

MOUSLIM ATTALAOUI

PAPPE NAGIOS XI

Installation, configuration et amélioration de Nagios XI

Sommaire

Qu'est-ce que NagiosXI ?	3
Introduction	3
Contexte	3
Installations et configurations de NAGIOS XI	4
Supervision du serveur GLPI (debian 12)	9
Ajout du serveur Debian dans Nagios XI	10
Supervision du contrôleur de domaine AD :	13
Ajout du serveur Windows (AD) sur NAGIOS XI	17
Supervision du DNS	20
Installation et configurations de FAIL2BAN	23
Conclusion	25

Qu'est-ce que NagiosXI ?

NagiosXI est une solution de supervision informatique avancée qui permet de surveiller les performances, la disponibilité et la santé des infrastructures IT. Il s'agit d'une version commerciale améliorée de Nagios Core, qui offre une interface utilisateur graphique (GUI) plus intuitive et de nombreuses fonctionnalités supplémentaires.

Principales fonctionnalités de NagiosXI :

- Surveillance des systèmes et des réseaux : Permet de suivre les serveurs, les services et les périphériques réseau en temps réel.
- Alertes et notifications : Envoie des alertes en cas de problème ou de dépassement de seuil critique.
- Rapports et tableaux de bord : Fournit des analyses détaillées sur les performances des équipements.
- Extensibilité : Compatible avec de nombreux plugins et modules complémentaires.
- Gestion des utilisateurs : Permet de créer des rôles et d'attribuer des droits spécifiques aux administrateurs et aux utilisateurs.

Introduction

Dans le cadre de ce projet, nous allons mettre en place NagiosXI sur un serveur Debian 12 afin de superviser notre infrastructure informatique. La surveillance des ressources est un élément clé pour garantir la disponibilité et la performance des services.

Nous allons également intégrer NCPA (Nagios Cross-Platform Agent) pour une supervision efficace des machines distantes et Fail2Ban pour renforcer la sécurité en bloquant automatiquement les tentatives de connexion suspectes.

Ce document détaille l'installation, la configuration et les améliorations apportées à NagiosXI afin de mieux répondre aux besoins de supervision et de sécurité dans un environnement Linux.

Contexte

Dans un environnement informatique en constante évolution, il est crucial de disposer d'un système de supervision robuste pour surveiller les serveurs, détecter les anomalies et prévenir les pannes avant qu'elles ne deviennent critiques.

Nous avons choisi NagiosXI pour plusieurs raisons :

- Son interface utilisateur complète et intuitive.
- La possibilité de surveiller un large éventail de services et de protocoles (HTTP, SSH, DNS, DHCP etc.).
- Sa compatibilité avec Debian 12, bien que nécessitant certaines adaptations spécifiques.

Cependant, la mise en place d'un tel système implique des défis :

- Configuration des agents de supervision : Nous utiliserons NCPA pour faciliter la collecte de données sur les machines surveillées.

- Sécurisation des accès : La supervision expose le serveur à des risques. Fail2Ban sera utilisé pour protéger le système contre les tentatives d'intrusion.
- Optimisation des performances : Un bon paramétrage est essentiel pour éviter les surcharges inutiles du serveur NagiosXI.

Installations et configurations de NAGIOS XI

Prérequis

Ouvrir votre session et mettre à jour les paquets.

```
login as: root
root@172.16.1.11's password:
Linux nagios 6.1.0-32-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.129-1 (2025-03-06)
x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have new mail.
Last login: Tue Mar 18 14:17:05 2025 from 172.16.1.7
root@nagios:~# apt update && apt upgrade
```

Installer les outils suivants.

```
root@nagios:~# apt install ssh
```

```
root@nagios:~# apt install apache2
```

```
root@nagios:~# apt install php
```

Installation Nagios XI

Ensuite créer un répertoire :

```
# mkdir /opt/nagios
```

Entrer dans le répertoire :

```
# cd /opt/nagios
```

Télécharger nagios XI :

```
# wget https://assets.nagios.com/downloads/nagiosxi/xi-latest.tar.gz
```

```
root@nagios:~# cd /opt/nagios
root@nagios:/opt/nagios# ls
xi-latest.tar.gz
root@nagios:/opt/nagios#
```

Ensuite Décompresser l'archive :

```
# tar -xvzf xi-latest.tar.gz
```

Vérifier dans le dossier avec ls :

```
root@nagios:~# cd /opt/nagios
root@nagios:/opt/nagios# ls
nagiosxi  xi-latest.tar.gz
root@nagios:/opt/nagios#
```

Entrer dans le répertoire nagiosxi :

```
# cd nagiosxi
```

Lancer le script d'installation :

```
# ./fullinstall « Y » pour continuer
```

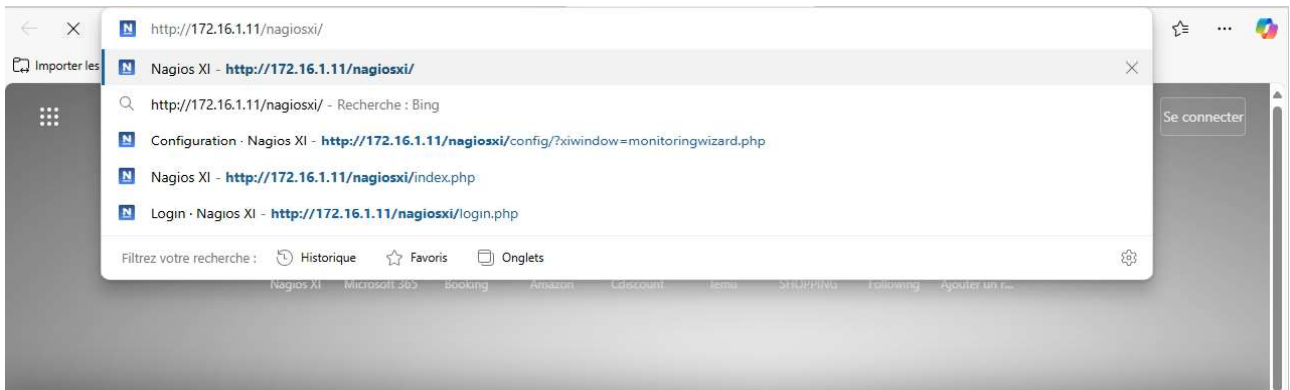
```
root@nagios:/opt/nagios# cd nagiosxi
root@nagios:/opt/nagios/nagiosxi# ./fullinstall
```

```
IMPORTANT: This script should only be used on a 'clean' install of CentOS, RHEL, Ubuntu LTS,
Debian, or Oracle. Do NOT use this on a system that has been tasked with other purposes or has
an existing install of Nagios Core. To create such a clean install you should have selected
only the base package in the OS installer.
Do you want to continue? [Y/n] y_
```

