Universidad Nacional Autónoma de México

Facultad de Ingeniería

Implementación de IBM Tivoli Monitoring como herramienta de monitoreo para servidores y aplicaciones

TESIS

QUE PARA OBTENER EL TÍTULO DE
INGENIERO EN COMPUTACIÓN
PRESENTA:

Jesús Antonio Castro Sánchez

DIRECTORA DE TESIS
M.C. Cintia Quezada Reyes

Ciudad Universitaria 2016

Agradecimiento

Cuando se consigue un objetivo tan importante en la vida, es necesario agradecer a todas aquellas personas que contribuyeron a alcanzar la meta propuesta.

En primer lugar he de agradecer a aquellos maestros que durante toda mi vida estudiantil me guiaron por el camino del conocimiento. La gran cantidad de conocimientos adquiridos durante este tiempo se debe a ustedes maestros que día con día entraban al salón de clases con el claro objetivo de enseñar lo mejor posible y que se esmeraban en ello.

Es importante hacer mención de mi Directora de Tesis, la Maestra Cintia Quezada que además de tomar un par de clases con ella, tuvo la disposición para ayudarme con la creación de este documento.

De esta forma quiero agradecer al más importante de todos mis maestros, mi padre; quien con su ejemplo me enseñó lo más importante en la vida, trabajar duro y constantemente para alcanzar las metas que te has propuesto, a dar siempre el cien por ciento.

A mi madre que en los momentos más difíciles siempre me dio motivos para creer. Quien sabe mi historia, por enseñarme a no dejar de intentarlo nunca. Sé que desafortunadamente no hay palabras para agradecer todo ese apoyo que ustedes me han brindado.

Finalmente he de agradecer a todos aquellos amigos que durante toda la carrera estuvieron ahí para apoyarme, para darme un consejo, para explicarme cosas que no entendía. Estudiar con ustedes fue un placer.

Índice

Índice de Figuras

Introducción

Durante los últimos años la seguridad de la información ha sido el centro de estudio y de los avances informáticos alrededor del mundo. Las instituciones tanto del sector privado como el sector público se han encargado de encontrar distintos métodos para salvaguardar información de carácter sensible.

Actualmente el debate se ha centrado sobre la vulnerabilidad de los sistemas informáticos, en la sensibilidad de la información y la protección de la misma. El mal uso de información ha llegado a tener consecuencias graves tanto económicas como legales.

En este campo, uno de los métodos más efectivos para mantener a salvo la información ha sido el monitoreo. El mantener activamente una vigilancia sobre los sistemas más sensibles de la organización brinda seguridad y reduce considerablemente los riesgos.

Es por esta razón que el objetivo principal por el cual se desarrolló esta tesis es para brindar una solución a esas instituciones que deseen implementar una herramienta que les ayude a resguardar su información y que busquen mitigar riesgos.

Los objetivos de la tesis son:

- Brindar un panorama general del monitoreo de servidores.
- Mostrar un panorama global de la herramienta IBM Tivoli Monitoring.
- Ejemplificar una instalación de la herramienta IBM Tivoli Monitoring.
- Mostrar los resultados que se conseguirían al tener instalada la herramienta IBM Tivoli Monitoring dentro de un sistema de TI.

Dentro de este escrito se guiará al implementador de soluciones de monitoreo por una instalación estándar de la herramienta IBM Tivoli Monitoring, la cual considero de las más completas y robustas dentro del mercado.

En el primer capítulo se plantea la problemática a la cual se busca hacer frente. Se dará un panorama de las distintas herramientas que se encuentran vigentes en el mercado actual de las soluciones de monitoreo.

En el segundo capítulo se explicará la arquitectura de la herramienta IBM Tivoli Monitoring, analizando su importancia y función dentro de la solución de monitoreo.

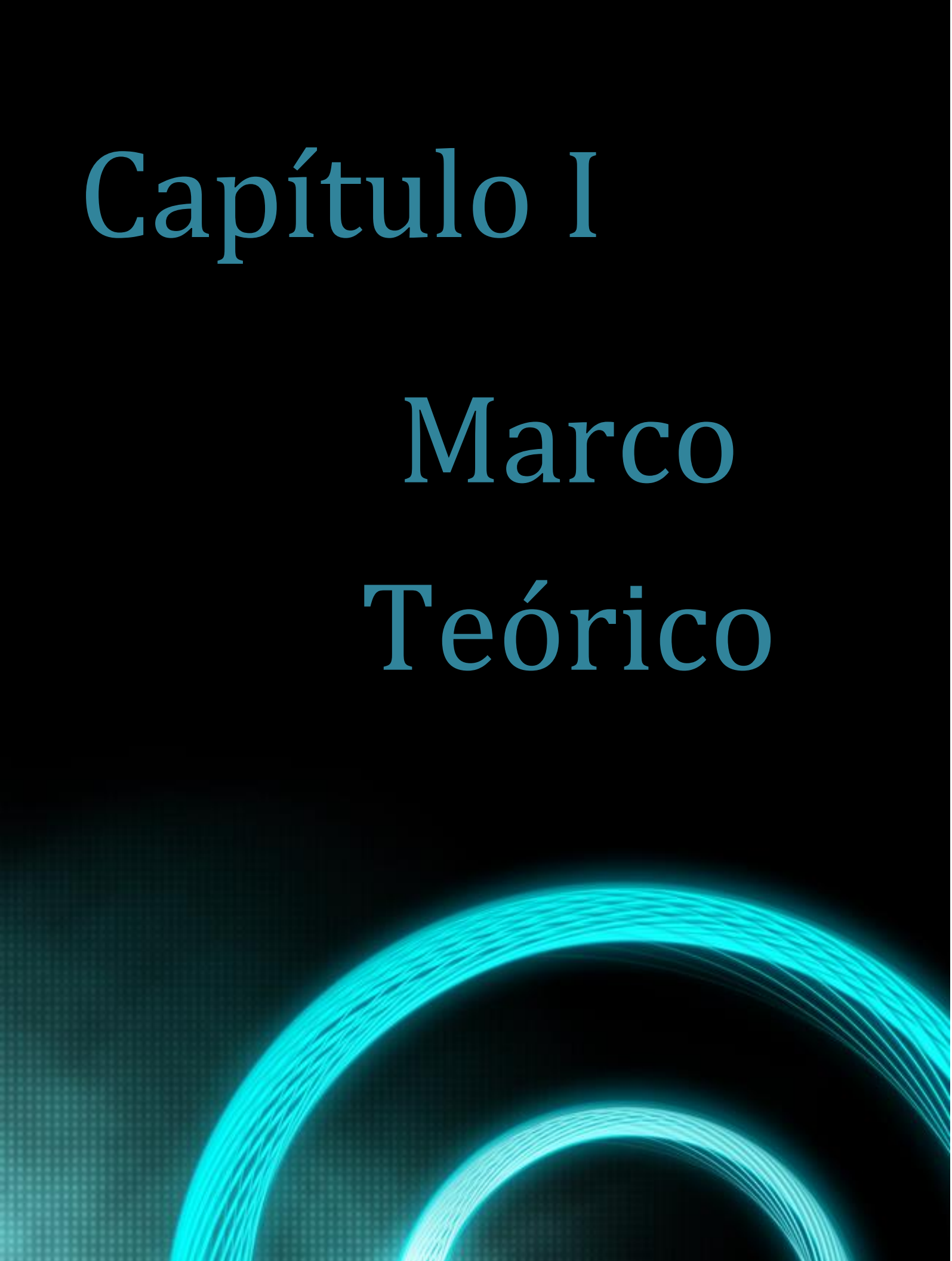
En el tercer capítulo se hablará del tema central de la tesis que es la implementación, en este apartado, se describirá de manera detallada cómo instalar y configurar cada componente de la herramienta de monitoreo. De esta forma se mostrará un caso estándar al cual se hizo frente.

Finalmente, en el cuarto capítulo, se mostrarán los resultados de la implementación. Se dará un panorama de los alcances que la herramienta puede llegar a tener dentro de los sistemas que monitorea.

De esta forma el lector podrá tener una visión general sobre los requerimientos y los beneficios que la herramienta otorga a manera de que este pueda discernir sobre si esta herramienta se ajusta a sus necesidades.

Capítulo I

Marco Teórico



1.1 Información

Se suele confundir los términos cuando se habla de datos, información y conocimiento. Si bien no son lo mismo, existe una estrecha relación entre ellos pero hay sutiles diferencias que se deben tener presentes para no cometer errores cuando se hace referencia a éstos.

Se dice que los datos son la base de todos estos conceptos. Los datos son elementos discretos, por ejemplo, una fecha, un importe, un domicilio, etcétera. Estos datos por sí mismos no tienen ningún valor puesto que no se ubican dentro de un contexto.

Por el contrario, al relacionar diferentes datos se unen y se estructuran para dar paso a la información. La información es "un mensaje, generalmente en forma de documento o comunicación audible o visible"[1].

Por último, el conocimiento se nutre de la información. Esta información debe ser útil y válida para el receptor. De tal forma que al hacer el esfuerzo mental de comprenderla se convierta en conocimiento.

Se concluye entonces que el conocimiento es toda aquella información que ha sido procesada por el receptor.

Se puede precisar que el desarrollo de la humanidad se debe en gran medida a la información. La vida diaria requiere de información para su realización.

La información se produce y se maneja para propiciar el desarrollo de la actividad económica, política y social. Es evidente que la información es una ventaja competitiva y decisiva en estos tiempos modernos. Para tomar una decisión lo más acertada posible es imprescindible basarse en información de calidad y actualizada.

1.1.1 Seguridad de la Información

Al comprender la importancia de la información se debe entender el privilegio que es el poseerla y las consecuencias que esto podría ocasionar si se encuentra en poder de la persona equivocada.

Se define entonces a la seguridad informática como "un conjunto de procedimientos, dispositivos y herramientas encargadas de asegurar la integridad,

[1] DAVENPORT, Thomas H. y L. Y PRUSAK, working knowledge. How organizations manage what they know, Harvard Business School Press 1998.

disponibilidad y privacidad de la información de un sistema informático e intentar reducir las amenazas que pueden afectar al mismo"[2].

Actualmente existen diversos tipos de amenazas a los sistemas informáticos. Una amenaza es todo aquello, ya sea físico o lógico, que puede provocar una pérdida de información, o de su privacidad, o bien un fallo en los sistemas.

Un sistema al estar compartiendo información y recursos se vuelve inmediatamente vulnerable a cualquier tipo de amenaza informática y ésta a su vez puede perjudicar a los demás sistemas conectados en red cuando explote alguna de las vulnerabilidades existentes y se convierta en un ataque.

Por tal motivo es prácticamente imposible encontrar un sistema que se pueda decir que es totalmente seguro. No obstante se pueden seguir las mejores prácticas y medidas de seguridad para reducir las vulnerabilidades del sistema al mínimo.

Es entonces que se pueden dividir las metodologías de seguridad en dos tipos: Seguridad Pasiva y Seguridad Activa. Esto depende en gran medida de los elementos que se van a utilizar y de los actos que desarrollen.

A. Seguridad Activa

"Se entiende por seguridad activa a todas aquellas medidas que se utilizan para detectar las amenazas, y en caso de su detección generar los mecanismos adecuados para evitar el problema."[3]

Un mecanismo de seguridad (también llamado herramienta de seguridad o control) es una técnica que se utiliza para implementar un servicio, es decir, es aquel mecanismo que está diseñado para detectar, prevenir o recobrarse de un ataque de seguridad. Los mecanismos de seguridad implementan varios servicios básicos de seguridad o combinaciones de estos servicios básicos – los servicios de seguridad especifican "qué" controles son requeridos y los mecanismos de seguridad especifican "cómo" deben ser ejecutados los controles.

En este rubro se pueden encontrar tres tipos de mecanismos que por las acciones que realizan se clasifican en:

a) Controles disuasivos: reducen la probabilidad de un ataque deliberado.

[2] Alfonso García. (2011). Razones para la seguridad Informática. En SEGURIDAD INFORMÁTICA (p. 2). Madrid, España.: Paraninfo.
[3] Íbid (p. 3).

b) Controles preventivos: protegen vulnerabilidades y hacen que un ataque fracase o reduzca su impacto.

c) Controles detectores: descubren ataques y disparan controles preventivos o correctivos.[4]

El monitoreo de los sistemas informáticos, en este caso, es un claro ejemplo de un mecanismo de seguridad activa. Por otra parte el uso de un antivirus o firewall y hasta el simple hecho de usar contraseñas para el acceso a los sistemas, son ejemplos de seguridad activa.

B. Seguridad Pasiva

Como se mencionó, ningún sistema está exento de sufrir algún ataque informático. Para ello es necesario estar preparado para cualquier eventualidad dañina y es por esto que surge la seguridad pasiva que "comprende todo el conjunto de medidas utilizadas para que una vez que se produzca el ataque o el fallo en la seguridad del sistema, hacer que el impacto sea el menor posible, y activar mecanismos de recuperación del mismo"[5]

"Un ataque informático consiste en aprovechar alguna debilidad o falla (vulnerabilidad) en el software, en el hardware, e incluso, en las personas que forman parte de un ambiente informático; a fin de obtener un beneficio, por lo general de índole económico, causando un efecto negativo en la seguridad del sistema, que luego repercute directamente en los activos de la organización."[6]

"A continuación se definen los tipos de ataque informáticos más usuales:

a) Ataques de repetición: se producen cuando un pirata informático copia una secuencia de mensajes entre dos usuarios y envía la secuencia a uno o más usuarios. El equipo objeto del ataque procesa la secuencia como mensajes legítimos y se producen consecuencias como pedidos redundantes.

b) Ataques de modificación de bits: se basan en las respuestas predecibles de las estaciones receptoras. El pirata informático modifica un mensaje (cambia los bits) para enviar un mensaje cifrado erróneo a una estación receptora, el cual entonces se puede comprar con la respuesta predecible para obtener la clave a través de múltiples interacciones.

[4] Quezada C. Mecanismos de Seguridad. Marzo 8, 2015, de UNAM Facultad de Ingeniería Sitio web: http://profesores.fi-b.unam.mx/cintia/Mecanismos.pdf
[5] Íbid. (p. 5).
[6] Mires J.. (2009). Ataques Informáticos. febrero 26, 2015, de evil fingers Sitio web: https://www.evilfingers.com/publications/white_AR/01_Ataques_informaticos.pdf

c) Ataques de denegación de servicio (DOS, Denial Of Service): consiste en colapsar total o parcialmente un servidor para que este no pueda realizar su tarea (no para obtener información). En internet, un ataque DOS se puede realizar inundando a un servidor con una gran cantidad de solicitudes. El servidor es incapaz de responder a todas las solicitudes, por tanto, se satura. En las redes inalámbricas este tipo de ataques se centra en saturar la banda de frecuencia con ruido. Una forma es colocar un teléfono inalámbrico de 2.4 GHz cerca de un punto de acceso y luego iniciar una llamada. La energía de radiofrecuencia que generan muchos teléfonos inalámbricos es suficiente para bloquear de manera efectiva gran parte del tráfico de un punto de acceso.

d) Ataques de diccionario: en algunos modelos de autenticación, la contraseña se mantiene en secreto, mientras que el nombre de usuario se envía en forma de texto simple y se puede interceptar fácilmente. En este caso, un pirata informático puede obtener distintos nombres de usuario y luego comenzar el proceso (generado por un ordenador) de adivinar las contraseñas que usan palabras que se encuentran en los diccionarios de idiomas. Este conocido ataque de fuerza bruta es exitoso debido a la alta capacidad de procesamiento de los sistemas informáticos y a lo poco creativo de la mayoría de usuarios cuando seleccionan contraseñas. Cuando el pirata informático consigue un nombre de usuario y la contraseña asociada válida, entonces, podrá entrar a la red, inalámbrica o cableada, haciéndose pasar por un usuario legítimo. Este tipo de ataques se hace poco efectivo si las contraseñas son largas, contienen números, letras y caracteres especiales y se combinan con mayúsculas y minúsculas."[7]

En este rubro se encuentra la clasificación de los mecanismos correctivos que su principal función es la de reducir el efecto del ataque.

El ejemplo típico de seguridad pasiva en los sistemas informáticos son los respaldos. Ya sea el uso de redundancia en discos RAID (Redundant Array Inexpensive Disks) o el uso de cintas para el respaldo de dicha información.

1.2 Protocolos de Red

Para que los sistemas informáticos puedan compartir entre ellos información fue necesaria la creación de una red de datos. Se denomina red de datos al sistema que enlaza dos o más puntos (terminales) por un medio de transmisión, el cual sirve para enviar o recibir un determinado flujo de información.

"Existen distintos tipos de redes dependiendo de muchos factores. Es posible clasificarlas por:

[7] Valdivia C.. (2014). Sistemas Informáticos y Redes Locales. Madrid, España: Paraninfo. (pp.156-157)

1) Extensión

La extensión se refiere a la distancia que las redes pueden alcanzar a cubrir (Figura 1.1).

a) PAN (Personal Area Network - Red de Área Personal) es la red inalámbrica de interconexión de periféricos que se puede encontrar tanto a unos pocos centímetros como a metros de distancia del emisor.

b) LAN (Local Area Network - Red de Área Local) es la red que suele situarse en el mismo edificio o en entornos de unos 200m llegando al kilómetro cuando se usan repetidores.

c) CAN (Campus Area Network – Red de Área Campus) es la red cuya extensión es la de un campus universitario, una base militar, un polígono industrial o un grupo de grandes edificios en un área geográfica limitada.

d) MAN (Metropolitan Area Network – Red de Área Metropolitana) es la red que se sitúa en un barrio, urbanización, ciudad o municipio pequeño (a pocos kilómetros, normalmente oscila entre 1 y 7 Km).

e) WAN (Wide Area Network – Red de Área Mundial) es la red global (varios países, un continente o incluso mundial). Estas redes suelen estar diseñadas para la interconexión de redes.

Figura 1.1 Extensión de las redes de datos.

2) Conexión

La conexión se refiere a la forma en que una red permite la conexión entre los dispositivos.

a) Guiado, alámbrico o terrestre. La señal es guiada por un cable u otro medio cerrado.

b) No guiado, aéreo o inalámbrico. Pueden utilizar sistemas de radio, infrarrojos, microondas, láser, entre otros.

3) Propiedad

La propiedad de una red se refiere al dueño de la misma. Las redes serán privadas si pertenecen a una empresa concreta y no las alquila o comparte. Por otro lado, serán públicas cuando se alquilan o dan acceso a internet, es decir, pertenecen a un proveedor de servicios de telecomunicaciones.

4) Topología

La topología (Figura 1.2) hace referencia a la forma en que una red permite las conexiones entre los dispositivos de la misma.

a) Centralizada. Todas las comunicaciones se centran en un solo equipo. Es una topología muy parecida a la estrella.

b) Descentralizada. Existen varios centros que concentran las comunicaciones, y éstos, a su vez, están centralizados en otro elemento de forma jerárquica. Es una topología en árbol.

c) Distribuida. Aparece cuando no existe ningún equipo que centralice las conexiones. También se llama de malla.

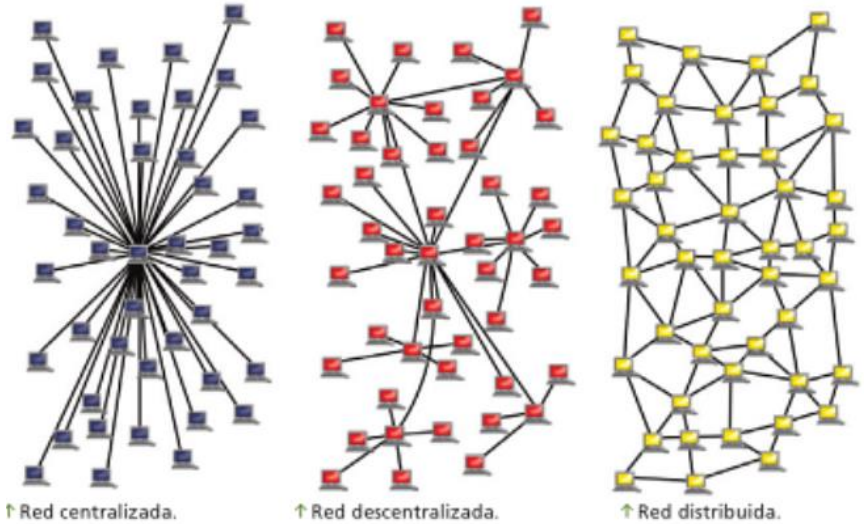


Figura 1.2 Topología de las redes de datos.

5) Dirección de transmisión

Las redes pueden clasificarse en función del sentido y la dirección de la emisión o transmisión de la información. Se hace según si ésta se realiza de forma unidireccional, bidireccional simultánea o bidireccional no simultánea."[8]

No obstante para que una red tan grande como internet sea posible y funcional es necesaria la implementación de protocolos de red y de transporte con el propósito de garantizar la entrega de datos independientemente de que una red pueda sufrir fallos o caídas de algunos enlaces durante la comunicación.

"Los protocolos son arreglos entre personas o procesos. En esencia, un protocolo es un conjunto de reglamentos acerca de la formalidad o procedencia, como por ejemplo un protocolo militar o diplomático. Un protocolo de red de comunicación de datos es un conjunto de reglas que gobierna el intercambio ordenado de datos dentro de la red."[9]

A continuación se mencionan algunos de los protocolos más utilizados e importantes para la implementación de una herramienta de monitoreo, a fin de entender la comunicación de los sistemas informáticos.

1. El UDP (user datagram protocol – Protocolo de Datagrama de Usuario) es un protocolo que no está orientado a la conexión, de esta manera es incapaz de proporcionar algún tipo de control de errores o de flujo aunque utilice mecanismos de detección de errores. Si el UDP detecta algún error no entrega el datagrama a la aplicación, simplemente lo descarta.

2. El TCP (transmission control protocol – Protocolo de control de transmisión) es el protocolo que garantiza la entrega de toda la información en el mismo orden en que ha sido emitida por el origen. Para conseguir esta fiabilidad, el TCP proporciona un servicio orientado a la conexión con un control de flujo y errores.

3. El ICMP (Internet Control Message Protocol – Protocolo de Mensajes de Control de Internet) funciona a través de IP y da la información de los errores y controles a TCP.

4. El protocolo IGMP (Internet Group Management Protocol – Protocolo de administración de grupos de Internet) pertenece a la capa de red y permite a una estación unirse o dejar a un grupo multidifusión (multicast). El encabezamiento IGMP se encapsula en un paquete IP con muy poca información dentro de la cual se encuentran las distintas acciones de

[8] Andréu J. (2011). Redes Locales. Libro Electrónico: Editex. (pp.23-25)
[9] Tomasi, W. (2003). Sistemas de comunicaciones electrónicas. (p. 605). México: Pearson Educación.

identificación para un grupo, un informe de pertenencia y retirada y la dirección del grupo al cual va dirigida la información.

5. ARP (Address Resolution Protocol – Protocolo de resolución de direcciones) permite determinar la dirección MAC del nodo a partir de su dirección IP efectuando una difusión. Esta resolución es necesaria para poder dirigir directamente la trama al periférico correcto en la red IP local.

6. RARP (Reverse Address Resolution Protocol – Protocolo de resolución de direcciones inverso) efectúa una resolución inversa en el caso de que una estación sin disco quiera obtener una dirección IP a partir de la única información de la cual dispone, su dirección MAC.

7. SMTP (Simple Mail Transfer Protocol – Protocolo para la transferencia simple electrónico) es un protocolo de transferencia simple utilizado en servicios de mensajería electrónica de correo. Se basa en TCP e IP y no integra ninguna interfaz de usuario. Desempeña el papel de enlace o transporte.

8. El protocolo POP3 (Post Office Protocol 3 – Protocolo de Oficina Postal 3) se dedica específicamente a la publicación y al acceso a distancia a un servidor de mensajería. El servidor POP se comunica con el Agente Usuario (User Agent) a través de una conexión síncrona. El servidor transfiere los mensajes hacia el cliente, luego los suprime si lo pide el cliente.

9. El protocolo IMAP (Internet Message Access Protocol – Protocolo de acceso a mensajes de internet) permite que se almacenen y que se conserven en el servidor de mensajería los mensajes electrónicos en lugar de transferirlo sistemáticamente hacia la estación cliente.

10. HTTP (HyperText Transfer Protocol – protocolo de transferencia de hipertexto) es un protocolo sencillo del tipo cliente-servidor que articula los intercambios de información entre los clientes Web y los servidores HTTP. Este protocolo se basa en sencillas operaciones de solicitud/respuesta. Un cliente establece una conexión con un servidor y envía un mensaje con los datos de la solicitud. El servidor responde con un mensaje similar, que contiene el estado de la operación y su posible resultado.

11. FTP (File Transfer Protocol – Protocolo de Transferencia de Archivos) es un protocolo de transferencia de archivos basado en un método fiable e implementado sobre TCP. La principal característica de FTP es que se puede utilizar entre sistemas operativos diferentes, que se basan en sistemas de archivos heterogéneos.

12. DHCP (Dynamic Host Configuration Protocol – Protocolo de Configuración Dinámica de Host) es un protocolo de configuración automático de las opciones TCP/IP para clientes de un entorno NetBIOS. Con este protocolo es posible asignar dinámicamente una dirección IP, una máscara de red secundaria, una dirección IP de puerta de enlace predeterminada (dirección IP que corresponde a un router que permite salir de la red local) y una dirección IP de servidor DNS.

13. Telnet es un protocolo de emulación de terminal. Establece una sesión entre una estación de trabajo (cliente Telnet) y una máquina (servidor Telnet). Se transmite cualquier comando escribiendo en el cliente y se ejecuta en el servidor Telnet. El eco del proceso distante es redirigido hacia la estación de trabajo, que se ve el resultado del comando. Telnet requiere conocer los comandos del sistema operativo del servidor.

14. El protocol NTP (Network Time Protocol – Protocolo de Tiempo en Red) permite sincronizar los ordenadores que funcionan en una red. Para esto el equipo hace referencia a un servidor horario que puede comparar y ajustar su hora con otro servidor NTP en Internet.

15. SNMP (Simple Network Management Protocol – Protocolo Simple de Administración de Red) es un protocolo de nivel de aplicación que utiliza como protocolo de transporte UDP. Define una relación cliente/servidor entre el gestor de red (que actúa de cliente) y los elementos gestionados (que son los servidores y reciben el nombre de “agentes SNMP”).

16. SSH (Secure Shell – intérprete de órdenes segura) es el nombre de un protocolo que sirve para acceder a máquinas remotas a través de una red, de forma similar a como lo hace telnet. La diferencia principal es que SSH usa técnicas de cifrado para que ningún atacante pueda descubrir el usuario y contraseña de la conexión ni lo que se escribe durante toda la sesión.

1.3 Software Libre y Software Propietario

El diccionario de la Real Academia Española define al software como el conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora[10].

Según el estándar 729 del IEEE, software es el conjunto de programas de cómputo, procedimientos, reglas, documentación y datos asociados que forman parte de las operaciones de un sistema de computación.

[10] Diccionario RAE http://buscon.rae.es/drae/srv/search?val=software [Marzo, 4, 2015]

En los años de 1970 las primeras computadoras eran esencialmente herramientas de búsqueda y de cálculo con fines militares. Rápidamente las empresas vieron el inmenso interés de automatizar algunas de sus tareas como la contabilidad, pagos, entre otros.

Con la compra de los primeros grandes ordenadores de gestión, se necesitaron programas que utilizaran el hardware de estos ordenadores. Estos programas tuvieron que ser protegidos como secretos industriales: había nacido una nueva industria: la creación de programas.

Con su entrada en la dinámica de las grandes empresas, la informática perdió rápidamente su inocencia y perdió la libertad. Se empezó a hablar de licencias, impuestos y tasas, derechos de autor, limitación de los derechos y prohibiciones de copiar. Surge el Software Propietario.

Se entiende por software propietario todo aquel programa o conjunto de programas cuyas limitaciones para el usuario que lo adquiere son la copia, modificación o distribución, tanto modificado, como no modificado.

Paralelo al fenómeno que surgía sobre el software y su comercialización Richard Stallman lamentaba profundamente este hecho. Informático en el laboratorio de inteligencia artificial en el MIT a finales de los años 1970. Usuario de una impresora que se averiaba a menudo, Stallman y sus compañeros disponían del código fuente del driver (programa de gestión) de la impresora, lo modifican para recibir una señal de cada avería.

En un momento dado, el laboratorio compra un nuevo modelo de Xerox más fiable, pero el driver para su sistema operativo no aparece. Como desea adaptar este driver a sus necesidades, Richard Stallman, recurre a otro laboratorio que dispone del código fuente, pero que se niega a proporcionárselo: Xerox lo prohíbe. Esto significaría que la impresora nunca funcionaría, y Stallman, muy contrariado por esta situación, decide obrar en pro de la defensa y difusión del software libre.

Stallman decide en 1983 escribir un nuevo sistema operativo de acceso, uso, modificación y redistribución completamente libres. Basado en Unix, lo nombra GNU (Gnu's Not Unix). Surge el Software Libre.

Según la página del mismo proyecto GNU estipula la definición de Software Libre como:

"«Software libre» es el software que respeta la libertad de los usuarios y la comunidad. En grandes líneas, significa que los usuarios tienen la libertad para ejecutar, copiar, distribuir, estudiar, modificar y mejorar el software. Es decir, el

«software libre» es una cuestión de libertad, no de precio. Para entender el concepto, piense en «libre» como en «libre expresión», no como en «barra libre». Promovemos estas libertades porque todos merecen tenerlas. Con estas libertades, los usuarios (tanto individualmente como en forma colectiva) controlan el programa y lo que éste hace. Cuando los usuarios no controlan el programa, se dice que dicho programa «no es libre», o que es «privativo». Un programa que no es libre controla a los usuarios, y el programador controla el programa, con lo cual el programa resulta ser un instrumento de poder injusto.

Un programa es software libre si los usuarios tienen las cuatro libertades esenciales:

a) La libertad de ejecutar el programa como se desea, con cualquier propósito (libertad 0).

b) La libertad de estudiar cómo funciona el programa, y cambiarlo para que haga lo que usted quiera (libertad 1). El acceso al código fuente es una condición necesaria para ello

c) La libertad de redistribuir copias para ayudar a su prójimo (libertad 2).

d) La libertad de distribuir copias de sus versiones modificadas a terceros (libertad 3).

Esto le permite ofrecer a toda la comunidad la oportunidad de beneficiarse de las modificaciones. El acceso al código fuente es una condición necesaria para ello.

Un programa es software libre si otorga a los usuarios todas estas libertades de manera adecuada. De lo contrario no es libre. Existen diversos esquemas de distribución que no son libres, y si bien podemos distinguirlos con base en cuánto les falta para llegar a ser libres, nosotros los consideramos contrarios a la ética a todos por igual."[11]

1.4 Servidores

Para hablar acerca de un servidor es necesario hacer referencia al concepto de la arquitectura cliente-servidor, la cual dará un panorama general de la función de un servidor dentro del ámbito empresarial.

[11] Gnu.org. (2016). *¿Qué es el software libre? - Proyecto GNU - Free Software Foundation*. https://www.gnu.org/philosophy/free-sw.es.html [Marzo, 23,2015]

1.4.1 Arquitectura cliente servidor

La arquitectura cliente-servidor (Figura 1.3) es un modelo de sistema en el que dicho sistema se organiza como un conjunto de servicios y servidores asociados más unos clientes que acceden y usan los servicios. Los principales componentes de este modelo son:

1. Un conjunto de servidores que ofrecen servicios a otros subsistemas.

2. Un conjunto de clientes que llaman a los servicios ofrecidos por los servidores.

3. Una red que permite a los clientes acceder a estos servicios.

El funcionamiento básicamente se basa en que los clientes acceden a los servicios proporcionados a través de llamadas a procedimientos remotos usando un protocolo de petición-respuesta como por ejemplo el http. Un cliente realiza la petición a un servidor y espera hasta que recibe una respuesta.

La ventaja más importante del modelo cliente-servidor es que es una arquitectura distribuida. Se puede hacer un uso efectivo de los sistemas en red con muchos procesadores distribuidos. Es fácil añadir un nuevo servidor e integrarlo con el resto del sistema o actualizar los servidores de forma transparente sin afectar al resto del sistema.[12]

Dicho lo anterior, un servidor puede encontrarse en un típico local. La máquina que tiene el cajero da un servicio; es un servidor, encargado de habilitar o deshabilitar una computadora personal (PC) para que pueda ser usada para navegar o jugar. Si deja de funcionar, el negocio no factura y ninguna de las máquinas cliente podría ser utilizada.

Los servidores son equipos informáticos que brindan un servicio en la red. Dan información a otros servidores y a los usuarios. Son equipos de mayores prestaciones y dimensiones que una PC de escritorio.

[12] Sommerville I., (2005). 11.2 Organización del Sistema en Ingeniería del Software (p.227). Madrid: PEARSON EDUCACIÓN, S.A.

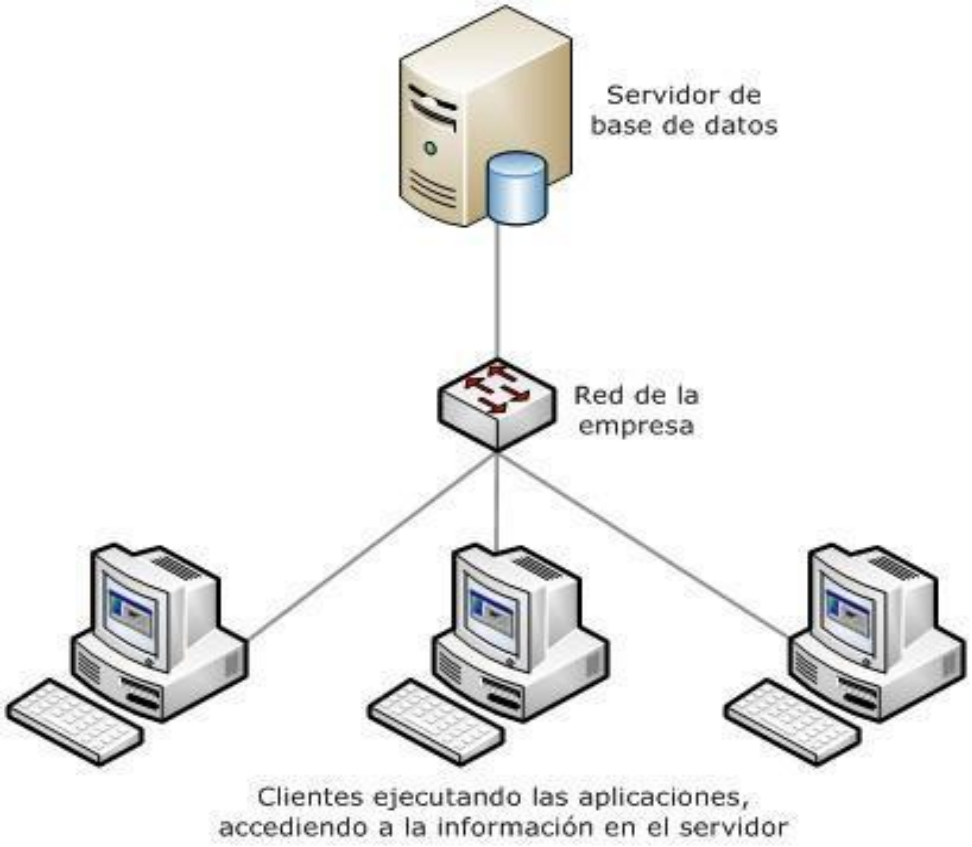


Figura 1.3 Arquitectura Cliente-Servidor

Una computadora común tiene un solo procesador, a veces de varios núcleos, pero uno solo. Incluye un disco rígido para el almacenamiento de datos con una capacidad de 250 GB a 300 GB, en tanto que la memoria RAM suele ser de 2 a 16 GB.

