

El Día a Día del Administrador de Sistemas: Dnsgraph

GRÁFICOS MAESTROS

Un servidor DNS sobrecargado puede retrasar todos los puestos de trabajo de una red. Dnsgraph es un sistema de aviso que proporciona a los administradores un gráfico de valores críticos. Sus diagramas le ayudarán a tener a punto sus sistemas servidores de nombres.

POR CHARLY KÜHNAST

Recientemente he oído hablar sobre un tipo con mucha memoria que podía recordar el valor de pi hasta varios miles de cifras decimales; al mismo tiempo, este hombre no podía explicar el valor práctico de este ejercicio. Personas como ésta no necesitan un servidor DNS; podrían memorizar algunos miles de direcciones IPs, al contrario que la gente normal, que prefiere el DNS. Si tú mismo llevas un servicio de resolución de nombres, estoy seguro de que apreciarás Dnsgraph [1].

El nombre del proyecto es muy parecido al de otros, como Mailgraph y Queuegraph, estando actualmente basado

en Mailgraph. La herramienta analiza un fichero de información generada por mi servidor DNS Bind 9 [2] y convierte las cifras en gráficos.

Para acceder a la información utilizo Rndc, un programa de control del paquete Bind que me permite enviar comandos firmados digitalmente al servidor de nombres. Esto me proporciona la habilidad de decirle al servidor que escriba la información de estado en un fichero, que Dnsgraph puede procesar posteriormente. También necesito la herramienta RRD y el módulo Perl File::Tail.

Tiempo de Configuración

Mi fichero de configuración Bind, *named.conf*, también tiene una sección de *options*, como es típicamente el caso. He añadido la siguiente línea:

```
statistics-file "/path_to/
/named-stats.log";
```

y luego los bloques del Listado 1 permiten las comunicaciones Rndc. Como contrapunto, el Listado 2 pertenece al fichero de configuración de Rndc, normalmente

Listado 2: Configuración Rndc

```
01 key "rndc-key2" {
02     algorithm hmac-md5;
03     secret
04         "<I>secretpassword<I>";
05 };
06 options {
07     default-key "rndc-key";
08     default-server 127.0.0.1;
09     default-port 953;
10 };
```

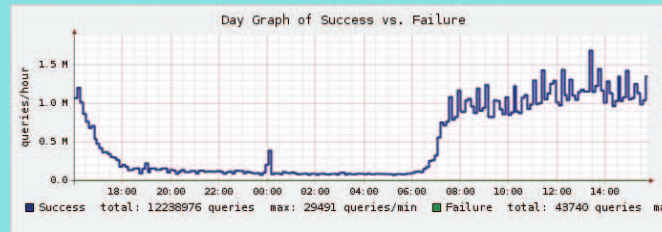


Figura 1: Los administradores que ejecutan un servidor Bind apreciarán cualquier información que Dnsgraph les proporcione.

/etc/rndc.conf. Esto permite a Rndc pasar comandos a Bind. El siguiente comando:

```
rndc stats
```

le indica a Bind que cree el fichero de registros previamente configurado y añada alguna información.

Adaptación de Scripts a Dnsgraph

Necesito añadir la ruta al fichero de registros o a RRD para *dnsanalyse.pl* y *dnsreport.pl*. En *dnsgraph.pl*, he de modificar la ruta de salida (TARGET) y la ruta a los scripts de Dnsgraph. La configuración final hace referencia a los ficheros del cron. El paquete viene con un fichero de ejemplo del *dnsgraph.cron*, por lo que tendré que modificar la ruta de entrada para que coincida con la de mi entorno. El paso final es lanzar el proceso de evaluación. Quince minutos después, la herramienta RRD me proporciona los resultados (Figura 1).

Listado 1: Añadir a named.conf

```
01 key "rndc-key" {
02     algorithm hmac-md5;
03     secret
04         "<I>secretpassword<I>";
05 };
06 controls {
07     inet 127.0.0.1 port 953
08     allow { 127.0.0.1; } keys
09         { "rndc-key"; };
10 };
```

SYSADMIN

El Ataque de los Bots 58

Aprenda cómo Charly se enfrenta a un spamming botnet sin escrúpulos.

Apache ModSecurity 60

ModSecurity es un cortafuegos integrado para los servidores web Apache.

RECURSOS

[1] Dnsgraph: dnsgraph.sourceforge.net

[2] Bind: <http://www.isc.org/index.pl?sw/bind/>

EL AUTOR

Charly Kühnast es Gerente de Sistemas Unix en el centro de datos de Moers, Alemania, cerca del conocido Rhin. Entre sus labores se incluye la seguridad del cortafuegos, la disponibilidad y cuidado de la DMZ (zona desmilitarizada).

