

MCours.com

Chapitre V

CONFIGURATION ET ADMINISTRATION

V.1 Introduction

Nagios est un outil libre et open-source qui est utilisé pour contrôler et monitorer les éléments et les services sur un réseau. Lorsqu'il détecte un problème il envoie des messages d'alerte, soit par mail, soit par d'autres techniques. Il peut aussi être configuré afin qu'un personnel désigné peut accéder à des informations, des services ou des équipements particulièrs. Ce chapitre vous explique comment mettre en place Nagios sur un Ubuntu 9.10 server.

V.2 Installation de Nagios

Avant d'installer Nagios, il est préférable d'installer le serveur web Apache (c'est plus commode pour tester le bon fonctionnement de Nagios). Sans entrer dans les détails d'installation d'Apache, vous pouvez déjà avoir un serveur web fonctionnel en installant le paquet **apache2**.

Ensuite, il ne vous reste plus qu'à installer Nagios proprement dit, installer le paquet **nagiostext**.

Installer le paquet nagios3 (apache2 s'installera automatiquement car c'est une dépendance).

A la fin de l'installation, Nagios va vous demander d'introduire un mot de passe pour «nagiosadmin ».

V.3. Configuration

Pour configurer le serveur Apache de telle manière que Nagios soit accessible, le paquet Nagios fait un lien symbolique /etc/apache2/conf.d/nagios.conf vers *etc/nagios3/apache.conf.*

Ensuite, vous devez recharger la configuration d'Apache à l'aide de la commande suivante

/etc/init.d/apache2 restart

V.3.1. Création des informations de compte utilisateur

Créez un nouveau compte utilisateur nagios et donnez-lui un mot de passe.

/usr/sbin/useradd nagios

passwd nagios

Sur les versions server d'Ubuntu, vous allez devoir créer manuellement un groupe d'utilisateur *nagios* (il n'est pas créé par défaut).

/usr/sbin/groupadd nagios

Il vous faut maintenant placer l'utilisateur nagios dans ce nouveau groupe.

/usr/sbin/usermod -G nagios nagios

Créez un nouveau groupe *nagcmd*qui permettra d'exécuter certaines commandes externes par l'intermédiaire de l'interface WEB. Placez ensuite dans ce groupe les utilisateurs nagios et apache.

/usr/sbin/groupadd nagcmd

/usr/sbin/usermod -G nagcmd nagios

/usr/sbin/usermod -G nagcmd www-data

Créez un compte nagiosadmin pour se connecter à l'interface Web de Nagios. N'oubliez pas le motde passe, vous en aurez besoin plus tard.

htpasswd -c /etc/nagios3/htpasswd.users nagiosadmin

V.3.2. Personnalisation de la configuration

Des exemples de fichiers de configuration sont maintenant installés dans le répertoire /

/etc/nagios3/

Ces fichiers d'exemple peuvent fonctionner correctement pour démarrer avec Nagios. Vous allez avoir besoin d'effectuer une petite modification avant de continuer...

Editez le fichier de configuration /*etc/nagios3/contacts.cfg* avec votre éditeur favori et remplacez l'adresse mail associée au contact *nagiosadmin* par votre adresse si vous désirez recevoir les alertes.

V.3.3. Configurez l'interface Web

Installez le fichier de configuration web de Nagios dans le répertoire conf.d d'Apache.

make install-webconf

Redémarrez Apache pour prendre en compte ces modifications.

/etc/init.d/apache2 restart

Démarrage de Nagios

Configurez Nagios pour démarrer automatiquement au démarrage du système.

/etc/init.d/nagios3 restart

Connexion à l'interface Web

Vous devriez pouvoir maintenant accéder à l'interface Web de Nagios avec l'adresse cidessous. Le nom d'utilisateur (nagiosadmin) et le mot de passe définis précédemment vous sont demandés. <u>http://localhost/nagios/</u>

Eichier Éditio <u>n A</u> ffichage <u>H</u> istorique <u>M</u> arque-pages	Qutils Aid <u>e</u>
🖕 🧅 🗸 🥑 😣 🏠 🝺 http://localhost/nagio:	53 🕄 🕄
🖻 Les plus visités 🗸 🛛 🔊 Getting Started 🔝 Latest Head	ines ~
Chargement	
Authorization Requir	red
This server could not verify that you are autho your browser doesn't understand how to supp	rized to access the document requested. Either you supplied the wrong credentials ly the credentials required.
Apache/2.2.12 (Ubuntu) Server at localhost Po	rt 80
0	Authentification requise
	Le site http://localhost demande un nom d'utilisateur et un mot de passe. Le site indique : « Nagios Access »
Utilisateur	r: nagiosadmin
Mot de passe	
	S Annuler V OK
Mot de passe	: ••••••



Cliquez sur le lien "Service Detail" de la barre de navigation pour voir ce qui est surveillé sur votre machine locale. Quelques minutes seront nécessaires à Nagios pour vérifier tous les services associés à votre machine.