Un servidor, en cambio, suele ser más potente. Puede tener varios procesadores con varios núcleos cada uno; incluye grandes cantidades de memoria RAM, entre 16 GB y 1 TB o más; mientras que el espacio de almacenamiento ya no se limita a un disco duro, sino que puede haber varios de ellos, con capacidad del orden del TB. Debido a sus capacidades, un servidor puede dar un solo servicio o más de uno.

En la Tabla 1.1 se compara el hardware de un servidor y una PC de escritorio:

Tabla 1.1 Comparación entre las características físicas de una PC de escritorio y un servidor.[13]

EQUIPOS DELL	Servidor PowerEdge R910	PC de Escritorio Optilex 960
Microprocesador	Eight-Core Intel Xeon 7500 and 65000 Series, hasta 24 MB de caché L3	Intel Core2 Quad Processor, hasta 12 MB de caché L2
Disco duro	Hasta 9 TB SSD y SAS	Hasta 320 GB SATA II
Memoria RAM	Hasta 1 TB, ECC DDR3, 1066 MHz	Hasta 16 GB, DDR2 SDRAM, 800 MHz
Placa Gráfica	Matrox G200eW/ 8 MB	512 MB NVIDIA NVS 420 Quad Monitor

En la figura 1.4 se pueden ubicar los principales componentes de un servidor.

Figura 1.4 Hardware de un servidor.

[13] Marchionni, E., (2011). Servidores en una red corporativa. En Administrador de servidores (p.23). Buenos Aires: Fox Andina S.A.

El número 1 marca el sistema de refrigeración. Dicho sistema contempla los componentes necesarios para mantener al servidor a una temperatura adecuada para su funcionamiento.

El número 2 muestra los discos duros del servidor. En algunos modelos estos discos duros pueden ser cambiados y reemplazados incluso si el servidor se encuentra encendido.

El número 3 ubica las fuentes de poder del servidor. Son las encargadas de regular, gestionar y proporcionar la correcta cantidad de energía eléctrica a cada componente del servidor. En la imagen se puede apreciar la ventilación independiente de la fuente de poder.

El número 4 muestra las placas del servidor, en ella se encuentra la memoria RAM, el CPU, las placas de expansión así como también disipadores de calor y conectores.

1.4.2 Tipos de Servidores

Existen distintos tipos de servidores y pueden ser virtuales o físicos. Se denomina servidor físico o dedicado, al servidor que se puede ver y tocar. Se trata de una configuración de hardware y software concreta. Al hablar de un servidor virtual se hace referencia a una instalación de software realizada sobre un servidor físico; este servidor físico puede alojar diferentes servidores virtuales que comparten entre sí el hardware y los recursos, pero su funcionamiento es completamente independiente (Figura 1.5)

Para lograr que un servidor físico almacene distintos servidores virtuales es necesario contar con un software de virtualización que permita asignar los recursos físicos como memoria RAM, núcleos de CPU, tarjeta de video y disco duro a los servidores virtuales. “Algunos virtualizadores conocidos son VMWare, Windows Virtual Server, Linux Virtual Server y Citrix.”[14]

[14] Colobran, M., Arqués, M. & Marco E.. (2008). Administración de sistemas operativos en red. Barcelona: Editorial UOC. (p. 32)

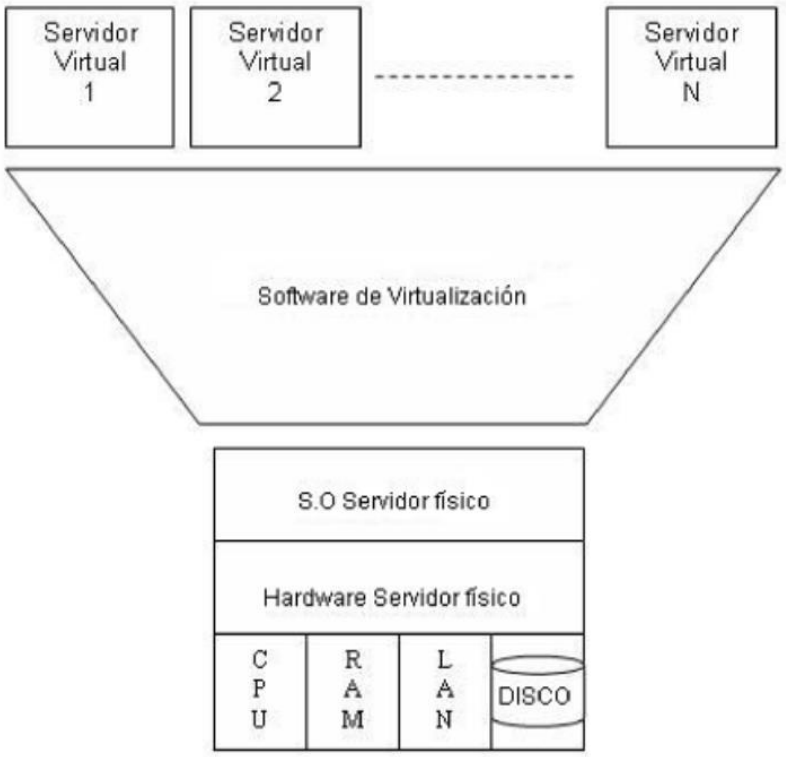


Figura 1.5 Diagrama de virtualización.

Generalmente, en un ambiente empresarial se suelen tener servidores físicos dentro de los cuales se virtualizan otros servidores con capacidades de software distribuidas, es decir, a un servidor virtual se les asigna un determinado número de núcleos del procesador una parte de memoria RAM y una capacidad determinada dentro del disco duro.

De igual forma los servidores se pueden clasificar dependiendo de los servicios que ofrecen. A continuación se describe esta categorización:

a) “Servidores de impresión: tienen conectadas varias impresoras de red y administran las colas de impresión según la petición de sus clientes.

b) Servidores web: este tipo de servidores se encargan de almacenar sitios en la red interna (intranet). Pueden publicar cualquier aplicación web, brindarle la seguridad correspondiente y administrarla por completo.

c) Servidores de base de datos: lo más importante de estos servidores es la posibilidad de manejar grandes cantidades de datos y generar información. Para contener todo ese material generalmente se conectan a un storage (almacén de información).

d) Servidores de correo electrónico: son capaces de administrar todos los correos de la empresa en un solo lugar. También trabajan con un storage, debido a la gran cantidad de datos que manejan. Allí se almacenan los correos, y se les redirecciona a clientes y servidores de seguridad, analizadores y replicadores. Algunos también brindan opciones de seguridad, como antispam, lista blanca, lista negra y antivirus.

e) Servidores de directorio: se ocupan de almacenar los datos de todos los usuarios de la red, propiedades y características que los identifican.

f) Servidores de comunicaciones: brindan servicios de chat, telefonía IP, teleconferencia, video, etcétera. También son capaces de entregar servicios de asistencia si se los conecta a una consola telefónica.

g) Servidores de archivos: permiten compartir el material y guardarlo de manera segura, y ofrecen una mayor capacidad de almacenamiento que los equipos de escritorio. Pueden tener conectados varios storage de distintas capacidades.

h) Servidores de seguridad: se dedican a escanear la red en busca de virus, máquinas desactualizadas por falta de parches del sistema operativo, equipos con determinado software instalado, etc.

i) Servidores proxy: brindan acceso a Internet. En ellos generalmente residen firewalls a los que se les configuran reglas para permitir la navegación por ciertas páginas y bloquear otras. Pueden redireccionar la navegación y mostrar algún cartel de advertencia o violación de la política empresarial.

j) Servidores de servidores virtuales: un solo servidor físico puede contener varios servidores virtuales, pero el usuario final no distinguirá las diferencias. Sólo desde su administración es posible explotar todas sus características.

k) Servidores particulares: se instalan para cada aplicación que se use en la red. Por ejemplo, servidores de workflows, de CRM, de RR.HH., de contaduría, etc."[15]

[15] Íbid. (pp.25-27).

Finalmente existen 3 tipos de tamaños que se han popularizado:

Los rackeables son aquellos que se pueden ubicar dentro de un rack y que van sujetos por correderas como el que se mostró en la figura 1.4. Los servidores Tower son parecidos a una PC de escritorio pero sus características de hardware son más potentes. Finalmente existen los blades; son servidores que trabajan en conjunto. Varios blades forman un servidor completo el cual se puede administrar como un servidor único. Estos blades se pueden intercambiar mientras el servidor está activo.

1.5 Monitoreo

Partiendo de la definición de la palabra "monitoreo", se encuentra la descrita en el Diccionario de la Real Academia Española que dice:

> A partir del sustantivo monitor (del inglés monitor, dispositivo o pantalla de control), se han creado en español los verbos monitorizar y monitorear, con el sentido de vigilar o seguir [algo] mediante un monitor.[16]

Entonces el monitoreo de Tecnologías de la información (TI) es principalmente vigilar cada uno de los componentes de la infraestructura, tanto de software como de hardware, para el correcto funcionamiento de la misma y en dado caso, avisar si algún fallo ocurriese.

1.5.1 Importancia del monitoreo

Anticiparse a los problemas permite tener una alta disponibilidad de los servicios que brinda el área de TI. Actualmente las compañías buscan la alta disponibilidad de todos sus servicios porque el mercado y los clientes así lo demandan.

Dentro del área de tecnología es de vital importancia el tener monitoreados todos los elementos que la componen. El exponencial crecimiento de las amenazas de intrusos hacen del monitoreo una herramienta cada vez más recurrente en todas las empresas.

De igual manera, se sabe que tanto el software como el hardware no están exentos de fallas. El saber que alguno de éstos no está trabajando dentro de un umbral adecuado o no tiene un funcionamiento normal, puede significar ~~el~~ solventar los problemas a tiempo.

Hoy en día, una empresa necesita contar con herramientas de monitoreo para su red de servidores. Con esto puede asegurar la continuidad operacional de aplicaciones de misión crítica. Es de vital importancia conocer en todo momento la calidad de operación, eficiencia y productividad.

[16] Diccionario de la Real Academia Española

1.5.2 Principales herramientas del monitoreo

Se denomina herramienta de monitoreo al software que constantemente monitorea una red de computadoras para detectar sistemas lentos o en mal funcionamiento y que notifica al administrador de la red en caso de falla por medio de correo, mensaje o alarma, entre otras.

Su funcionamiento se basa principalmente en recoger información de los dispositivos de la red entre lapsos muy cortos de tiempo para posteriormente graficarlos en una consola y alertar al responsable si algún fallo ocurriera.

Tal es la importancia del monitoreo en la actualidad que son diversas las soluciones que se ofrecen en el mercado. A continuación se mencionarán algunas de las más utilizadas en la industria.[17]

1. Herramientas de software libre

a) Nagios

Una de las herramientas más utilizados para el monitoreo de servidores y la red es Nagios. Gracias a que es un software libre, el único costo que requiere es el del personal de implementación.

Entre los servicios de red que Nagios monitorea está SMTP POP3, HTTP y SNMP. Monitoriza los recursos de hardware como el procesador, el disco, la memoria de servidores que incluso trabajan bajo sistema operativo Windows.

Así mismo, existe la posibilidad de que cualquiera pueda crear un plugin que permita monitorear sus propios servicios adecuándose a sus necesidades.

En cuanto a la presentación del monitoreo, Nagios puede notificar cuando algún problema ocurre, así como también cuando el problema fue resuelto. Todo esto puede ser vía correo electrónico o vía SMS. Por otra parte Nagios cuenta con una interfaz web con la cual se pueden generar informes y gráficas del comportamiento de todos los sistemas. Pueden visualizarse el historial de problemas, registros, etcétera.

b) Zabbix

Zabbix es una solución de código abierto que permite de forma rápida y sencilla monitorizar todo tipo de servidores, aplicaciones y equipos que hacen parte de una

[17] Fraterneo.blogspot.mx. (2010). *fraterneo GNU/Linux: 5 Aplicaciones Libres para Monitoreo de Redes y Servidores*. http://fraterneo.blogspot.mx/2010/12/5-aplicaciones-libres-para-monitoreo-de.html [Abril, 7, 2015]

red. Permite centralizar la información en un servidor y monitorear múltiples hosts. Tiene una administración vía web browser.

Proporciona información sobre la máquina que monitorea (disco, memoria, procesador) y muestra las estadísticas de manera cronológica. Puede descubrir nodos en un rango de IP's usando agentes SNMP y cuenta con la capacidad de monitorear servicios remotos.

Zabbix también es capaz de enviar avisos, alarmas y notificaciones de eventos previamente definidos mediante correo electrónico o SMS.

c) Cacti

Cacti es una interfaz desarrollada en PHP que se complementa con RRDtool (Round Robin Database Tool – Herramienta de Base de Datos Round Robin) para el manejo de los datos.

Por su parte Cacti maneja un pooler ágil, plantillas de gráficos personalizables para mostrar los datos, múltiples métodos para la recolección de datos y manejo de usuarios con niveles de privilegio.

Todo esto está envuelto en una interfaz intuitiva y fácil de usar que se puede usar para redes de tamaño LAN así como también para redes más complejas con cientos de dispositivos.

d) Zenoss

Zenoxx Core 5 promete ser la solución de monitoreo más potente en la industria de código abierto que ofrece una visibilidad de toda la plataforma de TI.

Dentro de sus características principales incluye la detección automática de dispositivos, un inventario a través de CMDB (Configuration Management Database – Base de datos de la gestión de la configuración), monitoreo de la disponibilidad, gráficos de rendimiento fáciles de interpretar, alertas y un portal web fácil de usar.

Unifica y automatiza la disponibilidad y gestión de eventos para toda la infraestructura (aplicaciones, servidores, almacenamiento y redes). De igual manera, automatiza la notificación y la solución de los eventos; conoce qué servicios se ven afectados e identifica rápidamente la causa raíz.

2. Herramientas de software propietario

a) **PRTG** (Paessler Router Traffic Grapher)

PRTG Network Monitor corre en una máquina de Windows dentro de la red, recolectando varias estadísticas acerca de las máquinas, del software y de los equipos los cuales se designan por el administrador. Retiene los datos para que se pueda visualizar un histórico ayudando a reaccionar a los cambios.[18]

PRTG cuenta con una interfaz web de fácil manejo con la cual se pueden compartir fácilmente los datos con todo el equipo técnico e incluso con los clientes. Incluye gráficas de tiempo real y reportes personalizados.

PRTG puede recolectar datos de cualquier dispositivo de la red y soporta múltiples protocolos como SNMP y WMI, husmeo (snifffing) de paquetes, Netflow, jFlow y sFlow.

La ventaja del licenciamiento de PRTG radica en que únicamente se paga un precio por la versión del software basado en el número de sensores o dispositivos que se desean monitorear.

b) Tivoli[19]

IBM Tivoli Monitoring ayuda a optimizar el rendimiento y la disponibilidad de la infraestructura de TI. Este software proactivo de supervisión del sistema gestiona sistemas operativos, bases de datos y servidores en entornos distribuidos y de host. Al proporcionar las mejores prácticas para identificar y resolver problemas de infraestructura ayuda a maximizar la eficiencia del departamento de TI.

Tivoli Monitoring permite identificar y arreglar interrupciones y atascos que amenazan aplicaciones clave, incluso:

- Supervisa de manera proactiva los recursos del sistema para detectar problemas potenciales y responde automáticamente a eventos. Al identificar los problemas pronto, permite arreglarlos rápidamente antes de que los usuarios noten alguna diferencia en el rendimiento.

- Proporciona un umbral dinámico y análisis de rendimiento para mejorar la prevención de riesgos. Este sistema de "avisos con anticipación" permite empezar a trabajar en un incidente antes de que afecte a los usuarios y a las aplicaciones o servicios empresariales.

[18] Es.paessler.com. (2016). *PRTG Network Monitor - monitorización de red fácil*. http://www.es.paessler.com/prtg [Abril, 7, 2015]
[19] Www-03.ibm.com. (2016). *IBM Productos de Software*. http://www-03.ibm.com/software/products/es/tivomoni [Abril, 7, 2015]

- Mejora la disponibilidad y la media de tiempo de recuperación gracias a la visualización rápida de incidentes y la búsqueda histórica de investigación rápida de incidentes. Puede identificar y resolver una interrupción de rendimiento o servicio en minutos en vez de horas.

- Recoge datos que puede utilizar para dirigir las actividades de rendimiento y planificación de la capacidad a tiempo y así evitar interrupciones debidas al exceso de uso de recursos. El software supervisa, alerta e informa de futuros atascos en la capacidad.

- Facilita la supervisión del sistema con una interfaz de navegación común, flexible e intuitiva y espacios de trabajo personalizables. Además incluye un almacén de datos fácil de utilizar y funciones avanzadas de creación de informes.

La solución de IBM Tivoli Monitoring en conjunto con Netcool/Omnibus es muy robusta y compleja. Del mismo modo el licenciamiento suele ser de un precio elevado. No obstante la gran ventaja que tiene por sobre las demás herramientas de monitoreo es su bajo consumo de recursos del sistema; así como también el gran respaldo de una compañía como IBM ante cualquier fallo de la herramienta.

Capítulo II

Capítulo 2 IBM Tivoli Netcool Omnibus

2.1 Introducción

Para entender el contexto al cual se hace frente en la implementación de IBM Tivoli Monitoring es necesario conocer la arquitectura completa de Netcool/OMNIbus puesto que éste es el motor principal de todo el ambiente de monitoreo.

IBM Tivoli Netcool/OMNIbus es una solución de monitoreo que permite gestionar los eventos en toda la infraestructura tecnológica del negocio prácticamente en tiempo real.

Tivoli Netcool/OMNIbus ayuda al área de TI a garantizar una alta disponibilidad del servicio de la infraestructura del negocio, sus aplicaciones, servidores, dispositivos y protocolos de red, protocolos de Internet, almacenamiento y dispositivos de seguridad.

Dentro de sus principales características y beneficios se encuentran:

1) Ayuda a incrementar la eficiencia y agilizar la resolución de problemas consolidando las operaciones de TI y las redes en una única solución de gestión.

2) Combina escalabilidad con una arquitectura flexible que ayuda a escalar de pequeños a grandes entornos, con más de 100 millones de sucesos al día en múltiples redes, silos de TI y zonas.

3) Agiliza la resolución al permitir que los operadores ejecuten scripts de resolución automatizados para resolver problemas recurrentes y predecibles.

4) Ayuda a hacer frente a los problemas más críticos, y automatiza el aislamiento y la resolución mediante agentes ligeros personalizables para recopilar sucesos de negocio y tecnológicos prácticamente en tiempo real.

5) Se integra con soluciones de gestión del rendimiento de aplicaciones para que pueda calcular de forma proactiva las experiencias del usuario y el rendimiento en todas las aplicaciones.[20]

El sistema Tivoli Netcool/OMNIbus es adaptable con casi cualquier herramienta. Gracias a esto, la información que maneja el sistema puede ser:

a) Asignada a operadores

   Los operadores de TI son las personas que llevan a cabo las actividades operativas. Entre sus responsabilidades se encuentran: Preparar copias de seguridad y velar para que se realicen las tareas programadas. De igual manera son los encargados del correcto funcionamiento de los sistemas y

[20] Información obtenida de la página de IBM http://www-03.ibm.com/software/products/es/ibmtivolinetcoolomnibus [Junio, 3, 2015]

es a éstos a los que se les debe informar si alguna falla o posible falla pudiera presentarse.

b) Enviada a sistemas HelpDesk

La mesa de ayuda o help desk es un conjunto de servicios destinados a la gestión y solución de todas las posibles incidencias relacionadas con las tecnologías de la información y comunicación. Con la mesa de ayuda se puede recibir reportes de fallos, consultas de información o resolución de dudas y seguimiento de problemas. Son precisamente los encargados de canalizar los problemas para que estos puedan ser solucionados.

c) Almacenada en alguna Base de Datos

Los problemas recurrentes pueden ser enviados a una base de datos para poder ser analizados posteriormente por el área de TI y buscar una solución que los evite.

d) Puede desencadenar respuestas automáticas a ciertos eventos.

La herramienta IBM Tivoli Monitoring, por medio de los agentes, tiene la posibilidad de ejecutar scripts cuando determinada situación se presente. Por ejemplo, si el disco duro de un servidor comienza a rebasar un umbral determinado, ITM activa una alerta la cual manda a ejecutar un script; en este caso el script podría ejecutar una compresión de logs a manera de liberar espacio en disco.

2.2 Arquitectura Netcool Omnibus

Los componentes de Tivoli Netcool Omnibus trabajan en conjunto para que los operadores de la herramienta puedan visualizar la información de los eventos de red. La herramienta de monitoreo realiza principalmente dos tareas, las cuales son fundamentales para el monitoreo, recoger y gestionar eventos.

En la siguiente imagen (Figura 2.1) se muestra la arquitectura básica de todos los componentes que conforman la arquitectura de Netcool Omnibus.

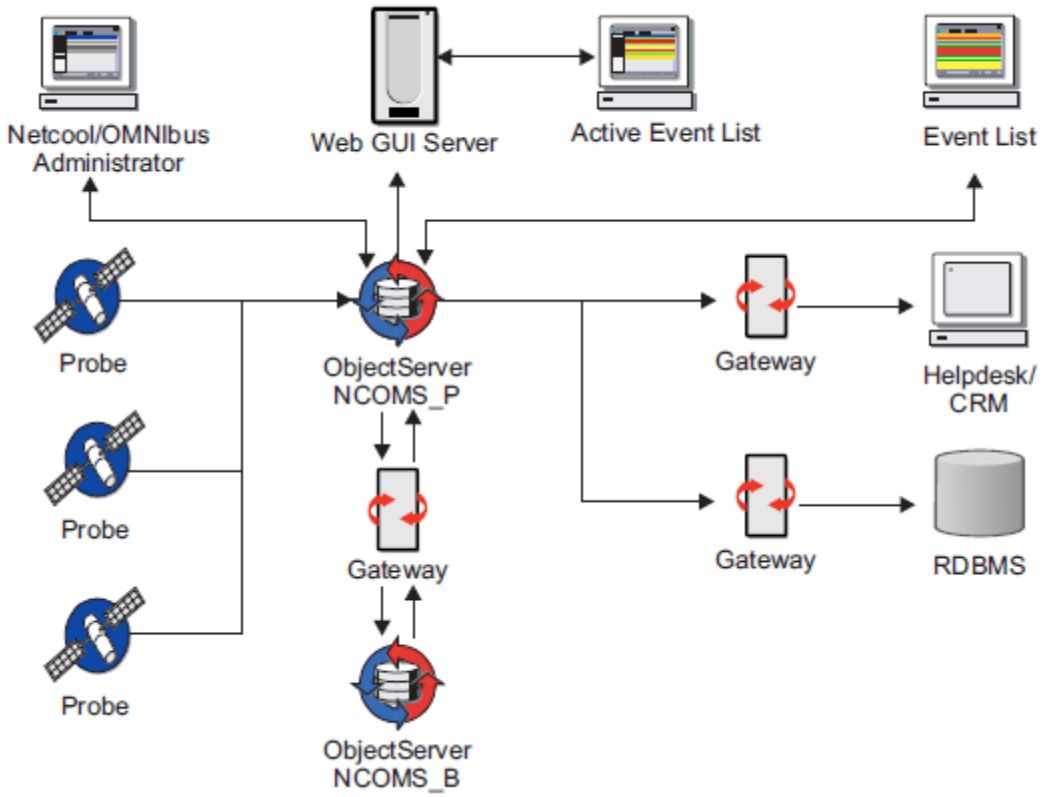


Fig. 2.1 Arquitectura Omnibus/Netcool.

A continuación se describen cada uno de estos componentes a fin de entender el funcionamiento de esta arquitectura.

2.2.1 El ObjectServer

El componente central de esta arquitectura es el llamado objectServer. Es el servidor de base de datos, núcleo de toda la implementación.

Los probes y los gateways envían información referente de los eventos de la red al objectServer. Éste se encarga de almacenar y administrar en su base de datos dichos eventos para posteriormente mostrar esta información en la Event List ya sea vía web o en la aplicación de escritorio.

Las principales cualidades del objectServer son la deduplicación (cada que se almacena un archivo, se descompone en partes, y a cada parte se le asocia un identificador único, que se almacena en un índice. El objetivo es almacenar una sola vez la misma parte de un archivo. Cada vez que se localiza una parte

idéntica, se reemplaza por un puntero hacia el identificador correspondiente[21]) y la automatización.

Un solo dispositivo puede generar el mismo error varias veces hasta que el problema se resuelve. El objectServer se asegura de que la información de los eventos no se duplique en la eventList guardando un conteo del número total de ocurrencias.

De igual manera se utiliza la automatización para crear respuestas automáticas cuando algún evento determinado ocurra. Todo esto sin necesidad de la intervención de algún operador.

2.2.2 Probes

Los probes o sondas, se conectan a una fuente de eventos detectan y recolectan los datos de los eventos para posteriormente enviarlos al objectServer.

Los probes obedecen a una lógica que se encuentra especificada en un archivo de reglas. Con base en dichas reglas, el probe es capaz de manipular los elementos de los eventos para así convertirlos en los campos de la tabla alert.status. De esta manera los probes únicamente pueden captar un determinado tipo de eventos provenientes de una fuente específica.

Los archivos de reglas de los probes tienden a personalizarse de tal manera que pueden obtener datos de cualquier fuente de datos estable, incluidos dispositivos, bases de datos y archivos de registro. Los probes también se pueden configurar para modificar y añadir datos a los eventos.

2.2.3 Gateways

Los gateways o puertas de enlace permiten el intercambio de eventos entre objectServers y aplicaciones de terceros, tales como bases de datos y servicios de asistencia.

Los gateways sirven para replicar eventos o para mantener una copia de seguridad de un objectServer. Así mismo permiten integrar diferentes funciones de la empresa. Por ejemplo, se puede configurar un gateway para enviar información de eventos a un sistema de mesa de ayuda. De igual manera se puede configurar el Gateway para guardar los eventos en una base de datos.

[21] Philippe G. (2010). Virtualización de sistemas de información con VMware. Barcelona, España: Ediciones ENI. p. 237.

2.2.4 Desktop Tools

Las Desktop Tools son un conjunto integrado de herramientas gráficas utilizadas para ver y gestionar eventos y para configurar la manera en que se presentará la información de un evento.

La idea principal de estas herramientas es el poder presentar la información relacionada con el evento de una forma entendible para el operador de tal manera que pueda identificar rápidamente la disponibilidad de servicios.

La mayor parte de estas herramientas se encuentran disponibles en el componente Web GUI. Desde este se puede acceder a la lista de eventos donde se pueden visualizar todas las alertas de la arquitectura monitoreada.

2.2.5 Netcool/OMNIbus

Toda herramienta robusta tiene como buena práctica un ambiente desde el cual se pueden configurar los diversos parámetros mediante los cuales funciona dicha herramienta. Este es el caso de Netcool/OMNIbus.

Esta es la interfaz de usuario desde la cual se gestiona todo el entorno de Netcool/OMNIbus a nivel administrador. Las reglas de almacenamiento de las alertas. Los umbrales para diferenciar los tipos de alertas, el color de las mismas.

Se puede administrar el rol de los usuarios. Crear o eliminar usuarios. El nivel de permisos que puede tener cada usuario. Las alertas que pueden visualizar.

2.2.6 Helpdesk /CRM

El Help Desk (Mesa de ayuda) es uno de los puntos clave de contacto con los clientes, es a veces el lugar donde se decide si va a seguir haciendo negocios con el cliente no. Los help desk siempre han brindado servicios más rápidos, seguimiento y resolución de problemas.

En un help desk se establecen diferentes niveles de soporte lo que hace que las preguntas más simples puedan automatizarse mientras que las más complejas serán respondidas por representantes más calificados.[22]

El objectServer puede enviar la información de las alertas a una mesa de ayuda de tal forma que se le dé solución inmediata a los problemas que pueden surgir. Esto se hace a través de un gateway. Una vez que el help desk ha obtenido la información de la falla, estos pueden canalizar el problema con la persona más capacitada que pueda darle solución al problema.

[22] Carranza O. & Sabría F. (2004). Logística: mejores prácticas en latinoamérica. México: Thomson. p.57

2.2.7 RDBMS

El objectServer tiene la capacidad de enviar la información a una RDBMS (Relational Database Management System – Sistema de Gestión de Base de Datos Relacional) a través de un Gateway.

Las ventajas de las RDBSM son:

a) Puede trabajar con más de una tabla a la vez y extraer información de dos tablas según un campo en común.

b) Añadir nuevos datos.

c) Editar datos almacenados.

d) Eliminar información.

e) Buscar y recuperar información.

f) Organizar y visualizar la DB de formas diferentes.

g) Diseñar o imprimir informes que listen, agrupen o resuman la información almacenada.[23]

2.3 Integración de Netcool Omnibus con IBM Tivoli Monitoring

Para integrar el monitoreo proveniente de IBM Tivoli Monitoring con las alertas de Netcool Omnibus a fin de tener las alertas de todos los sistemas en una sola consola, es necesario, instalar un probe que interprete las alertas que llegan a IBM Tivoli Monitoring.

Para este fin, IBM desarrolló un probe que es capaz de organizar la gran variedad de alertas que IBM Tivoli Monitoring gestiona. Este probe ya contiene el archivo de reglas necesario para la comunicación con el objectServer de Netcool Omnibus.

Este software se puede encontrar con el nombre de IBM Tivoli Netcool/OMNIbus Probe for Tivoli EIF (Event Integration Facility - facilitador de integración de eventos).

La instalación consiste en descargar el paquete de instalación correspondiente al sistema operativo en el cual se está integrando la solución, así como también se debe verificar que el Probe for Tivoli EIF sea compatible con la versión de Netcool Omnibus que se está ejecutando.[24]

Para comenzar a hablar de la implementación que se realizó, es necesario, en primera instancia, describir la herramienta. A continuación se describe el software de

[23] Gómez A. & De Abajo N.. (1997). Los sistemas de información en la empresa. Oviedo, España.: Servicio de publicaciones de la Universidad de Oviedo. p. 86

[24] IBM® Tivoli® Netcool/OMNIbus Probe for Tivoli EIF Version 13.0 Reference Guide November 8, 2013

monitoreo IBM Tivoli Monitoring para posteriormente entrar al detalle de la implementación.

2.4 Descripción de la herramienta IBM Tivoli Monitoring

Los productos de IBM Tivoli Monitoring supervisan el rendimiento y la disponibilidad de los sistemas operativos y sus aplicaciones. Estos productos se basan en un conjunto de componentes de servicios comunes, denominados conjuntamente Tivoli Management Services. Los componentes de Tivoli Management Services proporcionan la seguridad, la transferencia y el almacenamiento de datos, los mecanismos de notificación, la presentación de interfaz de usuario y los servicios de comunicaciones en una arquitectura de agente-servidor-cliente.[25]

Estos servicios son compartidos por un número de otros productos, entre los que se incluye productos de supervisión del sistema principal IBM Tivoli OMEGAMON XE y productos IBM Tivoli Composite Application Manager, así como otros productos de IBM Tivoli Monitoring tales como: Tivoli Monitoring for Applications, Tivoli Monitoring for Business Integration, Tivoli Monitoring for Cluster Managers, Tivoli Monitoring for Databases, Tivoli Monitoring for Energy Management, Tivoli Monitoring for Messaging and Collaboration, Tivoli Monitoring for Microsoft. NET, Tivoli Monitoring for Microsoft Applications, Tivoli Monitoring for Transaction Performance, Tivoli Monitoring for Virtual Servers y Tivoli Monitoring for Web Infrastructure.

Las principales características de Tivoli Monitoring son las siguientes:

a) Se trata de una solución inmediata para supervisar sistemas Windows®, UNIX®, Linux y OS/400®.La colección de datos y el análisis de problemas se realizan localmente en el sistema.

b) Modelos de recurso (conjuntos de características sobre un aspecto del sistema operativo como discos duros, procesos, memoria RAM, parámetros TCP/IP, etc.) listos para utilizarse en la redacción de informes sobre aspectos determinados del estado de un sistema. Por ejemplo, el modelo de recurso Proceso proporciona información acerca del estado de los procesos que están corriendo en el sistema, la utilización de la CPU, etc. La supervisión de recursos es una implementación del Common Information Model (CIM). CIM es un método de gestión de sistemas y redes que aplica técnicas orientadas a objetos para modelar el sistema.

c) Modelos de recurso también pueden agregarse fácilmente al perfil de la consola de IBM Tivoli Monitoring y que pueden distribuirse a varios sistemas simultáneamente.

[25] Información obtenida de la página de IBM http://www-01.ibm.com/support/knowledgecenter/SSDKXQ_6.3.0/com.ibm.itm.doc_6.2.2/itm_install06.htm%23itm_over?lang=es [Junio,16 2015]

d) Tiene la posibilidad de modificar modelos de recurso cambiando, por ejemplo, los niveles de umbral para ajustarlos a necesidades específicas.

e) Cuenta con la posibilidad de visualizar tanto los datos históricos como los datos en tiempo real para cualquier sistema desde una aplicación de supervisión centralizada llamada Consola de estado de Web, que se proporciona junto con el producto.

f) Puede enviar los resultados de la colección y análisis de datos a Tivoli Enterprise Console o a Tivoli Business Systems Manager.

g) Puede especificar acciones correctivas o preventivas para resolver situaciones que podrían derivar en problemas reales.

h) Cuenta con una función de planificación que permite que la supervisión se produzca en momentos especificados por el usuario.

i) Tiene una de latido que se ejecuta en gateways y comprueba regularmente la disponibilidad y el estado de los puntos finales adjuntos, enviando la información al servidor Tivoli Enterprise Console, a Tivoli Business Systems Manager o al Grupo de avisos de Tivoli Monitoring.[26]

A continuación se detalla la arquitectura básica de IBM Tivoli Monitoring y sus características.

2.5 Arquitectura estándar de IBM Tivoli Monitoring

Un entorno de IBM Tivoli Monitoring típico está formado por los siguientes componentes:

1) Uno o varios servidores de Tivoli Enterprise Monitoring, que actúan como una recopilación y punto de control de las alertas recibidas de agentes (se llama agente al software que se instala en el servidor que se desea monitorear), y recopilan los datos de rendimiento y disponibilidad. El servidor de supervisión también gestiona el estado de conexión de los agentes. Un servidor de cada entorno debe estar designado como *concentrador*.

