

# Monitorización de sistemas y servicios

## Contenidos

Contenidos .....	1
Resumen ejecutivo .....	2
Arquitectura de la plataforma de monitorización.....	2
Monitorización y alarmas .....	3
Monitorización .....	3
Servicios monitorizados .....	4
Parámetros de rendimiento .....	5
Sistemas soportados.....	6
Alarma .....	6
Servicios de monitorización .....	6
Ejemplos prácticos .....	7

## Resumen ejecutivo

Las infraestructuras de comunicaciones y los servidores de red como firewalls, proxies, servidores web, de correo, de ficheros y otros elementos existentes en la red, son piezas clave para el correcto funcionamiento del negocio de las empresas. Es fundamental garantizar su funcionamiento en condiciones óptimas.

Genos ofrece una solución integral de monitorización de servicios y de las condiciones en las que operan usando herramientas de software libre (Nagios y Cacti) y Linux.

La plataforma permite detectar rápidamente cuando se produce una incidencia en el servicio y notificar a la persona o personas apropiadas para su resolución, a través de la consola del sistema, mediante correo electrónico o directamente a un teléfono móvil mediante SMS.

Además, el sistema puede realizar acciones proactivas para resolver la incidencia automáticamente o integrarse con sistemas de seguimiento de incidencias o trouble ticketing, como GMF.

Estas herramientas permiten controlar desde el estado de los servicios de red hasta parámetros geofísicos, como la temperatura del CPD a través de módulos domóticos, o controlar voltajes de salidas de los SAIs.

Las alarmas pueden generarse en base a:

- conectividad de red a nivel IP
- incorrecto funcionamiento de los servicios de red a nivel de usuario: servidores web, servicios de correo (SMTP, POP3, IMAP, POP3s, IMAPs), etc., y también servidores como Exchange Server, SQL Server u Oracle fallos de discos en sistemas RAID (que degradan el servicio)
- por problemas de rendimiento o estado general del sistema: utilización excesiva de la CPU (debido a procesos colgados), particiones de disco sin espacio libre, etc.
- en base a parámetros físicos del hardware: temperatura de la CPU, estado de los ventiladores, voltajes
- parámetros geofísicos como la temperatura del CPD o centro de cálculo
- otros parámetros a partir de plugins desarrollados a medida.

## Arquitectura de la plataforma de monitorización

La monitorización de servicios y estado de los sistemas se realiza básicamente de dos formas distintas:

- monitorización remota a través de la red o a través de SNMP
- agentes locales instalados en los sistemas controlados

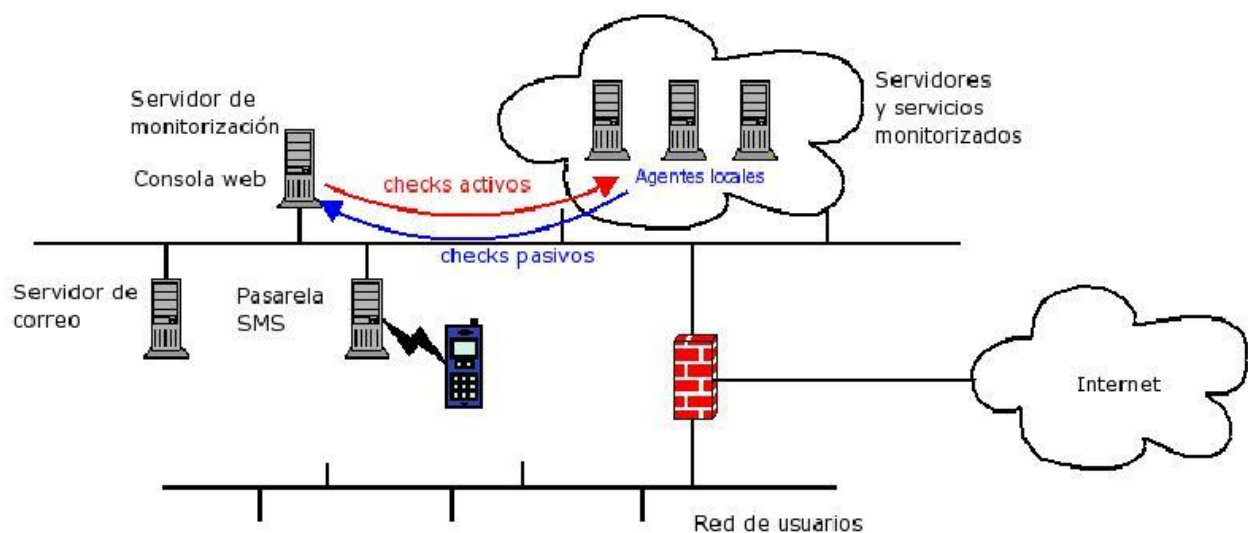
Si el sistema a monitorizar está compuesto por hardware industrial, es posible crear una MIB SNMP a medida e integrarla en la plataforma siempre que exista una interface entre el

