Nagios Installation and Configuration

Notes:
---
* Commands preceded with "$" imply that you should execute the command as
  a general user - not as root.
* Commands preceded with "#" imply that you should be working as root.
* Commands with more specific command lines (e.g. "RTR-GW>" or "mysql>")
  imply that you are executing commands on remote equipment, or within
  another program.

Exercises

Exercises Part I
---

0. Log in to your virtual machine as the sysadm user.

1. Install Nagios Version 3

```
$ sudo apt-get install nagios3 nagios3-doc
```

You will be prompted for nagiosadmin password. Give it the normal workshop
password.

Note: if you have not already done so, you may be asked to configure
the Postfix Mail Transport Agent during the Nagios installation process.
Just accept the default "Internet Site".

2. See Initial Nagios Configuration

Open a browser, and go to your machine like this:

```
http://pcN.ws.nsrc.org/nagios3/
```

At the login prompt, login as:

```
user: nagiosadmin
pass: <CLASS PASSWORD>
```

Browse to the "Host Detail" page to see what's already configured.

3. Remove the File host-gateway_nagios3.cfg

```
$ sudo bash
# cd /etc/nagios3/conf.d
# rm host-gateway_nagios3.cfg
```

4. Update the File hostgroups_nagios2.cfg

```
# editor hostgroups_nagios2.cfg
```

Go to the bottom of the file and find the entry:

```
define hostgroup {
        hostgroup_name  ping-servers
                alias           Pingable servers
                members         gateway
        }
```

Change the members line so that this looks like:

```
define hostgroup {
        hostgroup_name  ping-servers
                alias           Pingable servers
                members         rtrX
        }
```

Where "rtrX" is the router for your group. Now save and exit the from the file.

5. Add Routers, PCs and Switches

We will create three files, routers.cfg, switches.cfg and pcs.cfg and make entries for the hardware in our classroom.

5a. Creating the switches.cfg file

```
    # editor switches.cfg
```

In this file add the following entry:

```
define host {
    use         generic-host
    host_name   sw
    alias       Backbone Switch
    address     10.10.0.253
}
```

Save the file and exit.

5b. Creating the routers.cfg file

We have 10 total routers. These are rtr1-rtr9 and gw-rtr. We will define entries for each of these.

```
    # editor routers.cfg
```

```
define host {
    use         generic-host
    host_name   gw-rtr
    alias       Classrooom Gateway Router
    address     10.10.0.254
}

define host {
    use         generic-host
    host_name   rtr1
```

```
    alias       Group 2 Gateway Router
    address     10.10.1.254
}

define host {
    use         generic-host
    host_name   rtr2
    alias       Group 2 Gateway Router
    address     10.10.2.254
}

define host {
    use         generic-host
    host_name   rtr3
    alias       Group 3 Gateway Router
    address     10.10.3.254
}

define host {
    use         generic-host
    host_name   rtr4
    alias       Group 4 Gateway Router
    address     10.10.4.254
}

define host {
    use         generic-host
    host_name   rtr5
    alias       Group 5 Gateway Router
    address     10.10.5.254
}

define host {
    use         generic-host
    host_name   rtr6
    alias       Group 6 Gateway Router
    address     10.10.6.254
}

define host {
    use         generic-host
    host_name   rtr7
    alias       Group 7 Gateway Router
    address     10.10.7.254
}

define host {
    use         generic-host
    host_name   rtr8
    alias       Group 8 Gateway Router
    address     10.10.8.254
}

define host {
    use         generic-host
    host_name   rtr9
    alias       Group 9 Gateway Router
    address     10.10.9.254
}

define host {
```

```
    use         generic-host
    host_name   ap1
    alias       Wireless Access Point 1
    address     10.10.0.251
}

define host {
    use         generic-host
    host_name   ap2
    alias       Wireless Access Point 2
    address     10.10.0.252
}
```

Now save and exit from the file.

5c. Creating the pcs.cfg File

Now we will create entries for all the Virtual Machines in our classroom. Below we give you the first few entries. You should complete the file with as many PCs as you wish to add. We recommend thet, at least, you add the 4 PCs that are members of your group as well as an entry for the classroom NOC, and at least one PC from another group.

```
    # editor pcs.cfg


define host {
    use         generic-host
    host_name   noc
    alias       Workshop NOC machine
    address     10.10.0.250
}

#
# Group 1
#

define host {
    use         generic-host
    host_name   pc1
    alias       pc1
    address     10.10.1.1
}

define host {
    use         generic-host
    host_name   pc2
    alias       pc2
    address     10.10.1.2
}

define host {
    use         generic-host
    host_name   pc3
    alias       pc3
    address     10.10.1.3
}
```

```
define host {
    use         generic-host
    host_name   pc4
    alias       pc4
    address     10.10.1.4
}
```

You can save and exit from the file now, or you can continue to add more PC entries.
If you have not added PCs for your group be sure to do that before you exit from the file.

