Stress Tools: The Sysadmin's Daily Chores

That's What I Call Stress!

Production servers that collapse under the burden of user activity are not exactly the kind of visiting card an admin would want to hand out. So it makes sense to give your system a really tough load to cope with before you roll it out in your production environment. Is your server looking for trouble, mate? Look no further! **BY CHARLY KÜHNAST**

When configuring servers I know in advance that some of them will be subject to extreme loads. In this case, I like to find out whether the server will be able to handle the task in hand, or if one or two nuts and bolts need tightening up. Let's get in some target practice on a web server first. The range of tools I could use for this task is enormous, and it is admittedly difficult to see the wood for the trees. But hammerhead [1] seems to provide a fair compromise between performance and ease of configuration.

The tool, a 120Kb tarball, is easily customized to suit your current environment. You can use the config file */etc/hammerhead/ hh.conf* to specify the number of threads, timeout thresholds and so on. And hammerhead can use IP aliasing to simulate a number of users on various machines.

After letting hammerhead walk rough shod across your web server for a few seconds, you will be presented with a short report. The ratio of successful and unsuccessful access attempts, and the average response times, which indicate any shortcomings. Hammerhead also offers an option for testing SSL web servers, but this feature is relatively new, and I for one would not like to vouch for the results at the present time. So let us leave this job to a more capable and dedicated tool, such as the SSL Stress Client [2].

POP3 Under Fire

Servers that need to open and close hordes of connections and handle logons at the same time, such as POP3 servers are likely candidates for load testing. Smpop [3], a tool with an extremely small 5 kb footprint, is pre-destined for this task. As might be expected from such a small package, the tool is not exactly convenient to use, but it does exactly what it is supposed to – that is, it reads username/password pairs from a file and attempts a configurable number of simultaneous logins on POP3 servers. If you set the threshold high enough, you can make even the most powerful mail manglers skip a beat.

But there is no need to restrict your attack to a single service. If I want to know if a specific application will continue to perform smoothly, or if the CPU is in danger of melting down, or if the hard disks are taking a thrashing, it's "seconds out and round one" for stress [4]. Stress is capable of precisely simulating specific loads on a computer. Typing

```
stress --loadavg 20
```

will set a load of 20 (plus/minus ten per cent). And

```
stress --hogdisk 10000m test
```

tells stress to write 10 Gbytes of trash to the *test* file – that should keep your hard disks occupied. You might like to spend a few minutes experimenting to approach the load level you would expect in a production environment.

A word of warning: Any tools that allow you to perform effective load tests are also suitable for DoS attacks. If you are tempted to try out these stress tools on other people's computers, you can expect cars with flashing blue lights to pull up outside your door within no time at all – and the "admins" driving them might not be too friendly! ∎

INFO

[1] Hammerhead: *http://hammerhead. sourceforge.net*

[2] SSL Stress Client: *http://sslclient. sourceforge.net*

[3] Smpop: *http://www.pfy.nl/smpop/*

[4] Stress: *http://weather.ou.edu/~apw/ projects/stress/*

THE AUTHOR

Charly Kühnast is a Unix System Manager at a public datacenter in Moers, near Germany's famous River Rhine. His tasks include ensuring firewall security and availability and taking care of the DMZ (demilitarized zone). Although Charly started out on IBM mainframes, he has been working predominantly with Linux since 1995.