Nagios [®] General [®] Home [®] Documentation Monitoring	Current Ne Last Updated: Updated every Nagios® 3.0.6 Logged in as <i>r</i> View History F- View History F- View Hotfication	etwork Status . Tue Jun 7 20:24:50 y 90 seconds i- <u>www.nagios.org</u> nagiosadmin or all hosts ons For All Hosts tus Detail For All Ho) CEST 2011		Up Dow 1 1	lost Status Tota Unreachable 0 Problems All T 1 2	Als Service Status Totals Pending Ok Warning Unknown Critical Pending 0 3 1 0 3 0 ypes 4 7 7 7
Tactical Overview Service Detail Host Detail Hostoroup Overview					Service	Status Details	s For All Hosts
Hostgroup Summary	Host ᠰ	Service 🐴	Status ᠰ	Last Check ᠰ	Duration ᠰ	Attempt 🔨	Status Information
Hostgroup Grid	gateway	PING	CRITICAL	2011-06-01 12:23:13	15d 11h 8m 48s	1/4	CRITIQUE - Le rÃiûseau est inaccessible (192.168.1.1)
Servicegroup Overview							
Servicegroup Grid	<u>localhost</u> (O	Current Load	ОК	2011-06-01 12:19:43	15d 11h 7m 22s	1/4	OK - Charge moyenne: 0.37, 0.23, 0.19
Status Map		Current Users	OK	2011-06-01 12:21:13	15d 11h 5m 56s	1/4	UTILISATEURS OK - 1 utilisateurs actuellement connectés sur
3-D Status Map		Disk Space	CRITICAL	2011-06-01 12:22:43	12d 4h 55m 3s	4/4	DISK CRITIQUE - /root/.gv/s is not accessible: Permission non accordũe
Service Problems		<u>HTTP</u>	WARNING	2011-06-01 12:18:43	6d 8h 6m 7s	4/4	HTTP WARNING: HTTP/1.1 404 Not Found - 476 bytes in 0,002 second response time
Unhandled		<u>SSH</u>	CRITICAL	2011-06-01 12:20:13	15d 11h 6m 39s	4/4	Connexion refusée
Host Problems		Total Processes	ОК	2011-06-01 12:21:43	15d 11h 5m 13s	1/4	PROCS OK: 193 processus
OUnhandled							
onetwork Outages							
Show Host:							

Figure V.1: service détail pour une machine localhost

Nagios General Home Documentation Monitoring	Current Net Last Updated: V Updated every Nagios® 3.0.6 - Logged in as <i>na</i> View History Fo View Notification View Host Statu	work Status Wed Dec 7 16:03:59 C 90 seconds www.nagios.org agiosadmin r all hosts is For All Hosts is Der All Hosts	ET 2011		Host S Up Down Un 3 0 All Proble	tatus Totals reachable Pendil 0 0 ems All Types 3	Service Status Totals Ok Warning Unknown Critical Pending 9 0 0 2 0 All Problems All Types 11 3 </th
Tactical Overview Service Detail Host Detail Host Detail Host aroup Overview					Service Statu	s Details For <i>i</i>	All Hosts
Hostgroup Summary	Host 🐴 👘	Service 🐴	Status ↑↓	Last Check ᠰ	Duration ↑↓	Attempt ᠰ	Status Information
Hostgroup Grid	benaissa	Current Load	ОК	2011-12-07 16:03:44	0d 0h 5m 15s	1/4	OK - Charge moyenne: 0.00, 0.03, 0.00
Servicegroup Overview		Current Users	ОК	2011-12-07 16:00:06	0d 0h 3m 53s	1/4	UTILISATEURS OK - 1 utilisateurs actuellement connectés sur
Servicegroup Summary		Disk Space	CRITICAL	2011-12-07 16:03:28	0d 0h 2m 31s	3/4	DISK CRITIQUE - /root/.gvfs is not accessible: Permission non accordÃ@e
Status Map		Total Processes	ОК	2011-12-07 16:02:50	Od Oh 1m 9s	1/4	PROCS OK: 170 processus
3-D Status Map		0000	01/	0014 40 07 40 00 04	01001.40-0-		
Service Problems	<u>qateway</u>	PING	UK	2011-12-07 16:00:34	60 23N 42M 2S	1/4	PING OK - Paquets perdus = 0%, RTA = 0.06 ms
Unhandled	localhost	Current Load	ОК	2011-12-07 15:59:12	6d 23h 40m 36s	1/4	OK - Charge movenne: 0.06. 0.08. 0.02
Host Problems	201	Current Licere	OK	2011 12 07 16:03:26	6d 23h 30m 10c	1/4	ITTILISATELIDS OK 1 utilisateure actuellement connectÂ@e sur
O Unhandled		Dick Space	CRITICAL	2011-12-07 16:02:51	0d 1h 14m 8s	4/4	DISK ODITIONE - I tuisateurs acuelement connectavis sur
Network Outages		HTTP		2011-12-07 16:01:17	6d 23h 41m 19s	1/4	HTTP OK' HTTP/1 1 200 OK - 453 hutes in 0 001 second resonne time
Show Host:		SSH	OK	2011-12-07 15:58:57	6d 23h 37m 53s	1/4	SSH OK - OnenSSH 5 1n1 Debian Subuntu? (nrotocole 2.0)
		Total Processes	OK	2011-12-07 15:59:09	6d 23h 38m 27s	1/4	PROCS OK: 171 processus
		1000110000000		1011 12 0. 10.00.00	56 201 5011 215		
 Comments Downtime 							
Process Info Performance Info Scheduling Queue							

