Asociación Informáticos de
Instituciones Sanitarias de
Castilla y León

I CUADERNO TÉCNICO:

MONITORIZACIÓN DE SERVICIOS Y SISTEMAS

Autores:

Mariano Raboso Mateos
Juan Luis Blázquez Jiménez
Diego Calvo Avilés
Luis Mateos González
Arturo Quesada Olmo

Coordinador: **Mariano Raboso Mateos**

Septiembre de 2012

ISBN pendiente de asignación

CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

1. PRÓLOGO

Este trabajo es el resultado práctico del acuerdo de la pasada asamblea ordinaria celebrada el 25 en febrero en Burgos. Tiene especial relevancia para nuestra asociación, por ser el primer cuaderno técnico y por que sienta las bases de una nueva e interesante línea de actividades de Aiiscyl, basada en la publicación de material técnico.

Está alineado con uno de los objetivos que desde la junta directiva estamos impulsando, consistente en dotar de herramientas para mejorar la capacitación técnica de los socios y la organización de los trabajos. Todo ello basado en buenas prácticas, rigor técnico y calidad organizativa.

El tema elegido es la monitorización de sistemas y servicios, por ser procesos comunes de los responsables de sistemas en cualquier instalación. La supervisión y el control son tareas imprescindibles para conocer el estado de la instalación y los servicios, así como para tener capacidad de detección y corrección de errores. En un ecosistema tecnológico tan rico, heterogéneo y variado como es el sanitario, donde las relaciones e interdependencias entre servicios cada vez son mayores y la criticidad es muy alta, es imprescindible tener un control de la instalación, mantener el rendimiento en condiciones óptimas y anticiparse a los problemas para evitar paradas e indisponibilidades. Es la monitorización la herramienta que nos ayuda en estas tareas.

Debo agradecer al coordinador y a los compañeros que han participado en su realización, el esfuerzo generoso que han realizado así como felicitarlos por el resultado. Un cuaderno principalmente práctico, pero bien sustentado en disciplina técnica, que se ajusta perfectamente a las ideas iniciales que les habíamos transmitido cuando les realizamos el encargo. También por ajustarse a los plazos ya que en pocos meses han sido capaces de expresar de forma ordenada todo su conocimiento sobre el tema, que como se puede observar es amplio y profundo.

Esperamos que tanto los socios, como cualquier lector interesado que tenga oportunidad de acceder al documento le resulte de utilidad. Queremos también animaros a reportar al correo de la asociación (aiiscyl@gmail.com) las mejoras y sugerencias que nos permitan mantener vivo el documento, enriquecer su contenido y publicar futuras versiones mejoradas y ampliadas.

Juan F. Nieto, presidente de AIISCYL

2. OBJETIVOS DEL CUADERNO TÉCNICO

Este cuaderno técnico sobre gestión de red se ha realizado para que sea un documento útil en el que los administradores de sistemas puedan entender los principios básicos de la gestión de red y sobre todo disponer de una guía práctica para desplegar una plataforma de gestión de red.

En concreto, pretende cubrir los siguientes objetivos:

- Conocer qué es la gestión de red y cuáles son sus funciones.
- Comprender la importancia de la existencia de un centro de gestión de red.
- Aprender las características básicas de los modelos de gestión de red, en especial del modelo de gestión en Internet.
- Conocer la estructura y funcionamiento del protocolo SNMP y de RMON.
- Conocer las principales plataformas de gestión de red disponibles en el mercado.
- Instalar y configurar correctamente una plataforma de gestión de red.
- Identificar las necesidades de gestión de red en las organizaciones.

En los siguientes capítulos se desarrollan los principales servicios que ofrecen hoy en día las herramientas de gestión de red.

Primeramente se desarrollan una serie de conceptos básicos sobre la gestión de red. Estos conceptos básicos se describen en el capítulo 3 "Introducción a la Gestión de Red". Este capítulo es importante ya que se sientan las bases sobre la gestión de red, subrayando la importancia de disponer de herramientas que puedan realizar esta función con eficacia y eficiencia.

En el siguiente capítulo se describen los dos protocolos utilizados en el modelo de gestión de internet: SNMP y RMON. Aunque no se entra en profundidad, son necesarios unos conocimientos mínimos sobre los protocolos de gestión más importantes. Se describen las tres versiones del protocolo SNMP (v1, v2 y v3), así como RMON y RMON2. Se añaden las referencias bibliográficas más importantes para que el lector interesado pueda ampliar sus conocimientos.

Una vez completada la parte teórica, se propone la instalación y configuración de una plataforma de gestión de red. En el capítulo 5 se propone la instalación de Nagios, una de las mejores herramientas del mercado debido a su gran difusión y capacidades. Es una herramienta de libre distribución y gratuita. En la actualidad hay un gran número de desarrolladores en la red que amplían día a día la funcionalidad de esta herramienta añadiendo plugins, módulos y aplicaciones de interconexión con otras herramientas y servicios. También hay disponibles en la red multitud de tutoriales y foros donde los administradores pueden resolver sus dudas sobre la instalación y configuración de esta herramienta.

Para instalar y configurar correctamente la herramienta, el lector puede seguir paso a paso cada una de las tareas propuestas. En algunos casos se dan recomendaciones de

uso o configuración, así como ciertas comprobaciones que se deben tener en cuenta. Para cada tarea se adjuntan capturas de pantalla reales de la herramienta instalada en un sistema Ubuntu 11.06. Es importante tener cuidado con la sintaxis de los comandos, ya que un error podría hacer que la herramienta no se instalara o configurara correctamente.

En el capítulo 6 se describe la configuración de los distintos servicios de la herramienta. Debido a la extensión de los mismos, en este documento se reflejan aquellos que se han considerado más importantes. Se muestran detalles de la configuración de los ficheros de Nagios sobre los pasos básicos para monitorizar máquinas basadas en Sistemas Operativos Linux y Windows, y los pasos a seguir para actualizar el software principal de Nagios (Nagios Core y Nagios Plugins). Por último, en este capítulo se describen los pasos para configurar el envío de notificaciones. Como ejemplo se muestran los detalles para configurar las notificaciones por correo electrónico. De igual forma se puede configurar el servicio de envío de notificaciones por SMS.

Los siguientes capítulos (7 y 8) se dedican a SNMP. Se describe la instalación y configuración de servicios basados en la utilización de este protocolo, base para la gestión aquí propuesta. En el capítulo 8 se describe con mayor profundidad la configuración del protocolo y el uso de primitivas y plugins basados en SNMP.

Además de las configuraciones básicas de servidores, dispositivos de red, etc., en los capítulos 9 y 10 se muestran casos prácticos concretos de monitorización que se han identificado como importantes, e incluso críticos, en el trabajo diario del personal del servicio de informática del SACYL.

Por último se incluye la bibliografía y anexos para que el lector pueda ampliar sus conocimientos sobre la gestión de red.

Este documento pretende ser una guía útil de forma que cualquier instalación o configuración documentada se pueda replicar para su uso directo en la infraestructura de servicios del SACYL. Para ello se ha contado con personal experimentado en la gestión de dichos servicios, que ha trabajado para integrar la gestión de los mismos en una única plataforma de gestión de red.

Como líneas futuras de trabajo, una vez que los usuarios desplieguen esta infraestructura, se pretende integrar más servicios no contemplados en esta edición, así como ampliar la funcionalidad o el control sobre los ya gestionados.

3. INTRODUCCIÓN A LA GESTIÓN DE RED

3.1. Definiciones.

Desde el punto de vista de la gestión de red es necesario distinguir claramente los conceptos de **supervisión** y de **control**:

- La s**upervisión** consiste en conocer el estado actual de la red desde un puesto. Esta función es equivalente a monitorizar el estado de la red. No se ejerce ninguna acción de control; como mucho se activa una alarma o se avisa a la persona correspondiente.
- **El control** es la capacidad de detección de errores y su corrección. Implica la configuración de equipos de forma remota. Es una función de gestión de red mucho más completa y compleja, ya que involucra la participación de recursos humanos y la reconfiguración de dispositivos.

3.2. Justificación.

La gestión de red tuvo su origen en la necesidad de automatizar todos los procesos de supervisión y control de las redes. La filosofía que subyace debajo de la gestión de red ha tenido tanto éxito, que hoy en día se ha extendido para gestionar también servicios y aplicaciones.

A menudo las herramientas y plataformas de gestión de red disponibles en el mercado, como el caso de Nagios o HP Openview, permiten tanto la gestión de dispositivos de red como servicios y aplicaciones. Esta situación conlleva que, tanto los administradores de la red como los de sistemas, tengan que compartir estas herramientas por lo que a menudo éstas disponen de un sistema de autentificación de usuarios con perfiles diversos y complejos.

Por último, la complejidad de los sistemas informáticos de muchas organizaciones es tal, que el control "a mano" de sus sistemas es totalmente inviable. En muchos casos, incluso es necesario diseñar una arquitectura en varios niveles, con varios equipos supervisando la red formando una jerarquía de plataformas de gestión de red. Los propios protocolos de red como SNMP permiten trabajar de forma distribuida de forma que existen varias estaciones gestoras que controlan redes más complejas.

3.3. Objetivos de la Gestión de Red

La gestión de red tiene los siguientes objetivos, que han de tenerse siempre presente a la hora de diseñar cualquier sistema de gestión de red:

- **Control de activos estratégicos.** Muchos de los sistemas o servicios a gestionar a menudo se consideran activos estratégicos para nuestra organización. Es el caso, por ejemplo, de un servicio web para una empresa que vende productos por Internet, o la propia infraestructura de red en la mayor parte de los casos. Estos activos estratégicos han de ser supervisados y controlados en todo momento.

- **Control de complejidad.** Las organizaciones cada vez más poseen sistemas de información muy complejos que son muy difíciles de gestionar de forma independiente y manual. Por ejemplo, se pueden tener cientos de alarmas de dispositivos que sólo están accesibles a través de un router en la red. Si éste se cae o tiene un problema de conectividad con dicha red se dispararán un número elevado de alarmas. El sistema automático debe distinguir esta situación y enviar solamente las alarmas necesarias y significativas. De igual forma debe asignar un conjunto de prioridades en la gestión de las alarmas.
- **Mejora del servicio.** La mejora de los servicios ofrecidos siempre debe ser una constante en el personal encargado del diseño y administración de los sistemas de información. Los sistemas y el volumen de la información están en constante crecimiento, por lo que también lo estarán la demanda de ancho de banda y la capacidad de almacenamiento o CPU.
- **Equilibrio de necesidades.** A menudo muchos administradores tienen los recursos mal dimensionados, ya que no conocen de forma detallada el uso que los usuarios hacen de determinados recursos. Un ancho de banda mal gestionado, por ejemplo, puede provocar que los usuarios que generan un tráfico interactivo con requisitos de tiempo de respuesta, se vean afectados por otros que usan protocolos que tienden a consumir todo el ancho de banda disponible (por ejemplo el protocolo FTP).
- **Reducción de indisponibilidades.** Las indisponibilidades suponen graves pérdidas económicas y de otra índole para las empresas. Muchas de éstas se pueden evitar. La siguiente figura muestra la forma en que se aprovechan los recursos. La falta de rendimiento y las indisponibilidades evitables son la causa de una parte considerable de la pérdida de eficiencia del sistema.

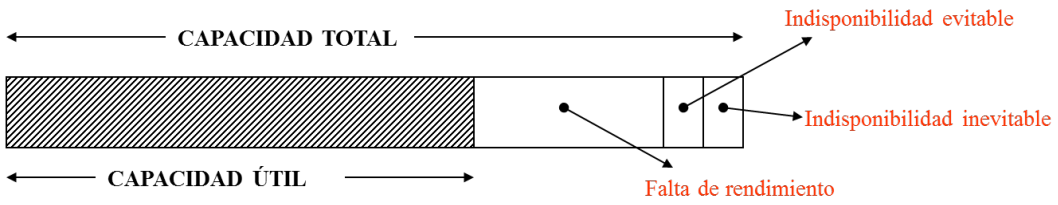


Fig. 1: Capacidad total y capacidad útil

3.4. Áreas de la Gestión de Red definidas por la ISO

La Organización Internacional de estándares (ISO) define una serie de áreas en las que se debe aplicar la gestión de red. Este modelo se denomina (por sus iniciales) **FCAPS** (**F**ault-**C**onfiguration-**A**ccounting-**P**erformance-**S**ecurity):

- Gestión de fallos.
- Gestión de la configuración y de nombres (identificación).
- Accounting.
- Gestión de las prestaciones.
- Gestión de la seguridad.

3.4.1. Gestión de fallos.

Para mantener en funcionamiento una infraestructura de red compleja hay que supervisar cada uno de los elementos de forma individual y de manera conjunta como un todo.

Un fallo es un estado anormal que requiere la gestión (atención) para que se solucione. Se puede producir tanto porque el servicio o equipo deje de funcionar, o porque se produzcan demasiados errores en su funcionamiento.

Hoy en día se monitoriza el estado de un servicio o dispositivo estableciendo unos niveles y márgenes de funcionamiento, de tal forma que se pueda determinar con más exactitud y de forma gradual cuándo está fallando un equipo. Esto permite poder anticiparse al fallo, ya que cuando éste aparece suele ser demasiado tarde y los usuarios pueden verse gravemente afectados. Hay que pensar que servicios como la telefonía (analógica o digital) se asumen que funcionan siempre. Todo el mundo espera tener tono de llamada en su teléfono, aunque asume que en algún momento puede fallar su conexión de datos en el PC. Por esta razón, detectar un fallo en el servicio de telefonía IP es crítico.

Cuando se produce un fallo, hay que poner en marcha lo antes posible los siguientes procedimientos:

- Determinar exactamente dónde se ha producido, ya que el fallo puede afectar a uno o varios servicios o dispositivos.
- Aislar el resto de la red, de tal forma que los usuarios puedan seguir trabajando.
- Reconfigurar o modificar la red para minimizar el impacto de los equipos/servicios que han dejado de funcionar.
- Reparar o reponer los equipos o servicios dañados.
- Restaurar la configuración de la red al estado inicial.

3.4.2. Gestión de configuración

La gestión de la configuración permite organizar, de forma lógica, el comportamiento de todos y cada uno de los componentes de la infraestructura, tanto físicos (dispositivos) como lógicos (drivers, SO,…).

La configuración va ligada a la identificación y nombrado de los distintos sistemas y servicios. Estas tareas es posible automatizarlas hoy en día, de tal forma que los dispositivos en la red se autoconfiguren e identifiquen.

Los sistemas de gestión de direcciones IP (servidores DHCP), nombres y nombres de dominio (WINS, DNS,…), y las capacidades inherentes a los protocolos actuales (como IPv6), permiten delegar a las herramientas estas tareas complejas, antes resueltas de forma tediosa por los administradores y operadores de red.

3.4.3. Accounting

Esta función, que literalmente se traduce por contabilidad, permite controlar el gasto de recursos, bien sean de cómputo, ancho de banda, tiempo de uso, etc. La utilidad más inmediata es la de establecer una compensación económica, aunque más allá de este propósito estará el correcto control del uso que los usuarios hacen de los recursos.

El equilibrio de necesidades siempre redundará en un menor coste y mejor servicio a los usuarios.

3.4.4. Gestión de las Prestaciones (Performance)

Las prestaciones están normalmente ligadas a la eficiencia y al equilibrio de necesidades. Para poder gestionar correctamente los recursos, hay que saber primero qué uso se está haciendo de los mismos.

Las prestaciones se refieren normalmente a cuestiones relacionadas con el ancho de banda y latencia en la red. Pero a medida que la gestión de red se extiende a la gestión de servicios, también podemos hablar de prestaciones, por ejemplo, en relación al número de transacciones con un servidor de base de datos o la utilización de la CPU.

La gestión de las prestaciones es crucial para verificar los acuerdos de nivel de servicio (SLA, Service Level Agreement) que se negocian con los proveedores. El caso más frecuente tiene que ver con la supervisión del ancho de banda contratado con el ISP. En determinados casos, el operador llega a instalar equipos propios para poder gestionar y monitorizar sus enlaces. El incumplimiento de los SLA es causa frecuente de demandas, por lo que es crucial disponer de pruebas que reflejen (con datos exhaustivos) el comportamiento de los equipos de la red.

3.4.5. Gestión de la Seguridad

Si bien es cierto que hace unos años los esfuerzos se concentraban en desarrollar nuevas funcionalidades en protocolos y herramientas, hoy en día son inútiles si no van protegidas por el paraguas del sistema de seguridad a todos los niveles.

El mismo protocolo SNMP, que en sus orígenes sólo tenía un sistema simple de control de acceso, en versiones posteriores ha introducido sistemas de seguridad en varios niveles.

Las estadísticas demuestran que la mayor parte de los ataques producidos a las redes se realizan desde el interior. Por este motivo, la gestión de red debe integrar sus propios sistemas de seguridad en las transmisiones y en el control de acceso.

3.5. Organización de Centros de Gestión de Red.

Un centro de gestión de red es una organización dedicada a la supervisión y control de la red. Aunque algunas organizaciones, por su tamaño, nunca necesitarán crear un centro o departamento independiente, las funciones y distribución de responsabilidades que involucran tendrán que asignarse igualmente a uno o varios administradores.

Hoy en día no hay ninguna excusa, ni siquiera de carácter económico, para no disponer de una plataforma de gestión de red y algunos recursos humanos dedicados a la misma. La siguiente figura muestra una distribución aproximada de los recursos dedicados a la gestión de red. La mayor partida de recursos está asociada al gasto corriente. La pérdida de servicio o ineficiencia del mismo también se pueden contabilizar como gasto.

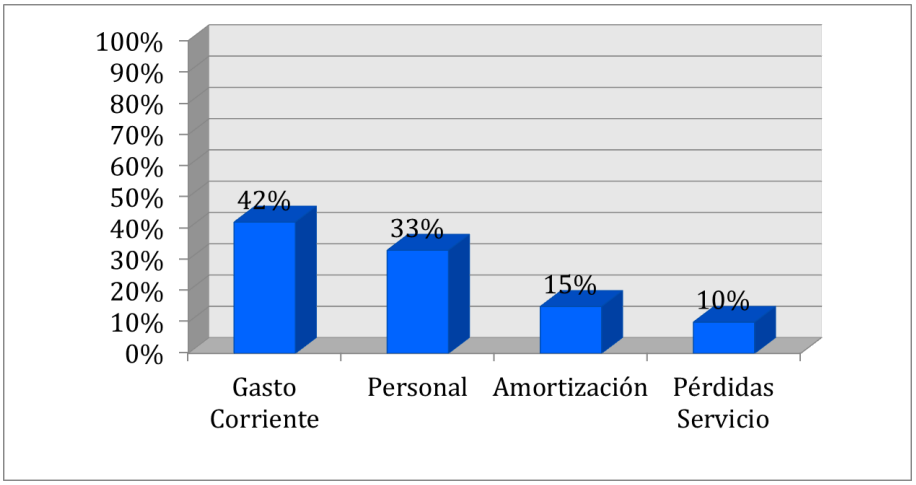


Fig. 2: Distribución del gasto en un centro de gestión de red.

Aunque dependerá del nivel de la organización, el personal asociado al servicio suele tener los siguientes perfiles:

- Operadores. Suelen ser usuarios poco cualificados, entrenados para detectar problemas simples y concretos (sólo supervisión). Suelen dar el servicio de soporte a usuarios o *helpdesk*.
- Administradores. Son personal de mayor cualificación, con capacidad para resolver determinados problemas. Sus funciones son:
  - » Control de operadores.
  - » Gestión de inventario.
  - » Gestión de seguridad (claves).
  - » Gestión de configuraciones.
- Analistas. Perfil del personal con capacidad para enfrentarse a nuevos problemas. También se encargan de la preparación de procedimientos y el análisis de la calidad de servicio. Intervienen en los rediseños de red.
- Planificadores. Son el enlace entre la parte técnica y ejecutiva. Se encargan de establecer la política de telecomunicaciones y la de costes y presupuestos.

3.6. Elementos de un sistema de Gestión de Red

Los distintos elementos que componen un sistema de gestión de red son:

- Elementos gestionables: PC, SAI, dispositivos de red, etc. Hoy en día prácticamente cualquier dispositivo es gestionable, o se le puede acoplar un módulo externo que lo permita.
- Gestores de elementos:

  - » Agentes software. Pequeños programas que consumen pocos recursos y que corren en los dispositivos a gestionar.
  - » Bases de información. Modelo de conocimiento que utiliza el sistema de gestión de red para llevar a cabo sus funciones.

Hoy en día los sistemas de gestión integran:

- Interfaces de usuario. Servicios de presentación de datos, visualización gráfica de datos en tiempo real, estadísticas, etc., tanto para desktops como dispositivos portátiles (smartphones).
- Aplicaciones de gestión.
- Bases de datos.
- Protocolos y servicios de comunicaciones.
- Pasarelas hacia otros sistemas de gestión de red.
- Sistemas con capacidad de gestión distribuida.

3.7. Modelos de Gestión de Red: OSI e Internet.

Por su gran difusión, el modelo que se seguirá en este documento es el de la gestión de red en Internet. El modelo OSI, mucho más potente, se utiliza a nivel de operadores de telecomunicación y está fuera de los objetivos de este documento.

El modelo de Internet es el modelo más extendido, llegando al 98% de penetración. Es un modelo para equipamiento simple, no para operadores de telecomunicación. Es pragmático y sencillo, y pretende solucionar los problemas del momento.

Este modelo pone de manifiesto un axioma: "Si la gestión de red es esencial, entonces debe ser implementada en TODOS los equipos de la red".

Debe ser un modelo de gestión que quepa en el más pequeño de los recursos, de forma que se asegure que funcionará en todos los demás. Como consecuencia, los agentes (programas que se ejecutan en los dispositivos) deben ser simples y pequeños. Por esta razón la complejidad es asumida por el gestor.

Los equipos sólo han de escuchar y saber responder a preguntas simples. Los protocolos se basan en intercambio de primitivas sencillas e intercambio de datos simples (cadenas de texto y valores numéricos simples).

4. LOS PROTOCOLOS SNMP Y RMON

4.1. SNMP

El protocolo SNMP (Simple Network Management Protocol) es un protocolo especialmente diseñado para tareas de gestión de redes interconectadas mediante TCP/IP. No sólo especifica cuestiones del protocolo, sino también del modelo de información asociado.

Se basa en la utilización de los siguientes elementos:

- Estación de gestión. Es la estación que se va a encargar de gestionar los dispositivos. Interrogará a los distintos agentes, recibiendo la información de cada uno de ellos.
- Agente de gestión. Es un software que se ejecuta en la estación o dispositivo a monitorizar. Ocupa pocos recursos de CPU y memoria, y tiene un comportamiento pasivo, es decir, que se limita a escuchar las peticiones de la estación gestora y a devolver la información solicitada.
- MIB (Management Information Base), o base de conocimiento. Es un fichero escrito en lenguaje ASN.1 que describe las propiedades de un dispositivo.
- Protocolo de gestión de red. Basado en la utilización de datagramas UDP, está diseñado para ser simple y eficaz. Utiliza tan sólo tres primitivas: *get*, *getnext* y *set*. Además de las anteriores, también permite enviar *traps* y *notificaciones*, que se disparan de forma asíncrona por eventos producidos en la estación a monitorizar.

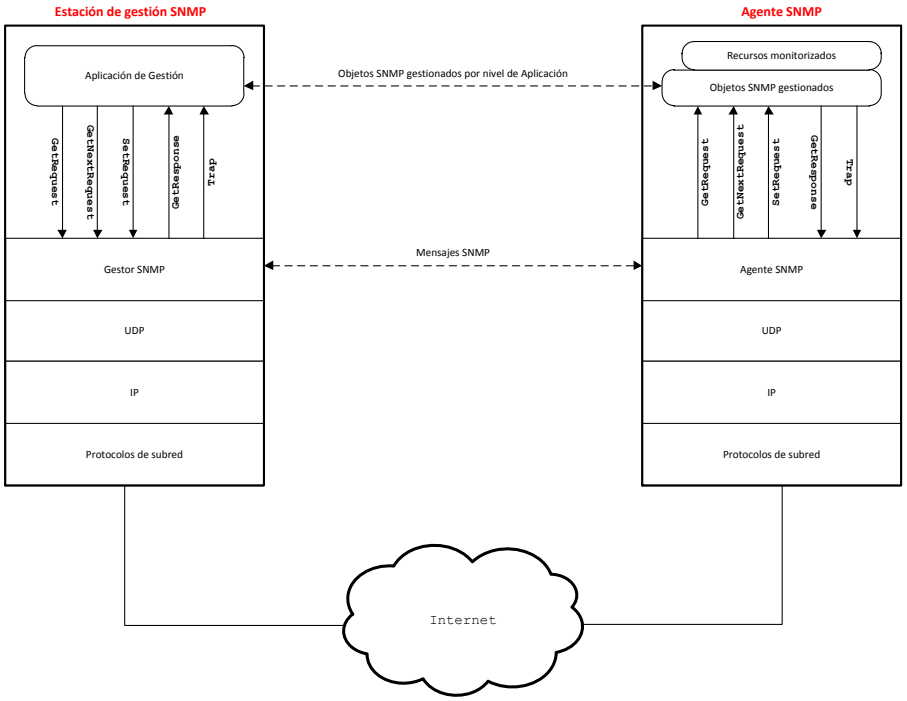


Fig. 3: Arquitectura protocolo SNMP.

Para dispositivos que no hablen directamente TCP/IP, es posible la comunicación a través de un agente proxy:

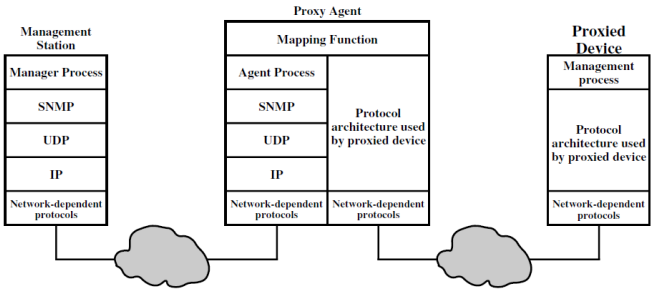


Fig. 4: Arquitectura software para utilización de SNMP vía proxy.

4.1.1. Desarrollo del protocolo.

El proceso de normalización ha sido lento y contemporáneo al modelo de gestión OSI. La normalización se ha desarrollado utilizando las RFC (Request For Comment) de la IETF, que generalmente es un proceso rápido y sin demasiada burocracia.

La primera aproximación data del año 1987, coincidente con el aumento del tráfico en Internet. En los inicios de los protocolos de gestión se encuentran:

- SGMP (Simple Gateway Monitoring Protocol). Protocolo diseñado para la monitorización de gateways. Desarrollado en 1987.
- HEMS (High-level entity Management Protocol). Fue una generalización de HMP (Host Monitoring Protocol), el primer protocolo de gestión en Internet.
- CMOT (CMIP over TCP/IP). Fue una iniciativa para extender la familia de protocolos de la ISO en Internet.

En el año 1998 surge SNMP (Simple Network Management Protocol), su modelo de información (SMI) y la MIB-I (Management Information Base). Las MIBs son ficheros públicos, escritos en lenguaje ASN.1 (Abstract Syntax Notation), que representan el modelo de información.

Además de las MIBs estándar que todos los fabricantes deben respetar, cada fabricante de un dispositivo puede añadir otras propias. Éstas se deben proporcionar en el dispositivo o deben estar disponibles en su página web. Existen algunos repositorios de MIBs en internet para podérselas descargar.

En el año 1991 se realizó una revisión de SNMP y apareció la MIB-II. Por motivos principalmente de falta de seguridad, en 1993 se publicó la versión 2 (SNMPv2) y en 1993 SNMPv3. Actualmente se trabaja con las tres versiones indistintamente, en función del nivel de seguridad que se desee.

Las RFCs básicas son las de la tabla siguiente. Para hacer una consulta completa, se recomienda buscar en bases de datos como el "RFC Editor"[1]. Por comodidad se incluyen en el Anexo V.

Tabla I: RFC básicas asociadas a SNMP.

RFC	Concepto
1155	SMI (Structure of Management Information)
1157	Protocolo SNMP
1212	Definiciones MIB
1156	MIB-I
1213	MIB-II
1155	SMI (Structure of Management Information)

4.1.2. MIBs y OIDs

Las MIBs almacenan conjuntos de objetos que modelan el funcionamiento de un dispositivo. Se pueden organizar en grupos para no tener que implementar todos los grupos de ese módulo.

Los objetos se identifican mediante un identificador u OID (Object Identifier), que están organizados de forma jerárquica en árbol:

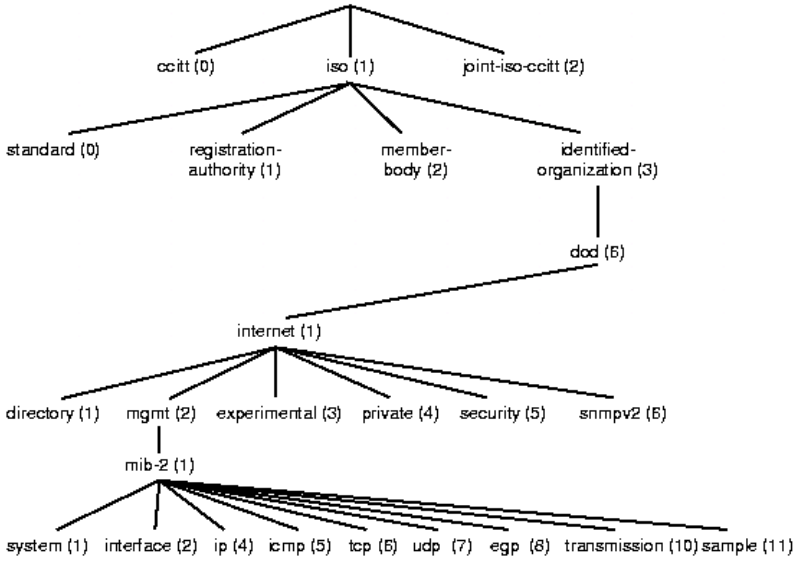


Fig. 5: Árbol de OIDs.

De esta manera el acceso a un OID, por ejemplo *sysUpTime*, se realiza haciendo la consulta:

```
alumno@nagios:~$ snmpget -v1 -c public 172.25.80.207 sysUpTime.0
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (28367859) 3 days, 6:47:58.59
alumno@nagios:~$
```

o mediante el OID correspondiente:

```
alumno@nagios:~$ snmpget  -v1 -c public 172.25.80.207 .1.3.6.1.2.1.1.3.0
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (28386764) 3 days, 6:51:07.64
```

[1] http://www.rfc-editor.org/

Los comandos que se pueden utilizar son *snmpget*, *snmpgetnext* y *snmpwalk*.

4.1.3. SMI (Structure of Management Information)

Definida por la RFC 1155, define el marco general por el que se definen y construyen las MIBs. Especifica los tipos de datos que se pueden utilizar en una MIB, así como la forma de representarlos y nombrarlos. Con el objetivo de simplicidad y escalabilidad, en las MIBs sólo se pueden almacenar escalares y arrays de escalares, aunque sólo se pueden transferir los primeros.

A diferencia de este modelo, en OSI se pueden almacenar estructuras de datos complejas.

En particular, SMI debe proveer:

- Un mecanismo para definir la estructura de una MIB.
- Una técnica estándar para definir objetos individuales, incluyendo la sintaxis y el valor de cada uno de ellos.
- Un mecanismo para codificar el valor de cada objeto.

Estructura general de una MIB

Todos los objetos e SNMP están organizados en una estructura jerárquica. Cada uno representa un recurso, una actividad o una información asociada que se ha de gestionar.

Asociado con cada tipo de objeto en una MIB, se encuentra un identificador en lenguaje ASN.1 (`OBJECT IDENTIFIER`). El identificador sirve para nombrar el objeto y, por tanto, la estructura jerárquica del modelo. Tiene un valor asociado que consiste en una secuencia de enteros (ver figura del apartado anterior). Por ejemplo, el objeto internet con OID .1.3.6.1:

```
internet OBJECT IDENTIFIER ::= { iso (1) org (3) dod (6) 1}
```

El subárbol *mgmt* contiene las definiciones de las bases de información de gestión que han sido aprobadas por la IAB (Internet Architecture Board). En la actualidad se han aprobado dos bases de datos *mib-1* y *mib-2*. La segunda es una extensión de la primera.

Los objetos se definen de las tres formas siguientes:

- El árbol de la mib-2 puede ser extendido o remplazado por una actualización (en un futuro mib-3). Por ejemplo, RMON es el subárbol 16 debajo de la *mib-2* (*mib-2 (16)*).
- Una MIB experimental se puede construir para una determinada aplicación. Los objetos se pueden mover al subárbol *mgmt*.
- Extensiones de tipo privado se pueden añadir al subárbol *private*. Éste subárbol tiene definido sólo un hijo (*enterprises*). En este subárbol los distintos fabricantes colocan sus objetos. Más adelante se utilizará esta rama para monitorizar equipos Cisco (Access Point y Call Manager).

Esta estructura permite conservar un estándar que puede ser ampliado en cualquier momento, aportando la suficiente flexibilidad para acomodar toda la funcionalidad que los fabricantes quieran aportar al modelo.

Los datos pueden ser de tipo:

» *UNIVERSAL*: integer, octetstring, null, object identifier, sequence y sequence-of.
» *APPLICATION*: networkaddress, ipaddress, counter, gauge, timeticks, opaque.

También se pueden definir tablas que son muy útiles para almacenar, por ejemplo, las conexiones activas del protocolo TCP (1.3.6.1.2.1.6.13). La tabla de este ejemplo contiene 5 entradas:

» *tcpConnState (1.3.6.1.2.1.6.13.1.1)*,
» *tcpConnLocalAddress (1.3.6.1.2.1.6.13.1.2)*,
» *tcpConnLocalPort (1.3.6.1.2.1.6.13.1.3)*,
» *tcpConnRemAddress (1.3.6.1.2.1.6.13.1.4)*,
» *tcpConnRemPort (1.3.6.1.2.1.6.13.1.5)*.

```
-- the TCP Connection table

          -- The TCP connection table contains information about this
          -- entity's existing TCP connections.

          tcpConnTable OBJECT-TYPE
              SYNTAX  SEQUENCE OF TcpConnEntry
              ACCESS  not-accessible
              STATUS  mandatory
              DESCRIPTION
                      "A table containing TCP connection-specific
                      information."
              ::= { tcp 13 }

          tcpConnEntry OBJECT-TYPE
              SYNTAX  TcpConnEntry
              ACCESS  not-accessible
              STATUS  mandatory
              DESCRIPTION
                      "Information about a particular current TCP
                      connection.  An object of this type is transient,
                      in that it ceases to exist when (or soon after)
                      the connection makes the transition to the CLOSED
                      state."
              INDEX   { tcpConnLocalAddress,
                        tcpConnLocalPort,
                        tcpConnRemAddress,
                        tcpConnRemPort }
              ::= { tcpConnTable 1 }

          TcpConnEntry ::=
              SEQUENCE {
                  tcpConnState
                      INTEGER,
                  tcpConnLocalAddress
                      IpAddress,
                  tcpConnLocalPort
                      INTEGER (0..65535),
                  tcpConnRemAddress
                      IpAddress,
                  tcpConnRemPort
                      INTEGER (0..65535)
              }

          tcpConnState OBJECT-TYPE
              SYNTAX  INTEGER {
                          closed(1),
                          listen(2),
                          synSent(3),
                          synReceived(4),
                          established(5),
                          finWait1(6),
                          finWait2(7),
                          closeWait(8),
                          lastAck(9),
```

```
                closing(10),
                timeWait(11),
                deleteTCB(12)
            }
        ACCESS  read-write
        STATUS  mandatory
        DESCRIPTION
                "The state of this TCP connection.

                The only value which may be set by a management
                station is deleteTCB(12).  Accordingly, it is
                appropriate for an agent to return a `badValue'
                response if a management station attempts to set
                this object to any other value.

                If a management station sets this object to the
                value deleteTCB(12), then this has the effect of
                deleting the TCB (as defined in RFC 793) of the
                corresponding connection on the managed node,
                resulting in immediate termination of the
                connection.

                As an implementation-specific option, a RST
                segment may be sent from the managed node to the
                other TCP endpoint (note however that RST segments
                are not sent reliably)."
        ::= { tcpConnEntry 1 }

    tcpConnLocalAddress OBJECT-TYPE
        SYNTAX  IpAddress
        ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
                "The local IP address for this TCP connection.  In
                the case of a connection in the listen state which
                is willing to accept connections for any IP
                interface associated with the node, the value
                0.0.0.0 is used."
        ::= { tcpConnEntry 2 }

    tcpConnLocalPort OBJECT-TYPE
        SYNTAX  INTEGER (0..65535)
        ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
                "The local port number for this TCP connection."
        ::= { tcpConnEntry 3 }

    tcpConnRemAddress OBJECT-TYPE
        SYNTAX  IpAddress
        ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
                "The remote IP address for this TCP connection."
        ::= { tcpConnEntry 4 }

    tcpConnRemPort OBJECT-TYPE
        SYNTAX  INTEGER (0..65535)
        ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
                "The remote port number for this TCP connection."
        ::= { tcpConnEntry 5 }
```

4.1.4. MIB-II (RFC1213)

Junto con la MIB de Ethernet, es la mib estándar más importante. Define la segunda versión de la MIB original (MIB-I, RFC1156). MIB-II es más amplia que su antecesora, incluyendo nuevos objetos y grupos.

- » `system`. Información general del sistema.
- » `interfaces`. Información sobre cada uno de las interfaces del dispositivo.
- » `at` (address translation). Deprecado.
- » `ip`. Información relativa al protocolo IP.
- » `icmp`. Información relativa al protocolo ICMP.
- » `tcp`: Información relativa al protocolo TCP.
- » `udp`. Información relativa al protocolo UDP.

» `egp` Información relativa al protocolo EGP.
» `dot3`. Información sobre reglas de transmisión y protocolos de cada interfaz.
» `snmp`. Información sobre implementación y ejecución del protocolo SMP en el sistema.

Si un dispositivo, por ejemplo, implementa el protocolo icmp, entonces debe implementar todos los objetos debajo de icmp.

Por su gran importancia, a continuación se muestran las tablas con los objetos de system (mib-2.1) e interfaces (mib-2.2):

Tabla II: Objeto *system* de la MIB-II.

OIDs	Objeto	Sintaxis	Acceso	Descripción
1.1	**sysDescr**	DisplayString (SIZE (0…255))	RO	Descripción hardware, SSOO, …
1.2	**sysObjectID**	OBJECT IDENTIFIER	RO	Identificación fabricante
1.3	**sysUpTime**	TimeTicks	RO	El tiempo desde que se reinició el software de red.
1.4	**sysContact**	DisplayString (SIZE (0…255))	RW	Información persona de contacto.
1.5	**sysName**	DisplayString (SIZE (0…255))	RW	Nombre del nodo.
1.6	**sysLocation**	DisplayString (SIZE (0…255))	RW	Nombre ubicación física del nodo.
1.7	**sysServices**	INTEGER (0…127)	RO	Un valor numérico que indica el conjunto de servicios que ofrece.

Tabla III: Objeto *interfaces* de la MIB-II.

OIDs	Objeto	Sintaxis	Acceso	Descripción
2.1	**ifNumber**	INTEGER	RO	Número de interfaces de red
2.2	**ifTable**	SEQUENCE OF ifEntry	NA	Lista de entradas de interfaz
2.2.1	**ifEntry**	SEQUENCE	NA	Entrada de interfaz
		Contenido de ifEntry		
2.2.1.1	**ifIndex**	INTEGER	RO	Identifcador único de cada interfaz
2.2.1.2	**ifDescr**	DisplayString (SIZE (0…255))	RO	Información: fabricante, nombre producto, versión.
2.2.1.3	**ifType**	INTEGER	RO	Tipo de interfaz
2.2.1.4	**ifMtu**	INTEGER	RO	Valor de MTU para la interfaz
2.2.1.5	**ifSpeed**	Gauge	RO	Velocidad (bps) de la interfaz
2.2.1.6	**ifPhysAddress**	PhysAddress	RO	MAC address
2.2.1.7	**ifAdminStatus**	INTEGER	RW	Estado deseado: up(1), down(2), testing(3)
2.2.1.8	**ifOperStatus**	INTEGER	RO	Estado actual: up(1), down(2), testing(3)
2.2.1.9	**ifLastChange**	TimeTicks	RO	Valor de sysUpTime desde el valor actual del estado de la inerfaz.
2.2.1.10	**ifInOctets**	Counter	RO	Número total de octetos recibidos.
2.2.1.11	**ifInUcasPackts**	Counter	RO	Número total de paquetes unicast recibidos.
2.2.1.12	**ifInNUcastPkts**	Counter	RO	Número total de paquetes no-unicast recibidos.
2.2.1.13	**ifInDiscards**	Counter	RO	Número de paquetes recibidos descartados.
2.2.1.14	**ifInErrors**	Counter	RO	Número de paquetes descartados por error.
2.2.1.15	**ifInUnknownProtos**	Counter	RO	Número de paquetes con protocolo destino no soportado.
2.2.1.16	**ifOutOctets**	Counter	RO	Número total de octetos transmitidos.
2.2.1.17	**ifOutUcastPkts**	Counter	RO	Número total de paquetes unicast transmitidos.
2.2.1.18	**ifOutNUcastPkts**	Counter	RO	Número total de paquetes no-unicast transmitidos.

OIDs	Objeto	Sintaxis	Acceso	Descripción
2.2.1.19	**ifOutDiscards**	Counter	RO	Número de paquetes transmitidos descartados.
2.2.1.20	**ifOutErrors**	Counter	RO	Número de paquetes descartados por error.
2.2.1.21	**ifOutQLen**	Gauge	RO	Longitud de la cola de paquetes de salida.
2.2.1.22	**ifSpecific**	OBJECT IDENTIFIER	RO	Definiciones específicas en función del medio físico.

4.1.5. Especificación del protocolo

El formato de la PDU (Protocol Data Unit) de SNMP es el siguiente:

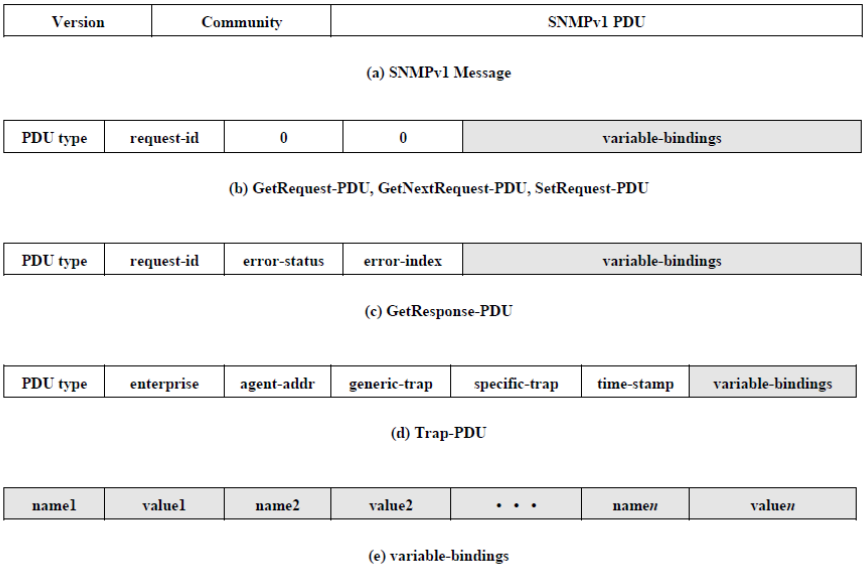


Fig. 6: Formato PDU-SNMP.

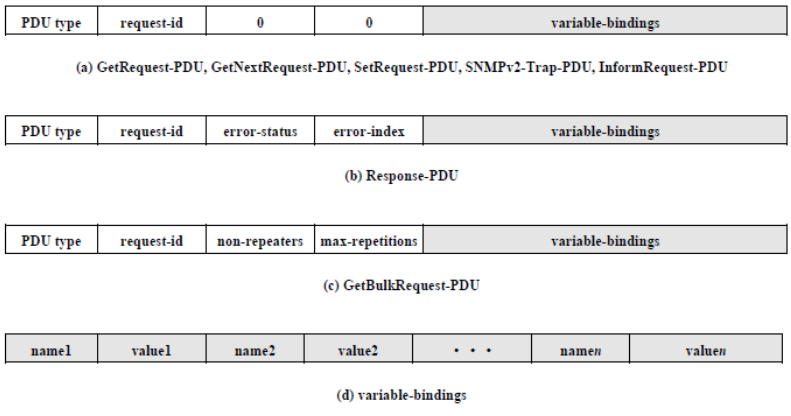


Fig. 7: Formato PDU-SNMPv2.

SNMP permite interrogar a los agentes de gestión por los valores y atributos de las MIBs que tienen implementadas. Es no fiable y no orientado a la conexión, utilizando UDP como protocolo de transporte.

Para la comunicación entre gestores y agentes, utiliza las llamadas *Comunidades*. Las comunidades son nombre (*strings)* que se definen en ambas máquinas para que puedan intercambiar información. La comunidad por defecto se denomina *public*.

Tabla IV: Descripción campos de la PDU de SNMP.

Campo	Descripción
`version`	Versión SNMP
`community`	String que sirve como mecanismo de autentificación entre agentes y estación gestora.
`request-id`	Identificador único para distinguir las peticiones enviadas.
`error-status`	Indica que se ha producido un error al procesar la petición.
`error-index`	Cuando el campo anterior es un valor distinto de cero, sirve para ampliar la información del error.
`variablebindings`	Lista de nombres de variables y valores (se explica más adelante)
`enterprise`	Tipo de objeto que genera el trap
`agent-addr`	Dirección del objeto que genera el trap
`generic-trap`	Tipo de trap genérico: *coldStart(0), warmStart(1), linkDown(2), linkUp(3), authentication-Faillure(4), egpNeighborLoss(5), enterprise-Specific(6).*
`specific-trap`	Código específico de trap.
`time-stamp`	Elapsed time entre la última inicialización de la entidad de red y la generación del trap. Contiene el valor de `sysUpTime`.

Las comunidades pueden ser de lectura o de lectura/escritura, ya que el protocolo permite actualizar variables mediante la primitiva *set*. Normalmente el protocolo se encuentra desactivado (no hay comunidad) o sólo hay una comunidad de lectura (read only community). El motivo principal es porque en algunos sistemas puede existir un agujero de seguridad al utilizar este protocolo.

La comunidad se debe definir en todos los dispositivos y sistemas (switches, routers, máquinas Windows y Linux, etc).

Los problemas más importantes de la versión 1 son que las claves no están cifradas y no hay ACKs (confirmaciones). Hay que tener en cuenta que los objetivos iniciales de diseño fueron la simplicidad y la eficiencia.

Las primitivas son:

- GET(*oid*)
- GET_NEXT(*oid*)
- SET (*oid.instancia=valor*)
- TRAP. Alarma transmitida por el agente. Cuando se produce un evento de un tipo determinado, el dispositivo envía un aviso o trap. Los motivos pueden ser:

coldstart, warmstart, linkup, linkdown, authentic faillure, neighbour loss, ...

Variable bindings

Es un procedimiento que se utiliza cuando se desea agrupar un número determinado de operaciones del mismo tipo (*get*, *set* o *trap*) en un único mensaje. Este procedimiento es muy útil para no generar demasiado tráfico en la red.

4.2. RMON

RMON es un estándar de la IETF (Internet Engineering Task Force) que permite que los agentes de red y los sistemas de gestión de red intercambien datos de monitorización. Se utiliza habitualmente con SNMP para monitorizar, por ejemplo, el tráfico de un conjunto de switches conectados a la red. Permite gestionar una red en vez de cada uno de los dispositivos conectados a ella.

Es la extensión más importante que se ha realizado al conjunto de estándares de SNMP. Los estándares originales relacionados con RMON son RF1513, RFC1757, RFC2021 y RFC2074.

De forma práctica RMON es una MIB especial para realizar funciones de monitorización. Es muy flexible y potente.

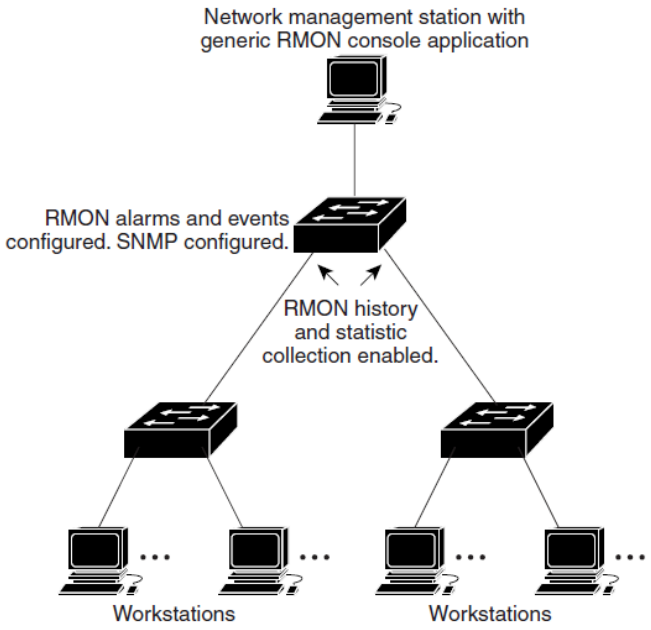


Fig. 8: Monitorización con RMON.

En la red existen dispositivos capaces de implementar funcionalidad RMON, como por ejemplo un router o un switch. Éstos procesan y envían información a la estación gestora.

A un dispositivo que implementa la MIB RMON se le denomina *rmon probe*. Es simplemente una estación con un agente SNMP que puede procesar y generar información RMON. Algunas veces se les denominan agentes RMON, aunque este término es menos apropiado.

La especificación de RMON define estadísticas y funciones a intercambiar y está organizado en 9 grupos. RMON fue definido por la IETF en 1992 (RFC 1271) y actualizado por las RFC 1757 y RFC2819. El estándar es el STD0059 (2000).

La nueva versión de RMON (v2) es Remote Network Monitoring Management Information Base Version 2 (RFC4502, draft standard). Fue desarrollada en 2006.

4.2.1. Objetivos de RMON

Aunque es una MIB, su objetivo principal es definir funciones e interfaces para proveer un mecanismo de comunicación entre estaciones de gestión SNMP y estaciones monitoras remotas. De forma específica, RMON persigue:

- Operaciones off-line. Son posibles bajo demanda para de recibir notificaciones de un monitor. Éste seguirá acumulando información y estadísticas hasta que vuelva a ser demandado por la estación gestora. Esta funcionalidad es interesante en caso de fallo de otros dispositivos, o para reducir el ancho de banda consumido por la gestión de red.
- Monitorización proactiva. Si el monitor tiene suficientes recursos, puede estar de forma continua ejecutando diagnósticos y evaluando el comportamiento de la red. Si se produce algún fallo en la red, el monitor puede enviar la información de forma rápida.
- Detección de fallos y generación de informes. El monitor puede analizar el tráfico en la red y detectar fallos sin necesidad de que la estación gestora esté de forma continua realizando sondeos.
- Pre-procesamiento de información. El monitor puede realizar análisis previos de los datos que recoge y enviar datos más elaborados a la estación gestora.
- Múltiples gestores. Capacidad para dialogar con más de una estación gestora. Esta funcionalidad es útil en redes complejas donde cada estación gestora está especializada en determinadas tareas.

4.2.2. MIB RMON. Grupos RMON

La parte esencial de la especificación de la MB RMON está ahora incluida en la MIB-II, debajo del subárbol 16 (mib-2.16).

La MIB RMON está dividida en diez grupos:

- Grupo 1 (`statistics`). Tiene que ver con la recolección de estadísticas en interfaces de tipo Ethernet.
- Grupo 2 (`history`). Tiene que ver con la recolección de grupos de históricos sobre estadísticas.
- Grupo 3 (`alarm`). Tiene que ver con la monitorización de un objeto específico de una MIB, en un intervalo dado.
- Grupo 4 (`host`). Contiene contadores para varios tipos de tráfico hacia y desde los host conectados a una subred.
- Grupo 5 (`hostTopN`). Contiene estadísticas ordenadas que informan de los hosts que están por encima de ellas en las tablas.
- Grupo 6 (`matrix`). Muestra errores e información de utilización en forma de matrices.
- Grupo 7 (`filter`). Permite al monitor buscar paquetes que se correspondan con filtros definidos.
- Grupo 8 (`capture`). Configura la forma de enviar la información a la estación gestora.

» Grupo 9 (`event`). Proporciona una tabla con todos los eventos generados por la estación RMON.
» Grupo 10 (`tokenRing`). Información de gestión para redes Token-Ring (en desuso).

Tabla V: Grupos RMON.

RMON GROUP	FUNCTION	ELEMENTS
Statistics	Contains statistics measured by the probe for each monitored interface on this device.	Packets dropped, packets sent, bytes sent (octets), broadcast packets, multicast packets, CRC errors, runts, giants, fragments, jabbers, collisions, and counters for packets ranging from 64 to 128, 128 to 256, 256 to 512, 512 to 1024, and 1024 to 1518 bytes.
History	Records periodic statistical samples from a network and stores them for later retrieval.	Sample period, number of samples, items sampled.
Alarm	Periodically takes statistical samples from variables in the probe and compares them with previously configured thresholds. If the monitored variable crosses a threshold, an event is generated.	Includes the alarm table and requires the implementation of the event group. Alarm type, interval, starting threshold, stop threshold.
Host	Contains statistics associated with each host discovered on the network.	Host address, packets, and bytes received and transmitted, as well as broadcast, multicast, and error packets.
HostTopN	Prepares tables that describe the hosts that top a list ordered by one of their base statistics over an interval specified by the management station. Thus, these statistics are rate-based.	Statistics, host(s), sample start and stop periods, rate base, duration.
Matrix	Stores statistics for conversations between sets of two addresses. As the device detects a new conversation, it creates a new entry in its table.	Source and destination address pairs and packets, bytes, and errors for each pair.
Filters	Enables packets to be matched by a filter equation. These matched packets form a data stream that might be captured or that might generate events.	Bit-filter type (mask or not mask), filter expression (bit level), conditional expression (and, or not) to other filters.
Packet Capture	Enables packets to be captured after they flow through a channel.	Size of buffer for captured packets, full status (alarm), number of captured packets.
Events	Controls the generation and notification of events from this device.	Event type, description, last time event sent.

4.3. RMON2

El estándar de RMON2 se empezó a desarrollar en 1994 como una extensión de la MIB RMON para incluir monitorización del tráfico sobre el nivel MAC[2]. El estándar se definió en 1997 mediante dos RFCs.

RMON2 decodifica paquetes de los niveles 3 al 7 del modelo OSI (red a aplicación). Esta posibilidad tiene dos implicaciones importantes:

» Una sonda RMON puede monitorizar tráfico a nivel de red del modelo OSI, incluyendo el protocolo IP. Esto posibilita a la sonda aprender más allá de los segmentos de LAN en los que están conectados y analizar el tráfico que reciben o generan los routers. Con esta capacidad una sonda RMON puede averiguar: si hay excesiva carga en la red debido al tráfico de entrada del router y qué redes o hosts son el destino/origen de ese tráfico; si un router está sobrecargado por excesivo tráfico saliente y el origen de ese tráfico; si hay demasiado tráfico que no tiene origen o destino en la propia subred y quién genera ese tráfico.
» Ya que RMON puede monitorizar tráfico a nivel de aplicación (p. ej. e-mail, transferencia de ficheros,…) las sondas pueden registrar tráfico asociado a una

[2] Subnivel de control de acceso al medio (Medium Access Control) del modelo IEEE802.

determinada aplicación. De esta forma se puede tener un control mucho más exhaustivo del tráfico que generan los usuarios y aplicaciones.

4.3.1. MIB RMON2

La MIB de RMON2 es simplemente una extensión de la MIB RMON original, a la que se añaden 9 grupos más:

Tabla VI: Grupos RMON2.

Grupo RMON2	Mib-2.16.x
protocoldir	(11)
protocoldist	(12)
addressmap	(13)
n1host	(14)
n1matrix	(15)
a1host	(16)
a1matrix	(17)
usrhistory	(18)
probeconfig	(19)

Incluye dos funcionalidades nuevas importantes: la posibilidad de utilizar objetos que permiten indexar tablas, y funcionalidad para filtrar en función del cambio de valor de un objeto desde la última vez que se sondeó.

4.4. SNMPv2

Uno de los problemas más graves con los que se ha identificado al protocolo SNMP es su falta de seguridad. En efecto, este protocolo ha sido uno de los agujeros de seguridad más importantes ya que el uso de nombres de comunidad y mensajes en texto plano es una técnica muy insegura.

Al igual que otros protocolos en sus inicios, los desarrolladores estuvieron más preocupados por la funcionalidad o las prestaciones, que en la seguridad, que por entonces no era un problema tan acuciante como en la actualidad. En la versión 1, la arquitectura es totalmente centralizada. Una estación gestora sólo se comunica con los agentes, por lo que se genera mucho tráfico hacia la estación que además es responsable de una carga de procesamiento considerable. Con SNMPv2, la arquitectura puede ser distribuida, pudiendo haber varias estaciones gestoras que se comuniquen entre sí.

SNMPv2 extiende la funcionalidad de SNMP para:

- Incluir gestión basada en OSI (CMIP over TCP).
- Ampliar su capacidad introduciendo nuevas definiciones de objetos, tablas, notificaciones y módulos de información. Las PDUs de SNMPv2 pueden ser encapsuladas en mensajes SNMPv1 y SNMPv3.

Con respecto al protocolo, SNMPv2 hay tres tipos de acceso a la información de gestión. Solamente es nuevo en SNMPv2 el segundo tipo de comunicación:

- Manager-agent request-response. Una entidad SNMPv2 actuando como gestor envía una petición a una entidad SNMPv2 actuando como agente. Ésta responde con una confirmación. Se utiliza como en SNMPv1, pero con confirmación.
- Manager-manager request-response. Una entidad SNMPv2 actuando con el rol de gestora, envía una petición a otra actuando con el mismo rol. Ésta devuelve una respuesta. Este tipo se utiliza para notificar el rol de manager entre estas entidades.
- Agent-manager unconfirmed. Una entidad SNMPv2 actuando como agente envía un mensaje no solicitado (trap) a una entidad gestora sin enviar respuesta. Se utiliza para notificar a la estación gestora un evento en el dispositivo monitorizado.

SNMPv2 incluye una nueva MIB (manager-to-manager MIB) que permite utilizar tablas para controlar eventos disparados por diversas circunstancias.

Otra ventaja de SNMPv2, es que añade la primitiva GetBulk que permite aumentar el volumen de datos que se pueden transferir en una PDU, reduciendo así el excesivo número de PDU de SNMP que se enviaban en la versión 1. También optimiza la primitiva Get. La primitiva GetBulk permite enviar tablas de datos, operación que antes se debía hacer utilizando una primitiva por fila.

4.5. SNMPv3

SNMPv2 amplía SNMPv1 pero no añade seguridad al protocolo. Por este motivo se desarrolló SNMPv3, normalizado originalmente en: RFC2271 a RFC2275 (enero 1998).

La novedad más importante en el desarrollo de esta versión, es la incorporación de mecanismos de seguridad: tunnelling, TLS, SSH, Kerberos. En las versiones anteriores el string de la comunidad se transmitía en ASCII plano. No todos los dispositivos permiten utilizar todos los mecanismos de seguridad, por lo que se aconseja verificar primero las especificaciones de cumplimiento de SNMP.

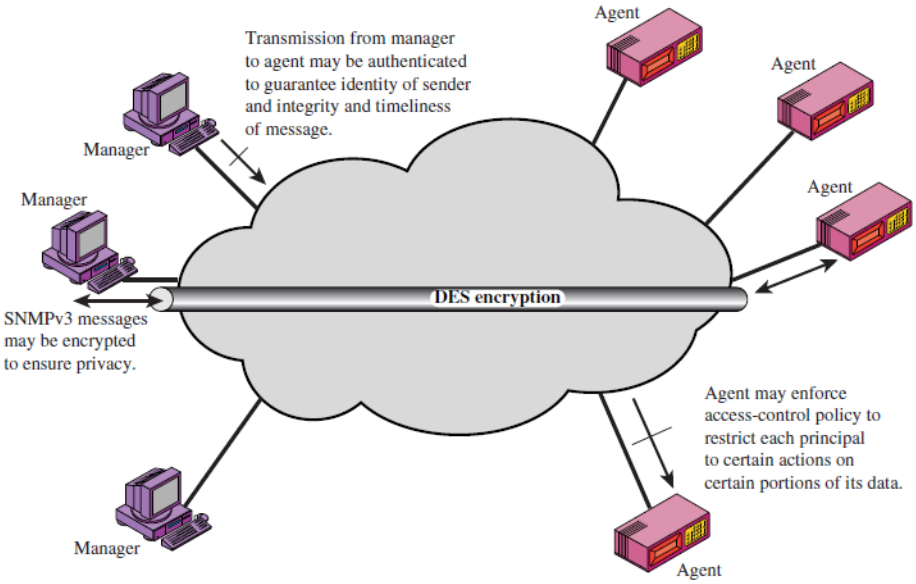


Fig. 9: Funcionamiento de SNMPv3.

Al igual que con SNMPv2, es posible la coexistencia con agentes y estaciones gestoras de las tres versiones del protocolo.

Muchos de los plugins y dispositivos utilizados para el desarrollo de este proyecto, permiten utilizar la versión 3 de este protocolo. Por cuestiones de simplicidad, ya que se supone que este documento es el primer paso para poder desarrollar la plataforma de gestión de red, se ha utilizado siempre la versión 1. En versiones sucesivas se podrán abordar más cuestiones de configuración de este protocolo.

5. INSTALACIÓN Y CONFIGURACIÓN DE UNA PLATAFORMA DE GESTIÓN DE RED

La instalación de la herramienta Nagios se puede realizar de formas diferentes: manual y automatizada.

La instalación manual supone la descarga del código fuente, configuración de los ficheros a compilar, compilación y configuración manual de las tareas post-instalación. Aunque no es un proceso demasiado complicado, requiere algunos conocimientos de administración de sistemas UNIX-LINUX.

Con la instalación automatizada a través del repositorio, se descargan los ficheros binarios y se realizan la mayor parte de tareas de instalación y configuración. Si la distribución del repositorio es correcta y está bien mantenida, el resultado deber ser equivalente a la instalación manual, por lo que deben existir los mismos directorios con el mismo o equivalente contenido. Tiene la ventaja de que sólo se necesita el conocimiento de las herramientas propias de descarga e instalación como *aptitude* (Advanced Packaging Tool, APT) o equivalentes.

En el manual para este curso se ha decidido incluir los dos modos, el manual y el automático. Como recomendación general, se suele realizar la instalación con binarios a menos que se necesite alguna configuración especial en la instalación, en cuyo caso la instalación manual es más específica.

5.1. Instalación automatizada

La instalación de Nagios es muy parecida en las distintas distribuciones LINUX. En este manual se utilizará como referencia Ubuntu LINUX. En el manual se utilizará la versión 11.04.

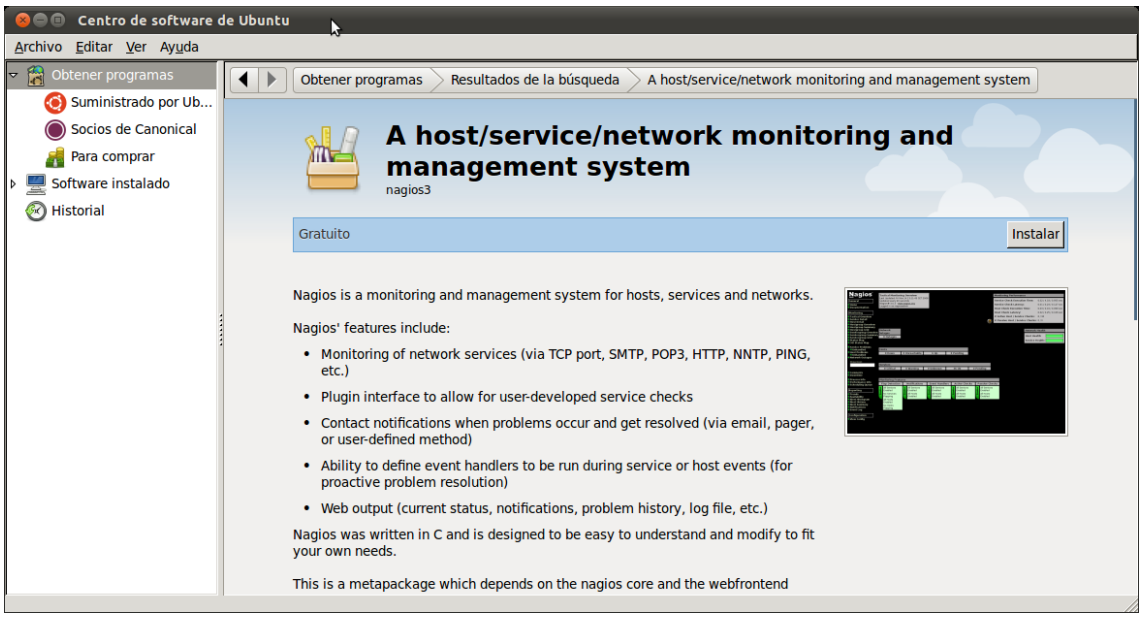


Fig. 10: Instalación de Nagios 3 desde el centro de software de Ubuntu

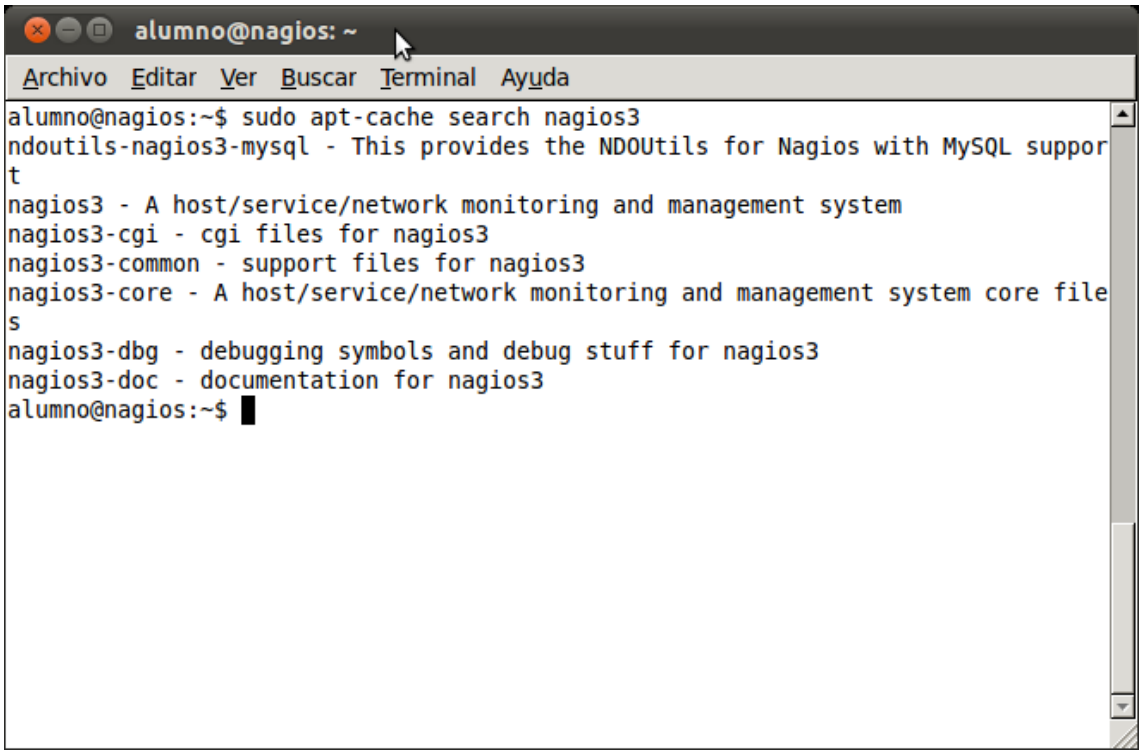


Fig. 11: Búsqueda de binarios de Nagios en Ubuntu.

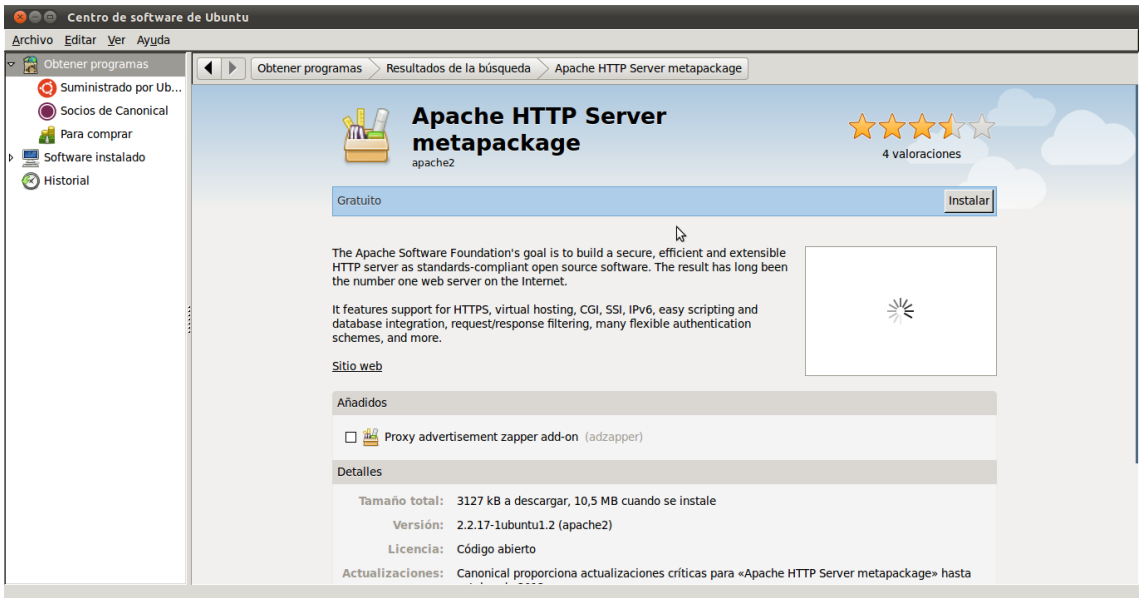


Fig. 12: Instalación del servidor Apache2 desde el centro de software de Ubuntu.

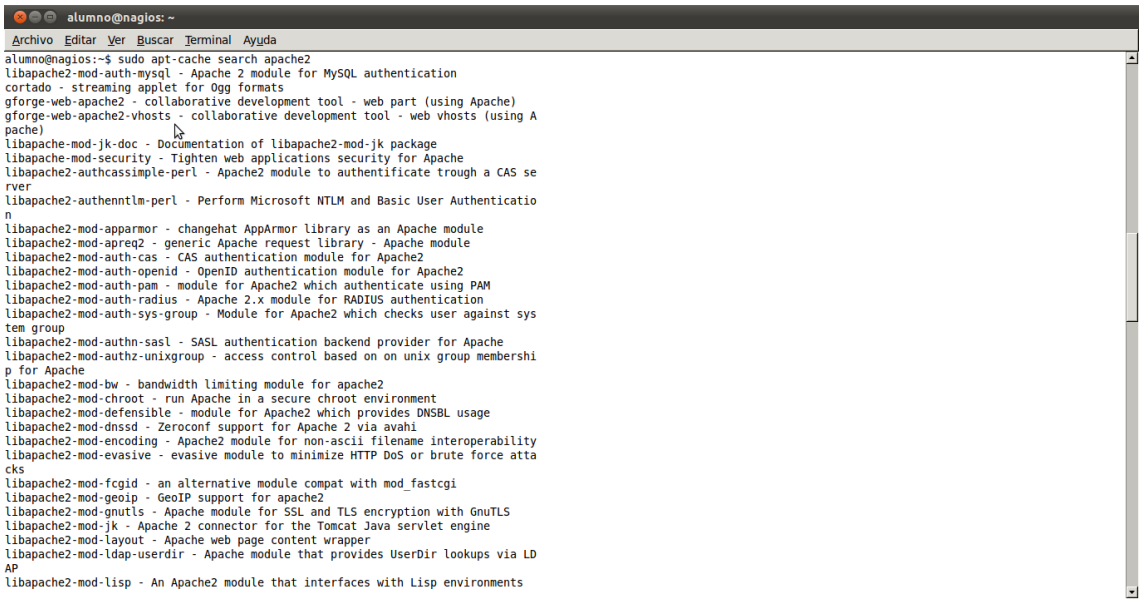


Fig. 13: Instalación de binarios de Apache.

5.2. Instalación Manual

5.2.1. Prerrequisitos y preparación de la instalación

Como prerrequisitos, se necesitan instalar las herramientas de compilación, librerías y el servidor web (Apache). Los paquetes a instalar son:

```
sudo apt-get install build-essential openssh-server
sudo apt-get install apache2 libgd2-xpm-dev php5 libapache2-mod-php5
```

Si se necesita un entorno seguro, se debe configurar Apache para poder acceder con conexión segura mediante ssl:

```
sudo a2enmod ssl
sudo a2ensite default-ssl
```

Reiniciar apache[3] y comprobar que el apache2 funciona:

```
sudo /etc/init.d/apache2 restart
```

[3] *restart* o *relod* según sea necesario

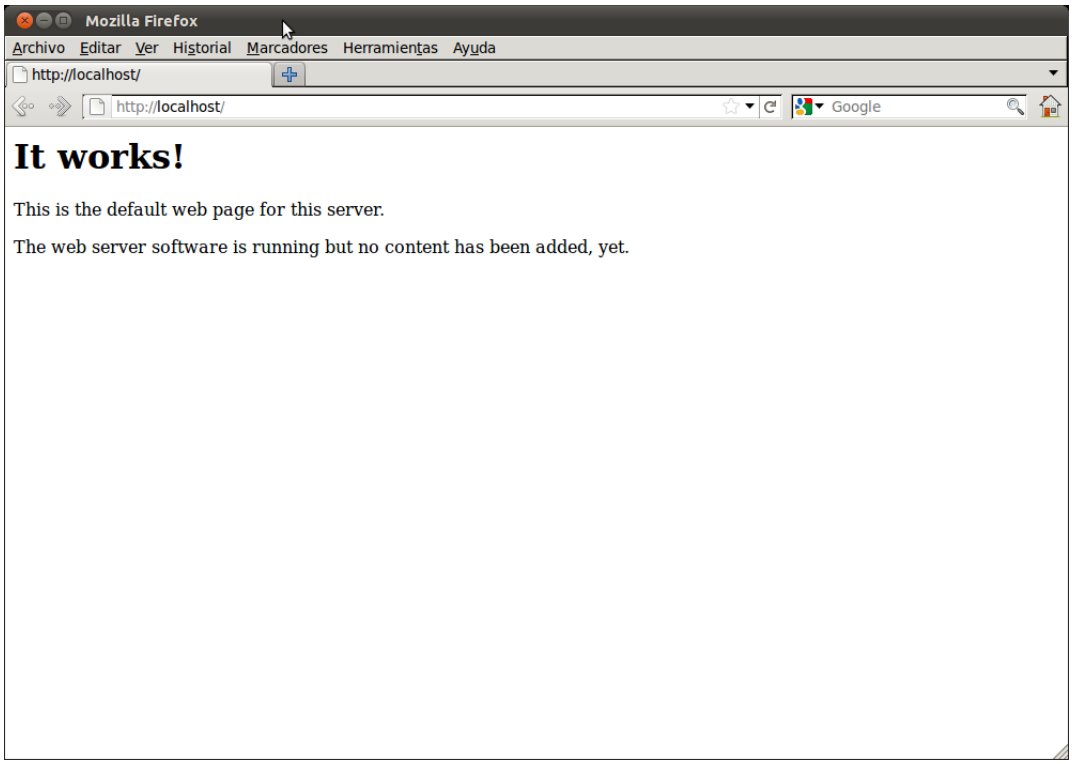


Fig. 14: Comprobación de la página inicial del servidor Apache.

