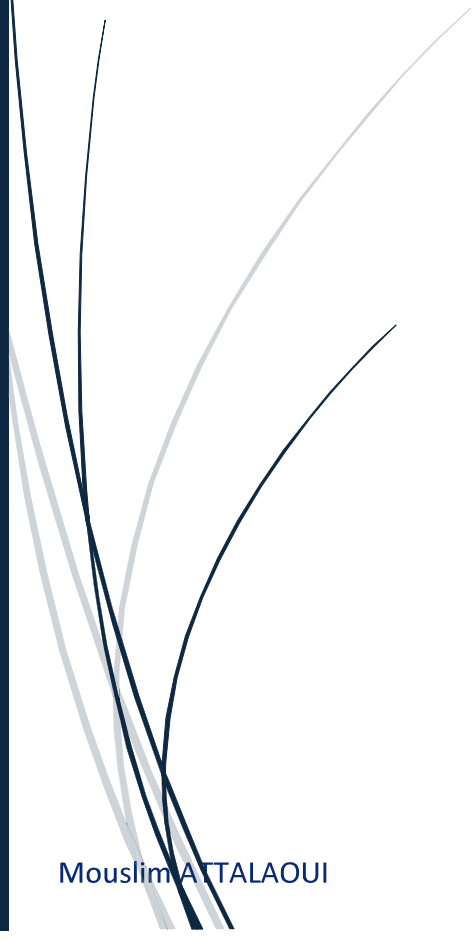
MOUSLIM ATTALAOUI

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 :

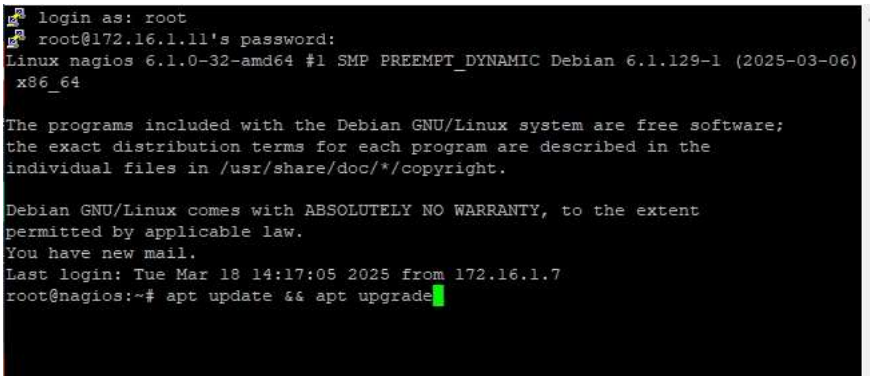
- Configuration des agents de supervision : Nous utiliserons NCPA pour faciliter la collecte de données sur les machines surveillées.

- 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.



Installer les outils suivants.

Installation Nagios XI

Ensuite créer un répertoire :

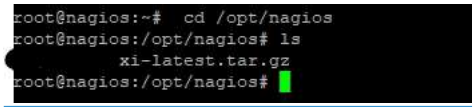
mkdir /opt/nagios

Entrer dans le répertoire :

cd /opt/nagios

Télécharger nagios XI :

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



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

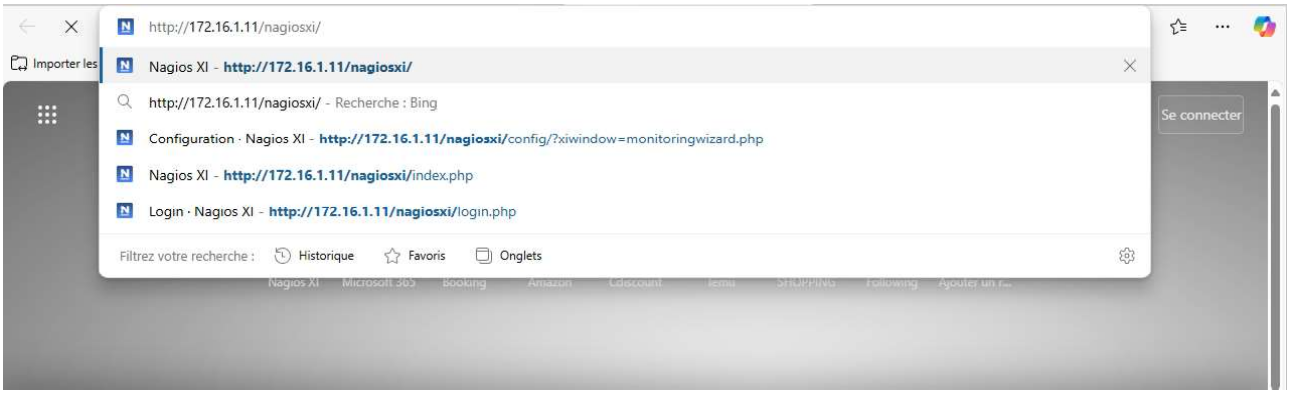
```
root@nagios:/opt/nagios# cd nagiosxi
root@nagios:/opt/nagios/nagiosxi#  ./fullinstall
```

```
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_
```

