ejecutar los siguientes trabajos de manera diaria:

Número	TAREAS
1.	Soporte On-Call ***Jefatura Desarrollo OSS*.**
2.	Verificación de estadísticas de la red "Control Data".
3.	Revisión CRONTAB: carga diaria de datos GIE (Gerencia de información y Estadística).
4.	Consultas SQL en Bases de Datos: TGESTION 1, TGESTION 2 y BI.
5.	Revisión de reportes UMTS - GSM - LTE.
6.	Revisión de archivos Logs de HLR Huawei.
7.	Revisión de sesiones IAS.
8.	Actualización archivo de Excel: Tablas Trafico
9.	Revisión Alarm-Point.
10.	Revisión de espacios de discos en Máximo.
11.	Revisión backup en OSS Ericsson - cambio de cintas del robot DYSBKP.
12.	Revisión backup en OSS HUAWEI.
13.	Reset de sesiones en Citrix: Regional Cluster.
14.	Revisión alarmas internas por TLUI en Regional Cluster.
15.	Revisión de espacio por GUI en Regional Cluster.
16.	Revisión email corporativo.
17.	Revisión base de datos de Cluster: GESTION.
18.	Revisión de backup BD Máximo.
19.	Revisión de tablespaces de TGESTION.
20.	Revisión de niveles de procesamiento, almacenamiento y mensajes de error: SUNFIRE.
21.	Revisión física de servidores.
22.	Revisión del proceso de calidad.
23.	Actualización archivo de casos OSS Ericsson.
24.	Revisión de backups Global Cluster.
25.	ACTIVIDAD DIA MARTES: Redirección del On-Call.
26.	ACTIVIDAD DIA JUEVES: Carga - descarga de cintas en robot DySBKP (backups).
27.	ACTIVIDAD DIA VIERNES: Revisión de OSS's.
28.	Administración de usuarios en plataformas (OSS HUAWEI – OSS ERICSSON – IAS – OSS NOKIA).

Tabla N° 1: Tareas ejecutadas diariamente.

Además de estas labores que son realizadas e informados sus resultados diariamente por medio del correo interno de la compañía, se plantea el proyecto ***Monitoreo de Plataformas por medio de BMC ProactiveNet***, el cual, busca la integración de las diferentes plataformas a cargo de la ***Jefatura Plataformas VAS***, en un sistema de monitoreo confiable, exacto, eficiente y claro, el cual, permita realizar la supervisión de diferentes componentes hardware y software de cada plataforma.

Las metas que se establecen en este proyecto, son:

- ✓ Supervisión de las plataformas a cargo de la *Jefatura Plataformas VAS* en una interfaz centralizada (BMC Proactive Net).

- ✓ Supervisar y reportar las posibles fallas presentes en las plataformas por medio del sistema de monitorio y otros medios; entre los cuales se presentan el correo electrónico y el mensaje de texto (SMS).

- ✓ Generar y enviar alarmas ante eventos de *Degradación (Warnings*) en las plataformas por medio del sistema de monitoreo, correo electrónico y mensaje de texto (SMS) hacia el personal encargado de la Jefatura.

- ✓ Generar y enviar alarmas ante fallas o daños en las plataformas monitoreadas (*Salud de discos, fans, temperatura máquinas, fuentes de poder, módulos de memoria, etc.*) hacia el personal encargado de la Jefatura.

4. MARCO TEÓRICO

Agente PATROL:

Es una aplicación de máquina virtual, la cual, se instala en cada computadora. La función principal de esta aplicación es el monitoreo y la administración de recursos de operación, tales como CPU, memoria, aplicaciones, y bases de datos, usando KMs.

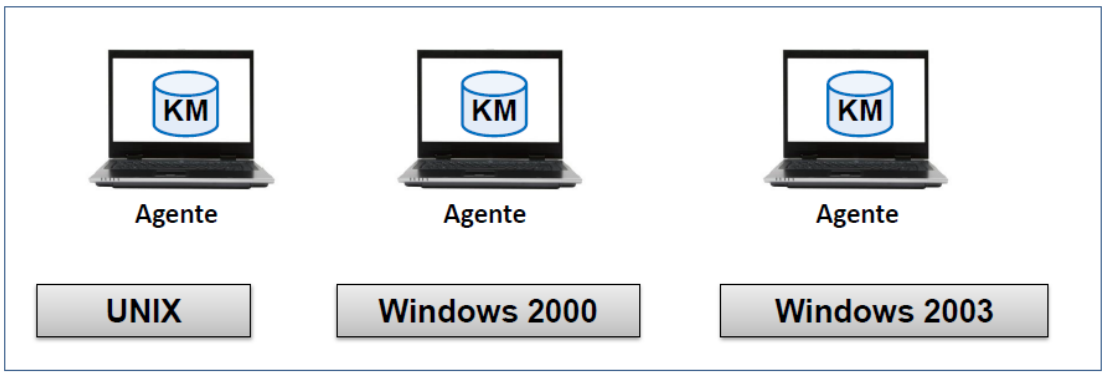

Figura N° 1: Agente Patrol. *Tomado de documento "02 – PATROL Agent.pdf"*.

Los módulos de conocimiento (KM's), son la base de conocimiento entera de un agente y su funcionalidad, y proporcionan las instrucciones de cómo debería el agente monitorear las consolas en las que se encuentra instalado.

Un agente PATROL, presenta las siguientes características:

- ✓ Self-tuning: El agente organiza cada proceso a ejecutar de acuerdo a la carga (uso de CPU) del servidor.
- ✓ Self-configuring: El agente remueve o agrega objetos de manera dinámica, dependiendo del proceso de descubrimiento.
- ✓ Resource efficient: el consumo de CPU que realiza el agente depende del número de objetos cargados. En su funcionamiento constante, el agente consume cantidades mínimas de recursos.

Las tareas que ejecuta un agente PATROL son:

- ✓ Recolección de información de servidores o aplicativos a partir de la ejecución de comandos.
- ✓ Almacenamiento de información de manera local.
- ✓ Carga de módulos de conocimiento (KM's) específicos.

BMC ProactiveNet:

BMC ProactiveNet, es una plataforma integrada que combina la gestión de eventos y el análisis de datos (incluyendo baselines, detección de anomalías y algoritmos de análisis de fallas) en una única solución integral.

La gestión de eventos proporciona una solución en tiempo real ante la detección de problemas y fallas, ocasionando una resolución proactiva de problemas de TI antes de que tengan un impacto en los sistemas críticos de telecomunicaciones.

La utilización de mediciones y métricas en el análisis de datos recopilados de la infraestructura del sistema, le permite a la plataforma BMC ProactiveNet detectar anomalías, predecir interrupciones y proporcionar diagnósticos detallados de información.

Los principales componentes que conforman la plataforma BMC ProactiveNet son:

- ✓ BMC ProactiveNet Server:
  El servidor BMC ProactiveNet, es el componente principal de la plataforma, el cual, recibe eventos y datos de diversas fuentes, tales como agentes BMC ProactiveNet, adaptadores de impacto o servicios integrales BMC ProactiveNet.
  El servidor se encarga de procesar los eventos, recolectar, almacenar y procesar información, y es responsable de la configuración y el control de los agentes BMC ProactiveNet.

- ✓ BMC ProactiveNet database:
  Es una base de datos Sybase ASA, la cual, se instala automáticamente junto con la instalación del BMC ProactiveNet Server.
  Esta base de datos actúa como un repositorio de información para toda la información estadística y de configuración; también, almacena información de reportes, datos de usuarios, configuración y desempeño de agentes, entre otros.

- ✓ BMC ProactiveNet agent:
  Dos agentes BMC ProactiveNet se incluyen dentro de la plataforma BMC ProactiveNet.
  El agente local, es un agente BMC ProactiveNet que se encuentra instalado en el servidor BMC ProactiveNet. Este agente monitorea la salud y el estado del servidor y asegura su correcto funcionamiento y desempeño.

El agente remoto BMC ProactiveNet, es aquel que se encuentra instalado en otra consola diferente al servidor BMC ProactiveNet. Este agente se debe instalar en cada servidor o máquina del sistema que se desea monitorear.

- ✓ BMC ProactiveNet administration console:
  La consola de administración de BMC ProactiveNet le permite al usuario modificar y hacer uso del servidor BMC ProactiveNet y de los agentes BMC ProactiveNet instalados en los servidores del sistema que se desea monitorear.

- ✓ BMC ProactiveNet operator console:
  Es un aplicativo web, el cual, le permite al usuario navegar a través de BMC ProactiveNet y observar toda la información colectada y procesada por el servidor BMC ProactiveNet.

Otros componentes que hacen parte de la plataforma BMC ProactiveNet son:

- ✓ BMC ProactiveNet SLO console.
- ✓ BMC ProactiveNet Integration Service.
- ✓ BMC Impact Model Designer.
- ✓ BMC ProactiveNet Impact Event Adapters.
- ✓ BMC ProactiveNet CMDB extensions.
- ✓ BMC ProactiveNet performance management web services.

Hardware Sentry:

Hardware Sentry, es un modulo de conocimiento (KM) especifico para un agente PATROL. Por medio de este modulo de conocimiento, es posible monitorear la salud y el estado de los componentes electrónicos que hacen parte de un servidor.

A partir del momento en el que este módulo ha sido instalado junto con el agente PATROL en todos los servidores a monitorear, es posible visualizar el estado de los componentes hardware de los servidores desde cualquier consola PATROL. El administrador u operador de la consola PATROL, será informado por medio de alarmas cuando el módulo de conocimiento detecte alguna falla o degradación del sistema monitoreado.