Fig. 15: Comprobación página inicial Apache con https.

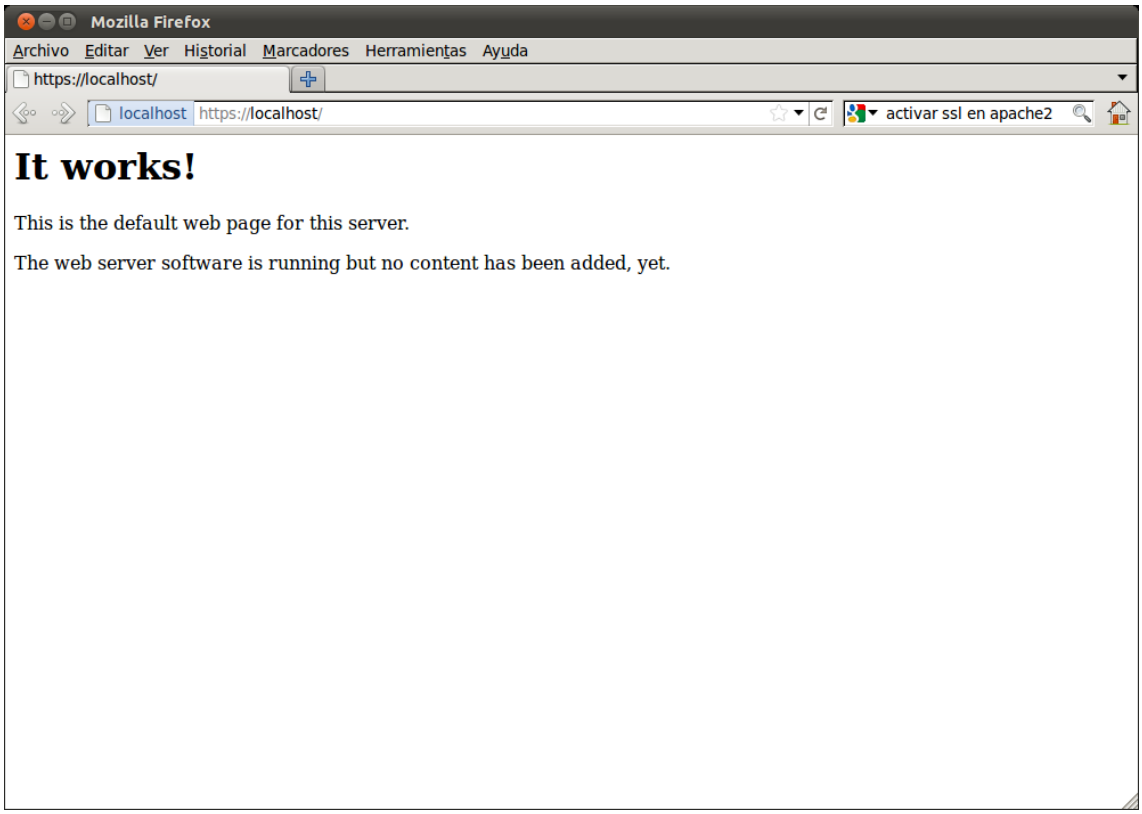


Fig. 16: Comprobación página inicial Apache con https (II).

Comprobación de PHP5:

Crear el fichero phpinfo.php en /var/www y comprobar con el navegador:

```
<?php
  phpinfo();
?>
```

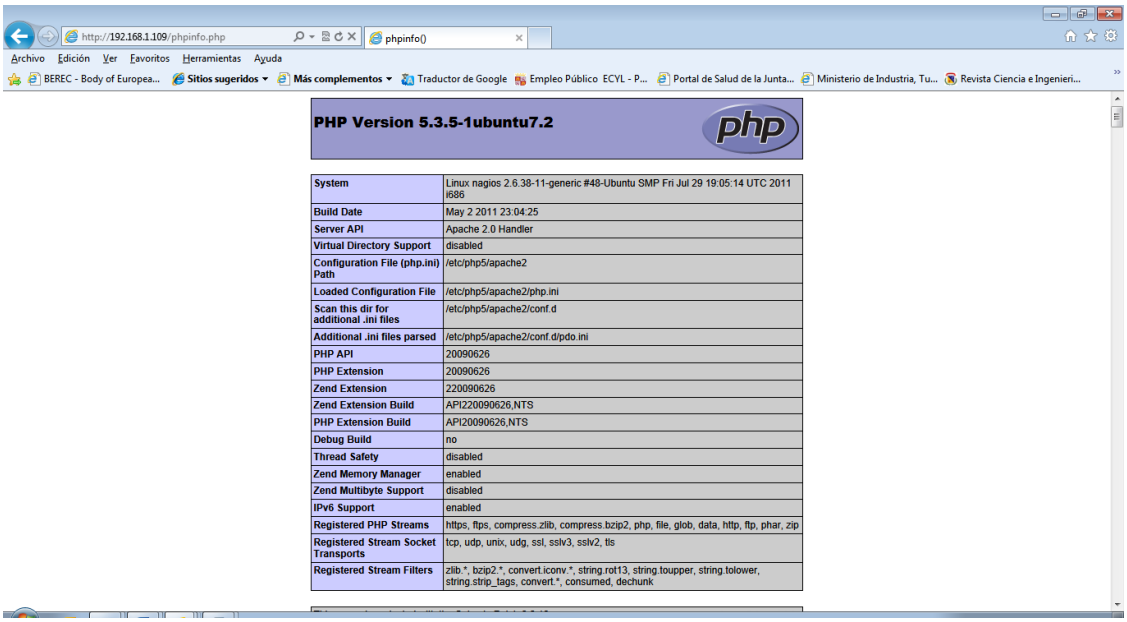


Fig. 17: Comprobación PHP5 instalado y configurado.

En las páginas de ayuda del servidor de Ubuntu se puede encontrar documentación sobre la instalación básica del servidor Apache[4].

También será necesario instalar el protocolo SNMP (net-snmp[5]) si se quiere utilizar posteriormente. Si no se instala previamente, la instalación de Nagios no lo tendrá en cuenta:

```
sudo apt-get install snmp
```

No obstante, es recomendable descargar el paquete de la web[6] y compilarlo en el sistema:

```
./configure
make
sudo make install
```

Este paquete lleva incorporada la MIBS que serán necesarias para utilizar SNMP más tarde.

Ninguna de las opciones anteriores instala el agente SNMP en el equipo. Para ello se debe instalar el paquete snmpd (demonio de Linux):

```
sudo apt-get install snmpd
```

5.2.2. Creación de usuarios y grupos

Entrar al modo root:

```
sudo -s
```

Crear el usuario nagios:

```
useradd -m -s /bin/bash nagios
passwd nagios
```

Crear un grupo y asociar los usuarios *nagios* y *www-data* (usuario Apache2[7]):

```
groupadd nagcmd
usermod -a -G nagcmd nagios
usermod -a -G nagcmd www-data
```

5.2.3. Compilación

Descargar y descomprimir el código fuente de Nagios core y plugins:

```
mkdir nagios
cd nagios
wget http://prdownloads.sourceforge.net/sourceforge/nagios/nagios-3.3.1.tar.gz
wget http://prdownloads.sourceforge.net/sourceforge/nagiosplug/nagios-plugins-1.4.15.tar.gz
tar xvf nagios-3.3.1.tar.gz
cd nagios
```

Primero se ha de compilar la herramienta y después los plugins:

[4] https://help.ubuntu.com/11.04/serverguide/C/httpd.html
[5] http://net-snmp.sourceforge.net
[6] http://www.net-snmp.org/download.html
[7] Comprobar con: sudo grep "USER" /etc/apache2/envvars

Tabla VII: Parámetros configuración instalación Nagios

Propiedad	Valor	Opción en configure
Root directory	/usr/local/nagios	--prefix
Configuration directory	/etc/nagios	--sysconfdir
Directory for variable data	/var/nagios	--localstatedir
Nagios user (UserID)	nagios (9000)	--with-nagios-user
Nagios group (GroupID)	nagios (9000)	--with-nagios-group
Nagios Command Group	nagcmd (9001)	--with-command-group

Preparar la instalación con *configure*:

```
./configure --sysconfdir=/etc/nagios --localstatedir=/var/nagios --with-command-group=nagcmd
```

Una vez haya terminado, se mostrará el resumen de la instalación que se va a realizar:

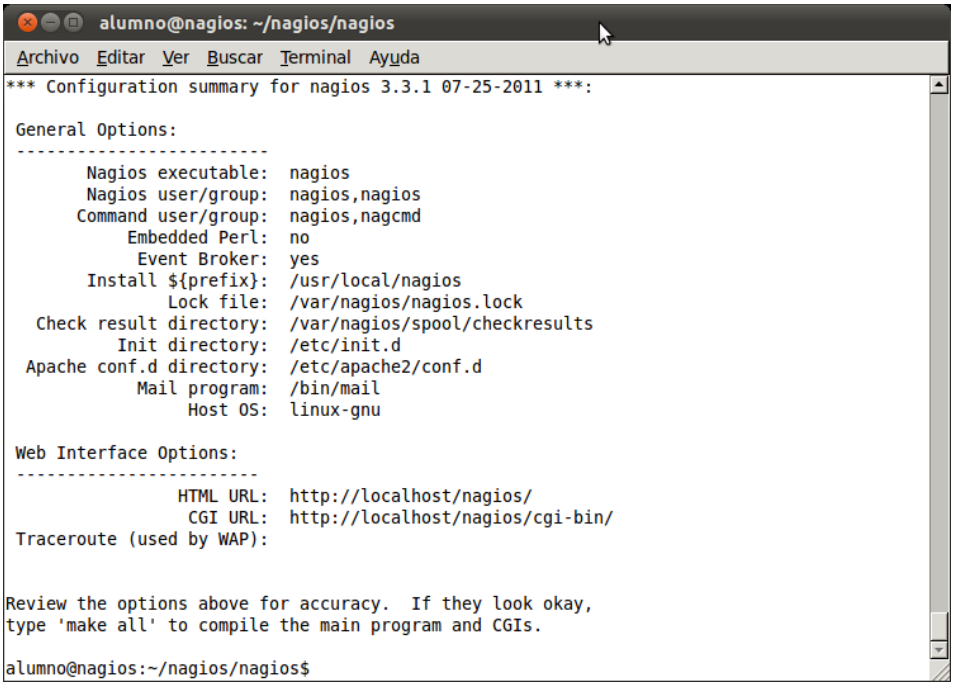


Fig. 18: Resultado de configure

```
make all

sed -i 's:for file in includes/rss/\*;:for file in includes/rss/\*.\*;:g' ./html/Makefile

sed -i 's:for file in includes/rss/extlib/\*;:for file in includes/rss/extlib/\*.\*;:g'
./html/Makefile

make install
make install-init
make install-commandmode
make install-config
```

Los comandos marcados con las líneas son los que hay que ejecutar si se instala con Ubuntu[8].

5.2.4. Configuración de la interfaz web (Apache)

Instalar interfaz web y añadir usuario administrador web:

```
sudo make install-webconf
cd /etc/nagios
sudo htpasswd -c htpasswd.users nagiosadmin
```

Arrancar de nuevo Apache:

```
sudo /etc/init.d/apache2 reload
```

5.2.5. Arranque automático

Para hacer que Nagios arranque automáticamente, ejecutar:

```
sudo update-rc.d nagios defaults 99
```

5.2.6. Instalación de plugins

Las siguientes líneas sirve para instalar los plugins de Nagios, una vez descargados de la página web de Nagios (archivo tar.gz):

```
sudo tar xvf nagios-plugins-1.4.15.tar.gz
cd nagios-plugins-1.4.15
./configure --with-nagios-user=nagios --with-nagios-group=nagios --sysconfdir=/etc/nagios --
localstatedir=/var/nagios
sudo make
sudo make install
```

5.2.7. Comprobación de la instalación de Nagios

A continuación se muestra una lista de comprobaciones que se deben realizar para verificar que Nagios y los plugins están correctamente instalados. Se recomienda reiniciar apache y nagios[9] si no aparece:

» Apache (https://direccionIP)

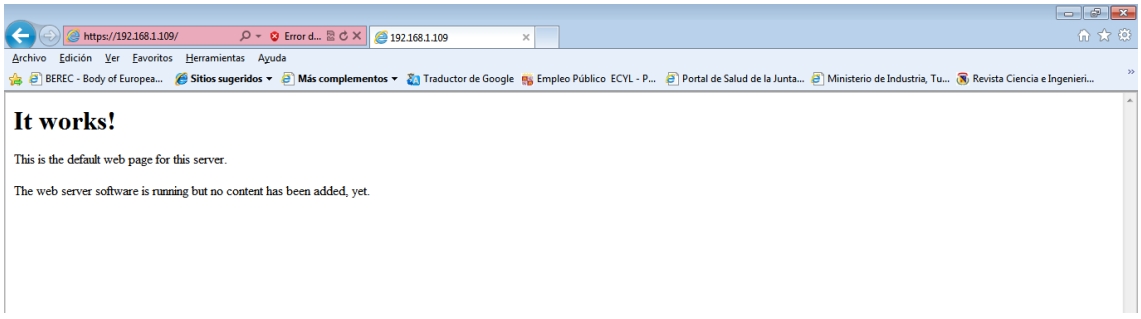


Fig. 19: Página de inicio de Apache.

» PHP (https://direccionIP/phpinfo.php)

[8] Son necesarias también para la útlima versión de Ubuntu (11.10).
[9] sudo /etc/init.d/apache2 restart y sudo /etc/init.d/nagios restart.

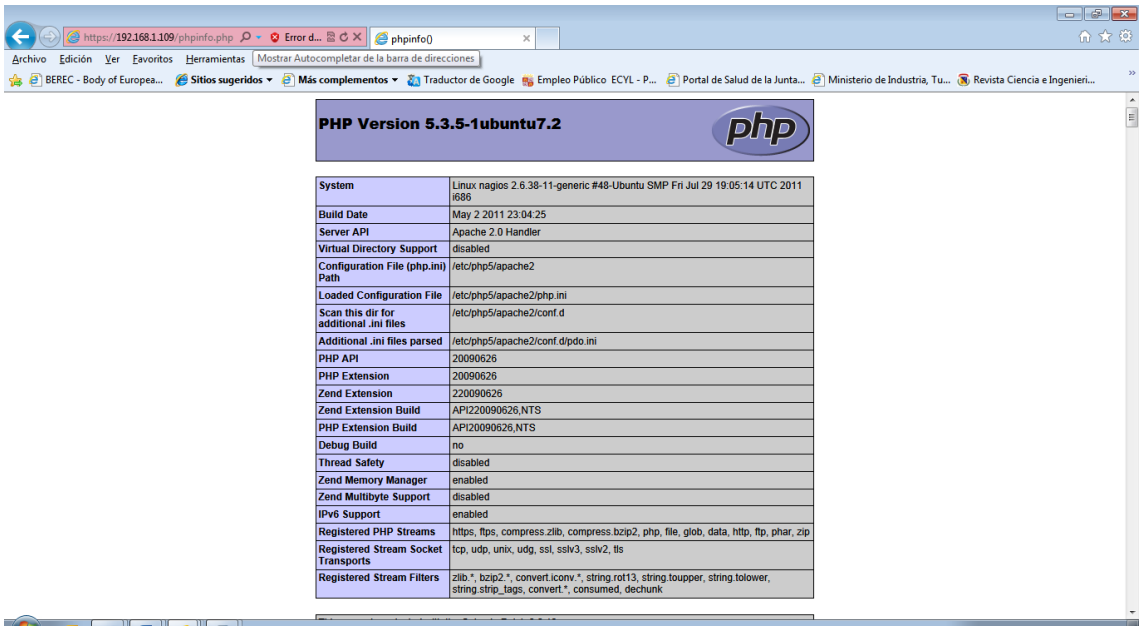


Fig. 20: Página de información de PHP5

» Nagios (https://direccionIP/nagios)

Fig. 21: Página de inicio de Nagios.

» Nagios plugins

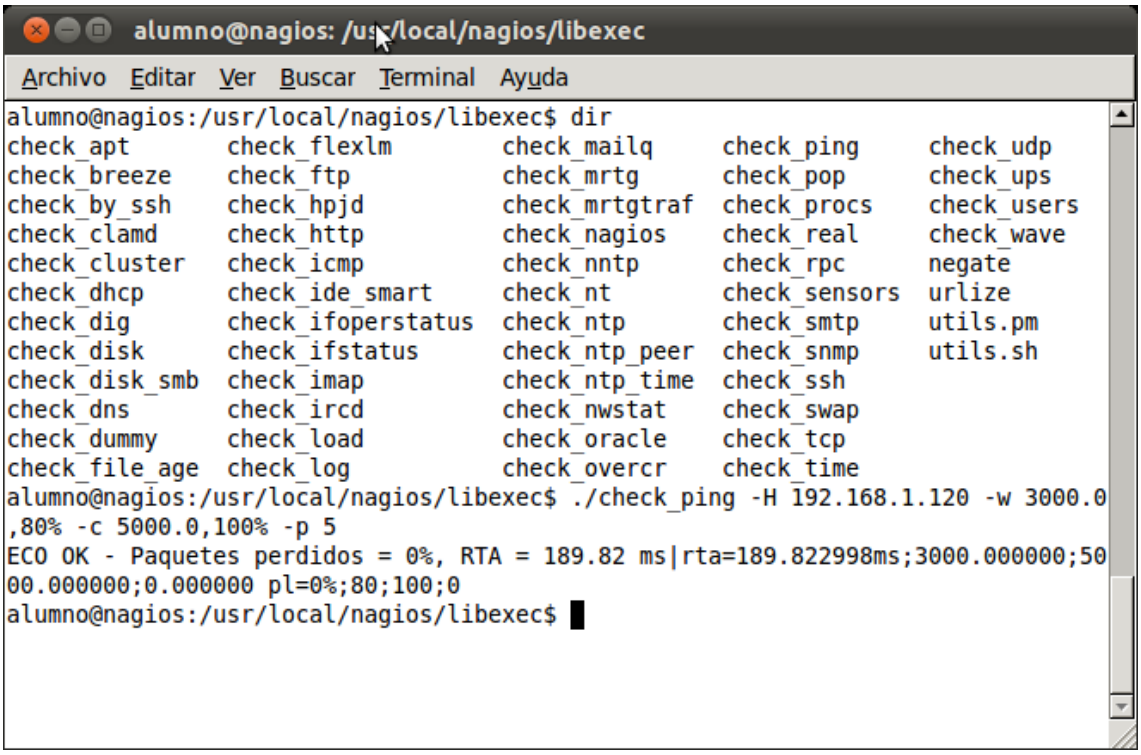


Fig. 22: Directorio de plugins de Nagios.

A continuación, se muestra el resultado de la ejecución del comando check_dhcp, que comprueba el estado de un servidor dhcp (192.168.0.1). Es recomendable probar con una dirección MAC de vuestra red:

```
alumno@nagios:/usr/local/nagios/libexec$ ./check_dhcp -v -s 192.168.1.1 -t 5.0 -m 1c:4b:d6:6f:60:c9
Dirección de servidor solicitada: 192.168.1.1
Dirección de hardware: 1c:4b:d6:6f:60:c9
DHCP socket: 3
DHCPDISCOVER a 255.255.255.255 puerto 67
DHCPDISCOVER XID: 1506331007 (0x59C8C97F)
DHCDISCOVER ciaddr:  0.0.0.0
DHCDISCOVER yiaddr:  0.0.0.0
DHCDISCOVER siaddr:  0.0.0.0
DHCDISCOVER giaddr:  0.0.0.0
resultado send_dhcp_packet: 548




recv_result_1: 548
recv_result_2: 548
resultado receive_dhcp_packet(): 548
fuente receive_dhcp_packet(): 192.168.1.1
Resultado=OK
DHCPOFFER desde la dirección IP 192.168.1.1 vía 192.168.1.1
DHCPOFFER XID: 1506331007 (0x59C8C97F)
DHCPOFFER chaddr: 1C4BD66F60C9
DHCPOFFER ciaddr: 0.0.0.0
DHCPOFFER yiaddr: 192.168.1.102
DHCPOFFER siaddr: 192.168.1.1
DHCPOFFER giaddr: 0.0.0.0
Option: 53 (0x01)
Option: 54 (0x04)
Option: 51 (0x04)
Option: 1 (0x04)
Option: 3 (0x04)
Option: 6 (0x08)
Option: 15 (0x04)
Tiempo de vida: 86400 segundos
Tiempo de renovación: 0 segundos
```

```
Tiempo de revinculación: 0 segundos
Oferta añadida del servidor @ 192.168.1.1 de la dirección IP 192.168.1.102

No (more) data received (nfound: 0)
Resultado=ERROR
Respuestas totales vistas sobre el cable: 1
Respuestas válidas para esta máquina: 1
Coincidencia del servidor DHCP: Oferente=192.168.1.1 Solicitado=192.168.1.1
OK: Received 1 DHCPOFFER(s), 1 de 1 servidores solicitados respondieron, tiempo máximo del
ofrecimiento = 86400 sec.
alumno@nagios:/usr/local/nagios/libexec$ ./check_dhcp -v -s 192.168.1.1 -t 5.0 -m 00-c0-9f-9e-1f-55
Dirección de servidor solicitada: 192.168.1.1
Dirección de hardware: 00:c0:9f:9e:1f:55
DHCP socket: 3
DHCPDISCOVER a 255.255.255.255 puerto 67
DHCPDISCOVER XID: 512946284 (0x1E92F06C)
DHCDISCOVER ciaddr:  0.0.0.0
DHCDISCOVER yiaddr:  0.0.0.0
DHCDISCOVER siaddr:  0.0.0.0
DHCDISCOVER giaddr:  0.0.0.0
resultado send_dhcp_packet: 548

recv_result_1: 548
recv_result_2: 548
resultado receive_dhcp_packet(): 548
fuente receive_dhcp_packet(): 192.168.1.1
Resultado=OK
DHCPOFFER desde la dirección IP 192.168.1.1 vía 192.168.1.1
DHCPOFFER XID: 512946284 (0x1E92F06C)
DHCPOFFER chaddr: 00C09F9E1F55
DHCPOFFER ciaddr: 0.0.0.0
DHCPOFFER yiaddr: 192.168.1.120
DHCPOFFER siaddr: 192.168.1.1
DHCPOFFER giaddr: 0.0.0.0
Option: 53 (0x01)
Option: 54 (0x04)
Option: 51 (0x04)
Option: 1 (0x04)
Option: 3 (0x04)
Option: 6 (0x08)
Option: 15 (0x04)
Tiempo de vida: 86400 segundos
Tiempo de renovación: 0 segundos
Tiempo de revinculación: 0 segundos
Oferta añadida del servidor @ 192.168.1.1 de la dirección IP 192.168.1.120

No (more) data received (nfound: 0)
Resultado=ERROR
Respuestas totales vistas sobre el cable: 1
Respuestas válidas para esta máquina: 1
Coincidencia del servidor DHCP: Oferente=192.168.1.1 Solicitado=192.168.1.1
OK: Received 1 DHCPOFFER(s), 1 de 1 servidores solicitados respondieron, tiempo máximo del
ofrecimiento = 86400 sec.
alumno@nagios:/usr/local/nagios/libexec$
```

6. CONFIGURACIÓN

6.1. Ficheros de Configuración de NAGIOS

6.1.1. Directorio de configuración de Nagios.

La configuración de la herramienta se hace desde el directorio /etc/nagios, cuya estructura se refleja en la siguiente figura:

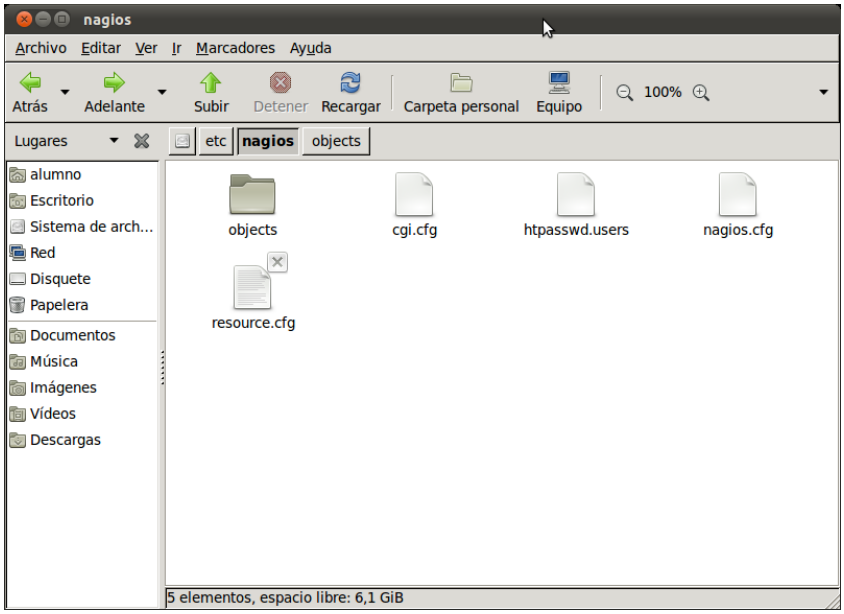


Fig. 23: Directorio de configuración de Nagios

En el directorio etc/nagios/objects se almacenan los ficheros de configuración de objetos:

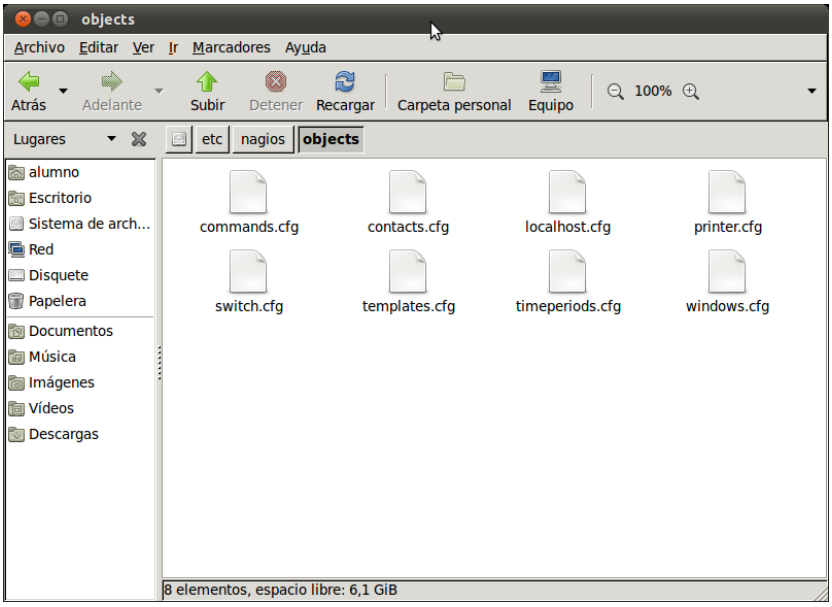


Fig. 24: Ficheros de configuración de Nagios.

Los tres ficheros principales de configuración son *nagios.cfg*, *cgi.cfg* y *resource.cfg*. Si alguno de los ficheros se edita o crea con el usuario *root*, hay que asegurarse después que todos los ficheros pertenezcan al usuario nagios:

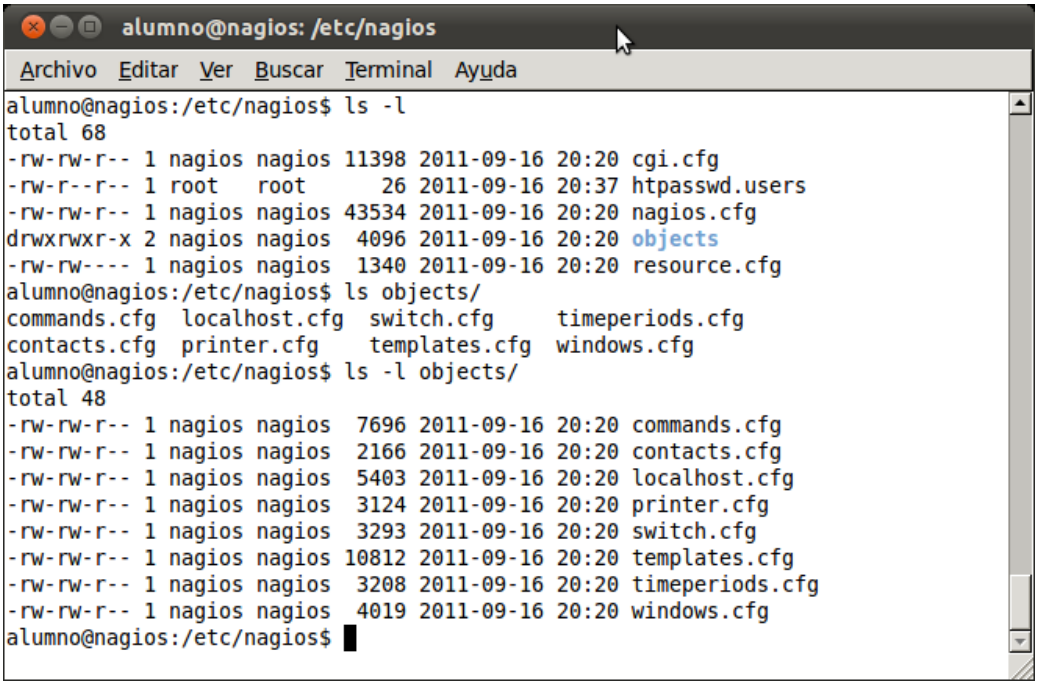


Fig. 25: Propietario de los ficheros de configuración

Si no es así, utilice los comandos *chmod* y *chown* para cambiar permisos y propietario (respectivamente).

6.1.2. Revisión fichero de Log

Es conveniente, para realizar tareas de depuración, consultar el fichero de log que está almacenado en */var/nagios/nagios.log*:

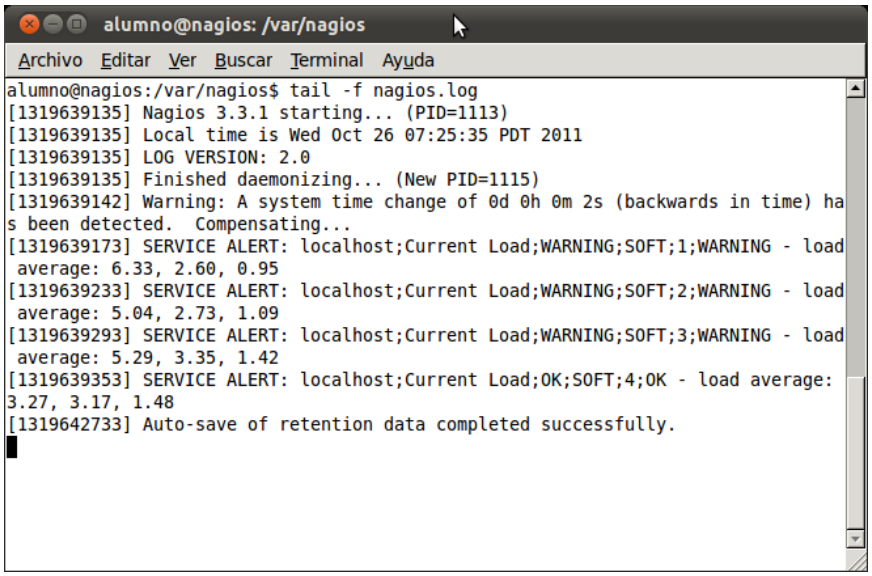


Fig. 26: Fichero de log de Nagios

6.1.3. Fichero de configuración nagios.cfg

La configuración de Nagios se maneja desde este fichero, que incluye a su vez otros ficheros. Esto posibilita organizar mejor toda la información de configuración.

Para ello se utiliza el parámetro cfg_file, que incluye un fichero de configuración que contiene otros objetos:

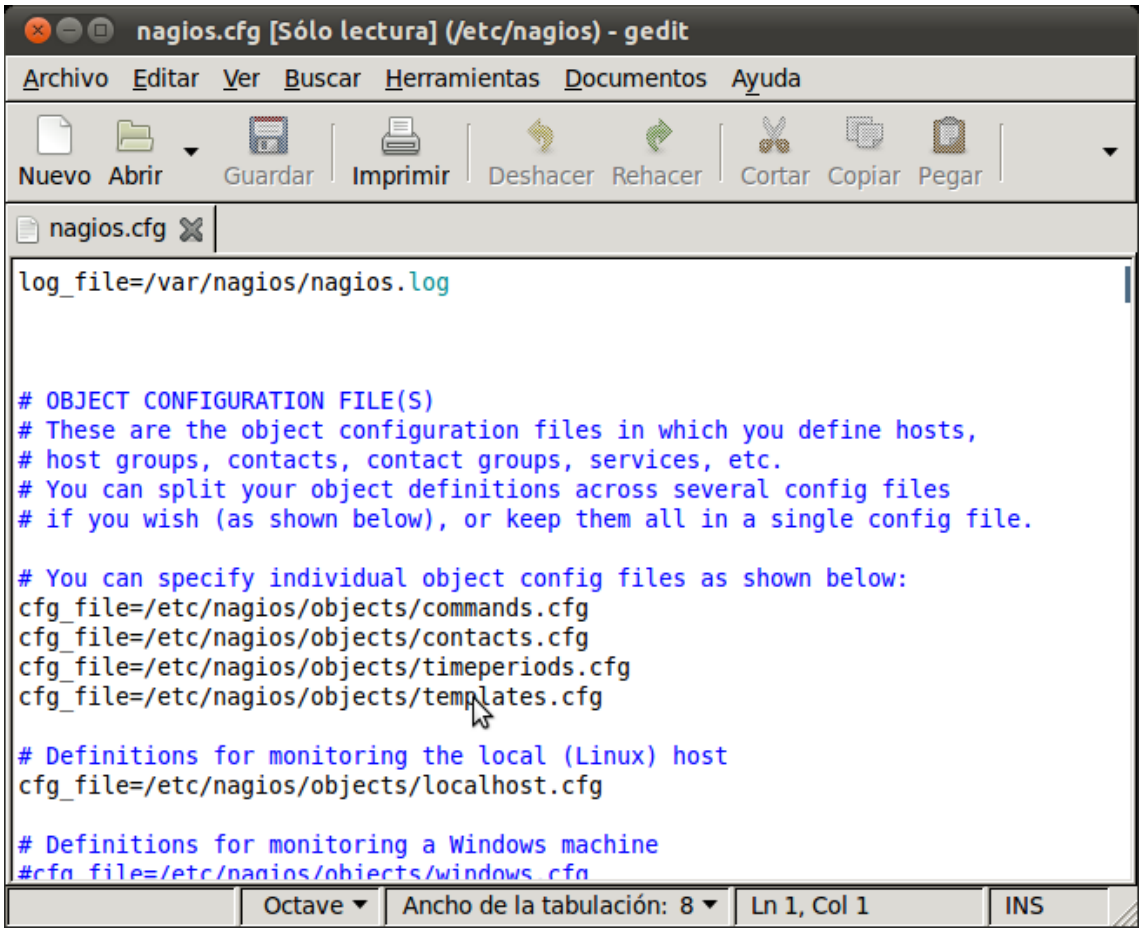


Fig. 27: Inclusión ficheros configuración mediante *cfg_file*.

También es posible incluir un directorio. Nagios buscará e incluirá todos los ficheros bajo la estructura del directorio especificado:

```
cfg_dir = /etc/nagios/SACYL
```

Se recomienda hacer un análisis previo de los requisitos y organizar la estructura de forma adecuada. Para grandes organizaciones, se recomienda definir objetos en ficheros separados y agrupar en subdirectorios:

```
.
|-- nagios.cfg
|-- cgi.cfg
|-- resource.cfg
|-- htpasswd
`-- mysite
    |-- contactgroups.cfg
    |-- misccommands.cfg
    |-- contacts.cfg
    |-- timeperiods.cfg
    |-- checkcommands.cfg
    |-- hosts.cfg
    |-- services.cfg
    `-- hostgroups.cfg
```

```
...
`-- mysite
    |-- linux
    |   |-- services
    |   `-- hosts
    |       |-- linux01.cfg
    |       |-- linux02.cfg
    |       `-- linux03.cfg
    |-- windows
    |   |-- services
    |   `-- hosts
    |       |-- win03.cfg
    |       `-- win09.cfg
    `-- router
        |-- services
        `-- hosts
            |-- edge01.cfg
            |-- edge02.cfg
            `-- backbone.cfg
```

```
|-- global
| |-- commands
| | |-- check-host-alive.cfg
| | |-- check_http.cfg
| | |-- check_icmp.cfg
... ... ...
| |-- contacts
| | |-- nagios.cfg
... ... ...
| |-- templates
| | |-- host_generic_t.cfg
| | |-- service_generic_t.cfg
| | |-- service_perfdata_t.cfg
... ... ...
| `-- timeperiods
`-- sites
|-- foreignsite
| |-- hosts
| `-- services
|-- mysite
| |-- hosts
| `-- services
`-- othersite
|-- hosts
`-- services
```

Fig. 28: Diferentes estructuras de directorios de configuración

Control de actualizaciones:

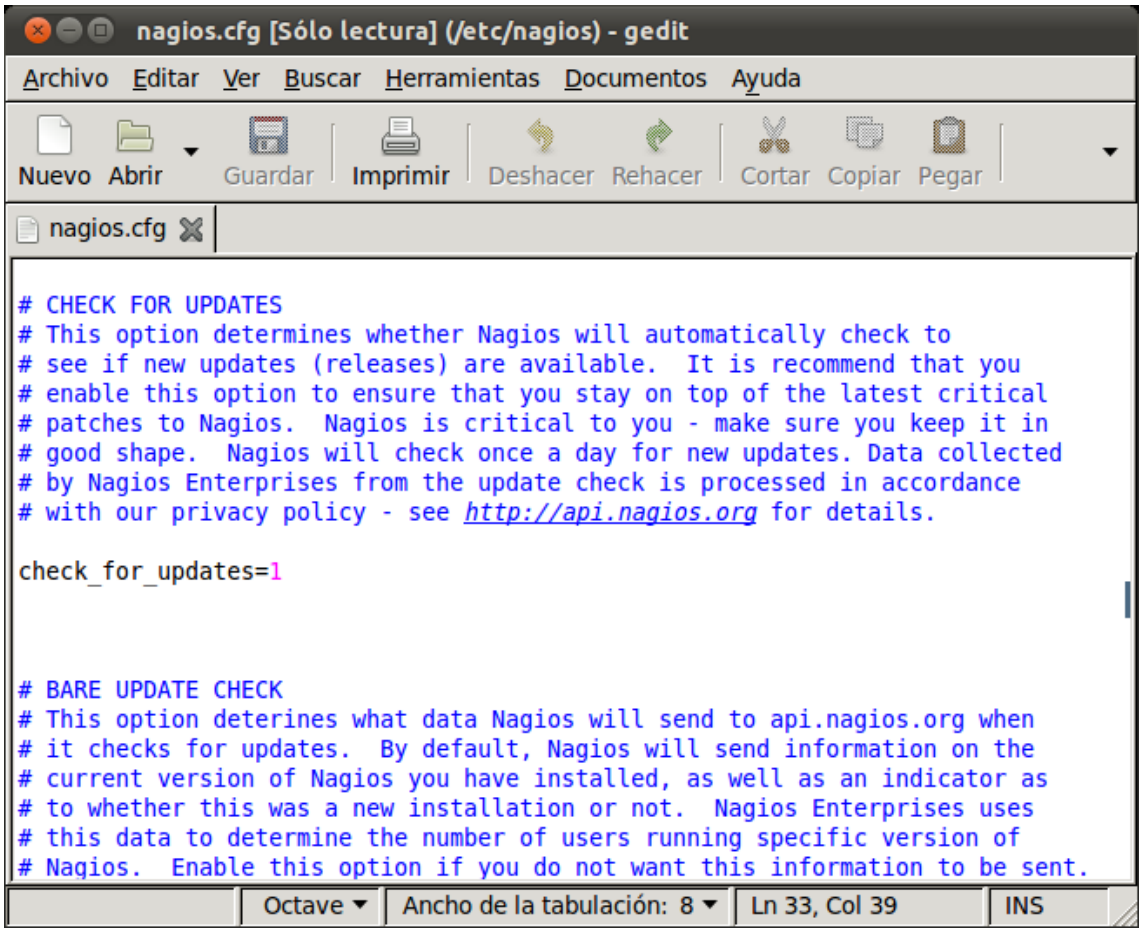


Fig. 29: Configuración de actualizaciones

También es importante definir el formato de la fecha:

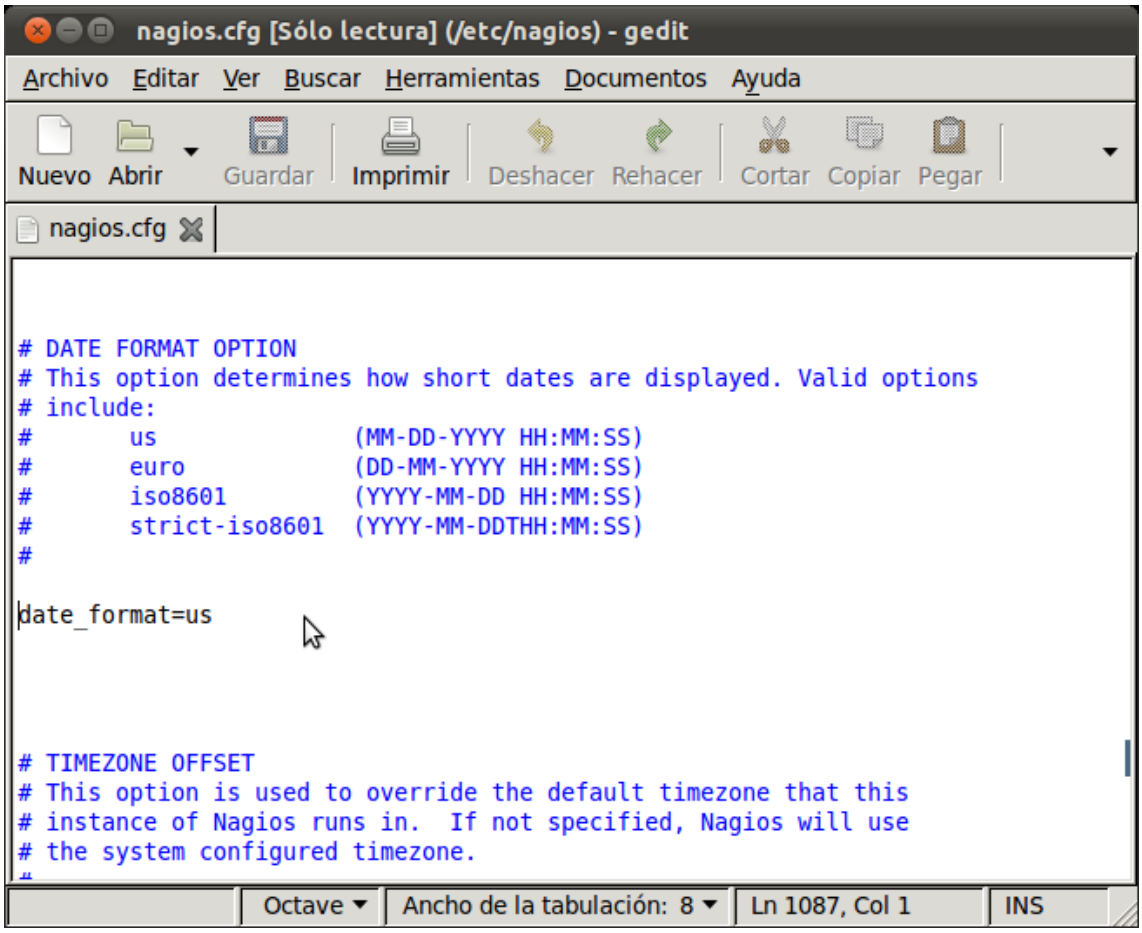


Fig. 30: Formato de fecha en Nagios.

Se puede definir la información de contacto en:

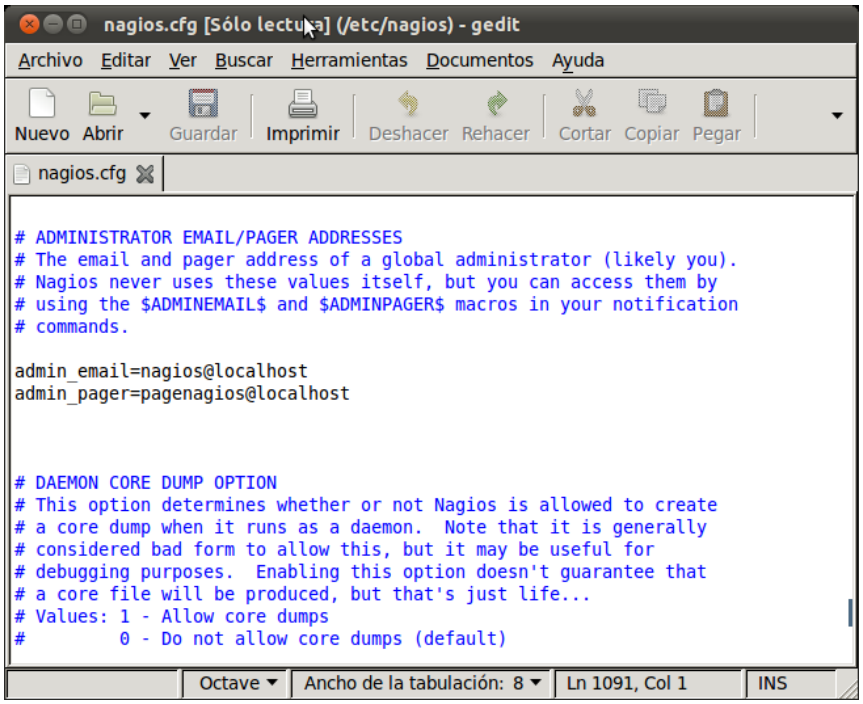


Fig. 31: Configuración de la información de contacto

6.1.4. Fichero de configuración cgi.cfg

En este fichero se podrán definir los directorios de Nagios y el uso o no de autentificación. Por defecto la autentificación está habilitada:

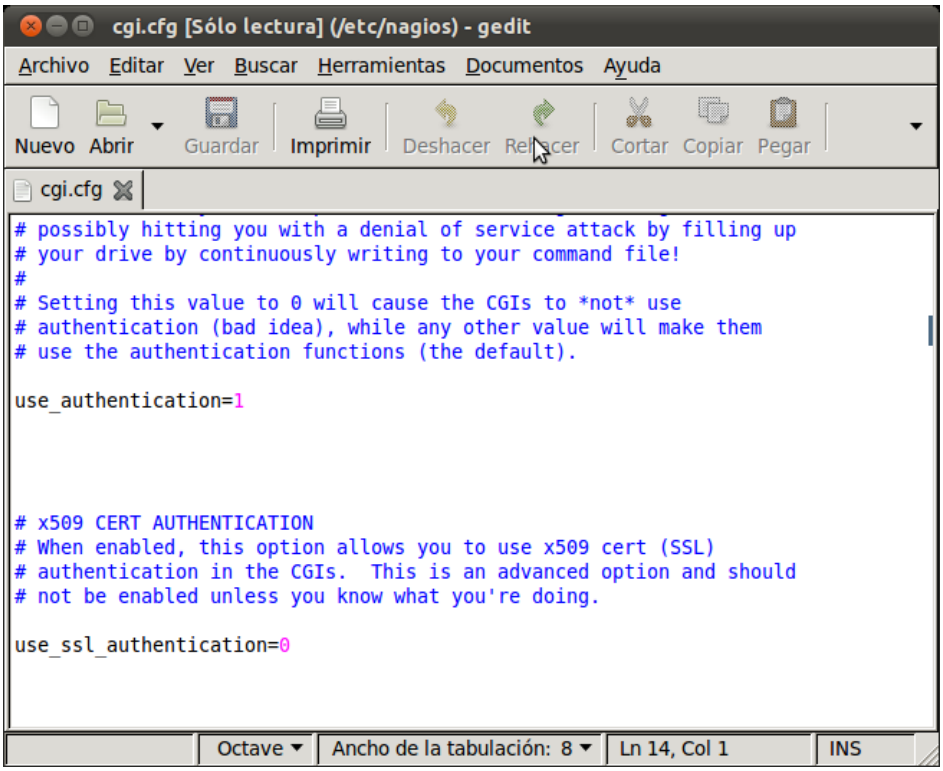


Fig. 32: Configuración autentificación

6.1.5. Arranque y parada de Nagios

Para actualizar cualquier configuración, se debe volver a cargar Nagios:

```
sudo /etc/init.d/nagios start/stop/restart/reload
```

Si hay algún problema con el servidor Apache, también se puede reiniciar:

```
sudo /etc/init.d/apache2 start/stop/restart/reload
```

Hay que tener en cuenta que para cualquier cambio en la configuración de Nagios, se debe actualizar con el comando nagios reload. Sin embargo, no se debe hacer de forma continua, ya que una vez actualizada la configuración, Nagios empezará a ejecutar las tareas programadas de nuevo.

Para que no arranquen todas a la vez[10], se pueden configurar los parámetros: *max_service_check_spread* y *max_host_check_spread*.

6.2. Tipos de Objetos en Nagios

La estructura de los objetos es la siguiente:

[10] El procedimiento se denomina *spreading*.

```
define object-type {
parameter value
parameter value
...
}
```

Los tipos son los siguientes (se incluyen las definiciones del manual de Nagios):

host
The host object describes one of the network nodes that are to be monitored. Nagios expects the IP address as a parameter here (or the Fully Qualified Domain Name) and the command that should define whether the host is alive. The host definition is re-referenced in the service definition.

hostgroup

Several hosts can be combined into a group. This simplifies configuration, since entire host groups instead of single hosts can be specified when defining services (the service will then exist for each member of the group). In addition, Nagios represents the hosts of a host group together in a table in the Web front end, which helps to increase clarity.

service

The individual services to be monitored are defined as service objects. A service never exists independently of a host. So it is quite possible to have several services with the same name, as long as they belong to different hosts. The following code,

```
define service
{
name PING
host_name linux01
...
}

define service
{
name PING
host_name linux03
}
```

describes two services that both have the same service name but belong to different hosts. So in the language of Nagios, a service is always a host-service pair.

servicegroup

As it does with host groups, Nagios combines several services and represents these in the Web front end as a unit with its own table. Service groups are not absolutely essential, but help to improve clarity, and are also used in reporting.

contact

A person who is to be informed by Nagios of specific events. Nagios uses contact objects to show to a user via the Web front end only those things for which the user is listed as a contact person. In the basic setting users do not get to see hosts and services for which they are not responsible.

contactgroup

Notification of events in hosts and services takes place via the contact group. A direct link between the host/service and a contact person is not possible.

timeperiod

Describes a time period within which Nagios should inform contact groups. Outside such a time slot, the system will not send any messages. The messaging chain can be fine-tuned via various time periods, depending on the host/service and contact/ contact groups.

command

Nagios always calls external programs via command objects. Apart from plugins, messaging programs also include e-mail or SMS messaging applications.

servicedependency

This object type describes dependences between services. If, for example, an application does not function without a database, a corresponding dependency object will ensure that Nagios will represent the failed database as the primary problem instead of just announcing the nonfunctioning of the application.

servicescalation

Used to define proper escalation management: if a service is not available after a specific time period, Nagios informs a further or different circle of people. This can also be configured on multiple levels in any way you want.

hostdependency

Like servicedependency, but for hosts.

hostscalation

Like servicescalation, but for hosts.

6.2.1. Definición de hosts

El siguiente código define localhost en el fichero de ejemplo (localhost.cfg), que por defecto crea la herramienta en la instalación:

```
define host{
        use     linux-server ; Name of host template to use
        ; This host definition will inherit all variables that are defined
        ; in (or inherited by) the linux-server host template definition.
        host_name               localhost
        alias                   localhost
        address                 127.0.0.1
        }
```

Utiliza las plantillas definidas en el fichero /etc/nagios/objects/*templates.cfg*:

```
define host{
        name    generic-host    ; The name of this host template
```

```
        notifications_enabled    1        ; Host notifications are enabled
        event_handler_enabled    1        ; Host event handler is enabled
        flap_detection_enabled   1        ; Flap detection is enabled
        failure_prediction_enabled      1 ; Failure prediction is enabled
        process_perf_data        1        ; Process performance data
        retain_status_information   1     ; Retain status information across program restarts
        retain_nonstatus_information    1 ; Retain non-status information across program restarts
        notification_period      24x7     ; Send host notifications at any time
        register  0  ;DONT REGISTER THIS DEFINITION - ITS NOT A REAL HOST, JUST A TEMPLATE!
        }


# Linux host definition template - This is NOT a real host, just a template!

define host{
        name     linux-server     ; The name of this host template
        use      generic-host     ; This template inherits other values from the generic-host
template
        check_period     24x7     ; By default, Linux hosts are checked round the clock
        check_interval   5                ; Actively check the host every 5 minutes
        retry_interval   1                ; Schedule host check retries at 1 minute intervals
        max_check_attempts       10               ; Check each Linux host 10 times (max)
        check_command            check-host-alive ; Default command to check Linux hosts
        notification_period      workhours        ; Linux admins hate to be woken up, so we only
notify during the day
        ; Note that the notification_period variable is being overridden from
        ; the value that is inherited from the generic-host template!
        notification_interval    120      ; Resend notifications every 2 hours
        notification_options     d,u,r    ; Only send notifications for specific host states
        contact_groups           admins   ; Notifications get sent to the admins by default
        register         0
; DONT REGISTER THIS DEFINITION - ITS NOT A REAL HOST, JUST A TEMPLATE!
        }

define host{
        name                     windows-server   ; The name of this host template
        use                      generic-host     ; Inherit default values from the generic-host
template
        check_period             24x7             ; By default, Windows servers are monitored round
the clock
        check_interval           5                ; Actively check the server every 5 minutes
        retry_interval           1       ; Schedule host check retries at 1 minute intervals
        max_check_attempts       10               ; Check each server 10 times (max)
        check_command            check-host-alive ; Default command to check if servers are "alive"
        notification_period      24x7             ; Send notification out at any time - day or night
        notification_interval    30               ; Resend notifications every 30 minutes
        notification_options     d,r              ; Only send notifications for specific host states
        contact_groups           admins           ; Notifications get sent to the admins by default
        hostgroups       windows-servers ; Host groups that Windows servers should be a member of
        register         0                ; DONT REGISTER THIS - ITS JUST A TEMPLATE
        }
```

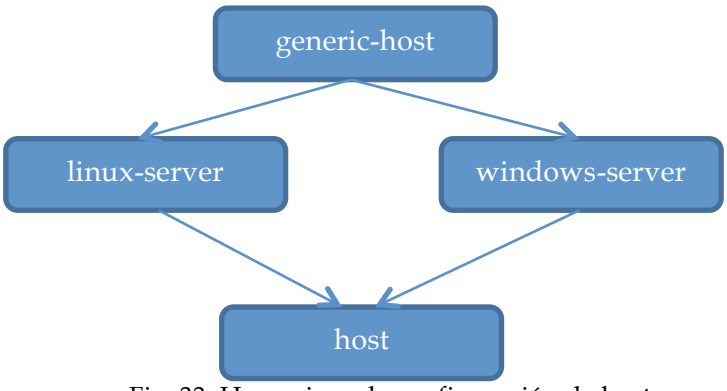


Fig. 33: Herencia en la configuración de hosts.

6.2.2. Agrupación de hosts

Se utiliza para agrupar un número determinado de hosts que aparecerán juntos en la interfaz web. Además, se pueden asociar determinados servicios a grupos de hosts, por lo que no es necesario ir asignándolos uno a uno.

El objeto necesario para agrupar host es *hostgroup*:

```
# Define an optional hostgroup for Linux machines

define hostgroup{
        hostgroup_name  linux-servers ; The name of the hostgroup
        alias           Linux Servers ; Long name of the group
        members         localhost     ; Comma separated list of hosts that belong to this group
        }
```

Una vez definido el grupo, se puede incluir el host en la sección *members*. La lista con los miembros se separa por comas.

En la definición de host, también se puede utilizar el parámetro *hostgroup*. Se pueden combinar ambas definiciones. En Nagios 3.0[11] se pueden hacer asociaciones de grupos y así crear una jerarquía.

También se puede utilizar * en el campo members, para incluir a todos los hosts.

6.2.3. Definición de servicios a monitorizar

Un servicio en Nagios consiste en la combinación de un host y un nombre de servicio. Esta combinación debe ser única. Los nombres de servicios pueden aparecer más de una vez ya que pueden estar asociados a otros hosts.

El servicio más simple es un *ping*. Testea si un host está online y además devuelve información sobre el tiempo de respuesta y la pérdida de paquetes. Nagios realiza un host check si no puede testear ningún otro servicio en el host. Es menos útil que un ping.

Ejemplo de definición de servicios:

```
# Define a service to "ping" the local machine

define service{
        use                             local-service         ; Name of service template to use
        host_name                       localhost
        service_description             PING
        check_command                     check_ping!100.0,20%!500.0,60%
        }
# Define a service to check the disk space of the root partition
# on the local machine.  Warning if < 20% free, critical if
# < 10% free space on partition.

define service{
        use                             local-service         ; Name of service template to use
        host_name                       localhost
        service_description             Root Partition
        check_command                     check_local_disk!20%!10%!/
        }
# Define a service to check the number of currently logged in
# users on the local machine.  Warning if > 20 users, critical
# if > 50 users.
```

[11] En la versión 2 de Nagios esto no es posible.

```
define service{
        use                             local-service         ; Name of service template to use
        host_name                       localhost
        service_description             Current Users
        check_command                     check_local_users!20!50
        }
# Define a service to check the number of currently running procs
# on the local machine.  Warning if > 250 processes, critical if
# > 400 users.

define service{
        use                             local-service         ; Name of service template to use
        host_name                       localhost
        service_description             Total Processes
        check_command                     check_local_procs!250!400!RSZDT
        }
# Define a service to check the load on the local machine.

define service{
        use                             local-service         ; Name of service template to use
        host_name                       localhost
        service_description             Current Load
        check_command                     check_local_load!5.0,4.0,3.0!10.0,6.0,4.0
        }
# Define a service to check the swap usage the local machine.
# Critical if less than 10% of swap is free, warning if less than 20% is free

define service{
        use                             local-service         ; Name of service template to use
        host_name                       localhost
        service_description             Swap Usage
        check_command                     check_local_swap!20!10
        }


# Define a service to check SSH on the local machine.
# Disable notifications for this service by default, as not all users may have SSH enabled.

define service{
        use                             local-service         ; Name of service template to use
        host_name                       localhost
        service_description             SSH
        check_command                     check_ssh
        notifications_enabled             0
        }

# Define a service to check HTTP on the local machine.
# Disable notifications for this service by default, as not all users may have HTTP enabled.

define service{
        use                             local-service         ; Name of service template to use
        host_name                       localhost
        service_description             HTTP
        check_command                     check_http
        notifications_enabled             0
        }
```

Estos servicios incluyen la definición de local-service, incluido en el fichero templates.cfg:

```
# Generic service definition template - This is NOT a real service, just a template!

define service{
        name                            generic-service    ; The 'name' of this service template
        active_checks_enabled           1                  ; Active service checks are enabled
        passive_checks_enabled          1                  ; Passive service checks are
enabled/accepted
        parallelize_check               1                  ; Active service checks should be
parallelized (disabling this can lead to major performance problems)
        obsess_over_service             1                  ; We should obsess over this service (if
necessary)
        check_freshness                 0                  ; Default is to NOT check service
'freshness'
        notifications_enabled           1                  ; Service notifications are enabled
        event_handler_enabled           1                  ; Service event handler is enabled
```

```
        flap_detection_enabled          1                ; Flap detection is enabled
        failure_prediction_enabled      1                ; Failure prediction is enabled
        process_perf_data               1                ; Process performance data
        retain_status_information       1                ; Retain status information across program
restarts
        retain_nonstatus_information    1                ; Retain non-status information across
program restarts
        is_volatile                     0                ; The service is not volatile
        check_period                    24x7                    ; The service can be checked at
any time of the day
        max_check_attempts              3                ; Re-check the service up to 3 times in
order to determine its final (hard) state
        normal_check_interval           10               ; Check the service every 10 minutes under
normal conditions
        retry_check_interval            2                ; Re-check the service every two minutes
until a hard state can be determined
        contact_groups                  admins                  ; Notifications get sent out to
everyone in the 'admins' group
        notification_options              w,u,c,r                ; Send notifications about
warning, unknown, critical, and recovery events
        notification_interval           60               ; Re-notify about service problems every
hour
        notification_period             24x7                    ; Notifications can be sent out
at any time
        register                         0               ; DONT REGISTER THIS DEFINITION - ITS NOT
A REAL SERVICE, JUST A TEMPLATE!
        }


# Local service definition template - This is NOT a real service, just a template!

define service{
        name                            local-service           ; The name of this service
template
        use                             generic-service         ; Inherit default values from the
generic-service definition
        max_check_attempts              4                ; Re-check the service up to 4 times in
order to determine its final (hard) state
        normal_check_interval           5                ; Check the service every 5 minutes under
normal conditions
        retry_check_interval            1                ; Re-check the service every minute until
a hard state can be determined
        register                        0                ; DONT REGISTER THIS DEFINITION - ITS NOT
A REAL SERVICE, JUST A TEMPLATE!
        }
```

Se puede especificar una lista de hosts o grupos en los parámetros *host_name* y *hostgroup_name*.

6.2.4. Contact y contactgroup

Se puede definir el contacto de Nagios cuando hay errores (*contact.cfg*):

```
define contact{
        contact_name                    nagiosadmin             ; Short name of user
        use                               generic-contact       ; Inherit default values from
generic-contact template (defined above)
        alias                           Nagios Admin            ; Full name of user

        email                           nagios@localhost   ; <<***** CHANGE THIS TO YOUR EMAIL
ADDRESS ******
        }
```

El objeto genérico está almacenado en el fichero de plantillas: *templates.cfg*.

```
# Generic contact definition template - This is NOT a real contact, just a template!

define contact{
        name                            generic-contact            ; The name of this contact
template
        service_notification_period     24x7                       ; service notifications can be
sent anytime
        host_notification_period        24x7                       ; host notifications can be sent
anytime
        service_notification_options    w,u,c,r,f,s                ; send notifications for all
service states, flapping events, and scheduled downtime events
        host_notification_options       d,u,r,f,s          ; send notifications for all host states,
flapping events, and scheduled downtime events
        service_notification_commands   notify-service-by-email    ; send service notifications via
email
        host_notification_commands      notify-host-by-email       ; send host notifications via
email
        register                        0                  ; DONT REGISTER THIS DEFINITION - ITS NOT
A REAL CONTACT, JUST A TEMPLATE!
        }
```

6.2.5. El objeto command

Cualquier cosa que Nagios es capaz de ejecutar, se hace mediante comandos. En el fichero commands.cfg están algunos:

```
# 'check_local_disk' command definition
define command{
        command_name    check_local_disk
        command_line    $USER1$/check_disk -w $ARG1$ -c $ARG2$ -p $ARG3$
        }
```

Los parámetros encerrados entre el símbolo $ son llamadas a macros.

Si se han instalado los plugins, éstos estarán almacenados en el directorio /usr/local/nagios/libexec:

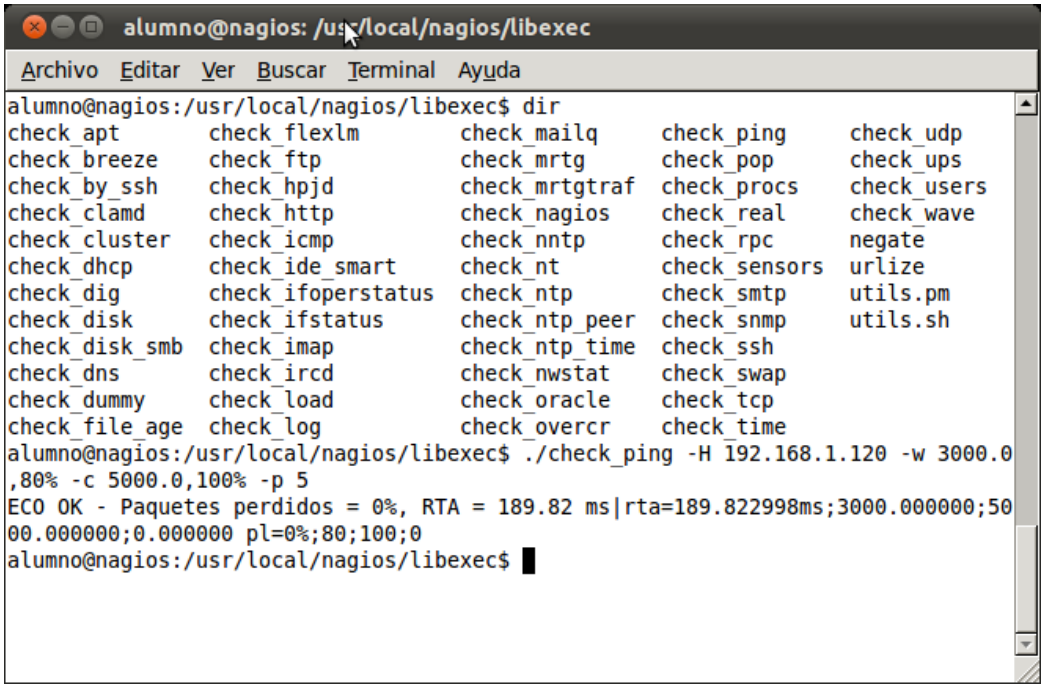


Fig. 34: Comandos de Nagios plugins

6.3. Comprobación de la configuración de Nagios

Siempre es recomendable la comprobación de la configuración de Nagios, antes de arrancar la herramienta. Esta comprobación de puede realizar con la opción –v:

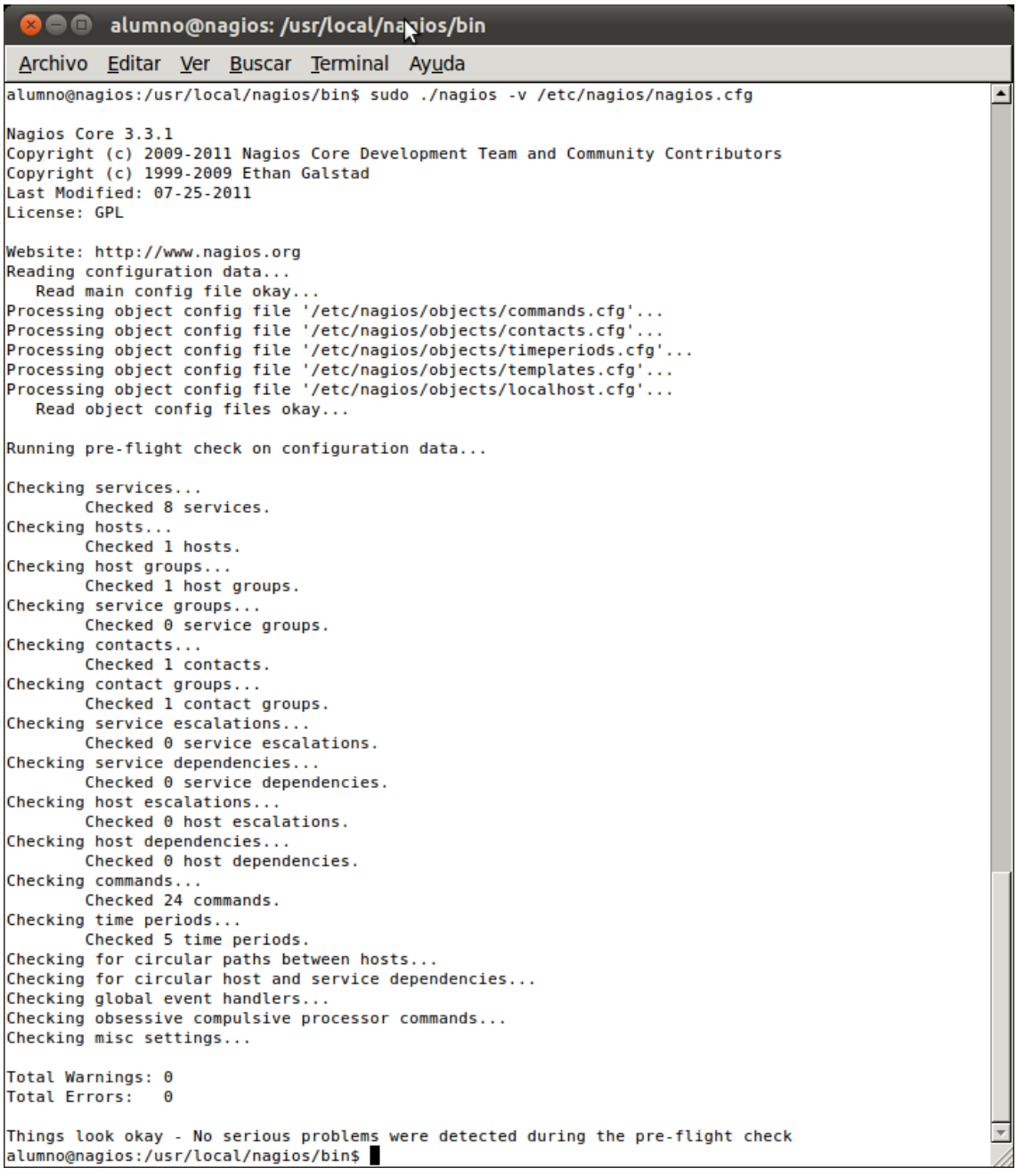


Fig. 35: Comprobación configuración de Nagios

6.4. Monitorización de máquinas Linux

El fichero de configuración localhost.cfg en el directorio objects se puede utilizar como plantilla para monitorizar máquinas Linux:

```
define host{
        use                     linux-server            ; Name of host template to use
                                                        ; This host definition will inherit all
variables that are defined
```

```
                                                        ; in (or inherited by) the linux-server
host template definition.
        host_name               moodle
        alias                   servidor moodle
        address                 192.168.1.115
        }

# Define a service to "ping" the local machine

define service{
        use                             local-service         ; Name of service template to use
        host_name                       moodle
        service_description             PING
        check_command                     check_ping!100.0,20%!500.0,60%
        }
```

Hay que tener en cuenta que en el fichero localhost.cfg ya hay definido un grupo que se puede utilizar para incluir estas máquinas:

```
define hostgroup{
        hostgroup_name  linux-servers ; The name of the hostgroup
        alias           Linux Servers ; Long name of the group
        members         localhost,moodle     ; Comma separated list of hosts that belong to this
group
        }
```

Este tipo de monitorización no requiere la instalación de ningún agente adicional en la máquina a monitorizar.

6.5. Utilización de un ping básico en Windows

Se puede utilizar la plantilla básica /etc/nagios/objects/windows.cfg como punto de partida:

```
define host{
        use             windows-server   ; Inherit default values from a template
        host_name       winserver        ; The name we're giving to this host
        alias           My Windows Server        ; A longer name associated with the host
        address         192.168.1.2      ; IP address of the host
        }
```

Y añadir el ping básico:

```
define service{
        use                             local-service         ; Name of service template to use
        host_name                       winserver
        service_description             PING
        check_command                     check_ping!100.0,20%!500.0,60%
        }
```

El resto de los servicios se implementan con el cliente de Windows que se describe en el apartado siguiente.

6.6. Instalación NSClient++

Antes de instalar el agente en la máquina aparecerá el siguiente estado:

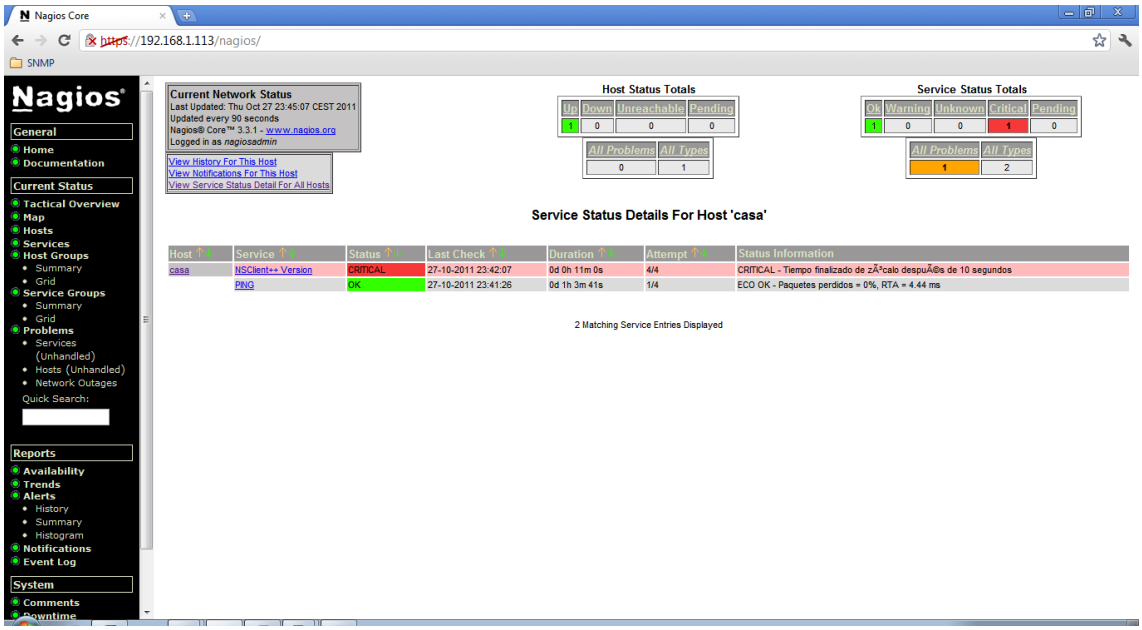


Fig. 36: Mensaje de error antes de instalación NSClient.