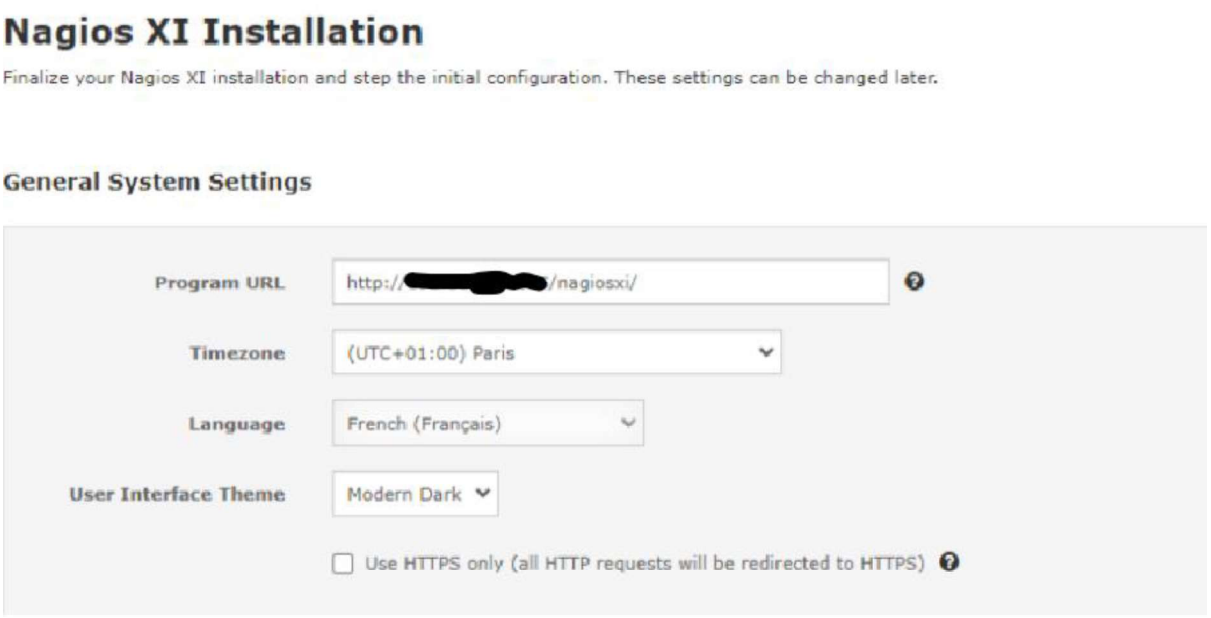
Laisser l'installations s'exécuter cela peut prendre plus de dix minutes.

```
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#
```

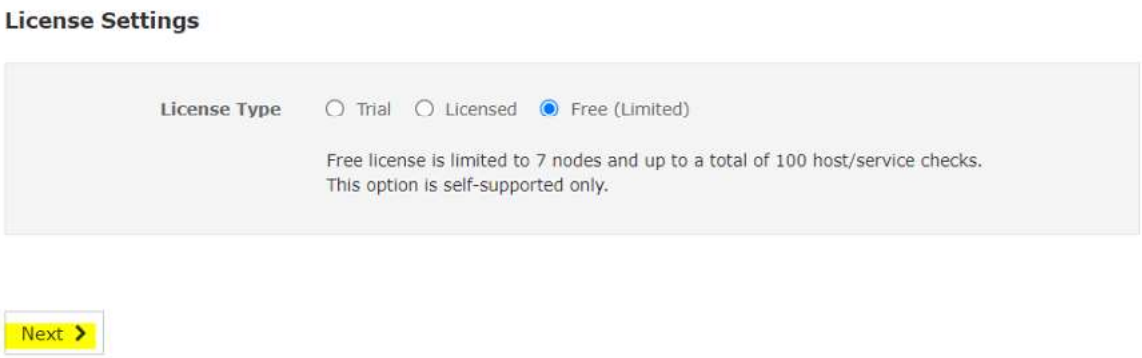
Pour finir votre installation, vous devez avoir accès à l'interface web, comme indiquez ci-dessus vous pouvez avoir accès au site a : http://172.16.1.11/nagiosxi/ .



