56

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

DISEÑO E IMPLANTACIÓN DE UNA SOLUCIÓN DE ADMINISTRACIÓN DE REDES Y SISTEMAS BAJO UN ESQUEMA DE OPERACIÓN DISTRIBUIDO

T E S I S

Que para obtener el Título de

INGENIERO EN COMPUTACIÓN

P r e s e n t a :

VICTOR MANUEL SIERRA MONTAÑÉS

Director: Ing. Adolfo Millán N.

MÉXICO 2001

Contenido

Índice de Figuras

Índice de Tablas

1.- Introducción

Hoy día las grandes organizaciones tienen que ser más eficientes y competitivas, a medida que la industria tecnológica evoluciona se complica cada vez más la administración de las redes y los sistemas que soportan los servicios sustantivos dentro de las empresas.

Para ello los Administradores de IT "Information Technology" tienen la responsabilidad de controlar el ambiente operativo garantizando la continuidad, integridad y disponibilidad de los servicios, asociando cada uno de los componentes que los conforman dentro de un factor de criticidad, simplificando con ello la administración de cambios y configuraciones, con lo cual se pueden prevenir y diagnosticar el impacto derivados de los cambios en el ambiente de producción.

De esta forma los Administradores de IT, han tenido que implantar dentro de sus organizaciones, esquemas robustos de Administración, Control y Monitoreo que les permita eficientar sus procesos y procedimientos operativos, permitiéndoles Conocer, Medir, Controlar y Mejorar su entorno informático, alineando al mismo tiempo las necesidades y requerimientos del usuario con las estrategias de desarrollo y la planeación operativa de la organización.

Dentro de la Industria Informática en nuestro país no se le ha dado la debida importancia a la Administración de los Servicios de Tecnología de la Información, quizá por cuestiones culturales o económicas, lo cierto es, que el contar dentro de las Organizaciones con un enfoque sistémico de procesos, alineado con los servicios y productos entregados y haciendo uso de la Tecnología, la Gente y los Procesos se logra eficientar la entrega de los servicios, disminuyendo al mismo tiempo los riesgos en la interrupción de los mismos y permitiéndole a los Administradores del negocio despreocuparse de las cuestiones técnicas sin la necesidad de dar en outsourcing tales servicios, así mismo les permite focalizar sus esfuerzos en los objetivos, las metas, la misión y visión del negocio.

Las soluciones de Administración de Servicios de Tecnología de la Información, su filosofía y metodología de implantación no tienen más de 5 años que se vienen practicando en nuestro País. Sus orígenes se remontan hacia el año de 1994 en Inglaterra y Holanda y tienen su base conceptual en el modelo de referencia ITSM "Information Tecnology Service Management", el cual adopta la filosofía ITIL "Information Tecnology Infraestructure Library", cuyo principal objetivo es proveer a la organización de la metodología que le permita convertirse en una organización de clase mundial, haciendo uso de buenas y mejores prácticas, mediante la definición y estandarización de procesos y procedimientos técnicos y operativos

Dentro de las grandes Organizaciones a nivel Mundial que han adoptado la filosofía de ITIL se pueden mencionar entre otras: First Bank of Chicago, Lufthansa Airlines, Telstra Telecom. Australia, Corpoven Oil, Pepsi-Cola, Alcatel Network Systems, Federal Express Corp y en nuestro País instituciones como Telmex, Pemex y algunas Instituciones Bancarias han iniciado con la práctica de la filosofía de ITIL a través del modelo de ITSM.

De ésta manera y con el fin de incrementar la calidad de sus servicios informáticos, la Secretaría de Hacienda y Crédito Público "SHCP" a través del Servicio de Administración Tributaría "SAT" responsable de la administración y operación de todos los centros informáticos de la institución se dio a la tarea de implantar una solución de Administración, Control y Monitoreo de Redes, Instalaciones, Equipos y Sistemas sobre 4 Disciplinas de administración dentro de sus unidades sustantivas de Recaudación y Aduanas, de acuerdo a los requerimientos planteados en el apartado 3.3.1 y conforme al ambiente planteado en el capítulo 2.

Cabe mencionar que la infraestructura del SAT ya cuenta con una serie de áreas tecnológicas tales como Seguridad, Mesa de Ayuda, Laboratorio de Pruebas, Administración de Versiones, Atención a usuarios, Integración de Sistemas, las cuales ya cuentan con los sistemas de administración de recursos informáticos, por lo que únicamente se acotaron los alcances del proyecto al diseño de solución e implantación sobre las 4 Disciplinas de Control mencionadas (Sistemas Operativos, Bases de Datos, Red de Comunicaciones y Procesos), considerándose la integración de la solución de Redes y Sistemas con los ambientes productivos de cada una de estas áreas.

Dentro de los resultados, ventajas y beneficios esperados por el SAT de la solución se encuentra entre otros:

- Disminución de Incidencias reactivas a problemas específicos
- Disminución de riesgos operativos
- Mejorar la calidad y continuidad de los servicios informáticos
- Proveer de las herramientas de control remoto y monitoreo en línea a los Administradores de los Sistemas Operativos, las Bases de Datos y la Red de Comunicaciones.
- Contar con la información histórica para el análisis de tendencias y crecimientos futuros.

2.- Infraestructura Soportada

2.1.- Servicios Informáticos

Por su origen e importancia recaudatoria, los servicios informáticos brindados por el SAT a nivel nacional, se pueden clasificar dentro de 2 grandes Unidades Administrativas, Recaudación y Aduanas, las cuales tienen entre sus funciones primordiales las siguientes:

- Determinación, liquidación y recaudación de impuestos
- Vigilancia del correcto cumplimiento de las obligaciones fiscales
- Atención fiscal al contribuyente
- Administración del Despacho Aduanero
- Correcta aplicación de la legislación fiscal y Aduanera

Dichas funciones se complementan con las de las Administraciones de Jurídica de Ingresos, la Administración Fiscal Federal, Política de Ingresos, Grandes Contribuyentes entre otras, las cuales colaboran en el cumplimiento de los objetivos y misión del SAT, el cual se puede resumir en: Recaudar con calidad y eficiencia las contribuciones federales necesarias para financiar el gasto público, garantizando la correcta y equitativa aplicación de la legislación fiscal y aduanera propiciando su cumplimiento voluntario y oportuno.

Para cumplir con sus funciones sustantivas la Administración General de Aduanas cuenta con 47 Aduanas distribuidas a los largo y ancho del territorio nacional; Por la naturaleza de sus importaciones, exportaciones, aranceles y ubicación geográfica las Aduanas se clasifican en 4 tipos: Fronteriza, Marítima, Aeroportuaria e Interior. Cada Aduana cuenta dentro de su rango perimetral de jurisdicción con una Sección Aduanera o bien una Garita de Internación, las cuales sirven como filtros de inspección y revisión de las importaciones y exportaciones que entran o salen del territorio nacional, en el anexo 1 se presenta la distribución de Aduanas a nivel nacional.

La Administración General de Recaudación cuenta con 8 Centros Regionales distribuidos estratégicamente a nivel Nacional, desde los cuales se controla la operación recaudatoria de las 66 Administraciones Locales del País (Anexo 2), teniendo bajo su responsabilidad la operación y atención al contribuyente a través de los sistemas y subsistemas recaudatorios de registro, contabilidad, control de obligaciones, devoluciones, compensaciones, pagos, notificaciones, etc.

Dentro de la operación de los Centros Regionales de Recaudación se lleva a cabo el proceso de cierres contables a través del procesamiento de declaraciones y obligaciones fiscales de todos los contribuyentes del País. Dicho proceso se inicia con el acopio de documentos a través de las Administraciones Locales, Bancos o electrónicamente por medio de Internet, posteriormente se lleva a cabo el proceso de captura óptica de caracteres "OCR" para finalmente consolidar e

integrar la información procesada de manera Regional en la Base de Datos Central de Hacienda, desde la cual se reporta mensualmente la Balanza Comercial del País.

Para el control y operación de los diferentes centros de cómputo tanto de Recaudación, Aduanas y el Centro de Procesamiento Nacional o "CPN" se cuenta con la infraestructura informática necesaria conformada por Hardware, Software, Redes de Comunicaciones, Sistemas, etc., a través de la cual se soporta la operación del SAT a nivel Nacional.

2.2.- Software

2.2.1.- Sistema Operativo

Se cuentan aproximadamente con 150 servidores Unix distribuidos a nivel nacional en 47 Aduanas, 8 Administraciones Regionales, 66 Locales de Recaudación y el Centro de Procesamiento Nacional.

Todas las Aduanas del País, las Administraciones Locales de Recaudación y el Centro de Procesamiento Nacional cuentan con Servidores HP 9000 Serie 800 con sistema operativo HP-UX 10.20

Las Administraciones Regionales de Recaudación cuentan con 8 Cluster's de Alta disponibilidad bajo plataforma IBM RS/6000 con Sistema Operativo AIX 4.3.2.

Para la operación de captura de los centros Regionales se cuenta con infraestructura soportada por Servidores HP 9000 Series 700 y 800 con sistema operativo HP-UX 10.20

2.2.2.- Base de Datos

El manejador de base de datos institucional es Informix Online versión IDNS "Informix Dinamic Server" 7.31, los nodos de Datawarehouse cuentan con Informix EPS "Enterprise Paralell Server" 8 21 con las herramientas de desarrollo Informix SQL y 4GL.

2.2.3 - Alta Disponibilidad

Actualmente se cuenta con 23 Cluster's de Alta disponibilidad integrados de la siguiente forma.

- 9 Cluster's sobre plataforma IBM con HACMP conformados por 2 nodos IBM RS/6000 H50 con 4 procesadores a 350 Mhz cada uno, 1 GB de memoria RAM y 100 GB de almacenamiento en disco

- 12 Cluster´s integrados con HP Service Guard conformados cada uno por 2 nodos HP9000 K460 y D370 con 2 Procesadores PA-RISK 8000 a 180 Mhz, 512 MB de memoria RAM y 40 GB en Disco promedio.

- 1 Cluster de 3 Nodos HP9000 K580 con HP/MC Service Guard, 4 Procesadores PA-RISK 8200 a 240 Mhz, 1 GB en RAM y 1.7 TB en Disco Raid 5 de EMC^2

- 1 Cluster de 8 Nodos HP9000 K580 con 4 procesadores PA-RISK 8200 a 240 Mhz, 1 GB en RAM y 1 TB en disco raid 5 de EMC^2, este cluster se encuentra integrado con Informix EPS 8.21 con tecnología Hiper-Fabric de HP, el cual se comunica a través de una red de alta velocidad ATM a 155 MB/s

2.3.- Hardware

La plataforma tecnológica es en el 95% HP9000 serie 800 con servidores de las familias "D" y "K" con capacidades de cómputo que van desde servidores con 1 procesador hasta servidores que soportan 16 procesadores y 8 GB en memoria RAM, almacenando desde 25 GB en Base de Datos hasta 1.7 TB de información

El 5% de la infraestructura restante son servidores IBM RS/6000 H50 con las características descritas anteriormente, aunque estos servidores son los menos en el ambiente operativo del SAT son los más críticos debido a las aplicaciones y el servicio que brindan, ya que se encuentran distribuidos en las 8 Administraciones Regionales del País.

Toda la infraestructura de almacenamiento de respaldos se encuentra soportada por librerías con tecnología DLT 7000, que van desde DLT´s Standalone para el caso de las Administraciones Locales hasta librerías de 494 slots y 10 Drives de almacenamiento, como es el caso del CPN.

Toda la información se encuentra almacenada en disco magnético integrada en estructuras de raid 5 por cuestiones de integridad y paridad de la información. La información almacenada en Base de Datos se encuentra integrada en Raw Device, lo cual representa una estructura de almacenamiento más seguro y eficiente que a través de las estructuras de archivos o File System, ya que el acceso a la información es de manera directa a secciones y sectores de disco

Para el caso del CPN se cuenta con 2 arreglos de disco Symetric EMC^2 con capacidad de almacenamiento de 1.0 y 1.7 TB de información cada uno almacenando únicamente información de Base de Datos Informix

2.4.- *Comunicaciones*

La red de comunicaciones se encuentra integrada de la siguiente forma:

- Integración de redes WAN sobre TCP/IP, ATM y Frame Relay con enlaces E0, E1 en el 95% de la red, el resto cuenta con enlaces de 128 Mb/s y redes LAN TCP/IP a 100 Mb/s (Anexo 3), cabe mencionar que sobre los anchos de banda mencionados se brindan tanto el servicio de voz como el de datos, multiplexando ambos a través de multiplexores GDC e IDNX.

- Se cuenta aproximadamente con 450 redes, 700 segmentos de red, 500 nodos y 2000 interfaces.

- La infraestructura informática de comunicaciones es By-Networks con rutedores, switches y multiplexores inteligentes configurados con OSF para habilitar la disponibilidad de ruteo dinámico a alta velocidad, interconectados a través de Multiplexores GDC con TMS5000.

- Para la conmutación de voz se cuentan con conmutadores Ericcson y Alcatel a través de los cuales se conforma la red de voz privada de la SHCP.

- Servicios conjuntos de ARPA/BERKLEY, bajo el protocolo TCP/IP e interfaces programáticas de alto nivel con SOCKETS de BSD

Los estándares utilizados son:

- IEEE 802.3 para interfaces de red local.
- UTP 5
- ATM, Frame Relay, FC
- TCP/IP en red local para enrutamiento y transporte
- NFS

Los servicios básicos de ARPA/BERKLEY utilizados son:

- Comandos "R" (rlogin, rcmd).
- Transferencia archivos (ftp, rpc).
- Emulación terminal (telnet, rlogin).

3.- Definición del Problema

3.1.- Objetivo

Diseñar e implantar una solución de Monitoreo de Redes y Sistemas basada en estándares de la industria, que integre toda la infraestructura identificada dentro del ambiente de operación bajo un esquema de administración y control centralizado, de tal manera que:

- Simplifique y unifique la administración de redes y sistemas, así como el acceso a las aplicaciones, redes, servidores, bases de datos, esquemas de seguridad y alta disponibilidad.

- Que permita conocer, controlar, mejorar y eficientar los procesos operativos del entorno administrado.

- Que cuente con esquemas consistentes sobre las disciplinas de administración, los cuales deberán ser independientes de las plataformas instaladas, así como de los cambios en la arquitectura administrada.

- Cuente con un esquema de detección y monitoreo que permita incrementar el grado de automatización de corrección de problemas, así como con la información oportuna para reaccionar proactivamente a los eventos y eleve así los niveles de servicios y productos.

- Que incremente el grado de automatización para la corrección de problemas.

- Que cumpla con los esquemas de seguridad que garanticen la continuidad de los servicios y la integridad de la información.

3.2.- Alcances

Considerando el ambiente operativo descrito en el inciso 2 y los requerimientos del apartado 3.3 se plantean 2 etapas a seguir para la implantación de la solución.

Etapa I.- Elaboración del Diseño Detallado de la Solución para cada disciplina de administración, que consiste en la definición y diseño de la solución en base al ambiente y requerimientos planteados, contemplando los siguientes aspectos:

- Análisis de requerimientos
- Objetivos y alcances de solución
- Diseño detallado de la arquitectura y descripción de los elementos integrados en la solución propuesta
- Desarrollo de políticas y procedimientos técnicos y operativos

- Descripción de las tecnologías, arquitectura, componentes y plataformas empleadas.
- Escalabilidad de la solución

Etapa II.- Implantación de la solución presentada en base a los alcances y prioridades definidas en la etapa I, incluyendo:

- Plan de trabajo de la implantación
- Herramientas (hardware y software)
- Desarrollo de la solución.
- Documentación (Memorias Técnicas, Políticas y Procedimientos)

3.3.- Funcionalidad

Las características básicas de la solución son:

- Estar basado en estándares de la industria.
- Capacidad de integración, monitoreo y administración en un único punto de control.
- Esquema distribuido de administración y control por función geográfica o unidad de negocios.
- Ser una solución abierta que permita la integración sencilla y completa de nuevos módulos en un ambiente heterogéneo y en una etapa de reingeniería y rearquitectura, esto es, una solución escalable y expandible
- Contar con un repositorio centralizado de información que pueda ser flexible para soportar multisites, y su transparente migración a este esquema.
- Establecer la solución automática de problemas, niveles de prioridades, o bien notificación a un punto central de monitoreo "Centro de Monitoreo CMN".
- Tener alta disponibilidad y resistencia a fallas. En particular, debe considerarse la dependencia que la solución tiene respecto a la red de comunicaciones.
- Ser flexible para adaptarse a un ambiente dinámico de operación, permitiendo su crecimiento, adecuación e incorporación de nuevas funcionalidades.
- Optimizar el contenido de la información enviada al Centro de Monitoreo, con el fin de reducir el tráfico de la red.

Que la administración y control del ambiente definido considere el aviso de eventos al repositorio central de manera automática y oportuna, bajo las siguientes premisas:

- El monitoreo y control debe llevarse a cabo a través de agentes SNMP (Simple Network Management Protocol)
- La solución incluirá una base de datos central, en la cual se deben registrar todos los eventos, de tal forma que se pueda contar con esta información

para referencias futuras, análisis estadístico, auditoria, administración de niveles de servicio, etc.

- Contará con un alto grado de automatización en la detección y corrección de eventos, corrigiendo de manera local mediante acciones definidas a problemas específicos, los cuales deberán catalogarse, registrarse y notificarse directamente al Centro de Monitoreo desde cualquier nodo administrado.
- Integrará un mecanismo de filtración que optimice el flujo y tráfico de información al Centro de Monitoreo y facilite la interpretación de mensajes, incluyendo en la medida de lo posible pre-diagnósticos y alternativas de solución.
- Dentro de cada una de las áreas de administración definidas, agrupar los mensajes en unidades lógicas de acuerdo a las clasificaciones específicas, tales como:

    * Incidencias (Problemas y Fallas)
    * Sistema operativo
    * Base de datos
    * Procesos
    * Comunicaciones
    * Rendimiento
    * Alta Disponibilidad
    * Niveles de Servicio

Los requerimientos a continuación descritos, se encuentran clasificados en dos categorías básicas, las cuales forman una solución integral, los cuales describen las características técnicas y operativas de la solución, que no necesariamente representan un desarrollo específico, si no son el resultado de la información generada durante el monitoreo y administración de los nodos, o bien requieren de la elaboración de estándares y procedimientos de control, administración u operación.

3.3.1.- Requerimientos por Disciplina de Administración

3.3.1.1.- Administración de la Red

- La solución contará con un esquema de control y administración total de la red.
- Capacidad para configurar remotamente los sistemas de comunicación, dependiendo de las características de los equipos que así lo permitan.
- Descubrimiento automático de la topología de la red, nodos, direcciones, segmentos de red, etc.
- Representación Gráfica a través de consolas de monitoreo de todos los enlaces y segmentos de red, incluyendo todos los componentes que los conforman (Servicios de datos), visualizando el nivel más básico de cada componente (interfaz, instancia, puertos, tarjetas, etc.)

- Identificación de direcciones IP duplicadas, descubrimiento de rutas y segmentos problema.
- Colección de variables MIB´s que permitan analizar el comportamiento de los enlaces de comunicación y los componentes que la integran.
- Representación gráfica de colecciones de información del comportamiento de ciertas variables MIB´s seleccionadas
- Esquemas de notificación cuando el estado de un nodo cambie mediante señales visuales y auditivas. Si el problema ocurriese fuera del horario de oficina, se contará con un dispositivo de notificación externa vía (Pagers).
- Habilitación de procesos y procedimientos de inspección remota y centralizada del nodo problemático, su posible corrección y notificación inmediata.
- La información detallada recopilada por la solución deberá ser registrada en la Base de Datos Central, para permitir el análisis periódico de la misma, esta característica permitirá a los administradores de la red:
    - ◊ Determinar problemas recurrentes y determinar cursos de acción para eliminarlos.
    - ◊ Examinar tendencias sobre tráfico de la red y optimizar la utilización de los canales mediante el establecimiento de calendarios de transmisión.

3.3.1.2.- Administración de Desempeño

- Se deberá llevar a cabo el ajuste o afinación (tunning) de los sistemas monitoreados, permitiendo realizar un análisis de capacidades (capacity planning).
- Monitoreo de los recursos del sistema operativo (Kernel, CPU, memoria, disco, usuarios, procesos, swap, File System´s, etc.), generando alarmas preventivas cuando éstos excedan los umbrales permisibles de operación.
- Despliegue gráfico y remoto de los nodos y sus recursos administrados a través de las consolas de monitoreo desde el CMN.
- Visualización gráfica histórica y en línea a manera de histogramas o tacómetros desde consolas remotas de los recursos vigilados.
- Detección de cambios dentro de la configuración del sistema operativo a nivel File System, Volúmenes Lógicos, Volúmenes Físicos, Versiones, parámetros de kernel, etc
- Banco de Datos y eventos de utilización de recursos, que permitan la planeación y prevención para efectos de crecimiento, optimización de aplicaciones, adecuación de calendarios de producción, etc.

3.3.1.3.- Administración de Bases de Datos

- Monitoreo de las Bases de Datos, Instancias y Recursos asignados al manejador.
- Monitoreo de los espacios asignados a la base de datos, a través de la interpretación de la información proporcionada por las herramientas del manejador de Bases de Datos, de acuerdo a los parámetros de medición establecidos.
- Monitoreo de la disponibilidad de los servicios del manejador de base de datos.
- Despliegue gráfico y remoto de las Bases de Datos y sus recursos administrados a través de las consolas de monitoreo desde el CMN.
- Visualización gráfica histórica y en línea a manera de histogramas o tacómetros desde consolas remotas de las Bases de Datos y sus recursos.
- Monitoreo de la integridad de los archivos de configuración y de los parámetros de ambiente requeridos por el manejador de base de datos.
- Detección de cambios en las estructuras del manejador de base de datos, para determinar y prevenir las causas posibles de corrupción, violaciones de seguridad, integridad, etc.
- Banco de Datos y eventos de utilización de recursos, que permitan la planeación y prevención para efectos de crecimiento, optimización de aplicaciones, adecuación de calendarios de producción, etc.

3.3.1.4.- Administración de Procesos.

Dentro del ambiente de producción existen procesos que se ejecutan de una manera automática (Daemons) o por medio de intervención del operador. Existen actividades planeadas y programadas a realizarse a una cierta hora o en un cierto día a cierta hora. Estos procesos automáticos son supervisados por los operadores, ya sea por medio de respuestas típicas o resultados planeados. Cuando una tarea automática no sea posible realizarla por falla de recursos, automáticamente se reprograman a un tiempo posterior y por un número limitado de veces

De hecho, cada proceso puede durar un cierto tiempo, dependiendo de ciertas circunstancias, o arrancarse para no ser interrumpido nunca, como podría ser un recurso del manejador de la base de datos o del Sistema operativo Los procesos consisten en un número determinado de pasos o uno solo. Dentro de esta denominación de procesos recaen los que el usuario puede llegar a arrancar por medio de terminales remotas y sin un horario establecido

Al tratarse de una solución integral, la tarea del administrador de procesos, deberá de interceptar cualquier proceso que se intente arrancar o que el mismo sistema operativo tenga programado arrancar Cada proceso que falle al lograr su objetivo, o que amenace con saturar la capacidad del propio equipo, deberá de reportarse

- Desarrollar las herramientas de explotación local y remota de las bases de datos generados por los eventos provocados por los procesos controlados por el administrador de procesos, y su relación con los niveles de servicio.
- Capacidad de autochequeo dentro de lo conceptual izado en seguridad.
- Poca necesidad de recursos de equipo para su operación, o bien, solución técnica que evite el sacrificio de recursos propios del equipo.
- Administración remota o local con niveles de administrador y operador de manera independiente.
- Intercepción de peticiones de ejecución.
- Registro de eventos por proceso, clase y tipo de proceso.
- Capacidad de monitoreo visual local y remoto.

4.- Método de Solución

4.1.- *Modelo de referencia ITSM*

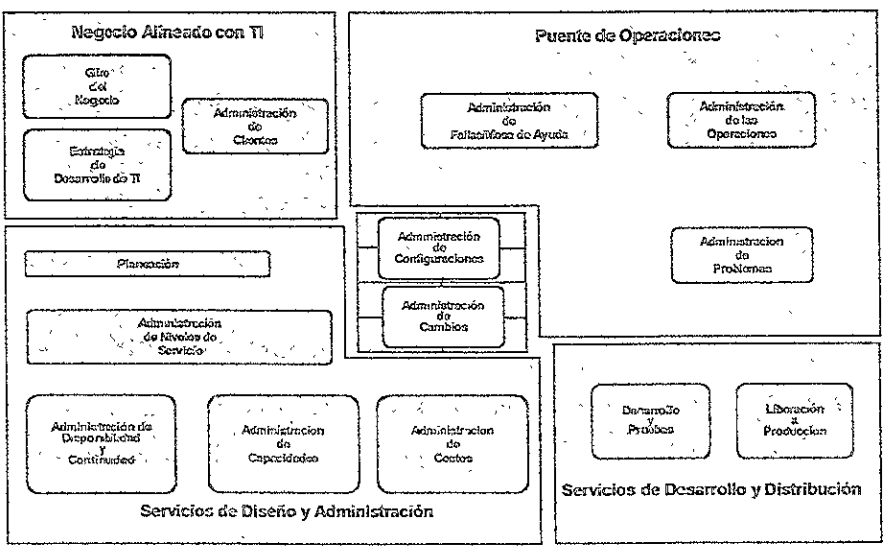


Figura 1 Modelo de referencia "ITSM"

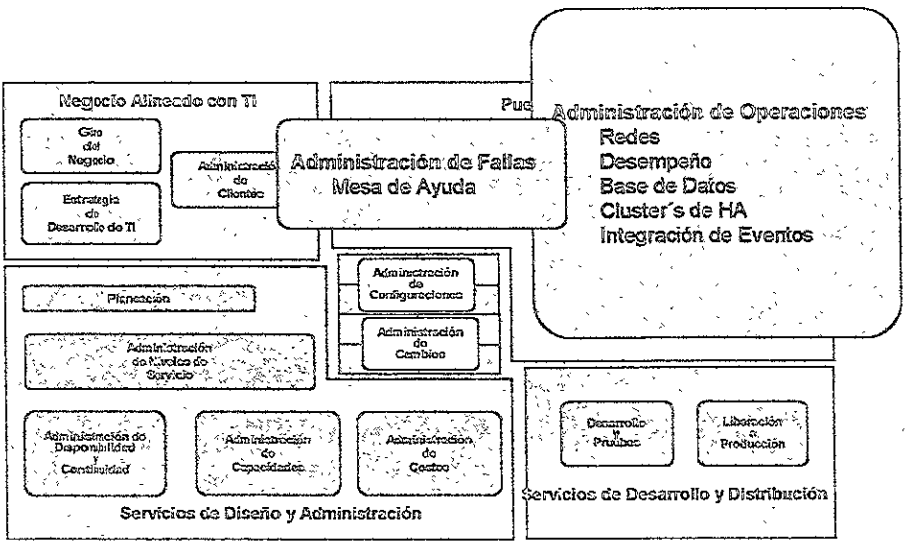


Figura 2. Descripción Modelo de Referencia "ITSM"

4.1.1.- Descripción del Modelo

El modelo de referencia de ITSM se basa en la estructura funcional de cualquier organización, de ahí su flexibilidad de implantación dentro del diseño de soluciones de Tecnología de la Información

Basados en los principales procesos de la metodología de ITIL, el modelo consta de cuatro cuadrantes y un cuadrante central donde se alinean los otros cuatro, cada cuadrante representa una etapa del proceso de la Administración de los Servicios de Tecnología de Información de la organización.

La aplicación de los procesos y procedimientos de la metodología de ITIL es completamente acorde con la arquitectura del modelo de referencia, de hecho dentro de cada cuadrante se integran diferentes procesos.

La estructura y funcionalidad de cada cuadrante se describe a continuación, así como una breve descripción de los objetivos de los principales procesos de ITIL

Primer Cuadrante, "Alineación del Negocio".- Este primer cuadrante está enfocado a los Administradores del Negocio, ya que es en él donde se definen las estrategias y el giro del negocio, también se identifican ahí nuevas áreas de oportunidad y es aquí donde se lleva a cabo la Administración de los clientes, cuentas empresariales, satisfacción de servicios, etc. En otras palabras este primer cuadrante representa las relaciones del negocio. En este primer cuadrante se enfocan algunos procesos y estrategias empresariales como son los procesos de B2B "Business to Business", CRM "Customer Relationship Management", CRC "Customer Relationship Clients" y otros procesos de continuidad estratégica del negocio como son los procesos de ERP "Enterprise Resource Planning", DRP "Disastry Recovery Planning", etc.

Segundo Cuadrante, "Servicios de Diseño y Administración".- En él se llevan a cabo una serie de funciones de vital importancia para el negocio, ya que es aquí donde se realizan las funciones de Planeación, Análisis, Administración de niveles de servicio, Administración de Costos, Capacidades, Disponibilidad, Continuidad y definición de estrategias corporativas; Dentro de este segundo cuadrante se ubican a los arquitectos empresariales, quienes con una visión global del negocio tienen a su cargo la difícil labor de diseñar y dimensionar las soluciones tecnológicas acordes a las necesidades del cliente, manteniendo estrecha relación con las áreas técnicas, operativas y administrativas para garantizar la completa funcionalidad de los requerimientos.

Tercer Cuadrante, "Desarrollo y Distribución".- En este cuadrante se lleva a cabo el proceso de construcción de las soluciones y los sistemas requeridos dentro de la organización, los cuales deben satisfacer los acuerdos de niveles de servicio definidos en el cuadrante anterior; Una vez construidos los sistemas deben ser evaluados previa implantación y liberación a producción, para ello dentro de las áreas de Laboratorio de Pruebas y Administración de Versiones se deben llevar a cabo las pruebas unitarias, integrales, de volumen, etc., que garanticen primero, la funcionalidad requerida por el usuario y segundo el no impactar a los ambientes de producción, también es aquí donde se deben llevar a cabo los procesos de versionamiento de toda la programación y código generado, así como los procesos de distribución e instalación de aplicaciones en los ambientes de operación de tal forma que garanticen su homologación de manera casi instantánea.

Cuarto Cuadrante, "Puente de Operaciones".- En este cuadrante recae la función de los administradores de TI, los administradores de telecomunicaciones, los administradores de los sistemas operativos, bases de datos, y en general de todos los ingenieros, técnicos y operadores que tienen a su cargo garantizar la continuidad y disponibilidad de los servicios informáticos; Para ello deben desarrollar e implantar sistemas automatizados que les ayude a eficientar sus funciones de administración, control, operación y mantenimiento aplicando estrategias operativas, definiendo estándares de calidad e implantando procesos, políticas y procedimientos de buenas y mejores prácticas

Dentro de este cuadrante se ubican una serie de procesos técnicos y operativos que aplicados de una manera eficiente pueden llegar a simplificar mucho las labores de administración y control de los ingenieros; Dentro de los principales procesos de administración de servicios se encuentran: Administración de respaldos, administración de seguridad, administración del almacenamiento, administración IP, administración de procesos, administración de disponibilidad, administración de alarmas, administración de reportes, administración de mesa de ayuda, administración de incidencias, etc.

Cuadrante Central.- Este cuadrante concentra la administración de cambios y la administración de configuraciones, en él se integran todos aquellos componentes que soportan los servicios de TI de la organización; Con una adecuada administración de este cuadrante las organizaciones podrán estar preparadas para identificar, cuantificar y minimizar el impacto y los riesgo de los cambios derivados de nuevos proyectos, actualizaciones tecnológicas o simplemente la ampliación o interrupción de sus servicios; Es muy importante mencionar que este último cuadrante debe tener estrecha relación con los procesos y procedimientos definidos en los otros cuatro cuadrantes, ya que cualquier cambio presentado dentro de la infraestructura administrada debe ser registrada dentro del proceso de administración de Cambios y Configuraciones, este cuadrante puede resultar muy trivial o sencillo, sin embargo entre más compleja sea la infraestructura y los servicios administrados más compleja se vuelve su integración.

Dentro de los principales procesos de ITIL se encuentran:

Service Desk o Mesa de Ayuda.- La cual provee un único punto de contacto entre los clientes o usuarios y la entrega de servicios, los operadores de la Mesa de Ayuda serán los responsables de proporcionar al usuario toda la información, guiarlo y advertirlo acerca de todos los aspectos referentes a la entrega de un servicio; no sólo advertirán al usuario acerca de la interrupción de los servicios, si no también lo aconsejarán sobre servicios brindados por la organización.

Incident Management o Administración de Incidencias.- Este proceso tiene como principal funcionalidad la detección oportuna y su pronta recuperación en caso de la degradación de algún servicio acorde con los acuerdos de niveles de servicio.

Problem Management o Administración de Problemas.- El objetivo de este proceso es disminuir el número de incidencias o problemas detectadas dentro de la infraestructura de TI, las actividades de este proceso son: Control de problemas, control de errores, prevención proactiva de problemas, identificación de tendencias y administración de la información integrada dentro del proceso.

Change Management o Administración de Cambios.- Provee los mecanismos necesarios para la administración y control de todos los posibles cambios a

implantar dentro de la infraestructura de TI, minimizando el impacto de dichos cambios sobre la entrega de servicios

Configuration Management o Administración de Configuraciones.- En este proceso se identifican, controlan y verifican todos los componentes de la infraestructura administrada así como todas sus interrelaciones, el principal objetivo de este proceso es proporcionar información sobre el uso de los componentes de TI.

Service Level Management o Administración de Niveles de Servicio.- Este proceso define las reglas del negocio en cuanto a negociación, contratación, monitoreo, entregables, niveles de servicio, etc.

Cost Management o Administración de Costos.- Se refiere al costeo, operación y mantenimiento de los servicios de TI brindados.

Availability Management o Administración de disponibilidad.- Su función es optimizar la disponibilidad de los servicios de TI.

Capacity Management o Administración de Capacidades.- Se enfoca en el monitoreo y afinación de los recursos de hardware que soportan los servicios de TI para garantizar el cumplimiento de niveles de servicio.

Contingency Planning o Administración de Contingencias.- Provee los medios necesarios para la recuperación del negocio en caso de situaciones de desastre.

Para nuestro caso de estudio nos concentraremos en el cuarto cuadrante "Puente de Operaciones" ya que es en él donde se integran la atención de los requerimientos de la solución de Redes y Sistemas.

Para dar inicio con la implantación del modelo ITSM dentro de una organización, lo primero que hay que hacer es identificar aquellos servicios críticos del negocio, sus procesos asociados, la tecnología que los soporta y la gente que los opera o administra; Una vez identificado el servicio y con el fin de simplificar su administración se plantean acuerdos o niveles de servicio, los cuales son indispensables para poder medir la calidad y satisfacción del cliente o usuarios funcionales.

Posteriormente se identifican los componentes de los cuales dependen los procesos asociados al servicio, tales componentes son normalmente recursos informáticos como sistemas operativos, manejadores de bases de datos, servidores de transacciones, enlaces de comunicaciones, componentes de red, esquemas redundantes, esquemas de alta disponibilidad, esquemas de seguridad, aplicaciones, herramientas de desarrollo, compiladores, etc Ya identificados dichos componentes se clasifican aquellos procesos que de acuerdo al nivel de servicio planteado son críticos para la continuidad del negocio Una vez identificado todos los procesos, sus componentes y los servicios brindados

se procede a integrarlos a través de soluciones tecnológicas que contribuyan a eficientar y simplificar su administración.

Dentro de la industria tecnológica se pueden encontrar diferentes fabricantes de software o plataformas tecnológicas que facilitan dicha integración, su implantación puede llegar a ser tan compleja como complejo sea el ambiente a administrar, sin embargo la intención no es complicar más las actividades de soporte del DBA, del Administrador del Sistema Operativo o el Administrador de la Red, si no todo lo contrario, la intención es apoyarlo con la solución idónea que simplifique sus funciones técnicas, pero sobre todo garantice la continuidad de los servicios de tecnología de la información.

Una vez adoptado el modelo de ITSM como método a seguir para la atención de los requerimientos planteados por la Solución de Monitoreo de Redes y Sistemas, lo primero que hay que hacer es dar inicio con la etapa de planeación y análisis de la solución, para ello y de acuerdo a los requerimientos planteados en el inciso 2, se procede a la elaboración de los diseños e implantación de la solución, los cuales describen detalladamente sus objetivos, alcances, ventajas, beneficios y productos, así como su nivel de integración con los sistemas operativos, las bases de datos, la red de comunicaciones, procesos, etc., de la infraestructura a administrar.

También se detallan los componentes de software, herramientas tecnológicas, configuraciones y los requerimientos técnicos y/o de proceso indispensables para el restablecimiento de la solución en caso de contingencia; Finalmente se llevarán a cabo una serie de recomendaciones a través de políticas y procedimientos operativos los cuales deberán actualizarse conforme evolucione la solución de monitoreo dentro del ambiente operativo de la organización.

Para facilitar la comprensión de la aplicación del método y enfocados sobre el cuarto cuadrante "Puente de Operaciones", el siguiente capítulo se estructuro atendiendo los requerimientos y objetivos planteados por cada una de las disciplinas de administración de la solución de Redes y Sistemas.

5.- Aplicación del Método

5.1.- Base de Datos y Desempeño

5.1.1.- Diseño de Solución

5.1.1.1.- Objetivo General

Integrar una solución de control, administración y monitoreo automatizada que apoye al monitoreo y administración de los equipos de cómputo de las diferentes entidades administrativas del SAT, con la finalidad de optimizar los recursos de cómputo, la disponibilidad y operabilidad de los mismos, al mismo tiempo que se minimiza la interrupción de los servicios brindados.