La siguiente figura muestra cómo Nagios se conecta a la máquina Windows utilizando el cliente:

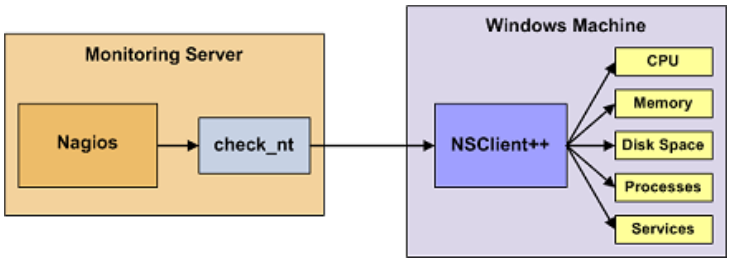


Fig. 37: Conexión Nagios con NSClient++

Instalar el servicio con la siguiente configuración (modificar, según el caso, la dirección del servidor Nagios):

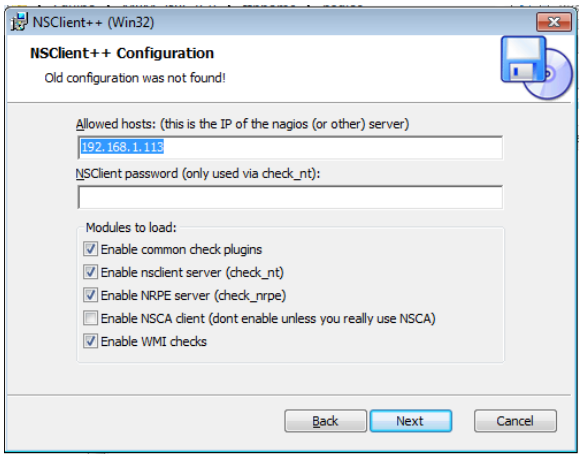


Fig. 38: Instalación NSClient++.

El comando a utilizar check_nt se puede encontrar en el directorio ../libexec:

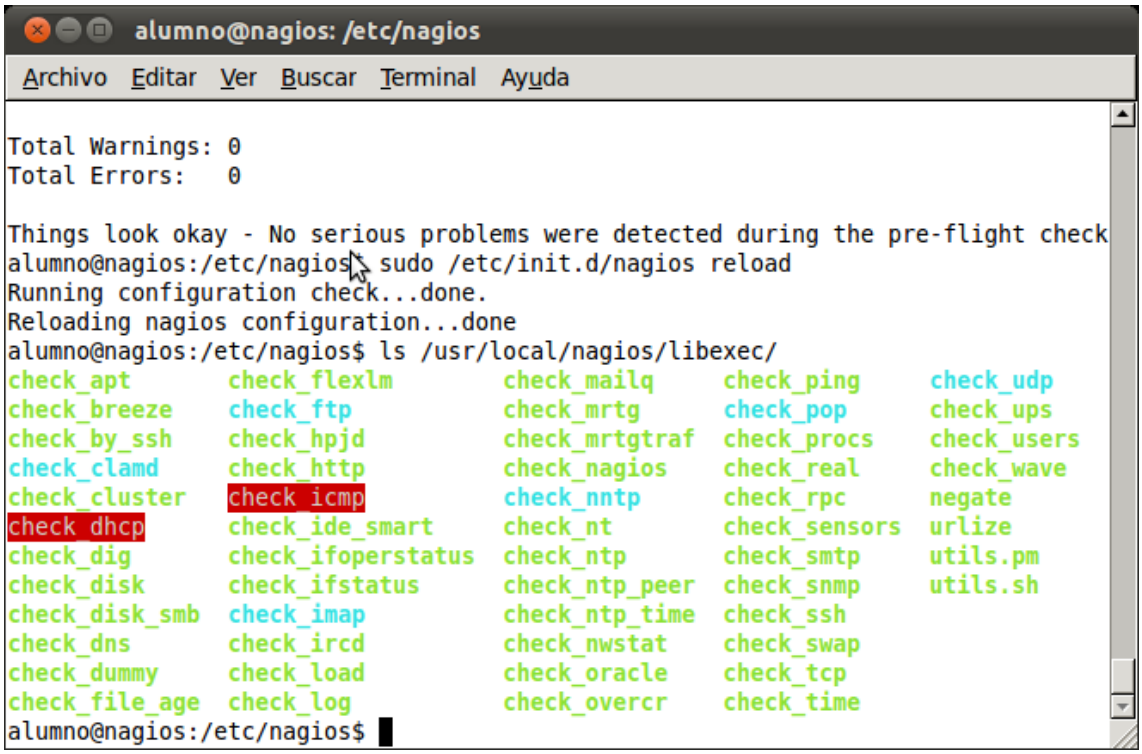


Fig. 39: Contenido del directorio ../libexec

Hay que configurar el password en el agente y en la configuración de Nagios. Si no se hace, aparecerá el error *invalid password*:

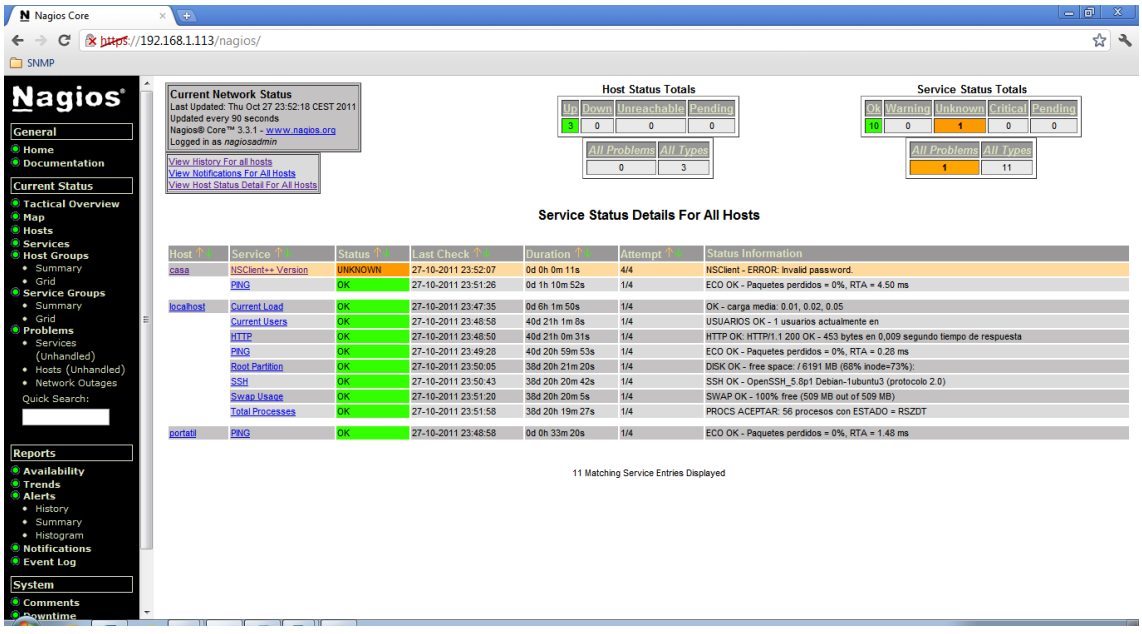


Fig. 40: Error de configuración de password NSClient

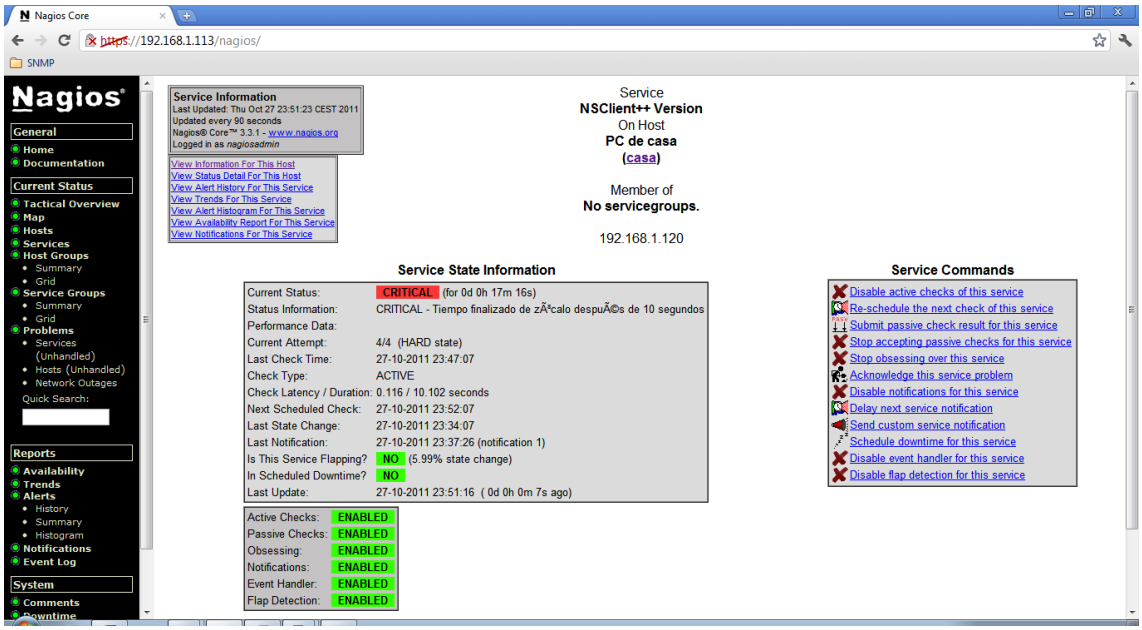


Fig. 41: Error de configuración de password en NSCient (detalle).

Configurar el password en el fichero de configuración de Nagios, añadiendo la opción –s:

```
define command{
        command_name    check_nt
#       command_line    $USER1$/check_nt -H $HOSTADDRESS$ -p 12489 -v $ARG1$ $ARG2$
        command_line    $USER1$/check_nt -H $HOSTADDRESS$ -p 12489 -s sacyl -v $ARG1$ $ARG2$
        }
```

Configurar el password en el fichero NSC.ini en la carpeta del programa:

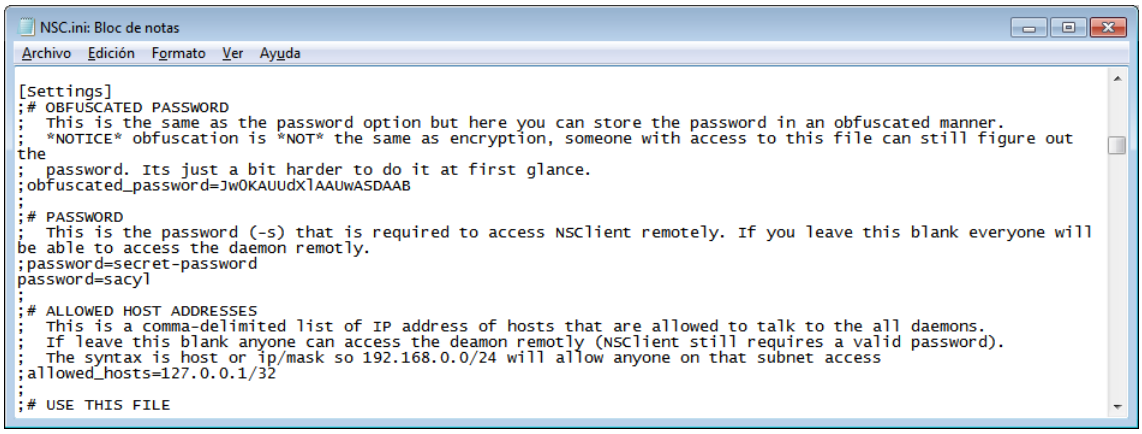


Fig. 42: Configuración password en NSC.ini

Una vez configurado el password en el fichero NSC.ini, arrancar de nuevo el servicio:

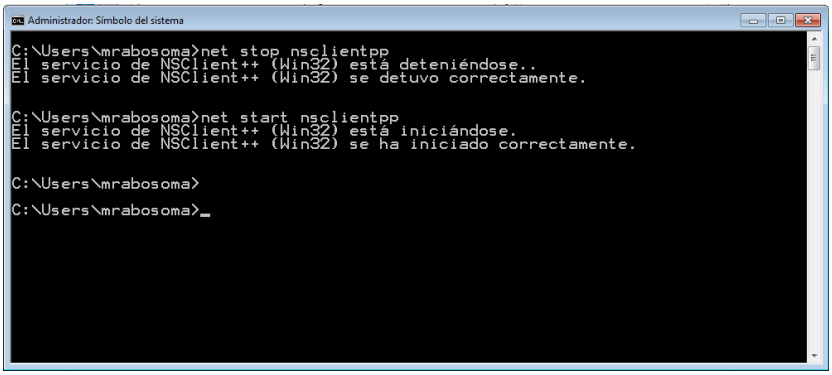


Fig. 43: Restart de servicio NSClient en Windows.

Una vez configurado, aparecerá como OK:

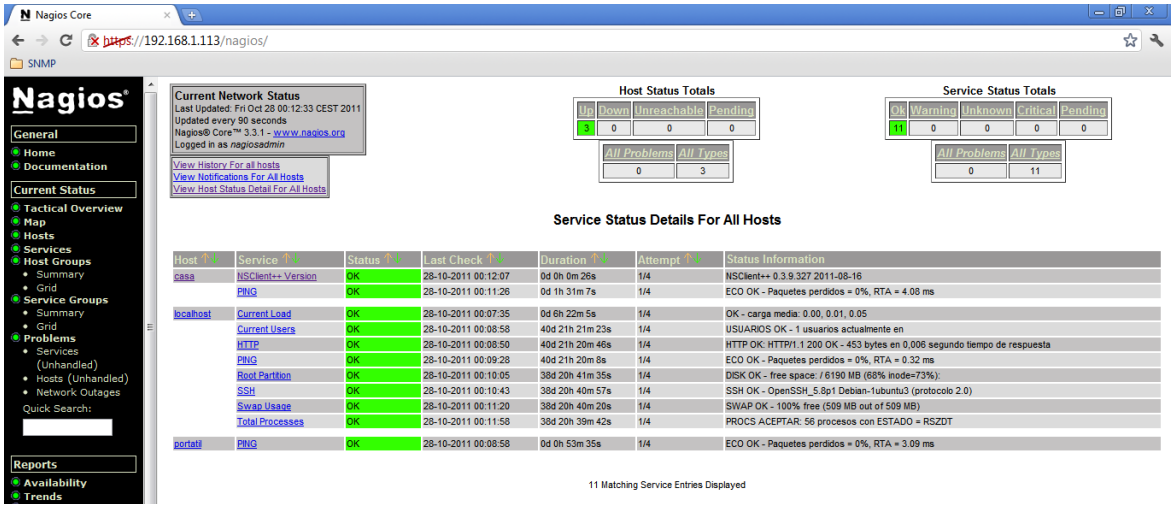


Fig. 44: Comprobación servicio NSClient.

6.7. Monitorización de Impresoras en Red

Para monitorizar impresoras se puede reutilizar la plantilla que Nagios proporciona: /etc/nagios/objects/printer.cfg:

```
define host{
        use                     generic-printer         ; Inherit default values from a template
        host_name               hplj2605dn              ; The name we're giving to this printer
        alias                   HP LaserJet 2605dn      ; A longer name associated with the printer
        address                 192.168.1.30            ; IP address of the printer
        hostgroups              network-printers        ; Host groups this printer is associated with
        }

define hostgroup{
        hostgroup_name  network-printers ; The name of the hostgroup
        alias           Network Printers ; Long name of the group
        }
define service{
        use                             generic-service         ; Inherit values from a template
        host_name                       hplj2605dn ; The name of the host the service is associated with
        service_description             Printer Status          ; The service description
        check_command                   check_hpjd!-C public    ; The command used to monitor the service
        normal_check_interval           10 ; Check the service every 10 minutes under normal conditions
        retry_check_interval            1 ; Re-check the service every minute until its final/hard state is
determined
```

```
        }

define service{
        use                     generic-service
        host_name               hplj2605dn
        service_description     PING
        check_command           check_ping!3000.0,80%!5000.0,100%
        normal_check_interval   10
        retry_check_interval    1
        }
```

Además del típico ping, define un servicio específico para impresoras que utilizan típicamente el servicio JetDirect (HP). Para este servicio, hay que hacer coincidir la comunidad SNMP de la impresora y la especificada en el comando *check_hpjd*.

6.8. Monitorización de routers y Switches

En las plantillas /etc/nagios/objects/switches y /etc/nagios/objects/routers se definen las características básicas de acceso a estos equipos. Sin configurar previamente SNMP en estos equipos, el único servicio que funcionará será el *check_ping*. En la parte III del manual de instalación y configuración de Nagios se detallará el proceso de configuración de SNMP.

Las plantillas proporcionadas se pueden utilizar directamente. No obstante, el servicio informará de errores ya que no se habrán configurado las MIBs[12].

```
define host{
        use             generic-switch          ; Inherit default values from a template
        host_name       linksys-wrt610N         ; The name we're giving to this switch
        alias           Linksys WRT610N Switch  ; A longer name associated with the switch
        address         192.168.1.1             ; IP address of the switch
        hostgroups      switches                ; Host groups this switch is associated with
        notes_url       https://192.168.1.1
        }
```

Con el comando use se heredan todas las características definidas en el objeto generic-switch definido en templates.cfg.

```
define service{
        use             generic-service  ; Inherit values from a template
        host_name       linksys-wrt610N  ; The name of the host the service is associated with
        service_description      PING            ; The service description
        check_command    check_ping!200.0,20%!600.0,60%    ; The command used to monitor the service
        normal_check_interval    5       ; Check the service every 5 minutes under normal conditions
        retry_check_interval 1 ; Re-check the service every minute until its final/hard state is
determined
        }
```

Se puede definir un acceso mediante url a una página con más información sobre el dispositivo. En este caso aparecerá un símbolo de una carpeta al lado del host:

[12] Los detalles del servicio se pueden ver haciendo clic en el servicio del host. Se verá un diagnóstico del error, por ejemplo que las mibs no se han encontrado.

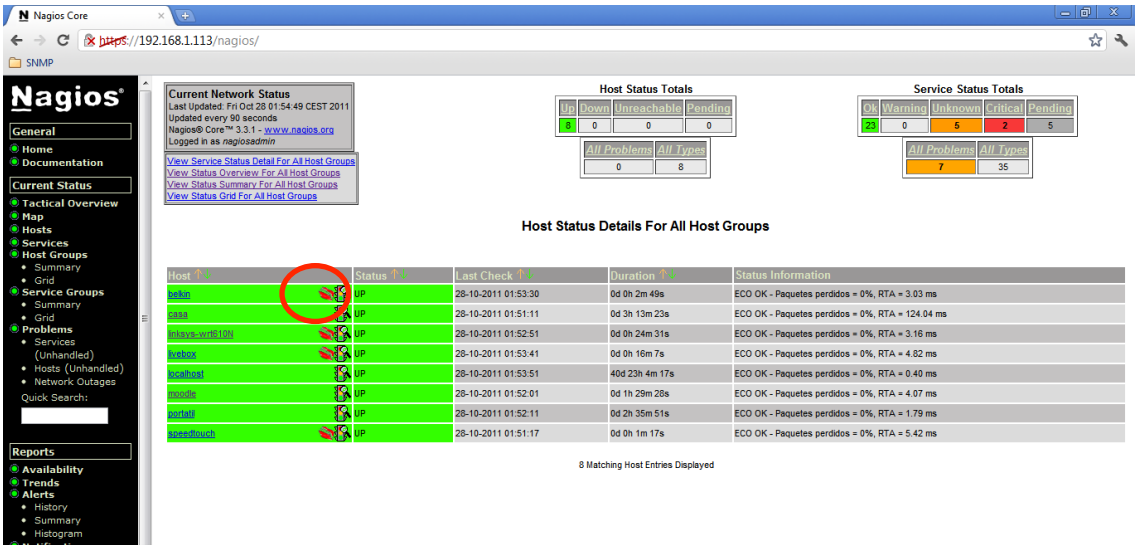


Fig. 45: Símbolo asociado a notes_url

6.9. Aviso de Flapping

Algunas veces los servicios se vuelven inestables y se entra en una situación de flap. Nagios lo indica mediante el aviso correspondiente:

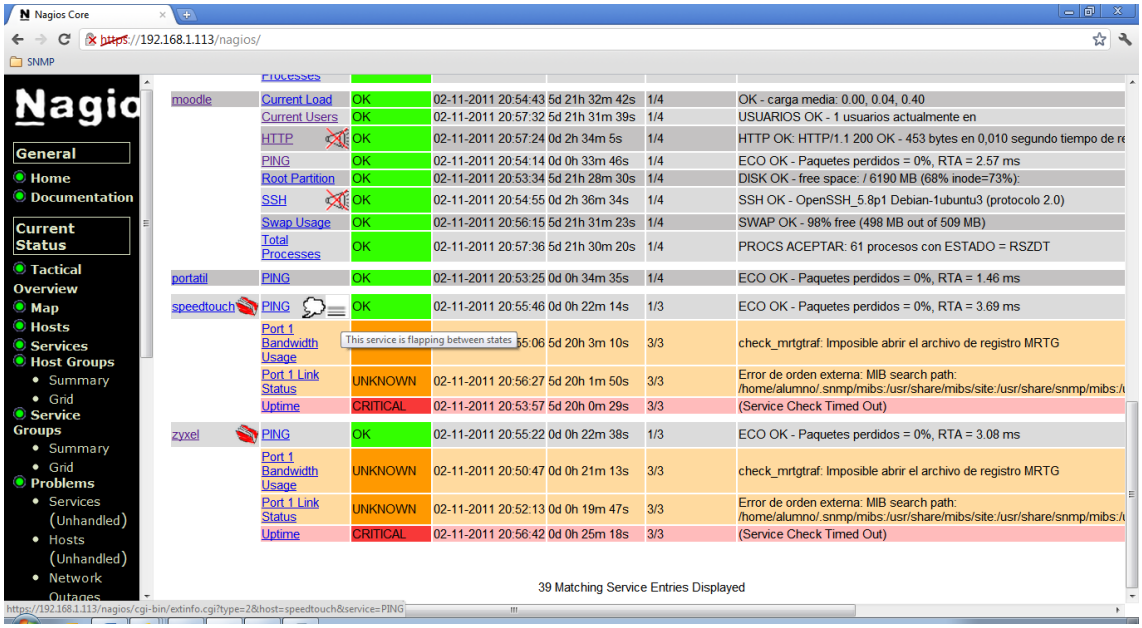


Fig. 46: Aviso de flapping

También indicará que hay un comentario:

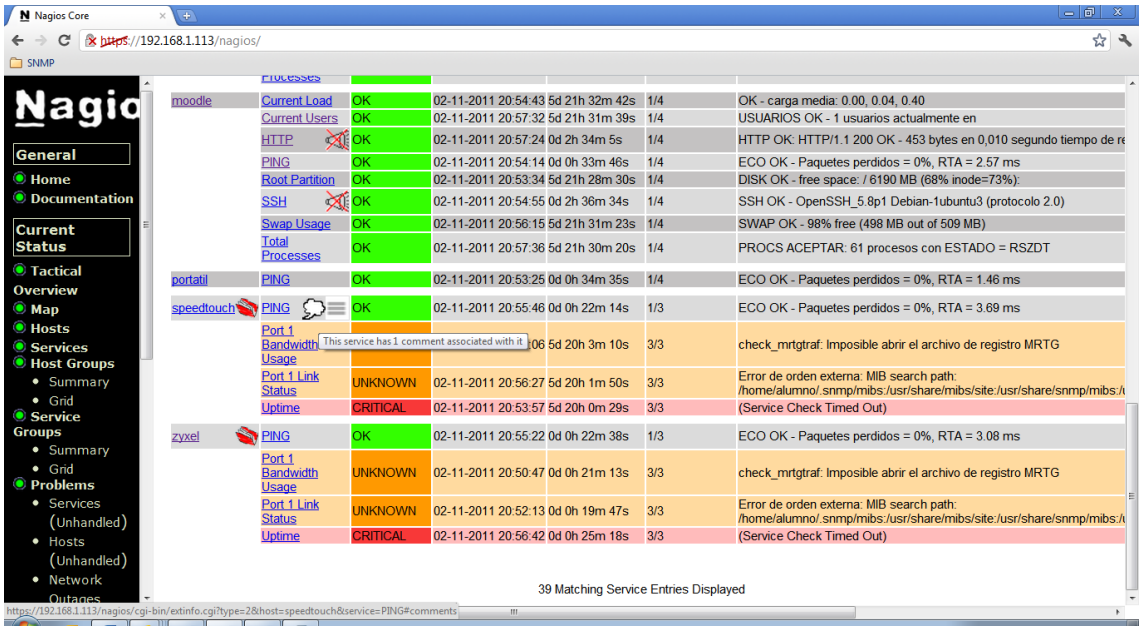


Fig. 47: Comentario sobre flapping

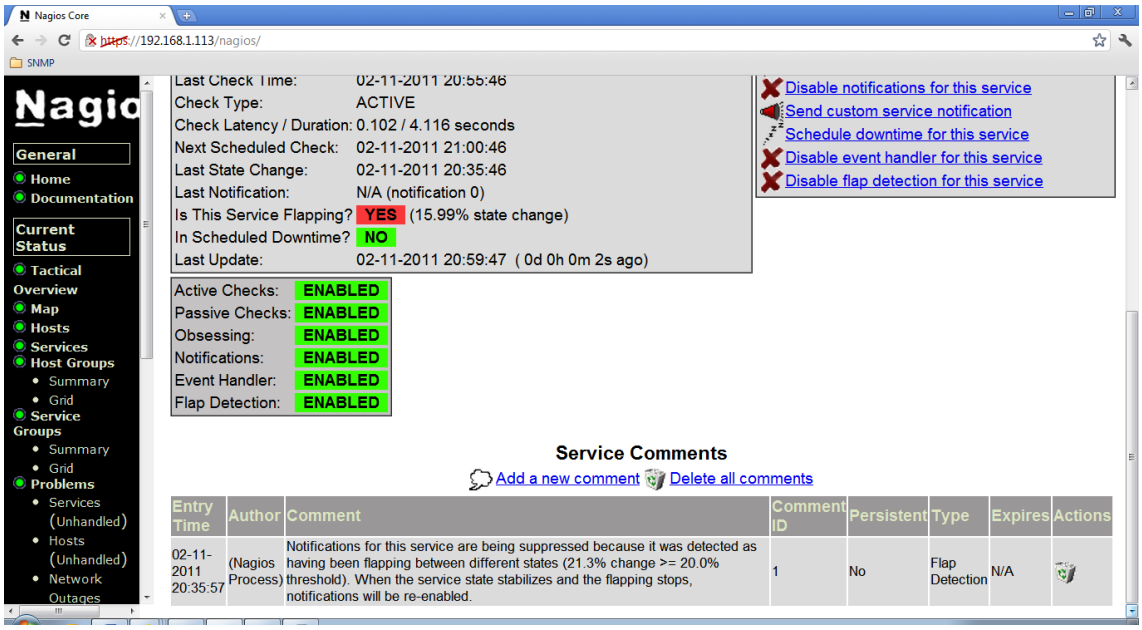


Fig. 48: Información de servicio haciendo flapping (detalle)

6.10. Actualización de Nagios

En la página principal de Nagios, hacer clic en *Check for updates*:

Fig. 49: Pantalla principal de Nagios para acceso a actualización.

Aparecerá otra página en la que se obtendrá la información correspondiente:

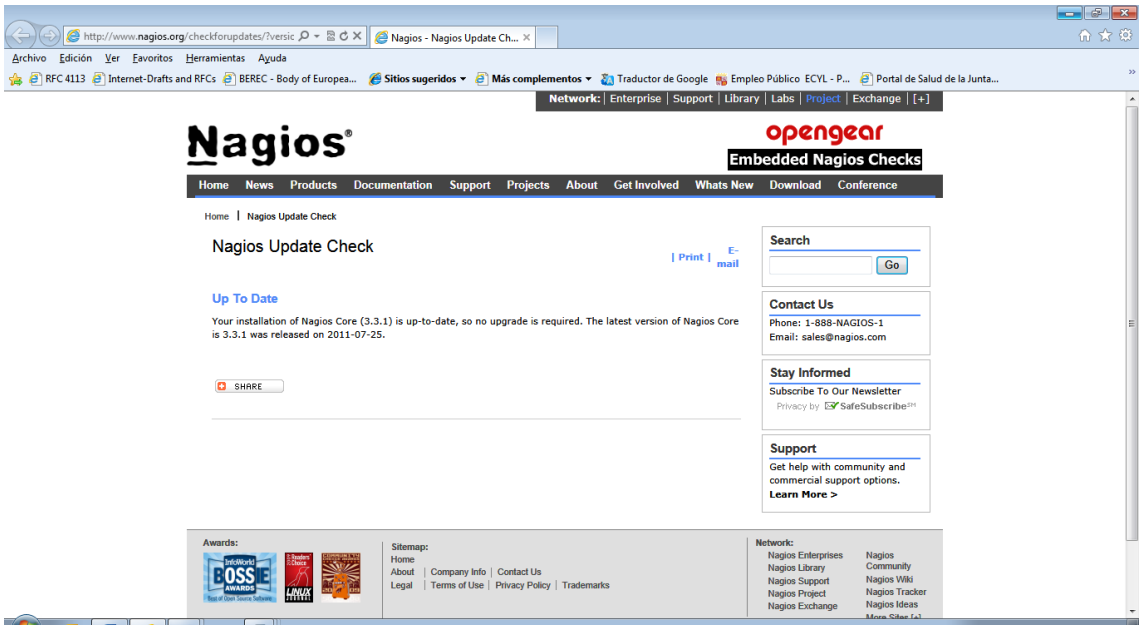


Fig. 50: Pantalla de información de actualizaciones.

Si fuera necesario actualizar, seguir las instrucciones de actualización de cada reléase. Siempre es conveniente no instalar sobrescribiendo otra instalación de Nagios, sino utilizar el comando make unistall o similar.

Si se actualiza desde una versión más antigua, se recomienda revisar el manual de Nagios Core[13]. Si se actualiza a la misma versión base, por ejemplo de la 3.3 a la 3.4, entonces los pasos son sencillos:

[13] http://library.nagios.com/library/products/nagioscore/manuals/

```
su -l nagios
rm /usr/local/Nagios/share/{main,side,index}.html
wget http://osdn.dl.sourceforge.net/sourceforge/nagios/nagios-3.4.1.tar.gz
tar xvzf Nagios-3.4.1.tar.gz
cd nagios
./configure --sysconfigdir=/etc/Nagios --localstatedir=/var/Nagios --with-command-group=nagcmd
make all
make install
/etc/init.d/nagios restart
```

6.11. Envío de notificaciones por correo electrónico

Nagios permite el envío de notificaciones por correo electrónico y SMS. De esta forma es posible estar avisado de cualquier problema que surja con un host o un servicio de un host.

A continuación se describe el proceso para configurar las notificaciones vía email utilizando un servidor de correo con autentificación. De esta forma se cubre el problema más general, ya que la mayoría de los servidores de correo actuales se configuran para autentificar a los usuarios antes de enviar correo saliente.

El primer paso es instalar las herramientas y el servidor de correo. Nagios instala automáticamente postfix. No obstante hay que comprobar su estado y configuración:

```
apt-get install mailutils
ln -s /usr/bin/mail /bin/mail
apt-get install postfix
```

Comprobar primero si existe. Si no, configurar de tipo *General Type* y asignar el nombre del servidor igual al de la máquina.

Editar el fichero /etc/postfix/main.cf y añadir:

```
relayhost = [smtp.gmail.com]:587
smtp_use_tls = yes
smtp_tls_CAfile = /etc/postfix/cacert.pem
smtp_sasl_auth_enable = yes
smtp_sasl_password_maps = hash:/etc/postfix/sasl/passwd
smtp_sasl_security_options = noanonymous
```

Crear el fichero /etc/postfix/sasl/passwd con la autenticación:

```
[smtp.gmail.com]:587 usuario@gmail.com:contraseña
```

Asignar permisos adecuados y transformar a un fichero indexado hash. Reiniciar postfix:

```
chmod 600 /etc/postfix/sasl/passwd
postmap /etc/postfixsasl/passwd
cat /etc/ssl/certs/Equifax_Secure_CA.pem >> /etc/postfix/cacert.pem
/etc/init.d/postfix restart
```

Para probar el envío, ejecutar el comando:

```
mail -s "asunto" usuario@gmail.com
```

A continuación editar el fichero objects/contacts.cfg y modificar la dirección de correo de la persona a la que se le enviarán las notificaciones:

```
define contact{
        contact_name    nagiosadmin         ; Short name of user
        use             generic-contact ; Inherit default values from generic-contact template
```

```
alias       Nagios Admin            ; Full name of user
email       nagios@localhost       ; <<***** CHANGE THIS TO YOUR EMAIL ADDRESS ******
}
```

Reiniciar Nagios y forzar un fallo para recibir las notificaciones. El correo incluirá un asunto y texto como los siguientes:

```
Asunto:  ** PROBLEM Host Alert: callmanager is DOWN **
Texto:

***** Nagios *****

Notification Type: PROBLEM
Host: callmanager
State: DOWN
Address: 172.25.80.136
Info: CRÍTICO -Anfitrión inalcanzable (172.25.80.136)

Date/Time: Mon Jul 23 22:59:12 CEST 2012
```

También avisará mediante notificación del momento en que un servicio se restablezca:

```
Asunto: ** RECOVERY Service Alert: zyxel Switch/Port 1 Interface Type is OK **

Texto:

***** Nagios *****

Notification Type: RECOVERY

Service: Port 1 Interface Type
Host: zyxel Switch
Address: 172.25.80.200
State: OK

Date/Time: Mon Jul 23 23:24:02 CEST 2012

Additional Info:

SNMP OK - 6
```

7. MONITORIZACIÓN VÍA SNMP

7.1. Directorio de configuración de Nagios.

Los comandos SNMP que se especifiquen, sin haber configurado las MIBs, provocarán errores a la hora de comprobar los servicios:

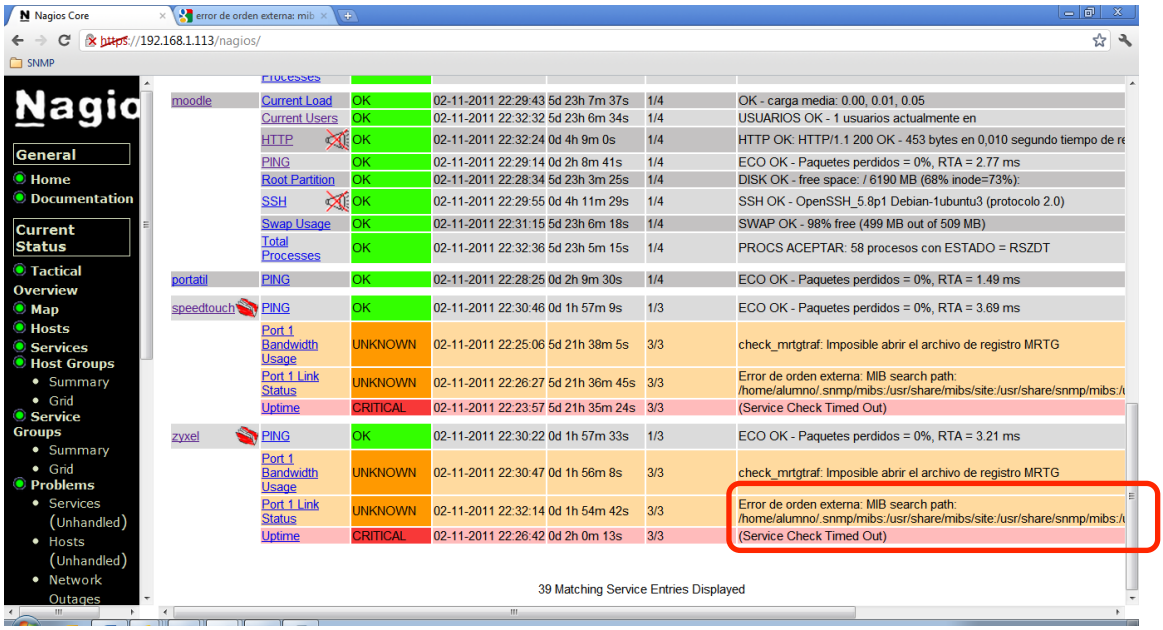


Fig. 51: Error de configuración de SNMP (MIB no encontrada)

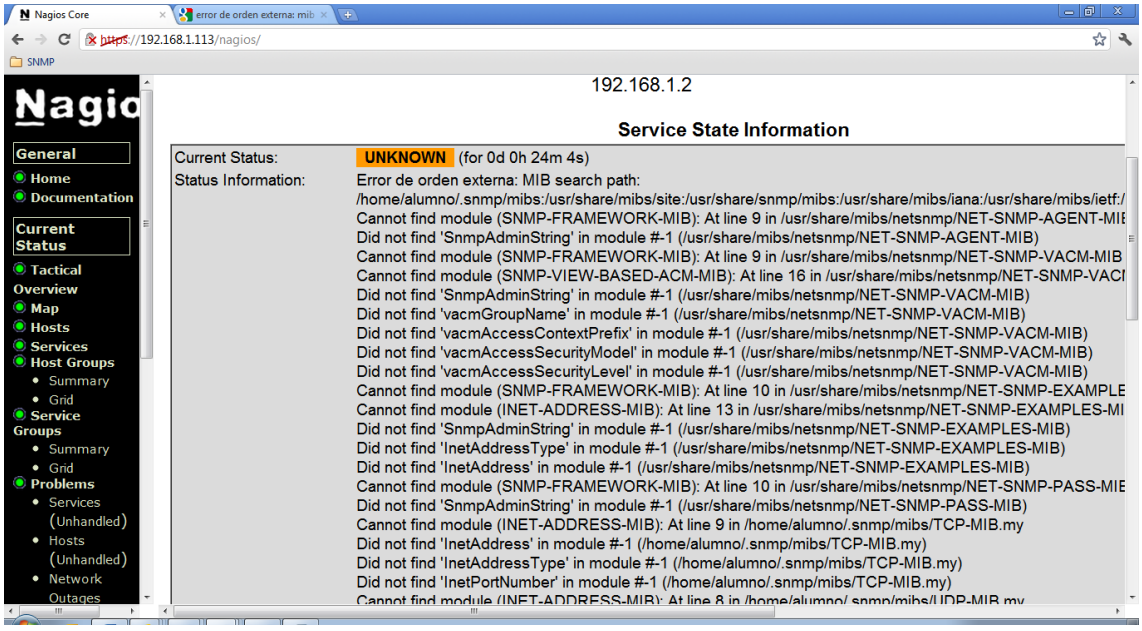


Fig. 52: Error de configuración de SNMP (MIB no encontrada), detalle del servicio

Este error se produce porque no se han encontrado las MIBs en el sistema. Para solucionarlo, descargar las MIBs[14] y copiarlas en el directorio apropiado. Según se vayan copiando, ya no aparecerán los errores correspondientes. Así se pueden ir eliminando hasta que no haya ninguno más. Hacer un restart de Nagios después de añadir más MIBs.

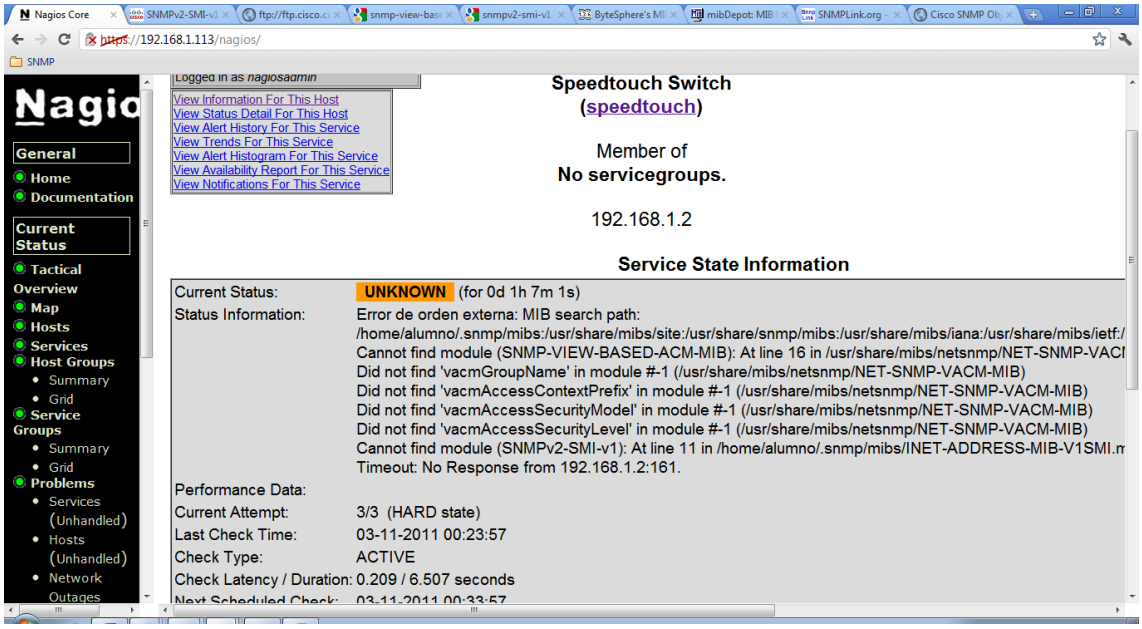


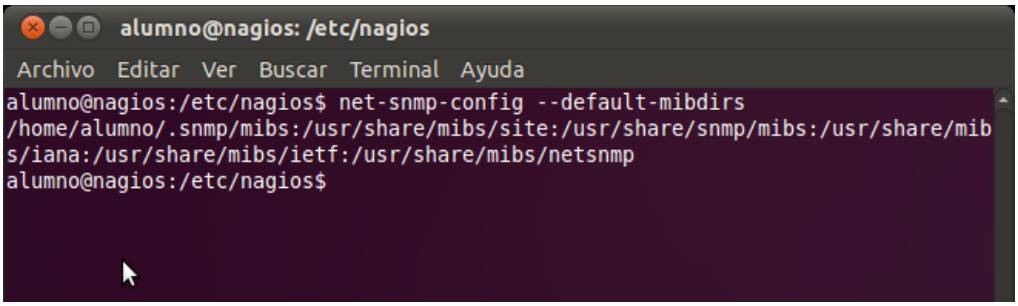
Fig. 53: Aviso de fichero de MIB no encontrado.

Las MIBs suelen estar en los siguientes directorios:

- $HOME/.snmp/mibs
- /usr/local/share/snmp/mibs

No obstante, en la herramienta se muestran las rutas en las que Nagios busca las MIBs. Para averiguar las rutas exactas, ejecutar el comando:

```
net-snmp-config --default-mibdirs
```



[14] Se pueden copiar las MIBs del paquete net-snmp: https://sourceforge.net/projects/net-snmp/files/net-snmp/5.7.1/

Fig. 54: Directorios de búsqueda de MIBs

Para averiguar cuáles son los directorios de configuración de SNMP, ejecutar el siguiente comando:

```
net-snmp-config -snmpconfpath
```

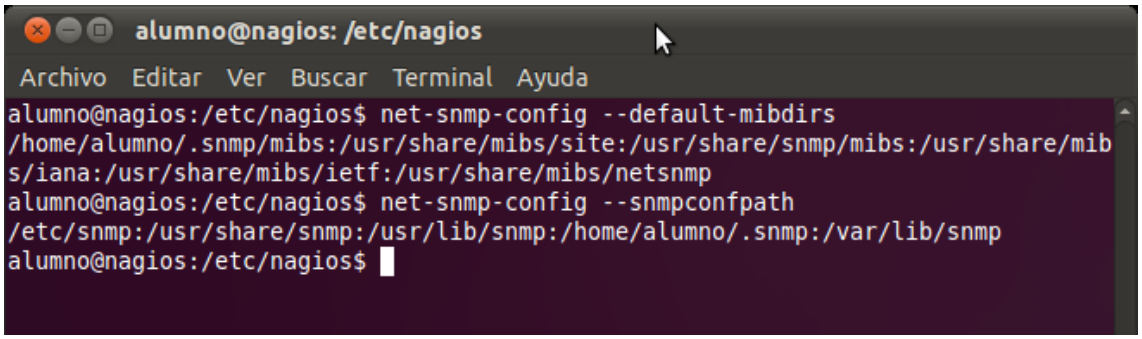


Fig. 55: Directorios de búsqueda de MIBs

Una vez copiadas (p. e. al directorio /home/alumno/.snmp) y hecho el restart de Nagios, aparecerán como OK en unos minutos. Para forzar una comprobación, hacer clic en los host command (servicio SNMP definido) y hacer clic en Re-schedule the next check of this host:

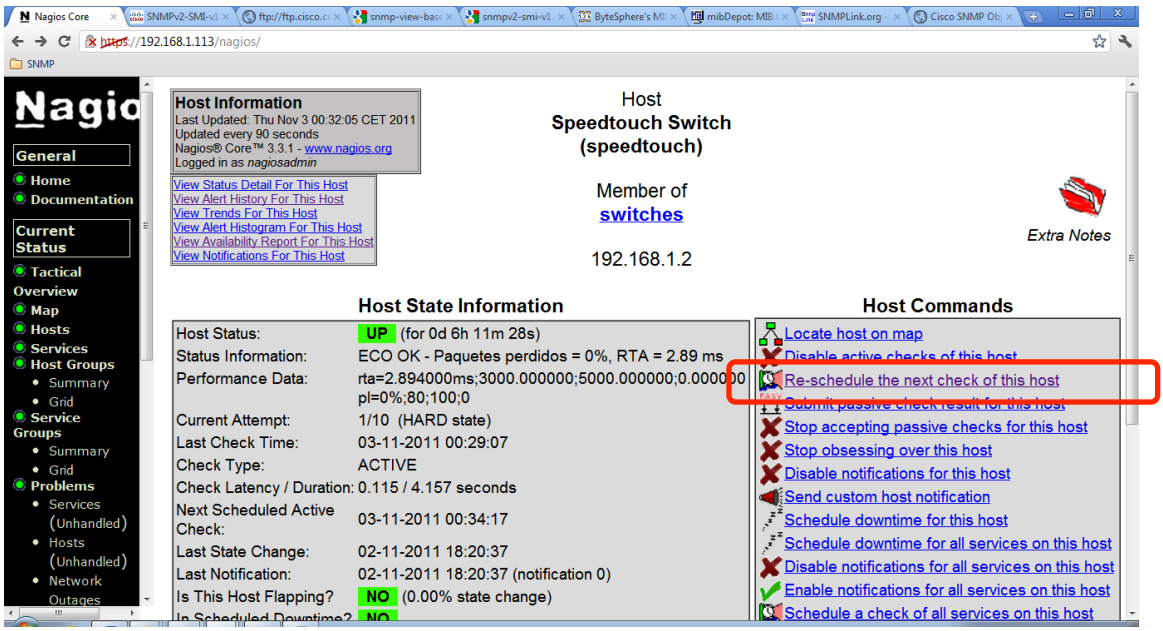


Fig. 56: Opciones para el host. Re-scheduling de un servicio.

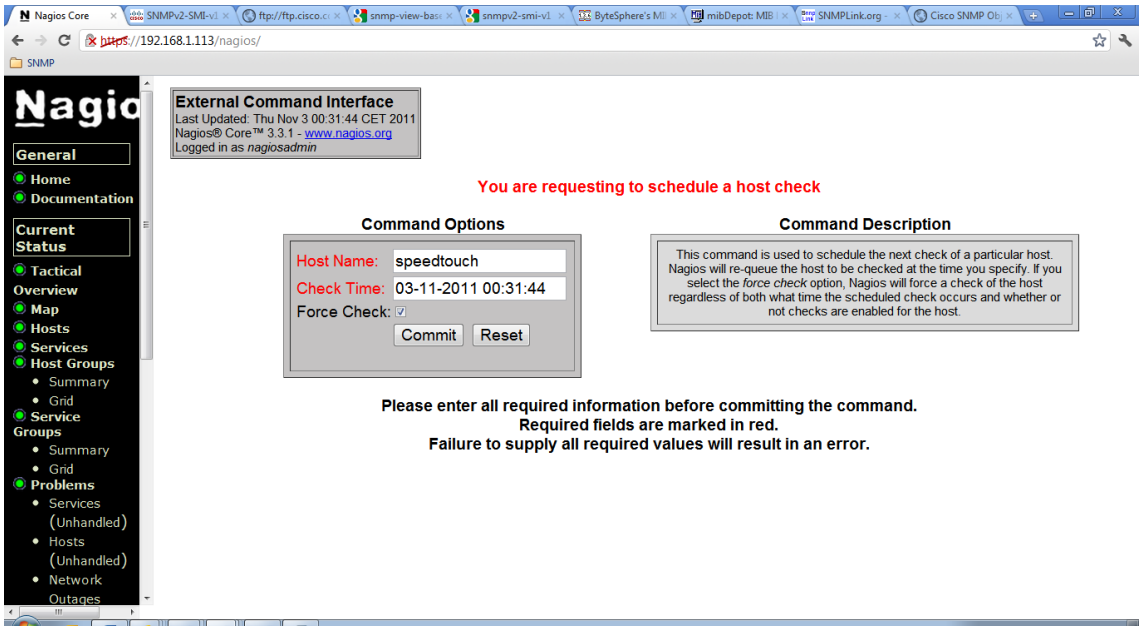


Fig. 57: Re-scheduling de un servicio.

7.2. Activar SNMP en router tipo residencial (Speedtouch/Zyxel)

No todos los routers-switches llevan incorporado SNMP. En las especificaciones del producto debe aparecer:

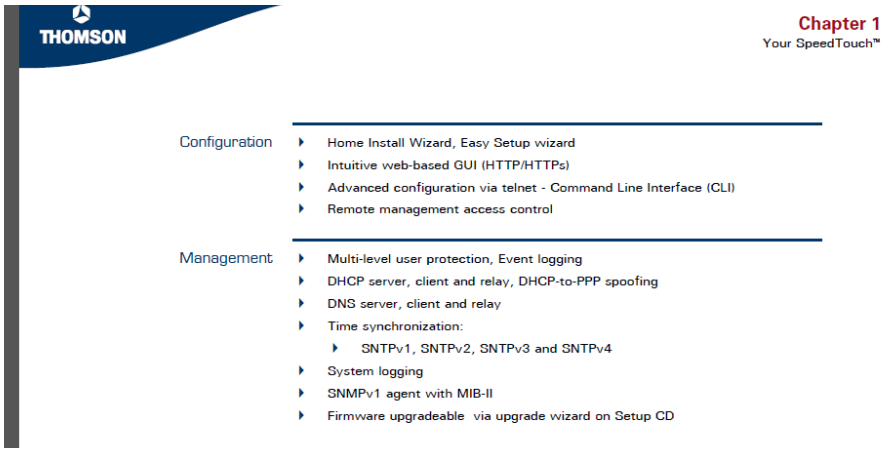


Fig. 58: Especificaciones de un router residencial relacionadas con SNMP.

7.2.1. Alcatel Speedtouch 580

Lo primero es verificar si el agente SNMP está activado. Para ello hacer un telnet y ejecutar el comando:

```
service system list
```

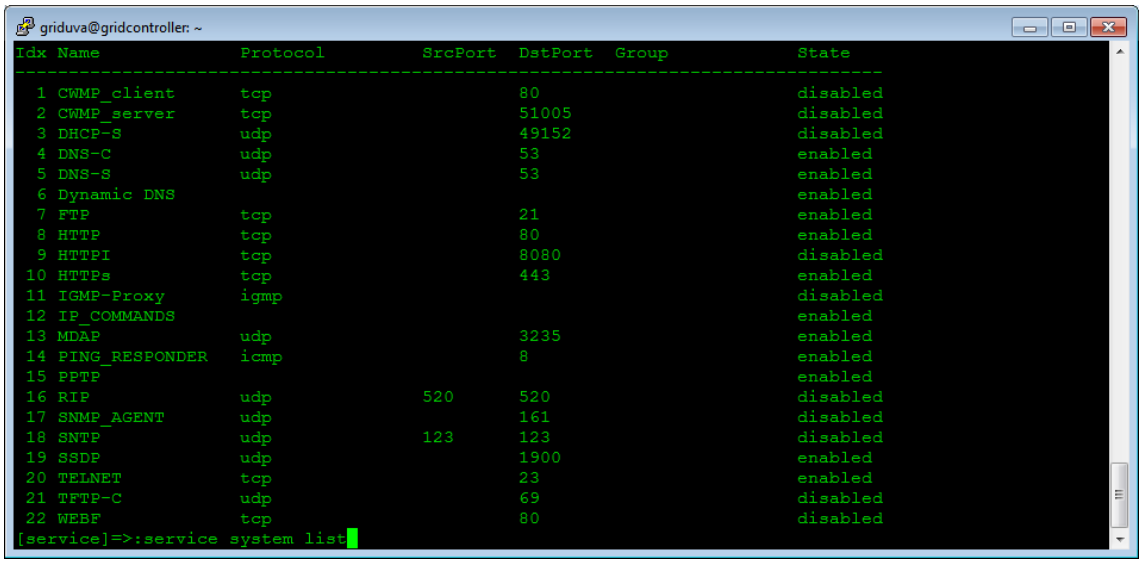


Fig. 59: Estado del protocolo SNMP en router Alcatel Speedtouch

Al no estar activado, no permitirá ninguna consulta. Activar mediante los comandos:

```
service system modify name=SNMP_AGENT state=enabled
snmp community add securityname=RWCommunity communityname=public
```

Comprobar la configuración de SNMP ahora:

```
service system list name=SNMP_AGENT expand=enabled
```

El resultado es el siguiente:

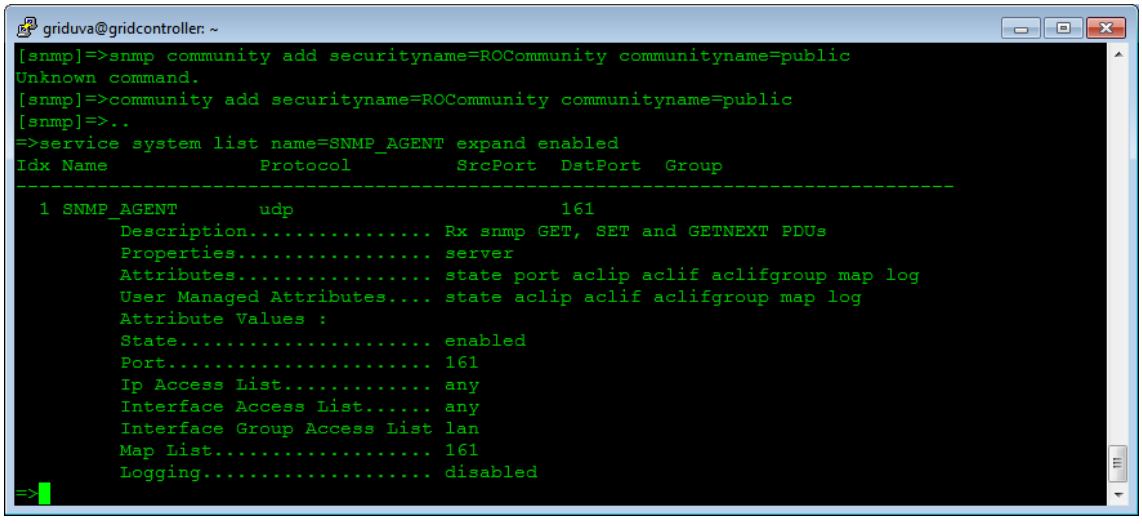


Fig. 60: Resultado configuración SNMP en router Alcatel Speedtouch 580.

7.2.2. Zyxel Prestige 650HW

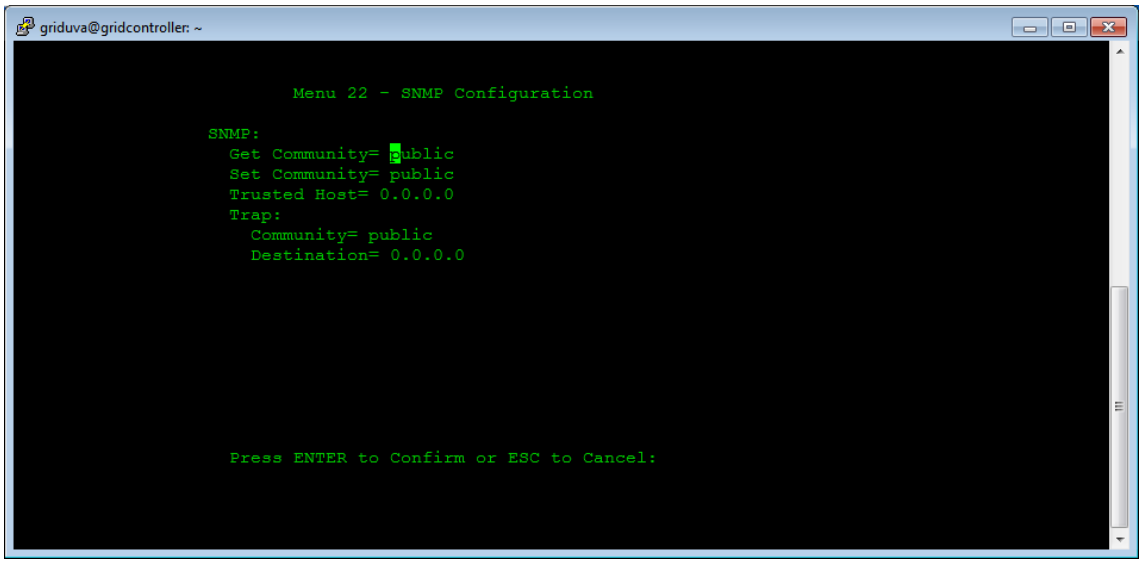


Fig. 61: Configuración SNMP router Zyxel.

7.3. Object Browser

Mediante el browser de CISCO[15] u otro, determinar otros parámetros a monitorizar como ifSpeed, ifPhysAddress, etc.

Las siguientes figuras muestran los oids y características de sysUptime y ifOperStatus:

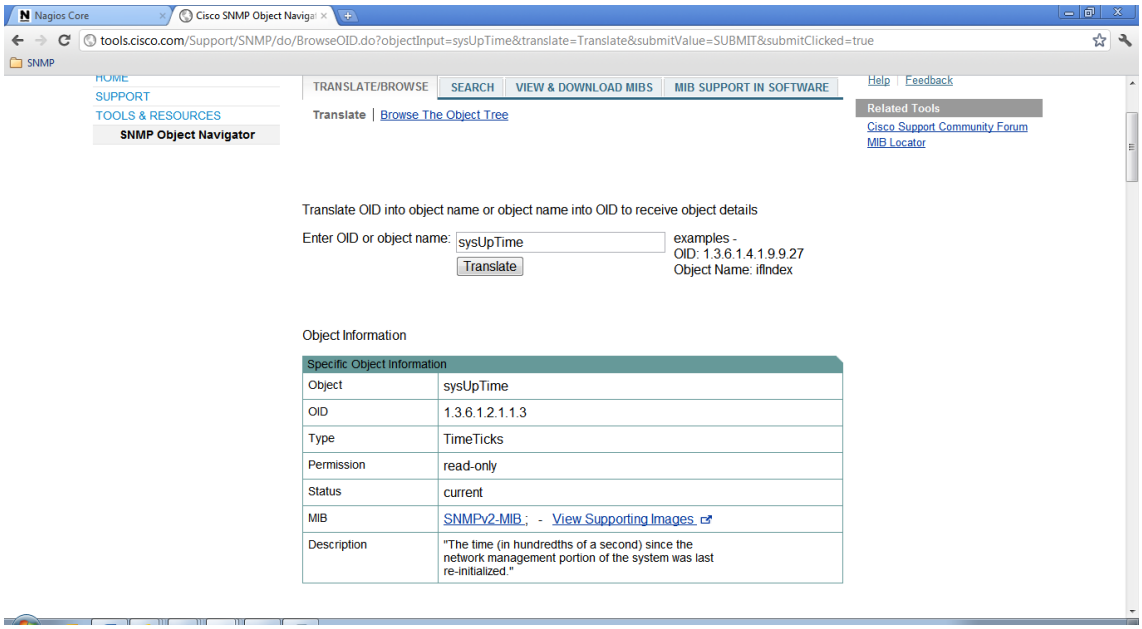


Fig. 62: Vista del SNMP Object Navigator de CISCO (I).

[15] http://tools.cisco.com/Support/SNMP/do/BrowseOID.do?local=en

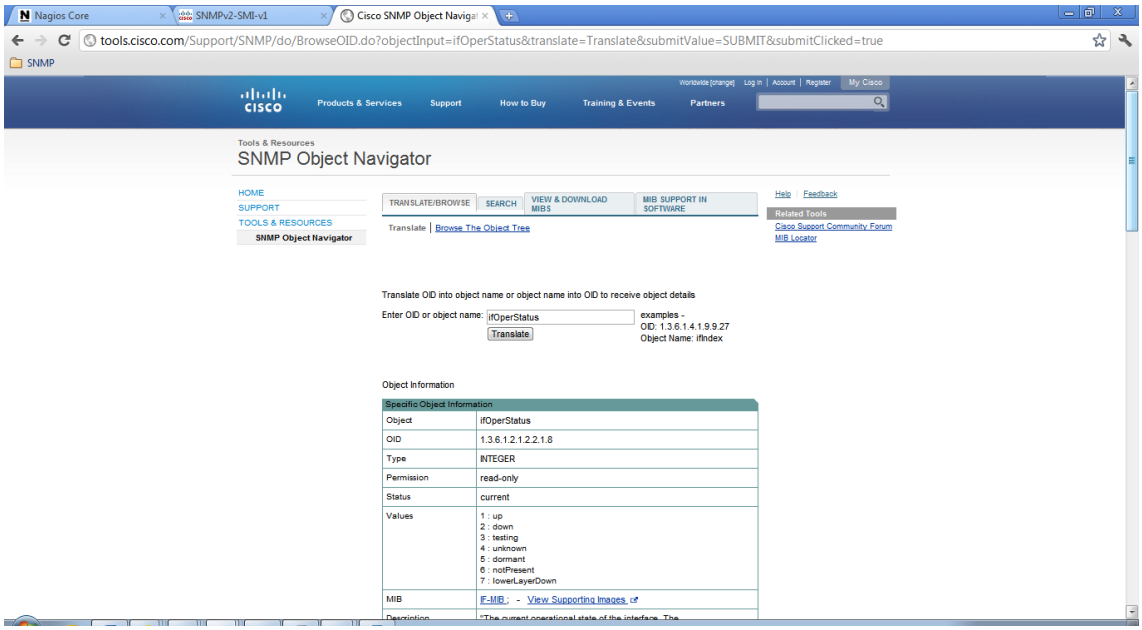


Fig. 63: Vista del SNMP Object Navigator de CISCO (II).

7.4. Comprobación de objetos en un dispositivo

Para comprobar de forma interactiva los OIDs, se puede utilizar el comando *snmpwalk*:

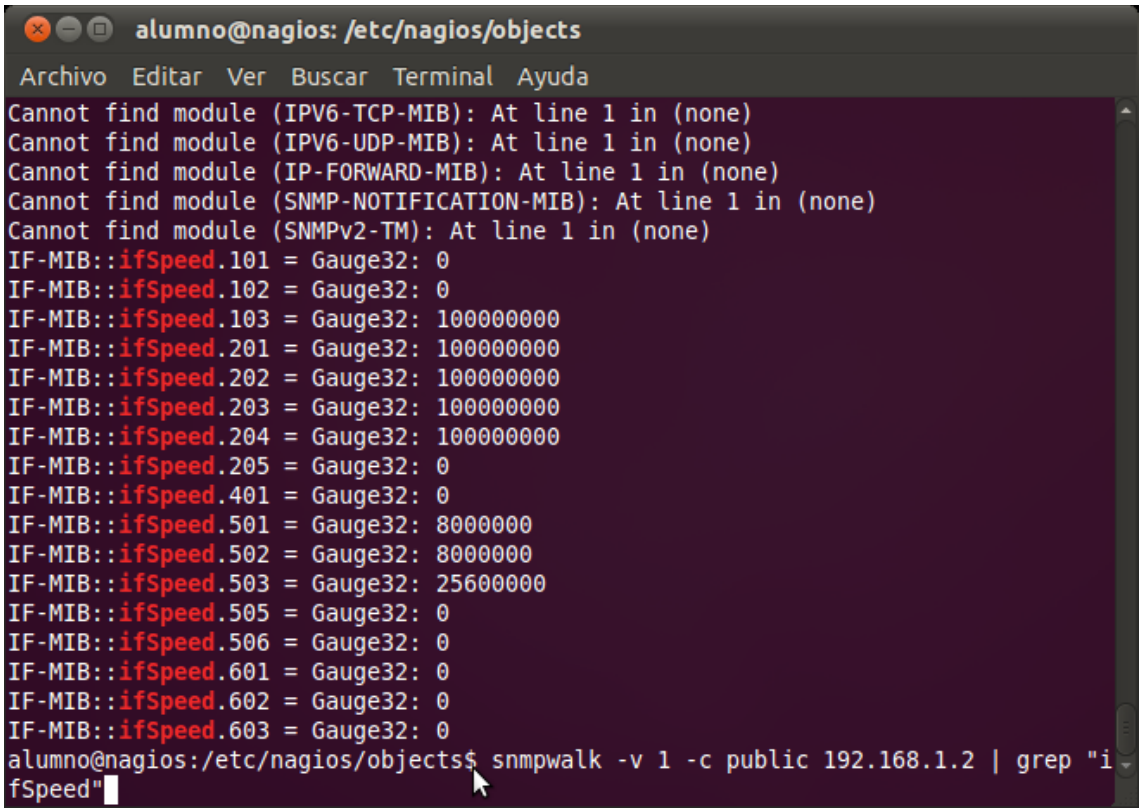


Fig. 64: Comprobación de objetos con el comando snmpwalk.

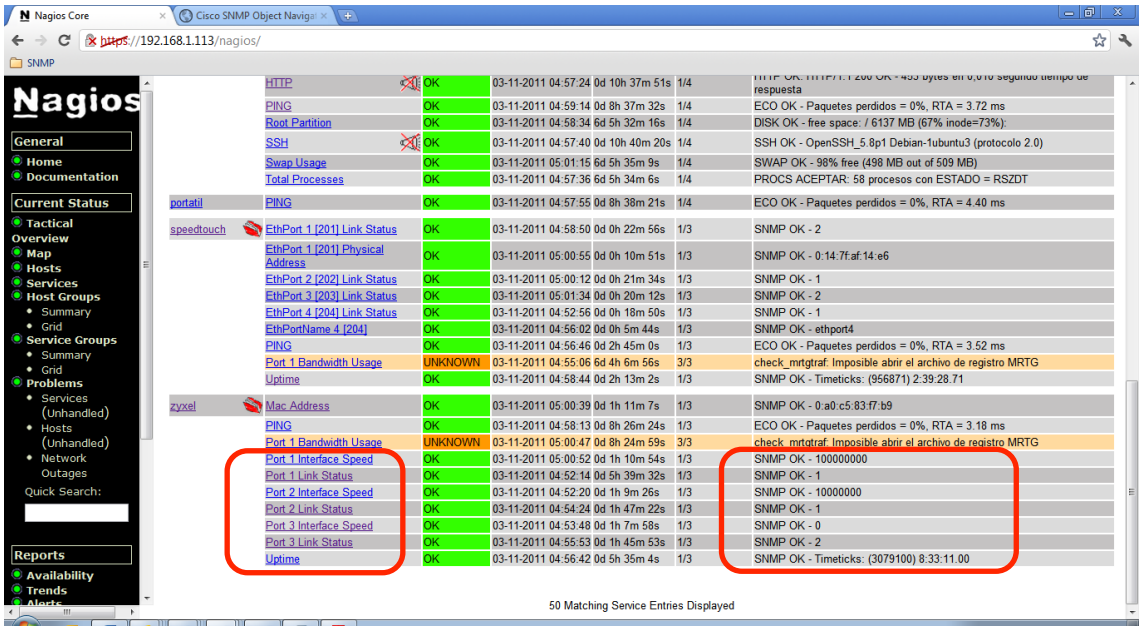


Fig. 65: Vista de Nagios con varios servicios SNMP.

7.5. Instalación de agentes SNMP

7.5.1. Instalación y configuración del agente SNMP en Windows

En el Panel de Control, seleccionar agregar características de Windows y luego protocolo SNMP.

Una vez instalado, ir de nuevo al Panel de Control □ Herramientas administrativas □ Servicios □ SNMP.

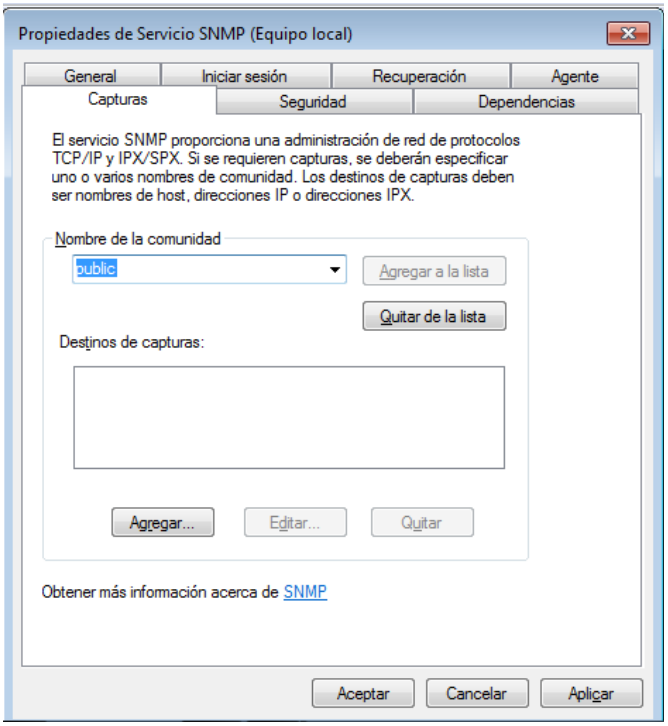


Fig. 66: Configuración comunidad SNMP en Windows.

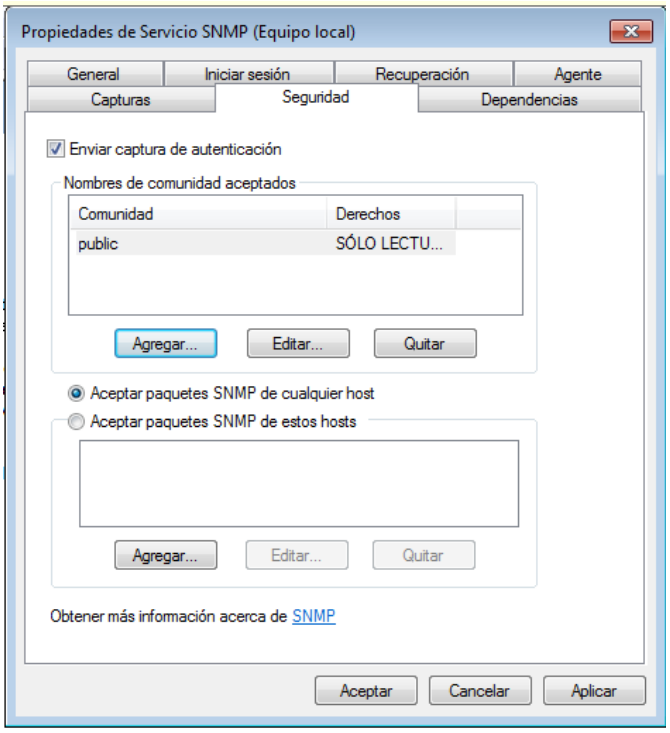


Fig. 67: Configuración seguridad SNMP en Windows.

Es importante revisar posteriormente el firewall y antivirus para desactivar las reglas que impidan el acceso.

7.5.2. Instalación y configuración de SNMP en Linux

El primer paso es instalar el demonio que implementará el agente SNMP:

```
sudo apt-get install snmpd
```

El siguiente paso es configurar SNMP (ejecutando el comando *snmpconf*), creando el fichero de configuración snmpd.conf. Una vez creado se deberá copiar en /etc/snmp. Las siguientes figuras describen el proceso:

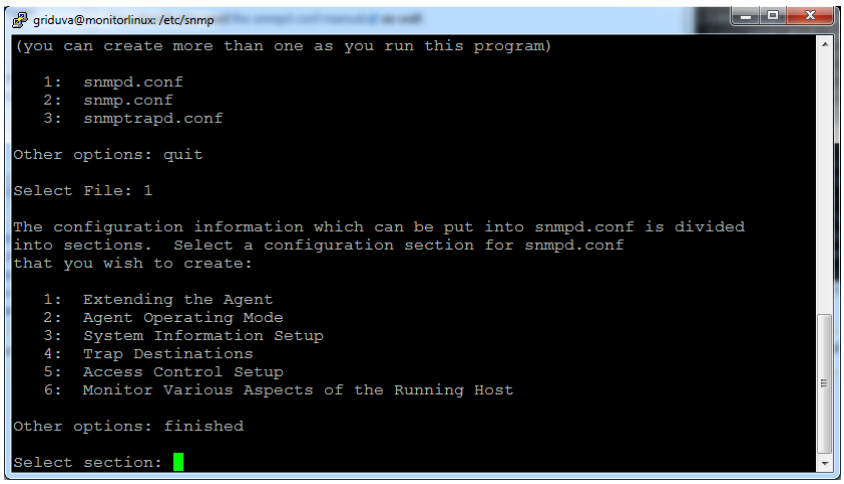


Fig. 68: Paso 1, configurar snmpd.conf y Access Control Setup.

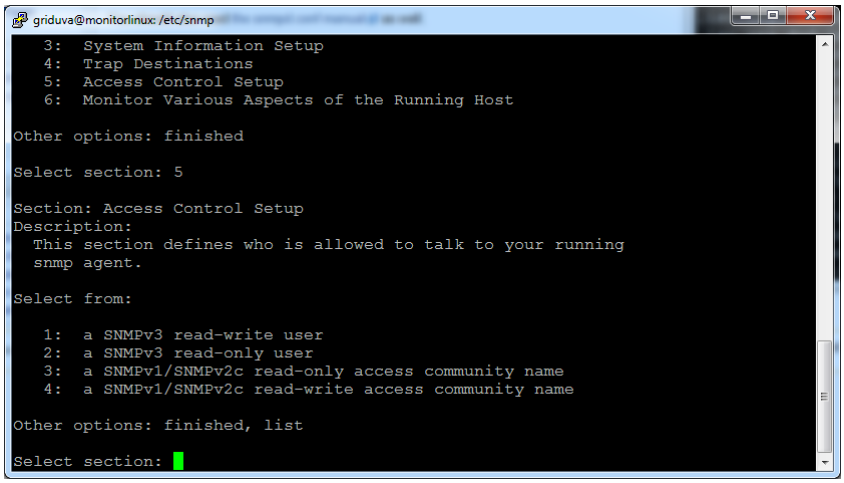


Fig. 69: Configurar opción de acceso a la comunidad.

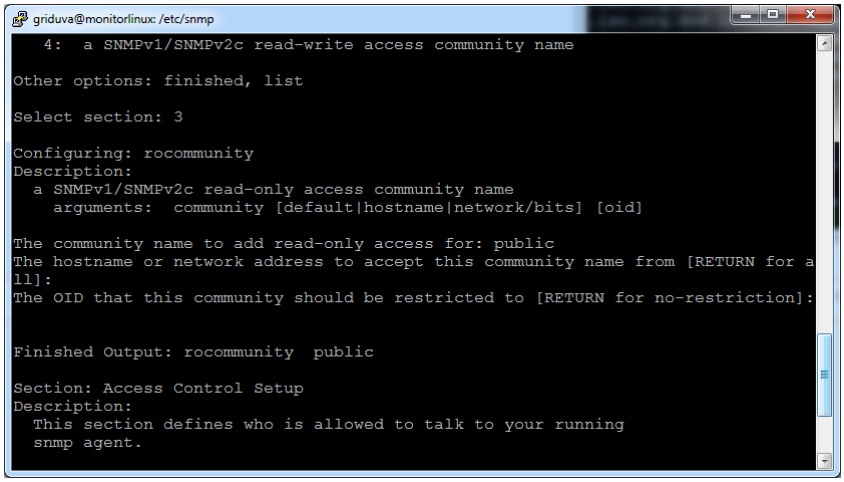


Fig. 70: Finalización configuración snmpd.

