
Installation serveur NAGIOS

J'installe les paquets xorg xfce4 dnsutils procs terminator firefox-esr putty openssh-server
#Utiliser debian 10

Ensuite j'installe nagios comme ceci

Installer apache et php au préalable

Nagios4,nagios-plugins-contrib,nagios-nrpe-plugin

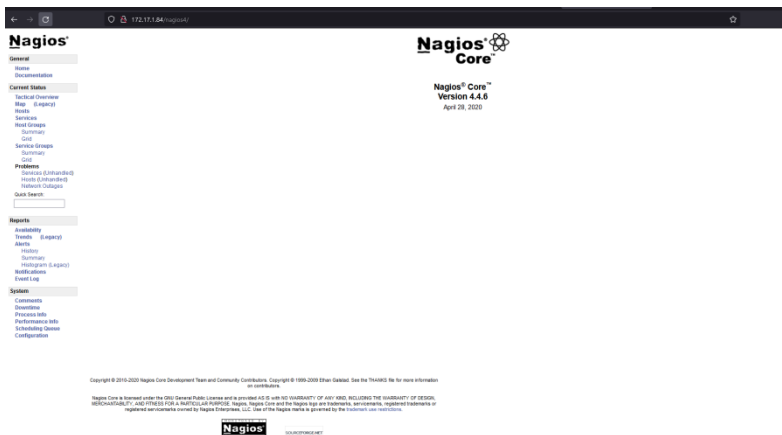
Ensuite activer ces deux modules apache

-auth_digest

-authz_groupfile

Ensuite avec le navigateur web aller sur <http://ipServeurNagios/nagios4>

Voila ce que je trouve



The screenshot shows the Nagios Core web interface. The browser address bar displays '172.17.1.84/nagios4'. The page features a dark header with the Nagios Core logo and version information: 'Nagios Core™ Version 4.4.6 April 28, 2020'. The main content area is divided into several sections: 'General' (Home, Documentation), 'Current Status' (Nagios Overview, Map, Services, Host Groups, Service Groups, Summary, Log), 'Problems' (Critical (2), Warning (0), Pending (0), Resolved (0)), 'Alerts' (Availability, Trends, Alerts, History, Summary, History (4.4.6.4.6)), 'System' (Overview, Processes, Performance, Scheduling, Database, Configuration), and a 'Quick Search' field. At the bottom, there is a copyright notice for Nagios Core and the Nagios logo.