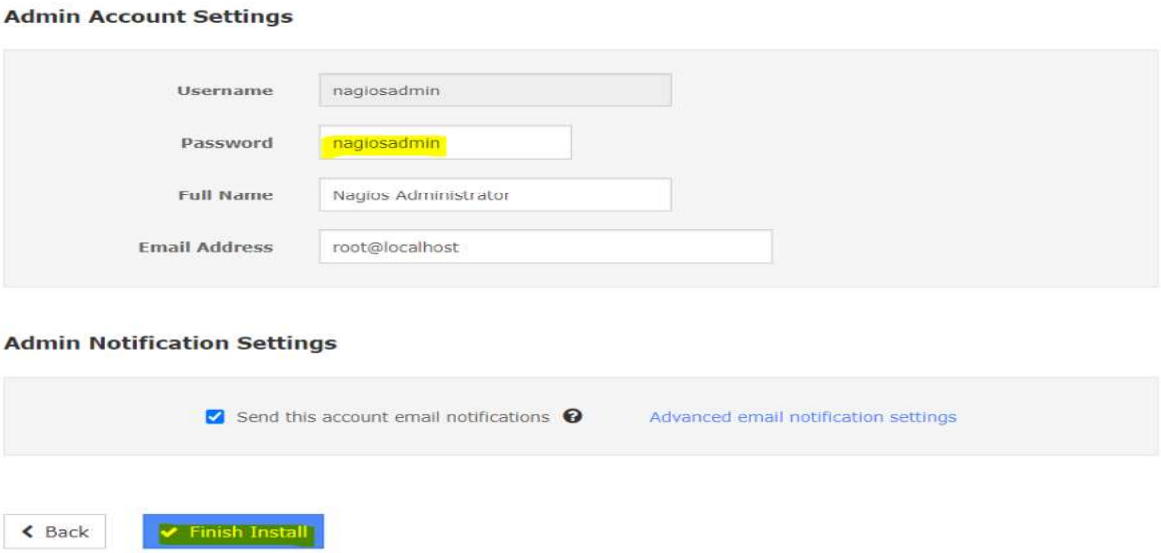
Entrer les paramètres suivants :



Entrer votre bonne IP dans le program url.