2) Un Servidor de Tivoli Enterprise Portal, que proporciona la capa de presentación central para la recuperación, manipulación, análisis y formato previo de datos. El servidor de portal recupera datos del servidor de supervisión (encargado de concentrar las alertas recibidas por los agentes) como respuesta de las acciones del usuario en el cliente del portal y devuelve los datos para su presentación. El servidor del portal también proporciona información de presentación al cliente del portal para que pueda representar las vistas de la interfaz de usuario de manera correcta.

[26] IBM Tivoli Monitoring Guía del Usuario.

3) Uno o varios clientes de Tivoli Enterprise Portal, con una interfaz de usuario basada en Java para ver y supervisar la empresa. Tivoli Enterprise Portal ofrece dos modalidades de funcionamiento: escritorio y navegador.

4) Agentes de Tivoli Enterprise Monitoring, instalados en los sistemas o subsistemas que desea supervisar. Estos agentes recopilan datos de sistemas supervisados o gestionados y distribuyen esta información a un servidor de supervisión o a un recopilador de sucesos SNMP como IBM Tivoli Netcool/OMNIbus.

5) Sólo z/OS: Tivoli Management Services:Engine (TMS:Engine) proporciona funciones comunes como, por ejemplo, comunicaciones, servicios de tiempo de ejecución de múltiples hebras, diagnósticos (vuelcos) y registro (RKLVLOG), para el servidor de Tivoli Enterprise Monitoring, agentes de supervisión y componentes de OMEGAMON de productos OMEGAMON XE que se ejecutan en z/OS.

6) El servidor de ayuda de Eclipse para presentar la ayuda para el portal y todos los agentes de supervisión para los que se ha instalado el soporte.

Opcionalmente la instalación también incluye los siguientes componentes:

7) Tivoli Data Warehouse para almacenar datos históricos recopilados de agentes del entorno. El almacén de datos está ubicado en una base de datos IBM DB2 para Linux, UNIX y Windows, DB2 en z/OS, Oracle o Microsoft SQL. Para almacenar los datos en esta base de datos, se debe instalar el agente de proxy de almacén. Para realizar las funciones de agregación y poda (técnica de exploración en la cual existe una cola de prioridad que es la encargada de elegir qué nodo es más prometedor y analizar la ramificación en ese orden) en los datos también se debe instalar el agente de resumen y poda.

8) El componente de sincronización de sucesos, Event Integration Facility, que envía actualizaciones a los sucesos de situación que se han reenviado a un servidor de sucesos de Tivoli Enterprise Console o un Netcool/OMNIbus ObjectServer de vuelta al servidor de supervisión.

9) Tivoli Performance Analyzer añade la función de predicción con Tivoli Monitoring, para que pueda supervisar las tendencias de consumo de recursos, prever los problemas de rendimiento en el futuro y evitar o resolver problemas de forma más rápida.

En la siguiente figura (Figura 2.2) se pueden ver los componentes antes mencionados para visualizar la comunicación que existe entre ellos.

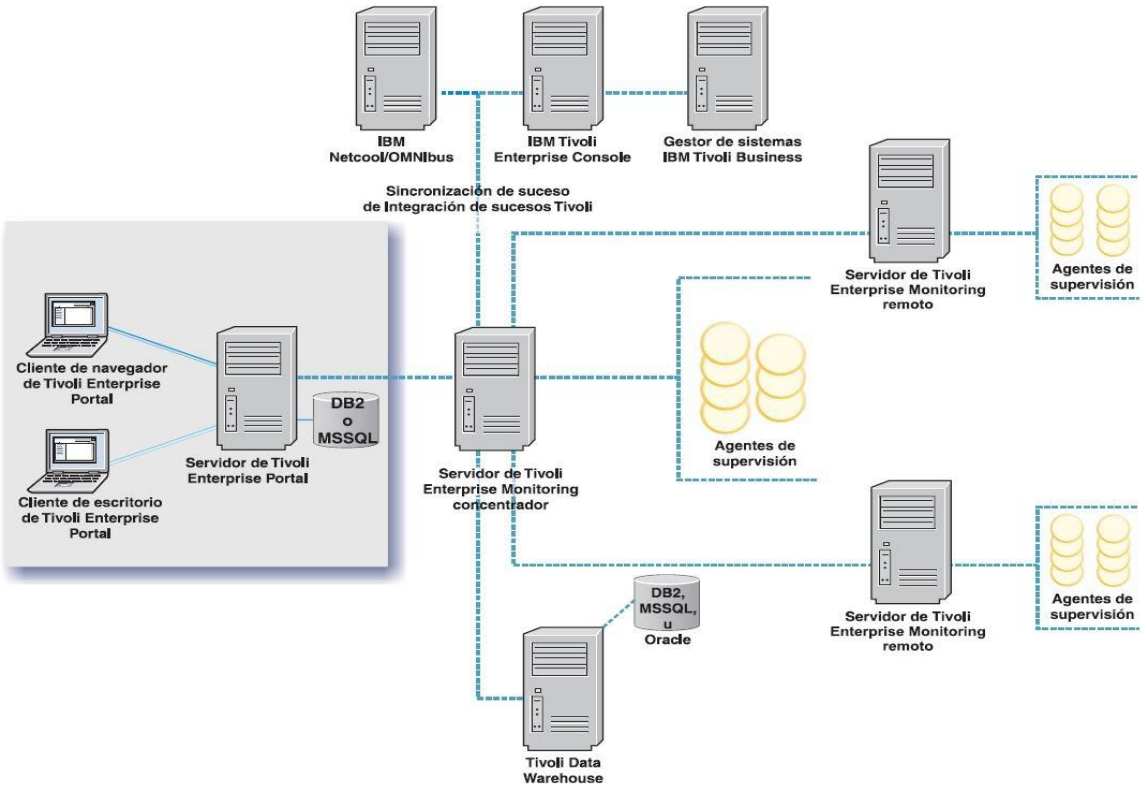


Fig.2.2 Arquitectura estándar de ITM.

Capítulo 3
IBM Tivoli Monitoring

3.1 Introducción.

En este capítulo se hablará a fondo de la arquitectura implementada en una infraestructura tecnológica general. En esta infraestructura se están considerando tres sistemas operativos que comúnmente se encuentran en la industria, Windows, Unix y Linux.

De igual forma se están considerando algunas de las aplicaciones más comunes que corren sobre estos sistemas operativos antes descritos, es decir, bases de datos, aplicaciones de virtualización, aplicaciones de correo electrónico, entre otros.

3.2 Arquitectura ITM Implementada.

En la siguiente imagen (Figura 3.1) se presenta la arquitectura de la instalación de la solución de ITM en un entorno empresarial. En esta arquitectura se pueden visualizar los agentes instalados así como también los servidores involucrados en la solución. Cada herramienta se instala en un servidor por separado debido a que en un entorno empresarial la carga de trabajo es grande.

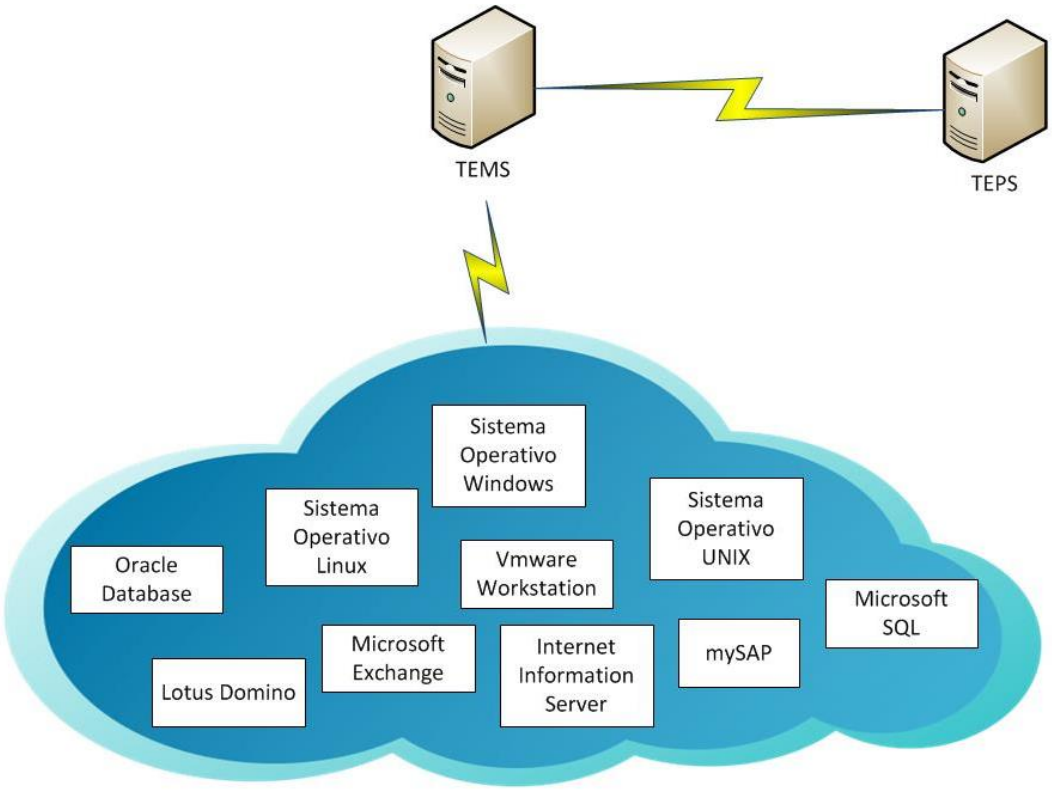


Fig. 3.1 Arquitectura de la implementación de ITM.

3.2.1 Servidor TEMS

El primer paso para la implementación de esta arquitectura es instalar el Servidor de Tivoli Enterprise Monitoring (TEMS por sus siglas en inglés). A este servidor se le denomina servidor de supervisión. Es el corazón de toda la arquitectura ya que de él dependen directamente todos los demás componentes de la arquitectura.

Este servidor se encarga de la recopilación y control de todos los datos y alertas de rendimiento y disponibilidad recibidos de los agentes de supervisión. Es indispensable pues informa del estado “en línea” (online) o “fuera de línea” (offline) de los agentes de supervisión.

Cabe mencionar que en la arquitectura estándar que se mostró anteriormente (Figura 3.1) podemos visualizar 3 servidores TEMS. En el caso especial de esta implementación únicamente es necesario instalar un servidor TEMS puesto que la carga de trabajo de este no será excesiva.

3.2.1.1 Instalación TEMS

Se realiza la instalación del servidor TEMS versión 6.2.3.1 vía un cliente de conexiones remotas SSH llamado XShell de XManager. El cual me permite ingresar al servidor de una forma segura y simple a través de una línea de comandos.

Como primer requisito, es necesaria la creación de un usuario llamado “netcool”. Éste se encargará de gestionar la aplicación de TEMS.

El servidor tiene una instalación del sistema operativo Linux, Red Hat 5.4.

Para iniciar la instalación es necesario ingresar al servidor con el usuario netcool previamente creado. Se dirige al paquete de instalación y se ejecuta el archivo “install.sh” (Figura 3.2).

```
[netcool@TEMS ~]$ cd /repo/ITM/
[netcool@TEMS ITM]$ ll
total 2172744
drwxrwxrwx 2 root root       4096 Feb 24  2012 Deploy
-rwxrwxrwx 1 root root       1288 Feb 24  2012 DeployLnk.sh
drwxrwxrwx 3 root root       4096 Feb 24  2012 InstallITM
-rwxrwxrwx 1 root root     149930 Feb 24  2012 install.sh
-rw-r--r-- 1 root root 2222254722 May 31 10:24 ITM_6.2.3_FIXPACK_1_BASE_LIN_ENG.tar.gz
-rwxrwxrwx 1 root root        734 Feb 24  2012 kcirunas.cfg
drwxrwxrwx 2 root root       4096 Feb 24  2012 license
-rwxrwxrwx 1 root root       2260 Feb 24  2012 non_ibm_license
-rwxrwxrwx 1 root root     248498 Feb 24  2012 notices
-rwxrwxrwx 1 root root        334 Feb 24  2012 README.TXT
-rwxrwxrwx 1 root root       6014 Feb 24  2012 silent_config.txt
-rwxrwxrwx 1 root root       6148 Feb 24  2012 silent_install.txt
drwxrwxrwx 5 root root       4096 Feb 24  2012 unix
[netcool@TEMS ITM]$ ./install.sh
```

Fig. 3.2 Paquete de instalación

Como todo programa de software, la instalación del TEMS da la opción de elegir la ruta de instalación la cual, en este caso, se deja por default (Figura 3.3). Así mismo pide aceptar el acuerdo de licencia (Figura 3.4).

```
Enter the name of the IBM Tivoli Monitoring directory
[ default = /opt/IBM/ITM ]:
```

Fig. 3.3 Directorio de Instalación

```
Please enter a valid number:  1

Initializing ...
International Program License Agreement

Part 1 - General Terms

BY DOWNLOADING, INSTALLING, COPYING, ACCESSING, CLICKING ON
AN "ACCEPT" BUTTON, OR OTHERWISE USING THE PROGRAM,
LICENSEE AGREES TO THE TERMS OF THIS AGREEMENT. IF YOU ARE
ACCEPTING THESE TERMS ON BEHALF OF LICENSEE, YOU REPRESENT
AND WARRANT THAT YOU HAVE FULL AUTHORITY TO BIND LICENSEE
TO THESE TERMS. IF YOU DO NOT AGREE TO THESE TERMS,

* DO NOT DOWNLOAD, INSTALL, COPY, ACCESS, CLICK ON AN
"ACCEPT" BUTTON, OR USE THE PROGRAM; AND

* PROMPTLY RETURN THE UNUSED MEDIA, DOCUMENTATION, AND

Press Enter to continue viewing the license agreement, or
enter "1" to accept the agreement, "2" to decline it, "3"
to print it, "4" to read non-IBM terms, or "99" to go back
to the previous screen.
1
```

Fig. 3.4 Acuerdo de licencia

Dentro del paquete de instalación se encuentran diferentes aplicaciones disponibles para instalar, por lo que se debe elegir la aplicación correcta, en este caso, TEMS (Figura 3.5).

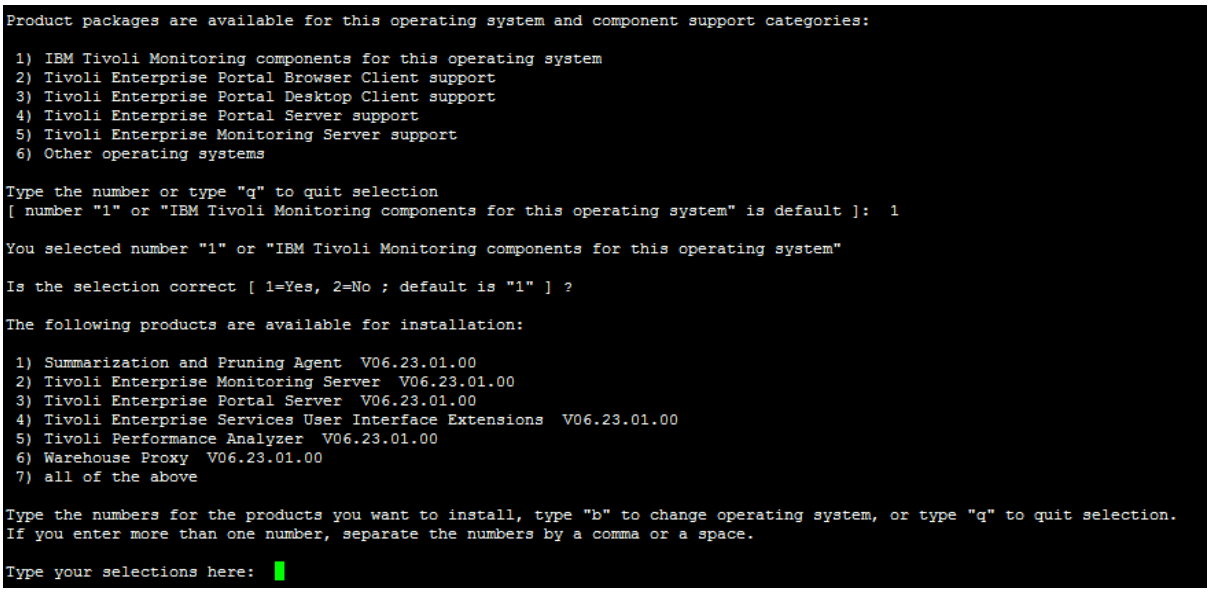


Fig. 3.5 Elección del producto TEMS V6.2.3.1

Finalmente comienza la instalación del servidor TEMS y permite la opción de elegir un nombre para éste (debido a que en una arquitectura más robusta pueden existir más de un servidor TEMS, se da la opción de cambiar el nombre para diferenciarlos). En este caso se selecciona el nombre por default, TEMS. (Figura 3.6).

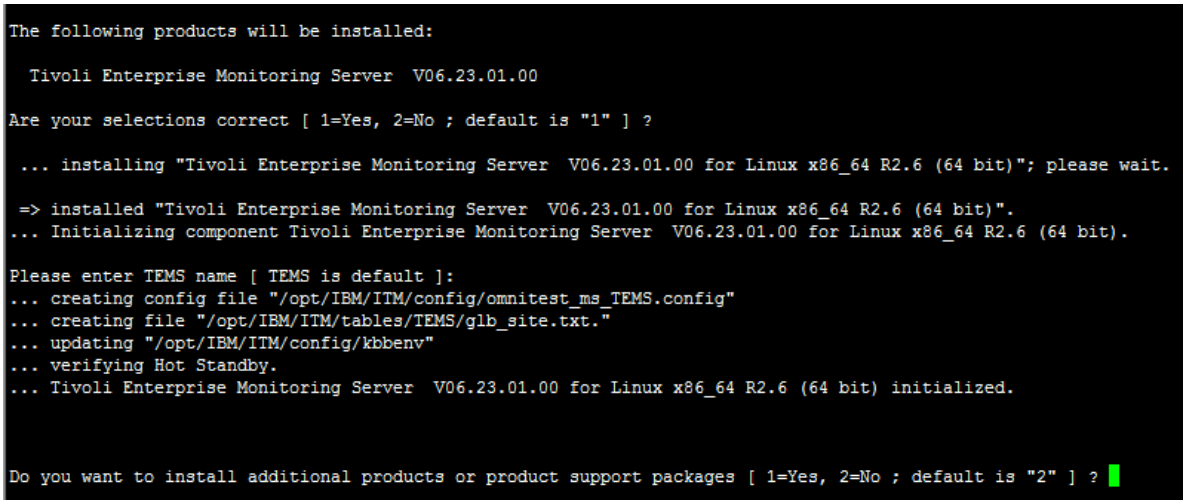


Fig. 3.6 Instalación TEMS V6.2.3.1

Adicionalmente a todo lo anterior, se necesita instalar una serie de soportes para que el servidor TEMS pueda interpretar la información recibida de los agentes. Por tal motivo cada agente de monitoreo que se instale en la arquitectura, requiere que también se instale su soporte correspondiente dentro del servidor TEMS (Figura 3.7).

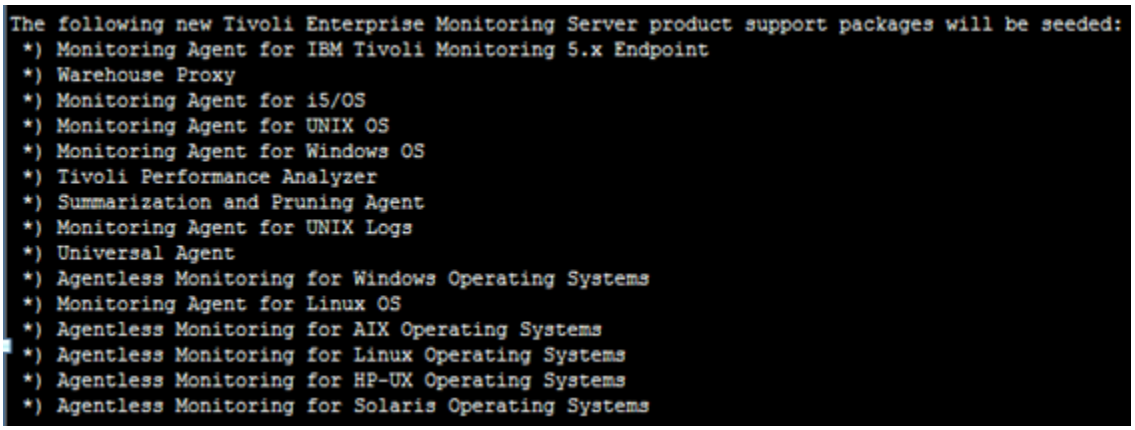


Fig. 3.7 Soportes TEMS

Finalmente la instalación es completada y hace mención de que se debe configurar al producto recientemente instalado.

3.2.1.2 Configuración TEMS

Para configurar e iniciar el servicio se ingresa a la ruta de instalación y se ejecuta el comando “itmcmd” con el parámetro “manage” como se muestra en la siguiente figura (Figura 3.8).

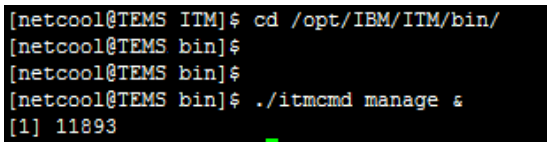


Fig. 3.8 Ejecución del comando itmcmd.

En la siguiente imagen (Figura 3.9) se aprecia la ventana del manejador de servicios de IBM Tivoli Monitoring. Se selecciona Tivoli Enterprise Monitoring Server, se da clic derecho sobre él y se elige configurar.

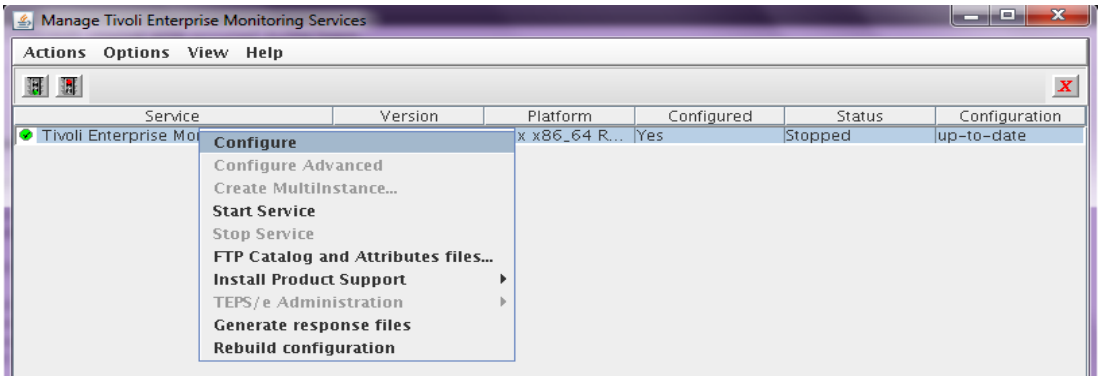


Fig. 3.9 Manejador de Servicios.

La configuración prácticamente se deja por default. Únicamente se ingresa el nombre del TEMS que se definió en la instalación y el nombre del servidor (Host Name), que en este caso también se definió como TEMS. El número de puerto utilizado es el que trae por default (1918). Este puerto es muy importante ya que a través de él se realizan todas las conexiones, tanto con los agentes de monitoreo como con el servidor TEPS (Figura 3.10).

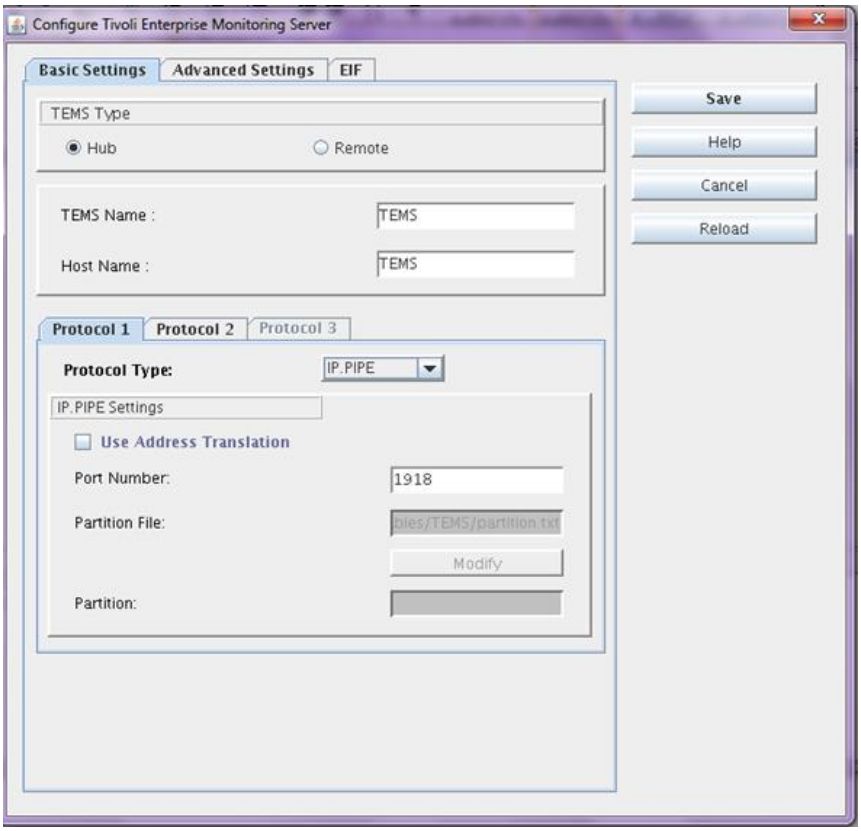


Fig. 3.10 Ventana de configuración.

Se guarda la configuración y en automático regresa al Manejador de Servicios. Se da clic derecho sobre el TEMS y se elige la opción “Start Service” para ejecutarlo (Figura 3.11).

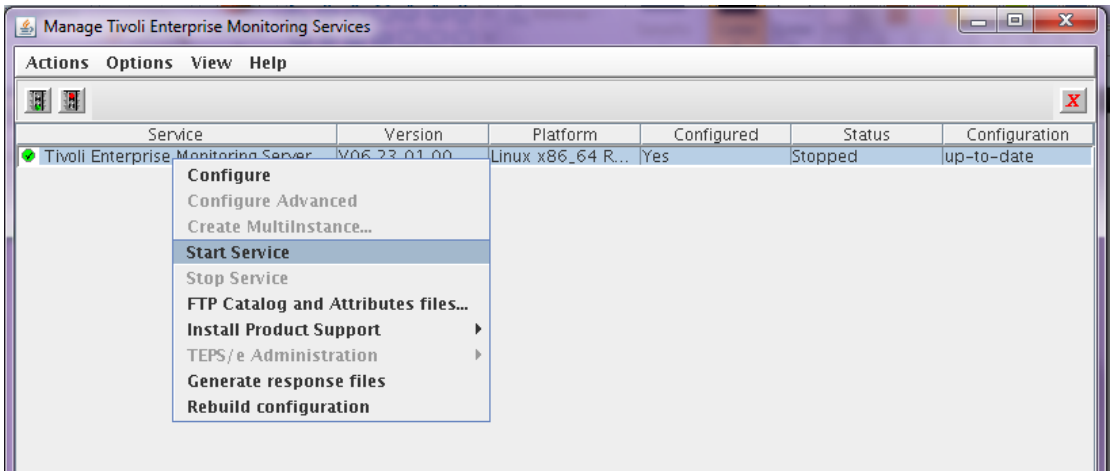


Fig. 3.11 Inicio del TEMS.

3.2.2 Servidor TEPS

El Servidor de Tivoli Enterprise Portal (TEPS) es el encargado de gestionar el acceso a los datos del TEMS mediante las consolas de espacio de trabajo de usuario.

A estas consolas se puede acceder de 2 maneras:

- Vía WEB.
  La interfaz del cliente de navegador se instala por defecto al instalar el TEPS. Y se puede acceder a través del navegador Microsoft Internet Explorer o Mozilla Firefox.

- Cliente de escritorio.
  Es una interfaz gráfica basada en java que se puede instalar en cualquier computadora personal con sistema operativo Windows o Linux.

3.1.2.1 Instalación TEPS

Para la instalación del TEPS fue necesario contar con anterioridad con una base de datos, en este caso se eligió DB2 versión 9.7. Se realizó una instalación típica de dicha base de datos, es decir, se eligieron los parámetros por default:

DB2 Administration Server
User name: **dasusr1**
Group name: **dasadm1**

Instance owner
User name: **db2inst1**
Group name: **db2iadm1**

Al igual que con el servidor TEMS, fue necesaria la creación del usuario netcool para la administración e instalación de la aplicación. El paquete para la instalación del servidor TEPS es el mismo que el del servidor TEMS. Se ingresa a la carpeta y se ejecuta el archivo install.sh (Figura 3.12).

```
[netcool@TEPS ~]$ cd /repo/ITM/
[netcool@TEPS ITM]$ ll
total 2172744
drwxrwxrwx 2 root root       4096 Feb 24  2012 Deploy
-rwxrwxrwx 1 root root       1288 Feb 24  2012 DeployLnk.sh
drwxrwxrwx 3 root root       4096 Feb 24  2012 InstallITM
-rwxrwxrwx 1 root root     149930 Feb 24  2012 install.sh
-rw-r--r-- 1 root root 2222254722 May 31 10:24 ITM_6.2.3_FIXPACK_1_BASE_LIN_ENG.tar.gz
-rwxrwxrwx 1 root root        734 Feb 24  2012 kcirunas.cfg
drwxrwxrwx 2 root root       4096 Feb 24  2012 license
-rwxrwxrwx 1 root root       2260 Feb 24  2012 non_ibm_license
-rwxrwxrwx 1 root root     248498 Feb 24  2012 notices
-rwxrwxrwx 1 root root        334 Feb 24  2012 README.TXT
-rwxrwxrwx 1 root root       6014 Feb 24  2012 silent_config.txt
-rwxrwxrwx 1 root root       6148 Feb 24  2012 silent_install.txt
drwxrwxrwx 5 root root       4096 Feb 24  2012 unix
[netcool@TEPS ITM]$ ./install.sh
```

Fig. 3.12 Paquete de instalación del TEPS.

Al igual que en la instalación del TEMS da a elegir la ruta de instalación, la cual se deja por default (Figura 3.13). Así mismo pide aceptar el acuerdo de licencia (Figura 3.14).

```
Enter the name of the IBM Tivoli Monitoring directory
[ default = /opt/IBM/ITM ]:
```

Fig. 3.13 Directorio de Instalación

```
Please enter a valid number:  1

Initializing ...
International Program License Agreement

Part 1 - General Terms

BY DOWNLOADING, INSTALLING, COPYING, ACCESSING, CLICKING ON
AN "ACCEPT" BUTTON, OR OTHERWISE USING THE PROGRAM,
LICENSEE AGREES TO THE TERMS OF THIS AGREEMENT. IF YOU ARE
ACCEPTING THESE TERMS ON BEHALF OF LICENSEE, YOU REPRESENT
AND WARRANT THAT YOU HAVE FULL AUTHORITY TO BIND LICENSEE
TO THESE TERMS. IF YOU DO NOT AGREE TO THESE TERMS,

* DO NOT DOWNLOAD, INSTALL, COPY, ACCESS, CLICK ON AN
"ACCEPT" BUTTON, OR USE THE PROGRAM; AND

* PROMPTLY RETURN THE UNUSED MEDIA, DOCUMENTATION, AND

Press Enter to continue viewing the license agreement, or
enter "1" to accept the agreement, "2" to decline it, "3"
to print it, "4" to read non-IBM terms, or "99" to go back
to the previous screen.
1
```

Fig. 3.14 Acuerdo de licencia

Como ya se vio, dentro del paquete de instalación se encuentran diferentes aplicaciones disponibles para instalar, en este caso se selecciona la opción 3) Tivoli Enterprise Portal Server V06.23.01.00. (Figura 3.15).

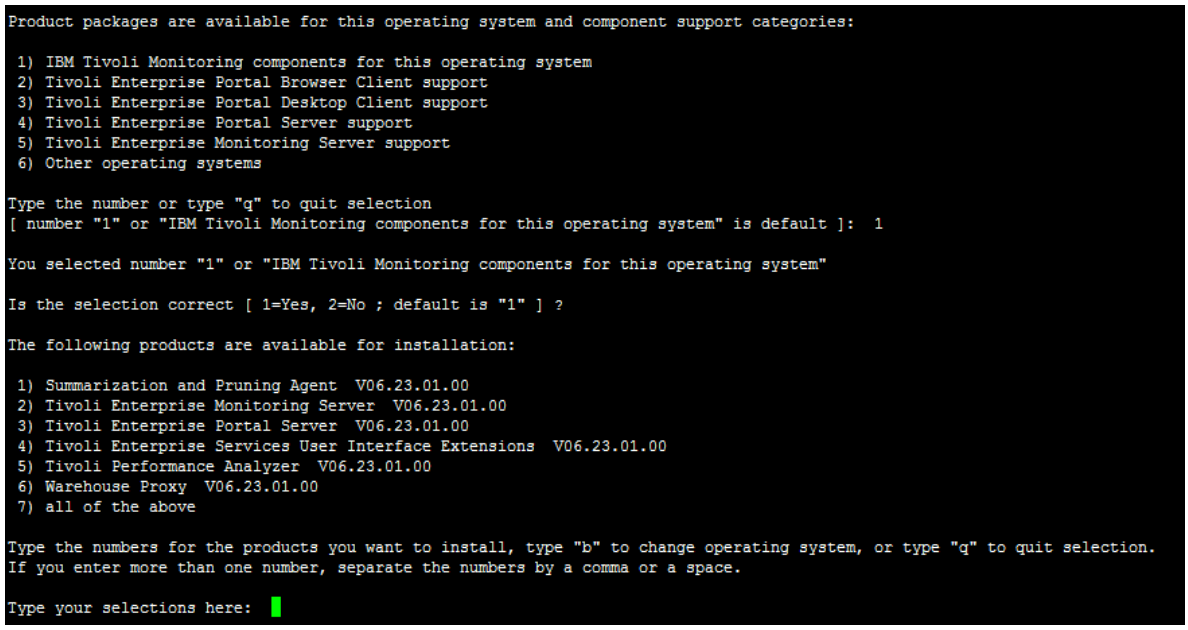


Fig. 3.15 Elección del producto TEPS V6.2.3.1

Al seleccionar el producto, pide la confirmación de que el producto es el correcto e inmediatamente comienza la instalación. Así mismo informa que instalará IBM Eclipse Help Server como prerrequisito (Figura 3.16).

