Qu’est-ce que Nagios ?

Nagios, ou Nagios Core est un logiciel ordonnanceur qui surveille les systèmes, les réseaux et l’infrastructure. Nagios offre des services de surveillance et d'alerte pour les serveurs, les commutateurs, les applications et les services. Il alerte les utilisateurs en cas d’incidents et les avertit une deuxième fois lorsque le problème a été résolu. Nagios a été conçu à l'origine pour fonctionner sous Linux, mais il fonctionne aussi bien sur d'autres variantes d’Unix.

Nagios a été le premier outil de monitoring IT open source à se positionner en 1999. Il se nommait alors NetSaint. Derrière le logiciel, une véritable communauté s’est créée avec plus d’un million d’utilisateurs à travers le monde.

Nagios permet :

* la surveillance des équipements et systèmes cibles, à travers notamment des protocoles tels SMTP, POP3, HTTP, NNTP, ICMP, SNMP, SNMP, FTP, SSH ((scripts shell, C+++, Perl, Ruby, Python, PHP, C#, etc...).
* la surveillance des réseaux, systèmes d’exploitation et tous types de matériel (comme les sondes de température, les alarmes, etc.) via des scripts communément appelé plugins de supervision.
* L’alerte en cas de de dépassement de seuil ou panne via un système de notification qu i prévient l’exploitant du SI ou l’administrateur.

Fort de son succès, le projet a été « forké » (reprise d’un code source projet pour développer un autre logiciel) à plusieurs reprises : Icinga, Shinken, Centreon-Engine, Naemon,..

Quelles sont les solutions de supervision de Nagios ?

Superviser permet d’indiquer et de commander l’état d’un appel, d’un système ou d’un réseau. Les informations techniques et fonctionnelles d’un SI peuvent ainsi être remontées.

A l’ère du Cloud et du Big Data, la supervision est essentielle afin de :

* Garantir la disponibilité et les niveaux de service en cas de panne ou dégradation de performance
* Prévenir les menaces et éviter une intervention

Nagios utilise deux types de supervision :

* Supervision active : le moteur va chercher l’information. C’est le cas des protocoles tels NRPE, NSCLient++, WMI et CNP

**NRPE**

Nagios Remote Plugin Executor (NRPE) est un agent Nagios qui permet de surveiller le système à distance à l'aide de scripts hébergés sur les systèmes distants. Il permet de surveiller les ressources telles que l'utilisation du disque, la charge du système ou le nombre d'utilisateurs actuellement connectés. Nagios interroge périodiquement l'agent sur le système distant en utilisant le plugin check\_nrpe.

NRPE vous permet d'exécuter à distance les plugins Nagios sur d'autres machines Linux/Unix. Cela vous permet de surveiller les paramètres de la machine à distance (utilisation du disque, charge du CPU, etc.). Le NRPE peut également communiquer avec certains des add-ons de l'agent Windows, ce qui vous permet d'exécuter des scripts et de vérifier les métriques sur les machines Windows distantes.

**NSClient+++**

Ce programme est principalement utilisé pour surveiller les machines Windows. En cours d'installation sur un système distant, NSClient+++ écoute le port TCP 12489. Le plugin Nagios utilisé pour collecter les informations de cet addon est appelé check\_nt. Comme NRPE, NSClient+++ permet de surveiller les « services privés » (utilisation de la mémoire, charge CPU, utilisation du disque, processus en cours d'exécution, etc.) Nagios est un moniteur d'hôtes et de services qui est conçu pour vous informer des problèmes de réseau.

* Supervision passive : les équipements envoient les informations aux moteurs de supervisions comme NSS par exemple.

Quelle alternative à Nagios ?

Nagios existe depuis maintenant vingt ans. Le logiciel a été historiquement déployé On Premise. A l’ère du Cloud et avec l’émergence du Big Data, le monitoring se transforme. Les entreprises utilisent davantage un monitoring hybride : Cloud et On Premise. Des solutions intelligentes comme Infrastructure Monitoring, avec les mêmes fonctionnalités de Nagios set qui exploitent du [Machine Learning](https://www.oracle.com/fr/cloud/it-operations-management-itom/intelligent.html), paraissent plus adaptées. Les algorithmes de Machine Learning permettent une meilleure détection des anomalies par exemple.

