Un exemple de plateforme de supervision : NAGIOS 3

1 Introduction

Les TPs précédents nous ont permis d'appréhender différentes techniques pour interroger des machines distantes, et savoir si elles fonctionnent correctement.

Dans ce TP, nous allons configurer une plateforme de supervision, qui permet de surveiller l'ensemble d'un parc : NAGIOS version 3. L'objectif est d'arriver à superviser un parc de 4 machines : votre serveur Nagios (machine viruelle Ubuntu), un serveur Windows (machine virtuelle XP), et deux matériels actifs (le switch de la salle de TP et le routeur de l'iut).

NAGIOS permet de vérifier la présence de machines sur le réseau (HÔTES), et la présence de services réseaux sur ces machines (SERVICES). Par défaut, pratiquement rien n'est configuré. Nous allons voir comment paramétrer le logiciel pour superviser un réseau.

2 Installation de NAGIOS 3 sous Ubuntu

Créez une machine virtuelle Ubuntu qui vous servira de serveur Nagios.

Nagios permet de visualiser l'état du réseau par pages Web. Normalement, l'installation de nagios3 devrait automatiquement provoquer l'installation d'Apache 2, il n'y a donc rien à faire au niveau du serveur Web.

Installez le paquetage « nagios3 »

Lors de la configuration des paquetages, le système vous demande de donner le mot de passe de l'utilisateur nagiosadmin, créé pour accéder aux pages Web gérées par le logiciel . Choisissez tprzo.40 comme mot de passe.

Verifiez qu'apache2 a bien été installé (http://127.0.0.1). Si ce n'est pas le cas, installez le paquetage « apache2 ». Puis ouvrez le fichier de configuration d'apache2 (/etc/apache2/apache2.conf) et rajoutez à la fin du fichier la ligne suivante :

include /etc/nagios3/apache2.conf

Connectez-vous ensuite sous nagios pour vérifier l'authentification de l'utilisateur nagiosadmin (http://127.0.0.1/nagios3)

Les pages de Nagios sont découpées en 2 parties : un menu sur la gauche, et une page centrale. Le menu de gauche vous permet de visualiser la documentation (très utile !). Il vous permet aussi de visualiser l'état de vos différentes machines (Hosts et Services).

Quelles ont les HOSTS définis par défaut ? Quels services sont supervisés sur ces machines ?

3 Configuration de Nagios 3

Nous allons maintenant modifier la configuration par défaut pour pouvoir superviser quatre machines particulières : un serveur Ubuntu (le serveur Nagios), une machine XP, le switch de la salle de TP, et le routeur de l'IUT.

Créez une machine virtuelle XP

Pour la suite du TP, un minimum d'information vous sera donné sur les configuration des fichiers de nagios. Vous trouverez les détails utiles soit dans la documentation de nagios, soit sur le site Web http://doc.ubuntu-fr.org/nagios (en français !)

3.1 Périodes de temps

Les « périodes de temps » permettent de définir des zones de temps dans la semaine. Les actions de supervision pourront être différentes en fonction de la période de temps dans laquelle on se trouve.

Les périodes de temps sont définies dans le fichier /etc/nagios3/conf.d/timeperiods_nagios2.cfg

Quelles sont les périodes de temps définies par défaut ?

3.2 Les contacts

Les « contacts » sont les administrateurs réseau qui peuvent être avertis (notifiés) par Nagios des problèmes du réseau. La liste des contacts est donnée dans le fichier /etc/nagios3/conf.d/contacts_nagios2.cfg.

Créez un contact appelé « admin » qui pourra être notifié pour les hôtes et les services, 24h sur 24. Tous les types de notification (hôtes / services) seront notifiés. Les notifications se feront par mail (utilisez votre propre adresse email).

3.3 Les hôtes

Nagios permet de superviser des HOSTS (des machines), et des SERVICES (les services sur chaque machine). La déclaration de ces HOSTS se fait dans des fichiers situés dans le répertoire /etc/nagios3/conf.d/. On peut déclarer tous les hôtes dans un seul fichier, où un hôte par fichier différent.

Quels sont les HOSTS prédéfinis dans Nagios ? Quels sont les fichiers dans lesquels sont définis ces hôtes et les services associés ? Rajoutez les HOSTS « switch », « routeur » et « xp », en vous basant sur le modèle localhost_nagios2.cfg (créez pour cela deux nouveaux fichiers .cfg dans /etc/nagios3/conf.d). Relancez Nagios, puis vérifiez vos définitions d'hôtes sur l'interface Web.

Les groupes d'hôtes permettent de regrouper les hôtes par type de supervision. Par exemple, on peut regrouper les serveurs entre eux, le matériel actif dans un autre groupe, ...

Créez deux groupes d'hôtes, un premier appelé « machines », qui regroupe votre serveur et la machine XP, et un second appelé « actifs », qui regroupe le routeur et le switch (fichier /etc/nagios3/conf.d/hostgroups_nagios2.cfg) Mettez en commentaires tous les autre groupes d'hôtes prédéfinis, sauf le groupe All. Attention, ces groupes sont référencés dans d'autres fichiers de config. Dès que vous allez relancer Nagios, des

messages d'erreurs apparaîtront. Il faudra que vous commentiez les actions faisant référence aux groupes supprimés, pour que Nagios puisse se lancer correctement.

Relancez Nagios, et vérifier que vous n'avez plus que 3 groupes d'hôtes.