5.1.1.2.- Objetivos Particulares

- Definición de políticas y procedimientos de administración y monitoreo centralizado de los equipos que soportan las operaciones del SAT.
- Definir las clases de métricas que proporcionen la información más relevante del desempeño y de las bases de datos de los diferentes equipos de producción.
- Determinar los parámetros asociados a las clases de métricas definidas.
- Monitorear todos los nodos de producción que componen la red del SAT.
- Generar información histórica que apoye a la toma adecuada de decisiones en la configuración de los diferentes equipos.
- Integración de la solución en una consola de integración de eventos y con la consola de administración de Incidencias (Mesa de Ayuda).
- Monitoreo centralizado a través de las diferentes consolas de las aplicaciones integradas.
- Prevenir cualquier cambio de estado en el ambiente de producción.
- Atender de manera inmediata y de forma especializada cualquier requerimiento de los equipos de producción.
- Se diseñará, desarrollará e implantará reportes que permitan analizar la utilización de recursos que facilite la planeación y/o prevención para efectos de toma de decisiones, usando las herramientas propias de monitoreo.
- Correlación de eventos involucrados en el sistema para la implantación de la herramienta

5.1.1.3.- Funcionalidad

- Definición de umbrales de operación (condiciones de excepción), establecidos en los recursos de los equipos, identificando estados normales, de advertencia y críticos en la operación de los equipos y sus recursos

- Capacidad de monitoreo de recursos por grupos de procesos, (ejemplo por nombre, usuario, terminal, identificador de proceso, fecha, etc.)
- Notificación automática a las áreas correctivas de las condiciones de excepción que se detecten, por medio de alarmas visuales, audibles o mensajes vía radiolocalizador.
- Facilidad de operar la solución mediante ventanas gráficas que muestren los diversos equipos y recursos monitoreados.
- Acceso a la información histórica de 30 días y en línea.
- Recolección de información histórica del comportamiento de los parámetros monitoreados, dejando archivos locales en los equipos administrados, para disminuir el tráfico en la red, así como la carga de trabajo en los equipos debido a la administración del desempeño.
- Administración centralizada bajo un esquema distribuido.
- Administración y monitoreo a través del uso de agentes que permitan tomar acciones en los clientes Unix o a través de órdenes desde la consola de monitoreo, para corregir en la medida de lo posible las incidencias presentadas.
- Monitoreo a través de diversas consolas de operación que ejecutan tareas predefinidas y/o calendarizadas, configurar de manera particular una consola, nodo, módulo, instancia, aplicación y parámetro según las características o necesidades.
- Contenedores de gráficas con los parámetros más representativos del desempeño y base de datos.
- Acceso de información histórica de 4 meses en una base de datos central.
- Emisión de análisis mensuales del comportamiento y tendencia de todos los nodos, con los parámetros más representativos.

5.1.1.4.- Detalle de la Solución

Para poder llevar a cabo el monitoreo de los diferentes equipos de producción en toda la República se utilizará el producto BMC PATROL v3.6, El producto cuenta con una licencia de administración en la consola central y una licencia de operación para cada uno de los servidores de interés. El software instalado en cada servidor contendrá además de los binarios de patrol, los módulos de conocimientos UNIX e INFORMIX necesarios para el monitoreo del sistema operativo Unix y el manejador de Base de Datos Informix.

Patrol a través de sus diferentes consolas de monitoreo, personalizadas y configuradas de manera individual nos permite tener un amplio panorama del comportamiento de los servidores, cada una de las consolas vigilará de manera continua el comportamiento de los recursos de cómputo las 24 hrs , del día los 365 días del año.

Todos los eventos generados a través de las consolas de patrol, tienen un seguimiento y dependiendo del nivel de criticidad siguen un flujo diferente de solución

Patrol a través de sus archivos históricos nos permite contar con un análisis previo de la tendencia de los equipos, y poder prevenir futuras fallas en cualquiera de los recursos de los sistemas.

Patrol se integra con diversas aplicaciones que nos permitirán conocer de manera exacta y en tiempo real cualquier cambio de estado en los nodos que conforman la red del SAT, cada parámetro vigilado nos permitirá unificar criterios para el seguimiento y solución de los diversos eventos que ocurran.

La consola principal de administración de Patrol integrará una serie de contenedores, dentro de los cuales se agruparán a todos y cada uno de los nodos administrados, dichos contenedores serán agrupados por unidad administrativa, lo cual simplificará los procesos y procedimientos de operación y monitoreo, la representación gráfica de esta consola se muestra en la siguiente figura

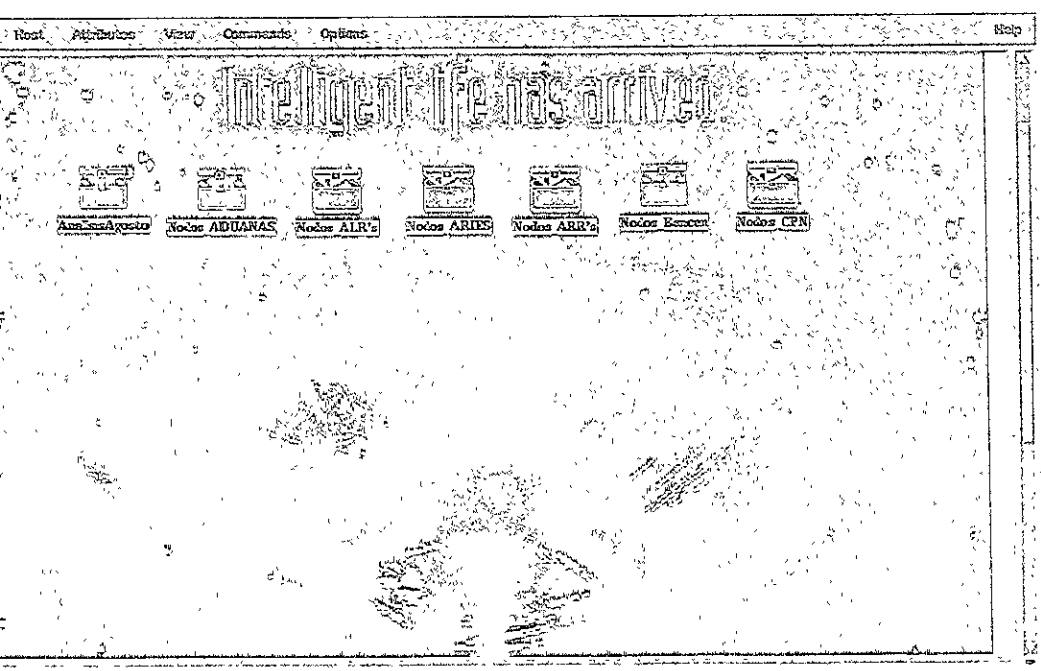


Figura 3 Contenedores Consola de Administración

En la consola de administración (que cuenta con interfaz gráfica), cada uno de los equipos a monitorear será representado mediante un icono de colores. Cada equipo estará identificado por el "alias" (nombre lógico) que se le ha asignado en la red, tal y como se muestra en las siguientes figuras. Éstos alias deben estar presentes en el archivo de configuración del sistema operativo /etc/hosts en el servidor central de monitoreo.

Figura 3. Consola de Administración de Patrol

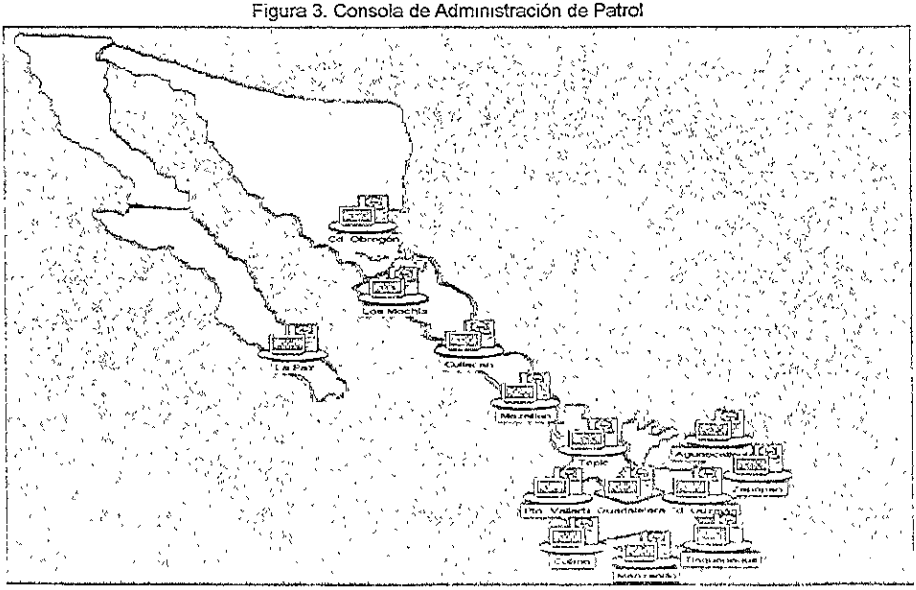


Figura 4. Consola de Administración Region Occidente

Existirán dos ambientes de trabajo para las consolas de operación, éstos contendrán todos los agentes y sólo los módulos de conocimiento correspondientes a Sistema Operativo y Base de datos. La configuración de los agentes será administrada de manera particular o al grupo al que pertenezcan

El agente (proceso) de Patrol con nombre PatrolAgent es instalado en cada uno de los equipos monitoreados, el agente una vez instalado comenzará su tarea de recolectar información, conforme a la calendarización de los colectores, El agente de monitoreo utilizará el módulo de conocimiento de UNIX e INFORMIX, para así conocer el estado de los parámetros de desempeño del equipo Los módulos de conocimiento UNIX e INFORMIX de Patrol a través de la consola de administración provee a los agentes las configuraciones para el monitoreo de los parámetros más representativos del desempeño del equipo: cpu, memoria, discos, red, procesos, bases de datos, instancias, dbspaces, archivos de configuración etc.

Al seleccionar el icono de alguno de los nodos mostrados en la consola aparecerán las diversas aplicaciones, Módulos de Conocimiento (KM) que serán monitoreadas por Patrol. Estas aplicaciones cuya representación gráfica es un icono, son los más relevantes a esta solución: memoria, cpu, disco, procesos, red, etc.

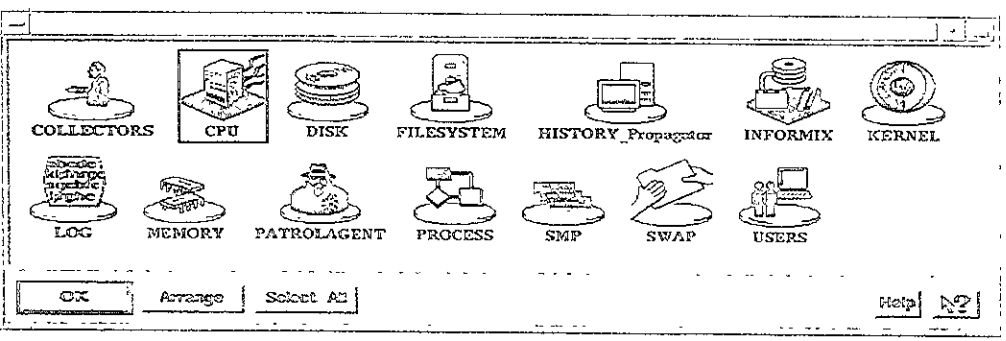


Figura 5 Consola de Módulos de Conocimiento

Al ir profundizando niveles de selección, aparecerán las instancias de esas aplicaciones y sucesivamente, los parámetros de la aplicación respectiva que ése agente de Patrol monitorea. Por último, se desplegará el valor actual del parámetro seleccionado y opcionalmente un histórico gráfico de los valores del parámetro seleccionado en el caso que aplique, de lo contrario la información instantánea que provee dicho parámetro.

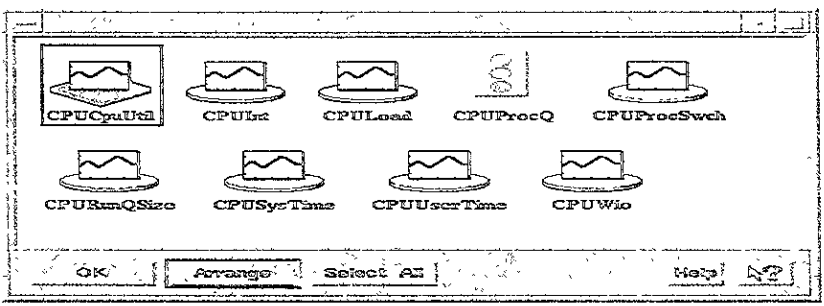


Figura 6 Instancias y aplicaciones Patrol

Los posibles estados en los que se puede encontrar cada parámetro se muestran en la tabla 1.

Estado	Ícono	Valor del parámetro con respecto a los rangos de umbrales
NORMAL	Multicolor	El monitoreo del parámetro indica que éste se encuentra en un estado de operación normal. Se denota por un ícono de colores.
ALERTA.	Rojo	El monitoreo del parámetro indica que éste se encuentra en un estado de alerta y requiere atención Se denota por un ícono en color rojo fijo
ALARMA	Intermitente	El monitoreo del parámetro indica que éste se encuentra en un estado de alarma y requiere atención inmediata. Se denota por un ícono centelleando.

Tabla 1. Posibles estados del valor de un parámetro

Cuando alguno de los parámetros a monitorear rebasa los umbrales definidos para su operación normal, se considerará una condición por excepción (es decir, si pasa del estado *normal* al de *alerta* o al de *alarma*, o bien se pasa del estado de *alerta* al de *alarma*). Cuando se da una condición por excepción, el control de atención será transferido a la consola de eventos y, de ser necesario, la notificación de la condición por excepción será enviada por la consola de eventos

Patrol maneja tres tipos de condiciones de excepción, definidos claramente entre rangos numéricos (cuantitativos):

- El primero es una condición de borde, que define el rango total posible en el que puede cambiar el valor de un parámetro, si el valor de un parámetro sale de ese rango, se levanta la condición de alarma.
- El segundo tipo es la condición de alerta, el rango que se define tiene por objeto que la condición por excepción nos muestre los valores de un comportamiento anormal.
- El tercero es la condición de alarma, los valores que se reflejan dentro de este rango definido son los valores de un comportamiento crítico.

Tanto alertas como alarmas encuentran la definición de sus rangos dentro del rango de BORDE (por ejemplo, de 80 a 90 y de 90 a 100, respectivamente).

Con la finalidad de no sobrecargar los equipos monitoreados, el muestreo de parámetros se llevará de acuerdo a los requerimientos. Para obtener una precisión aceptable acerca del consumo de los recursos de los distintos equipos, el período de muestreo habrá de definirse de tal forma que cubra todo el tiempo en que los servidores estén en operación (generalmente 7x24x365 días).

Una fase de prueba permitirá conocer el rendimiento de los servidores. Con esto, se podrán afinar los umbrales definidos para la operación.

La captura del muestreo que se lleve a cabo será la fuente de información que permitirá conocer el desempeño de cada uno de los equipos. Durante la fase de estabilidad se deberán afinar los umbrales constantemente según vaya siendo necesario, esto ayudará a evitar que se genere información irrelevante de eventos por condiciones de excepción a causa de umbrales mal establecidos.

Cada agente será responsable de mantener sus bitácoras de monitoreo (las cuales quedarán escritas en formato propietario de BMC), para evitar pérdidas de información en caso de que llegase a perderse la comunicación entre consola y agentes. Para observar e incluso obtener estadísticas del comportamiento de los parámetros monitoreados en los distintos equipos, se utilizará la consola central de Patrol. En ella se podrán generar gráficas del desempeño de los distintos parámetros monitoreados, obteniendo gráficos como el que se muestran en las siguientes figuras.

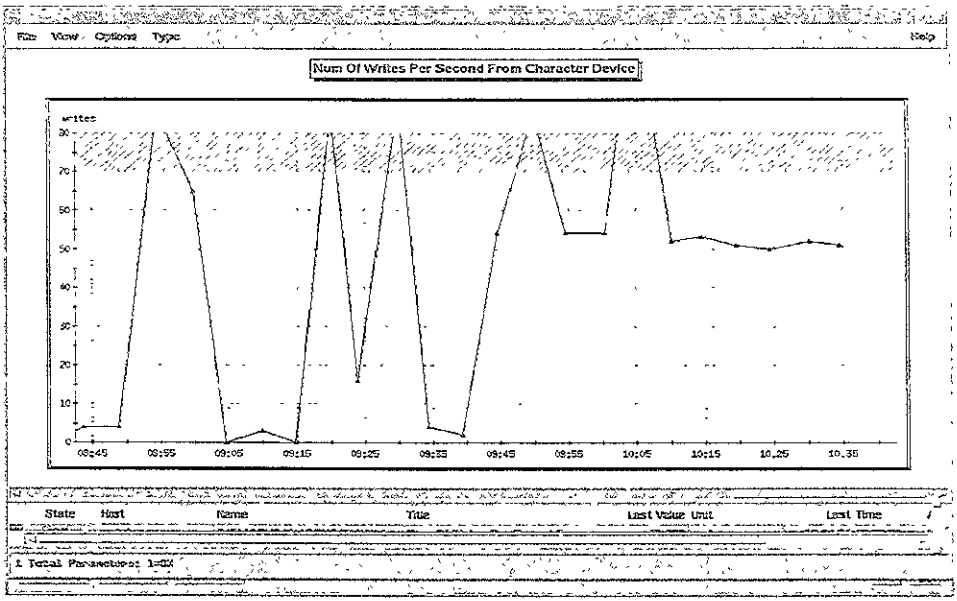


Figura 7. Ejemplo de gráfica generada por la consola de Patrol I

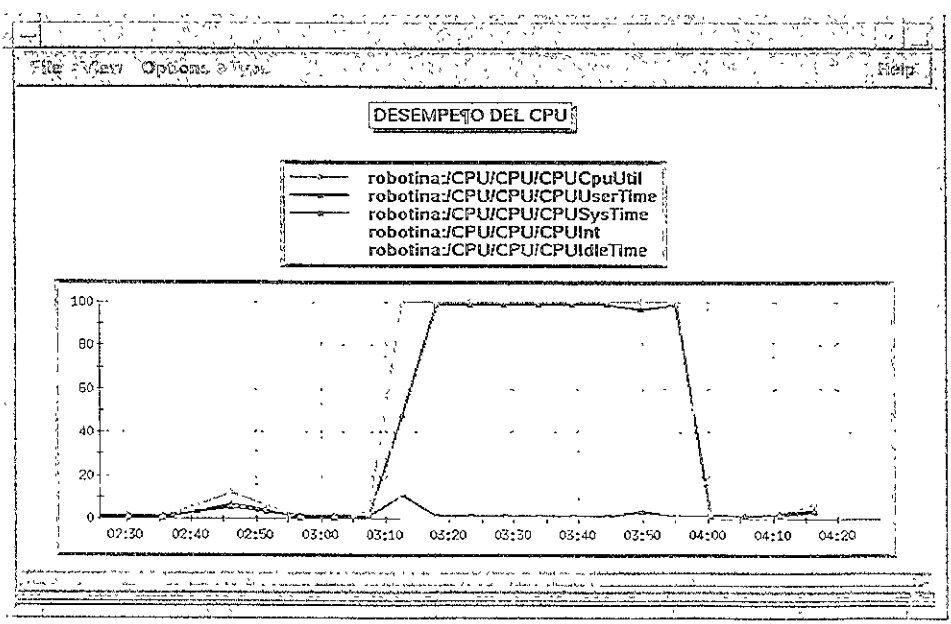


Figura 8 Ejemplo de gráfica generada por la consola de Patrol II

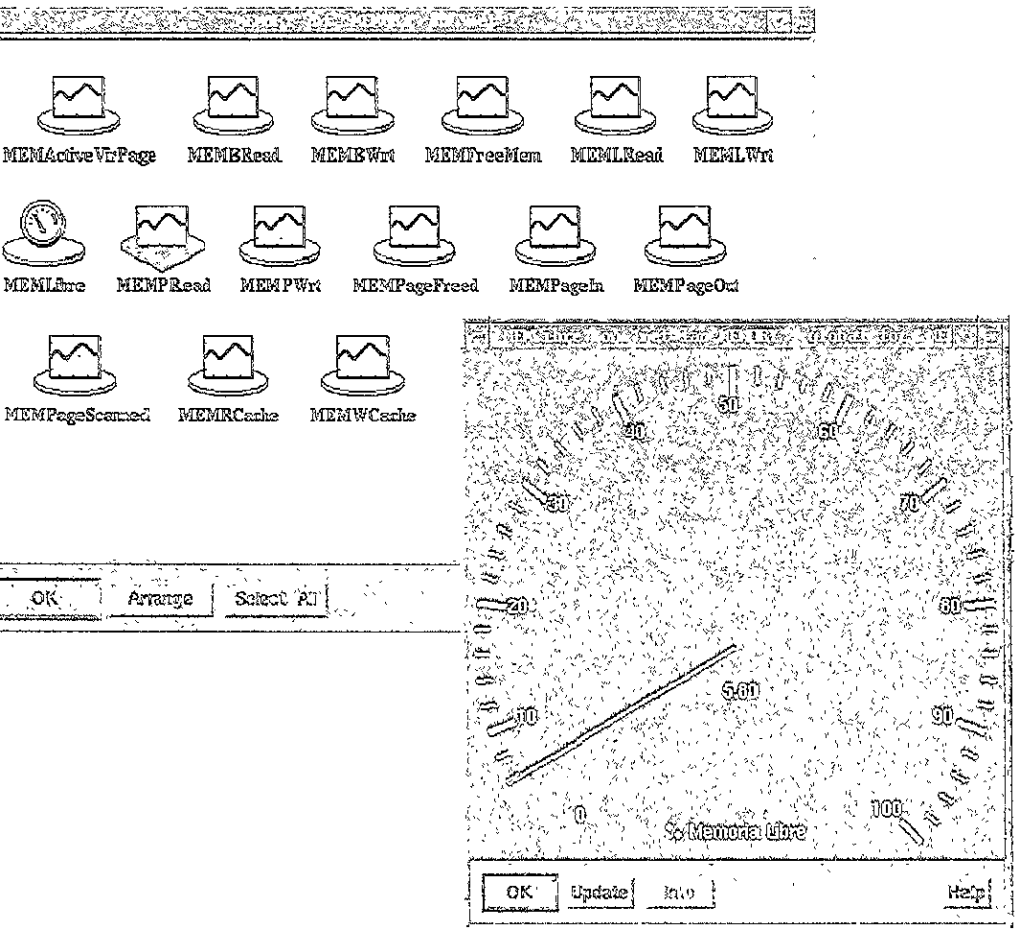


Figura 9 Ejemplo de gráfica generada por la consola de Patrol III

Para poder llevar históricos de la información recolectada será necesaria la configuración del tiempo de colección (history retention). Este periodo será de 30 días de colección esto significa que la bitácora de cada agente contendrá la información referente a los últimos 30 días de actividad del agente.

Esta información histórica será propagada (KM History_Propagator) por cada uno de los agentes al servidor central, cada uno de los agentes es calendarizado cada determinado periodo, establecido a conveniencia de la operación crítica de los servidores.

Sobre la base del análisis y requerimientos de la solución, se notificarán los parámetros más representativos en la operación de un equipo tanto en Sistema Operativo como en Base de Datos.

- Configuración de umbrales.
- Rangos de Warning y Alarm.
- Límite máximo y mínimo de operación.
- Número de ocurrencias.
- Acción de Recuperación.
- Severidad (Minor o Critical).
- Mensaje de notificación.

La configuración se lleva a cabo en la Consola de Administración de Patrol, la siguiente tabla muestra los parámetros que se notificarán y la configuración de umbrales, conforme a los acuerdos de niveles de servicio.

PARÁMETRO	TIPO DE ICONO	TIPO DE SALIDA	UMBRALES					
			WARNING	OCU-RREN-CIAS.	SEVE-RIDAD	ALARMA	OCU-RREN-CIAS.	SEVE-RIDAD
PUCpuUtil	Graf.	%	85-95	3	M	95-100	3	C
PURunQsize	Graf.	N	5-7	3	M	7-10	3	C
SCapacity	Graf.	%	93-97	3	M	97-100	3	C
EMFreeMem	Graf	N	80-90	3	M	90-100	3	C
WPTotSwapUsedPercent	Graf.	N	80-90	3	M	90-100	3	C
hunkDown	Gauge	N	1	1	M	1	1	C
Error	Text.	T	1	1	M	1	1	C
serOverflow	Graf	N	1-2	3	M	3	3	C
BSpaceUsed	Gauge	%	85-90	3	M	3	3	C
fLine						1	1	C

Tabla 2 Configuracion de parámetros

Cada parametro responderá a un cambio de estado (Alarm o Warning) dependiendo del rango en que se encuentren definidos los umbrales, evitando los posibles picos o eventos ocasionales se les definio un número de ocurrencias que nos expondrán si el evento es constante o no, dado que si fuera así y se cumplan en numero de ocurrencias definidas se activara la acción de recuperación o

trigger el cual se encargará de enviar el opcmsg (comando para mandar mensajes a HP OpenView IT/Operations) del nodo que generó el evento. El opcmsg se compone de los siguientes parámetros:

Opcmsg [estado, nodo, aplicación, parámetro, mensaje, grupo_mensaje]

Este mensaje será avanzado a la consola de HP OpenView IT/Operations el cual será desplegado en el browse de la consola de IT/O, el evento está compuesto de 9 parámetros como muestra la tabla 3, se le dará un seguimiento dependiendo de cualquiera de los dos estados de criticidad del evento (Minor o Critical).

Parámetro	Descripción
Sev	Severidad del evento
SUIAONE	Permisos del evento
Date	Fecha del evento
Time	Hora del evento
Node	Nombre del Nodo
Application	Aplicación del Nodo
MsgGroup	Grupo del mensaje
Object	Objeto o parámetro
Message text	Descripción del evento

Tabla 3 Parámetros de un evento en la Consola de IT/O.

Dependiendo de la severidad con la que son generados Minor o Critical cada evento tiene un seguimiento especifico.

Minor (warning o preventivos) estos eventos tendrán un seguimiento a través de las consolas de Patrol e IT/O, el operador mantendrá un monitoreo constante donde se está reportando el evento, hasta observar el cambio de estado en el icono alarmado en la Consola de Patrol.

Critical (Críticos) estos eventos serán avanzados a la consola de Remedy ARS (Action Request System), donde se levantará un ticket de manera automática y de igual manera en forma automática el evento llega al "pager" (Skytel, mensaje de radio) del personal responsable del equipo, el mensaje tiene los siguientes datos:

- Hostname (Nombre del equipo con problemas).
- Parámetro (parámetro de patrol que sufrió el cambio de estado).
- Mensaje (Mensaje descriptivo del problema).

Cuando una incidencia no sea atendida en los primeros 20 minutos el evento registrado en la mesa de ayuda contará con un esquema de escalamiento hasta su atención y corrección

Para que el mensaje tenga salida vía "pager" (Skytel, mensaje de radio), Remedy realiza tres validaciones:

- Valida en el catálogo de grupos que verifica el parámetro MsgGroup del evento.
- Valida en el catálogo de eventos donde checa el Object del evento..
- Valida el grupo que tiene asignado el skytel del personal responsable del equipo.

Los eventos que se notifican a mesa de ayuda tienen un seguimiento a través de las diferentes consolas de monitoreo de cada una de las aplicaciones que forman la integración.

Las consolas de monitoreo nos permiten realizar un seguimiento de manera detallada en tiempo real de cualquier tipo de evento generado, ya que se cuenta con todas las características de éste.

Hay dos tipos de consolas:

- Consolas de Administración
- Consolas de Operación.

Los eventos generados tiene el siguiente flujo de avance a través de las diferentes consolas de monitoreo de la integración figura 10.

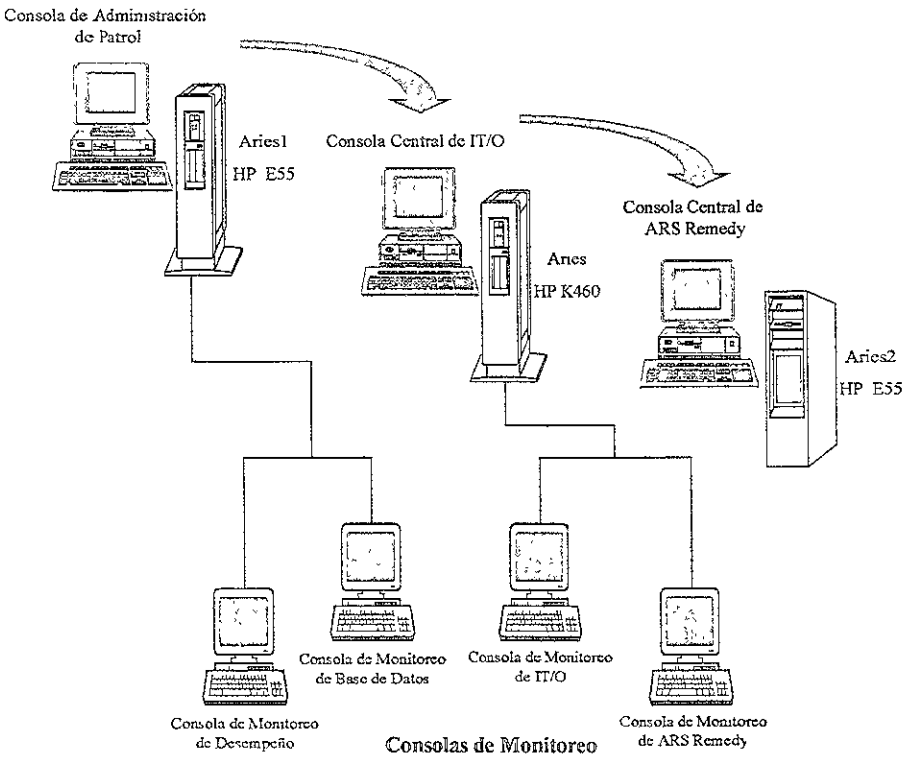


Figura 10 Flujo de Monitoreo

Con la finalidad de explotar la información (Datos y Eventos) referente al rendimiento de los sistemas y bases de datos de los servidores administrados por la solución para la emisión de reportes de comportamiento, toda la información histórica que los agentes de monitoreo (PatrolAgent) recolecten será cargada a una base de datos central RBDMS Oracle ubicada en el servidor central.

Cada uno de los agentes (PatrolAgent) propagará sus respectivos archivos de información hacia la consola central de Administración de Patrol en el servidor central, cada uno de los agentes está calendarizado para realizar la propagación de sus archivos bajo una determinada calendarización, esto con el fin de no impactar en el tráfico de la red

El esquema de transporte de esta información se plasma de manera gráfica en la siguiente figura

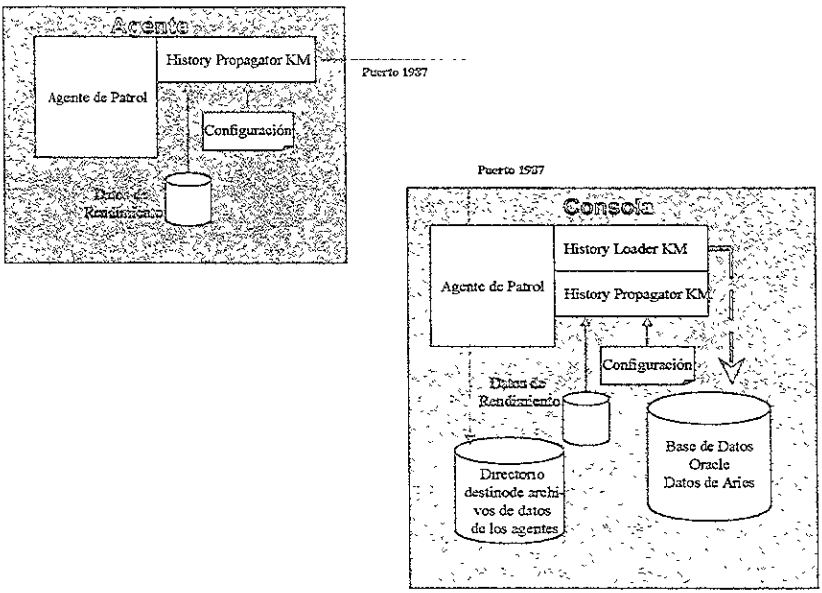


Figura 11. Flujo de transporte agentes – consola – base de datos

Como se puede observar, el envío de la información es realizado entre agentes directamente, de forma que esta información se deposita en un directorio de paso (Directorio destino de archivos de datos de los agentes).

Este envío de información está definido dentro de la configuración del módulo de conocimiento history Propagator. Posteriormente el agente, con el conocimiento que el módulo le agrega, extrae la información de las bitácoras contenidas en este directorio y la deposita en la base de datos de Oracle. Dentro de esta figura se muestra que la comunicación de los agentes se realiza a través de los puertos de comunicaciones 1987.

Es necesario también configurar los módulos de conocimiento para que el envío de la información esté calendarizado y automatizado.

Una vez almacenada la información del rendimiento de los servidores administrados y monitoreados, se puede entonces explotar y obtener datos de interés referentes a su comportamiento.

5.1.2.- Memoria Técnica

5.1.2.1.- Instalación y Configuración de Agentes

La instalación de los agentes de Patrol se lleva a cabo en cada uno de los servidores de producción a través de la red de comunicaciones. Ésta se realiza con los discos originales del software, para facilitar su instalación en cada una de las plataformas operativas (HP e IBM) se desarrollaron algunos programas tanto en PLS "Program Languaje Script" (Lenguaje propietario de Patrol), como en c-shell de Unix y ANSI "C"; referencia apartado 5.1.3

La configuración de los agentes de patrol se realiza desde una consola de administración a nivel central, posteriormente se envían a cada uno de los nodos monitoreados los cambios y configuraciones deseadas; La configuración de los agentes consiste en la adecuación de umbrales, alarmas y tiempos de verificación de valores por parte de los agentes sobre los módulos de conocimiento; Su finalidad es adecuar cada uno de los parámetros de monitoreo a las necesidades propias de cada uno de los ambientes administrados.

5.1.2.2.- Configuración de Módulos de Conocimiento "KM"

La configuración de los agentes involucra las adecuaciones de los módulos de conocimiento que los agentes utilizan para el monitoreo, cada módulo de conocimiento permanece activo de manera local, aún si la consola de monitoreo central pierde la comunicación con el nodo. A continuación muestro una lista de los módulos de conocimiento configurados en la solución.

MÓDULOS DE CONOCIMIENTO
History_Propagator
History_Loader
INFORMIX7
INFORMIX_DBS
INFORMIX_CHK
INFORMIX_FRAG_EXT
Filesystem
CPU
Kernel
Disk
Swap
Log
Process
SMP
PatrolAgent
HP o IBM
Users
Memory

Tabla 4 KM Configurados en la solución

Cada uno de los módulos de conocimiento está compuesto de diferentes parámetros que contienen información referente a cada una de sus aplicaciones. A continuación se muestra la configuración final de los parámetros con valores de umbrales y tiempos de colección de datos.