hardware y el sistema informático, ya sea a través de un protocolo de red, o puerto serie, o similar.

Para entornos muy grandes, los servicios de la red pueden monitorizarse de forma distribuida. De esta forma, se evita la sobrecarga del servidor central distribuyendo la carga y las tareas de monitorización entre distintos servidores satélite.

La disponibilidad del sistema de monitorización está asegurada configurando el sistema en alta disponibilidad.

Es posible continuar monitorizando la red en caso de fallo de cualquiera de los servidores de monitorización utilizando sistemas redundantes, que pueden estar situados en redes y ubicaciones físicas separadas.



## Monitorización y alarmas

### Monitorización

El sistema realiza dos funciones de comprobación:

- la de los servicios para asegurar su estado online y funcional
- la recopilación de información de rendimiento de parámetros relevantes como CPU, memoria, utilización de disco, de red, etc.

La primera de estas funciones permite saber de forma prácticamente instantánea cuando está fallando un servicio y realizar tareas predefinidas de recuperación del servicio de forma automática. Esto garantiza un tiempo de disponibilidad y una calidad de servicio máxima.

La segunda de las funciones permite disponer de una evolución histórica del grado de ocupación del sistema.

Esta información permite:

- dimensionar correctamente el hardware antes que éste sea insuficiente para dar el servicio requerido identificar la utilización excesiva de recursos que puede indicar procesos mal definidos o que están fallando, o una utilización no apropiada de los recursos por parte de los usuarios

