

Installation et Configuration de Nagios

Notes :

- * Les commandes précédées de "\$" signifient que vous devez exécuter la commande en tant qu'utilisateur général - et non en tant qu'utilisateur root.
- * Les commandes précédées de "#" signifient que vous devez travailler en tant qu'utilisateur root.
- * Les commandes comportant des lignes de commande plus spécifiques (par exemple "rtrX>" ou "mysql>") signifient que vous exécutez des commandes sur des équipements à distance, ou dans un autre programme.

Exercices

Exercices Partie I

=====

0. Ouvrez une session sur votre PC ou ouvrez une fenêtre de terminal

en tant qu'utilisateur sysadm.

1. Installez Nagios Version 3

```
$ sudo apt-get install nagios3 nagios3-doc
```

Il vous sera demandé de donner un mot de passe pour l'utilisateur "nagiosadmin". Donnez lui le mot de passe standard utilisé dans l'atelier.

Sauf si vous avez déjà un agent MTA installé, nagios3 va installer postfix en tant que dépendance. Sélectionnez l'option "Internet Site".

2. Regardez la configuration de base de Nagios

Ouvrez un navigateur et accédez à votre machine de la façon suivante :

<http://pcN.ws.nsrc.org/nagios3/>

À l'invite de connexion, répondez comme indiqué ci-dessous :

```
username: nagiosadmin
pass: <MOT DE PASSE DE LA CLASSE>
```

Cliquez sur le lien "Hosts" dans le menu à gauche pour voir ce qui est déjà configuré.

4. Ajout de Routeurs, PC et Commutateurs

Nous allons créer 3 fichiers:

```
routers.cfg switches.cfg pcs.cfg
```

... et créer des définitions pour le matériel qui se trouve dans notre atelier.

4a. Création du fichier switches.cfg

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

(pour être certains)

Dans ce fichier ajoutez une entrée pour cet élément :

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

Sauvez le fichier et quittez l'éditeur.

4b. Création du fichier routers.cfg

Nous avons au maximum 10 routeurs. Ceci sont rtr1-rtr9 et gw. Nous allons créer des définitions pour chacun d'entre eux.

Nous définissons ci-dessous les 4 premiers, à vous d'ajouter le

reste!

```
$ sudo editor routers.cfg
```

```
define host {  
    use          generic-host  
    host_name    gw  
    alias        Routeur de backbone  
    address      10.10.0.254  
}
```

```
define host {  
    use          generic-host  
    host_name    rtr1  
    alias        Routeur de groupe 1  
    address      10.10.1.254  
}
```

```
define host {  
    use          generic-host  
    host_name    rtr2  
    alias        Routeur de groupe 2  
    address      10.10.2.254  
}
```

Pas besoin d'ajouter tous les routeurs maintenant! Vous pouvez revenir plus tard et le faire...

On ajoute ici aussi les points d'accès sans fil:

```
define host {  
    use          generic-host  
    host_name    ap1  
    alias        Wireless Access Point 1  
    address      10.10.0.251  
}
```

```
define host {  
    # Pas toujours utilisé  
    use          generic-host  
    host_name    ap2  
    alias        Wireless Access Point 2  
    address      10.10.0.252  
}
```

Sauvez le fichier et quittez l'éditeur.

4c. Création du fichier pcs.cfg

Nous allons maintenant créer les définitions pour toutes les machines virtuelles (PC) dans notre atelier. Ci-dessous vous trouverez les quelques premières définitions. Vous devez compléter ce fichier comme vous l'avez fait ci-dessus pour les routeurs, et ajouter autant de PCs que vous le désirez.

Au minimum, nous vous demandons de créer les 4 PCs du groupe dont vous êtes le membre, et au moins 1 PC d'un autre groupe.

```
$ sudo editor pcs.cfg
```

```
define host {
    use          generic-host
    host_name    noc
    alias        Le NOC atelier
    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
}
```

Un PC d'un autre groupe (exemple! En choisir un autre!)

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

Vous pouvez sauver & quitter le fichier à ce stade, et continuer à ajouter d'autres PC pour les autres groupes.

**** LES ÉTAPES SUIVANTES DE 5a - 5c DOIVENT ÊTRE RÉPÉTÉES À CHAQUE MISE À ****

**** JOUR DE LA CONFIGURATION! ****

5a. Toujours vérifier que votre configuration est OK après l'avoir modifiée:


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

... vous devriez voir quelques avertissements (mais rien de critique) comme:

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 essaie de nous dire que c'est inhabituel de vouloir surveiller une machine pour laquelle on n'a pas configuré de service - c'est à dire autre chose que le ping.

5b. Recharger/redémarrer Nagios

```
$ sudo service nagios3 restart
```

ASTUCE : Vous allez devoir répéter cette opération à plusieurs reprises. Si vous regroupez l'ensemble sur une seule ligne, comme ci-dessous, alors vous pourrez utiliser la touche de déplacement vers le haut et relancer le tout en une seule fois :

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

Le '&&' garantit que le redémarrage ne se passe que si la configuration est valide.

5c. Vérification via l'interface web

Rendez-vous sur votre interface web (<http://pcN.ws.nsrc.org/nagios3/>) et vérifiez que les machines que vous avez ajoutées sont désormais visible via l'interface web.

Cliquer sur "Host Detail" dans le menu sur la gauche pour voir ceci. Vous verrez peut-être des machines en état "PENDING" (en cours) pendant que Nagios vérifie l'état des serveurs.

6. Visualisation des détails des machines et de la cartographie

Rendez-vous sur <http://pcN.ws.nsrc.org/nagios3/>

Cliquer sur "Host Detail" dans le menu sur la gauche. Est-ce que toutes les machines que vous avez définies sont listées ? Sont-elle "up" (en marche) ?

