

TUTORIEL PRATIQUE

BTS SIO SISR – 2ème année

SUPERVISION RÉSEAU AVEC NAGIOS CORE SUR DEBIAN 13

Installation, configuration des hôtes, des services et des alertes e-mail

POINTS CLÉS DU TUTORIEL

- ✓ Compilation et installation de Nagios Core depuis les sources
- ✓ Installation des Nagios Plugins (checks standards)
- ✓ Configuration de l'interface web Nagios (Apache + authentification)
- ✓ Déclaration et supervision d'hôtes Linux avec NRPE
- ✓ Supervision d'équipements réseau via SNMP (switch, routeur)
- ✓ Configuration des alertes par e-mail (notifications)

Utilisation commerciale interdite – 03/2026 © <https://tutos-info.fr>

Prérequis : Ce tutoriel nécessite une machine Debian 13 (Trixie) fonctionnelle avec accès internet. L'installation de Nagios Core se fait depuis les sources (compilation). Un accès SSH est fortement recommandé. Prévoyez 30 à 45 minutes pour l'installation complète.

Tutoriel généré par IA

1 – PRÉSENTATION DE NAGIOS CORE

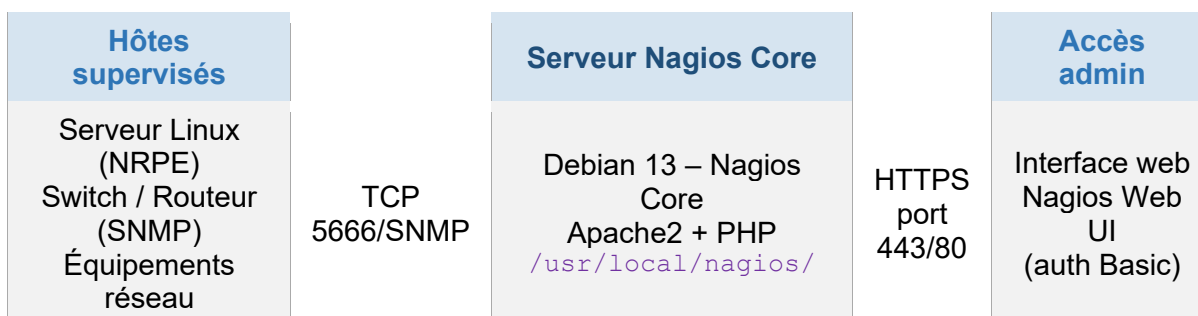
Nagios Core est une solution de supervision réseau et système **open source**, de référence dans le monde de l'administration système. Elle permet de surveiller en temps réel l'état des hôtes (serveurs, équipements réseau) et des services (HTTP, SSH, SMTP, disque, CPU, RAM...) et d'envoyer des **alertes** en cas de problème détecté.

Nagios Core fonctionne sur un modèle **actif** : le serveur Nagios interroge régulièrement les hôtes et services selon une planification définie. En cas d'anomalie, il passe par un système d'états :

État hôte	État service	Signification
UP	OK	Hôte ou service fonctionnel
DOWN	WARNING	Hôte inaccessible / Service en limite haute
UNREACHABLE	CRITICAL	Hôte injoignable / Service en état critique
–	UNKNOWN	Résultat du check indéterminé (plugin défaillant)

Architecture mise en place

Voici l'architecture que nous allons déployer :



2 – INSTALLATION DE NAGIOS CORE SUR DEBIAN 13

Nagios Core n'est pas disponible dans les dépôts officiels Debian. Il doit être **compilé depuis les sources**. Suivez scrupuleusement les étapes ci-dessous.

