PRACTICAL EXERCISE 2 (W2_PE2): MONITORING HOSTS WITH NAGIOS

This practical exercise consists in building a basic Nagios configuration to monitor one or several hosts in a network.

1. Nagios Configuration Files

The main configuration file of Nagios is `/usr/local/nagios/etc/nagios.cfg`. It contains notably the instructions for inclusion of all the services, hosts, commands, contacts and others.

These included files reside mainly in `/usr/local/nagios/etc/objects`. Please take the time to browse these different files. By default, Nagios comes with a large set of pre-configured services that e.g. allow to easily monitor a set of Linux hosts.

2. Configure a Group of Monitored Hosts

In this MOOC context, you are probably at home, and your set of machines to be monitored depends on your home configuration. At a bare minimum, you can monitor the virtual machine (VM) itself, its host, and your internet box.

Remark: depending on the resources of your host, you might also launch other virtual machines (that may serve as additional network nodes to be monitored). You might also find that your wifi-connected smartphone can be a friendly network node as well! You may moreover borrow a number of family or friend computers to be added to your LAN: all of them could be good monitoring candidates!

> **Note:** Build a list, on paper or text document, of all available computers, along with their IP addresses. Consider only computers with verified network access (i reachable with `ping`)!

First, we will make a backup of the configuration files (note : nous supposons que vous êtes toujours connecté en tant que root ici, suite à l'exercice 1):

```
# cd /usr/local/nagios/etc
# cp -R objects objects-old
# cp nagios.cfg nagios.cfg.old
```

2.1 Main File Setup

In order to customize our setup, edit the main configuration file `nagios.cfg` to modify the reference to the `localhost.cfg` file which should become `nagios-lab.cfg` (note : n'oubliez pas de sauvegarder le fichier pour que la modification

Week_Evaluation
Echéance le avril 10, 2022 at 22:00 UTC

Aidez-nous à améliorer ce MOOC

- Week 3: Instrumentation with JMX
- Week 4: Next-Generation Management Protocols
- Votre avis nous intéresse

```
# Definitions for monitoring the local (Linux) host
# cfg_file=/usr/local/nagios/etc/objects/localhost.cfg
# <------ commented
cfg_file=/usr/local/nagios/etc/objects/nagios-lab.cfg
# <------ new
```

Go to the `objects` folder and copy the (now useless) `localhost.cfg` towards `nagios-lab.cfg`:

```
# cd objects
# cp localhost.cfg nagios-lab.cfg
```

Now edit the `nagios-lab.cfg` file to reflect the organization of the lab layout.

2.2 The Hostgroup

First, rename the generic "linux-servers" group of hosts with a more appropriate name, like "lab-machines":

```
define hostgroup {
        hostgroup_name  lab-machines ; The name of the
hostgroup
        alias           lab machines ; Long name of the group
        members         localhost,box,host; Comma separated
list of hosts that belong to this group
}
```

2.3 The Hosts

Now it is time to retrieve the host list made earlier.

Each of the hosts of the lab network has to be declared individually; think of cut-and-paste the definition existing for `localhost`. Note: the names for the hosts should be representative of the target host and should match the `hostgroup`'s members!

Example for one host:

```
define host {
        use                     linux-server            ; Name
of host template to use
        host_name               box
        alias                   box
        address                 10.0.1.12
}
```

```
define hostgroup {
        hostgroup_name  lab-machines ; The name of the
hostgroup
        alias           home machines ; Long name of the group
        members         localhost,box,host ; Comma separated
list of hosts that belong to this group
}
```

2.4 The Services

To simplify the setup we will consider only some of all the declared services for the lab hosts. Let us for example select ping, http and ssh. All selected services have to be modified to reflect their linkage with our group of hosts. The original definition is:

```
define service {
        use                             local-service
; Name of service template
        host_name                       localhost
        service_description             PING
        check_command
check_ping!100.0,20%!500.0,60%
}
```

... and should become (note the change of `host_name` to `hostgroup_name`):

```
define service {
        use                             local-service
; Name of service template
        hostgroup_name                  lab-machines
        service_description             PING
        check_command
check_ping!100.0,20%!500.0,60%
}
```

Perform this modification for each of the ping, http and ssh services.

2.5 Final Check and Restart

The setup should now be ready for a *pre-flight test* e.g. an off-line syntactical and semantical check of the configuration files:

```
# /usr/local/nagios/bin/nagios -v
/usr/local/nagios/etc/nagios.cfg
```

corriger, puis à relancer cette commande de vérification (avant de passer à l'étape suivante).

If no errors were detected, the nagios server can be restarted:

```
# systemctl restart nagios
```

The Nagios web pages should now depict the whole lab network (based on the new definitions that we have added).

Bilan de l'exercice : nous avons ajouté de nouvelles définitions à la configuration de Nagios, afin que celui-ci monitore de nouvelles machines et leurs services associés.

QUESTION W2.PE2.1 (1/1 point)

We would now like to demonstrate the "live" monitoring functionality of Nagios.

What could we do? Check all that apply. (NA=4)

- [x] We might disconnect the virtual machine (VM) from the network through the VirtualBox setting (lower border of the VM's window).
- [ ] We might use the Nagios user interface for that purpose.
- [x] We might just cancel the connection of a "victim" node.
- [x] We might just disconnect the ethernet cable of one of our nodes.
- [x] Why not simply switching off a node?

✔

Correct:
Yes, this will impact all nodes except localhost!
Correct.
Yes, for instance cancel out your smartphone's wifi is easy.
Yes, if you have some nodes with ethernet connection!
Sure!

Vous avez utilisé 1 essais sur 3