Laisser l'installations s'exécuter cela peut prendre plus de dix minutes.

```
Nagios XI Installation Complete!
-----
You can access the Nagios XI web interface by visiting:
  http://172.16.1.11/nagiosxi/
root@nagios:/opt/nagios/nagiosxi#
```

Pour finir votre installation, vous devez avoir accès à l'interface web, comme indiquez ci-dessus vous pouvez avoir accès au site a : <http://172.16.1.11/nagiosxi/> .



Entrer les paramètres suivants :

Nagios XI Installation

Finalize your Nagios XI installation and step the initial configuration. These settings can be changed later.

General System Settings

Program URL	<input type="text" value="http://[redacted]/nagiosxi/"/>
Timezone	<input type="text" value="(UTC+01:00) Paris"/>
Language	<input type="text" value="French (Français)"/>
User Interface Theme	<input type="text" value="Modern Dark"/>
	<input type="checkbox"/> Use HTTPS only (all HTTP requests will be redirected to HTTPS)

Entrer votre bonne IP dans le program url.

License Settings

License Type	<input type="radio"/> Trial <input type="radio"/> Licensed <input checked="" type="radio"/> Free (Limited)
	Free license is limited to 7 nodes and up to a total of 100 host/service checks. This option is self-supported only.

Next >

Nous allons utiliser la version free

Admin Account Settings

Username	<input type="text" value="nagiosadmin"/>
Password	<input type="password" value="nagiosadmin"/>
Full Name	<input type="text" value="Nagios Administrator"/>
Email Address	<input type="text" value="root@localhost"/>

Admin Notification Settings

Send this account email notifications [Advanced email notification settings](#)

[< Back](#) [✔ Finish Install](#)

Nous allons configurer l'identifiant et le mot de passe, moi j'utiliserais "nagiosadmin", nous finirons l'installations avec "finish install".

⋮ installation de finition ...



Cliquer sur « Se connecter à nagios xi » pour être rediriger vers la page d'administration.

Installation terminée

toutes nos félicitations! vous avez installé avec succès nagios xi. vous pouvez maintenant vous connecter à nagios xi en utilisant les informations d'identification suivantes.

Nom d'utilisateur	<input type="text" value="nagiosadmin"/>
Mot de passe	<input type="password" value="nagiosadmin"/>

[se connecter à nagios xi >](#)

Entrer vos informations de connexion .

Login

<input type="text" value="nagiosadmin"/>
<input type="password" value="....."/>
Login
Mot de passe oublié?

Accepter le contrat.

Contrat de licence

Vous devez accepter les conditions de licence du logiciel Nagios et conditions avant de poursuivre l'utilisation de ce logiciel.

Nagios Software License Terms and Conditions

PLEASE READ THIS AGREEMENT CAREFULLY BEFORE PURCHASING OR USING NAGIOS SOFTWARE. BY PURCHASING OR USING NAGIOS ENTERPRISES' SOFTWARE, YOU SIGNIFY YOUR ASSENT TO THIS AGREEMENT. IF YOU ARE ACTING ON BEHALF OF AN ENTITY, THEN YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO ENTER INTO THIS AGREEMENT ON BEHALF OF THAT ENTITY. IF YOU DO NOT ACCEPT THE TERMS OF THIS AGREEMENT, THEN YOU MUST NOT PURCHASE OR USE NAGIOS SOFTWARE.

This Software License Terms and Conditions Agreement ("Agreement") is a legal agreement between Nagios Enterprises, LLC ("Nagios Enterprises") and the purchaser or user of Nagios Software ("Customer"). The effective date of this Agreement ("Effective Date") is the earlier of the date that Customer signs or accepts this Agreement or the date that Customer purchases or begins using Nagios Software.

1 DEFINITIONS

For the purposes of this Agreement, the following terms shall have the following meanings:

1.1 Nagios Software. All commercial and proprietary software programs, configurations, scripts, images, and intellectual property contained in Nagios Enterprises' commercial products and developed by, owned by, or licensed to Nagios Enterprises, with the exclusion of Third Party Software.

1.2 Third Party Software. Any software programs, configurations, scripts, images, and intellectual property contained in or distributed with Nagios Enterprises' products, with the exclusion of Nagios Software, made available in source code, object code form, or other

J'ai lu, compris et accepté d'être lié par les termes de la licence ci-dessus.

[Soumettre](#)

Le serveur est enfin prêt.

Nagios XI [Maison](#) [Vues](#) [Tableaux de bord](#) [Rapports](#) [Configurer](#) [Outils](#) [Aider](#) [Admin](#)

mise à niveau vers une version sous licence de nagios xi et obtenir le soutien et la mise à niveau des prestations.

Accueil Dashboard

Vue Rapide

- Accueil Dashboard
- Aperçu tactique
- Birdseye
- Centre des opérations
- Écran opérations
- Ouvrez problèmes de service
- Ouvrez les problèmes d'accueil
- Tous les problèmes de service
- Tous les problèmes d'accueil
- Pannes de réseau

Détails

- État du service
- Statut d'accueil
- Résumé hostgroup
- Vue d'ensemble du groupe d'hôtes
- Grille hostgroup
- Résumé servicegroup
- Servicegroup Aperçu
- Servicegroup Grille
- BPI
- Métrique

Graphiques

- Graphiques sur le rendement

Guide de démarrage

Tâches courantes:

- [Modifiez vos paramètres de compte](#)
Changez votre mot de passe et les préférences générales.
- [Modifiez vos paramètres de notification](#)
Changez comment et quand vous recevez des notifications d'alerte.
- [Configurez votre installation de surveillance](#)
Ajouter ou modifier des éléments à surveiller avec facile-à-utiliser des assistants.

