TP7 - Mise en place d'un outil de supervision

Objectifs

- Installer un outil de supervision : Nagios
- Superviser des postes windows et linux

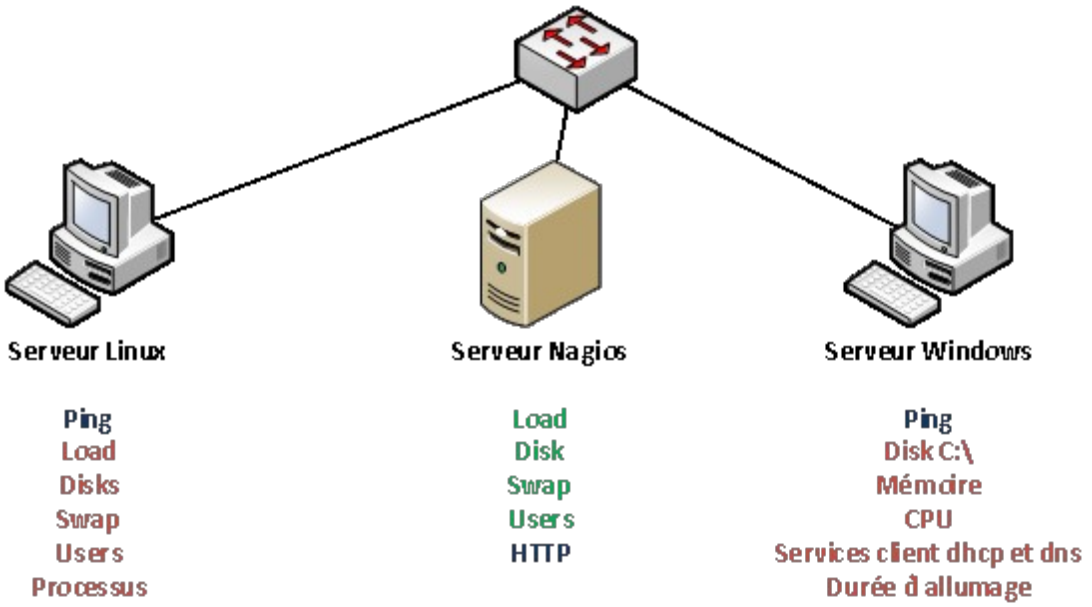
Documentation

- Documentation nagios [FR] : http://doc.monitoring-fr.org/
- Et celle d'ubuntu : http://doc.ubuntu-fr.org/nagios/

Présentation

Dans ce TP nous allons mettre en place et configurer une station de surveillance Nagios chargée d'avertir les administrateurs en cas de défaillance sur un des serveurs du réseau. Nous allons apprendre à configurer l'utilisation de différents plugins ainsi que certaines extensions de Nagios : NRPE et NSClient qui permettent de surveiller des machines distantes tournant sous Linux et Windows.

Schéma réseau avec les services à surveiller:



A chaque service correspond un plugin Nagios standard

En vert ce sont les services locaux, dans le sens qu'ils sont propres au serveur de supervision.
En bleu, ce sont les services réseaux, c'est-à-dire les services supervisables par une requête réseau (un ping, une requête http…) et ne nécessitant pas de droits particuliers sur les machines supervisées.
En rouge, ce sont les services nécessitant l'installation d'un programme (un agent) pour que Nagios puisse les superviser. En effet, il faut avoir des droits sur la machine pour pouvoir relever l'état de ces services.

Les machines seront réparties dans deux groupes :

- GrpLin : Groupe contenant les hôtes Linux
- GrpWin : Groupe contenant les hôtes Windows

Les administrateurs du réseau sont les suivants :

- linus : administrateur des machines linux
- bill : administrateur des machines windows
- 'vous' (votre compte) : administrateur général prévenu en cas de n'importe quelle panne sur le réseau

Les administrateurs de ce site sont répartis en deux groupes :

- AdminLin : ensemble des administrateurs de machines Linux
- AdminWin : ensemble des administrateurs de machines windows

Installation

- Installer le paquet nagios4
- Activer le mode cgi : a2enmod rewrite cgi
- Vous devez pouvoir accéder au site web sans authentification : http://IP/nagios4

Mise en place de l'authentification

Si on lit les commentaires notés dans le fichier /etc/apache2/conf-enabled/nagios4-cgi.conf, on peut voir que par défaut il n'y a pas d'authentification, nous allons remédier à cela.

