Nagios Installation and Configuration

Introduction

Goals

Install and configure Nagios

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. “rtrX>" or “mysql>") imply that you are executing commands on remote equipment, or within another program.

Exercises

PART I

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

```
##########################################################
##################
      PREREQUISITES
##################
$ uname -a
$ lsb_release -a

###Ensure you have the correct time on your server###
$ date
$ sudo dpkg-reconfigure tzdata

$ sudo apt-get update
$ sudo apt-get install screen
#########################################################
```

2. 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”.

3. 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.

4. 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.

4a. 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   BBX1
    alias       Backbone Switch
    address     10.X.255.4
}

define host {
    use         generic-host
    host_name   BBX2
    alias       Backbone Switch
    address     10.X.255.5
}

define host {
    use         generic-host
    host_name   SW11
    alias       Acces Switch
    address     10.X.255.6
}

define host {
    use         generic-host
    host_name   SW12
    alias       Access Switch
    address     10.X.255.7
}
```

Save the file and exit.

```
########Swithches IPs#############
10.X.255.4------------>BBX1
10.X.255.5------------>BBX2
10.X.255.6------------>SWX1
10.X.255.7------------>SWX2
```

4b. Creating the “routers.cfg” file

```
$ sudo editor routers.cfg
define host {
    use         generic-host
    host_name   RX1
    alias       RX1
    address     10.X.254.1
}

define host {
    use         generic-host
    host_name   RX2
    alias       RX2
    address     10.X.254.2
}

define host {
    use         generic-host
    host_name   RX3
    alias       RX3
    address     10.X.254.3
}

define host {
    use         generic-host
    host_name   ISPLOOPBACK
    alias       ISP LOOPBACK
    address     5.5.5.5
}
```

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

Now save the file and exit the editor.

```
##########ROUTERS##############
10.X.254.1------------->RX1
10.X.254.2------------->RX2
10.X.254.3------------->RX3
5.5.5.5---------------->ISP LOOPBACK
```

STEPS 5a - 5c SHOULD BE REPEATED WHENEVER YOU UPDATE THE CONFIGURATION!

5a. 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' 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.

5b. 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 && sudo service nagios3 restart
The '&&' ensures that the restart only happens if the config is valid.

5c. 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.

6. 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...)

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.

PART II - Defining Services for all Devices

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. The next step is to decide what services (web server, SSH, etc.) you wish to monitor for each device in the classroom.

In this particular class we have:

routers: running ssh and snmp
switches: running telnet and possibly ssh as well as snmp
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.

```
# 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 routers and the switches that run ssh. With this information and the network diagram you should be able complete this entry. Add the routers replacing X with the group you were in. E.g for group one: R11,R12,R13...

The entry will look something like this:

```
define hostgroup {
        hostgroup_name  ssh-servers
                alias           SSH servers
                members         localhost,RX1,RX2,RX3,...,
        }
```

Note: do not remove “localhost” - This is your PC and represents Nagios' network point of view.

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 routers that you have defined in the file “routers.cfg”. Only add entries from these files.

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

```
$ sudo nagios3 -v /etc/nagios3/nagios.cfg && sudo service 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 virtual 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 2901 Routers
                members         RX1,RX2,RX3,...
```

```
        }
```

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 ssh is running on all the classroom routers.

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

formatted by Markdeep ✒

~~~~~~~~~~~~~~~~~~~~~~~~~~~

SAMPLE ROUTERS.CFG FILE

```
<snip>
define host {
    use         generic-host
    host_name   R11
    alias       R11
    address     10.1.254.1
}

define host {
    use         generic-host
    host_name   R21
    alias       R21
    address     10.2.254.1
}

define host {
    use         generic-host
    host_name   R31
    alias       R31
    address     10.3.254.1
}

define host {
    use         generic-host
    host_name   R41
    alias       R41
    address     10.4.254.1
}
define host {
    use         generic-host
    host_name   R12
    alias       R12
    address     10.1.254.2
}
```
~~~~~~~~~~~~~~~~~~~~~~~~~~~

```
define host {
    use         generic-host
    host_name   R22
    alias       R22
    address     10.2.254.2
}

define host {
    use         generic-host
    host_name   R32
    alias       R32
    address     10.3.254.2
}

define host {
    use         generic-host
    host_name   R42
    alias       R42
    address     10.4.254.2
}



define host {
    use         generic-host
    host_name   R13
    alias       R13
    address     10.1.254.3
}

define host {
    use         generic-host
    host_name   R23
    alias       R23
    address     10.2.254.3
}

define host {
    use         generic-host
    host_name   R33
    alias       R33
    address     10.3.254.3
}

define host {
    use         generic-host
    host_name   R43
    alias       R43
    address     10.4.254.3
}

define host {
    use         generic-host
    host_name   ISPLOOPBACK
    alias       ISP LOOPBACK
    address     5.5.5.5
}
</snip>
```

~~~~~~~~~~~~~~~~~~~~~~~~~~~
SAMPLE SWITCHES.CFG FILES

```
<snip>
define host {
    use         generic-host
    host_name   BB11
    alias       Backbone Switch
    address     10.1.255.4
}

define host {
    use         generic-host
    host_name   BB21
    alias       Backbone Switch
    address     10.2.255.4
}

define host {
    use         generic-host
    host_name   BB31
    alias       Backbone Switch
    address     10.3.255.4
}

define host {
    use         generic-host
    host_name   BB41
    alias       Backbone Switch
    address     10.4.255.4
}

define host {
    use         generic-host
    host_name   BB12
    alias       Backbone Switch
    address     10.1.255.5
}
define host {
    use         generic-host
    host_name   BB22
    alias       Backbone Switch
    address     10.2.255.5
}
define host {
    use         generic-host
    host_name   BB32
    alias       Backbone Switch
    address     10.3.255.5
}
define host {
    use         generic-host
    host_name   BB42
    alias       Backbone Switch
    address     10.4.255.5
}

define host {
    use         generic-host
```
~~~~~~~~~~~~~~~~~~~~~~~~~~~

```
    host_name   SW11
    alias       Acces Switch
    address     10.1.255.6
}

define host {
    use         generic-host
    host_name   SW21
    alias       Acces Switch
    address     10.2.255.6
}
define host {
    use         generic-host
    host_name   SW31
    alias       Acces Switch
    address     10.3.255.6
}
define host {
    use         generic-host
    host_name   SW41
    alias       Acces Switch
    address     10.4.255.6
}
define host {
    use         generic-host
    host_name   SW12
    alias       Access Switch
    address     10.1.255.7
}

define host {
    use         generic-host
    host_name   SW22
    alias       Access Switch
    address     10.2.255.7
}

define host {
    use         generic-host
    host_name   SW32
    alias       Access Switch
    address     10.3.255.7
}

define host {
    use         generic-host
    host_name   SW42
    alias       Access Switch
    address     10.4.255.7
}
</snip>
```