2.1 – Installation des dépendances

- Connectez-vous en SSH à votre serveur Debian 13 et mettez à jour le système :

```
sudo apt update && sudo apt upgrade -y
```

- Installez toutes les dépendances nécessaires à la compilation et à l'interface web :

```
sudo apt install -y build-essential libgd-dev openssl libssl-dev unzip wget  
apache2 php libapache2-mod-php php-gd
```

- Activez le module CGI d'Apache (nécessaire pour l'interface web Nagios) :

```
sudo a2enmod cgi
sudo systemctl restart apache2
```

2.2 – Création de l'utilisateur Nagios

- Créez l'utilisateur système `nagios` et son groupe :

```
sudo useradd --system --no-create-home --shell /sbin/nologin nagios
sudo groupadd nagcmd
sudo usermod -aG nagcmd nagios
sudo usermod -aG nagcmd www-data
```

2.3 – Téléchargement et compilation de Nagios Core

- Téléchargez la dernière version stable de Nagios Core (vérifiez la version sur nagios.org) :

```
cd /tmp
wget
https://github.com/NagiosEnterprises/nagioscore/releases/download/nagios-4.5.3/nagios-4.5.3.tar.gz
tar xzf nagios-4.5.3.tar.gz
cd nagios-4.5.3
```

- Lancez la configuration de la compilation :

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

- Compilez et installez Nagios Core :

```
sudo make all
sudo make install-groups-users # crée les utilisateurs/groupes nagios
sudo make install # installe les binaires dans /usr/local/nagios/
sudo make install-daemoninit # crée le service systemd
sudo make install-commandmode # configure les permissions du répertoire de commandes
sudo make install-config # installe les fichiers de configuration exemples
sudo make install-webconf # installe la configuration Apache de Nagios
```

Note : La compilation prend quelques minutes. Si une erreur apparaît, vérifiez que toutes les dépendances ont bien été installées à l'étape 2.1.

2.4 – Création du compte administrateur web

- Créez le fichier de mots de passe Apache et ajoutez l'utilisateur **nagiosadmin** :

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

Saisissez et confirmez un mot de passe robuste lorsque demandé.

- Activez la configuration Apache de Nagios et redémarrez Apache :

```
sudo a2enconf nagios
sudo systemctl reload apache2
```

2.5 – Installation des Nagios Plugins

Les **Nagios Plugins** fournissent les scripts de vérification (**check_ping**, **check_http**, **check_disk**...). Ils doivent être installés séparément.

- Téléchargez et compilez les plugins :

```
cd /tmp
wget https://github.com/nagios-plugins/nagios-
plugins/releases/download/release-2.4.11/nagios-plugins-2.4.11.tar.gz
tar xzf nagios-plugins-2.4.11.tar.gz
cd nagios-plugins-2.4.11
sudo ./configure --with-nagios-user=nagios --with-nagios-group=nagios
sudo make && sudo make install
```

2.6 – Démarrage et vérification de Nagios

- Vérifiez la syntaxe des fichiers de configuration avant de démarrer :

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

- Activez et démarrez le service Nagios :

```
sudo systemctl enable --now nagios
sudo systemctl status nagios
```

- Accédez à l'interface web depuis votre navigateur :

```
http://ip_du_serveur/nagios
```

Connectez-vous avec l'identifiant **nagiosadmin** et le mot de passe défini précédemment.

Info : L'interface web affiche par défaut uniquement le localhost (le serveur Nagios lui-même). Les sections suivantes expliquent comment ajouter des hôtes à superviser.

3 – ORGANISATION DES FICHIERS DE CONFIGURATION

Nagios Core utilise une arborescence de fichiers de configuration texte situés dans `/usr/local/nagios/etc/`. Il est recommandé de créer un répertoire dédié aux hôtes et services personnalisés.

