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

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
```

During installation you will be prompted for the "Nagios web administration password:" - This will be for the Nagios user "nagiosadmin". When prompted enter in the password you are using your sysadm account.

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 Name: nagiosadmin
        Password:  <CLASS PASSWORD>
```

Click on the "Hosts" link on the left of the initial Nagios page to see what has already been configured.

3. Enable External commands in nagios.cfg

This change is required in order to allow users to "Acknowledge" problems with hosts and services in the Web interface.

First, edit the file "/etc/nagios3/nagios.cfg", and change the line:

```
        check_external_commands=0
```

to

```
        check_external_commands=1
```

Save the file and exit.

Then, perform the following commands to change directory permissions and to make the changes permanent:

```
$ sudo /etc/init.d/nagios3 stop
$ sudo dpkg-statoverride --update --add nagios www-data 2710 /var/lib/nagios3/rw
$ sudo dpkg-statoverride --update --add nagios nagios 751 /var/lib/nagios3
$ sudo /etc/init.d/nagios3 start
```

4. Update the File hostgroups_nagios2.cfg

```
        $ cd /etc/nagios3/conf.d
        $ sudo editor hostgroups_nagios2.cfg
```

Go to the bottom of the file and add the following entry (we STRONGLY encourage you to COPY and PASTE!):

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

Where "rtrX" is the router for your group. That is, if you are in group 1, then replace "rtrX" with "rtr1". 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.

6a. Creating the switches.cfg file

```
        $ cd /etc/nagios3/conf.d                                (just to be sure)
        $ sudo editor switches.cfg
```

In this file add the following entry (COPY and PASTE!):

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

Save the file and exit.

6b. Creating the "routers.cfg" file

We have up to 10 total routers. These are rtr1-rtr9 and gw-rtr. And, we have 1 or 2 wireless Access Points (ap1, ap2). We will define entries for some of these. If any of these devices do not exist in your workshop, then do not include them. Remember, COPY and PASTE!

```
        $ sudo 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 1 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
}

# Note: you do not need to add definitions for all routers now = you can
# always come back and add the rest later!

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 the file and exit the editor.

6c. Creating the pcs.cfg File

Now we will create entries for some of 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 that, 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 (remember to COPY and PASTE!):

```
        $ sudo 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
}

#
# Another PC (example only!)
#

define host {
    use         generic-host
    host_name   pc20
    alias       pc20
    address     10.10.5.20
}
```

You can save and exit from the file now. You can add more PC entries later.

STEPS 7a - 7c SHOULD BE REPEATED WHENEVER YOU UPDATE THE CONFIGURATION!
===

7a. Verify that your configuration files are OK

```
        $ sudo nagios3 -v /etc/nagios3/nagios.cfg
```

You will get some warnings like the ones below. You can ignore them for now.

```
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.

7b. Reload/Restart Nagios

```
        $ sudo service nagios3 restart
```

HINT: You will be doing this a lot. If you do it all on one line, like this, then you can use arrow-up and call back the command:

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

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

7c. 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 "Hosts" item on the left of the Nagios screen to see this. You may see it in "PENDING" status until the check is carried out.

8. View Status Map

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

Click on the "Map" item on the left. You should see all your hosts with the Nagios process in the middle. The "?" are because we have not told Nagios what type of host each items is (router, switch, AP, PC running Linux, etc...)

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

```
    $ sudo 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:

```
        $ sudo nagios3 -v /etc/nagios3/nagios.cfg
```

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

```
        $ sudo service nagios3 restart
```

In the Nagios web interface, find the "Services" link (left menu), and click on it.

You should be able to find your recent change:

```
    noc  SSH      PENDING ...
```

PART III
Defining Services for all PCs

Note: The default normal_check_interval is 5 (minutes) for checking services. This is defined in "generic-service_nagios2.cfg". You may wish to change this to 1 (1 minute) to speed up how quickly service issues are detected, at least during this workshop.

1. Determine what services to define for what devices

   - This is a central concept in using 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 (web server, SSH, etc.) 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 on 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,...,ap1,noc,rtr1,rtr2,...,gw-rtr
        }
```

Note: do not remove "localhost" - This is your PC and represents Nagios' network point of view. So, for instance, if you are on "pc3" you would NOT list "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. If you want to start additional entries on newline then use "\" to indicate a newline like this:

Remember to include all the PCs and routers that you have defined in the files "pcs.cfg", "switches.cfg" and "routers.cfg". Only add entries from these files (i.e.: don't add "pc8" in your hostgroup list if "pc8" isn't defined in "pcs.cfg" as well).

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

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

... 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 virtu routers. Go ahead and edit the file hostgroups_nagios2.cfg again:

```
$ sudo editor hostgroups_nagios2.cfg
```

and add the following to the end of the file (COPY and PASTE this):

```
# A list of our virtual routers

define hostgroup {
        hostgroup_name  routers
                alias           Cisco 7200 Routers
                members         rtr1,rtr2,...
        }
```

Only list the routers you have defined in the "routers.cfg".

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

```
$ sudo nagios3 -v /etc/nagios3/nagios.cfg
```

If everything looks good, then restart Nagios

```
$ sudo service nagios3 restart
```

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". Look for this hostgroup in the file hostgroups_nagios2.cfg and update the "members" line appropriately.

If you have questions or are confused please ask an instructor for help.