UNIVERSIDAD
REY JUAN CARLOS

ESCUELA SUPERIOR DE INGENIERÍA INFORMÁTICA

INGENIERÍA TÉCNICA EN INFORMÁTICA DE GESTIÓN

Curso Académico 2009 / 2010

Proyecto de Fin de Carrera

Monitorización de una red con IBM Tivoli Network Manager

Autor: Javier Sánchez Romero

Tutor: Javier Martínez Moguerza

RESUMEN

Hoy en día, es común que los equipos de muchas empresas y organizaciones se encuentren comunicados a través de una red. Esta red les permite estar en contacto entre sus distintas sedes o con el resto del mundo en tiempo real. Es por esto que cada vez es más necesaria una correcta administración de las redes por parte de personal cualificado. Debido a ello, surgen las herramientas para la monitorización, que nos permiten realizar un estudio detallado sobre la red supervisada conociendo su funcionamiento. Además, estas herramientas, nos dan la posibilidad de solucionar cualquier tipo de problema que surja en ella identificando rápidamente: su origen, su magnitud y su influencia en el resto de la red.

El presente proyecto consiste en la implantación de un sistema de monitorización de red en el cliente, su configuración y la formación de sus empleados para que en un futuro puedan utilizarlo en su actividad diaria. Además se realizará la puesta en marcha de la aplicación tras haber comprobado que todo funciona correctamente.

Es obvio apuntar además, que la solución que se aporta se puede extrapolar a otras redes fuera de la propia red del cliente, ya que la aplicación es altamente configurable. Este proyecto también puede servir como referencia para una monitorización de una red de ordenadores como la de la Universidad o la red de una empresa cualquiera sea cual sea su tamaño.

ÍNDICE

INTRODUCCIÓN

SATEC, Sistemas Avanzados de Tecnología, S.A. es una multinacional española integradora de soluciones tecnológicas y especializada en servicios avanzados asociados a las nuevas Tecnologías de la Información. De capital español, el Grupo SATEC es hoy en día un gran grupo empresarial internacional con presencia activa en siete países, y con una plantilla que supera las 1000 personas.

Los servicios de SATEC se han convertido en una valiosa herramienta para sus clientes, optimizando el uso y gestión de sus recursos de las TIC (*tecnologías de la información y la comunicación)*. No sólo les permite aprovechar al máximo las ventajas y el enorme potencial de las TIC, sino también hacer frente a la creciente complejidad que conlleva su implantación, así como su posterior mantenimiento y actualización. Los servicios que ofrece la compañía son a grandes rasgos: operación y supervisión, soporte, explotación y evolución, hosting/housing y formación.

Además del conjunto de soluciones propias desarrolladas por la compañía como consecuencia de la relación con sus clientes, los servicios ofrecidos por SATEC cubren las actividades diarias de estos. Mantenimiento de los sistemas actualizados, seguros, productivos, consistentes y disponibles en todo momento son algunos de los servicios ofrecidos en sus proyectos.

A lo largo de estos últimos años, la compañía ha conseguido notables éxitos y reconocimientos. Proyectos basados en firma electrónica, telemedicina, medioambiente o movilidad hacen de SATEC un referente en el mercado de las TIC en nuestro país.

Uno de estos proyectos es el consistente en la implantación para una de las más importantes compañías de telecomunicaciones de España, de un sistema de monitorización de red. Dicho sistema permitirá tener en todo momento monitorizada su red y tener control en tiempo real de lo que sucede en ella. Para ello, se utiliza una aplicación propietaria de IBM que permite al cliente tener un control absoluto de lo que está pasando en su red.

El proyecto abarca desde sus fases más tempranas en las que se realiza un estudio de las necesidades del cliente, hasta su puesta en funcionamiento. Además se realiza una verificación de que todo es correcto tras la implantación, así como multitud de controles y pruebas. Por último se imparte un curso de formación a los trabajadores del cliente que posteriormente utilizarán la aplicación, que por motivos de espacio y duración queda fuera de este proyecto.

De forma esquemática, los objetivos de este proyecto son los siguientes:

1. Estudio de las alternativas en el campo de las herramientas de monitorización antes de la implantación de la herramienta elegida.
2. Implantación y configuración de la herramienta de acuerdo a las necesidades del cliente de tal manera que se cubran sus necesidades.
3. Estudio de la herramienta de monitorización Tivoli ITNM, líder en el mercado de la monitorización de redes, centrándose en: vistas del sistema, facilidad de uso, posibilidades en la notificación de alarmas, seguridad, etc.

Por último, comentar que para mantener la confidencialidad del cliente, en ningún momento a lo largo de este proyecto se hace mención a él, a su nombre comercial o a cualquier dato que pudiera identificarlo, refiriéndose a él tan sólo como “el cliente”.

2. OBJETIVOS

2.1 ¿Qué es IBM Tivoli ITNM?

Dentro de las soluciones que los fabricantes nos ofrecen para la monitorización de redes, la creada por IBM destaca entre todas ellas. A día de hoy, el paquete ITNM (siglas de Tivoli Network Manager IP Edition) en su versión 3.8 proporciona todas las funcionalidades necesarias para la administración y monitorización de redes complejas. Estas funcionalidades incluyen descubrimientos de las redes y de los equipos que pertenecen a ellas, políticas de monitorización sobre estas, visualización de su topología, almacenamiento de informes y análisis realizados sobre la red.

ITNM, descubre las redes IP y realiza gráficas de la topología de estas mostrando información de capa 2 y 3. Se captura no sólo la información del inventario, sino también la información física: conectividad puerto a puerto, y conectividad entre dispositivos. Tivoli Network Manager captura además la información lógica de conectividad, incluyendo redes virtuales privadas (VPNs), redes locales virtuales (VLANs), ATMs, Frame Relay y MPLS.

2.2 Características básicas.

La aplicación monitorea los recursos de la red para conocer su estatus en tiempo real y continuamente actualiza su base de datos con nueva información, como pueden ser cambios realizados en la red. ITNM también sirve de soporte para identificar la causa raíz de los problemas en las redes y reducir significativamente el tiempo utilizado para resolverlos.

Cuando ocurre un problema, ITNM guía al operador que lo esté utilizando a través del mapa de topología de la red, al dispositivo que presenta el problema. El operador de la red puede inmediatamente ver la conectividad entre este y otros dispositivos y con los sistemas implicados.

Además, los mapas de la red son generados automáticamente y administrados por ITNM. A medida que se producen cambios en la red, ITNM actualiza la base de datos de la topología de la red y los mapas sin intervención manual, ahorrando tiempo y esfuerzo y reduciendo las tareas administrativas.

Para realizar todas estas tareas, ITNM utiliza el Object Server de Tivoli Netcool/OMNIbus[1], el cual se encarga de recibir, almacenar, correlacionar y administrar los eventos que ocurren en toda la red.

2.3 Descripción del problema

Como se ha comentado en la introducción de este proyecto, la implantación de ITMN se lleva a cabo sobre una red de tamaño medio-grande. Dicha red está compuesta por multitud de equipos de distintas características (pcs, routers, switches, etc), por lo que la monitorización se lleva a cabo sobre todos ellos.

Debido al gran tráfico que soporta constantemente esta red, se ha elegido ITMN como solución centralizada de monitorización y control de la red.

Hasta la implantación de ITNM en el cliente, este contaba con la aplicación HP OVO Openview. La herramienta de HP era probablemente la más utilizada en el campo de la monitorización hasta hace un tiempo, ya que la herramienta que nos ocupa (ITNM) y las herramientas de código abierto están ganando terreno en el mercado.

(1) Netcool Object Server: Es una base de datos residente en memoria, optimizada para la recolección de eventos y la proyección de filtros y vistas. Es el lugar en el que todos los mensajes del sistema procedentes de los elementos de red son almacenados y procesados en tiempo real. Tiene la tarea de consolidar, asociar y normalizar los datos procedentes de las sondas. Los eventos repetidos son asociados automáticamente, usando para ello un identificador único.

La principal motivación para el paso de OVO Openview a Tivoli ITNM se debe principalmente a dos puntos.

1. La solución de HP viene emparejada con un escollo para sus clientes: la dependencia de la arquitectura de HP. Sus servidores están basados en procesadores HP PA-RISC, un diseño propiedad de la compañía, que generalmente se vende conjuntamente con su sistema operativo HP-UX.
   IBM, por el contrario, se ha centrado cada vez más en los estándares industriales creados fuera de la empresa y aprobados por el amplio mercado de empresas de tecnología. Esta tendencia se refleja en el IBM System X de servidores, impulsados por procesadores x86 compatibles con AMD e Intel, en lugar de los procesadores propios de IBM.

2. La otra razón es la compatibilidad del software. Muchos de los clientes de HP, se enfrentan a una transición de software importante a fin de pasar a las modernas arquitecturas de 64 bits, mientras que los clientes de IBM no lo hacen.
   El Itanium (sucesor natural de los procesadores HP PA-RISC) a pesar de contar con una arquitectura de 64 bits, se basa en los chips RISC de HP, por lo que para obtener el mejor rendimiento, el software debe ser compilado específicamente para él.

2.4 Estudio de alternativas.

Actualmente existen en el mercado distintas aplicaciones para la monitorización de redes. Entre todas estas aplicaciones se encuentran algunas con licencia de software libre y otra con licencia propietaria. Desde siempre, la citada anteriormente HP OVO Openview es el principal competidor de ITNM, pero últimamente las herramientas de software libre están ganando importancia en el mundo de la monitorización. Algunos ejemplos de estas aplicaciones con sus principales características son:

- HP OVO Openview

  Es el principal rival de ITNM en el mercado. Las características de ambos son muy similares, tan sólo se diferencian en las citadas en los dos puntos anteriores y las que se exponen más abajo.

  Posee una arquitectura consola-agente, cuyos agentes son independientes de la consola central e informan a esta sólo en casos de excepciones (generalmente cuando se detecta alguna situación que requiera informarse). OVO Openview permite monitorizar ficheros de log, programar tareas, ejecutar programas de control, capturar eventos SNMP (traps), recolectar métricas de rendimiento de sistema y posee interfaces abiertas para envió de mensajes.

  Además permite el manejo de usuarios por responsabilidades, vistas y eventos que pueden asociarse a acciones, instrucciones, anotaciones y mantener un histórico para consultas y estadísticas.

  Como todas estas aplicaciones es escalable e integrable. Permite el manejo de una gran cantidad de dispositivos y posee integración con los otros módulos de OpenView.

- Naggios *(software libre)*

  Se trata de un software que proporciona una gran versatilidad para consultar prácticamente cualquier parámetro de interés de un sistema. Además genera alertas, que pueden ser recibidas por los responsables de la aplicación mediante correo electrónico o mensajes sms (entre otros medios), cuando algún parámetro excede de los márgenes definidos por el administrador de red.

  Entre sus características principales figuran la monitorización de servicios de red (SMTP, POP3, HTTP, SNMP...), la monitorización de los recursos de sistemas hardware (carga del procesador, uso de los discos, memoria, estado de los puertos...), independencia de sistemas operativos, posibilidad de monitorización remota mediante túneles SSL cifrados ó SSH, y la posibilidad de programar plugins específicos para nuevos sistemas. Actualmente cuenta con un interfaz gráfico poco desarrollado, lo que hace que la recepción de las alertas y la monitorización de los equipos, en el caso de que sean muy numerosos, no sea excesivamente cómoda.

- OpenNMS *(software libre)*

  Herramienta galardonada con varios premios por parte de la comunidad TIC debido a que se presenta como una seria alternativa a las soluciones de pago como las proporcionadas por HP o IBM.

  OpenNMS es elogiado por ser fácil de personalizar, fácil de integrar y - por supuesto – libre (estos atributos son característicos de cualquier producto de código abierto). Debido a su naturaleza de código abierto, OpenNMS tiene una comunidad de desarrolladores que contribuyen a su código, siendo este abierto para que cualquiera pueda verlo o adaptarlo a sus necesidades.

  La aplicación tiene como principal característica, que utiliza el protocolo SNMP para conocer el estado del dispositivo preguntándole a otros agentes. También soporta otro tipo de protocoles como HTTP y JMX. Está programado en Java por lo que puede funcionar en cualquier plataforma que soporte su máquina virtual 1.5 como Linux, Solaris, Mac OS X o Windows. Al igual que Nagios se puede extender su funcionalidad básica mediante complementos.