3.4 Les services

3.4.1 généralités

Pour chaque hôte superviser, on peut définir des SERVICES qui seront vérifiés sur cet hôte. Bien entendu, les services varient d'un hôte à l'autre.

La définition des services de chaque hôte se fait dans les mêmes fichiers que pour la définitions des hôtes. Par convention, on définira un hôte et ces services dans un même fichier .cfg. Il y aura donc autant de fichiers .cfg que d'hôtes supervisés.

Quels sont les services prédéfinis pour l'hôte « localhost » ?

Chaque service fait appel à une commande « check_xxx » qui permet de tester ce service sur l'hôte. Ces commandes sont appelés « plugins » chez Nagios. Ces plugins sont situés dans le répertoire /usr/lib/nagios/plugins. La configuration (si nécessaire) de ces plugins se fait dans les fichiers de configuration du répertoire /etc/nagios-plugins/config/

Par exemple, le plugin check_telnet est configuré dans le fichier check_telnet.cfg. Il fait appel au plugin check_tcp, est permet de tester une ouverture de conexion sur le port 23. Si cette ouverture de connexion réussi, c'est que le serveur telnet est en fonctionnement.

Tous ces plugins sont en fait des scripts (souvent shell, ou perl, ...) qui utilisent des commandes réseau classiques (rsh, ssh, ...) pour réaliser le test des services. Il est donc tout à fait possible de créer ses propres plugins (d'écrire ses propres scripts). C'est ce qui fait que de multiples plugins peuvent être trouvés sur Internet, et rajoutés à Nagios. Dans le cadre de ce TP, nous n'utiliserons que des plugins de base, pré-installés avec Nagios.

Installez les plugins supplémentaires dans nagios : paquetage nagios-plugins

Une aide en ligne des différents plugins de base peut être trouvée dans http://www.nagiosplugins.org/man

Rajoutez les services check_ping et check_telnet pour les hôtes « gateway » et « switch ». Pour la configuration de check_ping, basez-vous sur l'exemple dans le fichier de configuration services_nagios2.cfg (les explications des paramètres peuvent être trouvées dans http://doc.ubuntu-fr.org/nagios).

Relancez Nagios et vérifiez que les services Ping et Telnet fonctionnent correctement sur ces deux machines.

NB : pour éviter d'attendre trop longtemps les « check » de Nagios, vous pouvez modifier la définition du modèle generic-service pour passer la période de check de 5 minutes à 1 minute.

3.4.2 Cartographie

A partir des informations que vous avez saisi, Nagios est capable de générer une cartographie du réseau afin de visualiser d'un seul coup d'oeil l'état de vos machines.

Cliquez sur la carte 2D de Nagios, et essayez de comprendre toutes les options disponibles.

3.4.3 Supervision d'une machine Windows

Les machines sous OS Windows ne sont pas aussi facilement interrogeables à distances que les machines Linux. Certaines informations restent faciles à récupérer (comme, par exemple, si un service est présent ou non), mais d'autres non. Aussi, il est nécessaire d'installer sur ces machines un client spécifique, qui fera le lien entre la machine et le serveur Nagios. Aisni on pourra obtenir les mêmes informations que pour une machine Linux.

Dans ce TP, nous utiliserons le client Nsclient++.

Cherchez sur Internet et installez le client NSClient++ (NSClient++-0.3.5-RC7-x64.msi) sur votre machine XP.

Modifiez le fichier NSC.ini (c:\Program Files\NSClient) pour que le client NSClient accepte les communication depuis toutes les machines, sans demander de mot de passe. Activez tous les modules .dll sauf CheckWMI. Dans la partie [NSClient], précisez 102,18,0/24 Redémarrez NSClient (Panneau de configuration – Outils d'administration – Services), en ayant au préalable autorisé le service à interagir avec le bureau (onglet Connexion des propriétés de NSClient)

Une fois le client NS configuré sur la machine XP, il faut tester si le serveur Nagios peut le contacter et récupérer des infos. Vous devrez utiliser le plugin check_nt.

Depuis votre serveur Nagios, dans un terminal, tapez la commande :

/usr/lib/nagios/plugins/check_nt -H @IP-machine-XP -v UPTIME -p 12489

Si vous avez une réponse, c'est que votre client fonctionne bien. Sinon, pensez à vérifier que le firewall Windows ne vous joue pas des tours ;-)

A partir du contenu de la page http://blog.nicolargo.com/2007/10/surveiller-vos-serveurs-windows-avec-nagios.html, définissez trois services pour votre machine XP : l'affichage de l'utilisation de la mémoire, l'affichage de l'utilisation du disque, et le taux d'utilisation moyen de la CPU par minute.

Redémarrez Nagios, et vérifiez que les trois services fonctionnent correctement

3.4.4 Utilisation de snmp sous Nagios

Nagios autorise l'utilisation de snmp dans ces services. Le plugin check_snmp permet de faire des requêtes snmp auprès des matériels du réseau.

A partir de l'aide du plugin check_snmp, rajoutez un service sur l'hôte gateway permettant de savoir l'état de l'interface Gigabit Ethernet 0/0 (variable IfAdminStatus). Rajoutez un service identique sur l'hôte switch permettant de voir l'état de l'interface allant vers le réseau de l'IUT.

Redémarrez Nagios, et vérifiez le bon fonctionnement.

RQ : il existe un plugin check_logfiles (ou check_log) qui permet de scruter des fichiers de logs à la recherche de mots clé (critical, warning, …). On peut donc coupler Nagios à Syslog par ce biai.