- Créez un répertoire pour vos fichiers de configuration personnalisés :

```
sudo mkdir /usr/local/nagios/etc/servers
```

- Déclarez ce répertoire dans le fichier de configuration principal de Nagios :

```
sudo nano /usr/local/nagios/etc/nagios.cfg
```

Recherchez la ligne `cfg_file=...` et ajoutez en-dessous :

```
cfg_dir=/usr/local/nagios/etc/servers
```

Voici un aperçu de l'arborescence des principaux fichiers de configuration :

Fichier / Répertoire	Rôle
<code>nagios.cfg</code>	Fichier principal – paramètres globaux, chemins, intervalles
<code>objects/contacts.cfg</code>	Définition des contacts (adresse e-mail des administrateurs)
<code>objects/commands.cfg</code>	Déclaration des commandes de check (check_ping, check_http...)
<code>objects/templates.cfg</code>	Modèles réutilisables d'hôtes et de services
<code>objects/localhost.cfg</code>	Configuration de supervision du serveur Nagios lui-même
<code>servers/*.cfg</code>	Vos fichiers personnalisés : un fichier .cfg par hôte ou groupe d'hôtes

4 – SUPERVISION D'UN HÔTE LINUX AVEC NRPE

NRPE (Nagios Remote Plugin Executor) est un agent léger installé sur les machines Linux à superviser. Il permet à Nagios d'exécuter des plugins **à distance** pour vérifier des métriques locales : charge CPU, utilisation disque, RAM, processus actifs, etc.

4.1 – Installation de NRPE sur la machine cliente Linux

Connectez-vous en SSH sur la **machine Linux à superviser** (ex. : **10.10.10.71**) :

- Installez NRPE et les plugins Nagios sur le client :

```
sudo apt update
sudo apt install -y nagios-nrpe-server nagios-plugins
```

- Autorisez le serveur Nagios à interroger le client en modifiant la configuration NRPE :

```
sudo nano /etc/nagios/nrpe.cfg
```

Recherchez la directive **allowed_hosts** et ajoutez l'adresse IP du serveur Nagios :

```
# Adresses IP autorisées à interroger ce client NRPE
allowed_hosts=127.0.0.1,10.10.10.60
```

- Redémarrez le service NRPE sur le client :

```
sudo systemctl enable --now nagios-nrpe-server
sudo systemctl status nagios-nrpe-server
```

- Vérifiez que le port NRPE (TCP 5666) est bien en écoute :

```
ss -tlnp | grep 5666
```

Attention : Si un pare-feu est actif sur le client, autorisez le port TCP 5666 en entrée depuis l'adresse IP du serveur Nagios : `sudo ufw allow from 10.10.10.60 to any port 5666`

4.2 – Installation du plugin check_nrpe sur le serveur Nagios

De retour sur le **serveur Nagios**, installez le plugin **check_nrpe** qui permet d'interroger les agents NRPE distants :

```
sudo apt install -y nagios-nrpe-plugin
```

- Testez la communication avec le client depuis le serveur Nagios :

```
/usr/lib/nagios/plugins/check_nrpe -H 10.10.10.71 # doit afficher la
version NRPE du client
```

4.3 – Déclaration de l'hôte Linux dans Nagios

- Sur le serveur Nagios, créez un fichier de configuration dédié au client Linux :

```
sudo nano /usr/local/nagios/etc/servers/debian-client.cfg
```

- Saisissez la configuration suivante (adaptez l'IP, le nom et l'alias) :

```
# — Définition de l'hôte —
define host {
    use                linux-server
    host_name          debian-client
    alias              Serveur Debian Client
    address            10.10.10.71
    max_check_attempts 3
    check_period       24x7
    notification_interval 30
    notification_period 24x7
}

# — Services surveillés via NRPE —
define service {
    use                generic-service
    host_name          debian-client
    service_description Charge CPU
    check_command       check_nrpe!check_load
}

define service {
    use                generic-service
    host_name          debian-client
    service_description Espace disque /
    check_command       check_nrpe!check_disk
}

define service {
    use                generic-service
    host_name          debian-client
    service_description Mémoire RAM
    check_command       check_nrpe!check_mem
}

define service {
    use                generic-service
    host_name          debian-client
    service_description Processus SSH
    check_command       check_nrpe!check_procs
}
```

- Vérifiez la syntaxe et rechargez Nagios :

```
sudo /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg
sudo systemctl reload nagios
```

Info : Après le rechargement, le nouvel hôte apparaît dans l'interface web sous Hosts. Attendez quelques minutes que les premiers checks s'exécutent.

