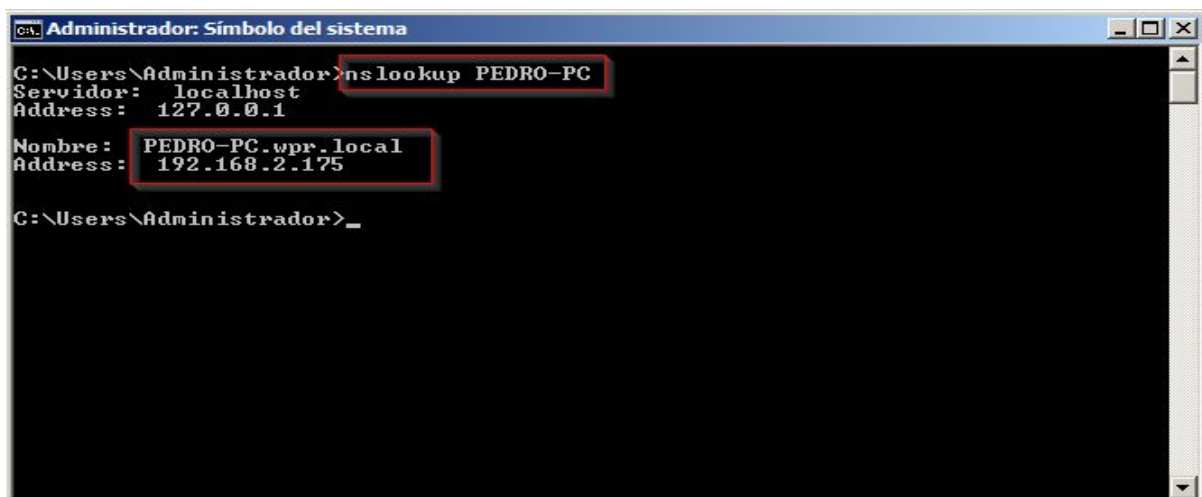


1. Realizar, en un sistema operativo Windows 2008, una monitorización de un equipo del dominio.

Para este punto de la tarea vamos a utilizar dos máquinas con S.O. Windows. La primera un Windows 2008 Server y la segunda un Windows 7 Profesional. El servidor tiene la Ip **192.168.2.161** y el nombre de la máquina es **WServer**, la máquina con Windows 7 tiene la IP **192.168.2.175** y el nombre de la máquina es **PEDRO-PC**. Vamos a realizar comprobaciones con **nslookup** para averiguar que estos datos son correctos:

Empezamos la comprobación desde la consola del servidor (cmd):

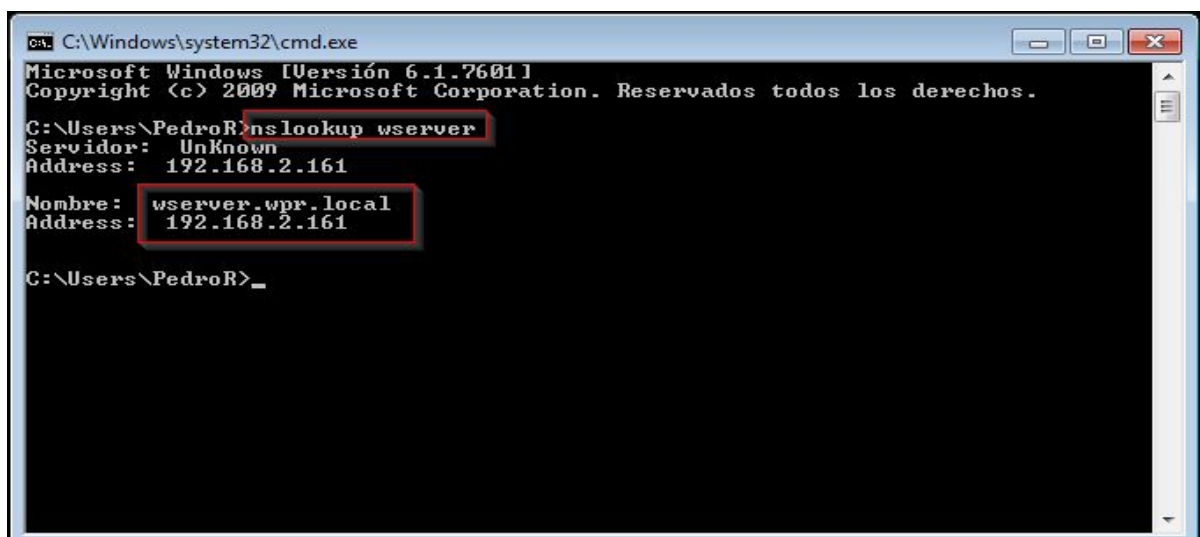


```
CA: Administrador: Símbolo del sistema
