

# Comment installer Nagios 4 dans Ubuntu et Debian

By Violette Laurent

Dans cette rubrique, nous allons apprendre comment installer et configurer la dernière version officielle de **Noyau de Nagios** à partir de sources sur les serveurs Debian et Ubuntu.

**Noyau de Nagios** est un gratuit Application de surveillance de réseau Open Source conçu pour surveiller les applications réseau, les périphériques et leurs services associés et dans un réseau.

**Nagios** peut surveiller à distance des paramètres spécifiques du système d'exploitation via des agents déployés sur des nœuds et envoyer des alertes par courrier ou SMS afin d'avertir les administrateurs en cas d'échec de services critiques dans un réseau, tels que SMTP, HTTP, SSH, FTP et autres.

## Exigences

### Étape 1: Installez les pré-requis pour Nagios

1. Avant d'installer Nagios Core à partir de sources dans **Ubuntu** ou **Debian**, installez d'abord les composants suivants de la pile LAMP dans votre système, sans **SGBDR MySQL** composant de base de données, en exécutant la commande ci-dessous.

```
# apt install apache2 libapache2-mod-php php
```

2. À l'étape suivante, installez les dépendances système et les utilitaires suivants requis pour compiler et installer **Noyau de Nagios** à partir des sources, en émettant la commande suivante.

```
# apt install wget unzip zip autoconf gcc libc6 make apache2-utils libgd-dev
```

### Étape 2: Installez Nagios 4 Core dans Ubuntu et Debian

3. Lors de la première étape, créez **Nagios** utilisateur système et groupe et ajouter un compte nagios à Apache **www-data** utilisateur, en émettant les commandes ci-dessous.

```
# useradd nagios
# usermod -a -G nagios www-data
```

4. Une fois que toutes les dépendances, packages et exigences système pour compiler Nagios à partir des sources sont présents dans votre système, allez sur la page Web de Nagios et récupérez le dernière version de Nagios Core archive source stable en émettant ce qui suit commande wget.

```
# wget https://assets.nagios.com/downloads/nagioscore/releases/nagios-4.4.6.tar.gz
```

5. Ensuite, extrayez l'archive tar de Nagios et entrez dans le répertoire nagios extrait, avec les commandes suivantes. Problème commande ls pour lister le contenu du répertoire nagios.

```
# tar xzf nagios-4.4.6.tar.gz
# cd nagios-4.4.6/
# ls
```

### Exemple de sortie

```
total 600
-rwxrwxr-x 1 root root 346 Apr 28 20:48 aclocal.m4
```

```

drwxrwxr-x 2 root root 4096 Apr 28 20:48 autoconf-macros
drwxrwxr-x 2 root root 4096 Apr 28 20:48 base
drwxrwxr-x 2 root root 4096 Apr 28 20:48 cgi
-rw-rw-r-- 1 root root 32590 Apr 28 20:48 Changelog
drwxrwxr-x 2 root root 4096 Apr 28 20:48 common
-rwxrwxr-x 1 root root 43765 Apr 28 20:48 config.guess
-rwxrwxr-x 1 root root 36345 Apr 28 20:48 config.sub
-rwxrwxr-x 1 root root 246354 Apr 28 20:48 configure
-rw-rw-r-- 1 root root 29812 Apr 28 20:48 configure.ac
drwxrwxr-x 5 root root 4096 Apr 28 20:48 contrib
-rw-rw-r-- 1 root root 6291 Apr 28 20:48 CONTRIBUTING.md
drwxrwxr-x 2 root root 4096 Apr 28 20:48 docs
-rw-rw-r-- 1 root root 886 Apr 28 20:48 doxy.conf
-rwxrwxr-x 1 root root 7025 Apr 28 20:48 functions
drwxrwxr-x 11 root root 4096 Apr 28 20:48 html
drwxrwxr-x 2 root root 4096 Apr 28 20:48 include
-rwxrwxr-x 1 root root 77 Apr 28 20:48 indent-all.sh
-rwxrwxr-x 1 root root 161 Apr 28 20:48 indent.sh
-rw-rw-r-- 1 root root 422 Apr 28 20:48 INSTALLING
...

