TP 2 : Supervision with check-mk

1. Introduction

Supervision is important in an Information System. Here we will use an interesting tool called Check-mk. This TP is not evaluated but you may need it for the third TP which will be.

1.1.Nagios

Mathias **K**ettner offered some interesting contributions to Nagios, an historical open-source Monitoring tool.
Nagios were created in 2002 (its predecessor, Netsaint were already available in 1999).
Nagios is a monitoring scheduler based on config files and plugin scripts.
Nagios uses Hosts and Services.

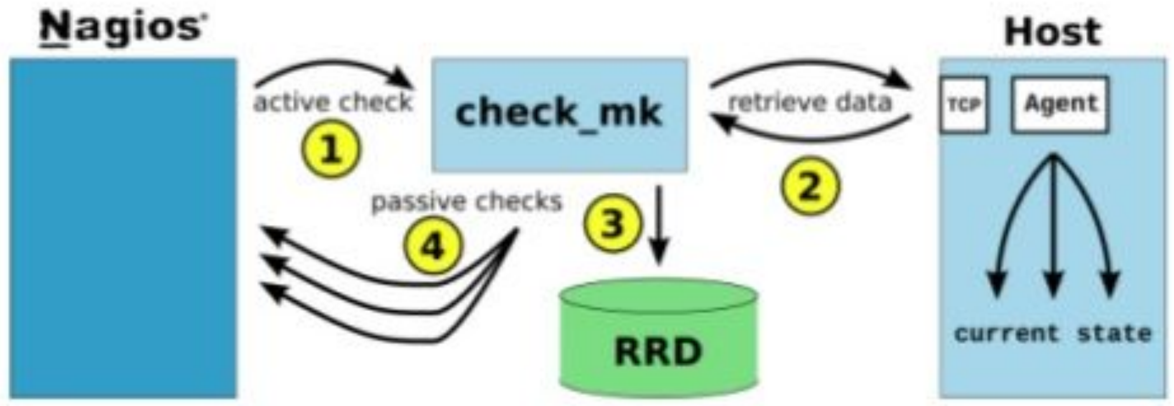
You can easy imagine Hosts as physical (or virtual) machines, each with its IP address.

Services will be useful to get and store different states of hosts. The name "service" comes from Network monitoring where a service like http or dns for example can have different states (OK/KO) on one host. Services are extended notions to any part of a host state.
Ex : Is the amount of RAM available consistent? It always defines a status (basically OK/KO)

Today, other information gan be gathered from one service (numerical or text) in addition.

1.2.Check-MK

In 2008, check-mk began as one of the multiple available Nagios plugins. Its philosophy differs from other plugins as one request to check-mk plugin will fill information for multiple services.



Today Check-mk is a full integrated tool. The open-source version still uses Nagios Core. The Licensed versions replaced Nagios with their own monitoring core.
One other advantage of this integration called OMD is the web GUI. It offers the possibility to make the complete configuration through an "intuitive Web interface". The plain Nagios Core still needs manual edition of local config files on the server.

2. Create two VMs

Using the services offered by ISTIC, please request the creation of two Linux Virtual Machines.
https://vm.istic.univ-rennes1.fr/

Remember to define a new password for zprojet users.

We will monitor one VM from the the other.
In real life, one server would monitor many machines

3. Install the Monitoring Server

Follow the installation instructions from https://checkmk.com/download?edition=cre&version=stable for the correct distribution

Once installed and started, don't forget to keep cmkadmin password safe

4. Install the agent

Install the agent from the offered packages (Setup > Agents > Linux)

Use wget or curl to download the agent on the vm you want to be monitored. Then apt or def to install it

Check port 6556 is open

```
sudo ss -lnpt
```

if not maybe need to start and enable

```
sudo systemctl enable check_mk.socket
sudo systemctl start check_mk.socket
```

5. Add the host

On the check-mk server, go in Setup > Hosts

"Add Host"

Define the hostname (xxx.istic.univ-rennes1.fr)

"Save and go to service configuration"

6. Services

Check all detected services

"Fix All"

7. Activate changes

In up right, there should be an info : "X changes"

"Activate on selected sites"

8. See data collected

Explore the Monitor part.
You will have some status available gradually.
You also could see some graphs.

9. Use SSH instead

9.1.Security issue

The agent is running as root and is available from the complete network. Even if it only reads data, this could be a security issue.

The first possible securing method could be to limit the access to the agent only from the monitoring server.
Depending on the agent running method, there are different solutions to achieve that.
A new security method exists and consists in mutual authentication between the client and server in TLS. This method is detailed in their documentation.

We will instead use ssh to secure the agent. So you will learn some interesting things about ssh.

9.2.Actions to do once on the monitoring server

We need to prepare the server and generate its ssh keys. On the server, we need to run command as the *monitoring* user. For that, you first need to be root, then type « su - *monitoring* »
With this prompt, run « ssh-keygen -t ed25519 » (and no passphrase)
Display the public key « cat .ssh/id_ed25519.pub » and keep the result for next steps

In "Setup > Agents > Other integrations > Individual program call instead of agent access", create a rule with the following parameters:

- "Command line to execute" : `ssh -o StrictHostKeyChecking=accept-new -T root@$HOSTADDRESS$`
- "Host labels" *has* "agentmode:ssh"

The "StrictHostKeyChecking=accept-new" is very important in our case.
Without, it would be necessary to add manually each host fingerprint to the server's known_hosts file.

9.3.Actions to do do for each machine to be monitored

Login on the machine to be monitored as root, then type these commands

```
mkdir /root/.ssh
chmod 700 /root/.ssh
echo 'command="/usr/bin/check_mk_agent" <Output of the previous cat>' > /root/.ssh/authorized_keys
chmod 600 /root/.ssh/authorized_keys
```

Then, on the monitoring server, add the label "agentmode:ssh" to the host configuration

And don't forget to apply...

On the monitored server, remove the systemd startup configuration

```
sudo systemctl stop cmk-agent-ctl-daemon.service
sudo systemctl disable cmk-agent-ctl-daemon.service
```

Then check that monitoring is still OK for your host and services

10. Explore and add external checks

Example for ssh :
Setup > Services > Other services > Check SSH service
Create rule in folder students
Explicit hosts : <your host>

Apply...

11. Annexes

11.1.Some interesting URL

The Nagios Core Documentation
https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/4/en/toc.html

Documentation to create Nagios Plugins
https://nagios-plugins.org/doc/guidelines.html

Some plugins maintained outside of Nagios
https://www.monitoring-plugins.org

A platform for sharing nagios plugins (Beware, the quality is random!)
https://exchange.nagios.org

Check-MK documentation
https://docs.checkmk.com/latest/en/

The Agent installation part with the new registration method.
https://docs.checkmk.com/latest/en/agent_linux.html

The Agent installation and ssh part
https://docs.checkmk.com/latest/en/agent_linux_legacy.html#ssh

11.2.Reminders

URL to create a VM
https://vm.istic.univ-rennes1.fr/

Check-mk server for this TP
http://esir-sys22.istic.univ-rennes1.fr/esir/

VPN ESIR + ISTIC
https://istic-vpn.univ-rennes1.fr/

Forti Client downloads
https://www.fortinet.com/fr/support/product-downloads

OpenFortiVPN client also works
https://github.com/adrienverge/openfortivpn