Parámetro		Tipo	Polling (m)	Umbrales	History
CPU					30 días (Agt)
	CPUCpuUtil	SARColl, VMColl		Border 0-100, Warn 90-95 n=2, Alarm 95-100 n=2	
	CPUIdleTime	SARColl, VMColl		Alarm 0-10 n=2	
	CPUInt	VMColl		No Aplica	
	CPULoad	UPTColl		No Aplica	
	CPUProcSwch	SARColl, VMColl		No Aplica	
	CPURunQSize	SARColl, VMColl		Alarm Border 0-150 n=2	
	CPUSysTime	SARColl, VMColl		Border 0-100, Warn 35-50 n=2, Alarm 50-100 n=2	
	CPUUserTime	SARColl, VMColl		Border 0-100, Warn 90-95 n=2, Alarm 95-100 n=2	
	CPUWGsw	SARColl		No Aplica	
	CPUWPhy	SARColl		No Aplica	
	CPUWSwp	SARColl		Alarm Border 0-500 n=2	
	CPUWtf	SARColl		No Aplica	
	CPUWts	SARColl		No Aplica	
	CPUWio	SARColl		No Aplica	

Parámetro		Tipo	Polling (m)	Umbrales	History
DISK					30 días (Agt)
	DSKAvgQueue	DISK Discovery		No Aplica	
	DSKAvgServ	DISK Discovery		No Aplica	
	DSKAvgWait	DISK Discovery		No Aplica	
	DSKBps	DISK Discovery		No Aplica	
	DSKMsps	DISK Discovery		No Aplica	
	DSKPercentBusy	DISK Discovery		Warn 95-100% n=2	
	DSKRead	DISK Discovery		No Aplica	
	DSKSps	DISK Discovery		No Aplica	
	DSKTps	DISK Discovery		No Aplica	
	DSKWrite	DISK Discovery		No Aplica	

Parámetro		Tipo	Polling (m)	Umbrales	History
FILESYSTEM					30 días (Agt)
	FSAvailableSpace	DF Collector		No Aplica	
	FSCapacity	DF Collector		Border 0-100, Warn 86-98, Alarm 98-100	
	FSFreeInodes	DF Collector		No Aplica	
	FSInodesUsedPercent	DF Collector		No Aplica	
	FSUsedSpace	DF Collector		No Aplica	

Parámetro		Tipo	Polling (m)	Umbrales	History
SWAP					30 días (Agt)
	SWPnPageSizeAvail	SWAP discovery		No Aplica	
	SWPSwapFreeSpace	SWAP discovery		No Aplica	
	SWPSwapSize	SWAP discovery		No Aplica	
	SWPSwapUsedPercent	SWAP discovery		Border 0-100	
	SWPSwapUsedSize	SWAP discovery		No Aplica	
	SWPSwapusedPercent	SWAP discovery		No Aplica	
	SWPTotSwapFreeSpace	SWAP discovery		No Aplica	
	SWPTotSwapSize	SWAP discovery		Alarm Border 0-100	
	SWPTotSwapUsedpercent	SWAP discovery		No Aplica	

Parámetro	Tipo	Polling (m)	Umbrales	History
KERNEL				30 dias (Agt)
KERDirBlk	SAR Collector		No Aplica	
KERFileUsedPercent	SAR Collector		Border 0-100, Warn 90-95, Alarm 95-100	
KERGnodeUsedPercent	SAR or PSTAT Coll		Border 0-100, Warn 90-95, Alarm 95-100	
KERIGet	PSTAT Coll		No Aplica	
KERINodeUsedPercent	SAR or PSTAT Coll		Border 0-100, Warn 90-100	
KERLgAlloc	SAR Collector		No Aplica	
KERLgFail	SAR Collector		No Aplica	
KERLgMem	SAR Collector		No Aplica	
LERLockUsedPercent	SAR Collector		Border 0-100, Warn 90-95,Alarm 95-100	
KERMsg	SAR Collector		No Aplica	
KERNamei	SAR Collector		No Aplica	
KEROvzAlloc	SAR Collector		No Aplica	
KEROvzFail	SAR Collector		No Aplica	
KERProcUsedPercent	SAR or PSTAT Coll		Border 0-100, Warn 90-95,Alarm 95-100	
KERSemOps	SAR Collector		Border 0-100, Warn 90-100 n=2	
KERSmAlloc	SAR Collector		No Aplica	
KERSmFail	SAR Collector		No Aplica	
KERSmMem	SAR Collector		No Aplica	
KERSysCall	SAR or VM Coll		No Aplica	

Parámetro	Tipo	Polling (m)	Umbrales	History
SMP				30 dias (Agt)
SMPContextSwitch	SMPColl		No Aplica	
SMPCrossCalls	SMPColl		No Aplica	
SMPIdlePercent	SMPColl		No Aplica	
SMPInterrupts	SMPColl		No Aplica	
SMPIntThread	SMPColl		No Aplica	
SMPInvContSwitch	SMPColl		No Aplica	
SMPMajorFaults	SMPColl		No Aplica	
SMPMinorFaults	SMPColl		No Aplica	
SMPRunQLen1Min	SMP Discovery		No Aplica	
SMPRunQLen5Min	SMP Discovery		No Aplica	
SMPRunQLen15Min	SMP Discovery		No Aplica	
SMPSpinMutex	SMPColl		No Aplica	
SMPSpinRdWr	SMPColl		No Aplica	
SMPSystemCall	SMPColl		No Aplica	
SMPSystemPrmt	SMPColl		No Aplica	
SMPThMigration	SMPColl		No Aplica	
SMPWaitPercent	SMPColl		No Aplica	
SMPUserPercent	SMPColl		No Aplica	

Parámetro	Tipo	Polling (m)	Umbrales	History
PROCESS				30 dias (Agt)
PROCAvgUsrProc	USRPROCColl		No Aplica	
PROCExec	SAR Coll		No Aplica	
PROCNoZombies	USRPROCColl		Warn 5-20 n=2	
PROCNumProcs	USRPROCColl		No Aplica	
PROCProcWait	VM Coll		No Aplica	
PROCProcWaitInt	PSColl		No Aplica	
PROCProcWaitUmnt	VM Coll		No Aplica	
PROCTopProcs	PSColl		No Aplica	
PROCUserProcs	USRPROCColl		No Aplica	

Parámetro	Tipo	Polling (m)	Umbrales	History
MEMORY				30 días (Agt)
MEMActiveVirPage	VM Collector		No Aplica	
MEMAddTransFault	SAR or VM Coll		No Aplica	
MEMAllocD	SAR Collector		No Aplica	
MEMBFree	SAR Collector		No Aplica	
MEMBRead	SAR Collector		No Aplica	
MEMBReq	SAR Collector		No Aplica	
MEMBWrt	SAR Collector		No Aplica	
MEMBlkPerReq	SAR Collector		No Aplica	
MEMCache	SAR Collector		No Aplica	
MEMCache	SAR Collector		No Aplica	
MEMCow	VM Collector		No Aplica	
MEMCpyW	SAR Collector		No Aplica	
MEMDFill	SAR Collector		No Aplica	
MEMFlush	SAR Collector		No Aplica	
MEMFreeMem	SAR or VmColl		Warn 200-100 n=2, Alarm 100-0 n=2	
MEMHeapMem	SAR Collector		No Aplica	
MEMIdGet	SAR Collector		No Aplica	
MEMIdPrg	SAR Collector		No Aplica	
MEMIdWrp	SAR Collector		No Aplica	
MEMLRead	SAR Collector		No Aplica	
MEMLWrt	SAR Collector		No Aplica	
MEMOverHd	SAR Collector		No Aplica	
MEMPFault	VM Collector		No Aplica	
MEMPRead	VM Collector		No Aplica	
MEMPWrt	SAR or VM Coll		No Aplica	
MEMPageAnticipated	SAR or VM Coll		No Aplica	
MEMPageFreed	SAR or VM Coll		Border 0-100, Warm 0-25 n=2, Alarm 25-100 n=2	
MEMPageIn	SAR Collector		No Aplica	
MEMPageOut	SAR Collector		Border 0-100, Warn 30-50 n=2,Alarm 50-100 n=2	
MEMPageScanned	SAR Collector		No Aplica	
MEMPgFlt	SAR Collector		No Aplica	
MEMPgSwp	SAR Collector		No Aplica	
MEMRCache	SAR Collector		Border 0-100, Alarm 20-10 n=2,Warm 30-20 n=2	
MEMRFault	SAR Collector		No Aplica	
MEMRegionsIn	SAR Collector		No Aplica	
MEMRegionsOut	SAR Collector		No Aplica	
MEMReq	SAR Collector		No Aplica	
MEMStcaf	SAR Collector		No Aplica	
MEMSwpBf	SAR Collector		No Aplica	
MEMSync	SAR Collector		No Aplica	
MEMTFault	SAR Collector		No Aplica	
MEMVmPrg	SAR Collector		No Aplica	
MEMVmWrp	SAR Collector		No Aplica	
MEMWCache	SAR Collector		Border 0-100, Warm 20-40 n=2, Alarm 40-70 n=2	
MEMWire	SAR Collector		No Aplica	
MEMZero	SAR Collector		No Aplica	

Parámetro	Tipo	Polling (m)	Umbrales	History
Informix				30 días (Agt)
SesSeqScans	SesMonitor		Warn 5-9, Alarm 10-100	
SysCpu	TbstatMonitor		No Aplica	
TableOverflow	DBSpaceMonitor		Warn 1-5, Alarm 6-100	
TableScans	TbstatMonitor		No Aplica	
TblDeadLocks	TblMonitor		Warn 5-19, Alarm 20-100	
TblLockWaits	TblMonitor		Warn 10-29, Alarm 30-100	
TblSeqScans	TblMonitor		Warn 20-49, Alarm 50-100	
Transactions	Tbstat_uMonitor		Warn 90-95, Alarm 95-100	
UsedSpace	Tbstat_dMonitor		Warn 80-90, Alarm 90-100	
UserCpu	TbstatMonitor		No Aplica	
UserOverflow	TbstatMonitor		Warn 1-5, Alarm 6-100	
Users	Tbstat_uMonitor		Warn 90-95, Alarm 95-100	
Write	DBSpaceMonitor		No Aplica	
WriteCache	TbstatMonitor		Warn 0-80	

Parámetro	Tipo	Polling (m)	Umbrales	History
Informix				30 dias (Agt)
ActiveLocks	Consumer		Warn 90-95, Alarm 96-100	
ArchiveFailures	ErrorLogMonitor		Alarm 1-100	
ArchiveLevel0	ArchiveMonitor		No Aplica	
ArchiveLevel1	ArchiveMonitor		No Aplica	
ArchiveLevel2	ArchiveMonitor		No Aplica	
BufferOverflow	TbstatMonitor		Warn 5-100	
BufferWaits	TbstatMonitor		Warn 40-60, Alarm 61-100	
CollectorConsole	Standard		No Aplica	
CheckpointTime	ErrorLogMonitor		No Aplica	
CheckpointWaits	TbstatMonitor		Warn 60-100	
ChunkDown	Tbstat_dMonitor		No Aplica	
DBSpacceAllocate	DBSpaceMonitor		Warn 80-89, Alarm 90-100	
DBSpaceUser	DBSpaceMonitor		Warn 80-89, Alarm 90-100	
DeadLock_Timeout	TbstatMonitor		Warn 1-50, Alarm 51-100	
Deadlocks	TbstatMonitor		Warn 10-50, Alarm 51-100	
ErrAlarm_1	ErrorLogMonitor		Alarm 1-100	
ErrAlarm_2	ErrorLogMonitor		Warn 1-10, Alarm 10-100	
ErrAlarm_3	ErrorLogMonitor		Warn 10-100	
FgWrites	Tbstat_FMonitor		Warn 1-5, Alarm 6-100	
FullestChunk	Tbstat_dMonitor		Warn 70-89, Alarm 90-100	
FullestDbs	Tbstat_dMonitor		Warn 80-90, Alarm 90-100	
IOError	ErrorLogMonitor		Alarm 1-100	
IOQueue	Standard		Alarm 30-100	
LatchWaits	TbstatMonitor		Warn 10-50, Alarm 50-100	
LockOverflow	TbstatMonitor		Warn 5-25, Alarm 25-100	
LockWaits	TbstatMonitor		Warn 10-20, Alarm 20-100	
LogicalLogBufSize	Tbstat_IMonitor		Warn 40-60, Alarm 1-39	
LogSpace	Standard		Alarm 80-100	
LongTrans	Tbstat_uMonitor		Warn 1-100	
Pageread	DBSpaceMonitor		No Aplica	
Pagewrite	DBSpaceMonitor		No Aplica	
PhysicalLogBufSize	Tbstat_IMonitor		Warn 40-60, Alarm 1-39	
PhysicalLogSize	Tbstat_IMonitor		Warn 1-39	
PhysicalLogUsed	Tbstat_IMonitor		No Aplica	
Read	DBSpaceMonitor		No Aplica	
ReadAhead	TbstatMonitor		Warn 1-84	
ReadCache	TbstatMonitor		Warn 0-90	
ReadyQueue	Standard		Warn 10-100	
SesDeadlocks	SesMonitor		Border 1-100, Warn 6-14, Alarm 15-100	
SesDeletes	SesMonitor		Border 0-100, Warn 50-99	
SesHeldResources	SesMonitor		Warn 6-9, Alarm 10-100	
SesLocksHeld	SesMonitor		Warn 50-99, Alarm 0-100	
SesLongTxs	SesMonitor		Warn 2-4, Alarm 5-100	

Tabla 5 Detalle de configuración de parámetros Patrol

5.1.2.3.- KM History_Propagator e History Loader

Éstos módulos de conocimiento se tratan por separado debido a que su función no es colectar información de algún parámetro referente al rendimiento del sistema o a la base de datos. La función del *KM History Propagator* es la de extraer la información histórica de las bitácoras de los parámetros colectados por el agente y transportarla al servidor central a través de una comunicación agente con agente. A continuación se muestran las características del calendario para que se realice la propagación de datos

- Horario único por nodo.
- Intervalo de 10 min. de diferencia por nodo, evitar saturar la red.
- Seis propagaciones durante el día en intervalos de cuatro hrs., por nodo.
- Propagaciones las 24 hrs. del día los 365 días del año por nodo.
- Usuario y password en la configuración del módulo.
- Directorio destino donde se depositan los archivos de propagación.

Todos los archivos recibidos, son colocados temporalmente hasta que el módulo history_loader los almacena en oracle, dentro del directorio remote, ubicado en:

/var/opt/ARIES/patrol/remote

La configuración del *KM History Loader* muestra todo lo relacionado con el almacenamiento de datos en oracle, dentro del servidor Central. Este módulo se encarga de almacenar la información enviada por los agentes. A continuación se muestran los datos de su configuración:

TableSpace	PATROL
Oracle User	Patrol_ora
ORACLE_HOME	/u01/home/oracle/product/8.0.5
ORACLE_SID	Openview

Tabla 6. Configuración KM History Loader

Las alarmas de los parámetros del módulo de conocimiento history_loader, nos permiten tener un mejor control sobre el almacenamiento de archivos en oracle. A continuación se muestra la configuración final, en la que también se puede obtener el calendario de almacenamiento de datos en Oracle.

Parámetro		Tipo	Polling (m)	Umbrales	History
ORACLE_History_Loader					30 días (Agt)
	FilesWaiting	Consumer	15 min	No Aplica	
	LoadHistoryData	Standard	Sábado, 2 00 am	No Aplica	
	LoaderErrors	Consumer	15 min	Border 0-100, Warn 1-3 , Alarm 4-100	
	LoaderStats	Collector	15 min	No Aplica	
	ServerFileSpaceUsed	Consumer	15 min	Border 1-100	

Tabla 7 Detalle alarmas History Loader

5.1.2.4.- Configuración de Colectores

La configuración de los colectores define el tiempo programado de colección de datos para que el agente extraiga información de los parámetros y recursos del sistema operativo y las bases de datos. Es importante definir la colección de datos suficiente para analizar la información, pero también moderada para no incrementar la carga del agente en el sistema, así que de esto depende en gran medida el rendimiento del agente en el servidor.

A continuación se muestra la configuración de los colectores

Colectores de INFORMIX	
Nombre	Tiempo de poleo
ArchiveMonitor	12 hrs
DBSpaceMonitor	11 min
ErrorLogMonitor	2.75 min
DataDistribution	8.25 min
SesMonitor	2.75 min
TabExtents	2.75 min
Tables	13.5 min
TblMonitor	2.75 min
TbsMonitor	14.5 min
TbstatMonitor	14.5 min
Tbstat_fMonitor	13 min
Tbstat_dMonitor	2.75 min
Tbstat_lMonitor	2.75 min
Tbstat_uMonitor	2.5 min

Colectores de UNIX	
Nombre	Tiempo de poleo
DFColl	5 min
NETColl	10 min
NFSColl	5 min
PSColl	7 min
PSTATColl	5 min
PrinterColl	5 min
SARColl	7 min
SMPColl	12 min
UTPColl	4.5 min
USRPROCColl	10 min
VMColl	1.75 min

Tabla 8. Configuración de Colectores

5.1.2.5.- Configuración de Tablespace para Información Histórica

Para almacenar la información de históricos de patrol, es necesario crear un tablespace en una base de datos. En los siguientes puntos se describen sus características y dimensionamiento.

Módulo de Conocimiento	Ubicación Física
History_Propagator	Agentes y Agente de consola Central
History_Loader	Consola Central

Tabla 9. Ubicación Tablespace de Patrol

Para el dimensionamiento del tablespace involucrado en el almacenamiento de los datos históricos, es necesario considerar diferentes datos referentes a los agentes y los parámetros monitoreados. A continuación se muestran los datos involucrados y los resultados del cálculo

Numero total de datos por agente, que correlacionan el numero total de renglones para la tabla p_history_data	168480
Número de Datos por muestreo a un nodo cada 360	351
Numero de Nodes en la solución	145
Numero de aplicaciones/nodo	18
Número de distintos parámetos por nodo	119
Número de bytes por rencion en la base de datos	129
Numero distinto de combinación de aplicación/instancia	85

Tabla	Número de Renglones	Descripcion
p_apps	2610	La multiplicación del numero de aplicaciones/nodo por el numero de nodos.
p_history	12325	Número de nodos por el numero distinto de combinaciones de aplicacion/instancia
p_history_data	24429600	Numero de nodos por el número total de datos por agente
p_instances	85	Número distinto de instancias
p_nodes	145	Número de nodos en la solución
p_parameters	119	Número de distintos parámetros por nodos

ALMACENAMIENTO PERMANENTE

Nombre de Objeto	Tipo de objeto	Bytes
P_APPS	tabla	326250
P_HISTORY_DATA	tabla	3053700000
P_INSTANCES	tabla	10625
P_NODES	tabla	18125
P_PARAMETERS	tabla	14875
P_HISTORY_ERROR	tabla	
P_HISTORY_TEMP	tabla	
P_HISTORY_TEMP	tabla	
Almacenamiento total para objetos permanentes		3056610500

ALMACENAMIENTO TEMPORAL

Nombre de Objeto	Tipo de objeto	Bytes
P_TMP_HISTORY_DATA	tabla	520000

ALMACENAMIENTO TOTAL

Nombre de Objeto	Tipo de objeto	Bytes
Espacio total para objetos permanentes		3056610500
Espacio total para objetos temporales		520000

Tabla 10 Dimensionamiento Tablespace Patrol

Las características del Tablespace de Oracle para el almacenamiento de los datos es el siguiente:

Atributo	Nombre	Características
Usuario de Oracle	Patrol_ora	Un tablespace por default en el que tenga capacidad de creación de índices, tablas y usuarios
TableSpace	Patrol	El espacio definido de 3Gbytes
Variable de Identificación de home	ORACLE_HOME	/u01/home/oracle/product/8 0 5
Variable de identificación de configuración	ORACLE_SID	Openview

Tabla 11. Características Tablespace Patrol

5.1.2.6.- Configuración de la Consola

La configuración de la consola define los nodos, tipos de mensajes y el tipo de integración que se tendrá. En éste caso la configuración de la consola se muestra a continuación

Configuración por nodo

Nombre de usuario	User name	Nombre del usuario para conexión con el agente (patrol)
Puerto de conexión	Number Port	Número de puerto de conexión con el agente (1987)
Tipo de mensajes	Message	Tipo de mensajes que llegan del agente (W,A)
Nombre del node	Node Name	Nombre del nodo agente
Contraseña	Password	Contraseña del usuario para al agente

Tabla 12. Configuración de Consola por nodo

Configuración para todos los nodos

Heartbeat	90	Latencia del nodo
Retries	5	Reintentos de conexión
Reconnect Interval	600	Intervalo de reconexión en segundos
Server Port	5000	No. De puerto de PatrolView
Local Port	0	Puerto local de PatrolView
Comm_SaveTime	0	
Frameworw	HP OpenView IT/Operations Integration	Nombre de la plataforma a integrarse
Message_output	Logfile	Tipo de salida de los mensajes de PatrolView
Message_level	WARN	Tipo de característica de los mensajes de salida de PatrolView
Connection_mode	UDP	Tipo de conexión entre los agente y el server
Acl	Patrol/*/*	Usuario para conexión con el servidor

Tabla 13 Configuración de Consola para todos los nodos

5.1.2.7.- Configuración de Eventos

Para garantizar la continuidad del monitoreo de patrol, son de suma importancia dos eventos que se generan internamente en patrol. A cada uno de estos eventos se les configuró una acción automática, y a continuación se muestra el evento, una breve explicación y el comando que se inicia al generarse dicho evento para cada nodo.

Estado de VOID	Este estado es causado cuando la consola de Patrol pierde comunicación con el agente de Patrol	/opt/patrol/PATROL3 2/prgs/notifi ca sh %{CON_INFO}
Estado de Offline	Este estado es causado cuando el nodo no esta sincronizado con la consola de Patrol	/opt/patrol/PATROL3 2/prgs/notifi ca sh %{CON_INFO}

Tabla 14 Configuración de eventos

Las acciones automáticas que se mencionan en la tabla anterior son llamados a shell pasando como parámetro el nombre del agente (%{CON_INFO}) que tiene el estado indicado (VOID u OK) Se utilizan tres shell para estas acciones

Cuando el estado es VOID, se inicia el shell notifica.sh, que se encarga de verificar si la comunicación con el agente está disponible, así como de iniciar un shell remoto en el servidor con problemas. A continuación se muestra el diagrama de flujo:

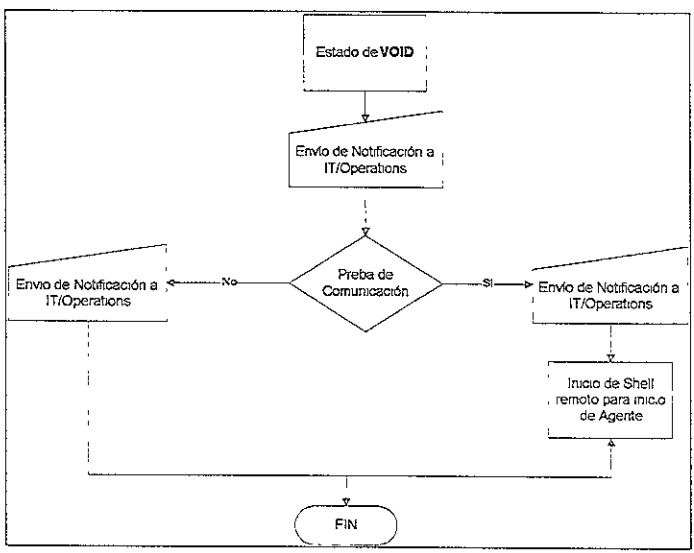


Figura 12 Diagrama de flujo de eventos Patrol

5.1.2.8.- Configuración de Notificaciones

La siguiente tabla muestra la configuración final de eventos de notificación preventiva configurados a través de las consolas de administración de Patrol; Dichos eventos de notificación se integran a la consola de administración de eventos del IT/Operation, quien a su vez se encarga de insertarlos en los tablespaces Oracle definidos para la disciplina de Bases de Datos y Desempeño; Así mismo el IT/Operation los avanza a los esquemas de administración de problemas de la Mesa de Ayuda del SAT, para que a través de ésta se lleve a cabo el seguimiento adecuado de solución a través de las áreas técnicas resolutoras.

Evento	Problema	Nivel 1	Nivel 2	Severidad
kmu_201_cpu_util	DESEMPEÑO	CPU	El nivel de utilización de CPU es alto	Advert.
kmu_202_cpu_util	DESEMPEÑO	CPU	El nivel de utilización de CPU es muy alto	Crítica
kmu_203_idle_time	DESEMPEÑO	CPU	El tiempo de ociosidad del CPU es alto	Advert
kmu_205_run_qsize	DESEMPEÑO	CPU	Hay varios procesos en la COLA de EJECUCIÓN	Advert
kmu_206_run_qsize	DESEMPEÑO	CPU	Hay demasiados procesos en la COLA de EJECUCIÓN	Crítica
kmu_207_sys_time	DESEMPEÑO	CPU	El CPU ha ejecutado muchas llamadas al sistema	Advert
kmu_208_sys_time	DESEMPEÑO	CPU	El CPU ha ejecutado demasiadas llamadas al sistema	Crítica
kmu_209_user_time	DESEMPEÑO	CPU	El CPU ha ejecutado muchas tareas de usuario	Advert
kmu_210_user_time	DESEMPEÑO	CPU	El CPU ha ejecutado demasiadas tareas de usuario	Crítica
kmu_211_swp	DESEMPEÑO	CPU	El CPU ha ejecutado muchas operaciones de salida y salida	Advert

kmu_212_swp	DESEMPEÑO	CPU	El CPU ha ejecutado demasiadas operaciones de entrada y salida	Crítica
kmu_300_avg_queue	DESEMPEÑO	DISCO	Hay muchas peticiones de DISCO de Entrada/salida en cola esperando	Advert.
kmu_301_avg_queue	DESEMPEÑO	DISCO	Hay demasiadas peticiones de DISCO de Entrada/salida en cola esperando	Crítica
kmu_302_read	DESEMPEÑO	DISCO	Se están ejecutando muchas operaciones de lectura a DISCO	Advert.
kmu_303_read	DESEMPEÑO	DISCO	Se están ejecutando demasiadas operaciones de lectura a DISCO	Crítica
kmu_304_write	DESEMPEÑO	DISCO	Las operaciones de escritura a DISCO están ocupando mucho espacio	Advert
kmu_305_write	DESEMPEÑO	DISCO	Las operaciones de escritura a DISCO están ocupando demasiado espacio	Crítica
kmu_340_capacity	DESEMPEÑO	FILE SYSTEM	El porcentaje de espacio libre en el FILESYSTEM es muy bajo	Advert.
kmu_341_capacity	DESEMPEÑO	FILE SYSTEM	El porcentaje de espacio libre en el FILESYSTEM es demasiado bajo	Crítica
kmu_342_free_inodes	DESEMPEÑO	FILE SYSTEM	El número de I-nodos libres en e FILESYSTEM es muy alto	Advert
kmu_344_inode_used_percent	DESEMPEÑO	FILE SYSTEM	El número de I-nodos libres en e FILESYSTEM es muy alto	Advert
kmu_408_sem_ops	DESEMPEÑO	KERNEL	El número de SEMÁFOROS operando es muy elevado	Advert.
kmu_409_sem_ops	DESEMPEÑO	KERNEL	El número de SEMAFOROS operando es demasiado elevado	Crítica
kmu_410_sys_call	DESEMPEÑO	KERNEL	El número de LLAMADAS al SISTEMA (lectura, escritura, bifurcaciones, ..etc) es muy grande	Advert
kmu_411_sys_call	DESEMPEÑO	KERNEL	El número de LLAMADAS al SISTEMA (lectura, escritura, bifurcaciones, ..etc) es demasiado grande	Crítica
kmu_500_active_virpage	DESEMPEÑO	MEMORIA	El número de páginas VIRTUALES ACTIVAS es muy grande	Advert.
kmu_501_active_virpage	DESEMPEÑO	MEMORIA	El número de páginas VIRTUALES ACTIVAS es demasiado grande	Crítica
kmu_502_bread	DESEMPEÑO	MEMORIA	Se realizan muchos procesos de LECTURA de disco a buffer cache	Advert.
kmu_503_bread	DESEMPEÑO	MEMORIA	Se realizan demasiados procesos de LECTURA de disco a buffer cache	Crítica
kmu_504_req	DESEMPEÑO	MEMORIA	La cantidad de MEMORIA requenda es elevada	Advert.
kmu_505_req	DESEMPEÑO	MEMORIA	La cantidad de MEMORIA requenda es demasiada.	Crítica
kmu_506_wrt	DESEMPEÑO	MEMORIA	El número de PROCESOS de ESCRITURA de cache a disco es grande	Advert.
kmu_507_wrt	DESEMPEÑO	MEMORIA	El número de PROCESOS de ESCRITURA de cache a disco es muy grande.	Crítica
kmu_508_free_mem	DESEMPEÑO	MEMORIA	La cantidad de MEMORIA en páginas de 1-KB disponible es insuficiente	Advert.
kmu_509_free_mem	DESEMPEÑO	MEMORIA	La cantidad de MEMORIA en páginas de 1-KB disponible está casi agotada.	Crítica
kmu_512_page_in	DESEMPEÑO	MEMORIA	La cantidad de páginas de SWAP en memoria secundaria es elevada	Advert.
kmu_851_no_session	DESEMPEÑO	USUARIOS	El número de SESIONES con usuario no root es muy elevado.	Crítica
kmu_852_no_user	DESEMPEÑO	USUARIOS	El número de USUARIOS conectados actualmente es elevado	Advert
kmu_853_no_user	DESEMPEÑO	USUARIOS	El número de USUARIOS conectados actualmente es muy elevado.	Crítica
kmi_900_chunk_down	B D	INFORMIX	El número de CHUNKS dados de baja en la instancia es elevado.	Advert.
kmi_901_chunk_down	B D	INFORMIX	El número de CHUNKS dados de baja en la instancia es muy elevado	Crítica
Kmi_902_io_error	B D	INFORMIX	El número de ERRORES de Entrada/Salida es elevado	Advert
Kmi_903_io_error	B D	INFORMIX	El numero de ERRORES de Entrada/Salida es muy elevado	Crítica
Kmi_904_user_over_flow	B D	INFORMIX	El número de USUARIOS configurados para la instancia es alto	Advert
Kmi_905_user_over_flow	B D	INFORMIX	El numero de USUARIOS configurados para la instancia es muy alto	Crítica
Kmi_906_chunk_low_S	B D	INFORMIX	El numero de espacios en disco del chunk es bajo	Advert

			(RESPALDO-1) que se realizó es grande.	
Kmi_907_archive_level0	B D	INFORMIX	El número de días transcurridos del último respaldo (RESPALDO-1) que se realizó es muy grande.	Crítica
Kmi_908_archive_level1	B D.	INFORMIX	El número de días transcurridos del último respaldo (RESPALDO-2) que se realizó es muy grande.	Crítica
Kmi_910_archive_level2	B D.	INFORMIX	El número de días transcurridos del último respaldo (RESPALDO-3) que se realizó es muy grande	Advert.
Kmi_914_archive_failures	B. D.	INFORMIX	El número de ARCHIVOS CANCELADOS es alto	Advert.
Kmi_915_archive_failures	B. D	INFORMIX	El número de ARCHIVOS CANCELADOS es muy alto	Crítica
Kmi_920_tbl_seq_scans	B. D.	INFORMIX	El número de tablas con NÚMERO SECUENCIAL de búsqueda errónea es alto.	Advert.
Kmi_921_tbl_seq_scans	B. D.	INFORMIX	El número de tablas con NÚMERO SECUENCIAL de búsqueda errónea es demasiado alto	Crítica
Kmi_922_acive_locks	B D.	INFORMIX	El porcentaje de LOCKS activos es alto en la instancia actual.	Advert
Kmi_923_acive_locks	B D	INFORMIX	El porcentaje de LOCKS activos es demasiado alto en la instancia actual.	Crítica
Kmi_924_buffer_overflow	B. D.	INFORMIX	El NÚMERO de VECES que se excede el buffer de la memoria compartida es muy elevado.	Advert.
Kmi_925_buffer_overflow	B D.	INFORMIX	El NÚMERO de VECES que se excede el buffer de la memoria compartida es demasiado elevado.	Crítica
Kmi_926_buffer_waits	B. D.	INFORMIX	El número de veces que el usuario tiene que ESPERAR BUFFER es muy elevado	Advert.
Kmi_927_buffer_waits	B D.	INFORMIX	El número de veces que el usuario tiene que ESPERAR BUFFER es demasiado elevado.	Crítica
Kmi_928_dbspace_allocate	B. D	INFORMIX	El porcentaje de ESPACIO ASIGNADO para un chunk en el dbspace es muy elevado.	Advert
Kmi_929_dbspace_allocate	B D.	INFORMIX	El porcentaje de ESPACIO ASIGNADO para un chunk en el dbspace es demasiado elevado.	Crítica
Kmi_930_dbspace_used	B. D	INFORMIX	El porcentaje de ESPACIO que ocupa el chunk es muy elevado.	Advert
Kmi_931_dbspace_used	B. D.	INFORMIX	El porcentaje de ESPACIO que ocupa el chunk es demasiado elevado.	Crítica
Kmi_932_dead_locks	B. D	INFORMIX	El número de DEADLOCKS que fueron detectados y prevenidos es elevado	Advert.
Kmi_933_dead_locks	B D.	INFORMIX	El número de DEADLOCKS que fueron detectados y prevenidos es muy elevado	Crítica
Kmi_934_lock_overflow	B. D	INFORMIX	El número de veces que un proceso intenta tomar un LOCK ASIGNADO es muy alto.	Advert.
Kmi_935_lock_overflow	B D	INFORMIX	El número de veces que un proceso intenta tomar un LOCK ASIGNADO es demasiado alto.	Crítica
Kmi_936_locks_waits	B. D	INFORMIX	El número de veces que el usuario tiene que esperar un LOCK LIBRE es muy alto	Advert.
Kmi_937_locks_waits	B D	INFORMIX	El número de veces que el usuario tiene que esperar un LOCK LIBRE es demasiado alto	Crítica
Kmi_938_sys_cpu	B D	INFORMIX	El tiempo de CPU del sistema para todos los usuarios es muy elevado	Advert
Kmi_939_sys_cpu	B D	INFORMIX	El tiempo de CPU del sistema para todos los usuarios es demasiado elevado.	Crítica
Kmi_940_table_overflow	B D	INFORMIX	El número de PETICIONES que exceden el numero de tablas activas para esta instancia es muy elevado	Advert
Kmi_941_table_overflow	B D	INFORMIX	El número de PETICIONES que exceden el número de tablas activas para esta instancia es demasiado elevado	Crítica
Kmi_942_user_cpu	B. D	INFORMIX	El tiempo de CPU para todos los usuarios es elevado.	Advert
Kmi_943_user_cpu	B D	INFORMIX	El tiempo de CPU para todos los usuarios es muy elevado	Crítica
Kmi_948_long_trans	B D	INFORMIX	El número de TRAMITES IDENTIFICADOS en la instancia es muy elevado	Advert
Kmi_950_transactions	B. D	INFORMIX	El porcentaje de trámites identificados en la instancia es muy alto	Advert
Kmi_951_transactions	B D	INFORMIX	El porcentaje de trámites identificados en la instancia es demasiado alto	Crítica
Kmi_952_user	B D	INFORMIX	El porcentaje de usuarios para la instancia es muy alto	Advert
Kmi_953_user	B D	INFORMIX	El porcentaje de usuarios para la instancia es	Crítica

			demasiado alto.	
Kmi_954_io_queue	B D.	INFORMIX	El máximo de encolamiento para procesos de informix Entrada/Salida es alto.	Advert.
Kmi_955_io_queue	B. D.	INFORMIX	El máximo de encolamiento para procesos de informix Entrada/Salida es muy alto.	Crítica
Kmi_956_log_space	B. D	INFORMIX	El porcentaje de espacio lógico disponible es alto	Advert.
Kmi_957_log_space	B D	INFORMIX	El porcentaje de espacio lógico disponible es muy alto	Crítica
kmu_513_page_in	DESEMPEÑO	MEMORIA	La cantidad de páginas de SWAP en memoria secundaria es muy elevada	Crítica
kmu_514_page_out	DESEMPEÑO	MEMORIA	La cantidad de páginas transfendas de RAM a SWAP es elevada	Advert.
kmu_515_page_out	DESEMPEÑO	MEMORIA	La cantidad de páginas transferidas de RAM a SWAP es muy elevada	Crítica
kmu_516_pread	DESEMPEÑO	MEMORIA	La cantidad de LECTURAS de DISPOSITIVO es elevada.	Advert
kmu_517_pread	DESEMPEÑO	MEMORIA	La cantidad de LECTURAS de DISPOSITIVO es muy elevada	Crítica
kmu_518_pwrt	DESEMPEÑO	MEMORIA	La cantidad de ESCRITURA a DISPOSITIVO es elevada.	Advert.
kmu_519_pwrt	DESEMPEÑO	MEMORIA	La cantidad de ESCRITURA a DISPOSITIVO es muy elevada.	Crítica
kmu_520_rcache	DESEMPEÑO	MEMORIA	El porcentaje de LECTURAS LÓGICAS de cache es elevada	Advert
kmu_521_rcache	DESEMPEÑO	MEMORIA	El porcentaje de LECTURAS LÓGICAS de cache es muy elevada	Crítica
kmu_600_no_zombies	DESEMPEÑO	PROCESOS	Existen muchos procesos ZOMBIE en el sistema	Advert.
kmu_601_no_zombies	DESEMPEÑO	PROCESOS	Existen demasiados procesos ZOMBIE en el sistema	Crítica
kmu_602_num_procs	DESEMPEÑO	PROCESOS	La cantidad de PROCESOS por USUARIO es alta	Advert
kmu_603_num_procs	DESEMPEÑO	PROCESOS	La cantidad de PROCESOS por USUARIO es muy alta	Crítica
kmu_604_proc_wait	DESEMPEÑO	PROCESOS	La COLA de PROCESOS en espera de recursos es muy larga	Advert.
kmu_605_proc_wait	DESEMPEÑO	PROCESOS	La COLA de PROCESOS en espera de recursos es demasiado larga	Crítica
kmu_606_top_procs	DESEMPEÑO	PROCESOS	El porcentaje de utilizacion de CPU de los procesos es muy alto	Advert
kmu_607_top_procs	DESEMPEÑO	PROCESOS	El porcentaje de utilizacion de CPU de los procesos es muy alto	Crítica
kmu_608_user_procs	DESEMPEÑO	PROCESOS	El número de PROCESOS que no son usuario root es muy elevado.	Advert
kmu_609_user_procs	DESEMPEÑO	PROCESOS	El número de PROCESOS que no son usuario root es demasiado elevado	Crítica
kmu_702_run_qlen_15min	DESEMPEÑO	SMP	El número de PROCESOS que no son usuario root es elevado.	Advert
Kmu_703_run_qlen_15min	DESEMPEÑO	SMP	El número de PROCESOS que no son usuario root es demasiado elevado	Crítica
Kmu_800_swap_free_space	DESEMPEÑO	SWAP	El espacio libre de SWAP esta casi agotado	Advert
Kmu_801_swap_free_space	DESEMPEÑO	SWAP	El espacio libre de SWAP esta casi totalmente agotado	Crítica
Kmu_802_swap_size	DESEMPEÑO	SWAP	El espacio total de SWAP esta casi agotado	Advert
Kmu_803_swap_size	DESEMPEÑO	SWAP	El espacio total de SWAP esta casi totalmente agotado	Crítica
Kmu_804_swap_used_percent	DESEMPEÑO	SWAP	EL porcentaje de SWAP ocupado es elevado	Advert.
Kmu_805_swap_used_percent	DESEMPEÑO	SWAP	EL porcentaje de SWAP ocupado es muy elevado	Crítica
Kmu_850_no_session	DESEMPEÑO	USUARIOS	El numero de SESIONES con usuario no root es elevado	Advert

Tabla 15 Notificación de Eventos

5.1.3.- Programas de Configuración

Al contar con dos diferentes plataformas, fue necesario crear dos paquetes de instalación del software de Patrol. En éste caso fue IBM y HP. A continuación se muestran cada uno de los shell.