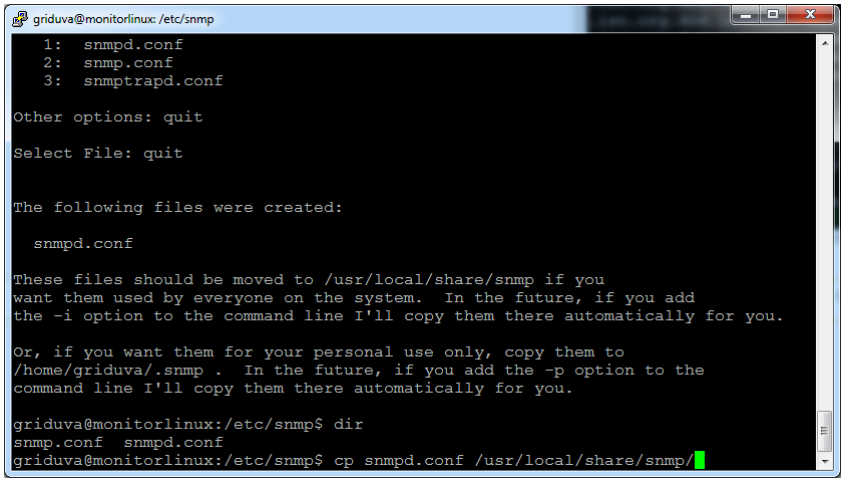


Fig. 71: Copia del archivo de configuración (snmpd.conf).

8. DEFINICIÓN DE SERVICIOS CON SNMP

8.1. Primitivas y utilidades de SNMP

Hay tres utilidades que permiten realizar consultas utilizando SNMP: snmpget, snmpgetnext y snmpwalk.

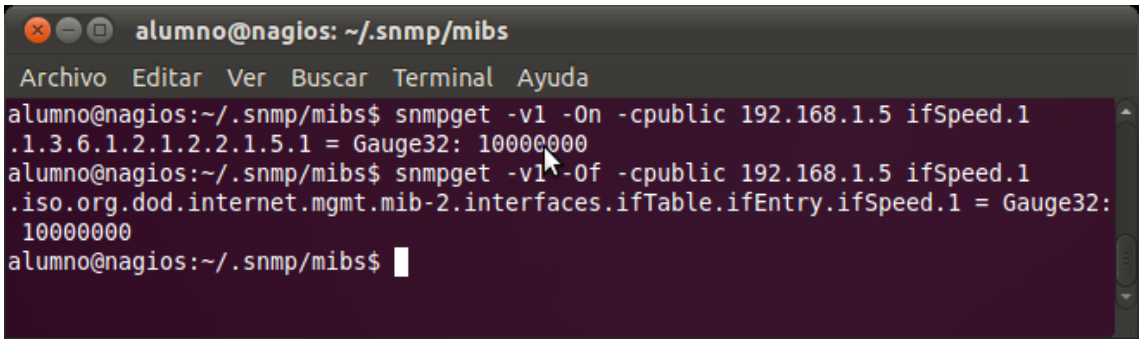
8.1.1. SNMPGET

Utiliza como parámetros:

-v: versión.

-O: n|f (numérico o texto).

-c: comunidad



8.1.2. SNMPGETNEXT

Muestra el siguiente elemento en el árbol:

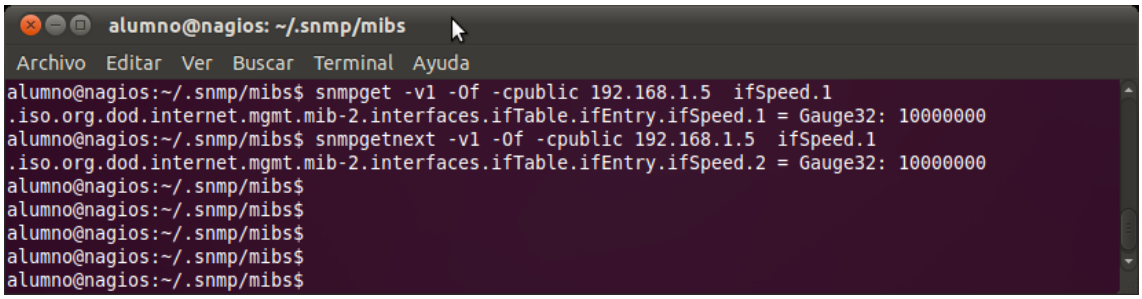


Fig. 72: Salida del comando snmpgetnext.

8.1.3. SNMPWALK

Hace una consulta de todos parámetros, o filtra por alguno en particular. Se puede utilizar la opción –Of para ver el árbol completo:

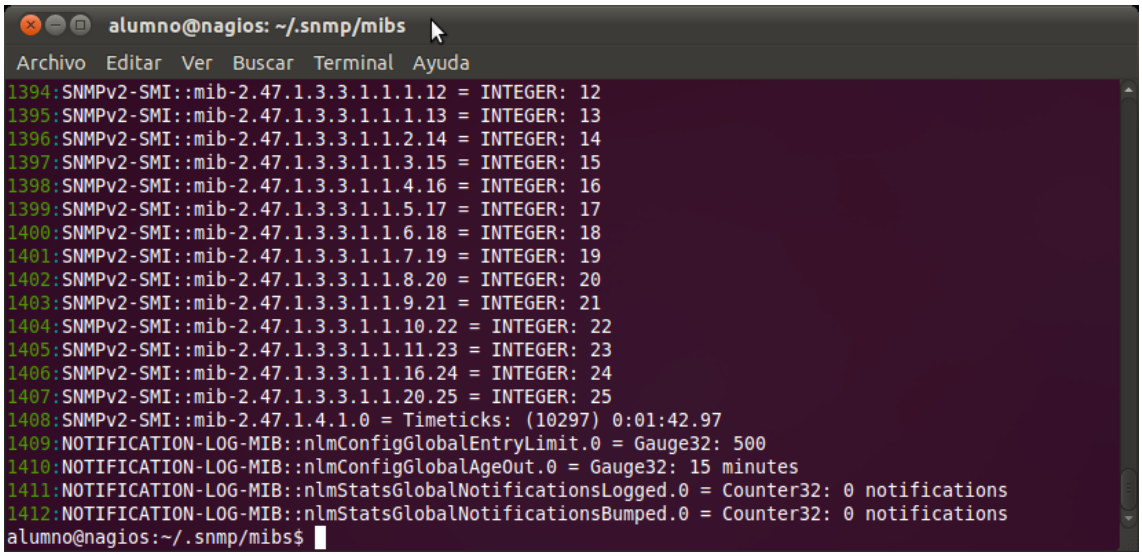


Fig. 73: Salida del comando smpwalk

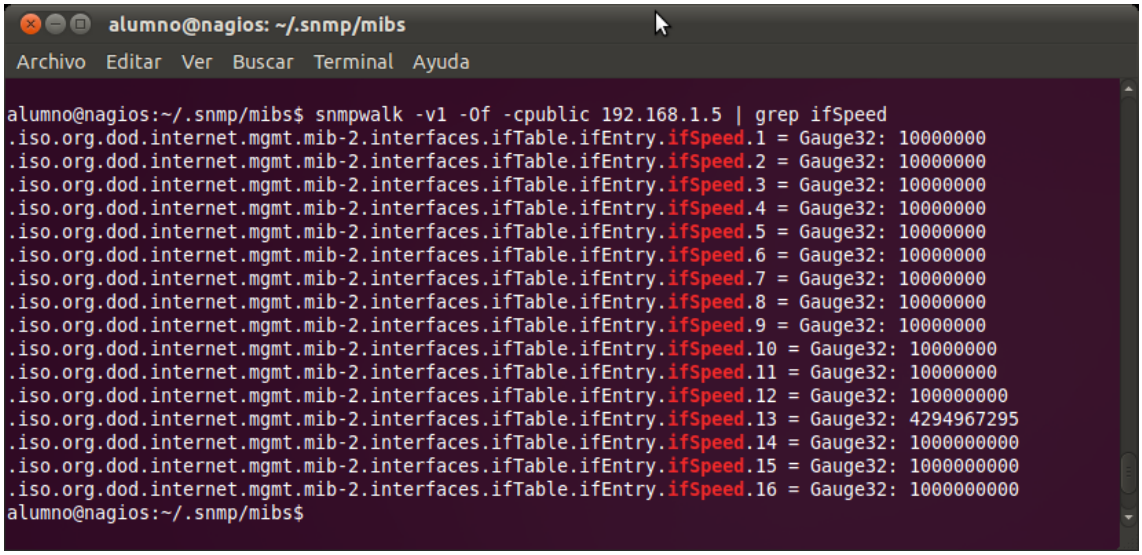


Fig. 74: Filtrado de la salida de snmpwalk

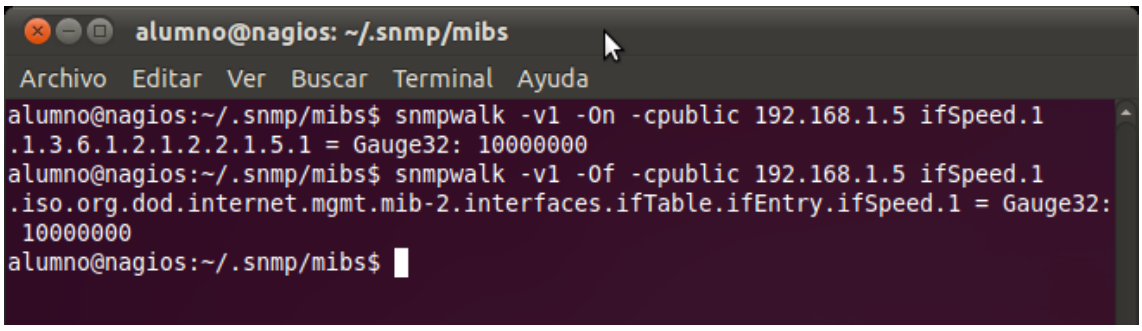


Fig. 75: Salidas con detalle del comando snmpwalk con parámetro fijado.

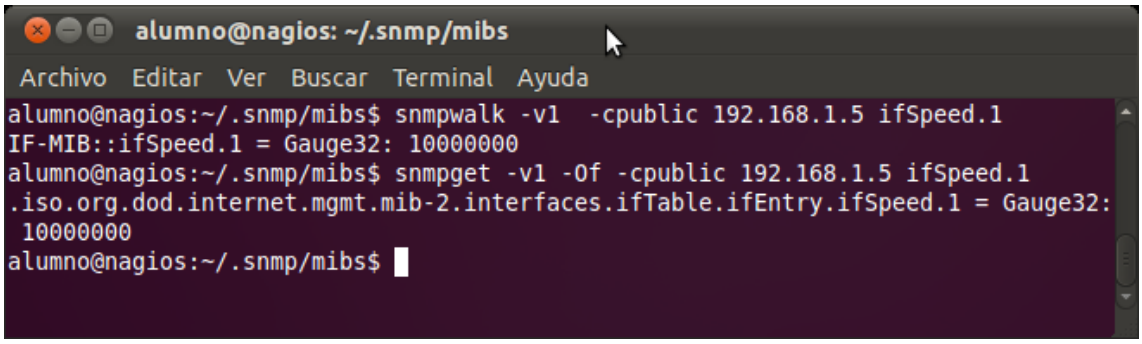


Fig. 76: Salida con y sin detalle de snmpwalk con parámetro fijado.

8.2. Plugins SNMP de Nagios[16]

8.2.1. Plugin check_snmp

Este plugin comprueba valores de OIDs utilizando el protocolo SNMP. Más adelante, en esta memoria, se detallan servicios que se pueden configurar con este comando. Puesto que es un comando muy utilizado, se adjunta la salida de la ayuda del comando (*check_snmp –h*):

```
check_snmp v1.4.15 (nagios-plugins 1.4.15)
Copyright (c) 1999-2007 Nagios Plugin Development Team
        <nagiosplug-devel@lists.sourceforge.net>

Comprueba el estado de mÃ¡quinas remotas y obtiene informaciÃ³n del sistema vÃ-a SNMP


Uso:
check_snmp -H <ip_address> -o <OID> [-w warn_range] [-c crit_range]
[-C community] [-s string] [-r regex] [-R regexi] [-t timeout] [-e retries]
[-l label] [-u units] [-p port-number] [-d delimiter] [-D output-delimiter]
[-m miblist] [-P snmp version] [-L seclevel] [-U secname] [-a authproto]
[-A authpasswd] [-x privproto] [-X privpasswd]

Options:
 -h, --help
    Print detailed help screen
 -V, --version
    Print version information
 -H, --hostname=ADDRESS
    Host name, IP Address, or unix socket (must be an absolute path)
 -p, --port=INTEGER
    Port number (default: 161)
 -n, --next
    Use SNMP GETNEXT en vez de SNMP GET
 -P, --protocol=[1|2c|3]
    VersiÃ³n del protocolo SNMP
 -L, --seclevel=[noAuthNoPriv|authNoPriv|authPriv]
    Nivel de seguridad SNMPv3
 -a, --authproto=[MD5|SHA]
    SNMPv3 auth proto
 -x, --privproto=[DES|AES]
    SNMPv3 priv proto (default DES)
 -C, --community=STRING
    Cadena de comunidad opcional para comunicaciÃ³n SNMP (el predeterminado es "public")
 -U, --secname=USERNAME
    nombre de usuario SNMPv3
 -A, --authpassword=PASSWORD
    contraseÃ±a de autenticaciÃ³n SNMPv3
 -X, --privpasswd=PASSWORD
    contraseÃ±a de privacidad SNMPv3
 -o, --oid=OID(s)
    Identificador(es) de objeto o variables SNMP cuyo valor desea consultar
```

[16] Ver apartados 11.3.1, 11.3.2 y 11.3.3 del libro Nagios 2nd edition.

```
 -m, --miblist=STRING
    List of MIBS to be loaded (default = none if using numeric OIDs or 'ALL'
    para OID simbÃ³licos)
 -d, --delimiter=STRING
    Delimitador a usar cuando se analizan datos retornados. Predeterminado "="
    Todos los datos sobre el lado derecho de la delimitador se considera
    que los datos que deben utilizarse en la evaluaciÃ³n.
 -w, --warning=THRESHOLD(s)
    Rango(s) de umbral de aviso
 -c, --critical=THRESHOLD(s)
    Rango(s) de umbral crÃ-tico
 --rate
    Enable rate calculation. See 'Rate Calculation' below
 --rate-multiplier
    Converts rate per second. For example, set to 60 to convert to per minute
 -s, --string=STRING
    Devuelve un estado OK (para esta OID) si CADENA coincide exactamente
 -r, --ereg=REGEX
    Return OK state (for that OID) if extended regular expression REGEX matches
 -R, --eregi=REGEX
    Return OK state (for that OID) if case-insensitive extended REGEX matches
 --invert-search
    Invert search result (CRITICAL if found)
 -l, --label=STRING
    Prefix label for output from plugin
 -u, --units=STRING
    Etiqueta(s) de unidades para datos de salida (p.ej. Â«seg.Â»).
 -D, --output-delimiter=STRING
    Separates output on multiple OID requests
 -t, --timeout=INTEGER
    Seconds before connection times out (default: 10)
 -e, --retries=INTEGER
    NÃºmero de intentos a usar en las peticiones
 -v, --verbose
    Show details for command-line debugging (Nagios may truncate output)

This plugin uses the 'snmpget' command included with the NET-SNMP package.
Si no tiene el paquete instalado, necesitarÃ¡ descargarlo desde
http://net-snmp.sourceforge.net antes de usar este complemento.

Notas:
 - Multiple OIDs may be indicated by a comma or space-delimited list (lists with
   internal spaces must be quoted). Maximum: 8 OIDs.
 - See:
 http://nagiosplug.sourceforge.net/developer-guidelines.html#THRESHOLDFORMAT
 for THRESHOLD format and examples.
 - Cuando se comprueban mÃºltiples OID, separe los rangos con comas como Â«-w 1:10,1:,:20Â»
 - Note that only one string and one regex may be checked at present
 - All evaluation methods other than PR, STR, and SUBSTR expect that the value
   returned from the SNMP query is an unsigned integer.

Rate Calculation:
 In many places, SNMP returns counters that are only meaningful when
 calculating the counter difference since the last check. check_snmp
 saves the last state information in a file so that the rate per second
 can be calculated. Use the --rate option to save state information.
 On the first run, there will be no prior state - this will return with OK.
 The state is uniquely determined by the arguments to the plugin, so
 changing the arguments will create a new state file.

Send email to nagios-users@lists.sourceforge.net if you have questions
regarding use of this software. To submit patches or suggest improvements,
send email to nagiosplug-devel@lists.sourceforge.net
```

8.2.2. Plugin check_ifstatus y check_ifoperstatus

Estos plugins permiten conocer el estado de las interfaces.

8.3. Otros Plugins SNMP

Se pueden descargar de la web de Nagios Exchange[17]. A continuación se muestra la utilización de cinco de ellos, escritos en lenguaje Perl:

- » check_catatlyst_temp.pl
- » check_catatlyst_flash.pl
- » check_catatlyst_mem.pl
- » check_catatlyst_fans.pl
- » check_catatlyst_load.pl

Antes de ejecutarlos, hay que instalar el módulo NET::SNMP de Perl. Si no está instalado, aparecerá el error:

Can't locate Net/SNMP.pm

Para instalarlo, ejecutar los siguientes comandos:

```
sudo perl -MCPAN -e shell
```

En la shell que aparecerá, ejecutar el install (es posible que pregunte cosas, aceptar todo):

```
CPAN>install Net::SNMP
```

Una vez instalado, hay que modificar la ruta a los plugins de Nagios. Para ello editar cada uno de los scripts y modificar las líneas para especificar la ruta correcta:

```
#use lib "/usr/lib/nagios/plugins/";
use lib "/usr/local/nagios/libexec/";
```

La imagen siguiente muestra la ejecución de los scripts:

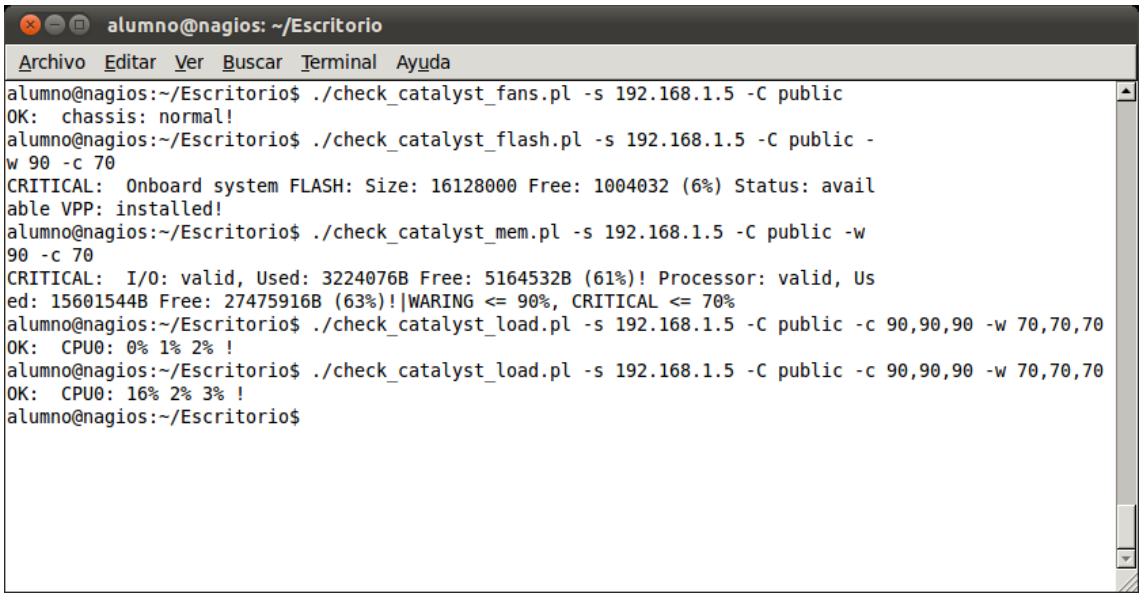


Fig. 77: Scripts en Perl para desarrollar más comandos en Nagios.

[17] http://exchange.nagios.org/directory/Plugins/Network-Protocols/SNMP

Estos comandos, una vez comprobado su funcionamiento, se pueden integrar en los ficheros .cfg de Nagios.

La ejecución anterior se ha hecho sobre un switch CISCO CATALYST 3550-12G. Este switch no soporta la consulta sobre sensores de temperatura. Otros switches de CISCO sí dan una lectura correcta.

8.4. SNMP Traps

8.4.1. Envío y recepción de traps

Para poder recbir traps, primero hay que configurar el dispositivo. Una vez habilitadas y configurada la estación que recibirá estos traps, hay que utilizar una herramienta que sea capaz de leerlas (UDP, puerto 162). La siguiente figura muestra unas traps recibidas al desconectar un puerto Ethernet (tipo linkdown) en un switch CISCO CATALYST 3550.

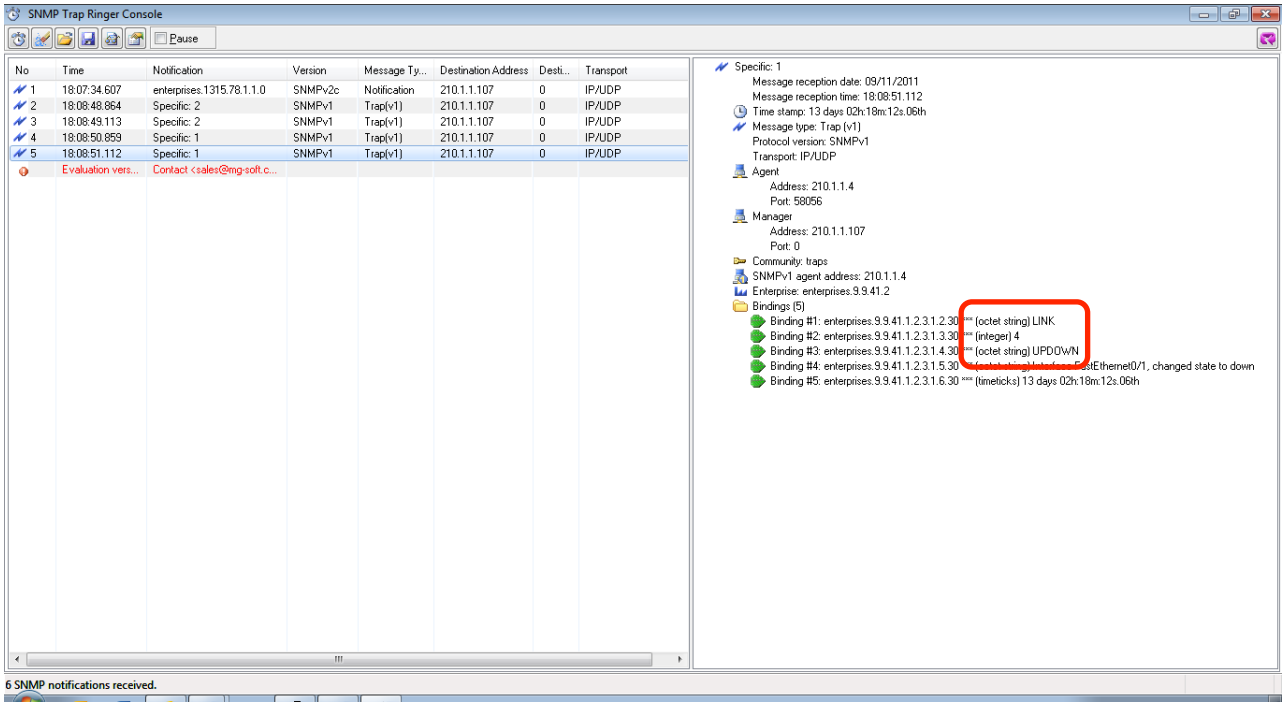


Fig. 78: Traps SNMP enviadas por un swtch y recibidas en la estación de gestión.

Las líneas siguientes habilitan el envío de traps a la estación gestora 192.168.1.100[18] en un switch snmp (desde modo config):

```
snmp-server community public ro
snmp-server community private rw
snmp-server host 192.168.1.100 traps public
snmp-server enable traps
```

[18] Desactivar el firewall de la estación o añadir reglas para ICMP y UDP en los puertos involucrados.

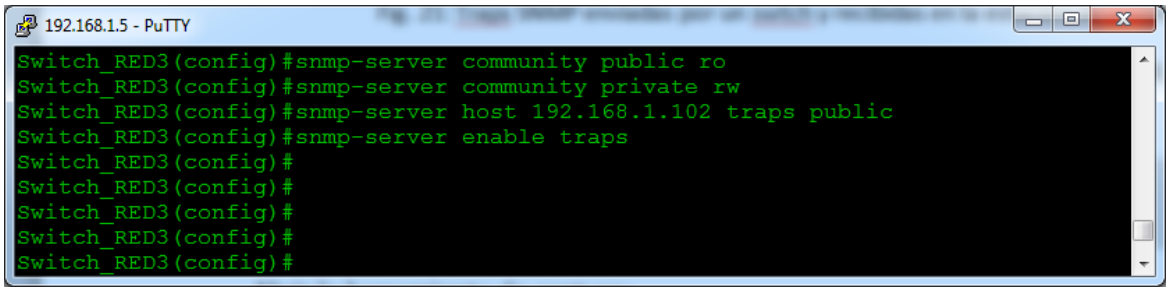


Fig. 79: Configuración comunidad y traps SNMP en switch CISCO.

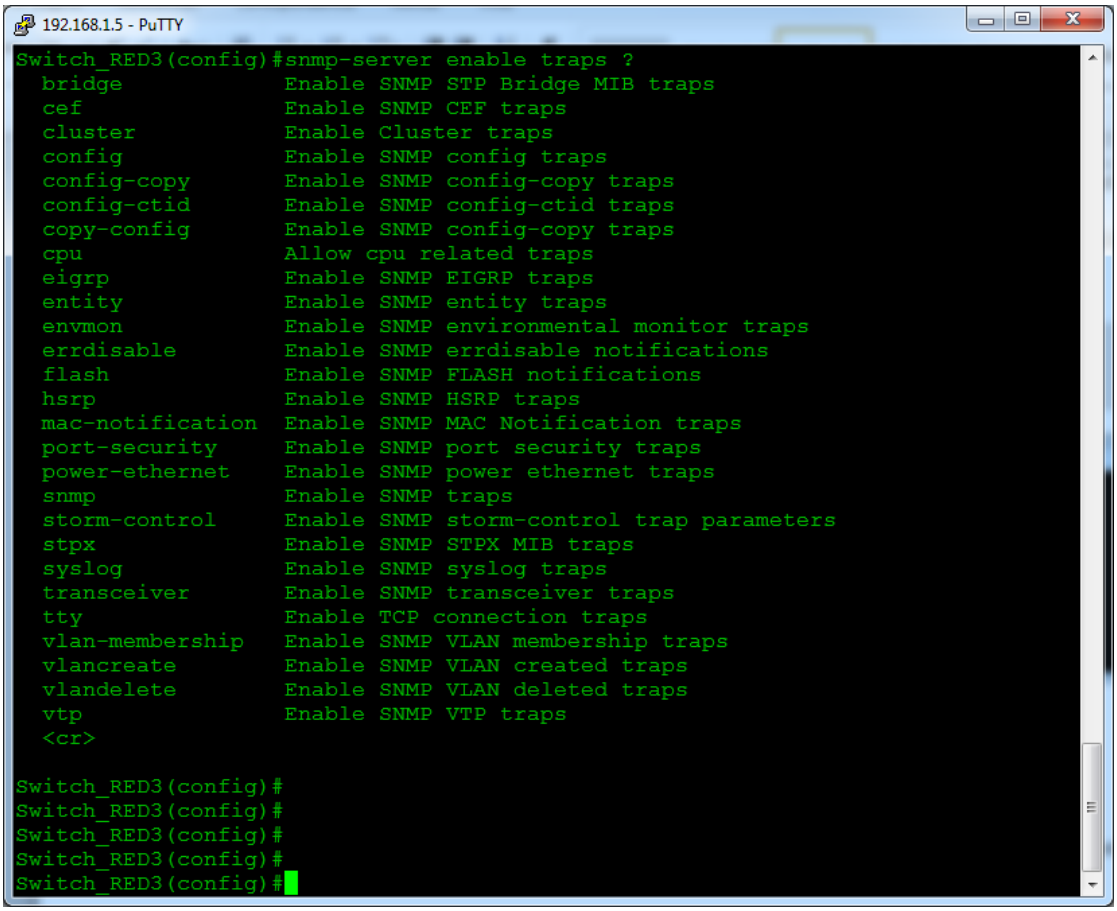


Fig. 80: Tipos de traps (CISCO CATALYST 3550-12G).

Abrir la herramienta de captura para recibir los traps. En el mercado hay numerosas herramientas con versiones de evaluación que, aunque tienen capacidades limitadas, permiten leer un número limitado de traps y así permitir verificar la configuración de los equipos.

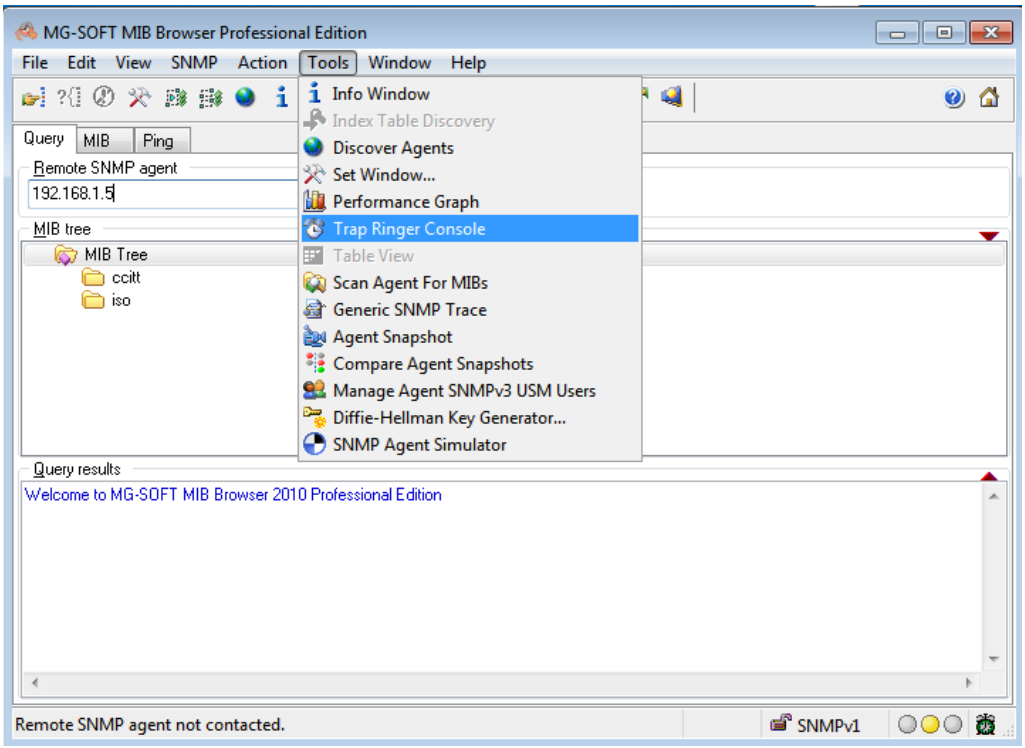


Fig. 81: Herramienta de captura de traps SNMP Trap Ringer Console de MG-SOFT.

Según se envíen los traps, aparecerán en la ventana. Esta herramienta sólo permite recibir los primeros 5 traps. Después de esto reiniciar para seguir recibiendo más:

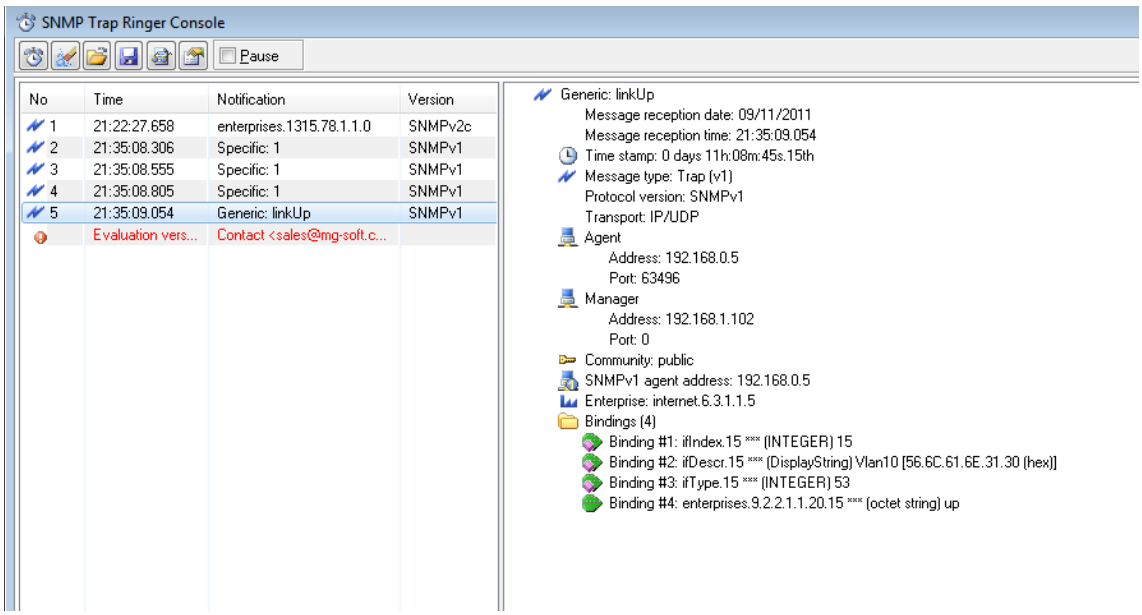


Fig. 82: Vista detalle de trap de tipo LINKUP.

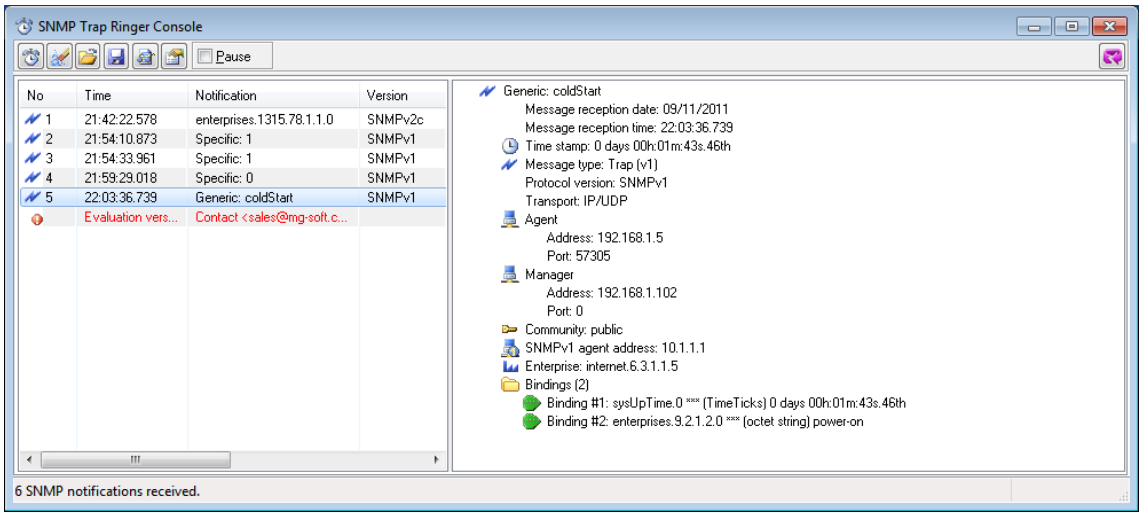


Fig. 83: Vista detalle de trap de tipo cold-start.

8.4.2. NSCA, configuración de traps en Nagios

Nagios tiene un sistema para poder recibir notificaciones mediante una tubería (pipe de UNIX). Se denomina NSCA[19][20](Nagios Service Check Acceptor). Sin embargo, se debe instalar un software que adapte los traps y se los envíe a este componente de Nagios.

Para ello, si no se ha hecho antes, se debe instalar el paquete completo net-snmp que incluye la herramienta *snmptrap*.

8.5. Desarrollo de una Herramienta de captura de Traps

A continuación se muestra el código fuente en Java de un programa que captura los paquetes enviados mediante los traps del protocolo SNMP.

```
package dsockets;

import java.net.*;
import java.io.*;

public class servidor {

        public static void main(String Args[]) throws IOException {

                byte buffer[] = new byte[500];
                String cadena;
                int p=162;
                DatagramSocket conexion = new DatagramSocket(p);
                System.out.println("Servidor escuchando en el puerto: "+p);
                DatagramPacket dp;
                int i=1;
                do {
                        dp = new DatagramPacket(buffer,buffer.length);
                        System.out.println("... esperando traps ...");
                        conexion.receive(dp);
                        buffer = dp.getData();
                        cadena = (new String(buffer)).substring(0,dp.getLength());
                        //System.out.write(dp.getData(),0,dp.getLength());
```

[19] http://nagios.sourceforge.net/download/contrib/documentation/misc/NSCA_Setup.pdf
[20] Ver apartado 14.6 del libro Nagios 2nd edition.

```
                        System.out.println("");
                        System.out.println("["+i+"] Se ha recibido un trap [longitud =
"+dp.getLength()+" bytes]");
                        System.out.println("-----------------------------------------------------
----------------------");
                        System.out.println(cadena);
                        System.out.println("-----------------------------------------------------
----------------------");
                        System.out.println("");
                        i++;
                }
                while (!cadena.equals("adios"));
                conexion.disconnect();
                conexion.close();
        }
}
```

A continuación se muestra una captura del programa en Java que captura traps:

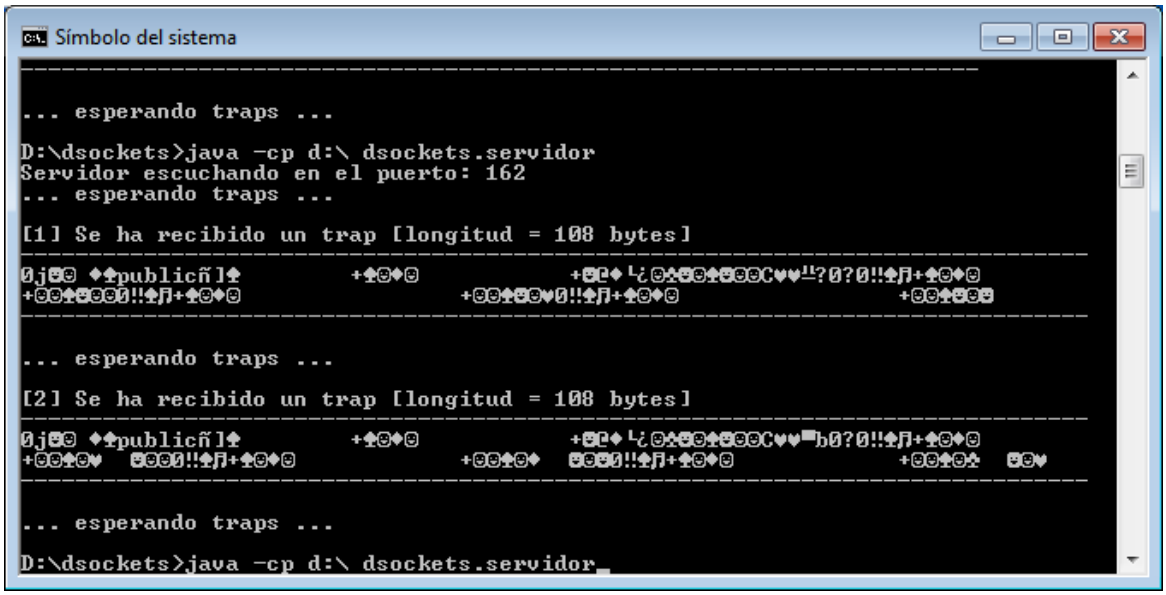


Fig. 84: Ejecución del servidor de lectura de traps (servidor.class)

Para ejecutarlo, se debe tener instalada una máquina Java (al menos JRE[21]). Se debe descomprimir y copiar en el directorio x:\dsockets, para que funcione la línea de la captura anterior.

Esta herramienta tan sólo pretende ser un ejemplo de captura. Existen librerías en Java para poder decodificar los paquetes recibidos.

[21] http://www.oracle.com/technetwork/java/javase/downloads/index.html

Fig. 85: Página de descarga de Java (JDK o JRE)

En caso de tener una herramienta de este tipo ya instalada, hay que deshabilitar el servicio para liberar el puerto del servicio (no puede haber dos servidores arrancados usando el mismo puerto). En este caso configurar el inicio manual (parar no suele ser suficiente):

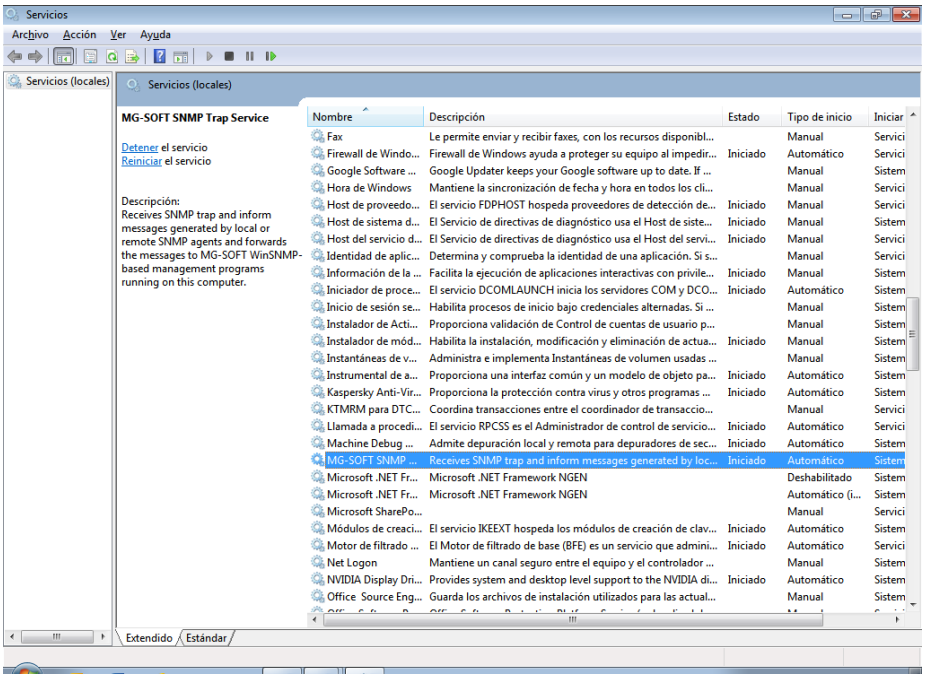


Fig. 86: Servicios relacionados con los traps SNMP.

9. CASOS PRÁCTICOS DE GESTIÓN DE SERVICIOS Y APLICACIONES

9.1. Informix

Utilizando SNMP, se puede monitorizar el estado de este servidor. Se sondea el puerto TCP 1527, que es donde está arrancado el servidor en los sistemas del SACYL, y se testea el proceso Oninit.

```
###############################################################################
#
# Informix ONLINE SERVICE DEFINITIONS
#
###############################################################################

# Define a service to check if process exist.
# 'Proceso Oninit'
# comando 'check_snmp_process_lento'
define service{
            use                     generic-service  ; Name of service template to use
            host_name               pacientes
            service_description     IFX Proceso Oninit
            check_command           check_snmp_process_lento!oninit!0!0!-r
}

# Define a service to check the conection to TCP port.
# Warning over 1 second on time response,critical over 2 seconds
# 'Puerto_Informix_1527'
define service{
            use                     generic-service     ;Name of service template to use
            hostgroup_name          informix-servers
            service_description     IFX Serv_ifx 1527
            check_command           check_tcp_hcuv!1527!1!2
}
```

El comando modificado check_snmp_lento se utiliza cuando es necesario ampliar el timeout en la ejecución del mismo, debido a la sobrecarga del servidor y el consiguiente tiempo de respuesta en ejecutarlo. Se puede añadir al fichero *commands.cfg*:

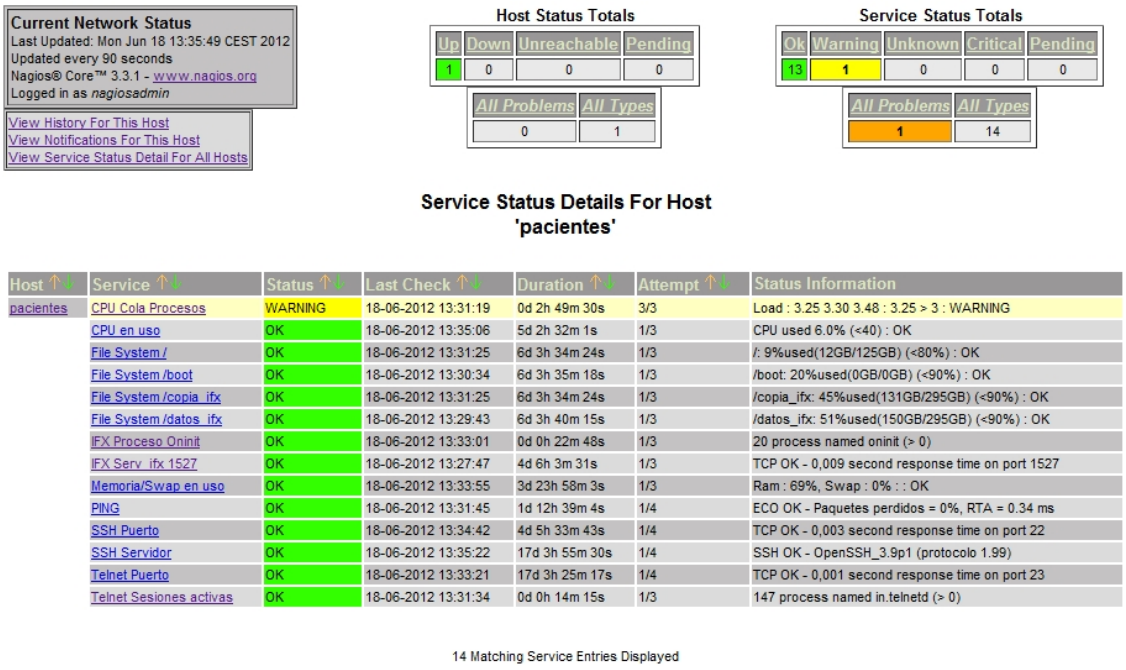
```
# 'check_snmp_process_lento' command definition. Servidor lento
# Comprueba si se encuentra en ejecución el proceso suministrado como argumento
define command{
            command_name         check_snmp_process_lento
            command_line              $USER1$/check_snmp_process_lento.pl  -H  $HOSTADDRESS$  -C
$USER5$ -n $ARG1$ -w $ARG2$ -c $ARG3$ $ARG4$
            ;$ARG1$                   proceso a comprobar
            ;$ARG2$                   warning
            ;$ARG3$                   critical
            ;$ARG4$                   parámetros opcionales (-r)
            }


# Check conection to tcp port
# 'check_tcp' command
define command{
            command_name         check_tcp_hcuv
            command_line              $USER1$/check_tcp -H $HOSTADDRESS$ -p $ARG1$ -w $ARG2$ -c
$ARG3$
            ;$ARG1$                   port
            ;$ARG2$                    warning
            ;$ARG3$                   critical
}
```

El fragmento de código modificado del script *snmp_process* en Perl es el siguiente:

```
#!/usr/bin/perl -w
############################## check_snmp_process ##############
my $Version='1.10';
# Date : Oct 12 2007
# Author  : Patrick Proy (patrick at proy dot org)
# Help : http://nagios.manubulon.com
# Licence : GPL - http://www.fsf.org/licenses/gpl.txt
# Contrib : Makina Corpus, adam At greekattic d0t com
```

```
# TODO : put $o_delta as an option
#    If testing on localhost, selects itself....
#############################################################
#
# help : ./check_snmp_process -h

use strict;
use Net::SNMP;
use Getopt::Long;

############## BASE DIRECTORY FOR TEMP FILE ########
my $o_base_dir="/tmp/tmp_Nagios_proc.";
my $file_history=2000;    # number of data to keep in files.
my $delta_of_time_to_make_average=300;  # 5minutes by default

# Nagios specific

#my $TIMEOUT = 15;
my $TIMEOUT = 70;
```

Como ejemplo práctico, se puede consultar el fichero de configuración completo para la gestión de pacientes en el anexo VI. El resultado es el de la figura siguiente:



Current Network Status
Last Updated: Mon Jun 18 13:35:49 CEST 2012
Updated every 90 seconds
Nagios® Core™ 3.3.1 - www.nagios.org
Logged in as *nagiosadmin*

View History For This Host
View Notifications For This Host
View Service Status Detail For All Hosts

Host Status Totals

Up	Down	Unreachable	Pending
1	0	0	0

All Problems	All Types
0	1

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
13	1	0	0	0

All Problems	All Types
1	14

Service Status Details For Host 'pacientes'

Host	Service	Status	Last Check	Duration	Attempt	Status Information
pacientes	CPU Cola Procesos	WARNING	18-06-2012 13:31:19	0d 2h 49m 30s	3/3	Load : 3.25 3.30 3.48 : 3.25 > 3 : WARNING
	CPU en uso	OK	18-06-2012 13:35:06	5d 2h 32m 1s	1/3	CPU used 6.0% (<40) : OK
	File System /	OK	18-06-2012 13:31:25	6d 3h 34m 24s	1/3	/: 9%used(12GB/125GB) (<80%) : OK
	File System /boot	OK	18-06-2012 13:30:34	6d 3h 35m 18s	1/3	/boot: 20%used(0GB/0GB) (<90%) : OK
	File System /copia_ifx	OK	18-06-2012 13:31:25	6d 3h 34m 24s	1/3	/copia_ifx: 45%used(131GB/295GB) (<90%) : OK
	File System /datos_ifx	OK	18-06-2012 13:29:43	6d 3h 40m 15s	1/3	/datos_ifx: 51%used(150GB/295GB) (<90%) : OK
	IFX Proceso Oninit	OK	18-06-2012 13:33:01	0d 0h 22m 48s	1/3	20 process named oninit (> 0)
	IFX Serv_ifx 1527	OK	18-06-2012 13:27:47	4d 6h 3m 31s	1/3	TCP OK - 0,009 second response time on port 1527
	Memoria/Swap en uso	OK	18-06-2012 13:33:55	3d 23h 58m 3s	1/3	Ram : 69%, Swap : 0% : : OK
	PING	OK	18-06-2012 13:31:45	1d 12h 39m 4s	1/4	ECO OK - Paquetes perdidos = 0%, RTA = 0.34 ms
	SSH Puerto	OK	18-06-2012 13:34:42	4d 5h 33m 43s	1/4	TCP OK - 0,003 second response time on port 22
	SSH Servidor	OK	18-06-2012 13:35:22	17d 3h 55m 30s	1/4	SSH OK - OpenSSH_3.9p1 (protocolo 1.99)
	Telnet Puerto	OK	18-06-2012 13:33:21	17d 3h 25m 17s	1/4	TCP OK - 0,001 second response time on port 23
	Telnet Sesiones activas	OK	18-06-2012 13:31:34	0d 0h 14m 15s	1/3	147 process named in.telnetd (> 0)

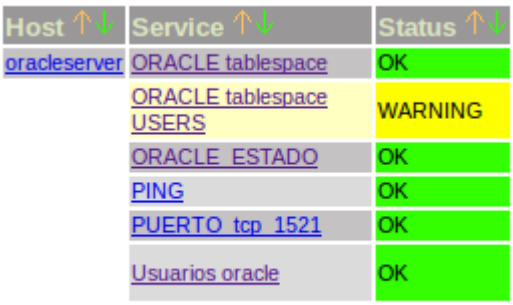
14 Matching Service Entries Displayed

Fig. 87: Estado de los servicios monitorizados para la gestión de pacientes.

9.2. Oracle

En la siguiente figura se muestran los servicios de Oracle que se han seleccionado como los importantes para monitorizar en el servicio.

Además de la comprobación de conexión utilizando un ping, y del puerto de escucha (TCP del servidor), se han incluido comprobaciones de los tablespace que se han identificado como importantes.



Host	Service	Status
oracleserver	ORACLE tablespace	OK
	ORACLE tablespace USERS	WARNING
	ORACLE_ESTADO	OK
	PING	OK
	PUERTO_tcp_1521	OK
	Usuarios oracle	OK

Fig. 88: Servicios de Oracle monitorizados.

Para la monitorización de los servicios en Nagios, se han creado comandos especfícos. Algunos son variaciones de los comandos estándar de Nagios y otros son nuevos, utilizando scripts de Perl y programas en Java.

Será necesario tener instalado el intérprete de Perl[22] y al menos el runtime de Java[23].

9.2.1. Servicio de comprobación de la máquina (ping)

Para comprobar que la máquina está online se usa el comando de comprobación que utiliza el comando *check_ping* integrado en la instalación base de Nagios:

```
define service{
        use                             local-service         ; Name of service template to use
        host_name                       oracleserver
        service_description             PING
            check_command               check_ping!100.0,20%!500.0,60%
        }
```

9.2.2. Servicio de comprobación del puerto del servidor Oracle

El servidor Oracle escucha en el puerto TCP 1521. Para monitorizar este servico se ha creado el comando *check_tcp_10*.

```
define service{
        use                             local-service         ; Name of service template to use
        host_name                       oracleserver
        service_description             PUERTO_tcp_1521
        check_command                   check_tcp_10

        }
```

El comando *check_tcp_10* se define de laa siguiente manera, en base al estándar de Nagios *check_tcp*:

```
define command{
         command_name        check_tcp_10
         command_line        $USER1$/check_tcp -H 10.36.32.10 -p 1521
                }
```

9.2.3. Servicio ORACLE tablespace

Este servicio comprueba el estado de un tablespace. El servicio se define de la forma:

```
define service{
        use                     local-service           ; Name of service template to use
        host_name               oracleserver
        service_description     ORACLE tablespace
```

[22] Ver instalación de Nagios en el capítulo correspondiente de este libro.
[23] Descargar Java SE (JRE o JSDK) en:
http://www.oracle.com/technetwork/java/javase/downloads/index.html

```
        check_command     check_tablespace_oracle
    }
```

Este servicio utiliza el comando check_tablespace_oracle que se crea con el siguiente código:

```
define command{
        command_name    check_tablespace_oracle
        command_line    java  -classpath  /usr/local/nagios/libexec/  check_tablespace_oracle
10.36.32.10 1521 orcl CSMA "CSMA" -d
}
```

La salida se puede observar en la siguiente figura:

Current Status:	OK (for 0d 9h 42m 27s)
Status Information:	DB connect: jdbc:oracle:thin:CSMA/CSMA@10.36.32.10:1521:orcl DB query: select df.TABLESPACE_NAME, df.FILE_ID, ((df.BYTES+fs.BYTES)/1024) kbytes_max, (df.BYTES/1024) kbytes_used, round(((df.BYTES - fs.BYTES) / df.BYTES) * 100) usage_pct from (select TABLESPACE_NAME, sum(BYTES) BYTES, count(distinct FILE_ID) FILE_ID from dba_data_files group by TABLESPACE_NAME) df, (select TABLESPACE_NAME, sum(BYTES) BYTES from dba_free_space group by TABLESPACE_NAME) fs where df.TABLESPACE_NAME=fs.TABLESPACE_NAME order by df.TABLESPACE_NAME asc Name: EXAMPLE Files: 1 Space total: 125568 KB Space used: 102400 KB Space % used: 77 % Name: SYSAUX Files: 1 Space total: 410304 KB Space used: 399360 KB Space % used: 97 % Name: SYSTEM Files: 1 Space total: 503104 KB Space used: 501760 KB Space % used: 100 % Name: UNDOTBS1 Files: 1 Space total: 422080 KB Space used: 215040 KB Space % used: 4 % Name: USERS Files: 3 Space total: 2421888 KB Space used: 1270016 KB Space % used: 9 %
Performance Data:	
Current Attempt:	1/4 (HARD state)

Fig. 89: Salida del commando de comprobación de tablespace.

En el resultado se puede ver que la conexión a la base de datos se ha realizado correctamente y por tanto podemos ejecutar la consulta SQL. En la parte inferior, en las cadenas que empiezan por "Name", se muestran los distintos tablespace que existen y porcentaje usado.

Este servicio utiliza el programa de Java *check_tablespace_oracle*. El código completo se puede consultar en el anexo X. Para invocarlo, se puede ejecutar el comando desde la línea de comandos:

```
java -classpath /usr/local/nagios/libexec/ check_tablespace_oracle 10.36.32.10 1521 orcl CSMA
"CSMA" -d
```

9.2.4. ORACLE tablespace USERS

Se utiliza el mismo código, pero esta vez sólo consulta un tablespace. El tablespace monitorizado es USERS. En el comando se fijan los parametros de warning y error.

La salida se muestra en la siguiente figura:

Service State Information

Current Status:	WARNING (for 0d 9h 44m 2s)
Status Information:	Tablespace WARN: USERS 9% used
Performance Data:	USERS: 3 datafiles, used 1270016 KB of 2421888 KB total

Fig. 90: Resultado de la consulta del tablespace USERS.

Se utiliza el servicio Oracle tablespace USERS:

```
define service{
        use                     local-service           ; Name of service template to use
        host_name               oracleserver
        service_description     ORACLE tablespace USERS
        check_command           check_tablespace_oracle2

        }
```

Este servicio utiliza un nuevo comando rescrito *check_tablaspace_oracle2*:

```
define command{
            command_name    check_tablespace_oracle2
            command_line    java  -classpath  /usr/local/nagios/libexec/  check_tablespace_oracle
10.36.32.10 1521 orcl CSMA "CSMA" USERS 1000000 3000000
}
```

Como en el servicio anterior, utiliza el programa de Java *check_tablespace_oracle*. El código completo se puede consultar en el anexo X.

9.2.5. ORACLE estado

Este commando, además de hacer una connexion con la base de datos, puede comprobar los parámetros de rendimiento de la base de datos que se necesiten en cualquier momento.

La siguiente figura muestra el resultado de la ejecución del comando:

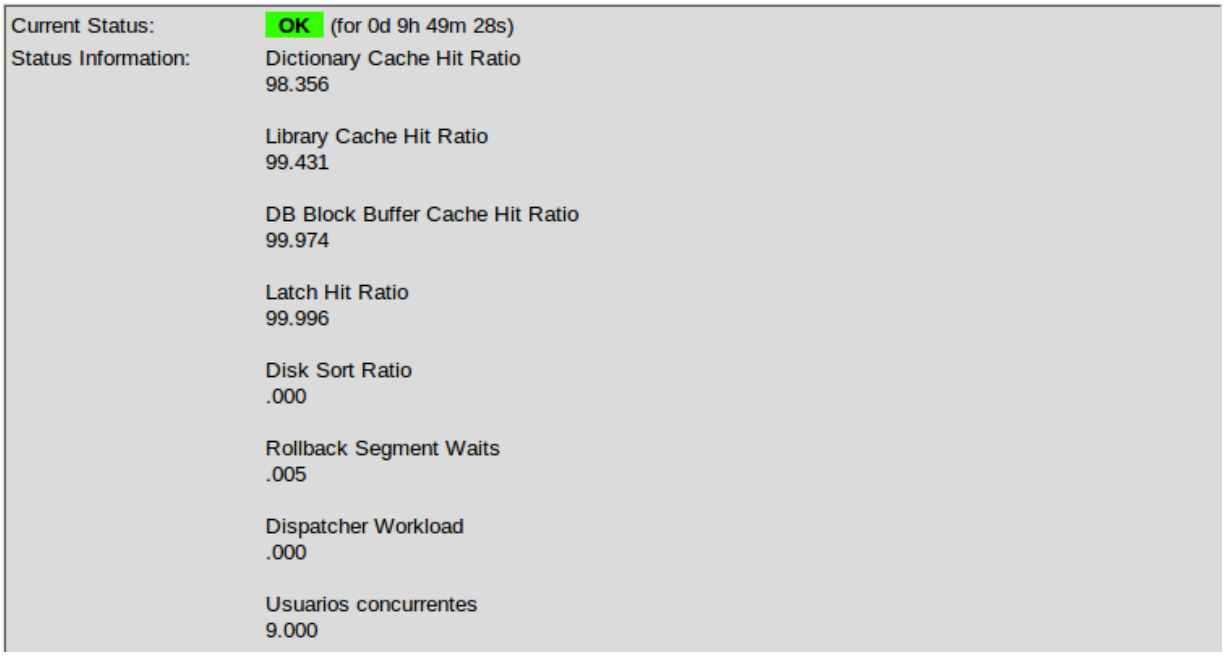


Fig. 91: Resultados de rendimiento de Oracle.

La definición del servicio es la siguiente:

```
define service{
        use                     local-service           ; Name of service template to use
        host_name               oracleserver
        service_description     ORACLE_ESTADO
            check_command       check_oracle_instant!1521!orcl!CSMA!CSMA

}
```

El servicio ORACLE_ESTADO utiliza el comando check_oracle_instant. Este es un script escrito en lenguaje Perl. El listado completo de este script se puede consultar en el anexo XIII.

9.2.6. Usuarios ORACLE

Este commando es interesante por dos motivos. En primer lugar, utilizando este comando se puede averigar qué usuarios están conectados. Además también permite conocer el número de conexiones simultáneas que existen en un determinado instante.

La siguiente figura muestra el resultado de la ejecución del servicio:

Service State Information

Current Status:	OK (for 0d 8h 43m 56s)
Status Information:	null, CSMA, SYSMAN, null, SYSMAN, SYSMAN, SYSMAN, DBSNMP, SYSMAN, DBSNMP, null, null, SYSMAN, null, null, null, null, null, null, null, null, null, null, null,
Performance Data:	
Current Attempt:	1/4 (HARD state)
Last Check Time:	15-06-2012 17:30:32
Check Type:	ACTIVE

Fig. 92: Resultado de Oracle users.

El servicio que se utiliza se define como:

```
define service{
        use                     local-service           ; Name of service template to use
        host_name               oracleserver
        service_description     Usuarios oracle
        check_command       check_users_oracle

        }
```

Utiliza el comando *check_users_oracle*:

```
define command{
    command_name     check_users_oracle
   command_line      java -classpath /usr/local/nagios/libexec/ check_users_oracle 10.36.32.10
1521 orcl CSMA "CSMA" 70 100
}
```

Este nuevo comando creado utiliza el programa Java *check_users_oracle*, que se incluye de forma completa en el anexo XI.

Para optimizar este commando se deberían quitar algunos null y los usuarios de sistema. También hay que tener en cuenta que algunos usuarios como por ejemplo CSMA, es un usuario de una aplicación.

9.3. Mysql

Al igual que en Oracle, este gestor permite verificar muchos de los parámetros que antes se han identificado como críticos. Sin embargo, Oracle se utiliza mucho más en los servicios, por lo que el trabajo se ha centrado en dicha herramienta.

Además de ver el estado de las tablas, el espacio en disco o memoria, también se puede monitorizar el estado del servidor verificando el proceso *mysqld*. Para ello, se puede utilizar el comando snmp para verificar los procesos que están arrancados:

```
define service {
        use                     generic-service
        host_name               monitorlinux
        service_description     Mysql service
        check_command           check_snmp_process!public!mysqld!0,2!0,2
}
```

9.4. SQL server

Para monitorizar el estado del servidor, se puede gestionar el proceso *sqlservr*:

```
define service{
        use                     generic-service
        host_name               callmanager
        service_description     SQL Server
        check_command           check_snmp_process!public!sqlservr!3,100!0!-2 -m 20,30 -u 90,99
}
```

Un ejemplo de monitorización se puede ver en la gestión de un Call Manager de Cisco, más adelante en este capítulo.

9.5. IIS

IIS ofrece los contadores para servicios de (SNMP). Estos contadores se definen con más detalle en tres archivos MIB: Inetsrv.mib, Http.mib y Ftp.mib, que se pueden encontrar en la carpeta Windir\System32. Inetsrv.MIB es un objeto contenedor para los otros dos archivos y, por tanto, no contiene contadores.

En la MIB (HTTP.MIB) se pueden ver alguno de ellos, por ejemplo el número de ficheros enviados (.1.3.6.1.4.1.311.1.7.3.1.5.0), o los usuarios anónimos actuales atendidos por el servidor (.1.3.6.1.4.1.311.1.7.3.1.7.0). Ver el siguiente fragmento de la MIB[24]:

```
HTTPSERVER-MIB DEFINITIONS ::= BEGIN

        IMPORTS
                enterprises,
                OBJECT-TYPE,
                Counter
                        FROM RFC1155-SMI
                internetServer
                        FROM INTERNETSERVER-MIB;

--      microsoft       OBJECT IDENTIFIER ::= { enterprises 311 }
--      software        OBJECT IDENTIFIER ::= { microsoft 1 }
--      internetServer  OBJECT IDENTIFIER ::= { software 7 }
        httpServer      OBJECT IDENTIFIER ::= { internetServer 3 }
        httpStatistics  OBJECT IDENTIFIER ::= { httpServer 1 }

-- Http Server Statistics

        totalBytesSentHighWord OBJECT-TYPE
                SYNTAX  Counter
                ACCESS  read-only
                STATUS  mandatory
                DESCRIPTION
                        "This is the high 32-bits of the total number of
                        of BYTEs sent by the HTTP Server."
                ::= { httpStatistics 1 }

        totalBytesSentLowWord OBJECT-TYPE
                SYNTAX  Counter
                ACCESS  read-only
                STATUS  mandatory
                DESCRIPTION
                        "This is the low 32-bits of the total number of
                        of BYTEs sent by the HTTP Server."
                ::= { httpStatistics 2 }

        totalBytesReceivedHighWord OBJECT-TYPE
                SYNTAX  Counter
                ACCESS  read-only
                STATUS  mandatory
                DESCRIPTION
                        "This is the high 32-bits of the total number of
                        of BYTEs received by the HTTP Server."
                ::= { httpStatistics 3 }
```

[24] La MIB complete se puede consultar en el anexo IX.

```
        totalBytesReceivedLowWord OBJECT-TYPE
                SYNTAX  Counter
                ACCESS  read-only
                STATUS  mandatory
                DESCRIPTION
                        "This is the low 32-bits of the total number of
                        of BYTEs received by the HTTP Server."
                ::= { httpStatistics 4 }

        totalFilesSent OBJECT-TYPE
                SYNTAX  Counter
                ACCESS  read-only
                STATUS  mandatory
                DESCRIPTION
                        "This is the total number of files sent by this
                        HTTP Server."
                ::= { httpStatistics 5 }

        totalFilesReceived OBJECT-TYPE
                SYNTAX  Counter
                ACCESS  read-only
                STATUS  mandatory
                DESCRIPTION
                        "This is the total number of files received by this
                        HTTP Server."
                ::= { httpStatistics 6 }

        currentAnonymousUsers OBJECT-TYPE
                SYNTAX  Counter
                ACCESS  read-only
                STATUS  mandatory
                DESCRIPTION
                        "This is the number of anonymous users currently
                        connected to the HTTP Server."
                ::= { httpStatistics 7 }
```

El siguiente fichero de configuración permite consultar algunos contadores interesantes:

```
define service{
        use                     generic-service ; Inherit values from a template
        host_name               monitorwindows
        service_description     HTTP counters files sent SNMP
        check_command           check_snmp!-C public -o .1.3.6.1.4.1.311.1.7.3.1.5.0
        }
define service{
        use                     generic-service ; Inherit values from a template
        host_name               monitorwindows
        service_description     HTTP usuarios actuales
        check_command           check_snmp!-C public -o .1.3.6.1.4.1.311.1.7.3.1.7.0
        }
define service{
        use                     generic-service ; Inherit values from a template
        host_name               monitorwindows
        service_description     HTTP conexiones actuales
        check_command           check_snmp!-C public -o .1.3.6.1.4.1.311.1.7.3.1.13.0
        }

define service{
        use                     generic-service ; Inherit values from a template
        host_name               monitorwindows
        service_description     HTTP num max conexiones simultaneas
        check_command           check_snmp!-C public -o .1.3.6.1.4.1.311.1.7.3.1.14.0
        }
```

Para comprobar si el plugin funciona, se puede utilizar la aplicación apache benchmarking tanto para apache como IIS. Esta aplicación permite lanzar peticiones concurrentes a un servidor http. En el siguiente ejemplo se lanzan 8000 en total en grupos de 600 concurrentes en el servidor IIS 172.25.80.132:

```
alumno@nagios:~$ ab -n 8000 -c 600 http://172.25.80.132/
This is ApacheBench, Version 2.3 <$Revision: 655654 $>
Copyright 1996 Adam Twiss, Zeus Technology Ltd, http://www.zeustech.net/
Licensed to The Apache Software Foundation, http://www.apache.org/


Benchmarking 172.25.80.132 (be patient)
Completed 800 requests
Completed 1600 requests
Completed 2400 requests
Completed 3200 requests
```

```
Completed 4000 requests
Completed 4800 requests
Completed 5600 requests
Completed 6400 requests
Completed 7200 requests
Completed 8000 requests
Finished 8000 requests


Server Software:        Microsoft-IIS/7.5
Server Hostname:        172.25.80.132
Server Port:            80

Document Path:          /
Document Length:        689 bytes

Concurrency Level:      600
Time taken for tests:   2.572 seconds
Complete requests:      8000
Failed requests:        0
Write errors:           0
Total transferred:      7456000 bytes
HTML transferred:       5512000 bytes
Requests per second:    3110.38 [#/sec] (mean)
Time per request:       192.902 [ms] (mean)
Time per request:       0.322 [ms] (mean, across all concurrent requests)
Transfer rate:          2830.93 [Kbytes/sec] received

Connection Times (ms)
              min  mean[+/-sd] median   max
Connect:        0    1   2.4      1      16
Processing:     6  148  22.7    150     200
Waiting:        6  148  22.7    149     200
Total:         22  150  20.9    151     201

Percentage of the requests served within a certain time (ms)
  50%    151
  66%    157
  75%    159
  80%    160
  90%    165
  95%    180
  98%    189
  99%    190
 100%    201 (longest request)
alumno@nagios:~$
```

La siguiente figura muestra el servidor IIS monitorizado en Nagios:

monitorwindows	Explorer	OK	03-08-2012 14:52:54	0d 0h 31m 56s	1/3	explorer.exe: Running
	HTTP conexiones actuales	OK	03-08-2012 14:54:15	0d 0h 2m 50s	1/3	SNMP OK - 600
	HTTP counters files sent SNMP	OK	03-08-2012 14:52:47	0d 0h 38m 2s	1/3	SNMP OK - 464395
	HTTP num max conexiones simultaneas	OK	03-08-2012 14:53:34	0d 0h 3m 55s	1/3	SNMP OK - 603
	HTTP usuarios actuales	OK	03-08-2012 14:54:27	0d 0h 29m 38s	1/3	SNMP OK - 1
	IIS - W3SVC	OK	03-08-2012 14:48:21	0d 0h 36m 29s	1/3	W3SVC: Started
	IIS via SNMP	WARNING	03-08-2012 14:47:19	0d 0h 17m 31s	3/3	15 process matching svchost (> 3) (<= 100):OK, Mem : 29.1Mb > 20 WARNING, Cpu : 1% OK
	NSClient++ Version	OK	03-08-2012 14:48:17	0d 0h 36m 33s	1/3	NSClient++ 0,4,0,172 2012-05-08
	Unidad C	OK	03-08-2012 14:49:15	0d 0h 45m 35s	1/3	C: Label:UnidadC Serial Number fca858e2: 45%used(11108MB/24474MB) (<80%) : OK
	Uptime	OK	03-08-2012 14:51:23	0d 0h 43m 27s	1/3	SNMP OK - Timeticks: (26466487) 3 days, 1:31:04.87
	Windows Load	OK	03-08-2012 14:52:08	0d 0h 2m 42s	1/3	1 CPU, load 0.0% < 4% : OK

Fig. 93: Servidor Microsoft Internet Information Server monitorizado con Nagios.

9.6. Apache

El comando incluido en el fichero commands.cfg permite comprobar el funcionamiento del servidor http:

```
# 'check_http' command definition
define command{
        command_name    check_http
        command_line    $USER1$/check_http -I $HOSTADDRESS$ $ARG1$
        }
```

monitorlinux	/	OK	03-08-2012 14:33:40	3d 19h 38m 51s	1/3	/: 44%used(4036MB/9070MB) (<80%) : OK
	Apache Processes	OK	03-08-2012 14:38:09	3d 19h 24m 22s	1/3	7 process matching apache2 (> 3) (<= 100):OK, Mem : 7.5Mb OK, Cpu : 0% OK
	HTTP	OK	03-08-2012 14:42:07	3d 19h 35m 24s	1/4	HTTP OK: HTTP/1.1 200 OK - 453 bytes en 0,002 segundo tiempo de respuesta
	Linux Load	OK	03-08-2012 14:38:05	3d 19h 34m 26s	1/3	Load : 0.00 0.01 0.05 : OK
	PING	OK	03-08-2012 14:40:03	3d 19h 38m 28s	1/4	ECO OK - Paquetes perdidos = 0%, RTA = 0.50 ms
	SSH	OK	03-08-2012 14:42:11	3d 19h 35m 20s	1/4	SSH OK - OpenSSH_5.8p1 Debian-1ubuntu3 (protocolo 2.0)
	Swap	OK	03-08-2012 14:38:09	3d 19h 34m 22s	1/3	Swap space: 1%used(6MB/1022MB) (<80%) : OK
	Uptime	OK	03-08-2012 14:42:15	3d 19h 30m 16s	1/3	SNMP OK - Timeticks: (34663151) 4 days, 0:17:11.51

Fig. 94: Resultado de la comprobación de un servidor Apache.