A continuación, se expresan los 3 parámetros principales que monitorea el módulo de conocimiento Hardware Sentry:

- ✓ Hardware Capacity Report.

- ✓ Computer.
- ✓ Detected Connectors.

Hardware Capacity Report:

Los atributos que se monitorean dentro de este reporte son:

- *ConnectedPorts*
- *CPUCount*
- *DegreesBelowWarning*
- *LogicalDiskSize*
- *MemorySize*
- *PhysicalDiskSize*
- *PowerConsumption*

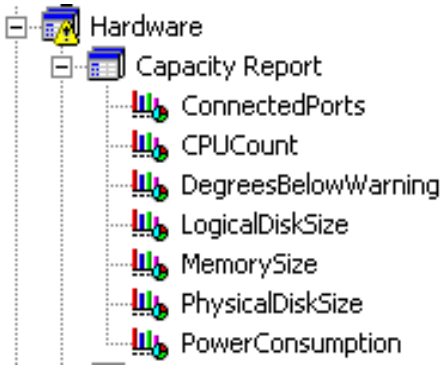

Figura N° 2: atributos monitoreados dentro de *"Hardware Capacity Report"*.

Attribute	Description	Unit	Default Alert Thresholds	Type
CPU Count	Host total number of physical processors (CPU).	CPUs	None	Statistics
Connected Ports	Number of connected ports.	ports	None	Statistics
Degrees Below Warning*	Number of degrees before reaching the closest warning threshold.	degrees Celsius	None	Statistics
Logical Disk Size	Host total logical disk size.	Gigabytes (GB)	None	Statistics
Memory Size	Host total memory (RAM).	Gigabytes (GB)	None	Statistics
Physical Disk Size	Host total physical disk size.	Gigabytes (GB)	None	Statistics
Power Consumption*	Power consumed by the host.	Watts	None	Statistics
Unallocated Disk Space	Host Total available disk space that is not allocated to any volume.	Gigabyte (GB)	None	Statistics

Figura N° 3: Tabla de atributos monitoreados dentro del *"Hardware Capacity Report"*. Documento anexo: mshw_BPPM_1900_Documentation.pdf.

- *CPU Count:*

  Por medio de Hardware Sentry, es posible realizar un chequeo del número total de procesadores físicos presentes en el servidor (sistema monitoreado). Este parámetro tipo estadístico, no tiene vinculado una alarma.

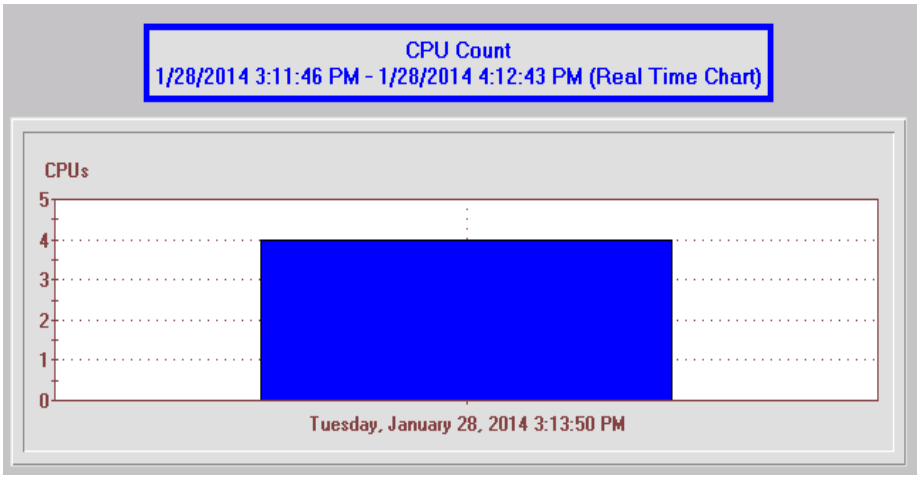

Figura N° 4: Número de procesadores presentes en el servidor.

- *Connected Ports:*

  Parámetro tipo estadístico de medición del número de puertos conectados al servidor (sistema monitoreado). Este parámetro no tiene un límite de conectividad para el disparo de una alarma.

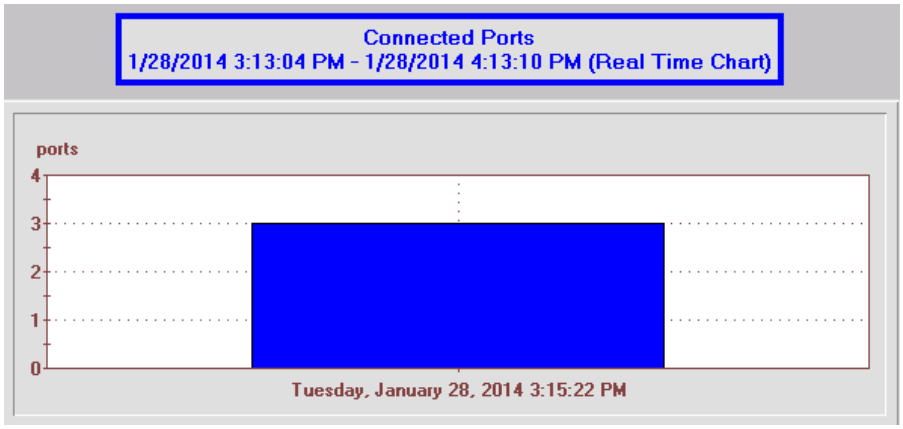

Figura N° 5: Número puertos conectados en el servidor.

- *Degrees Below Warning:*

  Parámetro tipo estadístico de medición de la temperatura del servidor (sistema monitoreado). Este parámetro indica el número de grados

Celsius antes de alcanzar la temperatura umbral del sistema monitoreado.

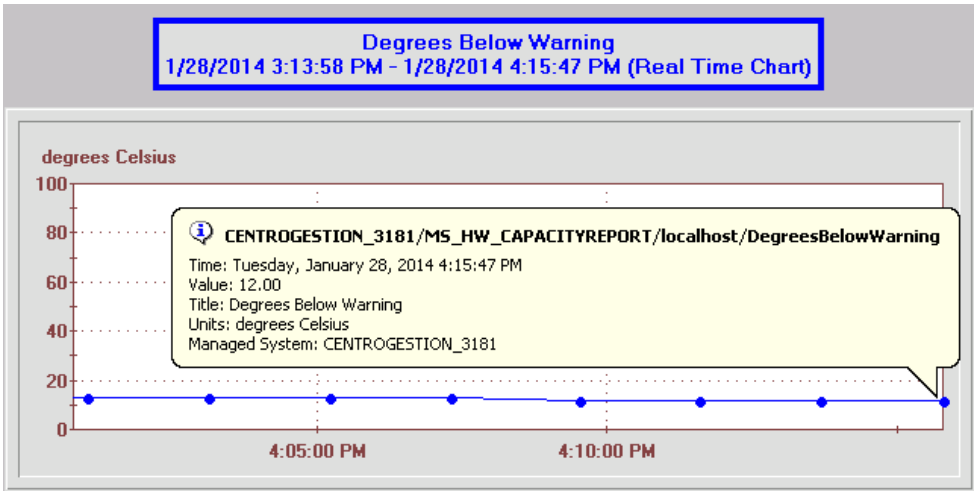

Figura N° 6: Temperatura del servidor.

- *Logical Disk Size:*

Parámetro estadístico de medición del espacio disponible en un disco lógico (varios discos físicos vistos por el sistema operativo como un único disco). Esta medición no tiene un límite definido para el disparo de una alarma.

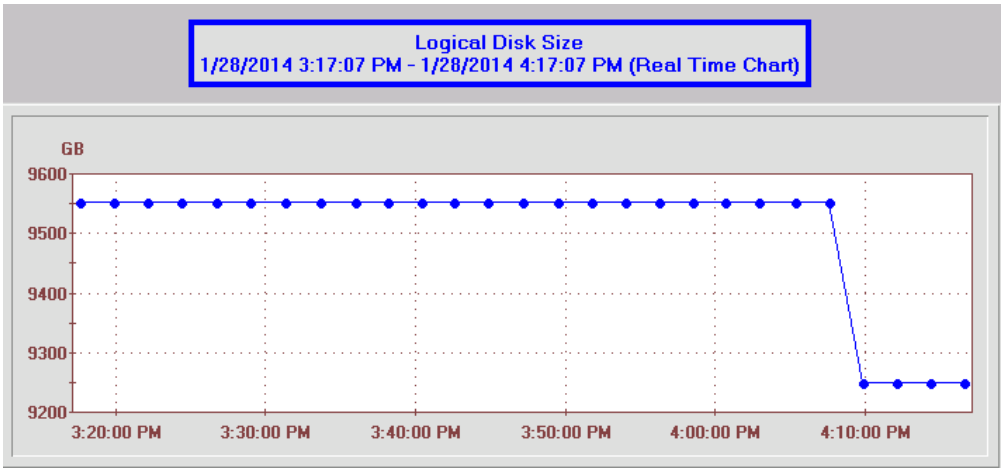

Figura N° 7: Espacio disponible en un disco lógico.

- *Memory Size:*

Parámetro estadístico de medición de la memoria RAM presente en el servidor. Esta medición no tiene un límite definido para el disparo de una alarma.