5.1.3.1.- Plataforma IBM

```
#!/usr/bin/ksh

## !/usr/bin/sh
##_____
## Instalación de Patrol 3.6 con nuevas versiones en los KMs
## Informix 3 2 03 y History Propagator 1 4
##_____
##_____
## Verifica que exista el directorio de /opt/ARIES/patrol
##_____
##

 if test -d /opt/ARIES/patrol
 then
    cd /opt/ARIES/patrol
    CERO=0
    AGENTE=`ps -ef|grep PatrolAgent|grep -v grep|wc -l`
    if test $AGENTE -gt $CERO
    then
       PA=`ps -ef |grep PatrolAgent|grep -v grep|awk -F" " '{print FS$2}'`
       kill $PA
       sleep 10
    fi
    > BitacoraP
    rm -Rf *
    echo "Borrando archivos \n" >> BitacoraP
    mv /opt/ARIES/Parches*.tar.Z
    mv /opt/ARIES/install* sh .
    chmod 777 BitacoraP
    chown patrol:patrol BitacoraP

    echo "\n" >> BitacoraP
    echo "\n" >> BitacoraP
    echo "\tINSTALANDO EL AGENTE DE PATROL " >> BitacoraP
    echo "\n" >> BitacoraP
 else
    cd /tmp
    echo "\n\tERROR: No se puede instalar Patrol" >> BitacoraP
    echo "\tNo existe el directorio de PATROL" >> BitacoraP
    exit 1
 fi

##_____
## Se descomprime el archivo * Z
##_____
##
 cd /opt/ARIES/patrol

  DESCMP=`find  -name P* Z  -print|cut -f2 -d '/'`
  uncompress $DESCMP >> BitacoraP

 ## _____
```

```
## Se desempaqueta el archivo  *.tar
##_____________________________________
##

   DESTAR=`find . -name P* tar  -print|cut -f2 -d '/'`
   tar -xvf $DESTAR >> BitacoraP

   echo "\n" >> BitacoraP
   echo "\n" >> BitacoraP


##-------------------------------------
## Se actualiza la licencia del Agente de Patrol
##_____________________________________________
##

  cd /opt/ARIES/patrol
  echo "  ACTUALIZANDO  LA LICENCIA " >> BitacoraP
  echo "\n" >> BitacoraP


  cd /opt/ARIES/patrol/lib
  mv license.*  license.`hostname`

##-------------------------------------
## Se actualiza el nombre del archivo de configuración
##-------------------------------------

  cd /opt/ARIES/patrol
  echo " ACTUALIZANDO ARCHIVO DE CONFIGURACIÓN " >> BitacoraP
  echo "\n" >> BitacoraP

  cd /opt/ARIES/patrol/AIX4.1-RS/config
  mv config* config_`hostname`-1987

##-------------------------
## Cambia permisos para informix
##_____________________________________
##

  cd /opt/ARIES/patrol
  echo "  OTORGANDO PERMISO DE LECTURA A LA bitácora "  >> BitacoraP
  echo "\n"  >> BitacoraP


  inf_dir=`awk -F: '/^informix/ {print $6}' /etc/passwd`

 instanc=`ls ${inf_dir}/etc/onconfig* 2>/dev/null|grep -v '\ sao$'|grep -v '\ tra$'|grep -v '\ std'`

## Instancias encontradas de informix 7 20  $instanc
## Determinar las instancias que estén dadas de alta en informix

  for i in $instanc
  do
     chmod +r $i
     bitácora =`grep MSGPATH $i|awk '{print $2}'`
     chmod +r $bitacora
  done


##-------------------------------
## Ejecuta el  comando configure
##_____________________________
```

```
##
  cd /opt/ARIES/patrol
  echo "  CONFIGURANDO AL AGENTE "  >> BitacoraP
  echo "\n"  >> BitacoraP

  cd /opt/ARIES/patrol
   /configure <dummy >> BitacoraP

##_____________________________
## Activa el agente de patrol PatrolAgent
##_____________________________________________
##
## cd /opt/ARIES/patrol

  echo "  ACTIVANDO EL AGENTE "  >> BitacoraP
  echo "\n"  >> BitacoraP

  cd /opt/ARIES/patrol
   /PatrolAgent & >> BitacoraP
   sleep 25

##_____________________________
## Verifica el agente de patrol PatrolAgent
##_____________________________________________
##
  CERO=0
  AGENTE=`ps -ef|grep PatrolAgent|grep -v grep|wc -l`
  if test $AGENTE -gt $CERO
  then
      echo "\n" >> BitacoraP
      echo "\n" >> BitacoraP
      echo " LA INSTALACIÓN DEL AGENTE DE PATROL ESTA COMPLETA " >> BitacoraP
  else
      echo "\n" >> BitacoraP
      echo "\n" >> BitacoraP
      echo " EL AGENTE DE PATROL NO ESTA ACTIVO " >> BitacoraP
  fi

  rm P* tar
  rm dummy
  rm install* sh
  exit 0


##_____________________________________________________
```

5.1.3.2.- *Plataforma HP*

```
#!/usr/bin/ksh

## !/usr/bin/sh
##-------------------------------------------
## Instalación de Patrol 3.6 con nuevas versiones en los KMs
## Informix 3.2.03 y History Propagator 1.4
##-------------------------------------------
##-------------------------------------------------------------------
## Verifica que exista el directorio de /opt/ARIES/patrol
##-------------------------------------------------------------------
##

 if test -d /opt/ARIES/patrol
 then
     cd /opt/ARIES/patrol
##      PCONF=`find . -name pconfig*`
##      if test -x $PCONF
     CERO=0
     AGENTE=`ps -ef|grep PatrolAgent|grep -v grep|wc -l`
     if test $AGENTE -gt $CERO
     then
##          $PCONF +KILL -host `hostname`
        PA=`ps -ef |grep PatrolAgent|grep -v grep|awk -F" " '{print FS$2}'`
        kill $PA
        sleep 10
     fi
     > BitacoraP
     rm -Rf *
     echo "Borrando archivos \n" >> BitacoraP
     mv /opt/ARIES/Parches* tar Z .
     mv /opt/ARIES/install* sh
     chmod  777  BitacoraP
     chown  patrol:patrol  BitacoraP

     echo "\n" >> BitacoraP
     echo "\n" >> BitacoraP
     echo "\tINSTALANDO EL AGENTE DE PATROL " >> BitacoraP
     echo "\n" >> BitacoraP
 else
     cd /tmp
     echo "\n\tERROR  No se puede instalar Patrol" >> BitacoraP
     echo "\tNo existe el directorio de PATROL" >> BitacoraP
     exit 1
 fi

##-------------------------------
## Se descomprime el archivo  * Z
##-------------------------------------------
##
 cd /opt/ARIES/patrol

  DESCMP=`find   -name P* Z  -print|cut -f2 -d '/'`
  uncompress $DESCMP >> BitacoraP

##-------------------------------
## Se desempaqueta el archivo  * tar
##-------------------------------------------
##

  DESTAR=`find   -name P* tar  -print|cut  -f2 -d '/'`
  for xyz in $DESTAR ; do tar xvf $xyz ; done
```

```
   echo "\n" >> BitacoraP
   echo "\n" >> BitacoraP

##-------------------------------------------------------
##  Mueve  el archivo para levantamiento o baja del Agente en un Reboot
##  del equipo
##-------------------------------------------------------------------------------
##

    cd /opt/ARIES/patrol
    echo " MUEVE EL ARCHIVO PATROL A /sbin/init d " >> BitacoraP
    echo "\n" >> BitacoraP

    mv  Patrol  /sbin/init.d
    cd /sbin/init d
    chmod 755  Patrol
    chown  root:sys  Patrol

##-------------------------------------------------------
## Crea una liga hacia el subdirectorio de archivos de configuración del nodo
##-------------------------------------------------------------------------------
##
    cd /opt/ARIES/patrol
    echo " CREANDO LA LIGA A /tmp " >> BitacoraP
    echo "\n" >> BitacoraP

        cd /tmp
        rm patrol

        cd /

        ln -s /etc/opt/ARIES/patrol  /tmp/patrol

##-------------------------------------------------------
## Crea ligas hacia el archivo de Patrol para el levantamiento o baja del agente
## en un reboot del equipo
##-------------------------------------------------------------------------------
##

    cd /opt/ARIES/patrol
    echo " CREANDO LAS LIGAS DE /sbin " >> BitacoraP
    echo "\n" >> BitacoraP

    cd /
    ln -s /sbin/init.d/Patrol /sbin/rc0 d/K150Patrol
    ln -s /sbin/init d/Patrol /sbin/rc1 d/K150Patrol
    ln -s /sbin/init d/Patrol /sbin/rc2 d/K150Patrol
    ln -s /sbin/init d/Patrol /sbin/rc3 d/S600Patrol

##-------------------------------------------
## Se actualiza la licencia del Agente de Patrol
##-------------------------------------------------------
##

   cd /opt/ARIES/patrol
   echo "  ACTUALIZANDO  LA LICENCIA " >> BitacoraP
   echo "\n" >> BitacoraP


   cd /opt/ARIES/patrol/lib
   mv license.* license.`hostname`
```

```
##-------------------------------------
## Se actualiza el nombre del archivo de configuración
##-------------------------------------

  cd /opt/ARIES/patrol
  echo " ACTUALIZANDO ARCHIVO DE CONFIGURACIÓN " >> BitacoraP
  echo "\n" >> BitacoraP

  cd /opt/ARIES/patrol/HPUX-PA1 0-V10/config
  mv config* config_`hostname`-1987

##-------------------------
## Cambia permisos para informix
##-------------------------------------
##

  cd /opt/ARIES/patrol
  echo "  OTORGANDO PERMISO DE LECTURA A LA bitácora "  >> BitacoraP
  echo "\n"  >> BitacoraP


  inf_dir=`awk -F: '/^informix/ {print $6}' /etc/passwd`

 instanc=`ls ${inf_dir}/etc/onconfig* 2>/dev/null|grep -v '\.sao$'|grep -v '\ tra$'|grep -v '\ std'`

## Instancias encontradas de informix 7 20. $instanc
## Determinar las instancias que estén dadas de alta en informix

  for i in $instanc
  do
      chmod +r $i
      bitácora =`grep MSGPATH $i|awk '{print $2}'`
      chmod +r $bitácora
  done

## Se termino de configurar los permisos de lectura para poder monitorear informix en Patrol
##-------------------------
## Se crea el archivo .rhosts
##-------------------------------------
##
#  cd /opt/ARIES/patrol
#  mv rhosts  rhosts
#  mv profile  profile
#  chmod 644  profile
#  chown patrol patrol  profile
#  chmod 644  rhosts
#  chown patrol patrol  rhosts

##-------------------------
## Ejecuta el comando configure
##-------------------------------------
##
  cd /opt/ARIES/patrol
  echo "  CONFIGURANDO AL AGENTE "  >> BitacoraP
  echo "\n"  >> BitacoraP

  cd /opt/ARIES/patrol
   /configure <dummy >> BitacoraP

##-------------------------
## Activa el agente de patrol PatrolAgent
##
##
```

```
## cd /opt/ARIES/patrol

  echo "  ACTIVANDO EL AGENTE "  >> BitacoraP
  echo "\n"  >> BitacoraP

  cd /opt/ARIES/patrol
  ./PatrolAgent & >> BitacoraP
   sleep 25

##-----------------------------------
## Verifica el agente de patrol PatrolAgent
##-------------------------------------------------
##
  ##CERO=0
  AGENTE=`ps -ef|grep PatrolAgent|grep -v grep|wc -l`
  if test $AGENTE -gt $CERO
  then
      echo "\n" >> BitacoraP
      echo "\n" >> BitacoraP
      echo " LA INSTALACIÓN DEL AGENTE DE PATROL ESTA COMPLETA " >> BitacoraP
  else
      echo "\n" >> BitacoraP
      echo "\n" >> BitacoraP
      echo " EL AGENTE DE PATROL NO ESTA ACTIVO " >> BitacoraP
  fi

  rm P*.tar
  rm dummy
  rm install* sh
  exit 0

##-------------------------------------------------------------
```

5.1.3.3.- Inicialización de agentes

Verificación

```
##########/##### verificación.sh
##
##
##

   /etc/ping aries 256 5 | grep " 0% packet loss" > /dev/null 2>&1
   if [ $? -eq 0 ], then
        remsh c10 -n /opt/ARIES/patrol/activacion sh
            echo "envío del mensaje ITO de iniciación de shell"
   else
        echo "envío de mensaje de no comunicación con el $NODO"
   fi
```

Notificación por estado VOID

```
#!/usr/bin/ksh
##-----------------------------------
## Notifica a IT/Operations
##        - Falta de Comunicacion
##        - Activación del Agente de Patrol
##-------------------------------------------------
##

   NODO="$1"
```

```
    /opt/OV/bin/OpC/opcmsg  severity=critical  msg_grp="Performance" application="PEM"
object="pem_patrol"                  msg_text=" El NODO esta fuera de linea "  node="$1"

    /etc/ping $NODO 256 5 | grep " 0% packet loss" > /dev/null 2>&1
    if [ $? -eq 0 ]; then

        /opt/OV/bin/OpC/opcmsg  severity=critical  msg_grp="Performance" application="ACTIVACION"
object="agente_patrol"          msg_text=" Si hay comunicación con el NODO."  node="$1"
        /opt/OV/bin/OpC/opcmsg  severity=critical  msg_grp="Performance" application="ACTIVACION"
object="agente_patrol"          msg_text=" Se verifica o reinicializa la ACTIVACIÓN del Agente de PATROL "
node="$1"

##        Ejecuta el shell que Activa el Agente de Patrol
        remsh $NODO -n /opt/ARIES/patrol/activacion.sh
    else
        /opt/OV/bin/OpC/opcmsg  severity=critical  msg_grp="Performance" application="ACTIVACION"
object="agente_patrol"          msg_text=" No hay COMUNICACIÓN con el nodo " node="$1"
    fi
##_____________________________________________________
```

Notificación por estado OK

```
#!/usr/bin/ksh
##_____________________________
## Notifica a IT/Operations
##        - Restablecimiento de Comunicación
##        - Activación del Agente de Patrol
##_____________________________________________
##

    NODO="$1"

    /opt/OV/bin/OpC/opcmsg  severity=critical  msg_grp="Performance" application="PEM"
object="pem_patrol"                  msg_text=" El Agente de PATROL esta activo en el nodo. "  node="$1"


##        /opt/OV/bin/OpC/opcmsg  severity=critical  msg_grp="Performance" application="ACTIVACION"
object="agente_patrol"          msg_text=" Se reinicializará la ACTIVACIÓN del Agente de PATROL. "
node="$1"
##        Ejecuta el shell que Activa el Agente de Patrol
##         remsh $NODO -n /opt/ARIES/patrol/activacion.sh


##_____________________________________________________
```

5.2.- Red de Comunicaciones

5.2.1.- Diseño de Solución

5.2.1.1.- Objetivo

Analizar, diseñar e implantar una solución que permita realizar de forma amigable, automatizada, eficiente y robusta, la administración, operación y monitoreo de la Red de Telecomunicaciones del SAT, compuesta por los ambientes actuales de interconectividad: X25, LAN, WAN e Internet, soportada por tecnologías de Frame Relay, RDI, TCP/IP y X25, así como de los equipos y sistemas que la conforman.

5.2.1.2.- Alcances

- Análisis detallado para el diseño, implantación y puesta en operación de la solución para la administración de redes
- Integración con la Consola Central de Eventos (HP OpenView IT Operations).
- Proporcionar información histórica para los análisis de tendencias y capacidades de los siguientes grupos de sistemas de acuerdo a las variables MIB descritas en la siguiente tabla.
- Definición de umbrales de operación para cada una de las variables consideradas.

Variable/Sistema	Enrutadores	Servidores	LanSwitch	Hub's
No_de nodos	X	X	X	X
If%InErrors	X	X	X	X
If%OutErrors	X	X	X	X
Ip%ReasmOks	X	NA	NA	NA
Ip%NoRoutes	X	NA	NA	NA
%avgBusy=f(dispositivo propietario)	X	NA	NA	NA
Fr%Error	X	NA	NA	NA
%frUtil	X	NA	NA	NA
IfInOctetos	X	X	X	X
IfOutOctects	X	X	X	X
If%Util	X	X	X	X
IfOperStatus	X	X	X	X
If%Collisions	X	X	X	X
If%InDiscards	X	X	X	X
If%OutDiscards	X	X	X	X
Hp_PktsIn_Out	X	X	X	X
Event_IntUp y event_IntDown	X	X	X	X
IfNode_Add	X	X	X	X

Nota: (X) Monitoreado (NA) No Aplica

Tabla 16 Variables MIB monitoreadas

Notificación de:

- Eventos generados como resultado de exceder los umbrales definidos para las variables y recolecciones de la tabla 16.
- Inconsistencias en el esquema de direccionamiento IP.
    - Dirección IP duplicada.
    - Error en la máscara de red.
- Estado operativo (Up/Down) de:
    - Nodo
    - Interfaz
- Descubrimiento de un nuevo nodo en la red.
- Notificación del estado operativo de dispositivos de comunicación (Router´s, Switche´s, Multiplexores, Hub´s, Lan Probe´s, Conmutadores), en la estricta medida de sus capacidades (lo posible).

Reporte de disponibilidad de enlaces (interfaces), segmentando por niveles:

- Dorsal
- Distribución
- Acceso

Reporte de contribución al tráfico por protocolo, en función de las facilidades y funcionalidades proporcionadas por los equipos de comunicación, así como de las tecnologías, de los protocolos: TCP/IP, IPX, UDP, etc.

Proporcionar elementos de análisis que permitan diagnosticar:

- Problemas de direccionamiento (a través de la notificación de inconsistencias en el direccionamiento)
- La utilización de los canales de comunicación (en base a las variables y expresiones de utilización definidas en la tabla 16, concretamente %ifUtil).
- La configuración de los equipos de comunicación (a partir del análisis de los datos obtenidos de las recolecciones y eventos generados por las variables de la tabla 16).

El alcance del presente proyecto también incluye los servidores de aplicaciones HP9000, Sun e IBM, que manejan SNMP y estén ubicados en las redes locales (LAN) y extendidas (WAN) a nivel nacional Para los equipos X25, se realizará el monitoreo de las variables MIB definidas en la tabla 16, siempre y cuando se encuentren dentro de las funcionalidades y capacidades tanto del equipo, como de HP NNM

Para los equipos que cuentan con SNMP, se podrá monitorear el estado operativo y se podrá obtener información de los sistemas a través de variables MIB (Management Information Base). En los equipos que cuentan con TCP/IP y no manejan SNMP (como una PC convencional por ejemplo) se podrá monitorear sólo el estado operativo (nodo activo o inactivo).

La configuración de los mapas de la topología de la red de comunicaciones se llevará a cabo a manera de Regiones y/o Unidades Administrativas representándose cada uno de los nodos de la red y su conectividad con nodos secundarios.

5.2.1.3.- Detalle de Solución

El monitoreo y la administración de la red se realizará de forma centralizada utilizando HP OpenView Network Node Manager versión 6.10 (al cual se hará referencia como HP NNM). HP NNM, permite el monitoreo de los elementos de red que utilicen el protocolo TCP/IP, y además permite realizar ciertas peticiones de información a los elementos de red que manejan el protocolo SNMP.

HP NNM se encargará de realizar las siguientes tareas:

- Realizar el descubrimiento automático de la red y representar gráficamente la topología en la que están organizados los elementos que integran la red del SAT.
- Conocer el estado operativo de los nodos que integran la red del SAT, que esencialmente se refiere a supervisar la disponibilidad de la interfaz de red de los nodos.
- Colectar el valor de diferentes variables (variables MIB), de cada uno de los nodos monitoreados que permitirán realizar análisis posteriores, apoyándose en la información recolectada de los nodos.
- De acuerdo al valor de las variables recolectadas será posible definir umbrales de operación para generar un evento cuando alguna de las variables en un nodo rebase un valor establecido.
- Recibir los eventos que envían los nodos monitoreados (estos eventos son llamados *traps*).
- Para determinados eventos, se levantará un reporte en la mesa de ayuda a través de la integración de HP NNM y HP OpenView IT Operations.

HP NNM realizará el descubrimiento automático y monitoreará el estado operativo para todos los nodos con TCP/IP que se encuentran en la red del SAT. HP NNM permitirá realizar el monitoreo del estado operativo de acuerdo al código del color con el que son representados los elementos que integran la misma

Todos los eventos (*traps*) que generen los nodos en la red serán recibidos por HP NNM Manager en el equipo denominado Management Console (HP9000/X460)

La obtención de estadísticas de los nodos administrados y supervisión de umbrales de operación, se realizará de manera centralizada desde la consola central de administración.

Para llevar a cabo la detección de eventos, la aplicación que realiza el monitoreo de la red TCP/IP, HP NNM, se basa en el protocolo SNMP. HP NNM interactúa con los nodos que cuentan con SNMP haciéndoles requerimientos y recibiendo respuestas y *traps* acerca de su estado. La forma en que se integra HP NNM se ilustra en la siguiente figura.

El bloque de la figura con la etiqueta "Administrador" corresponde a la estación de trabajo donde se ejecuta el manager de HP NNM. Los bloques de la figura con las etiquetas "Agente" y "MIB" corresponden a un nodo con SNMP monitoreado. NNMGR es el encargado del monitoreo de la red y la forma en que lo lleva a cabo es haciendo peticiones de información a través del protocolo SNMP y recibiendo respuestas a través del mismo protocolo. El nodo con el agente SNMP mantiene una base de datos llamada MIB con la información del estado del nodo.

Comunicación Administrador Agente vía SNMP

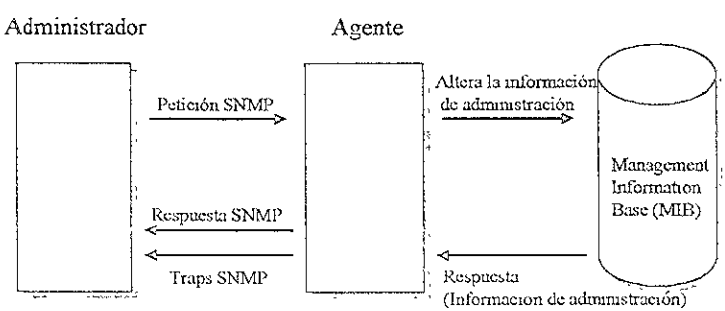


Figura 13. Comunicación vía SNMP

La red del SAT será descubierta y mostrada en forma de mapas de acuerdo a la funcionalidad de HP NNM. Dentro de cada mapa habrá símbolos representando objetos de la red (entidades físicas o lógicas como servidores, enrutadores, switches, lanswitches, segmentos, etc).

Para lograr una representación adecuada de los elementos que integran la red del SAT, se establecerá un esquema que concuerde con los siguientes lineamientos:

- Red del SAT.- Representación de los nodos y conexiones que integran la red del SAT organizados por regiones en toda la República Mexicana, incluyendo únicamente componentes de red y servidores.
- Sistemas en Oficinas de Recaudación.- Representación de las oficinas de recaudación del SAT como entidades lógicas y dentro de cada una de ellas los servidores que están incluidos en cada una de las oficinas, sin conexiones y representando únicamente enrutadores y servidores.
- Sistemas en oficinas de aduanas.- Representación de las oficinas de aduanas como entidades lógicas en un submapa y dentro de cada una de ellas, los elementos que la integran.
- Enrutadores en la red del SAT.- Representación de los enrutadores que integran la red del SAT organizados de manera jerárquica de acuerdo a las capas establecidas.

Dentro de la representación de la Red del SAT, se colocará un gráfico de fondo, este gráfico será un archivo en formato *gif* que representa la República Mexicana y si se desea, podrán usarse imágenes de mapas geográficos representando a las administraciones regionales con el objeto de configurar niveles de submapas dentro de la representación de la red del SAT, tal y como se representa en las siguientes figuras.

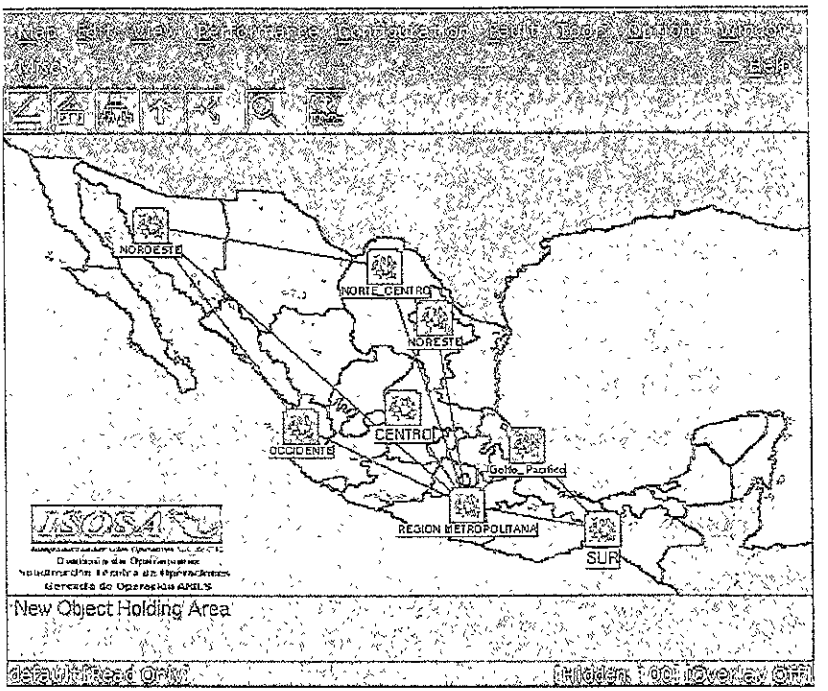


Figura 14. Consola de Monitoreo de Redes NNM.

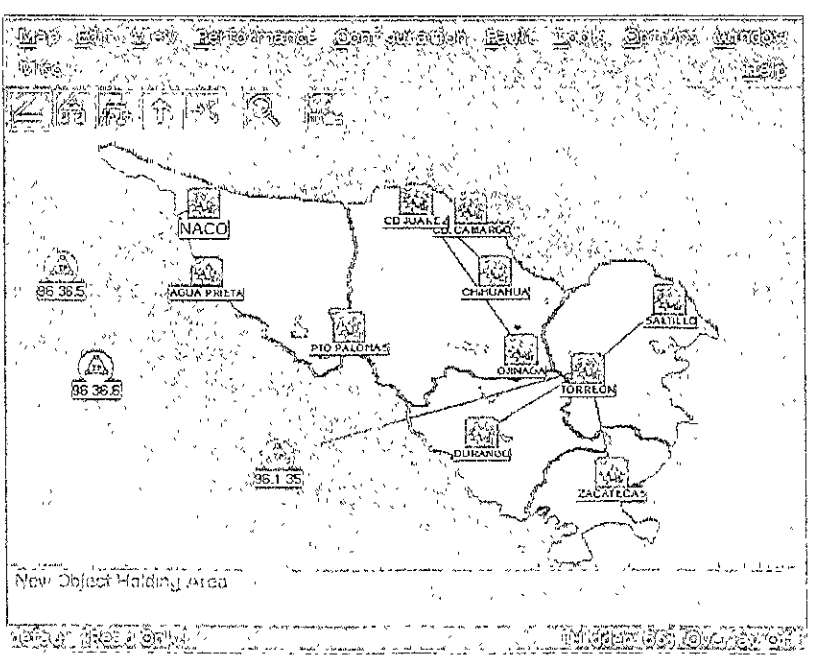


Figura 15 Consola de Monitoreo de Redes Region Occidente

Para que los nodos que se pretende monitorear, aquellos que tengan agente SNMP, envíen la información necesaria para ser monitoreados hacia el equipo que será utilizado como Management Console, será necesario configurar ciertos parámetros. Para configurar los parámetros SNMP en los nodos administrados se colocarán los siguientes valores en los equipos:

get-community-name:	*nombre de la comunidad a la que se realizará el get.*
set-community-name:	*nombre de la comunidad a la que se realizará el set.*
trap dest:	*equipo al que se enviarán los "traps".*
location:	*texto que indica la ubicación física, la sintaxis se describe más adelante.*
contact:	*Persona responsable del equipo, la sintaxis se describe más adelante.*

En la administración de los equipos que integran la red del SAT, las comunidades son asignadas por la Administración de Telecomunicaciones.

En los servidores con sistema operativo HP Unix, la configuración del agente SNMP se realiza en el archivo *snmpd.conf* ubicado en el directorio */etc/SnmpAgent.d*, para el caso de servidores IBM dicha configuración se llevará a cabo a través de la utilería Smit.

El campo *location* seguirá el siguiente formato: ciudad donde reside físicamente el equipo, una coma, un espacio, ubicación del edificio en la ciudad, una coma, un espacio y ubicación del equipo dentro del edificio. El tamaño de la cadena de caracteres es 255 caracteres máximo. Por ejemplo.

location: Cd. Obregón Son, calle Sonora #1000, site

El campo *contact* hace referencia a la persona a quien se puede dirigir cuando hay problemas o preguntas acerca del equipo, y tendrá el siguiente formato: nombre del responsable, una coma, un espacio, ubicación, una coma, un espacio, teléfono del responsable, una coma, un espacio y número de serie del equipo. El tamaño de la cadena de caracteres es 255 caracteres máximo. Por ejemplo:

contact: Enrique Cabrera, Monterrey, 91(64)165011, 800F303135A10340

El campo *trap destination* indica la dirección IP (o en su caso, el nombre del equipo) donde residirá NNMGR para que el nodo pueda reportarle los eventos relevantes. En el presente proyecto la dirección será 99.90.32.107, que identifica al servidor de nombre "Aries" y que es la dirección del equipo identificado como Management Console a nivel central.

Los dispositivos de red, concretamente los servidores y enrutadores podrán administrarse de manera tradicional, es decir estableciendo una conexión telnet al dispositivo en los casos en los que sea posible, o en su defecto conectando una

erminal a su puerto de consola, lo cual implicará la configuración del dispositivo de manera local.

HP NNM se ejecutará sobre el servidor HP 9000 K460 utilizado como Management Console y se utilizarán consolas *x-terminals* para realizar el despliegue gráfico. Estos equipos se concentrarán en un lugar especialmente diseñado para realizar el monitoreo de toda la red del SAT a nivel nacional.

Los eventos generados como parte del monitoreo de los umbrales de las variables MIB definidas en la tabla 16, serán avanzados hacia HP OpenView IT Operations como parte de la disciplina de Integración de Eventos, desplegándose de acuerdo a la siguiente figura.

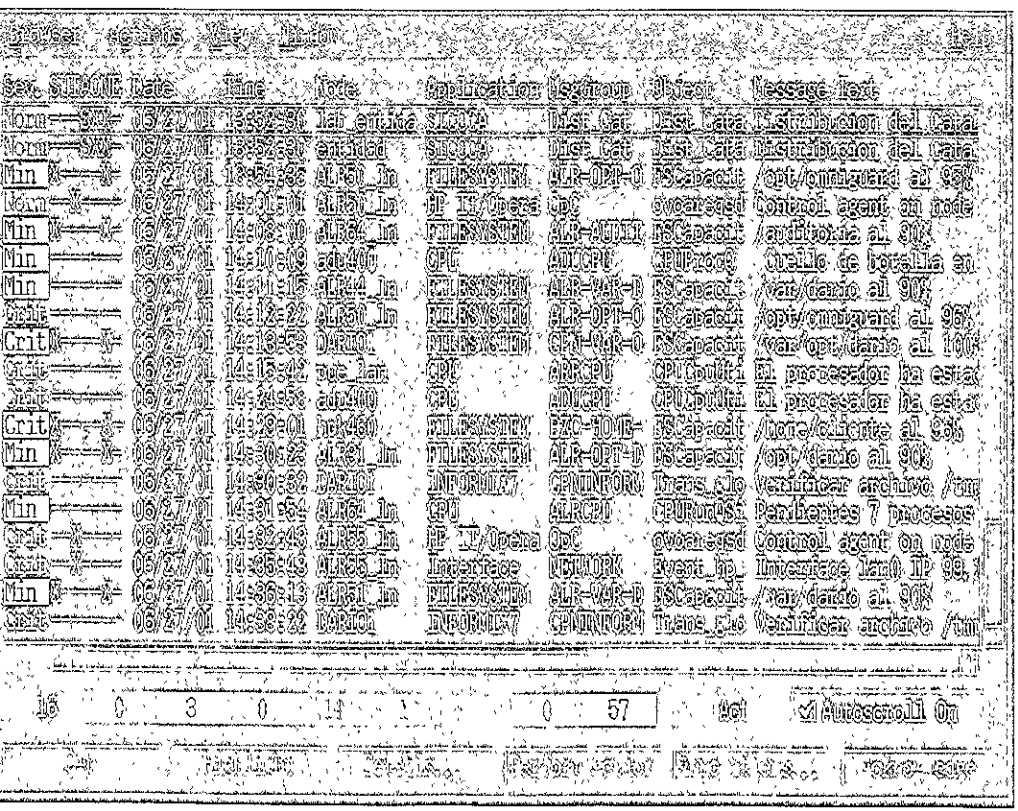


Figura 18. Consola de Integración de Eventos IT/Operations

La solución de administración y monitoreo de la red contempla los elementos principales de la red del Servicio de Administración Tributaria, es decir, incluir enrutadores y servidores como elementos de vital importancia para el funcionamiento de la red. Por lo tanto se contemplan dos grandes grupos:

- Servidores.
- Enrutadores

Para el grupo de servidores, la solución de administración de redes incluye todos aquellos que pertenecen a las siguientes oficinas:

- Oficinas de Aduanas
- Oficinas de Recaudación (Local y Regionalmente)
- Área Metropolitana

Para los enrutadores, se incluyen todos los que integran la red del SAT. Para ello se pretende organizar los enrutadores que existen en la red del SAT por capas, de tal forma que cada capa represente una categoría específica. Para ello, se sugieren las siguientes capas:

- Dorsal.- Se incluirán en esta capa todos los enrutadores que tengan una categoría máxima, determinada por la importancia de su función dentro de la red del SAT, concretamente, aquellos que puedan estar incluidos como parte de un backbone.

- Distribución.- Dentro de esta capa se considerarán los enrutadores cuya función es primordial para la comunicación entre las diferentes oficinas sin incluir aquellos que se encuentren como parte de las mismas.

- Acceso - Esta capa incluye a todos los enrutadores que están ubicados en cada una de las oficinas locales y que no afectan la comunicación entre otras oficinas, sino únicamente a la oficina que pertenecen.

Como parte de la solución, se pretende realizar el monitoreo de todos los elementos que integran la red, es decir, monitorear el estado operativo de todos los nodos que tengan TCP/IP, de acuerdo a las consideraciones descritas anteriormente.

Además, se pretende recolectar de manera continua, los valores de parámetros de interés para todos los nodos a los que se tenga acceso a través de un agente SNMP que permita realizar el monitoreo

Sin embargo, debido a las capacidades actuales de los enlaces que integran la red del SAT, los anchos de banda de dichos enlaces, los protocolos utilizados y el plan de actualización de la red que se realiza actualmente, se propone un esquema alterno que podría ser utilizado en caso de que no fuera posible realizar la recolección de variables de la totalidad de los elementos propuestos debido a

problemas que pudieran surgir en la red, tales como tráfico excesivo o cualquier otro inconveniente que afectara el funcionamiento normal de la misma.

Hay dos razones por las que se podría establecerse una política discriminatoria en el monitoreo de la red:

- Los recursos de la red son limitados y se pretende evitar un tráfico excesivo que afecte los sistemas en producción del SAT.
- Una cantidad excesiva de información de los nodos monitoreados no es necesaria y por ahora, podría utilizarse un muestreo de la información para tener una aproximación de las tendencias de los nodos.

El esquema alterno consiste en colectar y almacenar información de las variables MIB de manera continua sólo para un conjunto pequeño de nodos el cual será denominado conjunto de "nodos críticos" y establecer varios conjuntos de nodos denominados "nodos no-críticos". Los grupos de nodos críticos y nodos no-críticos serían determinados en base a las capacidades de la red y los requerimientos de solución, siendo éstos los más representativos.

Para robustecer el esquema alterno, al inicio de cada semana se realizarían gráficas y se generarían estadísticas con los datos colectados con el fin de emitir un reporte semanal. Del análisis de comportamiento y de las tendencias de los nodos monitoreados se obtendrían conclusiones que permitan generar reportes operativos. Si algún elemento presentara un comportamiento anormal, se procedería a investigar la causa de este comportamiento. En cualquier caso, el reporte obtenido sería archivado y debería compararse con los reportes previos para ese mismo conjunto de nodos; se establecerían comparaciones entre los reportes de diferentes conjuntos de nodos (comentados en el siguiente párrafo) que pudieran verse afectados por algún cambio en la red y se deberá encontrar la causa de posibles variaciones y observar tendencias para el análisis de riesgos.

Para el resto de equipos, que no pertenecen a los nodos críticos, se realizaría el monitoreo de manera periódica pero no simultáneamente y serían divididos en un número de subconjuntos. Para un subconjunto se colectan variables MIB durante una semana. Al inicio de la siguiente semana se cambia el subconjunto de nodos por el siguiente, para los cuales se colectan variables MIB y se genera un reporte similar al generado para los nodos críticos Durante la siguiente semana se realizan las mismas tareas para un subconjunto diferente de nodos. Este proceso se realizaría para cada uno de los subconjuntos y al terminar con el último se inicia un nuevo ciclo con el primer subconjunto. Al iniciar un nuevo ciclo se realizan las mismas tareas que en el ciclo previo, pero además el reporte obtenido debe compararse con los reportes previos para ese mismo subconjunto y establecer correlaciones

Sobre la base de los problemas o tendencias observadas en la red, se podrían realizar monitoreos extraordinarios de nodos específicos

El esquema alterno se presenta en la siguiente figura, en la cual se observa que un nodo que pertenezca a un grupo de nodos no críticos podría integrarse al grupo de nodos críticos de acuerdo a los análisis de los reportes generados del mismo.

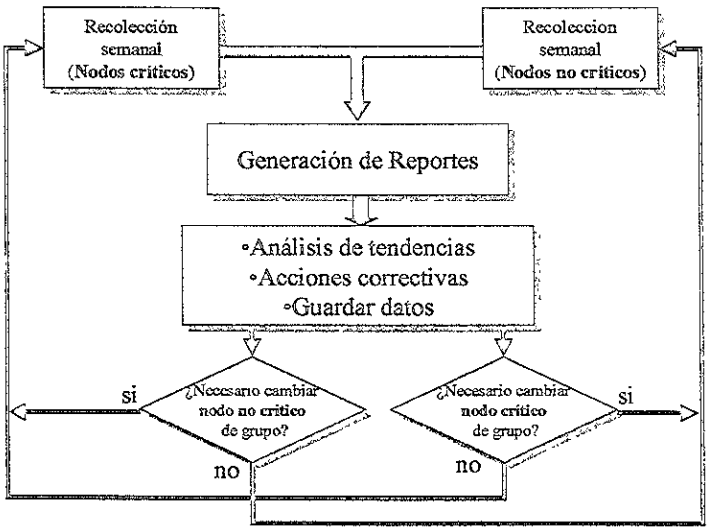


Figura 17. Esquema de monitoreo alterno.

El estado operativo de cada nodo, será representado por el color que rodea al símbolo que representa al nodo correspondiente, y que aparecerá en cada uno de los mapas donde aparezca el objeto. La posibilidad de tener submapas, que están incluidos en un mapa, y a su vez submapas dentro de los submapas, implica que el estado operativo de los nodos que se encuentran en los submapas de menor nivel, sea propagado hacia los mapas o submapas de niveles superiores. Existen tres maneras de propagar el estado de los símbolos de niveles de submapas más bajos hacia niveles superiores.

- Propagación por omisión
- Propagación por el nodo más crítico
- Propagación por umbrales

En los mapas de la red del SAT la propagación del estado será "por el nodo más crítico", debido a que es la más representativa.

Como parte del monitoreo de los nodos a través de SNMP, se pretende configurar ciertos parámetros cuyo valor será recolectado. Estos eventos, deben tener definido un nombre y un identificador dentro del árbol de variables MIB

OpenView	1 3 6 1 4 1 11 2 17 1

a razón por la que se encuentran en este lugar, es porque los eventos definidos or el usuario deben ser ubicados en ésta parte cuando es utilizado HP NNM.

A continuación se presentan los eventos y variables MIB que serán monitoreados, aclarando que los umbrales que inicialmente se propongan, serán los onfigurados de manera estándar, no hay que olvidar que cada ambiente perativo tiene un comportamiento diferente, por lo que los umbrales definitivos erán determinados después de un período que permitirá realizar una evaluación establecer el valor más adecuado.

Para los mensajes desplegados en la consola de administración, deberá aparecer el mensaje indicado para cada uno de los eventos siguientes, incluyendo además el nombre de la interfaz en cuestión.

