Smokeping lab part 2

Network Management & Monitoring - Smokeping - Part II

Add new probes to Smokeping

The current entry in the Probes file is fine, but if you wish to use additional Smokeping checks you can add them in here and you can specify their default behavior. You can do this, as well, in the Targets file if you wish.

To add a probe to check for DNS lookup latency, edit the Probes file and **add** the following text TO THE END of that file:

```
# editor Probes
```

```
+ DNS
binary = /usr/bin/dig
pings = 5
step = 180
lookup = www.nsrc.org
```

Be sure you did not remove the FPing entry from this file.

The DNS probe will look up the IP address of www.nsrc.org using any other open DNS server (resolver) you specify in the Targets file. You will see this a bit further on in the exercises.

Now Save and exit from the file and verify that your changes are working:

```
# systemctl restart smokeping
# journalctl -eu smokeping
```

> *Note: sadly, the "echoping" module, which could check HTTP/HTTPS latency, was unmaintained (https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=957161) and has been removed (https://tracker.debian.org/pkg/echoping) from Ubuntu 22.04.*

Add DNS latency checks

At the end of the Targets file we are going to add some entries to verify the latency from our location to remote recursive DNS servers to look up an entry for nsrc.org.

You would likely substitute an important address for your institution in the Probes file instead. In addition, you can change the address you are looking up inside the Targets file as well. For more information see:

http://oss.oetiker.ch/smokeping/probe/DNS.en.html (http://oss.oetiker.ch/smokeping/probe/DNS.en.html)

and

http://oss.oetiker.ch/smokeping/probe/index.en.html
(http://oss.oetiker.ch/smokeping/probe/index.en.html)

Now edit the Targets file again. Be sure to go to the end of the file:

```
# cd /etc/smokeping/config.d            (just to be sure...)
# editor Targets
```

At the **end** of the file add:

```
#
# Sample DNS probe
#

+DNS

probe = DNS
menu = DNS Latency
title = DNS Latency Probes

++LocalDNS1
menu = gw.ws.nsrc.org
title =  DNS Delay for local DNS Server on gw.ws.nsrc.org
host = gw.ws.nsrc.org

++GoogleA
menu = google-public-dns-a.google.com
title = DNS Latency for google-public-dns-a.google.com
host = 8.8.8.8

++GoogleB

menu = google-public-dns-b.google.com
title = DNS Latency for google-public-dns-b.google.com
host = 8.8.4.4

++OpenDNSA
```

```
menu = resolver1.opendns.com
title = DNS Latency for resolver1.opendns.com
host = 208.67.222.222

++OpenDNSB

menu = resolver2.opendns.com
title = DNS Latency for resolver2.opendns.com
host = 208.67.220.220
```

Now save the Targets file and exit and verify your work:

```
# systemctl restart smokeping
```

Look at additional Smokeping probes and consider implementing some of them if they are useful to your organization:

http://oss.oetiker.ch/smokeping/probe/index.en.html
(http://oss.oetiker.ch/smokeping/probe/index.en.html)

MultiHost graphing

Once you have defined a group of hosts under a single probe type in your /etc/smokeping/config.d/Targets file, then you can create a single graph that will show you the results of all smokeping tests for all hosts that you define. This has the advantage of letting you quickly compare, for example, a group of hosts that you are monitoring with the FPing probe.

The MultiHost graph function in Smokeping has difficult syntax - pay close attention!

To create a MultiHost graph first edit the file Targets:

```
# editor Targets
```

We will create a MultiHost graph for the DNS Latency probes we just added. To do this go to the **end** of the Targets file and add:

```
#
# Multihost Graph of all DNS latency checks
#

++MultiHostDNS

menu = MultiHost DNS
title = Consolidated DNS Responses
```

```
host = /DNS/LocalDNS1 /DNS/GoogleA /DNS/GoogleB /DNS/OpenDNSA
/DNS/OpenDNSB
```

And, as always, save and exit from the file Targets and test your new configuration.

```
# systemctl restart smokeping
# journalctl -eu smokeping
```

If this fails you almost certainly have an error in the entries. If you cannot figure out what the error is (also try “tail /var/log/syslog” first!) ask your instructor for some help.

You can add MultiHost graphs for any other set of probe tests (FPing, EchoPingHttp) that you have configured. You must add the MultiHost entry at the end of a probe section. If you don’t understand how this works you can ask your instructors for help.