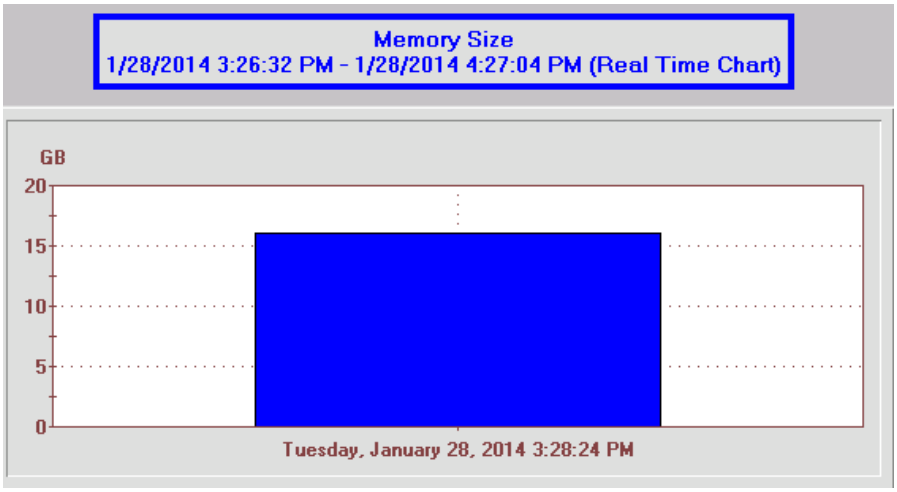

Figura N° 8: Memoria RAM del servidor.

- *Physical Disk Size:*

  Parámetro estadístico de medición del tamaño total del disco duro del servidor. Esta medición no tiene un límite definido para el disparo de una alarma.

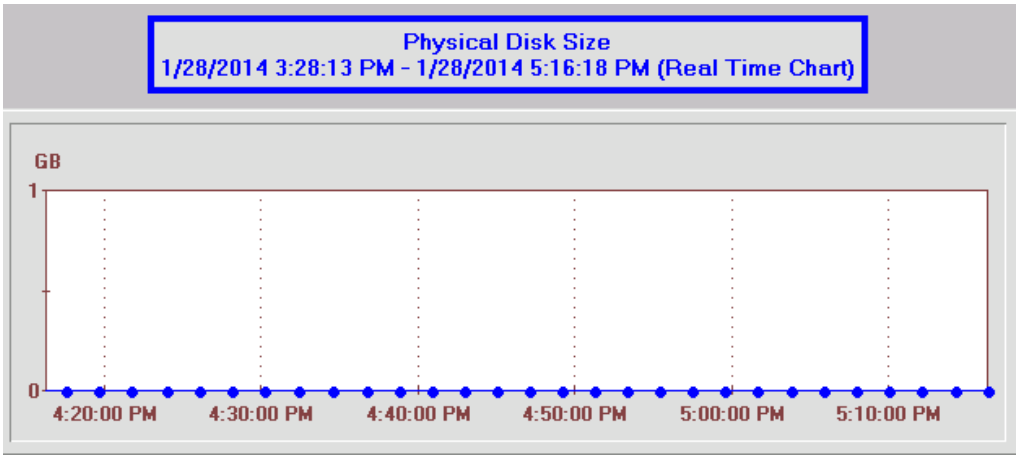

Figura N° 9: Monitoreo del tamaño total del disco duro.

- *Power Consumption:*

  Parámetro estadístico de medición de la potencia consumida por el servidor. Esta medición no tiene un límite definido para el disparo de una alarma.

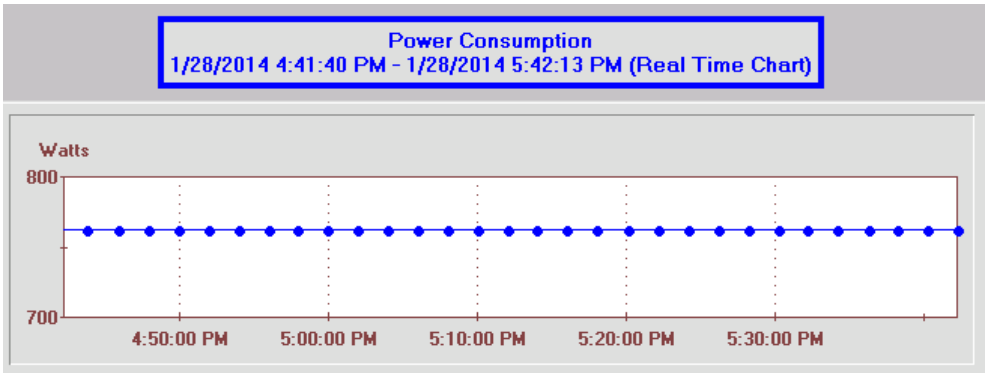

Figura N° 10 - a: Monitoreo del consumo de potencia del servidor.

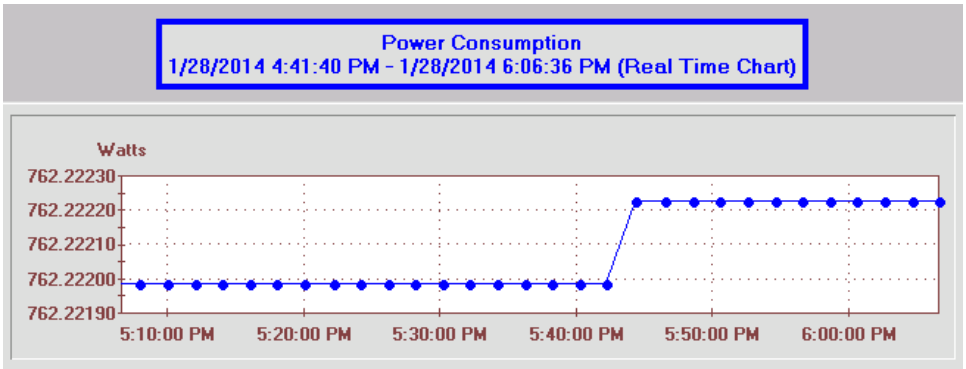

Figura N° 10 - b: Monitoreo del consumo de potencia del servidor.

Computer Report:

Los atributos que se monitorean dentro de este reporte son:

- *Fans*
- *Physical Disks*
- *Logical Disks*
- *Memory Modules*
- *Network Interfaces*
- *Other Devices*
- *Power Supplies*
- *Processors*
- *Temperatures*

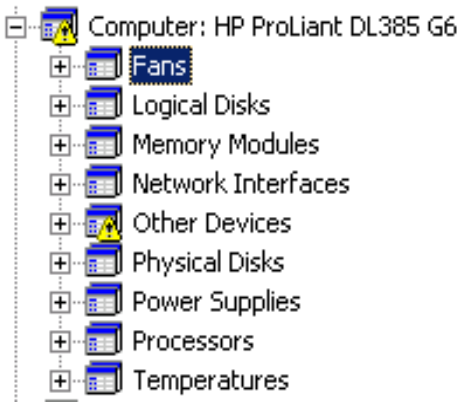

Figura N° 11: atributos monitoreados dentro de *"Computer Report"*.

- *Fans:*

  Para evitar el sobrecalentamiento, se instalan ventiladores en dispositivos críticos (procesadores, fuentes de alimentación, etc.) Si un sistema de enfriamiento no está presente, el aumento de temperatura puede afectar la velocidad de los procesadores y en casos extremos, generar el apagado del servidor. El monitoreo de los Fans, permite garantizar una temperatura adecuada para el funcionamiento óptimo de los sistemas.

Attribute	Description	Unit	Default Alert Thresholds	Type
Present	When the fan is no longer discovered, the attribute goes into alarm.	{0 = Missing; 1 = Present}	0 = Alarm	Availability
Speed*	Fan Speed.	Revolutions per minutes (RPM)	Automatic	Statistics
Speed Percent	Fan Speed as a percentage of its maximal speed.	% of maximum speed	Automatic	Statistics
Status*	Fan Status.	{0 = OK; 1 = Degraded; 2 = Failed}	1 = Warning 2 = Alarm	Availability

Figura N° 12: Tabla de atributos monitoreados para cada Fan presente en un servidor. Documento anexo: mshw_BPPM_1900_Documentation.pdf.

Los parámetros monitoreados para los ventiladores (fans) son:

Present: representa la disponibilidad del ventilador. Se dispara una alarma de disponibilidad cuando el ventilador ya no es encontrado por el módulo de conocimiento Hardware Sentry.

0: Ausencia del ventilador (disparo de alarma).

1: Presencia del ventilador.

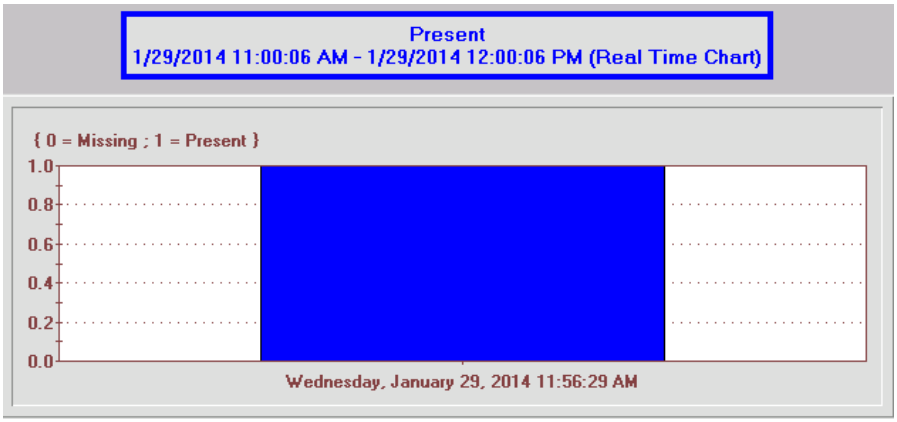

Figura N° 13: Estado de presencia de 1 ventilador.