Mise en route:

- [Renseignez-vous sur XI](#)
En savoir plus sur XI et de ses capacités.
- [Inscrivez-vous pour les nouvelles XI](#)
Restez informé des dernières mises à jour et des événements pour les XI.

Résumé de l'état d'accueil

Jusqu'à	Vers le bas	Inaccessible	En attendant
1	0	0	0
Non prise en charge		Problèmes	All
0		0	1

Dernière mise à jour: 2022-04-09 14:33:19

Résumé de l'état de service

Bien	Avertissement	Inconnu	Critique	En attendant
12	0	0	0	0
Non prise en charge		Problèmes		All
0		0		12

Dernière mise à jour: 2022-04-09 14:33:19

En cliquant sur « Détails » puis « Etat du service » vous pouvez voir l'état de service de votre serveur nagios (localhost).

Tous les problèmes de service
Tous les problèmes d'accueil
Pannes du réseau

Détails

État du service
Statut d'accueil
Résumé hostgroup
Vue d'ensemble du groupe d'hôtes
Grille hostgroup
Résumé servicegroup
Servicegroup Aperçu
Servicegroup Grille

BPI
Métrique

Graphiques

Graphiques sur le rendement
Graphique Explorateur

Cartes

World Map

Projection 1-12 de 12 nombre total d'enregistrements

Hôte	Service	Statut	Durée	Tentative
localhost	Current Load	Bien	21m 14s	1/4
	Current Users	Bien	20m 49s	1/4
	HTTP	Bien	20m 24s	1/4
	Memory Usage	Bien	19m 59s	1/4
	PING	Bien	19m 34s	1/4
	Root Partition	Bien	19m 9s	1/4
	SSH	Bien	18m 44s	1/4
	Service Status - crond	Bien	18m 19s	1/4
	Service Status - httpd	Bien	17m 54s	1/4
	Service Status - mysqld	Bien	17m 29s	1/4
	Swap Usage	Bien	16m 58s	1/4
	Total Processes	Bien	16m 43s	1/4

Dernière mise à jour: 2022-04-09 14:34:29

Supervision du serveur GLPI (debian 12)

Sur la machine à supervisé nous appliquer les prérequis :

```
# apt update
# apt upgrade
# apt install ssh
```

Nous allons utiliser NCPA pour faire remonter les informations au serveur, pour cela nous allons l'installer avec ce lien : <https://www.nagios.org/ncpa/#downloads>



Bien choisir la version debian 9+.

Une fois télécharger nous allons le transférer via winscp, dans un le repertoire de notre de choix.

```
root@debian:~# cd /home
root@debian:/home# ls
rootel
root@debian:/home# cd rootel
root@debian:/home/rootel# ls
ncpa-latest-1.amd64.deb
root@debian:/home/rootel#
```

Se positionner dans le répertoire où est stocké le fichier puis saisir la commande suivante :
dpkg -i ncpa-latest-1.amd64.deb

```
root@debian:/home/rootel# dpkg -i ncpa-latest-1.amd64.deb
root@debian:/home/rootel# dpkg -i ncpa-latest-1.amd64.deb
(Lecture de la base de données... 37154 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de ncpa-latest-1.amd64.deb ...
Try to stop services with systemctl
Try to stop services with service
Dépaquetage de ncpa (3.1.1-1) sur (3.1.1-1) ...
Paramétrage de ncpa (3.1.1-1) ...
Traitement des actions différées (« triggers ») pour libc-bin (2.36-9+deb12u9)
..
root@debian:/home/rootel#
```

Nous allons modifier le fichier de configurations pour ajouter un mot de passe (token):
nano /usr/local/ncpa/etc/ncpa.cfg

```
#
[api]
#
# The token that will be used to log into the basic web GUI (API browser, graph
# and to authenticate requests to the API and requests through check_ncpa.py
#
community_string = nagios
#
# -----
# Passive Configuration (daemon)
# -----
[passive]
#
# Handlers are a comma separated list of what you would like the passive agent
# Default: None
```

Aller à la section [api] puis modifier ce qu'il contient avec ce qu'il y'a au-dessus.
Puis redémarrer le service :
service ncpa restart

Ajout du serveur Debian dans Nagios XI

Pour ajouter le serveur Debian à superviser dans Nagios XI, accédez à l'interface d'administration de Nagios. Ensuite, rendez-vous dans le menu "Configurer", puis sélectionnez "Assistants de configuration" pour commencer l'ajout du nouvel hôte.



Chercher puis cliquez ensuite sur « Linux Serveur »

Il faut maintenant entrer les paramètre suivant :

connecter à NCPA

* Adresse ⓘ
172.16.14

* Port ⓘ
5693

ne pas vérifier le certificat ssl

* jeton ⓘ Hide
nagios

* système ⓘ
Debian

[Suivant >](#)

Il faudra utiliser l'adresse IP de votre serveur à superviser, du mot de passe (token) que nous avons configuré au préalable.

Sélectionner ensuite les paramètres que vous souhaitez superviser ainsi que les valeurs.

Spécifiez les paramètres que vous souhaitez surveiller sur le serveur MSSQL.

Ping
Surveille le serveur avec un ping ICMP. Utile pour regarder la latence du réseau et une disponibilité générale.

Processus totales
Surveille le nombre total de processus en cours d'exécution sur le serveur.
nombre de processus actuel: 84
⚠ 150 ⚠ 250

Utilisation de l'UC
vérifier l'utilisation du processeur du système..
utilisation actuelle du processeur: 0 %
⚠ 20 % ⚠ 40 %
 montrer l'utilisation moyenne de cpu au lieu de par cœur cpu

compte d'utilisateur
Surveille le nombre d'utilisateurs actuellement connectés au serveur.
nombre d'utilisateurs actuel: 2
⚠ 2 # ⚠ 4 #

métriques de mémoire

unités par défaut à utiliser pour la mémoire: Gi

utilisation de la mémoire mappée
surveiller l'utilisation de la mémoire en pourcentage de la mémoire utilisée.
utilisation actuelle de la mémoire: 9.8 %
⚠ 50 % ⚠ 80 %

Swap d'utilisation
surveiller le pourcentage d'échange alloué utilisé par le système..
utilisation actuelle du swap: 0 %

Puis cliquer sur « Suivant ».