C:\Users\Administrador>nslookup PEDRO-PC
Servidor: localhost
Address: 127.0.0.1

Nombre: PEDRO-PC.wpr.local
Address: 192.168.2.175

C:\Users\Administrador>_
```

Ahora desde la parte de la máquina con Windows 7:



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Versión 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Users\PedroR>nslookup wserver
Servidor: UnKnown
Address: 192.168.2.161

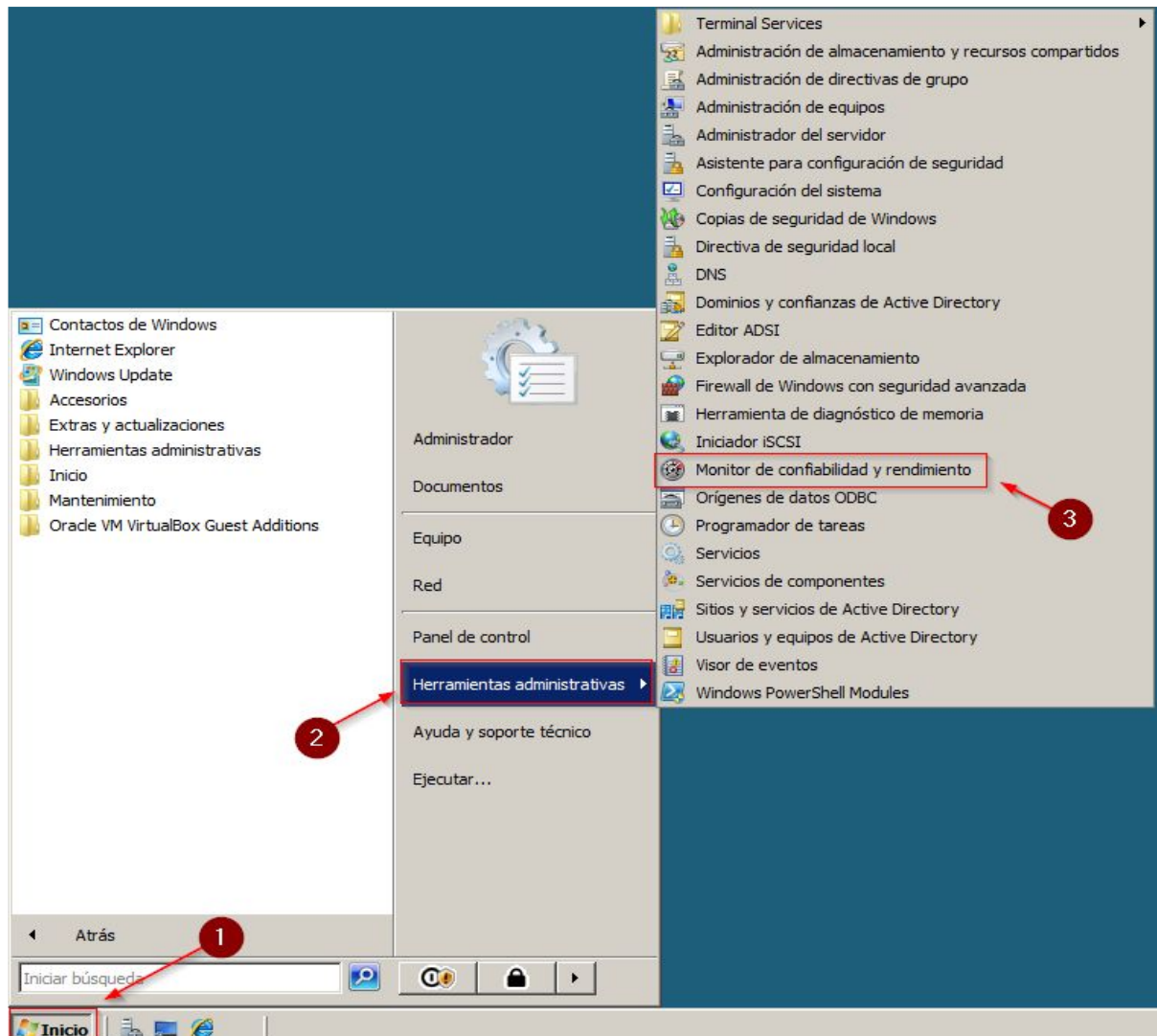
Nombre: wserver.wpr.local
Address: 192.168.2.161

C:\Users\PedroR>_
```

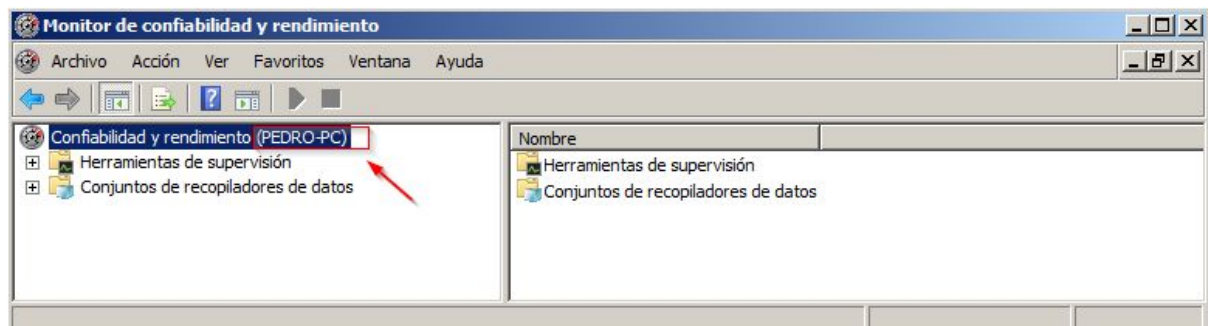
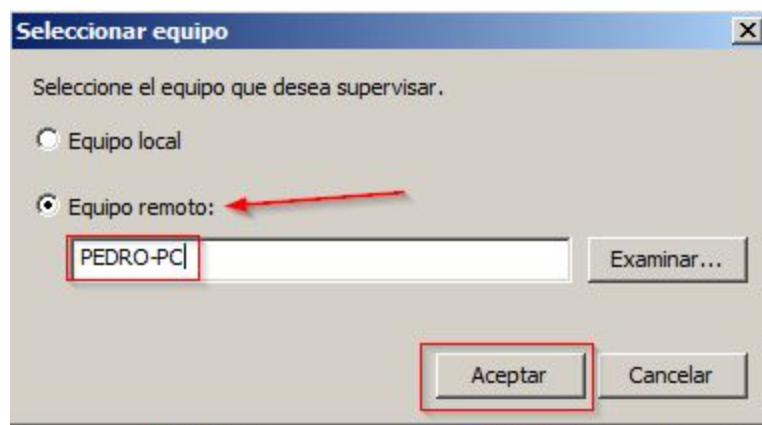
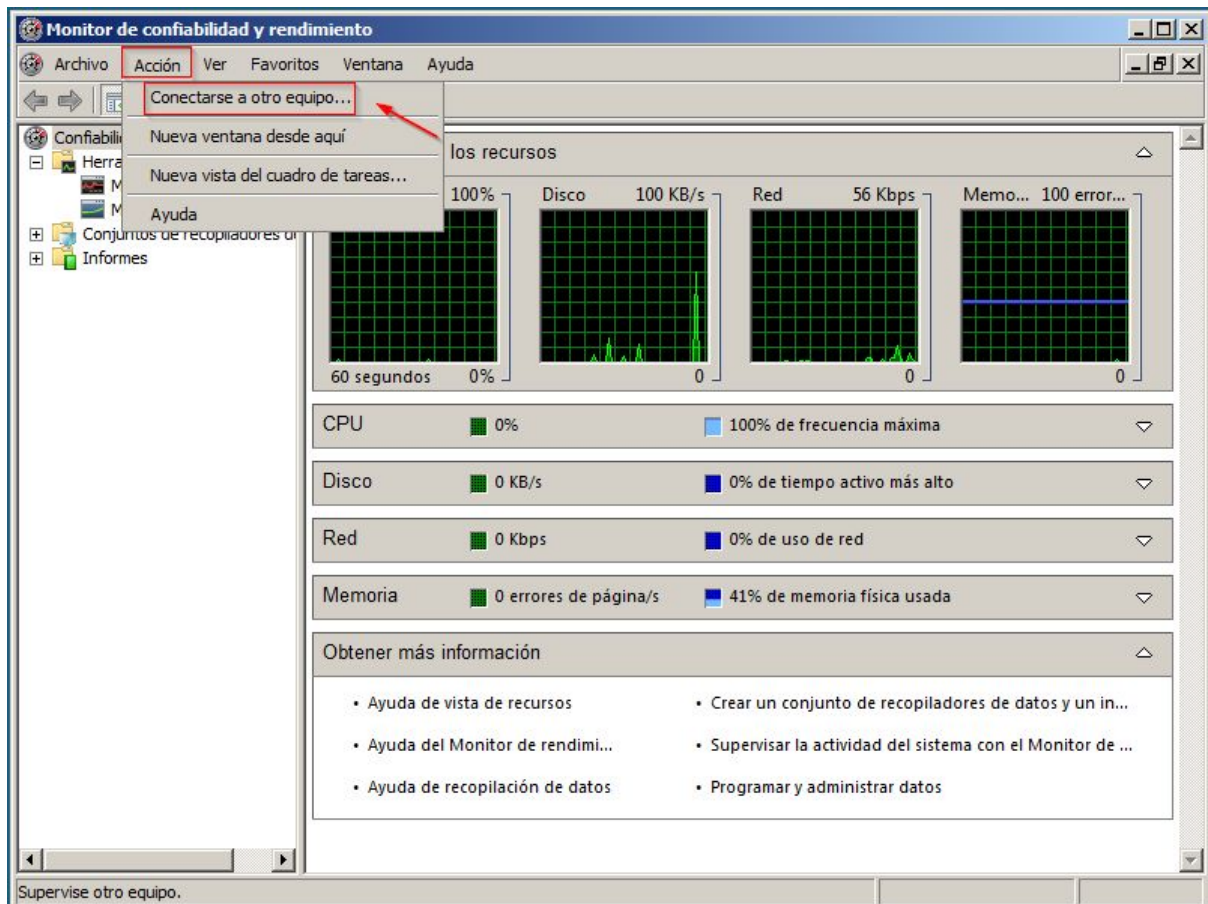
Podemos ver que los datos son correctos y que pertenecen al mismo dominio.