El fichero de configuración de la máquina a monitorizar deberá contener la línea:

```
define service{
        use                             local-service         ; Name of service template to use
        host_name                       monitorlinux
        service_description             HTTP
        check_command                   check_http
        notifications_enabled           0
        }
```

Además de este servicio, se puede monitorizar el número de procesos de apache, y así controlar el estado de las peticiones que Apache está sirviendo.

```
define service{
        use                     generic-service
        host_name               monitorlinux
        service_description     Apache Processes
        check_command           check_snmp_process!public!apache2!3,100!0!-2 -m 20,30 -u 90,99
}
```

Para comprobar si el plugin funciona, se puede utilizar la aplicación apache benchmarking tanto para apache como IIS. Esta aplicación permite lanzar peticiones concurrentes a un servidor http. En el siguiente ejemplo se lanzan 8000 en total en grupos de 600 concurrentes en el servidor apache 172.25.80.134:

```
alumno@nagios:~$ ab -n 6000 -c 800 http://172.25.80.134/
This is ApacheBench, Version 2.3 <$Revision: 655654 $>
Copyright 1996 Adam Twiss, Zeus Technology Ltd, http://www.zeustech.net/
Licensed to The Apache Software Foundation, http://www.apache.org/

Benchmarking 172.25.80.134 (be patient)
Completed 600 requests
Completed 1200 requests
Completed 1800 requests
Completed 2400 requests
Completed 3000 requests
Completed 3600 requests
Completed 4200 requests
Completed 4800 requests
Completed 5400 requests
Completed 6000 requests
Finished 6000 requests


Server Software:        Apache/2.2.17
Server Hostname:        172.25.80.134
Server Port:            80

Document Path:          /
Document Length:        177 bytes

Concurrency Level:      800
Time taken for tests:   4.988 seconds
Complete requests:      6000
Failed requests:        0
Write errors:           0
Total transferred:      2718000 bytes
HTML transferred:       1062000 bytes
Requests per second:    1202.97 [#/sec] (mean)
Time per request:       665.023 [ms] (mean)
Time per request:       0.831 [ms] (mean, across all concurrent requests)
Transfer rate:          532.17 [Kbytes/sec] received

Connection Times (ms)
              min  mean[+/-sd] median   max
Connect:        0    3   5.0      2      30
Processing:     2   77 313.5     18    4956
```

```
Waiting:        2   76 313.6     17    4955
Total:          9   80 316.5     20    4974

Percentage of the requests served within a certain time (ms)
  50%     20
  66%     22
  75%     24
  80%     26
  90%     31
  95%    233
  98%   1516
  99%   1523
 100%   4974 (longest request)
alumno@nagios:~$
```

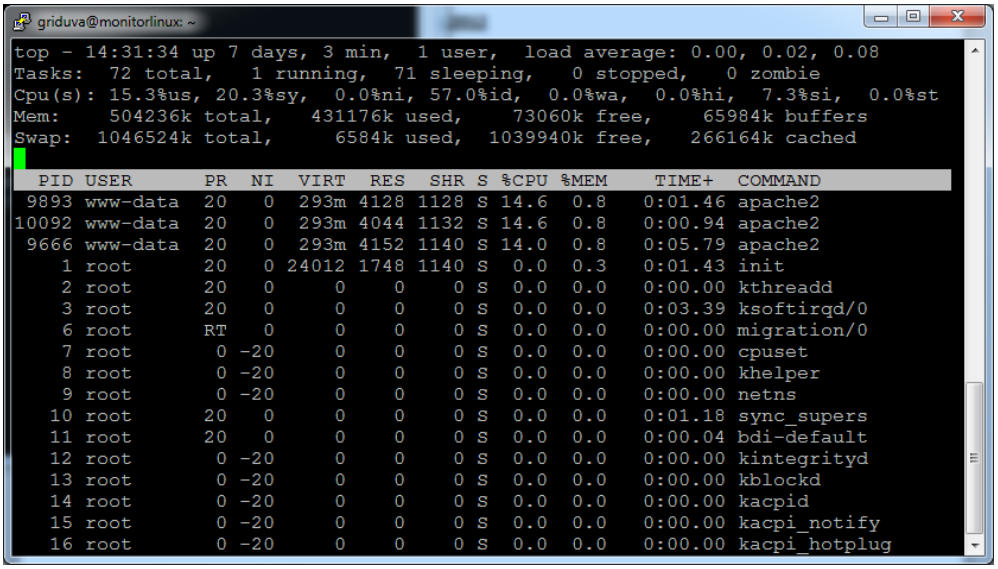


Fig. 95: Procesos apache2 lanzados con la aplicación apache benchmarking.

En la página web de Nagios Exchange se pueden descargar multitud de plugins de Apache para Nagios[25].

9.7. Cisco Call Manager

Al igual que otros dispositivos y servicios, es posible gestionar los servicios de telefonía IP de Cisco. Además de las variables SNMP que se pueden consultar como otra máquina cualquiera, Cisco pone a disposición una serie de MIBs para acceder a objetos propios con información sobre los servicios de telefonía IP.

Las MIBS son: CISCO-CCM-MIB.my, CISCO-CDP-MIB.my y SYS-APPL-MIB.my. Se pueden consultar y descargar en la web de Cisco[26] y en la web oidview.com seleccionando como fabricante Cisco (9)[27].

Algunos OIDs interesantes para consultar en Nagios son:

Tabla VIII: Resumen de objetos y OIDs gestionables para Cisco Call Manager.

[25] http://exchange.nagios.org/index.php?option=com_mtree&task=search&Itemid=74&searchword=apache2

[26] ftp://ftp.cisco.com/pub/mibs/supportlists/callmanager/callmanager-supportlist.html

[27] http://www.oidview.com/mibs/9/md-9-1.html

OBJETO	OID
"ccmPhoneInfo"	"1.3.6.1.4.1.9.9.156.1.2"
"ccmGatewayInfo"	"1.3.6.1.4.1.9.9.156.1.3"
"ccmPhoneTable"	"1.3.6.1.4.1.9.9.156.1.2.1"
"ccmPhoneExtensionTable"	"1.3.6.1.4.1.9.9.156.1.2.2"
"ccmPhoneFailedTable"	"1.3.6.1.4.1.9.9.156.1.2.3"
"ccmPhoneStatusUpdateTable"	"1.3.6.1.4.1.9.9.156.1.2.4"
"ccmPhoneExtnTable"	"1.3.6.1.4.1.9.9.156.1.2.5"
"ccmPhoneEntry"	"1.3.6.1.4.1.9.9.156.1.2.1.1"
"ccmPhoneIndex"	"1.3.6.1.4.1.9.9.156.1.2.1.1.1"
"ccmPhonePhysicalAddress"	"1.3.6.1.4.1.9.9.156.1.2.1.1.2"
"ccmPhoneType"	"1.3.6.1.4.1.9.9.156.1.2.1.1.3"
"ccmPhoneDescription"	"1.3.6.1.4.1.9.9.156.1.2.1.1.4"
"ccmPhoneUserName"	"1.3.6.1.4.1.9.9.156.1.2.1.1.5"
"ccmPhoneIpAddress"	"1.3.6.1.4.1.9.9.156.1.2.1.1.6"
"ccmPhoneStatus"	"1.3.6.1.4.1.9.9.156.1.2.1.1.7"
"ccmPhoneFailedRegFailReason"	"1.3.6.1.4.1.9.9.156.1.2.3.1.12"
"ccmPhoneStatusUpdateEntry"	"1.3.6.1.4.1.9.9.156.1.2.4.1"
"ccmPhoneStatusUpdateIndex"	"1.3.6.1.4.1.9.9.156.1.2.4.1.1"
"ccmPhoneStatusPhoneIndex"	"1.3.6.1.4.1.9.9.156.1.2.4.1.2"
"ccmPhoneStatusUpdateTime"	"1.3.6.1.4.1.9.9.156.1.2.4.1.3"
"ccmPhoneStatusUpdateType"	"1.3.6.1.4.1.9.9.156.1.2.4.1.4"
"ccmPhoneStatusUpdateReason"	"1.3.6.1.4.1.9.9.156.1.2.4.1.5"
"ccmPhoneStatusUnregReason"	"1.3.6.1.4.1.9.9.156.1.2.4.1.6"
"ccmPhoneStatusRegFailReason"	"1.3.6.1.4.1.9.9.156.1.2.4.1.7"
"ccmActivePhones"	"1.3.6.1.4.1.9.9.156.1.5.1"
"ccmInActivePhones"	"1.3.6.1.4.1.9.9.156.1.5.2"
"ccmActiveGateways"	"1.3.6.1.4.1.9.9.156.1.5.3"
"ccmInActiveGateways"	"1.3.6.1.4.1.9.9.156.1.5.4"
"ccmRegisteredPhones"	"1.3.6.1.4.1.9.9.156.1.5.5"

Para más detalle se puede consultar el árbol de OIDs disponible en la MIB CISCO-CDP-MIB.my en el anexo VII y en los enlaces de Cisco y oidview.com.

9.7.1. Configuración previa del Call Manager

Antes de utilizar las herramientas para consultar los servicios de telefonía IP con SNMP, hay que asegurarse de que los servidores estén correctamente instalados.

El primer paso es verificar en los servicios de Windows, si el servicio de agente SNMP está arrancado, y verificar (haciendo doble clic) la configuración del agente. Se debe verificar que la comunidad y permisos para la comunidad están configurados correctamente.

En la ventana de servicios en el menú de herramientas administrativas, se pueden ver los servicios relacionados con la telefonía IP que están corriendo:

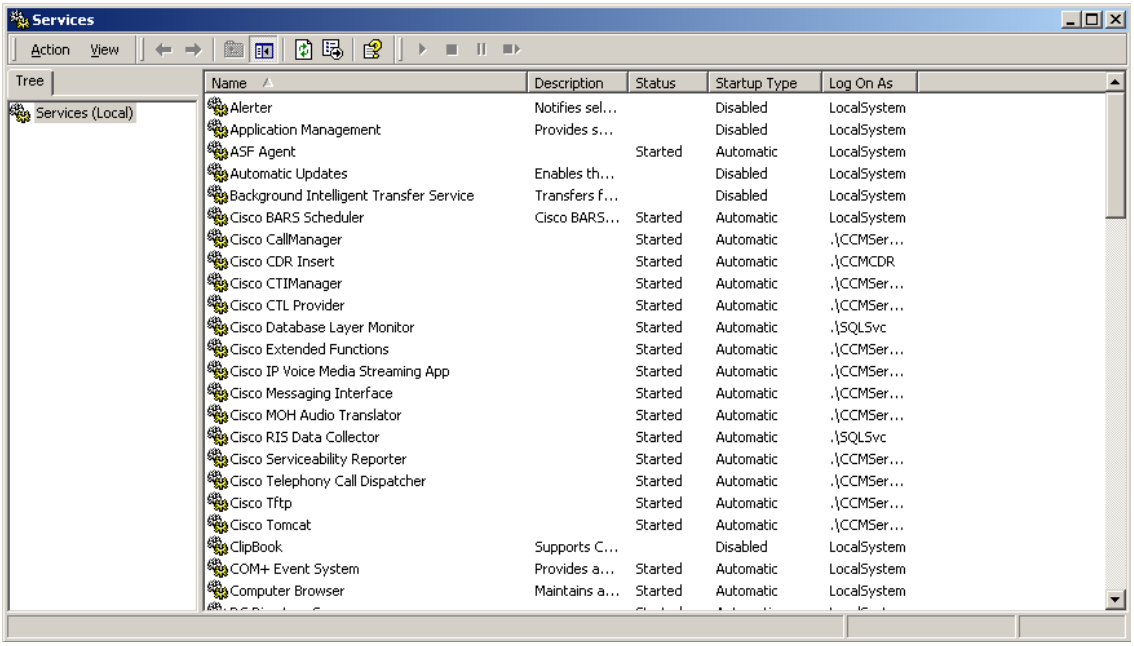


Fig. 96: Servicios de telefonía IP de Cisco.

Además de la telefonía, es necesario configurar el servicio SNMP. Para ello localizar el servicio SNMP Service:

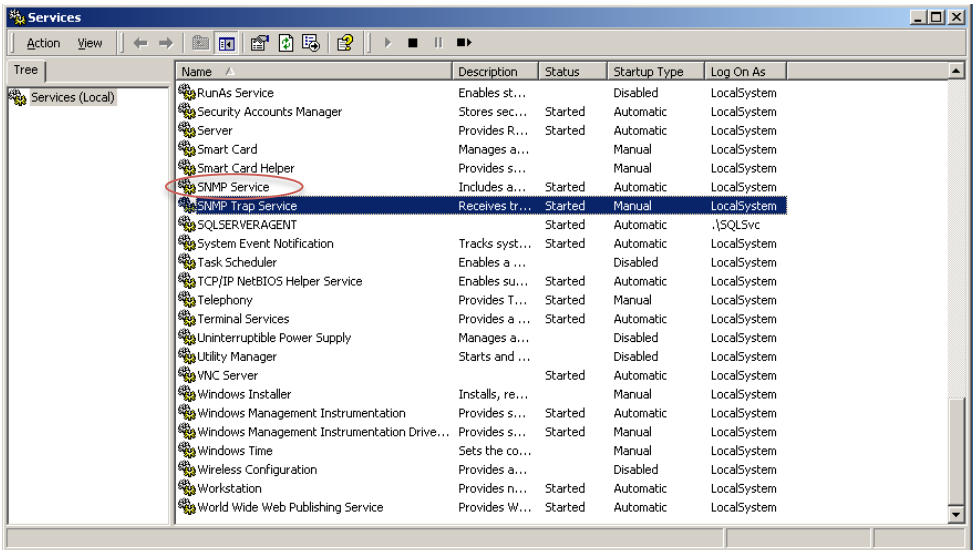


Fig. 97: Servicios SNMP del Cisco Call Manager.

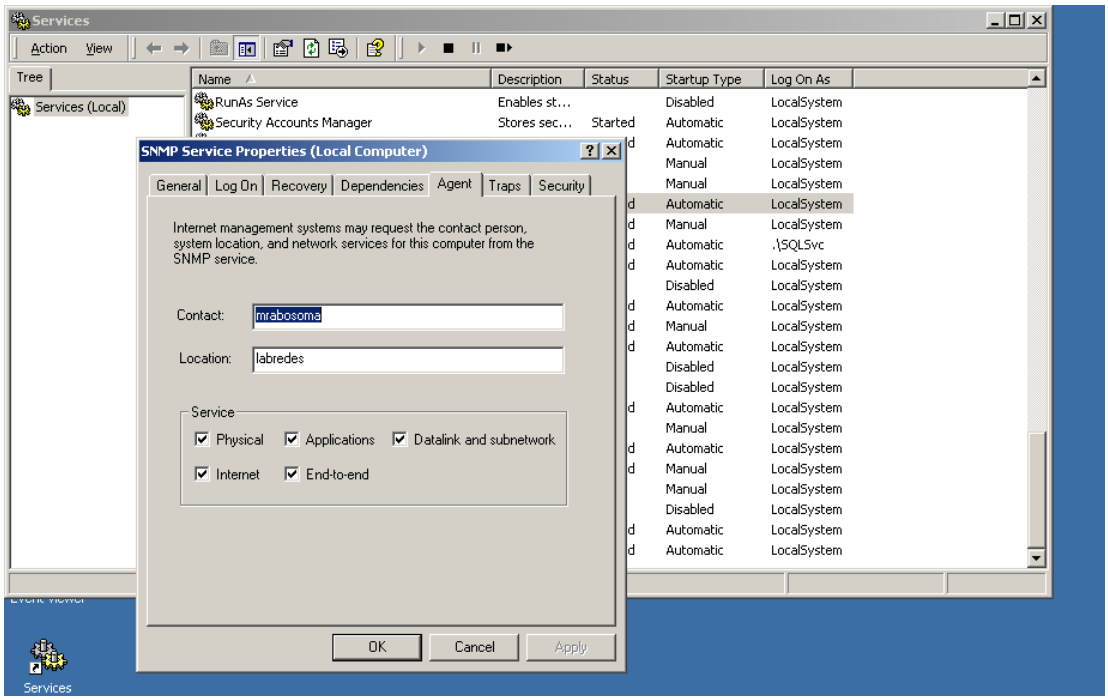


Fig. 98: Configuración del contacto y localización en SNMP.

Configurar la comunidad y los permisos para esa comunidad. Se pueden añadir varias con distintos perfiles cada una. Configurar también las estaciones que pueden acceder a este servicio para consultar objetos a través de SNMP:

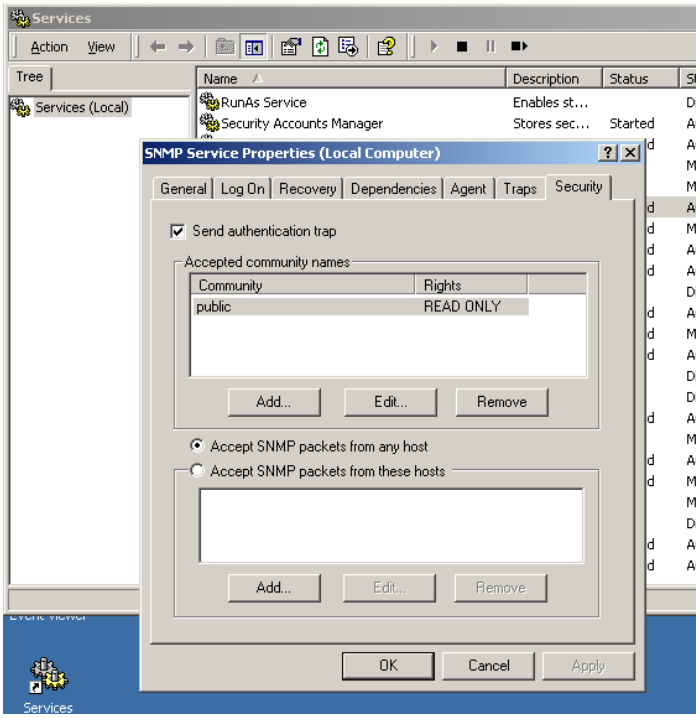


Fig. 99: Configuración de comunidad y permisos en el Call Manager.

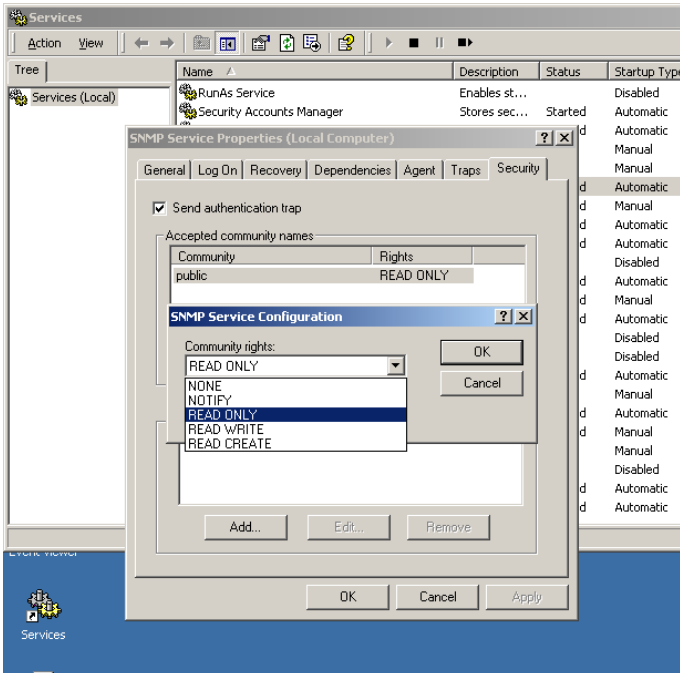


Fig. 100: Detalle de permisos en la configuración de las comunidades.

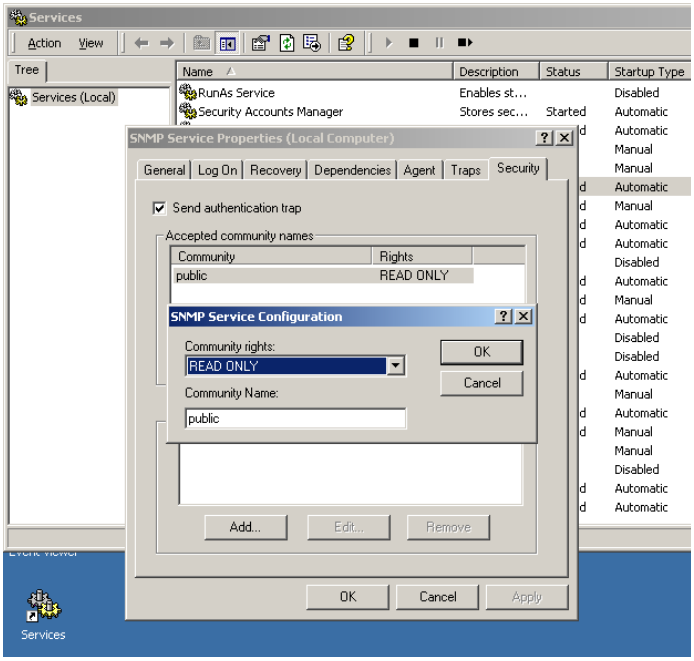


Fig. 101: Asignación permiso READ-ONLY en comunidad public del Call Manager.

Si se desean recibir traps, por ejemplo en el que caso de que un Gateway de voz no se encuentre accesible, se deben configurar en la pestaña correspondiente.

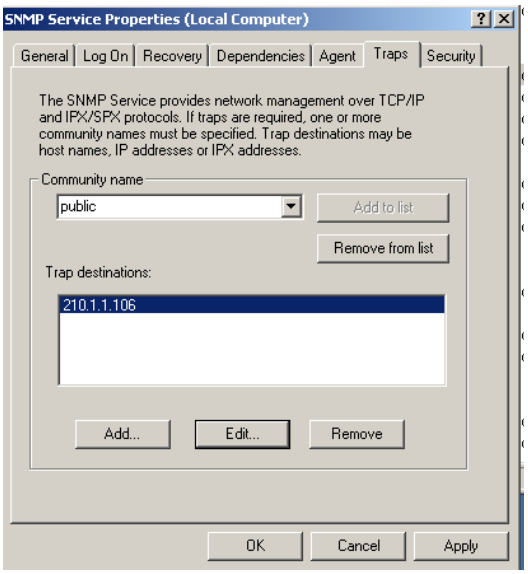


Fig. 102: Comunidad y estación gestora de traps en Cisco Call Manager.

Una vez configurado SNMP, hay que revisar el estado de los servidores en el Call Manager. Se puede consultar la ayuda proporcionada por el servidor. Es interesante revisar el checklist para estar seguros de que se configura correctamente:

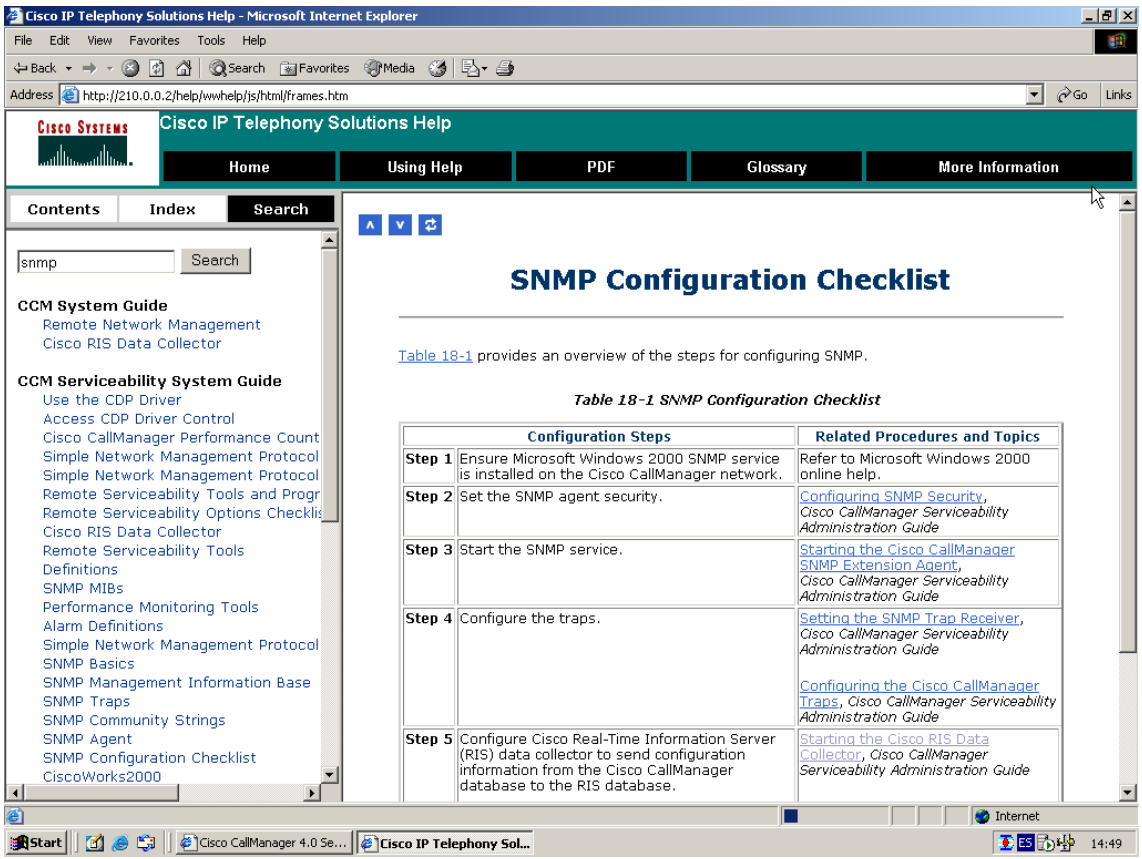


Fig. 103: Páginas de ayuda de los servicios asociados a SNMP.

En el grupo de programas Cisco Call Manager, arrancar Cisco Service Configuration:

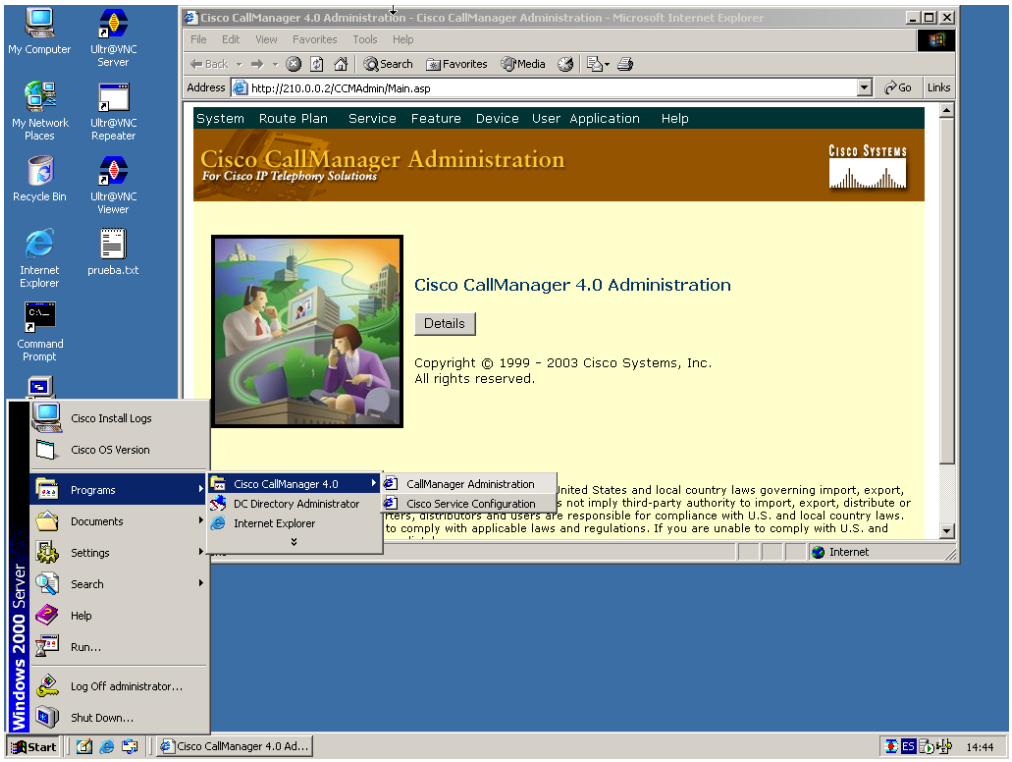


Fig. 104: Grupo de programas Cisco CallManager.

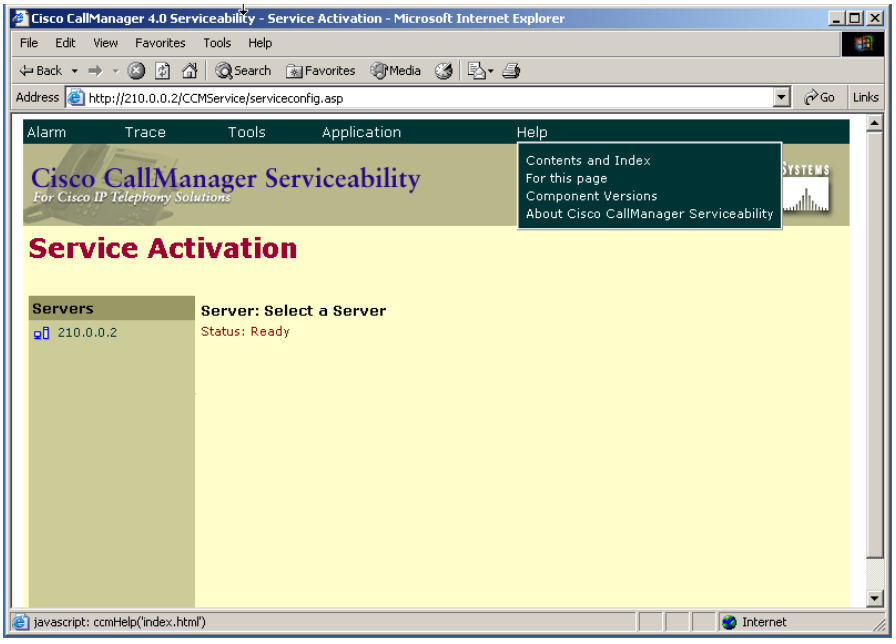


Fig. 105: Ventana del Cisco Service Configuration.

Seleccionar el servidor y comprobar que están activados los servicios, en concreto el Cisco RIS Data Colector que es el encargado de enviar la información de configuración cuando se interrogue al Call Manager:

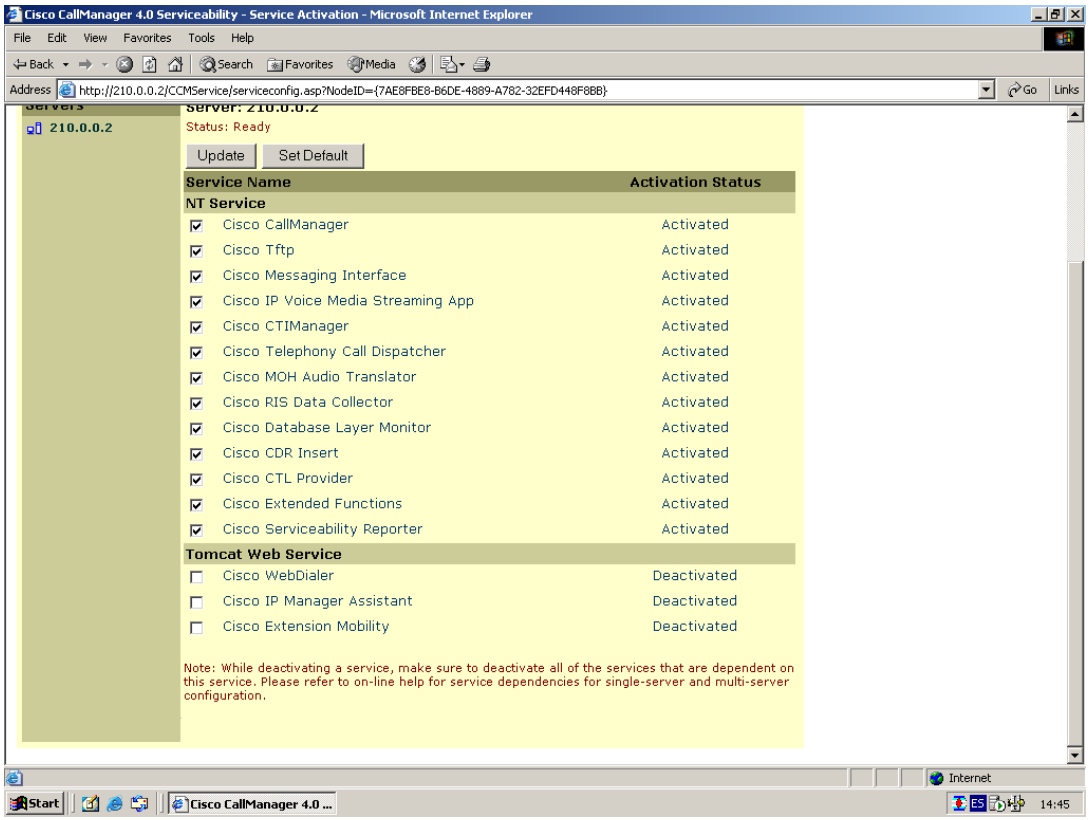


Fig. 106: Ventana de activación de servicios del Call Manager.

En el menú Trace Configuration, se desplegarán los servicios a configurar:

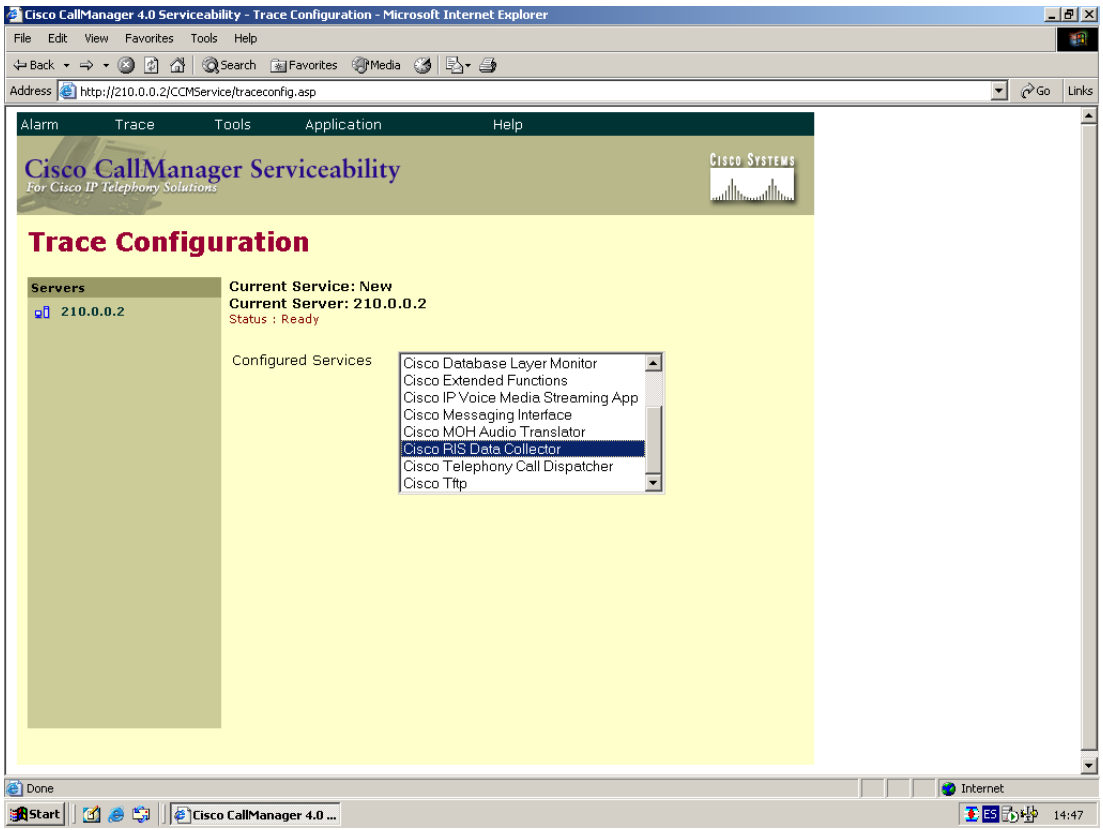


Fig. 107: Menú Trace Configuration.

Comprobar que están activados los servicios de SNMP:

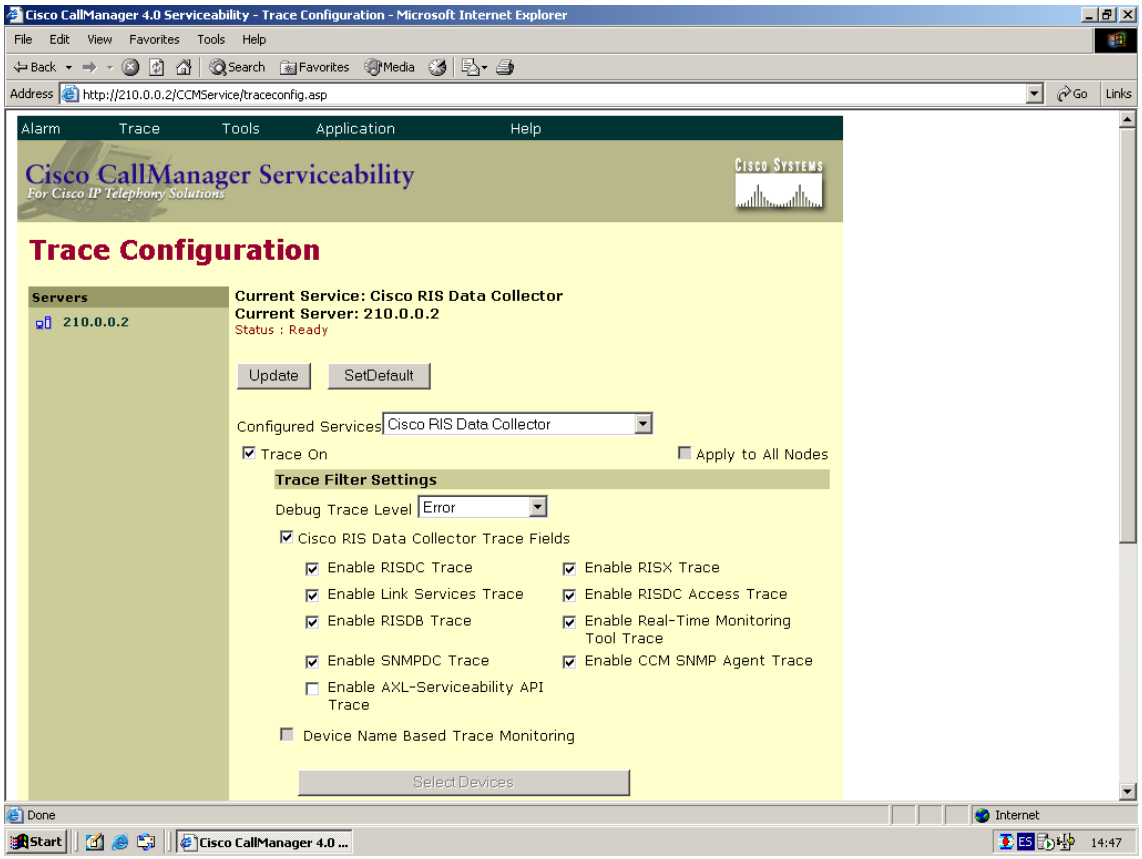


Fig. 108: Ventana de configuración de Cisco RIS Data Collector.

9.7.2. Consulta de objetos del árbol de OIDs de la MIB CISCO-CCM-MIB

Una vez activados y configurados los servicios, es posible realizar consultas utilizando SNMP. A continuación se muestran los resultados de consultar las OIDs:

Tabla IX: Tabla de OIDs en un Call Manager

OBJETO	OID
"ccmName"	"1.3.6.1.4.1.9.9.156.1.1.2.1.2.1"
"ccmVersion"	"1.3.6.1.4.1.9.9.156.1.1.2.1.4.1"
"ccmStstus"	"1.3.6.1.4.1.9.9.156.1.1.2.1.5.1"
"ccmPhoneType"	"1.3.6.1.4.1.9.9.156.1.2.1.1.3.1"
"ccmPhoneDescription"	"1.3.6.1.4.1.9.9.156.1.2.1.1.4.1"
"ccmPhoneDescription"	"1.3.6.1.4.1.9.9.156.1.2.1.1.4.2"
"ccmActivePhones"	"1.3.6.1.4.1.9.9.156.1.5.1.0"
"ccmInActivePhones"	"1.3.6.1.4.1.9.9.156.1.5.2.0"
"ccmActiveGateways"	"1.3.6.1.4.1.9.9.156.1.5.3.0"
"ccmInActiveGateways"	"1.3.6.1.4.1.9.9.156.1.5.4.0"
"ccmRegisteredPhones"	"1.3.6.1.4.1.9.9.156.1.5.5.0"
"ccmUnregisteredPhones"	"1.3.6.1.4.1.9.9.156.1.5.6.0"
"ccmRegisteredGateways"	"1.3.6.1.4.1.9.9.156.1.5.8.0"
"ccmUnregisteredGateways"	"1.3.6.1.4.1.9.9.156.1.5.9.0"
"ccmRegisteredMediaevices"	"1.3.6.1.4.1.9.9.156.1.5.11.0"
"ccmSystemVersion"	"1.3.6.1.4.1.9.9.156.1.5.29.0"

Una vez seleccionados los OIDs, se ejecuta el comando:

```
snmpget -c public -v1 210.0.0.2 OID
```

El resultado es el siguiente:

```
SNMPv2-SMI::enterprises.9.9.156.1.1.2.1.2.1 = STRING: "210.0.0.2"
SNMPv2-SMI::enterprises.9.9.156.1.1.2.1.4.1 = STRING: "4.0(0.0)"
SNMPv2-SMI::enterprises.9.9.156.1.1.2.1.5.1 = INTEGER: 2
SNMPv2-SMI::enterprises.9.9.156.1.2.1.1.3.1 = INTEGER: 9
SNMPv2-SMI::enterprises.9.9.156.1.2.1.1.4.1 = STRING: "IPT-Red2"
SNMPv2-SMI::enterprises.9.9.156.1.2.1.1.4.2 = STRING: "IPT-Red1"
SNMPv2-SMI::enterprises.9.9.156.1.5.1.0 = Counter32: 2
SNMPv2-SMI::enterprises.9.9.156.1.5.2.0 = Counter32: 0
SNMPv2-SMI::enterprises.9.9.156.1.5.3.0 = Counter32: 8
SNMPv2-SMI::enterprises.9.9.156.1.5.4.0 = Counter32: 0
SNMPv2-SMI::enterprises.9.9.156.1.5.5.0 = Counter32: 2
SNMPv2-SMI::enterprises.9.9.156.1.5.6.0 = Counter32: 0
SNMPv2-SMI::enterprises.9.9.156.1.5.8.0 = Counter32: 8
SNMPv2-SMI::enterprises.9.9.156.1.5.9.0 = Counter32: 0
SNMPv2-SMI::enterprises.9.9.156.1.5.11.0 = Counter32: 4
SNMPv2-SMI::enterprises.9.9.156.1.5.29.0 = STRING: "4.0(1)"
```

La siguiente figura muestra los parámetros monitorizados de un Call Manager en Nagios:

CM Nombre	OK	06-08-2012 13:28:03	3d 1h 11m 31s	1/3	SNMP OK - "210.0.0.2"
CM Status	OK	06-08-2012 13:28:52	3d 1h 10m 42s	1/3	SNMP OK - 2
CM System version	OK	06-08-2012 13:19:42	3d 1h 9m 52s	1/3	SNMP OK - "4.0(1)"
CM Version	OK	06-08-2012 13:20:31	3d 1h 9m 3s	1/3	SNMP OK - "4.0(0.0)"
GW Activos	OK	06-08-2012 13:21:21	3d 1h 8m 13s	1/3	SNMP OK - 8
GW Registrados	OK	06-08-2012 13:22:11	3d 1h 7m 23s	1/3	SNMP OK - 8
HTTP counters files sent SNMP	OK	06-08-2012 13:28:55	0d 0h 0m 39s	1/3	SNMP OK - 0
IIS via SNMP	WARNING	06-08-2012 13:28:40	3d 23h 30m 54s	3/3	3 process matching svchost (<= 3 : WARNING) (<= 100):OK, Mem : 6.1Mb OK, Cpu : 0% OK
Media Devices	OK	06-08-2012 13:23:00	3d 1h 6m 34s	1/3	SNMP OK - 4
SQL Server	CRITICAL	06-08-2012 13:23:23	3d 23h 46m 11s	3/3	1 process matching sqlservr (<= 3 : WARNING) (<= 100):OK, Mem : 75.3Mb > 30 CRITICAL, Cpu : 0% OK
Telefono[1]	OK	06-08-2012 13:23:50	3d 1h 5m 44s	1/3	SNMP OK - 9
Telefono[2]	OK	06-08-2012 13:24:39	3d 1h 4m 55s	1/3	SNMP OK - 9
Telf Activos	OK	06-08-2012 13:25:29	3d 1h 4m 5s	1/3	SNMP OK - 2
Telf Inactivos	OK	06-08-2012 13:28:08	3d 1h 12m 14s	1/3	SNMP OK - 0
Telf Registrados	OK	06-08-2012 13:28:10	3d 1h 11m 24s	1/3	SNMP OK - 2
Tomcat	CRITICAL	06-08-2012 13:23:20	3d 23h 46m 14s	3/3	1 process matching tomcat (<= 3 : WARNING) (<= 100):OK, Mem : 37.1Mb > 30 CRITICAL, Cpu : 0% OK
Unidad C	OK	06-08-2012 13:29:29	3d 23h 20m 5s	1/3	C: Label:W2K Serial Number 28f5373e: 12%used(9190MB/74308MB) (<80%) : OK
Unidad D	OK	06-08-2012 13:22:31	3d 23h 37m 3s	1/3	D: Label:STI_DATA Serial Number 185014d2: 0%used(0MB/2000MB) (<80%) : OK
Uptime	OK	06-08-2012 13:28:30	3d 23h 31m 4s	1/3	SNMP OK - Timeticks: (34271921) 3 days, 23:11:59.21
Windows Load	OK	06-08-2012 13:21:27	2d 12h 18m 7s	1/3	1 CPU, load 2.0% < 4% : OK

Fig. 109: Monitorización con Nagios de un Cisco Call Manager.

También se muestra el estado de los servicios asociados: SQL Server, Tomcat e IIS.

10. CASOS PRÁCTICOS DE GESTIÓN DE SISTEMAS

10.1. Monitorización de dispositivos de red (switches)

La gestión de equipos de red como switches, routers, Access Point, etc., se suele desplegar configurando los servicios del protocolo SNMP. Hay que tener en cuenta que no todos los equipos implementan este protocolo de comunicaciones, por lo que se deberán consultar las especificaciones del manual del equipo.

Los equipos Cisco y HP Procurve de los que dispone el SACYL implementan dicho servicio, por lo que se pueden gestionar de forma remota vía SNMP y cualquier aplicación que utilice dicho protocolo, en particular Nagios.

Antes de configurar Nagios se deberá consultar la configuración del equipo, en particular su dirección ip de gestión, comunidad(es) y versión del protocolo SNMP.

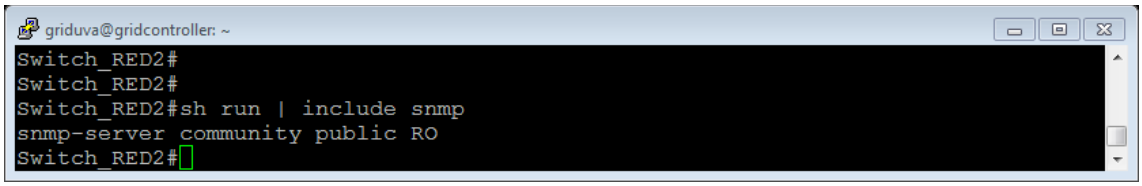


Fig. 110: Comprobación de la comunidad SNMP en un switch Cisco Catalyst.

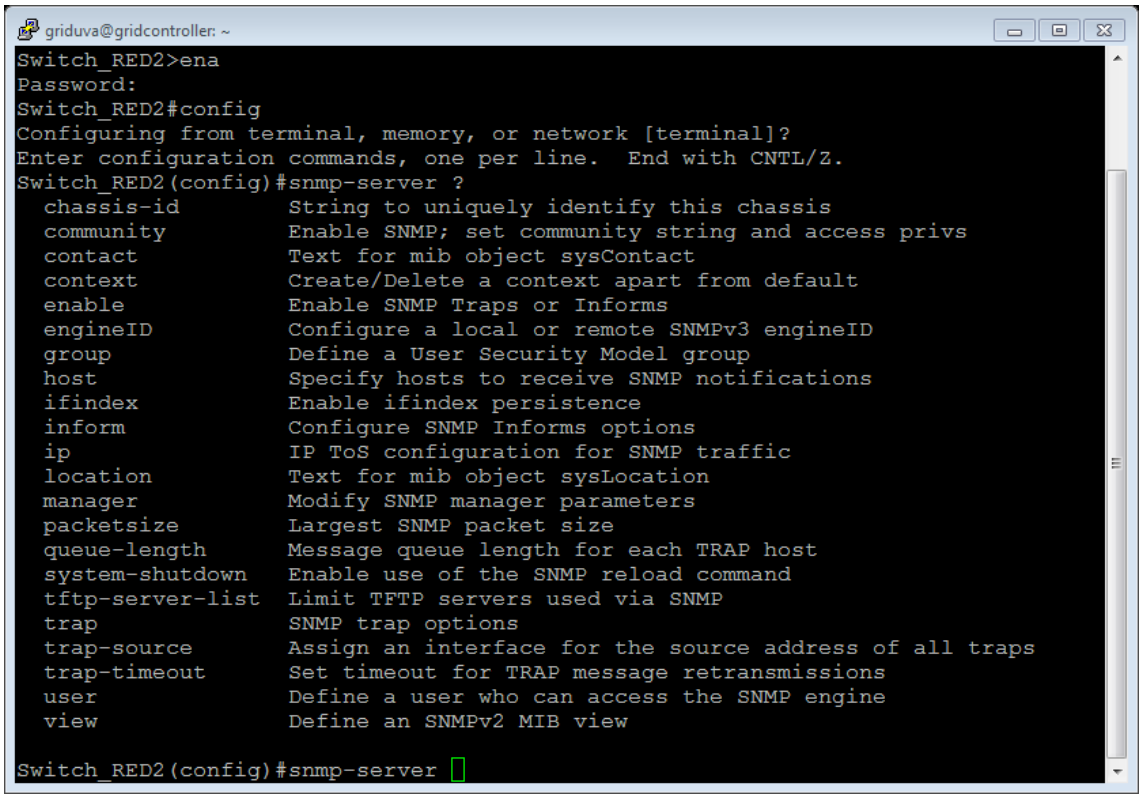


Fig. 111: Configuración parámetros SNMP en un switch Cisco Catalyst.

La configuración de Nagios se realiza a través de los ficheros de configuración antes descritos, que se localizan bajo el directorio /etc/nagios/objects.

Hay que tener en cuenta que los equipos son capaces de manejar cientos de variables (objetos) SNMP, por lo que se deberá buscar previamente el oid que interesa gestionar. Para ello, una vez instalado SNMP en el servidor Nagios, es de gran ayuda utilizar los comandos snmpwalk y snmpget para consultar oids y filtrar por las cadenas de interés. Las siguientes figuras muestran ejemplos de consulta utilizando estos comandos.

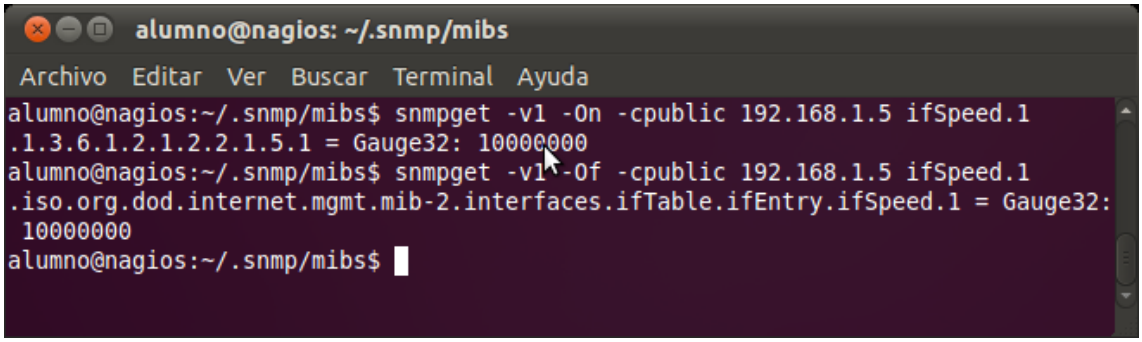


Fig. 112: Ejemplo de utilización primitiva *snmpget*.

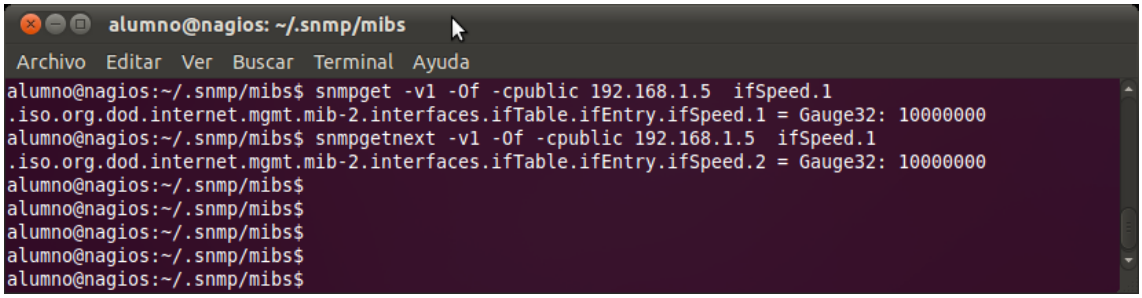


Fig. 113: Ejemplo de utilización primitiva *snmpgetnext*.

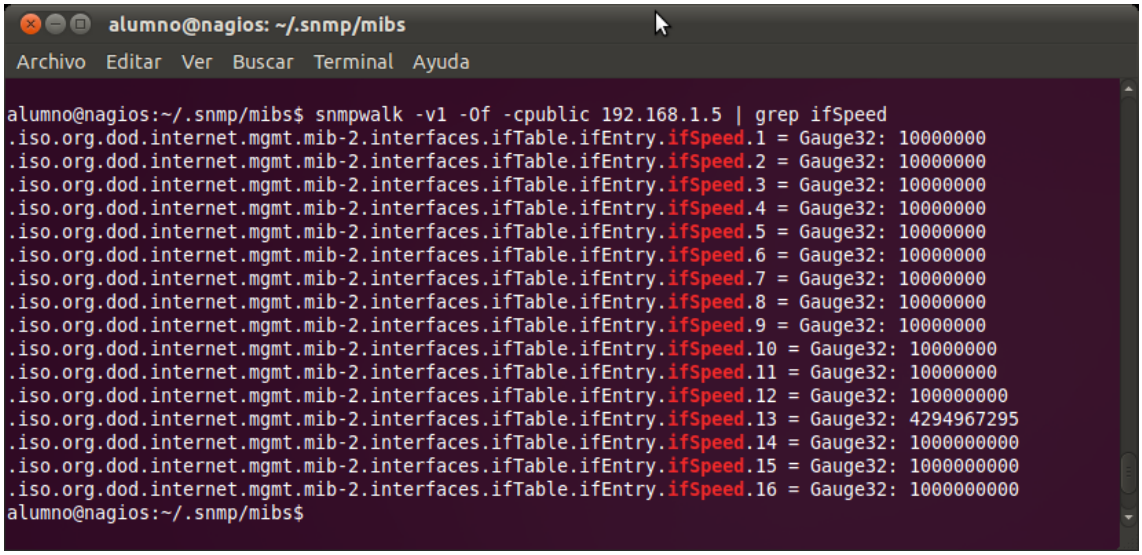


Fig. 114: Uso *snmpwalk* con filtro para consultar la velocidad de las interfaces.

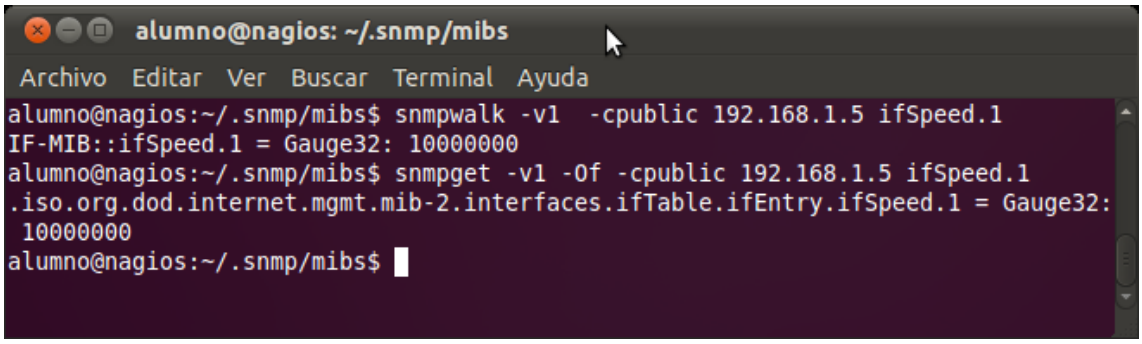


Fig. 115: Ejemplo de utilización primitiva *snmpwalk* con detalle del *oid*.

El árbol completo de *oids* dependerá del fabricante, por lo que se aconseja acudir a la sección correspondiente de su página web[28].

10.1.1. Switches HP Procurve

Una vez estudiada la MIB del fabricante y seleccionado los oids de interés, hay que crear el fichero *.cfg* con la definición de *host* y *services*. El siguiente extracto de código se puede utilizar como base para el acceso a un switch HP Procurve. Define un host y varios servicios utilizando SNMP. Si se desea consultar, el fichero completo se encuentra en el Anexo I.

```
define host{
    use             generic-switch          ; Inherit default values from a template
    host_name       swchcuv2176             ; The name we're giving to this switch
    alias           swchcuv2176.hcuv.sacyl.es - HP ProCurve 2650      ;     A     longer     name
associated with the switch
    address         10.40.83.184            ; IP address of the switch
    hostgroups      switches_procurve               ; Host groups this switch is associated
with
    notes_url       http://10.40.83.182
    }
# Service definition CPU Usada
# Define a service to check the CPU consuption
# on HP Procurve Switchs.  Warning if <40% free, critical if < 20% free.
# 'check_snmp_load.pl' command definition
define service{
    use                     generic-service         ; Name of service template to use
    hostgroup_name          switches_procurve
    service_description     CPU Usada
    is_volatile             0
    check_period            24x7
    max_check_attempts      3
    normal_check_interval   5
    retry_check_interval    1
#   contact_groups          switch-admins
    notification_interval   240
    notification_period     24x7
    notification_options    c,r
    check_command           check_snmp_load_v1!hp!60:80!80:100
    }

# Service definition - HP Procurve Switch - Memoria libre
define service{
    use                     generic-service         ; Name of service template to use
    hostgroup_name          switches_procurve
    service_description     Memoria Libre
    is_volatile             0
    check_period            24x7
    max_check_attempts      3
    normal_check_interval   5
    retry_check_interval    1
#   contact_groups          switch-admins
    notification_interval   240
    notification_period     24x7
    notification_options    c,r
    check_command           check_hpmemoryfree!2000:30000000!1000:30000000
```

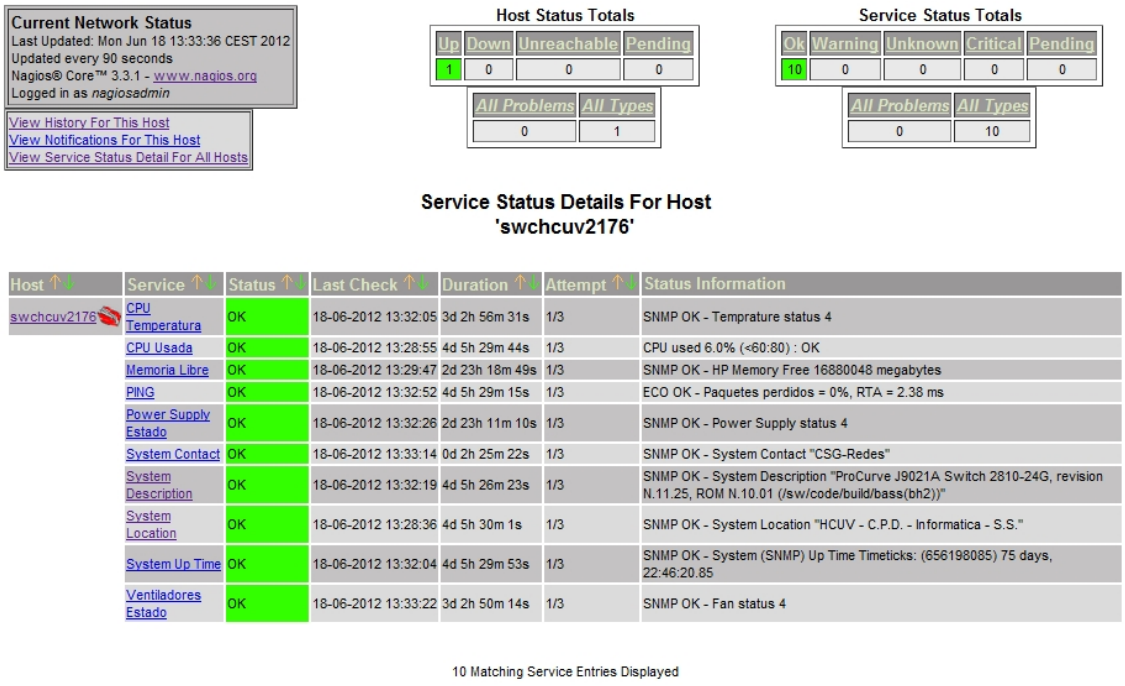
[28] Para Cisco, consultar: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml. Para HP: http://h40060.www4.hp.com/procurve/includes/software/index.php?cc=es&lc=es&content=mibs-oct09

```
}
```

Algunos servicios utilizan el comando check_snmp estándar instalado con Nagios en /usr/local/nagios/libexec, y otros como check_snmp_load (en Perl)[29]. Otros comandos se crean en base a éstos para seleccionar alguna funcionalidad, por ejemplo el comando check_hpmemoryfree:

```
# Monitor HP Procurve Switch Memory free
define command{
  command_name check_hpmemoryfree
  command_line      $USER1$/check_snmp      -H      $HOSTADDRESS$      -C      $USER5$      -o
.1.3.6.1.4.1.11.2.14.11.5.1.1.2.1.1.1.6.1 -t 5 -w $ARG1$ -c $ARG2$ -u megabytes -l 'HP Memory
Free'
 }
```

Las siguientes figuras muestran las vistas de los servicios de Nagios con la configuración del switch. Se muestra un switch funcionando de formal normal, una página de Nagios con un resumen compacto de aquellos hosts y servicios que se consideran críticos y por último la detección de un fallo en el ventilador de un switch.



Current Network Status
Last Updated: Mon Jun 18 13:33:36 CEST 2012
Updated every 90 seconds
Nagios® Core™ 3.3.1 - www.nagios.org
Logged in as *nagiosadmin*

View History For This Host
View Notifications For This Host
View Service Status Detail For All Hosts

Host Status Totals

Up	Down	Unreachable	Pending
1	0	0	0

All Problems	All Types
0	1

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
10	0	0	0	0

All Problems	All Types
0	10

Service Status Details For Host 'swchcuv2176'

Host	Service	Status	Last Check	Duration	Attempt	Status Information
swchcuv2176	CPU Temperatura	OK	18-06-2012 13:32:05	3d 2h 56m 31s	1/3	SNMP OK - Temprature status 4
	CPU Usada	OK	18-06-2012 13:28:55	4d 5h 29m 44s	1/3	CPU used 6.0% (<60:80) : OK
	Memoria Libre	OK	18-06-2012 13:29:47	2d 23h 18m 49s	1/3	SNMP OK - HP Memory Free 16880048 megabytes
	PING	OK	18-06-2012 13:32:52	4d 5h 29m 15s	1/3	ECO OK - Paquetes perdidos = 0%, RTA = 2.38 ms
	Power Supply Estado	OK	18-06-2012 13:32:26	2d 23h 11m 10s	1/3	SNMP OK - Power Supply status 4
	System Contact	OK	18-06-2012 13:33:14	0d 2h 25m 22s	1/3	SNMP OK - System Contact "CSG-Redes"
	System Description	OK	18-06-2012 13:32:19	4d 5h 26m 23s	1/3	SNMP OK - System Description "ProCurve J9021A Switch 2810-24G, revision N.11.25, ROM N.10.01 (/sw/code/build/bass(bh2))"
	System Location	OK	18-06-2012 13:28:36	4d 5h 30m 1s	1/3	SNMP OK - System Location "HCUV - C.P.D. - Informatica - S.S."
	System Up Time	OK	18-06-2012 13:32:04	4d 5h 29m 53s	1/3	SNMP OK - System (SNMP) Up Time Timeticks: (656198085) 75 days, 22:46:20.85
	Ventiladores Estado	OK	18-06-2012 13:33:22	3d 2h 50m 14s	1/3	SNMP OK - Fan status 4

10 Matching Service Entries Displayed

Fig. 116: Servicios gestionados de un switch HP Procurve2176.

[29] Script check_snmp_load.pl de Patrick Proy (Patrick at proy.org) en http://nagios.manubulon.com/

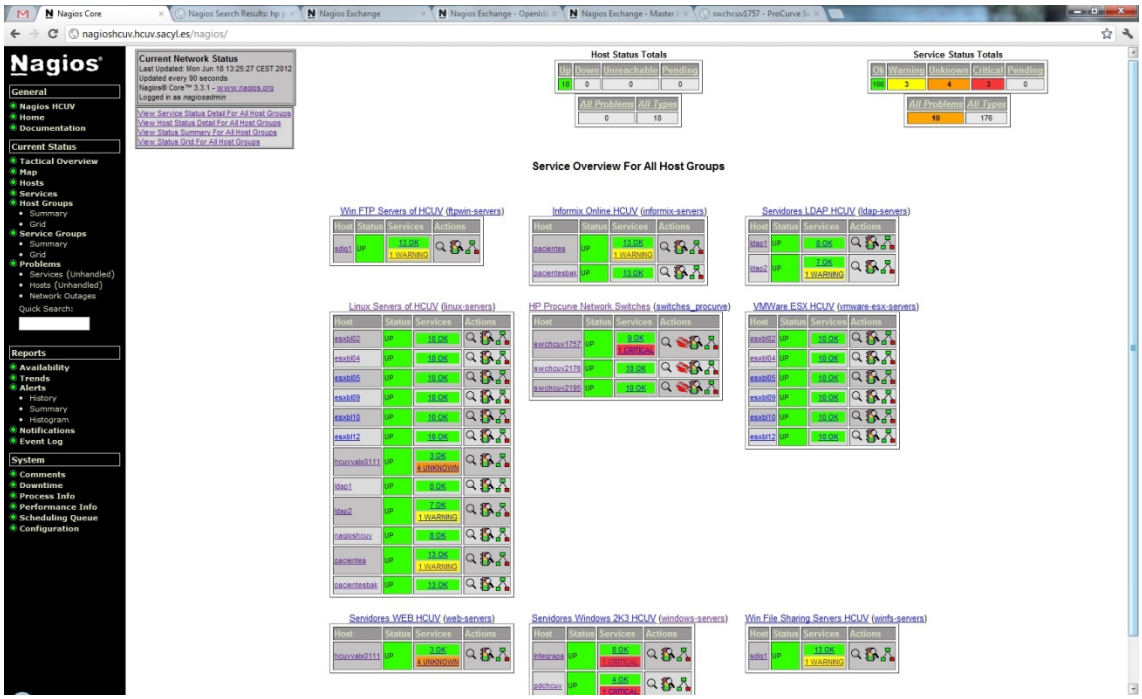


Fig. 117: Ventana de agrupación de servicios más críticos.

Si hubiese algún problema en el switch, como por ejemplo un fallo en un ventilador, debería aparecer un mensaje como el que se muestra en la siguiente figura:

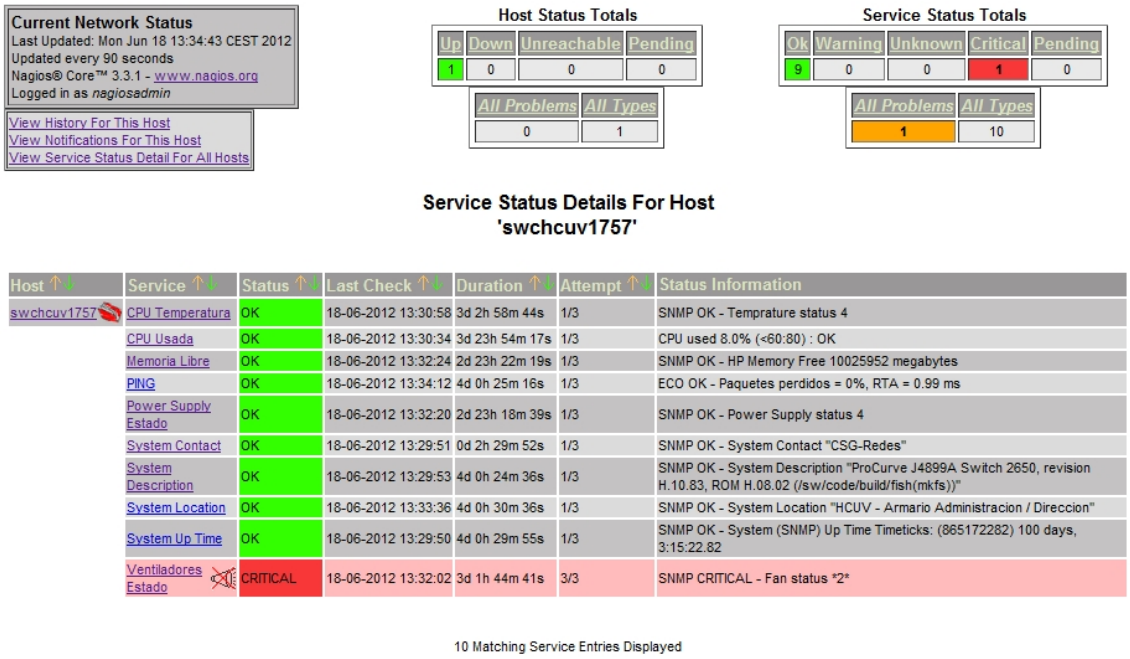


Fig. 118: Alarma en un switch por fallo del ventilador.

10.1.2. Switches Cisco Catalyst

Para los switches de Cisco, se recomienda consultar las MIBS de Cisco en su página web[30].

La utilización de las MIBS y SNMP no plantea ningún problema y es similar a los de HP, por lo que en este documento solamente se describirán algunos plugins interesantes. Antes de probarlos, hay que asegurarse que SNMP está activado y configurado correctamente. Véase el comando snmp-server y la configuración de SNMP en el apartado anterior.

En la web de Nagios Exchange se pueden descargar numerosos plugins interesantes[31], por ejemplo: check_catalyst_load, check_catalyst_flash, check_catalyst_mem, check_catalyst_fans y check_catalyst_temp. Estos scripts están escritos en Perl. Su uso es sencillo y similar para todos (check_catalyst-load –h):

```
Usage: ./check_catalyst_load.pl -s <SWITCH> -C <COMMUNITY-STRING> -w <WARNLEVEL in 5s,1min,5min>
-c <CRITLEVEL in 5s,1min,5min>
```

La salida de la ejecución para los cuatro primeros es la siguiente:

```
OK:  I/O: valid, Used: 3017144B Free: 5371464B (64%)! Processor: valid, Used: 10661848B Free:
36332176B (77%)!|WARING <= 20%, CRITICAL <= 10%
OK:  Onboard system FLASH: Size: 15998976 Free: 6638592 (41%) Status: available VPP: installed!
OK:  CPU0: 0% 2% 1% !
OK:  chassis: normal!
```

Para añadir los comandos, editar el fichero commands.cfg, o añadir uno nuevo:

```
# 'check_snmp_storage' command definition
define command{
        command_name    check_snmp_storage
        command_line    $USER1$/check_snmp_storage.pl -H $HOSTADDRESS$ $ARG1$
        }

# 'check_snmp' command definition
define command{
  command_name check_snmp_process
  command_line $USER1$/check_snmp_process.pl -H $HOSTADDRESS$ -C $ARG1$ -n $ARG2$ -w $ARG3$ -c
$ARG4$ $ARG5$
}

define command{
   command_name check_snmp_load_v1
   command_line $USER1$/check_snmp_load.pl -H $HOSTADDRESS$ -C $ARG1$ -T $ARG2$ -w $ARG3$ -c
$ARG4$ $ARG5$
}
define command{
   command_name check_catalyst_flash
   command_line $USER1$/check_catalyst_flash.pl -s $HOSTADDRESS$ -C $ARG1$ -w $ARG2$ -c $ARG3$
}
define command{
   command_name check_catalyst_mem
   command_line $USER1$/check_catalyst_mem.pl -s $HOSTADDRESS$ -C $ARG1$ -w $ARG2$ -c $ARG3$
}
define command{
   command_name check_catalyst_fans
   command_line $USER1$/check_catalyst_fans.pl -s $HOSTADDRESS$ -C $ARG1$
}
define command{
   command_name check_catalyst_load
   command_line $USER1$/check_catalyst_load.pl -s $HOSTADDRESS$ -C $ARG1$ -w $ARG2$ -c $ARG3$
}
```

Una vez añadidos los comandos, ya se pueden utilizar en el fichero .cfg del switch:

```
define service {
```

[30] http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml
[31] http://exchange.nagios.org/directory/Plugins/Hardware/Network-Gear/Cisco

```
        use                     generic-service
        host_name               CiscoSwitchRed2
        service_description     Mem Flash
        check_command           check_catalyst_flash!-C public!20!10
        }
define service {
        use                     generic-service
        host_name               CiscoSwitchRed2
        service_description     Mem RAM
        check_command           check_catalyst_mem!-C public!20!10
        }
define service {
        use                     generic-service
        host_name               CiscoSwitchRed2
        service_description     Ventiladores
        check_command           check_catalyst_fans!-C public
        }
define service {
        use                     generic-service
        host_name               CiscoSwitchRed2
        service_description     Load
        check_command           check_catalyst_load!-C public!80,80,80!90,90,90
        }
```

A continuación se muestra un switch de Cisco, monitorizado con Nagios:

Load	OK	06-08-2012 13:17:02	2d 23h 47m 27s	1/3	OK: CPU0: 0% 0% 0% !
Mac Address	OK	06-08-2012 13:19:42	6d 17h 44m 47s	1/3	SNMP OK - 00 11 21 A1 AF 01
Mem Flash	OK	06-08-2012 13:14:15	2d 23h 51m 31s	1/3	OK: Onboard system FLASH: Size: 15998976 Free: 6638592 (41%) Status: available VPP: installed!
Mem RAM	OK	06-08-2012 13:17:49	2d 23h 46m 40s	1/3	OK: I/O: valid, Used: 3017144B Free: 5371464B (64%)! Processor: valid, Used: 10661704B Free: 36332320B (77%)!
PING	OK	06-08-2012 13:20:43	6d 17h 43m 46s	1/3	ECO OK - Paquetes perdidos = 0%, RTA = 1.18 ms
Port 1 Interface Speed	OK	06-08-2012 13:23:35	6d 17h 41m 43s	1/3	SNMP OK - 100000000
Port 1 Interface Type	OK	06-08-2012 13:17:47	5d 17h 46m 42s	1/3	SNMP OK - 6
Port 1 Link Status	OK	06-08-2012 13:14:48	6d 17h 39m 41s	1/3	SNMP OK - 1
Port 2 Interface Speed	OK	06-08-2012 13:15:50	6d 17h 38m 39s	1/3	SNMP OK - 10000000
Port 2 Interface Type	OK	06-08-2012 13:23:35	5d 17h 50m 54s	1/3	SNMP OK - 6
Port 2 Link Status	OK	06-08-2012 13:17:48	6d 17h 46m 41s	1/3	SNMP OK - 2
Port 3 Interface Speed	OK	06-08-2012 13:18:50	6d 17h 45m 39s	1/3	SNMP OK - 100000000
Port 3 Link Status	OK	06-08-2012 13:19:51	6d 17h 44m 38s	1/3	SNMP OK - 2
Uptime	OK	06-08-2012 13:20:52	6d 17h 43m 37s	1/3	SNMP OK - Timeticks: (173078057) 20 days, 0:46:20.57
Ventiladores	OK	06-08-2012 13:18:37	2d 23h 45m 52s	1/3	OK: chassis: normal

Fig. 119: Monitorización con Nagios de un switch Cisco Catalyst.