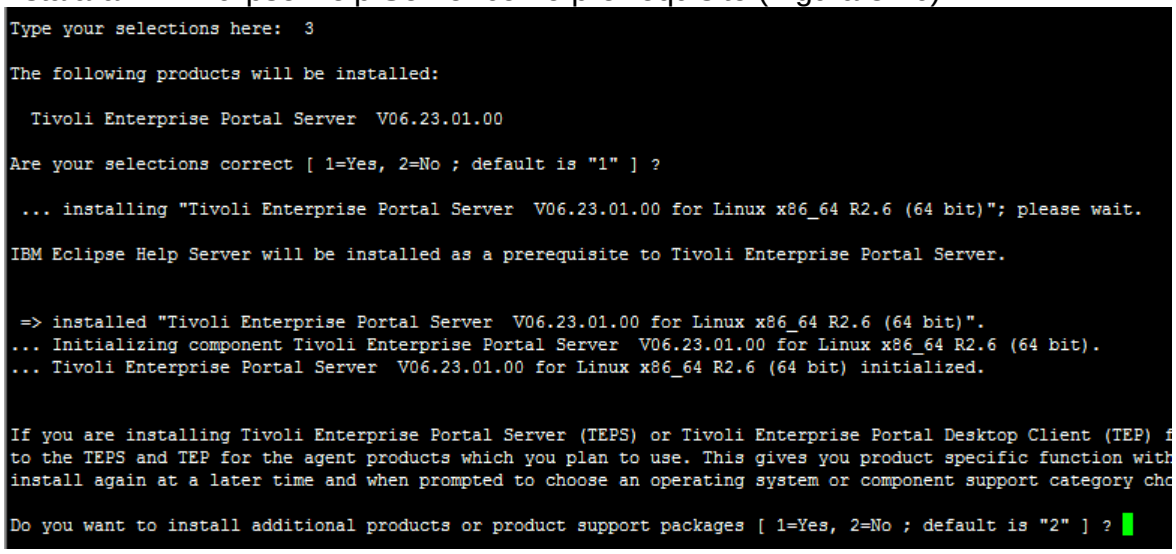


Fig. 3.16 Proceso de instalación de TEPS V6.2.3.1

También es necesario instalar los soportes para que los agentes de monitoreo puedan ser mostrados tanto en el portal web como en la aplicación de escritorio (Figura 3.17).

```
If you are installing Tivoli Enterprise Portal Server (TEPS) or Tivoli Enterprise Portal Desktop Client (TEP) for the first time you will probably want
to install product support to the TEPS and TEP for the agent products which you plan to use. This gives you product specific function within the TEP.
To install support packages choose yes below or run the install again at a later time and when prompted to choose an operating system or component
support category choose the appropriate support category.

Do you want to install additional products or product support packages [ 1=Yes, 2=No ; default is "2" ] ? 1

Product packages are available for this operating system and component support categories:

 1) IBM Tivoli Monitoring components for this operating system
 2) Tivoli Enterprise Portal Browser Client support
 3) Tivoli Enterprise Portal Desktop Client support
 4) Tivoli Enterprise Portal Server support
 5) Tivoli Enterprise Monitoring Server support
 6) Other operating systems

Type the number or type "q" to quit selection
[ number "1" or "IBM Tivoli Monitoring components for this operating system" is default ]:  4

You selected number "4" or "Tivoli Enterprise Portal Server support"

Is the selection correct [ 1=Yes, 2=No ; default is "1" ] ? 1

The following application supports are available for installation:

 1) Agentless Monitoring for AIX Operating Systems  V06.23.01.00
 2) Agentless Monitoring for HP-UX Operating Systems  V06.23.01.00
 3) Agentless Monitoring for Linux Operating Systems  V06.23.01.00
 4) Agentless Monitoring for Solaris Operating Systems  V06.23.01.00
 5) Agentless Monitoring for Windows Operating Systems  V06.23.01.00
 6) Monitoring Agent for IBM Tivoli Monitoring 5.x Endpoint  V06.23.01.00
 7) Monitoring Agent for Linux OS  V06.23.01.00
 8) Monitoring Agent for UNIX Logs  V06.23.01.00
 9) Monitoring Agent for UNIX OS  V06.23.01.00
10) Monitoring Agent for Windows OS  V06.23.01.00
11) Monitoring Agent for i5/OS  V06.23.01.00
12) Summarization and Pruning Agent  V06.23.01.00
13) TEC GUI Integration  V06.23.01.00
14) Tivoli Performance Analyzer  V06.23.01.00
15) Universal Agent  V06.23.01.00
16) Warehouse Proxy  V06.23.01.00
17) all of the above

Type the numbers for the products you want to install, type "b" to change operating system, or type "q" to quit selection.
If you enter more than one number, separate the numbers by a comma or a space.

Type your selections here:  17
```

Fig. 3.17 Instalación de los soportes para TEPS V6.2.3.1

Al terminar la instalación de estos soportes hace mención de que es necesario configurar el TEPS.

3.2.2.2 Configuración TEPS

Para iniciar la configuración es necesario ingresar al directorio de instalación y ejecutar la aplicación “itmcmd” con el parámetro “manage” (Figura 3.18).

```
[root@TEPS ~]# cd /opt/IBM/ITM/bin/
[root@TEPS bin]#
[root@TEPS bin]# ./itmcmd manage &
[1] 21105
```

Fig. 3.18 Iniciando el manejador de servicios.

Al iniciar el manejador de servicios se puede notar que existen dos. El primero IBM Eclipse Help Server y el segundo Tivoli Enterprise Portal Server. Se da clic derecho sobre éste último y se selecciona “configure” (Figura 3.19).

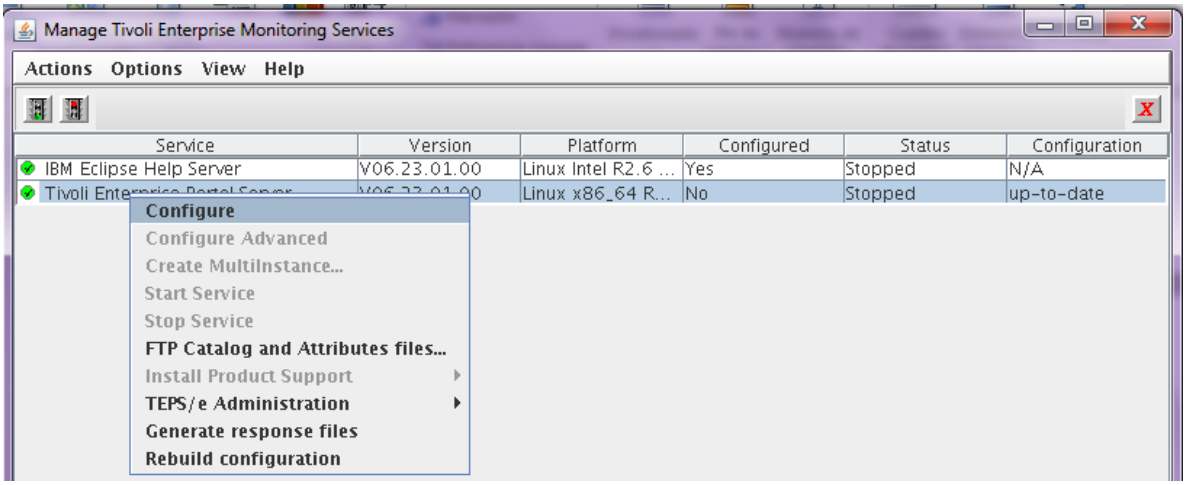


Fig.3.19 Iniciando el manejador de servicios.

En la primera ventana se deja la configuración por default en todas las pestañas (Figura 3.20). Puesto que como se mencionó, en esta implementación únicamente existe un servidor TEMS y otro servidor TEPS, de ahí el nombre del conector (ITM1). Se da clic en OK para pasar a la siguiente ventana de configuración.

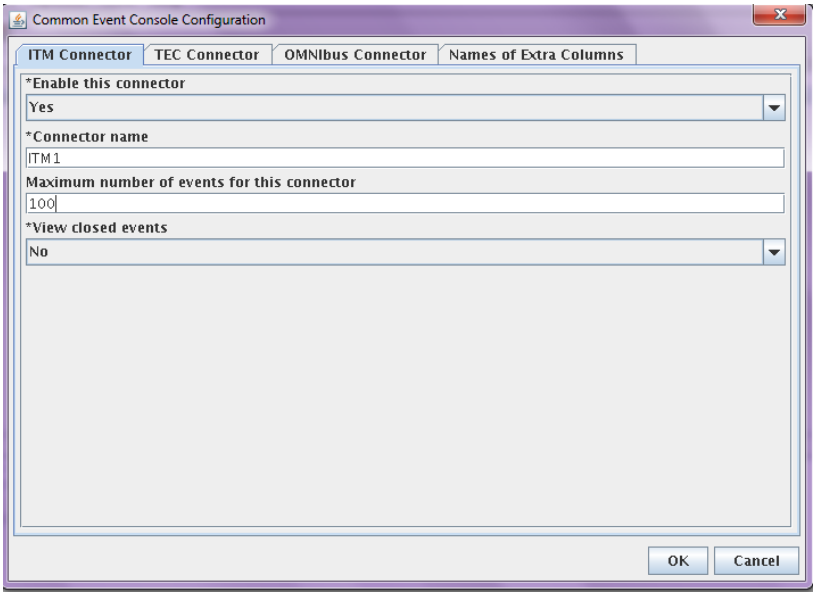


Fig.3.20 Iniciando el manejador de servicios.

La siguiente ventana (Figura 3.21) es muy importante ya que en ella se edita la configuración de la conexión con el servidor TEMS.

En el espacio destinado a ingresar el TEMS Hostname se ingresa la IP del servidor que se instaló anteriormente o también se puede ingresar el nombre del servidor si éste se encuentra mapeado en el archivo de hosts del servidor TEPS.

Por otra parte se indica el número de puerto por el que se dará la comunicación, el cual, fue definido durante la configuración del servidor TEMS y se deja por default.

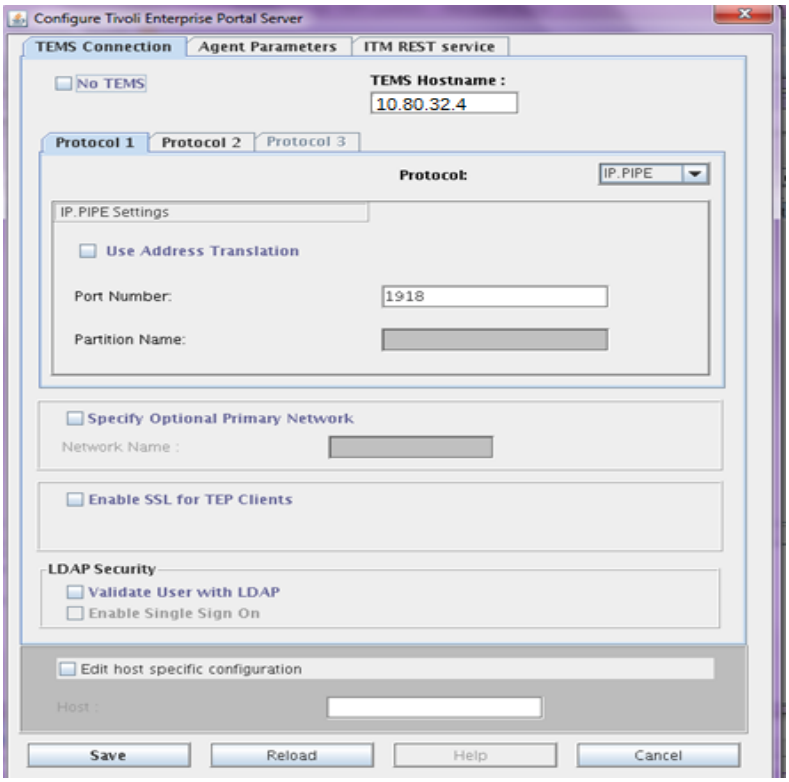


Fig.3.21 Configuración de conexión con TEMS.

Al cambiarse a la siguiente pestaña (Figura 3.22) pide los parámetros del agente. En la primera parte se indica el tipo de base de datos a utilizar, en este caso, DB2. Del otro lado pide el tipo de la base de datos en caso de utilizar la herramienta Warehouse. La cuál no fue necesaria ya que no se implementó.

Se ingresa el nombre de la instancia que se creó al instalar DB2. Así mismo el nombre del administrador de la instancia. En este caso fue el mismo nombre que se le dio a la instancia (db2inst1). Ingresa la contraseña que de igual forma fue definida en la instalación de la base de datos.

En la misma sección pide ingresar el nombre de la base de datos que se va a crear para el funcionamiento del TEPS. En este caso se le dio el nombre “TEPS”

para tener una buena referencia por si se necesitara realizar algún respaldo u otro tipo de procesos para su mantenimiento.

De igual forma pide indicar el nombre y password del usuario que será el que manejará la base de datos. Mismo que si no encuentra creará.

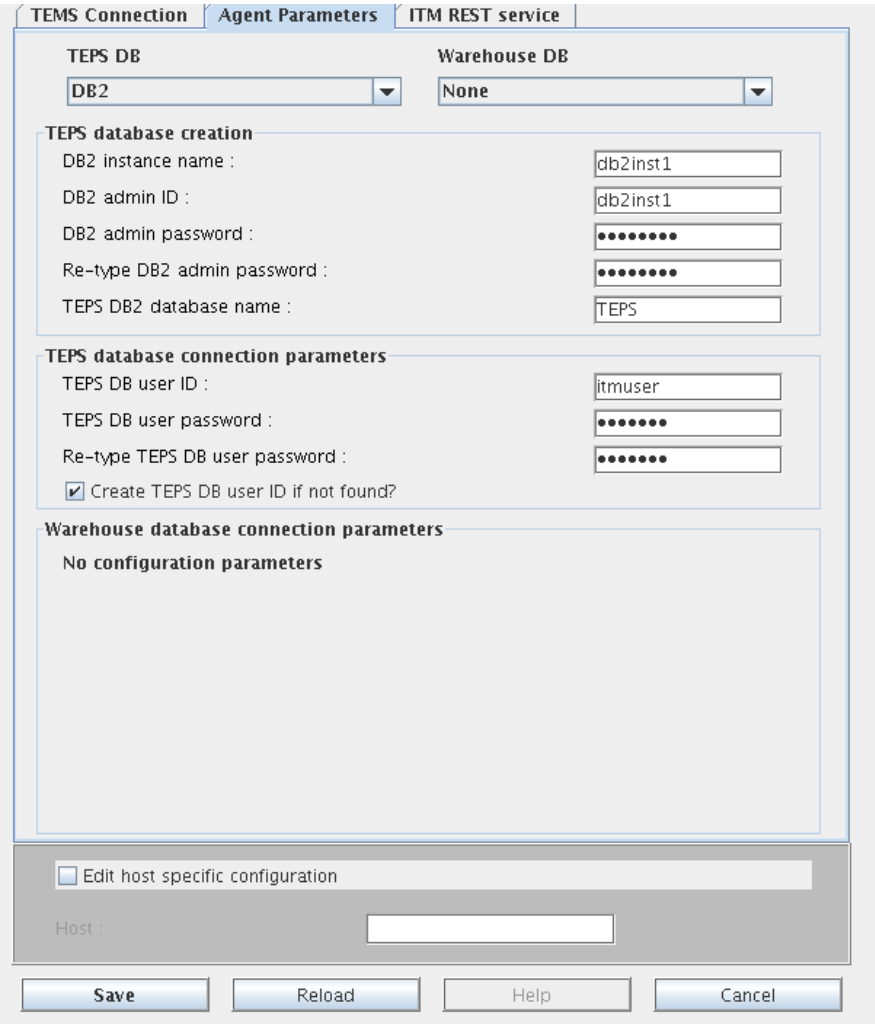


Fig.3.22 Configuración para la conexión con DB2.

Al dar clic en guardar el software comienza a hacer los procedimientos de creación de base de datos y usuario y si todo termina sin ningún fallo se regresa al manejador de servicios. Donde al dar clic derecho sobre el servicio TEPS e iniciarlo iniciará automáticamente el servicio de IBM Eclipse Help Server (Figura 3.23).

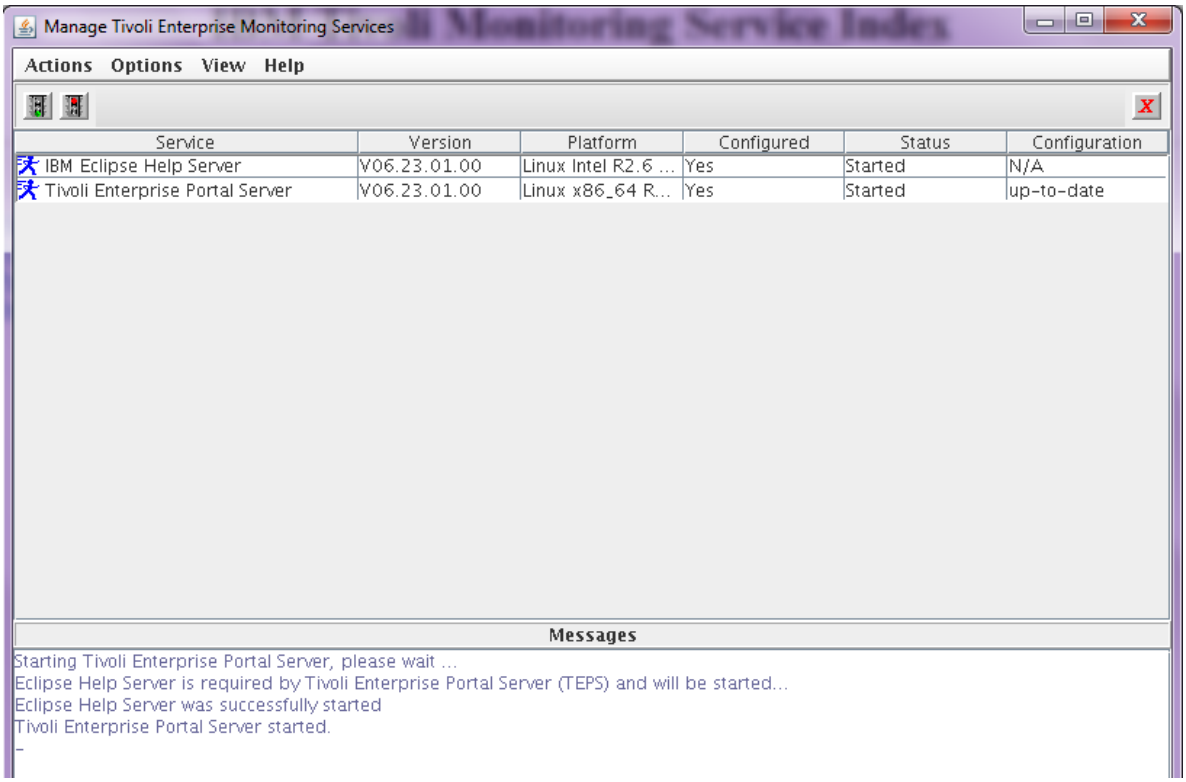


Fig. 3.23 Servicios iniciados correctamente.

Con este par de instalaciones se tiene configurada e instalada la base del monitoreo de IBM Tivoli Monitoring.

3.2.3 Agentes de monitoreo

Los agentes de monitoreo son recopiladores de datos. Los agentes supervisan sistemas, subsistemas o aplicaciones, recopilan datos y pasan los datos al servidor Tivoli Enterprise Portal a través del servidor del TEMS. Los agentes pasan instrucciones del usuario al sistema o aplicación. Un agente interactúa con un solo sistema o aplicación y, en la mayoría de los casos, está instalado en el mismo servidor en el que se ejecuta el sistema o aplicación.

Hay dos tipos de agente de supervisión:

1. Agentes de Sistema Operativo

   Los agentes de sistema operativo supervisan la disponibilidad y el rendimiento de los sistemas del entorno de supervisión. Existe un agente de Monitoreo específico para cada tipo de Sistema operativo:
   a) Windows
   b) UNIX
   c) Linux

Estos agentes se pueden instalar de dos maneras:

a) El agente de monitoreo se instala en el mismo servidor que va a supervisar.

b) El agente de monitoreo se puede instalar en un nodo remoto el cual, vía SNMP, supervisará al servidor.

Cabe señalar que en la implementación, todas las instalaciones se realizaron en el mismo servidor que se iba a monitorear.

2. Agentes de Aplicaciones

Se denominan “Agentes de Aplicaciones” a los agentes que supervisan las aplicaciones que se encuentran dentro de los servidores.

La siguiente es una lista de aplicaciones que se supervisan en la solución que se implementaron para el cliente:

a) VMware Workstation
b) Microsoft SQL
c) Lotus Domino
d) Microsoft Exchange
e) Internet Information Server (IIS).
f) Oracle Database
g) mySAP

Es importante mencionar que los agentes de monitoreo no requieren de un reinicio posterior a su instalación y generalmente no generan conflictos con alguna aplicación previamente instalada o que actualmente se esté ejecutando sobre el servidor a monitorear.

Como ya se mencionó, los agentes de monitoreo se instalaron sobre el mismo servidor que contenía la aplicación a monitorear. De esta manera se dividen las instalaciones en los siguientes 3 grupos, de tal modo que se explique de una forma clara la instalación de los mismos:

1. Agentes que monitorean el Sistema Operativo Windows y las aplicaciones que corren sobre este sistema operativo.

2. Agentes que monitorean el Sistema Operativo Linux y las aplicaciones que corren sobre este sistema operativo.

3. Agentes que monitorean el Sistema Operativo Unix y las aplicaciones que corren sobre este sistema operativo.

1. Agentes que monitorean el Sistema Operativo Windows y las aplicaciones que corren sobre este sistema operativo.

Para ingresar a los servidores con sistema operativo Windows fue necesario utilizar la utilería de Windows llamada “Remote Desktop Connection”.

Al ingresar al servidor es necesario copiar el paquete de instalación mediante el portapapeles compartido (opción únicamente disponible en Windows Server 2008 o superior) o mediante una carpeta compartida entre la máquina de escritorio y el servidor en cuestión.

Una vez copiada la paquetería, se ingresa a la carpeta Windows que se encuentra dentro de los archivos de instalación y se ejecuta el archivo “setup.exe” con permisos de administrador (Figura 3.24).

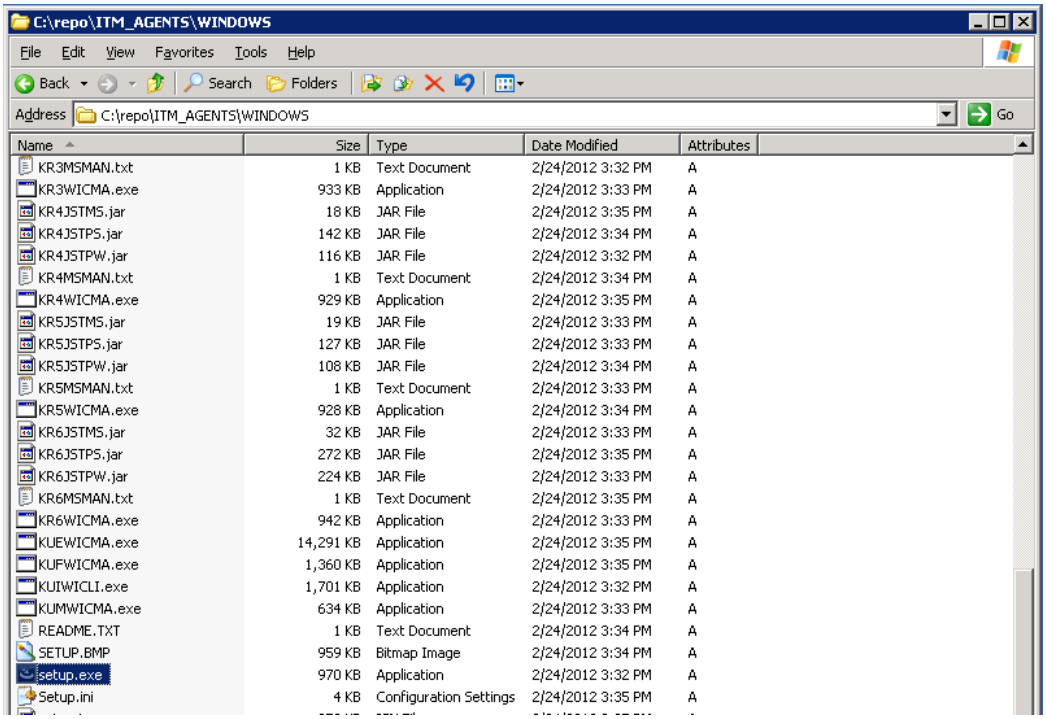


Fig. 3.24 Paquete de instalación de agentes de monitoreo de ITM.

Al pasar la pantalla de bienvenida y aceptar el acuerdo de licencia que en todo programa de instalación se encuentra. Se muestra la opción de elegir la ruta de instalación. Generalmente se deja la ruta por default “C:\IBM\ITM” (Figura 3.25).

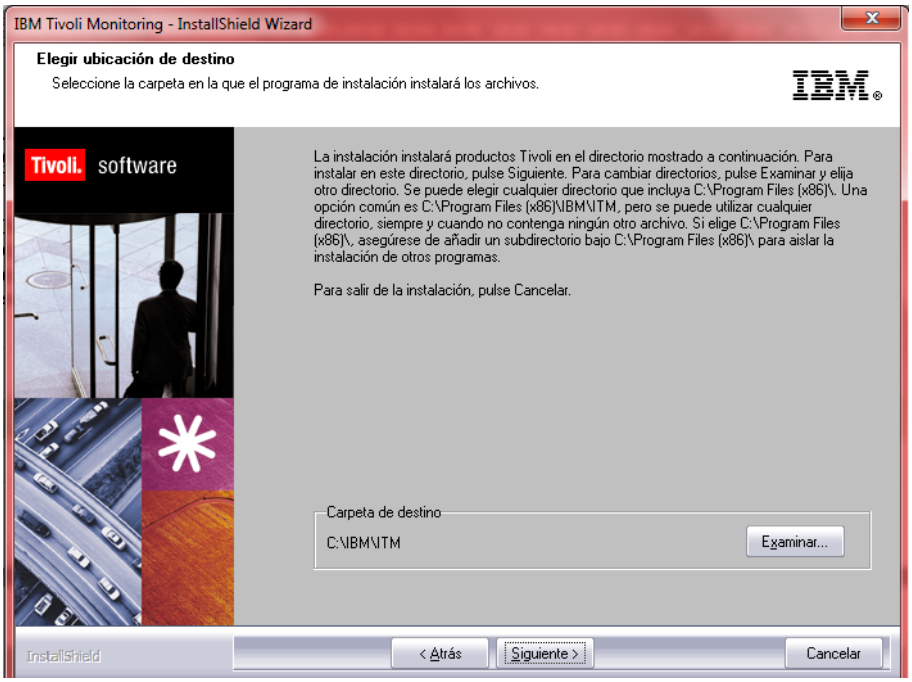


Fig. 3.25 Ruta de instalación.

Más adelante se presenta la siguiente pantalla en la cual se ingresa la clave de cifrado para las conexiones con TEMS a fin de salvaguardar la información que entre ellos se comparte (Figura 3.26).

Fig. 3.26 Clave de cifrado.

Una vez elegidos estos valores muestra la lista de Agentes que el paquete de instalación contiene. Se elige “Monitoring Agent for Windows OS” y por default se selecciona automáticamente “Tivoli Enterprise Monitoring Agent Framework” que es un paquete necesario para el correcto funcionamiento del agente de monitoreo (Figura 3.27).

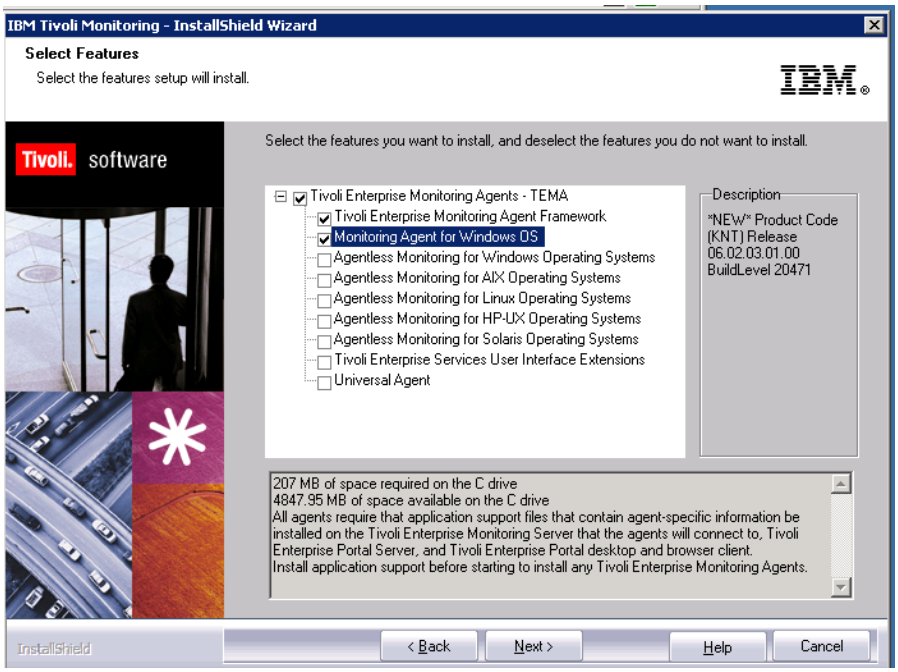


Fig. 3.27 Elección del Agente

Al presionar “Next” aparece una ventana de resumen donde se indica el listado de agentes a instalar así como también la ruta definida y el espacio en disco que utilizará la instalación. Se presiona aceptar y comienza la instalación (Figura 3.28).

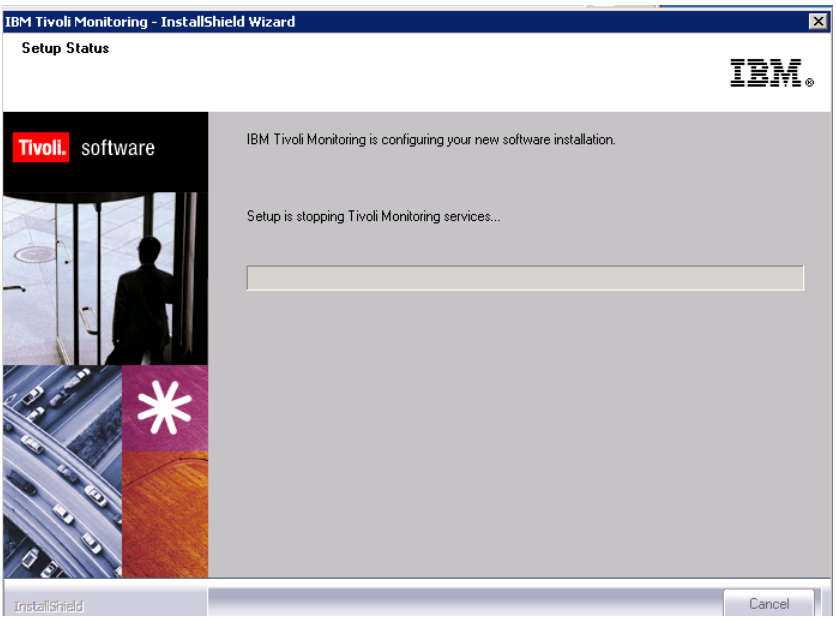


Fig. 3.28 Progreso de la instalación.

Al finalizar, la instalación pregunta si se desea configurar el agente y si quiere ejecutar el manejador de agentes (Figura 3.29). Se seleccionan ambas.

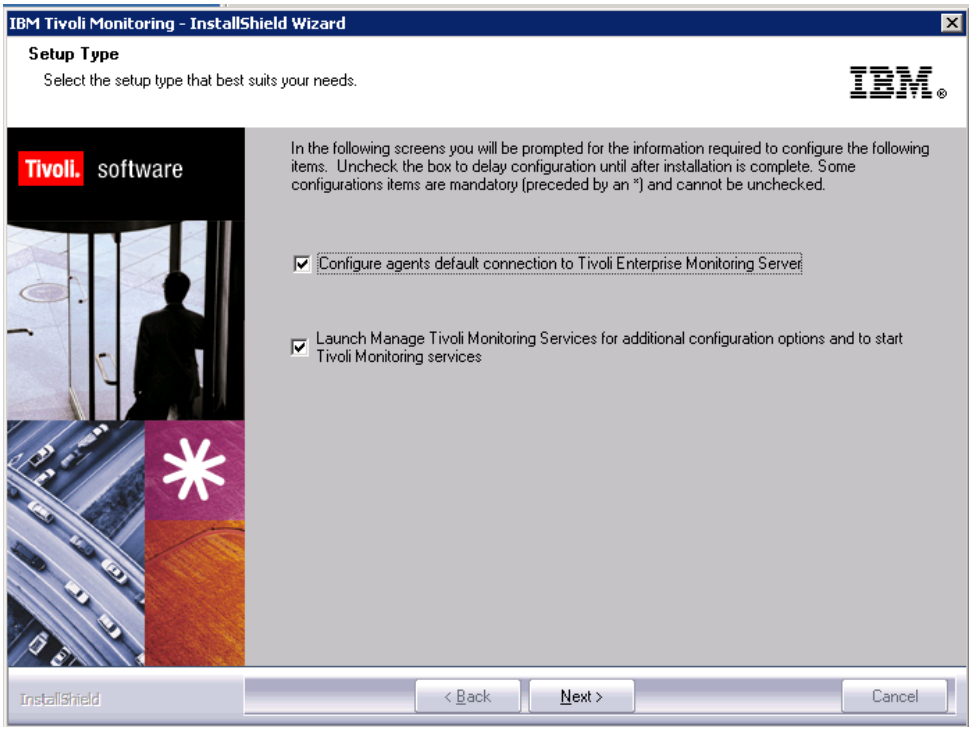


Fig. 3.29 Finalización de la instalación.

Se presentaba la ventana de configuración del agente en la cual se ingresa la dirección IP del servidor TEMS y el puerto de comunicación (el cual se había

elegido en la configuración del TEMS). El protocolo de conexión se deja por default IP:PIPE (Figura 3.30).

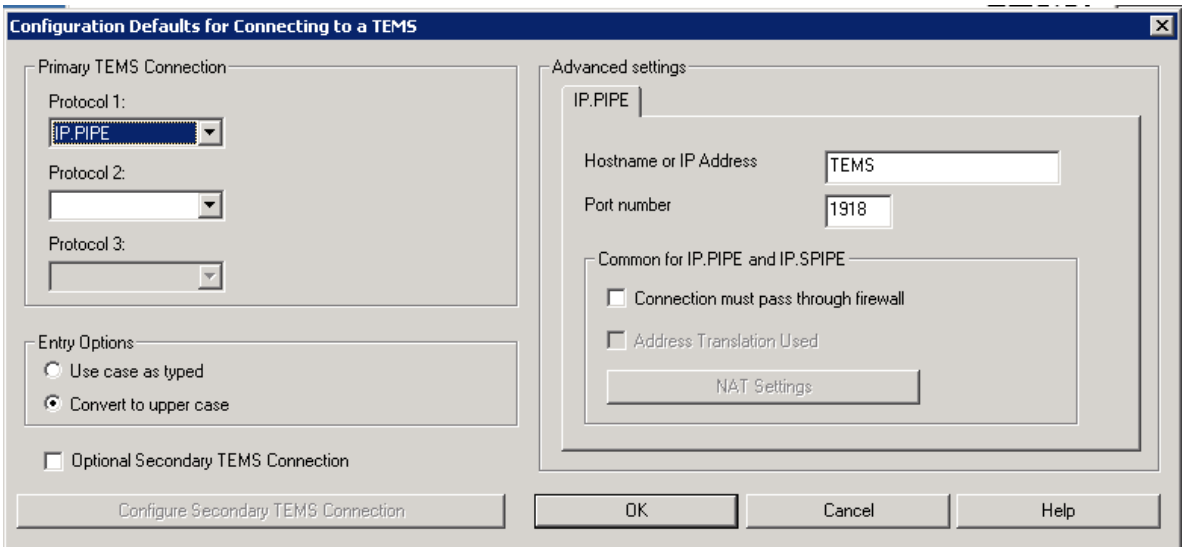


Fig. 3.30 Configuración de la conexión del Agente con el TEMS

Al presionar "OK" la configuración se guarda y automáticamente se ejecuta el servicio de monitoreo. Para verificar dicho hecho se dirige al menú de inicio, "All Programs", "IBM Tivoli Monitoring" y "Manage Tivoli Monitoring Services". En dicho manejador el agente aparece con un ícono azul al lado (Figura 3.31) lo que significa que se encuentra reportando información al servidor TEMS.