Parámetro	Descripción
IfInErrors	El número de paquetes de entrada descartados a causa de un error
IfInUcastPkts	El número de paquetes de entrada dirigidos a esta interfaz en específico, y que pasarán a capas superiores
IfInNUcastPkts	El número de paquetes de entrada no dirigidos a esta interfaz en específico (broadcast), y que pasarán a capas superiores
if%inErrors	Porcentaje de paquetes de entrada con error en la interfaz
Event_if%inErrors	Este evento se generará cuando el porcentaje de paquetes de entrada con error en una interfaz exceda un límite establecido.
Rearm_if%inErrors	Este es el rearmado del evento 1001
IfOutError	El número de paquetes de salida descartados a causa de un error
IfOutUcastPkts	El número de paquetes de salida dirigidos a una interfaz en específico.
IfOutNUcastPkts	El número de paquetes de salida no dirigidos a una interfaz en específico (broadcast).
If%outErrors	Porcentaje de paquetes de salida con error en la interfaz
Event_if%outErrors	Este evento se generará cuando el porcentaje de paquetes de salida con error en una interfaz exceda un límite establecido.
rearm_if%outErrors	Este es el rearmado del evento 1003.
IpInDelivers	El número total de datagramas de entrada que serán exitosamente enviados a capas superiores
IpUnknowProtos	El número de datagramas recibidos pero que serán descartados por tener un protocolo desconocido.
IpIn Discards	El número de datagramas de entrada para los cuales no fue encontrado un problema pero que fueron descartados (por ejemplo, por poco espacio de buffer)
IpReasmOKs	Número de datagramas ip exitosamente reensamblados
Ip%ReasmOKs	Porcentaje de datagramas que son reensamblados exitosamente y pasarán hacia capas superiores
event_ip%ReasmOKs	Este evento se generará cuando el porcentaje de datagramas reensamblados en un sistema exceda un límite establecido
rearm_ip%ReasmOKs	Este es el rearmado del evento 1011
IpOutNoRoutes	El número de datagramas descartados porque no pudo ser encontrada la ruta a donde deben ser transmitidos.
IpOutRequests	El número total de datagramas IP generados localmente que solicitan una transmisión
IpForwDatagrams	El número de datagramas IP que serán avanzados por no ser éste su destino final
Ip%OutNoRoutes	Porcentaje de datagramas IP descartados porque no se encuentra la ruta a

	donde deben ser mandados
event_ip%OutNoRoutes	Este evento se generará cuando el porcentaje de datagramas sin ruta en un sistema exceda un límite establecido
rearm_ip%OutNoRoutes	Este es el rearmado del evento 1013
FrCircuitReceivedFECSNs	El número de frames recibidos en un circuito FrameRelay para ser avanzados y que indican congestión
FrCircuitsBECNs	El número de frames recibidos en un circuito FrameRelay que deben ser rechazados y que indican congestión
FrCircuitsReceivedframes	Número de frames recibidos en un circuito Frame Relay
Ip%OutNoRoutes	Porcentaje de errores en un circuito FrameRelay
Event_fr%Errors	Este evento se generará cuando el porcentaje de errores en el circuito FrameRelay exceda un límite establecido
Rearm_fr%Errors	Este es el rearmado del evento 1013
IfInOctets	El número total de octetos recibidos en una interfaz incluyendo los caracteres de framing.
IfOutOctets	El número total de octetos transmitidos por una interfaz incluyendo los caracteres de framing
IfInSpeed	Un estimado actual del ancho de banda disponible por la interfaz en bits por segundo
if%util	Porcentaje del ancho de banda utilizado por la interfaz
event_if%util	Este evento se generará cuando el porcentaje de utilización de canal en una interfaz exceda un límite establecido.
rearm_if%util	Este es el rearmado del evento 1005
IfOperStatus	El estado actual de operación de la interfaz. Up(1) Down(2) Testing(3)
event_ifOperStatus	Este evento se generará cuando el estado operativo de la interfaz sea diferente a UP (la 1era. vez y cuando cambie).
rearm_ifOperStatus	Este es el rearmado del evento 1007 Nodos con severidad Critical.
Ieee8023MacSingleCollisions	El número total de retransmisiones debidas a una colisión
Ieee8023MacTransmitted	El número total de tramas exitosamente transmitidas
if%collison	Porcentaje de paquetes en una interfaz los cuales colisionaron
event_if%collision	Este evento se generará cuando el porcentaje colisiones en una interfaz exceda un límite establecido
rearm_if%collision	Este es el rearmado del evento 1009
IfInDiscards	El número de paquetes de entrada los cuales fueron descartados por alguna razón diferente a un error (por ejemplo, falta de buffers).
if%InDiscards	Porcentaje de paquetes de entrada descartados por la interfaz
Event_if%InDiscards	Este evento se generará cuando el porcentaje de paquetes descartados en la entrada de una interfaz exceda un límite establecido
Rearm_if%InDiscards	Este es el rearmado del evento 1015
IfOutDiscards	El número de paquetes de salida los cuales fueron descartados por alguna razón diferente a un error (por ejemplo, falta de buffers).
if%OutDiscards	Porcentaje de paquetes de salida que fueron descartados por la interfaz debido a causas diferentes a errores.
Event_if%OutDiscards	Este evento se generará cuando el porcentaje de paquetes descartados a la salida de una interfaz exceda un límite establecido
Event_IntUp	El presente evento es una copia del evento OV_ifUp, pero con un mensaje desplegable y con un mensaje de registro diferente y para un grupo de interfaces especificas, el texto que sigue a continuacion es original del evento

	mencionado.
Event_IntDown	El presente evento es una copia del evento OV_ifDown, pero con un mensaje desplegable y con un mensaje de registro diferente, y sólo para un grupo de Interfaces específicas (aquellas considerados como críticas), el texto que sigue a continuación es original del evento mencionado.
ifNode_Add	El presente evento es una copia del evento ifNodeAdd, pero con un mensaje desplegable y con un mensaje de registro diferente.

Tabla 17. Descripción de eventos y variables MIB monitoreadas

El MIB *Application Builder* permite construir, sin programación aplicaciones MIB para objetos MIB estándar y específicos. Lo anterior quiere decir que podemos escoger una variable MIB de nuestro interés y colocar un nuevo menú dentro de la barra de menú ya existente asociado con esa variable. Cuando se seleccione un objeto dentro de los submapas de HP OpenView Network Node Manager y se elija este menú, inmediatamente aparecerá una gráfica que mostrará los valores actuales de esa variable MIB. Estos datos se van obteniendo en línea del nodo y se van graficando a intervalos de tiempo configurables (por omisión es 1 minuto).

Los *Application Builder* a construir serán cinco con las características que se presentan a continuación.

nOctectes.- El objetivo de incluir la variable MIB ifInOctets es poder graficar en línea el tráfico de entrada en las interfaces de un nodo seleccionado.

Objeto MIB: iso.org.dod.internet.mgmt.MIB-2.interfaces.ifTable.ifEntry.ifInOctets
Título: Bytes Recibidos / seg
Menú: Muestreo->Bytes Recibidos / seg
Intervalo de *Poll*: 1m
Leyenda eje Y: Bytes
Descripción de la variable MIB colectada: Número de bytes recibidos por segundo por interfaz

fOutOctects.- El objetivo de incluir la variable MIB ifOutOctets es poder graficar en línea el tráfico de salida en las interfaces de un nodo seleccionado.

Objeto MIB:iso.org dod.internet.mgmt.MIB-2.interfaces.ifTable ifEntry.
ifOutOctets
Título: Bytes Enviados / seg
Menú: Muestreo->Bytes Enviados / seg
Intervalo de *Poll*: 1m
Leyenda eje Y: Bytes
Descripción de la variable MIB colectada. Número de bytes por segundo enviados por interfaz

ifInErrors.- El objetivo de incluir la variable MIB ifInErrors es poder graficar en línea los errores de entrada detectados en las interfaces de un nodo seleccionado.

Objeto MIB: iso.org.dod.internet.mgmt.MIB-2.interfaces.ifTable.ifEntry. ifInErrors
Título: Número de Paquetes con Error Recibidos en Capa Física
Menú: Muestreo->Paq. Error Rec./seg Capa 1
Intervalo de *Poll*. 1m
Leyenda eje Y: Paquetes
Descripción de la variable MIB colectada: El número de paquetes recibidos que contenían error previniendo de ser distribuidos a un protocolo de capa superior

ifOutQLen.- El objetivo de incluir la variable MIB ifOutLen es poder graficar en línea el tamaño de la cola de paquetes encolados para ser transmitidos por las interfaces de un nodo seleccionado.

Objeto MIB: iso.org.dod.internet.mgmt MIB-2.interfaces.ifTable.ifEntry. ifOutQLen
Título: Longitud de Cola de Salida
Menú: Muestreo->Long. Cola de Salida Interfaz
Poll Intervalo de *Poll*: 1m
Leyenda eje Y: Paquetes
Descripción de la variable MIB colectada: La longitud de la cola de paquetes de salida (medida en paquetes)

ipInReceived.- El objetivo de incluir la variable MIB ifOutQLen es poder graficar en línea el número total de datagramas recibidos en las interfaces, incluyendo aquellos recibidos con error, de un nodo seleccionado

Objeto MIB: iso.org.dod.internet.mgmt MIB-2.ip.ipInReceives
Título: Datagramas Recibidos / seg (Capa de Red)
Menú: Muestreo->Datagramas Rec. / seg
Poll Intervalo de *Poll*: 1m
Leyenda eje Y: Datagramas
Descripción de la variable MIB colectada: El número total de datagramas recibidos en las interfaces, incluyendo aquellos recibidos con error.

Los parámetros generales de muestreo (*polling*) para el monitoreo de la red del SAT serán los siguientes:

Parámetro	Intervalo o estado
Polling Master switch	encendido
Master polling switch	encendido
Delete nodes down for	7 días
New node discovery switch	encendido
Auto-adjusting discovery polling interval switch	encendido
Configuration checking switch	encendido
Configuration polling interval	1 día

Tabla 18 Parámetros de muestreo configurados

Polling Master switch.- Habilita el muestreo del estado de los nodos, para conocer su estado operativo y actualizarlo en NNMGR por lo que su estado es "encendido".

Master polling switch.- Es el control maestro de muestreo de datos de nodos en NNMGR por lo que su estado es "encendido".

Delete nodes down for.- Representa el número de días que NNMGR puede mantener en su base de datos un nodo que no responde y su valor es "7 días", por ser un periodo razonable para determinar que el nodo ya no existe en la red.

New node discovery switch.- Habilita a NNMGR para descubrir nuevos nodos, por lo que su estado es "encendido".

*Auto-adjusting discovery polling interval switch.-*Habilita a NNMGR para determinar automáticamente los intervalos de descubrimiento de nuevos nodos según su algoritmo interno, de otra manera se deberá proporcionar un intervalo de tiempo fijo; su estado es "encendido".

Configuration checking switch.- Habilita a NNMGR para realizar verificación de configuración de los equipos, por lo que su estado es "encendido".

Configuration polling interval.- Determina el intervalo de tiempo para realizar una verificación de la configuración de todos los nodos, su valor es de "1 día", dado que los equipos no se modifican de manera constante.

5.2.2.- Memoria Técnica

5.2.2.1.- Instalación y Activación de Licencia NNM

A partir de la versión 6.10 el software de HP OpenView Network Node Manager se incluye como parte boundle del software de HP Open View IT/O, por lo tanto se requiere realizar únicamente la instalación de éste último; La instalación del IT/Operations requiere previamente de la instalación de la Base de Datos Oracle for Open View, la cual será utilizada como banco de información.

La instalación del software HP OV IT/Operations se lleva a cabo como cualquier software instalable dentro de un ambiente HP-UX, es decir se instala a través del comando o utilería swinstall, la cual es una interfaz interactiva que permite la selección e instalación de productos de software o Filesets contenidos en una media instalable; para nuestro caso el único Fileset seleccionado es el llamado HPITOEngOraAll; Una vez concluida la instalación del software, se procede a la configuración del IT/O, esto se lleva a cabo a través de la ejecución del script de configuración "opcconfig", el cual se encarga de iniciar los procesos de HP NNM, HP IT/O y enlazar el funcionamiento de éste último con la base de datos de HP Open View, a través de la creación de la instancia de la Base de Datos, ambientación de usuarios y variables de ambiente.

Parte de la instalación de HP OpenView Network Node Manager, contempla la instalación de los parches liberados al momento de la actualización. En el caso de la versión 6.10 de HP NNM, se instaló el siguiente parche:

- PHSS_18891 S700_800 10.X OV NNM6.10 Consolidated Patch

Estos parches deben ser instalados una vez que se haya realizado la configuración del IT/Operations.

Cabe mencionar que antes de instalar algún parche para HP OpenView, debe consultarse la información que se anexa con el parche correspondiente. Usualmente, deben cerrarse las sesiones de HP NNM, HP IT/O y detenerse los procesos de HP OpenView ejecutando el siguiente comando como usuario administrador (*root*):

```
# ovstop –v
# opcagt -kill
```

Una vez que se han instalado los parches correspondientes, se reinician los procesos de HP OpenView utilizando el comando:

```
# ovstart –v
# opcagt –start
```

Una vez concluida la instalación de Open View, es recomendable que se habilite el esquema de licenciamiento a través del servidor de licencias, ya que esto permite controlar la administración de las mismas de manera centralizada; Los productos de HP Open View implementan un licenciamiento en red basado en la tecnología provista por ¡FOR/LS, formalmente llamada NetLS /Network Licensing System), el cual utiliza claves de activación que permiten un número autorizado de conexiones concurrentes.

El servidor de licencias de HP Open View consta de dos entidades: El servidor de licencias ¡FOR/LS con NCS y el administrador de licencias de HP Open View; Por default ambos componentes son instalados en cada nodo donde se instale HP NNM, la siguiente figura muestra la instalación por default de estos componentes

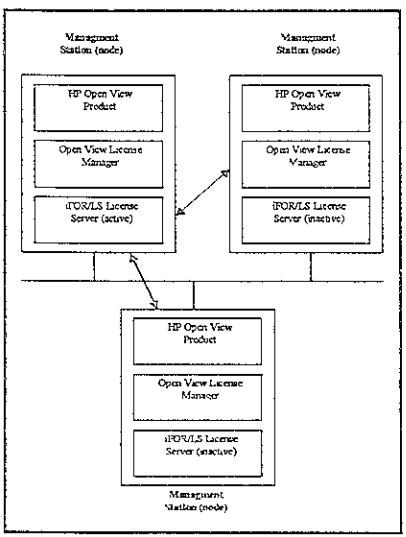


Figura 18. Componentes del Servidor de Licencias

La comunicación del servicio de licenciamiento se lleva a cabo de la siguiente forma: cuando un servidor ¡FOR/LS es por primera vez iniciado, deja que el Llbd (Local Location Broker Deamon) conozca que tiene una licencia para varias aplicaciones, envía un mensaje de broadcast, el cual es tomado por otro u otros Llbd, los cuales notifican a sus glbds (Global Location Broker Deamon) acerca de que aplicaciones se encuentran licenciadas en el servidor; El glbd almacena esta información en su base de datos, este concepto es ilustrado en la siguiente figura:

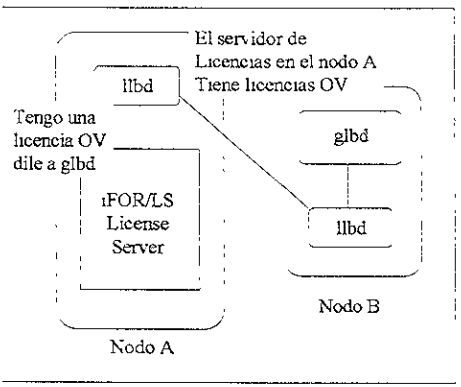


Figura 19 Comunicación del servidor de licenciamiento

El proceso que se sigue para habilitar el servidor de licencias es el siguiente:

- HP Open View solicita una licencia del manejador de licencias
- El manejador de licencias envía una petición en broadcast, la cual es "atrapada" por un Llbd.
- El Llbd pregunta al Glbd para que busque en su base de datos por un servidor de licencias que tenga licencias para el producto HP Open View.
- El Glbd le reporta de regreso al manejador de licencias con la locación del servidor de licencias.
- El manejador de licencias manda una solicitud específica al servidor de licencias, quien en respuesta le manda la licencia solicitada.
- El manejador de licencias le da la licencia al producto Open View.

5.2.2.2.- Descubrimiento y Ordenamiento de la Red

Para la representación de los nodos (servidores, router´s, interfaces de red, etc.), que integran la red del SAT se decidió que en los mapas correspondientes los objetos deberían cumplir con los siguientes requisitos:

1. Únicamente serán representados en los mapas aquellos objetos cuyo valor de la variable MIB *SysObjetID*, pertenezca a los siguientes tipos de nodos:

   - Servidores HP 9000 serie 800 con S.O. HP-UX 10.x o superior.
   - Workstations HP 9000 serie 700 con S O HP-UX 10 x o superior
   - Servidores IBM RS6000 con S O AIX 4 3.2 1 o superior
   - Cualquier componente de red Bay Networks o Cisco

2. Para cada uno de los componentes del punto anterior, únicamente serán representadas las interfaces de red

3. La Base de datos de topología incluirá los objetos mencionados en los 2 puntos anteriores y además los objetos correspondientes a las redes y segmentos de la red.

Para cumplir con la funcionalidad de los puntos anteriores se llevo a cabo la creación de un filtro de descubrimiento, que permitiera que únicamente los objetos que cumplieran con las características anteriores fueran descubiertos por HPNNM. Como consecuencia del filtro de descubrimiento, únicamente los objetos descubiertos formarían parte de la base de datos de topología, por ello no resulta necesario el desarrollo de un filtro de topología.

El filtro de descubrimiento desarrollado es el que se muestra en el apartado de programas de configuración como *Find_Nodes_SAT*

Para facilitar el proceso de descubrimiento de nodos, se utilizó la funcionalidad del proceso netmon que permite utilizar un archivo llamado semilla para acelerar el descubrimiento de los nodos de la red. El archivo semilla utilizado fue nodo_semilla que se muestra en el apartado de programas de configuración.

Una vez descubierta la red de comunicaciones se debe llevar a cabo el ordenamiento de los mapas, el cual incluye los siguientes pasos:

- Creación de objetos para representar las localidades geográficas en las que se ha dividido la red.
- Hacer operaciones de arrastrar y dejar ("drag and drop") para los objetos incluidos en cada una de las regiones geográficas contempladas en la red, manteniendo los enlaces que se hayan descubierto.
- Una vez ordenados los mapas se le puede agregar una imagen de fondo ("backgroud") la cual facilitará la interpretación y/o ubicación de los nodos, enlaces, componentes de red, etc., para éste caso se agregó un mapa de la Republica Mexicana; La integración de HPNNM con la consola de administración de IT/Operations y la representación final de los mapas de la red del SAT se muestra en las figuras siguientes:

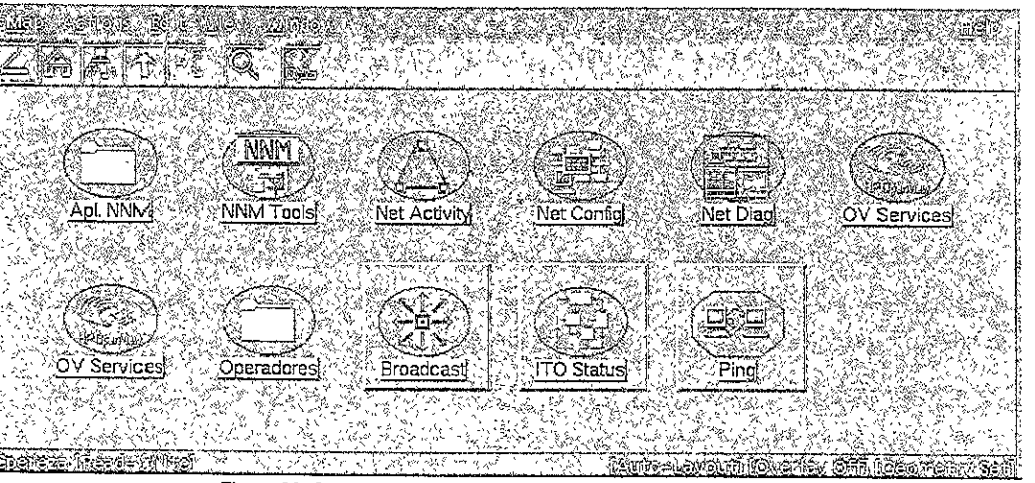


Figura 20 Ordenamiento de Mapas de la Red de Comunicaciones I.

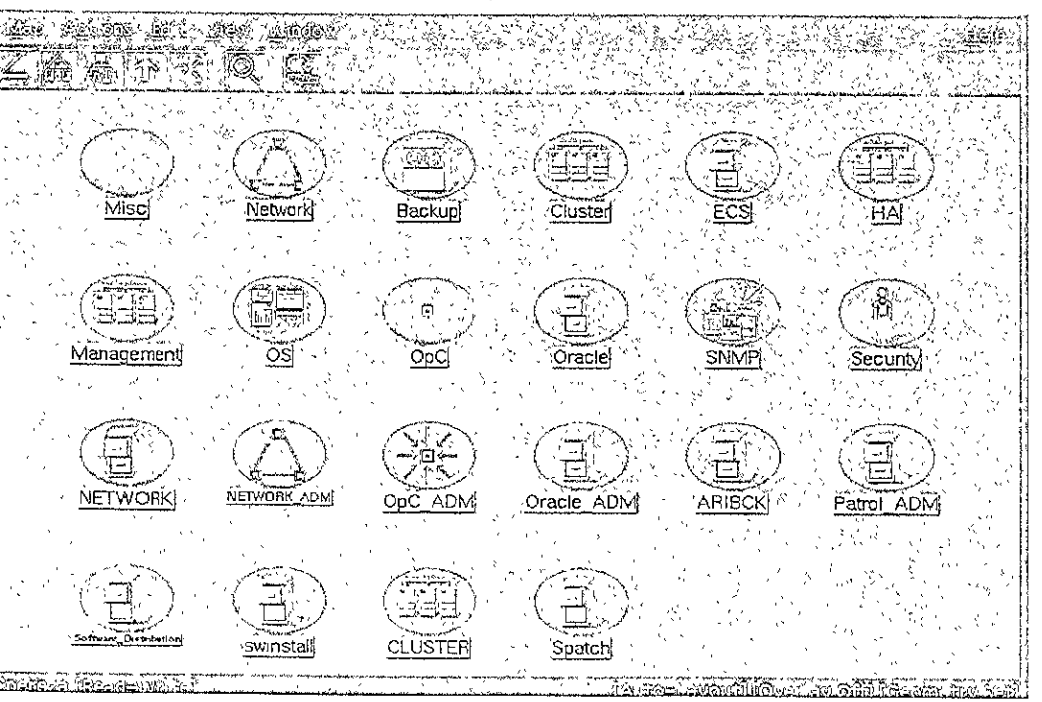


Figura 21 Ordenamiento de Mapas de la Red de Comunicaciones II

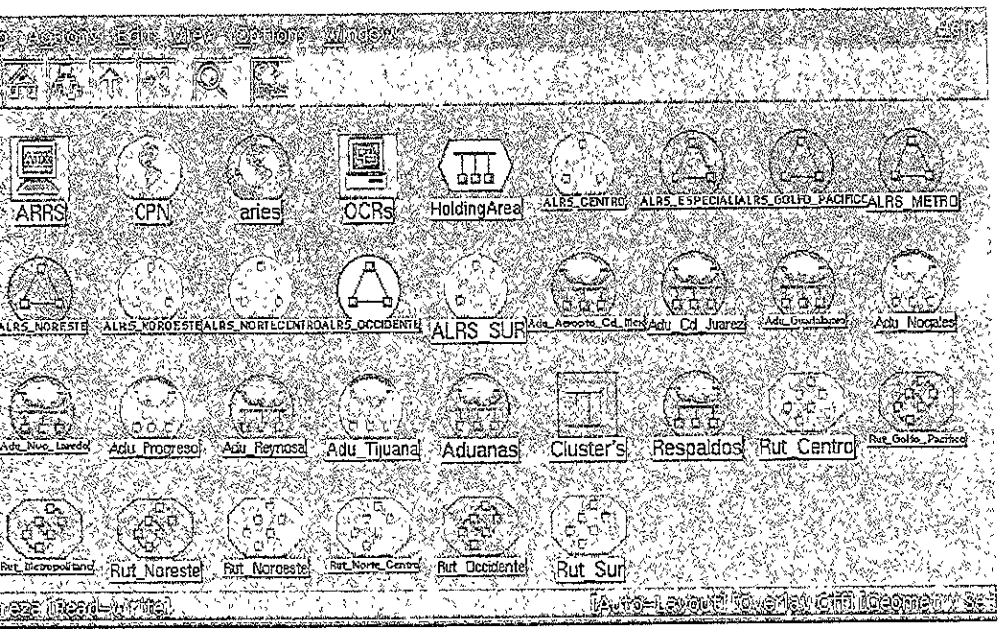


Figura 22. Ordenamiento de Mapas de la Red de Comunicaciones III.

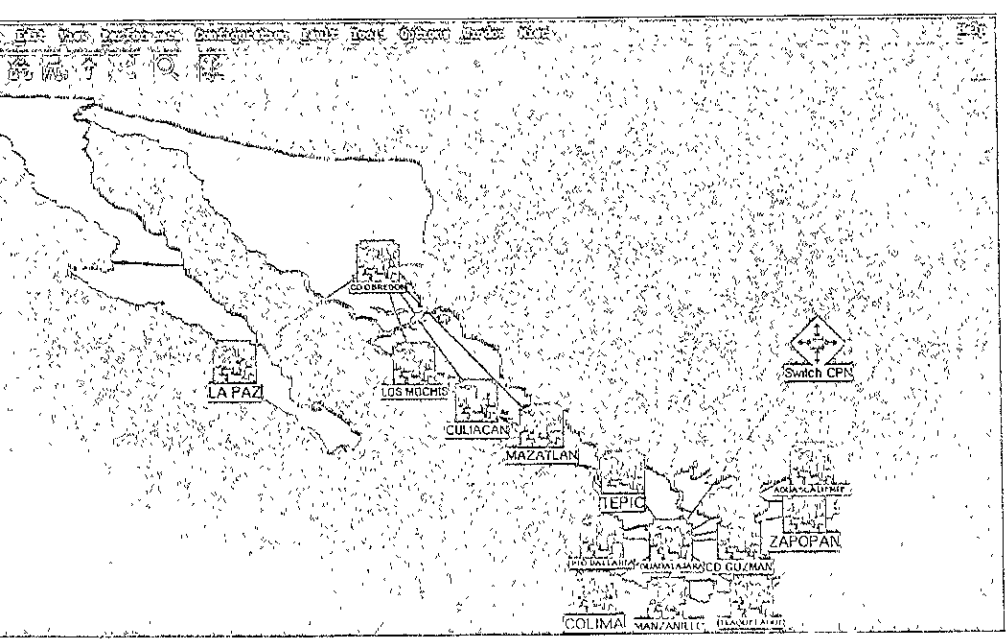


Figura 23. Ordenamiento de Mapas de la Red de Comunicaciones IV

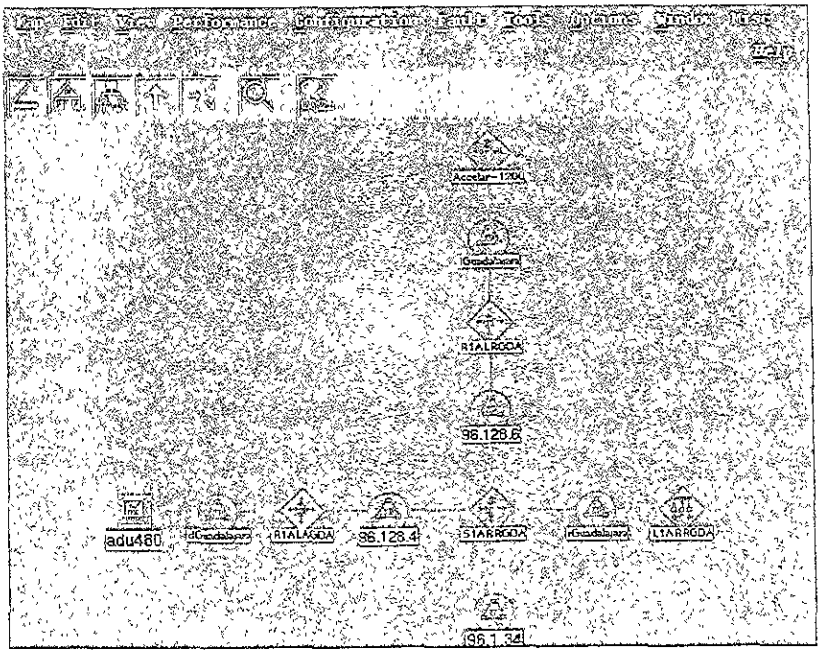


Figura 24. Visualización gráfica de componentes de red I

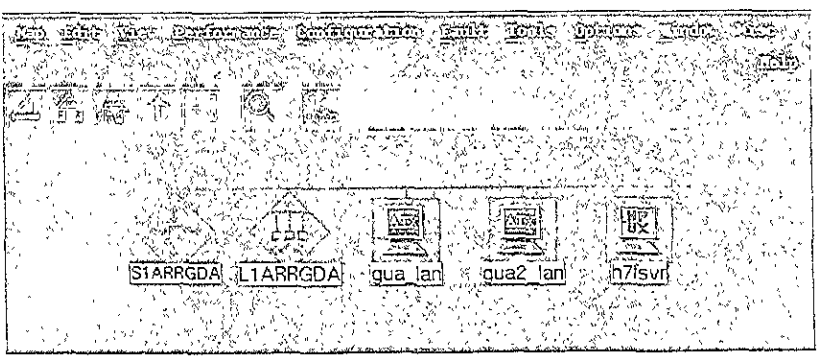


Figura 25. Visualización gráfica de componentes de red II

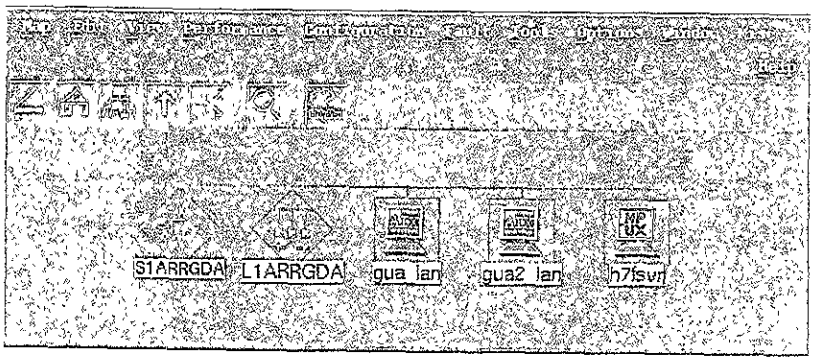


Figura 26. Visualización gráfica de componentes de red III

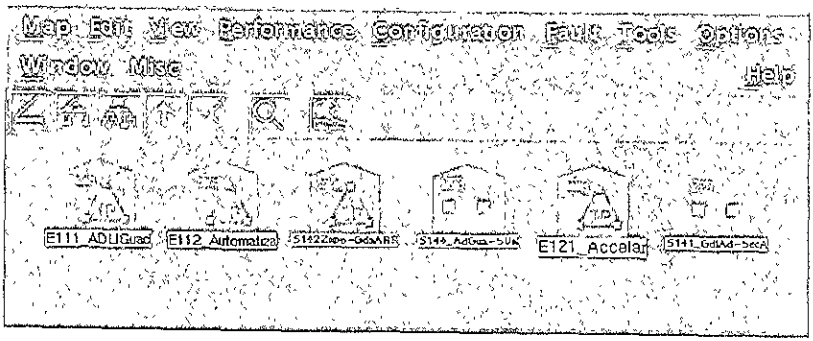


Figura 27 Visualización gráfica de componentes de red IV

5.2.2.3.- *Configuración del Agente SNMP*

La configuración del protocolo SNMP en la estación de administración de NNM se lleva a cabo desde la barra de menús Options → SNMP Configurations. La caja de diálogo aparece permitiéndonos cambiar los valores por default para los nombres de comunidades, poleos de intervalo, valores de timeout, agentes proxies y el número de reintentos en las operaciones de petición SNMP.

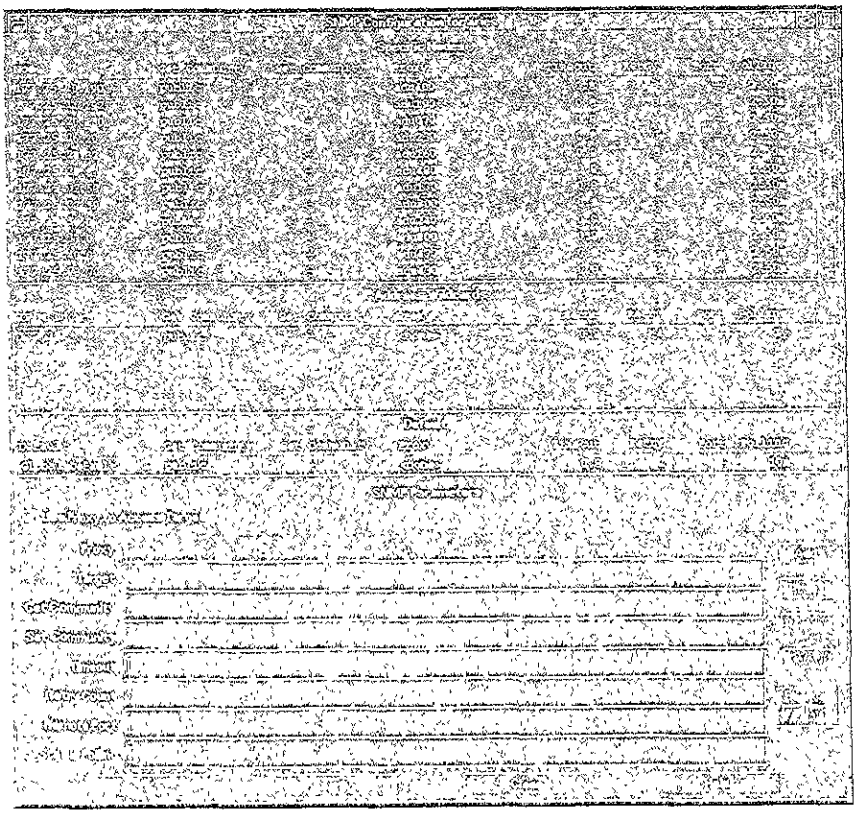


Figura 28 Configuración del agente SNMP en la Consola central

La figura anterior ejemplifica los valores proporcionados por la red en general, es decir por default. El administrador del sistema puede configurar para un nodo o para un grupo de nodos el uso de valores diferentes para los parámetros diferentes a los que otorga por default La configuración de un grupo de nodos se realiza a través de la utilización de caracteres comodín (*) en la asignación de direcciones IP

El agente SNMP que responde a las peticiones que se realizan con dicho protocolo está realmente a cargo del demonio /usr/sbin/snmpd cuando es

invocado, el demonio snmpd lee el archivo /etc/SnmpAgent.d/snmpd.conf para configurarse a sí mismo. Cualquier configuración del agente SNMP ocurre en este último archivo.

SNMP define comunidades para establecer una relación entre los agentes y una o más estaciones de administración. Sin embargo un nombre de comunidad ("Community Name") es únicamente una clave que habilita el acceso a las variables MIB en el agente; El uso de comunidades no es obligado, por ello se dice que el agente es llamado "public".

5.2.2.4.- Configuración de Expresiones MIB y Colecciones

Como parte de los requerimientos de diseño se debe llevar a cabo la colección de información histórica de instancias y componentes de red, para ello se configura la colección de expresiones MIB de manera continua a través del proceso snmpCollect.

Con la información colectada por una expresión MIB se pueden generar eventos basados en el valor de un objeto MIB, o basados en el valor de umbral pre-establecido que ha sido excedido, de ésta manera se pueden enviar mensajes a través de traps informando que se ha presentado un evento en la red.

El recolector de datos (Data Collector) es la herramienta de Open View usada para llevar a cabo las tareas de recolección de datos y almacenamiento, adicionalmente el colector de datos es usado para definir los valores de umbral a los que se sujetará el monitoreo de una instancia de objeto MIB, de manera que cuando este umbral sea rebasado se generará una alarma.

La definición de umbrales tiene como objetivo el definir valores límite determinados para una variable, los cuales pueden ser establecidos en una forma absoluta o porcentual, durante uno o más muestreos consecutivos; esto tiene lugar en las ventanas de diálogo de MIB Data Collection / Add Collection y Data Collection, para acceder a estos cuadros de diálogo se invoca desde la barra de herramientas Options → Data Collection & Threshold: SNMP desplegándose la siguiente figura.

En nuestro caso se definieron 4 grupos de expresiones MIB´s (Servidores HP, IBM, Bay Networks y Cisco) cada una identificadas a través de un prefijo que permite identificar a que grupo corresponden. Las expresiones son definidas en su mayoría a partir de variables MIB definidas dentro del grupo MIB2 que está constituido como estándar; Sin embargo para el caso de las expresiones MIB´s de los equipos Bay Networks se utilizaron variables MIB propietarias del Hardware.

Para cada una de las expresiones MIB´s descritas en el apartado 5.2.1.3 (Detalle de Solucion) se definió su correspondiente colección de datos

Las expresiones MIB definidas fueron agregadas en el archivo mibExpr.conf, del cual se presenta un extracto en el apartado de programas fuentes.

