

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 "RTR-GW>" ou "mysql>") signifient que vous exécutez des commandes sur des équipements à distance, ou dans un autre programme.

Exercices

Exercices 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 :

```
# nagios3 -v /etc/nagios3/nagios.cfg
```

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

```
# /etc/init.d/nagios3 restart
```

Cliquez sur "Service Detail" (Détails du service) dans l'interface web de Nagios pour voir votre nouvelle entrée.

PARTIE III

Définition des services pour tous les PC

0. 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,pc3,pc4...,pc32,...,ap1,ap2,noc,rtr1,rtr2,...,rtr9
,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 devriez 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.

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

```
# nagios3 -v /etc/nagios3/nagios.cfg
```

Si tout semble correct, redémarrez Nagios

```
# /etc/init.d/nagios3 stop  
# /etc/init.d/nagios3 start
```

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  
}
```

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

```
# nagios3 -v /etc/nagios3/nagios.cfg
```

Si tout semble correct, alors redémarrez Nagios

```
# /etc/init.d/nagios3 stop  
# /etc/init.d/nagios3 start
```

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".