## **Servicios monitorizados**

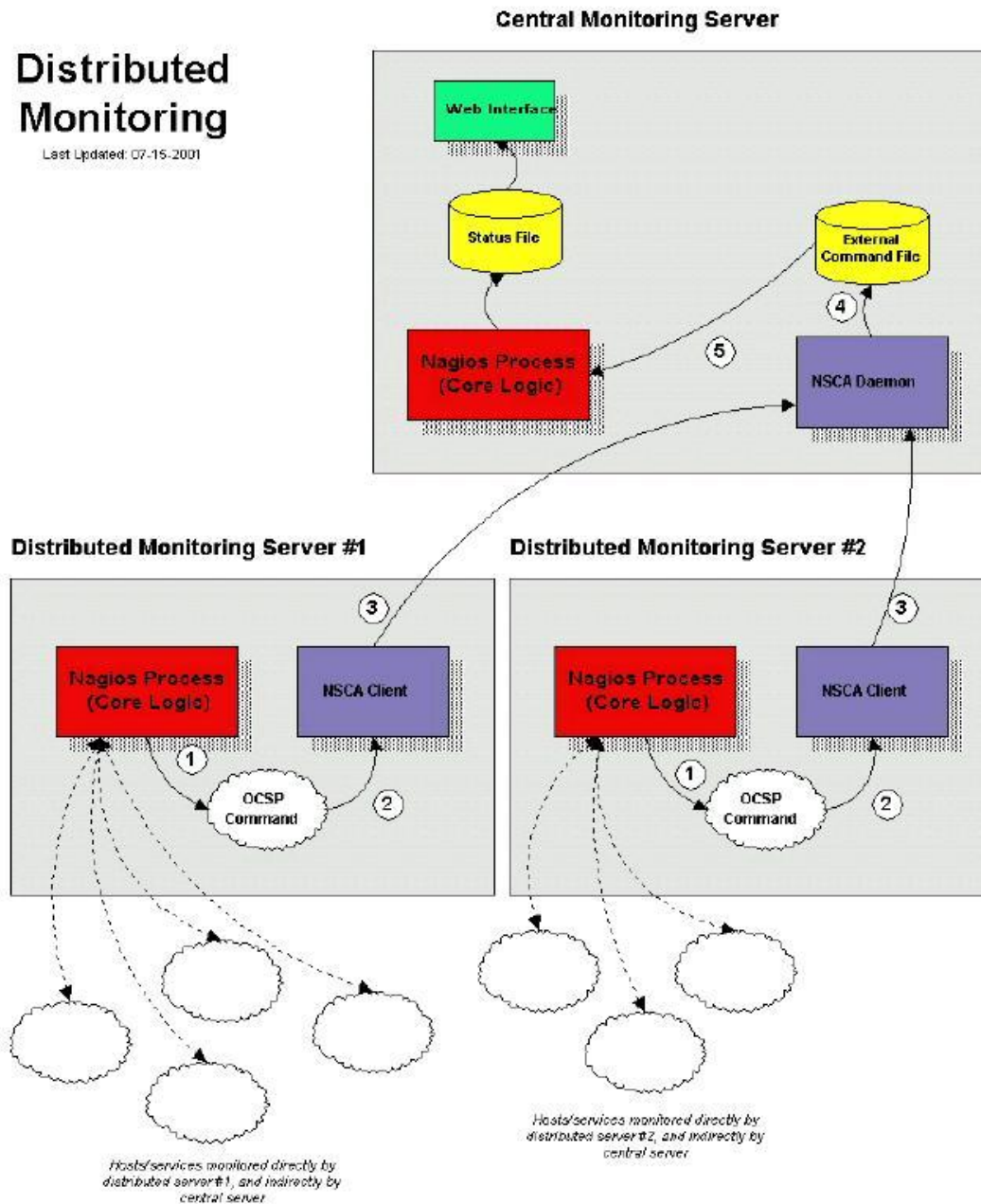
Las posibilidades de monitorización de servicios son muy amplias. Además de los servicios predefinidos, pueden programarse plugins personalizados para integrar en el sistema servicios no estándar.

Algunas características del sistema son:

- expansión del sistema a través de plugins
- posibilidad de definir una jerarquía de servicios, distinguiendo entre aquellos servicios caídos y aquellos inaccesibles
- notificación de las alarmas generadas a través de distintos canales
- posibilidad de definir gestores de eventos que se ejecutan cuando se produce un evento dado para actuar de forma proactiva en la prevención de incidencias

# Distributed Monitoring

Last Updated: 07-15-2001



## Parámetros de rendimiento

Los parámetros de rendimiento controlados y almacenados pueden ser:

- número de procesos
- utilización de la CPU
- carga del sistema
- memoria

- paginación
- ocupación de los discos
- grado de utilización de los discos (volumen de datos leídos y escritos)
- grado de utilización de la red (volumen de datos recibidos y transmitidos por red)

Todos aquellos parámetros accesibles a través de SNMP son susceptibles de ser monitorizados. Si no tienen interfaz SNMP pero puede consultarse sus valores a través de scripts u otros mecanismos, pueden integrarse de forma que es posible recolectar su valor de forma indirecta.

## **Sistemas soportados**

La plataforma de monitorización se ejecuta en un sistema Linux y los sistemas monitorizados pueden ser Linux, Windows, otros sistemas UNIX o elementos de red en general (como routers, switches, saís conectados a ethernet, etc.). También pueden integrarse todos aquellos dispositivos que soporten el protocolo SNMP o que puedan configurarse para enviar traps.