Figure V.2:service détail pour une machine l'inux

Maintenant, nous allons lister les principaux fichiers de configuration de Nagios. Ils ne sont pas tous mentionnés, seulement les plus importants. Ces fichiers se trouvent dans le répertoire /etc/nagios du répertoire d'installation de Nagios.

Fichiers	Description
cgi.cfg	Configuration du site web et des cgi (authorization).
checkcommands.cfg	Définition des tests.
contactgroups.cfg	Définition des groupes d'administrateurs.
contatcs.cfg	Définition des administrateurs (droits, adresse mail, nature des alertes)
hostextinfo.cfg	Définissions complémentaires des machines pour la cartographie du réseau par les cgi de l'interface web (icône, emplacement)
hostgroups.cfg	Définition des groupes de machines.
hosts.cfg	Définition des machines
miscommands.cfg	Définition des commandes. Notamment celle d'envoie par mail (host-notify-by-email)
nagios.cfg	Fichier de configuration principal (emplacement des fichiers, gestion des logs, user et group, comportement général).
resource.cfg	Définition des variables. Notamment \$USER1 = chemin d'accès aux plugins)
services.cfg	Définition des services à superviser. C'est le plus gros fichier à écrire. On y renseigne tous les services de toutes les machines que Nagios devra gérer.

Table V.1 : Les fichiers de configuration

Nous allons à présent voir à titre d'exemple quelques extraits choisis de ces fichiers de configuration. Le but est aussi pédagogique puisqu'il va nous permettre de concrétiser ce que nous avons vu depuis le début.

Exemple de fichier contacts.cfg : /etc/nagios3/conf.d/contacts.cfg

define contact{	
contact_name	ostaquet
alias	Oscar Staquetowski
service_notification_period	24x7
host_notification_period	24x7
service_notification_options	w,u,c,r
host_notification_options	d,u,r
service_notification_commands	notify-service-by-email
host_notification_commands	notify-host-by-email
email	username@domaine.net
pager	+329999999999
}	

Exemple de fichier hostgroups : /etc/nagios3/conf.d/hostgroups.cfg

define	hostgroup{	
	hostgroup_name	connectique
	alias	Routeurs, firewalls et gateway
	contact_groups	admins-router
	members	router
	}	
define	hostgroup{	
	hostgroup_name	mail-server
	alias	Serveurs de mails Ubuntu
	contact_groups	admins-ubuntu
	members	maill, mail2
	}	

Exemple dfichier services.cfg : /etc/nagios3/conf.d/services.cfg



V.4. Nsclient++

NSClient se base sur une architecture client/serveur. La partie cliente (nommée **check_nt**), doit être disponible sur le serveur Nagios. La partie serveur (**NSClient++**) est à installer sur chacune des machines Windows à surveiller.