Status: atributo indicador del estatus actual del ventilador. Este atributo presenta diferentes valores:

0: Funcionamiento correcto del ventilador.

1: Funcionamiento del ventilador degradado (se genera una alarma de advertencia).

2: Falla completa del ventilador (se genera una alarma de falla).

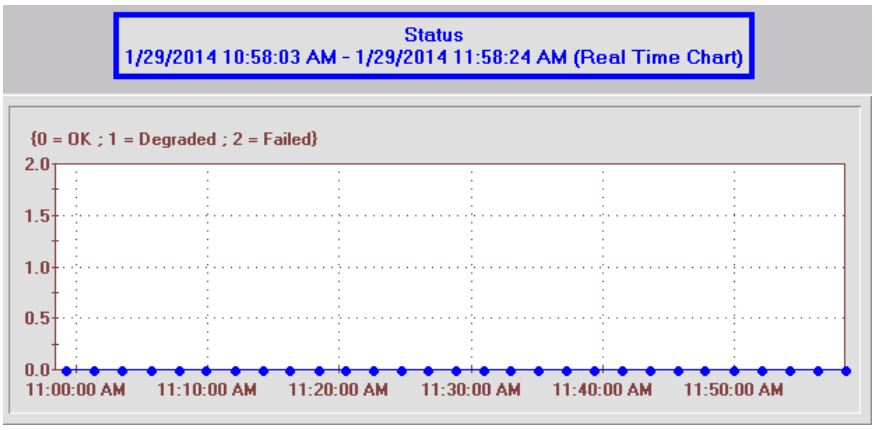

Figura N° 14: Estado de 1 ventilador.

Speed: parámetro tipo estadístico, indicador de la velocidad del ventilador. Unidad de medida: revoluciones por minuto (RPM).

Speed Percent: porcentaje de velocidad nominal del ventilador comparada con la velocidad máxima posible de este.

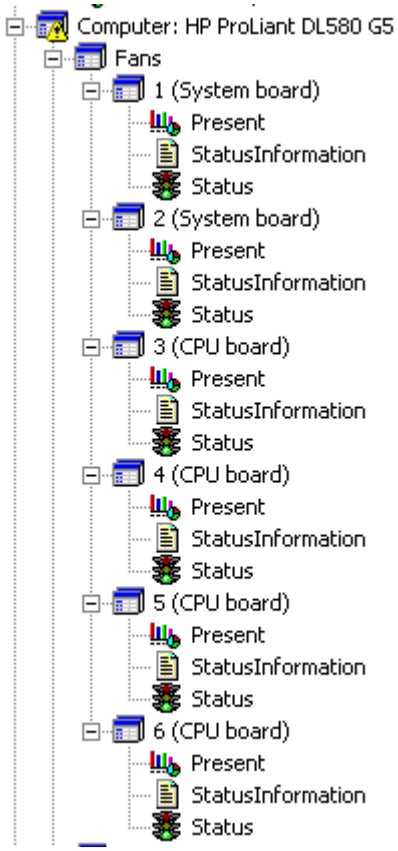

Figura N° 15: Fans del servidor reconocidas por Hardware Sentry. Atributos monitoreados para cada Fan.

- *Physical Disks:*

  Por medio de Hardware Sentry, es posible realizar un chequeo de la salud de los discos. Estos, al almacenar información y ser dispositivos con un corto tiempo de vida útil, se convierten en una prioridad critica de monitoreo.

  Los parámetros presentes en el monitoreo de discos físicos de un servidor son:

  Status: atributo indicador del estado actual de los discos. Este atributo presenta diferentes valores de evaluación:

  0: Funcionamiento correcto del disco.

  1: Funcionamiento degradado del disco (se genera una alarma de advertencia).

  2: Falla completa del disco (se genera una alarma de falla).

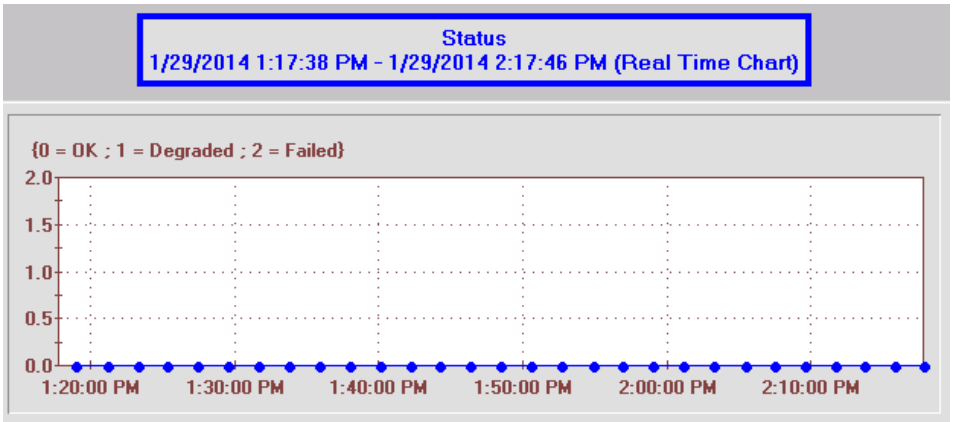

Figura N° 16: Estado de un disco físico.

Present: este parámetro representa la disponibilidad del disco. Se dispara una alarma de disponibilidad cuando el dispositivo ya no es encontrado por el módulo de conocimiento Hardware Sentry.

0: Ausencia del disco (disparo de alarma).

1: Presencia del disco.

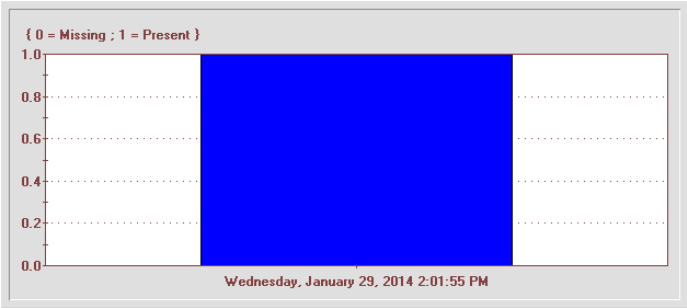

Figura N° 17: Estado de presencia de disco físico.

PredictedFailure: atributo indicador de un posible daño o degradación que se presente en un disco físico en un tiempo futuro. Este atributo presenta diferentes valores de evaluación:

0: Funcionamiento correcto del disco.

1: Degradación o daño predicho en el disco (se genera una alarma de advertencia).

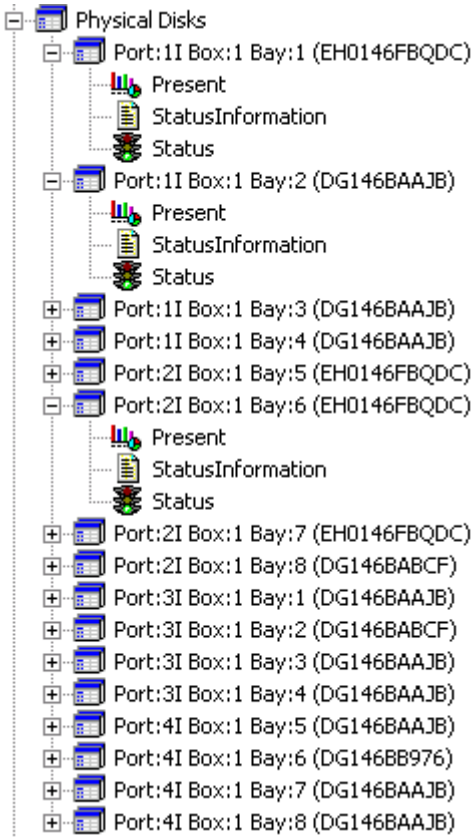

Figura N° 18: Discos físicos del servidor reconocidas por Hardware Sentry. Atributos monitoreados para cada disco.

- *Logical Disks:*

  Los **RAID** o los controladores de disco, muestran varios discos físicos como un único disco lógico para el sistema operativo. El estado de un disco lógico corresponde al estado de una matriz **RAID**.

  Por cada disco lógico encontrado, los parámetros monitoreados son:

  ErrorCount: Número de errores que se presentan en el disco.

  Present: este parámetro representa la disponibilidad del disco lógico. Se dispara una alarma de disponibilidad cuando el RAID ya no es encontrado por el módulo de conocimiento Hardware Sentry.

  0: Ausencia del disco (disparo de alarma).

  1: Presencia del disco.

  UnallocatedSpace: parámetro tipo estadísticos indicador de la cantidad de espacio libre en el disco lógico. Unidad de medida: Gigabytes (GB).

Status: atributo indicador del estado actual del disco lógico. Este atributo presenta diferentes valores de evaluación:

0: Funcionamiento correcto del disco lógico.

1: Funcionamiento degradado del disco lógico (se genera una alarma de advertencia).

2: Falla completa del disco lógico (se genera una alarma de falla).