Lo siguiente que haremos será monitorear desde el equipo servidor (Windows Server 2008) un equipo del dominio (PEDRO-PC):

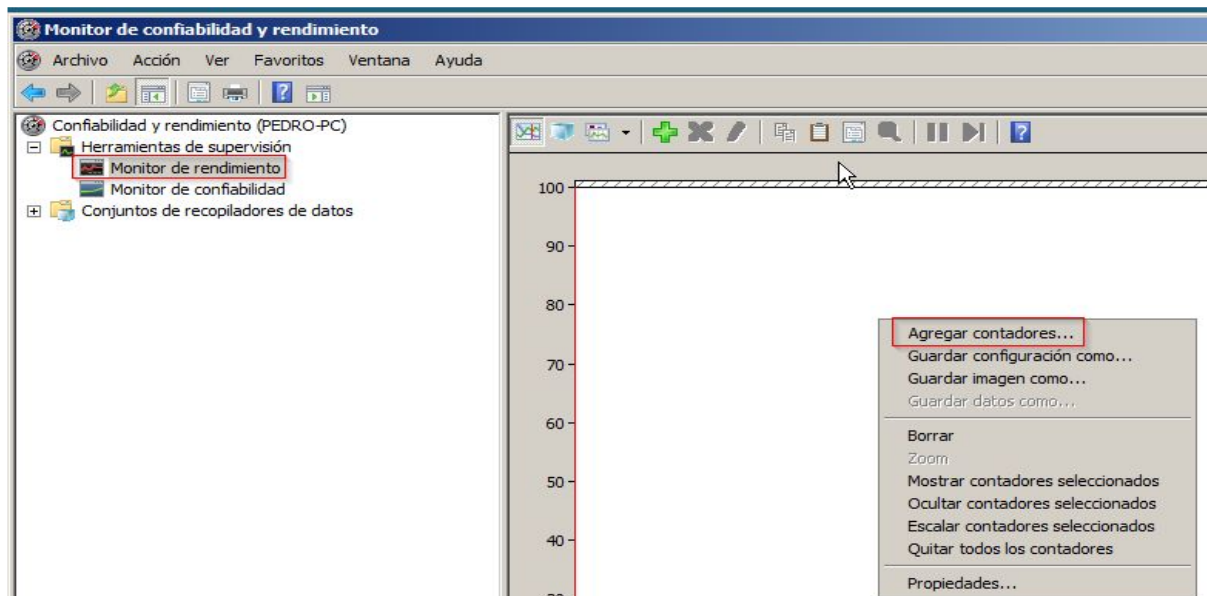
→ **Inicio Herramientas administrativas Monitor de rendimiento**



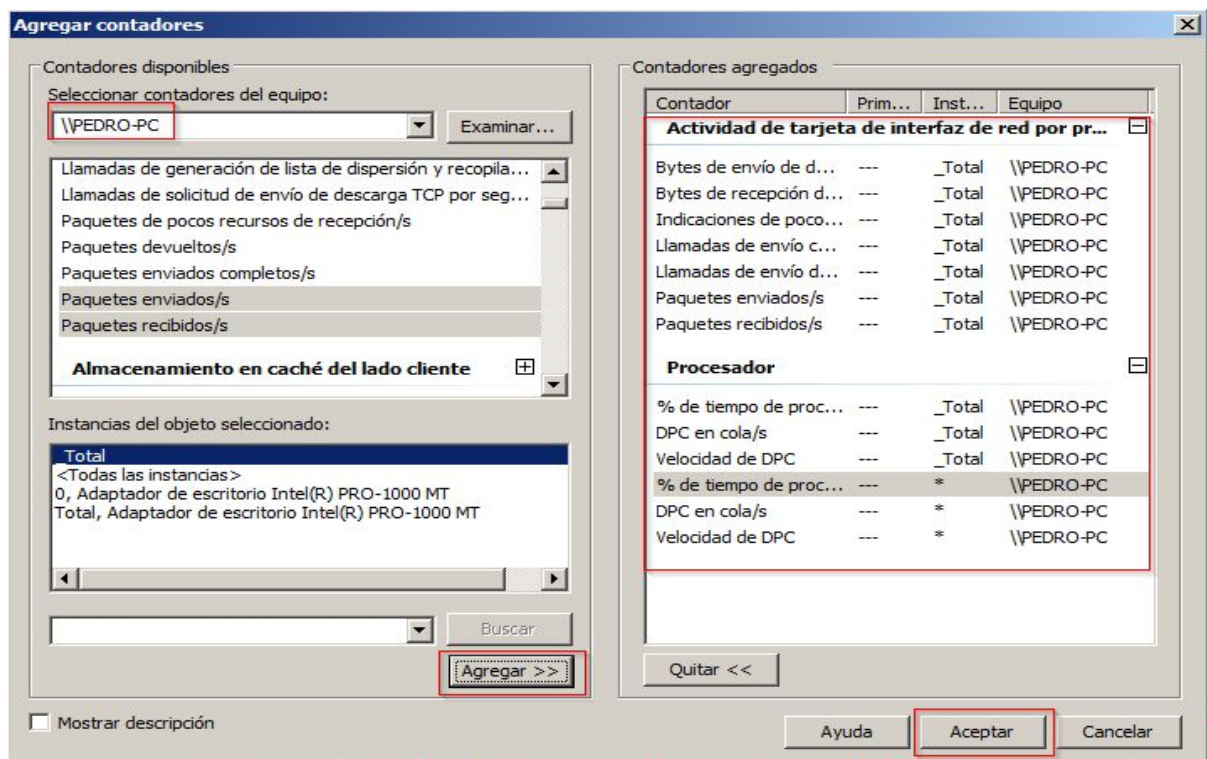
Una vez se ha abierto la ventana del **Monitor de confiabilidad y rendimiento**, clicamos en el menú **Acción Conectarse a otro equipo...**



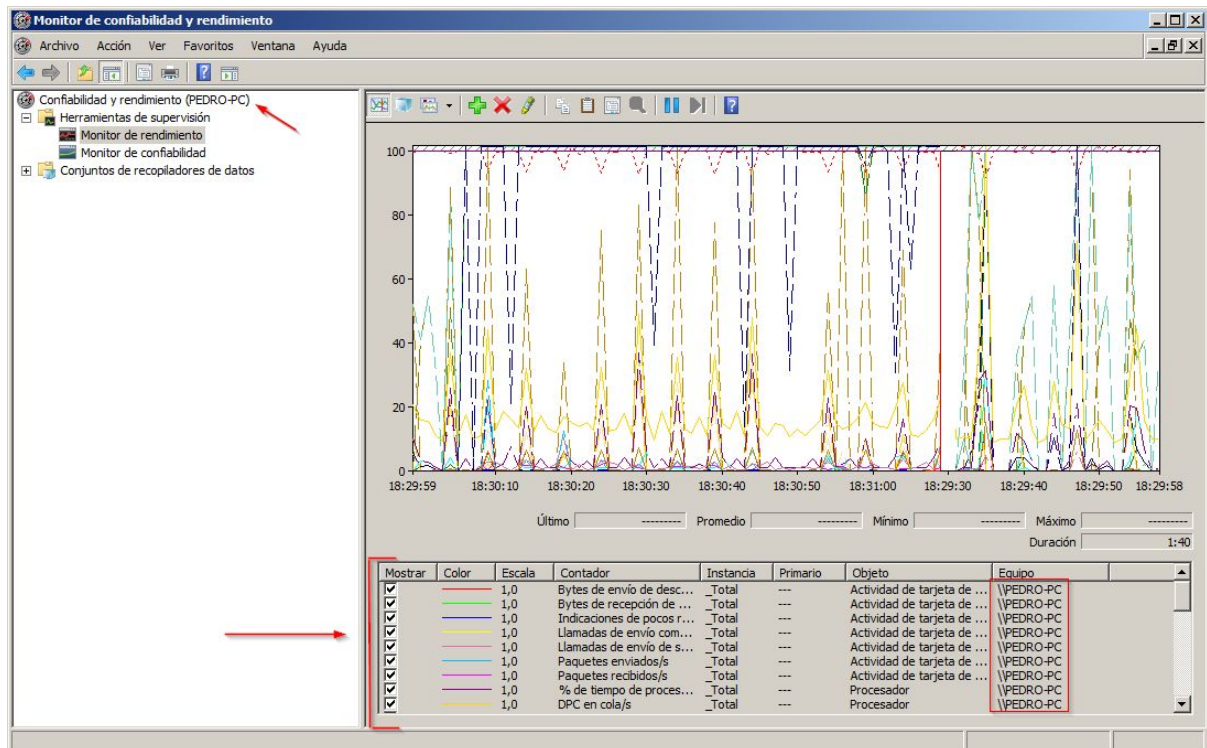
El siguiente paso vamos monitorear el equipo del dominio. Para ello nos situamos en el **Monitor de rendimiento** y agregamos un/os contadores:



Elegimos el equipo que queremos monitorizar y seleccionamos los contadores:

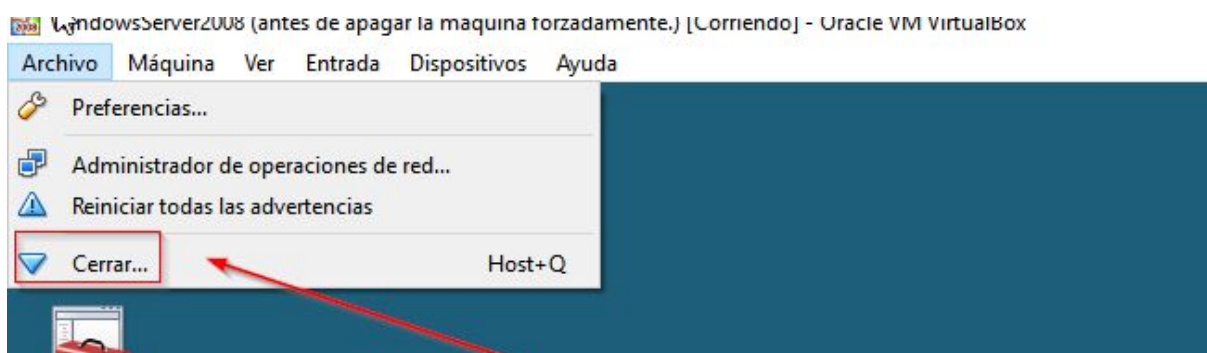


Una vez clicamos en **Aceptar** empezaremos a ver la información solicitada en forma de gráfico con leyenda que indica el color correspondiente a cada uno de los datos solicitados:

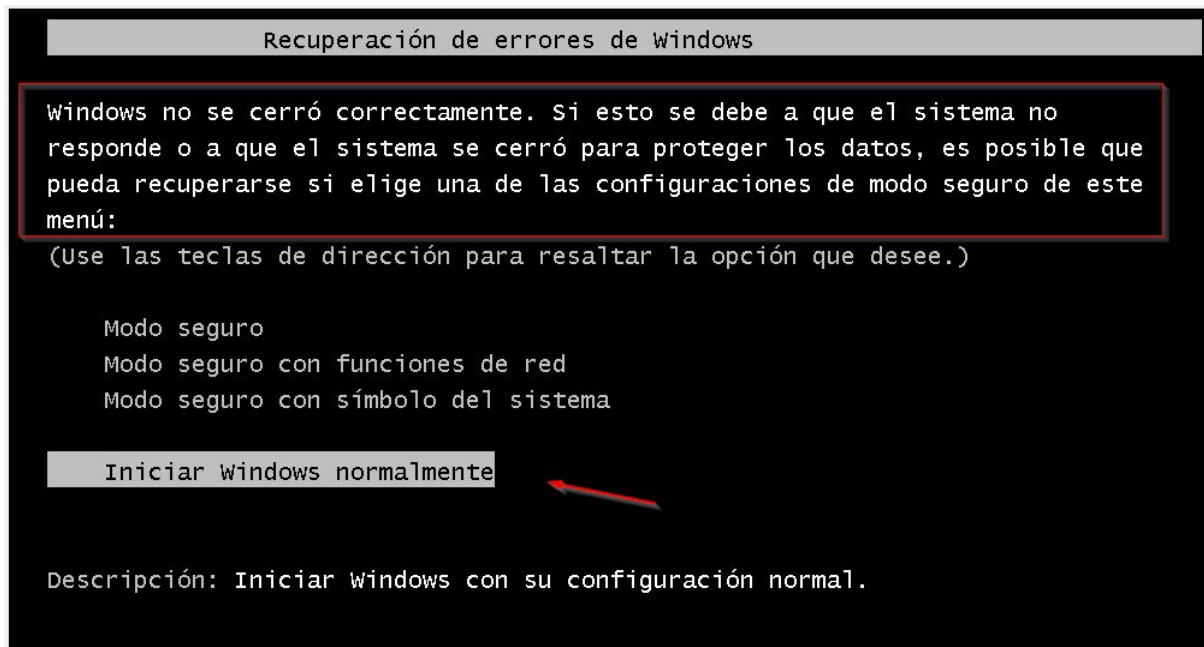


2. Realizar, también en un sistema operativo Windows 2008, un estudio de confiabilidad realizando una tarea que provoque un error y verificando que aparece registrado.

Para este punto vamos a simular un cierre forzado del sistema (por apagón, o cuelgue del S.O.) guardando previamente el estado de la máquina para poder recuperarla si después de realizar las pruebas no arranca.

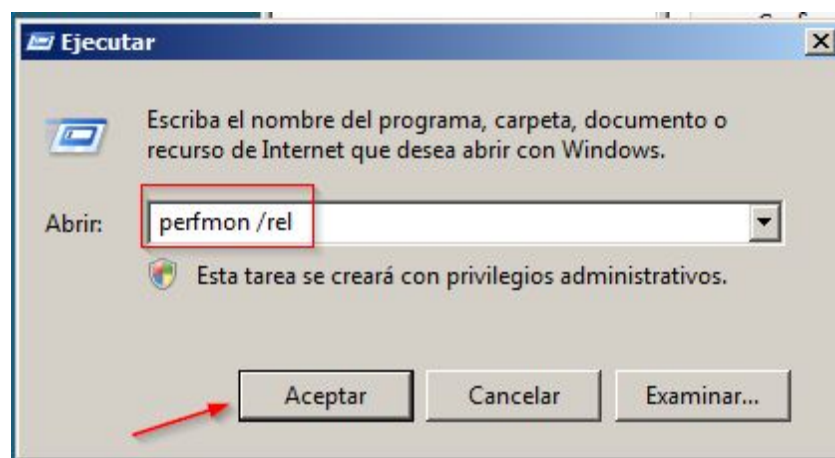


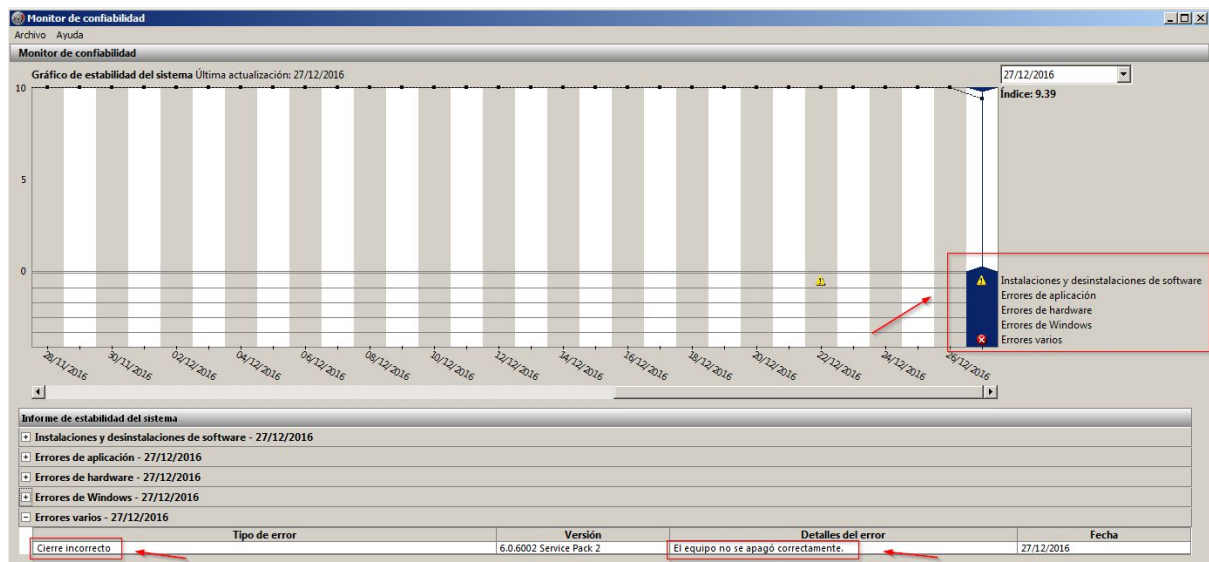
En la siguiente captura podemos observar que la máquina virtual de Windows 2008 Server no se apagado correctamente:



Ahora abriremos el **Monitor de confiabilidad y rendimiento** para comprobar si se ha registrado el evento.