V.4.1. Configuration de Nagios pour surveiller vos machines Windows

Une fois le client et le serveur installé, il faut configurer Nagios de la manière suivantes. Il faut dans un premier temps éditer votre fichier de configuration des hosts (hosts.cfg par défaut) et y ajouter votre machine Windows:

```
Define host {
use generic-hosthost_name nabila
alias Ma machine Win
address 192.168.0.4}
```

Puis ajouter les services offerts par NSClient (dans le fichier services.cfg):

```
# Affiche la version du NSClient
define service {
use generic-service
host_name benaissa
service description VERSION
check_command check_nt!CLIENTVERSION
}
# Temps écoulé depuis le dernier reboot (uptime)
define service {
use generic-service
host_name benaissa
service_description UPTIME
check_command check_nt!UPTIME
}
# Charge CPU
# WARNING si charge > 80% pendant plus de 5 minutes
# CRITICAL si charge > 90% pendant plus de 5 minutes
define service {
use generic-service
host name benaissa
```

service_description CPU
check_command check_nt!CPULOAD!-1 5,80,90}
Etat de la mémoire vive libre
WARNING si mémoire > 80%
CRITICAL si mémoire > 90%
define service {
use generic-service
host_name benaissa
service_description MEM
check_command check_nt!MEMUSE!-w 80 -c 90}
Etat de la mémoire disque libre (sur disque c:)
WARNING si mémoire > 80%
CRITICAL si mémoire > 90%
define service {
use generic-service
host_name benaissa
service_description DISK
check_command check_nt!USEDDISKSPACE!-l c -w 80 -c 90}

Pour monitorer des clients Windows avec Nagios il faut passer par l'installation d'un agent nagios, ici le choix se portera sur **NSClient**

mais il en existe d'autres comme NCNET. NSClient communiquera directement avec Check NT (voir schéma fonctionnel).



Figure V.3 Schéma fonctionnel de Nagios couplé à NSClient :

Configuration de NAGIOS pour accueillir des hôtes Windows

On va modifier la configuration de Nagios pour qu'ils connaissent l'hôte que l'on va superviser, pour cela on va modifier le fichier de config principal de Nagios pour accepter les clients Windows:

```
vim /usr/nagios/etc/nagios.cfg
```

Dans ce fichier on va dé commenter cette ligne :

#cfg file=/usr/nagios/etc/objects/windows.cfg

Une fois décommenté on l'enregistre et on ferme. Maintenant on va ouvrir le fichier **windows.cfg** pour y rajouter le nom d'hôte à monitorer et les services à surveiller

vim /usr/nagios/etc/objects/windows.cfg

Une fois ce fichier ouvert il faut rajouter le nom du serveur :

define host{			
use	windows-server		
host_name	servfichier		
alias	servfichier		
address	192.168.0.225		
}			

Ensuite suivant les services que vous voulez surveiller il faut rajouter le nom d'hôte toujours dans le même fichier :

```
define service{
    use generic-service
    host_name service_description NSClient++ Version
    check_command check_nt!CLIENTVERSION
    }
```

Maintenant il faut ouvrir le fichier de configuration commands.cfg pour mettre un mot de passe pour la communication entre NSClient et le CHECK NT de Nagios

vim /usr/nagios/etc/objects/commands.cf

```
# 'check_nt' command definition
define command{
    command_name check_nt
    command_line $USER1$/check_nt -H $HOSTADDRESS$ -p 12489 -v $ARG1$
$ARG2$ -s Ton_password
    }
```

Il faudra se rappeler de ce mot de passe car on l'utilisera plus tard pour la config client.

Installation de NSClient sur le serveur Windows:

Le logiciel NSClient est disponible à cette adresse : <u>http://sourceforge.net/projects/nscplus</u>

Une fois télécharger il faut dézipper l'archive par exemple dans C : maintenant il faut ouvrir une invite de commande dans C:\NSClient Et tapez ce qui suit :

```
nsclient++.exe /install
nstray.exe
```

Ensuite il faut ouvrir la mmc **services.msc** et configurer le démarrage automatique du service et l'autoriser à interagir avec le bureau



Ensuite on va éditer le fichier **NSC.ini** pour configurer la connexion entre le serveur à monitorer et nagios. Dans ce fichier il faut décommenter tous les modules de la section [**MODULES**] à l'exception de **checkWMI.dll** et **RemoteConfiguration.dll**

Ensuite il faut changer le **password** dans la section **[Settings]** pour que le client communique avec Nagios. On a entré le password pour nagios un peu plus haut, bien entendu il faut que ce soit le même.

```
;# PASSWORD
; This is the password (-s)
access the daemon remotly.
password=Ton_Password
```