Se ha elegido IBM Tivoli Network Manager debido a que, además de tener todas las funcionalidades ofertadas por las herramientas citadas anteriormente, ofrece algunas características adicionales. Estas características son por ejemplo: soporte para VoIP completa (Voz sobre IP), soporte de gestión de la calidad de voz, IPTV (Internet Protocol Television) y la configuración completa y mantenimiento de todos los componentes de la red a través de la infraestructura de prestación de servicios. Pero posiblemente la mayor característica que diferencia la aplicación de sus rivales es la "vista única" que permite un enfoque integrado y una perspectiva a vista de pájaro sobre todas las capas de red.

2.5 Metodología empleada.

Una vez se decide en el departamento de sistemas junto con el cliente de la necesidad de disponer de una aplicación que permita monitorizar la red, se inicia la búsqueda del software adecuado para realizar esa función. Tras el estudio de diversas

aplicaciones y sus correspondientes características, se opta por la solución ofrecida por IBM por ser la que más se ajusta a las necesidades del cliente.

La aplicación tiene que ser desplegada con todas las garantías de un funcionamiento puesto que ITMN va a controlar todos los equipos de la empresa.

Una vez instalado se procede a estudiar la documentación y el manual de usuario para realizar la configuración y realizar las pruebas más básicas. También se procede a realizar una documentación a medida para el cliente, que se le expone de forma impresa y mediante un curso presencial a los trabajadores que llevan a cabo el uso de la aplicación. Después de la realización de pruebas más exhaustivas y tras comprobar que tanto el entorno como las alertas configuradas (caída de un servidor, llenado del espacio en disco o una base de datos inaccesible) funcionan correctamente y que cumple las expectativas que esperábamos se procede a su puesta en marcha final configurando los chequeos de los servidores y servicios del cliente.

3. DESCRIPCIÓN INFORMÁTICA

En este apartado se explica cómo instalar la aplicación de monitorización de red y servicios Tivoli ITNM. Se realiza una configuración inicial para poner en funcionamiento la aplicación y posteriormente se ven los apartados más importantes de su interfaz web, de los archivos de configuración y de las alertas, con distintos ejemplos de chequeos, y los distintos pasos a realizar para una correcta monitorización y administración de nuestra red.

3.1 Preparando la instalación

Antes de instalar el Network Manager, hay que tener claro cuántos servidores se necesitarán y qué componentes se instalarán en cada uno de ellos.
Además, para que la monitorización se lleve a cabo de forma óptima, debe particionarse la red en varios dominios, ya que estos pueden ser monitorizados por separado, por las siguientes razones:

- Escalabilidad: La red puede que sea demasiado grande para descubrirla de una sola vez
- Razones geográficas: La red puede descomponerse en regiones y para cada una de ellas, crear un dominio
- Limitar lógicamente la red: Puede descubrirse y administrar la red estableciendo límites en ella.
- Pueden realizarse múltiples descubrimientos y ejecutar varios procesos de forma independiente si estos pertenecen a dominios distintos.
- Identificar el dominio para cada evento, permite generar una topología correcta tanto en la Vista de Red como en la Vista de Saltos.

Muchos de los productos que trabajan con Network Manager, llevan incorporado un modo failover[2], pero hay que decidir cuál de ellos queremos que lo implemente:

- ObjectServer Failover
  Dos ObjectsServers son unidos de forma bidireccional formando un par virtual, de forma que los eventos que se produzcan en uno de ellos se puedan copiar en el otro, por si el primer ObjectServer falla, tener como respaldo al segundo.
  Un proceso que necesite conectarse al ObjectServer activo, usará la información almacenada en los archivos de interfaz de Tivoli Netcool/OMNIbus.
  Tivoli Netcool/OMNIbus web GUI Failover, es conocido como Netcool/Webtop en versiones anteriores. Este es el elegido en nuestro caso.

- Arquitectura de Network Manager Failover
  Network Manager Web GUIs no implementa el modo failover, pero puede ser implementado.

3.2 Requisitos hardware y software

Una aplicación como ITNM depende claramente del tamaño de la red que va a monitorizar, para exigir unos requisitos determinados u otros. En este caso que nos ocupa, los requisitos que debemos cumplir son los siguientes.

NOTA: Como la instalación se ha llevado a cabo sobre equipos UNIX, son sus requisitos los que se detallan a continuación.

(2) Failover: Modo de operación de backup en el cual las funciones de un componente del sistema son asumidas por un segundo componente de este cuando el primero no se encuentra disponible debido a un fallo ó un tiempo de parada preestablecido. Es usado para hacer a los sistemas más tolerantes a fallos, y de esta forma hacer el sistema permanentemente disponible.

- **Requisitos hardware**

1. **Requisitos para ejecutar el instalador**
   - 150 MB en el directorio /tmp
   - 200 MB en los directorios /urs y /var
   - Si se instala en otro directorio como /opt, habrá que dejar al menos 50 MB libres en ese directorio.

2. **Requisitos para los componentes principales**

   Procesador
   - Procesadores Dual 3 Mhz o superiores

   Memoria
   - Para una instalación de un único servidor con las aplicaciones web, la BBDD de la topología y Tivoli NetCool/OMNIbus, un mínimo de 4 GB DRAM (8GB DRAM para grandes redes).
   - Para una instalación distribuida donde las aplicaciones residen en el servidor, 2 GB DRAM (4 GB DRAM para grandes redes)

   Espacio en disco

   2 GB de espacio en disco para almacenar el software 2 GB de espacio en disco para cache

   Ancho de banda

   Se requiere de una conexión 100Mbps full dúplex fast Ethernet con servidor de DNS

   Otros requisitos

   Lector de DVD si se instala en software de esta forma y no se instala tras su descarga

3. Requisitos para la consola de usuario de Tivoli Integrated Portal (TIP)

2GB de espacio en el disco duro

2GB DRAM como mínimo y 4 GB DRAM para redes grandes

Lector de DVD (si no se instala desde la descarga)

Procesador

Procesador Dual 3 GHz o superior

4. Requisitos para el servidor de la base de datos de la topología

Procesador

Procesador dual 3 GHz o superior

Memoria

Como mínimo 2 GB de memoria DRAM (4 GB para redes grandes)

Espacio en disco

3 discos en RAID1 (6 discos para redes grandes) SATA o SCSI de alta velocidad

5. Espacio en disco para eventos e interfaces (debe calcularse espacio adicional para ellos)

4 KB de espacio en disco para cada evento que se espere por día.

4 KB de espacio en disco para cada interfaz o puerto del dispositivo administrado

6. Ancho de banda requerido para los descubrimientos

La velocidad dependerá del tamaño de la red, pero hay que tener en cuenta que si no se cuenta con la velocidad necesaria los paquetes SNMP pueden perderse, por lo que la velocidad recomendada es:

- 10 Mbps full duplex para soportar 100 SNMP helper threads.
- 100Mbps full duplex fast ethernet para descubrir una red grande

7. **Requisitos de memoria para los descubrimientos**

   El proceso *ncp_disco* es el proceso que más procesador consume. Todo el Network Management debe tener acceso a 4 GB de memoria para realizar los descubrimientos de manera óptima.

- **Requisitos software**

1. **Requisitos sobre otros productos**

   Tivoli Netcool/OMNIbus

   Debe estar instalada la versión 7, 7.1, 7.2 o 7.3 en el servidor para que el Network Manager pueda conectarse a él. Si por un casual no se cuenta con una instalación de Tivoli Netcool/OMNIbus previa, debe instalarse.

   The Tivoli Netcool/OMNIbus Web GUI

   Si se instala Web GUI sin usar el instalador de Network Manager, debe instalarse desde una ventana distinta a la usada para instalar Network Manager, asegurándose de que todas las variables se establecen de acuerdo a la documentación de IBM Tivoli Business Service Manager.

   Versiones anteriores

   Instalar Network Manager en un directorio diferente al de Network Manager V3.7, Tivoli Netcool/OMNIbus V7.1 y Netcool/Webtop V2.1.

2. **Bases de datos de la topología soportadas**
   - Oracle 10g
   - Oracle 11g
   - DB2® 8.2
   - DB2 9.1
   - MySQL 5.0
   - IDS 11.5

3. **Sistemas operativos soportados**
   - Solaris 9 y 10 para SPARC
   - Red Hat Enterprise Linux 4.0 y 5.0 (x86-32, x86-64, zSeries y System z)
   - SUSE Enterprise Linux 9, 10, y 11 (x86-32, x86-64, zSeries y System z)

   En nuestro caso el elegido es Red Hat Enterprise 5.0

   Requisitos de shell para los sistemas operativos UNIX

   Hay que asegurarse que antes de ejecutar el instalador de Network Manager, está instalada la Shell Korn

4. **Navegadores soportados**

   Mozilla Firefox 3.x, para Red Hat Enterprise Linux (RHEL) 4.0, 5.0, SUSE Interprise Linux (SLES) 9, 10, Solaris 9, 10

5. **Requisitos de DNS**

   Hay que asegurarse de que el servidor en el que se instalan los componentes de Network Manager tiene correctamente definido un nombre.

   En plataformas UNIX, el nombre es definido en el archivo /etc/hosts

6. **Restricciones de usuarios UNIX**

   Si se ha instalado algún otro producto de Tivoli en un servidor, Network Manager debe instalarse en el mismo directorio como el mismo usuario.

   Si se instalan las aplicaciones Network Manager Web como root, Network Manager no se integrará con IBM Tivoli Business Service Manager.

   Si se instala Network Manager como un usuario no administrador deben configurarse posteriormente todos los componentes como root

- **Requisitos del directorio de instalación**

  Requisitos comunes para todas las plataformas
  - Todos los productos de Tivoli Network deben instalarse en el mismo directorio, el cual no debe contener espacios

- La ruta completa del directorio de instalación debe contener sólo caracteres alfanuméricos (A-Z, a-z, 0-9), puntos, guiones bajos, comas, slashes o espacios

Requisitos para plataformas UNIX

El directorio, si es diferente de /opt, debe ser propiedad del usuario que realiza la instalación

3.3 Instalación de la aplicación

En el caso de que exista una versión anterior de la aplicación instalada, habría que actualizarla y migrar los datos de esta. Como en el caso que nos ocupa, se realiza una instalación desde cero, se obviarán estos pasos.

La instalación se lleva a cabo en modo gráfico, utilizando el asistente habilitado para tal fin. Para lanzar el asistente, ejecutamos el script `launchpad.sh` y seleccionamos "Instalador para Network Manager". Lo siguiente es seleccionar la opción "Instalación personalizada", ya que al ser una red de un tamaño medio, los parámetros de la instalación básica no son los correctos, y seguir los siguientes pasos introduciendo los valores correctos para ellos:

1. Indicar dónde se realiza la instalación (ubicación de los directorios)
2. Indicar los componentes a instalar.
3. Seleccionar el directorio que contiene el paquete NetCool/OMNIbus.
4. Establecer los nombres de dominio.
5. Introducir la contraseña de administrador.
6. Establecer los puertos para NetCool/OMNIbus, TIP y la base de datos MySQL
7. Establecer los datos para NetCool/OMNIbus (contraseñas, nombres de dominio, etc)
8. Seleccionar la carpeta donde instalar TIP e introducir todos sus datos (nombres de dominio, contraseñas, etc).

9. Establecer la información referente a LDAP[3] (puerto, nombre del servidor, contraseñas, etc).
10. Establecer los parámetros para un descubrimiento inicial de la red una vez se haya instalado la aplicación. *Posteriormente se verá en detalle qué es un descubrimiento.*
11. Confirmar el sumario de todos los datos introducidos en la instalación.

3.4 Tareas Post-Instalación

Una vez hemos terminado con la instalación de la aplicación, debemos realizar una serie de tareas para configurarla de forma óptima. Estas tareas son las siguientes:

- Instalación root / no root

  ITNM puede instalarse con usuario distinto de root, pero para iniciar la aplicación se necesita que lo haga el usuario que realizó la instalación. Como se ha instalado como root, se da permiso a otro usuario para que pueda correr la aplicación dirigiéndonos al directorio `NCHOME/precision/scripts` y ejecutando el script `setup_run_as_setuid_root.sh`

- Permitir o no el acceso mediante http

  Como en el caso que nos ocupa sólo permitiremos el acceso a la aplicación mediante HTTPS para garantizar que la conexión es segura, no se va a cambiar el directorio donde se realizó la instalación y NetCool/OMNIbus ya se encuentra instalado y configurado, no es necesario realizar ninguna otra tarea de post-instalación.