[ajouter un autre plugin check](#)

Vous pouvez ensuite modifier les paramètres de surveillance, puis cliquer sur « Terminer »

Paramètres de surveillance des

Définir les paramètres de base qui déterminent la façon dont l'hôte et de service (s) doivent être surveillés.

Dans des circonstances normales:

Surveiller l'hôte et de service (s) à chaque minutes.

Lorsqu'un problème potentiel est détecté pour la première:

Vérifiez à nouveau l'hôte et de service (s) à chaque minutes jusqu'à fois avant [envoyer une notification](#).

Nous avons fini la configuration.

Linux Server Assistant de surveillance

✓ Configuration appliquée avec succès

Vos modifications de configuration ont été appliquées avec succès à la surveillance du moteur.

Demande Configuration réussie

Autres Options:

- [Voir détails sur l'état de debian-005](#)
- [Voir les photos récentes de configuration](#)

Pour vérifier le bon état de supervision, nous allons retourner à l'accueil, puis cliquer sur "détails" et "état du service".

Centre des opérations
Écran opérations
Ouvrez problèmes de service
Ouvrez les problèmes d'accueil
Tous les problèmes de service
Tous les problèmes d'accueil
Pannes du réseau
Détails
État du service
Statut d'accueil
Résumé hostgroup
Vue d'ensemble du groupe d'hôtes
Grille hostgroup
Résumé servicegroup
Servicegroup Aperçu
Servicegroup Grille
BPI
Métrique
Graphiques

Résumé de l'état d'acc

Jusqu'à	Vers le bas	Inaccessi
4	0	0
Non prise en charge		Problème
0		0

Dernière mise à jour: 2025-03-21 11:11

Mise en route
First steps any user can perform. Click

Run a Wizard
Start monitoring quickly with easy-to-use Configuration Wizards.

Tâches administrative:
Some first steps an administrator may

Nous constatons que la machine est bien présente.

Projection 1-15 de 44 nombre total d'enregistrements

Hôte	Service	Statut	Durée	Tentative	Dernière vérification	Informations sur l'état
172.16.1.4	CPU Usage	Bien	2d 23h 2m 58s	1/5	2025-03-21 11:23:52	OK: Percent was 0.00 %
	Disk Usage on /	Bien	2d 23h 2m 36s	1/5	2025-03-21 11:24:11	OK: Used disk space was 6.00 % (Used: 2.72 GiB, Free: 42.79 GiB, Total: 47.97 GiB)
	Disk Usage on /run/credentials/systemd-sysctl.service	Bien	2d 23h 2m 7s	1/5	2025-03-21 11:24:41	OK: Used disk space was 0.00 % (Used: 0.00 GiB, Free: 0.00 GiB, Total: 0.00 GiB)
	Disk Usage on /run/credentials/ssh-agent.service	Bien	2d 23h 1m 42s	1/5	2025-03-21 11:25:06	OK: Used disk space was 0.00 % (Used: 0.00 GiB, Free: 0.00 GiB, Total: 0.00 GiB)

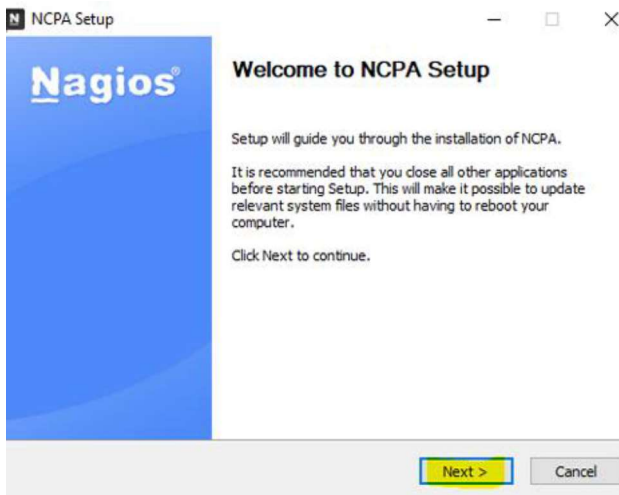
Supervision du contrôleur de domaine AD :

Comme le serveur debian, nous allons superviser le Windows server à l'aide de NCPA, télécharger NCPA pour Windows via le lien suivant : <https://www.nagios.org/ncpa/#downloads> sur votre machine à superviser.

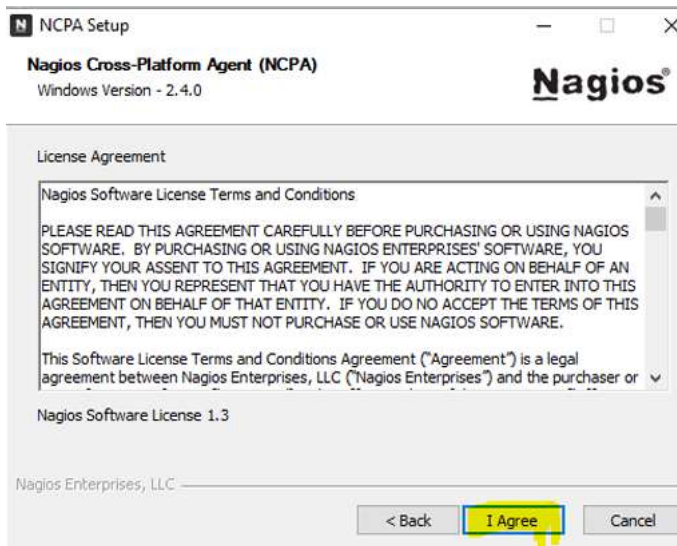


Bien choisir celui-ci.

Lancer le setup pour arriver sur cette page, puis cliquer sur Next :



Puis accepter les conditions :



Ajouter un Token, et cliquer sur Next :

N Listener Configuration — □ ×

Nagios Cross-Platform Agent (NCPA)
Windows Version - 2.4.0 **Nagios**[®]

Set configuration for API access, active checks via check_ncpa.py, and connection settings for the web GUI. These options are related to the NCPA listener service.