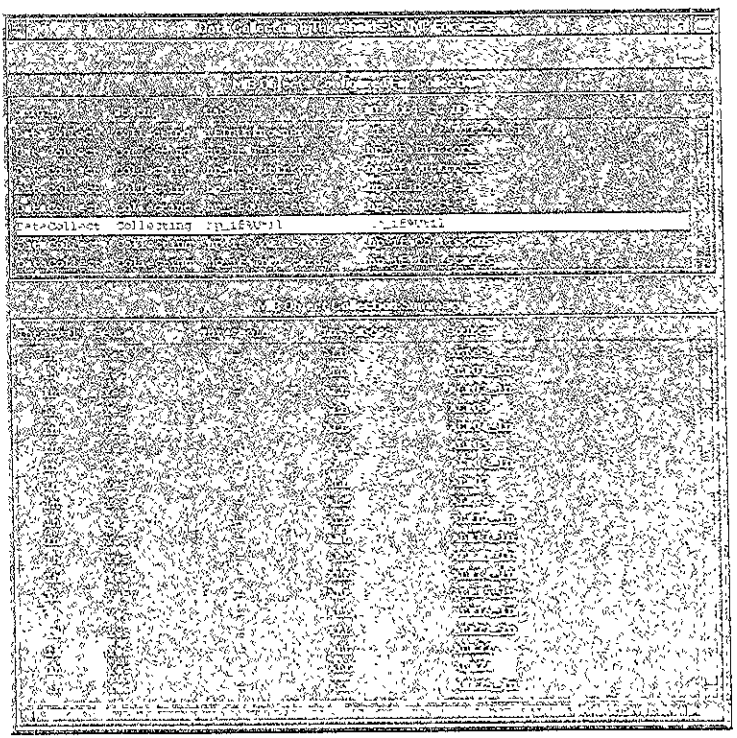


Figura 29 Ventana de configuración de colecciones MIB´s

5.2.2.5.- Configuración de Eventos de Notificación

La configuración de eventos dentro de HPNNM es una de las partes más importantes, ya que a partir de la colección de variables MIB´s y de sus umbrales definidos se debe asegurar la continuidad y disponibilidad del servicio cada vez que una interfaz, instancia o nodo de red envíen un trap o evento de alarma

Para cada uno de los eventos generados en el detalle de la solución del apartado 5.2.1.3 se definieron las siguientes características en su configuración:

- Nombre del evento
- ID específico
- Categoría
- Severidad
- Mensaje de Bitácora
- Mensaje de pantalla
- Comando y descripción

A continuación se describirán las políticas y lineamientos para la generación de los eventos configurados:

1. Definir un nombre significativo para el evento a generar, si el evento tiene relación con alguna recolección de datos el nombre debe ser un indicativo de dicha relación, de igual manera se definirá un nombre para el evento de regeneración.
2. Definir el tipo de trap genérico al cual corresponde este evento.
3. Definir un número de trap específico, este número debe corresponder con el número que se haya asignado dentro de la recolección de eventos.
4. Descripción de funcionalidad, objetivo y contenido del evento configurado
5. Definir las fuentes para las que se aplicará este evento.
6. Definir la categoría del evento a la cual se asignará el nuevo evento, se recomienda asignarlos a la categoría de eventos de umbral (Event Threshold).
7. Definir la severidad que tendrá dicho evento, las posibles opciones son: critical, major, minor, warning o normal
8. Definir el mensaje de bitácora que será mostrado en el Event Browser.
9. Definir un mensaje de ventana desplegable, en caso que se desee.
10. Definir algún comando adicional al detectarse el evento, por ejemplo: (Resetea la interfaz o reintenta establecer comunicación).
11. Definir si el evento debe ser avanzado hacia algún otro u otros nodos con capacidad de administración.

La configuración final de eventos para cada uno de los componentes de red, servidores e instancias se muestra en la siguiente tabla.

Servidores HP				
Evento	Problema	Nivel 1	Nivel 2	Severidad
nnm_000_if%InErrors	Redes	NNMGR	%inErrors: ZZ%. Interfaz: lan0'. El porcentaje de paquetes de entrada con error en la interfaz lan0' excedió el límite preestablecido del xx% durante yy muestreos consecutivos. Durante estos el valor maximo fue ZZ% el <date>	Warning
nnm_001_R_if%InErrors	Redes	NNMGR	Rearmado %inErrors ZZ% Interfaz: lan0' Umbral xx%.	NORMAL
nnm_002_if%OutErrors	Redes	NNMGR	%OutErrors zz% Interfaz lan0'. El porcentaje de paquetes de salida con error en la interfaz lan0' excedio el límite preestablecido del xx% durante yy muestreos consecutivos Durante estos el valor máximo fue ZZ% el <date>	Warning
nnm_003_R_if%OutErrors	Redes	NNMGR	Rearmado %OutErrors ZZ% Interfaz lan0' Umbral xx%	NORMAL
nnm_004_IfInOctets	Redes	NNMGR	InOctets, ZZ Interfaz. lan0' Umbral xx octetos El número total de octetos de entrada incluyendo los paquetes de framing excedió el límite preestablecido de xx octetos, durante yy muestreos consecutivos Durante estos el valor maximo fue ZZ octetos el <date>	Warning
nnm_005_R_IfInOctets	Redes	NNMGR	Rearmado IfInOctets ZZ Interfaz lan0' Umbral xx octetos	NORMAL
nnm_006_IfOutOctets	Redes	NNMGR	OutOctets ZZ Interfaz lan0' Umbral xx octetos El numero total de octetos de sal da incluyendo los paquetes de framing excedió el límite preestablecido de xx octetos, durante yy muestreos consecutivos Durante estos el valor maximo fue ZZ octetos el <date>	Warning
nnm_007_R_IfOutOctets	Redes	NNMGR	Rearmado IfOutOctets ZZ interfaz lan0' Umbral xx octetos	NORMAL

nnm_008_if%Util	Redes	NNMGR	%util: ZZ%. Interfaz: lan0[1]. Umbral xx% El porcentaje de utilización del canal en la interfaz lan0[1] excedió el límite preestablecido del xx% durante yy muestreos consecutivos. Durante estos el valor máximo fue ZZ% el <date>	Warning
nnm_009_R_if%Util	Redes	NNMGR	Rearmado If%Util ZZ%. Interfaz: lan0[1] Umbral: xx%	NORMAL
nnm_010_ifOperStatusDown	Redes	NNMGR	OperStatus. down. Interfaz: lan0[1]. El estado operativo de la interfaz lan0[1] esta down	CRITICAL
nnm_011_ifOperStatusTestin g	Redes	NNMGR	OperStatus: testing. Interfaz. lan0[1] El estado operativo de la interfaz lan0[1] es testing	CRITICAL
nnm_012_R_ifOperStatus	Redes	NNMGR	Rearmado del evento nnm_016_ifOperStatus	Normal
nnm_013_event_IntDown	Redes	NNMGR	Interfaz sin conectividad: lan0[1] Se perdió la conectividad hacia la interfaz lan0[1]	CRITICAL
nnm_014_event_IntUp	Redes	NNMGR	Se recupero la conectividad hacia la interfaz lan0[1]	Normal
nnm_015_ifNode_delete	Redes	NNMGR	Se borró el nodo <nodename> de la base de datos	CRITICAL
Nnm_016_procOVsPMD_do wn	procesos	NNMGR	El proceso OVsPMD en la consola central no se esta ejecutando.	CRITICAL
Nnm_017_procovwdb_down	procesos	NNMGR	El proceso ovwdb en la consola central no se esta ejecutando	CRITICAL
Nnm_018_procovtrapd_down	procesos	NNMGR	El proceso ovtrapd en la consola central no se esta ejecutando.	CRITICAL
Nnm_019_procovactiond_do wn	procesos	NNMGR	El proceso ovactiond en la consola central no se esta ejecutando.	CRITICAL
Nnm_020_procpmd_down	procesos	NNMGR	El proceso pmd en la consola central no se esta ejecutando	CRITICAL
Nnm_021_procsnmpCollect_ down	procesos	NNMGR	El proceso snmpCollect en la consola central no se esta ejecutando	CRITICAL
Nnm_022_procovrepld_down	procesos	NNMGR	El proceso ovrepld en la consola central no se esta ejecutando.	CRITICAL
Nnm_023_procovoacomm_do wn	procesos	NNMGR	El proceso ovoacomm en la consola central no se esta ejecutando	CRITICAL
Nnm_024_procopc_down	procesos	NNMGR	El proceso opc en la consola central no se esta ejecutando.	CRITICAL
Nnm_025_procOVLicenseMg r_down	procesos	NNMGR	El proceso OVLicenseMgr en la consola central no se esta ejecutando.	CRITICAL
Nnm_026_procovmon_down	procesos	NNMGR	El proceso ovmon en la consola central no se esta ejecutando	CRITICAL
Nnm_027_procovmmon_dow n	procesos	NNMGR	El proceso ovmmon en la consola central no se esta ejecutando	CRITICAL
Nnm_028_procnetmon_down	procesos	NNMGR	El proceso netmon en la consola central no se esta ejecutando	CRITICAL
Nnm_029_procovtopmd_dow n	procesos	NNMGR	El proceso ovtopmd en la consola central no se esta ejecutando.	CRITICAL
nnm_030_agentdown	redes	NNMGR	El agente snmp en el nodo <nodename> no esta ejecutándose[2].	CRITICAL
nnm_050_if%Collisions	Redes	NNMGR	%collisions: ZZ% Interfaz: lan0[1] Umbral xx%. El porcentaje de colisiones en la interfaz lan0[1] excedió el límite preestablecido del xx% durante yy muestreos consecutivos. Durante estos el valor máximo fue ZZ% el <date>	Warning
nnm_051_R_if%Collisions	Redes	NNMGR	Rearmado if%Collisios: ZZ%. Interfaz: lan0[1] Umbral: xx%.	NORMAL

Tabla 19 Eventos de notificaciones para servidores HP

Servidores IBM				
Evento	Problema	Nivel 1	Nivel 2	Severidad
nnm_100_if%InErrors	Redes	NNMGR	%inErrors ZZ%. Interfaz: lan0[1]. El porcentaje de paquetes de entrada con error en la interfaz lan0[1] excedió el límite preestablecido del xx% durante yy muestreos consecutivos. Durante estos el valor máximo fue ZZ% el <date>	Warning
nnm_101_R_if%InErrors	Redes	NNMGR	Rearmado %inErrors. ZZ%. Interfaz: lan0[1]. Umbral: xx%.	NORMAL
nnm_102_if%OutErrors	Redes	NNMGR	%OutErrors zz%. Interfaz: lan0[1]. El porcentaje de paquetes de salida con error en la interfaz lan0[1] excedió el límite preestablecido del xx% durante yy muestreos consecutivos Durante estos el valor máximo fue ZZ% el <date>	Warning
nnm_103_R_if%OutErrors	Redes	NNMGR	Rearmado %OutErrors: ZZ% Interfaz: lan0[1]. Umbral: xx%.	NORMAL
nnm_104_IfInOctets	Redes	NNMGR	ifInOctets: ZZ octetos. Interfaz: lan0[1] Umbral xx octetos El número total de octetos de entrada incluyendo los paquetes de framing excedió el límite preestablecido de xx octetos, durante yy muestreos consecutivos. Durante estos el valor máximo fue ZZ octetos el <date>	Warning
nnm_105_R_IfInOctets	Redes	NNMGR	Rearmado IfInOctets: ZZ. Interfaz: lan0[1]. Umbral xx octetos	NORMAL
nnm_106_IfOutOctets	Redes	NNMGR	ifOutOctets: ZZ. Interfaz: lan0[1]. Umbral xx octetos El número total de octetos de salida incluyendo los paquetes de framing excedió el límite preestablecido de xx octetos, durante yy muestreos consecutivos Durante estos el valor máximo fue ZZ el <date>	Warning
nnm_107_R_IfOutOctets	Redes	NNMGR	Rearmado IfOutOctets: ZZ. Interfaz: lan0[1]. Umbral xx octetos	NORMAL
nnm_108_if%Util	Redes	NNMGR	%util: ZZ%. Interfaz lan0[1] Umbral xx% El porcentaje de utilización del canal en la interfaz lan0[1] excedió el límite preestablecido del xx% durante yy muestreos consecutivos Durante estos el valor máximo fue ZZ% el <date>	Warning
nnm_109_R_if%Util	Redes	NNMGR	Rearmado if%Util ZZ%. Interfaz lan0[1]. Umbral xx%	NORMAL
nnm_110_ifOperStatusDown	Redes	NNMGR	OperStatus: down. Interfaz: lan0[1] El estado operativo de la interfaz lan0[1] esta down	CRITICAL
nnm_111_ifOperStatusTesting	Redes	NNMGR	OperStatus: testing. Interfaz: lan0[1]. El estado operativo de la interfaz lan0[1] es testing	CRITICAL
nnm_112_R_ifOperStatus	Redes	NNMGR	Rearmado ifOperStatus. El estado operacional de lan0[1] es OK.	Normal
nnm_113_event_IntDown	Redes	NNMGR	Interfaz sin conectividad: lan0[1]. Se perdió la conectividad hacia la interfaz lan0[1]	CRITICAL
nnm_114_event_IntUp	Redes	NNMGR	Se recupero la conectividad hacia la interfaz lan0[1]	Normal
nnm_115_ifNode_delete	Redes	NNMGR	Se borró el nodo <nodename> de la base de datos	CRITICAL
nnm_116_agentdown	Redes	NNMGR	El agente snmp en el nodo <nodename> no esta ejecutándose[2]	CRITICAL
nnm_150_if%Collisions	Redes	NNMGR	%collisions ZZ%. Interfaz. lan0[1]. El porcentaje de colisiones en la interfaz lan0[1] excedió el límite preestablecido del xx% durante yy muestreos consecutivos Durante estos el valor máximo fue ZZ% el <date>	Warning
nnm_151_R_if%Collisions	Redes	NNMGR	Rearmado if%Collisions ZZ% Interfaz lan0[1] Umbral xx%	NORMAL

Tabla 20. Eventos de notificación para servidores IBM

Dispositivos de red Bay Network				
Evento	Problema	Nivel 1	Nivel 2	Severidad
Nnm_500_if%InErrors	Redes	NNMGR	%inErrors: ZZ%. Interfaz: lan0[1] El porcentaje de paquetes de entrada con error en la interfaz lan0[1] excedió el límite preestablecido del xx% durante yy muestreos consecutivos. El valor máximo obtenido fue zz% en <date>	Warning
Nnm_501_R_if%InErrors	Redes	NNMGR	Rearmado %inErrors: ZZ%. Interfaz. lan0[1]. Umbral: xx%.	NORMAL
Nnm_502_if%OutErrors	Redes	NNMGR	%OutErrors: zz%. Interfaz: lan0[1]. Umbral: xx% El porcentaje de paquetes de salida con error en la interfaz lan0[1] excedió el límite preestablecido del xx% durante yy muestreos consecutivos Durante estos el valor máximo fue ZZ% el <date>	Warning
Nnm_503_R_if%OutErrors	Redes	NNMGR	Rearmado %OutErrors: ZZ%. Interfaz: lan0[1]. Umbral xx%.	NORMAL
Nnm_504_IfInOctets	Redes	NNMGR	ifInOctets: ZZ octetos Interfaz: lan0[1]. Umbral xx octetos El número total de octetos de entrada incluyendo los paquetes de framing excedió el límite preestablecido de xx octetos, durante yy muestreos consecutivos. Durante estos el valor máximo fue ZZ octetos el <date>	Warning
Nnm_505_R_IfInOctets	Redes	NNMGR	Rearmado IfInOctets: ZZ. Interfaz: lan0[1]. Umbral xx octetos	NORMAL
Nnm_506_IfOutOctets	Redes	NNMGR	ifOutOctets: ZZ octetos. Interfaz: lan0[1]. Umbral xx octetos. El número total de octetos de salida incluyendo los paquetes de framing excedió el límite preestablecido de xx octetos, durante yy muestreos consecutivos Durante estos el valor máximo fue ZZ el <date>	Warning
Nnm_507_R_IfOutOctets	Redes	NNMGR	Rearmado IfOutOctets. ZZ. Interfaz: lan0[1]. Umbral xx octetos	NORMAL
Nnm_508_if%Util	Redes	NNMGR	%util: ZZ%. Interfaz: lan0[1]. Umbral xx% El porcentaje de utilización del canal en la interfaz lan0[1] excedió el límite preestablecido del xx% durante yy muestreos consecutivos. Durante estos el valor máximo fue ZZ% el <date>	Warning
Nnm_509_R_if%Util	Redes	NNMGR	Rearmado if%Util: ZZ%. Interfaz. lan0[1] Umbral xx%	NORMAL
Nnm_510_ifOperStatusDown	Redes	NNMGR	OperStatus down. Interfaz: lan0[1]. El estado operativo de la interfaz lan0[1] esta down	CRITICAL
Nnm_511_ifOperStatusTesting	Redes	NNMGR	OperStatus: testing. Interfaz lan0[1]. El estado operativo de la interfaz lan0[1] esta testing	CRITICAL
Nnm_512_R_ifOperStatus	Redes	NNMGR	Rearmado ifOperStatus Ya se recupero el estado operativo de lan0[1]	Normal
Nnm_513_ip%ReasmOKs	Redes	NNMGR	ip%ReasmOKs: ZZ%. Interfaz lan0[1]. Umbral xx%. El porcentaje de datagramas reensamblados excedió el límite preestablecido del xx% durante yy muestreos consecutivos Durante estos el valor máximo fue ZZ% el <date>	Warning
Nnm_514_R_ip%ReasmOKs	Redes	NNMGR	Rearmado %ReasmOK. ZZ%. Interfaz lan0[1] Umbral xx%	NORMAL
Nnm_515_ip%NoRoutes	Redes	NNMGR	ip%NoRoutes: ZZ%. Interfaz: lan0[1]. El porcentaje de datagramas IP descartados excedió el límite preestablecido del xx% durante yy muestreos consecutivos Durante estos el valor máximo fue ZZ% el <date>	Warning
Nnm_516_R_ip%NoRoutes	Redes	NNMGR	Rearmado %NoRoutes ZZ%. Interfaz. lan0[1] Umbral xx%	NORMAL
Nnm_517_if%InDiscards	Redes	NNMGR	%InDiscards: ZZ%. Interfaz. lan0[1] Umbral xx%. El porcentaje de paquetes de entrada descartados en la interfaz lan0[1] excedió el límite preestablecido del xx% durante yy muestreos consecutivos Durante estos el valor máximo fue ZZ% el <date>	Warning
Nnm_518_R_if%InDiscards	Redes	NNMGR	Rearmado if%InDiscards ZZ% Interfaz lan0[1] Umbral xx%	NORMAL
Nnm_519_if%OutDiscards	Redes	NNMGR	%OutDiscards ZZ% Interfaz lan0[1] El porcentaje de paquetes de salida descartados en la interfaz lan0[1] excedió el límite preestablecido del xx% durante yy muestreos consecutivos Durante estos el valor máximo fue ZZ% el <date>	Warning

Nnm_520_R_if%OutDiscards	Redes	NNMGR	Rearmado %OutDiscards: ZZ% Interfaz: lan0[1] Umbral xx%	NORMAL
Nnm_521_event_IntDown	Redes	NNMGR	Interfaz sin conectividad: lan0[1] Se perdió la conectividad hacia la interfaz lan0[1]	CRITICAL
Nnm_522_event_IntUp	Redes	NNMGR	Se recupero la conectividad hacia la interfaz lan0[1]	Normal
Nnm_523_ifNode_delete	Redes	NNMGR	Se borró el nodo <nodename> de la base de datos	CRITICAL
Nnm_524_agentdown	Redes	NNMGR	El agente snmp en el nodo <nodename> no esta ejecutándose[2].	CRITICAL
Nnm_525_%CPU	Redes	NNMGR	%CPU. ZZ% CPU: vv El porcentaje de utilización de CPU excedió el límite preestablecido del xx% durante yy muestreos consecutivos. Durante estos el valor máximo fue ZZ% el <date>	
Nnm_526_R_%CPU	Redes	NNMGR	Rearmado %CPU: ZZ%. CPU: vv	
Nnm_527_%MEM	Redes	NNMGR	%MEM: ZZ%. El porcentaje de utilización de memoria excedió el límite preestablecido del xx% durante yy muestreos consecutivos. Durante estos el valor máximo fue ZZ% el <date>	
Nnm_528_R_%MEM	Redes	NNMGR	Rearmado %MEM: ZZ%. Umbral xx%.	
Nnm_600_%frError	Redes	NNMGR	%frError: ZZ%. Interfaz: lan0[1]. El porcentaje de errores en un circuito Frame Relay excedió el límite preestablecido del xx% durante yy muestreos consecutivos Durante estos el valor máximo fue ZZ% el <date>	Warning
Nnm_601_R_%frError	Redes	NNMGR	Rearmado %frError: ZZ%. Interfaz lan0[1]. Umbral xx%.	NORMAL
Nnm_640_if%Collisions	Redes	NNMGR	%collisions: ZZ%. Interfaz: lan0[1] Umbral xx%. El porcentaje de colisiones en la interfaz lan0[1] excedió el límite preestablecido del xx% durante yy muestreos consecutivos. Durante estos el valor máximo fue ZZ% el <date>	Warning
Nnm_641_R_if%Collisions	Redes	NNMGR	Rearmado if%Collisiones: ZZ%. Interfaz: lan0[1]. Umbral xx%	NORMAL

Tabla 21. Eventos de notificación para dispositivos By Networks.

Para verificar la correcta configuración de los eventos, es posible iniciar la ventana de configuración de eventos seleccionando el menú Options -> Event Configuration. Como resultado aparecerá la siguiente ventana.

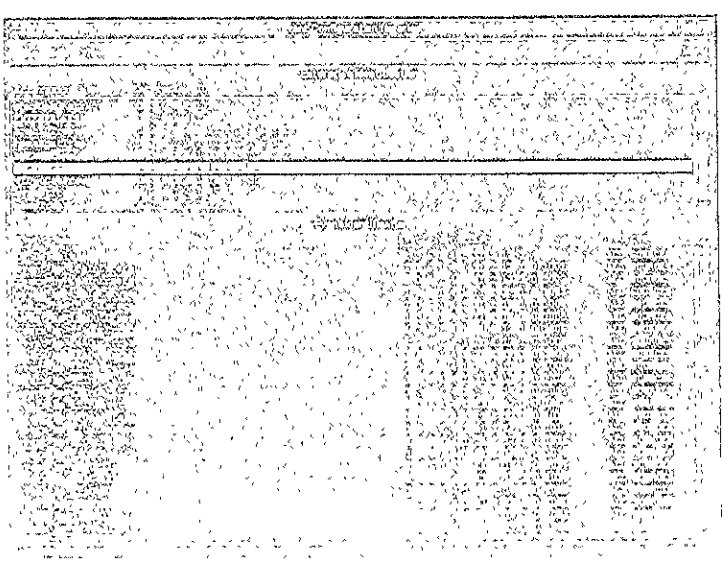


Figura 30. Ventana de configuración de eventos en NNM

5.2.2.6.- Configuración de Application Builder

Los application builder construidos fueron los 5 descritos en el detalle de la solución, para cada uno de ellos se diseño una gráfica la cual muestra el nombre de la interfaz correspondiente; Para cubrir este requerimiento fue necesario editar los archivos de configuración de los application builder y recompilarlos.

Los pasos a seguir para diseñar un application builder son:

1. Asegurarse de que el objeto a partir del cual va a crear su aplicación está cargado en la base de datos MIB
2. Asegurarse de entender el significado del objeto MIB que va a utilizar para construir su aplicación, ya que la mayoría de los fabricantes incluyen documentación de sus objetos MIB con sus productos.
3. Diseñar su aplicación, por ejemplo:

    - Cual(es) objeto(s) va a incluir en su aplicación
    - Cual(es) objeto(s) son sensibles de ser agrupados
    - Seleccionar la forma en que va a ser presentada la información (Texto, Tabla o Gráfica).

4. Planear la estructura de Menú que guardará su aplicación, es decir, la ubicación que tendrá dentro de los menús de HPNNM.
5. Proceder a construir su aplicación invocando el application builder a partir del menú Options → Application Builder:SNMP, desplegándose la ventana siguiente.

Figura 31 Ventana de configuración de Aplicaciones MIB

5.2.2.7.- Estructura de Datos Oracle

Una de las principales funcionalidades de HPNNM es que permite que los datos de topología de la red administrada sean almacenados en tablas de topología de la Base de Datos de Open View, es decir, la Base de Datos Oracle. El dimensionamiento y asignación de espacios de los tablespaces requeridos se determina de acuerdo a diferentes factores, tales como: el número de nodos de red administrados, número de instancias por nodo, número de objetos MIB colectados, intervalo de poleo, modo de transferencia de datos, número de días de almacenamiento de datos, etc. Con estos datos se proyecta el espacio requerido en disco para el almacenamiento de la información de datos, eventos y topología de la red de comunicaciones.

La asignación, creación y administración del espacio requerido por HPNNM no son actividades propias del Administrador de la Red, sino del DBA "Database Administrator" cuya principal función es mantener la integridad y disponibilidad de la información resguardada en la Base de Datos; Sin embargo y conservando la finalidad de las soluciones de Administración de Servicios de Tecnología de Información y tal y como se menciona en el apartado 5.2.2.1 tanto la Base de Datos y los Tablespaces requeridos por NNM son creados durante la instalación del IT/Operations con valores por default, por lo que es responsabilidad del DBA ajustarlos según los requerimientos.

HPNNM requiere de la creación de cuando menos 2 tablespaces para el almacenamiento de la topología de datos OV_DATA y OV_INDEX; Para nuestro caso y de acuerdo a los criterios descritos anteriormente se llegó a la conclusión de que dichos tablespaces fueran de 1 GB y 250 MB respectivamente, dicho cálculo se determina con la ayuda del script ovdbsetup proporcionado como parte de las herramientas del administrador de NNM y que se muestra en el apartado de programas fuente; Los comandos para la creación de los tablespaces en Oracle son sentencias básicas de SQL Oracle y son las siguientes:

```
SQL > CREATE TABLESPACE OV_DATA
      DATAFILE '/u03/oradata/openview/OV_DATA.dbf' size 1000M
      AUTOEXTEND ON NEXT 2M MAXSIZE 2000M
      DEFAULT STORAGE (INITIAL 2M NEXT 2M
      PCTINCREASE 0),

SQL > CREATE TABLESPACE OV_INDEX
      DATAFILE '/u02/oradata/openview/OV_INDEX.dbf' size 250M
      AUTOEXTEND ON NEXT 1M MAXSIZE 500M
      DEFAULT STORAGE (INITIAL 1M NEXT 1M
      PCTINCREASE 0),
```

Una vez creadas las estructuras de datos y topología en la Base de Datos se procede a la activación y configuración de los servicios de SQL Net para la Base de Datos Oracle for Open View procedimiento que consiste en editar los archivos

listener.ora y tnsnames.ora para indicar entre otras cosas: puertos de comunicaciones, protocolos, nombre del host donde reside la Base de Datos, etc., para la comunicación de los nodos administrados, NNM y la Base de Datos. Estos servicios de comunicaciones también deben darse de alta en algunos archivos de configuración del Sistema Operativo tales como el /etc/services, /etc/inetd.conf, etc.

Los archivos de configuración listener.ora y tnsnames.ora se muestran en el apartado de programas.

5.2.3.- Programas de Configuración

5.2.3.1.- Descubre Nodos

Filtro de descubrimiento Find_Nodes_SAT

```
//
// @(#)$OV_CONF/$LANG/filters
// @(#)HP OpenView NNM Release 6.10 Jan 21 2001
// $Revision: /main/TORNADO/NNM_NT/5
//

Sets {
}

Filters {
    Networks "Any network" { isNetwork }
    Segments "Any segment" { isSegment }
    Nodes "Any node" { isNode }
    Routers "Any Router" { isRouter }
    IPRouters "Any IP Router" { isIPRouter }
    Bridges "Any bridge" { isBridge }
    Hubs "Any multi-port repeater" { isHub }
    SNMPNode "Any node supporting SNMP" { isNode && isSNMPSupported }
    HPNodes "Hewlett-Packard nodes"
            { isNode && "SNMP sysObjectID" ~ " 1.3 6 1.4 1 11.*" }
    HPs700 "Hewlett Packard Workstations"
            { isNode && "SNMP sysObjectID" ~ ".1 3.6 1 4.1 11.2 3.2 5" }
    HPs800 "Hewlett Packard Servers"
            { isNode && "SNMP sysObjectID" ~ ".1 3 6.1 4.1 11 2 3 2.3" }
    BayNodes "Bay Networks nodes"
            { isNode && "SNMP sysObjectID" ~ ".1.3 6.1 4 1.18 *" }
    IBMServers "Servidores IBM"
            { isNode && "SNMP sysObjectID" ~ " 1 3 6.1 4 1.2 3 1 2.1 1.3" }
    NTServers "Servidor NT de GAVC"
            { "IP Address" ~ 99 90 128 227 }
}

FilterExpressions {
    SATNodes "Only the nodes of interest, servers, networks connectors"
            {( ( HPs700 || HPs800 ) && SNMPNode ) || BayNodes || IBMServers || NTServers }
            }
```