---

(3) LDAP: (*Lightweight Directory Access Protocol*, Protocolo Ligero de Acceso a Directorios) es un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red. LDAP también es considerado una base de datos (aunque su sistema de almacenamiento puede ser diferente) a la que pueden realizarse consultas.

3.5 Componentes importantes

El servidor ITNM puede ser dividido en varios componentes clave, gestionando todos ellos funciones particulares del producto: Base de datos de alarmas (Omnibus), Interfaz gráfico (TIP), Base de datos de topología (NCIM) y Descubrimiento y monitorización (núcleo de ITNM).

Cada componente posee su propio archivo de configuración, el cual define cómo será el comportamiento del componente resultante en la memoria principal.

Los principales archivos que tenemos en ITNM podemos encontrarlos bajo los directorios NCHOME y TIPHOME y son los siguientes:

- **ncp_auth** - proporciona autentificación a los componentes del servidor ITNM. Además supervisa todas las transacciones de usuario, asegurando que los usuarios tienen permiso para acceder a la red o configurar servidor.
- **ncp_ctrl** - proceso maestro encargado de arrancar y gestionar los componentes del servidor ITNM. Lanza éstos componentes en orden apropiado, tal y como se índica en las dependencias configuradas para los procesos.
- **ncp_class** - proporciona una definición de estructura jerárquica para los dispositivos dentro de la red.
- **ncp_model** - Lleva a cabo la instalación basada en definiciones de clases, y maneja la topología “activa”.
- **ncp_store** - Proporciona recuperación de errores para eventos y topología.
- **ncp_disco** - Define y lleva a cabo el auto- descubrimiento de red, construye la topología para el servicio MODEL.
- **ncp_d_helpserv** - Gestiona las consultas que se mandan a los dispositivos de la red que realizan los agentes del descubrimiento.

Así mismo los principales directorios de la aplicación son:

- **$ITNM_HOME/bin –** Para ejecutables
- **$NCHOME/etc/ITNM –** Para ficheros de configuración
- **$ITNM_HOME/disco/agents** y **$ITNM_HOME/disco/stitchers** Para agentes de descubrimiento
- **$NCHOME/log/ITNM** – Para logs

3.6 Primeros pasos

Una vez tenemos instalada correctamente la aplicación debemos ponerla en funcionamiento, para ello se utiliza el comando **itnm_start**, que hará que arranquen todos los procesos de la aplicación.

Para comprobar posteriormente el estado de estos procesos podrá usarse el comando: **itnm_status** (**itnm_stop** para pararlos). En el caso de que quisiéramos iniciar o detener algún proceso determinado lo haríamos con:

itnm_start -domain <nombre_proceso>

Una vez tenemos inicializada la aplicación, abrimos un navegador web y tecleamos la dirección:

`https://localhost:puerto/ibm/console`

donde localhost es la dirección IP del servidor de ITNM y puerto es el puerto a través del que nos conectaremos. Al hacer esto nos parece la pantalla inicial de la aplicación.

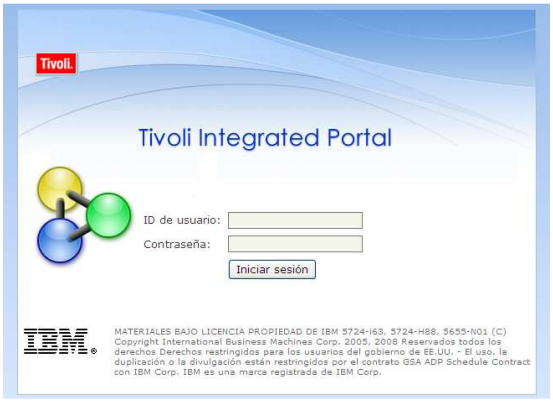


Figura 1. Pantalla inicial de IBM Tivoli Integrated Portal.

Tras introducir el usuario y la contraseña correctos, entramos en el portal donde nos aparece la primera pantalla de la aplicación en la que se puede ver el menú en forma de árbol con todas las opciones que se explican a continuación.

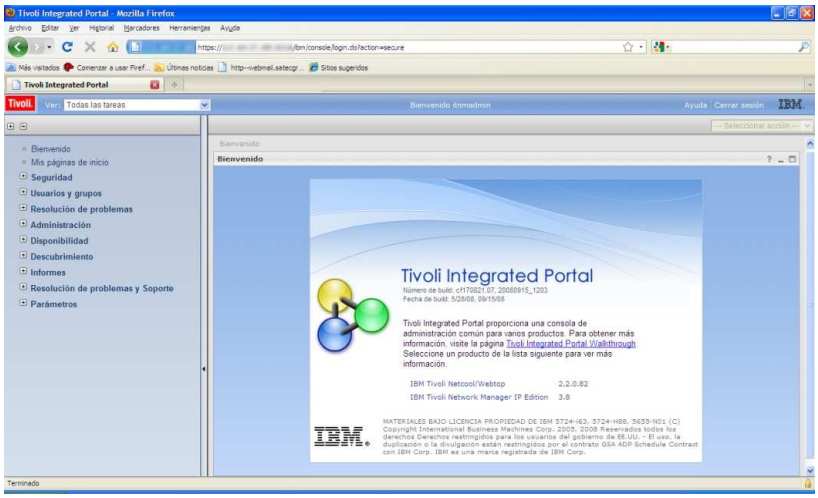


Figura 2. Pantalla inicial de IBM Tivoli Integrated Portal una vez nos hemos identificado correctamente.

Como no es objetivo de este proyecto explicar en detalle cada una de las opciones de la aplicación, comentaremos cada una de ellas de forma breve para hacernos una idea de para qué sirve y nos centraremos en las opciones importantes que sirven para realizar la monitorización de la red *(en este proyecto se muestran tan sólo las opciones que aparecen en el portal al entrar como usuario Administrador)*.

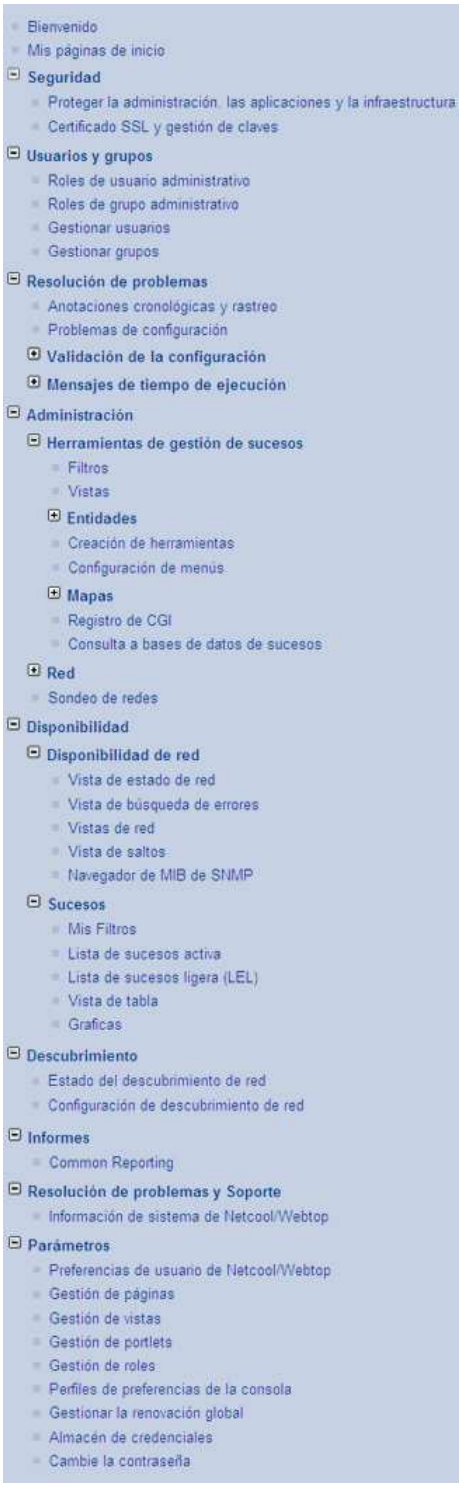


Figura3. Menú principal de ITNM

Las opciones que encontramos en ITNM son:

Seguridad

Nos permite configurar las opciones de SSL para establecer comunicaciones seguras entre los procesos, así como las opciones de autenticación de los usuarios y el manejo de certificados digitales.

Usuarios y grupo

Permite gestionar los usuarios y los grupos definidos en la aplicación. Además permite buscar usuarios o grupos y definir los roles para cada uno de ellos en el sistema.

Resolución de problemas

Muestra toda la información referente al sistema (versiones, compatibilidades, etc), para que podamos detectar posibles incidencias en él.

Administración

Configuración de las políticas de sondeo de la red, creación de filtros para realizar descubrimientos, configuración de los accesos a las bases de datos, etc.

Disponibilidad

Permite comprobar el estado de la red a través de las vistas que ofrece la aplicación, que se detallarán más adelante.

Descubrimientos

Posiblemente la opción más importante de la aplicación ya que es la que nos permite realizar los descubrimientos de la red y configurarlos a medida. También se verá en detalla un poco más adelante.

Informes

Permite obtener informes del estado de la red y de los posibles problemas.

Parámetros

Permite configurar todos los parámetros de la aplicación tales como las vistas, las gráficas generadas, los informes. Además permite realizar cambios en los parámetros de la aplicación como contraseñas, etc.

3.7 Descubrimientos

Como hemos visto, el punto fuerte de ITNM son los descubrimientos de la red. Podemos definir un descubrimiento como el procedimiento que nos permite descubrir que dispositivos existen en nuestra red, aprender cómo están conectados y construir un mapa de su topología.

Los dispositivos que son identificados por los descubrimientos de ITNM son de varios tipos: dispositivos de capa 2 (si son Ethernet), de capa 3 (si son IP), Frame Relay y ATM (si tienen interfaz de gestión de Ips).

ITNM tiene unas herramientas fundamentales para descubrir equipos, que se denominan **finders.** Los finders son los encargados de determinar la existencia de los dispositivos mediante solicitudes de eco ICMP para direcciones broadcast o multicast, o direcciones IP individuales. Una vez se conocen los dispositivos, entran en juego los **agentes**. Los agentes del descubrimiento son los encargados de rellenar las tablas de las bases de datos con la información que recopilan de los diferentes equipos.

La primera vez que un descubrimiento es ejecutado, se lleva a cabo uno completo. Una vez se ha completado es posible hacer:

- un redescubrimiento completo, el cual implica la utilización del ámbito y de las fuentes ya existentes.
- un descubrimiento parcial, el cual implica añadir (posiblemente) nuevos ámbitos, y la selección de direcciones IP o direcciones de subred para volver a comprobar la existencia de dispositivos y volver a sondear para comprobar la conectividad.

Todo esto lo tenemos disponible en el menú principal de la aplicación, dentro de la opción **Descubrimiento**, donde encontramos a su vez dos opciones: **Estado del descubrimiento** y **Configuración del descubrimiento**.

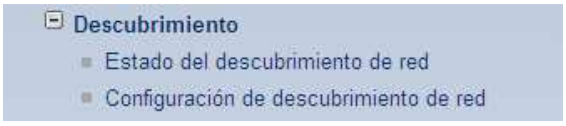


Figura 4. Opciones del menú "Descubrimiento".

3.7.1 Configuración del descubrimiento.

Esta opción nos permite configurar todos los parámetros referentes al descubrimiento de la red.