API Configuration

Token

The token used for API access, active checks, and logging into the web GUI.

Listener Configuration

Bind IP

Bind Port

Advanced Listener Configuration

SSL Version

Log Level

Nagios Enterprises, LLC

Ensuite passer cette étape avec Next :

N Passive Configuration — □ ×

Nagios Cross-Platform Agent (NCPA)
Windows Version - 2.4.0 **Nagios**[®]

Set configuration for the passive service. This service handles sending passive check results to Nagios via NRDP or other protocols in the future.

NRDP Configuration

Send passive checks over NRDP

URL

NRDP Token

Hostname

Advanced Passive Configuration

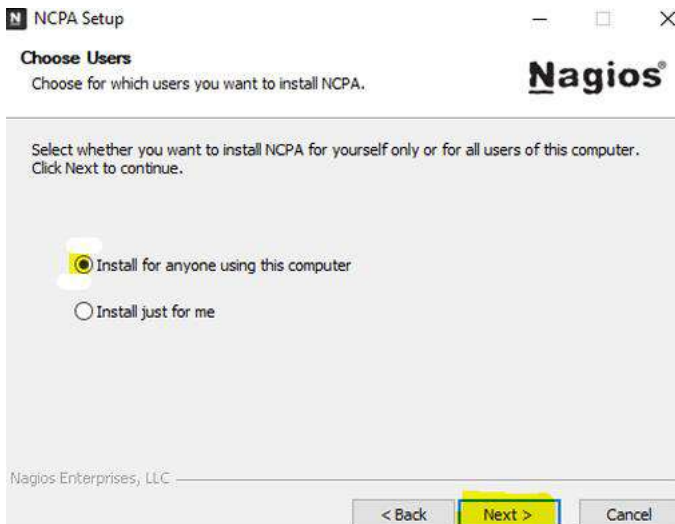
Check Interval

The default check interval in seconds. This is how often the passive checks will be sent.

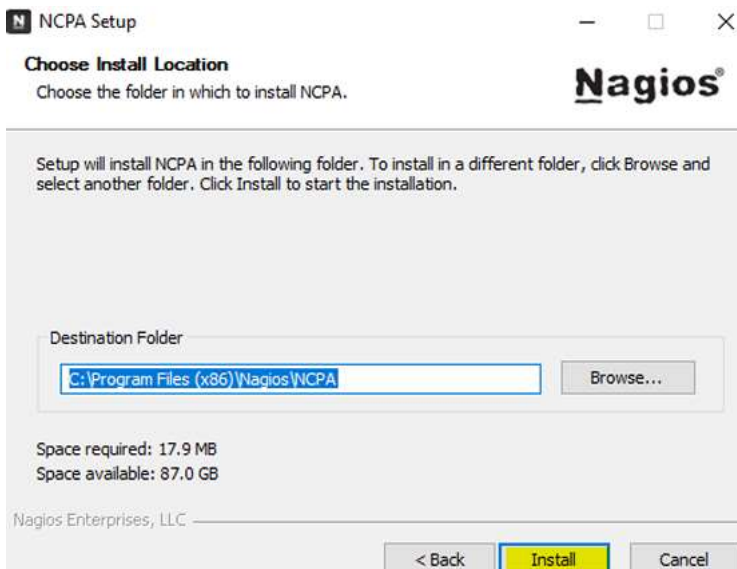
Log Level

Nagios Enterprises, LLC

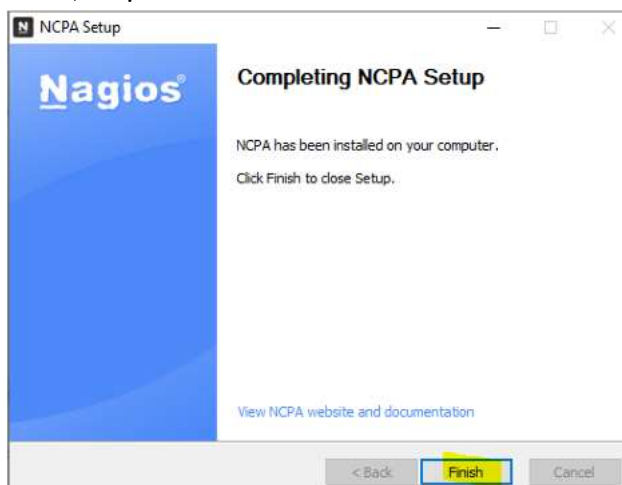
Cocher la case Install, puis cliquer sur Next :



Continuer avec Install :



Enfin, cliquer sur finish :



Ajout du serveur Windows (AD) sur NAGIOS XI

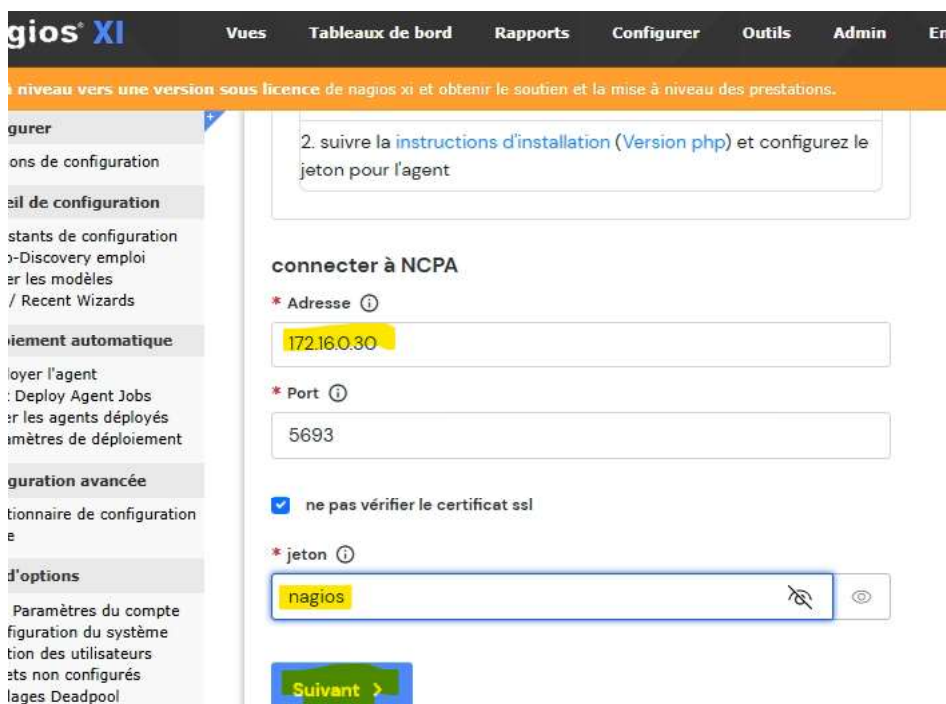
Pour ajouter le serveur Windows à superviser dans Nagios XI, accédez à l'interface d'administration de Nagios. Ensuite, rendez-vous dans le menu "Configurer", puis sélectionnez "Assistants de configuration" pour commencer l'ajout du nouvel hôte.