Para abrir el monitor nos vamos a **Inicio Ejecutar** y en el cuadro de diálogo escribimos: **perfmon/rel**





Si nos vamos al visor de eventos, podemos observar que también registra el evento como se muestra en la siguiente captura:

Administrador del servidor

Sistema 36.441 eventos

Nivel	Fecha y hora	Origen	Id. del evento	Categoría de la tarea
Información	27/12/2016 21:11:15	Proveedor de registro de eventos del Administr...	7036	Ninguno
Información	27/12/2016 21:11:15	Proveedor de registro de eventos del Administr...	7036	Ninguno
Información	27/12/2016 21:10:44	DistributedCOM	10029	Ninguno
Información	27/12/2016 21:10:41	DistributedCOM	10029	Ninguno
Información	27/12/2016 21:10:38	DistributedCOM	10029	Ninguno
Información	27/12/2016 21:10:08	ResourcePublication	104	Ninguno
Advertencia	27/12/2016 21:10:09	Time-Service	12	Ninguno
Información	27/12/2016 21:10:08	Time-Service	143	Ninguno
Información	27/12/2016 21:10:08	Time-Service	139	Ninguno
Información	27/12/2016 21:10:08	DfsSvc	14531	Ninguno
Información	27/12/2016 21:10:08	DfsSvc	14533	Ninguno
Advertencia	27/12/2016 21:10:08	LsaSrv	40960	(3)
Advertencia	27/12/2016 21:09:40	Kerberos-Key-Distribution-Center	29	Ninguno
Información	27/12/2016 21:09:32	FilterManager	6	Ninguno
Información	27/12/2016 21:09:29	E1G60	30	Ninguno
Información	27/12/2016 21:09:33	EventLog	6013	Ninguno
Información	27/12/2016 21:09:33	EventLog	6005	Ninguno
Información	27/12/2016 21:09:33	EventLog	6009	Ninguno
Error	27/12/2016 21:09:33	EventLog	6008	Ninguno
Información	27/12/2016 21:09:33	EventLog	4201	Ninguno
Información	27/12/2016 21:09:33	EventLog	6	Ninguno
Información	27/12/2016 21:09:33	EventLog	4	Ninguno
Información	27/12/2016 21:09:33	EventLog	4201	Ninguno
Información	27/12/2016 21:09:33	EventLog	1	Ninguno
Información	27/12/2016 21:09:33	EventLog	7036	Ninguno

Propiedades de evento: Evento 6008, EventLog

General Detalles

El cierre anterior del sistema a las 21:05:38 del 27/12/2016 resultó inesperado.

Nombre de registro: Sistema

Origen: EventLog Registrado: 27/12/2016 21:09:33

Id. del evento: 6008 Categoría de tarea: Ninguno

Nivel: Error Palabras clave: Clásico

Usuario: No disponible Equipo: WServer.wpr.local

Código de operación:

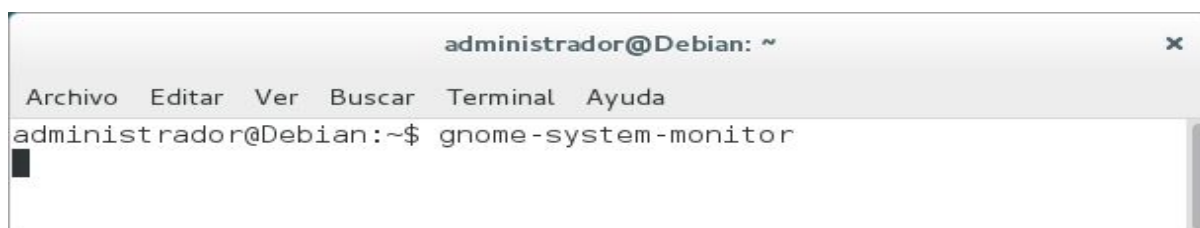
Más información: [Ayuda de Registro de eventos](#)

Copiar Cerrar

Registrado: 27/12/2016 21:09:33
Categoría de tarea: Ninguno
Palabras clave: Clásico
Equipo: WServer.wpr.local

3. En GNU/Linux buscar una herramienta que permita verificar el rendimiento del equipo por completo.

Para este punto de la tarea utilizaremos la aplicación que viene integrada en el sistema, **Monitor del sistema**:



Una vez que se abre la aplicación podemos ver que recopila diferentes tipos de información en las diferentes pestañas.

Por ejemplo, en la primera pestaña, **Procesos** podemos ver los procesos que tiene activos el sistema. Podemos ordenarlos por porcentaje de consumo de la CPU para ver cual es el proceso que más consume:

Procesos							Recursos	Sistemas de archivos
Nombre del proceso	Usuario	% CPU	ID	Memoria	Prioridad			
gnome-shell	administrador	22	1599	194,3 MiB	Normal			
gnome-system-monitor	administrador	15	2372	17,4 MiB	Normal			
firefox-esr	administrador	0	2416	113,3 MiB	Normal			
bash	administrador	0	2365	2,4 MiB	Normal			
gnome-pty-helper	administrador	0	2364	84,0 KiB	Normal			
gnome-terminal-server	administrador	0	2361	6,8 MiB	Normal			
dconf-service	administrador	0	2043	512,0 KiB	Normal			
gvfsd-burn	administrador	0	2034	716,0 KiB	Normal			
dleyna-renderer-service	administrador	0	2012	1,6 MiB	Normal			
epiphany-search-provider	administrador	0	1896	4,6 MiB	Normal			
uim-helper-server	administrador	0	1796	96,0 KiB	Normal			
gconfd-2	administrador	0	1773	572,0 KiB	Normal			
cat	administrador	0	1761	80,0 KiB	Normal			
evolution-calendar-factory	administrador	0	1760	36,4 MiB	Normal			
zeitgeist-fts	administrador	0	1746	2,3 MiB	Normal			
tracker-miner-user-guides	administrador	0	1738	2,1 MiB	Muy baja			
nm-applet	administrador	0	1735	5,2 MiB	Normal			
zeitgeist-daemon	administrador	0	1725	1,0 MiB	Normal			
evolution-alarm-notifu	administrador	0	1713	8,8 MiB	Normal			

La segunda pestaña, **Recursos** podemos ver de una forma más gráfica, el histórico de uso de la CPU, el estado de la memoria, el intercambio de la misma y el uso de la red:



En la última pestaña, podemos ver los sistemas de archivos del host monitorizado. En este caso, sólo tenemos un disco al 33% de su capacidad



4. También en GNU/Linux buscar un paquete que permita monitorizar el rendimiento tanto de nuestro equipo como de otro dentro de la red local, ya sea con el sistema operativo Windows o GNU/Linux.