Toute la partie ssh nommage dns etc a été faite dans des tp précédents

Je dois installer les agents Nagios qui permettent de faire la remontée SNMP

J'installe ncpa-2.2.0 sur windows

J'installe en ne paramétrant que les active checks

A l'emplacement token je mets le mdp de la communauté qui sera siojrr

Ensuite le reste je laisse vide et je fais l'installation pour l'other computer

Ne pas configurer NRDP

J'installe l'agent sur linux

J'installe depuis un serveur web le package .deb pour ce client nagios et je l'installe avec dpkg

```
root@smtp:~# wget https://assets.nagios.com/download/ncpa/ncpa-latest.d10.amd64.deb
--2021-11-17 11:42:43-- https://assets.nagios.com/download/ncpa/ncpa-latest.d10.amd64.deb
Résolution de assets.nagios.com (assets.nagios.com): 45.79.49.120, 2600:3c00::f03c:92ff:fe77:45ce
Connexion à assets.nagios.com (assets.nagios.com)[45.79.49.120]:443_ connecté.
requête HTTP transmise, en attente de la réponse... 301 Moved Permanently
Emplacement : https://assets.nagios.com/redirects/redirect.php?url=https://assets.nagios.com/download/ncpa/ncpa-latest.d10.amd64.deb [suivant]
--2021-11-17 11:42:44-- https://assets.nagios.com/redirects/redirect.php?url=https://assets.nagios.com/download/ncpa/ncpa-latest.d10.amd64.deb
Réutilisation de la connexion existante à assets.nagios.com:443.
requête HTTP transmise, en attente de la réponse... 404 Not Found
2021-11-17 11:42:44 erreur 404 : Not Found.
root@smtp:~# wget https://assets.nagios.com/downloads/ncpa/ncpa-latest.d10.amd64.deb
--2021-11-17 11:43:00-- https://assets.nagios.com/downloads/ncpa/ncpa-latest.d10.amd64.deb
Résolution de assets.nagios.com (assets.nagios.com): 45.79.49.120, 2600:3c00::f03c:92ff:fe77:45ce
Connexion à assets.nagios.com (assets.nagios.com)[45.79.49.120]:443_ connecté.
requête HTTP transmise, en attente de la réponse... 200 OK
Taille : 8074128 (7,7M) [application/vnd.debian.binary-package]
Sauvegarde en : « ncpa-latest.d10.amd64.deb »

ncpa-latest.d10.amd64.deb 100%[=====] 7,70M 1,10MB/s ds 14s
2021-11-17 11:43:23 (558 KB/s) - « ncpa-latest.d10.amd64.deb » sauvegardé [8074128/8074128]

root@smtp:~# dpkg -i ncpa-latest.d10.amd64.deb
Sélection du paquet ncpa précédemment désélectionné.
(Lecture de la base de données... 75067 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de ncpa-latest.d10.amd64.deb ...
The memcache was not invalidated by NSS responder.
Dépaquetage de ncpa (2.3.1-1) ...
Paramétrage de ncpa (2.3.1-1) ...
Traitement des actions différées (« triggers ») pour libc-bin (2.31-13) ...
root@smtp:~#
```

Je vais dans /usr/local/ncpa/etc/ncpa.cfg

Et je mets à l'emplacement community_string = siojrr

J'insère siojrr

Je redémarre l'agent comme ceci

Systemctl restart ncpa_listener.service

Configuration SNMP sur switch et routeur cisco

J'installe SNMPPB sur ma machine windows

Je vais sur mon switch cisco

Les droits seront en lecture seul

RO = pour readonly (lecture seulement)

RW = pour readwrite (lecture et ecriture)

D'abord je désactive la communauté publique en mode lecture seulement par défaut c'est active en lecture publique seulement

```
No snmp-server community public RO
```

Ensuite j'active la communauté privé en lecture seulement

```
Snmp-server community siojrr RO
```

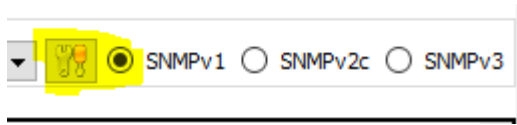
Ensuite je définis l'ip du serveur nagios pour la destination SNMP

Je fais ceci

```
Snmp-server host @ipnagios <nomCommunauté>
```

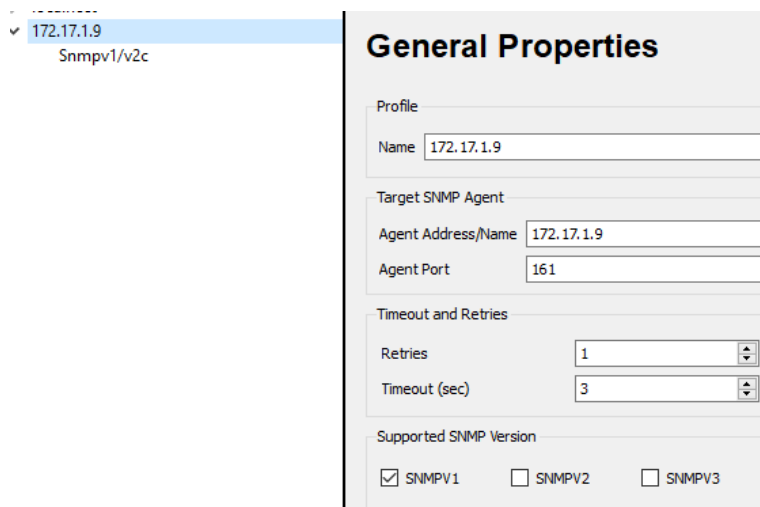
```
Switch(config)#snmp-server host 172.17.1.84 siojrr  
Switch(config)#
```

