Network Management & Monitoring
Smokeping

Exercises
----

0. Connect to your PC as the sysadm user and start a root shell

        $ sudo bash
        #

1. Install Smokeping

        # apt-get install smokeping

Then point your web browser at

        http://pcN.ws.nsrc.org/cgi-bin/smokeping.cgi

to check that it is running.

2. Initial Configuration

        # cd /etc/smokeping/config.d
        # ls -l

    -rwxr-xr-x 1 root root 578 2010-02-26 01:55 Alerts
    -rwxr-xr-x 1 root root 237 2010-02-26 01:55 Database
    -rwxr-xr-x 1 root root 413 2010-02-26 05:40 General
    -rwxr-xr-x 1 root root 271 2010-02-26 01:55 pathnames
    -rwxr-xr-x 1 root root 859 2010-02-26 01:55 Presentation
    -rwxr-xr-x 1 root root 116 2010-02-26 01:55 Probes
    -rwxr-xr-x 1 root root 155 2010-02-26 01:55 Slaves
    -rwxr-xr-x 1 root root 8990 2010-02-26 06:30 Targets

The files that you'll need to change, at a minimum, are:

    * Alerts
    * General
    * Probes
    * Targets

Now open the General file (note the first capital letter)

```
# editor General
```

Change the following lines (DON'T LEAVE THEM INDENTED):

```
owner    = NOC
contact  = sysadm@localhost
mailhost = localhost
cgiurl   = http://localhost/cgi-bin/smokeping.cgi
# specify this to get syslog logging
syslogfacility = local5
```

Save the file and exit. Now let's restart the Smokeping service to verify
that no mistakes have been made before going any further:

```
# service smokeping stop
# service smokeping start
```

A quicker way to do this is:

```
# service smokeping restart
```

We'll use this for the rest of the exercises, or we'll just use the "reload" directive as this is
all you need for Smokeping to see configuration file changes.

Now open the Alerts file (note the first capital letter)

```
# editor Alerts
```

Change the following lines (DON'T LEAVE THEM INDENTED):

```
to = root@localhost
from = smokeping-alert@localhost
```

Save the file and exit. Restart Smokeping:

```
# service smokeping reload
```


3. Configure monitoring of devices

The majority of your time and work configuring Smokeping will be

done in the
file /etc/smokeping/config.d/Targets.

For this class please do the following:

Use the default FPing probe to check:

        - all the student NOC PCs
        - classroom NOC
        - switches
        - routers

You can use the classroom Network Diagram on the classroom wiki to figure out addresses
for each item, etc.

Create some hierarchy to the Smokeping menu for your checks. For example, the Targets
file is already partially preconfigured. To start we are going to add some entries to
this file. Start with:

                # cd /etc/smokeping/config.d
                # editor Targets

You can take the section from *** Targets *** to the end of the LocalMachine and make it
look something like this. Feel free to use your own "remark", "menu" text and titles. Note
that we remove the commented lines "#parents = owner:/Test/James location:/", and the "Alerts"
line.

NOTE: We strongly recommend that you COPY and PASTE text from these exercises directly in to the
Targets file. Typing all this by hand will take too long.

The ">>>>>>>>" are not in the file, this indicates start of text, then "<<<<<<<<" is end
of text:

>>>>>>>>

*** Targets ***

probe = FPing

```
menu = Top
title = Network Latency Grapher
remark = Smokeping Latency Grapher for Network Monitoring \
         and Management Workshop.

+Local

menu = Local Network Monitoring and Management
title = Local Network

++LocalMachine

menu = Local Machine
title = This host
host = localhost

<<<<<<<


Now, below the "localhost" we start with the configuration of items
for our class.
We can start simple and add just the first 4 PCs that are in Group 1
as well as an
entry for our classroom NOC.

>>>>>>>>

#
# ********* Classroom Servers **********
#

+Servers

menu = Servers
title = Network Management Servers

++noc

menu = noc
title = Workshop NOC
host = noc

#
# ******** Student Machines (VMs) ***********
#
```

```
+PCs

menu = Lab PCs
title = Virtual PCs Network Management

++pc1

menu = pc1
title = Virtual Machine 1
host = pc1


++pc2

menu = pc2
title = Virtual Machine 2
host = pc2


++pc3

menu = pc3
title = Virtual Machine 3
host = pc3


++pc4

menu = pc4
title = Virtual Machine 4
host = pc4

<<<<<<<<
```