- Activation de l'authentification MD5

  Nagios utilise par défaut l'authentification MD5, nous allons vérifier si les modules sont actifs avec la commande suivante :

  apachectl -M | grep -iE 'digest|group'

  S'ils sont actifs, vous devez voir ceci :

  auth_digest_module (shared)

  authz_groupfile_module (shared)

  S'ils ne sont pas actifs, activez-les avec la commande suivante :

  a2enmod auth_digest authz_groupfile

- Création du compte

  Pour configurer l'authentification Web de Nagios, vous devez créer un utilisateur Apache pour l'authentification. Le fichier d'authentification par défaut est /etc/nagios4/htdigest.users

  Voici la commande générique pour créer un utilisateur apache :

  htdigest [-c] passwdfile realm username (-c permet d'écraser l'ancien fichier)

  L'utilisateur 'nagiosadmin' est utilisé par défaut et est défini par défaut dans le fichier /etc/nagios4/cgi.cfg. Nous créons donc le compte 'nagiosadmin' avec pour mot de passe 'root'. Attention de bien saisir "Nagios4" en domaine (realm).

  htdigest -c /etc/nagios4/htdigest.users "Nagios4 " nagiosadmin

  Le fichier htdigest.users devrait contenir ceci :

  nagiosadmin:Accès restreint Nagios4:749ea1ba882261bd393a7b0399881459

  → Le 3ème élément est le hash md5 de 'root'

Remarque importante : Si nous souhaitons utiliser un autre compte que nagiosadmin, il faudrait remplacer toutes les occurrences de 'nagiosadmin' par le nom d'utilisateur choisi dans le fichier /etc/nagios4/cgi.bin. Ceci serait une bonne pratique en terme de sécurisation, en effet, une attaque par brut force qui utiliserait le compte par défaut (nagiosadmin) ne pourrait pas aboutir.

Par exemple, si vous voulez utiliser le compte 'admin' plutôt que 'nagiosadmin', vous pouvez utiliser la commande suivante pour remplacer toutes les occurrences de 'nagiosadmin' par 'admin' dans le fichier cgi.cfg :

```
sed -i 's/nagiosadmin/admin/g' /etc/nagios4/cgi.cfg
```

- Prise en compte de l'authentification

Modifier le fichier /etc/apache2/conf-enabled/nagios4-cgi.conf :

```
<Files "*.cgi">
   AuthDigestDomain "Nagios4"
   AuthDigestProvider file
   AuthUserFile    "/etc/nagios4/htdigest.users"
   AuthGroupFile   "/etc/group"
   AuthName        "Nagios4"
   AuthType        Digest
   #Require all     granted
   Require valid-user
</Files>
```

Modifier le fichier /etc/nagios4/cgi.cfg afin d'activer l'authentification : use_authentication=**1**

Puis redémarrer apache2 et vérifiez que l'authentification fonctionne maintenant : http://IP/nagios4

Changement des fichiers des objets bases

Les différents fichiers d'exemple fournis par nagios sont plutôt mal organisés, nous allons donc les supprimer et les remplacer par ceux fourni dans un fork de nagios (icinga1).

- Faire une sauvegarde du dossier /etc/nagios4/ (cp /etc/nagios4 /root -R)
- Se positionner dans le dossier /etc/nagios4/objects.
- Supprimer l'ensemble des fichiers de ce dossier **sauf le fichier commands.cfg !!!**
- Télécharger le fichier icinga_objects.zip présent ici http://192.168.1.19/nagios
- Installer le paquet unzip
- Déziper le contenu du fichier zip : unzip icinga_objects.zip

Dans sa configuration de base nagios4 nécessite de préciser chaque fichier de configuration d'objet à utiliser, pour faire plus simple et pour éviter de devoir modifier à plusieurs reprises le fichier 'nagios.cfg' nous allons inclure l'ensemble des fichiers du dossier objects :

- Commenter les lignes suivantes dans le fichier /etc/nagios4/nagios.cfg et ajouter la ligne cfg_dir :

```
#cfg_file=/etc/nagios4/objects/commands.cfg
#cfg_file=/etc/nagios4/objects/contacts.cfg
#cfg_file=/etc/nagios4/objects/timeperiods.cfg
#cfg_file=/etc/nagios4/objects/templates.cfg
#cfg_file=/etc/nagios4/objects/localhost.cfg
cfg_dir=/etc/nagios4/objects
```

Pour le TP vous utiliserez ce dossier (/etc/nagios4/objetcs) pour créer vos fichiers de configuration.