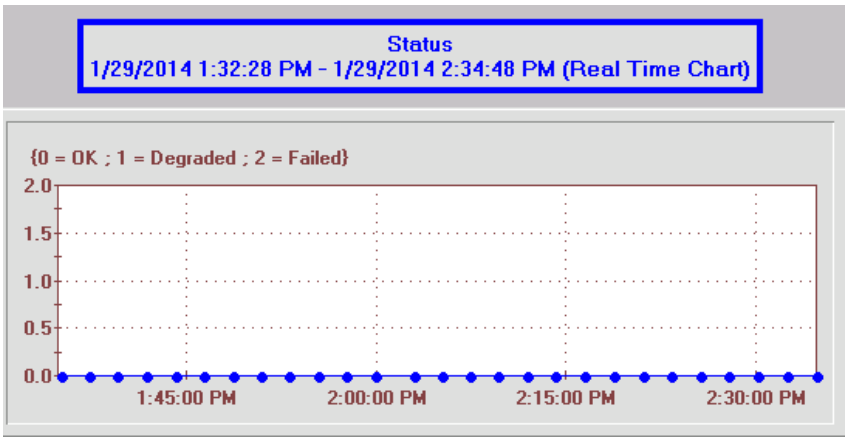

Figura N° 19: Estado de un disco lógico.

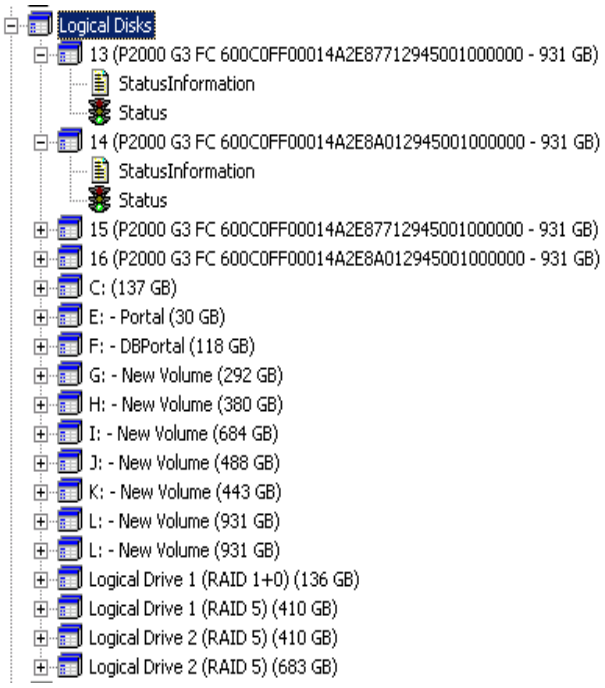

Figura N° 20: Discos lógicos del servidor reconocidas por Hardware Sentry.
Atributos monitoreados para cada disco.

- *Memory Modules:*

La memoria principal de un computador es igual de crítica que los procesadores, ya que la mayoría de las operaciones de estos, hacen uso de la memoria. Una simple falla de memoria, puede llevar a un

incidente severo en un computador, y potencialmente ocasionar la corrupción de la información presente en el servidor.

Los parámetros de monitoreo de los módulos de memoria son:

Present: este parámetro representa la disponibilidad del módulo de memoria. Se dispara una alarma de disponibilidad cuando el módulo ya no es encontrado por Hardware Sentry.

0: Ausencia del módulo de memoria (disparo de alarma).

1: Presencia del módulo de memoria.

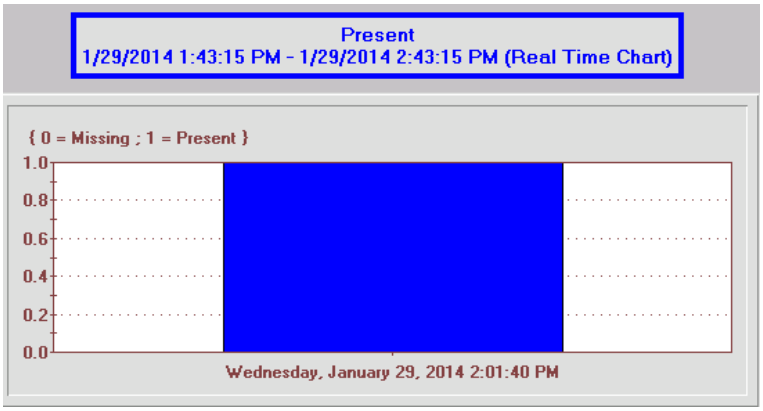

Figura N° 21: Estado de presencia de un módulo de memoria.

Status: atributo indicador del estado actual del módulo de memoria. Este atributo presenta diferentes valores de evaluación:

0: Funcionamiento correcto del módulo de memoria.

1: Funcionamiento degradado del módulo de memoria (se genera una alarma de advertencia).

2: Falla completa del módulo de memoria (se genera una alarma de falla).

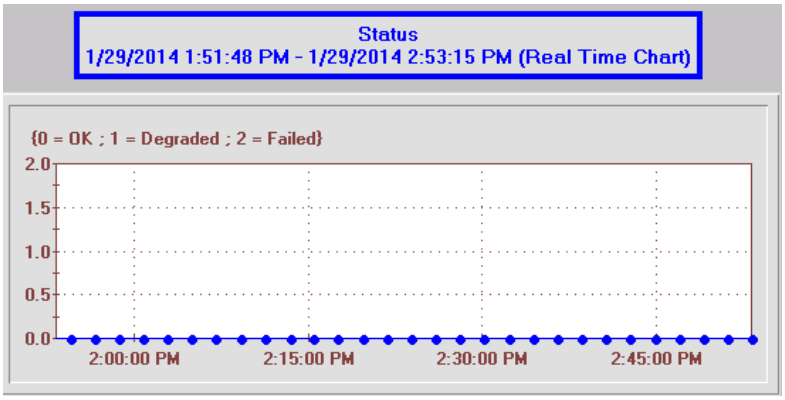

Figura N° 22: Estado de un módulo de memoria.

ErrorStatus: descripción exacta del número de errores detectados y corregidos por el módulo de memoria.

ErrorCount: medición estadística del número de errores detectados y corregidos por el módulo de memoria. Unidad de medida: errores.

PredictedFailure: atributo indicador de un posible daño o degradación que se presente en un módulo de memoria para un tiempo futuro. Este atributo presenta diferentes valores de evaluación:

0: Funcionamiento correcto del módulo de memoria.

1: Degradación o daño predicho en el módulo de memoria (se genera una alarma de advertencia).

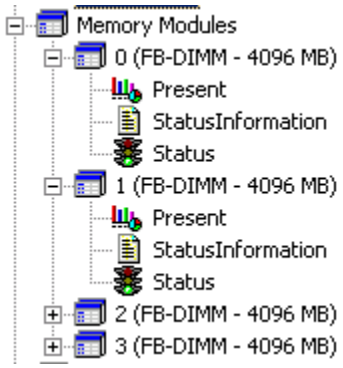

Figura N° 23: Módulos de memoria del servidor reconocidas por Hardware Sentry. Atributos monitoreados para cada fuente.

Attribute	Description	Unit	Default Alert Thresholds	Type
Error Count	Number of detected (and possibly, corrected) errors.	Errors	1 = Warning	Statistics
Error Status	This attribute will trigger an alert if the number of memory errors reaches a threshold set by the manufacturer's agent.	{0 = No Errors; 1 = Detected Errors; 2 = Too Many Errors}	1 = Warning 2 = Alarm	Availability
Predicted Failure	This attribute will trigger a warning if a memory failure is predicted to happen.	{0 = OK; 1 = Failure Predicted}	1 = Alarm	Availability
Present	When the memory module is no longer discovered, the attribute goes into alarm.	{0 = Missing; 1 = Present}	0 = Alarm	Availability
Status*	Memory Status.	{0 = OK; 1 = Degraded; 2 = Failed}	1 = Warning 2 = Alarm	Availability

Figura N° 24: Tabla de atributos monitoreados para cada módulo de memoria presente en un servidor. Documento anexo: mshw_BPPM_1900_Documentation.pdf.

- *Power Supplies:*

  El monitoreo de las fuentes de alimentación, le permite a los operadores recibir una alerta cuando se presenta una falla en la fuente de poder de algún servidor, o incluso en los casos en donde se presente una sobrecarga de energía en el sistema.

  Los parámetros de monitoreo de los módulos de memoria son:

  Status: atributo indicador del estado actual de las fuentes de poder. Este atributo presenta diferentes valores de evaluación:

  0: Funcionamiento correcto de las fuentes de poder.

  1: Funcionamiento degradado de las fuentes de poder (se genera una alarma de advertencia).

  2: Falla completa de las fuentes de energía (se genera una alarma de falla).

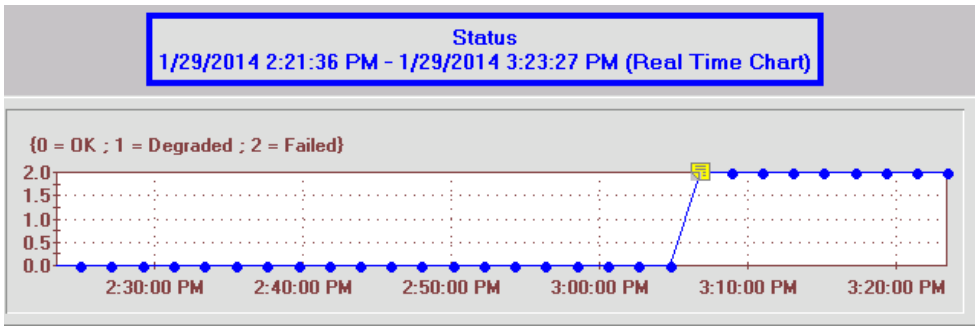

Figura N° 25: Estado de una fuente de energía.

