

Nouvelle édition

# Nagios

La clé de la supervision  
informatique



Informatique technique

Fichiers complémentaires  
à télécharger



  
Collection

epsilon

Anis MAJDOUB

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.

## Avant-propos

- 1. Objectifs .....9
- 2. Public visé .....10
- 3. Remerciements .....10

## Chapitre 1

### La supervision informatique

- 1. Le référentiel ITIL .....13
- 2. La mise en place d'une solution de supervision .....15
  - 2.1 L'intérêt de la supervision .....19
  - 2.2 Les critères de choix d'un outil de supervision .....20
  - 2.3 Les étapes de déroulement d'un projet de supervision .....23
- 3. Introduction à Nagios .....24
  - 3.1 Principe de fonctionnement et fonctionnalités de Nagios .....25
  - 3.2 Les atouts de Nagios .....27
  - 3.3 Les nouveautés de Nagios Core 4 .....28

## Chapitre 2

### Installation et configuration

- 1. Installation de Nagios 4 .....31
  - 1.1 Installation des prérequis .....32
  - 1.2 Compilation et installation .....34
  - 1.3 Installation et compilation des plugins .....36
  - 1.4 Lancement de Nagios .....38

1.5	Mise à jour de Nagios depuis les versions précédentes. . . . .	41
2.	Configuration de Nagios 4. . . . .	43
2.1	Arborescence des fichiers de configuration. . . . .	43
2.2	Configuration des hôtes. . . . .	49
2.3	Configuration des groupes d'hôtes . . . . .	52
2.4	Configuration des services . . . . .	53
2.5	Configuration des groupes de services . . . . .	57
2.6	Configuration des contacts . . . . .	58
2.7	Configuration des groupes de contacts. . . . .	60
2.8	Configuration des commandes et des macros . . . . .	61
2.9	Configuration des périodes de temps . . . . .	64
2.10	Modèle et héritage . . . . .	65
2.11	Vérification de la configuration. . . . .	70

### **Chapitre 3**

#### **Découverte et utilisation de l'interface web**

1.	Mise en place de l'interface web . . . . .	73
1.1	Configuration du serveur web. . . . .	74
1.2	Accès à l'interface web. . . . .	76
2.	Découverte de l'interface web . . . . .	78
2.1	Menu General . . . . .	79
2.2	Menu Current Status. . . . .	80
2.2.1	Vue globale tactique. . . . .	80
2.2.2	La carte d'état . . . . .	82
2.2.3	Détails des hôtes. . . . .	84
2.2.4	Détails des services . . . . .	87
2.2.5	Détails des groupes des hôtes . . . . .	89
2.2.6	Détails des groupes des services. . . . .	91
2.2.7	Problèmes . . . . .	93

- 2.3 Menu Reports . . . . . 93
  - 2.3.1 Rapport de disponibilité. . . . . 93
  - 2.3.2 Rapport de tendance . . . . . 95
  - 2.3.3 Rapport d'alerte . . . . . 96
  - 2.3.4 Rapport des notifications. . . . . 98
  - 2.3.5 Rapport des évènements . . . . . 98
- 2.4 Menu System . . . . . 99
  - 2.4.1 Gestion des commentaires. . . . . 99
  - 2.4.2 Gestion des temps d'arrêt . . . . . 101
  - 2.4.3 Détails du processus . . . . . 102
  - 2.4.4 Données de performance . . . . . 104
  - 2.4.5 Ordonnancement de la file d'attente. . . . . 105
  - 2.4.6 La configuration . . . . . 106
- 3. Amélioration de l'interface web . . . . . 106
  - 3.1 Le thème Vautour. . . . . 107
  - 3.2 Nagios V-Shell. . . . . 108

**Chapitre 4**  
**Aperçu sur les plugins Nagios**

- 1. Principe de fonctionnement du contrôle. . . . . 113
- 2. Supervision basique d'un hôte. . . . . 114
- 3. Supervision des services réseau . . . . . 118
  - 3.1 Contrôle d'un port réseau . . . . . 118
  - 3.2 Contrôle d'un serveur DNS . . . . . 121
  - 3.3 Contrôle d'un serveur SSH . . . . . 125
  - 3.4 Contrôle d'un serveur NTP . . . . . 126
  - 3.5 Contrôle d'un serveur FTP. . . . . 128
  - 3.6 Contrôle d'un serveur DHCP. . . . . 129
  - 3.7 Contrôle d'un serveur HTTP et HTTPS . . . . . 131