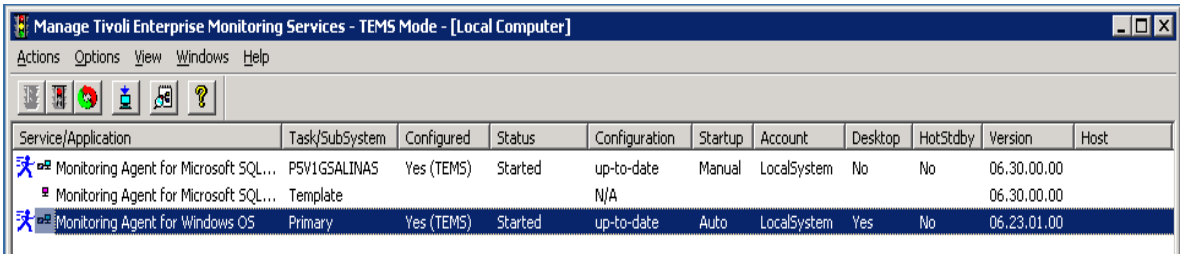


Fig. 3.31 Agente de Monitoreo de Sistema Operativo Windows corriendo.

Configuración de los Agentes que monitorean las aplicaciones que corren sobre el Sistema Operativo Windows.

La instalación de las aplicaciones que trabajan sobre el sistema Operativo Windows sigue el mismo esquema que el anteriormente descrito. No obstante la configuración del agente cambia. A continuación se describen las configuraciones necesarias para que los agentes de monitoreo de aplicaciones, que se ejecutan sobre el sistema operativo Windows, reporten al servidor TEMS.

a) Configuración del agente de monitoreo de Internet Information Services (IIS)

El agente de monitoreo de IIS se apoya en los Logs de los servicios. Por ello la configuración de este agente requiere mapear la ruta donde estos Logs se encuentran. En esta primera pestaña (Figura 3.32) se ingresa la ruta del Log de errores de HTTP.

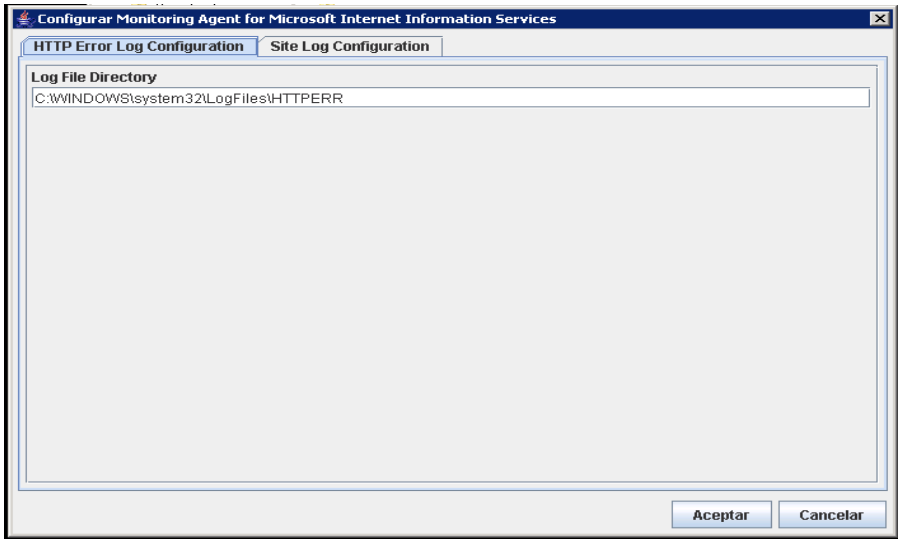


Fig. 3.32 Configuración Logs HTTP

En la segunda pestaña (Figura 3.33) se indica la ruta donde se encuentran los logs del sitio.

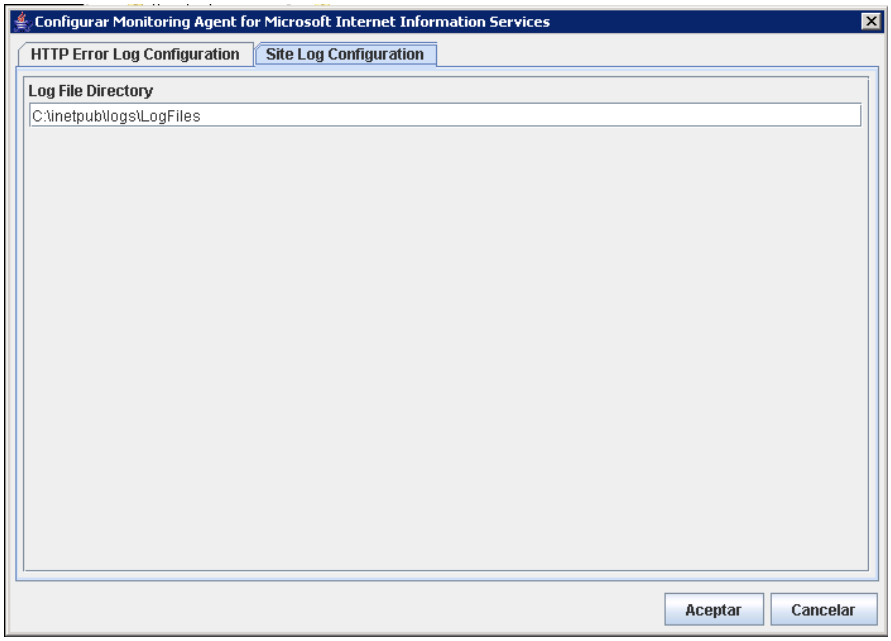


Fig. 3.33 Configuración Logs del sitio.

b) Configuración del agente de monitoreo de Microsoft Exchange Server

Como requisito previo para la configuración del Agente de monitoreo de Microsoft Exchange Server es necesario crear un usuario en la aplicación de Microsoft Exchange Server que debe ser un Administrador de Dominios con derechos de administrador completos.

La primera pestaña de la ventana de configuración pide las propiedades del servidor. Su nombre, el dominio, el usuario y el password así como también su confirmación (Figura 3.34).

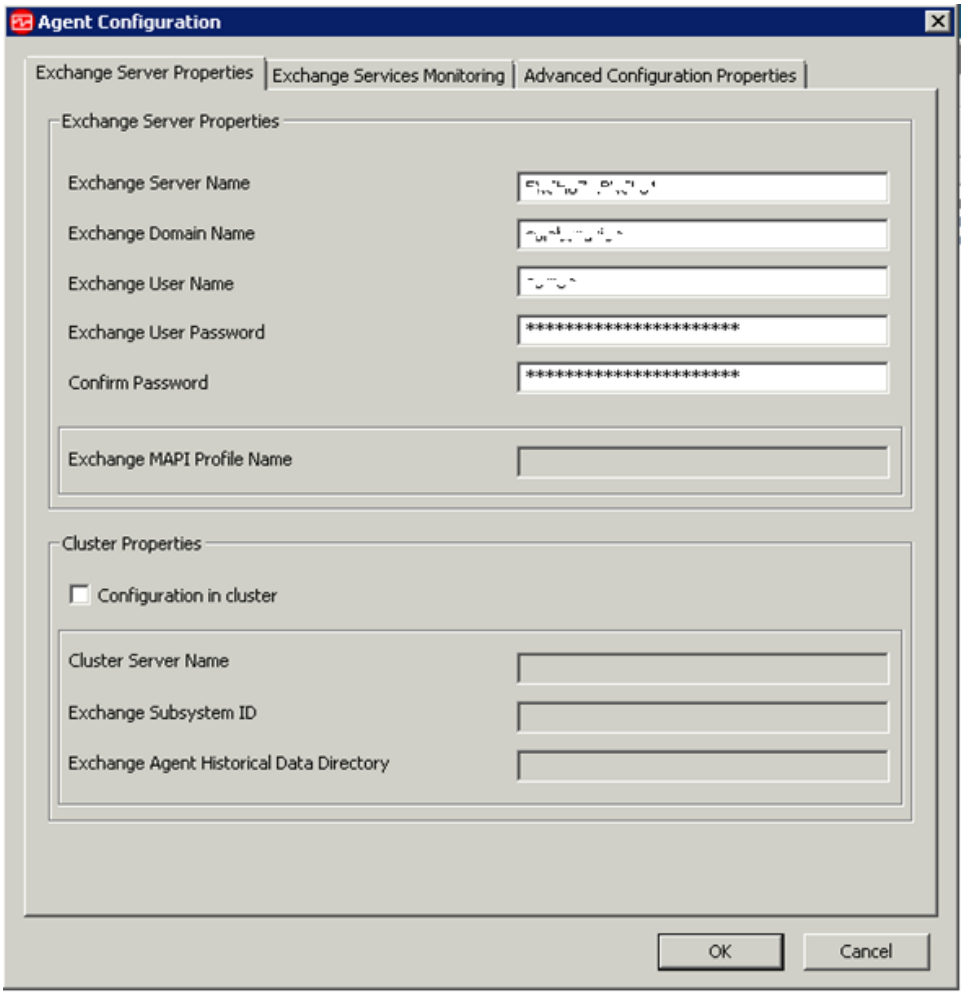


Fig. 3.34 Configuración de los datos del servidor Exchange.

La configuración de las 2 pestañas siguientes se dejan por default. Al presionar “OK” el agente hace una validación de los datos ingresados, si presenta algún problema con la autentificación con la aplicación de Exchange marca el error (Figura 3.35) y será necesario verificar los datos ingresados. En el caso contrario

que estén los datos correctos, la ventana de configuración simplemente se cierra y regresa a la ventana del manejador de agentes (Figura 3.30).

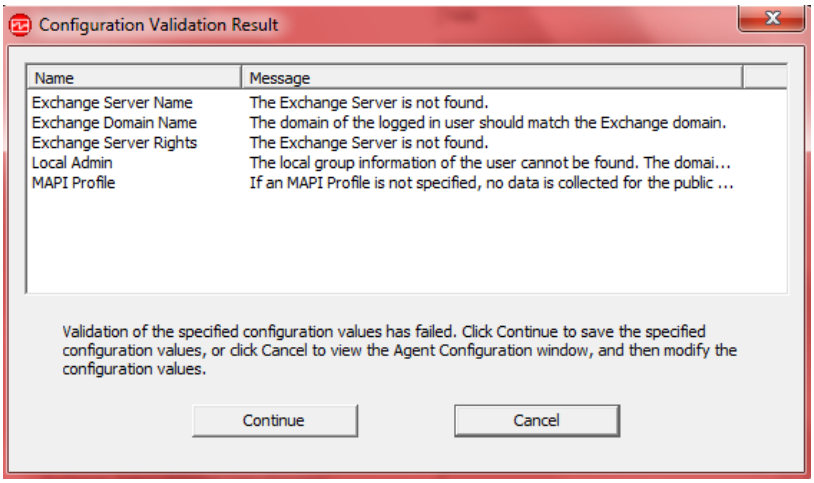


Fig. 3.35 Errores en la configuración del Agente Exchange.

c) Configuración del agente de monitoreo de VMware.

Para monitorear el VCenter fue necesario crear una instancia dentro del manejador de agentes. Se da doble clic sobre el agente ya instalado y en la ventana que aparece se ingresa el nombre de la instancia, en este caso, VCENTERIBM (esto se hace por si existe más de un VCenter que se desea monitorear, gracias a este nombre de instancia se pueden diferenciar). Se presiona Aceptar (Figura 3.36).

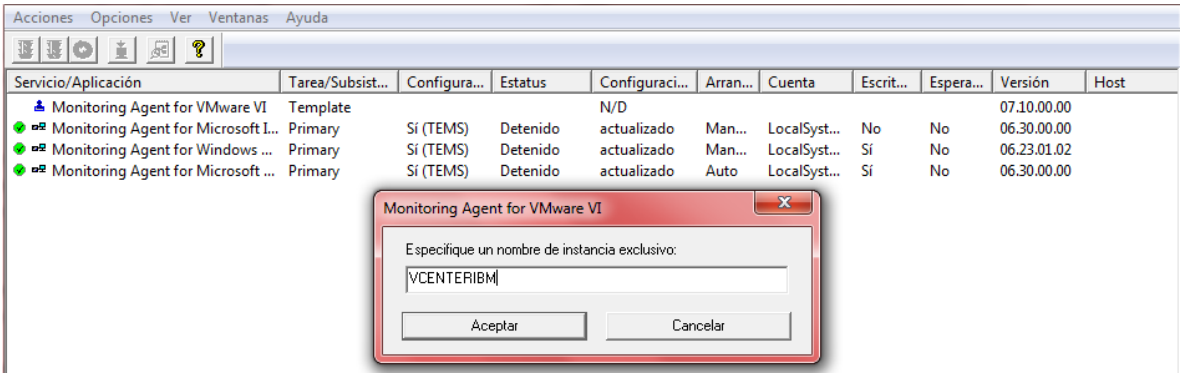


Fig. 3.36 Ingreso del nombre de la instancia.

En la siguiente ventana se dejan por default los valores que aparecen en los pestañas “Data Provider”, “IBM Systems Director” y “Storage Agent” (Figura 3.37).

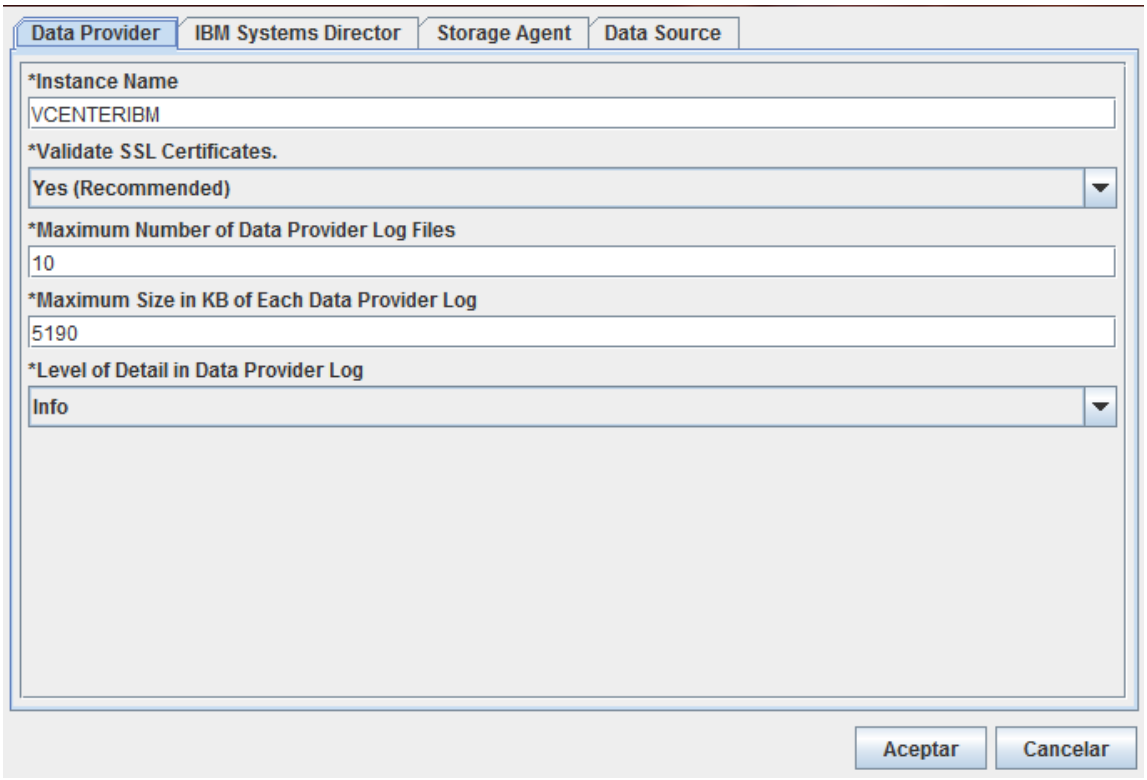


Fig. 3.37 Configuraciones de la Instancia.

Al dar clic en la pestaña “Data Source” y después en “New…” (Figura 3.38), en el campo de Data Source ID se ingresa el nombre del VCENTER. En Data Source Address se ingresa la dirección IP del VCENTER. En Data Source ID se ingresa el usuario que se creó especialmente para el monitoreo del VCENTER. Así mismo se introduce el password y su confirmación. Al presionar aceptar se cierra la ventana y regresa al manejador de agentes en el cual ya se puede iniciar el agente para su monitoreo.

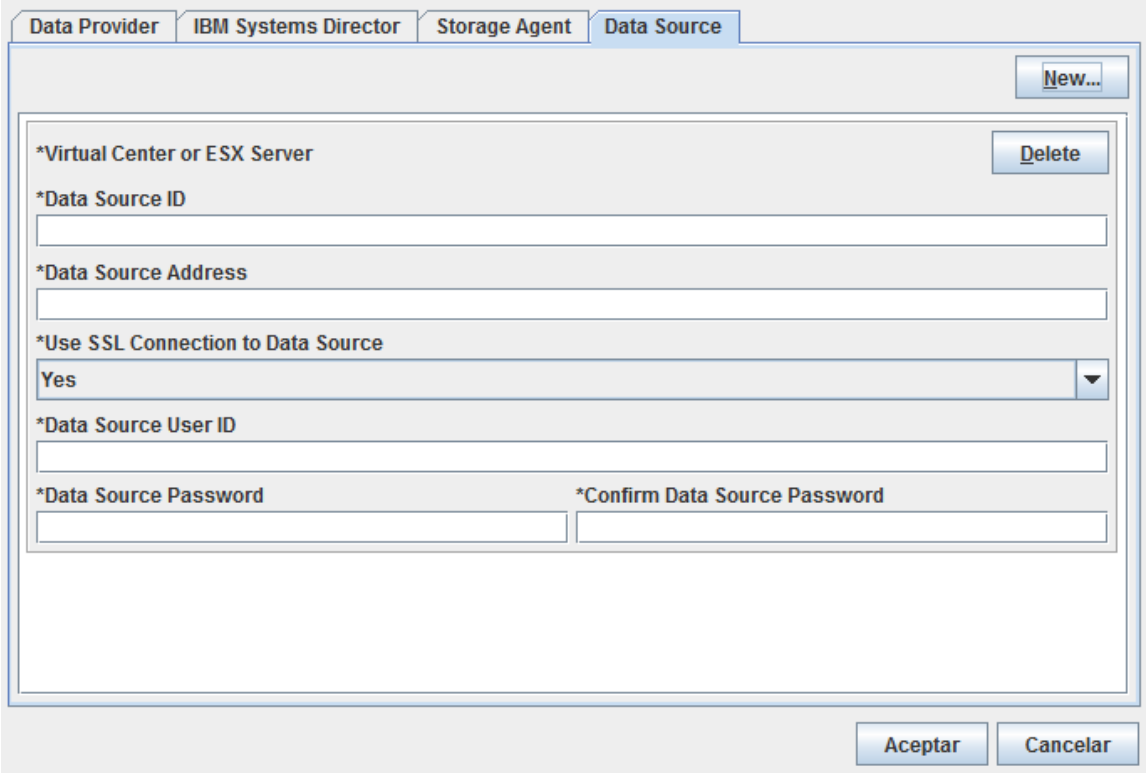


Fig. 3.38 New Data Source VCENTER.

d) Configuración del agente de monitoreo de SQL.

Al igual que en la configuración de los anteriores agentes de monitoreo, en este, es necesario como prerrequisito crear un usuario para que el agente pueda monitorear la instancia de la Base de Datos.

Recién instalado el agente, se da doble clic sobre él y automáticamente detecta las bases de datos existentes en el servidor. Se selecciona la base de datos que se encuentra en el lado de disponibles y con el botón "<<" se pasa al recuadro donde aparecen las bases de datos que se van a monitorear. Tal como se ve en la imagen siguiente (Figura 3.39).

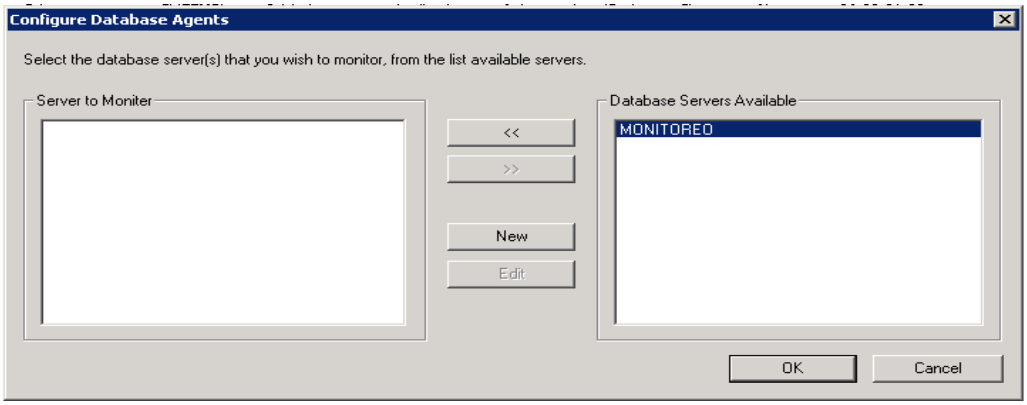


Fig. 3.39 Elección de la base de datos.

En la siguiente ventana (Figura 3.40) se ingresa el nombre del usuario de la base de datos que fue creado especialmente para el monitoreo. El “Server Name”, la “Database Version”, el “Home Directory” y el “Error Log File” se detectan en automático y se ingresan los datos en los campos requeridos.

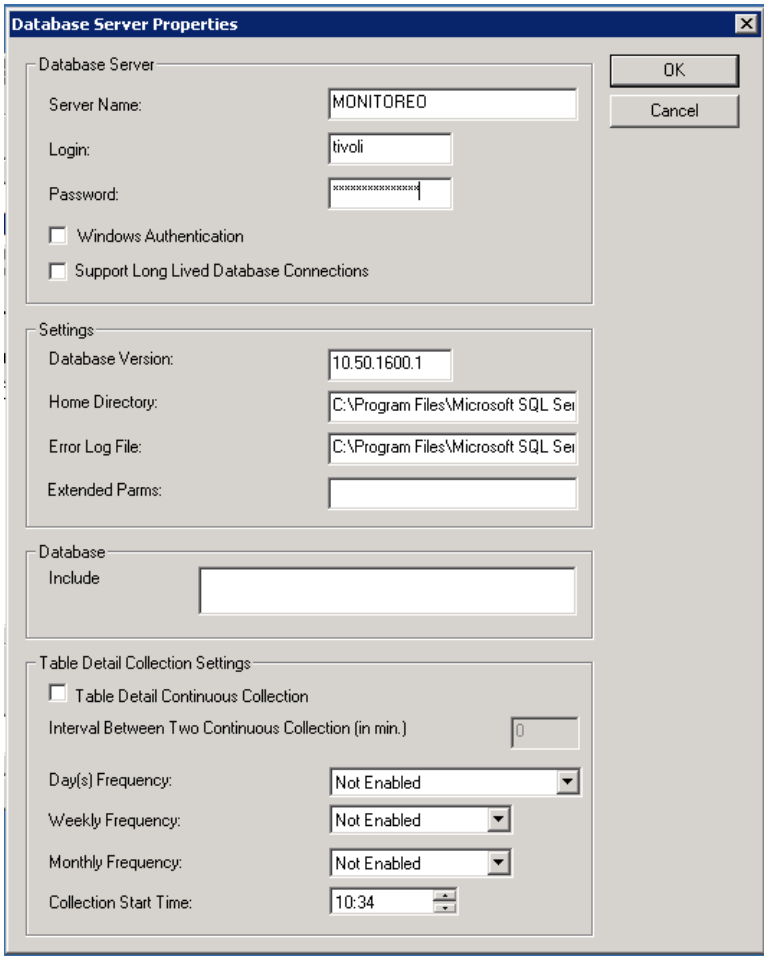


Fig. 3.40 Propiedades de la base de datos.

2. Agentes que monitorean el Sistema Operativo Linux y las aplicaciones que corren sobre este sistema operativo.

Para ingresar a los servidores con sistema operativo Linux es necesario contar con un cliente de conexiones SSH llamado XShell de XManager. El comando que se ingresa para conectarse a los servidores es el siguiente (Figura 3.41):

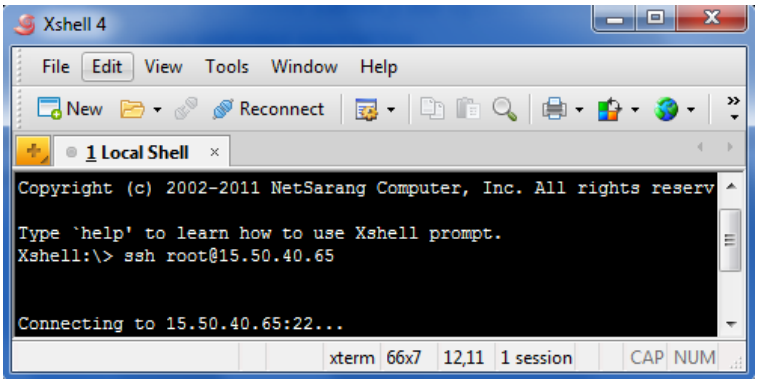


Fig. 3.41 Conexión al servidor vía SSH.

A continuación aparece un recuadro en el cual se debe ingresar la contraseña. Si la contraseña fue correcta regresa a la pantalla de línea de comandos propia del servidor.

Para copiar los archivos de instalación, se crea una carpeta en el servidor TEMS que contenía dichos archivos. Desde el servidor que se iba a monitorear se ejecuta el comando scp para conseguir una copia segura como se muestra en la siguiente imagen (Figura 3.42). Al ingresar la contraseña, si ésta era correcta, comenzaba la copia de los archivos.

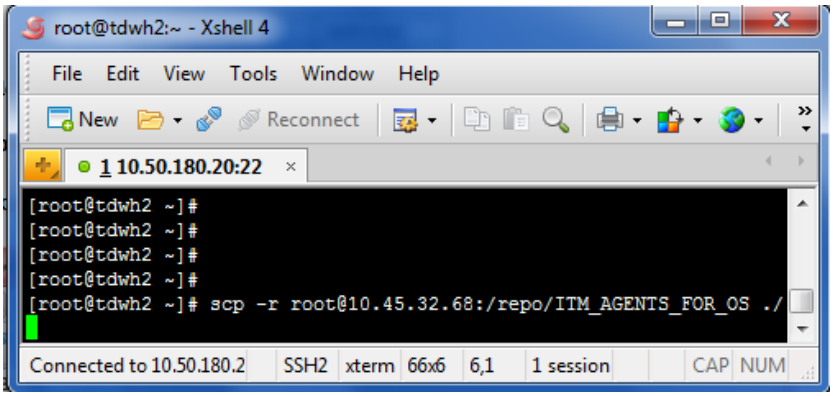


Fig. 3.42 Ejecutando Copia Segura.

Una vez que se copia la carpeta de instalación se ingresa a la misma y se ejecuta el archivo “install.sh”. Cabe señalar que el paquete para instalar los agentes de monitoreo de sistema operativo es el mismo tanto para Linux, Windows y UNIX.

Al igual que en los agentes anteriores, la instalación pide elegir la ruta del agente, se deja la que tiene por default. Advierte que dicha ruta no existe y pregunta si se desea crear (Figura 3.43).

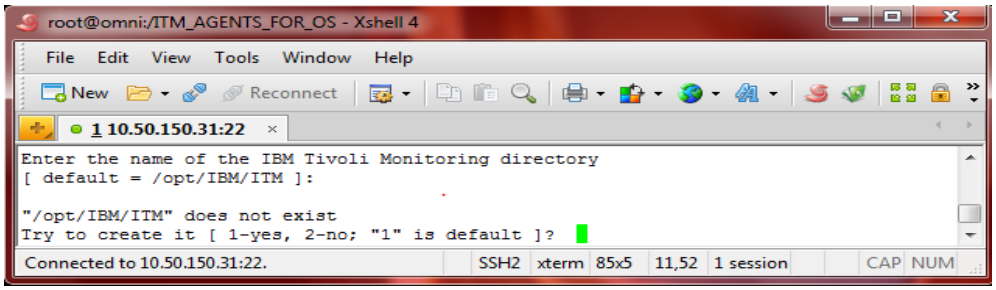


Fig. 3.43 Ruta de instalación.

Posteriormente se muestra el menú de instalación. Se elige la primera opción para instalar los agentes de monitoreo en el servidor en el que se está ejecutando la instalación (Figura 3.43).

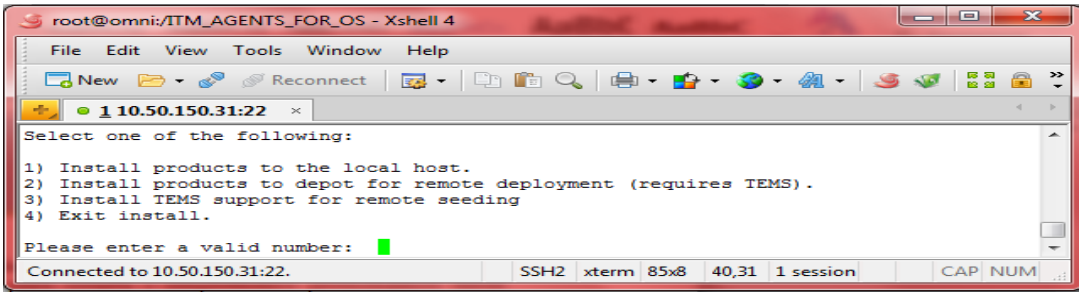


Fig. 3.44 Menú de instalación.

Se acepta el acuerdo de licencia del producto para que permita continuar con la instalación. (Figura 3.45).

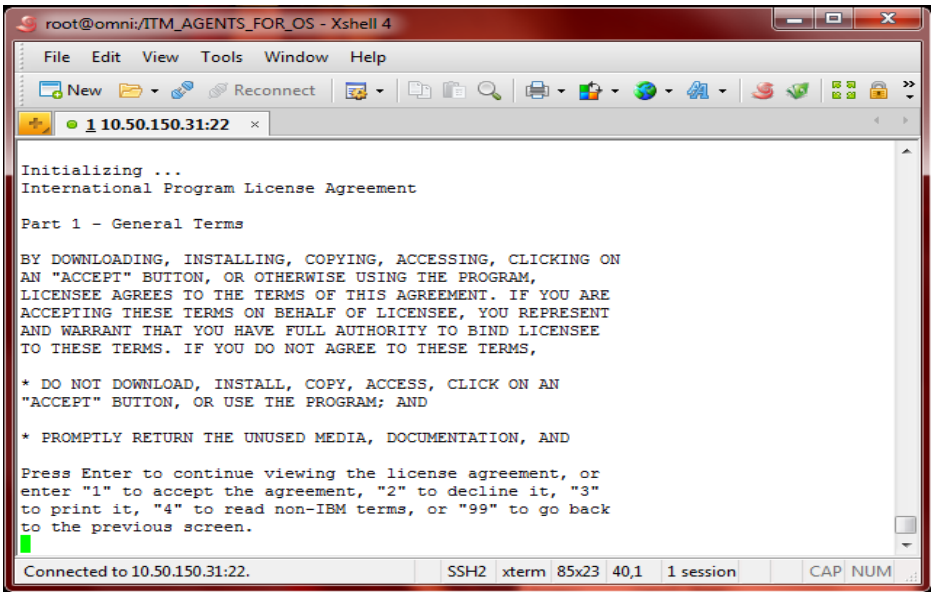


Fig. 3.45 Acuerdo de licencia.

Al igual que en el sistema operativo Windows, se tiene que elegir la clave de encriptación, necesaria para que la información del monitoreo viaje de una manera segura a través de la red (Figura 3.46).

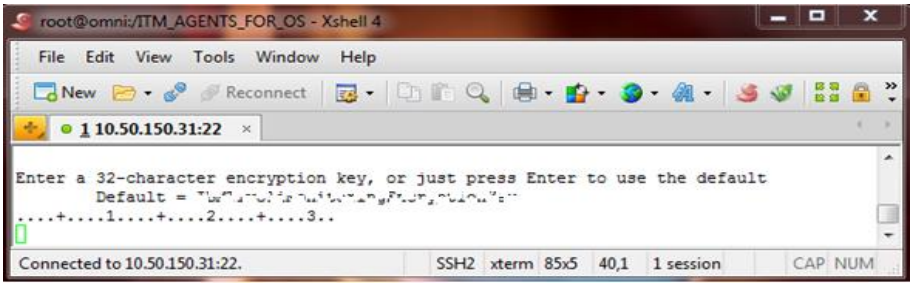


Fig. 3.46 Clave de encriptación.

Una vez que se ingresa la clave, muestra un menú en el cual da la opción de elegir al agente que se desea instalar. En este caso se selecciona la opción “6) Monitoring Agent for Linux OS V06.23.01.00” (Figura 3.47).

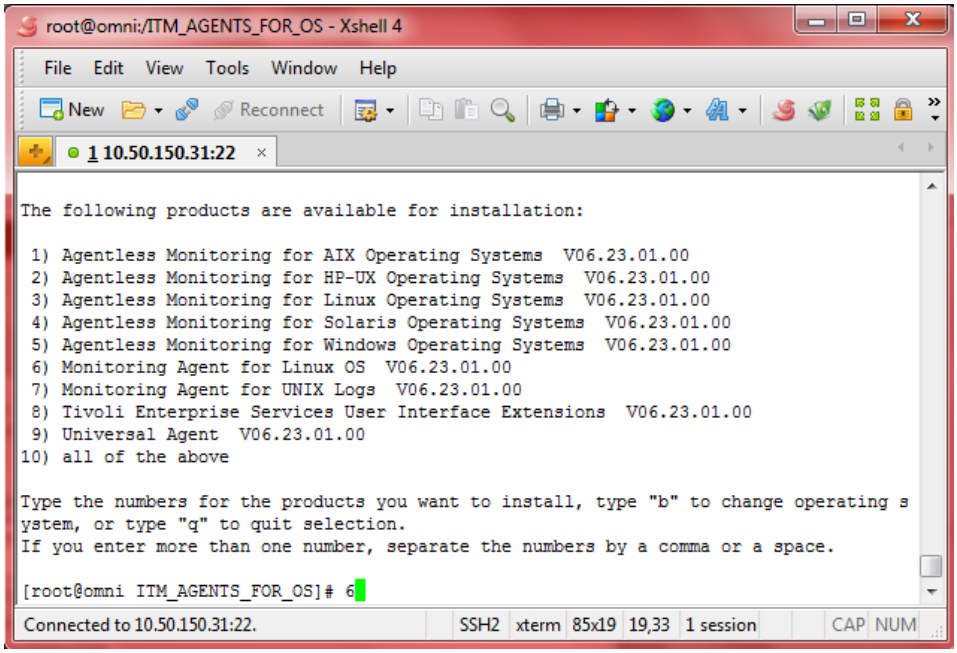


Fig. 3.47 Menú de productos disponibles.