10.2. Dispositivos de la red inalámbrica

Los Access Point de Cisco permiten monitorización utilizando SNMP. Además de los comandos habituales para cualquier sistema Linux/Unix, como por ejemplo check_snmp (sysUpTime), check_http, check_ping, …, los APs de Cisco permiten ser gestionados de forma más detallada utilizando las MIBs correspondientes a cada modelo. Éstas se pueden descargar de la web de Cisco. Por ejemplo, para APs de la serie C1100 están disponibles las MIBS: CISCO-DOT11-ASSOCIATION-MIB y CISCO-DOT11-IF-MIB, que pueden ser interesantes para un conocimiento básico del estado del AP.

```
alumno@nagios:~$ snmpget  -c public -v1 192.168.1.10 .1.3.6.1.4.1.9.9.273.1.1.2.1.1.1
1.3.6.1.4.1.9.9.273.1.1.2.1.1
```

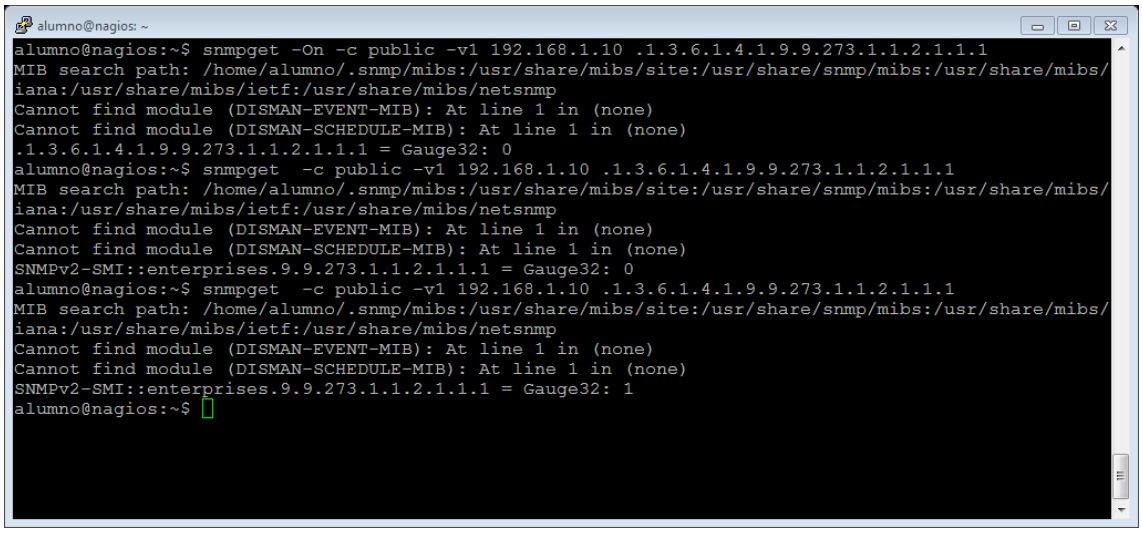


Fig. 120: Consulta en SNMP de clientes asociados en un AP de Cisco.

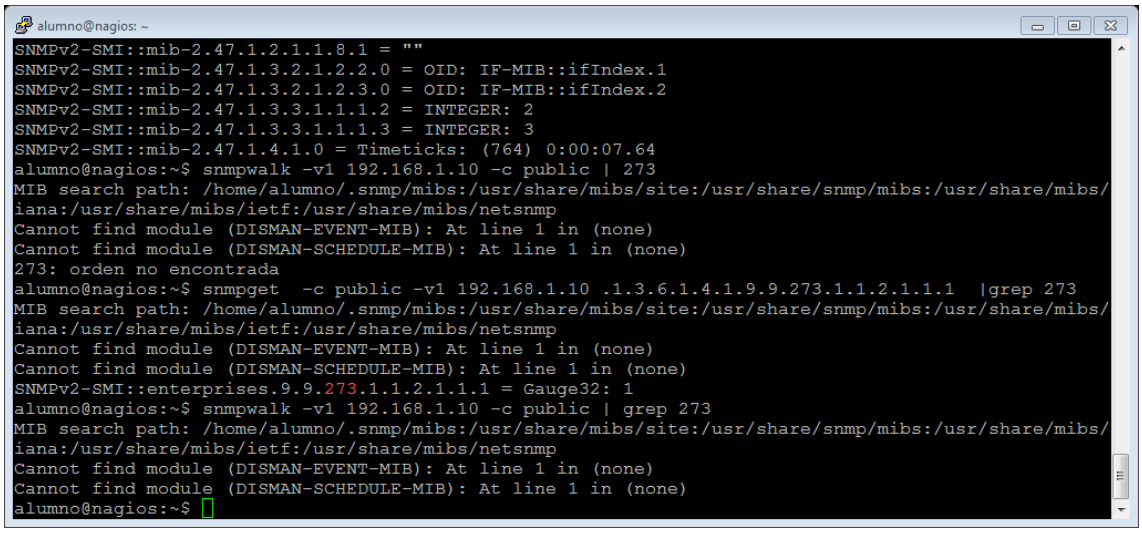


Fig. 121: Uso de la herramienta snmpwalk con MIB privadas (Enterprise).

La lista completa con todos los OIDs disponibles se pueden consultar en la página web de Cisco[32] o en oidview.com. En el anexo VIII se incluye la lista con todos los OIDs de la MIB CISCO-DOT11-ASSOCIATION-MIB.my.

Para descargar todas las MIBs disponibles se debe tener en cuenta la versión de la IOS[33]. Algunas, como las anteriores, están disponibles para todas las versiones.

En el caso de necesitar monitorizar parámetros de clientes concretos, hay que averiguar primero su dirección MAC para saber que OID consultar. Los siguientes resultados muestran el nivel de señal (en dBm) y la relación señal/ruido (en dB) de un cliente cuya dirección MAC es 74-2F-68-9F-D6-5D (116.47.104.159.214.93). Los OIDs a consultar son:

```
"cDot11ClientSignalStrength"          "1.3.6.1.4.1.9.9.273.1.3.1.1.3"
```

[32] ftp://ftp.cisco.com/pub/mibs/oid/CISCO-DOT11-ASSOCIATION-MIB.oid
[33] ftp://ftp.cisco.com/pub/mibs/supportlists/c1100/c1100-supportlist.html

```
"cDot11ClientSigQuality"            "1.3.6.1.4.1.9.9.273.1.3.1.1.4"
```

Los OIDs finales deben ser:

```
.1.3.6.1.4.1.9.9.273.1.3.1.1.3.1.5.85.80.83.65.49.116.47.104.159.214.93
.1.3.6.1.4.1.9.9.273.1.3.1.1.4.1.5.85.80.83.65.49.116.47.104.159.214.93
```

Los comandos a ejecutar son:

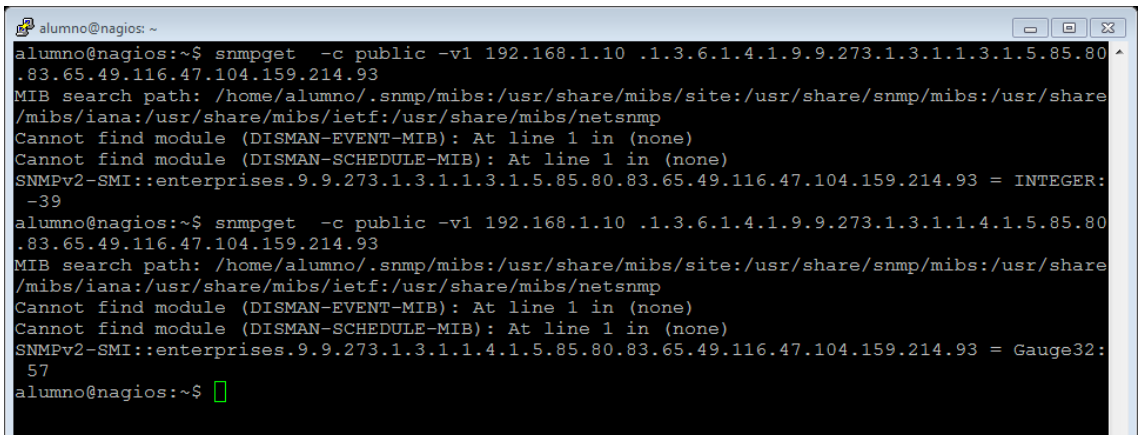


Fig. 122: Lectura SNMP del nivel de señal y relación señal ruido en AP Cisco.

Para comprobar los resultados, se puede consultar la página web del dispositivo, donde aparece esta información:

MAC Address	742f.689f.d65d	Name	NONE
IP Address	192.168.1.53	Class	unknown
Device	unknown	Software Version	NONE
CCX Version	NONE		
State	Associated	Parent	self
SSID		VLAN	
Hops To Infrastructure	1	Communication Over Interface	Radio0-802.11G
Clients Associated	0	Repeaters Associated	0
Key Mgmt type	NONE	Encryption	Off
Current Rate (Mb/sec)	54.0	Capability	WMM ShortHdr ShortSlot
Supported Rates(Mb/sec)	1.0, 2.0, 5.5, 11.0, 6.0, 9.0, 12.0, 18.0, 24.0, 36.0, 48.0, 54.0		
Voice Rates(Mb/sec)	disabled	Association Id	123
Signal Strength (dBm)	-38	Connected For (sec)	1996
Signal to Noise (dBm)	57	Activity TimeOut (sec)	60
Power-save	Off	Last Activity (sec)	0
Apsd DE AC(s)	NONE	Posture Token	
Session TimeOut (sec)		Reauthenticate In (sec)	Never
Receive/Transmit Statistics			
Total Packets Input	5870	Total Packets Output	3816
Total Bytes Input	865711	Total Bytes Output	2455597
Duplicates Received	1	Maximum Data Retries	132
Decrypt Errors	0	Maximum RTS Retries	0

Fig. 123: Página web de un AP Cisco con información de clientes asociados.

Por último, el AP monitorizado con Cisco se muestra en la siguiente figura:

apcisco	Calidad senal [dB]	OK	03-08-2012 13:40:57	0d 1h 42m 24s	1/3	SNMP OK - 37
	Clientes Wireless Asociados	OK	03-08-2012 13:40:31	3d 0h 25m 43s	1/3	SNMP OK - 2
	Clientes Wireless Asociados Totales	OK	03-08-2012 13:38:34	2d 17h 14m 47s	1/3	SNMP OK - 54700
	HTTP	WARNING	03-08-2012 13:39:53	3d 18h 1m 28s	4/4	HTTP WARNING: HTTP/1.1 401 Unauthorized - 192 bytes en 0,022 segundo tiempo de respuesta
	Nivel de senal [dBm]	OK	03-08-2012 13:41:18	0d 1h 42m 3s	1/3	SNMP OK - 58
	Port 1 Interface Speed	OK	03-08-2012 13:35:32	2d 18h 7m 49s	1/3	SNMP OK - 54000000
	Port 2 Interface Speed	OK	03-08-2012 13:37:00	2d 18h 6m 50s	1/3	SNMP OK - 100000000
	Uptime	OK	03-08-2012 13:35:24	3d 17h 58m 24s	1/3	SNMP OK - Timeticks: (146912584) 17 days, 0:05:25.84

Fig. 124: Cisco Access Point monitorizado con Nagios.

Las ligeras diferencias de nivel y calidad de señal del cliente, se deben al momento exacto de la lectura de los objetos.

10.3. Impresoras de red

Para la monitorización de impresoras, se puede utilizar la plantilla que Nagios proporciona: /etc/nagios/objects/printer.cfg:

```
define host{
use             generic-printer          ; Inherit default values from a template
host_name       Contabilidad             ; The name we're giving to this printer
alias                   Contabilidad4050         ; A longer name associated with the printer
address                 10.37.15.63              ; IP address of the printer
hostgroups      HP                       ; Host groups this printer is associated with
}
define hostgroup{
hostgroup_name          network-printers         ; The name of the hostgroup
alias                   Network Printers         ; Long name of the group
}
define service{
use             generic-service          ; Inherit values from a template
hostgroup_name          HP,O                     ; The name of the host the service is associated
with
service_description     Printer Status           ; The service description
check_command           check_hpjd!-C public             ; The command used to monitor the service
normal_check_interval   10                       ; Check the service every 10 minutes under normal
conditions
retry_check_interval 1                           ; Re-check the service every minute until its
final/hard state is determined
}
define service{
use             generic-service
hostgroup_name          HP,R,Lex,O,B
service_description     PING
check_command           check_ping!3000.0,80%!5000.0,100%
normal_check_interval   10
retry_check_interval 1
}
```

Además del típico ping, define un servicio específico para impresoras que utilizan típicamente el servicio JetDirect (HP). Para este servicio, hay que hacer coincidir la comunidad SNMP de la impresora y la especificada en el comando *check_hpjd*. Este comando funciona muy bien con impresoras HP y algunas otras que hemos probado (Brother) pero no devuelve valores correctos para otras marcas probadas (Lexmark, Oki).

Como para todos los comandos de nagios, existen plugins que se pueden descargar de la página http://exchange.nagios.org/

Para nuestro uso, hemos utilizado el check_snmp_printer que pasamos a describir a continuación en la versión original del programador del plugin:

```
Universal printer check. Check for specific consumables or report on all. Query model/serial #,
event messages, tray status and much more!
Originally based on Monitoring Solutions' check_snmp_printer, this provides friendly output,
quick execution and thorough pre-flight checking.
*** NOW COMPATIBLE WITH UBUNTU ***
I liked the original plugin but wanted to be able to report the status of all consumables. For
some devices this output can get huge. When only 1 component is empty, it becomes a challenge to
find what needs to be replaced in the output. So this script was born.
I added checks for user input and better feedback for improper parameters. The same goes for
SNMP status - before any code is executed, this is tested.
Usage is as follows:
check_snmp_printer -H {HOSTADDRESS} -C {COMMUNITY} -x "{CHECK}" -w {WARNING} -c {CRITICAL} -S
{separator string} | -V | -h
{CHECK} can be one of the following:
CONSUM {"string" | TEST | ALL}
DEVICES
DISPLAY
MESSAGES
MODEL
PAGECOUNT
STATUS
TRAY {number(s) | TEST | ALL}
VERSION
If you want the output for consumables to contain multiple lines, pass the following argument:
-S "n"
Then you need to edit your service notifications. Just after the $SERVICEOUTPUT$ macro, you will
need to add "n$LONGSERVICEOUTPUT$". E-mails will finally contain lines 2 and up of the output.
The CONSUM option gives results for all consumable names that match the string passed. For
instance, you can pass "CONSUM Toner" and see all toner levels (no staple cartridges or imaging
units). Similarly, "CONSUM Black" will show you the Black imaging unit and Black toner levels
all at once. The ALL option gives all consumable status at once, and TEST will show you which
CONSUMABLES can be monitored.
CONSUMX reports on consumables that match the eXact string passed to it. This helps allevíate
problems when a "unique" string is not possible. For example, "CONSUMX Black Toner" would give
an error unless the FULL description of the consumable (from a CONSUM TEST) is "Black Toner".
Any consumable named "Black Toner1" or "Black Toner Cartridge" would be overlooked.
TRAY can be passed a number or list of numbers (comma-separated) as a parameter. The ALL
parameter reports all tray statuses and TEST lets you know which trays the device has. In
addition to generic status, the tray function tries to calculate paper remaining as a % of
capacity (if possible), although this only works as good as the sensors on the device (and often
only returns values at fixed intervals, such as 25%, 50%, 75%, etc.)
DEVICE, DISPLAY, MESSAGES, MODEL and STATUS report information about the printer's hardware
devices, physical display, event log messages, model/serial or overall status (respectively).
```

If looking to add this to a new configuration, your command descriptions should look something like the following:

```
define service{
use generic-service
service_description          Toner Supply
check_command                check_snmp_printer!public!"CONSUM Toners"!20!10
}
define service{
use                          generic-service
service_description          Printer Model
check_command                check_snmp_printer!public!"MODEL"
}
define command{
command_namecheck_printers
command_line         $USER1$/check_snmp_printer -H $HOSTADDRESS$ -C $ARG1$ -x $ARG2$ -w $ARG3$ -
c $ARG4$
}
```

Para que el plugin funcione hay que descargar el script en la carpeta donde están los demás plugins (en nuestro caso está en /usr/local/nagios/libexec/) y cambiarle los propietarios y los permisos de ejecución para que pueda funcionar. Editar el fichero y comprobar después de la descarga, que no se ven caracteres extraños en el código fuente. Una vez resueltos todos los problemas hay que definir el comando en el fichero commands.cfg (se trata de copiar y pegar las últimas tres líneas del define command que están en negrita según las instrucciones del autor) para que Nagios pueda utilizarlo, quedando el fichero de la siguiente forma:

```
define command{
command_namecheck_printers
command_line         $USER1$/check_snmp_printer -H $HOSTADDRESS$ -C $ARG1$ -x $ARG2$ -w $ARG3$ -
c $ARG4$
}
```

Después de esto, ya podernos utilizarlo en nuestro Nagios como el siguiente ejemplo:

```
##############################################################################
##############################################################################
# SERVICE DEFINITIONS
#
##############################################################################
##############################################################################
# Create a service for monitoring the status of the printer
# Change the host_name to match the name of the host you defined above
# If the printer has an SNMP community string other than "public", change the check_command
directive to reflect that

define service{
use         generic-service
host_name   Contabilidad
service_description  Devices
check_command       check_printers!public!"DEVICES"
}

define service{
use         generic-service
host_name   Facturacion
service_description  Display
check_command       check_printers!public!"DISPLAY"
}

define service{
use         generic-service
host_name   H51
service_description  Mensajes Log
check_command       check_printers!public!"MESSAGES"
}

define service{
use         generic-service
host_name   Suministros1300
service_description  Modelo
 check_command      check_printers!public!"MODEL"
}

define service{
use         generic-service
host_name   A
service_description  Estado
check_command       check_printers!public!"STATUS"
}

define service{
use         generic-service
host_name    A
service_description  Consumibles 1
check_command       check_printers!public!"CONSUM  Toner  Cartridge  Brother  TN-550/TN-3130/TN-
3145/TN-35J/TN-3135"
}

define service{
use         generic-service
host_name   A
service_description  Consumibles 2
check_command       check_printers!public!"CONSUM  Toner  Cartridge  Brother  TN-580/TN-3170/TN-
3185/TN-37J/TN-3175"
}

define service{
use         generic-service
host_name   A
service_description  Drum Unit
check_command       check_printers!public!"CONSUM  Drum  Unit  Brother  DR-520/DR-3100/DR-3115/DR-
31J/DR-3150"
}

define service{
use         generic-service
host_name   H5
service_description  Consumibles Toner
check_command       check_printers!public!"CONSUM Black Toner"
}

define service{
use         generic-service
host_name   H5
service_description  Consumibles Kit Mantenimiento
check_command       check_printers!public!"CONSUM Maintenance Kit"
}

define service{
```

```
use         generic-service
host_name   H8
service_description  Bandeja 1
check_command        check_printers!public!"TRAY 1"
}

define service{
use         generic-service
host_name   H8
service_description  Bandeja 2
check_command        check_printers!public!"TRAY 2"
}

define service{
use         generic-service
host_name   H8
service_description  Numero de paginas
check_command        check_printers!public!"PAGECOUNT"
}
```

El primer check utilizado es DEVICES y nos da información de los distintos dispositivos hardware que se testean en la máquina.

Con el check DISPLAY vemos el mensaje que se muestra en el visor LCD de la impresora.

Con el check MESSAGES devuelve el valor que tiene en event log messages; según las pruebas realizadas devuelve información hexadecimal que no hemos llegado a descifrar.

Con el check MODEL devuelve el modelo y número de serie de la impresora.

Con el check STATUS devuelve el estado de la impresora. Los valores van de 1 a 5 y dependiendo del modelo se refieren a WarmUp, OK, Printing, etc. Si el estado no es uno de estos, devuelve un WARNING. Lo más seguro es que devuelva un WARNING, ya que si el tóner y el nivel de papel es bajo, entonces el estado devuelto es el 1 (WARNING), aunque la impresora funciona perfectamente.

Con el check CONSUM nos devuelve el estado de los consumibles de la impresora. Los argumentos que se pueden pasar a CONSUM son {"string"|TEST|ALL}. Con ALL devuelve información de todos los consumibles sin ordenar. Si ejecutamos TEST nos devuelve el nombre (string) de todos los consumibles que se pueden testear. Una vez obtenidas estas cadenas de caracteres, se puede construir un comando como *check_printers!public!"CONSUM Black Toner"* o *check_printers!public!"CONSUM Toner Cartridge Brother TN-580/TN-3170/TN-3185/TN-37J/TN-3175"* donde después de CONSUM se escribe el "string" que antes obtuvimos en la opción de TEST.

Con el check TRAY vemos el estado de las bandejas. Los argumentos que se pueden pasar a TRAY son {"number(s)"|TEST|ALL}. Al igual que el check anterior, con ALL devuelve información de todas las bandejas sin ordenar. Si ejecutamos TEST nos devuelve el número de bandejas que se pueden testear. Una vez obtenidos estos números se puede construir un comando como *check_printers!public!"TRAY 1"* o *check_printers!public!"TRAY 2"*.

Con el check PAGECOUNT se obtiene el número de páginas impresas por la impresora.

Al final de todos los comandos se pueden pasar los argumentos 3 y 4 del ejemplo:

```
command_line $USER1$/check_snmp_printer -H $HOSTADDRESS$ -C $ARG1$ -x $ARG2$ -w $ARG3$ -c $ARG4$
```

para pasar un valor numérico del umbral en el que queremos que Nagios nos de un WARNING o un CRITICAL, como por ejemplo:

```
check_snmp_printer!public!"CONSUM Toners"!20!10
```

Con la anterior configuración de Nagios, obtenemos la siguiente respuesta en la interfaz Web:

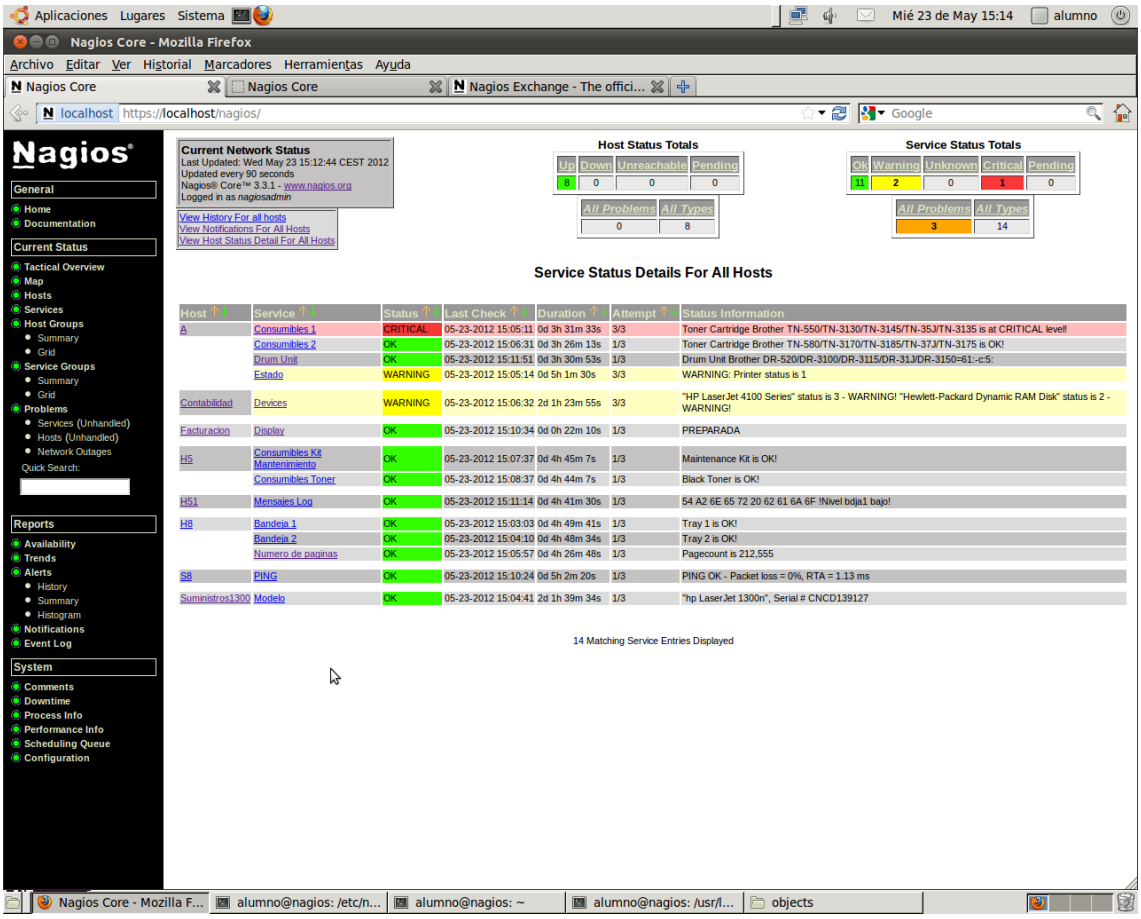


Fig. 125: Vista gestión de impresoras en Nagios.

Para que sirva de ejemplo, se ha abierto la bandeja 2 de una impresora. La interfaz de Nagios muestra el siguiente mensaje:

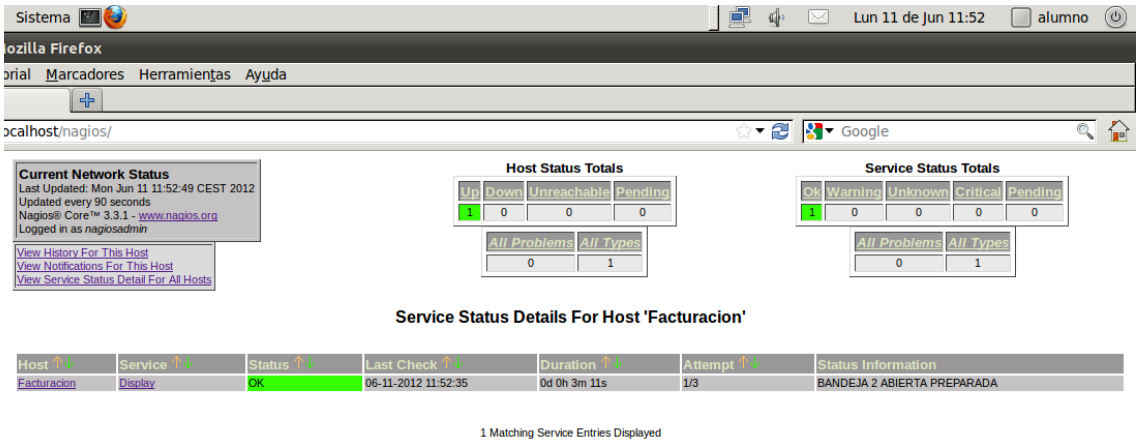


Fig. 126: Detección de bandeja abierta en una impresora.

Y a continuación muestro el mensaje que da localmente el display de la impresora. Muestra alternativamente "Preparada" y "Bandeja 2 abierta":

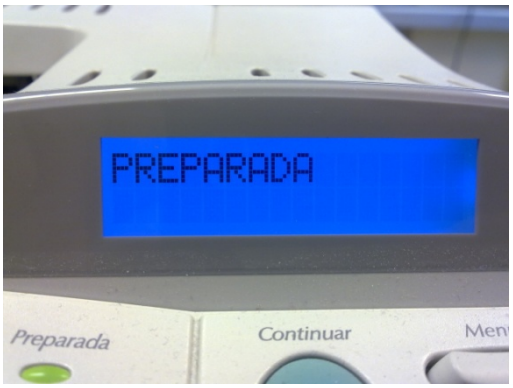


Fig. 127: Mensaje en el display de la impresora del aviso en Nagios.

10.4. Servidores LINUX (Ubuntu)

El fichero de configuración localhost.cfg en el directorio objects se puede utilizar como plantilla para monitorizar máquinas Linux:

```
define host{
        use                     linux-server            ; Name of host template to use
                                                        ; This host definition will inherit all
variables that are defined
                                                        ; in (or inherited by) the linux-server
host template definition.
        host_name               moodle
        alias                   servidor moodle
        address                 192.168.1.115
        }

# Define a service to "ping" the local machine

define service{
        use                             local-service         ; Name of service template to use
        host_name                       moodle
        service_description             PING
    check_command                   check_ping!100.0,20%!500.0,60%
        }
```

Hay que tener en cuenta que en el fichero localhost.cfg ya hay definido un grupo, que se puede utilizar para incluir estas máquinas:

```
define hostgroup{
        hostgroup_name  linux-servers ; The name of the hostgroup
        alias           Linux Servers ; Long name of the group
        members         localhost,moodle     ; Comma separated list of hosts that belong to this
group
        }
```

Este tipo de monitorización no requiere la instalación de ningún agente adicional en la máquina a monitorizar. Si se quiere monitorizar una máquina remota hay varias soluciones.

La primera consiste en la instalación del software NRPE (Nagios Remote Plugin Executor). La siguiente figura muestra la arquitectura software de este plugin:

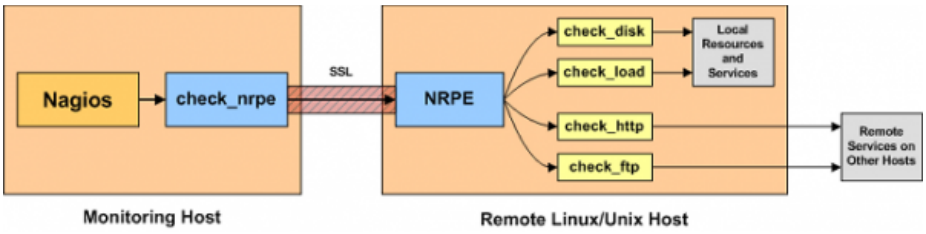


Fig. 128: Monitorización remota vía NRPE.

La segunda posibilidad es utilizar el comando *check_by_ssh*. Este comando también permite consultar información de forma remota, pero consume más recursos de cpu en la máquina donde está instalado Nagios.

La tercera es la más adecuada a la infraestructura hospitalaria objetivo de este proyecto. Consiste en utilizar SNMP para consultar a los servidores (también en Windows). A continuación se muestran algunos comandos que se han seleccionado por su importancia en la gestión de la infraestructura hospitalaria.

10.4.1. Check_snmp

Es el comando snmp básico que está disponible en la instalación estándar de Nagios. Con este comando se puede consultar la información que devuelve un host con un agente SNMP instalado.

El siguiente fichero de configuración consulta el objeto *sysUpTime* y la velocidad de la interfaz 1 (*ifSpeed.1*):

```
# Monitor uptime vía SNMP

define service{
        use                     generic-service ; Inherit values from a template
        host_name               zyxel
        service_description     Uptime
        check_command           check_snmp!-C public -o sysUpTime.0
        }

# Monitor interface speed vía SNMP

define service {
        use                     generic-service
        host_name               zyxel
```

```
        service_description     Port 1 Interface Speed
        check_command           check_snmp!-C public -o ifSpeed.1 -r 1 -m RFC1213-MIB
        }
```

Con este comando, y averiguando el oid a consultar, se puede monitorizar cualquier dispositivo vía SNMP. No obstante, a veces es interesante escribir un script customizado para conseguir averiguar el estado del dispositivo. Es muy habitual encontrar scripts hechos en lenguaje Perl, ya que es un lenguaje muy apropiado para desarrollar aplicaciones de red.

10.4.2. Check_snmp_storage

El script check_snmp_storage.pl[34] escrito en lenguaje Perl, se ha utilizado para monitorizar el estado de los sistemas de almacenamiento. Para poder utilizar este comando, se han de configurar los siguientes ficheros:

- Crear un fichero de comandos nuevo, por ejemplo *miscomandos.cfg*. Añadir el nuevo comando con los parámetros correspondientes:

```
# 'check_snmp_storage' command definition
define command{
        command_name    check_snmp_storage
        command_line    $USER1$/check_snmp_storage.pl -H $HOSTADDRESS$ $ARG1$
        }
```

- Editar el fichero *nagios.cfg* y añadir el nuevo fichero de comandos creado:

```
cfg_file=/etc/nagios/objects/miscomandos.cfg
```

- Editar el fichero de configuración del host/servicio, añadiendo el comando al servicio con los parámetros deseados:

```
define service{
        use                     generic-service
        host_name               monitorlinux
        service_description     Swap
        check_command           check_snmp_storage!-C public -m Swap -w80 -c 90
}
```

Descripción :

```
This scripts checks by snmp (V1 and v3) disks, memory, swap, everthing in hrStorage table.
Storages selection can be done :
- by perl regexp on description or index (-m)
- and (optional) by storage type (-q) : Other, Ram, VirtualMemory, FixedDisk, RemovableDisk,
FloppyDisk, CompactDisk, RamDisk, FlashMemory, NetworkDisk

One or multiple storages can be selected.
It is also possible to sum all selected storages (-s)

Warning and critical levels can be checked based on : Percent of disk used, Percent of disk
left, MB left or MB used

Output options (-S):
-S can have 3 options : <type>[,<where>,<cut>]
<type> : Make the output shorter :
0 : only print the global result except the disk in warning or critical
1 : Don't print all info for every disk
<where> : (optional) if = 1, put the OK/WARN/CRIT at the beginning
<cut> : take the <n> first caracters or <n> last if n<0

With the following disks : /home : 51% used and / : 90% used
99%         /home: 51%used(1012MB/1969MB) /: 90%used(5781MB/6390MB) (<99%) : OK
90%         /home: 51%used(1012MB/1969MB) /: 90%used(5781MB/6390MB) (>90%) : WARNING
-S0         90%      All selected storages (<99%) : OK
```

[34] Descargar en: http://nagios.manubulon.com/

```
-S0         99%     /: 90%used(5781MB/6390MB) (>90%) : WARNING
-S1         90%     /home: 51% /: 90% (<99%) : OK
-S1         99%     /home: 51% /: 90%used(5781MB/6390MB) (>90%) : WARNING
-S0,1       90%     OK : (<99%) All selected storages
-S0,1       90%     WARNING : (>90%) /: 90%used(5781MB/6390MB)
-S1,,2      99%     /h: 51% /: 90% (<99%) : OK
-S1,,-2     99%     me: 51% /: 90% (<99%) : OK
-S0,1,-2    30%     WARNING : (>30%) me: 51%used(1012MB/1969MB) /: 90%used(5781MB/6390MB)

Performance output (-f option)
The performance will remove any weird caracters ( `~!$%^&*'"<>|?,(= ) ) from the drive name.

Msg size option (-o option)
In case you get a "ERROR: running table : Message size exceeded maxMsgSize" error, you may need
to adjust the maxMsgSize, i.e. the maximum size of snmp message with the -o option. Try a value
with the -o AND the -v option : the script will output the actual value so you can add some
octets to it with the -o option.

Requirements :
- Perl in /usr/bin/perl - or just run 'perl script'
- Net::SNMP
- file 'utils.pm' in plugin diretory (/usr/local/nagios/libexec)

Configurations examples
Changelog : On CVS repository on sourceforge : http://nagios-snmp.cvs.sourceforge.net/nagios-
snmp/plugins/.

Examples :
All examples below are considering the script is local directory. Host to be checked is
127.0.0.1 with snmp community "public".
```

Ayuda de la sintaxis:

```
./check_snmp_storage.pl -h
List all storage     ./check_snmp_storage.pl -H 127.0.0.1 -C public -m zzzz -w 80 -c 81 -v
snmpv3 login         ./check_snmp_storage.pl -H 127.0.0.1 -l login -x passwd

%used of /home is less than 80% and 90%
./check_snmp_storage.pl -H 127.0.0.1 -C public -m /home -w 80% -c 90%

%free of /home is above 10% and 5%
./check_snmp_storage.pl -H 127.0.0.1 -C public -m /home -w 10% -c 5% -T pl

Mb used of /home is less than 800 Mb and 900 Mb
./check_snmp_storage.pl -H 127.0.0.1 -C public -m /home -w 800 -c 900 -T bu

Mb free of /home is above 100Mb and 30Mb
./check_snmp_storage.pl -H 127.0.0.1 -C public -m /home -w 100 -c 30 -T bl

All mountpoints have %used less than 80% and 90%
./check_snmp_storage.pl -H 127.0.0.1 -C public -m / -w 80% -c 90%

%used of / mountpoint only is less than 80% and 90%
./check_snmp_storage.pl -H 127.0.0.1 -C public -m / -r -w 80% -c 90%

%used of mountpoint index 1 only is less than 80% and 90%
./check_snmp_storage.pl -H 127.0.0.1 -C public -m 1 -p -w 80% -c 90%

Swap %used is less than 80% and 90%
./check_snmp_storage.pl -H 127.0.0.1 -C public -m Swap -w 80% -c 90%

Memory %used is less than 80% and 90%
./check_snmp_storage.pl -H 127.0.0.1 -C public -m "Real Memory" -w 80% -c 90%
```

Salida de check_snmp_storage.pl -h

```
example :
Browse storage list : <script> -C <community> -H <host> -m <anything> -w 1 -c 2 -v
the -m option allows regexp in perl format :
Test drive C,F,G,H,I on Windows : -m ^[CFGHI]:
Test all mounts containing /var : -m /var
Test all mounts under /var : -m ^/var
Test only /var : -m /var -r
Test all swap spaces : -m ^Swap
Test all but swap spaces : -m ^Swap -e
```

Un ejemplo de la información que se gestiona con este plugin es la siguiente (además de las correspondientes notificaciones por correo):

Host	Service	Status	Last Check	Duration	Attempt	Status Information
Cabinas1	Boot Partition	OK	06-26-2012 09:29:42	5d 17h 40m 17s	1/3	/boot: 28%used(27MB/99MB) (<90%) : OK
	File System	OK	06-26-2012 09:31:38	5d 17h 38m 41s	1/3	/boot: 28%used(27MB/99MB) /: 7%used(4129MB/61934MB) (<90%) : OK
	PING	OK	06-26-2012 09:36:48	5d 17h 11m 31s	1/3	PING OK - Packet loss = 0%, RTA = 1.73 ms
	Swap linux	OK	06-26-2012 09:35:31	4d 21h 46m 17s	1/3	Swap space: 0%used(0MB/5952MB) (<60%) : OK
Cabinas2	Boot Partition	OK	06-26-2012 09:30:01	5d 17h 3m 51s	1/3	/boot: 28%used(27MB/99MB) (<90%) : OK
	File System	OK	06-26-2012 09:31:57	5d 17h 2m 39s	1/3	/boot: 28%used(27MB/99MB) /: 4%used(2191MB/61934MB) (<90%) : OK
	PING	OK	06-26-2012 09:36:54	5d 17h 11m 31s	1/3	PING OK - Packet loss = 0%, RTA = 0.94 ms
	Swap linux	OK	06-26-2012 09:35:50	4d 21h 44m 21s	1/3	Swap space: 0%used(0MB/5952MB) (<60%) : OK
Cabinas3	Boot Partition	OK	06-26-2012 09:30:21	5d 17h 19m 35s	1/3	/boot: 28%used(27MB/99MB) (<90%) : OK
	File System	OK	06-26-2012 09:32:17	5d 17h 2m 39s	1/3	/boot: 28%used(27MB/99MB) /: 4%used(2192MB/61934MB) (<90%) : OK
	PING	OK	06-26-2012 09:37:13	5d 17h 11m 31s	1/3	PING OK - Packet loss = 0%, RTA = 1.09 ms
	Swap linux	OK	06-26-2012 09:36:09	4d 21h 42m 24s	1/3	Swap space: 0%used(0MB/5952MB) (<60%) : OK
Clinica	Boot Partition	OK	06-26-2012 09:30:40	5d 18h 2m 36s	1/3	/boot: 12%used(12MB/99MB) (<90%) : OK
	File System	WARNING	06-26-2012 09:32:36	5d 17h 35m 41s	3/3	/var/lib/nfs/rpc_pipefs: 0%used(0MB/0MB) /datos-informix: 91%used(67672MB/74587MB) /boot: 12%used(12MB/99MB) /sys: 0%used(0MB/0MB) /: 17%used(23015MB/133539MB) /proc/sys/fs/binfmt_misc: 0%used(0MB/0MB) (>90%) : WARNING
	PING	OK	06-26-2012 09:37:32	5d 16h 22m 33s	1/3	PING OK - Packet loss = 0%, RTA = 0.72 ms
	Swap linux	OK	06-26-2012 09:36:29	4d 21h 45m 58s	1/3	Swap Space: 0%used(0MB/1984MB) (<60%) : OK
Ldap1	Boot Partition	OK	06-26-2012 09:30:59	5d 18h 0m 41s	1/3	/boot: 36%used(35MB/99MB) (<90%) : OK
	File System	OK	06-26-2012 09:33:48	5d 16h 22m 41s	1/3	/boot: 36%used(35MB/99MB) /: 58%used(3378MB/5796MB) /var: 65%used(14439MB/22206MB) (<90%) : OK
	PING	OK	06-26-2012 09:36:52	0d 19h 55m 14s	1/3	PING OK - Packet loss = 0%, RTA = 1.05 ms
	Swap linux	OK	06-26-2012 09:36:48	0d 22h 16m 8s	1/3	Swap Space: 44%used(902MB/2048MB) (<60%) : OK
Ldap2	Boot Partition	OK	06-26-2012 09:31:19	5d 18h 0m 17s	1/3	/boot: 36%used(35MB/99MB) (<90%) : OK
	File System	OK	06-26-2012 09:33:48	5d 17h 32m 39s	1/3	/boot: 36%used(35MB/99MB) /: 53%used(3081MB/5796MB) /var: 64%used(14279MB/22206MB) (<90%) : OK
	PING	OK	06-26-2012 09:37:11	5d 16h 22m 33s	1/3	PING OK - Packet loss = 0%, RTA = 1.08 ms
	Swap linux	OK	06-26-2012 09:37:07	4d 21h 42m 5s	1/3	Swap Space: 11%used(223MB/2048MB) (<60%) : OK

Fig. 129: Utilización en Nagios del comando check_snmp_storage (Swap Linux).

10.4.3. Check_snmp_process

Es un script en lenguaje Perl que se utiliza para conocer los procesos que se están ejecutando en memoria[35]. La sintaxis del comando se puede consultar en el anexo IV o ejecutando el script con la opción –h.

/		OK	14-07-2012 19:09:23	0d 4h 57m 3s	1/3	/: 35%used(3204MB/9070MB) (<80%) : OK
Apache Processes		OK	14-07-2012 19:13:22	0d 4h 23m 4s	1/3	4 process matching apache2 (> 3) (<= 100):OK, Mem : 3.3Mb OK, Cpu : 0% OK
HTTP		OK	14-07-2012 19:13:14	1d 4h 24m 38s	1/4	HTTP OK: HTTP/1.1 200 OK - 453 bytes en 0,001 segundo tiempo de respuesta
PING		OK	14-07-2012 19:13:27	1d 4h 32m 59s	1/4	ECO OK - Paquetes perdidos = 0%, RTA = 0.40 ms
SSH		OK	14-07-2012 19:15:57	1d 4h 30m 29s	1/4	SSH OK - OpenSSH_5.8p1 Debian-1ubuntu3 (protocolo 2.0)
Swap		OK	14-07-2012 19:16:17	0d 6h 30m 9s	1/3	Swap space: 0%used(1MB/1022MB) (<80%) : OK
Uptime		OK	14-07-2012 19:08:02	1d 4h 28m 24s	1/3	SNMP OK - Timeticks: (10612390) 1 day, 5:28:43.90

Fig. 130: Consulta en Nagios utilizando el comando check_snmp_process.

El fichero de configuración que refleja la consulta de la figura anterior, es el siguiente:

```
define service{
        use                     generic-service
        host_name               monitorlinux
        service_description     Apache Processes
        check_command           check_snmp_process!public!apache2!3,100!0!-2 -m 20,30 -u 90,99
}
```

Se puede averiguar el número de procesos de un tipo, y el consumo de recursos de memoria y cpu.

[35] Descargar en: http://nagios.manubulon.com/index_commands.html#process

10.4.4. Check_snmp_load

Este script en Perl permite averiguar la carga de CPU de una máquina Windows o Linux, además de varios dispositivos de red, de Cisco y otros fabricantes.

La siguiente tabla muestra las distintas opciones disponibles:

Tabla X: Valores para los parámetros del comando check_snmp_load

-T value	System	-w & -c values
netsl	Linux : load provided by Net SNMP	3 values : load average on 1 min, 5 min, 15 min (absolute)
netsc	Linux : CPU usage given by net-snmp	1 value in %
as400	as400 CPU usage	1 value in %
cisco	cisco CPU usage	3 values : CPU average on 5sec, 1 min & 5 min (%)
cata	cisco catalyst CPU usage	3 values : CPU average on 5sec, 1 min & 5 min (%)
nsc	Netscreen CPU usage	3 values : CPU average on 5sec, 1 min & 5 min (%)
fg	Fortigate CPU usage	1 value in %
bc	bluecoat CPU usage	1 value in %
nokia	nokia CPU usage	1 value in %
hp	HP procurve switch CPU usage	1 value in %
lp	Linkproof CPU usage	1 value in %
hpux	HP-UX load	3 values : load average on 1 min, 5 min, 15 min

El siguiente código define el comando a utilizar y el servicio para el host. Cada uno de ellos se debe copiar en el fichero *.cfg* correspondiente:

```
define command {
   command_name check_snmp_load_v1
   command_line $USER1$/check_snmp_load.pl -H $HOSTADDRESS$ -C $ARG1$ -T $ARG2$ -w $ARG3$ -c
$ARG4$ $ARG5$
}

define service {
        use                     generic-service
        host_name               monitorlinux
        service_description     Linux Load
        check_command           check_snmp_load_v1!public!netsl!4,3,3!8,5,5
}
```

La siguiente figura muestra el resultado de la ejecución de comando:

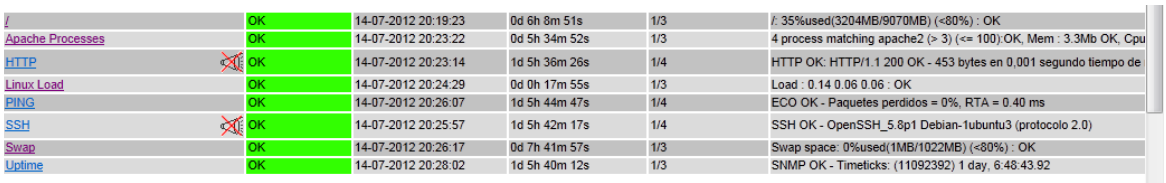


Fig. 131: Resultado de la ejecución del commando check_snmp_load en Nagios.

10.5. Servidores VMware ESX/ESXi

Los servidores ESX para desplegar infraestructuras basadas en virtualización son, en esencia, servidores con Linux Red Hat. Para gestionar estas máquinas con Nagios el procedimiento es similar al anterior: mediante el protocolo SNMP.

Para poder gestionar a bajo nivel la configuración del servidor o las máquinas virtuales, se pueden ejecutar comando vía ssh o scripts en Perl[36]. Nagios permite la creación de comandos personalizados para estas tareas más avanzadas.

El siguiente fichero de configuración define los servicios que se han identificado como importantes en la monitorización de estos servidores:

```
##############################################################################
#
# VMWare ESX Server SERVICE DEFINITIONS
#
##############################################################################

# Define a service to check if process exist.
# 'Proceso vpxa' relacionado con HA Cluster VMWare
# comando 'check_snmp_process'
define service{
    use                     generic-service          ; Name of service template to use
    hostgroup_name          vmware-esx-servers
    service_description     HA VMWare-Proc. VPXA
    check_command           check_snmp_process!vpxa!0!0!-r
}

# Define a service to check if process exist.
# 'Proceso vmware-hostd' relacionado con HA Cluster VMWare
# comando 'check_snmp_process'
define service{
    use                     generic-service          ; Name of service template to use
    hostgroup_name          vmware-esx-servers
    service_description     HA VMWare-Proc. VMWARE-HOSTD
    check_command           check_snmp_process!vmware-hostd!0!0!-r
}

# Define a service to check the disk space of the /var/log partition.
# Warning if < 20% free, critical if < 10% free space on partition.
# 'check_snmp_storage.pl' command definition
define service {
    use                     generic-service
    hostgroup_name                  vmware-esx-servers
    service_description     File System /var/log
    check_command           check_snmp_storage_v1!/var/log!80!90!-r -G
}
```

En el servidor se monitoriza el proceso y servicio vmware-vpxa (vCenter Server Agent). Éste permite a un servidor vCenter conectarse a servidores ESX. "vpxa" es el canal de comunicación con el hostd, que a su vez permite la conexión con el kernel.

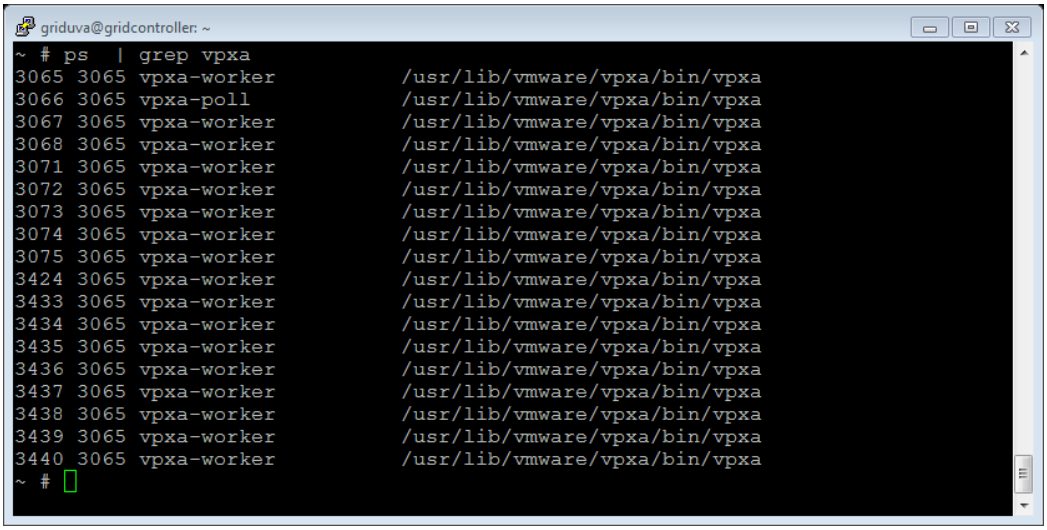
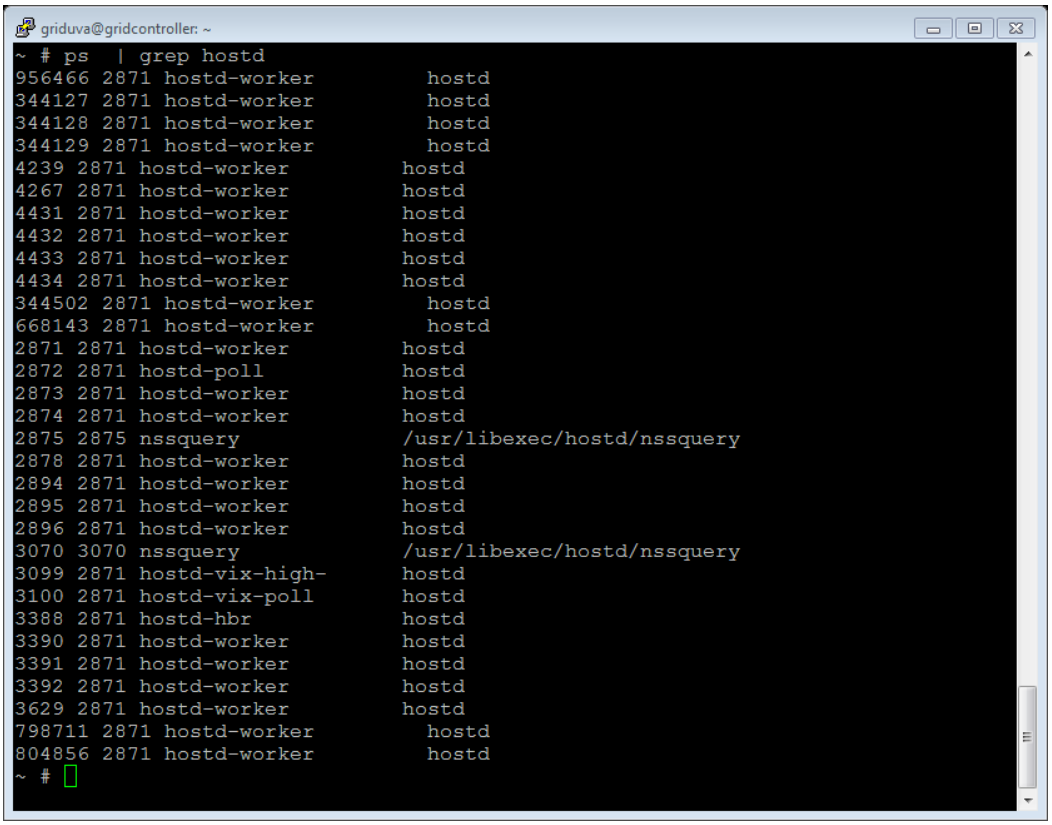


Fig. 132: Procesos vpxa arrancados en un servidor ESXi.

[36] Ver la herramienta "vSphere Remote Command Line", descargable desde la página web del servidor ESXi.



Otros procesos a monitorizar, como por ejemplo vmx-vthread, permite conocer qué máquinas virtuales están arrancadas. La siguiente figura muestra los procesos correspondientes a tres máquinas virtuales arrancadas en un servidor ESXi:

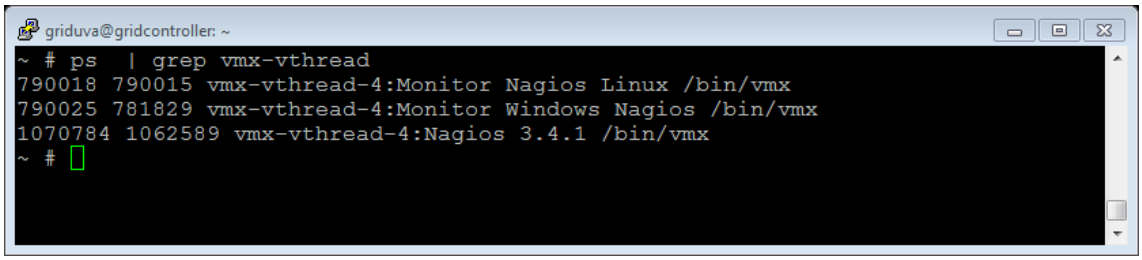


Fig. 133: Procesos vmx-vthread de ESXi asociados a máquinas virtuales arrancadas.

Los otros procesos relacionados con las máquinas arrancadas son:

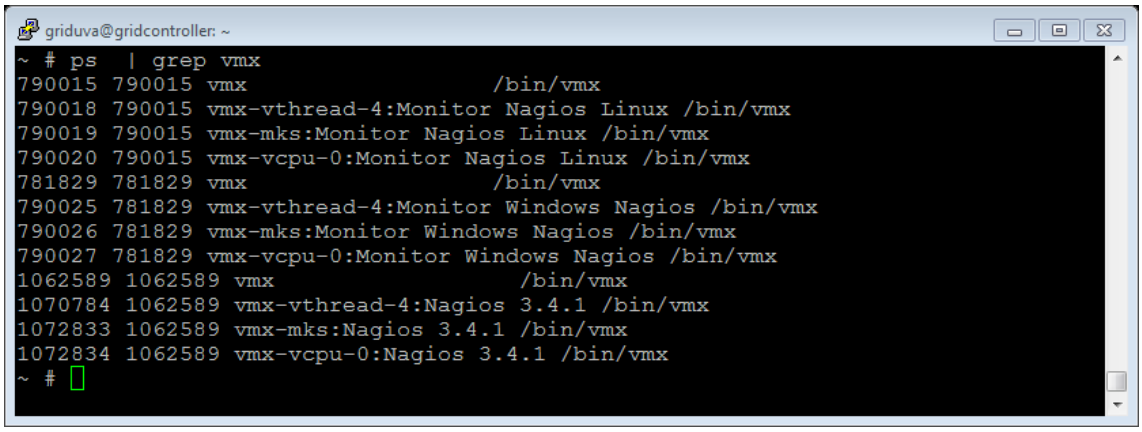


Fig. 134: Procesos asociados a una máquina virtual VMware ESXi.

El plugin *check_esx3-0.5.pl* de Nagios Exchange permite obtener información del servidor y de las máquinas virtuales: uso de cpu, disco, memoria, file systems, etc[37]. Se añade en el anexo VII los parámetros del plugin, para que el lector pueda ver su funcionalidad con detalle. En la página de Nagios Exchange existen muchos más plugins para productos VMware[38].

10.6. Servidores Windows

Antes de instalar plugins adicionales y crear ficheros de configuración de servicios que dependen del NSClient, hay que asegurarse que este software está instalado en los clientes. Para ver la instalación con detalle, consultar el capítulo 6 (Instalación de NSClient++).

Las ventajas e inconvenientes de este plugin son fundamentalmente que funciona bien, pero requiere instalar el cliente en la máquina a monitorizar. En las pruebas que se han realizado en el hospital de Ávila se ha utilizado esta opción y se ha combinado con un chequeo directo con SNMP a otros dispositivos de las máquinas Windows, como ventiladores y temperaturas de CPU.

A continuación se muestra el ejemplo de dos máquinas Windows (servidores Proliant MD360) junto a otros dispositivos.

[37] http://exchange.nagios.org/directory/Plugins/Operating-Systems/*-Virtual-Environments/VMWare/Vmware-ESX-%26-VM-host/details

[38] http://exchange.nagios.org/directory/Plugins/Operating-Systems/%2A-Virtual-Environments/VMWare

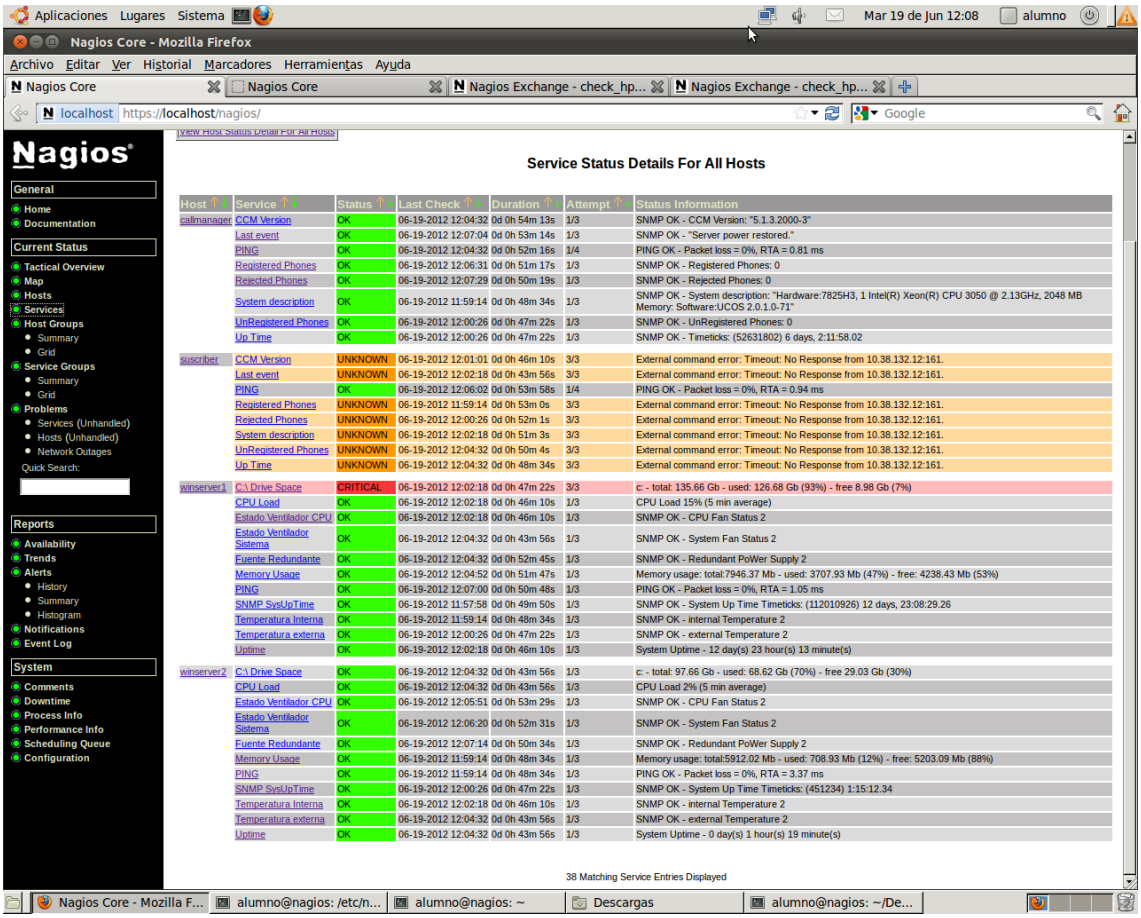


Fig. 135: Gestión en Nagios de servidores Windows Proliant.

A continuación se muestra el fichero con los comandos requeridos:

```
##############################################################################
HOST DEFINITIONS
##############################################################################
# Define a host for the Windows machine we'll be monitoring
# Change the host_name, alias, and address to fit your situation

define host{
use         windows-server   ; Inherit default values from a template
host_name   winserver1       ; The name we're giving to this host
alias               Aplicaciones1    ; A longer name associated with the host
address             10.36.64.85      ; IP address of the host
}
define host {
use         windows-server
host_name   winserver2
alias                Aplicaciones2
address             10.36.64.86
}
##############################################################################
# HOST GROUP DEFINITIONS
##############################################################################
# Define a hostgroup for Windows machines
# All hosts that use the windows-server template will automatically be a member of this group
define hostgroup{
hostgroup_name       windows-servers  ; The name of the hostgroup
alias                Windows Servers  ; Long name of the group
}
define hostgroup {
hostgroup_name       informatica
alias                Informatica
members              winserver1,winserver2
}
##############################################################################
# SERVICE DEFINITIONS
##############################################################################
# Define a service to "ping" the local machine
```

```
define service{
use                 generic-service  ; Name of service template to use
hostgroup_name              informatica
service_description         PING
check_command               check_ping!100.0,20%!500.0,60%
}

# Create a service for monitoring the uptime of the server
# Change the host_name to match the name of the host you defined above

define service{
use         generic-service
hostgroup_name      informatica
service_description  Uptime
check_command       check_nt!UPTIME
}

# Create a service for monitoring CPU load
# Change the host_name to match the name of the host you defined above

define service{
use         generic-service
hostgroup_name      informatica
service_description  CPU Load
check_command       check_nt!CPULOAD!-l 5,80,90
}
# Create a service for monitoring memory usage
# Change the host_name to match the name of the host you defined above

define service{
use         generic-service
hostgroup_name      informatica
service_description  Memory Usage
check_command       check_nt!MEMUSE!-w 80 -c 90
}
# Create a service for monitoring C:\ disk usage
# Change the host_name to match the name of the host you defined above

define service{
use         generic-service
hostgroup_name      informatica
service_description  C:\ Drive Space
check_command       check_nt!USEDDISKSPACE!-l c -w 80 -c 90
}

define service{
use         generic-service  ; Inherit values from a template
hostgroup_name      informatica
service_description  Fuente Redundante
check_command       check_snmp!  -C  SACYLCom  -o  .1.3.6.1.4.1.232.6.2.9.1.0  -w  3  -c  4  -l
'Redundant PoWer Supply'
}
define service{
use         generic-service  ; Inherit values from a template
hostgroup_name      informatica
service_description  Temperatura externa
check_command       check_snmp!-C SACYLCom -o .1.3.6.1.4.1.232.6.2.6.1.0 -w 3 -c 4 -l 'external
Temperature'
}

define service{
use         generic-service  ; Inherit values from a template
hostgroup_name      informatica
service_description  Temperatura Interna
check_command       check_snmp!-C SACYLCom -o .1.3.6.1.4.1.232.6.2.6.3.0 -w 3 -c 4 -l 'internal
Temperature'
}

define service{
use         generic-service  ; Inherit values from a template
hostgroup_name      informatica
service_description  Estado Ventilador Sistema
check_command       check_snmp!-C SACYLCom -o .1.3.6.1.4.1.232.6.2.6.4.0 -w 3 -c 4 -l 'System
Fan Status'
}
define service{
use         generic-service  ; Inherit values from a template
hostgroup_name      informatica
service_description  Estado Ventilador CPU
check_command       check_snmp!-C SACYLCom -o .1.3.6.1.4.1.232.6.2.6.5.0 -w 3 -c 4 -l 'CPU Fan
Status'
}

# Create a service for monitoring the System Up Yime
define service{

use         generic-service
hostgroup_name      informatica
```

```
service_description  SNMP SysUpTime
check_command        check_snmp!-C SACYLCom -o .1.3.6.1.2.1.1.3.0 -l 'System Up Time'
}
```

No se han podido realizar todas las pruebas pertinentes, ya que hubiera significado desconectar la alimentación o para los ventiladores de una CPU en servicio.

Respecto al tamaño de disco y otros valores comprobables, la información se corresponde fielmente con la realidad. Existen más plugins en la página de Exchange de Nagios. Muchos de ellos necesitan que en el cliente HPASM esté instalado para que de una respuesta correcta. A continuación se incluye el texto original en inglés describiendo el comando "check_hpasm"[39].

> ***"This plugin monitors the hardware health of HP Proliant Servers, provided that the hpasm (HP Advanced Server Management) software is installed. It is also able to monitor the system health of HP Bladesystems and storage systems.***
>
> ***The components checked for failures and/or operation outside the normal range are CPUs, power supplies, fans, temperatures and memory modules.***
>
> ***The latest release also checks IML log events for memory errors during POST. These are very dangerous: "Memory initialization error... The OS may not have access to all of the memory installed in the system"***

Un resultado de este plugin ejecutado por línea de comandos sería el siguiente:

```
check_hpasm --hostname bladec1 -v
CRITICAL - power supply 1:1:1 is present, condition is failed (Ser: 5AXXD0AHLY403L, FW: )
(SparePartNum 500242-001), power supply 1:1:2 is present, condition is failed (Ser:
5AXXD0AHLY403Y, FW: ) (SparePartNum 500242-001), power supply 1:1:3 is present, condition is
failed (Ser: 5AXXD0AHLY403W, FW: ) (SparePartNum 500242-001), common enclosure KDZ-BC3 condition
is degraded (Ser: GB1147A1WH, FW: 2.60) (SparePartNum 519345-001), power enclosure 1:1 'SDF-BC3'
condition is degraded, System: 'bladesystem c7000 enclosure g2', S/N: 'GB1147A1WH'
common enclosure SDF-BC3 condition is degraded (Ser: GB1147A1WH, FW: 2.60)
fan 1:1:1 is present, location is 1, redundance is other, condition is ok
fan 1:1:10 is present, location is 10, redundance is other, condition is ok
fan 1:1:2 is present, location is 2, redundance is other, condition is ok
fan 1:1:3 is present, location is 3, redundance is other, condition is ok
fan 1:1:4 is present, location is 4, redundance is other, condition is ok
fan 1:1:5 is present, location is 5, redundance is other, condition is ok
fan 1:1:6 is present, location is 6, redundance is other, condition is ok
fan 1:1:7 is present, location is 7, redundance is other, condition is ok
fan 1:1:8 is present, location is 8, redundance is other, condition is ok
fan 1:1:9 is present, location is 9, redundance is other, condition is ok
power enclosure 1:1 'SDF-BC3' condition is degraded
power supply 1:1:1 is present, condition is failed (Ser: 5AXXD0AHLY403L, FW: )
power supply 1:1:1 status is generalFailure, inp.line status is linePowerLoss
power supply 1:1:2 is present, condition is failed (Ser: 5AXXD0AHLY403Y, FW: )
power supply 1:1:2 status is generalFailure, inp.line status is linePowerLoss
power supply 1:1:3 is present, condition is failed (Ser: 5AXXD0AHLY403W, FW: )
power supply 1:1:3 status is generalFailure, inp.line status is linePowerLoss
power supply 1:1:4 is present, condition is ok (Ser: 5AXXD0AHLY403M, FW: )
power supply 1:1:5 is present, condition is ok (Ser: 5AXXD0AHLY404O, FW: )
power supply 1:1:6 is present, condition is ok (Ser: 5AXXD0AHLY403N, FW: )
net connector 1:1:1 is present, model is HP HP VC Flex-10 Enet Module (Ser: TW294123TF, FW: )
net connector 1:1:2 is present, model is HP HP VC Flex-10 Enet Module (Ser: TW294123TL, FW: )
net connector 1:1:3 is present, model is HP HP VC 8Gb 24-Port FC Module (Ser: CN8921D08D, FW: )
net connector 1:1:4 is present, model is HP HP VC 8Gb 24-Port FC Module (Ser: CN8921D087, FW: )
server blade 1:1:1 'linuxbl1' is present, status is value_unknown, powered is value_unknown
server blade 1:1:9 'linuxbl2' is present, status is value_unknown, powered is value_unknown
```

[39] Descargar en: http://labs.consol.de/nagios/check_hpasm/

11. BIBLIOGRAFÍA

[1] The Nagios Exchange. Disponible en:

http://www.nagiosexchange.org

[2] Nagios mailing lists. Disponible en:

http://www.nagios.org/support/mailinglists.php

[3] Multi router traffic grapher (MRTG). Disponible en:

http://www.mrtg.org

[4] Nagios (2nd edition). Wolfgang Barth. Ed. No starch press.

http://nostarch.com/nagios.htm

[5] Learning Nagios 3.0. Wojciech Kocjan. Ed. Packt Publishing.