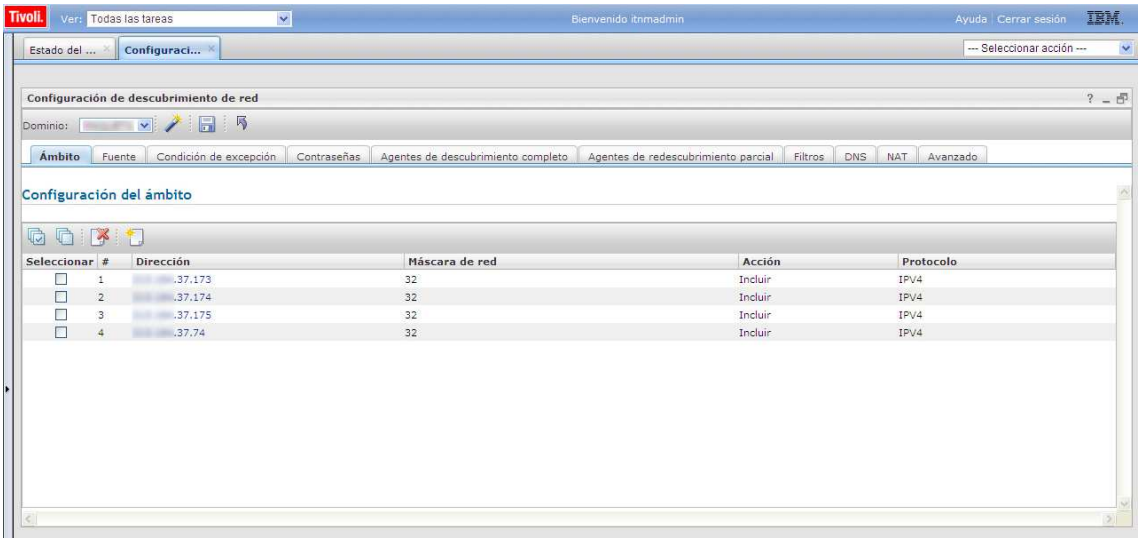


Figura 5. Pantalla para la configuración del descubrimiento donde se muestran las pestañas con todas las opciones disponibles

Como puede verse en la figura 5, a través de las distintas pestañas podemos ir configurando los parámetros que se consideren oportunos:

- El ámbito del descubrimiento (subred a examinar, máscaras de red, etc)
- Las fuentes (si quiere incluirse un equipo o una subred directamente para que se incluya en el descubrimiento).
- Las cadenas SMNP de cada red o equipo
- Activar los distintos agentes de descubrimiento para que funcionen con NAT, MPLS, etc.
- Filtros para indicar qué tipo de equipos se quieren buscar (impresoras, routers, etc).

NOTA: *En los anexos de este proyecto se pueden encontrar capturas de cada una de las opciones disponibles en la aplicación.*

3.7.2. Estado del descubrimiento.

Los descubrimientos constan siempre de 4 fases ya sean descubrimientos parciales o descubrimientos completos. Estas fases son:

i. Fase 0

   Es la fase de inicialización que termina cuando el primer dispositivo es encontrado.

ii. Fase 1

   Se identifican todos los dispositivos de la red. Para asegurarse que el descubrimiento se realiza rápidamente, la fase 1 se completa cuando la "find rate" o tasa de descubrimiento cae por debajo de un cierto nivel o no encuentra nada en un determinado periodo de tiempo.

   Cualquier dispositivo encontrado después será enviado a finders.pending para ser incluido en el próximo descubrimiento.

iii. Fase 2

Se completa la resolución de las direcciones IP a direcciones MAC. Esta fase se competa cuando cada dispositivo de la tabla de envíos tiene una entrada en la tabla de retorno.

iv. Fase 3

Al finalizar, el proceso de descubrimiento tiene total conocimiento de los dispositivos que existen dentro de la red y acceso a todos los mapeos de direcciones IP a direcciones MAC de todos los dispositivos del servidor Helper.

Se puede proceder a descargar toda la tabla de información de los switches de red mientras se realizan pings a todos los dispositivos para confirmar la precisión del contenido de las tablas.

Cuando la fase 3 se ha completado, el descubrimiento está preparado para ofrecer toda la información de conectividad, que será unida para conformar la topología de la red.

Se puede conocer la fase en laque se encuentra el descubrimiento en la opción: **Descubrimiento > Estado del descubrimiento de red**

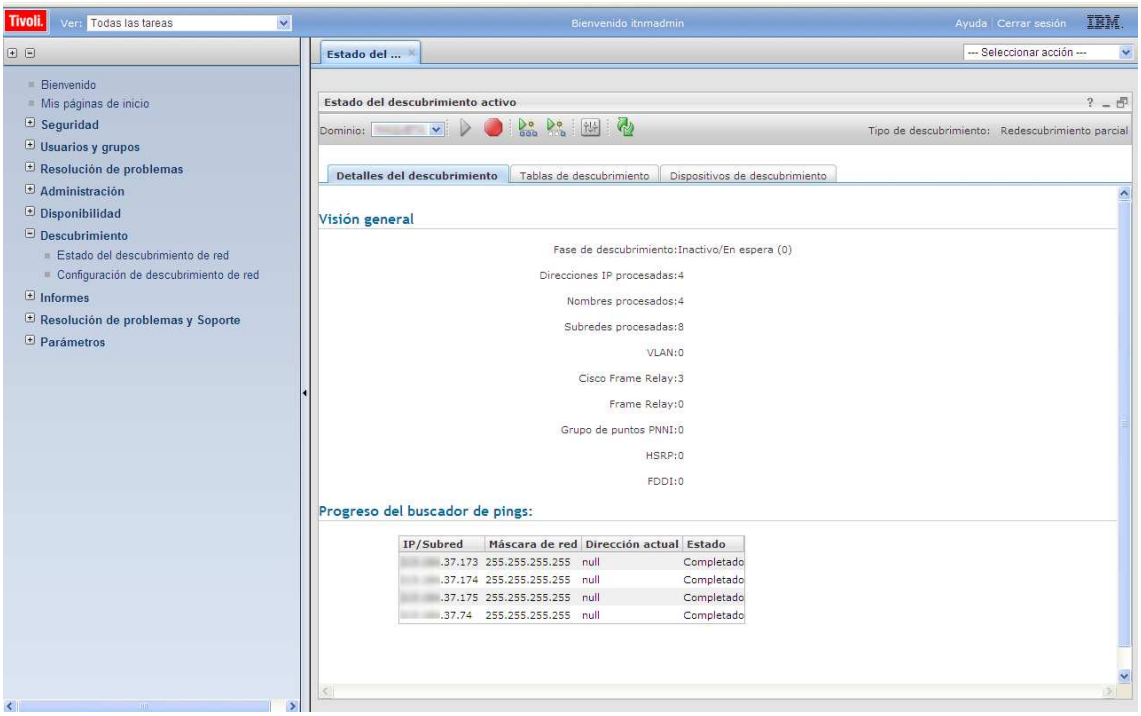


Figura 6. Pantalla donde puede verse la fase del descubrimiento en la que nos encontramos.

Además una vez que se ha llegado a la fase 3 del descubrimiento, mediante las pestañas **Tablas de descubrimiento** y **Dispositivo de descubrimiento**.

3.7.3 Filtros de descubrimiento

Hay ocasiones en las que es beneficioso reducir los pings no requeridos. Es útil cuando se desea prevenir el testeo de rutas de 'backup', lo que puede dar lugar a que se activen. Para ello, se crean filtros que restringen el Ping Finder para no realizar ping en las máquinas que le indiquemos (para ellos, se requiere las direcciones IP de los dispositivos o el rango de la subred).

Existen dos tipos de filtro dentro del proceso de descubrimiento: **Pre-descubrimiento** (activos al inicio del ciclo de descubrimiento) y **Post-descubrimiento** (activos al final del ciclo de descubrimiento).

Normalmente los filtros utilizados son Pre-descubrimiento. Los filtros Post-descubrimiento, descubren los equipos pero no clasifican la información sobre estos, por lo que puede ser útil para filtrar equipos como impresoras o equipos de trabajo, que están presentes, pero no se muestran en la topología de la red.

Tanto si quieren hacerse filtros Pre-descubrimiento, como filtros Post-descubrimiento, se configuran desde **Descubrimientos > Configuración del descubrimiento > Filtros**.

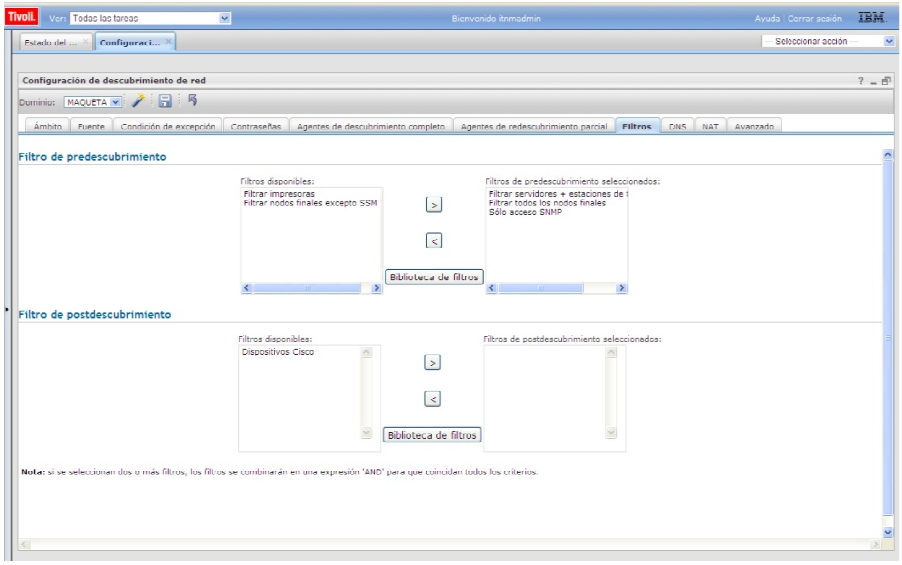


Figura 7. Configuración de filtros de descubrimiento.

3.7.4 Visualización de la topología

ITNM posee dos herramientas que permiten visualizar la topología obtenida durante el proceso de descubrimiento. Estas herramientas son las *vistas de red* y las *vistas de saltos*. Ambas podemos encontrarlas en **Disponibilidad > Disponibilidad de Red.**

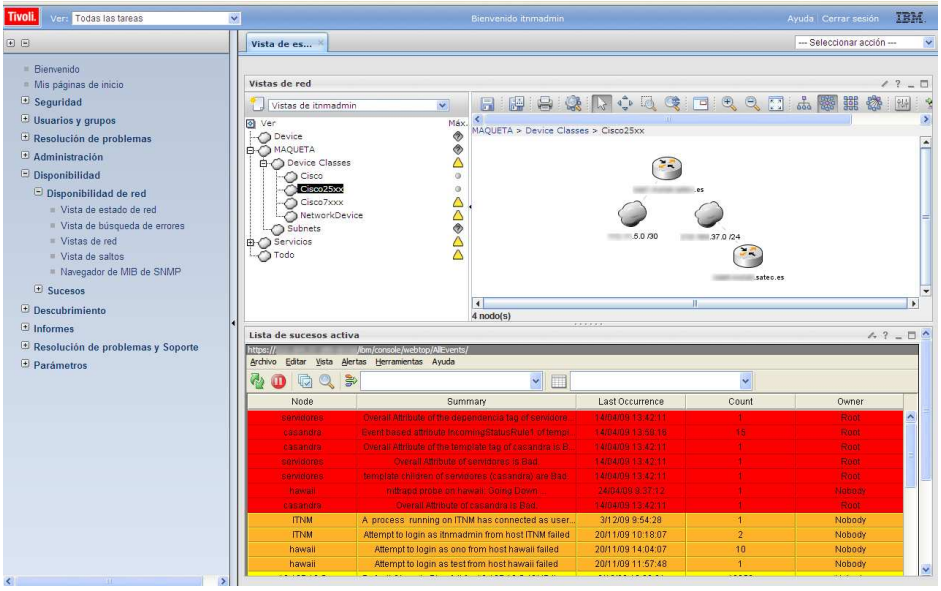


Figura 8. Pantalla de Vista de Estado de la red, donde podemos ver un resumen de las características de la red analizada

La figura 8 muestra una captura de pantalla de la opción **Vista de Estado de Red,** que ofrece un breve resumen del estado de la red, que puede conocerse en detalle mirando el resto de opciones. Las opciones realmente útiles para la visualización de la topología, son las dos comentadas anteriormente:

3.7.4.1 Vista de saltos

Accedemos a ella mediante: **Disponibilidad>Disponibilidad de Red > Vista de saltos.** Esta opción permite buscar y mostrar los dispositivos de la red, dibujando la topología entorno a uno de ellos. Además, podemos ver el número de saltos desde el dispositivo origen y la conectividad de este en la capa que le especifiquemos (capa 2, capa 3 y subredes IP).

