Nouvelle édition

Nagios

La clé de la supervision informatique

informatique technique

Fichiers complémentaires à télécharger

Collection EPSILON

Anis MAJDOUB

Table des matières

Les éléments à télécharger sont disponibles à l'adresse suivante :
http://www.editions-eni.fr
Saisissez la référence de l'ouvrage **EP4NAG** dans la zone de recherche et validez. Cliquez sur le titre du livre puis sur le bouton de téléchargement.

Chapitre 3
Découverte et utilisation de l'interface web

Chapitre 4
Aperçu sur les plugins Nagios

Chapitre 5
Supervision à distance

Chapitre 8
Gestion des notifications et des événements

Chapitre 9
Amélioration de Nagios

Chapitre 5
Supervision à distance

1. Les méthodes de supervision à distance

Nagios a plusieurs manières pour superviser les hôtes, les ressources et les services qu'ils proposent. Tout dépend de l'architecture de la plateforme de supervision à implémenter.

Deux modes de contrôle sont utilisés par Nagios pour superviser les machines : mode passif et mode actif.

Avec le mode passif, l'hôte doit fournir et envoyer l'information à Nagios en cas d'un évènement particulier.

Par contre avec le mode actif, Nagios a l'initiative d'interroger la machine pour avoir l'information. Dans ce cas, Nagios doit exécuter le plugin pour communiquer avec la machine. Il y a deux manières d'exécution :

– La première consiste à exécuter les plugins localement dans le serveur de supervision de Nagios.
– La deuxième consiste à exécuter les plugins à distance dans la machine cible.

Le principe de la supervision à distance est semblable à la supervision locale. En fait, des agents SSH (*Secure Shell*) ou NRPE (*Nagios Remote Plugin Executor*) vont être installés et utilisés pour lancer les plugins dans la machine distante et renvoyer les résultats au serveur Nagios.

L'intérêt d'utiliser la supervision à distance est de contrôler des ressources particulières dans la machine distante. Parmi les exemples typiques, il y a la supervision de l'état d'un service donné, le contrôle de la mise à jour du système et le contrôle de l'espace disque ou de la mémoire utilisée. Les informations (l'état d'un service donné ou la mise à jour du système, etc.) ne peuvent être contrôlées qu'après l'exécution d'une commande dans la machine supervisée.

Dans ce chapitre, nous allons étudier le fonctionnement de ces agents, connaître les étapes de leurs installations et leurs utilisations avec Nagios.

2. Supervision avec NRPE

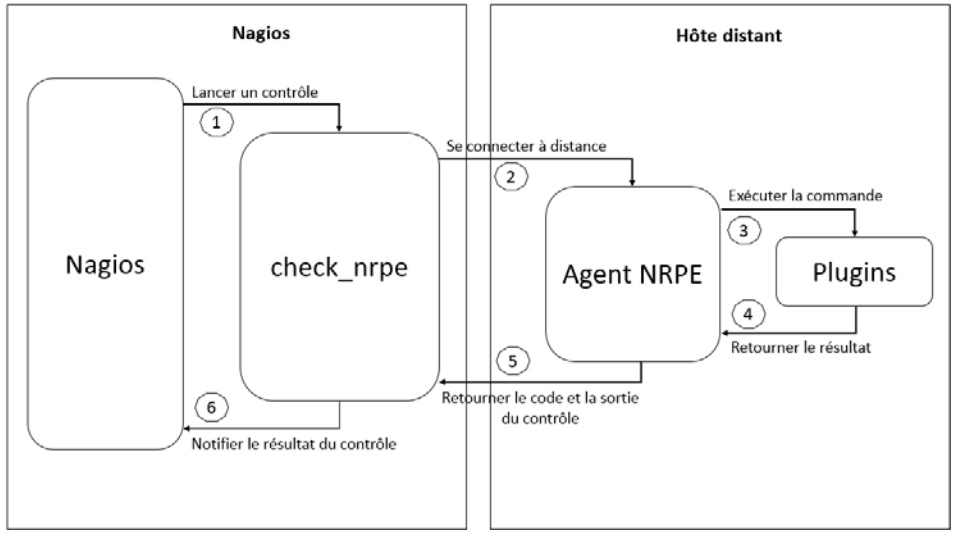
2.1 Principe de fonctionnement

NRPE est l'agent le plus utilisé pour superviser les serveurs Linux mais il peut être utilisé aussi avec les machines Windows. Son principe de fonctionnement ressemble beaucoup à Nagios. Il permet d'exécuter les plugins localement dans la machine distante et de renvoyer le résultat à Nagios.

Nagios fait appel à NRPE en utilisant le plugin `check_nrpe` pour lancer la commande et exécuter le plugin. À la fin de l'exécution de la commande, NRPE renvoie les informations à `check_nrpe`. Ces informations correspondent à un code de résultat (0= OK, 1=WARRING, 2=CRITICAL et 3=UNKNOWN) et d'autres informations utiles comme les données de performance.

La communication entre Nagios et le daemon NRPE se fait par le flux SSL et par défaut NRPE utilise le port TCP 5666 pour assurer cette communication.

L'intérêt d'utiliser NRPE par rapport à SSH est de minimiser l'utilisation des ressources sur l'hôte distante et sur le serveur Nagios. Par contre NRPE est moins sécurisé que SSH puisqu'il utilise un mécanisme d'authentification auprès de l'hôte basé sur l'adresse IP ou la plage d'adresses IP du demandeur. Le diagramme suivant résume ce principe de fonctionnement.



2.2 Installation et configuration

2.2.1 Installation

Après avoir compris le principe de fonctionnement de NRPE, il est temps de passer à l'installation sur l'hôte. Nous allons exécuter cette installation dans une machine Linux Ubuntu et une machine Linux CentOS.