A partir de este punto comienza la instalación del agente y después de un par de minutos finaliza (Figura 3.48). Ahora es necesario configurar e iniciar al agente para que exista una conexión con el TEMS.

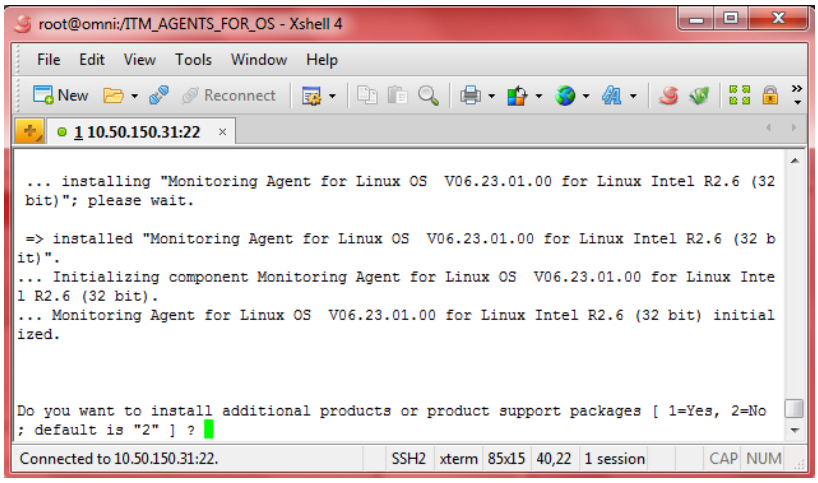


Fig. 3.48 Instalación del agente finalizado.

Configuración de los Agentes que monitorean las aplicaciones que corren sobre el Sistema Operativo Linux.

La instalación de las aplicaciones que trabajan sobre el sistema Operativo Linux sigue el mismo proceso que el anteriormente descrito. No obstante la configuración de los agentes cambia. A continuación se describen las configuraciones necesarias para que los agentes de monitoreo de aplicaciones, que se ejecutan sobre el sistema operativo Linux, reporten al servidor TEMS.

a) Configuración del agente de monitoreo de Sistema Operativo Linux.

Una vez instalado el agente es necesario situarse en la ruta de instalación y posteriormente a la carpeta “bin”. Ahí se ejecuta el comando “itmcmd” con el parámetro “manage” (Figura 3.49).

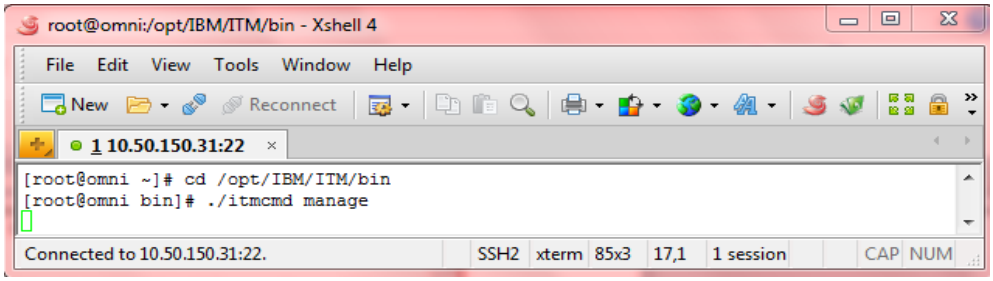


Fig. 3.49 Instalación del agente finalizado.

Haciendo lo anterior se abre la ventana del manejador de agentes donde se da clic derecho sobre el agente instalado y posteriormente se selecciona “configure” (Figura 3.50).

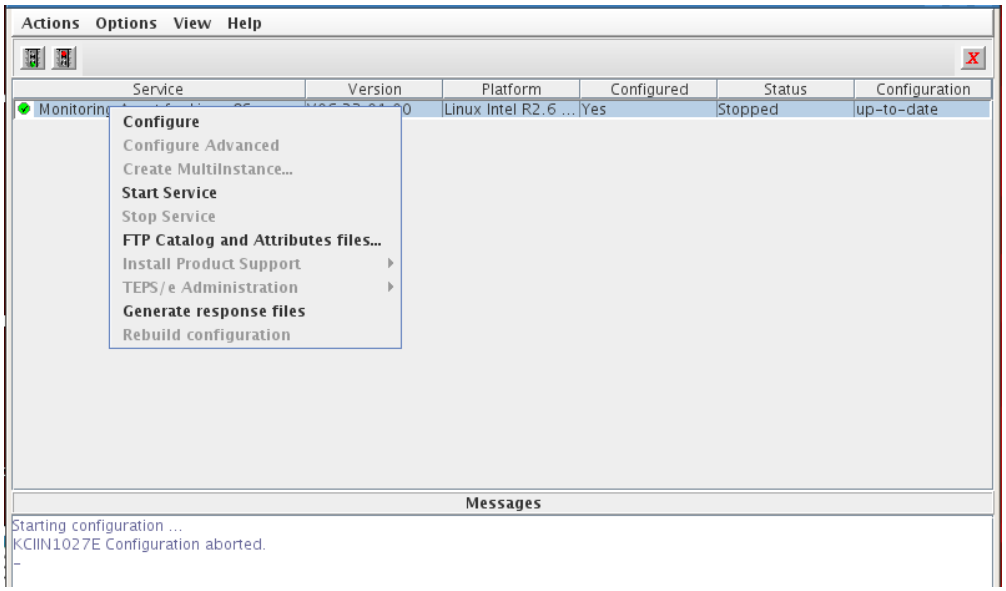


Fig. 3.50 Manejador de Agentes.

En la siguiente ventana se configura la conexión con el servidor TEMS por lo que en “TEMS Hostname” se ingresa la IP del servidor TEMS y el puerto destinado para la conexión (Figura 3.51).

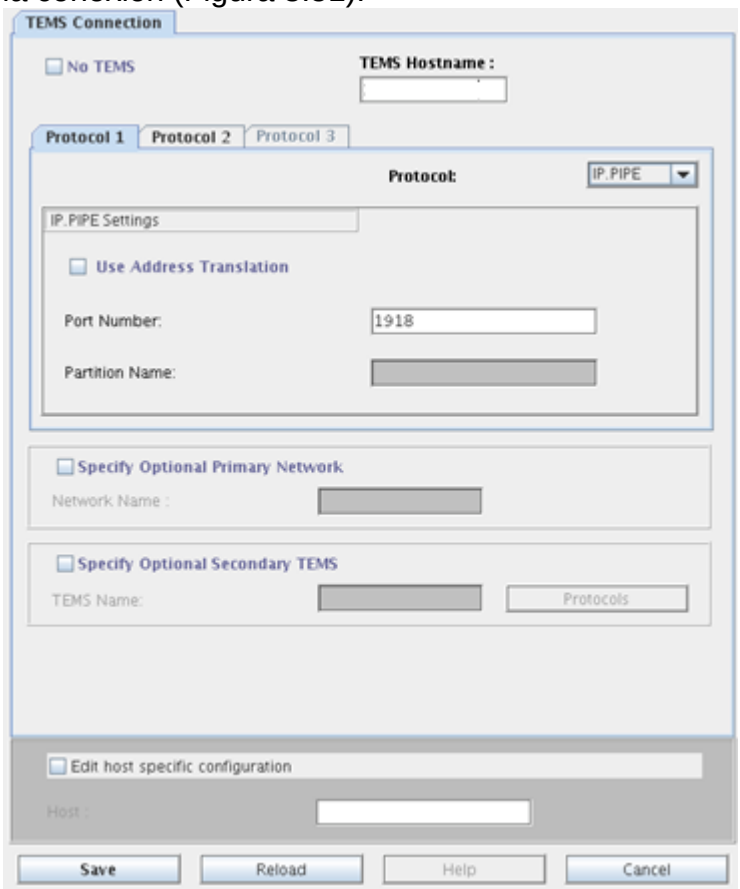


Fig. 3.51 Configuración del Agente.

Finalmente al guardar la configuración se regresa automáticamente a la ventana de manejo de agentes y se inicia el servicio dando doble clic sobre él. El icono cambiará de color y se muestra un ícono de color azul (Figura 3.52).

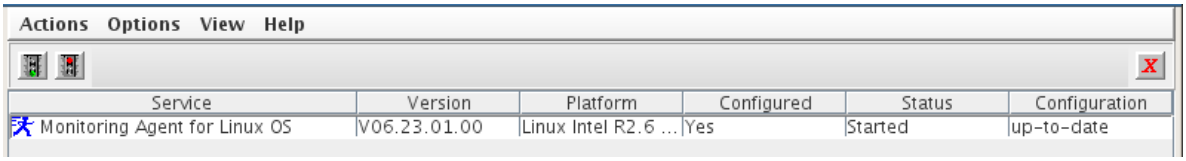


Fig. 3.52 Agente de SO Linux Iniciado.

b) **Configuración del agente de monitoreo de Lotus Domino**

Al igual que con el agente de Sistema operativo, se ingresa a la ruta de instalación y se ejecuta el comando “itmcmd” como se muestra en la figura 3.49. Y como se muestra en la figura 3.50, se da clic derecho sobre el agente de monitoreo de Lotus Domino.

Al hacer lo anterior, el agente muestra automáticamente la instancia que detecta en el servidor dónde se realizó la instalación. Entonces se presiona “OK” (Figura 3.53).

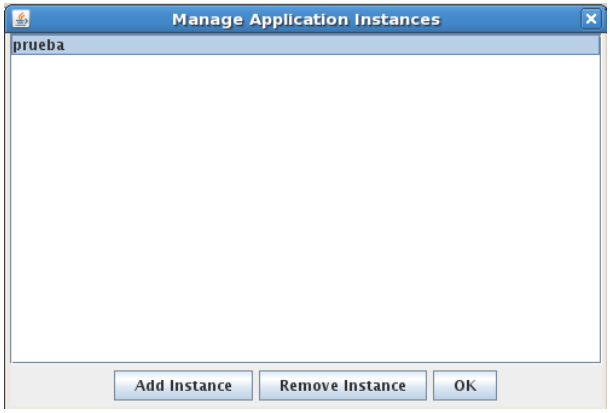


Fig. 3.53 Elección de Instancia Lotus Domino.

A continuación se presenta la siguiente ventana (Figura 3.54) en la cual se configuran los siguientes directorios:

En el primero, “Full path to the local notes.ini file”, se busca el archivo “notes.ini” dentro de los directorios del servidor. Se copia esta ruta y se coloca en el espacio en blanco.

En el segundo, “Monitored Domino Server Name”, se busca dentro del archivo “notes.ini” (antes mencionado) la variable “ServerName=” y se copia toda la ruta. Se pega el directorio en el espacio en blanco.

Los demás parámetros se configuran por defecto y se dejan como están.

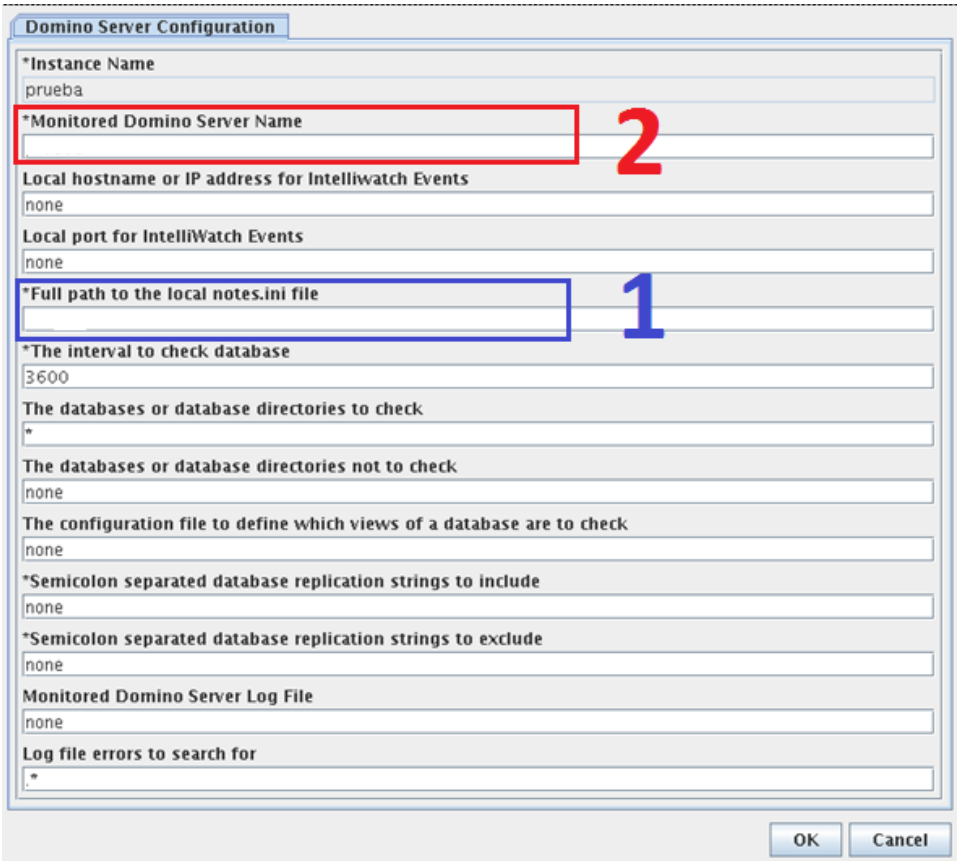


Fig. 3.54 Configuración del agente de monitoreo de Lotus Domino.

Al presionar OK se envía la ventana de configuración de la conexión del agente con el servidor TEMS. Dicha configuración se encuentra en la figura 3.51, se llenan los campos indicados y así finaliza la configuración de este agente.

3. Agentes que monitorean el Sistema Operativo UNIX y las aplicaciones que corren sobre este sistema operativo.

Para ingresar a los servidores con sistema operativo AIX (al igual que con los servidores Linux) fue necesario contar con un cliente de conexiones SSH llamado XShell de XManager. El comando que se ingresa para establecer la conexión a los servidores es el siguiente (Figura 3.55):

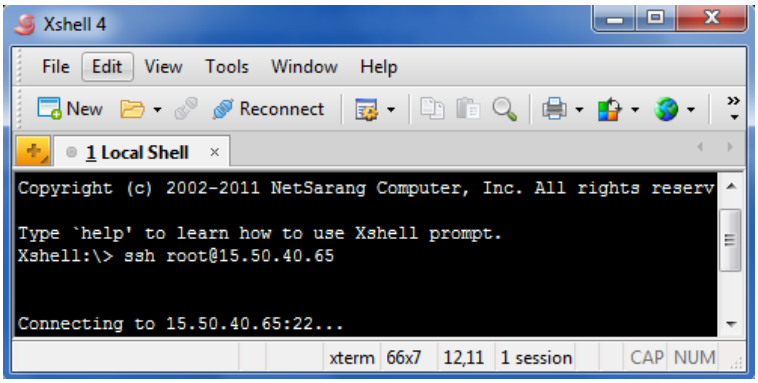


Fig. 3.55 Conexión al servidor AIX vía SSH.

A continuación aparece un recuadro en el cual se debe ingresar la contraseña. Si la contraseña fue correcta se regresa a la pantalla de línea de comandos propia del servidor. En este caso, a diferencia de los sistemas operativos Linux, la línea de comandos del servidor no muestra el nombre ni el usuario con el que se conecta. Cabe señalar que el sistema operativo del servidor es AIX 7.1

Como se explicó, se creó una carpeta en el servidor TEMS que contenía los archivos de instalación. Desde el servidor AIX que se iba a monitorear se ejecutaba el siguiente comando cuál (Figura 3.56) para realizar una copia segura de los archivos de instalación. Al ingresar la contraseña, si ésta era correcta, comenzaba la copia de los archivos.

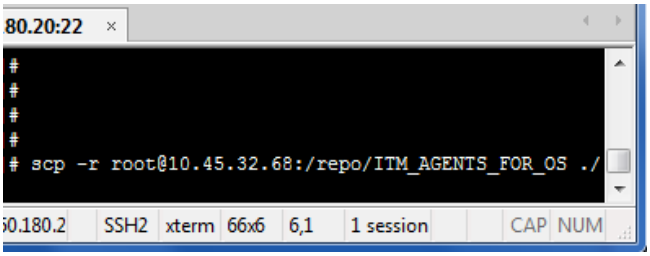


Fig. 3.56 Ejecutando Copia Segura.

Una vez copiada la carpeta de instalación se ingresaba a ella y se ejecuta el archivo “install.sh”. En este caso el paquete de instalación, aunque es el mismo para todos los sistemas operativos, logra diferenciar sobre qué Kernel se está ejecutando.

Al igual que en el sistema operativo Linux, la ruta de instalación por default es la misma y así se deja (Figura 3.57).

```
# ./install.sh
INSTALL

Enter the name of the IBM Tivoli Monitoring directory
[ default = /opt/IBM/ITM ]:
```

Fig. 3.57 Ruta de Instalación.

Se acepta el acuerdo de licencia. Que es el mismo que presenta en el sistema operativo Linux (Figura 3.45). Y después de ingresar la clave de encriptación (Figura 3.46) muestra la siguiente lista de productos disponibles para instalar (Figura 3.58).

```
The following products are available for installation:

 1) Agentless Monitoring for AIX Operating Systems  V06.23.01.00
 2) Agentless Monitoring for HP-UX Operating Systems  V06.23.01.00
 3) Agentless Monitoring for Linux Operating Systems  V06.23.01.00
 4) Agentless Monitoring for Solaris Operating Systems  V06.23.01.00
 5) Agentless Monitoring for Windows Operating Systems  V06.23.01.00
 6) Monitoring Agent for UNIX Logs  V06.23.01.00
 7) Monitoring Agent for UNIX OS  V06.23.01.00
 8) Tivoli Enterprise Services User Interface Extensions  V06.23.01.00
 9) Universal Agent  V06.23.01.00
10) all of the above
```

Fig. 3.58 Lista de productos disponibles.

Se elige la opción 7 y pide confirmar la elección. Se acepta presionando la tecla “enter” y así comienza la instalación (Figura 3.59).

```
... installing "Monitoring Agent for UNIX OS  V06.23.01.00 for AIX R5.3 (64 bit)  AIX R6.1 (64 bit)"; please wait.

=> installed "Monitoring Agent for UNIX OS  V06.23.01.00 for AIX R5.3 (64 bit)  AIX R6.1 (64 bit)".
... Initializing component Monitoring Agent for UNIX OS  V06.23.01.00 for AIX R5.3 (64 bit)  AIX R6.1 (64 bit).
... Monitoring Agent for UNIX OS  V06.23.01.00 for AIX R5.3 (64 bit)  AIX R6.1 (64 bit) initialized.



Do you want to install additional products or product support packages [ 1=Yes, 2=No ; default is "2" ] ?
... postprocessing; please wait.
... finished postprocessing.
Installation step complete.
```

Fig. 3.59 Instalación de agente de monitoreo en UNIX.

La instalación finaliza en un corto periodo de tiempo. Ahora es necesario configurar y activar el agente de monitoreo.

Configuración de los Agentes que monitorean las aplicaciones que corren sobre el Sistema Operativo UNIX.

El procedimiento para instalar los diferentes agentes que monitorean las aplicaciones que trabajan sobre el sistema operativo UNIX es básicamente el anteriormente descrito a diferencia del paquete de instalación, así como también el agente que se debe seleccionar.

En este apartado se detalla la configuración de estos agentes una vez que ya han sido instalados.

a) Configuración del agente de monitoreo de Sistema Operativo UNIX.

Una vez que se encuentra establecida la conexión al servidor es necesario dirigirse hacia la ruta de instalación en la carpeta bin (Figura 3.60). Se ejecuta el manejador de agentes como se muestra en la siguiente imagen.

```
# cd /opt/IBM/ITM/bin/
# ./itmcmd manage
```

Fig. 3.60 Comando para iniciar el manejador de Agentes.

Una vez abierta la ventana se selecciona el agente, se da clic derecho sobre él y se presiona configurar (Figura 3.61).

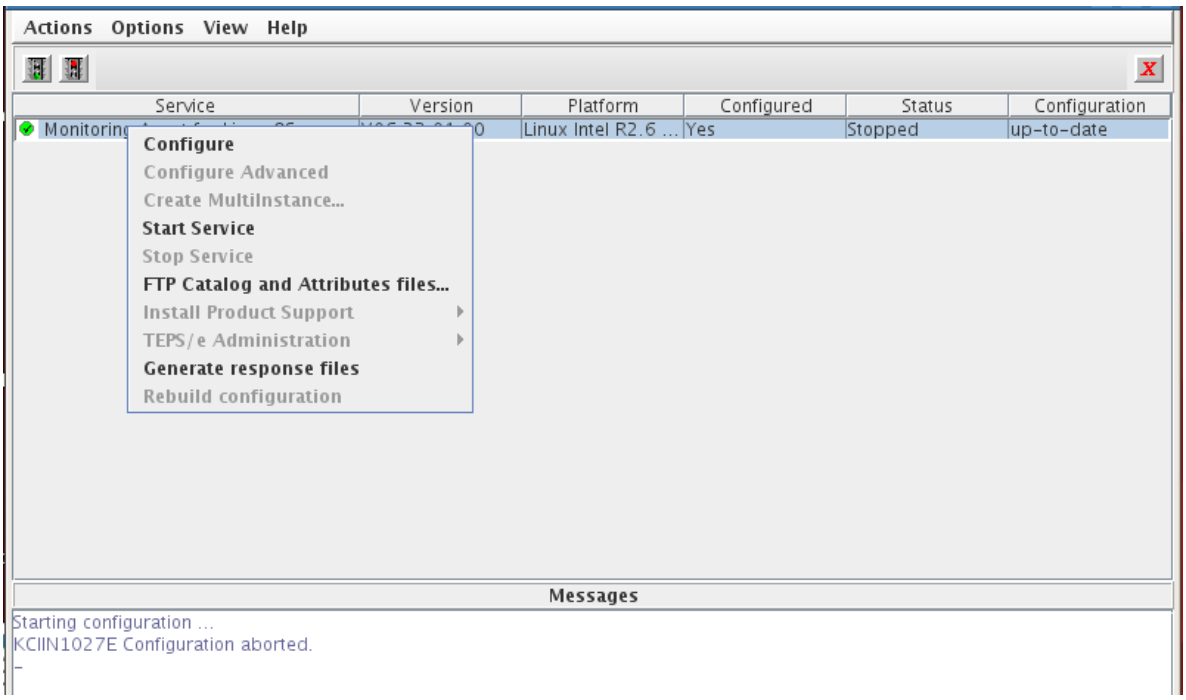


Fig. 3.61 Manejador de agentes.

Para este agente, al igual que para los demás agentes de sistema operativo (Linux y Windows) únicamente se configura la conexión con el TEMS. Indicando la IP del TEMS y el puerto de comunicación. Así queda configurado el agente de SO UNIX (Figura 3.62).

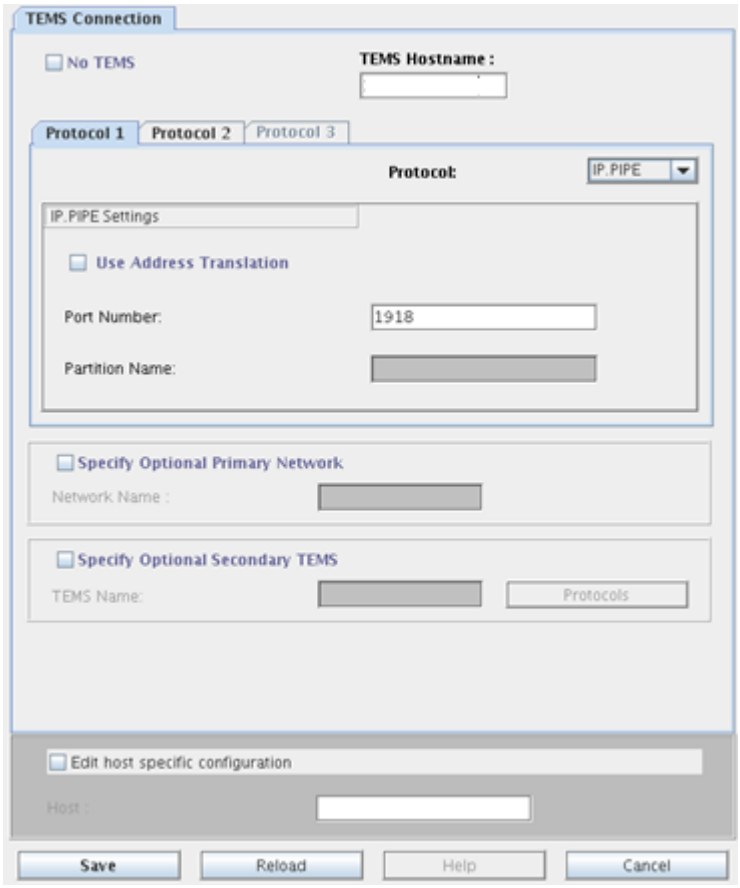


Fig. 3.62 Configuración de la conexión con el TEMS.

Finalmente se regresa a la ventana del manejador de agentes (Figura 3.63) y dando doble clic sobre el agente de monitoreo se inicia cambiando el ícono de dicho agente.

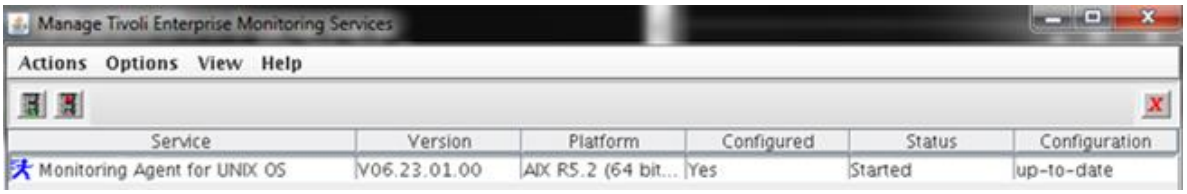


Fig. 3.63 Configuración de la conexión con el TEMS.

b) Configuración del agente de monitoreo de Oracle Database.

Se inicia el manejador de agentes como se detalla en la figura 3.60. Se selecciona el agente de monitoreo de Oracle Database y se presiona configurar (Figura 3.64).

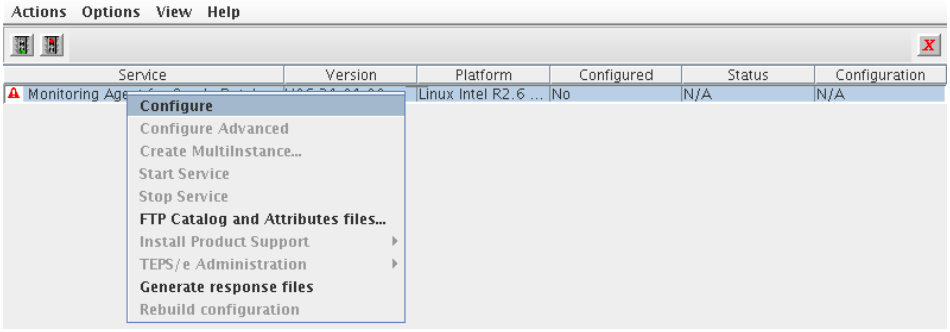


Fig. 3.64 Configuración de la conexión con el TEMS.

Se abre la siguiente ventana en la cual se elige “Add instance” para agregar una nueva instancia para ser monitoreada (Figura 3.65).

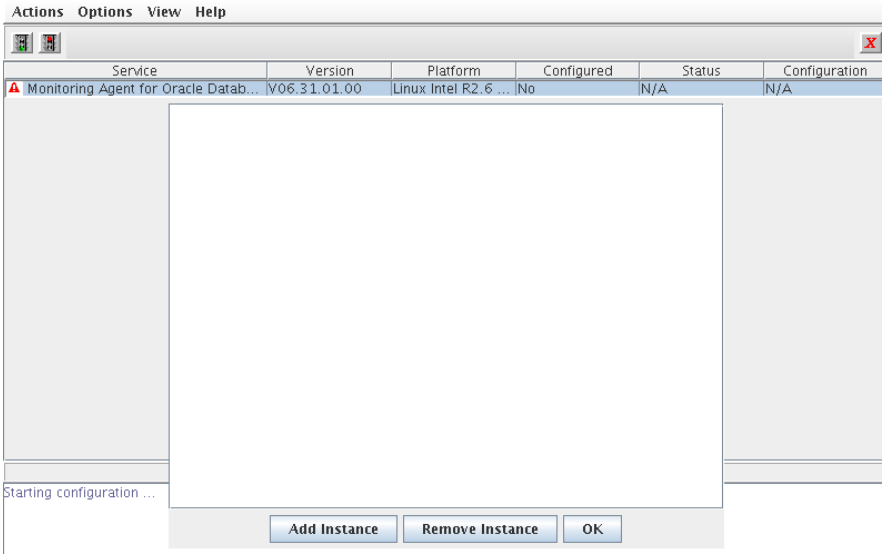


Fig. 3.65 Añadir una nueva instancia.

En la siguiente ventana (Figura 3.66) se ingresa el nombre de la instancia de la base de datos que se quiere monitorear.

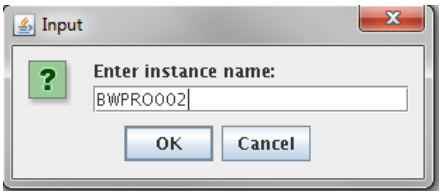


Fig. 3.66 Nombre de la instancia.

De igual manera es necesario crear un usuario administrador de la base de datos, necesario para el monitoreo. Las credenciales de dicho usuario se ingresan en la siguiente ventana (Figura 3.67) que se abre al presionar “OK” en el cuadro anterior. Así mismo se elige la opción “Use libraries in Oracle instant client”.

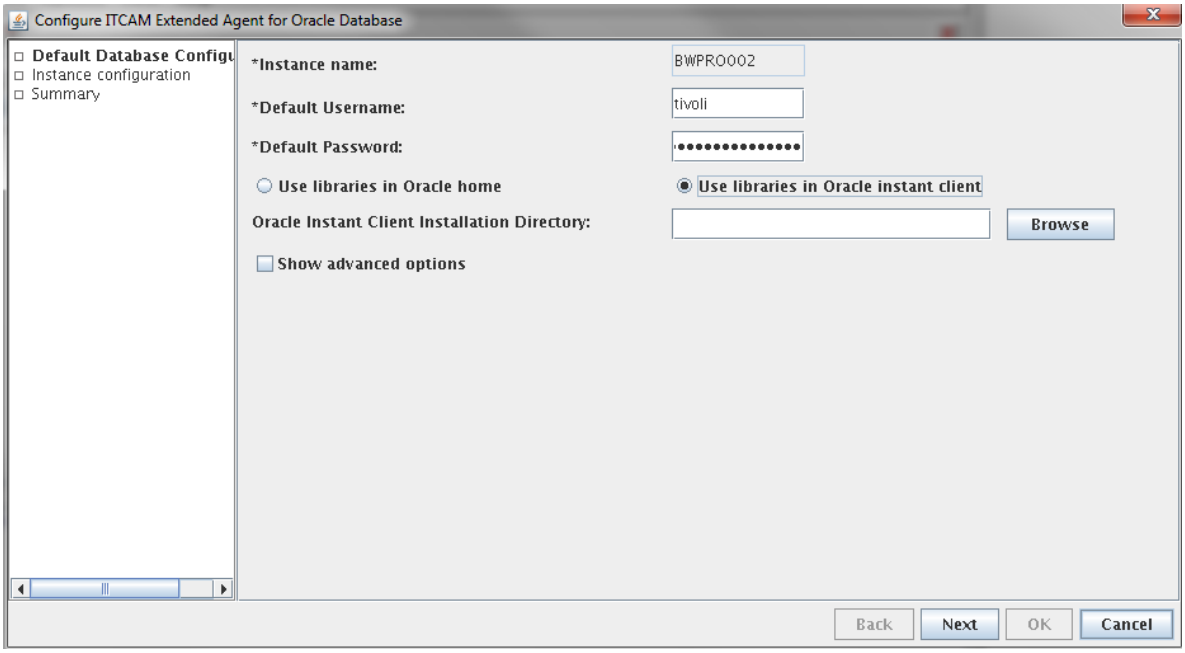


Fig. 3.67 Nombre de la instancia.

En la misma ventana se presiona “Browse” y se busca el directorio donde se encuentran las librerías del cliente de Oracle que generalmente es “/oracle/client/10x_64/instantclient_10205”. (Dependiendo de la versión de la Base de Datos, dicho directorio cambia). Una vez seleccionado se presiona “Open”. Y posteriormente se dio clic en “Next” (Figura 3.68).

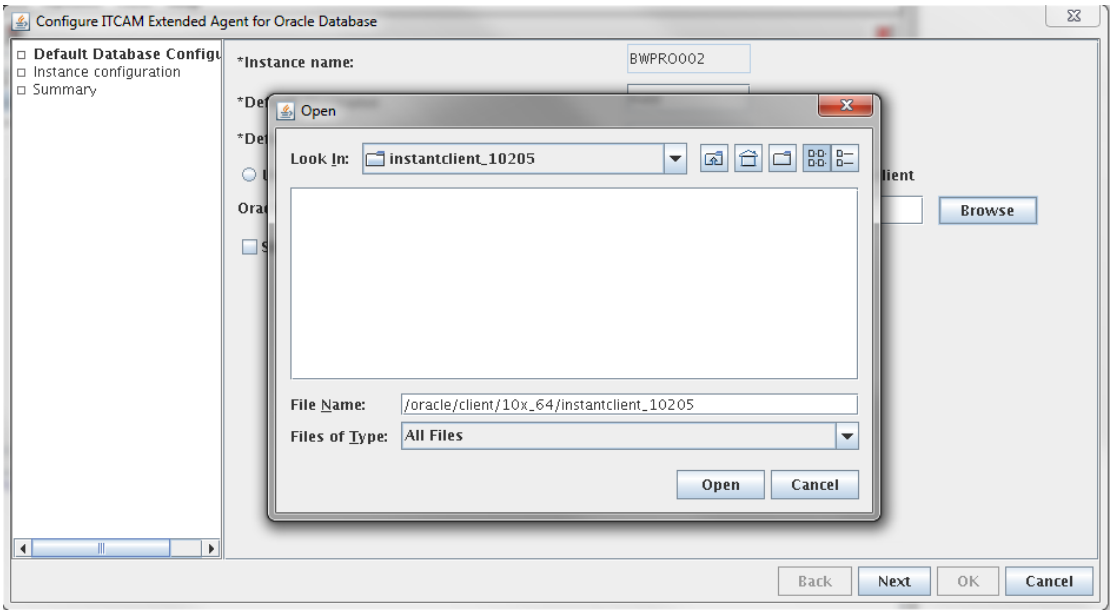


Fig. 3.68 Directorio de la librería de cliente de Oracle.