Dentro de esta opción podemos encontrarnos algo como lo mostrado en la figura 9, donde especificando el dominio, la fuente y el número de saltos, podemos obtener la información referente al equipo y sobre todo la información referente a la conectividad del equipo con los demás elementos de la red.

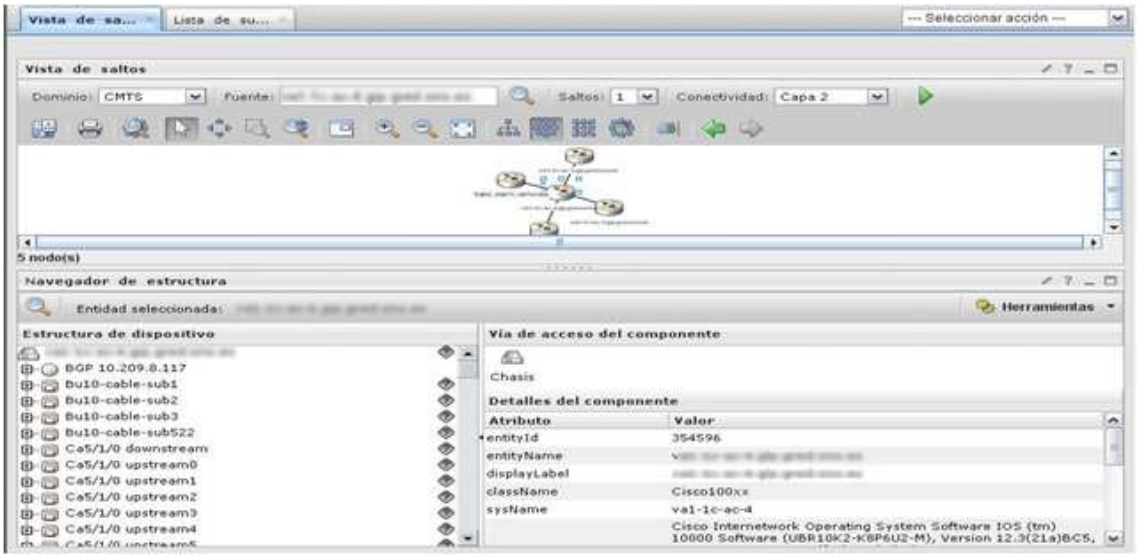


Figura 9. Pantalla principal de la vista de saltos.

Figura 10. Campos con los criterios de búsqueda de entidades y los resultados obtenidos.

Dentro de la vista de saltos, existe otra opción interesante que es la que nos permite conocer la conectividad del dispositivo

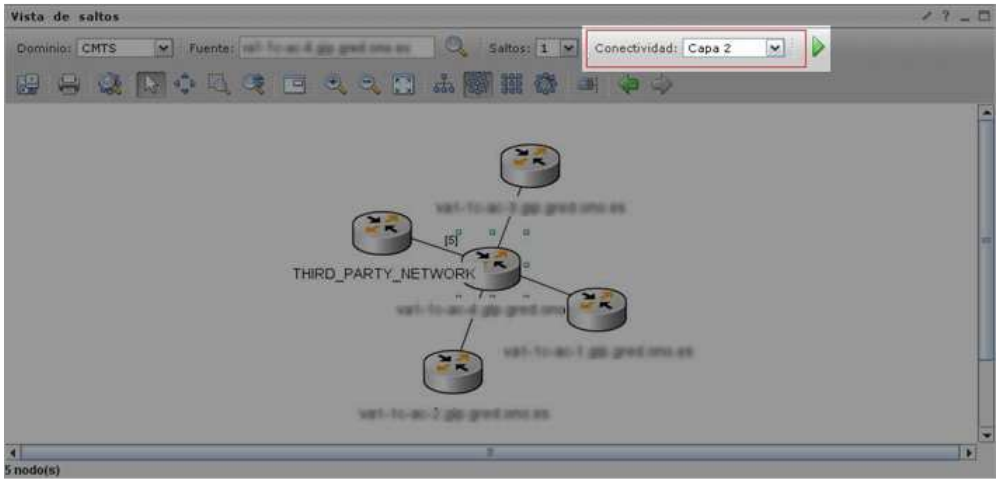


Figura 11. Opción que permite cambiar el tipo de conectividad en la vista de saltos.

En ella podemos seleccionar varios tipos:

- Capa 2, muestra todas las conexiones conmutadas entre los dispositivos de la topología, normalmente muestra conexiones switch y hub.
- Capa 3, muestra los routers y las conexiones entre ellos. Los Switches normalmente no son mostrados.
- Subredes IP, muestra todos los dispositivos dentro de una subred conectada a un grupo de subredes. Esto ayuda a simplificar la red mostrada en el mapa de red. Si deseas ver todas las conexiones, elige Capa 3 para mostrar todos los routers y conexiones entre ellos o Capa 2 para las conexiones de enlaces de datos (figura 12)

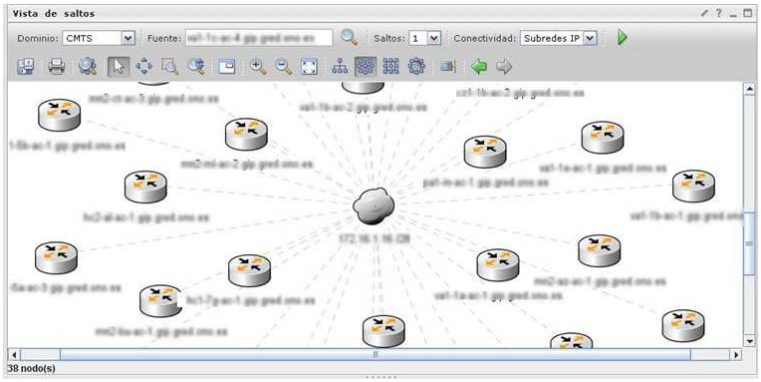


Figura 12. Vista de saltos mostrada con conectividad de subredes IP.

Una vez localizado el dispositivo deseado, ya sea porque esté afectado por algún problema o simplemente porque queremos conocer su información, podemos ejecutar una serie de acciones sobre este. Estas opciones son las que aparecen en el menú desplegable de la figura 13.

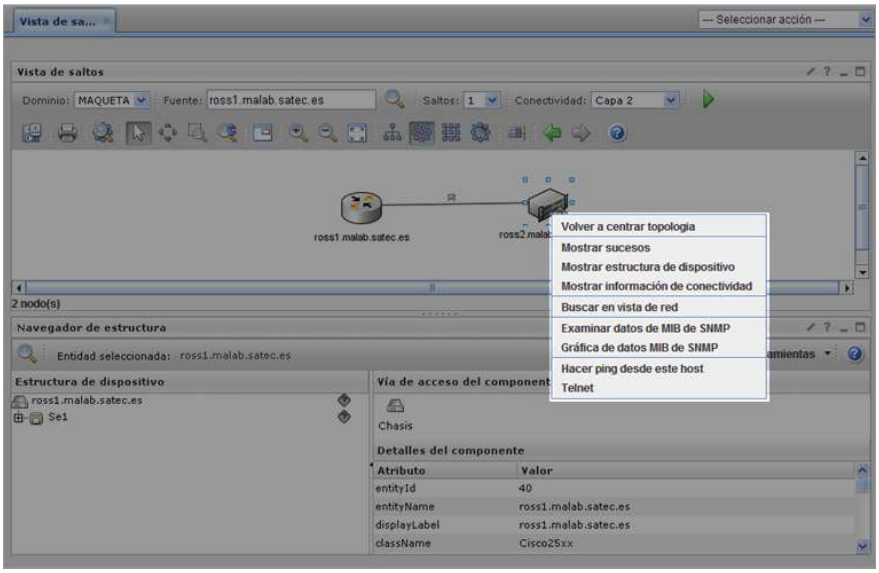


Figura 13. Menú desplegable con las opciones disponibles para cada dispositivo.

De las opciones disponibles, las realmente útiles para conocer la información detallada del equipo o su conectividad, son: Mostrar sucesos (figura 14), Mostrar estructura de dispositivo (figura 15) y Mostrar información de conectividad (figura 16).

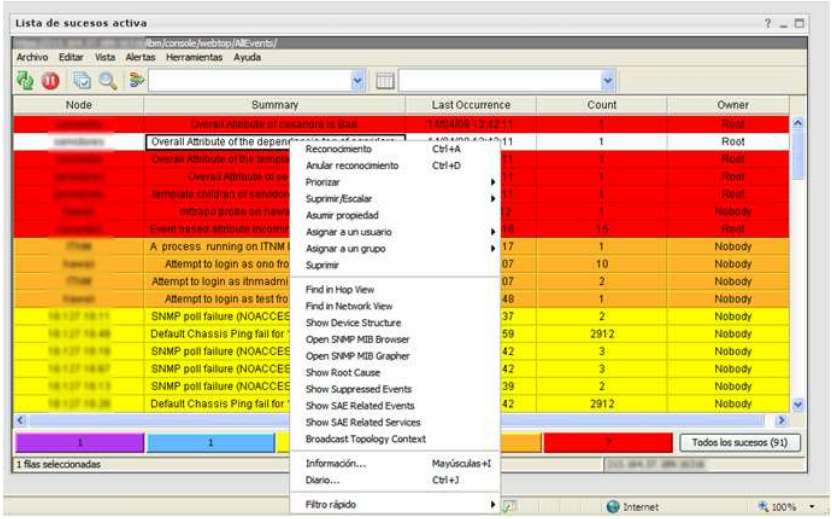


Figura 14. Lista de sucesos activos para cada dispositivo. Se ordenan por colores dependiendo de lo crítico del suceso. El menú desplegable muestra las acciones que pueden llevarse a cabo.

Figura 15. Pantalla que muestra la información de cada dispositivo.

Nodo local			Nodo vecino		
Nombre de entidad	Descripción de interfaz	Tipo de interfaz	Nombre de entidad	Descripción de interfaz	Tipo de interfaz
[redacted].satec.es	Serial0.1	frame-relay [32]	[redacted].satec.es	Serial1.1	frame-relay [32]
[redacted].satec.es	Serial0	frame-relay [32]	[redacted].satec.es	Serial1	frame-relay [32]
[redacted].satec.es	Ethernet0	ethernet-csmacd [6]	[redacted].satec.es	Ethernet0	ethernet-csmacd [6]

Figura 16. Pantalla que muestra la información de conectividad de cada dispositivo.

Otra de las opciones que se nos permite seleccionar es la de examinar es la de examinar los datos de MIB[4] de SNMP (figura 17), que posteriormente pueden ser mostradas en forma de gráfica que representa en tiempo real el comportamiento del dispositivo, ya que las variables MIB son sondeadas cada cierto tiempo.

[4]MIB: La **Base de Información Gestionada** (***M**anagement **I**nformation **B**ase*) es un tipo de base de datos que contiene información jerárquica, estructurada en forma de árbol, de todos los dispositivos gestionados en una red. Define las variables usadas por el protocolo SNMP para supervisar y controlar los componentes de una red. Está compuesta por una serie de objetos que representan los dispositivos (como routers o switches) en la red. Cada objeto manejado en un MIB tiene un identificador de objeto único e incluye el tipo de objeto (tal como contador, secuencia o gauge), el nivel de acceso (tal como lectura y escritura), restricciones de tamaño, y la información del rango del objeto.

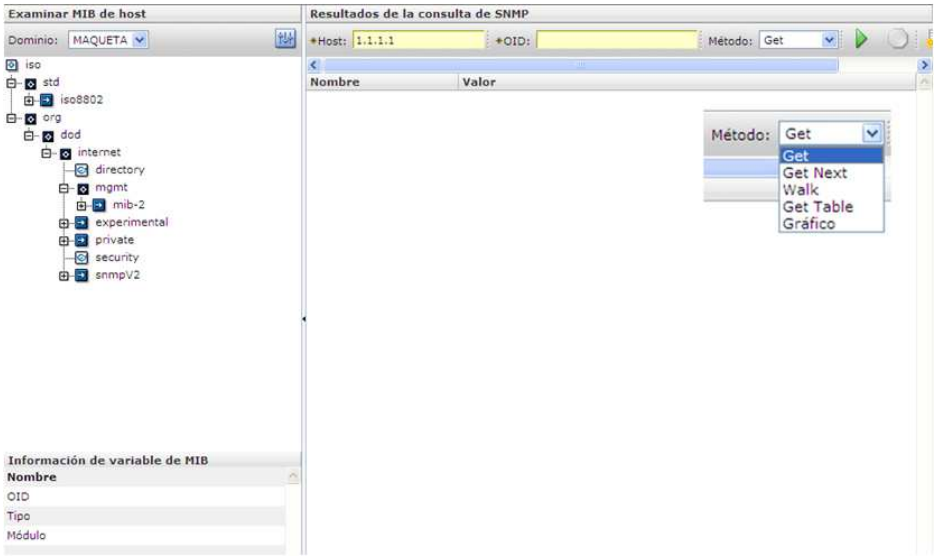


Figura 17. Pantalla que nos permite examinar el árbol de las MIBs del dispositivo seleccionado.