Choisissez ensuite Windows Server :



Vous devez maintenant ajouter l'adresse IP du server et le token configurer avant, puis cliquer sur Suivant :



Maintenant à vous de choisir les paramètres que vous voulez configurer :

Configurer


- Options de configuration
- Accueil de configuration**
- Assistants de configuration
- Auto-Discovery emploi
- Gérer les modèles
- Top / Recent Wizards
- déploiement automatique**
- déployer l'agent
- Past Deploy Agent Jobs
- gérer les agents déployés
- paramètres de déploiement
- Configuration avancée**
- Gestionnaire de configuration de base
- Plus d'options**
- Mes Paramètres du compte
- Configuration du système
- Gestion des utilisateurs
- Objets non configurés
- Réglages Deadpool

Système d'information

Adresse
172.16.0.30

Nom de l'hôte ⓘ
LABANNU.gsb.local

Port
5693

système


métriques système
Specify the metrics you'd like to monitor with the NCPA Agent.

Utilisation de l'UC ⓘ

⚠ 20 %	🔴 40 %	CPU 1.55 % ⓘ
--------	--------	--------------

montrer l'utilisation moyenne de cpu au lieu de par cœur cpu

compte d'utilisateur ⓘ

⚠ 2	🔴 4	👤 1 ⓘ
-----	-----	-------

métriques de mémoire

Puis cliquer sur suivant :

- Options de configuration
- Accueil de configuration**
- Assistants de configuration
- Auto-Discovery emploi
- Gérer les modèles
- Top / Recent Wizards
- déploiement automatique**
- déployer l'agent
- Past Deploy Agent Jobs
- gérer les agents déployés
- paramètres de déploiement
- Configuration avancée**
- Gestionnaire de configuration de base
- Plus d'options**
- Mes Paramètres du compte
- Configuration du système
- Gestion des utilisateurs
- Objets non configurés
- Réglages Deadpool

plugins

Si vous avez fourni des plugins sur le client que vous voudriez voir exécuter par ncpa, spécifiez-les :

Make your Plugin Selections ⓘ

Selected Plugins

Description du service	nom du plugin	arg

< Arrière
Suivant >

Vous pouvez maintenant cliquer sur le bouton "Finish with default" :

Assistants de configuration
 Auto-Discovery emploi
 Gérer les modèles
 Top / Recent Wizards

✓ **déploiement automatique**

- ▶ déployer l'agent
- ▶ Past Deploy Agent Jobs
- gérer les agents déployés
- ⚙️ paramètres de déploiement

✓ **Configuration avancée**

- ⚙️ Gestionnaire de configuration de base

✓ **Plus d'options**

- ⚙️ Mes Paramètres du compte
- ⚙️ Configuration du système
- ⚙️ Gestion des utilisateurs
- ⚙️ Objets non configurés
- ⚙️ Réglages Deadpool

Paramètres de surveillance des

Définir les paramètres de base qui déterminent la façon dont l'hôte et de service (s) doivent être surveillés.

Dans des circonstances normales:

Surveiller l'hôte et de service (s) à chaque procès-verbal

Lorsqu'un problème potentiel est détecté pour la première:

Vérifiez à nouveau l'hôte et de service (s) à chaque minutes jusqu'à fois avant envoyer une notification

< Arrière Suivant > **Finish with Defaults**

La configuration est terminée :



Windows Server Assistants de configuration

✓ Configuration appliquée avec succès:

- Vos modifications de configuration ont été appliquées avec succès à la surveillance du moteur.

Demande Configuration réussie

[↻ Exécuter cet Assistant à nouveau suivi](#) [↻ Exécutez un autre assistant de surveillance](#)

Autres Options:

- [Voir détails sur l'état de LABANNU.gsb.local](#)
- [Voir les photos récentes de configuration](#)

Si vous souhaitez vérifier si la machine est bien présente :

Tous les problèmes de service
 Tous les problèmes d'accueil
 Pannes du réseau

✓ **Détails**

État du service
 Statut d'accueil
 Résumé hostgroup
 Vue d'ensemble du groupe d'hôtes

Et vous pouvez constater qu'elle est bien présente :

Service	Statut	Durée	Tentative	Dernière vérification	Informations su
CPU Usage	Ok	5h 3m 24s	1/5	2025-03-26 14:29:15	OK: Percent was 0
Disk Usage on C:/	Ok	8d 0h 30m 48s	1/5	2025-03-26 14:30:44	OK: Used disk spa (GiB)
Disk Usage on D:/	Critical	8d 0h 26m 19s	5/5	2025-03-26 14:30:10	CRITICAL: Used di (4.97 GiB)
Ethernet Bandwidth - Inbound	Ok	8d 0h 29m 52s	1/5	2025-03-26 14:31:36	OK: Bytes_recv wi
Ethernet Bandwidth - Outbound	Ok	8d 0h 29m 26s	1/5	2025-03-26 14:27:15	OK: Bytes_sent wa
Memory Usage	Ok	8d 0h 28m 49s	1/5	2025-03-26 14:27:54	OK: Memory usag (GiB, Used: 2.50 G
Swap Usage	Critical	1d 1h 44m 50s	5/5	2025-03-26 14:26:51	CRITICAL: Swap u (GiB)
User Count	Ok	8d 0h 28m 5s	1/5	2025-03-26 14:28:41	OK: Count was 1 .
DHCP	Ok	8d 0h 27m 17s	1/5	2025-03-26 14:29:10	OK: Reçu 1 DHCP