- Vérifier que la configuration de nagios est correcte :
  nagios4 -v /etc/nagios4/nagios.cfg

  Vous devez avoir ceci : Total Warnings: 0
  Total Errors: 0

- Redémarrer le service nagios4

Observations de l'interface de nagios

- Afficher l'interface web de Nagios (http://IP/nagios4). Et regarder les différents menus.
- Combien de machines sont supervisées ? une seul lui-même
- Combien y'a-t-il de groupes de machines ? Listez-les. il y a 4 group (all, linux-server, http server, ssh servers)
- Quels éléments sont supervisés pour chaque hôte ? Quels sont leurs états ?(current load ok, current users ok, disk space ok, http ok , ssh ok, total processes ok)
- Dans combien de temps le service web de votre serveur Nagios sera-t-il à nouveau supervisé ?
  Entre 4 et 5 minute
- Aller dans la rubrique 'System>Configuration' ; vous voyez que plusieurs objets ont été configurés ; regardez plus particulièrement les hôtes, les services et les commandes. Pouvez-vous modifier la configuration depuis l'interface web ?
  Non on ne peut pas modifier la configuration depuis l'interface web

Observations des fichiers

Notez les noms des fichiers de configuration présents dans /etc/nagios4 et /etc/nagios4/objects. Faites des recherches pour connaître l'utilité de ces différents fichiers de configuration.

Observez le fichier /etc/nagios4/objects/contacts.cfg :

- Qu'est-ce que signifie '24*7'? A quel fichier fait-il référence ?
- A quoi correspondent les lettres w,u,c,r,d? Que signifient-elles ?

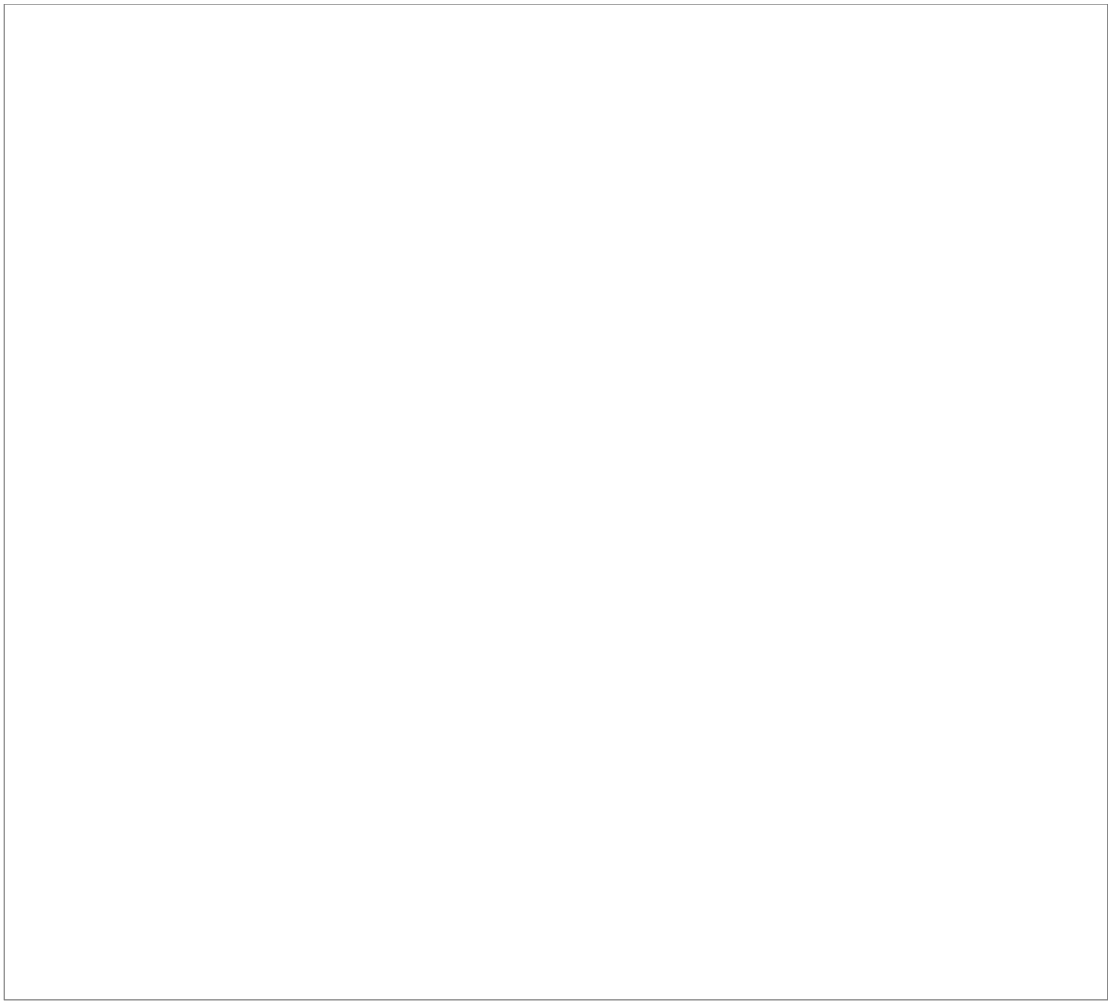
Qu'est ce qu'un template ? Combien y'en a-t-il de définis par défaut ?