OK. Let's see if we can get Smokeping to stop and start with the changes we have
made, so far. Save and exit from the Targets file. Now try doing:

```
# service smokeping reload
```

If you see error messages, then read them closely and try to correct the problem
in the Targets file. In addition, Smokeping is now sending log message to the file
/var/log/syslog. You can view what Smokeping is saying by typing:

```
                    # tail /var/log/syslog
```

If you want to see all smokeping related messages in the file /var/log/syslog you
can do this:

```
                    # grep smokeping /var/log/syslog
```

If there are no errors you can view the results of your changes by
going to:

```
                    http://pcN.ws.nsrc.org/cgi-bin/smokeping.cgi
```

When you are ready you can edit the Targets file again and continue
to add machines.
At the bottom of the file you can add the next group of PCs:

>>>>>>>>

++pc5

menu = pc5
title = Virtual Machine 5
host = pc5

++pc6

menu = pc6
title = Virtual Machine 6
host = pc6

++pc7

menu = pc7
title = Virtual Machine 7
host = pc7

++pc8

menu = pc8
title = Virtual Machine 8
host = pc8

<<<<<<<<

Add as many PCs as you want, then Save and exit from the Targets
file and verify
that the changes you have made are working:

                 # service smokeping reload

You can continue to view the updated results of your changes on the
Smokeping
web page. It may take up to 5 minutes before graphs begin to appear.

                 http://pcN.ws.nsrc.org/cgi-bin/smokeping.cgi

4. Configure monitoring of routers and switches

Once you have configured as many PCs as you want to configure, then
it's time to
add in some entries for the classroom routers and switch(es).

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

Go to the bottom of the file and add in some entries for routers and
switches:

>>>>>>>>

#
********** Classroom Backbone Switch *********
#

+Switches

menu = Switches
title = Switches Network Management

++sw

menu = sw
title = Backbone Switch

```
host = sw

#
# ********** Virtual Routers: Cisco 7200 images *********
#

+Routers

menu = Routers
title = Virtual and Physical Routers Network Management

++gw

menu = rtr
title = Gateway Router
host = rtr

++router1

menu = router1
title = Virtual Router 1
host = rtr1

++router2

menu = router2
title = Virtual Router 2
host = rtr2

++router3

menu = router3
title = Virtual Router 3
host = rtr3

<<<<<<<
```

If you wish you can continue and add in entries for routers 4 to 6, or up to 9 if there are
that many in your class. When you are ready Save and Exit from the Targets file and verify
your work:

```
# service smokeping reload
```

If you want you might consider adding the Wireless Access Point:

```
                # editor Targets


>>>>>>>>

#
# Classrom Wireless Access Point
#

++ap1

menu = ap1
title = Wireless Access Point 1
host = ap1

<<<<<<<<

Save and Exit from the file and reload the Smokeping service:

                # service smokeping reload


5. 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 HTTP latency as well as DNS lookup
latency add the
following TO THE END of the Probes file (remember ">>>>" and "<<<<<"
are not to be
included):

                # editor Probes


>>>>>>>>

+ EchoPingHttp

+ DNS
binary = /usr/bin/dig
```

```
pings = 5
step = 180
lookup = www.nsrc.org
```

<<<<<<<

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
futher on in the exercises.

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

```
# service smokeping reload
```

6. Add HTTP latency checks for the classroom PCs

Edit the Targets file again and go to the end of the file:

```
# editor Targets
```

At the end of the file add:

>>>>>>>

```
#
# Local Web server response
#

+HTTP

menu = Local HTTP Response
title = HTTP Response Student PCs

++pc1

menu = pc1
title = pc1 HTTP response time
probe = EchoPingHttp
host = pc1
```

```
++pc2

menu = pc2
title = pc2 HTTP response time
probe = EchoPingHttp
host = pc2

++pc3

menu = pc3
title = pc3 HTTP response time
probe = EchoPingHttp
host = pc3

++pc4

menu = pc4
title = pc1 HTTP response time
probe = EchoPingHttp
host = pc4

<<<<<<<<
```

You could actually just use the "probe = EchoPingHttp" statement
once for pc1,
and then this would be the default probe until another "probe = "
statement is
seen in the Targets file.