In addition, on the workshop NOC there are sample configuration files available, including one for SmokePing that includes multiple MultiHost graph examples.

Send Smokeping alerts

Update your device entries to include a line that reads:

```
alerts = alertName1, alertName2, etc, etc...
```

For instance, the alert named, “someloss” has already been defined in the file Alerts:

To read about Smokeping alerts and what they are detecting, how to create your own, etc. see:

http://oss.oetiker.ch/smokeping/doc/smokeping_config.en.html
(http://oss.oetiker.ch/smokeping/doc/smokeping_config.en.html)

and at the bottom of the page is a section titled `*** Alerts ***`

To place some alert detection on some of your hosts, open the Targets file:

```
# editor Targets
```

and go near the start of the file where we defined our hosts. Just under the “host =” line add another line that looks like this:

```
alerts = someloss
```

So, for example, the entry for host1 on campusY would look like this:

```
++host1

menu = host1
```

```
title = Host 1 Campus Y
host = host1.campusY.ws.nsrc.org
alerts = someloss
```

If you want to add an alerts option to other hosts go ahead. Once you are done save and exit from the Targets file and then verify that your configuration works:

```
# systemctl restart smokeping
```

If any of the hosts that have the “alerts =” option set meet the conditions to set off the alert, then an email will arrive to the sysadm user’s mailbox on the Smokeping server machine (localhost). It’s not likely that an alert will be set off for most machines. To check you can read the email for the sysadm user by using an email client like “mutt” -

```
# su - sysadm              (changes you to the sysadm user from
root)
$ mutt
```

Say yes to mailbox creation when prompted, then see if you have email from the smokeping-alerts@localhost user. You probably will not. To exit from Mutt press “q”.

To leave the sysadm user shell type:

```
$ exit   - (Ctrl + D)
#
```

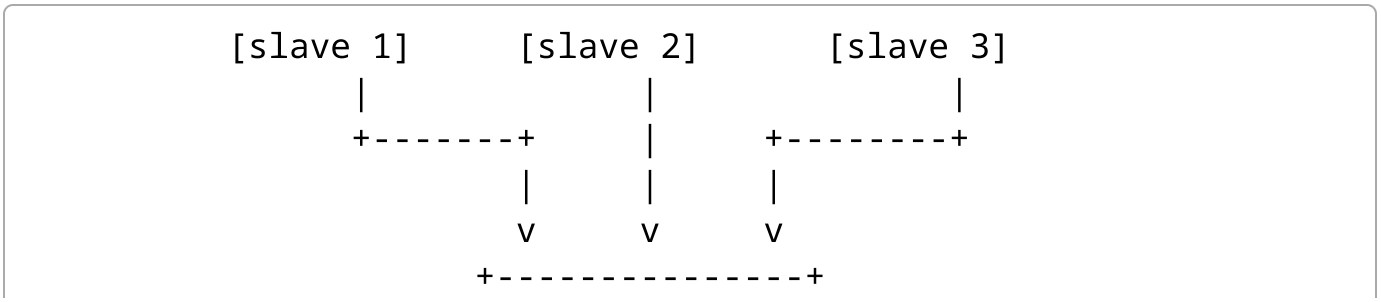
Slave instances - Informational Only

This is a description only for informational purposes in case you wish to attempt this type of configuration once the workshop is over.

The idea behind this is that you can run multiple smokeping instances at multiple locations that are monitoring the same hosts and/or services as your master instance. The slaves will send their results to the master server and you will see these results side-by-side with your local results. This allows you to view how users outside your network see your services and hosts.

This can be a powerful tool for resolving service and host issues that may be difficult to troubleshoot if you only have local data.

Graphically this looks this:



```
                    |    master     |
                    +---------------+
```

You can see example of this data here:

http://oss.oetiker.ch/smokeping-demo/ (http://oss.oetiker.ch/smokeping-demo/)

Look at the various graph groups and notice that many of the graphs have multiple lines with the color code chart listing items such as “median RTT from mipsrv01” - These are not MultiHost graphs, but rather graphs with data from external smokeping servers.

To configure a smokeping master/slave server you can see the documentation here:

http://oss.oetiker.ch/smokeping/doc/smokeping_master_slave.en.html (http://oss.oetiker.ch/smokeping/doc/smokeping_master_slave.en.html)

In addition, a sample set of steps for configuring this is available in the file sample-smokeping-master-slave.txt which should be listed as an additional reference at the bottom of the Agenda page on your classroom wiki.