Sur snmpb je fais ceci je configure un agent en appuyant ici

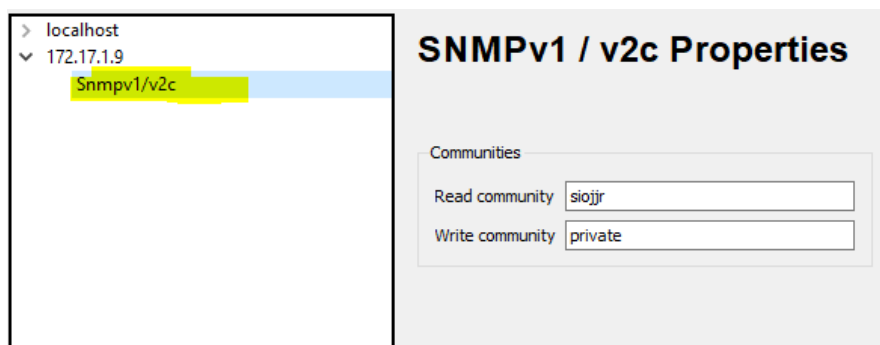


Je configure ensuite un agent et je mets a communauté une

Pour mon switch le premier onglet je configure comme sa



Ensuite je vais snmpbv1 et v2 et je configure comme sa je met le nom de la communauté



Je fais clic droit sur ifnumber et j'appuie sur walk

```
Query Results
-----SNMP query started-----
1: ifNumber.0 30
-----SNMP query finished-----
Total # of Requests = 2
Total # of Objects = 2
```

Voila ce qui est afficher

Je vais sur nagios et j'execute cette commande

```
/usr/lib/nagios/plugins/check_snmp -H <ipSwitch> -C <nomCommunauté> -o 1.3.6.1.2.1.2.2.1.5.1 --
w 1000000000 -c 10000000
```

-w = Seuil de warning

-c = seuil de critical

Ce noeud correspond à ma première interface réseau sur mon switch

Voici le résultat de la commande

```
root@smtp:/srv/tftp/switchCiscoDir# /usr/lib/nagios/plugins/check_snmp -H 172.17.1.9 -C siojrr -o .1.3
.6.1.2.1.2.2.1.5.1
SNMP OK - 1000000000 | iso.3.6.1.2.1.2.2.1.5.1=1000000000
root@smtp:/srv/tftp/switchCiscoDir# /usr/lib/nagios/plugins/check_snmp -H 172.17.1.9 -C siojrr -o .1.3
.6.1.2.1.2.2.1.5.1 -w 1000000000 -c 100000000
SNMP CRITICAL - *1000000000* | iso.3.6.1.2.1.2.2.1.5.1=1000000000;1000000000;1000000000
root@smtp:/srv/tftp/switchCiscoDir#
```

je vais dans le dossier /etc/nagios/conf.d

Pour créer un fichier de groupe et un fichier par utilisateur pour nagios

Je crée bookticgroupes.cfg et je met toutes les config dans ce fichier

Nagios ne fonctionnant pas sur debian 11 je passe sur une debian 10 son ip sera la 40 je crée donc le groupe bookticgroupes.cfg dessus je reconfigure ncpa sur windows et je modifie le fichier cgi comme prévue

Le fichier de conf ressemble à sa pour l'instant je vais sur ce lien <http://<ipNagios>/nagios4> je trouve ceci quand je touche à map

```
define hostgroup {
hostgroup_name group1
alias group1
members serverNagios
}

define host{
use linux-server
host_name serverNagios
alias serverNagios
address 172.17.1.40
}
```