## **Alarma**

En el momento de generar una alarma, el sistema puede ejecutar una acción preventiva para intentar recuperar el servicio de forma automática, y generar una alarma para informar a los administradores de sistemas de la incidencia.

Las alarmas pueden ser notificadas a través de alguno de los siguientes mecanismos:

- alerta en la consola de monitorización
- correo electrónico
- SMS a móviles (esta funcionalidad requiere de una pasarela a la red de telefonía móvil)

La pasarela SMS permite también realizar consultas al sistema para saber el estado de determinados parámetros de forma remota.

## **Servicios de monitorización**

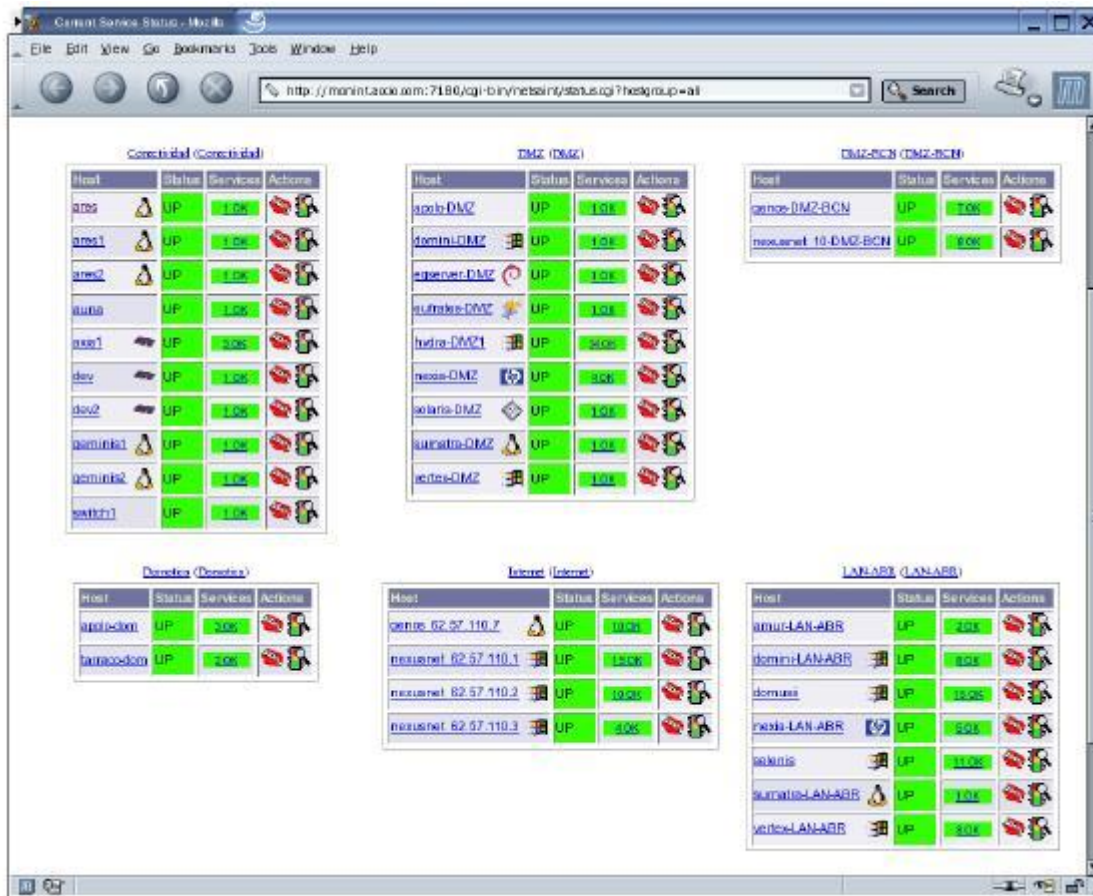
Genos realiza proyectos de implantación de sistemas de monitorización instalando el servidor de gestión en la red del cliente, integrando los servicios que se desean monitorizar y desarrollando los plugins a medida para el control de plataformas sin interfaces estándar.