[6] Nagios Core 3.x Documentation. Disponible en:

http://library.nagios.com/library/products/nagioscore/manuals/

[7] Net-snmp project. Disponible en:

http://net-snmp.sourceforge.net

[8] MIBS de productos CISCO:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

[9] CISCO Object Browser:

http://tools.cisco.com/Support/SNMP/do/BrowseOID.do?local=en

[10] CISCO OIDs por MIB:

ftp://ftp.cisco.com/pub/mibs/oid/

[11] CISCO oid view:

http://www.oidview.com/mibs/9/md-9-1.html

[12] Nagios NCSA:

http://nagios.sourceforge.net/download/contrib/documentation/misc/NSCA_Setup.pdf

[13] VMware Workstation Users Manual. Disponible en:

http://www.vmware.com/support/pubs

[14] VMware vCenter Converter Standalone User's Guide. vCenter Converter Standalone 4.3. Disponible en:

http://www.vmware.com/support/pubs

[15] Guest Operating System Installation Guide. Disponible en:

http://www.vmware.com/support/pubs

[16] VMware Compatibility Guide. Disponible en:

http://www.vmware.com/support/pubs

[17] VMware Workstation 7.1.3 Release Notes

http://www.vmware.com/support/ws71/doc/releasenotes_ws713.html

[18] Nagios plug-in development guidelines

http://nagiosplug.sourceforge.net/developer-guidelines.html

[19] Cisco Unified Serviceability Administration Guide

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/service/7_0_1/admin_master/sadmn.pdf

[20] Cisco IOS Software Configuration Guide for Cisco Aironet Access Points

http://www.cisco.com/en/US/docs/wireless/access_point/12.2_15_JA/configuration/guide/s15pdf.pdf

12. ANEXOS

12.1. ANEXO I: Fichero de configuración switch HP Procurve

```
# Define the switch that we'll be monitoring

define host{
    use             generic-switch          ; Inherit default values from a template
    host_name       swchcuv2176             ; The name we're giving to this switch
    alias           swchcuv2176.hcuv.sacyl.es - HP ProCurve 2650      ;     A     longer     name
associated with the switch
    address         10.40.83.184            ; IP address of the switch
    hostgroups      switches_procurve               ; Host groups this switch is associated
with
    notes_url       http://10.40.83.182
    }

define host{
    use             generic-switch          ; Inherit default values from a template
    host_name       swchcuv2195             ; The name we're giving to this switch
    alias           swchcuv2195.hcuv.sacyl.es - HP ProCurve 2810-24G   ;     A     longer     name
associated with the switch
    address         10.40.83.184            ; IP address of the switch
    hostgroups      switches_procurve       ; Host groups this switch is associated with
    notes_url       http://10.40.83.184
    }


###############################################################################
###############################################################################
#
# SERVICE DEFINITIONS
#
###############################################################################
###############################################################################

# Service definition - HP Procurve Switch - Temperatura CPU
define service{
    use                     generic-service         ; Name of service template to use
    hostgroup_name          switches_procurve
    service_description     CPU Temperatura
    is_volatile             0
    check_period            24x7
    max_check_attempts      3
    normal_check_interval   5
    retry_check_interval    1
#   contact_groups          switch-admins
    notification_interval   240
    notification_period     24x7
    notification_options    c,r
    check_command           check_hptemp!4!3:5
    }

# Service definition CPU Usada
# Define a service to check the CPU consuption
# on HP Procurve Switchs.  Warning if <40% free, critical if < 20% free.
# 'check_snmp_load.pl' command definition
define service{
    use                     generic-service         ; Name of service template to use
    hostgroup_name          switches_procurve
    service_description     CPU Usada
    is_volatile             0
    check_period            24x7
    max_check_attempts      3
    normal_check_interval   5
    retry_check_interval    1
#   contact_groups          switch-admins
    notification_interval   240
    notification_period     24x7
    notification_options    c,r
    check_command           check_snmp_load_v1!hp!60:80!80:100
    }

# Service definition - HP Procurve Switch - Memoria libre
define service{
    use                     generic-service         ; Name of service template to use
    hostgroup_name          switches_procurve
    service_description     Memoria Libre
    is_volatile             0
    check_period            24x7
    max_check_attempts      3
    normal_check_interval   5
    retry_check_interval    1
```

```
#   contact_groups           switch-admins
    notification_interval    240
    notification_period      24x7
    notification_options     c,r
    check_command            check_hpmemoryfree!2000:30000000!1000:30000000
    }

# Create a service to PING to IP host

define service{
    use                      generic-service  ; Inherit values from a template
    hostgroup_name           switches_procurve        ; The name of the host the service is
associated with
    service_description      PING             ; The service description
    check_command            check_ping!200.0,20%!600.0,60%    ; The command used to monitor the
service
    normal_check_interval    1                ; Check the service every 5 minutes under normal
conditions
    retry_check_interval     0.5              ; Re-check the service every minute until its
final/hard state is determined
    }

# Service definition - HP Procurve Switch - Estado Power Supply
define service{
    use                      generic-service          ; Name of service template to use
    hostgroup_name           switches_procurve
    service_description      Power Supply Estado
    is_volatile              0
    check_period             24x7
    max_check_attempts       3
    normal_check_interval    5
    retry_check_interval     1
#   contact_groups           switch-admins
    notification_interval    240
    notification_period      24x7
    notification_options     c,r
    check_command            check_hppower!4!3:5
    }

# Service definition HP Procurver Switch system Description
define service{
    use                      generic-service          ; Name of service template to use
    hostgroup_name           switches_procurve
    service_description      System Description
    is_volatile              0
    check_period             24x7
    max_check_attempts       3
    normal_check_interval    5
    retry_check_interval     1
#   contact_groups           switch-admins
    notification_interval    240
    notification_period      24x7
    notification_options     c,r
    check_command            snmp_sysDescription
    }

  # Monitor SNMP System Up Time
   define command{
    command_name snmp_sysUpTime
    command_line $USER1$/check_snmp -H $HOSTADDRESS$ -C $USER5$ -o .1.3.6.1.2.1.1.3.0 -l 'System
  (SNMP) Up Time'
 }

# Service definition HP Procurver Switch System Location
define service{
    use                      generic-service          ; Name of service template to use
    hostgroup_name           switches_procurve
    service_description      System Location
    is_volatile              0
    check_period             24x7
    max_check_attempts       3
    normal_check_interval    5
    retry_check_interval     1
#   contact_groups           switch-admins
    notification_interval    240
    notification_period      24x7
    notification_options     c,r
    check_command            snmp_sysLocation
    }

# Service definition - HP Procurve Switch - sysUpTime
define service{
    use                      generic-service          ; Name of service template to use
    hostgroup_name           switches_procurve
    service_description      System Up Time
    is_volatile              0
    check_period             24x7
    max_check_attempts       3
```

```
    normal_check_interval    5
    retry_check_interval     1
#   contact_groups           switch-admins
    notification_interval    240
    notification_period      24x7
    notification_options     c,r
    check_command            snmp_sysUpTime
    }

# Service definition - HP Procurve Switch - Estado ventiladores
define service{
    use                      generic-service          ; Name of service template to use
    hostgroup_name           switches_procurve
    service_description      Ventiladores Estado
    is_volatile              0
    check_period             24x7
    max_check_attempts       3
    normal_check_interval    5
    retry_check_interval     1
#   contact_groups           switch-admins
    notification_interval    240
    notification_period      24x7
    notification_options     c,r
    check_command            check_hpfan!4!3:5
    }

###############################################################################
###############################################################################
#
# Command DEFINITIONS
#
###############################################################################
###############################################################################

# Monitor HP Procurve Switch Temperature status
 define command{
  command_name check_hptemp
  command_line      $USER1$/check_snmp      -H      $HOSTADDRESS$      -C      $USER5$      -o
.1.3.6.1.4.1.11.2.14.11.1.2.6.1.4.4 -w $ARG1$ -c $ARG2$ -l 'Temprature status'
 }

# Monitor CPU Load % for several systems
 define command{
  command_name check_snmp_load_v1
    command_line     $USER1$/check_snmp_load.pl -H $HOSTADDRESS$ -C $USER5$ -T $ARG1$ -w $ARG2$
-c $ARG3$ $ARG4$
    ;$ARG1$                          Tipo sistema: netsl - Linux load (1, 5, 15); netsc - Linux
CPU Usage (%)
    ;$ARG1$                          Tipo sistema: hp - Procurve Switch CPU Usage (%); stand -
Windows CPU Usage (%)
    ;$ARG2$                          warning
    ;$ARG3$                          critical
    ;$ARG4$                          optional args
 }

# Monitor HP Procurve Switch Memory free
define command{
  command_name check_hpmemoryfree
  command_line      $USER1$/check_snmp      -H      $HOSTADDRESS$      -C      $USER5$      -o
.1.3.6.1.4.1.11.2.14.11.5.1.1.2.1.1.1.6.1 -t 5 -w $ARG1$ -c $ARG2$ -u megabytes -l 'HP Memory
Free'
 }

# 'check_ping' command definition
define command{
        command_name    check_ping
        command_line    $USER1$/check_ping -H $HOSTADDRESS$ -w $ARG1$ -c $ARG2$ -p 5
        }

# Monitor HP Procurve Switch Power Suply status
 define command{
  command_name check_hppower
  command_line      $USER1$/check_snmp      -H      $HOSTADDRESS$      -C      $USER5$      -o
.1.3.6.1.4.1.11.2.14.11.1.2.6.1.4.2 -w $ARG1$ -c $ARG2$ -l 'Power Supply status'
 }

# Monitor SNMP System Contact
 define command{
  command_name snmp_sysContact
  command_line $USER1$/check_snmp -H $HOSTADDRESS$ -C $USER5$ -o .1.3.6.1.2.1.1.4.0 -l 'System
Contact'
 }

# Monitor SNMP System Decription
 define command{
  command_name snmp_sysDescription
  command_line $USER1$/check_snmp -H $HOSTADDRESS$ -C $USER5$ -o .1.3.6.1.2.1.1.1.0 -l 'System
Description'
```

```
 }

# Monitor SNMP System Location
 define command{
  command_name snmp_sysLocation
  command_line $USER1$/check_snmp -H $HOSTADDRESS$ -C $USER5$ -o .1.3.6.1.2.1.1.6.0 -l 'System
Location'
 }

# Monitor SNMP System Up Time
 define command{
  command_name snmp_sysUpTime
  command_line $USER1$/check_snmp -H $HOSTADDRESS$ -C $USER5$ -o .1.3.6.1.2.1.1.3.0 -l 'System
(SNMP) Up Time'
 }

# Monitor HP Procurve Fan status
 define command{
  command_name check_hpfan
  command_line      $USER1$/check_snmp      -H      $HOSTADDRESS$      -C      $USER5$      -o
.1.3.6.1.4.1.11.2.14.11.1.2.6.1.4.1 -w $ARG1$ -c $ARG2$ -l 'Fan status'
 }
```

12.2. ANEXO II: Fichero de configuración servidores Windows

```
##############################################################################
HOST DEFINITIONS
##############################################################################
# Define a host for the Windows machine we'll be monitoring
# Change the host_name, alias, and address to fit your situation

define host{
use         windows-server   ; Inherit default values from a template
host_name   winserver1       ; The name we're giving to this host
alias               Aplicaciones1    ; A longer name associated with the host
address             10.36.64.85      ; IP address of the host
}
define host {
use         windows-server
host_name   winserver2
alias                Aplicaciones2
address             10.36.64.86
}
##############################################################################
# HOST GROUP DEFINITIONS
##############################################################################
# Define a hostgroup for Windows machines
# All hosts that use the windows-server template will automatically be a member of this group
define hostgroup{
hostgroup_name      windows-servers  ; The name of the hostgroup
alias               Windows Servers  ; Long name of the group
}
define hostgroup {
hostgroup_name      informatica
alias               Informatica
members             winserver1,winserver2
}
##############################################################################
# SERVICE DEFINITIONS
##############################################################################
# Define a service to "ping" the local machine

define service{
use                 generic-service  ; Name of service template to use
hostgroup_name              informatica
service_description         PING
check_command               check_ping!100.0,20%!500.0,60%
}

# Create a service for monitoring the uptime of the server
# Change the host_name to match the name of the host you defined above

define service{
use         generic-service
hostgroup_name      informatica
service_description Uptime
check_command       check_nt!UPTIME
}

# Create a service for monitoring CPU load
# Change the host_name to match the name of the host you defined above

define service{
use         generic-service
hostgroup_name      informatica
service_description CPU Load
check_command       check_nt!CPULOAD!-l 5,80,90
```

```
}
# Create a service for monitoring memory usage
# Change the host_name to match the name of the host you defined above

define service{
use         generic-service
hostgroup_name       informatica
service_description  Memory Usage
check_command        check_nt!MEMUSE!-w 80 -c 90
}
# Create a service for monitoring C:\ disk usage
# Change the host_name to match the name of the host you defined above

define service{
use         generic-service
hostgroup_name       informatica
service_description  C:\ Drive Space
check_command        check_nt!USEDDISKSPACE!-l c -w 80 -c 90
}

define service{
use         generic-service  ; Inherit values from a template
hostgroup_name       informatica
service_description  Fuente Redundante
check_command        check_snmp!  -C  SACYLCom  -o  .1.3.6.1.4.1.232.6.2.9.1.0  -w  3  -c  4  -l
'Redundant PoWer Supply'
}
define service{
use         generic-service  ; Inherit values from a template
hostgroup_name       informatica
service_description  Temperatura externa
check_command        check_snmp!-C SACYLCom -o .1.3.6.1.4.1.232.6.2.6.1.0 -w 3 -c 4 -l 'external
Temperature'
}

define service{
use         generic-service  ; Inherit values from a template
hostgroup_name       informatica
service_description  Temperatura Interna
check_command        check_snmp!-C SACYLCom -o .1.3.6.1.4.1.232.6.2.6.3.0 -w 3 -c 4 -l 'internal
Temperature'
}

define service{
use         generic-service  ; Inherit values from a template
hostgroup_name       informatica
service_description  Estado Ventilador Sistema
check_command        check_snmp!-C SACYLCom -o .1.3.6.1.4.1.232.6.2.6.4.0 -w 3 -c 4 -l 'System
Fan Status'
}
define service{
use         generic-service  ; Inherit values from a template
hostgroup_name       informatica
service_description  Estado Ventilador CPU
check_command        check_snmp!-C SACYLCom -o .1.3.6.1.4.1.232.6.2.6.5.0 -w 3 -c 4 -l 'CPU Fan
Status'
}

# Create a service for monitoring the System Up Yime
define service{

use         generic-service
hostgroup_name       informatica
service_description  SNMP SysUpTime
check_command        check_snmp!-C SACYLCom -o .1.3.6.1.2.1.1.3.0 -l 'System Up Time'
}
```

12.3. Anexo III: Sintaxis comando check_snmp_storage

```
SNMP Disk Monitor for Nagios version 1.3.3
(c)2004-2007 Patrick Proy

Usage: check_snmp_storage [-v] -H <host> -C <snmp_community> [-2] | (-l login -x passwd [-X pass
-L <authp>,<privp>]) [-p <port>] -m <name in desc_oid> [-q storagetype] -w <warn_level> -c
<crit_level> [-t <timeout>] [-T pl|pu|bl|bu ] [-r -s -i -G] [-e] [-S 0|1[,1,<car>]] [-o
<octet_length>] [-R <% reserved>]
By default, plugin will monitor %used on drives :
warn if %used > warn and critical if %used > crit
-v, --verbose
   print extra debugging information (and lists all storages)
-h, --help
   print this help message
-H, --hostname=HOST
   name or IP address of host to check
-C, --community=COMMUNITY NAME
   community name for the host's SNMP agent (implies SNMP v1)
-2, --v2c
```

```
   Use snmp v2c
-l, --login=LOGIN ; -x, --passwd=PASSWD
   Login and auth password for snmpv3 authentication
   If no priv password exists, implies AuthNoPriv
-X, --privpass=PASSWD
   Priv password for snmpv3 (AuthPriv protocol)
-L, --protocols=<authproto>,<privproto>
   <authproto> : Authentication protocol (md5|sha : default md5)
   <privproto> : Priv protocole (des|aes : default des)
-x, --passwd=PASSWD
   Password for snmpv3 authentication
-p, --port=PORT
   SNMP port (Default 161)
-m, --name=NAME
   Name in description OID (can be mounpoints '/home' or 'Swap Space'...)
   This is treated as a regexp : -m /var will match /var , /var/log, /opt/var ...
   Test it before, because there are known bugs (ex : trailling /)
   No trailing slash for mountpoints !
-q, --storagetype=[Other|Ram|VirtualMemory|FixedDisk|RemovableDisk|FloppyDisk
                   CompactDisk|RamDisk|FlashMemory|NetworkDisk]
   Also check the storage type in addition of the name
   It is possible to use regular expressions ( "FixedDisk|FloppyDisk" )
-r, --noregexp
   Do not use regexp to match NAME in description OID
-s, --sum
   Add all storages that match NAME (used space and total space)
   THEN make the tests.
-i, --index
   Parse index table instead of description table to select storage
-e, --exclude
   Select all storages except the one(s) selected by -m
   No action on storage type selection
-T, --type=TYPE
   pl : calculate percent left
   pu : calculate percent used (Default)
   bl : calculate MegaBytes left
   bu : calculate MegaBytes used
-w, --warn=INTEGER
   percent / MB of disk used to generate WARNING state
   you can add the % sign
-c, --critical=INTEGER
   percent / MB of disk used to generate CRITICAL state
   you can add the % sign
-R, --reserved=INTEGER
   % reserved blocks for superuser
   For ext2/3 filesystems, it is 5% by default
-G, --gigabyte
   output, warning & critical levels in gigabytes
-f, --perfparse
   Perfparse compatible output
-S, --short=<type>[,<where>,<cut>]
   <type>: Make the output shorter :
     0 : only print the global result except the disk in warning or critical
         ex: "< 80% : OK"
     1 : Don't print all info for every disk
         ex : "/ : 66 %used  (<  80) : OK"
   <where>: (optional) if = 1, put the OK/WARN/CRIT at the beginning
   <cut>: take the <n> first caracters or <n> last if n<0
-o, --octetlength=INTEGER
  max-size of the SNMP message, usefull in case of Too Long responses.
  Be carefull with network filters. Range 484 - 65535, default are
  usually 1472,1452,1460 or 1440.
-t, --timeout=INTEGER
   timeout for SNMP in seconds (Default: 5)
-V, --version
   prints version number
Note :
  with T=pu or T=bu : OK < warn < crit
  with T=pl ot T=bl : crit < warn < OK

  If multiple storage are selected, the worse condition will be returned
  i.e if one disk is critical, the return is critical

  example :
  Browse storage list : <script> -C <community> -H <host> -m <anything> -w 1 -c 2 -v
  the -m option allows regexp in perl format :
  Test drive C,F,G,H,I on Windows       : -m ^[CFGHI]:
  Test all mounts containing /var       : -m /var
  Test all mounts under /var            : -m ^/var
  Test only /var                        : -m /var -r
  Test all swap spaces                  : -m ^Swap
  Test all but swap spaces              : -m ^Swap -e
```

12.4. Anexo IV: Sintaxis commando check_snmp_process

```
SNMP Process Monitor for Nagios version 1.10
GPL licence, (c)2004-2006 Patrick Proy
```

```
Usage: ./check_snmp_process.pl [-v] -H <host> -C <snmp_community> [-2] | (-l login -x passwd) [-
p <port>] -n <name> [-w <min_proc>[,<max_proc>] -c <min_proc>[,max_proc] ] [-m<warn Mb>,<crit
Mb> -a -u<warn %>,<crit%> -d<delta> ] [-t <timeout>] [-o <octet_length>] [-f -A -F ] [-r] [-V]
[-g]
-v, --verbose
   print extra debugging information (and lists all storages)
-h, --help
   print this help message
-H, --hostname=HOST
   name or IP address of host to check
-C, --community=COMMUNITY NAME
   community name for the host's SNMP agent (implies SNMP v1 or v2c with option)
-l, --login=LOGIN ; -x, --passwd=PASSWD, -2, --v2c
   Login and auth password for snmpv3 authentication
   If no priv password exists, implies AuthNoPriv
   -2 : use snmp v2c
-X, --privpass=PASSWD
   Priv password for snmpv3 (AuthPriv protocol)
-L, --protocols=<authproto>,<privproto>
   <authproto> : Authentication protocol (md5|sha : default md5)
   <privproto> : Priv protocole (des|aes : default des)
-p, --port=PORT
   SNMP port (Default 161)
-n, --name=NAME
   Name of the process (regexp)
   No trailing slash !
-r, --noregexp
   Do not use regexp to match NAME in description OID
-f, --fullpath
   Use full path name instead of process name
   (Windows doesn't provide full path name)
-A, --param
   Add parameters to select processes.
   ex : "named.*-t /var/named/chroot" will only select named process with this parameter
-F, --perfout
   Add performance output
   outputs : memory_usage, num_process, cpu_usage
-w, --warn=MIN[,MAX]
   Number of process that will cause a warning
   -1 for no warning, MAX must be >0. Ex : -w-1,50
-c, --critical=MIN[,MAX]
   number of process that will cause an error (
   -1 for no critical, MAX must be >0. Ex : -c-1,50
Notes on warning and critical :
   with the following options : -w m1,x1 -c m2,x2
   you must have : m2 <= m1 < x1 <= x2
   you can omit x1 or x2 or both
-m, --memory=WARN,CRIT
   checks memory usage (default max of all process)
   values are warning and critical values in Mb
-a, --average
   makes an average of memory used by process instead of max
-u, --cpu=WARN,CRIT
   checks cpu usage of all process
   values are warning and critical values in % of CPU usage
   if more than one CPU, value can be > 100% : 100%=1 CPU
-d, --delta=seconds
   make an average of <delta> seconds for CPU (default 300=5min)
-g, --getall
  In some cases, it is necessary to get all data at once because
  process die very frequently.
  This option eats bandwidth an cpu (for remote host) at breakfast.
-o, --octetlength=INTEGER
  max-size of the SNMP message, usefull in case of Too Long responses.
  Be carefull with network filters. Range 484 - 65535, default are
  usually 1472,1452,1460 or 1440.
-t, --timeout=INTEGER
   timeout for SNMP in seconds (Default: 5)
-V, --version
   prints version number
Note :
  CPU usage is in % of one cpu, so maximum can be 100% * number of CPU
  example :
  Browse process list : <script> -C <community> -H <host> -n <anything> -v
  the -n option allows regexp in perl format :
  All process of /opt/soft/bin          : -n /opt/soft/bin/ -f
  All 'named' process                   : -n named
```

12.5. ANEXO V: RFCs relacionadas con SNMP

Number	Title	Author or Ed.	Date	Format	More Info (Obs&Upd)	Status
STD0062 RFC3411	**An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks**	D. Harrington, R. Presuhn, B. Wijnen	December 2002	ASCII	Obsoletes RFC2571, Updated by RFC5343, RFC5590	STANDARD
STD0062 RFC3412	**Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)**	J. Case, D. Harrington, R. Presuhn, B. Wijnen	December 2002	ASCII	Obsoletes RFC2572, Updated by RFC5590	STANDARD
STD0062 RFC3413	**Simple Network Management Protocol (SNMP) Applications**	D. Levi, P. Meyer, B. Stewart	December 2002	ASCII	Obsoletes RFC2573	STANDARD
STD0062 RFC3414	**User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)**	U. Blumenthal, B. Wijnen	December 2002	ASCII	Obsoletes RFC2574, Updated by RFC5590	STANDARD
STD0062 RFC3415	**View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)**	B. Wijnen, R. Presuhn, K. McCloghrie	December 2002	ASCII	Obsoletes RFC2575	STANDARD
STD0062 RFC3416	**Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)**	R. Presuhn, Ed.	December 2002	ASCII	Obsoletes RFC1905	STANDARD
STD0062 RFC3417	**Transport Mappings for the Simple Network Management Protocol (SNMP)**	R. Presuhn, Ed.	December 2002	ASCII	Obsoletes RFC1906, Updated by RFC4789, RFC5590	STANDARD
STD0062 RFC3418	**Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)**	R. Presuhn, Ed.	December 2002	ASCII	Obsoletes RFC1907	STANDARD
STD0050	**[Reserved for Definitions of Managed Objects for the Ethernet-like Interface Types. See RFC 3638.]**			ASCII	Errata	STD

Number	Title	Author or Ed.	Date	Format	More Info (Obs&Upd)	Status
RFC6353	**Transport Layer Security (TLS) Transport Model for the Simple Network Management Protocol (SNMP)**	W. Hardaker	July 2011	ASCII	Obsoletes RFC5953	DRAFT STANDARD
RFC5953	**Transport Layer Security (TLS) Transport Model for the Simple Network Management Protocol (SNMP)**	W. Hardaker	August 2010	ASCII	Obsoleted by RFC6353 Errata	PROPOSED STANDARD
RFC5935	**Expressing SNMP SMI Datatypes in XML Schema Definition Language**	M. Ellison, B. Natale	August 2010	ASCII	Errata	PROPOSED STANDARD
RFC5676	**Definitions of Managed Objects for Mapping SYSLOG Messages to Simple Network Management Protocol (SNMP) Notifications**	J. Schoenwaelder, A. Clemm, A. Karmakar	October 2009	ASCII	Errata	PROPOSED STANDARD
RFC5675	**Mapping Simple Network Management Protocol (SNMP) Notifications to SYSLOG Messages**	V. Marinov, J. Schoenwaelder	October 2009	ASCII		PROPOSED STANDARD
RFC5608	**Remote Authentication Dial-In User Service (RADIUS) Usage for Simple Network Management Protocol (SNMP) Transport Models**	K. Narayan, D. Nelson	August 2009	ASCII	Errata	PROPOSED STANDARD
RFC5607	**Remote Authentication Dial-In User Service (RADIUS) Authorization for Network Access Server (NAS) Management**	D. Nelson, G. Weber	July 2009	ASCII		PROPOSED STANDARD
RFC5592	**Secure Shell Transport Model for the Simple Network Management Protocol (SNMP)**	D. Harrington, J. Salowey, W. Hardaker	June 2009	ASCII		PROPOSED STANDARD
RFC5591	**Transport Security Model for the Simple Network Management Protocol (SNMP)**	D. Harrington, W. Hardaker	June 2009	ASCII		DRAFT STANDARD [pub as:PROPOSED STANDARD]

Number	Title	Author or Ed.	Date	Format	More Info (Obs&Upd)	Status
RFC5590	**Transport Subsystem for the Simple Network Management Protocol (SNMP)**	D. Harrington, J. Schoenwaelder	June 2009	ASCII	Updates RFC3411, RFC3412, RFC3414, RFC3417	DRAFT STANDARD [pub as:PROPOSED STANDARD]
RFC5428	**Management Event Management Information Base (MIB) for PacketCable- and IPCablecom-Compliant Devices**	S. Channabasappa, W. De Ketelaere, E. Nechamkin	April 2009	ASCII		PROPOSED STANDARD
RFC5345	**Simple Network Management Protocol (SNMP) Traffic Measurements and Trace Exchange Formats**	J. Schoenwaelder	October 2008	ASCII	Errata	INFORMATIONAL
RFC5343	**Simple Network Management Protocol (SNMP) Context EngineID Discovery**	J. Schoenwaelder	September 2008	ASCII	Updates RFC3411	DRAFT STANDARD [pub as:PROPOSED STANDARD]
RFC5098	**Signaling MIB for PacketCable and IPCablecom Multimedia Terminal Adapters (MTAs)**	G. Beacham, S. Kumar, S. Channabasappa	February 2008	ASCII	Errata	PROPOSED STANDARD
RFC5066	**Ethernet in the First Mile Copper (EFMCu) Interfaces MIB**	E. Beili	November 2007	ASCII		PROPOSED STANDARD
RFC4878	**Definitions and Managed Objects for Operations, Administration, and Maintenance (OAM) Functions on Ethernet-Like Interfaces**	M. Squire	June 2007	ASCII		PROPOSED STANDARD
RFC4789	**Simple Network Management Protocol (SNMP) over IEEE 802 Networks**	J. Schoenwaelder, T. Jeffree	November 2006	ASCII	Obsoletes RFC1089, Updates RFC3417	PROPOSED STANDARD
RFC4712	**Transport Mappings for Real-time Application Quality-of-Service Monitoring (RAQMON) Protocol Data Unit (PDU)**	A. Siddiqui, D. Romascanu, E. Golovinsky, M. Rahman,Y. Kim	October 2006	ASCII		PROPOSED STANDARD

Number	Title	Author or Ed.	Date	Format	More Info (Obs&Upd)	Status
RFC4710	**Real-time Application Quality-of-Service Monitoring (RAQMON) Framework**	A. Siddiqui, D. Romascanu, E. Golovinsky	October 2006	ASCII		PROPOSED STANDARD
RFC4682	**Multimedia Terminal Adapter (MTA) Management Information Base for PacketCable- and IPCablecom-Compliant Devices**	E. Nechamkin, J-F. Mule	December 2006	ASCII		PROPOSED STANDARD
RFC4639	**Cable Device Management Information Base for Data-Over-Cable Service Interface Specification (DOCSIS) Compliant Cable Modems and Cable Modem Termination Systems**	R. Woundy, K. Marez	December 2006	ASCII	Obsoletes RFC2669	PROPOSED STANDARD
RFC4547	**Event Notification Management Information Base for Data over Cable Service Interface Specifications (DOCSIS)-Compliant Cable Modems and Cable Modem Termination Systems**	A. Ahmad, G. Nakanishi	June 2006	ASCII		PROPOSED STANDARD
RFC4545	**Definitions of Managed Objects for IP Storage User Identity Authorization**	M. Bakke, J. Muchow	May 2006	ASCII	Errata	PROPOSED STANDARD
RFC4441	**The IEEE 802/IETF Relationship**	B. Aboba, Ed.	March 2006	ASCII		INFORMATIONAL
RFC4369	**Definitions of Managed Objects for Internet Fibre Channel Protocol (iFCP)**	K. Gibbons, C. Monia, J. Tseng, F. Travostino	January 2006	ASCII	Obsoleted by RFC6173	PROPOSED STANDARD
RFC4323	**Data Over Cable System Interface Specification Quality of Service Management Information Base (DOCSIS-QoS MIB)**	M. Patrick, W. Murwin	January 2006	ASCII		PROPOSED STANDARD
RFC4268	**Entity State MIB**	S. Chisholm, D. Perkins	November 2005	ASCII	Errata	PROPOSED STANDARD

Number	Title	Author or Ed.	Date	Format	More Info (Obs&Upd)	Status
RFC4188	**Definitions of Managed Objects for Bridges**	K. Norseth, Ed., E. Bell, Ed.	September 2005	ASCII	Obsoletes RFC1493 Errata	PROPOSED STANDARD
RFC4133	**Entity MIB (Version 3)**	A. Bierman, K. McCloghrie	August 2005	ASCII	Obsoletes RFC2737 Errata	PROPOSED STANDARD
RFC4131	**Management Information Base for Data Over Cable Service Interface Specification (DOCSIS) Cable Modems and Cable Modem Termination Systems for Baseline Privacy Plus**	S. Green, K. Ozawa, E. Cardona, Ed., A. Katsnelson	September 2005	ASCII		PROPOSED STANDARD
RFC4097	**Middlebox Communications (MIDCOM) Protocol Evaluation**	M. Barnes, Ed.	June 2005	ASCII		INFORMATIONAL
RFC4088	**Uniform Resource Identifier (URI) Scheme for the Simple Network Management Protocol (SNMP)**	D. Black, K. McCloghrie, J. Schoenwaelder	June 2005	ASCII		PROPOSED STANDARD
RFC4036	**Management Information Base for Data Over Cable Service Interface Specification (DOCSIS) Cable Modem Termination Systems for Subscriber Management**	W. Sawyer	April 2005	ASCII		PROPOSED STANDARD
RFC4011	**Policy Based Management MIB**	S. Waldbusser, J. Saperia, T. Hongal	March 2005	ASCII		PROPOSED STANDARD
RFC3826	**The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model**	U. Blumenthal, F. Maino, K. McCloghrie	June 2004	ASCII		PROPOSED STANDARD
RFC3806	**Printer Finishing MIB**	R. Bergman, H. Lewis, I. McDonald	June 2004	ASCII		INFORMATIONAL
RFC3805	**Printer MIB v2**	R. Bergman, H. Lewis, I. McDonald	June 2004	ASCII	Obsoletes RFC1759	PROPOSED STANDARD

Number	Title	Author or Ed.	Date	Format	More Info (Obs&Upd)	Status
RFC3781	**Next Generation Structure of Management Information (SMIng) Mappings to the Simple Network Management Protocol (SNMP)**	F. Strauss, J. Schoenwaelder	May 2004	ASCII	Errata	EXPERIMENTAL
RFC3638	**Applicability Statement for Reclassification of RFC 1643 to Historic Status**	J. Flick, C. M. Heard	September 2003	ASCII	Obsoletes RFC1643	INFORMATIONAL
RFC3592	**Definitions of Managed Objects for the Synchronous Optical Network/Synchronous Digital Hierarchy (SONET/SDH) Interface Type**	K. Tesink	September 2003	ASCII	Obsoletes RFC2558	DRAFT STANDARD
RFC3591	**Definitions of Managed Objects for the Optical Interface Type**	H-K. Lam, M. Stewart, A. Huynh	September 2003	ASCII	Errata	PROPOSED STANDARD
RFC3584 BCP0074	**Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework**	R. Frye, D. Levi, S. Routhier, B. Wijnen	August 2003	ASCII	Obsoletes RFC2576	BEST CURRENT PRACTICE
RFC3512	**Configuring Networks and Devices with Simple Network Management Protocol (SNMP)**	M. MacFaden, D. Partain, J. Saperia, W. Tackabury	April 2003	ASCII		INFORMATIONAL
RFC3434	**Remote Monitoring MIB Extensions for High Capacity Alarms**	A. Bierman, K. McCloghrie	December 2002	ASCII		PROPOSED STANDARD
RFC3433	**Entity Sensor Management Information Base**	A. Bierman, D. Romascanu, K.C. Norseth	December 2002	ASCII	Errata	PROPOSED STANDARD
RFC3430	**Simple Network Management Protocol Over Transmission Control Protocol Transport Mapping**	J. Schoenwaelder	December 2002	ASCII		EXPERIMENTAL
RFC3410	**Introduction and Applicability Statements for Internet-Standard Management Framework**	J. Case, R. Mundy, D. Partain, B. Stewart	December 2002	ASCII	Obsoletes RFC2570 Errata	INFORMATIONAL

Number	Title	Author or Ed.	Date	Format	More Info (Obs&Upd)	Status
RFC3216	**SMIng Objectives**	C. Elliott, D. Harrington, J. Jason, J. Schoenwaelder, F. Strauss, W. Weiss	December 2001	ASCII		INFORMATIONAL
RFC3159	**Structure of Policy Provisioning Information (SPPI)**	K. McCloghrie, M. Fine, J. Seligson, K. Chan, S. Hahn, R. Sahita, A. Smith, F. Reichmeyer	August 2001	ASCII		PROPOSED STANDARD
RFC2962	**An SNMP Application Level Gateway for Payload Address Translation**	D. Raz, J. Schoenwaelder, B. Sugla	October 2000	ASCII		INFORMATIONAL
RFC2856	**Textual Conventions for Additional High Capacity Data Types**	A. Bierman, K. McCloghrie, R. Presuhn	June 2000	ASCII		PROPOSED STANDARD
RFC2742	**Definitions of Managed Objects for Extensible SNMP Agents**	L. Heintz, S. Gudur, M. Ellison	January 2000	ASCII		DRAFT STANDARD [pub as:PROPOSED STANDARD]
RFC2741	**Agent Extensibility (AgentX) Protocol Version 1**	M. Daniele, B. Wijnen, M. Ellison, D. Francisco	January 2000	ASCII	Obsoletes RFC2257	DRAFT STANDARD [pub as:PROPOSED STANDARD]
RFC2737	**Entity MIB (Version 2)**	K. McCloghrie, A. Bierman	December 1999	ASCII	Obsoletes RFC2037, Obsoleted by RFC4133 Errata	PROPOSED STANDARD
RFC2576	**Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework**	R. Frye, D. Levi, S. Routhier, B. Wijnen	March 2000	ASCII	Obsoletes RFC1908, RFC2089, Obsoleted by RFC3584 Errata	PROPOSED STANDARD
RFC2575	**View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)**	B. Wijnen, R. Presuhn, K. McCloghrie	April 1999	ASCII	Obsoletes RFC2275, Obsoleted by RFC3415	DRAFT STANDARD
RFC2574	**User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)**	U. Blumenthal, B. Wijnen	April 1999	ASCII	Obsoletes RFC2274, Obsoleted by RFC3414	DRAFT STANDARD

Number	Title	Author or Ed.	Date	Format	More Info (Obs&Upd)	Status
RFC2573	**SNMP Applications**	D. Levi, P. Meyer, B. Stewart	April 1999	ASCII	Obsoletes RFC2273, Obsoleted by RFC3413	DRAFT STANDARD
RFC2572	**Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)**	J. Case, D. Harrington, R. Presuhn, B. Wijnen	April 1999	ASCII	Obsoletes RFC2272, Obsoleted by RFC3412	DRAFT STANDARD
RFC2571	**An Architecture for Describing SNMP Management Frameworks**	B. Wijnen, D. Harrington, R. Presuhn	April 1999	ASCII	Obsoletes RFC2271, Obsoleted by RFC3411	DRAFT STANDARD
RFC2570	**Introduction to Version 3 of the Internet-standard Network Management Framework**	J. Case, R. Mundy, D. Partain, B. Stewart	April 1999	ASCII	Obsoleted by RFC3410	INFORMATIONAL
RFC2558	**Definitions of Managed Objects for the SONET/SDH Interface Type**	K. Tesink	March 1999	ASCII	Obsoletes RFC1595, Obsoleted by RFC3592	PROPOSED STANDARD
RFC2275	**View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)**	B. Wijnen, R. Presuhn, K. McCloghrie	January 1998	ASCII	Obsoletes RFC2265, Obsoleted by RFC2575	PROPOSED STANDARD
RFC2274	**User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)**	U. Blumenthal, B. Wijnen	January 1998	ASCII	Obsoletes RFC2264, Obsoleted by RFC2574	PROPOSED STANDARD
RFC2273	**SNMPv3 Applications**	D. Levi, P. Meyer, B. Stewart	January 1998	ASCII	Obsoletes RFC2263, Obsoleted by RFC2573	PROPOSED STANDARD
RFC2272	**Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)**	J. Case, D. Harrington, R. Presuhn, B. Wijnen	January 1998	ASCII	Obsoletes RFC2262, Obsoleted by RFC2572	PROPOSED STANDARD
RFC2271	**An Architecture for Describing SNMP Management Frameworks**	D. Harrington, R. Presuhn, B. Wijnen	January 1998	ASCII	Obsoletes RFC2261, Obsoleted by RFC2571	PROPOSED STANDARD

Number	Title	Author or Ed.	Date	Format	More Info (Obs&Upd)	Status
RFC2265	**View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)**	B. Wijnen, R. Presuhn, K. McCloghrie	January 1998	ASCII	Obsoleted by RFC2275	PROPOSED STANDARD
RFC2264	**User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)**	U. Blumenthal, B. Wijnen	January 1998	ASCII	Obsoleted by RFC2274	PROPOSED STANDARD
RFC2263	**SNMPv3 Applications**	D. Levi, P. Meyer, B. Stewart	January 1998	ASCII	Obsoleted by RFC2273	PROPOSED STANDARD
RFC2262	**Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)**	J. Case, D. Harrington, R. Presuhn, B. Wijnen	January 1998	ASCII	Obsoleted by RFC2272	PROPOSED STANDARD
RFC2261	**An Architecture for Describing SNMP Management Frameworks**	D. Harrington, R. Presuhn, B. Wijnen	January 1998	ASCII	Obsoleted by RFC2271	PROPOSED STANDARD
RFC2257	**Agent Extensibility (AgentX) Protocol Version 1**	M. Daniele, B. Wijnen, D. Francisco	January 1998	ASCII	Obsoleted by RFC2741	PROPOSED STANDARD
RFC2248	**Network Services Monitoring MIB**	N. Freed, S. Kille	January 1998	ASCII	Obsoletes RFC1565, Obsoleted by RFC2788	PROPOSED STANDARD
RFC2089	**V2ToV1 Mapping SNMPv2 onto SNMPv1 within a bi-lingual SNMP agent**	B. Wijnen, D. Levi	January 1997	ASCII	Obsoleted by RFC2576	INFORMATIONAL
RFC2037	**Entity MIB using SMIv2**	K. McCloghrie, A. Bierman	October 1996	ASCII	Obsoleted by RFC2737	PROPOSED STANDARD
RFC2013	**SNMPv2 Management Information Base for the User Datagram Protocol using SMIv2**	K. McCloghrie, Ed.	November 1996	ASCII	Obsoleted by RFC4113, Updates RFC1213	PROPOSED STANDARD
RFC2012	**SNMPv2 Management Information Base for the Transmission Control Protocol using SMIv2**	K. McCloghrie, Ed.	November 1996	ASCII	Obsoleted by RFC4022, Updates RFC1213	PROPOSED STANDARD

Number	Title	Author or Ed.	Date	Format	More Info (Obs&Upd)	Status
RFC2011	**SNMPv2 Management Information Base for the Internet Protocol using SMIv2**	K. McCloghrie, Ed.	November 1996	ASCII	Obsoleted by RFC4293, Updates RFC1213	PROPOSED STANDARD
RFC1910	**User-based Security Model for SNMPv2**	G. Waters, Ed.	February 1996	ASCII		HISTORIC [pub as:EXPERIMENTAL]
RFC1909	**An Administrative Infrastructure for SNMPv2**	K. McCloghrie, Ed.	February 1996	ASCII		HISTORIC [pub as:EXPERIMENTAL]
RFC1907	**Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)**	J. Case, K. McCloghrie, M. Rose, S. Waldbusser	January 1996	ASCII	Obsoletes RFC1450, Obsoleted by RFC3418	DRAFT STANDARD
RFC1906	**Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2)**	J. Case, K. McCloghrie, M. Rose, S. Waldbusser	January 1996	ASCII	Obsoletes RFC1449, Obsoleted by RFC3417	DRAFT STANDARD
RFC1905	**Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)**	J. Case, K. McCloghrie, M. Rose, S. Waldbusser	January 1996	ASCII	Obsoletes RFC1448, Obsoleted by RFC3416	DRAFT STANDARD
RFC1904	**Conformance Statements for Version 2 of the Simple Network Management Protocol (SNMPv2)**	J. Case, K. McCloghrie, M. Rose, S. Waldbusser	January 1996	ASCII	Obsoletes RFC1444, Obsoleted by RFC2580	DRAFT STANDARD
RFC1903	**Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2)**	J. Case, K. McCloghrie, M. Rose, S. Waldbusser	January 1996	ASCII	Obsoletes RFC1443, Obsoleted by RFC2579	DRAFT STANDARD
RFC1902	**Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2)**	J. Case, K. McCloghrie, M. Rose, S. Waldbusser	January 1996	ASCII	Obsoletes RFC1442, Obsoleted by RFC2578	DRAFT STANDARD
RFC1901	**Introduction to Community-based SNMPv2**	J. Case, K. McCloghrie, M. Rose, S. Waldbusser	January 1996	ASCII		HISTORIC [pub as:EXPERIMENTAL]
RFC1749	**IEEE 802.5 Station Source Routing MIB using SMIv2**	K. McCloghrie, F. Baker, E. Decker	December 1994	ASCII	Updates RFC1748	HISTORIC [pub as:PROPOSED STANDARD]

Number	Title	Author or Ed.	Date	Format	More Info (Obs&Upd)	Status
RFC1748	**IEEE 802.5 MIB using SMIv2**	K. McCloghrie, E. Decker	December 1994	ASCII	Obsoletes RFC1743, RFC1231, Updated by RFC1749	DRAFT STANDARD
RFC1743	**IEEE 802.5 MIB using SMIv2**	K. McCloghrie, E. Decker	December 1994	ASCII	Obsoletes RFC1231, Obsoleted by RFC1748	DRAFT STANDARD
RFC1666	**Definitions of Managed Objects for SNA NAUs using SMIv2**	Z. Kielczewski, D. Kostick, K. Shih, Eds.	August 1994	ASCII	Obsoletes RFC1665	HISTORIC [pub as:PROPOSED STANDARD]
RFC1643	**Definitions of Managed Objects for the Ethernet-like Interface Types**	F. Kastenholz	July 1994	ASCII	Obsoletes RFC1623, Obsoleted by RFC3638	HISTORIC [pub as:STANDARD]
RFC1604	**Definitions of Managed Objects for Frame Relay Service**	T. Brown, Ed.	March 1994	ASCII	Obsoletes RFC1596, Obsoleted by RFC2954	PROPOSED STANDARD
RFC1596	**Definitions of Managed Objects for Frame Relay Service**	T. Brown, Ed.	March 1994	ASCII	Obsoleted by RFC1604	PROPOSED STANDARD
RFC1595	**Definitions of Managed Objects for the SONET/SDH Interface Type**	T. Brown, K. Tesink	March 1994	ASCII	Obsoleted by RFC2558	PROPOSED STANDARD
RFC1592	**Simple Network Management Protocol Distributed Protocol Interface Version 2.0**	B. Wijnen, G. Carpenter, K. Curran, A. Sehgal, G. Waters	March 1994	ASCII	Obsoletes RFC1228	EXPERIMENTAL
RFC1559	**DECnet Phase IV MIB Extensions**	J. Saperia	December 1993	ASCII	Obsoletes RFC1289	DRAFT STANDARD
RFC1525	**Definitions of Managed Objects for Source Routing Bridges**	E. Decker, K. McCloghrie, P. Langille, A. Rijsinghani	September 1993	ASCII	Obsoletes RFC1286	HISTORIC [pub as:PROPOSED STANDARD]
RFC1516	**Definitions of Managed Objects for IEEE 802.3 Repeater Devices**	D. McMaster, K. McCloghrie	September 1993	ASCII	Obsoletes RFC1368, Obsoleted by RFC2108	DRAFT STANDARD

Number	Title	Author or Ed.	Date	Format	More Info (Obs&Upd)	Status
RFC1515	**Definitions of Managed Objects for IEEE 802.3 Medium Attachment Units (MAUs)**	D. McMaster, K. McCloghrie, S. Roberts	September 1993	ASCII	Obsoleted by RFC3636	PROPOSED STANDARD
RFC1514	**Host Resources MIB**	P. Grillo, S. Waldbusser	September 1993	ASCII	Obsoleted by RFC2790	PROPOSED STANDARD
RFC1513	**Token Ring Extensions to the Remote Network Monitoring MIB**	S. Waldbusser	September 1993	ASCII	Updates RFC1271	HISTORIC [pub as:PROPOSED STANDARD]
RFC1512	**FDDI Management Information Base**	J. Case, A. Rijsinghani	September 1993	ASCII	Updates RFC1285	HISTORIC [pub as:PROPOSED STANDARD]
RFC1503	**Algorithms for Automating Administration in SNMPv2 Managers**	K. McCloghrie, M. Rose	August 1993	ASCII		INFORMATIONAL
RFC1493	**Definitions of Managed Objects for Bridges**	E. Decker, P. Langille, A. Rijsinghani, K. McCloghrie	July 1993	ASCII	Obsoletes RFC1286, Obsoleted by RFC4188	DRAFT STANDARD
RFC1461	**SNMP MIB extension for Multiprotocol Interconnect over X.25**	D. Throop	May 1993	ASCII		HISTORIC [pub as:PROPOSED STANDARD]
RFC1452	**Coexistence between version 1 and version 2 of the Internet-standard Network Management Framework**	J. Case, K. McCloghrie, M. Rose, S. Waldbusser	April 1993	ASCII	Obsoleted by RFC1908	PROPOSED STANDARD
RFC1451	**Manager-to-Manager Management Information Base**	J. Case, K. McCloghrie, M. Rose, S. Waldbusser	April 1993	ASCII		HISTORIC
RFC1450	**Management Information Base for version 2 of the Simple Network Management Protocol (SNMPv2)**	J. Case, K. McCloghrie, M. Rose, S. Waldbusser	April 1993	ASCII	Obsoleted by RFC1907	PROPOSED STANDARD
RFC1449	**Transport Mappings for version 2 of the Simple Network Management Protocol (SNMPv2)**	J. Case, K. McCloghrie, M. Rose, S. Waldbusser	April 1993	ASCII	Obsoleted by RFC1906	PROPOSED STANDARD

Number	Title	Author or Ed.	Date	Format	More Info (Obs&Upd)	Status
RFC1448	**Protocol Operations for version 2 of the Simple Network Management Protocol (SNMPv2)**	J. Case, K. McCloghrie, M. Rose, S. Waldbusser	April 1993	ASCII	Obsoleted by RFC1905	PROPOSED STANDARD
RFC1447	**Party MIB for version 2 of the Simple Network Management Protocol (SNMPv2)**	K. McCloghrie, J. Galvin	April 1993	ASCII		HISTORIC
RFC1446	**Security Protocols for version 2 of the Simple Network Management Protocol (SNMPv2)**	J. Galvin, K. McCloghrie	April 1993	ASCII		HISTORIC
RFC1445	**Administrative Model for version 2 of the Simple Network Management Protocol (SNMPv2)**	J. Galvin, K. McCloghrie	April 1993	ASCII		HISTORIC
RFC1444	**Conformance Statements for version 2 of the Simple Network Management Protocol (SNMPv2)**	J. Case, K. McCloghrie, M. Rose, S. Waldbusser	April 1993	ASCII	Obsoleted by RFC1904	PROPOSED STANDARD
RFC1443	**Textual Conventions for version 2 of the Simple Network Management Protocol (SNMPv2)**	J. Case, K. McCloghrie, M. Rose, S. Waldbusser	April 1993	ASCII	Obsoleted by RFC1903	PROPOSED STANDARD
RFC1442	**Structure of Management Information for version 2 of the Simple Network Management Protocol (SNMPv2)**	J. Case, K. McCloghrie, M. Rose, S. Waldbusser	April 1993	ASCII	Obsoleted by RFC1902	PROPOSED STANDARD
RFC1441	**Introduction to version 2 of the Internet-standard Network Management Framework**	J. Case, K. McCloghrie, M. Rose, S. Waldbusser	April 1993	ASCII		HISTORIC [pub as:PROPOSED STANDARD]
RFC1420	**SNMP over IPX**	S. Bostock	March 1993	ASCII	Obsoletes RFC1298	PROPOSED STANDARD
RFC1419	**SNMP over AppleTalk**	G. Minshall, M. Ritter	March 1993	ASCII		HISTORIC [pub as:PROPOSED STANDARD]
RFC1418	**SNMP over OSI**	M. Rose	March 1993	ASCII	Obsoletes RFC1161, RFC1283	HISTORIC [pub as:PROPOSED STANDARD]

Number	Title	Author or Ed.	Date	Format	More Info (Obs&Upd)	Status
RFC1414	**Identification MIB**	M. St. Johns, M. Rose	February 1993	ASCII		HISTORIC [pub as:PROPOSED STANDARD]
RFC1407	**Definitions of Managed Objects for the DS3/E3 Interface Type**	T. Cox, K. Tesink	January 1993	ASCII	Obsoletes RFC1233, Obsoleted by RFC2496	PROPOSED STANDARD
RFC1406	**Definitions of Managed Objects for the DS1 and E1 Interface Types**	F. Baker, J. Watt, Eds.	January 1993	ASCII	Obsoletes RFC1232, Obsoleted by RFC2495	PROPOSED STANDARD
RFC1382	**SNMP MIB Extension for the X.25 Packet Layer**	D. Throop, Ed.	November 1992	ASCII		PROPOSED STANDARD
RFC1381	**SNMP MIB Extension for X.25 LAPB**	D. Throop, F. Baker	November 1992	ASCII		PROPOSED STANDARD
RFC1353	**Definitions of Managed Objects for Administration of SNMP Parties**	K. McCloghrie, J. Davin, J. Galvin	July 1992	ASCII		HISTORIC [pub as:PROPOSED STANDARD]
RFC1352	**SNMP Security Protocols**	J. Galvin, K. McCloghrie, J. Davin	July 1992	ASCII		HISTORIC [pub as:PROPOSED STANDARD]
RFC1351	**SNMP Administrative Model**	J. Davin, J. Galvin, K. McCloghrie	July 1992	ASCII		HISTORIC [pub as:PROPOSED STANDARD]
RFC1303	**A Convention for Describing SNMP-based Agents**	K. McCloghrie, M. Rose	February 1992	ASCII		INFORMATIONAL
RFC1298	**SNMP over IPX**	R. Wormley, S. Bostock	February 1992	ASCII	Obsoleted by RFC1420	INFORMATIONAL
RFC1289	**DECnet Phase IV MIB Extensions**	J. Saperia	December 1991	ASCII	Obsoleted by RFC1559	PROPOSED STANDARD
RFC1286	**Definitions of Managed Objects for Bridges**	E. Decker, P. Langille, A. Rijsinghani, K. McCloghrie	December 1991	ASCII	Obsoleted by RFC1493, RFC1525	PROPOSED STANDARD
RFC1285	**FDDI Management Information Base**	J. Case	January 1992	ASCII	Updated by RFC1512	HISTORIC [pub as:PROPOSED STANDARD]

Number	Title	Author or Ed.	Date	Format	More Info (Obs&Upd)	Status
RFC1284	**Definitions of Managed Objects for the Ethernet-like Interface Types**	J. Cook, Ed.	December 1991	ASCII	Obsoleted by RFC1398	PROPOSED STANDARD
RFC1283	**SNMP over OSI**	M. Rose	December 1991	ASCII	Obsoleted by RFC1418	EXPERIMENTAL
RFC1270	**SNMP Communications Services**	F. Kastenholz	October 1991	ASCII		INFORMATIONAL
RFC1228	**SNMP-DPI: Simple Network Management Protocol Distributed Program Interface**	G. Carpenter, B. Wijnen	May 1991	ASCII	Obsoleted by RFC1592	EXPERIMENTAL
RFC1227	**SNMP MUX protocol and MIB**	M.T. Rose	May 1991	ASCII	Errata	HISTORIC
RFC1215	**Convention for defining traps for use with the SNMP**	M.T. Rose	March 1991	ASCII		INFORMATIONAL
RFC1187	**Bulk Table Retrieval with the SNMP**	M.T. Rose, K. McCloghrie, J.R. Davin	October 1990	ASCII		EXPERIMENTAL
RFC1161	**SNMP over OSI**	M.T. Rose	June 1990	ASCII	Obsoleted by RFC1418	EXPERIMENTAL
RFC1157	**Simple Network Management Protocol (SNMP)**	J.D. Case, M. Fedor, M.L. Schoffstall, J. Davin	May 1990	ASCII	Obsoletes RFC1098	HISTORIC [pub as:STANDARD]
RFC1098	**Simple Network Management Protocol (SNMP)**	J.D. Case, M. Fedor, M.L. Schoffstall, J. Davin	April 1989	ASCII	Obsoletes RFC1067, Obsoleted by RFC1157	UNKNOWN
RFC1089	**SNMP over Ethernet**	M. Schoffstall, C. Davin, M. Fedor, J. Case	February 1989	ASCII	Obsoleted by RFC4789	UNKNOWN

12.6. Anexo VI: Fichero de configuración de gestión de pacientes

```
##############################################################################
# pacientes.cfg - Gestión de Pacientes - Desarrollo
#
# Last Modified: 18-06-2012
#
# Se le asignarán todos los servicios definidos para el grupo linux-servers
# al que pertenece, en el fichero service_Linux_HCUV.cfg
##############################################################################

##############################################################################
##############################################################################
#
# HOST DEFINITION
#
```

```
##############################################################################
##############################################################################

# Define a host for the server

define host{
        use                     linux-server            ; Name of host template to use
                                                        ; This host definition will inherit all
variables that are defined
                                                        ; in (or inherited by) the linux-server
host template definition.
        host_name               pacientes
        alias                   Servidor HP-H.I.S. Clinica
        address                 10.xx.yy.zz
        }

##############################################################################
##############################################################################
#
# SERVICE DEFINITIONS
#
##############################################################################
##############################################################################

# Intenta conectar al puerto TCP/23 usado por servidor Telnet

define service{
        use                             local-service         ; Name of service template to use
        host_name                       pacientes
        service_description             Telnet Puerto
    check_command                   check_tcp_hcuv!23!1!2
        }

# Define a service to check the disk space of the /boot partition.
# Warning if < 10% free, critical if < 5% free space on partition.
# 'check_snmp_storage_v1' command definition
define service {
    use                     generic-service
    host_name               pacientes
    name                    Pac_Check_LinDisk_boot
    service_description     File System /boot
    check_command           check_snmp_storage_v1!/boot!90!95!-r -G
}

# Define a service to check the disk space of the /copia_ifx partition.
# Warning if < 10% free, critical if < 5% free space on partition.
# 'check_snmp_storage_v1' command definition
define service {
    use                     generic-service
    host_name               pacientes
    name                    Pac_Check_LinDisk_copia_ifx
    service_description     File System /copia_ifx
    check_command           check_snmp_storage_v1!/copia_ifx!90!95!-r -G
}

# Define a service to check the disk space of the /datos_ifx partition.
# Warning if < 10% free, critical if < 5% free space on partition.
# 'check_snmp_storage_v1' command definition
define service {
    use                     generic-service
    host_name               pacientes
    name                    Pac_Check_LinDisk_datos_ifx
    service_description     File System /datos_ifx
    check_command           check_snmp_storage_v1!/datos_ifx!90!95!-r -G
}

# Define a service to check if process exist.
# 'Proceso Oninit'
# comando 'check_snmp_process_lento'
define service{
    use                             generic-service          ; Name of service template to use
    host_name                       pacientes
    service_description             IFX Proceso Oninit
    check_command                   check_snmp_process_lento!oninit!0!0!-r
}

# Define a service to check if process exist.
# 'Proceso in.telnetd'
# comando 'check_snmp_process_lento'
define service{
    use                             generic-service          ; Name of service template to use
    host_name                       pacientes
    service_description             Telnet Sesiones activas
    check_command                   check_snmp_process_lento!in.telnetd!0!0!-r
}

##############################################################################
##############################################################################
```

```
#
# SERVICE DEFINITIONS
#
###############################################################################
###############################################################################

# Define a service to "ping" all linux-servers

define service{
        use                             local-service         ; Name of service template to use
    hostgroup_name                  linux-servers
        service_description             PING
    check_command                   check_ping!100.0,20%!500.0,60%
        }

# Intenta conectar a un servidor SSH a un servidor específico y puerto

define service{
        use                             local-service         ; Name of service template to use
    hostgroup_name                  linux-servers
        service_description             SSH Servidor
    check_command                   check_ssh
        }

# Intenta conectar al puerto TCP/22 usado por servidor SSH

define service{
        use                     local-service         ; Name of service template to use
    hostgroup_name              linux-servers
        service_description     SSH Puerto
    check_command               check_tcp!22!1!2
        }

# Define a service to check the Memory and Cache use
# on Linux Servers.  Warning at 80% memory used and 60% swap used,
# critical at 95% memory and 90% swap
# 'check_snmp_mem_v1' command definition
# 'check_snmp_mem.pl' command definition
define service{
    use                         generic-service          ; Name of service template to use
    hostgroup_name              linux-servers
    service_description         Memoria/Swap en uso
    is_volatile                 0
    check_period                24x7
    max_check_attempts          3
    normal_check_interval       2
    retry_check_interval        1
#   contact_groups              linux-admins
    notification_interval       240
    notification_period         24x7
    notification_options        c,r
    check_command               check_snmp_mem_v1!-N!80,60!95,90
    }

# Define a service to check the Linux CPU % Use.
#  Warning at 40% of CPU use, critical at 60%
# 'check_snmp_load_v1' command definition
define service{
    use                         generic-service          ; Name of service template to use
    hostgroup_name              linux-servers
    service_description         CPU en uso
    is_volatile                 0
    max_check_attempts          3
    normal_check_interval       5
    retry_check_interval        1
#   contact_groups              linux-admins
    notification_interval       240
    notification_period         24x7
    notification_options        c,r
    check_command               check_snmp_load_v1!netsc!40!60
    }

# Define a service to check the Linux Load (1min, 5min, 15min)
# on Linux Servers.  Warning at 3,2,2 proccess queue,
# critical at 6,4,4 proccess queue
# 'check_snmp_load_v1' command definition
define service{
    use                         generic-service          ; Name of service template to use
    hostgroup_name              linux-servers
    service_description         CPU Cola Procesos
    is_volatile                 0
    max_check_attempts          3
    normal_check_interval       5
    retry_check_interval        1
#   contact_groups              linux-admins
    notification_interval       240
    notification_period         24x7
    notification_options        c,r
```

```
    check_command            check_snmp_load_v1!netsl!3,2,2!6,4,4
    }

# Define a service to check the disk space of the / (root) partition.
# Warning if < 20% free, critical if < 10% free space on partition.
# 'check_snmp_storage.pl' command definition
define service {
    use                      generic-service
    hostgroup_name           linux-servers
    service_description      File System /
    check_command            check_snmp_storage_v1!/!80!90!-r -G
}

################################################################################
################################################################################
#
# Command DEFINITIONS
#
################################################################################
################################################################################

# Check conection to tcp port
# 'check_tcp' command
define command{
    command_name     check_tcp_hcuv
    command_line     $USER1$/check_tcp -H $HOSTADDRESS$ -p $ARG1$ -w $ARG2$ -c $ARG3$
    ;$ARG1$          port
    ;$ARG2$          warning
    ;$ARG3$          critical
}

# Command to check the disk space of partitions on linux server.
define command {
    command_name     check_snmp_storage_v1
    command_line     $USER1$/check_snmp_storage.pl  -H  $HOSTADDRESS$  -C  $USER5$  -m  $ARG1$  -w
$ARG2$ -c $ARG3$ $ARG4$
}

# 'check_snmp_process_lento' command definition. Servidor lento
# Comprueba si se encuentra en ejecución el proceso suministrado como argumento
define command{
    command_name     check_snmp_process_lento
    command_line     $USER1$/check_snmp_process_lento.pl -H $HOSTADDRESS$ -C $USER5$ -n $ARG1$ -
w $ARG2$ -c $ARG3$ $ARG4$
    ;$ARG1$          proceso a comprobar
    ;$ARG2$          warning
    ;$ARG3$          critical
    ;$ARG4$          parámetros opcionales (-r)
    }

# 'check_ping' command definition
define command{
        command_name    check_ping
        command_line    $USER1$/check_ping -H $HOSTADDRESS$ -w $ARG1$ -c $ARG2$ -p 5
        }

# 'check_ssh' command definition
define command{
    command_name     check_ssh
    command_line     $USER1$/check_ssh $ARG1$ $HOSTADDRESS$
    }

# Monitor Linux Memory and Swap use (real & %)
#
 define command{
  command_name check_snmp_mem_v1
    command_line     $USER1$/check_snmp_mem.pl -H $HOSTADDRESS$ -C $USER5$ $ARG1$ -w $ARG2$ -c
$ARG3$ $ARG4$
 }
```

Anexo VII: Plugin check_esx3-0.5.pl

```
usage: esx_cpu.pl -D | -H [ -N ]
-u -p | -f
-l [ -s ]
[ -x ]
[ -t ] [ -w ] [ -c ]
[ -V ] [ -h ]


-?, --usage
Print usage information
-h, --help
Print detailed help screen
-V, --version
Print version information
```

```
--extra-opts=[[@]]
Section and/or config_file from which to load extra options (may repeat)

-H, --host=
ESX or ESXi hostname.

-D, --datacenter=
Datacenter hostname.

-N, --name=
Virtual machine name.

-u, --username=
Username to connect with.

-p, --password=
Password to use with the username.

-f, --authfile=
Authentication file with login and password. File syntax :
username=
password=
-w, --warning=THRESHOLD
Warning threshold. See
http://nagiosplug.sourceforge.net/developer-guidelines.html#THRESHOLDFORMAT
for the threshold format.
-c, --critical=THRESHOLD
Critical threshold. See
http://nagiosplug.sourceforge.net/developer-guidelines.html#THRESHOLDFORMAT
for the threshold format.
-l, --command=COMMAND
Specify command type (CPU, MEM, NET, IO, VMFS, RUNTIME, ...)
-s, --subcommand=SUBCOMMAND
Specify subcommand
-S, --sessionfile=SESSIONFILE
Specify a filename to store sessions for faster authentication
-x, --exclude=
Specify black list
-t, --timeout=INTEGER
Seconds before plugin times out (default: 30)
-v, --verbose
Show details for command-line debugging (can repeat up to 3 times)


Supported commands(^ means blank or not specified parameter) :
Common options for VM, Host and DC :

* cpu - shows cpu info
+ usage - CPU usage in percentage
+ usagemhz - CPU usage in MHz
^ all cpu info

* mem - shows mem info
+ usage - mem usage in percentage
+ usagemb - mem usage in MB
+ swap - swap mem usage in MB
+ overhead - additional mem used by VM Server in MB
+ overall - overall mem used by VM Server in MB
^ all mem info

* net - shows net info
+ usage - overall network usage in KBps(Kilobytes per Second)
+ receive - receive in KBps(Kilobytes per Second)
+ send - send in KBps(Kilobytes per Second)
^ all net info

* io - shows disk io info
+ read - read latency in ms
+ write - write latency in ms
^ all disk io info

* runtime - shows runtime info
+ status - overall host status (gray/green/red/yellow)
+ issues - all issues for the host
^ all runtime info

VM specific :
* cpu - shows cpu info
+ wait - CPU wait in ms
* mem - shows mem info
+ swapin - swapin mem usage in MB
+ swapout - swapout mem usage in MB
+ active - active mem usage in MB
* io - shows disk I/O info
+ usage - overall disk usage in MB/s
* runtime - shows runtime info
+ con - connection state
+ cpu - allocated CPU in MHz
```

```
+ mem - allocated mem in MB
+ state - virtual machine state (UP, DOWN, SUSPENDED)
+ consoleconnections - console connections to VM
+ guest - guest OS status, needs VMware Tools
+ tools - VMWare Tools status
Host specific :
* net - shows net info
+ nic - makes sure all active NICs are plugged in
* io - shows disk io info
+ aborted - aborted commands count
+ resets - bus resets count
+ kernel - kernel latency in ms
+ device - device latency in ms
+ queue - queue latency in ms
* vmfs - shows Datastore info
+ (name) - info for datastore with name (name)
^ all datastore info
* runtime - shows runtime info
+ con - connection state
+ health - checks cpu/storage/memory/sensor status
+ maintenance - shows whether host is in maintenance mode
+ list(vm) - list of VMWare machines and their statuses
* service - shows Host service info
+ (names) - check the state of one or several services specified by (names), syntax for
(names):,,...,
^ show all services
DC specific :
* io - shows disk io info
+ aborted - aborted commands count
+ resets - bus resets count
+ kernel - kernel latency in ms
+ device - device latency in ms
+ queue - queue latency in ms
* vmfs - shows Datastore info
+ (name) - info for datastore with name (name)
^ all datastore info
* runtime - shows runtime info
+ list(vm) - list of VMWare machines and their statuses
+ listhost - list of VMWare esx host servers and their statuses
* recommendations - shows recommendations for cluster
+ (name) - recommendations for cluster with name (name)
^ all clusters recommendations


CHEC_ESX Version - 0.5 :
------------------------


Posted new Version 0.5.
Examples.....



ESX Base OS :
----------------

check_esx -H 10.8.3.115 -u xxx -p xxx -l cpu
CHECK_ESX OK - cpu usage=1169.82 MHz (4.99%) | cpu_usagemhz=1169.82Mhz;; cpu_usage=4.99%;;


#check_esx -H 10.8.3.115 -u xxx -p xxx -l cpu -s usage -w 80 -c 90 -t 60
CHECK_ESX OK - cpu usage=3.56 % | cpu_usage=3.56%;80;90


#check_esx -H 10.8.3.115 -u xxx -p xxx -l vmfs
CHECK_ESX OK - storages : Storage1=2287.00 MB (3.36%), Storage3=35440.00 MB (3.72%),
Storage2=40352.00 MB (14.49%) | Storage1=2287.00MB;; Storage3=35440.00MB;; Storage2=40352.00MB;;

#check_esx -H 10.8.3.115 -u xxx -p xxx -l net
CHECK_ESX OK - net receive=4.40 KBps, send=0.30 KBps, all 1 NICs are connected |
net_receive=4.40KBps;; net_send=0.30KBps;; OK_NICs=1;; Bad_NICs=0;;

#check_esx -H 10.8.3.115 -u xxx -p xxx -l io
CHECK_ESX OK - io commands aborted=0, io bus resets=0, io read latency=0 ms, write latency=0 ms,
kernel latency=0 ms, device latency=0 ms, queue latency=0 ms | io_aborted=0;; io_busresets=0;;
io_read=0ms;; io_write=0ms;; io_kernel=0ms;; io_device=0ms;; io_queue=0ms;;

#check_esx -H 10.8.3.115 -u xxx -p xxx -l runtime
CHECK_ESX OK - 3/4 VMs up, overall status=green, connection state=connected, maintenance=no, All
175 health checks are Green, no config issues | vmcount=3units;;

#check_esx -H 10.8.3.115 -u xxx -p xxx -l service
CHECK_ESX OK - services : ntpd (down), sshd (up), vmware-vpxa (up), vmware-webAccess (up)



VM checks from Base OS:
-------------------------------
```

```
#check_esx -H 10.8.3.115 -N cs1 -u xxx -p xxx -l cpu
CHECK_ESX OK - "cs1" cpu usage=467.13 MHz(3.99%) wait=19626.20 ms | cpu_usagemhz=467.13Mhz;;
cpu_usage=3.99%;; cpu_wait=19626.20ms;;



CHEC_ESX Version - 0.5 :
------------------------
Along with other improvement, It has new features like:

Cluster monitoring.
Storage (SAN - Luns/Paths/adapters etc).
Vmware Tools

I like the extra feature where you can call native nagios
options via vcenter or esx....

--extra-opts=[section][@file]
Read options from an ini file. See http://nagiosplugins.org/extra-opts for usage
```