```

6. Maintenant, commencez à compiler Nagios à partir des sources en émettant les commandes ci-dessous. Assurez-vous de configurer Nagios avec une configuration de répertoire activée pour les sites Apache en exécutant la commande ci-dessous.

```
# ./configure --with-httpd-conf=/etc/apache2/sites-enabled
```

#### Exemple de sortie

```
*** Configuration summary for nagios 4.4.6 2020-04-28 ***:
```

##### General Options:

```

-----
Nagios executable: nagios
Nagios user/group: nagios,nagios
Command user/group: nagios,nagios
Event Broker: yes
Install ${prefix}: /usr/local/nagios
Install ${includedir}: /usr/local/nagios/include/nagios
Lock file: /run/nagios.lock
Check result directory: /usr/local/nagios/var/spool/checkresults
Init directory: /lib/systemd/system
Apache conf.d directory: /etc/apache2/sites-enabled
Mail program: /bin/mail
Host OS: linux-gnu
IOBroker Method: epoll

```

##### Web Interface Options:

```

-----
HTML URL: http://localhost/nagios/
CGI URL: http://localhost/nagios/cgi-bin/
Traceroute (used by WAP):

```

Review the options above for accuracy. If they look okay, type 'make all' to compile the main program and CGIs.

7. À l'étape suivante, créez des fichiers Nagios en exécutant la commande suivante.

```
# make all
```

**8.** Maintenant, installez les fichiers binaires Nagios, les scripts CGI et les fichiers HTML en exécutant la commande suivante.

```
# make install
```

**9.** Ensuite, installez les fichiers de configuration d'initialisation du démon Nagios et du mode de commande externe et assurez-vous d'activer le démon nagios à l'échelle du système en exécutant les commandes suivantes.

```
# make install-init  
# make install-commandmode  
# systemctl enable nagios.service
```

**dix.** Ensuite, exécutez la commande suivante afin d'installer quelques exemples de fichiers de configuration Nagios nécessaires à Nagios pour fonctionner correctement en exécutant la commande ci-dessous.

```
# make install-config
```

**11.** Installez également le fichier de configuration Nagios pour le serveur Web Apache, qui peut être installé dans / **etc** / **apache2** / **sites-enabled** / répertoire, en exécutant la commande ci-dessous.

```
# make install-webconf
```

**12.** Ensuite, créez **nagiosadmin** compte et un mot de passe pour ce compte nécessaire au serveur Apache pour se connecter au panneau Web Nagios en exécutant la commande suivante.