Supervision du DNS

Nous allons maintenant superviser le DNS

Pour cela se rendre dans "Configurer" puis sur "Assistants de configurations" :



Puis choisir DNS :



Maintenant entre le nom de domaine du contrôleur de domaine, puis cliquer sur suivant :



Nom de domaine

* Nom de domaine complet ⓘ

LABANNU.gsb.local

Suivant >

Verifier si tout est correct puis cliquer sur suivant :

Query Information

Nom de domaine complet

LABANNU.gsb.local

Adresse IP ⓘ

172.16.0.30

Nom de l'hôte ⓘ

LABANNU.gsb.local

Options de requête DNS

Serveur DNS ⓘ

Enter DNS Server

Réponse autorité ⓘ

Services DNS Query

Résolution DNS ⓘ

Concordance IP DNS ⓘ

Réponse autorité ⓘ

Services DNS Query

Résolution DNS ⓘ

Concordance IP DNS ⓘ

< Arrière

Suivant >

Pour finir cliquer sur "Suivant" :



DNS Query Configuration Wizard

Step 3



Paramètres de surveillance des

Définir les paramètres de base qui déterminent la façon dont l'hôte et de service (s) doivent être surveillés.

Dans des circonstances normales:

Surveiller l'hôte et de service (s) à chaque procès-verbal

Lorsqu'un problème potentiel est détecté pour la première:

Vérifiez à nouveau l'hôte et de service (s) à chaque minutes jusqu'à fois avant envoyer une notification

[< Arrière](#)

[Suivant >](#)

[Finish with Defaults](#)

[Annuler](#)

La configuration est maintenant terminée :



DNS Query Assistants de configuration

✓ Configuration appliquée avec succès.

- Vos modifications de configuration ont été appliquées avec succès à la surveillance du moteur.

Demande Configuration réussie

[↻ Exécuter cet Assistant à nouveau suivi](#)

[➕ Exécutez un autre assistant de surveillance](#)

Autres Options:

- [Voir détails sur l'état de LABANNU.gsb.local](#)
- [Voir les photos récentes de configuration](#)

Nous allons maintenant vérifier s'il est bien présent :

u accueil

Tous les problèmes de service
Tous les problèmes d'accueil

🚩 Pannes du réseau

✓ **Détails**

État du service
Statut d'accueil

Résumé hostgroup
Vue d'ensemble du groupe d'hôtes

Event	Message	Time	Source	Destination	Event	Message
	DNS IP Match - LABANNU.gsb.local	Bien	20m 8s	1/5	2025-03-26 17:31:34	DNS OK: 0,027 secondes de temps de réponse . LABANNU.gsb.local returns 172.16.0.30
	DNS Resolution - LABANNU.gsb.local	Bien	19m 42s	1/5	2025-03-26 17:27:00	DNS OK: 0,028 secondes de temps de réponse . LABANNU.gsb.local returns 172.16.0.30

Il est bien présent comme on peut le voir.

Installation et configurations de FAIL2BAN

Avant de commencer, mettre à jour mon serveur : apt update && apt upgrade -y -

- Puis installe Fail2Ban : apt update && sudo apt upgrade -y

```
root@mousslim:~# apt install fail2ban -y
```

- Vérifie que Fail2Ban est bien installé et actif : systemctl status fail2ban

```
root@mousslim:~# systemctl status fail2ban
● fail2ban.service - Fail2Ban Service
   Loaded: loaded (/lib/systemd/system/fail2ban.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2025-03-04 16:49:26 CET; 2 days ago
     Docs: man:fail2ban(1)
  Main PID: 696 (fail2ban-server)
    Tasks: 3 (limit: 2280)
   Memory: 7.2M
      CPU: 2.540s
   CGroup: /system.slice/fail2ban.service
           └─696 /usr/bin/python3 /usr/bin/fail2ban-server -xf start

mars 04 16:49:26 mousslim systemd[1]: Starting Fail2Ban Service...
mars 04 16:49:26 mousslim systemd[1]: Started Fail2Ban Service.
mars 04 16:49:26 mousslim fail2ban-server[696]: Server ready
lines 1-14/14 (END)
```

- Maintenant démarre-le :

```
root@mousslim:~# systemctl start fail2ban
root@mousslim:~# systemctl enable fail2ban
Synchronizing state of fail2ban.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable fail2ban
```

Configuration de Fail2Ban :

- Créer le fichier de configuration personnalisé : cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local

```
root@mousslim:~# cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local
```

Puis édite le fichier : nano /etc/fail2ban/jail.local

- Ajoute ou modifie la section suivante pour activer la protection de Samba :

```

GNU nano 5.4 /etc/fail2ban/jail.local
# "backend" specifies the backend used to get files modification.
# Available options are "pyinotify", "gamin", "polling", "systemd" and "auto".
# This option can be overridden in each jail as well.
#
# pyinotify: requires pyinotify (a file alteration monitor) to be installed.
#             If pyinotify is not installed, Fail2ban will use auto.
# gamin:     requires Gamin (a file alteration monitor) to be installed.
#             If Gamin is not installed, Fail2ban will use auto.
# polling:   uses a polling algorithm which does not require external libraries.
# systemd:   uses systemd python library to access the systemd journal.
#             Specifying "logpath" is not valid for this backend.
#             See "journalmatch" in the jails associated filter config
# auto:      will try to use the following backends, in order:
#             pyinotify, gamin, polling.
#
# Note: if systemd backend is chosen as the default but you enable a jail
#       for which logs are present only in its own log files, specify some other
#       backend for that jail (e.g. polling) and provide empty value for
#       journalmatch. See https://github.com/fail2ban/fail2ban/issues/959#issuecomment-74901200
backend = systemd

# "usedns" specifies if jails should trust hostnames in logs,
# warn when DNS lookups are performed, or ignore all hostnames in logs
#

```

Pour que fail2ban puisse se baser sur systemd, le backend doit être modifié dans la configuration de fail2ban .