12.7. Anexo VII: Árbol de OIDs MIB telefonía IP CISCO-CCM-MIB.my

```
### THIS FILE WAS GENERATED BY MIB2SCHEMA
"org"               "1.3"
"dod"               "1.3.6"
"internet"          "1.3.6.1"
"directory"         "1.3.6.1.1"
"mgmt"              "1.3.6.1.2"
"experimental"              "1.3.6.1.3"
"private"           "1.3.6.1.4"
"enterprises"               "1.3.6.1.4.1"
"cisco"             "1.3.6.1.4.1.9"
"ciscoMgmt"         "1.3.6.1.4.1.9.9"
"ciscoCcmMIB"               "1.3.6.1.4.1.9.9.156"
"ciscoCcmMIBObjects"        "1.3.6.1.4.1.9.9.156.1"
"ccmMIBNotificationPrefix"          "1.3.6.1.4.1.9.9.156.2"
"ciscoCcmMIBConformance"            "1.3.6.1.4.1.9.9.156.3"
"ccmGeneralInfo"            "1.3.6.1.4.1.9.9.156.1.1"
"ccmPhoneInfo"              "1.3.6.1.4.1.9.9.156.1.2"
"ccmGatewayInfo"            "1.3.6.1.4.1.9.9.156.1.3"
"ccmGatewayTrunkInfo"               "1.3.6.1.4.1.9.9.156.1.4"
"ccmGlobalInfo"             "1.3.6.1.4.1.9.9.156.1.5"
"ccmMediaDeviceInfo"        "1.3.6.1.4.1.9.9.156.1.6"
"ccmGatekeeperInfo"         "1.3.6.1.4.1.9.9.156.1.7"
"ccmCTIDeviceInfo"          "1.3.6.1.4.1.9.9.156.1.8"
"ccmAlarmConfigInfo"        "1.3.6.1.4.1.9.9.156.1.9"
"ccmNotificationsInfo"              "1.3.6.1.4.1.9.9.156.1.10"
"ccmH323DeviceInfo"         "1.3.6.1.4.1.9.9.156.1.11"
"ccmVoiceMailDeviceInfo"            "1.3.6.1.4.1.9.9.156.1.12"
"ccmQualityReportAlarmConfigInfo"           "1.3.6.1.4.1.9.9.156.1.13"
"ccmSIPDeviceInfo"          "1.3.6.1.4.1.9.9.156.1.14"
"ccmGroupTable"             "1.3.6.1.4.1.9.9.156.1.1.1"
"ccmTable"          "1.3.6.1.4.1.9.9.156.1.1.2"
"ccmGroupMappingTable"              "1.3.6.1.4.1.9.9.156.1.1.3"
"ccmRegionTable"            "1.3.6.1.4.1.9.9.156.1.1.4"
"ccmRegionPairTable"        "1.3.6.1.4.1.9.9.156.1.1.5"
"ccmTimeZoneTable"          "1.3.6.1.4.1.9.9.156.1.1.6"
"ccmDevicePoolTable"        "1.3.6.1.4.1.9.9.156.1.1.7"
"ccmProductTypeTable"               "1.3.6.1.4.1.9.9.156.1.1.8"
"ccmGroupEntry"             "1.3.6.1.4.1.9.9.156.1.1.1.1"
"ccmGroupIndex"             "1.3.6.1.4.1.9.9.156.1.1.1.1.1"
"ccmGroupName"              "1.3.6.1.4.1.9.9.156.1.1.1.1.2"
"ccmGroupTftpDefault"               "1.3.6.1.4.1.9.9.156.1.1.1.1.3"
"ccmEntry"          "1.3.6.1.4.1.9.9.156.1.1.2.1"
"ccmIndex"          "1.3.6.1.4.1.9.9.156.1.1.2.1.1"
"ccmName"           "1.3.6.1.4.1.9.9.156.1.1.2.1.2"
"ccmDescription"            "1.3.6.1.4.1.9.9.156.1.1.2.1.3"
"ccmVersion"        "1.3.6.1.4.1.9.9.156.1.1.2.1.4"
"ccmStatus"         "1.3.6.1.4.1.9.9.156.1.1.2.1.5"
"ccmInetAddressType"        "1.3.6.1.4.1.9.9.156.1.1.2.1.6"
"ccmInetAddress"            "1.3.6.1.4.1.9.9.156.1.1.2.1.7"
"ccmClusterId"              "1.3.6.1.4.1.9.9.156.1.1.2.1.8"
"ccmInetAddress2Type"               "1.3.6.1.4.1.9.9.156.1.1.2.1.9"
"ccmInetAddress2"           "1.3.6.1.4.1.9.9.156.1.1.2.1.10"
"ccmGroupMappingEntry"              "1.3.6.1.4.1.9.9.156.1.1.3.1"
"ccmCMGroupMappingCMPriority"               "1.3.6.1.4.1.9.9.156.1.1.3.1.1"
"ccmRegionEntry"            "1.3.6.1.4.1.9.9.156.1.1.4.1"
"ccmRegionIndex"            "1.3.6.1.4.1.9.9.156.1.1.4.1.1"
"ccmRegionName"             "1.3.6.1.4.1.9.9.156.1.1.4.1.2"
"ccmRegionPairEntry"        "1.3.6.1.4.1.9.9.156.1.1.5.1"
"ccmRegionSrcIndex"         "1.3.6.1.4.1.9.9.156.1.1.5.1.1"
"ccmRegionDestIndex"        "1.3.6.1.4.1.9.9.156.1.1.5.1.2"
```

```
"ccmRegionAvailableBandWidth"                "1.3.6.1.4.1.9.9.156.1.1.5.1.3"
"ccmTimeZoneEntry"           "1.3.6.1.4.1.9.9.156.1.1.6.1"
"ccmTimeZoneIndex"           "1.3.6.1.4.1.9.9.156.1.1.6.1.1"
"ccmTimeZoneName"            "1.3.6.1.4.1.9.9.156.1.1.6.1.2"
"ccmTimeZoneOffset"          "1.3.6.1.4.1.9.9.156.1.1.6.1.3"
"ccmTimeZoneOffsetHours"             "1.3.6.1.4.1.9.9.156.1.1.6.1.4"
"ccmTimeZoneOffsetMinutes"           "1.3.6.1.4.1.9.9.156.1.1.6.1.5"
"ccmDevicePoolEntry"         "1.3.6.1.4.1.9.9.156.1.1.7.1"
"ccmDevicePoolIndex"         "1.3.6.1.4.1.9.9.156.1.1.7.1.1"
"ccmDevicePoolName"          "1.3.6.1.4.1.9.9.156.1.1.7.1.2"
"ccmDevicePoolRegionIndex"           "1.3.6.1.4.1.9.9.156.1.1.7.1.3"
"ccmDevicePoolTimeZoneIndex"         "1.3.6.1.4.1.9.9.156.1.1.7.1.4"
"ccmDevicePoolGroupIndex"            "1.3.6.1.4.1.9.9.156.1.1.7.1.5"
"ccmProductTypeEntry"                "1.3.6.1.4.1.9.9.156.1.1.8.1"
"ccmProductTypeIndex"                "1.3.6.1.4.1.9.9.156.1.1.8.1.1"
"ccmProductType"             "1.3.6.1.4.1.9.9.156.1.1.8.1.2"
"ccmProductName"             "1.3.6.1.4.1.9.9.156.1.1.8.1.3"
"ccmProductCategory"         "1.3.6.1.4.1.9.9.156.1.1.8.1.4"
"ccmPhoneTable"              "1.3.6.1.4.1.9.9.156.1.2.1"
"ccmPhoneExtensionTable"             "1.3.6.1.4.1.9.9.156.1.2.2"
"ccmPhoneFailedTable"                "1.3.6.1.4.1.9.9.156.1.2.3"
"ccmPhoneStatusUpdateTable"          "1.3.6.1.4.1.9.9.156.1.2.4"
"ccmPhoneExtnTable"          "1.3.6.1.4.1.9.9.156.1.2.5"
"ccmPhoneEntry"              "1.3.6.1.4.1.9.9.156.1.2.1.1"
"ccmPhoneIndex"              "1.3.6.1.4.1.9.9.156.1.2.1.1.1"
"ccmPhonePhysicalAddress"            "1.3.6.1.4.1.9.9.156.1.2.1.1.2"
"ccmPhoneType"               "1.3.6.1.4.1.9.9.156.1.2.1.1.3"
"ccmPhoneDescription"                "1.3.6.1.4.1.9.9.156.1.2.1.1.4"
"ccmPhoneUserName"           "1.3.6.1.4.1.9.9.156.1.2.1.1.5"
"ccmPhoneIpAddress"          "1.3.6.1.4.1.9.9.156.1.2.1.1.6"
"ccmPhoneStatus"             "1.3.6.1.4.1.9.9.156.1.2.1.1.7"
"ccmPhoneTimeLastRegistered"         "1.3.6.1.4.1.9.9.156.1.2.1.1.8"
"ccmPhoneE911Location"               "1.3.6.1.4.1.9.9.156.1.2.1.1.9"
"ccmPhoneLoadID"             "1.3.6.1.4.1.9.9.156.1.2.1.1.10"
"ccmPhoneLastError"          "1.3.6.1.4.1.9.9.156.1.2.1.1.11"
"ccmPhoneTimeLastError"              "1.3.6.1.4.1.9.9.156.1.2.1.1.12"
"ccmPhoneDevicePoolIndex"            "1.3.6.1.4.1.9.9.156.1.2.1.1.13"
"ccmPhoneInetAddressType"            "1.3.6.1.4.1.9.9.156.1.2.1.1.14"
"ccmPhoneInetAddress"                "1.3.6.1.4.1.9.9.156.1.2.1.1.15"
"ccmPhoneStatusReason"               "1.3.6.1.4.1.9.9.156.1.2.1.1.16"
"ccmPhoneTimeLastStatusUpdt"         "1.3.6.1.4.1.9.9.156.1.2.1.1.17"
"ccmPhoneProductTypeIndex"           "1.3.6.1.4.1.9.9.156.1.2.1.1.18"
"ccmPhoneProtocol"           "1.3.6.1.4.1.9.9.156.1.2.1.1.19"
"ccmPhoneName"               "1.3.6.1.4.1.9.9.156.1.2.1.1.20"
"ccmPhoneInetAddressIPv4"            "1.3.6.1.4.1.9.9.156.1.2.1.1.21"
"ccmPhoneInetAddressIPv6"            "1.3.6.1.4.1.9.9.156.1.2.1.1.22"
"ccmPhoneIPv4Attribute"              "1.3.6.1.4.1.9.9.156.1.2.1.1.23"
"ccmPhoneIPv6Attribute"              "1.3.6.1.4.1.9.9.156.1.2.1.1.24"
"ccmPhoneActiveLoadID"               "1.3.6.1.4.1.9.9.156.1.2.1.1.25"
"ccmPhoneUnregReason"                "1.3.6.1.4.1.9.9.156.1.2.1.1.26"
"ccmPhoneRegFailReason"              "1.3.6.1.4.1.9.9.156.1.2.1.1.27"
"ccmPhoneExtensionEntry"             "1.3.6.1.4.1.9.9.156.1.2.2.1"
"ccmPhoneExtensionIndex"             "1.3.6.1.4.1.9.9.156.1.2.2.1.1"
"ccmPhoneExtension"          "1.3.6.1.4.1.9.9.156.1.2.2.1.2"
"ccmPhoneExtensionIpAddress"         "1.3.6.1.4.1.9.9.156.1.2.2.1.3"
"ccmPhoneExtensionMultiLines"                "1.3.6.1.4.1.9.9.156.1.2.2.1.4"
"ccmPhoneExtensionInetAddressType"           "1.3.6.1.4.1.9.9.156.1.2.2.1.5"
"ccmPhoneExtensionInetAddress"               "1.3.6.1.4.1.9.9.156.1.2.2.1.6"
"ccmPhoneFailedEntry"                "1.3.6.1.4.1.9.9.156.1.2.3.1"
"ccmPhoneFailedIndex"                "1.3.6.1.4.1.9.9.156.1.2.3.1.1"
"ccmPhoneFailedTime"         "1.3.6.1.4.1.9.9.156.1.2.3.1.2"
"ccmPhoneFailedName"         "1.3.6.1.4.1.9.9.156.1.2.3.1.3"
"ccmPhoneFailedInetAddressType"              "1.3.6.1.4.1.9.9.156.1.2.3.1.4"
"ccmPhoneFailedInetAddress"          "1.3.6.1.4.1.9.9.156.1.2.3.1.5"
"ccmPhoneFailCauseCode"              "1.3.6.1.4.1.9.9.156.1.2.3.1.6"
"ccmPhoneFailedMacAddress"           "1.3.6.1.4.1.9.9.156.1.2.3.1.7"
"ccmPhoneFailedInetAddressIPv4"              "1.3.6.1.4.1.9.9.156.1.2.3.1.8"
"ccmPhoneFailedInetAddressIPv6"              "1.3.6.1.4.1.9.9.156.1.2.3.1.9"
"ccmPhoneFailedIPv4Attribute"                "1.3.6.1.4.1.9.9.156.1.2.3.1.10"
"ccmPhoneFailedIPv6Attribute"                "1.3.6.1.4.1.9.9.156.1.2.3.1.11"
"ccmPhoneFailedRegFailReason"                "1.3.6.1.4.1.9.9.156.1.2.3.1.12"
"ccmPhoneStatusUpdateEntry"          "1.3.6.1.4.1.9.9.156.1.2.4.1"
"ccmPhoneStatusUpdateIndex"          "1.3.6.1.4.1.9.9.156.1.2.4.1.1"
"ccmPhoneStatusPhoneIndex"           "1.3.6.1.4.1.9.9.156.1.2.4.1.2"
"ccmPhoneStatusUpdateTime"           "1.3.6.1.4.1.9.9.156.1.2.4.1.3"
"ccmPhoneStatusUpdateType"           "1.3.6.1.4.1.9.9.156.1.2.4.1.4"
"ccmPhoneStatusUpdateReason"         "1.3.6.1.4.1.9.9.156.1.2.4.1.5"
"ccmPhoneStatusUnregReason"          "1.3.6.1.4.1.9.9.156.1.2.4.1.6"
"ccmPhoneStatusRegFailReason"                "1.3.6.1.4.1.9.9.156.1.2.4.1.7"
"ccmPhoneExtnEntry"          "1.3.6.1.4.1.9.9.156.1.2.5.1"
"ccmPhoneExtnIndex"          "1.3.6.1.4.1.9.9.156.1.2.5.1.1"
"ccmPhoneExtn"               "1.3.6.1.4.1.9.9.156.1.2.5.1.2"
"ccmPhoneExtnMultiLines"             "1.3.6.1.4.1.9.9.156.1.2.5.1.3"
"ccmPhoneExtnInetAddressType"                "1.3.6.1.4.1.9.9.156.1.2.5.1.4"
"ccmPhoneExtnInetAddress"            "1.3.6.1.4.1.9.9.156.1.2.5.1.5"
"ccmPhoneExtnStatus"         "1.3.6.1.4.1.9.9.156.1.2.5.1.6"
"ccmGatewayTable"            "1.3.6.1.4.1.9.9.156.1.3.1"
"ccmGatewayEntry"            "1.3.6.1.4.1.9.9.156.1.3.1.1"
```

```
"ccmGatewayIndex"           "1.3.6.1.4.1.9.9.156.1.3.1.1.1"
"ccmGatewayName"            "1.3.6.1.4.1.9.9.156.1.3.1.1.2"
"ccmGatewayType"            "1.3.6.1.4.1.9.9.156.1.3.1.1.3"
"ccmGatewayDescription"             "1.3.6.1.4.1.9.9.156.1.3.1.1.4"
"ccmGatewayStatus"          "1.3.6.1.4.1.9.9.156.1.3.1.1.5"
"ccmGatewayDevicePoolIndex"         "1.3.6.1.4.1.9.9.156.1.3.1.1.6"
"ccmGatewayInetAddressType"         "1.3.6.1.4.1.9.9.156.1.3.1.1.7"
"ccmGatewayInetAddress"             "1.3.6.1.4.1.9.9.156.1.3.1.1.8"
"ccmGatewayProductId"               "1.3.6.1.4.1.9.9.156.1.3.1.1.9"
"ccmGatewayStatusReason"            "1.3.6.1.4.1.9.9.156.1.3.1.1.10"
"ccmGatewayTimeLastStatusUpdt"              "1.3.6.1.4.1.9.9.156.1.3.1.1.11"
"ccmGatewayTimeLastRegistered"              "1.3.6.1.4.1.9.9.156.1.3.1.1.12"
"ccmGatewayDChannelStatus"          "1.3.6.1.4.1.9.9.156.1.3.1.1.13"
"ccmGatewayDChannelNumber"          "1.3.6.1.4.1.9.9.156.1.3.1.1.14"
"ccmGatewayProductTypeIndex"        "1.3.6.1.4.1.9.9.156.1.3.1.1.15"
"ccmGatewayUnregReason"             "1.3.6.1.4.1.9.9.156.1.3.1.1.16"
"ccmGatewayRegFailReason"           "1.3.6.1.4.1.9.9.156.1.3.1.1.17"
"ccmGatewayTrunkTable"              "1.3.6.1.4.1.9.9.156.1.4.1"
"ccmGatewayTrunkEntry"              "1.3.6.1.4.1.9.9.156.1.4.1.1"
"ccmGatewayTrunkIndex"              "1.3.6.1.4.1.9.9.156.1.4.1.1.1"
"ccmGatewayTrunkType"               "1.3.6.1.4.1.9.9.156.1.4.1.1.2"
"ccmGatewayTrunkName"               "1.3.6.1.4.1.9.9.156.1.4.1.1.3"
"ccmTrunkGatewayIndex"              "1.3.6.1.4.1.9.9.156.1.4.1.1.4"
"ccmGatewayTrunkStatus"             "1.3.6.1.4.1.9.9.156.1.4.1.1.5"
"ccmActivePhones"           "1.3.6.1.4.1.9.9.156.1.5.1"
"ccmInActivePhones"         "1.3.6.1.4.1.9.9.156.1.5.2"
"ccmActiveGateways"         "1.3.6.1.4.1.9.9.156.1.5.3"
"ccmInActiveGateways"               "1.3.6.1.4.1.9.9.156.1.5.4"
"ccmRegisteredPhones"               "1.3.6.1.4.1.9.9.156.1.5.5"
"ccmUnregisteredPhones"             "1.3.6.1.4.1.9.9.156.1.5.6"
"ccmRejectedPhones"         "1.3.6.1.4.1.9.9.156.1.5.7"
"ccmRegisteredGateways"             "1.3.6.1.4.1.9.9.156.1.5.8"
"ccmUnregisteredGateways"           "1.3.6.1.4.1.9.9.156.1.5.9"
"ccmRejectedGateways"               "1.3.6.1.4.1.9.9.156.1.5.10"
"ccmRegisteredMediaDevices"         "1.3.6.1.4.1.9.9.156.1.5.11"
"ccmUnregisteredMediaDevices"               "1.3.6.1.4.1.9.9.156.1.5.12"
"ccmRejectedMediaDevices"           "1.3.6.1.4.1.9.9.156.1.5.13"
"ccmRegisteredCTIDevices"           "1.3.6.1.4.1.9.9.156.1.5.14"
"ccmUnregisteredCTIDevices"         "1.3.6.1.4.1.9.9.156.1.5.15"
"ccmRejectedCTIDevices"             "1.3.6.1.4.1.9.9.156.1.5.16"
"ccmRegisteredVoiceMailDevices"             "1.3.6.1.4.1.9.9.156.1.5.17"
"ccmUnregisteredVoiceMailDevices"           "1.3.6.1.4.1.9.9.156.1.5.18"
"ccmRejectedVoiceMailDevices"               "1.3.6.1.4.1.9.9.156.1.5.19"
"ccmCallManagerStartTime"           "1.3.6.1.4.1.9.9.156.1.5.20"
"ccmPhoneTableStateId"              "1.3.6.1.4.1.9.9.156.1.5.21"
"ccmPhoneExtensionTableStateId"             "1.3.6.1.4.1.9.9.156.1.5.22"
"ccmPhoneStatusUpdateTableStateId"          "1.3.6.1.4.1.9.9.156.1.5.23"
"ccmGatewayTableStateId"            "1.3.6.1.4.1.9.9.156.1.5.24"
"ccmCTIDeviceTableStateId"          "1.3.6.1.4.1.9.9.156.1.5.25"
"ccmCTIDeviceDirNumTableStateId"            "1.3.6.1.4.1.9.9.156.1.5.26"
"ccmPhStatUpdtTblLastAddedIndex"            "1.3.6.1.4.1.9.9.156.1.5.27"
"ccmPhFailedTblLastAddedIndex"              "1.3.6.1.4.1.9.9.156.1.5.28"
"ccmSystemVersion"          "1.3.6.1.4.1.9.9.156.1.5.29"
"ccmInstallationId"         "1.3.6.1.4.1.9.9.156.1.5.30"
"ccmPartiallyRegisteredPhones"              "1.3.6.1.4.1.9.9.156.1.5.31"
"ccmH323TableEntries"               "1.3.6.1.4.1.9.9.156.1.5.32"
"ccmSIPTableEntries"        "1.3.6.1.4.1.9.9.156.1.5.33"
"ccmMediaDeviceTable"               "1.3.6.1.4.1.9.9.156.1.6.1"
"ccmMediaDeviceEntry"               "1.3.6.1.4.1.9.9.156.1.6.1.1"
"ccmMediaDeviceIndex"               "1.3.6.1.4.1.9.9.156.1.6.1.1.1"
"ccmMediaDeviceName"        "1.3.6.1.4.1.9.9.156.1.6.1.1.2"
"ccmMediaDeviceType"        "1.3.6.1.4.1.9.9.156.1.6.1.1.3"
"ccmMediaDeviceDescription"         "1.3.6.1.4.1.9.9.156.1.6.1.1.4"
"ccmMediaDeviceStatus"              "1.3.6.1.4.1.9.9.156.1.6.1.1.5"
"ccmMediaDeviceDevicePoolIndex"             "1.3.6.1.4.1.9.9.156.1.6.1.1.6"
"ccmMediaDeviceInetAddressType"             "1.3.6.1.4.1.9.9.156.1.6.1.1.7"
"ccmMediaDeviceInetAddress"         "1.3.6.1.4.1.9.9.156.1.6.1.1.8"
"ccmMediaDeviceStatusReason"        "1.3.6.1.4.1.9.9.156.1.6.1.1.9"
"ccmMediaDeviceTimeLastStatusUpdt"          "1.3.6.1.4.1.9.9.156.1.6.1.1.10"
"ccmMediaDeviceTimeLastRegistered"          "1.3.6.1.4.1.9.9.156.1.6.1.1.11"
"ccmMediaDeviceProductTypeIndex"            "1.3.6.1.4.1.9.9.156.1.6.1.1.12"
"ccmMediaDeviceInetAddressIPv4"             "1.3.6.1.4.1.9.9.156.1.6.1.1.13"
"ccmMediaDeviceInetAddressIPv6"             "1.3.6.1.4.1.9.9.156.1.6.1.1.14"
"ccmMediaDeviceUnregReason"         "1.3.6.1.4.1.9.9.156.1.6.1.1.15"
"ccmMediaDeviceRegFailReason"               "1.3.6.1.4.1.9.9.156.1.6.1.1.16"
"ccmGatekeeperTable"        "1.3.6.1.4.1.9.9.156.1.7.1"
"ccmGatekeeperEntry"        "1.3.6.1.4.1.9.9.156.1.7.1.1"
"ccmGatekeeperIndex"        "1.3.6.1.4.1.9.9.156.1.7.1.1.1"
"ccmGatekeeperName"         "1.3.6.1.4.1.9.9.156.1.7.1.1.2"
"ccmGatekeeperType"         "1.3.6.1.4.1.9.9.156.1.7.1.1.3"
"ccmGatekeeperDescription"          "1.3.6.1.4.1.9.9.156.1.7.1.1.4"
"ccmGatekeeperStatus"               "1.3.6.1.4.1.9.9.156.1.7.1.1.5"
"ccmGatekeeperDevicePoolIndex"              "1.3.6.1.4.1.9.9.156.1.7.1.1.6"
"ccmGatekeeperInetAddressType"              "1.3.6.1.4.1.9.9.156.1.7.1.1.7"
"ccmGatekeeperInetAddress"          "1.3.6.1.4.1.9.9.156.1.7.1.1.8"
"ccmCTIDeviceTable"         "1.3.6.1.4.1.9.9.156.1.8.1"
"ccmCTIDeviceDirNumTable"           "1.3.6.1.4.1.9.9.156.1.8.2"
"ccmCTIDeviceEntry"         "1.3.6.1.4.1.9.9.156.1.8.1.1"
```

```
"ccmCTIDeviceIndex"          "1.3.6.1.4.1.9.9.156.1.8.1.1.1"
"ccmCTIDeviceName"           "1.3.6.1.4.1.9.9.156.1.8.1.1.2"
"ccmCTIDeviceType"           "1.3.6.1.4.1.9.9.156.1.8.1.1.3"
"ccmCTIDeviceDescription"            "1.3.6.1.4.1.9.9.156.1.8.1.1.4"
"ccmCTIDeviceStatus"         "1.3.6.1.4.1.9.9.156.1.8.1.1.5"
"ccmCTIDevicePoolIndex"              "1.3.6.1.4.1.9.9.156.1.8.1.1.6"
"ccmCTIDeviceInetAddressType"                "1.3.6.1.4.1.9.9.156.1.8.1.1.7"
"ccmCTIDeviceInetAddress"            "1.3.6.1.4.1.9.9.156.1.8.1.1.8"
"ccmCTIDeviceAppInfo"                "1.3.6.1.4.1.9.9.156.1.8.1.1.9"
"ccmCTIDeviceStatusReason"           "1.3.6.1.4.1.9.9.156.1.8.1.1.10"
"ccmCTIDeviceTimeLastStatusUpdt"             "1.3.6.1.4.1.9.9.156.1.8.1.1.11"
"ccmCTIDeviceTimeLastRegistered"             "1.3.6.1.4.1.9.9.156.1.8.1.1.12"
"ccmCTIDeviceProductTypeIndex"               "1.3.6.1.4.1.9.9.156.1.8.1.1.13"
"ccmCTIDeviceInetAddressIPv4"                "1.3.6.1.4.1.9.9.156.1.8.1.1.14"
"ccmCTIDeviceInetAddressIPv6"                "1.3.6.1.4.1.9.9.156.1.8.1.1.15"
"ccmCTIDeviceUnregReason"            "1.3.6.1.4.1.9.9.156.1.8.1.1.16"
"ccmCTIDeviceRegFailReason"          "1.3.6.1.4.1.9.9.156.1.8.1.1.17"
"ccmCTIDeviceDirNumEntry"            "1.3.6.1.4.1.9.9.156.1.8.2.1"
"ccmCTIDeviceDirNumIndex"            "1.3.6.1.4.1.9.9.156.1.8.2.1.1"
"ccmCTIDeviceDirNum"         "1.3.6.1.4.1.9.9.156.1.8.2.1.2"
"ccmCallManagerAlarmEnable"          "1.3.6.1.4.1.9.9.156.1.9.1"
"ccmPhoneFailedAlarmInterval"                "1.3.6.1.4.1.9.9.156.1.9.2"
"ccmPhoneFailedStorePeriod"          "1.3.6.1.4.1.9.9.156.1.9.3"
"ccmPhoneStatusUpdateAlarmInterv"            "1.3.6.1.4.1.9.9.156.1.9.4"
"ccmPhoneStatusUpdateStorePeriod"            "1.3.6.1.4.1.9.9.156.1.9.5"
"ccmGatewayAlarmEnable"              "1.3.6.1.4.1.9.9.156.1.9.6"
"ccmMaliciousCallAlarmEnable"                "1.3.6.1.4.1.9.9.156.1.9.7"
"ccmAlarmSeverity"           "1.3.6.1.4.1.9.9.156.1.10.1"
"ccmFailCauseCode"           "1.3.6.1.4.1.9.9.156.1.10.2"
"ccmPhoneFailures"           "1.3.6.1.4.1.9.9.156.1.10.3"
"ccmPhoneUpdates"            "1.3.6.1.4.1.9.9.156.1.10.4"
"ccmGatewayFailCauseCode"            "1.3.6.1.4.1.9.9.156.1.10.5"
"ccmMediaResourceType"               "1.3.6.1.4.1.9.9.156.1.10.6"
"ccmMediaResourceListName"           "1.3.6.1.4.1.9.9.156.1.10.7"
"ccmRouteListName"           "1.3.6.1.4.1.9.9.156.1.10.8"
"ccmGatewayPhysIfIndex"              "1.3.6.1.4.1.9.9.156.1.10.9"
"ccmGatewayPhysIfL2Status"           "1.3.6.1.4.1.9.9.156.1.10.10"
"ccmMaliCallCalledPartyName"         "1.3.6.1.4.1.9.9.156.1.10.11"
"ccmMaliCallCalledPartyNumber"               "1.3.6.1.4.1.9.9.156.1.10.12"
"ccmMaliCallCalledDeviceName"                "1.3.6.1.4.1.9.9.156.1.10.13"
"ccmMaliCallCallingPartyName"                "1.3.6.1.4.1.9.9.156.1.10.14"
"ccmMaliCallCallingPartyNumber"              "1.3.6.1.4.1.9.9.156.1.10.15"
"ccmMaliCallCallingDeviceName"               "1.3.6.1.4.1.9.9.156.1.10.16"
"ccmMaliCallTime"            "1.3.6.1.4.1.9.9.156.1.10.17"
"ccmQualityRprtSourceDevName"                "1.3.6.1.4.1.9.9.156.1.10.18"
"ccmQualityRprtClusterId"            "1.3.6.1.4.1.9.9.156.1.10.19"
"ccmQualityRprtCategory"             "1.3.6.1.4.1.9.9.156.1.10.20"
"ccmQualityRprtReasonCode"           "1.3.6.1.4.1.9.9.156.1.10.21"
"ccmQualityRprtTime"         "1.3.6.1.4.1.9.9.156.1.10.22"
"ccmTLSDevName"              "1.3.6.1.4.1.9.9.156.1.10.23"
"ccmTLSDevInetAddressType"           "1.3.6.1.4.1.9.9.156.1.10.24"
"ccmTLSDevInetAddress"               "1.3.6.1.4.1.9.9.156.1.10.25"
"ccmTLSConnFailTime"         "1.3.6.1.4.1.9.9.156.1.10.26"
"ccmTLSConnectionFailReasonCode"             "1.3.6.1.4.1.9.9.156.1.10.27"
"ccmGatewayRegFailCauseCode"         "1.3.6.1.4.1.9.9.156.1.10.28"
"ccmH323DeviceTable"         "1.3.6.1.4.1.9.9.156.1.11.1"
"ccmH323DeviceEntry"         "1.3.6.1.4.1.9.9.156.1.11.1.1"
"ccmH323DevIndex"            "1.3.6.1.4.1.9.9.156.1.11.1.1.1"
"ccmH323DevName"             "1.3.6.1.4.1.9.9.156.1.11.1.1.2"
"ccmH323DevProductId"                "1.3.6.1.4.1.9.9.156.1.11.1.1.3"
"ccmH323DevDescription"              "1.3.6.1.4.1.9.9.156.1.11.1.1.4"
"ccmH323DevInetAddressType"          "1.3.6.1.4.1.9.9.156.1.11.1.1.5"
"ccmH323DevInetAddress"              "1.3.6.1.4.1.9.9.156.1.11.1.1.6"
"ccmH323DevCnfgGKInetAddressType"            "1.3.6.1.4.1.9.9.156.1.11.1.1.7"
"ccmH323DevCnfgGKInetAddress"                "1.3.6.1.4.1.9.9.156.1.11.1.1.8"
"ccmH323DevAltGK1InetAddressType"            "1.3.6.1.4.1.9.9.156.1.11.1.1.9"
"ccmH323DevAltGK1InetAddress"                "1.3.6.1.4.1.9.9.156.1.11.1.1.10"
"ccmH323DevAltGK2InetAddressType"            "1.3.6.1.4.1.9.9.156.1.11.1.1.11"
"ccmH323DevAltGK2InetAddress"                "1.3.6.1.4.1.9.9.156.1.11.1.1.12"
"ccmH323DevAltGK3InetAddressType"            "1.3.6.1.4.1.9.9.156.1.11.1.1.13"
"ccmH323DevAltGK3InetAddress"                "1.3.6.1.4.1.9.9.156.1.11.1.1.14"
"ccmH323DevAltGK4InetAddressType"            "1.3.6.1.4.1.9.9.156.1.11.1.1.15"
"ccmH323DevAltGK4InetAddress"                "1.3.6.1.4.1.9.9.156.1.11.1.1.16"
"ccmH323DevAltGK5InetAddressType"            "1.3.6.1.4.1.9.9.156.1.11.1.1.17"
"ccmH323DevAltGK5InetAddress"                "1.3.6.1.4.1.9.9.156.1.11.1.1.18"
"ccmH323DevActGKInetAddressType"             "1.3.6.1.4.1.9.9.156.1.11.1.1.19"
"ccmH323DevActGKInetAddress"         "1.3.6.1.4.1.9.9.156.1.11.1.1.20"
"ccmH323DevStatus"           "1.3.6.1.4.1.9.9.156.1.11.1.1.21"
"ccmH323DevStatusReason"             "1.3.6.1.4.1.9.9.156.1.11.1.1.22"
"ccmH323DevTimeLastStatusUpdt"               "1.3.6.1.4.1.9.9.156.1.11.1.1.23"
"ccmH323DevTimeLastRegistered"               "1.3.6.1.4.1.9.9.156.1.11.1.1.24"
"ccmH323DevRmtCM1InetAddressType"            "1.3.6.1.4.1.9.9.156.1.11.1.1.25"
"ccmH323DevRmtCM1InetAddress"                "1.3.6.1.4.1.9.9.156.1.11.1.1.26"
"ccmH323DevRmtCM2InetAddressType"            "1.3.6.1.4.1.9.9.156.1.11.1.1.27"
"ccmH323DevRmtCM2InetAddress"                "1.3.6.1.4.1.9.9.156.1.11.1.1.28"
"ccmH323DevRmtCM3InetAddressType"            "1.3.6.1.4.1.9.9.156.1.11.1.1.29"
"ccmH323DevRmtCM3InetAddress"                "1.3.6.1.4.1.9.9.156.1.11.1.1.30"
"ccmH323DevProductTypeIndex"         "1.3.6.1.4.1.9.9.156.1.11.1.1.31"
```

```
"ccmH323DevUnregReason"              "1.3.6.1.4.1.9.9.156.1.11.1.1.32"
"ccmH323DevRegFailReason"            "1.3.6.1.4.1.9.9.156.1.11.1.1.33"
"ccmVoiceMailDeviceTable"            "1.3.6.1.4.1.9.9.156.1.12.1"
"ccmVoiceMailDeviceDirNumTable"              "1.3.6.1.4.1.9.9.156.1.12.2"
"ccmVoiceMailDeviceEntry"            "1.3.6.1.4.1.9.9.156.1.12.1.1"
"ccmVMailDevIndex"          "1.3.6.1.4.1.9.9.156.1.12.1.1.1"
"ccmVMailDevName"           "1.3.6.1.4.1.9.9.156.1.12.1.1.2"
"ccmVMailDevProductId"               "1.3.6.1.4.1.9.9.156.1.12.1.1.3"
"ccmVMailDevDescription"             "1.3.6.1.4.1.9.9.156.1.12.1.1.4"
"ccmVMailDevStatus"         "1.3.6.1.4.1.9.9.156.1.12.1.1.5"
"ccmVMailDevInetAddressType"         "1.3.6.1.4.1.9.9.156.1.12.1.1.6"
"ccmVMailDevInetAddress"             "1.3.6.1.4.1.9.9.156.1.12.1.1.7"
"ccmVMailDevStatusReason"            "1.3.6.1.4.1.9.9.156.1.12.1.1.8"
"ccmVMailDevTimeLastStatusUpdt"              "1.3.6.1.4.1.9.9.156.1.12.1.1.9"
"ccmVMailDevTimeLastRegistered"              "1.3.6.1.4.1.9.9.156.1.12.1.1.10"
"ccmVMailDevProductTypeIndex"                "1.3.6.1.4.1.9.9.156.1.12.1.1.11"
"ccmVMailDevUnregReason"             "1.3.6.1.4.1.9.9.156.1.12.1.1.12"
"ccmVMailDevRegFailReason"           "1.3.6.1.4.1.9.9.156.1.12.1.1.13"
"ccmVoiceMailDeviceDirNumEntry"              "1.3.6.1.4.1.9.9.156.1.12.2.1"
"ccmVMailDevDirNumIndex"             "1.3.6.1.4.1.9.9.156.1.12.2.1.1"
"ccmVMailDevDirNum"         "1.3.6.1.4.1.9.9.156.1.12.2.1.2"
"ccmQualityReportAlarmEnable"                "1.3.6.1.4.1.9.9.156.1.13.1"
"ccmSIPDeviceTable"         "1.3.6.1.4.1.9.9.156.1.14.1"
"ccmSIPDeviceEntry"         "1.3.6.1.4.1.9.9.156.1.14.1.1"
"ccmSIPDevIndex"            "1.3.6.1.4.1.9.9.156.1.14.1.1.1"
"ccmSIPDevName"             "1.3.6.1.4.1.9.9.156.1.14.1.1.2"
"ccmSIPDevProductTypeIndex"          "1.3.6.1.4.1.9.9.156.1.14.1.1.3"
"ccmSIPDevDescription"               "1.3.6.1.4.1.9.9.156.1.14.1.1.4"
"ccmSIPDevInetAddressType"           "1.3.6.1.4.1.9.9.156.1.14.1.1.5"
"ccmSIPDevInetAddress"               "1.3.6.1.4.1.9.9.156.1.14.1.1.6"
"ccmSIPInTransportProtocolType"              "1.3.6.1.4.1.9.9.156.1.14.1.1.7"
"ccmSIPInPortNumber"        "1.3.6.1.4.1.9.9.156.1.14.1.1.8"
"ccmSIPOutTransportProtocolType"             "1.3.6.1.4.1.9.9.156.1.14.1.1.9"
"ccmSIPOutPortNumber"                "1.3.6.1.4.1.9.9.156.1.14.1.1.10"
"ccmSIPDevInetAddressIPv4"           "1.3.6.1.4.1.9.9.156.1.14.1.1.11"
"ccmSIPDevInetAddressIPv6"           "1.3.6.1.4.1.9.9.156.1.14.1.1.12"
"ccmMIBNotifications"                "1.3.6.1.4.1.9.9.156.2"
"ciscoCcmMIBCompliances"             "1.3.6.1.4.1.9.9.156.3.1"
"ciscoCcmMIBGroups"         "1.3.6.1.4.1.9.9.156.3.2"
"ciscoCcmMIBCompliance"              "1.3.6.1.4.1.9.9.156.3.1.1"
"ciscoCcmMIBComplianceRev1"          "1.3.6.1.4.1.9.9.156.3.1.2"
"ciscoCcmMIBComplianceRev2"          "1.3.6.1.4.1.9.9.156.3.1.3"
"ciscoCcmMIBComplianceRev3"          "1.3.6.1.4.1.9.9.156.3.1.4"
"ciscoCcmMIBComplianceRev4"          "1.3.6.1.4.1.9.9.156.3.1.5"
"ciscoCcmMIBComplianceRev5"          "1.3.6.1.4.1.9.9.156.3.1.6"
"ciscoCcmMIBComplianceRev6"          "1.3.6.1.4.1.9.9.156.3.1.7"
"ciscoCcmMIBComplianceRev7"          "1.3.6.1.4.1.9.9.156.3.1.8"
"ccmInfoGroup"              "1.3.6.1.4.1.9.9.156.3.2.1"
"ccmPhoneInfoGroup"         "1.3.6.1.4.1.9.9.156.3.2.2"
"ccmGatewayInfoGroup"                "1.3.6.1.4.1.9.9.156.3.2.3"
"ccmInfoGroupRev1"          "1.3.6.1.4.1.9.9.156.3.2.4"
"ccmPhoneInfoGroupRev1"              "1.3.6.1.4.1.9.9.156.3.2.5"
"ccmGatewayInfoGroupRev1"            "1.3.6.1.4.1.9.9.156.3.2.6"
"ccmMediaDeviceInfoGroup"            "1.3.6.1.4.1.9.9.156.3.2.7"
"ccmGatekeeperInfoGroup"             "1.3.6.1.4.1.9.9.156.3.2.8"
"ccmCTIDeviceInfoGroup"              "1.3.6.1.4.1.9.9.156.3.2.9"
"ccmNotificationsInfoGroup"          "1.3.6.1.4.1.9.9.156.3.2.10"
"ccmInfoGroupRev2"          "1.3.6.1.4.1.9.9.156.3.2.12"
"ccmPhoneInfoGroupRev2"              "1.3.6.1.4.1.9.9.156.3.2.13"
"ccmGatewayInfoGroupRev2"            "1.3.6.1.4.1.9.9.156.3.2.14"
"ccmMediaDeviceInfoGroupRev1"                "1.3.6.1.4.1.9.9.156.3.2.15"
"ccmCTIDeviceInfoGroupRev1"          "1.3.6.1.4.1.9.9.156.3.2.16"
"ccmH323DeviceInfoGroup"             "1.3.6.1.4.1.9.9.156.3.2.17"
"ccmVoiceMailDeviceInfoGroup"                "1.3.6.1.4.1.9.9.156.3.2.18"
"ccmNotificationsInfoGroupRev1"              "1.3.6.1.4.1.9.9.156.3.2.19"
"ccmInfoGroupRev3"          "1.3.6.1.4.1.9.9.156.3.2.20"
"ccmNotificationsInfoGroupRev2"              "1.3.6.1.4.1.9.9.156.3.2.21"
"ccmSIPDeviceInfoGroup"              "1.3.6.1.4.1.9.9.156.3.2.23"
"ccmPhoneInfoGroupRev3"              "1.3.6.1.4.1.9.9.156.3.2.24"
"ccmGatewayInfoGroupRev3"            "1.3.6.1.4.1.9.9.156.3.2.25"
"ccmMediaDeviceInfoGroupRev2"                "1.3.6.1.4.1.9.9.156.3.2.26"
"ccmCTIDeviceInfoGroupRev2"          "1.3.6.1.4.1.9.9.156.3.2.27"
"ccmH323DeviceInfoGroupRev1"         "1.3.6.1.4.1.9.9.156.3.2.28"
"ccmVoiceMailDeviceInfoGroupRev1"            "1.3.6.1.4.1.9.9.156.3.2.29"
"ccmPhoneInfoGroupRev4"              "1.3.6.1.4.1.9.9.156.3.2.30"
"ccmSIPDeviceInfoGroupRev1"          "1.3.6.1.4.1.9.9.156.3.2.31"
"ccmNotificationsInfoGroupRev3"              "1.3.6.1.4.1.9.9.156.3.2.32"
"ccmInfoGroupRev4"          "1.3.6.1.4.1.9.9.156.3.2.34"
"ccmPhoneInfoGroupRev5"              "1.3.6.1.4.1.9.9.156.3.2.35"
"ccmMediaDeviceInfoGroupRev3"                "1.3.6.1.4.1.9.9.156.3.2.36"
"ccmSIPDeviceInfoGroupRev2"          "1.3.6.1.4.1.9.9.156.3.2.37"
"ccmNotificationsInfoGroupRev4"              "1.3.6.1.4.1.9.9.156.3.2.38"
"ccmH323DeviceInfoGroupRev2"         "1.3.6.1.4.1.9.9.156.3.2.39"
"ccmCTIDeviceInfoGroupRev3"          "1.3.6.1.4.1.9.9.156.3.2.40"
"ccmPhoneInfoGroupRev6"              "1.3.6.1.4.1.9.9.156.3.2.41"
"ccmNotificationsInfoGroupRev5"              "1.3.6.1.4.1.9.9.156.3.2.42"
"ccmGatewayInfoGroupRev4"            "1.3.6.1.4.1.9.9.156.3.2.43"
"ccmMediaDeviceInfoGroupRev4"                "1.3.6.1.4.1.9.9.156.3.2.44"
```

```
"ccmCTIDeviceInfoGroupRev4"          "1.3.6.1.4.1.9.9.156.3.2.45"
"ccmH323DeviceInfoGroupRev3"         "1.3.6.1.4.1.9.9.156.3.2.46"
"ccmVoiceMailDeviceInfoGroupRev2"            "1.3.6.1.4.1.9.9.156.3.2.47"
"ccmNotificationsGroup"              "1.3.6.1.4.1.9.9.156.3.2.11"
"ccmNotificationsGroupRev1"          "1.3.6.1.4.1.9.9.156.3.2.22"
"ccmNotificationsGroupRev2"          "1.3.6.1.4.1.9.9.156.3.2.33"
"ccmNotificationsGroupRev3"          "1.3.6.1.4.1.9.9.156.3.2.48"
```

12.8. Anexo VIII: Árbol de OIDs de la MIB CISCO-ASSOCIATION-MIB.my

```
### THIS FILE WAS GENERATED BY MIB2SCHEMA
"org"               "1.3"
"dod"               "1.3.6"
"internet"          "1.3.6.1"
"directory"         "1.3.6.1.1"
"mgmt"              "1.3.6.1.2"
"experimental"              "1.3.6.1.3"
"private"           "1.3.6.1.4"
"enterprises"               "1.3.6.1.4.1"
"cisco"             "1.3.6.1.4.1.9"
"ciscoMgmt"         "1.3.6.1.4.1.9.9"
"ciscoDot11AssociationMIB"          "1.3.6.1.4.1.9.9.273"
"ciscoDot11AssocMIBObjects"         "1.3.6.1.4.1.9.9.273.1"
"ciscoDot11AssocMIBConformance"             "1.3.6.1.4.1.9.9.273.2"
"cDot11AssociationGlobal"           "1.3.6.1.4.1.9.9.273.1.1"
"cDot11ClientConfiguration"         "1.3.6.1.4.1.9.9.273.1.2"
"cDot11ClientStatistics"            "1.3.6.1.4.1.9.9.273.1.3"
"cDot11ParentAddress"               "1.3.6.1.4.1.9.9.273.1.1.1"
"cDot11ActiveDevicesTable"          "1.3.6.1.4.1.9.9.273.1.1.2"
"cDot11AssociationStatsTable"               "1.3.6.1.4.1.9.9.273.1.1.3"
"cd11IfCipherStatsTable"            "1.3.6.1.4.1.9.9.273.1.1.4"
"cDot11ActiveDevicesEntry"          "1.3.6.1.4.1.9.9.273.1.1.2.1"
"cDot11ActiveWirelessClients"               "1.3.6.1.4.1.9.9.273.1.1.2.1.1"
"cDot11ActiveBridges"               "1.3.6.1.4.1.9.9.273.1.1.2.1.2"
"cDot11ActiveRepeaters"             "1.3.6.1.4.1.9.9.273.1.1.2.1.3"
"cDot11AssociationStatsEntry"               "1.3.6.1.4.1.9.9.273.1.1.3.1"
"cDot11AssStatsAssociated"          "1.3.6.1.4.1.9.9.273.1.1.3.1.1"
"cDot11AssStatsAuthenticated"               "1.3.6.1.4.1.9.9.273.1.1.3.1.2"
"cDot11AssStatsRoamedIn"            "1.3.6.1.4.1.9.9.273.1.1.3.1.3"
"cDot11AssStatsRoamedAway"          "1.3.6.1.4.1.9.9.273.1.1.3.1.4"
"cDot11AssStatsDeauthenticated"             "1.3.6.1.4.1.9.9.273.1.1.3.1.5"
"cDot11AssStatsDisassociated"               "1.3.6.1.4.1.9.9.273.1.1.3.1.6"
"cd11IfCipherStatsEntry"            "1.3.6.1.4.1.9.9.273.1.1.4.1"
"cd11IfCipherMicFailClientAddress"          "1.3.6.1.4.1.9.9.273.1.1.4.1.1"
"cd11IfCipherTkipLocalMicFailures"          "1.3.6.1.4.1.9.9.273.1.1.4.1.2"
"cd11IfCipherTkipRemotMicFailures"          "1.3.6.1.4.1.9.9.273.1.1.4.1.3"
"cd11IfCipherTkipCounterMeasInvok"          "1.3.6.1.4.1.9.9.273.1.1.4.1.4"
"cd11IfCipherCcmpReplaysDiscarded"          "1.3.6.1.4.1.9.9.273.1.1.4.1.5"
"cd11IfCipherTkipReplaysDetected"           "1.3.6.1.4.1.9.9.273.1.1.4.1.6"
"cDot11ClientConfigInfoTable"               "1.3.6.1.4.1.9.9.273.1.2.1"
"cDot11ClientConfigInfoEntry"               "1.3.6.1.4.1.9.9.273.1.2.1.1"
"cDot11ClientAddress"               "1.3.6.1.4.1.9.9.273.1.2.1.1.1"
"cDot11ClientParentAddress"         "1.3.6.1.4.1.9.9.273.1.2.1.1.2"
"cDot11ClientRoleClassType"         "1.3.6.1.4.1.9.9.273.1.2.1.1.3"
"cDot11ClientDevType"               "1.3.6.1.4.1.9.9.273.1.2.1.1.4"
"cDot11ClientRadioType"             "1.3.6.1.4.1.9.9.273.1.2.1.1.5"
"cDot11ClientWepEnabled"            "1.3.6.1.4.1.9.9.273.1.2.1.1.6"
"cDot11ClientWepKeyMixEnabled"              "1.3.6.1.4.1.9.9.273.1.2.1.1.7"
"cDot11ClientMicEnabled"            "1.3.6.1.4.1.9.9.273.1.2.1.1.8"
"cDot11ClientPowerSaveMode"         "1.3.6.1.4.1.9.9.273.1.2.1.1.9"
"cDot11ClientAid"           "1.3.6.1.4.1.9.9.273.1.2.1.1.10"
"cDot11ClientDataRateSet"           "1.3.6.1.4.1.9.9.273.1.2.1.1.11"
"cDot11ClientSoftwareVersion"               "1.3.6.1.4.1.9.9.273.1.2.1.1.12"
"cDot11ClientName"          "1.3.6.1.4.1.9.9.273.1.2.1.1.13"
"cDot11ClientAssociationState"              "1.3.6.1.4.1.9.9.273.1.2.1.1.14"
"cDot11ClientIpAddressType"         "1.3.6.1.4.1.9.9.273.1.2.1.1.15"
"cDot11ClientIpAddress"             "1.3.6.1.4.1.9.9.273.1.2.1.1.16"
"cDot11ClientVlanId"        "1.3.6.1.4.1.9.9.273.1.2.1.1.17"
"cDot11ClientSubIfIndex"            "1.3.6.1.4.1.9.9.273.1.2.1.1.18"
"cDot11ClientAuthenAlgorithm"               "1.3.6.1.4.1.9.9.273.1.2.1.1.19"
"cDot11ClientAdditionalAuthen"              "1.3.6.1.4.1.9.9.273.1.2.1.1.20"
"cDot11ClientDot1xAuthenAlgorithm"          "1.3.6.1.4.1.9.9.273.1.2.1.1.21"
"cDot11ClientKeyManagement"         "1.3.6.1.4.1.9.9.273.1.2.1.1.22"
"cDot11ClientUnicastCipher"         "1.3.6.1.4.1.9.9.273.1.2.1.1.23"
"cDot11ClientMulticastCipher"               "1.3.6.1.4.1.9.9.273.1.2.1.1.24"
"cDot11ClientDevObjectID"           "1.3.6.1.4.1.9.9.273.1.2.1.1.25"
"cDot11ClientNewKeyManagement"              "1.3.6.1.4.1.9.9.273.1.2.1.1.26"
"cDot11ClientStatisticTable"        "1.3.6.1.4.1.9.9.273.1.3.1"
"cDot11ClientStatisticEntry"        "1.3.6.1.4.1.9.9.273.1.3.1.1"
"cDot11ClientCurrentTxRateSet"              "1.3.6.1.4.1.9.9.273.1.3.1.1.1"
"cDot11ClientUpTime"        "1.3.6.1.4.1.9.9.273.1.3.1.1.2"
"cDot11ClientSignalStrength"        "1.3.6.1.4.1.9.9.273.1.3.1.1.3"
"cDot11ClientSigQuality"            "1.3.6.1.4.1.9.9.273.1.3.1.1.4"
"cDot11ClientAgingLeft"             "1.3.6.1.4.1.9.9.273.1.3.1.1.5"
```

```
"cDot11ClientPacketsReceived"                "1.3.6.1.4.1.9.9.273.1.3.1.1.6"
"cDot11ClientBytesReceived"          "1.3.6.1.4.1.9.9.273.1.3.1.1.7"
"cDot11ClientPacketsSent"            "1.3.6.1.4.1.9.9.273.1.3.1.1.8"
"cDot11ClientBytesSent"              "1.3.6.1.4.1.9.9.273.1.3.1.1.9"
"cDot11ClientDuplicates"             "1.3.6.1.4.1.9.9.273.1.3.1.1.10"
"cDot11ClientMsduRetries"            "1.3.6.1.4.1.9.9.273.1.3.1.1.11"
"cDot11ClientMsduFails"              "1.3.6.1.4.1.9.9.273.1.3.1.1.12"
"cDot11ClientWepErrors"              "1.3.6.1.4.1.9.9.273.1.3.1.1.13"
"cDot11ClientMicErrors"              "1.3.6.1.4.1.9.9.273.1.3.1.1.14"
"cDot11ClientMicMissingFrames"               "1.3.6.1.4.1.9.9.273.1.3.1.1.15"
"ciscoDot11AssocMIBCompliances"              "1.3.6.1.4.1.9.9.273.2.1"
"ciscoDot11AssocMIBGroups"           "1.3.6.1.4.1.9.9.273.2.2"
"ciscoDot11AssocMIBCompliance"               "1.3.6.1.4.1.9.9.273.2.1.1"
"ciscoDot11AssocMIBComplianceRev1"           "1.3.6.1.4.1.9.9.273.2.1.2"
"ciscoDot11AssocMIBComplianceRev2"           "1.3.6.1.4.1.9.9.273.2.1.3"
"ciscoDot11AssocMIBComplianceRev3"           "1.3.6.1.4.1.9.9.273.2.1.4"
"ciscoDot11AssocMIBComplianceRev4"           "1.3.6.1.4.1.9.9.273.2.1.5"
"ciscoDot11AssocMIBComplianceRev5"           "1.3.6.1.4.1.9.9.273.2.1.6"
"ciscoDot11AssocGlobalGroup"         "1.3.6.1.4.1.9.9.273.2.2.1"
"ciscoDot11ClientConfigGroup"                "1.3.6.1.4.1.9.9.273.2.2.2"
"ciscoDot11ClientStatGroup"          "1.3.6.1.4.1.9.9.273.2.2.3"
"ciscoDot11ClientInfoGroup"          "1.3.6.1.4.1.9.9.273.2.2.4"
"ciscoDot11ApAssocGlobalGroup"               "1.3.6.1.4.1.9.9.273.2.2.5"
"ciscoDot11IfAssocStatGroup"         "1.3.6.1.4.1.9.9.273.2.2.6"
"ciscoDot11IfCipherStatGroup"                "1.3.6.1.4.1.9.9.273.2.2.7"
"ciscoDot11ClientAuthenGroup"                "1.3.6.1.4.1.9.9.273.2.2.8"
"ciscoDot11ClientConfigExtGroup"             "1.3.6.1.4.1.9.9.273.2.2.9"
"ciscoDot11ClientNewAuthenGroup"             "1.3.6.1.4.1.9.9.273.2.2.10"
```

12.9. Anexo IX: HTTP MIB

```
HTTPSERVER-MIB DEFINITIONS ::= BEGIN

        IMPORTS
                enterprises,
                OBJECT-TYPE,
                Counter
                        FROM RFC1155-SMI
                internetServer
                        FROM INTERNETSERVER-MIB;

--      microsoft       OBJECT IDENTIFIER ::= { enterprises 311 }
--      software        OBJECT IDENTIFIER ::= { microsoft 1 }
--      internetServer  OBJECT IDENTIFIER ::= { software 7 }
        httpServer      OBJECT IDENTIFIER ::= { internetServer 3 }
        httpStatistics  OBJECT IDENTIFIER ::= { httpServer 1 }

-- Http Server Statistics

        totalBytesSentHighWord OBJECT-TYPE
                SYNTAX  Counter
                ACCESS  read-only
                STATUS  mandatory
                DESCRIPTION
                        "This is the high 32-bits of the total number of
                        of BYTEs sent by the HTTP Server."
                ::= { httpStatistics 1 }

        totalBytesSentLowWord OBJECT-TYPE
                SYNTAX  Counter
                ACCESS  read-only
                STATUS  mandatory
                DESCRIPTION
                        "This is the low 32-bits of the total number of
                        of BYTEs sent by the HTTP Server."
                ::= { httpStatistics 2 }

        totalBytesReceivedHighWord OBJECT-TYPE
                SYNTAX  Counter
                ACCESS  read-only
                STATUS  mandatory
                DESCRIPTION
                        "This is the high 32-bits of the total number of
                        of BYTEs received by the HTTP Server."
                ::= { httpStatistics 3 }

        totalBytesReceivedLowWord OBJECT-TYPE
                SYNTAX  Counter
                ACCESS  read-only
                STATUS  mandatory
                DESCRIPTION
                        "This is the low 32-bits of the total number of
                        of BYTEs received by the HTTP Server."
                ::= { httpStatistics 4 }

        totalFilesSent OBJECT-TYPE
                SYNTAX  Counter
```

```
        ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
                "This is the total number of files sent by this
                HTTP Server."
        ::= { httpStatistics 5 }

totalFilesReceived OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
                "This is the total number of files received by this
                HTTP Server."
        ::= { httpStatistics 6 }

currentAnonymousUsers OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
                "This is the number of anonymous users currently
                connected to the HTTP Server."
        ::= { httpStatistics 7 }

currentNonAnonymousUsers OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
                "This is the number of nonanonymous users currently
                connected to the HTTP Server."
        ::= { httpStatistics 8  }

totalAnonymousUsers OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
                "This is the total number of anonymous users that
                have ever connected to the HTTP Server."
        ::= { httpStatistics 9  }

totalNonAnonymousUsers OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
                "This is the total number of nonanonymous users that
                have ever connected to the HTTP Server."
        ::= { httpStatistics 10  }

maxAnonymousUsers OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
                "This is the maximum number of anonymous users
                simultaneously connected to the HTTP Server."
        ::= { httpStatistics 11 }

maxNonAnonymousUsers OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
                "This is the maximum number of nonanonymous users
                simultaneously connected to the HTTP Server."
        ::= { httpStatistics 12 }

currentConnections OBJECT-TYPE
        SYNTAX  INTEGER
        ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
                "This is the current number of connections to the
                HTTP Server."
        ::= { httpStatistics 13 }

maxConnections OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
                "This is the maximum number of simultaneous
                connections to the HTTP Server."
        ::= { httpStatistics 14 }
```

```
connectionAttempts OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
                "This is the number of connection attempts that
                have been made to the HTTP Server."
        ::= { httpStatistics 15 }

logonAttempts OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
                "This is the number of logon attempts that have
                been made to this HTTP Server."
        ::= { httpStatistics 16 }

totalOptions OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
                "This is the number of requests using the OPTIONS method
                that have been made to this HTTP Server."
        ::= { httpStatistics 17 }

totalGets OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
                "This is the number of requests using the GET method
                that have been made to this HTTP Server."
        ::= { httpStatistics 18 }

totalPosts OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
                "This is the number of requests using the POST method
                that have been made to this HTTP Server."
        ::= { httpStatistics 19 }

totalHeads OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
                "This is the number of requests using the HEAD method
                that have been made to this HTTP Server."
        ::= { httpStatistics 20 }

totalPuts OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
                "This is the number of requests using the PUT method
                that have been made to this HTTP Server."
        ::= { httpStatistics 21 }

totalDeletes OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
                "This is the number of requests using the DELETE method
                that have been made to this HTTP Server."
        ::= { httpStatistics 22 }

totalTraces OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
                "This is the number of requests using the TRACE method
                that have been made to this HTTP Server."
        ::= { httpStatistics 23 }

totalMove OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
                "This is the number of requests using the MOVE method
                that have been made to this HTTP Server."
```

```
        ::= { httpStatistics 24 }

totalCopy OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
                "This is the number of requests using the COPY method
                that have been made to this HTTP Server."
        ::= { httpStatistics 25 }

totalMkcol OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
                "This is the number of requests using the MKCOL method
                that have been made to this HTTP Server."
        ::= { httpStatistics 26 }

totalPropfind OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
                "This is the number of requests using the PROPFIND method
                that have been made to this HTTP Server."
        ::= { httpStatistics 27 }

totalProppatch OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
                "This is the number of requests using the PROPPATCH method
                that have been made to this HTTP Server."
        ::= { httpStatistics 28 }

totalSearch OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
                "This is the number of requests using the MS-SEARCH method
                that have been made to this HTTP Server."
        ::= { httpStatistics 29 }

totalLock OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
                "This is the number of requests using the LOCK method
                that have been made to this HTTP Server."
        ::= { httpStatistics 30 }

totalUnlock OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
                "This is the number of requests using the UNLOCK method
                that have been made to this HTTP Server."
        ::= { httpStatistics 31 }

totalOthers OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
                "This is the number of requests not using the OPTIONS, GET, HEAD
                POST, PUT, DELETE, TRACE, MOVE, COPY, MKCOL, PROPFIND, PROPPATCH,
                MS-SEARCH, LOCK or UNLOCK method that have been made to this HTTP
                Server. This may include LINK or other methods supported by gateway
                applications."
        ::= { httpStatistics 32 }

currentCGIRequests OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
                "This is the number of Common Gateway Interface (CGI)
                 requests that are currently being serviced by this HTTP Server."
        ::= { httpStatistics 33 }

currentBGIRequests OBJECT-TYPE
        SYNTAX  Counter
```

```
        ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
                "This is the number of Binary Gateway Interface (BGI)
                requests that are currently being serviced by this HTTP Server."
        ::= { httpStatistics 34 }

totalCGIRequests OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
                "This is the number of Common Gateway Interface (CGI)
                requests that have been made to this HTTP Server."
        ::= { httpStatistics 35 }

totalBGIRequests OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
                "This is the number of Binary Gateway Interface (BGI)
                requests that have been made to this HTTP Server."
        ::= { httpStatistics 36 }

maxCGIRequests OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
                "This is the maximum number of Common Gateway Interface (CGI)
                requests simultaneous processed by this HTTP Server."
        ::= { httpStatistics 37 }

maxBGIRequests OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
                "This is the maximum number of Binary Gateway Interface (BGI)
                requests simultaneous processed by this HTTP Server."
        ::= { httpStatistics 38 }

currentBlockedRequests OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
                "This is the current number of requests that have been temporarily
                blocked by this HTTP Server due to bandwidth throttling settings."
        ::= { httpStatistics 39 }

totalBlockedRequests OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
                "This is the total number of requests that have been temporarily
                blocked by this HTTP Server due to bandwidth throttling settings."
        ::= { httpStatistics 40 }

totalAllowedRequests OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
                "This is the total number of requests that have been allowed
                by the bandwidth throttling settings on this HTTP Server."
        ::= { httpStatistics 41 }

totalRejectedRequests OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
                "This is the total number of requests that have been rejected
                by this HTTP Server due to bandwidth throttling settings."
        ::= { httpStatistics 42 }

totalNotFoundErrors OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
                "This is the total number of requests the HTTP server could
                not satisfy because the requested resource could not
                be found."
        ::= { httpStatistics 43 }
```

```
        totalLockedErrors OBJECT-TYPE
                SYNTAX  Counter
                ACCESS  read-only
                STATUS  mandatory
                DESCRIPTION
                        "This is the total number of requests the HTTP server could
                        not satisfy because the requested resource was locked."
                ::= { httpStatistics 44 }

        measuredBandwidth OBJECT-TYPE
                SYNTAX  Counter
                ACCESS  read-only
                STATUS  mandatory
                DESCRIPTION
                        "This is the I/O bandwidth used by this HTTP Server,
                        averaged over a minute."
                ::= { httpStatistics 45 }

        currentCALsforAuthenticatedUsers OBJECT-TYPE
                SYNTAX  Counter
                ACCESS  read-only
                STATUS  mandatory
                DESCRIPTION
                        "This is the current count of Client Access Licenses (CALs)
                        available to this HTTP Server for simultaneous use by authenticated
                        users."
                ::= { httpStatistics 46 }

        maxCALsforAuthenticatedUsers OBJECT-TYPE
                SYNTAX  Counter
                ACCESS  read-only
                STATUS  mandatory
                DESCRIPTION
                        "This is the maximum count of Client Access Licenses (CALs)
                        used by this HTTP Server for simultaneous use by authenticated
                        users."
                ::= { httpStatistics 47 }

        totalCALFailedAuthenticatedUser OBJECT-TYPE
                SYNTAX  Counter
                ACCESS  read-only
                STATUS  mandatory
                DESCRIPTION
                        "This is the total number of HTTP requests that have failed on this
                        HTTP server due to a Client Access License (CAL) being unavailable for
                        an authenticated user."
                ::= { httpStatistics 48 }

        currentCALsforSecureConnections OBJECT-TYPE
                SYNTAX  Counter
                ACCESS  read-only
                STATUS  mandatory
                DESCRIPTION
                        "This is the current count of Client Access Licenses (CALs)
                        available to this HTTP Server for simultaneous use by secure
                        connections."
                ::= { httpStatistics 49 }

        maxCALsforSecureConnections OBJECT-TYPE
                SYNTAX  Counter
                ACCESS  read-only
                STATUS  mandatory
                DESCRIPTION
                        "This is the maximum count of Client Access Licenses (CALs)
                        available to this Http Server for simultaneous use by secure
                        connections."
                ::= { httpStatistics 50 }

        totalCALFailedSecureConnection OBJECT-TYPE
                SYNTAX  Counter
                ACCESS  read-only
                STATUS  mandatory
                DESCRIPTION
                        "This is the total number of HTTP requests that have failed on this
                        HTTP server due to a Client Access License (CAL) being unavailable for
                        use by a secure connection."
                ::= { httpStatistics 51 }

END
```

12.10. Anexo X: Código Java check_tablespace_oracle

```
// ----------------------------------------------------------------------------
// check_tablespace_oracle.java 20100820 frank4dd version 1.0
// ----------------------------------------------------------------------------
```

```
// e-mail: support[at]frank4dd.com
// web: http://www.frank4dd.com/howto/nagios/db-monitoring.htm
//
// This nagios plugin queries the Oracle dba_free_space and dba_data_files
// system tables. Supported are Oracle versions 10g and up.
//
// Pre-requisites: Oracle JDBC driver installed and a valid DB user.
// ------------------------------------------------------------------------
// Example Output:
// > java check_tablespace_oracle 127.0.0.1 1521 XE system test -d
// DB connect: jdbc:oracle:thin:system/test@127.0.0.1:1521:XE
// DB query: select  df.TABLESPACE_NAME, df.FILE_ID, ((df.BYTES+fs.BYTES)/1024) kbytes_max,
// (df.BYTES/1024) kbytes_used, round(((df.BYTES - fs.BYTES) / df.BYTES) * 100) usage_pct
// from ( select  TABLESPACE_NAME, sum(BYTES) BYTES, count(distinct FILE_ID) FILE_ID from
// dba_data_files group by TABLESPACE_NAME ) df, ( select TABLESPACE_NAME, sum(BYTES) BYTES
// from dba_free_space group by TABLESPACE_NAME) fs where df.TABLESPACE_NAME=fs.TABLESPACE_NAME
// order by df.TABLESPACE_NAME asc
//Name:                  SYSAUX Files:  1 Space total:      374912 KB Space used:      317440 KB
Space % used:  82 %
//Name:                  SYSTEM Files:  1 Space total:      350208 KB Space used:      348160 KB
Space % used:  99 %
//Name:                    UNDO Files:  1 Space total:      384384 KB Space used:      215040 KB
Space % used:  21 %
//Name:                   USERS Files:  1 Space total:      203136 KB Space used:      102400 KB
Space % used:   2 %
// ------------------------------------------------------------------------
import java.sql.*;

class check_tablespace_oracle {

  static int kbytes_warn = 0;  // the commandline argument for warning threshold of KB used
  static int kbytes_crit = 0;  // the commandline argument for critical threshold of KB used
  static int dfiles_total= 0;  // the returned number of tablespace files
  static int kbytes_used = 0;  // the returned tablespace value of used KB
  static int kbytes_total= 0;  // the returned tablespace value of total KB available
  static int percent_used= 0;  // the returned tablespace value, current space used in percent
  static int return_code = 0;  // 'OK'=>0,'WARNING'=>1,'CRITICAL'=>2,'UNKNOWN'=>3,'DEPENDENT'=>4
  static int debug       = 0;  // 'normal'=>0,'verbose'=>1 when -d parameter is given
  static String output   = ""; // the plugin output string
  static String perfdata = ""; // the plugin perfdata output, returning the KB values
  static String tbspname = ""; // the tablespace to check
  static String dbUrl    = ""; // the access URL for the database to query
  static String query    = ""; // the SQL query to execute

  public static void main (String args[]) {
    if (args.length < 6) {
      System.err.println("Error: Missing Arguments.");
      System.err.println("Syntax: java check_tablespace_oracle <db-ip> <db-port> <db-instance>
<db-user> <db-pwd> <tablespace-name> <kbytes-warn> <kbytes-crit>");
      System.err.println("         java check_tablespace_oracle <db-ip> <db-port> <db-instance>
<db-user> <db-pwd> -r <tablespace-name>");
      System.err.println("         java check_tablespace_oracle <db-ip> <db-port> <db-instance>
<db-user> <db-pwd> -d");
      System.exit(-1);
    }
    // Check if we got a particular tablespace to check for
    if (args.length == 6 && args[5].equals("-d")) { debug = 1;}

    dbUrl = "jdbc:oracle:thin:" + args[3] + "/" + args[4] + "@" + args[0] +":" + args[1] +":" +
args[2];
    if (debug == 1) { System.out.println("DB connect: " + dbUrl); }

    // Check if we just return the data without any values to compare to
    if (args.length == 7 && args[5].equals("-r")) {
      tbspname = args[6];
    }

    // Check if we got warn and crit values to check against
    if (args.length == 8) {
      tbspname = args[5];
      kbytes_warn = Integer.parseInt(args[6]);
      kbytes_crit = Integer.parseInt(args[7]);
    }


    try {
      // use the Oracle JDBC driver
      Class.forName("oracle.jdbc.driver.OracleDriver");
    } catch (ClassNotFoundException e) {
      System.err.println("Error: JDBC Driver Problem.");
      System.err.println (e);
      System.exit (3);
    }
   try {
      // open connection to database "jdbc:oracle:thin:@destinationhost:port:dbname", "dbuser",
"dbpassword"
      Connection connection = DriverManager.getConnection(dbUrl);
```

```
      // build query

      // table dba_data_files: TABLESPACE_NAME,  FILE_NAME, BYTES, MAXBYTES, AUTOEXTENSIBLE
      // dba_free_space: TABLESPACE_NAME,  FILE_ID, BYTES
      // Show free tablespace: Select tablespace_name, Sum(bytes/(1024)) "Total Free (KB) " From
dba_free_space Group By tablespace_name;
      // Show used tablespace: Select tablespace_name, Sum(bytes/(1024)) "Total Used (KB) " From
dba_data_files Group By tablespace_name;
      if (tbspname == "") {
        query = "select  df.TABLESPACE_NAME, df.FILE_ID, ((df.BYTES+fs.BYTES)/1024) kbytes_max,
(df.BYTES/1024) kbytes_used, round(((df.BYTES - fs.BYTES) / df.BYTES) * 100) usage_pct from (
select  TABLESPACE_NAME, sum(BYTES) BYTES, count(distinct FILE_ID) FILE_ID from dba_data_files
group by TABLESPACE_NAME ) df, ( select TABLESPACE_NAME, sum(BYTES) BYTES from dba_free_space
group   by   TABLESPACE_NAME)   fs   where   df.TABLESPACE_NAME=fs.TABLESPACE_NAME   order   by
df.TABLESPACE_NAME asc";
      } else {
        query = "select  df.TABLESPACE_NAME, df.FILE_ID, ((df.BYTES+fs.BYTES)/1024) kbytes_max,
(df.BYTES/1024) kbytes_used, round(((df.BYTES - fs.BYTES) / df.BYTES) * 100) usage_pct from (
select  TABLESPACE_NAME, sum(BYTES) BYTES, count(distinct FILE_ID) FILE_ID from dba_data_files
where  TABLESPACE_NAME  =  '" + tbspname + "' group by TABLESPACE_NAME) df, ( select
TABLESPACE_NAME, sum(BYTES) BYTES from dba_free_space group by TABLESPACE_NAME) fs where
df.TABLESPACE_NAME=fs.TABLESPACE_NAME order by df.TABLESPACE_NAME asc";
      }
      if (debug == 1) { System.out.println ("DB query: " + query); }

      // execute query
      Statement statement = connection.createStatement ();
      ResultSet rs = statement.executeQuery (query);

      while ( rs.next () ) {
        // get content from column "1 -4"
        if (debug == 1) {
          System.out.format ("Name: %20s ", rs.getString (1));      // TBSP_NAME, VARCHAR(128)
          System.out.format ("Files: %2d ", rs.getInt(2));// TBSP_TOTAL_SIZE_KB, BIGINT
          System.out.format  ("Space  total:  %10d  KB  ",  rs.getInt(3));//  TBSP_TOTAL_SIZE_KB,
BIGINT
          System.out.format ("Space used: %10d KB ", rs.getInt(4)); // TBSP_USED_SIZE_KB, BIGINT
          System.out.format    ("Space    %%    used:    %3d    %%\n",    rs.getInt(5));    //
TBSP_UTILIZATION_PERCENT, BIGINT
        }
        tbspname=rs.getString (1);
        dfiles_total=rs.getInt(2);
        kbytes_total=rs.getInt(3);
        kbytes_used=rs.getInt(4);
        percent_used=rs.getInt(5);
      }

      rs.close () ;
      statement.close () ;
      connection.close () ;

    } catch (java.sql.SQLException e) {
      System.err.println (e) ;
      System.exit (3) ; // Unknown
    }

    perfdata = tbspname + ": " +dfiles_total + " datafiles, used " + kbytes_used + " KB of " +
kbytes_total + " KB total";
    output = tbspname + " " + percent_used + "% used" + "|" + perfdata;

    if ( (kbytes_warn != 0) && (kbytes_crit != 0) ) {
      if ( kbytes_used < kbytes_warn ) {
        System.out.println("Tablespace OK: " + output);
        System.exit (0); // OK
      }
      if ( kbytes_used >= kbytes_warn && kbytes_used < kbytes_crit ) {
        System.out.println("Tablespace WARN: "  + output);
        System.exit (1); // WARN
      }
      if ( kbytes_used  >= kbytes_crit ) {
        System.out.println("Tablespace CRIT: "  + output);
        System.exit (2); // CRIT
      }
    }
    if (args.length == 7 && args[5].equals("-r")) {
      System.out.println("Tablespace OK: " + output);
      System.exit (0); // OK
    }
  }
}
```

12.11. Anexo XI: Código Java de check_users_oracle

```
// --------------------------------------------------------------------------
// check_tablespace_oracle.java 20100820 frank4dd version 1.0
// --------------------------------------------------------------------------
```

```
// e-mail: support[at]frank4dd.com
// web: http://www.frank4dd.com/howto/nagios/db-monitoring.htm
//
// This nagios plugin queries the Oracle dba_free_space and dba_data_files
// system tables. Supported are Oracle versions 10g and up.
//
// Pre-requisites: Oracle JDBC driver installed and a valid DB user.
// ------------------------------------------------------------------------
// Example Output:
// > java check_tablespace_oracle 127.0.0.1 1521 XE system test -d
// DB connect: jdbc:oracle:thin:system/test@127.0.0.1:1521:XE
// DB query: select  df.TABLESPACE_NAME, df.FILE_ID, ((df.BYTES+fs.BYTES)/1024) kbytes_max,
// (df.BYTES/1024) kbytes_used, round(((df.BYTES - fs.BYTES) / df.BYTES) * 100) usage_pct
// from ( select  TABLESPACE_NAME, sum(BYTES) BYTES, count(distinct FILE_ID) FILE_ID from
// dba_data_files group by TABLESPACE_NAME ) df, ( select TABLESPACE_NAME, sum(BYTES) BYTES
// from dba_free_space group by TABLESPACE_NAME) fs where df.TABLESPACE_NAME=fs.TABLESPACE_NAME
// order by df.TABLESPACE_NAME asc
//Name:                  SYSAUX Files:  1 Space total:      374912 KB Space used:      317440 KB
Space % used:  82 %
//Name:                  SYSTEM Files:  1 Space total:      350208 KB Space used:      348160 KB
Space % used:  99 %
//Name:                    UNDO Files:  1 Space total:      384384 KB Space used:      215040 KB
Space % used:  21 %
//Name:                   USERS Files:  1 Space total:      203136 KB Space used:      102400 KB
Space % used:   2 %
// ------------------------------------------------------------------------
import java.sql.*;

class check_users_oracle {

  static int usuarios_warn = 0;  // the commandline argument for warning threshold of KB used
  static int usuarios_crit = 0;  // the commandline argument for critical threshold of KB used

  static String output   = ""; // the plugin output string

  static String dbUrl    = ""; // the access URL for the database to query
  static String query    = ""; // the SQL query to execute
  static int usuarios_conectados = 0;
  public static void main (String args[]) {


    dbUrl = "jdbc:oracle:thin:" + args[3] + "/" + args[4] + "@" + args[0] +":" + args[1] +":" +
args[2];


      usuarios_warn = Integer.parseInt(args[5]);
      usuarios_crit = Integer.parseInt(args[6]);



    try {
      // use the Oracle JDBC driver
      Class.forName("oracle.jdbc.driver.OracleDriver");
    } catch (ClassNotFoundException e) {
      System.err.println("Error: JDBC Driver Problem.");
      System.err.println (e);
      System.exit (3);
    }
   try {
      // open connection to database "jdbc:oracle:thin:@destinationhost:port:dbname", "dbuser",
"dbpassword"
      Connection connection = DriverManager.getConnection(dbUrl);

      // build query

      // table dba_data_files: TABLESPACE_NAME,  FILE_NAME, BYTES, MAXBYTES, AUTOEXTENSIBLE
      // dba_free_space: TABLESPACE_NAME,  FILE_ID, BYTES
      // Show free tablespace: Select tablespace_name, Sum(bytes/(1024)) "Total Free (KB) " From
dba_free_space Group By tablespace_name;
      // Show used tablespace: Select tablespace_name, Sum(bytes/(1024)) "Total Used (KB) " From
dba_data_files Group By tablespace_name;

        query = "SELECT username,sid,serial# FROM v$session";



      // execute query
      Statement statement = connection.createStatement ();
      ResultSet rs = statement.executeQuery (query);

      while ( rs.next () ) {
        // get content from column "1 -4"
        usuarios_conectados++;
        output += rs.getString (1) + ", ";

      }

      rs.close () ;
```

```
      statement.close () ;
      connection.close () ;

    } catch (java.sql.SQLException e) {
      System.err.println (e) ;
      System.exit (3) ; // Unknown
    }
System.out.println(output);

if (usuarios_conectados > usuarios_warn)
{
    if(usuarios_conectados > usuarios_crit)
            System.exit(2);
    else
            System.exit(1);
}
else
    System.exit(0);


  }
}
```

12.12. Anexo XII: Comandos y servicios de Oracle configurados

```
COMANDOS

define command{
            command_name        check_oracle_instant
            command_line               $USER1$/check_oracle_instant  $HOSTADDRESS$  $ARG1$  $ARG2$
$ARG3$ $ARG4$
}

define command{
            command_name        check_tablespace_oracle
            command_line                              java   -classpath   /usr/local/nagios/libexec/
check_tablespace_oracle 10.36.32.10 1521 orcl CSMA "CSMA" -d
}
define command{
            command_name        check_tablespace_oracle2
            command_line                              java   -classpath   /usr/local/nagios/libexec/
check_tablespace_oracle 10.36.32.10 1521 orcl CSMA "CSMA" USERS 1000000 3000000
}
define command{
            command_name        check_users_oracle
            command_line           java -classpath /usr/local/nagios/libexec/ check_users_oracle
10.36.32.10 1521 orcl CSMA "CSMA" 70 100
}

SERVICIOS

define service{
        use                             local-service         ; Name of service template to use
        host_name                       oracleserver
        service_description             PING
            check_command                                 check_ping!100.0,20%!500.0,60%
        }



define service{
        use                             local-service         ; Name of service template to use
        host_name                       oracleserver
        service_description             PUERTO_tcp_1521
            check_command                                 check_tcp_10

        }


define service{
        use                                                     local-service            ; Name of
service template to use
        host_name                       oracleserver
        service_description             ORACLE_ESTADO
            check_command                                 check_oracle_instant!1521!orcl!CSMA!CSMA

        }

define service{
        use                                                     local-service            ; Name of
service template to use
        host_name                       oracleserver
        service_description             ORACLE tablespace
            check_command                                 check_tablespace_oracle
```

```
        }


define service{
        use                                                     local-service           ; Name of
service template to use
        host_name                       oracleserver
        service_description             ORACLE tablespace USERS
            check_command                               check_tablespace_oracle2

        }

define service{
        use                                                     local-service           ; Name of
service template to use
        host_name                       oracleserver
        service_description             Usuarios oracle
            check_command                               check_users_oracle

        }
```

12.13. Anexo XIII: Código fuente de Check_Oracle_Instant

```
#!/usr/bin/perl

$host = $ARGV[0];
$port = $ARGV[1];
$sid  = $ARGV[2];
$user  = $ARGV[3];
$pass  = $ARGV[4];

sub trim($);
my @result;
my %ERRORS=('OK'=>0,'WARNING'=>1,'CRITICAL'=>2);
my @param_array = (
    [90,">","Dictionary Cache Hit Ratio",'SELECT (1 - (Sum(getmisses)/(Sum(gets) +
Sum(getmisses)))) * 100 FROM v\$rowcache;'],
    [95,">","Library Cache Hit Ratio",'SELECT (1 -(Sum(reloads)/(Sum(pins) + Sum(reloads)))) *
100 FROM v\$librarycache;'],
    [89,">","DB Block Buffer Cache Hit Ratio",'SELECT (1 - (phys.value / (db.value +
cons.value))) * 100 FROM v\$sysstat phys,v\$sysstat db,v\$sysstat cons WHERE phys.name =
\'physical reads\' AND db.name = \'db block gets\' AND cons.name = \'consistent gets\';'],
    [98,">","Latch Hit Ratio",'SELECT (1 - (Sum(misses) / Sum(gets))) * 100 FROM v\$latch;'],
    [5,"<","Disk Sort Ratio",'SELECT (disk.value/mem.value) * 100 FROM v\$sysstat
disk,v\$sysstat mem WHERE disk.name = \'sorts (disk)\' AND mem.name = \'sorts (memory)\';'],
    [5,"<","Rollback Segment Waits",'SELECT (Sum(waits) / Sum(gets)) * 100 FROM
v\$rollstat;'],
    [50,"<","Dispatcher Workload",'SELECT NVL((Sum(busy) / (Sum(busy) + Sum(idle))) * 100,0)
FROM v\$dispatcher;'],
    [51,"<","Usuarios concurrentes",'select count(*) from v\$session where username is not null
;']
                );
# is possible define own selects [reference value,operator (<;>;eq;ne etc.),Description,select]

my @results;

sub array_rows {
    my ($array_rows) = @_;

    my $rows = @$array_rows;
    return $rows;
       }

sub trim($)
{
        my $string = shift;
        $string =~ s/^\s+//;
        $string =~ s/\s+$//;
        return $string;
}


sub logon {
open                    (SQL,"/home/nagios/Descargas/instantclient10_1/sqlplus                  -s
JODER/CARD@\\(DESCRIPTION=\\(ADDRESS=\\(PROTOCOL=TCP\\)\\(Host=10.36.32.10\\)\\(Port=1521\\)\\)\
\(CONNECT_DATA=\\(SID=orcl\\)\\)\\)</dev/null
|") or die;
  while ( my $res = <SQL> )
             {
           if ($res =~ /^(ORA-\d{5})/) {return $1;}
             }
}

if (logon() eq "ORA-01017"){
```

```
 for (my $i=0; $i<array_rows(\@param_array); $i++){
      print "$param_array[$i][2] \n";

open                  (SQL,"/home/nagios/Descargas/instantclient10_1/sqlplus                  -s
$user/$pass@\\(DESCRIPTION=\\(ADDRESS=\\(PROTOCOL=TCP\\)\\(Host=$host\\)\\(Port=$port\\)\\)\\(CO
NNECT_DATA=\\(SID=$sid\\)\\)\\) << EOF
set pagesize 0
set numformat 999.999
$param_array[$i][3]
EOF |") or die;
  while ( my $res = <SQL> )
            {
   print trim($res)."\n";
   if ( $res =~/^\s*\S+/ ) { push(@results,trim($res));}
            }
  }


  for ($i=0;$i<@results;$i++) {
     print $i." hodnota je ".$result[$i]." a ma byt ".$param_array[$i][0];
    eval       "unless       (".$results[$i].$param_array[$i][1].$param_array[$i][0].")       {
print\"".$param_array[$i][2]." ".$sid." KO \\n\"; exit ".$ERRORS{"WARNING"}.";}";

  }
print "DISPONIBILIDAD E INDICADORES DE RENDIMIENTO DE LA INSTANCIA $sid ORACLE OK";
exit $ERRORS{"OK"};



} else {print "JODER QUE cojones $sid , $user, $host, $port"; exit $ERRORS{"CRITICAL"};}
```