En la siguiente pantalla (Figura 3.69) se ingresan los detalles de la conexión con la base de datos. Se da clic en “New” y se procede a ingresar los datos en el formulario que aparece debajo.

En primer lugar se ingresa el nombre de la conexión con la base de datos que para poderla identificar en algún momento dado se nombró como tivoli.

En el siguiente campo se introduce un arreglo de caracteres con el siguiente formato: //<hostname>:<port>/<service ID>

Donde el “hostname” es el nombre de la máquina. “Port” es el puerto del servicio y “Service ID” es el identificador del servicio.

Se deja el Role en “DEFAULT” y se presiona “Apply” para que guarde los datos.

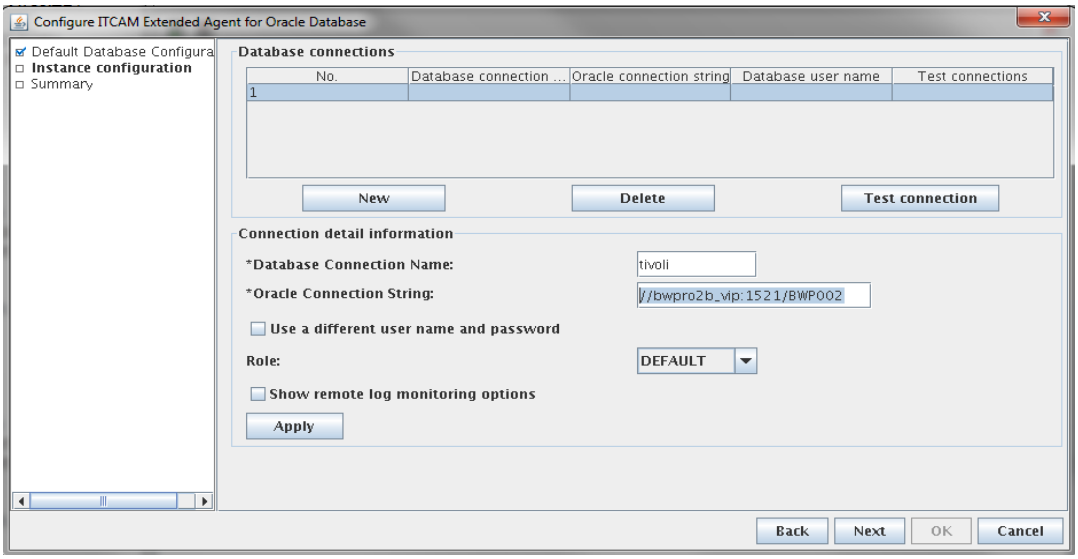


Fig. 3.69 Conexión de la bases de datos.

Para cerciorarse de que los datos ingresados son los correctos, se presiona el botón “Test connection”. Se abre un cuadro de dialogo en el que se indicaba si la conexión era exitosa o si existía algún problema (Figura 3.70).

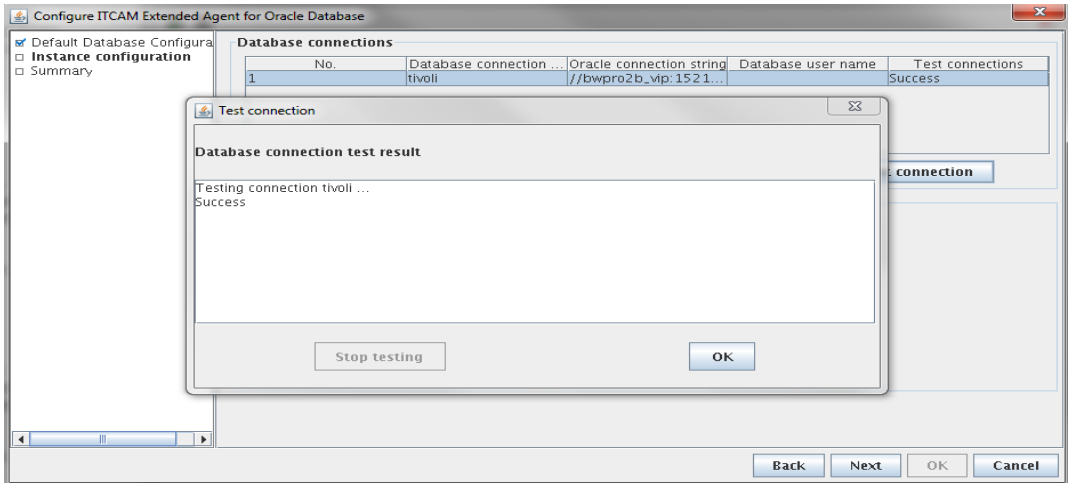


Fig. 3.70 Conexión exitosa.

Se presiona “OK” y posteriormente “Next”. Finalmente muestra el resumen de lo que se ha configurado (Figura 3.71).

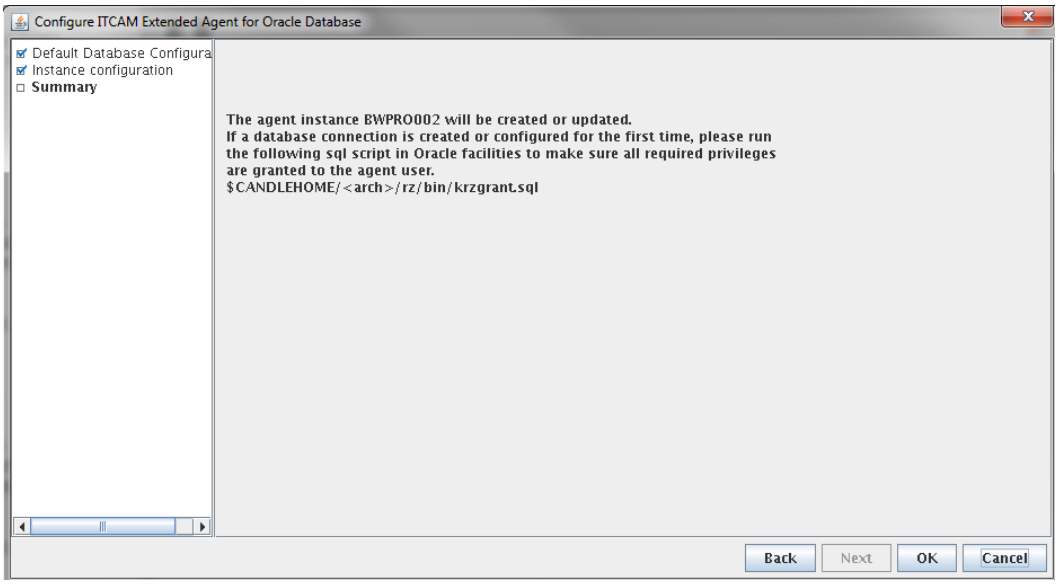


Fig. 3.71 Resumen de la configuración

Al presionar OK se muestra la ventana de configuración de la conexión con el TEMS que ya se detalló en la figura 3.62. Con esto finaliza la configuración del agente de monitoreo de Oracle DB.

c) Configuración del agente de monitoreo de SAP

Para configurar al agente de monitoreo de SAP es necesaria la creación de un usuario dentro de la plataforma para que el agente de monitoreo pueda autenticarse, es decir, el usuario creado para el monitoreo cuenta con todos los permisos sobre el sistema SAP.

Para iniciar es necesario posicionarse en la carpeta “bin” que se encuentra dentro de la ruta de instalación del agente. Una vez ahí se inicia el manejador de agentes como se muestra en la figura 3.60. Dentro de dicho manejador se seleccionó el agente de monitoreo de SAP, se da clic derecho sobre él y se elige configurar (Figura 3.72).

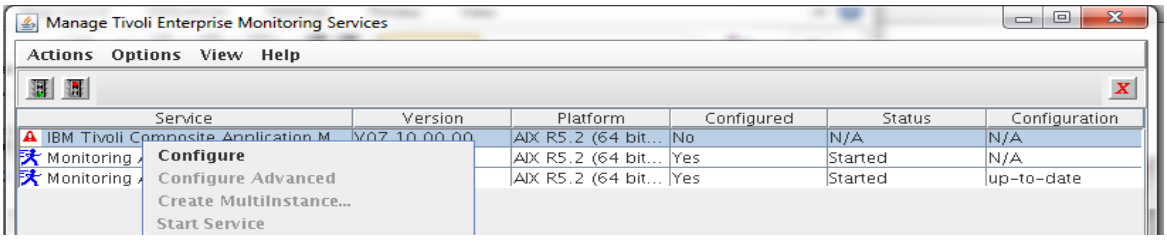


Fig. 3.72 Agente de monitoreo SAP

En la siguiente ventana (Figura 3.73) se da clic en “Add Instance” y en la ventana que aparece se agrega el nombre de la instancia de SAP del servidor.

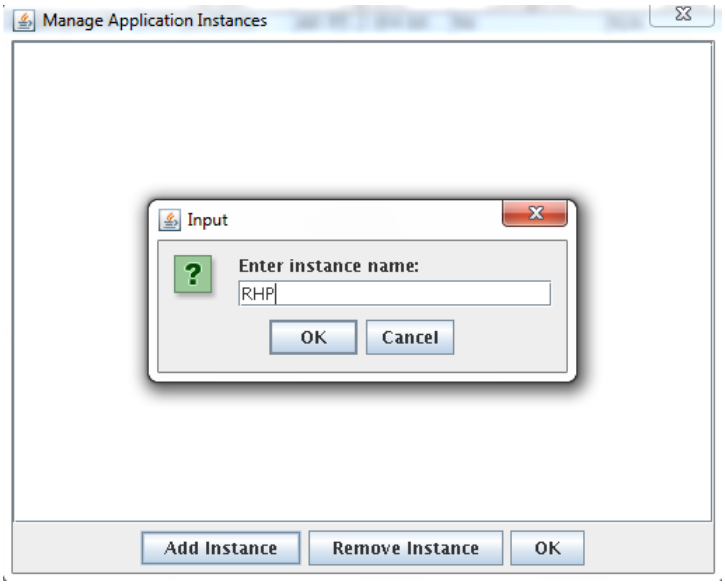


Fig. 3.73 Instancia SAP

Después de lo anterior aparece la siguiente ventana en la que se configuran algunos parámetros de la instancia. En la primera pantalla (Figura 3.74) se dejan los datos por default y se presiona siguiente.

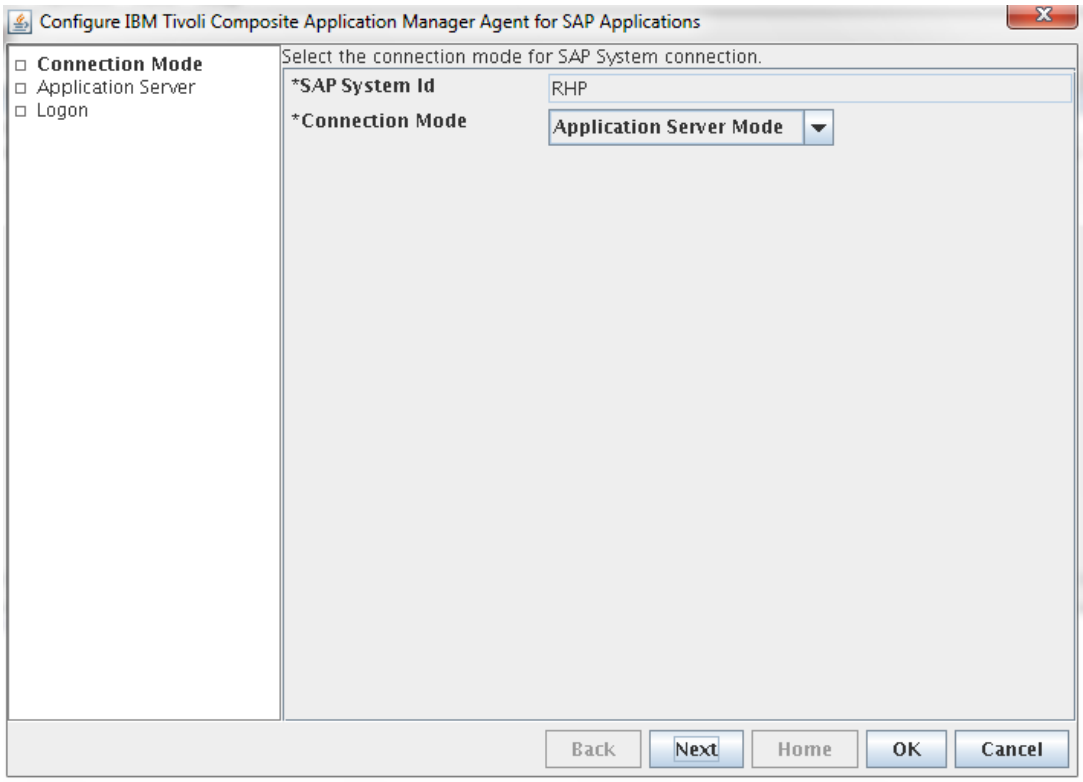


Fig. 3.74 Connection Mode Instancia SAP

En la siguiente pantalla (Figura 3.75) sólo se editan 2 parámetros: el “SAP Hostname” que en este caso es el nombre del servidor y el “SAP Gateway Name” que es el nombre de la puerta de enlace. Los demás parámetros se dejan por default.

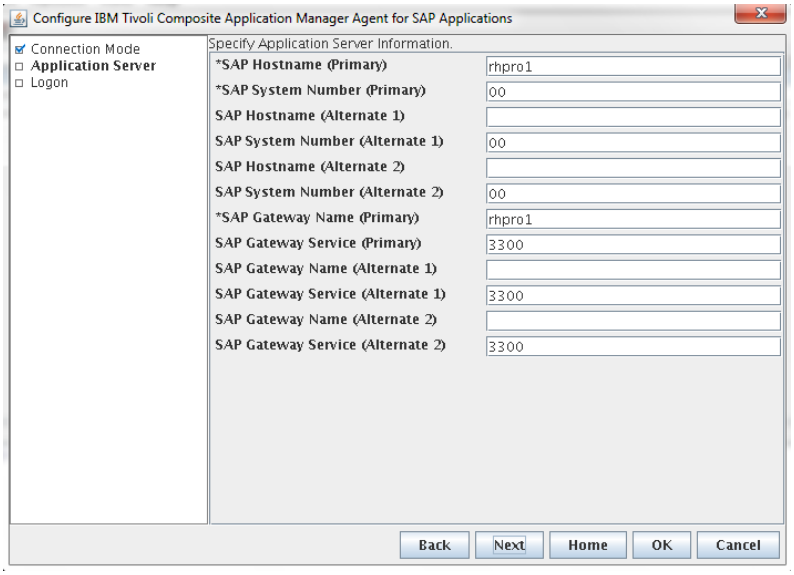


Fig. 3.75 Application Server Instancia SAP

Se da clic en next y muestra la siguiente ventana (Figura 3.76) en la cual se editan los parámetros de la autenticación. Para esto, se ingresa en “SAP User Id” y “SAP User Password”. Así mismo se indica el número de cliente y el SAP Language Code. Características de la configuración de la instancia de SAP. Se marca la casilla de RFC Trace. Y para verificar que toda la configuración fuera correcta se da clic sobre “Test Connection”.

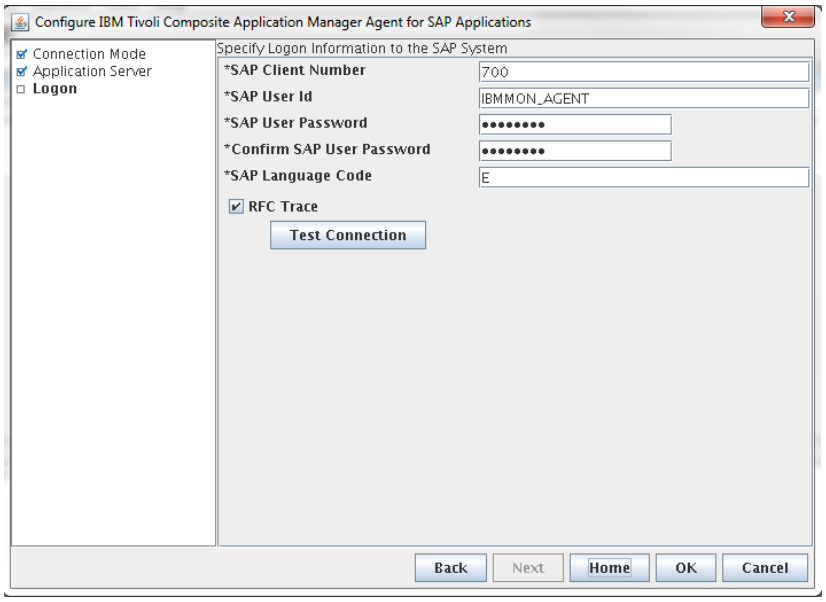


Fig. 3.76 Loggon Instancia SAP

Si todos los campos eran llenados correctamente, mandaba un mensaje de que la conexión era exitosa (Figura 3.77).

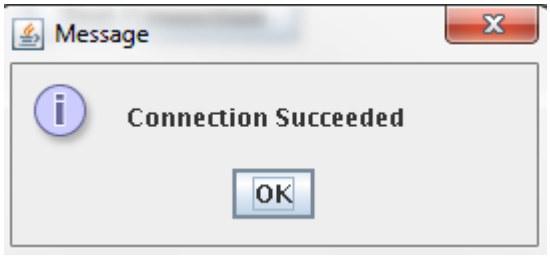


Fig. 3.77 Conexión exitosa Instancia SAP

Finalmente se edita la conexión del agente con el servidor TEMS como se muestra en la figura 3.62. Después de esto el agente se encontraba configurado y listo para iniciarse.

Capítulo IV
Resultados

4.1 Introducción

El principal objetivo de la implementación de una herramienta de monitoreo es la alta disponibilidad de los servicios del área de Tecnologías de la Información.

Tener los diversos servidores monitoreados, ayuda a los administradores de infraestructura a prevenir problemas. Solucionar los potenciales problemas antes de que estos sucedan le da al área de TI una alta confiabilidad. De igual forma, tener identificadas las causas del problema ayuda a solucionar el mismo.

Los resultados de esta implementación se basan en 2 aspectos importantes: Los workspace y las situaciones. Los primeros sirven para tener una visión general, ya sea de un equipo en particular o de todos los equipos en general. Las segundas sirven para alertar los problemas o posibles problemas que pudieran ocurrir.

Para poder acceder al portal de monitoreo existen 2 formas: para la primera es necesario contar con un navegador de internet, ya sea Microsoft Internet Explorer o Mozilla Firefox. La segunda es tener la aplicación TEP instalada.

Se ingresa a la página https://<IPdelServidorTEPS>:1920/ y se da clic en “IBM Tivoli Enterprise Portal Web Client” si se desea ingresar vía web o “IBM Tivoli Enterprise Portal Webstart Client” si se desea iniciar la aplicación de escritorio (Figura 4.1).

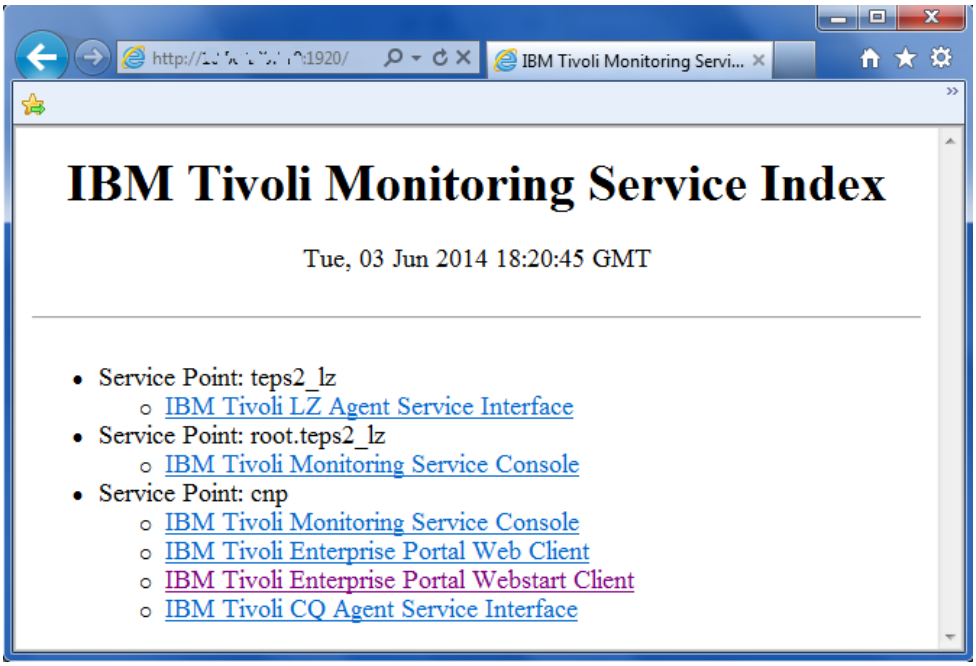


Fig. 4.1 Pagina TEPS.

Para ambas opciones se deben ingresar las credenciales de usuario (Figura 4.2). Por default se crea un usuario Administrador, posteriormente se pueden crear múltiples usuarios con privilegios diferentes.

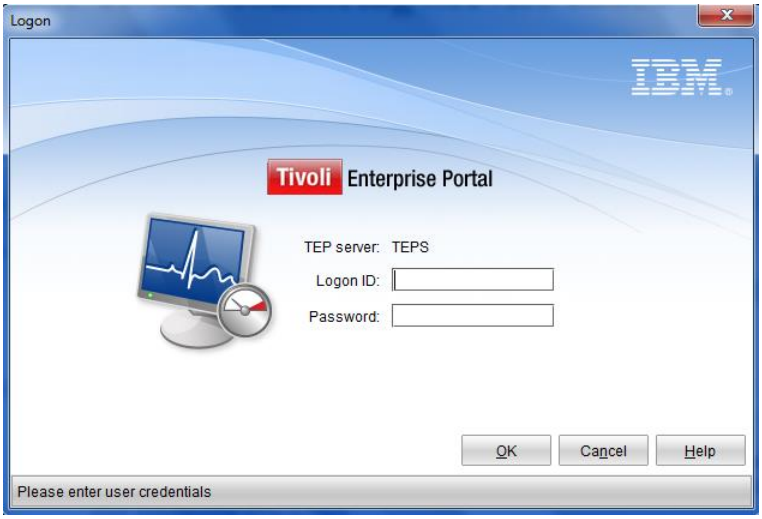


Fig. 4.2 Logon TEPS.

Una vez ingresando el ID y el Password correcto se abre la siguiente ventana en la cual se encuentra una visión general del monitoreo (Figura 4.3). Del lado izquierdo están unas listas desplegables de los servidores organizados por sistema operativo (Linux, UNIX y Windows). De lado derecho se pueden encontrar alertas que van surgiendo en tiempo real de los sistemas y aplicaciones monitoreados.

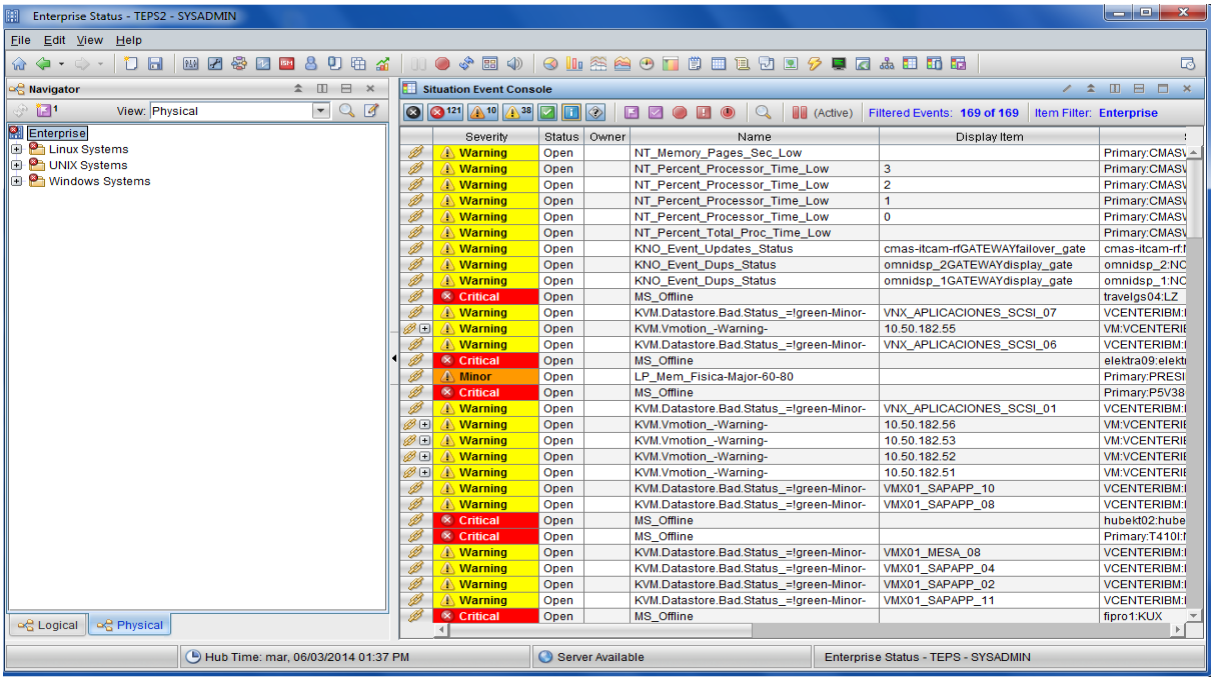


Fig. 4.3 Panel principal de monitoreo.

Si se expanden las carpetas que se encuentran del lado izquierdo dando clic sobre el icono de “+” se puede observar la lista de servidores que se encuentran monitoreados y separados por el tipo de sistema operativo. De igual forma se pueden ver las aplicaciones que se están monitoreando en cada servidor (Figura 4.4).

Si algún agente de monitoreo se encuentra fuera de servicio se muestra de un color grisáceo, dando a entender que por algún motivo ese agente de monitoreo está deshabilitado.

En la parte superior del lado derecho se puede elegir qué tipo de alertas se desean visualizar (Critical, Warning o Minor). De igual forma se puede observar la severidad, el nombre de la alerta (situación) y demás características que la alerta pueda tener.

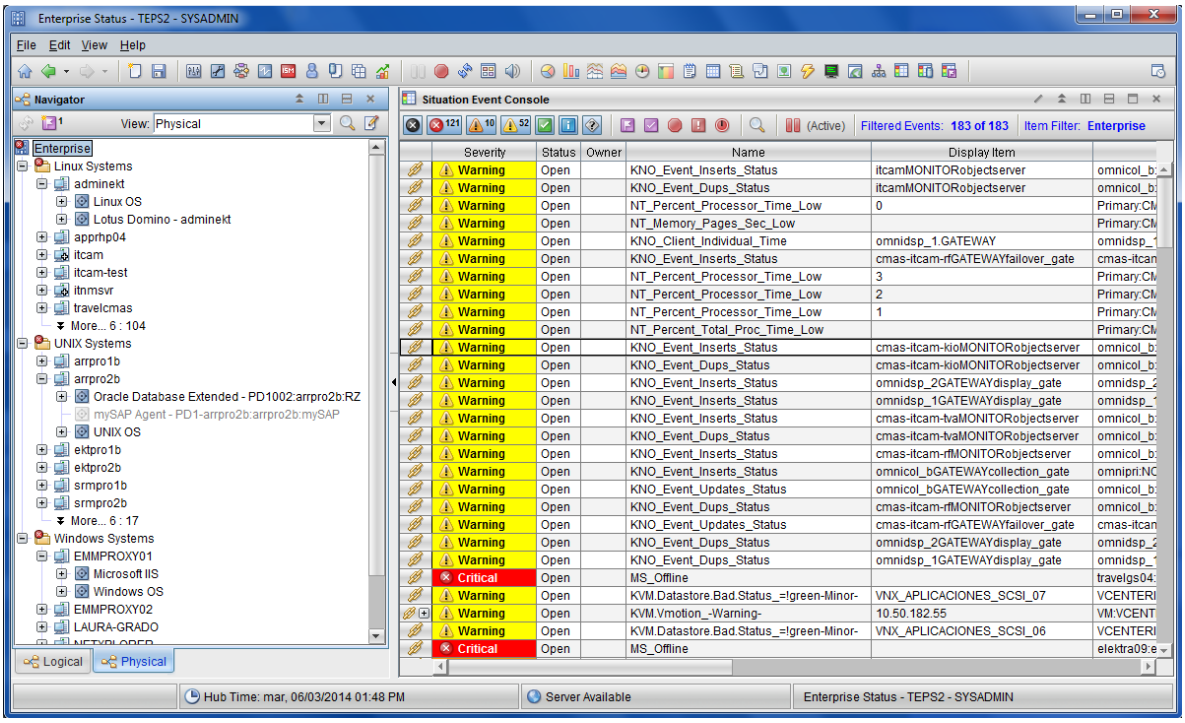


Fig. 4.4 Lista de servidores y sus aplicaciones.

Esta es una visión general del resultado de la implementación de ITM. A continuación se detallan los dos principales beneficios de lo implementado, los workspace y las situaciones.

4.2 Workspace

El workspace es un marco personalizable en el cual se puede analizar los diferentes sistemas operativos y sus aplicaciones para las cuales se ha instalado

un agente de monitoreo. Estos Workspace están definidos por default y agrupan atributos que tienen una estrecha relación entre sí.

Los workspaces se pueden modificar e incluso es posible crear nuevos workspaces, dentro de los cuales, las tablas de atributos se pueden graficar de diferentes maneras. En la siguiente imagen (Figura 4.5) se pueden ver los diferentes nombres de los grupos de workspace que contienen los agentes de SO Linux y Lotus Domino, solo por mostrar algunos ya que cada agente tiene sus propios grupos de Workspace diseñado a necesidades estándar de las aplicaciones.

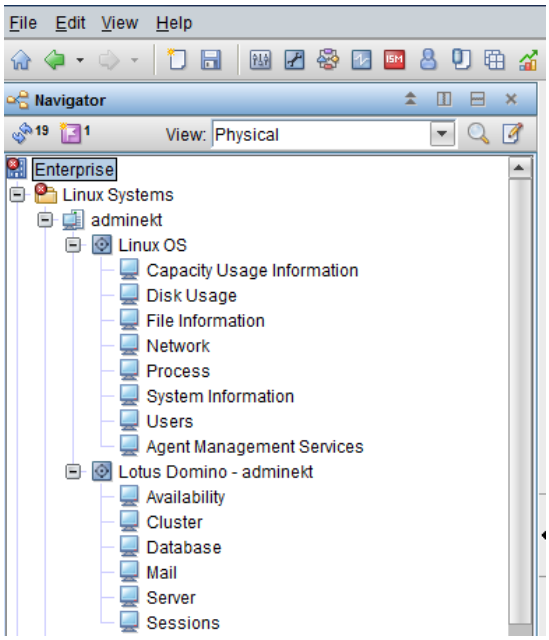


Fig. 4.5 Nombres de los Workspace.

Si se da clic derecho sobre un grupo de workspace aparecen los distintos workspaces prediseñados por IBM. Al seleccionar alguno de estos aparece con una paloma del lado izquierdo y muestra una serie de tablas y gráficas propias del workspace (Figura 4.6).

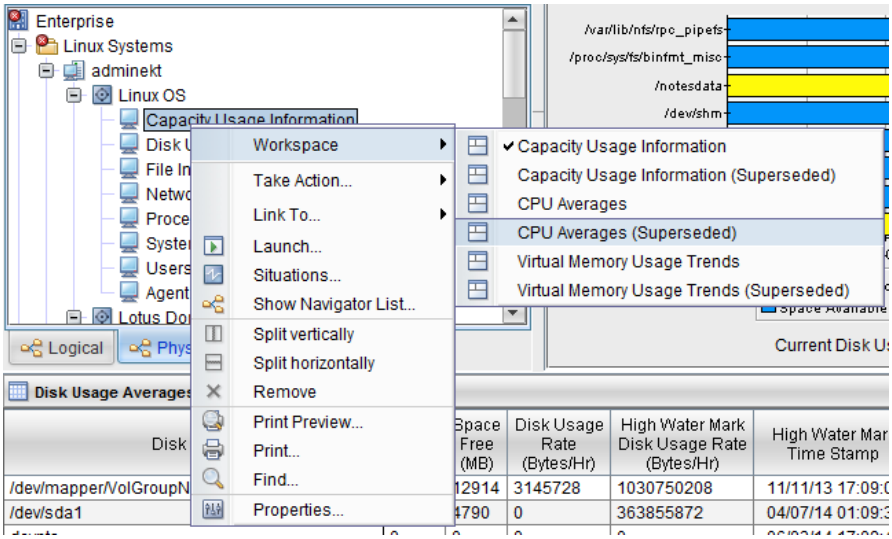


Fig. 4.6 Nombres de los Workspace.

La siguiente imagen (Figura 4.7) es un ejemplo de cómo se visualiza el workspace del Sistema Operativo Linux en el apartado de “Disk Usage” (uso de disco). Aquí se muestran los puntos de montaje con los que cuenta el Servidor (Tabla inferior izquierda) y el uso de estos (gráfica inferior derecha).

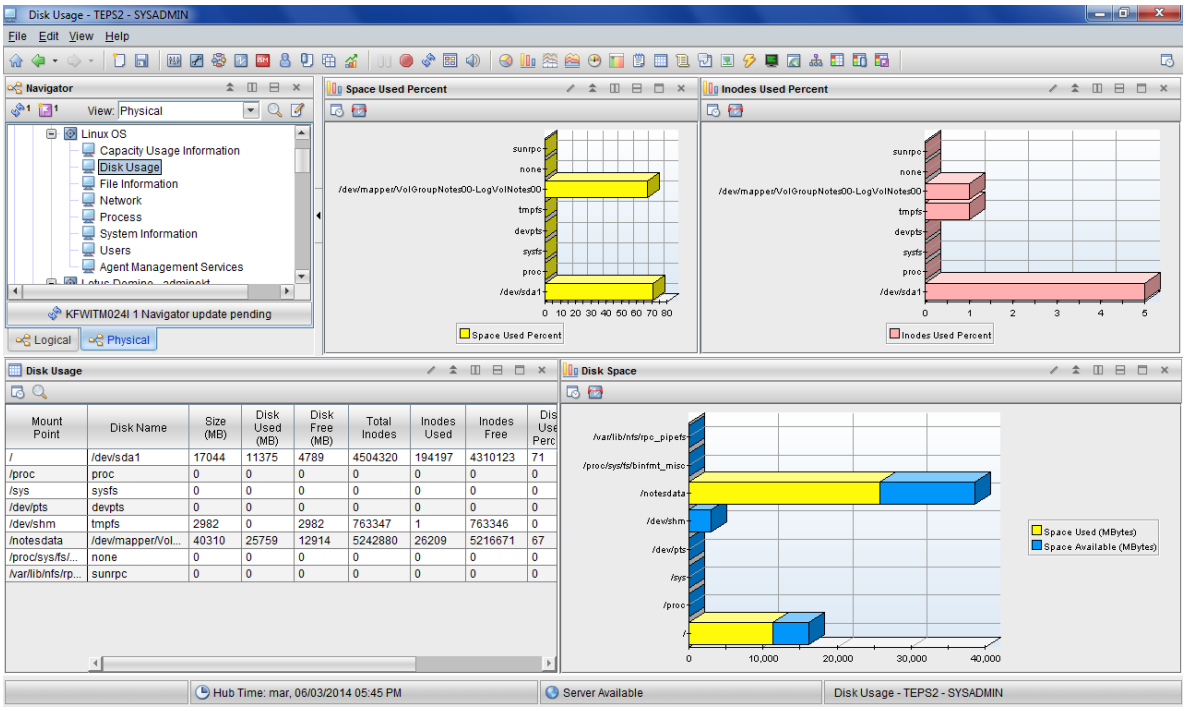


Fig. 4.7 Workspace Disk Usage.