STEPS 6a - 6c SHOULD BE REPEATED WHENEVER YOU UPDATE THE CONFIGURATION!
==========

6a. Verify that your configuration files are OK

```
    # nagios3 -v /etc/nagios3/nagios.cfg
```

    ... You should get some warnings like :

```
Checking services...
    Checked 7 services.
Checking hosts...
Warning: Host 'gw-rtr' has no services associated with it!
Warning: Host 'rtr1' has no services associated with it!
Warning: Host 'rtr2' has no services associated with it!

etc....
...
Total Warnings: N
Total Errors:   0

Things look okay - No serious problems were detected during the check.
Nagios is saying that it's unusual to monitor a device just for its
existence on the network, without also monitoring some service.
```

6b. Reload/Restart Nagios

```
    # service nagios3 restart
```

Not always 100% reliable to use the "restart" option due to a bug in the Nagios init script. To be sure you may want to get used to doing:

```
    # service nagios3 stop
    # service nagios3 start
```

HINT: You will be doing this a lot. If you do it all on one line, like this, then you can hit cursor-up and rerun all in one go:

```
    # nagios3 -v /etc/nagios3/nagios.cfg && /etc/init.d/nagios3 restart
```

The '&&' ensures that the restart only happens if the config is valid.

6c. Verify via the Web Interface

Go to the web interface (http://pcN.ws.nsrc.org/nagios3) and check that the hosts you just added are now visible in the interface. Click on the "Host Detail" item on the left of the Nagios screen to see this. You may see it in "PENDING" status until the check is carried out.

7. View Host Detail and Status Map

Go to http://pcN.ws.nsrc.org/nagios3

Click on the "Host Detail" item on the left. Are all the hosts you have defined listed? Are they up?

Click on the "Status Map" item on the left. You should see all your hosts with the Nagios process in the middle.

PART II
Configure Service check for the classroom NOC
---

0. Configuring

Now that we have our hardware configured we can start telling Nagios what services to monitor on the configured hardware, how to group the hardware in interesting ways, how to group services, etc.

1. Associate a service check for our classroom NOC

```
# editor hostgroups_nagios2.cfg
```

- Find the hostgroup named "ssh-servers". In the members section of the defintion change the line:

```
members         localhost
```

to

```
members         localhost,noc
```

Exit and save the file.

Verify that your changes are OK:

```
# nagios3 -v /etc/nagios3/nagios.cfg
```

Restart Nagios to see the new service assocation with your host:

```
# /etc/init.d/nagios3 restart
```

Click on the "Service Detail" link in the Nagios web interface to see your new entry.

PART III
Defining Services for all PCs
---

0. For services, the default normal_check_interval is 5 (minutes) in

generic-service_nagios2.cfg. You may wish to change this to 1 to speed up how quickly service issues are detected, at least in the workshop.

1. Determine what services to define for what devices

- This is core to how you use Nagios and network monitoring tools in general. So far we are simply using ping to verify that physical hosts are up on our network and we have started monitoring a single service on a single host (your PC). The next step is to decide what services you wish to monitor for each host in the classroom.

- In this particular class we have:

  routers: running ssh and snmp
  switches: running telnet and possibly ssh as well as snmp
  pcs: All PCs are running ssh and http and should be running snmp
  The NOC is currently running an snmp daemon

  So, let's configure Nagios to check for these services for these devices.

2.) Verify that SSH is running on the routers and workshop PCs images

- In the file services_nagios2.cfg there is already an entry for the SSH service check, so you do not need to create this step. Instead, you simply need to re-define the "ssh-servers" entry in the file /etc/nagios3/conf.d/hostgroups_nagios2.cfg. The initial entry in the file looked like:

```
# A list of your ssh-accessible servers
define hostgroup {
        hostgroup_name  ssh-servers
                alias           SSH servers
                members         localhost
        }
```

What do you think you should change? Correct, the "members" line. You should add in entries for all the classroom pcs, routers and the switches that run ssh. With this information and the network diagram you should be able complete this entry.

The entry will look something like this:

```
define hostgroup {
        hostgroup_name  ssh-servers
                alias           SSH servers
                members         localhost,pc1,pc2,pc3,pc4...,pc32,….ap1,ap2,noc,rtr1,rtr2…rtr
        }
```

Note: leave in "localhost" - This is your PC and represents Nagios' network point of view. So, for instance, if you are on "pc3" you would not include "pc3" in the list of all the classroom pcs as it is represented by the "localhost" entry.

The "members" entry will be a long line and will likely wrap on the screen.

Remember to include all your PCs and all your routers that you have defined. Do not include any entries if they are not already defined in pcs.cfg, switches.cfg or routers.cfg.

- Once you are done, run the pre-flight check:

```
# nagios3 -v /etc/nagios3/nagios.cfg
```

If everything looks good, then restart Nagios

```
# /etc/init.d/nagios3 stop
# /etc/init.d/nagios3 start
```

and view your changes in the Nagios web interface.

To continue with hostgroups you can add additional groups for later use, such as all our virt servers. Go ahead and edit the file hostgroups_nagios2.cfg again:

```
 # editor hostgroups_nagios2.cfg
```

and add the following to the end of the file:

```
# A list of our virtual routers
define hostgroup {
        hostgroup_name  cisco7200
                alias           Cisco 7200 Routers
                members         rtr1,rtr2,rtr3,rtr4,rtr5,rtr6,rtr7,rtr8,rtr9
        }
```

Save and exit from the file. Verify that everything is OK:

```
# nagios3 -v /etc/nagios3/nagios.cfg
```

If everything looks good, then restart Nagios

```
# service nagios3 stop
# service nagios3 start
```

3.) Check that http is running on all the classroom PCs.

- This is almost identical to the previous exercise. Just make the change to the HTTP service adding in each PC (no routers or switches). Remember, you don't need to add your machine as it is already defined as "localhost".