Para redes pequeñas y medianas puede realizarse la monitorización remota de sistemas, utilizando como plataforma la propia de Genos en modalidad ASP, sin instalar servidores adicionales en la red del cliente.

La monitorización y los servicios de mantenimiento de sistemas de Genos garantizan la máxima disponibilidad de los servidores y de los servicios de red, también en entornos donde se requiere una disponibilidad 24x7.

## Ejemplos prácticos

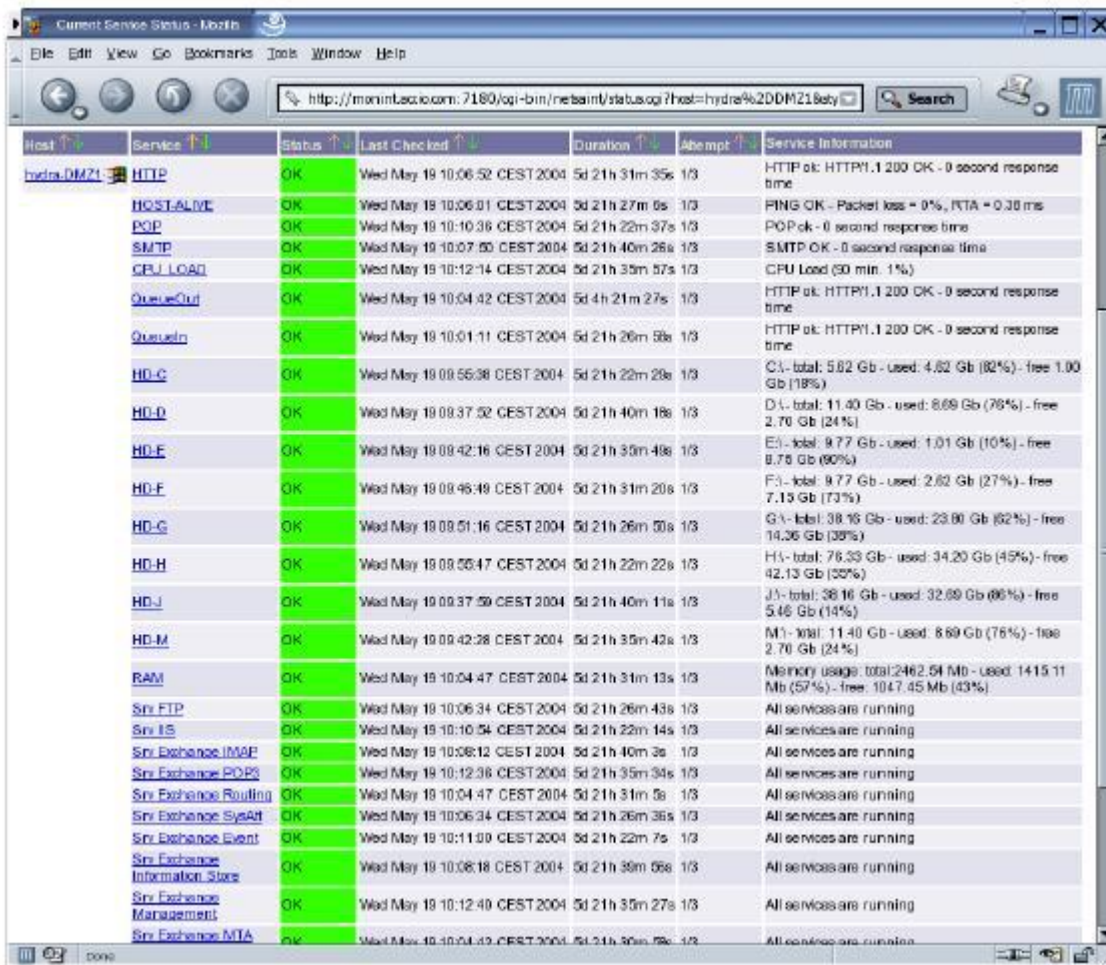
Pantalla general de estado de hosts monitorizados