Dans tous les cas, il sera nécessaire sur le serveur de supervision de modifier ou non le fichier « /usr/local/nagios/etc/objects/commande.cfg » afin de créer une nouvelle commande. C'est souvent le cas pour de nouveaux plugins utilisant SNMP.

Lorsque la communication se fait via NRPE, il est nécessaire de faire une modification dans le fichier « /usr/local/nagios/etc/nrpe.cfg » sur le serveur Linux à surveiller pour configurer la ligne de commande.

Une fois ces améliorations apportées, il ne reste plus qu'à définir ses services pour chaque serveur et matériel à superviser. Vous verrez dans les exemples ci-dessous différentes écritures pour faire passer les arguments. Soyez attentif !

Je vous recommande un peu de lecture pour en savoir plus sur Nagios, NSClient++…

* [**NSClient++ - documentation française**](http://wiki.monitoring-fr.org/nagios/addons/nsclient).
* [**NSClient++ - documentation officielle**](http://nsclient.org/nscp/).
* [**Installation et configuration de Nagios pour débutants**](https://djibril.developpez.com/tutoriels/linux/nagios-pour-debutant/).

## V. Services à surveiller

## Rappels Nagios[▲](https://djibril.developpez.com/tutoriels/linux/nagios-services/)

Nagios est un moniteur de supervision qui nous alerte de toutes pannes ou anomalies rencontrées sur les serveurs ou tous équipements réseau que nous surveillons. Cette surveillance se fait à l'aide d'agents installés sur ces équipements. Dans ce tutoriel, nous allons surveiller certains services et utiliser certains agents.

### IV-A. Sous Windows[▲](https://djibril.developpez.com/tutoriels/linux/nagios-services/)

L'agent utilisé est l'un des plus répandus : « NSClient++ ».

Il est dédié à l'environnement Windows et joue trois rôles essentiels :

* agent de supervision ;
* fonction de transport NRPE ;
* fonction de transport NSCA.

Dans ce tutoriel, nous utiliserons deux modes de fonctionnement de NSClient sur les trois existant.

#### IV-A-1. Mode nsclient[▲](https://djibril.developpez.com/tutoriels/linux/nagios-services/" \o "Haut de page)

Historiquement, c'est le premier mode de NSClient++ à sa création. En fait, il existait un agent nommé « nsclient » qui était interrogé via le plugin standard « check\_nt » de Nagios[(1)](https://djibril.developpez.com/tutoriels/linux/nagios-services/#noteBasPage1). Pour configurer ce mode (comme les autres), tout se fait dans le fichier de configuration NSC.ini dans la section [NSClient] ou [Settings]. Pour en savoir plus, lisez la documentation d'[**installation de Nagios**](https://djibril.developpez.com/tutoriels/linux/nagios-pour-debutant/#LIII-B-1).

À travers ce mode et le plugin « check\_nt », nous avons la possibilité de surveiller facilement plusieurs services sous Windows (Version NSClient++, CPU, Uptime, espace disque, mémoire, services Windows, nombre d'utilisateurs…). On l'utilise tout au long de cet article.

#### IV-A-2. Mode NRPE[▲](https://djibril.developpez.com/tutoriels/linux/nagios-services/)

Le mode NRPE a un très grand avantage, car il permet à l'administrateur de développer des plugins en divers langages (Visual Basics, Perl…) et de les déposer sur les machines à superviser. Ainsi, ils seront lancés par l'agent à travers ce mode après réception de la demande du serveur Nagios. Le mode NRPE de Nagios permet aussi d'interroger les différents modules de NSClient++ et d'encrypter les échanges.

Pour utiliser ce mode depuis le serveur Nagios, on utilise le plugin « check\_nrpe ». On l'utilise dans ce tutoriel, surtout pour surveiller des machines Linux.

#### IV-A-3. Mode NSCA[▲](https://djibril.developpez.com/tutoriels/linux/nagios-services/)

Ce mode utilise le protocole NSCA que nous n'utiliserons pas dans ce tutoriel.

### IV-B. Sous Linux[▲](https://djibril.developpez.com/tutoriels/linux/nagios-services/)

Nous utiliserons la plupart du temps le protocole NRPE pour échanger avec les serveurs surveillés et y lancer des programmes locaux via le plugin « check\_nrpe ». Parfois, nous utiliserons SNMP soit via le plugin Nagios « check\_snmp » ou via des plugins personnels SNMP.