Como se puede notar en estas imágenes, estos workspace sirven para que el administrador del sistema operativo o los expertos de las aplicaciones tenga una visión general de sus sistemas y puedan hacer un análisis de posibles riesgos o de posibles causas de sus actuales problemas.

Todas estas posibilidades dentro de una herramienta de fácil acceso y muy gráfica. Se pueden enlistar entonces algunos de los beneficios que la implementación ha originado:

- Mayor eficiencia del personal.
- Herramienta para el análisis de los administradores.
- Menor tiempo de respuesta de los administradores a los problemas.
- Prevención de Problemas.
- Reducción de fallas en los sistemas.
- Alta disponibilidad de los sistemas.
- Optimización de los recursos de TI

4.3 Situaciones

Las situaciones, en la herramienta de ITM, son una regla o un conjunto de reglas que se tienen que cumplir para que el TEPS muestre una alerta en la consola de monitoreo.

Como los workspace, las situaciones, vienen predefinidas en la instalación de los soportes de los agentes dentro del servidor TEMS y TEPS. Así mismo, estas pueden ser modificadas y creadas para la personalización del monitoreo como un sistema a medida.

La personalización de estas situaciones es tan detallada al grado de poder ser aplicadas a solo un servidor, a un grupo de estos o a todos los servidores que tengan instalado el mismo agente de monitoreo.

Como podemos visualizar en la siguiente imagen (Figura 4.~~4~~8) las situaciones que han generado una alerta aparecen del lado derecho de la consola de monitoreo del TEPS.

Para visualizar las situaciones existentes relacionadas con algún equipo es necesario situarse en dicho equipo y dar clic derecho sobre él y posteriormente hacer clic sobre situaciones (Figura 4.8).

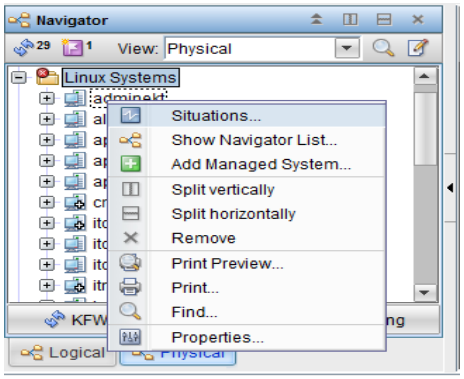


Fig. 4.8 Situaciones.

Entonces se abre el editor de situaciones en el cual se puede observar qué situaciones se encuentran disponibles para este sistema. En este caso se selecciona el servidor llamado “adminekt” al cual se le pueden activar alertas de Sistema Operativo Linux y alertas de Lotus Domino como se puede observar del lado izquierdo de la siguiente imagen (Figura 4.9). Al desplegar la lista se mostrarán las situaciones activas en color verde y las situaciones deshabilitadas en color gris.

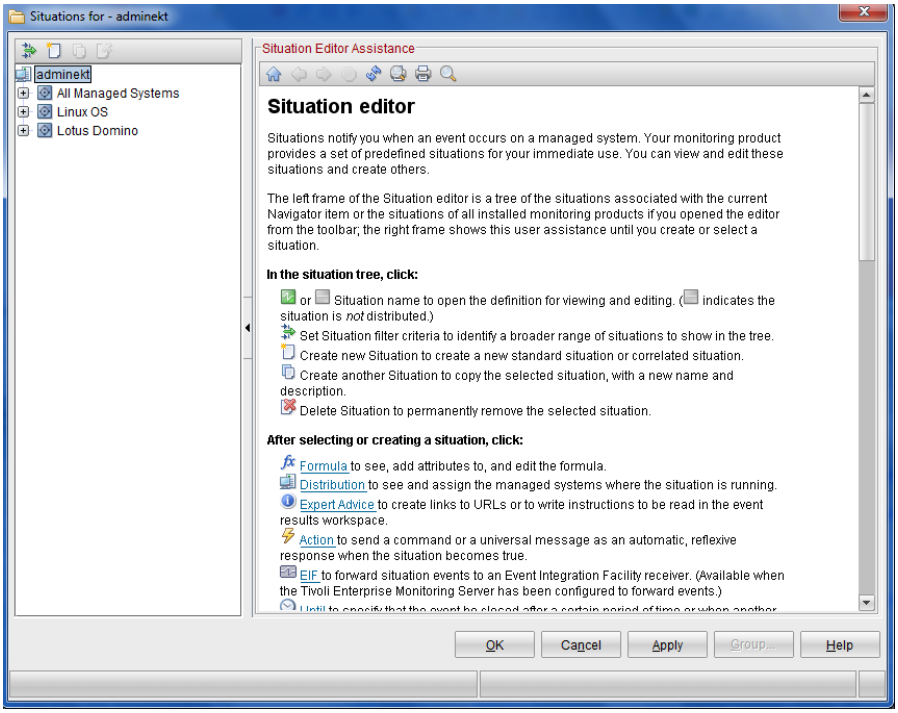


Fig. 4.9 Situaciones.

Al seleccionar la situación se pueden ver sus características y editarlas (Figura 4.10). Entre estas características se encuentra el nombre de la situación, así como también una descripción. Debajo de estos apartados se muestra la formula en la cual aparecen en forma de tabla los atributos a monitorear. En este caso el porcentaje de uso del CPU y el identificador del CPU.

El primer atributo indica que tiene que ser menor a 10%. El segundo atributo designa que el identificador del CPU es “Aggregate”, es decir, el acumulado de los identificadores. Cuando todos los núcleos del procesador estén trabajando arriba del 90% la situación generará una alerta.

Si se presiona en “Advanced” mostrará cuántas revisiones tiene que realizar antes de mandar la alarma. En este caso con una vez que encuentre trabajando el CPU al 90% alertará. Si este dato se cambiara por el número 5; a la quinta vez que encuentre el CPU arriba del 90%, se informaría que esta situación se está presentando.

En el apartado de “Sampling Interval” se puede elegir con precisión de segundos, cada cuánto tiempo la situación estará verificando estos valores. En este particular caso, la situación estará verificando que el Procesador del Servidor no esté por encima del 90% de uso cada 15 minutos.

Así mismo se puede elegir, si es que se desea, que se reproduzca algún sonido en la consola del TEPS si esto ocurre. En esta implementación en particular se ha deshabilitado esta opción.

Por último se puede seleccionar la criticidad de esta situación. Si lo que se alarma es Fatal, Critical, Minor, Warning, Harmless, Informational o Unknown. En este caso se selecciona Critical.

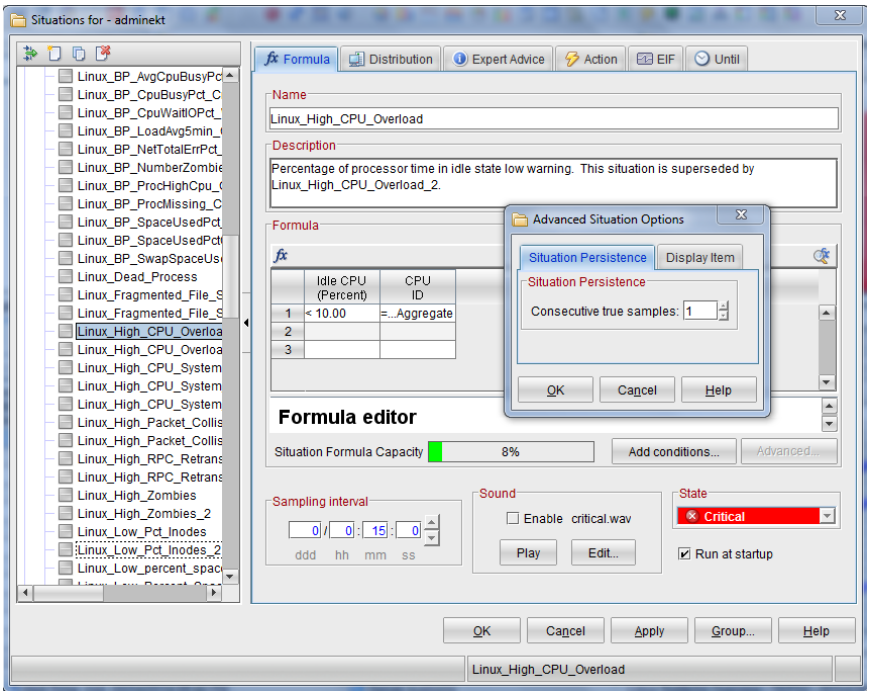


Fig. 4.10 Editor de Situaciones.

En la pestaña de “Distribution” (Figura 4.11) se puede elegir a qué servidores se aplica esta situación. Por ejemplo, si se tienen servidores que siempre presentan un alto consumo de CPU se pueden dejar fuera de esta lista, puesto que ese sería un comportamiento normal y no sería útil alarmar un comportamiento normal.

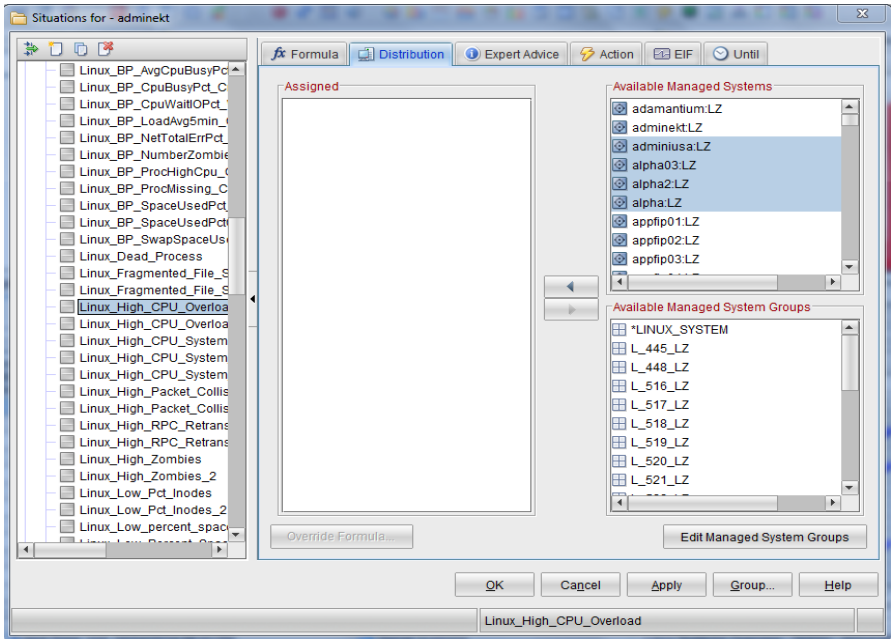


Fig. 4.11 Distribución de las Situaciones.

De igual forma, al dirigirse a la pestaña llamada “Action” (Figura 4.12) se puede ejecutar un comando en el servidor si esta situación se presenta. En el recuadro debajo de “System Command” se ingresa el comando a ejecutar, tal cual como si se estuviera en la línea de comandos del servidor. Esto puede servir ya que si se conoce la causa que detona una situación en particular y su respectiva solución, se puede ejecutar un script dentro del servidor que resuelva ese determinado problema.

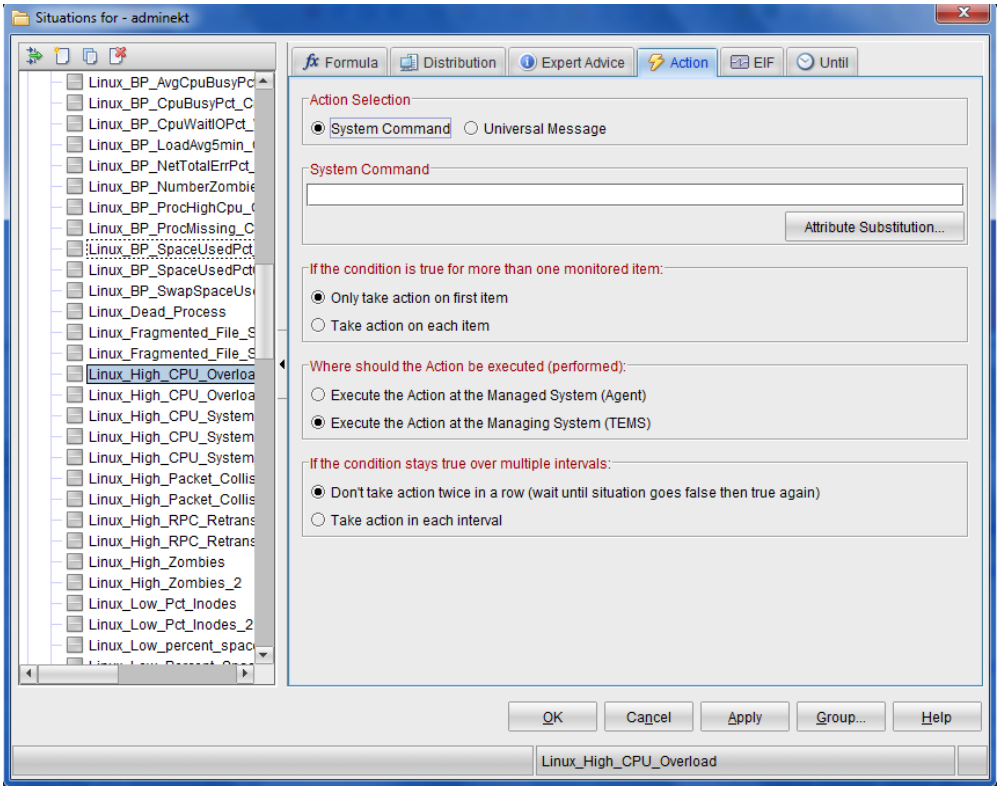


Fig. 4.12 Distribución de las Situaciones.

Al presionar el ícono de “Apply” se guarda la configuración de la situación modificada.

La personalización de las situaciones es a tal grado que se tiene la oportunidad de monitorear todas las variables que el agente recoge del sistema operativo o de las aplicaciones que en él residen. Para dichas variables se puede establecer cualquier umbral y un periodo de muestreo. De igual forma, se cuenta con la posibilidad de verificar una o más variables dentro de la misma situación.

Por ejemplo, si se requiere monitorear un servidor con alto uso de sus recursos, se puede verificar el CPU, la memoria RAM y el disco duro en una misma situación. Alertar si alguna de estas 3 se cumple o si las 3 se cumplen al mismo tiempo según requiera el cliente.

De esta forma se puede enlistar los beneficios que un posible cliente es capaz de conseguir con la implementación de las situaciones:

- Prevención de pérdida de datos.
- Prevención de pérdida de servicio
- Histórico de sucesos que pudieron suscitar un problema para un mejor análisis a posteriori.
- Tener mejor disponibilidad de los servicios
- Mejor rendimiento de los sistema.

Conclusiones

Conclusiones

A lo largo de esta tesis se ha descrito un panorama general de lo que el monitoreo de servidores puede representar para una institución. Actualmente cualquier organización, incluso si no se dedica al ramo de las tecnologías de la información, necesita de sistemas informáticos para mantener en funcionamiento toda su infraestructura.

Desde lo más simple y cotidiano como un correo electrónico, hasta lo más complejo y especializado como transacciones bancarias. Tener vigilados sus sistemas informáticos siempre será de vital importancia.

De igual forma, se ha mostrado un panorama general de la herramienta IBM Tivoli Monitoring, que por su personalización, su alcance y los resultados que entrega se ha elegido como motivo de estudio de esta tesis.

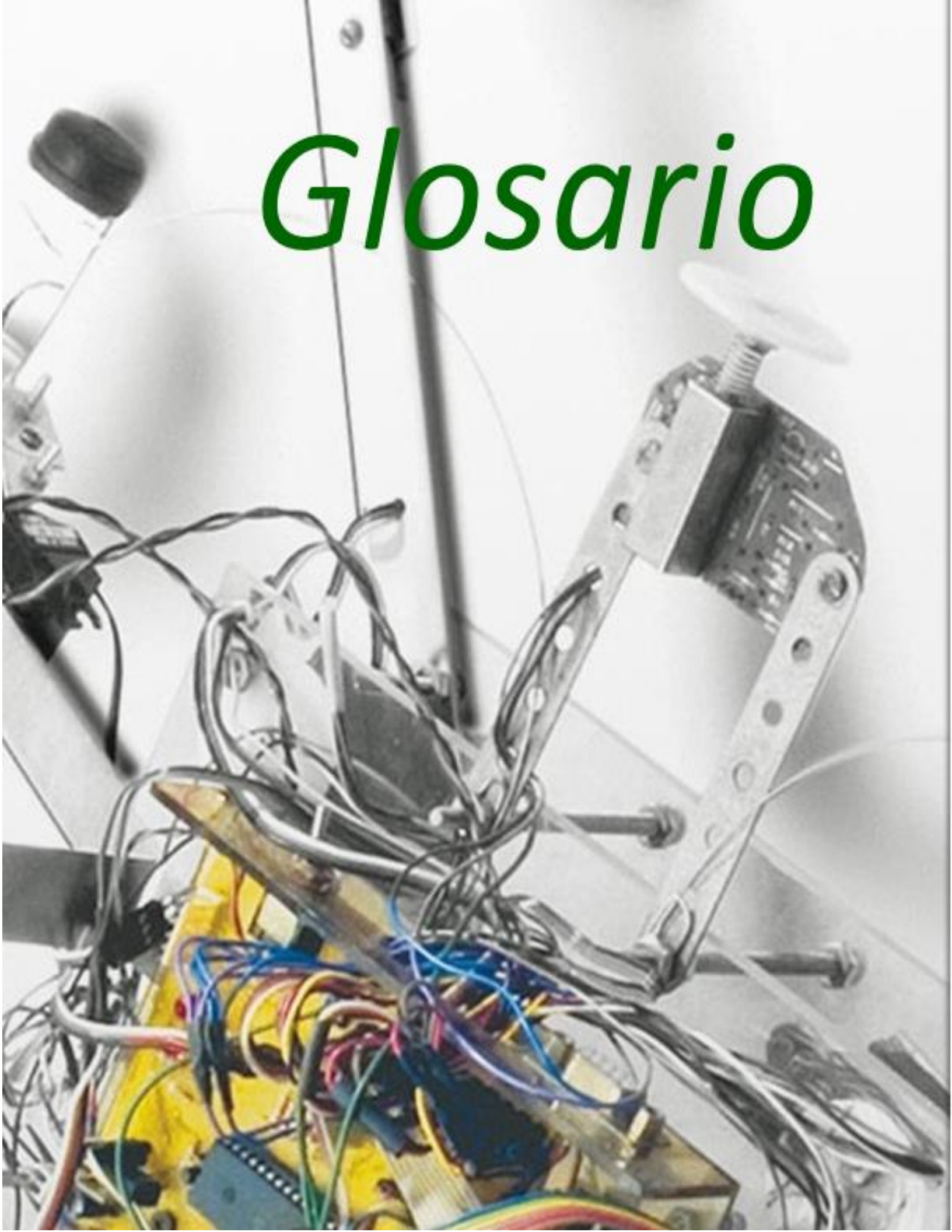
Mediante la ejemplificación de una instalación de esta herramienta se ha demostrado que pese a no ser una instalación sencilla, permite adaptarse a los diferentes sistemas operativos que se encuentran vigentes en la industria. Con esto, la herramienta obtiene un alcance de monitoreo mucho mayor que otras herramientas existentes en el mercado que solo se enfocan a una parte específica de la infraestructura como las redes.

Por tales motivos se puede fácilmente apreciar que es una herramienta tan robusta y especializada que está pensada únicamente para grandes organizaciones con sistemas tecnológicos de gran magnitud.

De igual forma, para poder aprovechar todo el potencial que esta herramienta de monitoreo brinda, se debe tener una infraestructura tecnológica grande y diversa. Así mismo, se debe considerar la relación costo-beneficio para que sea rentable implementar esta herramienta de monitoreo.

En conclusión, para una empresa grande suele ser redituable el tener implementada una herramienta de gran magnitud como lo es IBM Tivoli Monitoring pues se logran evitar grandes problemas. Por ejemplo, en las instituciones bancarias el costo de comprometer la información tanto la de los clientes como de la misma institución pone en un alto riesgo a la entidad financiera; se pone en juego dinero y el prestigio, aspectos primordiales en el éxito de cualquier banco.

Glosario



Glosario

ARP (Address Resolution Protocol – Protocolo de resolución de direcciones) permite determinar la dirección MAC del nodo a partir de su dirección IP efectuando una difusión.

Agente Los Agentes de Tivoli Enterprise Monitoring, son programas instalados en los sistemas o subsistemas que se desea supervisar. Estos agentes recopilan datos de sistemas supervisados o gestionados y distribuyen esta información a un servidor de supervisión o a un recopilador de sucesos SNMP como IBM Tivoli Netcool/OMNIbus.

CAN (Campus Area Network – Red de Área Campus) es la red cuya extensión es la de un campus universitario, una base militar, un polígono industrial o un grupo de grandes edificios en un área geográfica limitada.

CPU (Central Processing Unit – Unidad central de proceso) es la parte de una computadora en la que se encuentran los elementos que sirven para procesar los datos.

CRM (Customer Relationship Management – Gestión de relaciones con los clientes) es una estrategia de negocios dirigida a entender, anticipar y responder a las necesidades de los clientes actuales y potenciales de una empresa para poder hacer crecer el valor de la relación.

DB2 es una familia de productos de sistema de gestión de bases de datos relacionales (RDBMS) de IBM que sirve en varias plataformas de sistemas operativos (GNU Linux, Windows y UNIX).

DDR2 (Double Data Rate - Doble velocidad de datos) son una mejora de las memorias DDR. En ellas los búfers de entrada/salida trabajan al doble de la frecuencia del nucleo, permitiendo que durante cada ciclo de reloj se realicen cuatro transferencias.

DDR3 (Double Data Rate - Doble velocidad de datos) es el sucesor de las memorias estrándar DDR2 puesto que tiene mejor rendimiento en niveles de bajo voltaje; funciona a 1.5V. De igual forma realiza ocho transferencias durante cada ciclo de reloj.

DHCP (Dynamic Host Configuration Protocol – Protocolo de Configuración Dinámica de Host) es un protocolo de configuración automático de las opciones TCP/IP para clientes de un entorno NetBIOS.

ECC (Error Correctin Code – Código de Corrección de errores) son memorias que tienen un sistema que permite detectar errores de datos y corregirlos. Este sistema las vuelve ligeramente más lentas pero suelen utilizarse en sistemas con aplicaciones críticas.

FTP (File Transfer Protocol – Protocolo de Transferencia de Archivos) es un protocolo de transferencia de archivos basado en un método fiable e implementado sobre TCP.

GB Un gigabyte es una unidad de medida de almacenamiento de información equivalente a 10^9 (mil millones) bytes.

HTTP (HyperText Transfer Protocol – protocolo de transferencia de hipertexto) es un protocolo sencillo del tipo cliente-servidor que articula los intercambios de información entre los clientes Web y los servidores HTTP. Este protocolo se basa en sencillas operaciones de solicitud/respuesta.

ICMP (Internet Control Message Protocol – Protocolo de Mensajes de Control de Internet) funciona a través de IP y da la información de los errores y controles a TCP.

IGMP (Internet Group Management Protocol – Protocolo de administración de grupos de Internet) pertenece a la capa de red y permite a una estación unirse o dejar a un grupo multidifusión (multicast).

IMAP (Internet Message Access Protocol – Protocolo de acceso a mensajes de internet) permite que se almacenen y que se conserven en el servidor de mensajería los mensajes electrónicos en lugar de transferirlo sistemáticamente hacia la estación cliente.

IP (Internet Protocol – Protocolo de Internet) es un estándar que se emplea para el envío y la recepción de información mediante una red que reúne paquetes conmutados.

ITM (IBM Tivoli Monitoring) Es una herramienta de software que supervisa el rendimiento y la disponibilidad de los sistemas operativos y las aplicaciones que en ellos residen.

LAN (Local Area Network - Red de Área Local) es la red que suele situarse en el mismo edificio o en entornos de unos 200m llegando al kilómetro cuando se usan repetidores.

MAN (Metropolitan Area Network – Red de Área Metropolitana) es la red que se sitúa en un barrio, urbanización, ciudad o municipio pequeño (a pocos kilómetros, normalmente oscila entre 1 y 7 Km).

MB Un megabyte es una unidad de medida de almacenamiento de información equivalente a 10^6 (un millón) bytes.

MHz Un megahercio es una unidad de medida de la frecuencia; equivale a 10^6 (un millón) hercios.

NTP (Network Time Protocol – Protocolo de Tiempo en Red) permite sincronizar los ordenadores que funcionan en una red. Para esto el equipo hace referencia a un servidor horario que puede comparar y ajustar su hora con otro servidor NTP en Internet.

PAN (Personal Area Network - Red de Área Personal) es la red inalámbrica de interconexión de periféricos que se puede encontrar tanto a unos pocos centímetros como a metros de distancia del emisor.

PC (Personal Computer- computadora Personal) Computadoras de tamaño medio diseñadas para ser usadas por un solo usuario a la vez.

Plugin Es una aplicación complementaria que se relaciona con otra para aportarle una función nueva y generalmente muy específica.

POP3 (Post Office Protocol 3 – Protocolo de Oficina Postal 3) se dedica específicamente a la publicación y al acceso a distancia a un servidor de mensajería. El servidor POP se comunica con el Agente Usuario (User Agent) a través de una conexión síncrona.

Probes Los Probes o también conocidos como sondas son dispositivos encargados de recolectar información de una red. Obedecen a una lógica que se encuentra especificada en un archivo de reglas.

RAM (Random Access Memory – Memoria de Acceso Aleatorio) es una memoria de tipo volátil, la información almacenada en ella se pierde al desconectarle la energía.

RARP (Reverse Address Resolution Protocol – Protocolo de resolución de direcciones inverso) efectúa una resolución inversa en el caso de que una estación sin disco quiera obtener una dirección IP a partir de la única información de la cual dispone, su dirección MAC.

RR. HH. El término recursos humanos (abreviado como RRHH, RH, RR.HH., y también conocido como capital humano) se originó en el área de economía política y ciencias sociales, donde se utilizaba para identificar a uno de los tres factores de producción, también conocido como trabajo (los otros dos son tierra y capital).

SAP (Systeme, Anwendungen und Produkte – Sistemas, Aplicaciones y Productos) Es un sitema de gestión empresarial ERP (Enterprise Resource Planning – Planificación de Recursos Empresariales) que administra los recursos financieros, recursos humanos, canales de ventas, proicesos de logística, manejo de stock, entre otros.

SAS (Serial Attached SCSI – SCSI conectada en serie) Es una interfaz de conexión que permite un incremento en la velocidad de la conexión SCSI además de permitir una conexión y desconexión de los dispositivos aun cuando estos están funcionando.

SATA Son las iniciales de Serial-ATA, mezcla de las tecnologías de señal con los discos ATA. Mediante esta tecnología se evitan los autobloqueos en los Discos Duros ya que la conexión entre los discos y el controlador son una conexión punto a punto en lugar de una conexión bus.

SDRAM (Synchronous Dynamic RAM – Dinámica Sincrona RAM) son memorias capaces de trabajar de forma sincronizada con los ciclos de la placa base, sin tiempos de espera.

Silo Un silo en TI hace referencia a los grandes cuartos donde se encuentran los diversos dispositivos de la infraestructura tecnológica.

SMTP (Simple Mail Transfer Protocol – Protocolo para la transferencia simple electrónico) es un protocolo de transferencia simple utilizado en servicios de mensajería electrónica de correo.

SNMP (Simple Network Management Protocol – Protocolo Simple de Administración de Red) es un protocolo de nivel de aplicación que utiliza como protocolo de transporte UDP. Define una relación cliente/servidor entre el gestor

de red (que actúa de cliente) y los elementos gestionados (que son los servidores y reciben el nombre de “agentes SNMP”).

SO (Sistema Operativo) Un sistema operativo es un conjunto de programas informáticos que oermiten a los usuarios de computadoras utilizar el hardware y programas de aplicaciones.

SSD (Solid State Drive – Unidad de Estado Sólido) es un dispositivo de almacenamiento de datos que usa una memoria no volátil como flash, o memoria volátil como la SDRAM, para almacenar datos, en lugar de los platos de los discos duros convencionales.

SSH (Secure Shell – intérprete de órdenes segura) es el nombre de un protocolo que sirve para acceder a máquinas remotas a través de una red, de forma similar a como lo hace telnet.

Storage Almacenamiento. Se utiliza principalmente para definir todos los componentes tecnológicos que sirven para el almacenamiento de grandes cantidades de información.

TB Un Terabyte es una unidad de medida de almacenamiento de información equivalente a 10^{12} (mil millones) bytes.

TCP (transmission control protocol – Protocolo de control de transmisión) es el protocolo que garantiza la entrega de toda la información en el mismo orden en que ha sido emitida por el origen.TCP

Telnet es un protocolo de emulación de terminal. Establece una sesión entre una estación de trabajo (cliente Telnet) y una máquina (servidor Telnet). Se transmite cualquier comando escribiendo en el cliente y se ejecuta en el servidor Telnet.

TEMS (Tivoli Enterprise Monitoring Server – Servidor de Tivoli Enterprise Monitoring) Es el componente principal de ITM pues se encaraga de la recopilación y control de todos los datos y alertas de rendimiento y disponibilidad recibidos de los agentes de supervisión.

TEP (Tivoli Enterprise Portal – Portal de Tivoli Enterprise) Aplicación de escritorio que sirve para conectarse al servidor de Tivoli Enterprise Portal (TEPS) y desde el cual se administra el mismo.

TEPS (Tivoli Enterprise Portal Server – Servidor de Tivoli Enterprise Portal) es el componente de ITM encargado de gestionar el acceso a los datos del TEMS mediante las consolas (web o desktop) de trabajo del usuario.

TI (Tecnologías de la Información) es un amplio concepto que abarca todo lo relacionado a la conversión, almacenamiento, protección, procesamiento y transmisión de la información. El concepto se emplea para englobar cualquier tecnología que permite administrar y comunicar información.

UDP (user datagram protocol – Protocolo de Datagrama de Usuario) es un protocolo del nivel de transporte basado en el intercambio de datagramas.

VMware es un software de virtualización de sistemas operativos. Permite a los usuarios crear varias máquinas virtuales (con diferentes sistemas operativos) dentro de una sola máquina física.

VCenter es la consola central de VMware desde la cual se administran las máquinas virtuales creadas. Desde esta se pueden crear o eliminar máquinas virtuales, programar respaldos, etc**.**

WAN (Wide Area Network – Red de Área Mundial) es la red global (varios países, un continente o incluso mundial). Estas redes suelen estar diseñadas para la interconexión de redes.

Referencias

Referencias

Andréu J. (2011). *Redes Locales.* Libro Electrónico: Editex.

Buscon.rae.es. (s.f.). Software. Recuperado el 4 de marzo 2015, Sitio web: http://buscon.rae.es/drae/srv/search?val=software

Carranza O. & Sabría F. (2004). *Logística: mejores prácticas en latinoamérica*. México.: Thomson.

Colobran, M., Arqués, J. & Galindo, E.. (2008). *Administración de sistemas operativos en red*. Barcelona, España.: Editorial UOC.

Davenport, T. y Prusak, L. (1998) *Working knowledge: How organizations manage what they know*. Massachusetts, USA. Harvard Business School Press.

Fraterneo.blogspot.mx. (2010). fraterneo GNU/Linux: 5 Aplicaciones Libres para Monitoreo de Redes y Servidores. Recuperado el 22 de Mayo de 2015. Sitio web: http://fraterneo.blogspot.mx/2010/12/5-aplicaciones-libres-para-monitoreo-de.html

García., A. (2011). *Razones para la seguridad Informática.* Madrid, España.: Parainfo.

Gnu.org. (s.f.). ¿Qué es el software libre? Proyecto GNU - Free Software Foundation. Recuperado el 4 de Mayo de 2015. Sitio Web: https://www.gnu.org/philosophy/free-sw.es.html

Gómez A. & De Abajo N.. (1997). Los sistemas de información en la empresa. Oviedo, España.: Servicio de publicaciones de la Universidad de Oviedo.

Ibm.com. (s.f.). IBM - Tivoli Netcool/OMNIbus. Recuperado el 3 de Junio de 2015. Sitio web: http://www-03.ibm.com/software/products/es/ibmtivolinetcoolomnibus

Ibm.com. (s.f.). IBM Knowledge Center. Recuperado el 16 de Junio de 2015. Sitio web: http://www-01.ibm.com/support/knowledgecenter/SSDKXQ_6.3.0/com.ibm.itm.doc_6.2.2/itm_install06.htm%23itm_over?lang=es

Ibm.com. (s.f.). IBM Productos de Software. Recuperado el 3 de Junio de 2015. Sitio web: http://www-03.ibm.com/software/products/es/tivomoni

IBM® Tivoli® Netcool/OMNIbus Probe for Tivoli EIF Version 13.0 Reference Guide November 8, 2013

Marchionni, E., (2011). *Administrador de servidores.* Buenos Aires, Argentina.: Fox Andina S.A.

Mires J.. (2009). Ataques Informáticos. Recuperado el 26 febrero 2015, de evil fingers Sitio web: https://www.evilfingers.com/publications/white_AR/01_Ataques_informaticos.pdf

Paessler.com. (s.f.). *PRTG Network Monitor - monitorización de red fácil*. Recuperado el 3 de Junio de 2015. Sitio web: http://www.es.paessler.com/prtg

Referencias

Philippe G. (2010). *Virtualización de sistemas de información con VMware.* Barcelona, España: Ediciones ENI.

Quezada, C. (s.f.). *Mecanismos de Seguridad.* Recuperado el 8 de Marzo de 2015, de UNAM Facultad de Ingeniería, : http://profesores.fi-b.unam.mx/cintia/Mecanismos.pdf

Sommerville I., (2005). *Ingeniería del Software*. Madrid, España.: PEARSON EDUCACIÓN, S.A

Tomasi, W. (2003). *Sistemas de comunicaciones electrónicas*. México.: Pearson Educación.

Valdivia C. (2014). *Sistemas Informáticos y Redes Locales*. Madrid, España: Paraninfo.