Present: este parámetro representa la disponibilidad de las fuentes de energía. Se dispara una alarma de disponibilidad cuando alguna de las fuentes ya no es encontrada por Hardware Sentry.

0: Ausencia de la fuente de energía (disparo de alarma).

1: Presencia de la fuente de energía.

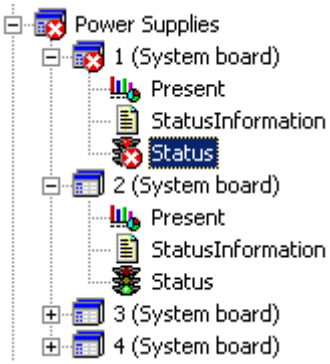

Figura N° 26: Fuentes de energía del servidor reconocidas por Hardware Sentry. Atributos monitoreados para cada fuente.

- *Processors:*

Dependiendo de la información que disponen los servidores, los siguientes parámetros son monitoreados para cada procesador (CPU) encontrado:

Present: este parámetro representa la disponibilidad de los procesadores. Se dispara una alarma de disponibilidad cuando el procesador ya no es encontrado por Hardware Sentry.

0: Ausencia del procesador (disparo de alarma).

1: Presencia del procesador.

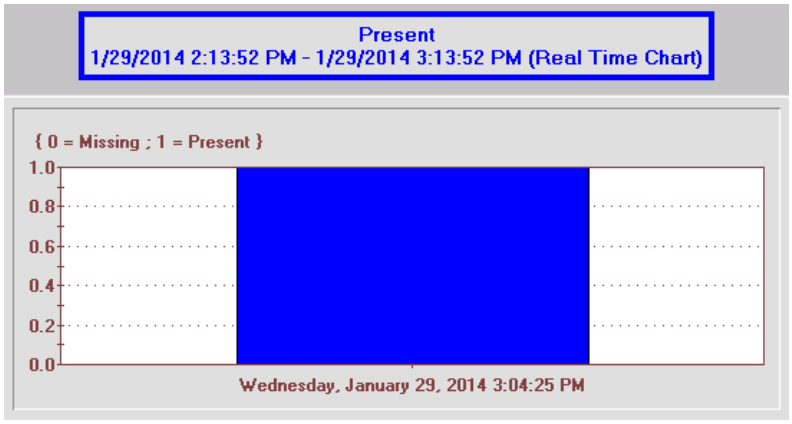

Figura N° 27: Estado de presencia de un procesador.

Status: atributo indicador del estado actual del procesador. Este atributo presenta diferentes valores de evaluación:

0: Funcionamiento correcto del procesador.

1: Funcionamiento degradado del procesador (se genera una alarma de advertencia).

2: Falla completa del procesador (se genera una alarma de falla).

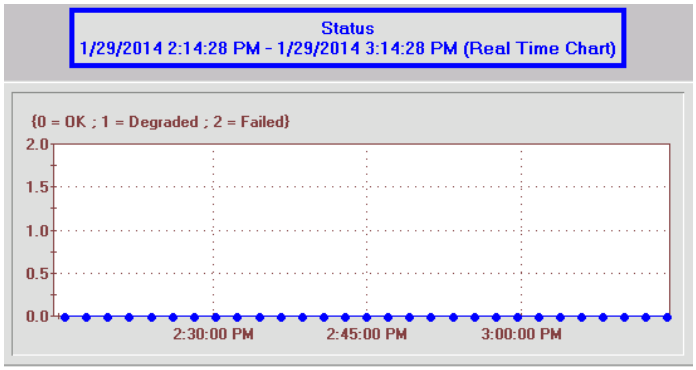

Figura N° 28: Estado de un procesador.

StatusInformation: atributo indicador de información adicional sobre el estado actual de los procesadores.

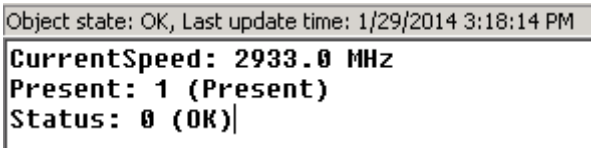

Figura N° 29: Información adicional.

PredictedFailure: atributo indicador de un posible daño o degradación que se presente en un procesador para un tiempo futuro. Este atributo presenta diferentes valores de evaluación:

0: Funcionamiento correcto del procesador.

1: Degradación o daño predicho en el procesador (se genera una alarma de advertencia).

CurrentSpeed: Reporte de la velocidad actual del procesador. La velocidad del procesador puede variar ddependiendo de la carga de trabajo del servidor. Unidad de medida: MegaHertz (MHz).

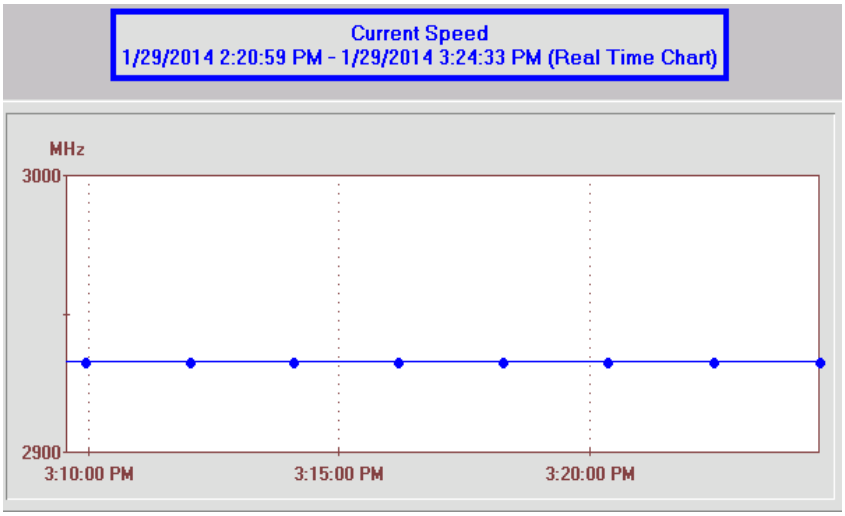

Figura N° 30: Velocidad actual del servidor.

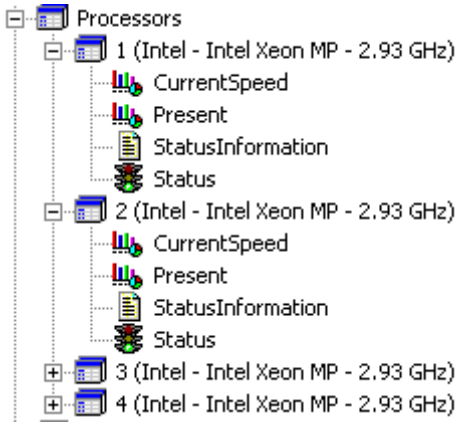

Figura N° 31: procesadores del servidor reconocidas por Hardware Sentry. Atributos monitoreados para cada procesador.

Attribute	Description	Unit	Default Alert Thresholds	Type
Corrected Error Count	Number of detected and corrected errors.	Errors	None	Statistics
Current Speed	CPU speed.	MHz	None	Statistics
Predicted Failure	This attribute will trigger a warning if a CPU failure is predicted to happen.	{0 = OK; 1 = Failure Predicted}	1 = Warning	Availability
Present	When the physical processor is no longer discovered, the attribute goes into alarm	{0 = Missing; 1 = Present}	0 = Alarm	Availability
Status*	CPU Status.	{0 = OK; 1 = Degraded; 2 = Failed}	1 = Warning 2 = Alarm	Availability

Figura N° 32: Tabla de atributos monitoreados para cada procesador presente en un servidor. Documento anexo: mshw_BPPM_1900_Documentation.pdf.

- *Temperatures:*

  El monitoreo de las temperaturas en los dispositivos críticos de un sistema, permite tomar medidas preventivas y evitar un daño o interrupción funcional debida al sobrecalentamiento.

  Los parámetros de monitoreo de temperatura son:

  Status: Estatus actual de la temperatura. Una alarma se activa en caso de presentarse un sobrecalentamiento.

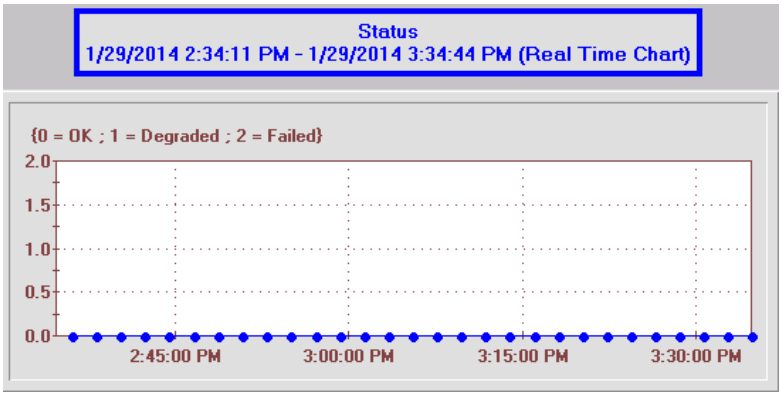

Figura N° 33: Estado de la temperatura presente en un servidor.