Cliquer sur "Status Map" dans le menu de gauche. Vous devriez y voir vos machines, avec le processus Nagios figurant au milieu.

Partie II - Configurer le contrôle des services du NOC de la classe

0. Configuration

Maintenant que notre matériel est configuré, nous pouvons commencer à indiquer à Nagios les services à surveiller sur le matériel configuré, comment regrouper le matériel de façon intéressante, comment regrouper les services, etc.

1. Affectez un contrôle de services au NOC de notre classe

```
# editor hostgroups_nagios2.cfg
```

- Trouver le groupe d'hôtes nommé "ssh-servers". Dans la section membres

de la définition, remplacez la ligne :

```
members                localhost
```

par

```
members                localhost,noc
```

Sauvegardez le fichier et quittez

Vérifiez que vos modifications sont correctes :

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

Redémarrez Nagios pour voir les nouveaux services associés à votre hôte :

```
$ sudo service nagios3 restart
```

Cliquez sur le lien "Services" dans l'interface web (menu de gauche) de Nagios.

Vous devriez pouvoir trouver votre nouveau service:

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

PARTIE III

Définition des services pour tous les PC

Note: Par défaut, l'intervalle de contrôle normal (normal_check_interval) des services est de 5 (minutes) dans `generic-service\_nagios2.cfg`.

Vous pouvez porter cette valeur à 1 pour accélérer la détection des problèmes de service, tout du moins dans l'atelier.

1. Déterminez les services à définir et les périphériques associés

- C'est le coeur même de l'utilisation de Nagios et des outils de surveillance réseau en général.

Jusqu'ici, nous avons simplement utilisé la commande ping pour vérifier que les hôtes physiques sont actifs sur notre réseau et nous avons commencé à surveiller un seul service sur un seul hôte (votre PC). La prochaine étape consiste à décider quels services vous souhaitez surveiller pour chacun des hôtes de la classe.

- Caractéristiques de cette classe particulière :

Routeurs : Service ssh et snmp

Commutateurs : Service telnet et éventuellement ssh ainsi que snmp

PC : Tous les PC offrent un service ssh et http et devraient

avoir un service SNMP maintenant
Le NOC offre aussi un service snmp

Nous allons donc configurer Nagios afin qu'il vérifie ces services sur ces périphériques.

2.) Vérifiez que SSH est exécuté sur les routeurs et les images des PC de l'atelier

- Dans le fichier services_nagios2.cfg, il existe déjà une entrée pour le contrôle des services SSH, vous n'avez donc pas besoin de créer cette étape. Au lieu de cela, il vous suffit de redéfinir l'entrée "ssh-servers" dans le fichier /etc/nagios3/conf.d/hostgroups_nagios2.cfg.

L'entrée initiale dans le fichier ressemblait à ceci :

```
# A list of your ssh-accessible servers
define hostgroup {
    hostgroup_name  ssh-servers
        alias      SSH servers
        members     localhost
    }
```

Que faut-il modifier à votre avis ?

Corriger la ligne "members". Vous devez créer des entrées pour tous les PC de la classe, les routeurs et les commutateurs exécutant ssh.

Avec ces informations et le schéma du réseau, vous devriez pouvoir finaliser cette entrée.

L'entrée devrait ressembler à ceci :

```
define hostgroup {
    hostgroup_name  ssh-servers
        alias      SSH servers
        members     localhost,pc1,pc2,...,ap1,noc,rtr1,rtr2,..,gw
    }
```

Remarque : conservez "localhost" - Cette entrée identifie votre PC et représente le point de vue réseau de Nagios. Ainsi, par exemple, si vous êtes sur le "pc3", vous ne devez pas inclure "pc3" dans la liste des PC de la classe, car il est représenté par l'entrée "localhost".

L'entrée "members" sera une longue ligne et bouclera probablement à l'écran.

Pensez à inclure l'ensemble des PC et routeurs que vous avez définis. N'incluez pas d'entrées si elles ne sont pas déjà définies dans pcs.cfg, switches.cfg ou routers.cfg - cela veut dire: si vous n'avez, par exemple, PAS créé de "pc8" dans pcs.cfg, alors n'allez pas ajouter "pc8" dans le hostgroup!

- Lorsque vous avez terminé, effectuez le contrôle avant démarrage :

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

et visualisez vos modifications dans l'interface web de Nagios.

Pour poursuivre avec les groupes d'hôtes, vous pouvez créer des

groupes supplémentaires pour une utilisation ultérieure, comme par

exemple tous nos serveurs virtuels. N'hésitez pas à modifier de

nouveau le fichier hostgroups_nagios2.cfg :

```
# editor hostgroups_nagios2.cfg
```

et ajoutez les lignes suivantes à la fin du fichier :

```
# Une liste de routeurs virtuels
define hostgroup {
    hostgroup_name cisco7200
    alias          Cisco 7200 Routers
    members
    rtr1,rtr2,rtr3,rtr4,rtr5,rtr6,rtr7,rtr8,rtr9
}
```

Ne mettre dans le groupe ci-dessus QUE les routeurs que vous avez définis dans routers.cfg.

Enregistrez et fermez le fichier. Vérifiez que tout est correct :

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

Si tout semble correct, alors redémarrez Nagios

```
$ sudo service nagios3 restart
```

3.) Vérifiez que http fonctionne sur tous les PC de la classe.

- Cette étape est presque identique à l'exercice précédent. Il vous suffit de modifier la création du service HTTP pour chaque

PC (pas de routeurs ou de commutateurs). Rappelez-vous que vous n'avez pas besoin d'ajouter votre machine car celle-ci est déjà définie en tant que "localhost".

Si vous avez des questions ou des problèmes de compréhension, demander de l'aide à un formateur.