Bisoños Usuarios de GNU/Linux de Mallorca y Alrededores | Bergantells Usuaris de GNU/Linux de Mallorca i Afegitons

Ntop, o el mejor amigo del administrador de red (63833 lectures)

Per **Xus**, ***Xus*** (http://www.zoyolabs.com)

Creado el 14/03/2002 00:35 modificado el 14/03/2002 00:35

Ntop significa Network TOP, y muestra el uso de la red. Es uno de los más completos programas sobre la monitorización de red que he visto, y además es GNU

Hoy en dia el tema de las redes cada vez es más importante, por eso conviene saber qué está pasando en cada momento. Hay muchos sniffers hechos, como por ejemplo el sniffit, el ethereal, pero no tiene nada que ver con el Ntop.

Los porotocolos que es capaz de monitorizar éste último son: TCP/UDP/ICMP, (R)ARP, IPX, DLC, Decnet, AppleTalk, Netbios, y ya dentro de TCP/UDP es capaz de agruparlos por FTP, HTTP, DNS, Telnet, SMTP/POP/IMAP, SNMP, NFS, X11.

Para instalarlo, nada más sencillo que bajarse los fuentes de http://snapshot.ntop.org/tgz/ntop-current.tgz(1), hacerle el "./configure; make; make install", pero conviene estar atentos por si no encuentra alguna que otra librería. Para hacerlo funcionar con todas sus prestaciones, conviene tener instalado:
- GDChart(2): Es un programa para poder hacer gráficos. Ya viene integrado en el fichero ntop-current.tgz, pero también hay que dejarlo instalado.
- lsof(3): Es un programa capaz de listar que ficheros están abiertos en el sistema.
- nmap(4): Es un programa capaz de escanear una red de ordenadores en busca de información.
- Librerías OpenSSL(5): Para poder optar a que el servidor web acepte conexiones seguras (SSL).
- Servidor MySQL(6): Para permitir almacenar toda la información en una base de datos. Para poder conectar NTOP con el MySQL, hay que ayudarse de un pequeño programita hecho en perl que viene dentro del paquete y se llama "mySQLserver.pl". Evidentemente se ha de tener el módulo DBI(7) de perl para acceder al MySQL.

Ahora ya estamos en condiciones de verlo funcionar, osea que vamos allá. Para arrancarlo, acepta muchas condiciones, de las que destaco estas: -P /var/lib/ntop -w 3000 -W 3003 -i eth0 -b localhost:4000 -d -E -L -a /www/logs/ntop.log

-P /var/lib/ntop: Donde se dejan las tablas hash.
-w 3000: Abrimos el servidor en el puerto 3000.
-W 3003: Abrimos el servidor SSL en el puerto 3003.
-i eth0: Escuchamos todo el tráfico que pasa por la tarjeta de red eth0.
-b localhost:4000 : Donde está el programa puente para el servidor MySQL.
-d: Para que se convierta en demonio.
-E: Para que se ayude de herramientas externas (lsof, nmap, ...).
-L: Habilita la salida al syslog.
-a /www/logs/ntop.log: Es el fichero de acceso a la página web del ntop.

Una vez que ha arrancado, podemos ver qué está pasando en nuestra red visitando la página web http://localhost:3000/, o http**S**://localhost:3003/. El menú de navegación principal se encuentra en el frame de arriba, y nos permite ver las siguientes opciones:
- **About**: Muestra una explicación del programa, así como los créditos de las personas que lo han hecho.
- **Data Rcvd, Data Sent**: Nos enseña que datos se han recibido/transmitido. Las posibilidades para visualizarlo es agrupándolo por protocolos, por TCP/UDP, qué cantidad se ha tratado, la actividad de cada host, y netflows.
- **Stats**: Es el apartado de estadísticas, en la que nos eseña información muy completa acerca del estado de la red. Nos enseña si es tráfico unicast, o multicast, la longitud de los paquetes, el Time To Live del paquete, y el tipo de tráfico que viaja (todo ello con porcentajes). También saca un listado de dominios, y qué plugins podemos activar o desactivar.
- **IP Traffic**: Nos da información acerca del sentido del tráfico, si va de la red local a una red remota, o viecevera.

- **IP Protos**: Nos da estadísticas del uso, pero a nivel de red como conjunto de hosts.
- **Admin**: Sirve para poder cambiar la inerfaz de red, crear filtros, y un mantenimiento de usuarios.

Resumiendo:
Es una herramienta que no puede faltar al administrador de red, porque además de monitorizar todo lo que pasa en la red, es capaz de ayudarnos a la hora de detectar malas configuraciones de algún equipo (esto salta a la vista porque al lado del host sale un banderín amarillo o rojo, dependiendo si es un error leve o grave), o a nivel de servicio.

Lista de enlaces de este artículo:

1. http://snapshot.ntop.org/tgz/ntop-current.tgz
2. http://www.fred.net/brv/chart
3. ftp://vic.cc.purdue.edu/pub/tools/unix/lsof
4. http://www.insecure.org/nmap
5. http://www.openssl.org/source
6. http://www.mysql.com/downloads
7. http://www.mysql.com/downloads/api-dbi.html

E-mail del autor: xus _ARROBA_ binissalem.net
Podrás encontrar este artículo e información adicional en: http://bulma.net/body.phtml?nIdNoticia=1226