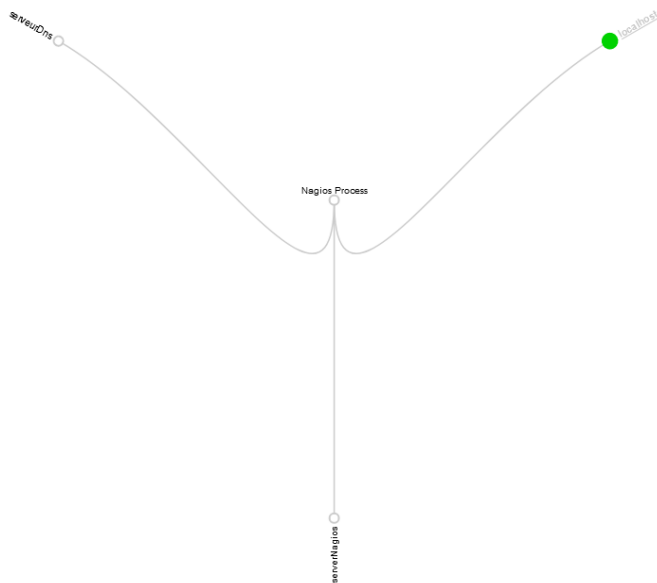


Je rajoute d'autres machine comme ceci

Par exemple la j'ai rajouter le serveur DNS

```
define host{
use linux-server
host_name serveurDns
alias serveurDns
address 172.17.1.88
}
```

Sa me donne sa



Pour que je puisse superviser des machines Windows il faut que je vais dans ce fichier et je décommente ces deux lignes

```
# Definitions for monitoring a Windows machine
cfg_file=/etc/nagios4/objects/windows.cfg

# Definitions for monitoring a router/switch
cfg_file=/etc/nagios4/objects/switch.cfg
```

Je rajoute ensuite ma machine Windows

Comme ceci

```
define host{
use windows-server
host_name adel
alias adel
address 172.17.1.3
}
define host{
use windows-server
host_name serveurAD
alias serveurAD
address 172.17.1.8
}
```

Ne pas oublier au fur à mesure de rajouter des membres dans le hostgroup

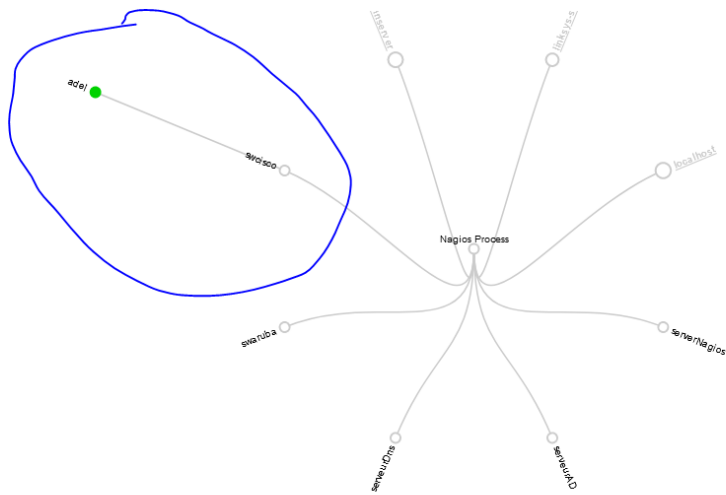
J'identifie les 2 switch comme ceci

```
define host{
use generic-switch
host_name swcisco
alias swcisco
address 172.17.1.8
}
define host{
use generic-switch
host_name swaruba
alias swaruba
address 172.17.1.16
}
```

Et pour rajouter une dépendance dire que tel machine est connecter à tel switch il faut que je définis la directive parent exemple pour la machine adel Windows server

```
define host{
use windows-server
host_name adel
alias adel
address 172.17.1.3
parents swcisco
}
```