### IV-C. Équipements réseau (switches…)[▲](https://djibril.developpez.com/tutoriels/linux/nagios-services/)

Le seul moyen de superviser ces équipements est d'utiliser SNMP. Il faudra juste s'assurer qu'il est bien activé. Le plugin Nagios « check\_snmp » ou des plugins personnels SNMP seront nécessaires.

### IV-D. Généralité[▲](https://djibril.developpez.com/tutoriels/linux/nagios-services/)

Dans tous les cas, il sera nécessaire sur le serveur de supervision de modifier ou non le fichier « /usr/local/nagios/etc/objects/commande.cfg » afin de créer une nouvelle commande. C'est souvent le cas pour de nouveaux plugins utilisant SNMP.

Lorsque la communication se fait via NRPE, il est nécessaire de faire une modification dans le fichier « /usr/local/nagios/etc/nrpe.cfg » sur le serveur Linux à surveiller pour configurer la ligne de commande.

Une fois ces améliorations apportées, il ne reste plus qu'à définir ses services pour chaque serveur et matériel à superviser. Vous verrez dans les exemples ci-dessous différentes écritures pour faire passer les arguments. Soyez attentif !

Je vous recommande un peu de lecture pour en savoir plus sur Nagios, NSClient++…

* [**NSClient++ - documentation française**](http://wiki.monitoring-fr.org/nagios/addons/nsclient).
* [**NSClient++ - documentation officielle**](http://nsclient.org/nscp/).
* [**Installation et configuration de Nagios pour débutants**](https://djibril.developpez.com/tutoriels/linux/nagios-pour-debutant/).

### Fonctionnalités de Nagios

* La supervision réseau
* La supervision des ressources systèmes
* La supervision applicative
* La notification par différents moyens de communication
* L'exécution de commandes manuelles ou automatiques
* La représentation des états des ressources supervisées, par coloration
* La cartographie du système d'informations supervisé
* Le reporting

<http://www-igm.univ-mlv.fr/~dr/XPOSE2004/nchaveron/images/Architecture.png>

Les plugin sont des programmes exécutables ou des scripts (perl, shell, etc..) qui peuvent être lancés depuis une ligne de commande pour tester un hôte ou un service.  
Le résultat de l'exécution d'un plugin est utilisé par Nagios pour déterminer le statut des hôtes ou des services sur le réseau.

Le développement des plugins pour Nagios est fait sur SourceForge. La page du projet de développement de plugins pour Nagios (où vous trouverez toujours la dernière version des plugins) se trouve à [http://sourceforge.net/projects/nagiosplug/](http://sourceforge.net/projects/netsaintplug/)

Les plugins développés pour Nagios doivent respecter un certain format d'affichage de retour afin de garantir leur intégration. Tous les plugins qui respectent les consignes minimales de développement pour ce projet contiennent une documentation interne. Cette documentation peut être affichée en exécutant le plugin avec le paramétre "-h" ("--help" si les paramétres longs sont activés).

Par exemple, si vous voulez savoir comment fonctionne le plugin check\_http ou quels paramétres il accepte, vous devez saisir :

#### Pré-requis

Nagios a, en plus des plugins, besoin de satisfaire un certain nombre de dépendances.

Les pré-requis à l'installation sont les suivants :

* Un serveur web (ex: Apache)
* Une base de données (si utilisée)
* Les librairies graphiques suivantes : libgd 1.6.3 ou plus, libjpeg, libpng

#### Création d'un utilisateur nagios

Avant même d'installer Nagios, la première chose à faire est de créer un utilisateur pour Nagios, ainsi que son groupe

# groupadd nagios

# useradd -g nagios -m -d /home/nagios -G apache nagios

## **Protocoles**

Les protocoles par défaut utilisés par Nagios sont indiqués sous -

* http(s), ports 80 et 443 − Les interfaces du produit sont basées sur le Web dans Nagios. Les agents Nagios peuvent utiliser http pour déplacer des données.
* snmp, ports 161 et 162 - snmp est une partie importante de la surveillance du réseau. Le port 161 est utilisé pour envoyer des requêtes aux nœuds et le poste 162 est utilisé pour recevoir les résultats.
* ssh, port 22 - Nagios est conçu pour fonctionner nativement sur CentOS ou RHEL Linux. L'administrateur peut se connecter à Nagios via SSH chaque fois qu'il le souhaite et effectuer des vérifications.