The screenshot displays a web-based monitoring interface with a browser window titled "Current Service Status - Hosts". The address bar shows the URL: `http://monit.la000.com:7186/cgi-bin/hosts/status.cgi?hostgroup=all`. The main content area is organized into six panels, each representing a different network segment:

- CoreSwitch (CoreSwitch):** Lists hosts like `core1`, `core2`, `core3`, `core4`, `core5`, `core6`, `core7`, `core8`, `core9`, `core10`, `core11`, `core12`, `core13`, `core14`, `core15`, `core16`, `core17`, `core18`, `core19`, `core20`, `core21`, `core22`, `core23`, `core24`, `core25`, `core26`, `core27`, `core28`, `core29`, `core30`, `core31`, `core32`, `core33`, `core34`, `core35`, `core36`, `core37`, `core38`, `core39`, `core40`, `core41`, `core42`, `core43`, `core44`, `core45`, `core46`, `core47`, `core48`, `core49`, `core50`.
- DMZ (DMZ):** Lists hosts like `dmz1`, `dmz2`, `dmz3`, `dmz4`, `dmz5`, `dmz6`, `dmz7`, `dmz8`, `dmz9`, `dmz10`, `dmz11`, `dmz12`, `dmz13`, `dmz14`, `dmz15`, `dmz16`, `dmz17`, `dmz18`, `dmz19`, `dmz20`.
- DMZ-RCN (DMZ-RCN):** Lists hosts like `dmz-rcn1`, `dmz-rcn2`.
- Directos (Directos):** Lists hosts like `directos1`, `directos2`.
- Internet (Internet):** Lists hosts like `internet1`, `internet2`, `internet3`, `internet4`, `internet5`.
- LAN-ARR (LAN-ARR):** Lists hosts like `lan-arr1`, `lan-arr2`, `lan-arr3`, `lan-arr4`, `lan-arr5`, `lan-arr6`, `lan-arr7`, `lan-arr8`, `lan-arr9`, `lan-arr10`, `lan-arr11`, `lan-arr12`, `lan-arr13`, `lan-arr14`, `lan-arr15`, `lan-arr16`, `lan-arr17`, `lan-arr18`, `lan-arr19`, `lan-arr20`.