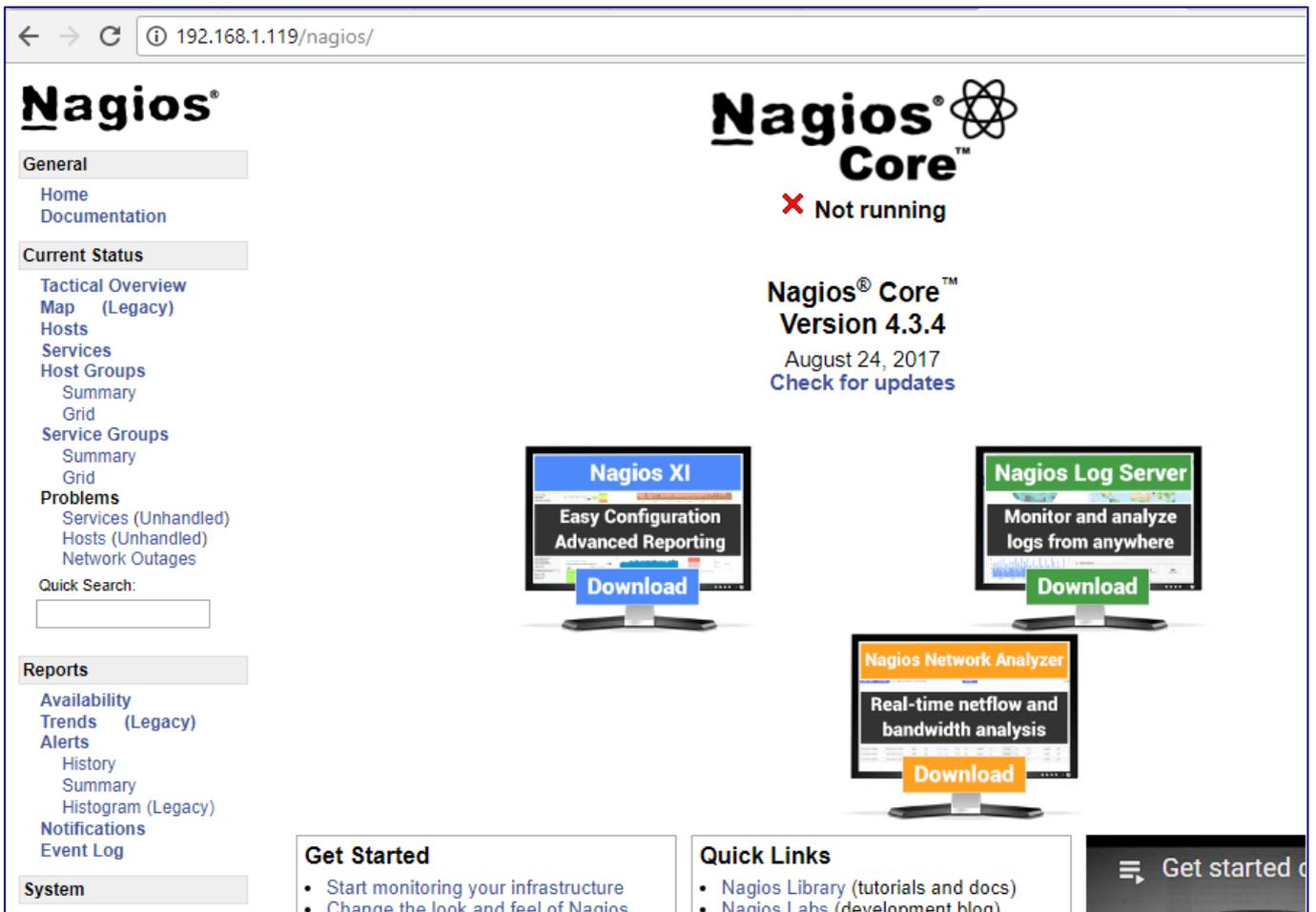
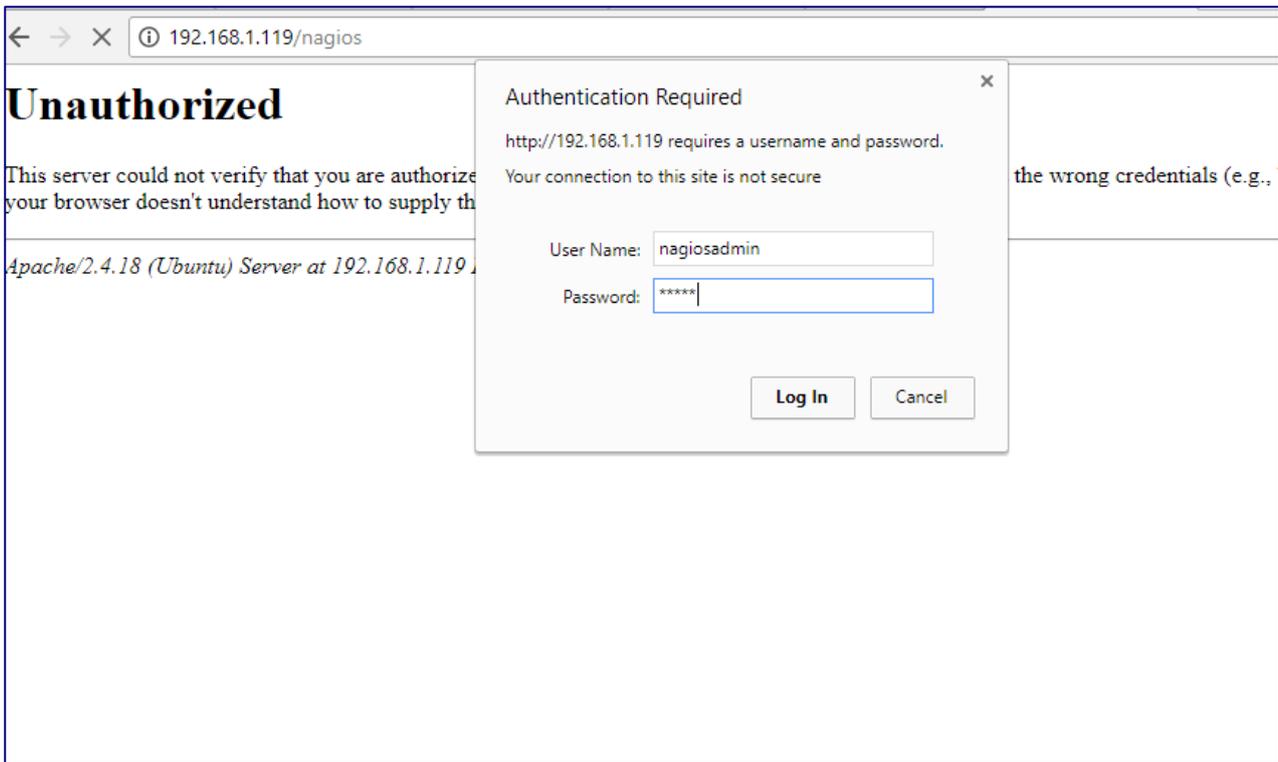
```
# htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin
```