Voilà la dépendance s'affiche sur la carte

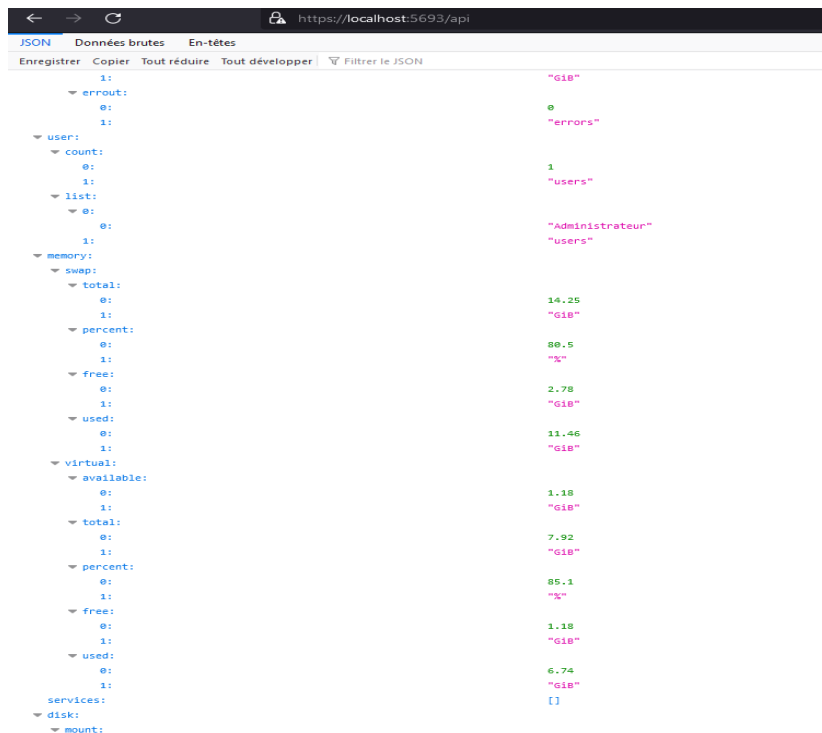


Suite nagios TP n°7 : utilisation des commandes

Comme j'avais installé ncpa sur mon windows dans le tp précédent je vais aller sur ce lien et mettre mon mdp « siojrr »

<https://localhost:5693/api>

J'ai accès à différentes informations comme la mémoire libre quel user est utilisé etc



Chaque point de contrôle est représenté par un chemin

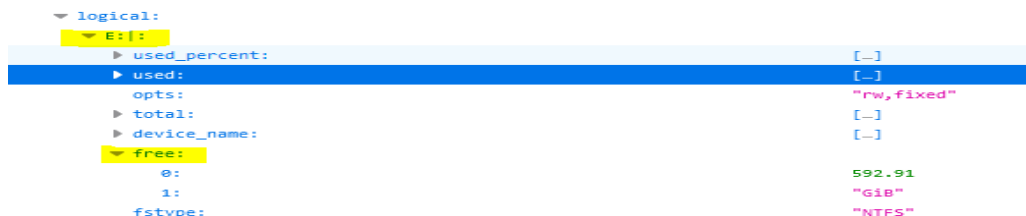
Sur le serveur nagios je vais installer la commande check_ncpa.py qui me permettra d'installer les différents points de contrôle

Wget https://assets.nagios.com/downloads/ncpa/check_ncpa.tar.gz

Ensuite je décompresse et je copie dans /usr/lib/nagios/plugins

```
root@SA:/tmp# tar -xvzf check_ncpa.tar.gz -C /usr/lib/nagios/plugins
CHANGES.rst
check_ncpa.py
```

Je veux vérifier cette information avec la ligne de commande



Il faut bien préciser la barre après « : » comme on est sur du windows

La syntaxe de la commande ressemble à sa

```
./check_ncpa.py -H <ip> -t <mdp> -M 'Chemin/point/de/contrôle' --warning <chiffre> --critical <chiffre>
```

--warning = Au bout de combien d'espace disque utiliser le message WARNING sera afficher

--critical = Pareil que warning juste le message change

```
root@SA:/usr/lib/nagios/plugins# ./check_ncpa.py -H 172.17.1.3 -t siojrr -M 'disk/logical/E:|/free' --warning 20 --critical 10
CRITICAL: Free was 592.91 GiB | 'free'=592.91GiB;20;10;
root@SA:/usr/lib/nagios/plugins#
```

Ici sa affiche critical parce que il y'a 10 giga d'espace libre au moins la commande ici n'a aucun sens mais pour de la RAM etc sa pourrai être beaucoup plus intéressant

Ou si je remplace la fin 'free' par 'used_percent' sa me donne le pourcentage du disque utiliser et la commande aura plus d'intérêt

```
root@SA:/usr/lib/nagios/plugins# ./check_ncpa.py -H 172.17.1.3 -t siojrr -M 'disk/logical/E:|/used_percent' --warning 20 --critical 10
CRITICAL: Used_percent was 13.70 % | 'used_percent'=13.70%;20;10;
root@SA:/usr/lib/nagios/plugins# _
```

Ici 13% sont utiliser donc sa passe dans le CRITICAL

Ensuite je dans /etc/nagios4/conf.d

Et je crée le fichier cmdes_servicesNCPA.cfg

```
define command {
    command_name checkncpa
    command_line $USER1$/check_ncpa.py -H $HOSTADDRESS$ $ARG1$
}
```