4.	Supervision d'un serveur de messagerie	134
4.1	Contrôle d'un serveur SMTP	135
4.2	Contrôle d'un serveur POP	137
4.3	Contrôle d'un serveur IMAP	138
4.4	Contrôle de la messagerie de bout en bout	140
5.	Supervision des bases de données	141
5.1	Contrôle d'un serveur MySQL	141
5.2	Contrôle d'un serveur PostgreSQL	144
5.3	Contrôle d'un serveur Oracle	145
6.	Supervision des ressources système	147
6.1	Contrôle de la charge du système	147
6.2	Contrôle des processus	149
6.3	Contrôle de l'espace disque	151
6.4	Contrôle de l'espace swap	153
6.5	Contrôle des utilisateurs connectés	155
7.	Autres plugins	155
7.1	Contrôle de la mise à jour du système	155
7.2	Contrôle avec le plugin dummy	158

## Chapitre 5

### Supervision à distance

1.	Les méthodes de supervision à distance	159
2.	Supervision avec NRPE	160
2.1	Principe de fonctionnement	160
2.2	Installation et configuration	161
2.2.1	Installation	161
2.2.2	Configuration de NRPE	163
2.2.3	Démarrage de l'agent	167
2.3	Contrôle à distance avec NRPE	169
2.3.1	Configuration Nagios pour NRPE	169
2.3.2	Contrôler un serveur Linux avec NRPE	171

- 2.4 Diagnostic et solutions pour les problèmes du contrôle avec NRPE..... 174
- 3. Supervision avec SSH..... 177
  - 3.1 Le principe de fonctionnement ..... 177
  - 3.2 Configuration de la connexion SSH ..... 178
  - 3.3 Contrôle à distance avec SSH ..... 181
  - 3.4 Diagnostic et solutions pour les problèmes du contrôle avec SSH ..... 184

**Chapitre 6**  
**Supervision avec SNMP**

- 1. Introduction à SNMP..... 187
  - 1.1 Fichier MIB ..... 189
  - 1.2 Les requêtes et les messages SNMP..... 193
  - 1.3 Les versions du protocole SNMP..... 194
- 2. Installation et configuration de l’agent SNMP..... 196
  - 2.1 Activer SNMP sur un serveur Linux ..... 196
  - 2.2 Activer SNMP sur un serveur Windows..... 198
  - 2.3 Activer SNMP sur un équipement Cisco ..... 207
  - 2.4 Test SNMP ..... 208
- 3. Contrôle d’un hôte avec SNMP..... 210
- 4. Diagnostic et solutions pour les problèmes du contrôle avec SNMP ..... 214

**Chapitre 7**  
**Supervision avancée**

- 1. Supervision d’un serveur Windows..... 217
  - 1.1 Installation de NSClient++ ..... 218
  - 1.2 Configuration de NSClient++ ..... 220

1.3	Configuration de Nagios pour surveiller une machine Windows . . . . .	227
1.3.1	NSClient++ en mode nsclient . . . . .	227
1.3.2	NSClient++ en mode NRPE . . . . .	231
1.3.3	NSClient++ en mode NSCA . . . . .	232
2.	Supervision VMware . . . . .	233
2.1	Installation VMware SDK . . . . .	234
2.2	Installation du plugin check_vmware_api.pl . . . . .	235
2.3	Contrôle d'un serveur VMware ESXi . . . . .	238
2.4	Contrôle d'une machine virtuelle VMware . . . . .	243
3.	Supervision des équipements réseau . . . . .	245
3.1	Contrôle l'état d'un port réseau . . . . .	246
3.2	Contrôle de la bande passante . . . . .	247
4.	Supervision d'un site web . . . . .	249
5.	Développement des plugins Nagios . . . . .	253
5.1	Les bonnes pratiques . . . . .	254
5.2	Exemple d'un plugin shell . . . . .	257
5.3	Exemple d'un plugin Perl . . . . .	261