Insataller syslog celui-ci fournira les logs dans /var/log/ :

```
root@mousslim:~# apt install syslog_
```

Décommenter ### la ligne commençant par ignoreip dans /etc/fail2ban/jail.local

Configurer ces paramètres de Fail2Ban définissent les règles de bannissement :

- bantime = 1d → L'adresse IP est bannie pendant 1 jour (24 heures) après avoir dépassé le nombre de tentatives autorisées.
- findtime = 10m → La fenêtre de détection des échecs est de 10 minutes : si un utilisateur échoue plusieurs fois dans ce laps de temps, il sera banni.
- maxretry = 5 → Une IP est bannie après 5 échecs de connexion détectés dans la période findtime.

```

# ignorecommand = /path/to/command <ip>
ignorecommand =

# "bantime" is the number of seconds that a host is banned.
bantime = 1d

# A host is banned if it has generated "maxretry" during the last "findtime"
# seconds.
findtime = 10m

# "maxretry" is the number of failures before a host get banned.
maxretry = 5

```

- Après toute modification de la configuration et l'installation de rsyslog, il est important de redémarrer le service fail2ban pour que les changements soient pris en compte :

```
root@nagios:~# systemctl restart fail2ban
```

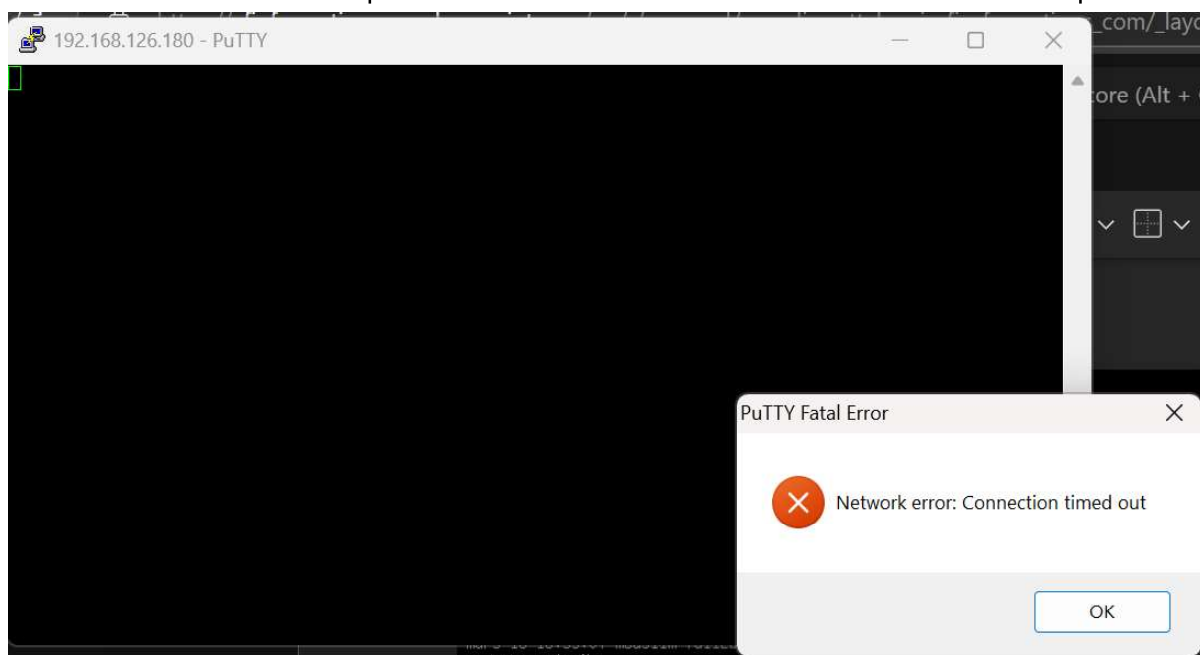
- Nous allons vérifier si tout fonctionne bien :

```
root@mouislam:~# systemctl status fail2ban
• fail2ban.service - Fail2Ban Service
  Loaded: loaded (/lib/systemd/system/fail2ban.service; enabled; vendor preset: enabled)
  Active: active (running) since Thu 2025-03-13 13:55:06 CET; 1h 50min ago
  Docs: man:fail2ban(1)
  Process: 1612 ExecStartPre=/bin/mkdir -p /run/fail2ban (code=exited, status=0/SUCCESS)
  Main PID: 1613 (fail2ban-server)
  Tasks: 5 (limit: 4618)
  Memory: 18.2M
  CPU: 8.131s
  CGroup: /system.slice/fail2ban.service
          └─1613 /usr/bin/python3 /usr/bin/fail2ban-server -xf start

mars 13 13:55:06 mouislam systemd[1]: Starting Fail2Ban Service...
mars 13 13:55:06 mouislam systemd[1]: Started Fail2Ban Service.
mars 13 13:55:07 mouislam fail2ban-server[1613]: Server ready
root@mouislam:~# _
```

Pour s'assurer que fail2ban bannis bien les IP :

- Se connecter avec puTTY mettre le bon identifiant et 5 mauvais mot de passe :



Fail2ban a bien fonctionné, l'IP est banni pendant 1 jour.

Conclusion

Au cours de cette activité, j'ai supervisé efficacement l'état de mon serveur GLPI sous Debian ainsi que mon serveur Windows (Active Directory) en utilisant Nagios comme outil de supervision centralisé. Pour améliorer cette supervision, j'ai mis en place deux améliorations majeures. La première a été l'intégration de NCPA (Nagios Cross Platform Agent), qui m'a permis de surveiller plus précisément les ressources et services sur mes serveurs. La seconde a été l'installation et la configuration de Fail2ban, une solution de sécurité essentielle qui protège mon serveur Nagios contre les tentatives de connexion malveillantes. Ces améliorations renforcent la fiabilité et la sécurité de mon infrastructure, tout en garantissant un suivi en temps réel de ses performances.