Para este punto de la tarea, utilizaremos la herramienta de monitorización **ntop**. Para ellos abrimos un terminal y escribimos lo siguiente:

sudo apt-get install ntop

```
pedro@pedro-VirtualBox: ~  
pedro@pedro-VirtualBox:~$ sudo apt-get install ntop  
Leyendo lista de paquetes... Hecho  
Creando árbol de dependencias  
Leyendo la información de estado... Hecho  
ntop ya está en su versión más reciente (3:5.0.1+dfsg1-2.2ubuntu1).  
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 283 no actualizados.
```

En mi caso ya tenía instalado la aplicación por lo que vemos el mensaje de “0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 283 no actualizados.”.

Una vez hemos instalado la aplicación tenemos que iniciarla como servicio. Para ello en el mismo terminal o en cualquier otro escribimos la siguiente sentencia:

`sudo /etc/init.d/ntop start`

```
pedro@pedro-VirtualBox: ~  
pedro@pedro-VirtualBox:~$ sudo /etc/init.d/ntop start  
[ ok ] Starting ntop (via systemctl): ntop.service.  
pedro@pedro-VirtualBox:~$
```

Una vez iniciado el servicio, abrimos el navegador e introducimos la dirección de localhost **127.0.0.1 - localhost** ó la dirección IP de la máquina con la que vamos a monitorear. En mi caso **192.168.2.178**.

Por defecto **ntop** escucha por el puerto **3000**. Lo podemos comprobar escribiendo la siguiente sentencia:

`sudo netstat -tulpn | grep :3000`

```
pedro@pedro-VirtualBox: ~  
pedro@pedro-VirtualBox:~$ sudo netstat -tulpn | grep :3000  
tcp        0      0 0.0.0.0:3000 0.0.0.0:*        LISTEN      4755/ntop  
pedro@pedro-VirtualBox:~$
```

Así que una vez abierto el navegador escribiremos:

Localhost:3000 ó 192.168.2.178:3000

The screenshot shows the ntop web interface in a browser. The address bar contains '192.168.2.178:3000'. The interface has a navigation bar with links: About, Summary, All Protocols, IP, Utils, Plugins, Admin. Below the navigation bar, there are links for Global Statistics, enp0s3 Report, Protocol Distribution, and Application Protocols. A table titled 'Network Interface(s)' is displayed, showing details for enp0s3 and NetFlow-device.2. Below the table, there are sections for Capturing Since, Hosts, and Active Sessions.

Network Interface(s)	Name	Device	Type	Speed	Sampling Rate	MTU	Header	Address	IPv6 Addresses
enp0s3	enp0s3	Ethernet			0	1514	14	192.168.2.178	
NetFlow-device.2	NetFlow-device.2	Ethernet			1	1514	14	0.0.0.0	

Capturing Since: Tue Dec 27 19:55:50 2016 [10:18]

Hosts: [33 active] [45 total]

Active Sessions: 60 [Max: 69]

La pantalla principal de **Ntop** consta de los siguientes menús:

- **About:** información sobre ntop, créditos, documentaciones y configuraciones.
- **Summary:** tráfico, hosts, carga de red, flujos de red
- **All protocols:** tráfico, actividad
- **IP:** resumen, direcciones de tráfico, local
- **Utils:** volcado de datos, registro de vista
- **Plugins:** sección donde habilitar complementos
- **Admin:** configuración y cierre de la aplicación.

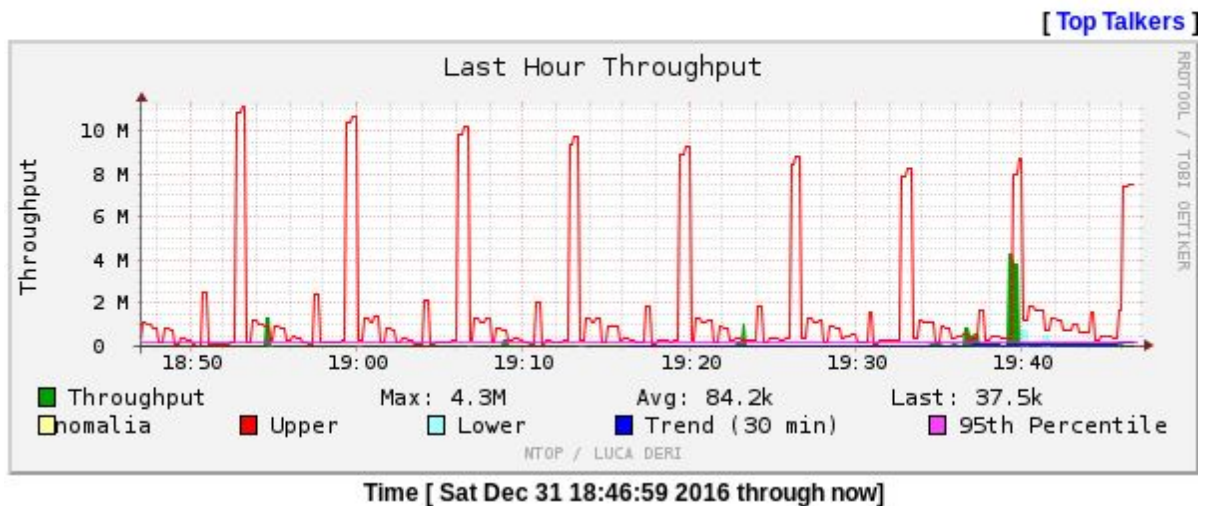
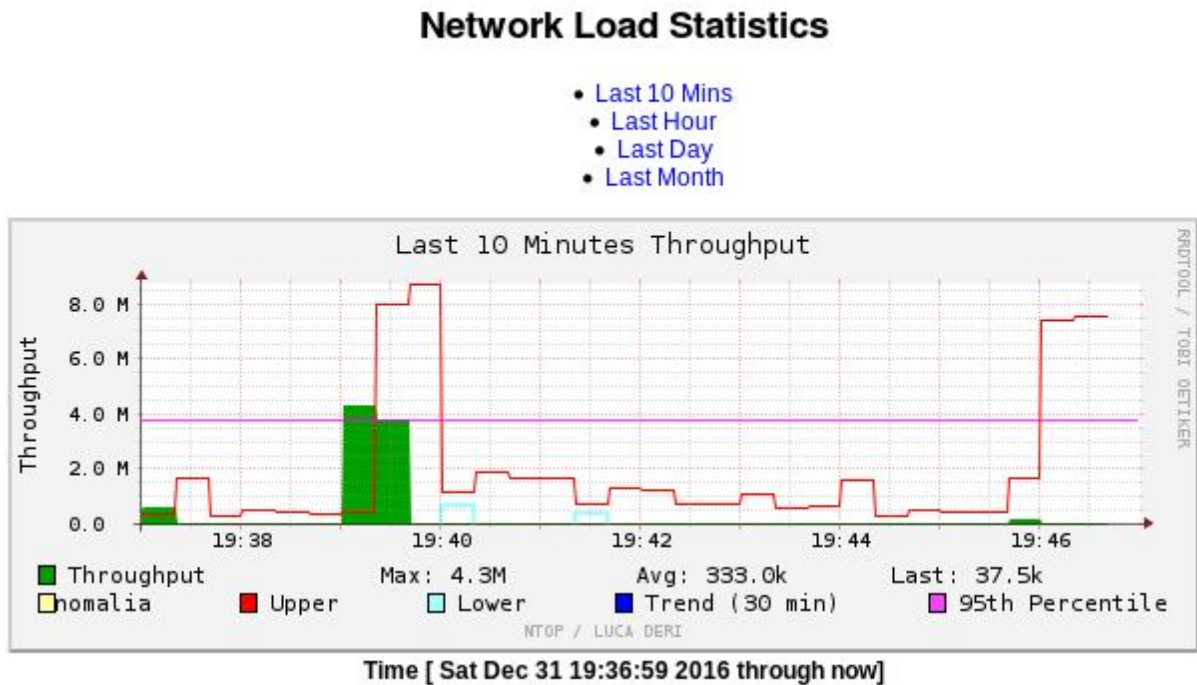
La cantidad de cosas que podemos ver es muy extensa, pero sobre todo se utiliza para monitorizar el tráfico de la red y los posibles picos de tráfico, en qué host se han producido, etc.