5.2.3.2.- Archivo Semilla

```
#-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
127 0 0 1      localhost
#-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
#Equipos ARIES
#Servidores
99 90 32 101  aries1                #Servidor primario de transmision TIVOLI
177 25 10 60  aries1_x25 #Servidor primario de transmision TIVOLI
99 90 32 102  aries2                #Servidor MESA de AYUDA ARS
99 90 32 103  openview   #Servidor secundario de Monitoreo de Comunicaciones NNM
99 90 32 104  lucero                #Servidor de pruebas HP9000-E25 (temporal) SCANDA
99 90 32 105  aries3                #Servidor de pruebas UX (E35)
99 90 32 106  aries4                #Servidor de pruebas UX (G??)
```

```
177.25.10 62  aries4_x25 #Servidor de pruebas UX (827)
99 90 32 107  aries              #Servidor primario de monitoreo (Direccion primaria)
99 90 36 80   aries_lan0 #Servidor primario de monitoreo (Dirección secundaria)
177.25.10.61  aries_x25  #Servidor primario de monitoreo
99 90 32.108  NT_ARIES #Servidor de pruebas NT
99 90.32.109  aries_nt    #Servidor de pruebas TIVOLI_NT
99 90.32.110  aries5             #Servidor de pruebas de la gerencia (antes E35 aries2)
99 90.32.168  openview_nt        #PC de pruebas con Windows NT Workstation
99 90.32.169  pruebas_nt#PC de pruebas con Windows NT Workstation
99.90 128 254 dis_apl            #Servidor secundario de Transmision (U6060)
#-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
#Xterminals
99.90 32.111  xterm1
99.90 32 112  xterm2
99 90 32.113  xterm3
99 90 32 114  xterm4
99 90 32 115  xterm5
99.90.32.116  xterm6
#-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
#Impresoras
99 90.32.130  deskjet
99 90.32.140  lexmark_bun
99.90.32.141  lexmark_of2
99.90.32.150  lexmark_ofi
#-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
#PC's
99.90.32.165  admaries5
99.90.32.238  admaries1
99.90 32.242  admaries3
99.90 32.244  admobi             #Equipo PC de Jaime Enrique Cabrera.
99.90 32.245  operadores
99.90 32.247  jsoto
99.90 32.249  Oparies_s
99 90.32.254  Oparies
#-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
#-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
#Equipos Aduanas
#-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
#Regional Cd Juarez
99 21.128.100 adu070_cl #Cd Juarez "CLUSTER"
99 21.128.105 adu070          #Cd. Juárez equipo "K"
99 21.128 106 adu070_c  #Cd Juarez equipo "D"
177.25 20 130 adu070_x25      #Cd. Juárez
99 27.128 100 adu250          #Ojinaga
177 25 27 42  adu250_x25      #Ojinaga
99 21 64.100  adu260          #Puerto Palomas
177 25 20 132 adu260_x25      #Puerto Palomas
99 20.128 100 adu460          #Torreon
177 25 22 16  adu460_x25      #Torreón
99 22.128.100 adu670          #Chihuahua
177 25 22 42  adu670_x25      #Chihuahua
#-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
#Regional Reynosa
99 33.128 100 adu170_cl #Matamoros "CLUSTER"
99 33.128 105 adu170          #Matamoros equipo "K"
99 33 128 106 adu170_c  #Matamoros equipo "D"
177 25 32 58  adu170_x25      #Matamoros
99 32.128 100 adu300_cl #Reynosa "CLUSTER"
99 32.128 105 adu300          #Reynosa equipo "K"
99 32.128 106 adu300_c  #Reynosa equipo "D"
177 25 32 59  adu300_x25      #Reynosa
99 33.64.100  adu340          #Cd. Miguel Aleman
177 25 32 63  adu340_x25      #Cd. Miguel Alemán
99 38 128 100 adu820          #Cd Camargo
177 25 32 71  adu820_x25      #Cd Camargo
#-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
#Regional Nogales
99 14 64 100  adu020          #Agua Prieta
177 25 26 32  adu020_x25      #Agua Prieta
99 10 128.100 adu120          #Guaymas
177 25 26.42  adu120_x25      #Guaymas
99 14 96 100  adu220          #Naco
177 25 26 30  adu220_x25      #Naco
99 14 128 100 adu230_cl #Nogales "CLUSTER"
99 14 128 105 adu230          #Nogales equipo "K"
99 14 128 106 adu230_c  #Nogales equipo "D"
177 25 26 20  adu230_x25      #Nogales
#-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
#Regional Nuevo Laredo
99 36 128 100 adu240_cl #Nuevo Laredo "CLUSTER"
99 36 128 105 adu240          #Nuevo Laredo equipo "K1"
99 36 128 106 adu240_c  #Nuevo Laredo equipo "K2"
```

```
177.25 36 0    adu240_x25             #Nuevo Laredo
99 24.128 100 adu270                  #Piedras Negras
177 25 22 51   adu270_x25             #Piedras Negras
99 24 64 100   adu440                 #Cd  Acuña
177.25.22 52   adu440_x25             #Cd. Acuña
99 30.128.100 adu520                  #Monterrey
177.25 24.30   adu520_x25             #Monterrey
99.37 64.100   adu800_cl #Colombia "CLUSTER"
99.37.64.105   adu800                 #Colombia equipo "K"
99 37.64.106   adu800_c  #Colombia equipo "D"
177 25 37.0    adu800_x25             #Colombia
#-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
#Regional Progreso
99 66 128.100 adu050                  #Subtte  López
177 25 34.68   adu050_x25             #Subtte  López
99.63 128.100 adu060                  #Cd  del Carmen
177 25 34.63   adu060_x25             #Cd. del Carmen
99 64.128 100 adu280                  #Progreso
177 25 34 64   adu280_x25             #Progreso
99 65.128.100 adu530                  #Cancún
177 25 34.65   adu530_x25             #Cancun
#-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
#Regional Tijuana
99.11 96.100   adu110                 #Ensenada
177.25 10.193 adu110_x25              #Ensenada
99 12.128.100 adu190_cl #Mexicali "CLUSTER"
99 12.128 105 adu190                  #Mexicali equipo "K"
99 12.128 106 adu190_c  #Mexicali equipo "D"
177.25.11.192 adu190_x25              #Mexicali
99.12 64 100   adu330                 #Sn  Luis Río Colorado
177.25.11.195 adu330_x25              #Sn  Luis Río Colorado.
99.11 64 100   adu390                 #Tecate
177.25 10.194 adu390_x25              #Tecate
99 11.128 100 adu400_cl #Tijuana "CLUSTER"
99 11.128 105 adu400                  #Tijuana equipo "K"
99 11.128 106 adu400_c  #Tijuana equipo "D"
177.25.10.190 adu400_x25              #Tijuana
99.18 128.100 adu500                  #Sonoyta
177.25.11.194 adu500_x25              #Sonoyta
#-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
#Regional Veracruz
99 76.128 100 adu080                  #Coatzacoalcos
177 25 32 35   adu080_x25             #Coatzacoalcos
99 60 128 100 adu310                  #Salina Cruz
177 25 34 8    adu310_x25             #Salina Cruz
99.34 128 100 adu380                  #Tampico
177.25 24.10   adu380_x25             #Tampico
99 73 128.100 adu420                  #Tuxpan
177 25 73.75   adu420_x25             #Tuxpan
99 75.128 100 adu430_cl #Veracruz
99 75.128.105 adu430                  #Veracruz equipo "K"
99.75 128 106 adu430_c  #Veracruz equipo "D"
177 25 73 70   adu430_x25             #Veracruz
99 35 128 100 adu810                  #Altamira Tmps
177 25 24 15   adu810_x25             #Altamira Tmps
#-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
#Regional Aeropuerto Cd  de Mexico
99 72 128.100 adu010                  #Acapulco
177 25 35.10   adu010_x25             #Acapulco
99 81 128 100 adu200                  #Pantaco
177 25 81 100 adu200_x25              #Pantaco
99 67 128 100 adu370                  #Cd  Hidalgo
177 25 34 67   adu370_x25             #Cd  Hidalgo
99 80 128.100 adu470_cl #Aeropuerto de La Cd  de Mexico
99 80 128.105 adu470                  #Aeropuerto de La Cd  de Mexico equipo "K"
99 80 128 106 adu470_c  #Aeropuerto de La Cd  de México equipo "D"
177 25 40 0    adu470_x25             #Aeropuerto Cd  de Mexico
99 56 128 100 adu510                  #Lazaro Cardenas
177 25 32 64   adu510_x25             #Lázaro Cárdenas
99 54 128 100 adu650                  #Toluca
177 25 20 12   adu650_x25             #Toluca
99 70 128 100 adu750                  #Puebla
177 75 32 70   adu750_x25             #Puebla
#-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
#Regional Guadalajara
99 13 128 100 adu140                  #La paz
177 25 26 10   adu140_x25             #La Paz
99 42 128 100 adu160_cl #Manzanillo "CLUSTER"
99 42 128 105 adu160                  #Manzanillo equipo "K"
99 42 128 106 adu160_c  #Manzanillo equipo "D"
177 25 28 32   adu160_x25             #Manzanillo
99 [illegible] 128 100 adu180         #[illegible]
```

```
177.25.25.15  adu180_x25          #Mazatlan
99.40.128.100 adu480_cl  #Guadalajara "CLUSTER"
99.40.128.105 adu480             #Guadalajara equipo "K"
99.40.128.106 adu480_c  #Guadalajara equipo "D"
177.25.28.8   adu480_x25          #Guadalajara
99.53.128.100 adu640              #Querétaro
177.25.30.15  adu640_x25          #Querétaro
99.43.128.100 adu730              #Aguascalientes
177.25.28.22  adu730_x25          #Aguascalientes
#-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
#Equipos Recaudación
#-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
#Regional Centro
#ARR
99.50.28.100  cel_lan             #Centro
177.25.30.0   cel_lan_x25         #Centro
99.50.28.105  cel2_lan    #Centro
#-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
#OCR
179.99.51.50  h6fsvr              #Centro Servidor Principal, linea 6
179.99.51.60  h6scan              #Centro Servidor del Scan 6
179.99.51.70  h6arch01  #Centro Servidor de Almacenamiento 6
179.99.51.51  h4fsvr              #Centro Servidor Principal, linea 4
179.99.52.60  h4scan              #Centro Servidor del Scan 4
#-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
#ALR's
99.50.24.100  ALR01_ln  #Celaya
177.25.30.1   ALR01_x25           #Celaya
99.51.24.100  ALR02_ln  #León
177.25.30.30  ALR02_x25           #Leon
99.52.24.100  ALR03_ln  #Morelia
177.25.30.31  ALR03_x25           #Morelia
99.53.24.100  ALR04_ln  #Querétaro
177.25.30.10  ALR04_x25           #Querétaro
99.55.24.100  ALR05_ln  #Pachuca
177.25.30.40  ALR05_x25           #Pachuca
99.54.24.100  ALR06_ln  #Sn  Luis Potosí
177.25.30.20  ALR06_x25           #Sn  Luis Potosi
99.56.24.100  ALR07_ln  #Irapuato
177.25.30.2   ALR07_x25           #Irapuato
99.57.24.100  ALR08_ln  #Uruapan
177.25.30.57  ALR08_x25           #Uruapan
#-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
#Regional Metropolitano
#ARR
99.85.28.100  met_lan             #Metropolitano
177.25.20.0   met_lan_x25         #Metropolitano
99.85.28.105  met2_lan   #Metropolitano
99.90.100.252 ALR96_ln  #Administración Especial de Recaudación (Paris No  15)
#-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
#OCR
179.99.87.161 hdfsvr              #Metropolitano Servidor Principal, linea d
179.99.80.151 hdscan              #Metropolitano Servidor del Scan d
179.99.88.161 hefsvr              #Metropolitano Servidor Principal, linea e
179.99.80.152 hescan              #Metropolitano Servidor del Scan e
179.99.89.161 hffsvr              #Metropolitano Servidor Principal, linea f
179.99.80.153 hfscan              #Metropolitano Servidor del Scan f
179.99.84.161 hgfsvr              #Metropolitano Servidor Principal, linea g
179.99.85.161 hhfsvr              #Metropolitano Servidor Principal, linea h
179.99.86.161 hifsvr              #Metropolitano Servidor Principal, linea i
179.99.80.70  h1arch01   #Metropolitano Servidor Almacenamiento 1
179.99.80.71  h1arch02   #Metropolitano Servidor Almacenamiento 2
179.99.80.101 h1nfs               #Metropolitano Servidor nfs 1
179.99.80.102 h2nfs               #Metropolitano Servidor nfs 2
179.99.80.103 h3nfs               #Metropolitano Servidor nfs 3
#-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
#Equipos de pruebas del proveedor UNISYS ubicados en CPM
99.85.28.35   unisys_lan #PRODUCCIÓN para pruebas UNISYS en CPM
99.85.28.37   unisys2_lan         #DUCTO para pruebas UNISYS en CPM
#-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
#ALR's
99.85.120.100 ALR11_ln  #Norte D F
177.25.20.40  ALR11_x25           #Norte D F
99.85.56.100  ALR12_ln  #Centro D F
177.25.20.60  ALR12_x25           #Centro D F
99.85.24.100  ALR13_ln  #Sur D F
177.25.20.50  ALR13_x25           #Sur D F
99.85.88.100  ALR14_ln  #Oriente D F
177.25.20.30  ALR14_x25           #Oriente D F
99.85.152.100 ALR15_ln  #Naucalpan
177.25.10.11  ALR15_x25           #Naucalpan
99.85.24.100  ALR16_ln  #Tol...
```

```
177 25 20.10  ALR16_x25             #Toluca
#-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
#Regional Golfo-Pacifico
#ARR
99 70 28.100  pue_lan               #Golfo-Pacifico
177.25 32.0   pue_lan_x25           #Golfo-Pacifico
99 70.28 105  pue2_lan  #Golfo-Pacifico
#-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
#OCR
179.99.71 50  h5fsvr                #Golfo-Pacifico Servidor Principal, linea 5
179.99.71.60  h5scan                #Golfo-Pacifico Servidor del Scan 5
179.99 71.70  h5arch01  #Golfo-Pacifico Servidor de Almacenamiento 5
179.99 71.51  hcfsvr                #Golfo-Pacifico Servidor Principal, línea c
179.99 72 60  hcscan                #Golfo-Pacifico Servidor del Scan c
#-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
#ALR's
99.70 24.100  ALR21_ln  #Puebla
177 25 32.1   ALR21_x25             #Puebla
99.77.24.100  ALR22_ln  #Tlaxcala
177 25 32.10  ALR22_x25             #Tlaxcala
99.70 56.100  ALR23_ln  #Puebla II
99.74.24.100  ALR24_ln  #Xalapa
177.25.32.20  ALR24_x25             #Xalapa
99 75.24.100  ALR25_ln  #Veracruz
177 25 32.75  ALR25_x25             #Veracruz
99.76.24.100  ALR26_ln  #Coatzacoalcos
177.25 32 30  ALR26_x25             #Coatzacoalcos
99.72 24.100  ALR27_ln  #Acapulco
177.25.32.72  ALR27_x25             #Acapulco
99.71.24.100  ALR28_ln  #Cuernavaca
177.25.20.20  ALR28_x25             #Cuernavaca
99.78.24.100  ALR29_ln  #Cordoba
177.25.32 78  ALR29_x25             #Córdoba
99.73 24.100  ALR30_ln  #Iguala
177.25 32.73  ALR30_x25             #Iguala
#-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
#Regional Noreste
#ARR
99.30 28.100  mon_lan               #Noreste
177.25.24 0   mon_lan_x25           #Noreste
99 30 28.105  mon2_lan  #Noreste
99.30.29.119  ALR95_ln  #Administración Especial de Recaudación MONTERREY
#-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
#OCR
179 99 31 50  h8fsvr                #Noreste Servidor Principal, linea 8
179 99 31 60  h8scan                #Noreste Servidor del Scan 8
179 99.31 70  h8arch01  #Noreste Servidor de Almacenamiento 8
179 99 31.51  h2fsvr                #Noreste Servidor Principal, línea 2
179 99 32 60  h2scan                #Noreste Servidor del Scan 2
#-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
#ALR's
99 30.24.100  ALR31_ln  #Guadalupe
177 25.24 25  ALR31_x25             #Guadalupe
99.32 24.100  ALR32_ln  #Reynosa
177 25 32 60  ALR32_x25             #Reynosa
99.34 24.100  ALR33_ln  #Tampico
177.25 24.11  ALR33_x25             #Tampico
99 35 24 100  ALR34_ln  #Tuxpan
177 25 24.20  ALR34_x25             #Tuxpan
99 30.88 100  ALR35_ln  #San Pedro
177 25 24 27  ALR35_x25             #San Pedro
99.30.56.100  ALR36_ln  #Monterrey
177 25 24 26  ALR36_x25             #Monterrey
99 36 24.100  ALR37_ln  #Nvo Laredo
177 25 36.1   ALR37_x25             #Nvo Laredo
99 33 24 100  ALR38_ln  #Matamoros
177 25 32 57  ALR38_x25             #Matamoros
99 31 24.100  ALR39_ln  #Cd. Victoria
177 25 32 61  ALR39_x25             #Cd_Victoria
#-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
#Regional Noroeste
#ARR
99 10 28 100  cob_lan               #Noroeste
177 25 26 0   cob_lan_x25           #Noroeste
99 10 28 105  cob2_lan  #Noroeste
#-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
#OCR
179 99 11 50  h9fsvr                #Noroeste Servidor Principal, linea 9
179 99 11 60  h9scan                #Noroeste Servidor del Scan 9
179 99 11 70  h9arch01  #Noroeste Servidor de Almacenamiento 9
179 99 11 51  h1fsvr                #Noroeste Servidor Principal, linea 1
179 99 12 60  h1scan                #Noroeste Servidor del Scan 1
```

```
#-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
#ALR's
99.11.24.100  ALR41_In  #Tijuana
177 25.10.191 ALR41_x25          #Tijuana
99.12 24.100  ALR42_In  #Mexicali
177 25.11.193 ALR42_x25          #Mexicali
99.13.24.100  ALR43_In  #La paz
177.25.26.14  ALR43_x25          #La paz
99.16.24.100  ALR44_In  #Culiacan
177 25.26.11  ALR44_x25          #Culiacan
99.10.24.100  ALR45_In  #Cd. Obregón
177.25.26.40  ALR45_x25          #Cd. Obregon
99.15.24.100  ALR46_In  #Hermosillo
177.25.26.50  ALR46_x25          #Hermosillo
99.11.88.100  ALR47_In  #Ensenada
177.25 10.192 ALR47_x25          #Ensenada
99.18.24 100  ALR48_In  #Los Mochis
177.25.26.18  ALR48_x25          #Los Mochis
99.17.24.100  ALR49_In  #Mazatlán
177.25.26.12  ALR49_x25          #Mazatlan
99.14.24.100  ALR50_In  #Nogales
177.25.26.21  ALR50_x25          #Nogales
#-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
#Regional Note-Centro
#ARR
99.20.28.100  tor_lan            #Norte-Centro
177.25.22.0   tor_lan_x25        #Norte-Centro
99.20.28.105  tor2_lan  #Norte-Centro
#-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
#OCR
179.99.21 50  hafsvr             #Norte-Centro Servidor Principal, línea a
179 99.21.60  hascan             #Norte-Centro Servidor del Scan a
179.99.21.70  haarch01  #Norte-Centro Servidor de Almacenamiento a
179.99.21.233 haedit13  #Norte-Centro Estacion de edición
179.99.21.243 haedit23  #Norte-Centro Estación de edición
179.99.21.245 haedit25  #Norte-Centro Estación de edición
179.99.21.51  hjfsvr             #Norte-Centro Servidor Principal, línea j
179 99.22 60  hjscan             #Norte-Centro Servidor del Scan j
#-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
#ALR's
99 20 24.100  ALR51_In  #Torreon
177.25 22.11  ALR51_x25          #Torreon
99.23.24.100  ALR52_In  #Saltillo
177.25 22 30  ALR52_x25          #Saltillo
99 21.24 100  ALR53_In  #Cd  Juárez
177.25.22.60  ALR53_x25          #Cd  Juárez
99 22 24.100  ALR54_In  #Chihuahua
177.25.22.40  ALR54_x25          #Chihuahua
99 25 24.100  ALR55_In  #Durango
177.25 22.20  ALR55_x25          #Durango
99 26 24 100  ALR56_In  #Zacatecas
177 25.22 10  ALR56_x25          #Zacatecas
99.24.24 100  ALR57_In  #Piedras Negras
177.25.22.50  ALR57_x25          #Piedras negras
#-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
#-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
#Regional Occidente
#ARR
99 40 28.100  gua_lan            #Occidente
177 25 28 0   gua_lan_x25        #Occidente
99 40.28 105  gua2_lan  #Occidente
99 40 24 119  ALR94_In  #Administracion Especial de Recaudacion GUADALAJARA
#-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
#-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
#OCR
179.99 41 50  h7fsvr             #Occidente Servidor Principal, línea 7
179 99 41 60  h7scan             #Occidente Servidor del Scan 7
179 99 41 70  h7arch01  #Occidente Servidor de Almacenamiento 7
179 99 41 51  h3fsvr             #Occidente Servidor Principal, linea 3
179 99 42 60  h3scan             #Occidente Servidor del Scan 3
#-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
#ALR's
99 43 24 100  ALR61_In  #Aguascalientes
177 25 28 20  ALR61_x25          #Aguascalientes
99 42 24 100  ALR62_In  #Colima
177 25 28 30  ALR62_x25          #Colima
99 40 24 100  ALR63_In  #Guadalajara
177 25 28 2   ALR63_x25          #Guadalajara
99 41 24 100  ALR64_In  #Tepic
177 25 28 10  ALR64_x25          #Tepic
99 44 24 100  ALR65_In  #Cd Guzman
177 25 28 4   ALR65_x25          #Cd Guzman
```

```
99 40.56.100  ALR66_In  #Tlaquepaque
177.25 28 3   ALR66_x25          #Tlaquepaque
99.40 88 100  ALR67_In  #Zapopan
177.25.28.1   ALR67_x25          #Zapopan
99 45 24 100  ALR68_In  #Pto Vallarta
177 25.28 5   ALR68_x25          #Pto. vallarta
#-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
#Regional Sur
#ARR
99.60 28.100  oax_lan            #Sur
177 25.34.0   oax_lan_x25        #Sur
99 60 28.105  oax2_lan  #Sur
#-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
#OCR
179 99 61.50  hbfsvr             #Sur Servidor Principal, linea b
179 99.61 60  hbscan             #Sur Servidor del Scan b
179.99.61 70  hbarch01  #Sur Servidor de Almacenamiento b
179.99.61 51  hkfsvr             #Sur Servidor Principal, línea k
179.99 62 60  hkscan             #Sur Servidor del Scan k
#-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
#ALR's
99.60 24 100  ALR71_In  #Oaxaca
177.25.34.1   ALR71_x25          #Oaxaca
99 63 24 100  ALR72_In  #Campeche
177.25 34.30  ALR72_x25          #Campeche
99 65.24.100  ALR73_In  #Cancún
177.25 34.10  ALR73_x25          #Cancún
99.61.24 100  ALR74_In  #Villahermosa
177 25.34 40  ALR74_x25          #Villahermosa
99 64.24.100  ALR75_In  #Merida
177.25.34 50  ALR75_x25          #Mérida
99 62 24.100  ALR76_In  #Tuxtla
177 25 34.20  ALR76_x25          #Tuxtla
99 66.24 100  ALR77_In  #Chetumal
177.25 34.60  ALR77_x25          #Chetumal
99.67.24.100  ALR78_In  #Tapachula
177.25.34.70  ALR78_x25          #Tapachula
#-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
#-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
#RUTEADORES
#
# Region Noroeste
#
99.11.128.1   S1ALATIJ
99 11.12 1    L1ALRTIJ
96.34 1 1     S1ALRTIJ
96.35 5 2     R1SECTIJ
96 32.1 1     S1ARROBR
99 10 16.1    L1ARROBR
99 16.12.1    R1ALRCUL
97 39.1 2     R1ALJCUL
99 18 16 2    R1ALJMOC
99 18 24 1    R1ALRMOC
96 32 6 2     R1ALAGUA
96 33 1 1     S1ALRHER
99.15 12.1    L1ALRHER
96.36 1 1     S1ALANOG
99 14 16 1    R1ALRNOG
96 37 1 1     S1ALRMAZ
96 33 4 2     R1ALASON
97 36 1 2     R1GARSON
99 12 160 1   R1ALASLC
99 12 128 1   R1ALAMEX
97 34 3 2     R1ALFMEX
99.18 16 1    L1ALJMOC
99 12 20.1    R1ALRMEX
97 34 4 2     R1SECMEX
99 11 64 1    R1ALATEC
96 35 2 2     R1ALRENS
97 32 4 1     R1ALAENS
97 32 3 2     R1ALFENS
97 32 1 2     R1ALJENS
99 14 96 1    R1ALANAC
99 16 32 1    R1ALAAGU
#
# Region Norte Centro
#
99 21 128 1   S1ALAJUA
96 165 1 1    S1ALRCHI
99 22 12 1    L1ALRCHI
96 161 1 1    S1ARRTOR
99 20 180 1   L1ARRTOR
```

```
96.164.6.2     R1ALRZAC
97.164 1.2     R1ALFZAC
96.165 5.2     R1ALACHI
96.164.3.2     R1ALRDUR
99.25.16.1     L1ALRDUR
99 21.24.1     S1ALRJUA
99 21.96.1     R1ALAZAR
101 24.128 2   R1ALAPIE
99 24.128 1    L1ALAPIE
97.96.15.2     R1ALAACU
99.21.64.1     R1SECJUA
#
# Región Noreste
#
96.96.16.1     S1ARRMTY
99.30.16.1     L1ARRMTY
96.96.12.2     R1ALRMTY
99.30.56.1     L1ALRMTY
96.96.13.2     R1ALAMTY
96.96.15 2     R2ALAMTY
99.32.24 2     R1ALRREY
99.32 20.1     L1ALRREY
96.97.2.2      S1ALAMAT
96.97.10 2     S1ALACMO
99.39.32.1     R1ALAALE
99 33.24.1     R1ALRMAT
96.98.11.2     R1ALFMAT
96.99.11.1     S1ALATAM
96.99.2.2      R1ALRTAM
99.34.20 1     L1ALRTAM
96 98.11.2     S1ALRVIC
99 31 24.1     L1ALRVIC
99 37 32 1     R1ALACLB
96 97 1.1      R1ALRLAR
99 36 24 1     L1ALRLAR
97 96 11 1     R1ALALAR
99 30 68 2     R1ALRSPE
99 30 84 1     L1ALRSPE
96 99.10.2     R1ALAALT
#
# Región Occidente
#
96 128 1 1     S1ARRGDA
99 40 156.1    L1ARRGDA
99 40 88 1     R1ALRZAP
99 40 48 1     R1ALFGDA
96 128 4 2     R1ALAGDA
96 128 6 2     R1ALRGDA
96 128 7.2     R2ALRGDA
96 128 8.2     R1ALRPVA
99 45 24.1     L1ALRPVA
97.128 1.1     R1ALRCOL
96.128 10 2    R1ALRGUZ
99.44.20.1     R1ALJGUZ
99 42 128 1    R1ALAMAN
96 128 2.2     R1ALRAGS
99 43 20 1     L1ALRAGS
99 43 128 1    R1ALAAGS
#
# Región Centro
#
97 160 2 2     R1ALRURU
99 54 24 1     L1ALRSLP
96 160 8 2     S1ALRSLP
99 52 24 1     L1ALRMOR
96 160 7 2     S1ALRMOR
99 50 20.1     L1ARRCEL
96 160 1 1     S1ARRCEL
99 51 20 1     L1ALRLEO
99 51 24 2     S1ALRLEO
97 160 4 2     R1ALALEO
96 161 1 1     S1ALRQUE
99 53 12 1     L1ALRQUE
97 161 1 1     S1ALAQUE
96 160 5 2     R1ALALCA
#
# Region Sur
#
96 194 10 1    S1ARROAX
96 194 5 2     S1ARJOAX
96 194 6 2     S2ARROAX
96 194 7 2     S1ALROAX
```

```
99 60.12.1      S2ALRAMA
99 60.156 1     R1ARROAX
96 195.1 1      S1ALRTGZ
99 62.20.1      L1ALRTGZ
97 195 1 1      S1ALRTAP
96.192 4 1      S1ALRVHM
99.61.24.1      L1ALRVHM
96.193 1.1      S1ALRMER
99.64.20.1      L1ALRMER
97 192.1.1      S1ALRCUN
99 65.12.1      L1ALRCUN
99 66.24.2      R1ALRCHE
99 66.24.1      L1ALRCHE
101.65.128.2    R1ALACUN
99.60.128 1     R1ALASCZ
101.63 128.2    R1ALACAR
97.192 2.1      R1ALRCAM
97 192 2.2      R1ALFCAM
#
# Region Golfo Pacifico
#
96.227.2.2      S1ALFCUE
99 71 24 1      S1ALRCUE
99.72.24.2      S1ALRACA
97.224.1.1      R1ALRACA
99.72.24 1      L1ALRACA
99.73.20.1      R1ALRIGU
96.227 4.2      R1ALFIGU
96.224 10 1     S1ARRPUE
99.70.28.1      L1ARRPUE
99.70.32.1      S1ALAPUE
96.224 6.2      R1ALJPUE
97 224 3.1      S1ALRTLA
101 72.128.2    R1ALFTLA
99 77 20.1      R1ALJTLA
96 225.1.1      S1ALRVER
96 225.7.2      S1ALFVER
96 225 5.2      S1ARAVER
99 75 20 1      S1ALJVER
99 74.24.2      R1ALRJAL
99.74.24 1      L1ALRJAL
99 78.20.1      R1ALRCOR
99 76 32.1      S1ALACOA
96 226.1.1      S1ALRCOA
99.76 20.1      L1ALRCOA
#
# Region Metropolitana
#
99.85.120.2     R1ALRNTE
99.85.108.1     L1ALRNTE
99 85.88.2      R1ALROTE
99 85 84.1      L1ALROTE
99 80.128 1     R1ALAAPT
99 80 128.1     L1ALAAPT
99 92 172.1     R1ALRSIN

96 2 1 1        S1CH
96 1 100 7      S2CH
99 97 240 1     R1CAB
96 1 49 2       R1ALRTOL
99 86 24 1      L1ALRTOL
99 87 24 1      R1ALRNAU
99 87 24 1      L1ALRNAU
96 1.3 2        S1ARRMET
96 1 35.1       Switch_CPN
96 3 3 1        S2ARRMET
99 85.168 1     L1ARRMET
96 1 51.2       R1PARIS
96 1 8 1        S1CPN
99 90 48 1      R1CPN
96 1 22 2       R2CPNPPI
99 85 56.2      R1ALRCEN
99 85 48 1      L1ALRCEN
96 2 40 2       R1ALAPAN
96 2 3 2        R1LIV
96 2 4 2        R1CJA
96 1 23 2       R2CH
//+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
//SE ESTAN CAMBIANDO LOS NOMBRES, ACTUALIZARLOS CONFORME LOS VAYAN REPORTANDO
"+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
99 99 100 1.70 CPN
96 6 240 2      Pa
```

```
96 1 30.2      BANCEN
96 1 30.2      BANCEN_SWFR
96 0 240.4     Aero_DF
96.0.240 5     Oriente_AL
96.0.240 6     Norte_AL
96.0 240.7     Centro_DF
96 0.240 8     Toluca_AL
96 0.240 9     Naucalpan_ALR
#+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
#+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
96.0.247.3     Acapulco_AL
96.0.247.1     Puebla_ADU
96.224.1.2     Puebla_ALRF_
96.1 4.2       Puebla_ALRF
96.224.2.2     Veracruz_ALR
96 225.2.2     Coatzacoalcos_AL
96.0 247.2     Veracruz_ADU
#+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
96.194.1.4     Oaxaca_AL
96.1 8.2       Oaxaca_ALAR
96 0 246.2     Oaxaca_ALJI
96.0.246 3     Oaxaca_ARR
96 0.246.4     Oaxaca_ALAF
96.194.2.2     TuxtlaG_AL
96.192.4.1     Villahermosa_AL
96.192.3.2     Merida_AL
96 0 246.1     Cancun_AL
#+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
96 164.3.1     Torreon_AL
96 165.5.1     Chihuahua_AL
96 0.242 1     Chihuahua_ADU
96 166.3 1     CdJuarez_ADU
96 0.242 3     Zaragoza_ADU
#+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
101 17.128.2   Mazatlan_ADU
96 32 3.1      Cd.Obregon_AL
96 33 4.1      Hermosillo_AL
99 14 128.1    Nogales_ADU
96 0.242 4     Nogales_AL
96 0 241.3     Sonoyta_ADU
97 34 3.1      Mexicali_ADU
97 33.1.1      Tecate_ADU
96 35.1.4      Tijuana_ADU
96 0.241 6     Aero_Tijuana
#+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
96 0 245.1     Queretaro_ADU
96 0.245.2     Leon_AL
96.0.245.3     SLP_AL
96.160 8.1     Celaya_AL_
#+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
96 96 2 1      Monterrey_SWARR
96.97 11.1     Reynosa_ADU
97 96.3 2      NvoLaredo_ADU
97 96 2 2      Colombia
97 96.4 2      Monterrey_ADU
97 96.5.2      Monterrey_ALR
96 0 243 3     SnPedro_AL
97 99 2 2      Tampico_ALR
97 97.2 2      Reynosa_ALR
#+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
96 128.6 1     Guadalajara_SWARR
96 0 244 1     GuadaCen_ALR
96.0 244.3     Tlaquepaque_ALR
96 0 244 6     Aguascalientes_ADU
#+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
#+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
#AQUI ACABAN LOS RUTEADORES
#+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
#Idiomatre
#+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
#Equipos de produccion
#+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
99 35 28 37    cel2_con   #IBM G40 de Contingencia en ARR Metro
99 60 28 35    oax2_con   #IBM G40 de Contingencia en ARR Oaxaca
99 70 28 35    pue2_con   #IBM G40 de Contingencia en ARR Puebla
#+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
99 90 100 236 cpnk1                  #HP-9000 K580 CLUSTER CPN maquina 1
99 90 100 237 cpnk2                  #HP-9000 K580 CLUSTER CPN maquina 2
99 90 100 238 cpnk3                  #HP-9000 K580 CLUSTER CPN maquina 3
#+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
#+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
99 90 100 47 [illegible]
```

```
99.90.128 80  ibmver         #Servidor Administracion Versiones ARR (Mensajes instalacion paquetes)
99.90.128 82  cvaduana  #Servidor Administracion Versiones Aduanas (Mensajes instalacion paquetes)
99 90 128 227 dccs_nt        #Servidor Administracion Versiones NT
99.90 24 235  entidad        #Servidor de Desarrollo para Aduanas (SICOCA)
99 90.128.82  lab_entidad    #Servidor de Laboratorio para Aduanas (SICOCA)
#-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
148.250.88.2  cpndecel  #Declaraciones Electronicas por Internet
#-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
#-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
#Fin de equipos de produccion (detectados como de . )
#-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
177.25.10.0   hp890_x25
177.25.10 13  aaa001         #Validador AMIA
177.25.10.16  hp845
177.25.10 18  hp847
177 25.10 20  DGR
177.25.10 21  DGR1
177.25.10.22  SSI
177.25 10.23  CGA
177.25 10 24  DTI
177.25.10.26  DPI
177.25.10.27  DPIHP
177.25.10.28  DPE
177.25.10.29  CEIE
177.25.10.30  DGF
177.25.10.31  DGFHP
177.25.10 32  CEF
177.25.10 33  SOPTEC_OLI
177.25 10 34  SCG_PW
177 25 10 35  amiares
177.25.10 36  scg
177.25.10 37  CI_PW
177.25 10.40  DPEHP
177.25.10.45  sst01_x25
177.25.10.49  hpcitev_x25    #HP de Control de Internacion Temporal de
177.25.10 50  GAT832
#-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
177.25.15 0   HPDGR
177.25.15.10  DGE_10
177.25.15 12  DTI1
#-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
177.25 38 0   DICG
#-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
177.25 95 10  DGR2
#-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
177.25 240 1  roudgp1        #router cpn
#-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
99.90 8.107   optivity
99 90.8.211   SHCP
99 95.124.115 hp845
99 95.124.116 shcp827r
#-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
#Segmento 99.90.100 Administado por GAT
99 90.100 63  sso1020
99 90.100 66  hpgatk
99 90 100 207 DARIO1
99 90 100 202 DARIO2
99 90 100 123 dario5
99 90 100 125   gat_lan      #Servidor de pruebas Apoyo Tecnico
99 90 100 126   gat2_lan     #Servidor de pruebas Apoyo Técnico
99 90 100 241 hp890
99 90 100.242 shcp870
99 90 100 244 hp847
99.90.100.245 shcp857
99 90.100.246 shcpf30
99 90.100.250 hpcitev        #HP de Control de Internacion Temporal de
99.90.100.254 hpk460         #Servidor de Balanza Comercial en Bunker C P N
#-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
#Segmento 99.90 128 Administrado por LABORATORIO
99 90 128 62  avc_nt         #Servidor NT de Administración de Versiones
99 90 128 84  cvsir05        #Equipo de control de versiones para SIR
99 90 128 178 adu2000        #Equipo de pruebas de integracion de versiones

99 11 128 50  aries_tj
99 90 204 71  AT_UX071 #Equipo de pruebas HP 400 de la GAT

#Equipos de Respaldos
99 90 100 248 armemexrsp cpn df cu armemexrsp      #Cell Manager Proyecto Respaldos Nt
99 90 100 249 cpn_cs         #CELL SERVER Proyecto de Respaldos verificar con Jaime E Cabrera
99 32 128 118 su herexrsp reynosa tamaulipas cu #Cell Server Reynosa
99 64 24 118  sumeridir p merida yucatan cu     #Cell Server Merida
```

```
"Porcentaje utilizado del ancho de banda del canal disponible para\n\
la interfaz. La interfaz fue definida para equipos Hewlett Packard.\n\
El resultado fue calculado a partir de \n\
   (Received byte rate + transmitted byte rate) * 8\n\
   ------------------------------------------------\n\
              interface link speed\n\
then converted to a percentage."\
    .1.3 6.1 2 1 2 2.1 10 \
    .1.3 6.1 2 1.2 2 1 16 \
    + 8 * \
    .1 3.6.1.2 1.2 2 1 5 \
    / 100 *

hp_if%Collisions \
"Porcentaje de paquetes que colisionaron para la interfaz. La\n\
expresión fue definida para equipos Hewlett Packard.\n\
El resultado es calculado a partir de:\n\
   (collision rate/packets transmitted rate)\n\
then converted to a percentage " \
    .1.3 6.1 4 1.11 2 4.1.1 1.6 \
    .1 3 6.1 4.1.11.2.4.1.1.1.2. \
    / 100 *

hp_if%InDiscards \
"Porcentaje de paquetes de entrada dirigidos a esta interfaz\n\
en específico, que son descartados por causa diferentes a un error.\n\
La expresión fue definida para equipos Hewlett Packard."\
     1.3 6.1.2.1.2 2.1 13 \
    .1.3 6.1.2 1.2 2.1 11 \
    .1.3 6.1.2 1.2.2.1 12. \
    + / 100 *

hp_if%OutDiscards \
"Porcentaje de paquetes de salida de la interfaz que seran\n\
descartados por causas diferentes a errores La expresión fue\n\
definida para equipos Hewlett Packard "\
     1.3 6.1.2 1.2 2.1.19. \
     1.3 6.1.2.1.2.2.1 11 \
     1.3 6.1 2 1.2.2 1.12 \
     + / 100 *

hp_ifOperStatus \
"Estado operativo de la interfaz. La expresión fue definida\n\
para equipos Hewlett Packard."\
    .1 3.6 1.2.1 2.2.1 8. \
     1 *

hp_PktsIn_Out \
"Relación entre los paquetes de entrada y salida de una interfaz.\n\
Un valor mayor de 1 indica que la interfaz recibe mayor número de\n\
paquetes de entrada que paquetes de salida y menor que 1 en caso\n\
contrario La expresión fue definida para equipos Hewlett Packard "\
     1 3 6 1 2 1.2.2 1.10. \
     1 3 6 1 2 1.2.2 1.16. /

hp_ifInOctets \
"Número de paquetes de entrada en la interfaz La expresion\n\
fue definida para equipos Hewlett Packard."\
     1 3 6 1 2 1 2 2 1.10

hp_ifOutOctets \
"Número de paquetes de salida en la interfaz. La expresión\n\
fue definida para equipos Hewlett Packard "\
     1.3 6.1.2 1.2 2 1 16

hp_snmpdStatus \
"Estatus del agente SNMP en equipos Hewlett Packard."\
     1 3 6 1 4 1 11 2 13 2 6

##########################################################################
#
# Las siguientes expresiones MIB fueron definidas para los
# equipos IBM
#
##########################################################################

ibm_if%InErrors \
"Porcentaje de paquetes de entrada que son recibidos con error\n\
en la interfaz. Expresión definida para equipos IBM.\n\
El resultado es calculado por:\n\
   (Paquetes recibidos con error/Total de paquetes recibidos)\n\
convertido a porcentaje."\
```

```
    1.3.6.1.2.1.2.2.1.14. \
    1.3.6.1.2.1.2.2.1.11. \
    1.3.6.1.2.1.2.2.1.12. \
    + / 100 *

ibm_if%OutErrors \
" Porcentaje de paquetes de salida con error en la interfaz.\n\
La expresion fue definida para equipos IBM.\n\
El resultado es calculado por\n\
   (Paquetes que salieron con error/Número total de paquetes)\n\
convertidos a porcentaje " \
    .1.3.6.1.2.1.2.2.1.20. \
    .1.3.6.1.2.1.2.2.1.17. \
    1.3.6.1.2.1.2.2.1.18. \
    + / 100 *

ibm_ip%ReasmOKs \
"Porcentaje de datagramas que son reensamblados exitosamente en\n\
nodo y que pasaran a capas superiores  La expresión fue definida\n\
para equipos IBM."\
    1.3.6.1.2.1.4.15. \
    .1.3.6.1.2.1.4.9. \
    1.3.6.1.2.1.4.8. \
    1.3.6.1.2.1.4.7. \
    + + / 100 *

ibm_ip%NoRoutes \
"Porcentaje de datagramas descartados porque no pudo ser encontrada\n\
la ruta a donde deben ser transmitidos  La expresion fue definida\n\
para equipos IBM."\
    1.3.6.1.2.1.4.12. \
    1.3.6.1.2.1.4.10. \
    1.3.6.1.2.1.4.6. \
    + / 100 *

ibm_if%Util \
"Porcentaje utilizado del ancho de banda del canal disponible para\n\
la interfaz  La interfaz fue definida para equipos IBM.\n\
El resultado fue calculado a partir de.\n\
   (Received byte rate + transmitted byte rate) * 8\n\
   ------------------------------------------\n\
                interface link speed\n\
then converted to a percentage "\
    1.3.6.1.2.1.2.2.1.10. \
    1.3.6.1.2.1.2.2.1.16. \
    + 8 * \
    .1.3.6.1.2.1.2.2.1.5. \
    / 100 *

ibm_if%Collisions \
"Porcentaje de paquetes que colisionaron para la interfaz  La\n\
expresion fue definida para equipos IBM.\n\
El resultado es calculado a partir de.\n\
   (collision rate/packets transmitted rate)\n\
then converted to a percentage " \
    1.3.6.1.4.1.11.2.4.1.1.1.5. \
    1.3.6.1.4.1.11.2.4.1.1.1.2. \
    / 100 *

ibm_if%InDiscards \
"Porcentaje de paquetes de entrada dirigidos a esta interfaz\n\
en especifico, que son descartados por causa diferentes a un error.\n\
La expresion fue definida para equipos IBM."\
    .1.3.6.1.2.1.2.2.1.13. \
    1.3.6.1.2.1.2.2.1.11. \
    1.3.6.1.2.1.2.2.1.12. \
    + / 100 *

ibm_if%OutDiscards \
"Porcentaje de paquetes de salida de la interfaz que seran\n\
descartados por causas diferentes a errores  La expresion fue\n\
definida para equipos IBM."\
    1.3.6.1.2.1.2.2.1.19. \
    1.3.6.1.2.1.2.2.1.11. \
    1.3.6.1.2.1.2.2.1.12. \
    + / 100 *

ibm_if%OperStatus \
"Estado operativo de la interfaz  La expresion fue definida\n\
para equipos IBM."\
    1.3.6.1.2.1.2.2.1.8. \
```

```
ibm_PktsIn_Out \
"Relacion entre los paquetes de entrada y salida de una interfaz.\n\
Un valor mayor de 1 indica que la interfaz recibe mayor número de\n\
paquetes de entrada que paquetes de salida y menor que 1 en caso\n\
contrario. La expresión fue definida para equipos IBM "\
    .1.3.6.1.2.1.2.2.1.10. \
    .1.3.6.1.2.1.2.2.1.16. /

ibm_ifInOctets \
"Número de paquetes de entrada en la interfaz  La expresión\n\
fue definida para equipos Hewlett Packard."\
    .1.3.6.1.2.1.2.2.1.10.

ibm_ifOutOctets \
"Número de paquetes de salida en la interfaz. La expresión\n\
fue definida para equipos Hewlett Packard "\
    .1.3.6.1.2.1.2.2.1.16.

ibm_snmpdStatus \
"Estatus del agente SNMP en equipos IBM."\
    .1.3.6.1.4.1.11.2.13.2.6

###############################################################
#
# Las siguientes expresiones MIB fueron definidas para los
# equipos Bay Networks.
#
###############################################################

bay_if%InErrors \
"Porcentaje de paquetes de entrada que son recibidos con error\n\
en la interfaz. Expresión definida para equipos Bay Networks.\n\
El resultado es calculado por.\n\
    (Paquetes recibidos con error/Total de paquetes recibidos)\n\
convertido a porcentaje." \
    .1.3.6.1.2.1.2.2.1.14. \
    .1.3.6.1.2.1.2.2.1.11  \
    .1.3.6.1.2.1.2.2.1.12  \
    + / 100 *

bay_if%OutErrors \
" Porcentaje de paquetes de salida con error en la interfaz \n\
La expresion fue definida para equipos Bay Networks \n\
El resultado es calculado por\n\
    (Paquetes que salieron con error/Número total de paquetes)\n\
convertidos a porcentaje." \
    .1.3.6.1.2.1.2.2.1.20  \
    .1.3.6.1.2.1.2.2.1.17  \
    .1.3.6.1.2.1.2.2.1.18  \
    + / 100 *

bay_ip%ReasmOKs \
"Porcentaje de datagramas que son reensamblados exitosamente el\n\
nodo y que pasaran a capas superiores  La expresion fue definida\n\
para equipos Bay Networks "\
    1.3.6.1.2.1.4.15  \
    .1.3.6.1.2.1.4.9. \
    1.3.6.1.2.1.4.8  \
    1.3.6.1.2.1.4.7  \
    + + / 100 *

bay_ip%NoRoutes \
"Porcentaje de datagramas descartados porque no pudo ser encontrada\n\
la ruta a donde deben ser transmitidos  La expresion fue definida\n\
para equipos Bay Networks "\
    1.3.6.1.2.1.4.12  \
    1.3.6.1.2.1.4.10  \
    1.3.6.1.2.1.4.6. \
    + / 100 *

bay_if%Util \
"Porcentaje utilizado del ancho de banda del canal disponible para\n\
la interfaz  La interfaz fue definida para equipos Bay Networks. \n\
El resultado fue calculado a partir de \n\
    (Received byte rate + transmitted byte rate) * 8\n\
    ---------------------------------------- x\n\
                interface link speed\n\
then converted to a percentage "\
    1.3.6.1.2.1.2.2.1.10  \
    1.3.6.1.2.1.2.2.1.16  \
    + 8 *
```

```
   1 3 6 1.2 1 2.2.1.5. \
   / 100 *

bay_if%Collisions \
"Porcentaje de paquetes que colisionaron para la interfaz. La\n\
expresion fue definida para equipos Bay Networks.\n\
El resultado es calculado a partir de.\n\
   (collision rate/packets transmitted rate)\n\
then converted to a percentage " \
   .1.3.6 1.4.1.11.2.4.1 1.1.6. \
   1 3 6.1 4.1.11.2.4.1.1 1 2. \
   / 100 *


bay_if%InDiscards \
"Porcentaje de paquetes de entrada dirigidos a esta interfaz\n\
en especifico, que son descartados por causa diferentes a un error.\n\
La expresión fue definida para equipos Bay Networks "\
   1.3 6 1 2.1.2.2.1.13. \
   .1.3.6.1.2 1 2.2 1.11 \
   .1.3 6 1.2.1 2.2.1 12. \
   ÷ / 100 *

bay_if%OutDiscards \
"Porcentaje de paquetes de salida de la interfaz que seran\n\
descartados por causas diferentes a errores. La expresion fue\n\
definida para equipos Bay Networks."\
   .1.3.6.1.2 1.2.2.1 19. \
   1 3 6.1 2.1.2.2 1.11. \
   .1.3.6.1 2 1.2.2.1 12 \
   + / 100 *

bay_ifOperStatus \
"Estado operativo de la interfaz. La expresión fue definida\n\
para equipos Bay Networks "\
   .1.3 6.1.2 1.2.2.1 8 \
   1 *


bay_PktsIn_Out \
"Relación entre los paquetes de entrada y salida de una interfaz.\n\
Un valor mayor de 1 indica que la interfaz recibe mayor número de\n\
paquetes de entrada que paquetes de salida y menor que 1 en caso\n\
contrario. La expresión fue definida para equipos Bay Networks."\
   1 3 6 1.2 1.2.2.1.10 \
   1 3 6.1.2.1.2.2 1.16. /

bay_ifInOctets \
"Número de paquetes de entrada en la interfaz  La expresión\n\
fue definida para equipos Hewlett Packard "\
   1.3 6 1 2 1.2.2 1.10

bay_ifOutOctets \
"Numero de paquetes de salida en la interfaz. La expresion\n\
fue definida para equipos Hewlett Packard."\
   1 3 6 1 2 1 2 2 1 16

bay_snmpdStatus \
"Estatus del agente SNMP en equipos Bay Networks "\
   .1 3 6.1 4 1 11.2 13 2 6

bay_fr%Errors \
"Porcentaje de frames recibidos en un circuito FrameRelay para\n\
ser avanzados y que indican congestion. esta expresion fue\n\
definida para router's BayNetworks. La expresión fue definida\n\
como \n\
   (WfFrCircuitReceivedFECNs + WfFrCircuitReceivedBECNs) * 100\n\
   ──────────────────────────────────────────\n\
            WfFrCircuitReceivedFrames ÷ 1"\
   1 3 6 1 4.1 18 3 5 9 9 2 1 8 \
   1 3 6 1 4 1 18 3 5 9 9 2 1 9 \
   + \
   1 3 6 1 4 1 18 3 5 9 9 2 1 12 \
   1 \
   + / 100 *

bay_PoreCPURout \
"Porcentaje de utilización de CPU en router, BayNetworks.
\
Computed by
\
   (Total Cpu Used) * 100
```

```
  ---------------
\
      TotalCpuMax
\
then converted to a percentage "\
    .1 3 6 1.4 1.18 3.3.2 5 7 1 2  \
     1.3 6.1 4.1.18 3 3 2.5 7.1.4  \
    / 100 *


bay_PorcMEMRout \
"Porcentaje de utilización de Memoria en routers BayNetworks
\
Computed by:
\
    (TotalMemUsed) * 100
\
   ---------------
\
       TotalMemMax
\
then converted to a percentage."\
     1.3 6.1.4.1.18.3.3.2.5.7 1.5. \
     .1 3 6.1 4.1 18 3 3.2 5.7.1.7  \
     / 100 *

bay_DLCiUtil \
"Porcentaje de utilización por DLCI
\
Computed by:
\
    (wfFrCircuitSentOctets + wfFrCircuitReceivedOctets) * 8
\
    ------------------------------------
\
                Ancho de Banda CIR
\
then converted to a percentage "\
     .1 3.6.1 4 1.18 3.5 9.9.2 1 11. \
     .1.3 6 1.4.1.18.3 5 9 9.2.1.13. \
     + 8 * \
     1048576 / 100 *

### Fin de las expresiones MIB

##############################################################################
#
# Below are some expressions which are valid on any agent which
# supports the hp-unix MIB
#
##############################################################################

Disk%util \
"Percentage of disk utilization, as reported by bdf,\n\
(blocks - free) / (blocks - free + avail)" \
                                1 3 6 1 4 1.11 2 3 1 2 2.1 4  \
                                1 3 6 1 4 1 11 2 3 1 2 2 1.5  - \
                                1.3 6 1 4 1 11 2 3 1.2 2 1 4  \
                                1 3 6 1.4 1 11 2.3.1 2.2.1 5  - \
                                1 3 6 1 4 1 11 2 3.1 2 2 1 6. + / 100 *

##############################################################################
#
# Below are some expressions which are only valid when using the
# HP extensible agent.  To enable them if you do have the HP
# extensible agent, remote the leading comment character (#)
# before the expression
#
##############################################################################

#EA_ProcSize \
#"Only obtainable when using the HP Extensible Agent \n\
#This is the size (in ps(1) or monitor(1m) units of\n\
#4 Kbyte pages or blocks) of the core image of process,\n\
#as reported by the HP Extensible Agent \n\
#This expression is only available on nodes which\n\
#have the HP Extensible Agent software running \n\
#This expression is calculated by\n\
#adding (data size + text size + stack size)" \
#                               1 3 6 1 4 1 11 2 3 1 4 2 1 5  \
#                               1 3 6 1 4   11 2 3 1 1 2 1 6   \
```

```
#                                1 3 6 1 4 1 11 2 3.1.4 2 1 7 +


#EA_negFreeMem \
#"Only obtainable when using the HP Extensible Agent \n\
#This is the number of Bytes of free memory left on the\n\
#system times -1.  This allows a threshold to be set when\n\
#the amount of free memory drops below a threshold.\n\

#For example, if you want a threshold to be generated\n\
#when you have less than 1000 bytes, set the data\n\
#collector threshold to be generated when it exceeds a\n\
#value of -1000 (i.e., 1000 * -1)."\
#                                .1 3 6 1.4 1.11 2.3.1.1.7 0 -1 *

#EA_negFreeSwap \
#"Only obtainable when using the HP Extensible Agent \n\
#This is the number of Bytes of free swap left on the\n\
#system times -1.  This allows a threshold to be set when\n\
#the amount of free swap drops below a threshold.\n\
#For example, if you want a threshold to be generated\n\
#when you have less than 10000 bytes, set the data\n\
#collector threshold to be generated when it exceeds a\n\
#value of -10000 (i e , 10000 * -1)."\
#                                1 3 6.1.4 1.11.2.3.1 1.12 0 -1 *

#EA_swapUsed \
#"Only obtainable when using the HP Extensible Agent.\n\
#This is the number of bytes of swap utilized on the\n\
#system"\
# 1.3 6 1.4 1 11 2 3.1.1.11.0 .1.3.6 1.4 1.11.2 3 1.1 12 0 -

#EA_%swapUsed \
#"Only obtainable when using the HP Extensible Agent.\n\
#This is the percent of swap utilized on the system"\
# 1.3 6 1 4.1 11 2 3 1.1 11 0  1 3 6 1 4 1 11 2.3 1.1.12 0 - \
#          .1 3 6.1.4 1.11.2.3 1.1.11 0 /

#EA_memUsed \
#"Only obtainable when using the HP Extensible Agent \n\
#This is the number of bytes of memory utilized on the\n\
#system"\
#.1.3.6.1.4 1.11.2.3.1.1.9 0  1 3 6 1.4 1 11 2 3.1 1 7.0 -

#EA_%memUsed \
#"Only obtainable when using the HP Extensible Agent \n\
#This is the number of free bytes of memory utilized on the\n\
#system divided by memory available to user"\
#.1 3 6.1.4 1 11.2.3 1 1 9 0  1 3 6 1 4 1 11 2 3 1 1 7 0 - \
# 1 3 6 1 4 1 11 2 3 1 1 9 0 /

##########################################################################

#
# EXPRESIONES AGREGADAS
#

PorcCPURout \
"Porcentaje de utilizacion de CPU en routers BayNetworks
\
Computed by
\
   (TotalCpuUsed) * 100
\
   ---------------
\
       TotalCpuMax
\
then converted to a percentage "\
    1 3 6 1 4 1 18 3 3 2 5 7 1 2  \
    1 3 6 1 4 1 18 3 3 2 5 7 1 4  \
   / 100 *


PorcMEMRout \
"Porcentaje de utilizacion de Memoria en routers BayNetworks
\
Computed by
\
   (TotalMemUsed) * 100
```

```
-------------------
\
      TotalMemMax
\
then converted to a percentage."\
   .1 3.6 1.4 1.18.3 3.2 5 7.1 5 \
    1.3 6.1 4.1.18 3 3 2.5 7 1.7 \
   / 100 *

DLCIUtil \
"Porcentaje de utilización por DLCI
\
Computed by:
\
   (wfFrCircuitSentOctets + wfFrCircuitReceivedOctets) * 8
\
   ------------------------------------------------
\
              Ancho de Banda CIR
\
then converted to a percentage."\
   .1 3.6.1.4.1.18 3 5.9.9.2.1.11. \
    1.3.6.1.4 1.18.3.5 9 9.2 1.13 \
   + 8 * \
   1048576 / 100 *
```