StatusInformation: información adicional de la temperatura del sistema.

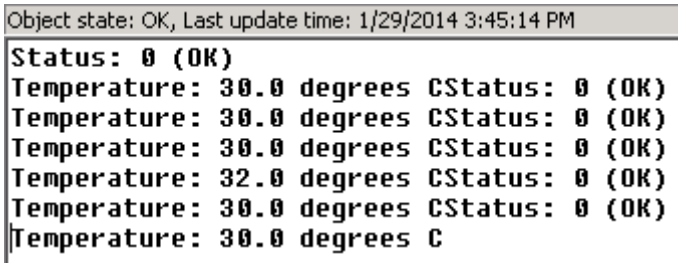

Figura N° 34: Información adicional.

Temperature: medida de la temperatura en grados Celsius (°C) del servidor.

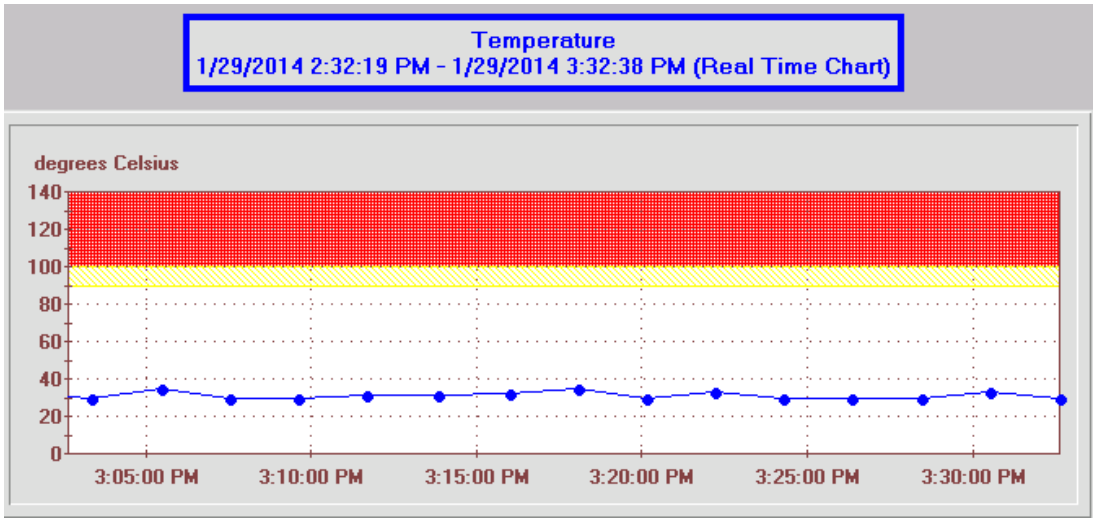

Figura N° 35: Monitoreo de la temperatura actual del servidor.

XYMON – HOBBIT:

Xymon es una herramienta para monitorear servidores, aplicaciones y redes. Este colecta información sobre la salud de los computadores, las aplicaciones que estos ejecutan y las conexiones de red entre ellos.

Toda esta información se presenta en páginas web, las cuales, son refrescadas en intervalos de tiempo, con el fin de reflejar los cambios en los estados de los sistemas monitoreados.

La plataforma XYMON, como sistema de monitoreo de otras plataformas (servidores y redes), provee diferentes capacidades, dentro de las cuales se encuentran:

- ✓ Monitoreo en tiempo real.
- ✓ Interfaz web de fácil acceso.
- ✓ Información histórica.
- ✓ Disponibilidad de reportes.
- ✓ Gráficos de desempeño.

Las características principales de este sistema son:

- ✓ Realización de tareas repetitivas y monótonas, ayudando al administrador del sistema a garantizar respuestas efectivas en tiempos considerables.
- ✓ Presencia de métricas de monitoreo. Por ejemplo: carga de CPU, mensaje del registro de sistema, ocupación de espacios es discos, conectividad, entre otros.
- ✓ Capacidad de llevar a cabo estadísticas y record de incidencias para un posterior estudio.
- ✓ Capacidad de implementación de acciones para disminuir las fallas de la plataforma tecnológica.

Las plataformas monitoreadas por XYMON son:

- ✓ Altamira.
- ✓ SMS.
- ✓ MMS.
- ✓ OTA.
- ✓ RBT.
- ✓ OSS Ericsson.
- ✓ Red Inteligente.
- ✓ 25K.
- ✓ Vm.
- ✓ GWS Acision.
- ✓ SDP Huawei.
- ✓ USSD.
- ✓ TDC.
- ✓ Altamira Fija.
- ✓ Tasación Emulador.
- ✓ Correo Corporativo.

5. DESARROLLO DEL PLAN DE TRABAJO

Durante el desarrollo de la práctica Empresarial, se efectúan diariamente las siguientes actividades:

Número	TAREAS
1.	Soporte On-Call ***Jefatura Desarrollo OSS*.**
2.	Verificación de estadísticas de la red "Control Data".
3.	Revisión CRONTAB: carga diaria de datos GIE (Gerencia de información y Estadística).
4.	Consultas SQL en Bases de Datos: TGESTION 1, TGESTION 2 y BI.
5.	Revisión de reportes UMTS - GSM - LTE.
6.	Revisión de archivos Logs de HLR Huawei.
7.	Revisión de sesiones IAS.
8.	Actualización archivo de Excel: Tablas Trafico
9.	Revisión Alarm-Point.
10.	Revisión de espacios de discos en Máximo.
11.	Revisión backup en OSS Ericsson - cambio de cintas del robot DYSBKP.
12.	Revisión backup en OSS HUAWEI.
13.	Reset de sesiones en Citrix: Regional Cluster.
14.	Revisión alarmas internas por TLUI en Regional Cluster.
15.	Revisión de espacio por GUI en Regional Cluster.
16.	Revisión email corporativo.
17.	Revisión base de datos de Cluster: GESTION.
18.	Revisión de backup BD Máximo.
19.	Revisión de tablespaces de TGESTION.
20.	Revisión de niveles de procesamiento, almacenamiento y mensajes de error: SUNFIRE.
21.	Revisión física de servidores.
22.	Revisión del proceso de calidad.
23.	Actualización archivo de casos OSS Ericsson.
24.	Revisión de backups Global Cluster.
25.	ACTIVIDAD DIA MARTES: Redirección del On-Call.
26.	ACTIVIDAD DIA JUEVES: Carga - descarga de cintas en robot DySBKP (backups).
27.	ACTIVIDAD DIA VIERNES: Revisión de OSS's.
28.	Administración de usuarios en plataformas (OSS HUAWEI – OSS ERICSSON – IAS – OSS NOKIA).

Tabla N° 2: Tareas ejecutadas diariamente.

Cada una de las actividades realizadas, se expresan en más detalle a continuación:

- ✓ Soporte on-call de la *Jefatura Desarrollo OSS*: Consiste en la atención telefónica de las alarmas y los inconvenientes que se presenten con los sistemas, plataformas, aplicativos y reportes a cargo de la *Jefatura de Desarrollo OSS*.

- ✓ Verificación de estadísticas de la red: Monitoreo, revisión y gestión del tráfico de datos presente en los elementos de red GSM, UMTS y LTE pertenecientes a la compañía.

- ✓ Verificación del proceso GIE – Información en bases de datos: Revisión, monitoreo, gestión y manejo de la carga de datos de tráfico de los elementos de red GSM, UMTS y LTE en las diferentes bases de datos de la compañía.

- ✓ Reportes GSM – UMTS – LTE: Generación y validación de reportes GSM, UMTS y LTE utilizados por la compañía para el monitoreo del comportamiento de la red.

- ✓ Revisión de servidores: Revisión física de los servidores que componen los sistemas de la *Jefatura Plataformas VAS*. Esta actividad también incluye la revisión de filesystems, espacio disponible en disco, uso de CPU, uso de memoria en cada servidor, etc.

- ✓ Manejo de backups: Manejo y supervisión de la correcta generación de backups realizados en las plataformas de la Jefatura (OSS Ericsson 3G – OSS Ericsson 4G – OSS Huawei – OSS Nokia).

- ✓ Monitoreo de alarmas: Revisión continúa de las alarmas presentes en las plataformas de la Jefatura. Estas alarmas son procesadas por diferentes aplicativos, para ser observadas por el administrador de la red por medio de correo electrónico, mensajes de texto, interfaces gráficas, y sistemas de gestión (*Xymon – BEM)*.

- ✓ Prueba de servicios: Realización de pruebas de los servicios que ofrece la compañía, con el fin de garantizar su correcto funcionamiento. Algunos de estos servicios son:
    - Voice mail.
    - Llamada.
    - Mensaje de texto.
    - Spinvox.
    - Internet prepago.

- Revisión de saldo.
- Realización de recargas.
- Número preferidos.
- Correo corporativo.

Además de estas labores que son realizadas e informados sus resultados diariamente por medio del correo interno de la compañía, se desarrolla el proyecto ***Monitoreo de Plataformas por medio de BMC ProactiveNet***, el cual, ha sido explicado y descrito en el marco teórico de este documento.