3.7.4.2 Vista de Red

La segunda opción que tenemos disponible para comprobar de forma gráfica el estado de la red y sus dispositivos es la **Vista de Red.** Al entrar en ella obtenemos una pantalla similar a la de la figura 18.

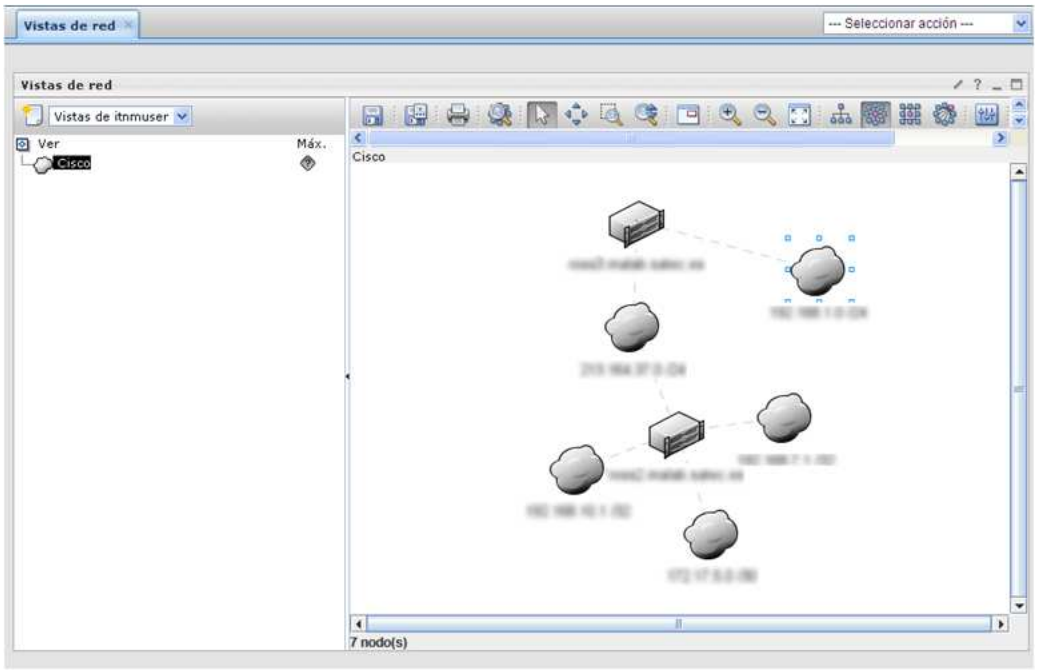


Figura 18. Pantalla principal de la vista de saltos.

Es una pantalla parecida a la de la vista de saltos, en la que podemos realizar prácticamente las mismas tareas sobre cada uno de los dispositivos, pero a diferencia de de la vista de saltos, las características que esta nueva vista nos ofrece son:

- Permite presentar una parte de la topología de la red a partir de filtros a las tablas de la base de datos.
- Se puede asociar estas vistas a usuarios o a grupos de usuarios
- Muestras el estado de los equipos a partir de las alarmas de Omnibus
- Se pueden ordenar un grupo de vistas bajo un árbol de jerarquía

Las opciones a las que tenemos acceso al desplegar el menú de cada uno de los dispositivos son las mismas que las de la vista de saltos, es decir: Mostrar sucesos (figura 14), Mostrar estructura de dispositivo (figura 15), Mostrar información de conectividad (figura 16) o examinar los datos de MIB de SNMP (figura 17), que se han comentado anteriormente, por lo que no se comentan.

Algo común a las dos vistas (la de saltos y la de red) es una serie de opciones denominadas **WebTools** (figura 19)**.**

Figura 19. Pantalla con las opciones de WebTools.

Estas opciones nos permiten entre otras cosas llevar a cabo opciones sobre dispositivos específicos de nuestra red, como realizar ping a un equipo o subred, consultar la ruta por la que pasarán los paquetes enviados hasta llegar a su destino (*traceroute*), o ver información personalizada de los dispositivos dependiendo del fabricante de estos.

3.7.6 Ejemplo de descubrimiento

Como ya se ha comentado, a la hora de realizar un descubrimiento de los equipos de la red, podemos hacer un descubrimiento completo o definir un ámbito sobre el que se llevará a cabo. Al definir un ámbito hacemos una especie de filtro entre todos los equipos, lo que nos permitirá descubrir tan sólo los equipos que nos interesan.

Para cada ámbito puede definirse el tipo de protocolo utilizado o un rango de IP's, como parámetros más utilizados.

A continuación se muestra un ejemplo de cómo podemos incluir o excluir dispositivos en el descubrimiento, agrupándolos en "zonas".

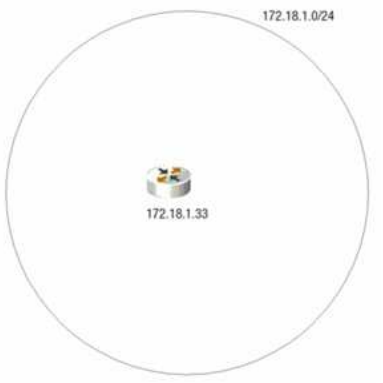


Figura 20.

La **figura 20**, muestra una zona de inclusión. El dispositivo con la dirección IP 172.16.1.33 se encuentra dentro de la zona en la que se realizará el descubrimiento, por lo que será descubierto.

La **figura 21** por el contrario, muestra una zona de exclusión dentro de la propia zona de inclusión, por lo que en este caso el equipo anterior no sería descubierto, y tan sólo se descubrirían los equipos que están en la red 172.18.1.0/24, excluyendo al ya citado 172.18.1.33.

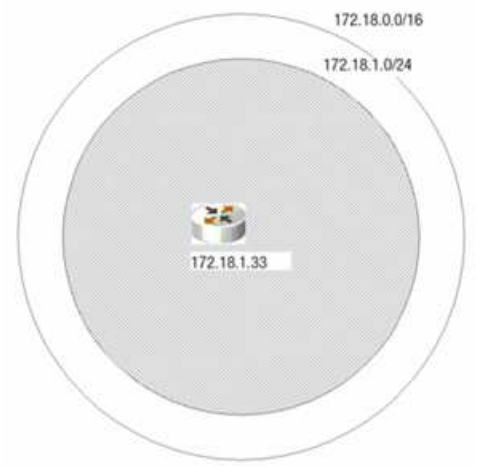


Figura 21.

Además de zonas de inclusión, como se ha visto antes, podemos definir directamente zonas de exclusión dentro de la red. Esto se muestra en la **figura 22**, donde vemos que el equipo con la dirección IP 172.16.1.33 está dentro de la zona que se ha declarado como exclusión, no es descubierto.

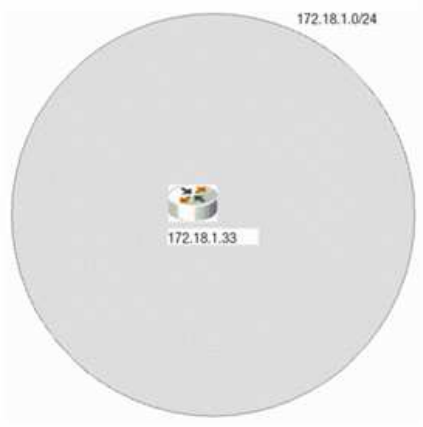


Figura 22.

Al igual que antes en la figura 2, se ha mostrado un ejemplo de una zona de exclusión dentro de una zona de inclusión, podemos hacer lo contrario, es decir, dentro de una zona de exclusión, definir una de inclusión. Esto puede verse en la **figura 23.** En este caso todos los equipos que se encuentren en la zona sombreada (la subred 172.18.1.0/24 no serán descubiertos.

Figura 23.

Estas zonas de exclusión o inclusión nombradas anteriormente deben ser definidas correctamente para que el descubrimiento se ejecute de forma óptima. Para ilustrar mejor lo anterior, se muestran 3 ejemplos de cómo definir las zonas asociadas al descubrimiento.

Definición de una zona de inclusión simple

En el ejemplo definimos la zona de inclusión sobre el protocolo IP y la asociamos a la subred 172.16.1.0/24. Esto nos permite descubrir cualquier equipo que esté dentro de la subred.

```
 insert into scope.zones
(
        m_Protocol,
        m_Action,
        m_Zones
)
values
(
        1,
        1,
        [
            {
                m_Subnet="172.16.1.0",
                m_NetMask=24
            }
        ]
);
```

Definición de una zona de inclusión múltiple

En este caso vemos cómo pueden definirse varias zonas de inclusión al mismo tiempo.

```
 insert into scope.zones
(
    m_Protocol,
    m_Action,
    m_Zones
)
values
(
1,
1,
[
   {
     m_Subnet="172.16.1.0",
     m_NetMask=24
              },
   {
    m_Subnet="172.16.2.*"
   },
              {
     m_Subnet="172.16.3.0",
     m_NetMask=255.255.255.0
   }
]
);
```

Mediante este insert, serán descubiertos los siguientes dispositivos:

- Cualquier dispositivo dentro de la subred 172.16.1.0/24 (máscara de subred 255.255.255.0)
- Cualquier dispositivo cuya dirección IP comience por "172.16.2"
- Cualquier dispositivo perteneciente a la subred 172.16.3.0, con máscara de subred 255.255.255.0.

  NOTA: La máscara de subred puede definirse de forma explícita como en el tercer caso o con la notación CIDR como en el primer caso

Definición de una zona de exclusión

Estas zonas pueden ser simples o múltiples y se crean del mismo modo que hemos creado las zonas de inclusión, salvo que ahora el campo m_Action debe tener valor 2, para indicar que es una zona de exclusión.

```
insert into scope.zones
(
m_Protocol,
m_Action,
m_Zones
)
values
(
1,
2,
[
{
m_Subnet="172.16.1.0",
m_NetMask=24
]
);
```

3.8 Monitorización de la red

En ITNM la monitorización es independiente para cada dominio de descubrimiento. Para monitorizar un equipo hay que configurar dos elementos: las definiciones de sondeos, y las políticas de sondeo. Esto se lleva a cabo en la opción: **Administración>Sondeo de redes**

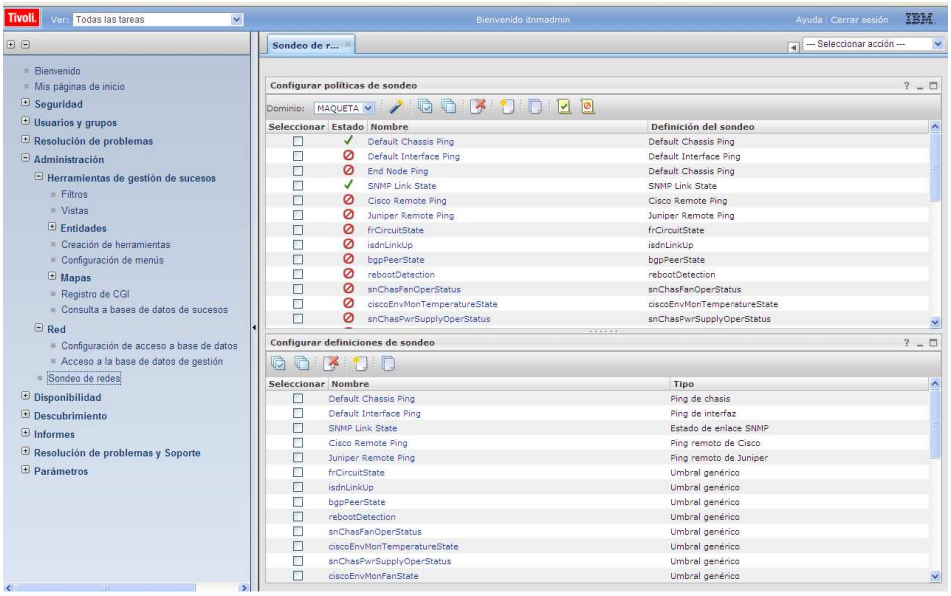


Figura 24. Pantalla principal de la vista de saltos.