Comme Nagios, NRPE qui est développé et maintenu par l'équipe de Nagios, peut être installé avec deux méthodes :

– La première méthode est d'installer NRPE en utilisant les gestionnaires de paquetages apt-get pour Ubuntu ou yum pour CentOS.
– La deuxième consiste à télécharger et compiler le fichier source disponible sur le site web Nagios :
https://www.nagios.org/downloads/nagios-core-addons/

Il est recommandé d'installer NRPE en utilisant le gestionnaire des paquets apt-get ou yum pour faciliter ensuite la configuration, l'exploitation et la mise à jour.

Dans une machine Linux Ubuntu, les paquets qui sont nécessaires pour installer NRPE s'appellent nagios-nrpe-server et nagios-nrpe-plugin. La commande pour les installer est la suivante :

```
apt-get install nagios-nrpe-server nagios-nrpe-plugin
```

Pour une machine Linux CentOS, les deux paquets s'appellent nagios-nrpe et nagios-plugins-nrpe et ils s'installent avec cette commande :

```
yum install nagios-nrpe nagios-plugins-nrpe
```

Nous allons maintenant employer la deuxième méthode pour l'installation qui utilise la compilation des sources.

Avant de commencer l'installation, il y a des prérequis à faire et des paquets à installer comme le compilateur GCC (*GNU C Compiler*).

Dans une machine Linux Ubuntu, ces prérequis peuvent être installés par cette commande :

```
apt-get install gcc make binutils cpp pkg-config libc6-dev libssl-dev openssl
```

Pour un système CentOS, la commande pour installer les prérequis est la suivante :

```
yum install --y mod_ssl openssl--devel xinetd gcc make gcc
glibc glibc-common gd gd-devel
```

Pour des raisons de sécurité, il faut créer un utilisateur et un groupe nagios pour lancer NRPE comme il est déjà fait lors de l'installation de Nagios dans le chapitre Installation et configuration.

```
groupadd        nagios
useradd -r -g nagios nagios
```

L'étape suivante consiste à télécharger et décompresser le fichier source fourni par l'équipe de Nagios dans le répertoire tmp.

```
cd /tmp
wget http://sourceforge.net/projects/nagios/files/nrpe-2.x/
nrpe-2.15/ nrpe-2.15.tar.gz
```

Voilà nous avons maintenant les paquets prêts pour la compilation, l'étape suivante consiste à exécuter le script *configure* pour installer NRPE.

```
./configure ---with--ssl=/usr/bin/openssl ----with--ssl--lib=/
usr/lib --enable-command-args
```

Suite à cette commande, un résumé de la configuration va s'afficher :

```
*** Configuration summary for nrpe 2.15 03-10-2008 ***:
 General Options:
 -------------------------
 NRPE port:            5666
 NRPE user:            nagios
 NRPE group:           nagios
 Nagios user:          nagios
 Nagios group:         nagios
```

La dernière étape de cette installation consiste à compiler et installer NRPE avec les deux commandes :

```
make
make install
```

L'installation de NRPE ne suffit pas pour contrôler la machine. Il nous manque les plugins pour être exécutés par NRPE. Pour les installer, il suffit de lancer la commande suivante :

```
make install-plugin
```

Si le processus de compilation échoue, il est très probable que ce soit en raison des prérequis manquants. Dans ce cas, installez les packages mentionnés ci-dessus.

En supposant que l'installation par compilation réussit, la prochaine étape est de configurer NRPE pour communiquer avec le serveur Nagios.

2.2.2 Configuration de NRPE

Après avoir installé NRPE dans la machine distante, nous devons faire la configuration nécessaire et la mise en place du système NRPE afin qu'il accepte les requêtes à partir du serveur central où est installé Nagios.

Si vous avez fait l'installation par le gestionnaire de paquets `apt` ou `yum` selon la distribution utilisée, vous devez trouver le fichier de configuration nrpe.cfg sous le répertoire /etc/nagios.

Si votre installation est faite par compilation du fichier source, il faut créer le fichier de configuration nrpe.cfg dans le répertoire /usr/local/nagios/etc/ à partir de l'exemple fourni par le fichier source.

```
cd /tmp/nrpe-15
cp sample-config/nrpe.cfg /usr/local/nagios/etc/
```

Le fichier principal de NRPE nrpe.cfg contient plusieurs paramètres, il est nécessaire de les comprendre pour bien configurer l'agent de supervision.

Voici la liste des paramètres qui peuvent être utilisés :

– `server_port` : c'est le port TCP utilisé pour la communication entre Nagios et l'agent NRPE. Par défaut, sa valeur vaut 5666. Il faut s'assurer qu'il n'y a aucun firewall dans la machine distante ou dans le réseau qui bloque ce port.

– `server_address` : dans le cas où la machine distante contient plus d'une seule interface réseau, vous pouvez choisir l'interface à travers une adresse IP où NRPE écoute les requêtes de Nagios. Si non spécifiée, le démon écoute sur toutes les interfaces disponibles.

– `allowed_hosts` : généralement ce paramètre contient l'adresse IP du serveur Nagios. Comme nous avons parlé dans la première partie de ce chapitre que NRPE utilise un mécanisme de sécurité basé sur l'adressage IP pour accepter la requête de la part des serveurs. Le paramètre `allowed_hosts` peut contenir plusieurs adresses IP et aussi des plages sous réseaux.

– `dont_blame_nrpe` : cette option détermine s'il est autorisé ou pas de passer des arguments dans la commande. Par défaut le passage des arguments est désactivé et le paramètre `dont_blame_nrpe` a comme valeur 0. Il faut changer cette valeur à 1 pour autoriser les arguments.