Je définis un nom de commande et je définis elle correspond à quoi la variable users1 c'est pour préciser le chemin les plugins hostaddress c'est l'ip et arg c'est un argument

Ensuite à la suite je définis le service

```
define service {
    use generic-service
    host_name adel
    service_description Mémoire Libre
    check_command checkncpa! -t siojrr -M memory/virtual/percent -w 80 -c 90
}_
```

Son nom sa description et la commande à exécuter

Host_name : Ici cela correspond à quel hôte va s'appliquer cette commande

Ensuite relancer le service nagios4

Aller dans services attendre 2 minutes réactualiser

Et voila

Host	Service	Status	Last Check	Duration	Attempt	Status Information
adel	Mémoire Libre	WARNING	12-01-2021 12:00:54	0d 0h 0m 10s	1/3	WARNING: Percent was 89.80 %

Pour les switches ça va être avec SNMP

Je crée le fichier cmdes_servicesSNMP.cfg

```
define command {
    command_name snmp_up
    command_line $USER1$/check_snmp -H '$HOSTADDRESS$' -C '$ARG1$' -o .1.3.6.1.2.1.2.2.1.8.'$ARG2$' -c 1 -l Status
}
```

Pareil je définis la commande son nom ici les arguments et host sont entre parenthèses

```
define service {
    use generic-service
    host swcisco
    service_description Verification si un port est activé
    check_command snmp_up!siojjr!10001
}
```

Ici je teste le port 1 remplacer par 10024 pour le port 24 sur cisco

Ensuite je définis le service la commande vérifiera si le port 24 est activé

Je relance le service nagios4

ARG1 = Sa définit la communauté
ARG2 = Sa spécifie le numéro de port

Ce qu'il y a entre les deux points d'exclamations c'est la communauté ARG1 ce qu'il y'a juste après c'est l'ARG2

Ensuite j'attends un peu et voilà ce qui m'est affiché sur nagios

Host	Service	Status	Last Check	Duration	Attempt	Status Information
swcisco	Verification si un port est activé	CRITICAL	01-05-2022 11:07:41	27d 22h 41m 54s	3/3	SNMP CRITICAL - Status *2*

La directive hostgroup_name peut servir à définir un groupe au lieu de définir des utilisateurs

Mise en place alerte par email

Au préalable il faut installer postfix sur la machine

Il faut se rendre dans le fichier « /etc/nagios4/object/contact.cfg »

Et pour avoir les alertes basiques il faut simplement modifier une ligne et mettre son mail juste ici

```
define contact{
    contact_name      nagiosadmin      ; Short name of user
    use                generic-contact  ; Inherit default values from gener$
    alias              Nagios Admin    ; Full name of user

    email              adel.sadek752@gmail.com ; <<***** CHANGE THIS TO YOUR EMAIL$
}
```

Ensuite dans nagios il faut aller dans « System > Configuration » ensuite sélectionner l'objet contact et vérifier si le mail a bien été prit en compte

Contacts						
Contact Name	Alias	Email Address	Pager Address/Number	Minimum Importance	Service Notification Options	Host Notification Options
nagiosadmin	Nagios Admin	adel.sadek752@gmail.com		0	Unknown, Warning, Critical, Recovery, Flapping, Downtime	Down, Unreachable, Recovery, Flapping, Downtime

Après avoir bien suivi toute ses étapes et vérifier que postfix fonctionne et peut envoyer des mails voici le résultat :

```
** PROBLEM Service Alert: the_cafe_du_monde/HTTP actif is CRITICAL **  
  
N nagios@Nagios  
  À adel.sadek752@gmail.com  
  
***** Nagios *****  
  
Notification Type: PROBLEM  
  
Service: HTTP actif  
Host: the_cafe_du_monde  
Address: 79.137.36.71  
State: CRITICAL  
  
Date/Time: Thu Jun 9 14:21:26 CEST 2022  
  
Additional Info:  
  
HTTP CRITICAL: HTTP/1.1 503 Service Unavailable - 4057 bytes in 0.333 second response time
```