5.2.3.4.- Tablespaces Oracle

Listado de programa ovdbsetup para el cálculo de tablespaces

```
aries:/opt/OV/bin # ./ovdbsetupo sh
Entering Phase 3 (ovdbsetupo sh)

Will you export topology data into
the Oracle openview database (y/n) ? [y]
n
Will your installation export snmp trend
(data collector) data in the Oracle database (y/n) ?[n]
y

Answers to the following questions will be used to estimate
RDBMS disk requirements for NNM SNMP Data Collector data
Default answers are provided within []'s  If necessary,
allocations may be altered later using mechanisms provided
by Oracle.  See the "Oracle Server Administrator's Guide"
for details.

If at any point, you wish to abort this program
(perhaps to research your data collection needs),
simply press Ctrl-C

On how many nodes (approximately) will you be collecting SNMP data?  [300]


How many MIB objects (average) will you be collecting per node?  [20]


On how many instances per node (average) will you be collecting data?  [10]


Will you be exporting this data in raw or reduced form? (raw/red) [red]


What reduction interval, in minutes, will be used?  [240]


How long will reduced data reside in Oracle before being deleted (days)?  [30]
15

Disk space to be allocated for data collector data

      Data tablespace   1024 MB
      Index tablespace   256 MB
      Temporary tablespace   100 MB

Do you wish to revisit the data collection questions? (y n)
n
Enter password for Oracle user ovdb [ovdb]
[illegible]
```

```
spool file is  /u01/home/oracle/admin/openview/create/crdbov3 lst
Oracle configuration for Network Node Manager completed
Using existing /etc/listener ora
Using existing /etc/tnsnames ora
Using existing /etc/sqlnet ora

LSNRCTL for HPUX  Version 8 0 5 0 0 - Production on 24-AUG-99 18:12 42

TNS-01106  Listener using listener name LISTENER has already been started
Regenerating libclntsh sl for Oracle 8
Building client shared library libclntsh.so ...
Call script /u01/home/oracle/product/8 0.5/bin/genclntsh
        /u01/home/oracle/product/8 0 5/bin/genclntsh
ld: Can't create /u01/home/oracle/product/8 0 5/lib/libclntsh sl 1 0
ld  Text file busy
Built /u01/home/oracle/product/8 0 5/lib/libclntsh.so . . DONE
Validate User/password in oracle database

Connecting as user "ovdb" with password
Validate accessability to "OVoracle" database

Changing Data Warehouse configuration to use oracle
Validate ovdw configuration using ovdbcheck
Connecting as user "ovdb" with password
Validate accessability to "OVoracle" database

Creating tables
Disabling embedded database

ovdbsetupo sh phase for NNM configuration completed
```

5.2.3.5.- *Servicios SQL Net*

Listado de archivos listener.ora y tnsnames.ora

```
############
# FILENAME: listener.ora
# DATE  .: Jan 7 2001
# NETWORK.: openview
# NODE  .: Server
# SERVICE.: LISTENER
############

LISTENER =
  (ADDRESS_LIST =
      (ADDRESS=
        (PROTOCOL=IPC)
        (KEY= openview)
      )
      (ADDRESS =
        (PROTOCOL = TCP)
        (HOST = aries)
        (PORT = 1521)
      )
      (ADDRESS =
        (PROTOCOL = TCP)
        (HOST = aries)
        (PORT = 1526)
      )
  )

STARTUP_WAIT_TIME_LISTENER = 0
CONNECT_TIMEOUT_LISTENER = 10

SID_LIST_LISTENER =
  (SID_LIST =
    (SID_DESC =
      (SID_NAME=openview)
      (GLOBAL_DBNAME= openview.listener)
      (ORACLE_HOME=/u01/home/oracle/product/8 0 5)
    )
  )

LOG_DIRECTORY_LISTENER  /u01/home/oracle/product/8 0 5/network/log
LOG_FILE_LISTENER = listener

TRACE_LEVEL_LISTENER  OFF
```

```
############
# FILENAME. tnsnames ora
# DATE.. .: Jan 7 2001
# NETWORK : openview
# NODE ...: Client
# SERVICE.: C_OPENVIEW_COMMUNITY
############

tcp.loopback.world =
 (DESCRIPTION =
    (ADDRESS_LIST =
     (ADDRESS =
      (COMMUNITY = ov_net)
      (PROTOCOL = TCP)
      (HOST = anes)
      (PORT = 1521)
     )
    )
  (CONNECT_DATA = (SID = openview))

    (ADDRESS_LIST =
     (ADDRESS =
      (COMMUNITY = ov_net)
      (PROTOCOL = TCP)
      (HOST = anes)
      (PORT = 1526)
     )
    )
  (CONNECT_DATA = (SID = openview))
 )

ov_net =
 (DESCRIPTION =
    (ADDRESS_LIST =
     (ADDRESS =  (PROTOCOL = IPC)(KEY =openview))
     (ADDRESS =
      (COMMUNITY = OPENVIEW_COMMUNITY)
      (PROTOCOL = TCP)
      (HOST = anes)
      (PORT = 1521)
     )
    )

    (CONNECT_DATA = (SID = openview))
    (ADDRESS_LIST =
     (ADDRESS =
      (COMMUNITY = ov_net)
      (PROTOCOL = TCP)
      (HOST = anes)
      (PORT = 1526)
     )
    )

    (CONNECT_DATA = (SID = openview))
 )

test world =
 (DESCRIPTION =
    (ADDRESS_LIST =
     (ADDRESS =
      (COMMUNITY = ov_net)
      (PROTOCOL = TCP)
      (HOST = anes)
      (PORT = 1521)
     )
    )
    (CONNECT_DATA = (SID = openview))
 )
```

6.- Presentación y Discusión de Resultados

6.1.- Pruebas de Laboratorio

Una vez desarrollada y construida la solución de Redes y Sistemas bajo un ambiente de operación controlado y de acuerdo a los requerimientos planteados, se procede con la etapa de pruebas de laboratorio que garantice la integridad del ambiente operativo una vez implantada y puesta en marcha la solución.

Las pruebas de laboratorio se llevaron a cabo dentro de las instalaciones del Laboratorio de Calidad de Sistemas, donde se contaron con replicas de los ambientes operativos de producción, tanto a nivel software base como aplicativos, ambientes de comunicaciones, accesos a bases de datos y simulación de rendimiento de los servidores prueba en cuestión; Los ambientes de operación replicados en el laboratorio fueron:

- La Aduana Marítima del Puerto de Veracruz con un esquema de alta disponibilidad a través de 2 servidores HP9000 k460.
- La Administración Regional Golfo-Pacífico con esquema de alta disponibilidad soportada por 2 servidores IBM RS6000 H50.
- La Administración Local de San Pedro Garza García de Nuevo León Mty. Con un servidor HP9000 D370 con configuración Standalone.

La selección de estos ambientes de prueba se debe a que de acuerdo a las características operativas de la zona geográfica donde se encuentran, resultan los más representativos debido a los volúmenes de operaciones que se manejan, así como la flexibilidad de su ambientación dentro de un ambiente de pruebas, pues si bien no son los más robustos tecnológicamente hablando, si representan un alto grado de confiabilidad para las pruebas de calidad requeridas.

Dentro del checklist de pruebas que se aplicaron a la solución de Redes y Sistemas se encuentran entre otras.

- Pruebas de instalación, donde se revisaron todos los aspectos relativos a la ambientación requerida para la instalación de los productos, activación de servicios, modificación de archivos de configuración, espacios en File System, etc.
- Pruebas de funcionalidad, donde se superviso no tanto la funcionalidad de la solución de Redes y Sistemas, si no más bien la funcionalidad de los aplicativos, los sistemas y las bases de datos de los equipos de producción, cuidando primordialmente no impactar con su funcionamiento al momento de activar los agentes de monitoreo
- Pruebas de Volumen y Rendimiento, donde además de checar la saturación de los recursos del sistema operativo y las bases de datos también se auditó la saturación del tráfico en la red de datos al momento de activar la colección y replica de los agentes, durante estas pruebas se interrumpió de manera

intencional la comunicación entre las consolas de monitoreo y los servidores vigilados, con la intención de checar el comportamiento de los servicios activos por la solución, así como la notificación de alarmas de perdidas de enlace y conectividad.

- Pruebas de Seguridad, donde se inspeccionaron todos los aspectos relativos a la seguridad lógica de la Solución, desde permisos y privilegios de usuarios hasta intentos de violaciones a través de las consolas gráficas de monitoreo.
- Y finalmente se llevaron a cabo pruebas integrales durante las cuales los servidores de prueba simularon operar bajo condiciones reales; Estas pruebas se llevaron a cabo durante 24 Hrs. durante las cuales no se presentó ningún incidente relevante que afectará la continuidad de los servicios brindados, estas pruebas marcaron ciertos indicios de la necesidad de afinación de algunos umbrales de monitoreo, principalmente del sistema operativo, afinación que se tendría que llevar a cabo durante la activación de cada uno de los agentes sobre los servidores de producción.

Una vez concluidas satisfactoriamente las pruebas de laboratorio se procede con la implantación, piloteo y puesta en operación de la solución de Redes y Sistemas bajo el ambiente de producción donde se debe llevar a cabo una fase de estabilización, durante la cual se adecuarán y afinarán los umbrales y parámetros monitoreados de acuerdo a su comportamiento dentro de cada uno de los sistemas, servidores de producción, bases de datos, segmentos de red, componentes y otros factores que afecten la continuidad de los servicios, tales como tráfico en la red, protocolos de comunicaciones, cargas a Bases de Datos, tareas del sistema operativo y la línea de producción operativa.

Dentro de los resultados obtenidos con la solución de Redes y Sistemas, además de cumplir ampliamente con los objetivos, alcances y funcionalidades requeridas por la solución de monitoreo, se logró conjuntar e identificar a través del método aplicado "Administración de Servicios de Tecnología de Información", todos aquellos elementos o componentes sustantivos o críticos que contribuyen a garantizar la continuidad del negocio desde el punto de vista operativo, ya que se cuenta con todos los recursos que nos permiten identificar, prevenir y reaccionar con la suficiente anticipación y oportunidad a todas aquellas desviaciones y malos funcionamientos de los sistemas, las bases de datos y la red de comunicaciones a través de la administración y control desde un punto central de monitoreo.

Así mismo se cuenta con toda la información histórica en línea (mínimo 30 días, dependiendo del parámetro monitoreado) de todos los componentes administrados, esta información será útil para el análisis de tendencias, comportamientos y crecimientos futuros; A manera de resumen se presentan los resultados obtenidos de toda la infraestructura soportada, eventos y datos colectados de los sistemas administrados.

6.2.- *Estadísticas de Desempeño y Bases de Datos*

Desempeño de Sistema Operativo Unix (HP-UX, AIX)

◦ Servidores monitoreados	153
◦ Parámetros activos por Servidor	78
◦ Elementos de Sistema Operativo detectados por Servidor	24
◦ Datos Colectados por Servidor diariamente	22,294
◦ Eventos Detectados por Servidor diariamente	138
◦ Alarmas Warning detectadas por Servidor diariamente	52
◦ Eventos reportados a la Mesa de Ayuda como Critical por Servidor diariamente	8

Desempeño de Bases de Datos Informix

◦ Servidores monitoreados	142
◦ Instancias de Bases de Datos Detectadas	168
◦ Bases de Datos vigiladas	585
◦ Parámetros activos por Servidor	42
◦ Elementos de Bases de Datos detectados por Servidor	8
◦ Datos Colectados por Base de Datos diariamente	17,530
◦ Eventos Detectados por Base de Datos diariamente	167
◦ Alarmas Warning detectadas por Base de Datos diariamente	66
◦ Eventos reportados a la Mesa de Ayuda como Critical por Base de Datos diariamente	27

6.3.- *Estadísticas de la Red de Comunicaciones*

Enlaces de Comunicaciones (Lan y Wan)

◦ Redes Monitoreadas	453
◦ Segmentos de Red detectados	682
◦ Nodos Descubiertos	517
◦ Interfaces detectadas	2345
◦ Variables MIB activas por interfaz	7
◦ Datos Colectados por Interfaz diariamente	87,966
◦ Eventos Detectados por Nodo diariamente	371
◦ Alarmas Warning detectadas por Nodo diariamente	183
◦ Eventos reportados a la Mesa de Ayuda como Critical por Nodo diariamente	72

De las estadísticas expuestas anteriormente se evidencia la complejidad de administrar la infraestructura soportada sin la ayuda de un esquema de detección y monitoreo que simplifique la administración de los servicios brindados, por ello resulta más que justificada la imperosa necesidad de contar con la solución de Redes y Sistemas, la cual además de cubrir y satisfacer con las necesidades expuestas simplifica y minimiza la intervención humana y con ello la disminución de riesgos e interrupción del servicio.

6.4.- Evidencia de Resultados

Dentro de otros de los resultados importantes que se evidenciaron con la funcionalidad de la solución de redes y sistemas fueron:

1. Un inadecuado balanceo o distribución de los espacios asignados a las Bases de Datos de los servidores de las Aduanas de Puebla, Naco, Camargo y Cd. Acuña, donde se detecto una sobre carga en el Bus SCSI 2 donde se aloja el Dbspace histórico de la Base de datos, esto se debe a una constante lectura a disco de la aplicación de Aduanas.

2. Una saturación permanente y constante de CPU del Servidor IBM de la Regional de Torreón, principalmente durante la ejecución de un proceso masivo que segrega información sobre la Base de Datos de Recaudación, lo importante de este descubrimiento fue el hecho de que dicha saturación únicamente se presentaba en este equipo y no así en los otros 7 Servidores donde se ejecutaba dicho proceso, esto derivó en un análisis más detallado por parte de los Administradores del Sistema Operativo, los Desarrolladores de la aplicación y el personal responsable de Laboratorio, donde se diagnosticó que el problema era causado por una inadecuada versión de algunos de los programas ejecutables liberados recientemente.

3. Una altísima utilización de procesos del sistema en la ALR de Chihuahua, derivada de una inadecuada afinación del Kernel del Sistema Operativo al estar configurados de manera insuficiente algunos parámetros de usuario que los limitaban en el uso de recursos del sistema.

4. Saturación en los recursos de memoria del servidor HP de la ALR de Puebla, derivado de la falta de swapeo por parte de Sistema Operativo, al encontrarse inhabilitadas algunas funciones de swapeo dinámico.

5. La detección y prevención de transacciones heurísticas del manejador de Base de Datos Informix en los servidores IBM del CPN las cuáles ponían en alto riesgo la integridad y seguridad de la información al no poderse detectar cual había sido el último log accesado a través de un proceso de replicación

6 El diagnóstico adecuado de los problemas de lentitud en la red de comunicaciones de la ALR Norte del área Metropolitana, donde continuamente se reportaba una degradacion en el tiempo de respuesta de las terminales de

atención al público; El diagnóstico evidenció una inadecuada habilitación y configuración del segmento de red de automatización de oficinas, donde se encontraban conectados los servidores de correo corporativo, internet y PC´s de oficina los cuales sobrecargaban la Red Lan de la ALR durante la transferencia de correo interno.

7. La extremada perdida de paquetes y retransmisiones de información entre 2 router´s ByNetworks ubicados en la red Wan de la Región Noreste que interconectan a las oficinas de Recaudación y Jurídica, esto se debía a una inadecuada configuración del puerto Wan del router de Jurídica, al haber sido reemplazada una tarjeta por parte del proveedor durante un servicio correctivo.

8. Disminución de la cantidad de reportes levantados en la Mesa de Ayuda por parte de los usuarios y administradores de los sistemas en tópicos relativos al Sistema Operativo, Bases de Datos y Red de Comunicaciones.

Además de las ventajas y beneficios alcanzados con la solución de Redes y Sistemas no se deben olvidar otros aspectos importantes que complementen la continuidad del negocio tales como, el contar con los programas y esquemas de contingencia y recuperación en caso de desastre, así como de los esquemas de seguridad y mantenimiento a los sistemas, bases de datos y componentes de red; Otro factor importante y que generalmente obvian los Administradores de Sistemas son los planes y programas de liberaciones de aplicaciones, ya que de no contar con los procesos y procedimientos adecuados resulta fácilmente impactar a los ambientes de producción saturando o sobrecargando los recursos de red o del sistema operativo, degradando directamente los tiempos de respuesta de los usuarios finales.

Para facilitar las tareas de administración, control y seguridad de los procesos operativos de pruebas y liberaciones de software a producción, se pueden diseñar y aplicar estrategias operativas a través del modelo de referencia de "ITSM", particularmente dentro del tercer cuadrante donde recaen los procesos y procedimientos de Pruebas de laboratorio o "Testing" y Distribución de Software o "Software Distributión" cuyo principal objetivo es garantizar la integridad, funcionalidad y eficiencia de los nuevos productos liberados a producción, a través de la adecuada administración de versiones de los sistemas liberados, homologando al mismo tiempo la versión ejecutable en todos los sistemas productivos.

7.- Conclusiones

Si bien es cierto que el administrar una infraestructura operativa tan robusta como la del "SAT" puede llegar a ser sumamente complicado. la realidad es que con la implantación de la solución de administración de redes y sistemas se han visto notables beneficios en cuanto a la disponibilidad y continuidad de los servicios brindados, esto es un claro ejemplo en Centros de Cómputo como el de la Aduana de Nuevo Laredo Tamaulipas, la cual es la Aduana más importante de entrada de importaciones al País; Dicha Aduana tiene una operación diaria de 24 hrs., los 365 días del año, por lo que el contar con la solución de monitoreo de los sistemas operativos, bases de datos, aplicativos y enlaces de comunicación que conforman los servicios sustantivos de la Aduana, la ha llevado a tener un porcentaje de disponibilidad operativa del 99.99 %, lo cual ha sido reconocido no sólo por las autoridades Mexicanas sino también por las autoridades Norte Americanas de Laredo Texas.

Otro ejemplo de los palpables beneficios de la Solución de Redes y Sistemas son las 8 Administraciones Regionales de Recaudación, las cuales procesan durante todo el año toda la información tributaría del País, obteniéndose resultados nunca antes logrados hasta el cierre contable del año 2001, donde se logró reducir los tiempos de entrega de información a la SHCP hasta por 8 días, esto gracias a la prevención proactiva de problemas y fallas que garantizaron la continuidad y disponibilidad de los servicios informáticos.

No hay que perder de vista, que el éxito de las soluciones de Administración de Servicios de Tecnología de Información radica en identificar adecuadamente todos aquellos componentes de la infraestructura que conforman los servicios sustantivos de las organizaciones, asociarlos dentro de procesos y procedimientos de buenas prácticas e involucrar a la gente responsable de su mantenimiento, afinación y soporte para que los Administradores de "IT" integren la solución adecuada a las necesidades del negocio.

Hoy día el éxito empresarial de organizaciones como Nestle, Sabritas, Bimbo, Telmex, Tv Azteca, PEMEX, Vitro, Cervecería Modelo, Prosa Carnet, Banamex, Bancomer y Bital entre otras se debe a que han adoptado dentro de ellas la cultura de la Administración de Servicios de Tecnología de Información, a través de la implantación de soluciones de Redes y Sistemas con lo cual han llegado a eficientar sus servicios, garantizando la continuidad y disponibilidad de los mismos.

Si bien es cierto que el diseñar, implantar y administrar este tipo de soluciones no es fácil, lo cierto es que trae grandes beneficios y ventajas competitivas a quienes las adoptan, ya que el retorno de inversión de implantarlas es relativamente corto comparado con las perdidas y el impacto de sufrir interrupciones a la operación, corrupciones a la información o simplemente no contar con la información necesaria para el dimensionamiento de crecimientos operativos o la administración de cambio y configuraciones

Otro beneficio de las soluciones de "ITSM", dentro de las organizaciones es que una vez implantadas y estabilizadas, su administración requiere de un equipo de ingenieros muy reducido que cuente con las habilidades y experiencia necesaria para visualizar los cambios y áreas de oportunidad dentro del negocio. El perfil de este grupo de Ingenieros se adecua perfectamente al de las carreras de Ingeniería en Computación, Electrónica, Telecomunicaciones, Industrial o a las carreras de Actuaría, Físico-Matemáticas, Ingeniería en Sistemas Computacionales, etc., por lo que el campo profesional para los egresados de estas licenciaturas es demasiado amplio y con excelentes oportunidades de desarrollo profesional no sólo en nuestro País, sino también en todo Centro y Sudamérica.

Profesionalmente el diseñar, implantar y administrar la solución de Redes y Sistemas me ha dejado sumamente satisfecho, no sólo por el hecho de contribuir al crecimiento y estabilidad operativa de los servicios informáticos del SAT, si no también por haberme dado la oportunidad de aplicar todos los conocimientos adquiridos a través de la licenciatura de Ingeniería en Computación la cual además de inculcarme una cultura profesional en el área de la computación me sentó las bases para desarrollar mi ingenio y creatividad en el campo de la Ingeniería, así como también formarme académicamente con principios y valores de honestidad, responsabilidad, actitud de servicio, lealtad y orientación en logros y resultados.

8.- Anexos Técnicos

8.1.- Anexo 1 "Distribución de Aduanas"

Regional	Localidad	Tipo
GERENCIA REGIONAL A.I.C.M.		
	AEROPUERTO	A
	ACAPULCO	A
	CD HIDALGO	A
	Cd Cuahutemoc	S
	Talismán	S
	LAZARO CARD	A
	PANTACO	A
	PUEBLA	A
	Morelos	S
	Tlaxcala	S
	TOLUCA	A
GERENCIA REGIONAL CD.JUÁREZ		
	JUÁREZ	A
	Ganta Km 30	G
	Ferrocarril	M
	Aeropuerto	S
	Gpe De Bravos	S
	San Jerónimo	S
	Zaragoza	S
	CHIHUAHUA	A
	Aeropuerto	M
	Américas	S
	OJINAGA	A
	El Peguis	G
	La Mula	G
	Pte Internal	M
	PTO PALOMAS	A
	Janos	G
	TORREON	A
GERENCIA REGIONAL GUADALAJARA		
	AGUASCALIENTES	A
	San Luis Potosí	S
	Zacatecas	S
	GUADALAJARA	A
	Ferropuerto	S
	Puerto Vallarta	S
	LA PAZ	A
	San Jose Del Cabo	S
	Santa Rosalia	S
	MANZANILLO	A
	[illegible]	M

	Flechita	M
	MAZATLÁN	A
	Culiacán	S
	Topolobampo	S
	QUERÉTARO	A
	Celaya	S
	León	S
	Morelia	S
	Silao	S
GERENCIA REGIONAL NOGALES		
	AGUA PRIETA	A
	Cabullona	G
	GUAYMAS	A
	Muelle	M
	NACO	A
	NOGALES	A
	Km 21	G
	Cruce De Carga	M
	Cruce Vehicular	M
GERENCIA REGIONAL NVO. LAREDO		
	CD ACUÑA	A
	Garita Km 53	G
	COLOMBIA	A
	Garita Km 55	G
	MONTERREY	A
	Aeropuerto	M
	NUEVO LAREDO	A
	Garita Km 26	G
	Módulo Aeropuerto	M
	Módulo C Autobuses	M
	Módulo Ferrocarril	M
	PIEDRAS NEGRAS	A
	Garita Km 53	G
	Ferrocarril	M
	Ramos Arizpe	S
GERENCIA REGIONAL PTO. PROGRESO		
	CANCÚN	A
	El Ideal	G
	Nuevo Xcan	G
	Tepich	G
	Cozumel	S
	Isla Mujeres	S
	Pto. Morelos	S
	CD. DEL CARMEN	A
	Frontera	S
	Lerma	S
	PROGRESO	A
	Mérida	S
	SUBTENIENTE L	A

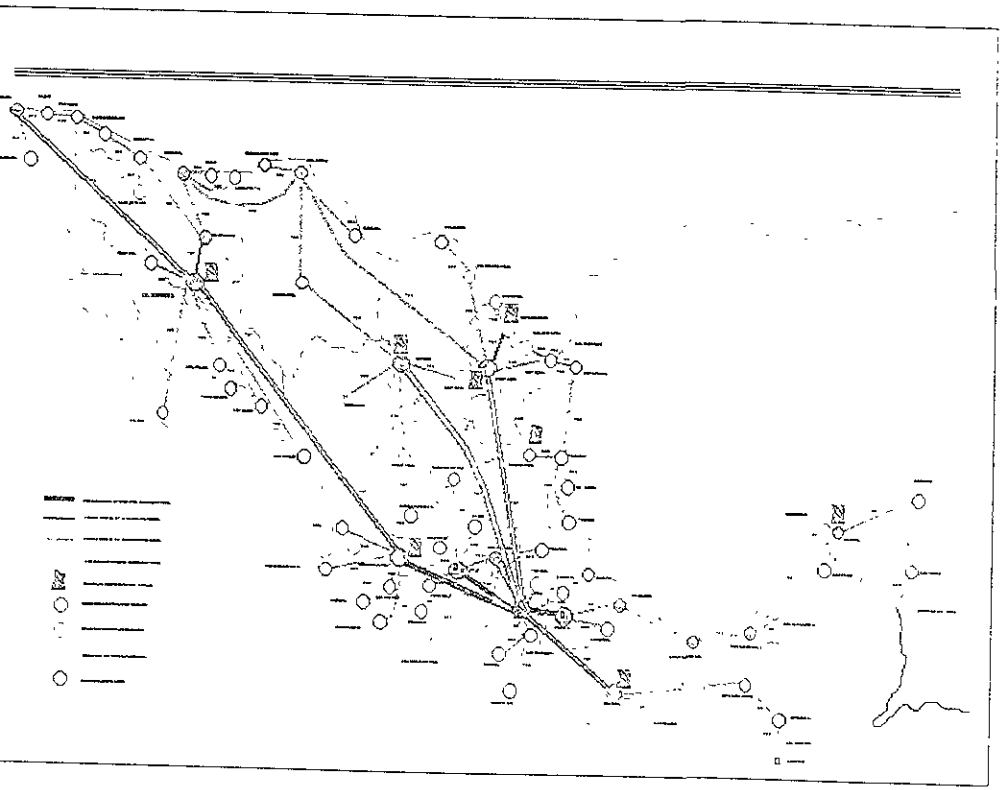
	SUBTENIENTE L	A
	Caobas	G
	Dziuche	G
GERENCIA REGIONAL REYNOSA		
	CAMARGO	A
	Garita Km 35 "S Gertrudis"	G
	Díaz Ordaz "El Vado"	M
	MIGUEL ALEMÁN	A
	Garita Km 26 "Mier"	G
	Garita Parás	G
	Falcón"	M
	MATAMOROS	A
	Garita Km 22 "La China"	G
	Garita Km 57 "La Siberia"	G
	Puente I. Zaragoza	M
	Libre Comercio	S
	Pte. Nuevo	S
	Pte Viejo	S
	REYNOSA	A
	Garita Km 26	G
	Garita Km 30	G
	Pequeña Importación	M
	Plataforma Fiscal	M
	Nuevo Progreso	S
	Puente Nvo. Amanecer	S
GERENCIA REGIONAL TIJUANA		
	ENSENADA	A
	Unión Agrícola	M
	MEXICALI	A
	Ferrocarril	M
	Mexicali I (*)	M
	Aeropuerto San Felipe	S
	Algodones	S
	SAN LUIS, R C	A
	SONOYTA	A
	San Emeterio	G
	Almejas	S
	Puerto Peñasco	S
	TECATE	A
	TIJUANA	A
	Puerta México	M
	Aeropuerto	S
GERENCIA REGIONAL VERACRUZ		
	ALTAMIRA	A
	COATZACOALCOS	A
	Villahermosa Tabasco	S
	SALINA CRUZ	A
	Xoxocotlan Oaxaca	S
	TAMPICO	A

	TAMPICO	A
	TUXPAN	A
	VERACRUZ	A
	Bodega 20	M
	Icave	M
	Aeropuerto "Heriberto Jara Corona"	S

8.2.- *Anexo 2 "Distribución de Recaudación*

Regional	Local	Tipo
REGIONAL CENTRO	Celaya	A
	León	B
	Morelia	B
	Querétaro	B
	Pachuca	B
	San Luis Potosí	B
	Irapuato	C
	Uruapan	C
REGIONAL METROPOLITANA	Sur	AAA
	Norte	A
	Centro	A
	Oriente	A
	Naucalpan	A
	Toluca	B
REGIONAL GOLFO - PACIFICO	Puebla	AA
	Tlaxcala	C
	Jalapa	B
	Veracruz	B
	Coatzacoalcos	C
	Acapulco	C
	Cuernavaca	B
	Córdoba	B
	Iguala	B
REGIONAL NORESTE	Guadalupe	AA
	San Pedro	AA
	Monterrey	AA
	Reynosa	B
	Tampico	B
	Tuxpan	C
	Nuevo Laredo	C
	Matamoros	B
	Ciudad Victoria	B

8.3.- Anexo 3 "Red de Comunicaciones"



Bibliografía

BMC PATROL for Unix Installation Guide. BMC Software. Junio 6 de 1999.

BMC PATROL Agent Reference Manual. BMC Software. Junio 6 de 1999.

BMC PATROL for Unix Getting Started. BMC Software. Junio 6 de 1999.

BMC PATROL for Unix User Guide. BMC Software. Junio 6 de 1999.

BMC PATROL Knowledge Module for Informix, User Guide. BMC Software. Noviembre 14 de 1999.

BMC PATROL Knowledge Module for Unix, User Guide. BMC Software. Junio 6 de 1999.

BMC PATROL History Loader Knowledge Module, User Guide. BMC Software. Noviembre 14 de 1999.

BMC PATROLVIEW for HP OpenView IT/Operations, User Guide. BMC Software. Marzo 6 de 1998.

HP OpenView IT/Operations Release Notes Version A.5.0 Management Server on HP-UX 10.x August 1999.

HP OpenView IT/Operations Installation Guide for the Management Server English Version. Edition 4 Management Server on HP-UX 10.x / Oracle Database August 1999.

HP OpenView IT/Operations Administrator's Task Guide Management Server on HP-UX 10.x August 1999.

HP OpenView IT/Operations Concepts Guide Management Server on HP-UX 10.x August 1999

HP OpenView IT/Operations Administrator's Reference Management Server on HP-UX 10.x August 1999

HP OpenView IT/Operations, Error Message Reference Management Server on HP-UX 10.x August 1999

Referencias electrónicas

http://www.hp.com

http://www.bmc.com

http://www.proactive-sv.com.au/itsm.htm

http://www.it-smp.com

http://www.tools2manage-it.com/

http://www.tools2manage-it.com/model.shtml

http://www.rational.com/products/rup/index.jsp

http://www.itil-itsm-world.com/

http://www.ccta.gov.uk/itil

http://www.itil.co.uk/index.html

http://www.proactive-sv.com.au/public.htm

http://www.pdatrain.com.sg/itil/what_is_itil.htm