Por ejemplo, podemos desglosar el tráfico por IP:

Network Traffic [IP]: All L3 Hosts - Data Sent+Received

Host	Location	Data	Unknown	Mail_POP	Mail_SMTP	HTTP	MDNS	SSDP
192.168.2.50		548.8 KBytes 40.4 %	11.0 KBytes	551.7 KBytes	3.2 KBytes	20.6 KBytes	0	4.8 KBytes
www.youtube.com		250.4 KBytes 18.4 %	0	284.1 KBytes	0	0	0	0
ubun...server.monitor.local		159.9 KBytes 11.8 %	0	142.8 KBytes	28.7 KBytes	0	0	0
fonts.gstatic.com		102.9 KBytes 7.6 %	0	104.3 KBytes	0	0	0	0
wo-in-f189.1e100.net		96.6 KBytes 7.1 %	0	96.6 KBytes	0	0	0	0
192.168.2.1		35.5 KBytes 2.6 %	0	0	34.1 KBytes	0	0	0
mad0...09-in-f142.1e100.net		26.5 KBytes 1.9 %	0	28.9 KBytes	0	0	0	0
192.168.2.111		24.1 KBytes 1.8 %	0	0	0	0	19.9 KBytes	3.2 KBytes
192.168.1.116		20.9 KBytes 1.5 %	2.8 KBytes	0	0	18.1 KBytes	0	0
224.0.0.251		19.9 KBytes 1.5 %	0	0	0	0	19.9 KBytes	0
csi.gstatic.com		13.0 KBytes 1.0 %	0	13.0 KBytes	0	0	0	0
\$		11.6 KBytes 0.9 %	0	14.4 KBytes	0	0	0	0
239.255.255.250		9.3 KBytes 0.7 %	0	0	0	0	0	9.3 KBytes
mad01s25-in-f4.1e100.net		8.5 KBytes 0.6 %	0	8.5 KBytes	0	0	0	0
162.254.196.40		7.2 KBytes 0.5 %	7.2 KBytes	0	0	0	0	0
mad0...10-in-f170.1e100.net		6.5 KBytes 0.5 %	0	6.5 KBytes	0	0	0	0
mad0...26-in-f162.1e100.net		5.4 KBytes 0.4 %	0	5.4 KBytes	0	0	0	0
		5.1 KBytes 0.4 %	0	5.8 KBytes	0	0	0	0
192.168.1.108		2.5 KBytes 0.2 %	0	0	0	2.5 KBytes	0	0
wm-in-f188.1e100.net		1.1 KBytes 0.1 %	1.1 KBytes	0	0	0	0	0
goog...lic-dns-a.google.com		1008 0.1 %	0	0	1008	0	0	0
goog...lic-dns-b.google.com		593 0.0 %	0	0	593	0	0	0
pedro-pc [NetBIOS]		311 0.0 %	0	0	0	0	0	0
dlink-b52993 [NetBIOS]		251 0.0 %	0	0	0	0	0	0
lgmp.mcast.net		240 0.0 %	0	0	0	0	0	0
all-systems.mcast.net		60 0.0 %	0	0	0	0	0	0

Gráficos con la carga de la red por tiempo:



Incluso configurar alarmas para que salten cuando se llegue a cierto pico de tráfico.

Para monitorizar un equipo en particular, debemos seguir la siguiente ruta:

Hosts Hosts

Welcome to ntopng

localhost:3000/ua/host_details.lua?host=igmp.mcast.net

Search

ntop

Flows

Hosts

Interfaces

Host: 224.0.0.22

Traffic

Ports

Peers

Protocols

Flows

Talkers

Similarity

(Router) MAC Address

IPv4mcast_00:00:16 (01:00:5E:00:00:16)

IP Address

224.0.0.22

Name

igmp.mcast.net Remote

First / Last Seen

02/01/2017 21:10:38 [21 sec ago]

02/01/2017 21:10:38 [21 sec ago]

Sent vs Received Traffic Breakdown

Traffic Sent / Received

0 Pkts / 0 Bytes

6 Pkts / 0 Bytes

Hosts

Networks

MAC Addresses

Autonomous Systems

Countries

Operating Systems

HTTP Servers (Local)

Top Hosts (Local)

Geo Map

Tree Map

Local Flow Matrix