Ensuite il faut décommenter **allowed_hosts** option toujours dans la section **[Settings]**. Et il faut rajouter l'**adresse IP du serveur Nagios** avec lequel il va communiquer.

```
;# ALLOWED HOST ADDRESSES
; This is a comma-delimited list of IP
; If leave this blank anyone can access
; The syntax is host or ip/mask so 192.:
allowed_hosts=Adresse IP de Nagios
```

Ensuite il faut vérifier la ligne ou se configure le **port** sur lequel NSClient va communiquer par défaut c'est le **12489** (décommenter la ligne si elle est commentée et penser bien à l'ouvrir dans le pare-feu en TCP)

```
;# NSCLIENT PORT NUMBER
; This is the port the NSClientListener.dll will listen to.
port=12489
```

Voilà la configuration de NSClient et Nagios est terminé donc maintenant on va démarrer NSClient :

```
nsclient++.exe /start
```

Maintenant on vérifie la configuration de nagios

```
/usr/nagios/bin/nagios -v /usr/ nagios/etc/nagios.cfg
```

Current Ne Last Updated: Updated every Nagios® 3.0.6 Logged in as / View History F View Notificatio View Host Stat	twork Status Wed Dec 7 15:34:38 / 90 seconds - www.nadios.org agiosadmin or all hosts ons For All Hosts us Detail For All Hosts	CET 2011		H Up Down 3 0 All F Service S	ost Status Total Unreachable 0 Problems All Ty 0 3 Status Details	s Pending 0 PPES For All Hosts	Service Status Totals Ok Warning Unknown Critical Pending 8 0 3 2 0 All Problems All Types 13	8
Host 🛝	Service 1	Status 1	Last Check		Attempt	Status Information		
benaissa	CPU	UNKNOWN	2011-12-07 15:30:51	0d 0h 11m 47s	4/4	NSClient - ERROR: Could not a	et data for 5 perhaps we don't collect data this far back?	
	DISK	CRITICAL	2011-12-07 15:32:00	0d 0h 10m 38s	4/4	c: - total: 76,97 Gb - utilisé: 76,	65 Gb (100%) - libre 0.32 Gb (0%)	
	MEM	UNKNOWN	2011-12-07 15:33:09	0d 0h 9m 29s	4/4	NSClient - ERROR: Failed to ge	t PDH value.	
	PING	ОК	2011-12-07 15:31:18	0d 0h 8m 20s	1/4	PING OK - Paquets perdus = 0%	6, RTA = 0.61 ms	
	UPTIME	UNKNOWN	2011-12-07 15:30:28	0d 0h 7m 10s	4/4	NSClient - ERROR: Could not ge	et value	
	nsclient++ version	ОК	2011-12-07 15:33:14	0d 0h 11m 24s	1/4	NSClient++ 0.3.9.327 2011-08-1	.6	
gateway	PING	ОК	2011-12-07 15:30:34	6d 23h 12m 41s	1/4	PING OK - Paquets perdus = 0%	6, RTA = 0.04 ms	
localhost	Current Load	ОК	2011-12-07 15:32:00	6d 23h 11m 15s	1/4	OK - Charge moyenne: 0.00, 0.0	03, 0.01	
	Current Users	ОК	2011-12-07 15:33:26	6d 23h 9m 49s	1/4	UTILISATEURS OK - 1 utilisateu	urs actuellement connectés sur	
	Disk Space	CRITICAL	2011-12-07 15:32:51	0d 0h 44m 47s	4/4	DISK CRITIQUE - /root/.gvfs is r	not accessible: Permission non accordée	
	HTTP	ОК	2011-12-07 15:31:17	6d 23h 11m 58s	1/4	HTTP OK: HTTP/1.1 200 OK - 4	153 bytes in 0,001 second response time	
	<u>SSH</u>	ОК	2011-12-07 15:33:57	6d 23h 8m 32s	1/4	SSH OK - OpenSSH_5.1p1 Deb	ian-6ubuntu2 (protocole 2.0)	
	Total Processes	ОК	2011-12-07 15:34:09	6d 23h 9m 6s	1/4	PROCS OK: 171 processus		
13 Matching Service Entries Displayed								

Figure V.4:Services détaillé pour une machines Windows

V.5. Conclusion

Avec les tests que nous pouvons conclure que Nagios est un outil qui fournit une analyse du trafic, le contrôle des liens, services de vérification et même de dispositifs qui prennent en charge SNMP avec Nagios. Malgré la complexité dans la mise en, pourrait déployer un système qui permet au gouvernement central pour contrôler l'ensemble du réseau et d'alerter la personne responsable pour les points de défaillance sont rapidement résolus.

MCours.com