Finalmente, algunos de los recursos e instrumentos utilizados durante el desarrollo de las actividades diarias y el proyecto son:

- ✓ *Computador Pentium Dual-Core.*
- ✓ *Celular Nokia 3500.*
- ✓ *Teléfono fijo CISCO IP Phone 7942.*
- ✓ *2 Bases de datos (PTM – BI).*
- ✓ *1 Servidor de plataforma CENTROGESTION.*
- ✓ *2 servidores de plataforma OSS NOKIA.*
- ✓ *10 servidores de plataforma OSS ERICSSON 3G.*
- ✓ *12 servidores de plataforma OSS ERICSSON 4G.*
- ✓ *50 servidores de plataforma TRAFFICA.*
- ✓ Acceso como administrador a todas las plataformas.
- ✓ Orientación por parte de profesionales y empleados de *TELEFÓNICA-MOVISTAR*.
- ✓ Capacitaciones internas (Personal de *TELEFÓNICA-MOVISTAR*)
- ✓ Capacitaciones externas (Ingenieros – Especialistas externos).

5.1 Cronograma de Actividades:

	TIEMPO DE EJECUCIÓN						
TAREAS	***Julio Año 2013***	***Agosto Año 2013***	***Septiembre Año 2013***	***Octubre Año 2013***	***Noviembre Año 2013***	***Diciembre Año 2013***	***Enero Año 2014***
Soporte On-Call ***Jefatura Desarrollo OSS .***	X	X	X	X	X	X	X
Verificación de estadísticas de la red "Control Data".	X	X	X	X	X	X	X
Revisión CRONTAB: carga diaria de datos GIE (Gerencia de información y Estadística).	X	X	X	X	X	X	X
Consultas SQL en Bases de Datos: TGESTION 1, TGESTION 2 y BI.	X	X	X	X	X	X	X
Revisión de reportes UMTS - GSM - LTE.	X	X	X	X	X	X	X
Revisión de archivos Logs de HLR Huawei.	X	X	X	X	X	X	X
Revisión de sesiones IAS.	X	X	X	X	X	X	X
Actualización archivo de Excel: Tablas Trafico	X	X	X	X	X	X	X
Revisión Alarm-Point.	X	X	X	X	X	X	X
Revisión de espacios de discos en Máximo.	X	X	X	X	X	X	X
Revisión backup en OSS Ericsson - cambio de cintas del robot DYSBKP.	X	X	X	X	X	X	X
Revisión backup en OSS HUAWEI.	X	X	X	X	X	X	X
Reset de sesiones en Citrix: Regional Cluster.	X	X	X	X	X	X	X
Revisión alarmas internas por TLUI en Regional Cluster.	X	X	X	X	X	X	X
Revisión de espacio por GUI en Regional Cluster.	X	X	X	X	X	X	X
Revisión email corporativo.	X	X	X	X	X	X	X
Revisión base de datos de Cluster: GESTION.	X	X	X	X	X	X	X
Revisión de backup BD Máximo.	X	X	X	X	X	X	X
Revisión de tablespaces de TGESTION.	X	X	X	X	X	X	X
Revisión de niveles de procesamiento, almacenamiento y mensajes de error:	X	X	X	X	X	X	X
Revisión física de servidores.	X	X	X	X	X	X	X
Revisión del proceso de calidad.	X	X	X	X	X	X	X
Actualización archivo de casos OSS Ericsson.	X	X	X	X	X	X	X
Revisión de backups Global Cluster.	X	X	X	X	X	X	X
ACTIVIDAD DIA MARTES: Redirección del On-Call.	X	X	X	X	X	X	X
ACTIVIDAD DIA JUEVES: Carga - descarga de cintas en robot DySBKP (backups).	X	X	X	X	X	X	X
ACTIVIDAD DIA VIERNES: Revisión de OSS's.	X	X	X	X	X	X	X
Administración de usuarios en plataformas (OSS HUAWEI – OSS ERICSSON – IAS – OSS	X	X	X	X	X	X	X
Prueba se servicios: Voice mail - SMS - Spinvox - Internet prepago.	X	X	X	X	X	X	X
Proyecto ***Monitoreo de Plataformas por medio de BMC ProactiveNet***					X	X	X

Tabla N° 3: Cronograma de actividades.

6. APORTES AL CONOCIMIENTO

La práctica empresarial elaborada en ***TELEFÓNICA MOVISTAR****,* le permite al estudiante afianzar los conocimientos en redes y en telecomunicaciones, teniendo como base de desarrollo una serie de actividades de monitoreo y soporte de los servicios que ofrece la compañía, junto con la realización de un proyecto principal, vinculado a la labor diaria del estudiante y a las necesidades presentes en el día a día para la ***Jefatura Plataformas VAS***.

Los aportes al conocimiento específicos que se adquieren durante el desarrollo de la práctica empresarial en ***TELEFÓNICA MOVISTAR*** son:

- ✓ Atención a usuarios internos de la compañía ante alarmas e inconvenientes que se presenten con los diferentes sistemas, plataformas, aplicativos o reportes de la compañía.

- ✓ Identificación y reconocimiento de fallas presentes en los servicios que ofrece la compañía mediante la realización de pruebas a estos, con el fin de garantizar su correcto funcionamiento.

- ✓ Conocimientos del tráfico estadístico de la red 2G – 3G y 4G de la compañía.

- ✓ Conocimientos básicos en la consulta de información presente en las bases de datos de la compañía. Adquisición de un nuevo lenguaje de programación (SQL) para la realización de la actividad anteriormente descrita.

- ✓ Adquisición de un nuevo lenguaje de programación para sistemas operativos Linux. Generación de scripts que permiten ejecutar tareas computacionales repetitivas.

- ✓ Análisis y detección de fallas en el flujo de estadísticas obtenidas de las redes GSM – UMTS y LTE.

- ✓ Conocimientos en la revisión, monitoreo, gestión y manejo de la carga de datos de tráfico de los elementos de red GSM, UMTS y LTE en las diferentes bases de datos de la compañía.

- ✓ Generación y validación de reportes GSM, UMTS y LTE utilizados por la compañía para el monitoreo del comportamiento de la red.

- ✓ Manejo y supervisión de la correcta generación de backups realizados en las plataformas de la Jefatura (OSS Ericsson 3G – OSS Ericsson 4G – OSS Huawei – OSS Nokia).

- ✓ Revisión continúa de las alarmas presentes en las plataformas de la compañía.

7. CONCLUSIONES

Los módulos de conocimiento (KM's), son la base de conocimiento entera de un agente y su funcionalidad, y proporcionan las instrucciones de cómo debería el agente monitorear las consolas en las que se encuentra instalado.

La gestión de eventos proporciona una solución en tiempo real ante la detección de problemas y fallas, ocasionando una resolución proactiva de problemas de TI antes de que tengan un impacto en los sistemas críticos de telecomunicaciones.

Hardware Sentry, es un modulo de conocimiento (KM) especifico para un agente PATROL. Por medio de este modulo de conocimiento, es posible monitorear la salud y el estado de los componentes electrónicos que hacen parte de un servidor.

BMC ProactiveNet, es una plataforma integrada que combina la gestión de eventos y el análisis de datos (incluyendo baselines, detección de anomalías y algoritmos de análisis de fallas) en una única solución integral.

El área de *Plataformas VAS y Tasadores* es una gerencia que se deriva de la Dirección de Redes. Esta área es la encargada de gestionar y mantener en óptimo funcionamiento diversas plataformas de servicios de voz móvil de Telefónica Móviles Colombia y a su vez de realizar la tasación de los servicios y el tráfico generado por los abonados de la red en servicios de voz y de valor agregado.

Un sistema de monitoreo confiable y constante, que permita realizar la supervisión de diferentes componentes hardware y software de cada plataforma, le permite al ingeniero Administrador tener un control más eficiente y claro ante los problemas que se presenten en la red; además, le permite ejecutar acciones de solución de una manera proactiva y rápida, para garantizar la continuidad del servicio prestado a los usuarios.

8. ANEXOS

Los anexos de este documento se encuentran de manera digital en el CD adjunto a este trabajo denominado "*Anexos Práctica Empresarial".*

REFERENCIAS BIBLIOGRÁFICAS.

http://www.bmc.com/products/product-listing/ProactiveNet-Performance-Management.html

http://hobbitmon.sourceforge.net/

http://xymon.sourceforge.net/xymon/help/xymon-config.html

http://sourceforge.net/apps/mediawiki/xymon/index.php?title=XymonFaq

http://en.wikibooks.org/wiki/System_Monitoring_with_Xymon/Other_Docs/FAQ

http://en.wikibooks.org/wiki/System_Monitoring_with_Xymon/User_Guide

http://bbwin.sourceforge.net/

http://en.wikibooks.org/wiki/System_Monitoring_with_Xymon/Other_Docs/FAQ

http://en.wikibooks.org/wiki/System_Monitoring_with_Xymon/User_Guide

http://www.oracle-base.com/

http://www.consumoteca.com/telecomunicaciones/derechos-usuarios-telecomunicaciones/abonado/

http://office.microsoft.com/es-mx/access-help/conceptos-basicos-sobre-bases-de-datos-HA010064450.aspx#BMwhatisadatabase

http://www.slideshare.net/senaticscesar/bases-de-datos-conceptos-basicos

http://www.ajpdsoft.com/modules.php?name=News&file=article&sid=379

http://es.wikipedia.org/wiki/Sistema_de_archivos

http://www.kmlmedia.mx/clientes/nxr_oculto/productos-3.html

http://cezequiel.wordpress.com/tag/monitoreo-de-redes-linux/

http://www.sentrysoftware.com/library/mshw/index.html?monitoring_logical_disks.htm

https://communities.bmc.com/

http://www.sentrysoftware.com/library/mshw/index.html?ms_hw_physicaldisk.htm