10 Filter Hosts

Input

ops

ops

ops

All Hosts

Local Only

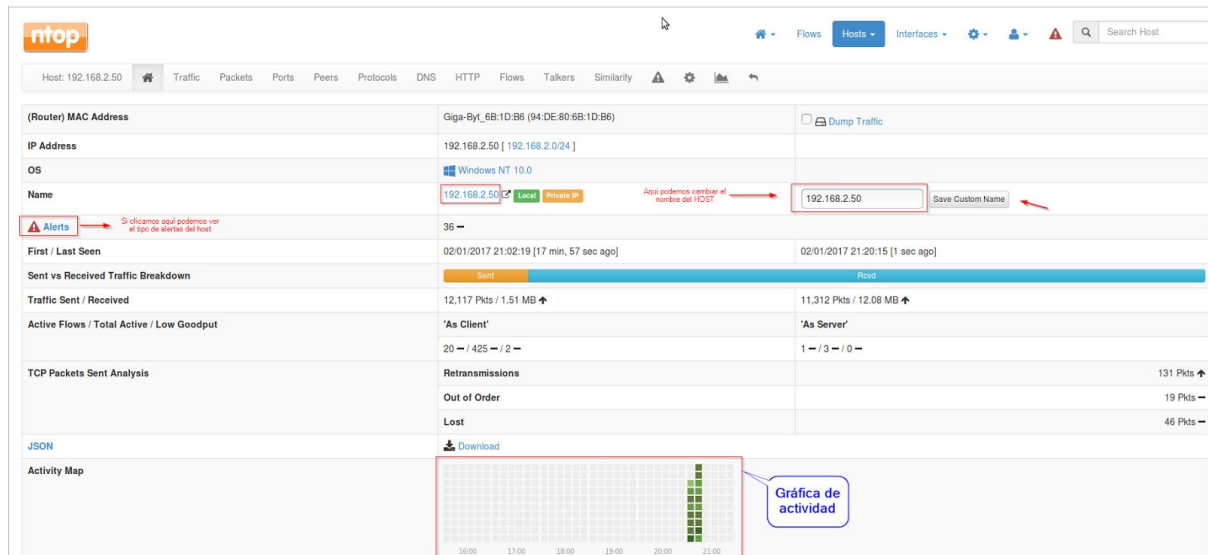
Remote Only

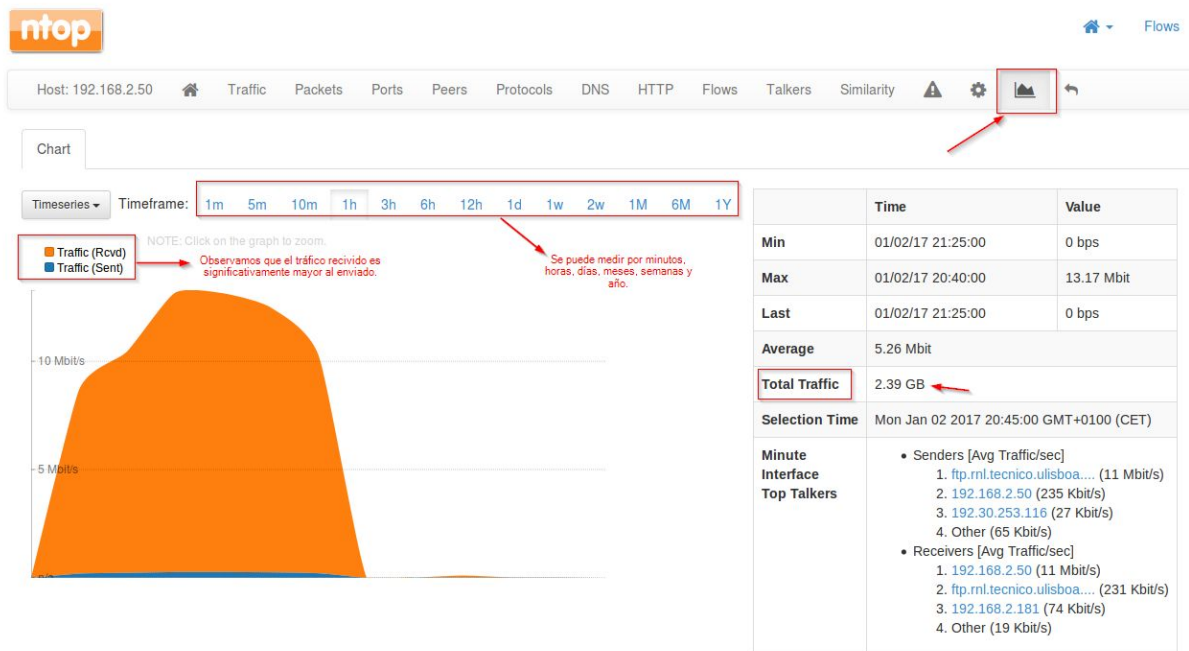
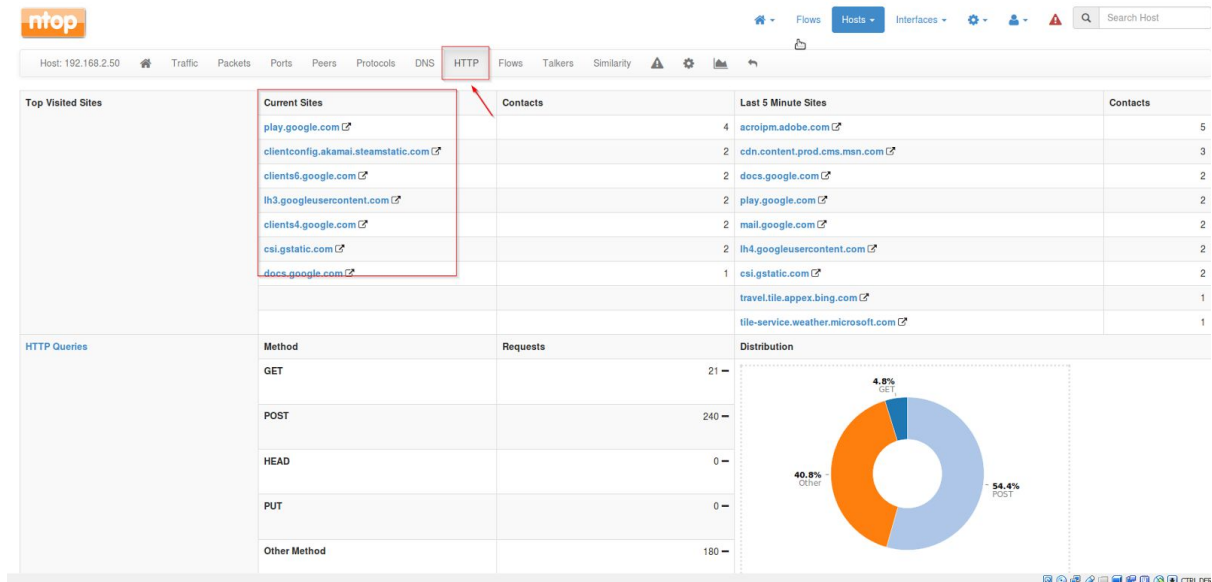
Local Networks

Local Hosts

IP Address	Location	Alerts	Name	Seen Since	ASN	Breakdown	Throughput	Traffic
192.168.2.50	Local	23	192.168.2.50	12 min, 5 sec		Rowd	513.6 bps	12.92 MB
192.168.2.255	Local	0	192.168.2.255	11 min, 53 sec		Rowd	0 bps	12.65 KB
192.168.2.181	Local	0	192.168.2.181	12 min, 6 sec		Rowd	28.56 Kbit	4.56 MB
192.168.2.180	Local	0	192.168.2.180	12 min, 1 sec		Sent	0 bps	360 B
192.168.2.175	Local	0	192.168.2.175 [Windows]	12 min, 3 sec		Sent	0 bps	603 B
192.168.2.112	Local	0	192.168.2.112	12 min, 4 sec		Sent	0 bps	44.6 KB
192.168.2.111	Local	0	192.168.2.111	12 min, 1 sec		Sent	544 bps	48.26 KB
192.168.2.102	Local	0	192.168.2.102	12 min, 1 sec		Sent	286.4 bps	221.8 KB
192.168.2.1	Local	0	192.168.2.1	12 min, 6 sec		Sent	0 bps	1.5 KB

Podemos ver todos los hosts conectados en la misma red. Si pulsamos sobre alguno de ellos, por ejemplo el 192.168.2.50, el cual tiene un S.O. Windows tal y como aparece en la imagen, nos aparece toda la información del mismo.





ntop Hosts

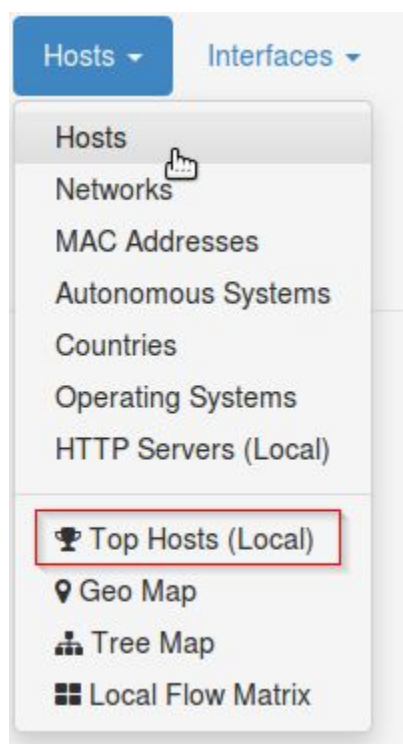
Host: 192.168.2.50 Traffic Packets Ports Peers Protocols DNS HTTP Flows Talkers Similarity ⚠ ⚙ 📊 ↶

Every Minute Every 5 Minutes Hourly Daily

Alert Function	Threshold
bytes → Cada cuantos Bytes ya sea >, >=, <, <= saltará la alarma	> 10 Bytes delta (sent + received)
dns	> <input type="text"/> DNS traffic delta bytes (sent + received)
idle	> <input type="text"/> Idle time since last packet sent (seconds)
p2p	> <input type="text"/> Peer-to-peer traffic delta bytes (sent + received)
packets	> <input type="text"/> Packets delta (sent + received)
Rearm minutes → Cada cuantos minutos quieres que te salte la alarma	2 <input type="text"/> The rearm is the dead time between one alert generation and the potential generation of the next alert of the same kind.

Save Configuration [Delete All Host Configured Alerts]

Por último si queremos ver el ranking de host por tráfico:



Top Hosts (Local)


09:10 09:15 09:20 09:25 09:30 09:35 09:40 09:45

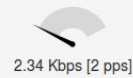


192.168.2.50
192.168.2.181
192.168.2.102
192.168.2.112
192.168.2.111
192.168.2.255
192.168.2.1
192.168.2.175
192.168.2.180

© 1998-2017 - nmap.org
Generated by ntopng Community v.2.4.161220
for user [admin](#) and interface [enp0s3](#)

[Upgrade to Professional version](#)

 Star 958



2.34 Kbps [2 pps]



1.96 Kbps
0 bps