Definiciones de sondeo

Las definiciones de sondeo es donde se especifica qué es lo que queremos monitorizar. Se pueden crear, borrar y copiar definiciones (también llamadas monitores).

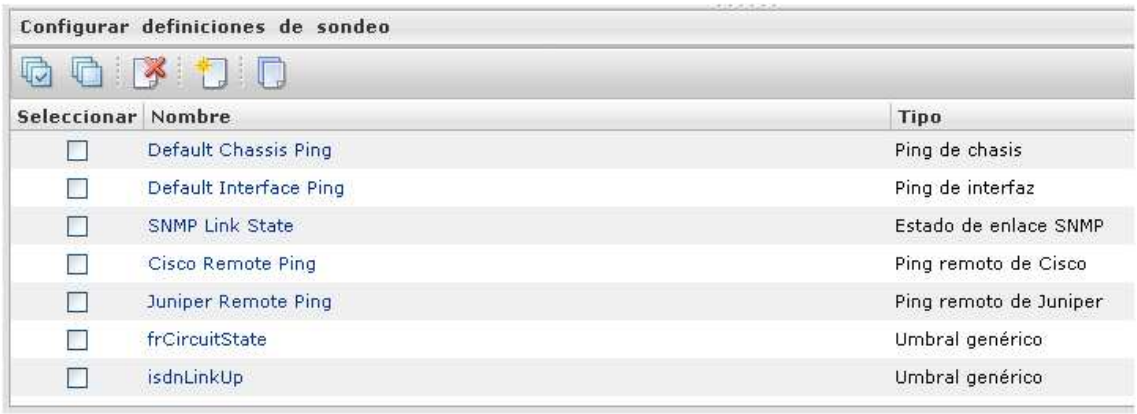


Figura 25. Pantalla que nos permite ver las definiciones de sondeo creadas, a la vez que permite crear una nueva definición.

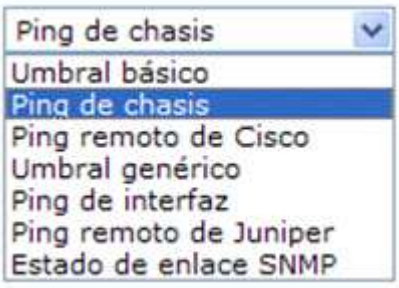
Hay una serie de definiciones de sondeo que ITNM incorpora por defecto como realizaciones de pings entre otras herramientas, pero para que el sondeo resulte eficaz, es conveniente definir definiciones propias adaptadas a nuestras necesidades. Para ello se pulsa sobre la opción "Agregar nuevo" y dependiendo del tipo de monitor que se quiera crear, se seleccionará una opción u otra de la lista desplegable que aparece.
Si queremos crear una definición de ping de chasis podemos configurar la criticidad con la que se enviaran las alarmas a Omnibus o el nº de reintentos antes de generar una alarma por ejemplo. Lo mismo podemos hacer para comprobar el estado de los enlaces SNMP.

En el caso de querer crear un "umbral genérico", podemos definir un umbral a partir del cual se genera una alarma de tipo problema y un umbral a partir del cual se genera una alarma resolución que esté relacionada con el problema.
Un ejemplo de estos sondeos podría ser:

```
(eval(int,"&SNMP.VALUE.ciscoMemoryPoolValid") = 1)
```

donde se indica si los objetos que pertenecen a esta entrada contienen datos precisos. Si una instancia de este objeto tiene el valor falso (valor distinto de 1), los valores de los objetos pueden contener información inexacta.

Políticas de sondeo



Lo que se especifica en esta opción es qué equipos se quieren monitorizar, cada cuanto tipo se quieren monitorizar y si tienen asociado una definición para saber que se quiere monitorizar dentro de cada uno de ellos.

Figura 26. Pantalla que nos permite ver las políticas de sondeo creadas, a la vez que permite crear una nueva.

Para crear una nueva política usamos la opción "Agregar nueva" donde especificamos la definición a usar, el intervalo de monitorización y si se utiliza un filtro que puede ser sobre la clase del equipo, sobre las distintas tablas de la base de datos o sobre los tipos de interfaces.

3.9 Seguridad

Cuando un usuario se autentifica en el sistema, se le da acceso a la aplicación dependiendo del rol que tenga dentro de esta. Estos roles están asociados a recursos de ITNM, por esto, son los roles los encargados de definir lo que un usuario puede ver, crear y modificar dentro de ITNM.

Estos roles, junto con los usuarios y los grupos, se pueden gestionar en un repositorio externo al que se accede desde la consola web de ITNM. Una vez completada la instalación es posible combinar varios repositorios de información en un único repositorio lógico llamado repositorio federado, que servirá de almacén de datos interno para el servidor.

La configuración del repositorio se realiza desde **Seguridad > Proteger la administración, las aplicaciones y la infraestructura**

Tipo de entidad	Entrada base para el padre por omisión.	Propiedades del nombre distinguido relativo
Group	o=netcoolObjectServerRepository	cn
OrgContainer	o=netcoolObjectServerRepository	o:ou:dc:cn
PersonAccount	o=netcoolObjectServerRepository	uid
Total 3		

Figura 27. Pantalla donde se muestra información sobre los repositorios.

En el caso de que no se haya elegido Omnibus como depósito de usuarios y grupos durante la instalación será necesario instalar un pluging para realizar la autenticación de usuarios a partir de la información de Omnibus. La modificación de usuarios y grupos se puede realizar desde Omnibus y desde ITNM, pero la asignación de roles solamente se puede realizar desde ITNM.

Una parte importante del trabajo del administrador es definir los roles que deben tener los distintos usuarios de la red para que dichos usuarios puedan realizar su trabajo diario. Por ello, una vez que se ha definido un repositorio para almacenar la información, se pueden crear usuarios y grupos. La administración de usuarios y grupos se encuentra en la opción **Usuarios y grupos** del menú principal.

3.9.1 Gestión de usuarios y grupos

Toda la administración de usuarios se encuentra en la opción Gestionar usuarios o bien en la opción Gestionar Grupos en el caso de querer gestionar un grupo de usuarios. En ambas opciones podemos consultar tanto los usuarios como los grupos creados, realizar búsqudas o crear uno nuevo.

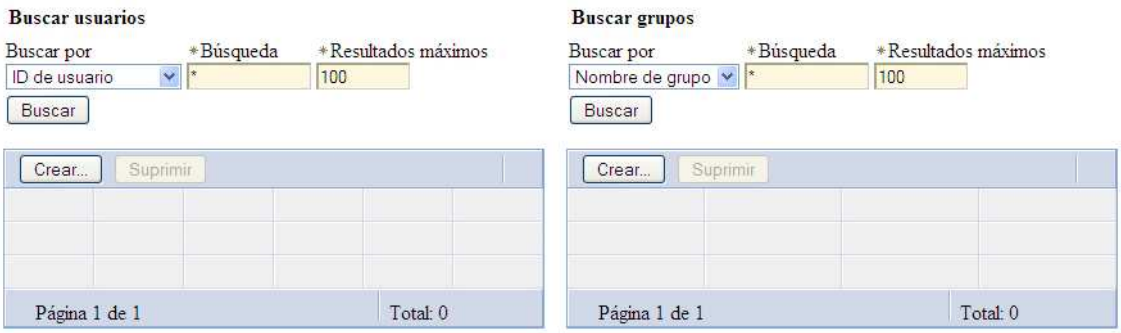


Figura 28. Pantalla donde se muestran las distintas opciones sobre los usuarios y grupos, como buscar, crear uno nuevo, etc.

Además de los grupos que creamos a medida para el cliente, ITNM incorpora una serie de grupos predefinidos que son los siguientes:

- **Network_Manager_IP_Admin**: Tiene acceso de administración sobre todas la páginas de ITNM
- **Network_Manager_User**: Contiene los roles necesarios para que un usuario de operación puede realizar su trabajo habitual con ITNM
- **Network_Manager_Client**: Contiene los roles necesarios para permitir que un cliente tenga un acceso básico a ITNM

3.9.2 Permisos y roles

El acceso a los recursos de ITNM se realiza por medio de roles, que pueden ser asignados tanto a usuarios como a grupos. Cuando un usuario es asignado a un grupo hereda los roles de este grupo, pero para simplificar la asignación de estos, se deben crear grupos de acuerdo con la estructura de la empresa para poder asignarles roles a medida y por último, los usuarios que se incluyen en él.

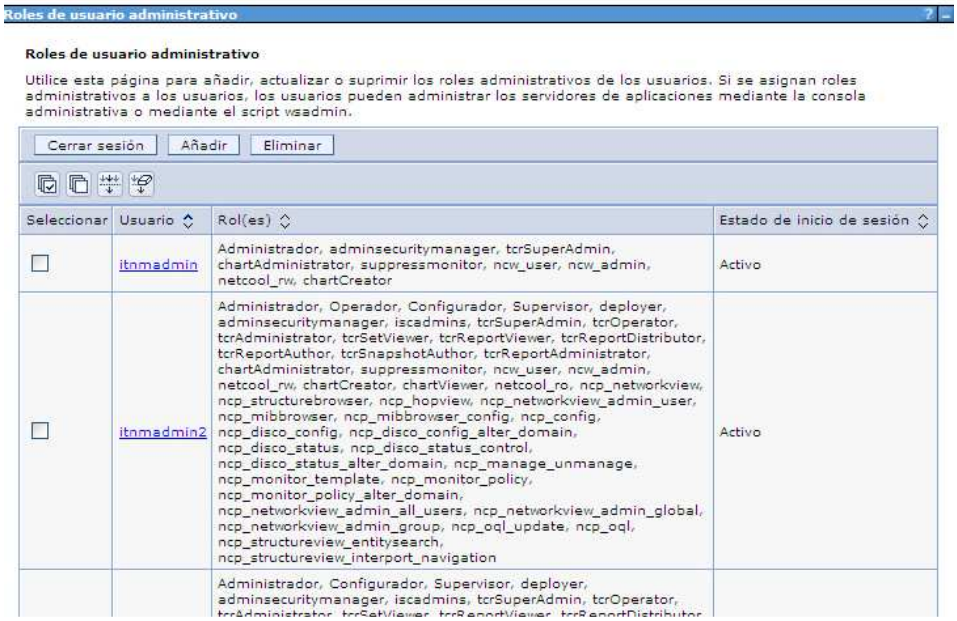


Figura 29. Pantalla donde se muestran las distintas opciones sobre los roles de los usuarios, además de las opciones para añadir o eliminar roles a usuarios existentes en la aplicación.

La asociación de roles-usuarios (figura 29) y roles-grupos (figura 30) se guarda dentro de la configuración de TIP a modo de "copia de seguridad", ya que llegado el caso de que se borre un usuario o un grupo en un repositorio la asociación de los roles se mantiene y es necesario eliminarla de forma manual.

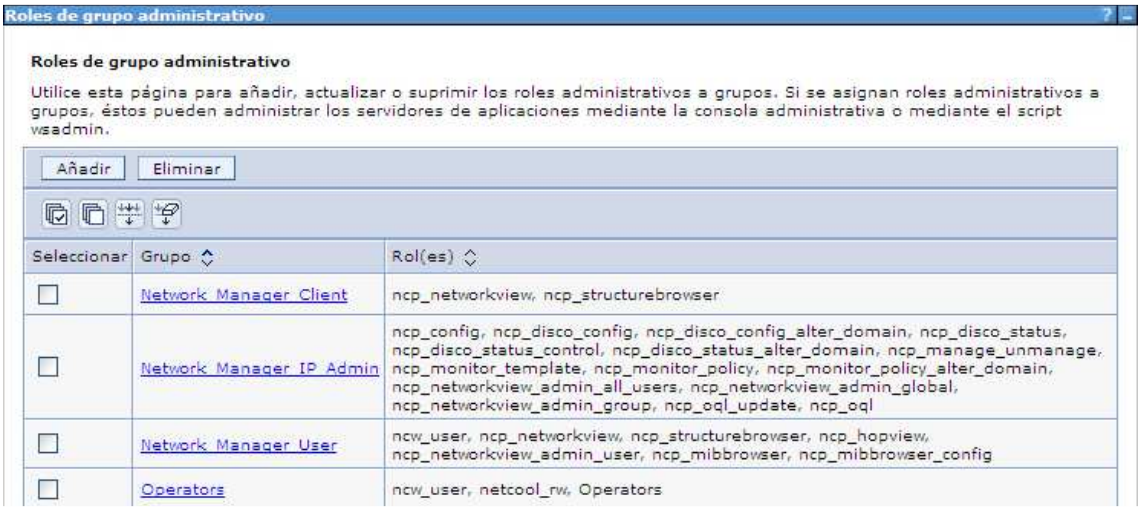


Figura 30. Pantalla donde se muestran las distintas opciones sobre los roles de los grupos, además de las opciones para añadir o eliminar roles a grupos existentes en la aplicación.