**13.** Pour permettre au serveur HTTP Apache d'exécuter des scripts Nagios cgi et d'accéder au panneau d'administration de Nagios via HTTP, activez d'abord le module cgi dans Apache, puis redémarrez le service Apache et démarrez et activez le démon Nagios à l'échelle du système en émettant les commandes suivantes.

```
# a2enmod cgi  
# systemctl restart apache2  
# systemctl start nagios  
# systemctl enable nagios
```

**14.** Enfin, connectez-vous à l'Interface Web de Nagios en pointant un navigateur vers l'adresse IP ou le nom de domaine de votre serveur à l'adresse URL suivante via le protocole HTTP. Connectez-vous à Nagios avec l'utilisateur nagiosadmin la configuration du mot de passe avec le script htpasswd.

```
http://IP-Address/nagios  
OR  
http://DOMAIN/nagios
```



15. Pour afficher l'état de vos hôtes, accédez à **État actuel** -> **Hôtes** menu où vous remarquerez que certaines erreurs sont affichées pour l'hôte local, comme illustré dans la capture d'écran ci-dessous. L'erreur apparaît car Nagios n'a pas installé de plugins pour vérifier l'état des hôtes et des services.

The screenshot shows the Nagios web interface at 192.168.1.119/nagios/. The interface includes a sidebar with navigation links for General, Current Status, Problems, Reports, and System. The main content area displays:

- Current Network Status:** Last Updated: Fri Oct 27 20:11:05 EEST 2017, Updated every 90 seconds, Nagios® Core™ 4.3.4 - www.nagios.org, Logged in as nagiosadmin.
- Host Status Totals:** Up: 0, Down: 1, Unreachable: 0, Pending: 0. All Problems: 1, All Types: 1.
- Service Status Totals:** Ok: 0, Warning: 0, Unknown: 0, Critical: 6, Pending: 2. All Problems: 6, All Types: 8.
- Host Status Details For All Host Groups:** A table showing one host, 'localhost', which is DOWN. The last check was on 10-27-2017 at 20:10:58, with a duration of 0d 0h 0m 7s. The status information indicates a failure: '(No output on stdout) stderr: execvp(/usr/local/nagios/libexec/check\_ping, ...) failed. errno is 2: No such file or directory'.