Pantalla de detalle de los servicios de un host monitorizado



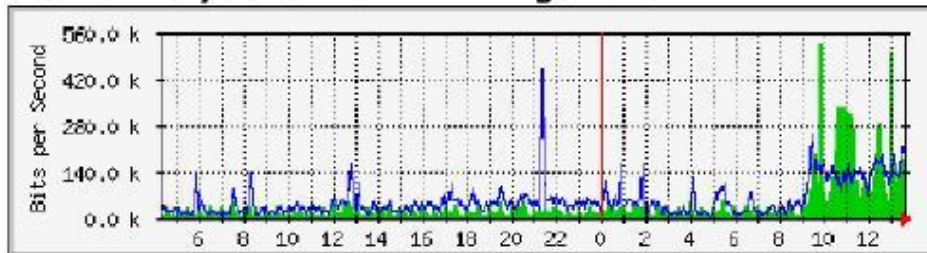
Host	Service	Status	Last Checked	Duration	Attempts	Service Information
hydra.DM21	HTTP	OK	Wed May 19 10:06:52 CEST 2004	5d 21h 31m 35s	1/3	HTTP ok: HTTP/1.1 200 OK - 0 second response time
	HOSTALIVE	OK	Wed May 19 10:06:01 CEST 2004	5d 21h 27m 6s	1/3	PING OK - Packet loss = 0%, RTA = 0.20 ms
	POP	OK	Wed May 19 10:10:36 CEST 2004	5d 21h 22m 37s	1/3	POP ok - 0 second response time
	SMTP	OK	Wed May 19 10:07:50 CEST 2004	5d 21h 40m 26s	1/3	SMTP OK - 0 second response time
	CPU_LOAD	OK	Wed May 19 10:12:14 CEST 2004	5d 21h 35m 57s	1/3	CPU Load (50 min. 1%)
	QueueOut	OK	Wed May 19 10:04:42 CEST 2004	5d 4h 21m 27s	1/3	HTTP ok: HTTP/1.1 200 OK - 0 second response time
	QueueIn	OK	Wed May 19 10:01:11 CEST 2004	5d 21h 26m 58s	1/3	HTTP ok: HTTP/1.1 200 OK - 0 second response time
	HD-C	OK	Wed May 19 09:55:38 CEST 2004	5d 21h 22m 28s	1/3	C:- total: 5.82 Gb - used: 4.82 Gb (82%) - free 1.00 Gb (18%)
	HD-D	OK	Wed May 19 09:37:32 CEST 2004	5d 21h 40m 18s	1/3	D:- total: 11.40 Gb - used: 8.69 Gb (76%) - free 2.70 Gb (24%)
	HD-E	OK	Wed May 19 09:42:16 CEST 2004	5d 21h 30m 48s	1/3	E:- total: 9.77 Gb - used: 1.01 Gb (10%) - free 8.76 Gb (90%)
	HD-F	OK	Wed May 19 09:46:49 CEST 2004	5d 21h 31m 20s	1/3	F:- total: 9.77 Gb - used: 2.82 Gb (27%) - free 7.13 Gb (73%)
	HD-G	OK	Wed May 19 09:51:16 CEST 2004	5d 21h 26m 50s	1/3	G:- total: 38.16 Gb - used: 23.80 Gb (62%) - free 14.36 Gb (38%)
	HD-H	OK	Wed May 19 09:55:47 CEST 2004	5d 21h 22m 22s	1/3	H:- total: 76.33 Gb - used: 34.20 Gb (45%) - free 42.13 Gb (55%)
	HD-I	OK	Wed May 19 09:37:59 CEST 2004	5d 21h 40m 11s	1/3	I:- total: 38.16 Gb - used: 32.69 Gb (86%) - free 5.46 Gb (14%)
	HD-M	OK	Wed May 19 09:42:28 CEST 2004	5d 21h 35m 42s	1/3	M:- total: 11.40 Gb - used: 8.69 Gb (76%) - free 2.70 Gb (24%)
	RAM	OK	Wed May 19 10:04:47 CEST 2004	5d 21h 31m 13s	1/3	Memory usage: total:2462.54 Mb - used: 1415.11 Mb (57%) - free: 1047.45 Mb (43%)
	Srv FTP	OK	Wed May 19 10:06:34 CEST 2004	5d 21h 26m 43s	1/3	All services are running
	Srv IS	OK	Wed May 19 10:10:54 CEST 2004	5d 21h 22m 14s	1/3	All services are running
	Srv Exchange IMAP	OK	Wed May 19 10:08:12 CEST 2004	5d 21h 40m 3s	1/3	All services are running
	Srv Exchange POP3	OK	Wed May 19 10:12:36 CEST 2004	5d 21h 35m 34s	1/3	All services are running
	Srv Exchange Routing	OK	Wed May 19 10:04:47 CEST 2004	5d 21h 31m 3s	1/3	All services are running
	Srv Exchange SysAtt	OK	Wed May 19 10:06:34 CEST 2004	5d 21h 26m 36s	1/3	All services are running
	Srv Exchange Event	OK	Wed May 19 10:11:09 CEST 2004	5d 21h 22m 7s	1/3	All services are running
	Srv Exchange Information Store	OK	Wed May 19 10:08:18 CEST 2004	5d 21h 39m 58s	1/3	All services are running
	Srv Exchange Management	OK	Wed May 19 10:12:40 CEST 2004	5d 21h 35m 27s	1/3	All services are running
	Srv Exchange MTA	OK	Wed May 19 10:04:43 CEST 2004	5d 21h 36m 5s	1/3	All services are running

Los servicios monitorizados para este host concreto son:

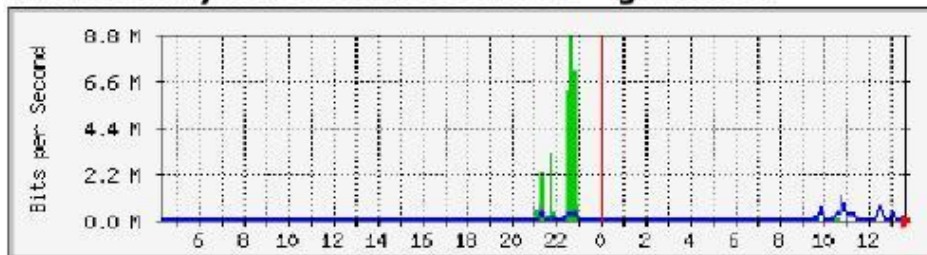
- estado de ocupación de discos y CPU
- servicios de red: HTTP, SMTP, POP3
- estado de servicios MS Exchange Server y MS SQL Server

Monitorización del tráfico de los distintos interfaces de red de un firewall Linux

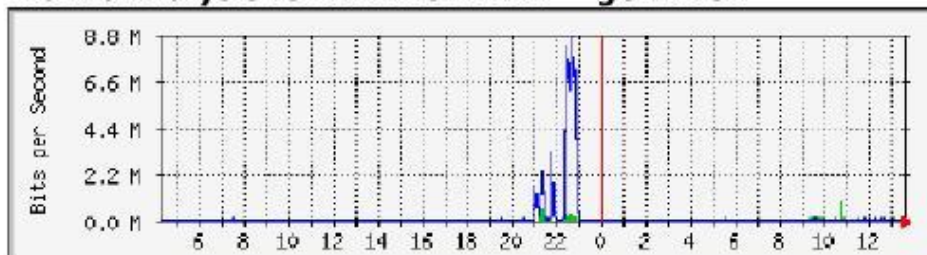
### Traffic Analysis for 10.1.2.11 -- geminis1



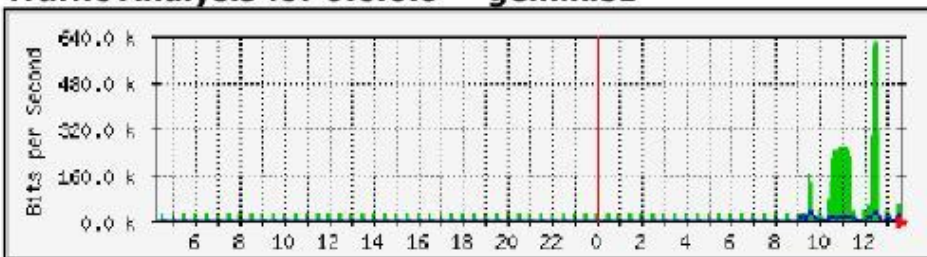
### Traffic Analysis for 192.168.11.11 -- geminis1



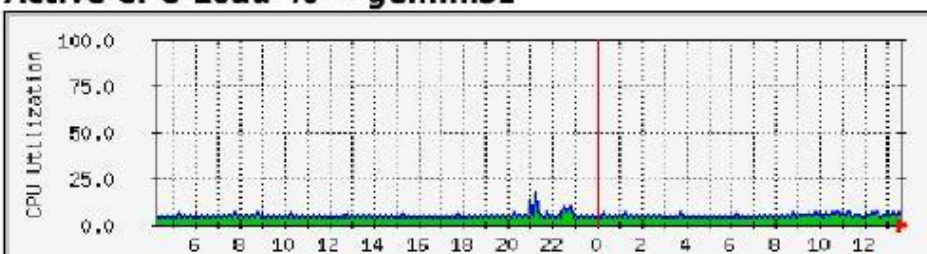
### Traffic Analysis for 172.16.74.21 -- geminis1



### Traffic Analysis for 0.0.0.0 -- geminis1



### Active CPU Load % -- geminis1



### Uptime -- geminis1