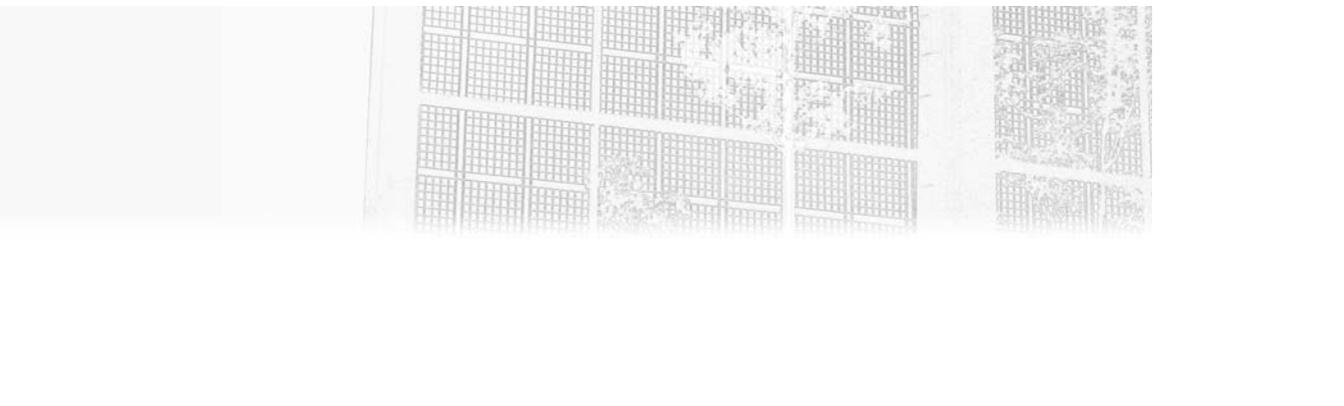
## **Chapitre 8**

### **Gestion des notifications et des événements**

1.	Gestion des notifications . . . . .	267
1.1	Configuration de notification sur les hôtes et les services . . . . .	267
1.2	Notification par un serveur mail externe . . . . .	272
1.3	Notifications par SMS . . . . .	275
1.4	Notification par messagerie instantanée . . . . .	279
2.	Gestionnaires d'événements . . . . .	281

**Chapitre 9**  
**Amélioration de Nagios**

- 1. Faciliter la configuration de Nagios avec NConf ..... 285
  - 1.1 Installation et configuration de NConf ..... 286
  - 1.2 Synchronisation avec Nagios..... 291
  - 1.3 Utilisation de NConf ..... 296
- 2. Générer des graphes avec PNP4Nagios ..... 298
  - 2.1 Installation de PNP..... 300
  - 2.2 Intégration avec Nagios ..... 303
- 3. La cartographie avec NagVis ..... 305
  - 3.1 Installation de NagVis ..... 306
  - 3.2 Configuration et intégration avec Nagios..... 308
- 4. Automatiser la configuration de Nagios avec Ansible ..... 309
  - 4.1 Principe de fonctionnement et d’installation d’Ansible..... 310
  - 4.2 Configuration de Ansible pour automatiser Nagios..... 315
- 5. Améliorer le suivi d'exploitation avec ELK ..... 317
  - 5.1 La stack ELK ..... 318
  - 5.2 Suivre les messages Nagios vers ELK..... 321
  
- Index ..... 325



# 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

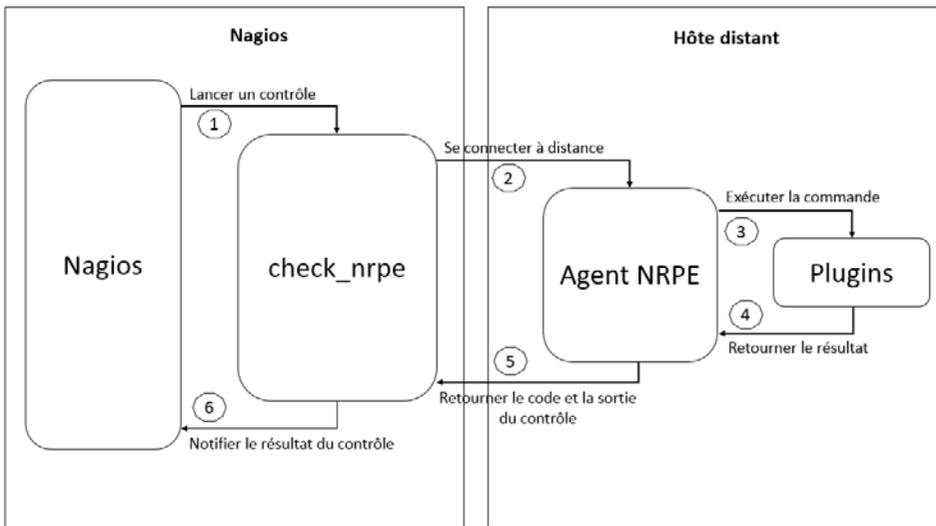
### 2.1 Principe de fonctionnement

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=WARNING, 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 paquets 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.