5 – SUPERVISION D'ÉQUIPEMENTS RÉSEAU VIA SNMP

Le protocole **SNMP** (Simple Network Management Protocol) permet de superviser des équipements réseau (switches, routeurs, imprimantes) qui ne peuvent pas exécuter d'agent NRPE. Nagios interroge les équipements en leur envoyant des requêtes SNMP sur le **port UDP 161**.

5.1 – Installation des outils SNMP sur le serveur Nagios

- Installez les outils SNMP et le plugin Nagios correspondant :

```
sudo apt install -y snmp snmpd libnet-snmp-perl nagios-snmp-plugins
```

- Testez une requête SNMP vers un équipement (remplacez l'IP et la communauté) :

```
snmpwalk -v2c -c public 10.10.10.1 system # remplacez 'public' par votre communauté SNMP
```

5.2 – Configuration SNMP sur les équipements Cisco

Sur un équipement Cisco IOS, activez SNMP v2c avec une communauté en lecture seule :

```
Router# configure terminal
Router(config)# snmp-server community public RO
Router(config)# snmp-server location Salle-Reseau
Router(config)# snmp-server contact admin@domaine.fr
Router(config)# end
Router# write memory
```

Sécurité : Pour la sécurité, remplacez la communauté 'public' par une chaîne complexe et limitez les accès SNMP à l'adresse IP du serveur Nagios avec une ACL : `snmp-server community MON_SECRET RO ACCESS_LIST_NUMBER`

5.3 – Déclaration d'un équipement réseau dans Nagios

- Créez un fichier de configuration pour le switch ou le routeur à superviser :

```
sudo nano /usr/local/nagios/etc/servers/cisco-switch.cfg
```

- Saisissez la configuration suivante :

```
# — Définition de l'hôte (switch Cisco) —
define host {
    use                generic-host
    host_name          cisco-switch-01
    alias              Switch Cisco Salle Reseau
    address             10.10.10.1
    max_check_attempts 3
    check_period        24x7
    notification_interval 30
    notification_period 24x7
    check_command       check-host-alive
}

# — Supervision SNMP —
define service {
    use                generic-service
    host_name          cisco-switch-01
    service_description SNMP - Statut
    check_command       check_snmp!-C public -o sysDescr.0
}

define service {
    use                generic-service
    host_name          cisco-switch-01
    service_description SNMP - Charge CPU
    check_command       check_snmp!-C public -o cpmCPUTotal5min.1 -
w 80 -c 95
}

define service {
    use                generic-service
    host_name          cisco-switch-01
    service_description Ping
    check_command       check_ping!100.0,20%!500.0,60%
}
```

- Vérifiez la syntaxe et rechargez Nagios :

```
sudo /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg
sudo systemctl reload nagios
```

6 – CONFIGURATION DES NOTIFICATIONS PAR E-MAIL

Nagios Core peut envoyer des **alertes par e-mail** lorsqu'un hôte ou un service change d'état. Cette fonctionnalité repose sur un agent de messagerie installé sur le serveur.

6.1 – Installation de l'agent de messagerie

- Installez **mailutils** et **msmtp** pour l'envoi d'e-mails via un serveur SMTP externe (Gmail, OVH, etc.) :

```
sudo apt install -y mailutils msmtp msmtp-mta
```

- Créez le fichier de configuration msmtp (remplacez les valeurs par celles de votre compte SMTP) :

```
sudo nano /etc/msmtprc
```

```
# — Configuration msmtp (compte Gmail en exemple) —————
defaults
auth            on
tls             on
tls_trust_file  /etc/ssl/certs/ca-certificates.crt
logfile         /var/log/msmtp.log

account         gmail
host            smtp.gmail.com
port           587
from            votre.adresse@gmail.com
user            votre.adresse@gmail.com
password        votre_mot_de_passe_application

account default : gmail
```