En observant le fichier /etc/nagios4/objects/generic-service.cfg, dites combien de temps s'écoule entre 2 vérifications de l'état d'un service ? (Reproduire la ligne correspondant). En cas d'échec de cette vérification, que va-t-il se passer ?

Dans quel répertoire sont stockés les plugins de nagios ? Quelle variable utilise nagios pour faire référence à ce répertoire ?

Dans quel répertoire sont stockées les commandes de base de nagios?

Les relations entre les différents objets



http://www.smartmon.com.au/docs/tiki-index.php%3Fpage=Nagios+Objects.html

Configuration du serveur Nagios

A – Création de la structure des objets (sauf les services et les commandes)

Dans cette partie vous allez configurer votre serveur Nagios afin de créer la structure de base des objets présentés précédemment dans la partie 'Présentation'.

Afin de vérifier que vos fichiers de configuration sont corrects, n'hésitez pas à utiliser cette commande :

```
nagios4 -v /etc/nagios4/nagios.cfg
```

B- Configuration des services locaux et réseaux

Vous allez donc créer des services, qui utilisent des commandes.

Ces commandes peuvent être des commandes existantes, ou des commandes que vous allez créer.

Ces commandes utilisent des plugins.

Vous suivez ;-)

Commencez par créer les services locaux (sur le serveur Nagios), et les services réseaux (ex : ping). (le reste sera traité plus loin)

Démarche conseillée :

1- Regarder d'abord si vous trouvez une commande existante qui correspond à votre besoin. Sinon vous devrez trouver le plugin adéquat et créer la commande qui l'utilise.

2- Pour comprendre le fonctionnement de la commande et notamment les arguments, regardez l'aide du plugin qu'elle utilise. Après vous être positionné dans le répertoire des plugins faites :

./« nom du plugin » -h

3- Vous pouvez tester le plugin avec les paramètres souhaités, ainsi vous serez plus à l'aise pour trouver/créer la commande qui correspond à ce que vous voulez.

./« nom du plugin » avec éventuellement des paramètres adéquats

4- N'oubliez pas de créer ensuite le service et de vérifier qu'il fonctionne depuis l'interface web.

5- Vérifier que les mails sont bien arrivés dans les bonnes boites.

C- Configuration des services pour le client windows

1- Pour pouvoir surveiller les services disponibles sur le client windows, vous allez devoir installer le serveur NSClient sur la machine windows, ainsi que le plugin check_nt, disponible avec NSClient, afin d'interroger le serveur.

2- Quelle commande permet de vérifier la version de NSClient sur le serveur windows ? Testez-la.

3- Vous pourrez ensuite créer les services pour la machine windows. N'hésitez pas à regarder l'aide du plugin check_nt.

D-Configuration des services pour le client linux

1- Nous allons maintenant surveiller les services disponibles sur le client linux. Pour cela, vous devrez installer sur cette machine le serveur NRPE, et les plugins nrpe sur votre serveur Nagios.

4- Quelle commande permet de vérifier que le serveur NRPE fonctionne ? Testez-la.

```
root@debian:/usr/lib/nagios/plugins# ./check_nrpe -H 192.168.119.2
NRPE v4.0.3
```

5- Vous pourrez ensuite créer les services pour la machine linux. N'hésitez pas à regarder l'aide du plugin check_nrpe.

E-Vous avez fini…

- Essayer d'utiliser NRPE avec windows. (ex : créer une commande qui permet de surveiller l'ensemble des disques durs, créer une commande qui surveille la durée d'allumage du pc et envoie une alerte s'il a rebooté il y a moins d'une heure ou moins d'un jour)
- Essayer de chercher comment utiliser la commande check_by_ssh