La asignación de roles dentro de un grupo se realiza igual que la asignación de roles dentro a un usuario, de modo que al borrar un grupo de esta lista se borra la asociación rol-grupo, pero no se borra el usuario.

3.10 Administración de páginas

Antes de ver algunos aspectos referentes a la seguridad de ITNM, hay que definir unos términos necesarios para poder comprenderlos.

- Vistas: Es una agrupación de tareas y páginas
- Carpeta: Es un contenedor de otras carpetas y páginas
- Página: Es una área de trabajo que puede contener uno o varios portlets
- Portlet: Es un pequeño programa que puede mostrar información o permitir el acceso a determinadas funciones.

El acceso a páginas, vistas, carpetas y portlets se realiza a partir de la asignación de roles. Adicionalmente se puede seleccionar entre tres niveles de acceso distintos para cada uno de los roles. Los posibles niveles de acceso son:

- Usuario
- Usuario con privilegios
- Editor

Un pequeño cuadro resumen de los privilegios de cada uno de estos niveles es el siguiente:

Recurso	Nivel de acceso		
	Usuario	Usuario con privilegios	Editos
Portlet	Ver e interactuar con el portlet y acceder a la ayuda	Ver e interactuar con el portlet, editar las preferencias personales y acceder a la ayuda	Ver e interactuar con el portlet, editar las preferencias personales, editar las preferencias globales y acceder a la ayuda
Pagina y carpeta	Ejecutar desde el árbol de navegación	Ejecutar desde el árbol de navegación	Ejecutar desde el árbol de navegación. Para las páginas modificar el contenido y la plantilla
Vista	Seleccionar la vista	Seleccionar la vista	Seleccionar la vista

Figura 31. Cuadro resumen donde se muestran los niveles de accedo a las distintas herramientas

Estos portlets, vistas, carpetas y páginas nos permiten definir qué será lo que vea un usuario o un grupo de estos, teniendo así una mayor seguridad a la hora de mostrar tan sólo lo que nosotros queremos de nuestra red.

La gestión de estos elementos se realiza desde la capeta **Parámetros** de la vista **Todas las tareas,** habiendo una opción específica para cada uno de estos elementos

Figura 32. Menú de configuración de páginas, vistas, portlets y roles, entre otros aspectos.

Carga automática de páginas

Al añadir una página a una vista se puede elegir si dicha página será cargada de forma automática cuando el usuario entre en la vista, siendo esta página la que se muestre como página de inicio para ese usuario en concreto.

La creación de estos perfiles de preferencia se realiza en la opción **Parámetros > Perfiles de preferencias de la consola.** Nos permite definir qué es lo que va a ver el usuario cuando se conecte a ITNM.

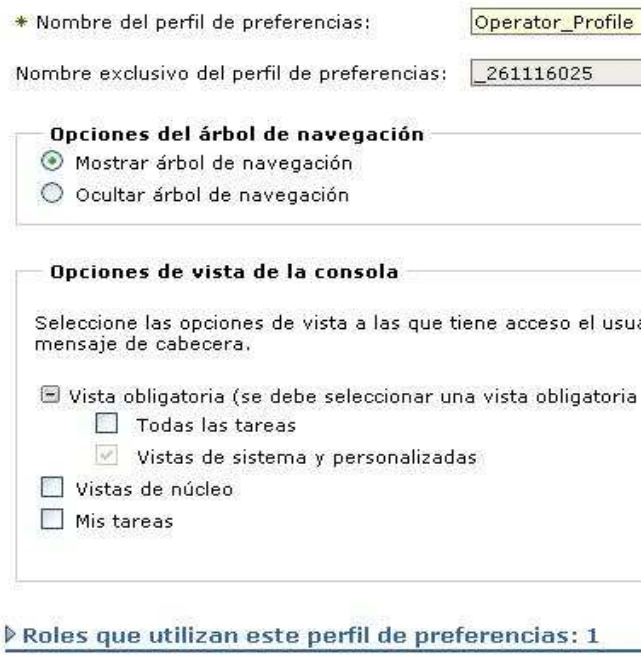


Figura 33. Captura de pantalla que nos muestra el proceso de creación de un perfil de preferencia para la vista de la consola de un usuario.

Además se pueden asociar los roles existentes o roles a medida al perfil de la consola, por lo que todos los usuarios con el rol verán las vistas definidas con la perfil de la consola (se les cargará de forma automática la vista definida dentro del perfil de consola).

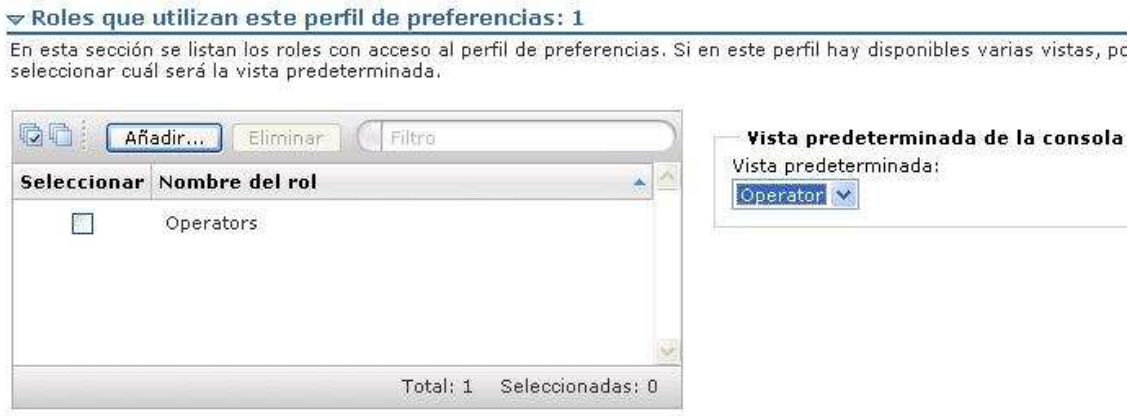


Figura 34. Captura de pantalla cómo asociar los distintos perfiles y roles

4. CONCLUSIONES

Desde que entre a formar parte del equipo de sistemas de SATEC S.A., he tenido la posibilidad de trabajar con distintas aplicaciones para la monitorización y administración de redes, profundizando más o menos en ellas, en cada uno de los proyectos en los que he colaborado.

Para cada nuevo proyecto, con sus propios requisitos y características, generalmente se necesita la creación de un nuevo entorno, ya sea por medio de virtualización o en un servidor nativo. En definitiva, son nuevos sistemas a supervisar para asegurar su correcto funcionamiento en servidores de la empresa y posteriormente para dar soporte a un cliente final.

Después de haber visto la funcionalidad de varias de estas aplicaciones para monitorizar una red, la elección de IBM Tivoli ITNM creo que ha sido acertada, ya que de entre todas las soluciones para la gestión de redes a que he tenido la oportunidad de utilizar, es la que ofrece un mejor interfaz, ya que permite a la persona que la utiliza encontrar todo rápidamente. Además, consta de una serie de opciones configurables que lo hacen lo suficientemente seguro y estable para poder ser utilizado en empresas de tamaño medio o grande.

Este Proyecto Fin de Carrera me ha permitido conocer de una forma bastante detallada, aplicaciones de monitorización, y trabajar con la aplicación de IBM, Tivoli ITNM, de la que puedo decir: que no tiene nada que envidiar a otras aplicaciones comerciales ni a las aplicaciones de software libre que actualmente están ganando mercado.

Para la realización de este proyecto he necesitado en torno a 640 horas repartidas de la siguiente manera:

- 25 horas/semana en los meses de octubre, noviembre y diciembre (2 primeras semanas)
- 30 horas/semana en el mes de diciembre (2 últimas semanas)
- 35 horas/semana entre los meses de enero y abril

Si hablamos de posibles trabajos futuros relacionados con el proyecto, la próxima línea de investigación, muy interesante para mí, es la posibilidad de asentar definitivamente ITNM en el cliente, dejando su red monitorizada de una forma correcta, para que la actividad diaria que realice, pueda llevarse a cabio de forma óptima.

Además de los conocimientos adquiridos en la empresa, esta experiencia me ha servido para asentar materias aprendidas durante la carrera como son:

1. Comprender la arquitectura Unix de las maquetas de pruebas; éstas son las réplicas de los sistemas reales donde se realiza el proceso de certificación.

2. Poner en práctica algunos conocimientos de SQL mediante el acceso a la base de datos en un sistema real con gran carga de trabajo. Tan sólo he utilizado consultas sencillas, pero ha servido para ver cómo se utilizan en el mundo real los conocimientos adquiridos en clase.

3. Realizar o revisar scripts de Shell Bash utilizados en la vida real, conociendo así una aplicación real de estos.

4. Asentar los conocimientos sobre redes adquiridos en las diferentes asignaturas de la carrera que han tratado sobre este tema.

5. BIBLIOGRAFÍA

Para la realización de este proyecto he consultado los siguientes medios:

- Tanenbaum, Andrew S. (2003), **Redes de Computadoras**, (4ª Edición), Ed. PrenticeHall

- IBM. **IBM Developers Works** [En línea] Disponible en: http://www.ibm.com/developerworks/wikis/display/tivolidoccentral/Tivoli+Network+Manager+IP+Edition (consultado entre enero de 2009 y abril de 2010)

- Wikipedia, **Conceptos varios**, [En línea] Disponible en: http://es.wikipedia.org (consultado entre enero de 2009 y abril de 2010)

APÉNDICE I: GLOSARIO DE TÉRMINOS

A continuación se encuentran recogidas todas las siglas empleadas durante este proyecto, de las que se especifica su significado.

- ATM = Asynchronous Transfer Mode (*Modo de transferencia asíncrono*)
- CIDR = Classless Inter-Domain Routing (*Encaminamiento Inter-Dominios sin Clases*).
- DNS = Domain Name System (*Servidor de nombres de dominio*).
- GUI = Graphic user interface (*Interfaz gráfica de usuario*).
- HTTP = Hypertext Transfer Protocol (P*rotocolo de transferencia de hipertexto*).
- HTTPS = Hypertext Transfer Protocol Secure (*Protocolo seguro de transferencia de hipertexto*).
- ICMP = Internet Control Message Protocol (*Protocolo de Mensajes de Control de Internet)***.**
- IP = Internet Protocol *(Protocolo de Internet)*
- IPTV = Internet Protocol Television *(Protocolo de internet para televisión)*
- JMX = Java Management eXtensions
- LDAP = Lightweight Directory Access Protocol (*Protocolo Ligero de Acceso a Directorios*).
- MAC = Media Access Control (*control de acceso al medio*)
- MIB = Management Information Base *(Base de Información Gestionada)*
- MPLS = Multiprotocol Label Switching *(Conmutación de etiquetas multiprotocolo)*

- NAT = Network Address Translation *(Traducción de Dirección de Red)*.
- POP3 = Post Office Protocol (*Protocolo de la oficina de correo*).
- SMTP = Simple Mail Transfer Protocol *(Protocolo Simple de Transferencia de Correo).*
- SNMP = Simple Network Administration Protocol *(Protocolo Simple de Administración de Red)*
- SSH = **S**ecure **Sh**ell *(Intérprete de órdenes segura)*.
- SSL = Secure Sockets Layer *(Protocolo de Capa de Conexión Segura)*
- TIC = Tecnologías de la información y la comunicación.
- TIP = Tivoli Integrated Portal (*Portal integrado de Tivoli)*
- VLAN = Virtual LAN *(Red de área local virtual).*