- Définissez les permissions du fichier (il contient un mot de passe) :

```
sudo chmod 600 /etc/msmtprc
```

- Testez l'envoi d'un e-mail :

```
echo "Test Nagios" | mail -s "Test envoi e-mail" votre.adresse@gmail.com
```

Gmail : Pour Gmail, vous devez créer un mot de passe d'application dans les paramètres de sécurité de votre compte Google (authentification à deux facteurs requise). N'utilisez pas votre mot de passe principal.

6.2 – Configuration du contact Nagios

- Ouvrez le fichier des contacts Nagios :

```
sudo nano /usr/local/nagios/etc/objects/contacts.cfg
```

- Modifiez l'adresse e-mail du contact `nagiosadmin` :

```
define contact {
    contact_name      nagiosadmin
    use                generic-contact
    alias              Nagios Admin
    email              votre.adresse@gmail.com
}
```

- Vérifiez la configuration et rechargez Nagios :

```
sudo /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg
sudo systemctl reload nagios
```

6.3 – Test d'une notification depuis l'interface web

- Dans l'interface web Nagios, naviguez vers **Services** et cliquez sur un service supervisé.
- Cliquez sur « **Send custom service notification** » dans le menu de gauche.
- Saisissez un commentaire et validez. Vous devriez recevoir un e-mail de notification dans les instants qui suivent.

Info : Par défaut, Nagios n'envoie des notifications que lorsqu'un état passe de OK à WARNING ou CRITICAL, et lors du retour à la normale. La fréquence et les conditions de notification sont configurables dans `templates.cfg`.

7 – UTILISATION DE L'INTERFACE WEB NAGIOS

L'interface web de Nagios Core propose un tableau de bord complet pour superviser l'ensemble de votre infrastructure. Voici les menus principaux :

Menu	Fonction
Tactical Overview	Tableau de bord global : nombre d'hôtes et services OK / WARNING / CRITICAL
Hosts	Liste de tous les hôtes supervisés avec leur état actuel
Services	Liste de tous les services avec état, durée et dernier résultat du check
Host Groups	Vue groupée des hôtes par catégorie (serveurs Linux, équipements réseau...)
Problems	Vue filtrée : uniquement les hôtes et services en état anormal
Reports → Availability	Calcul automatique du taux de disponibilité (SLA) sur une période donnée
Configuration	Visualisation des objets de configuration (hôtes, services, contacts, commandes)

Commandes utiles de gestion du service Nagios

Commande	Action
<code>sudo systemctl status nagios</code>	Vérifier l'état du service Nagios
<code>sudo systemctl reload nagios</code>	Recharger la configuration sans interrompre la supervision
<code>sudo systemctl restart nagios</code>	Redémarrer Nagios complètement
<code>nagios -v nagios.cfg</code>	Vérifier la syntaxe des fichiers de configuration
<code>tail -f /usr/local/nagios/var/nagios.log</code>	Suivre le journal Nagios en temps réel

CONCLUSION

Nagios Core est un outil de supervision incontournable dans le monde de l'administration système et réseau. Sa **flexibilité**, sa **légèreté** et son **écosystème de plugins** extrêmement riche en font une solution de référence, aussi bien dans les petites infrastructures que dans les environnements d'entreprise.

À travers ce tutoriel, vous avez mis en place une supervision complète : serveur Nagios Core compilé depuis les sources, agents NRPE sur les machines Linux, requêtes SNMP vers les équipements réseau, et envoi d'alertes par e-mail. Ces compétences correspondent directement aux attendus du **BTS SIO SISR Bloc 3** en matière de supervision et d'exploitation des infrastructures réseau.

Documentation officielle Nagios Core : <https://www.nagios.org/documentation/>

Bibliothèque de plugins : <https://exchange.nagios.org/>