You can add more PC entries if you wish, or you could consider
checking the
latency on remote machines - these are likely to be more
interesting. Machines
such as your own publicly accessible servers are a good choice, or,
perhaps other
web servers you use often (Google, Yahoo, Government pages, stores,
etc.?).

For example, consider adding something like this at the bottom of
the Targets file:

```
>>>>>>>>

#
# Remote Web server response
```

```
#

+HTTPRemote

menu = Remote HTTP Response
title = HTTP Response Remote Machines

++google

menu = Google
title = Google.com HTTP response time
probe = EchoPingHttp
host = www.google.com

++nsrc

menu = Network Startup Resource Center
title = nsrc.org HTTP response time
probe = EchoPingHttp
host = nsrc.org

<<<<<<<<
```

Add your own hosts that you use at your organization to the list of
Remote Web Servers.

Once you are done, save and exit from the Targets file and verify
your work:

```
                # service smokeping reload
```

7. 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 substitue 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

and

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 = 10.10.0.250
title =  DNS Delay for local DNS Server on noc.ws.nsrc.org
host = noc.ws.nsrc.org

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

++GoogleB

menu = 8.8.8.4
title = DNS Latency for google-public-dns-b.google.com
host = google-public-dns-b.google.com

++OpenDNSA

menu = 208.67.222.222
```

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

++OpenDNSB

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

<<<<<<<<
```

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

```
# service smokeping reload
```

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

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


8. 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 is extremely picky - 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.

                    # service smokeping reload

If this fails you almost certainly have an error in the entries. If
you cannot figure
out what the error is (remember to 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.

9. Send Smokeping alerts

If you wish to receive an email when an alert condition is met on one of the
Smokeping checks first do this:

```
# cd /etc/smokeping/config.d
# editor Alerts
```

Update the top of the file where it says:

```
*** Alerts ***
to = alertee@address.somewhere
from = smokealert@company.xy
```

to include a proper "to" and "from" field for your server. Something like:

```
*** Alerts ***
to = sysadm@localhost
from = smokeping-alert@localhost
```

Now you must 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
```

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

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

```
# editor Targets
```

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

```
alerts = someloss
```

So, for example, the pc1 entry would not look like this:

```
>>>>>>>

++pc1

menu = pc1
title = Virtual Machine 1
host = pc1
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:

```
# service smokeping reload
```

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" -

```
# apt-get install 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".

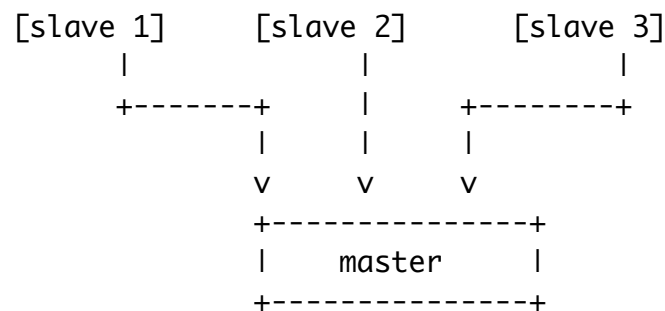To leave the sysadm user shell type:

```
$ exit
#
```

10. 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:

```
        [slave 1]     [slave 2]      [slave 3]
            |             |              |
        +-------+         |       +--------+
                |         |       |
                v         v       v
                +---------------+
                |    master     |
                +---------------+
```

You can see example of this data here:

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

In addition, a sample set of steps for configuring this is available

in
the file sample-smokeping-master-slave.txt which should be lisetd as
an
additional reference at the bottom of the Agenda page on your
classroom wiki.