### Étape 3: Installez les plugins Nagios dans Ubuntu et Debian

16. Pour compiler et installer les plugins Nagios à partir de sources dans Debian ou Ubuntu, à la première étape, installez les dépendances suivantes dans votre système, en exécutant la commande ci-dessous.

```
# apt install libmcrypt-dev make libssl-dev bc gawk dc build-essential snmp
libnet-snmp-perl gettext libldap2-dev smbclient fping libmysqlclient-dev libdbi-
dev
```

17. Ensuite, visitez la page des dépôts de plugins Nagios et télécharger la dernière archive tar du code source en émettant la commande suivante.

```
# wget https://github.com/nagios-plugins/nagios-plugins/archive/release-
2.3.3.tar.gz
```

18. Allez-y et extrayez l'archive du code source de Nagios Plugins et changez le chemin vers le répertoire nagios-plugins extrait en exécutant les commandes suivantes.

```
# tar xzf release-2.3.3.tar.gz
# cd nagios-plugins-release-2.3.3/
```

19. Maintenant, commencez à compiler et installer les plugins Nagios à partir des sources, en exécutant la série de commandes suivante dans la console de votre serveur.

```
# ./tools/setup
# ./configure
```

```
# make
# make install
```

20. Les plugins Nagios compilés et installés peuvent être situés dans /usr/local/nagios/libexec/ annuaire. Répertoriez ce répertoire pour afficher tous les plugins disponibles dans votre système.

```
# ls /usr/local/nagios/libexec/
```

```
root@ubuntu:~# ls /usr/local/nagios/libexec/
check_apt      check_disk_smb  check_icmp      check_load      check_nttps     check_ping      check_spop      check_users
check_breeze  check_dns       check_ide_smart check_log       check_nt       check_pop       check_ssh       check_wave
check_by_ssh  check_dummy     check_ifoperstatus check_mailq     check_ntp      check_procs    check_ssmtp     negate
check_clamd   check_file_age  check_ifstatus  check_mrtg     check_ntp_peer check_real      check_swap     urlize
check_cluster check_flexlm    check_imap      check_mrtgtraf check_ntp_time  check_rpc       check_tcp       utils.pm
check_dbi     check_fping     check_ircd      check_mysql     check_nwstat   check_sensors  check_time     utils.sh
check_dhcp    check_ftp       check_jabber    check_mysql_query check_oracle    check_simap     check_udp
check_dig     check_hpjd      check_ldap      check_nagios    check_overcr   check_smtp     check_ups
check_disk    check_http      check_ldaps     check_nntp      check_pgsql    check_snmp     check_uptime
root@ubuntu:~#
```

21. Enfin, redémarrez le démon Nagios afin d'appliquer les plugins installés, en exécutant la commande ci-dessous.

```
# systemctl restart nagios.service
```

22. Ensuite, connectez-vous au panneau Web de Nagios et accédez à **État actuel** -> **Services** et vous devriez remarquer que tous les services des hôtes sont vérifiés maintenant par les plugins Nagios.

À partir du code couleur, vous devriez voir l'état actuel des services: la couleur verte est pour **D'accord** statut, jaune pour **avertissement** et rouge pour **Critique** statut.

Host	Service	Status	Last Check	Duration	Attempt	Status Information
localhost	Current Load	OK	10-27-2017 20:21:32	0d 0h 1m 48s	1/4	OK - load average: 0.36, 0.20, 0.07
	Current Users	OK	10-27-2017 20:21:18	0d 0h 2m 0s	1/4	USERS OK - 2 users currently logged in
	HTTP	OK	10-27-2017 20:21:42	0d 0h 1m 36s	1/4	HTTP OK: HTTP/1.1 200 OK - 11595 bytes in 0.000 second response time
	PING	OK	10-27-2017 20:21:45	0d 0h 1m 33s	1/4	PING OK - Packet loss = 0%, RTA = 0.05 ms
	Root Partition	OK	10-27-2017 20:21:20	0d 0h 1m 58s	1/4	DISK OK - free space: / 8492 MB (80.51% inode=84%)
	SSH	OK	10-27-2017 20:21:58	0d 0h 1m 20s	1/4	SSH OK - OpenSSH_7.2p2 Ubuntu-4ubuntu2.2 (protocol 2.0)
	Swap Usage	CRITICAL	10-27-2017 20:22:35	0d 0h 5m 43s	4/4	SWAP CRITICAL - 0% free (0 MB out of 0 MB) - Swap is either disabled, not present, or of zero size.
	Total Processes	OK	10-27-2017 20:23:06	0d 0h 0m 12s	1/4	PROCS OK: 62 processes with STATE = RSDZT

23. Enfin, pour accéder à l'interface Web d'administration de Nagios via le protocole HTTPS, émettez les commandes suivantes pour activer les configurations SSL Apache et redémarrez le démon Apache pour refléter les changements.

```
# a2enmod ssl
# a2ensite default-ssl.conf
# systemctl restart apache2
```

24. Après avoir activé les configurations SSL Apache, ouvrez `/etc/apache2/sites-enabled/000-default.conf` fichier à modifier et ajoutez le bloc de code suivant après `DocumentRoot` déclaration comme indiqué dans l'extrait ci-dessous.

```
RewriteEngine on
RewriteCond %{HTTPS} off
RewriteRule ^(.*) https://%{HTTP_HOST}/$1
```

```
<VirtualHost *:80>
    # The ServerName directive sets the request scheme, hostname and port that
    # the server uses to identify itself. This is used when creating
    # redirection URLs. In the context of virtual hosts, the ServerName
    # specifies what hostname must appear in the request's Host: header to
    # match this virtual host. For the default virtual host (this file) this
    # value is not decisive as it is used as a last resort host regardless.
    # However, you must set it for any further virtual host explicitly.
    #ServerName www.example.com

    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/html

RewriteEngine on
RewriteCond %{HTTPS} off
RewriteRule ^(.*) https://%{HTTP_HOST}/$1

    # Available loglevels: trace8, ..., tracel, debug, info, notice, warn,
    # error, crit, alert, emerg.
    # It is also possible to configure the loglevel for particular
    # modules, e.g.
    #LogLevel info ssl:warn

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

    # For most configuration files from conf-available/, which are
    # enabled or disabled at a global level, it is possible to
    # include a line for only one particular virtual host. For example the
    # following line enables the CGI configuration for this host only
    # after it has been globally disabled with "a2disconf".

root@nagios:~# systemctl restart apache2
root@nagios:~#
```

25. Vous devez redémarrer le démon Apache pour appliquer les règles configurées, en exécutant la commande ci-dessous.

```
# systemctl restart apache2.service
```

26. Enfin, actualisez le navigateur afin d'être redirigé vers le panneau d'administration de Nagios via le protocole HTTPS. Acceptez le message souhaité qui s'affiche dans le navigateur et connectez-vous à nouveau à Nagios avec vos informations d'identification.

← → ↻ ⚠ Not secure | <https://192.168.1.119/nagios/>

# Nagios®

**General**

- Home
- Documentation

**Current Status**

- Tactical Overview
- Map (Legacy)
- Hosts
- Services
- Host Groups
  - Summary
  - Grid
- Service Groups
  - Summary
  - Grid
- Problems
  - Services (Unhandled)
  - Hosts (Unhandled)
  - Network Outages

Quick Search:

**Reports**

- Availability

**Current Network Status**  
Last Updated: Fri Oct 27 20:29:14 EEST 2017  
Updated every 90 seconds  
Nagios® Core™ 4.3.4 - [www.nagios.org](http://www.nagios.org)  
Logged in as *nagiosadmin*

View Service Status Detail For All Host Groups  
View Status Overview For All Host Groups  
View Status Summary For All Host Groups  
View Status Grid For All Host Groups

Limit Results:

Host	Status	Last Check	Duration
localhost	UP	10-27-2017 20:26:20	0d 0h 7m 52s

Results 1 - 1 of 1 Matching Hosts

**Host Status Totals**

Up	Down	Unreachable	Pending
1	0	0	0
<a href="#">All Problems</a>		<a href="#">All Types</a>	
0		1	

**Service Status Totals**

Ok	Warning	Unknown	Critical
7	0	0	1
<a href="#">All Problems</a>		<a href="#">All Types</a>	
1		8	

**Host Status Details For All Host Groups**

Toutes nos félicitations! Vous avez installé et configuré avec succès **Noyau de Nagios** système de surveillance à partir de sources **Ubuntu** serveur ou **Debian**.