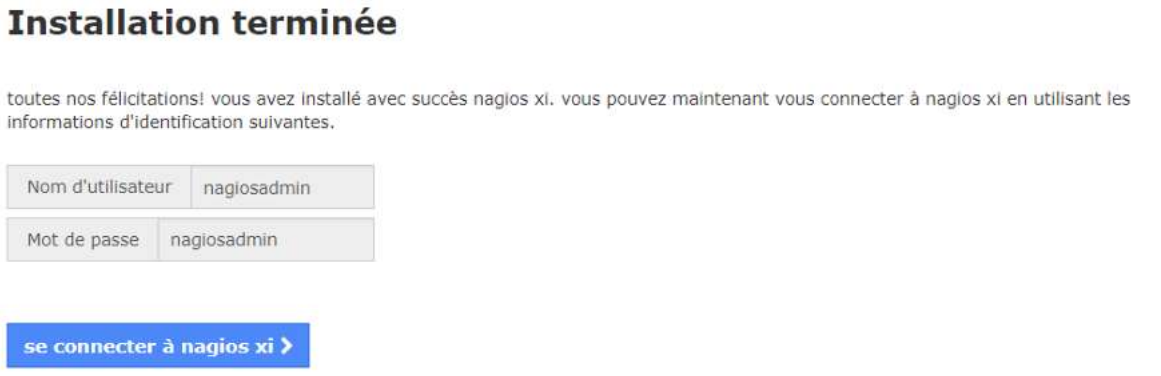


Nous allons utiliser la version free



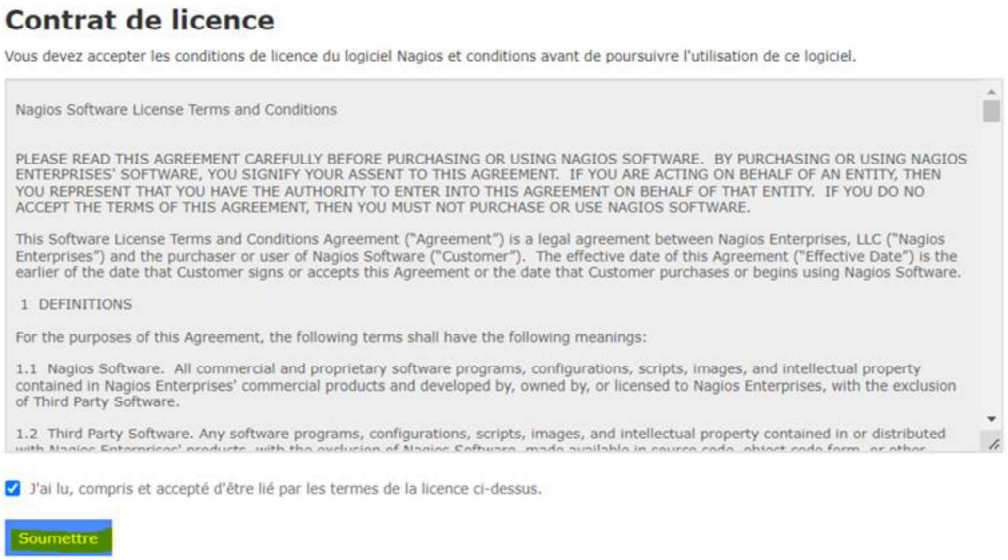
Nous allons configurer l'identifiant et le mot de passe, moi j'utiliserais "nagiosadmin", nous finirons l'installations avec "finish install".

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

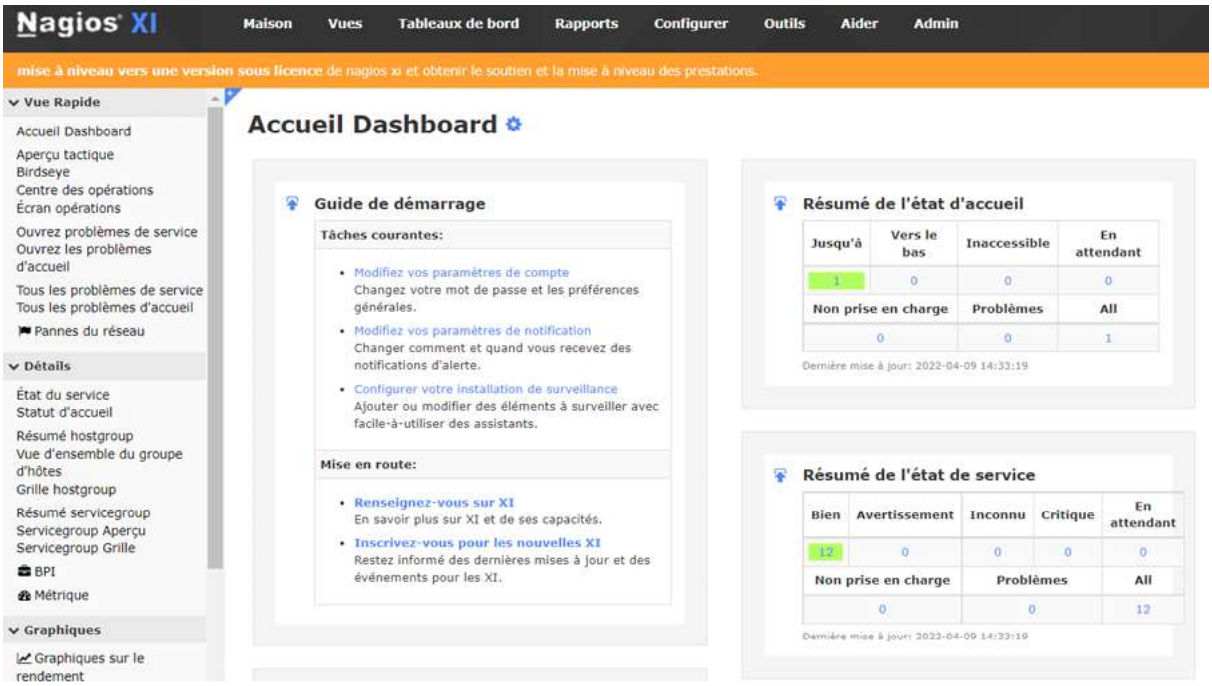


Entrer vos informations de connexion .

Accepter le contrat.



Le serveur est enfin prêt.



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

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 repertoir 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

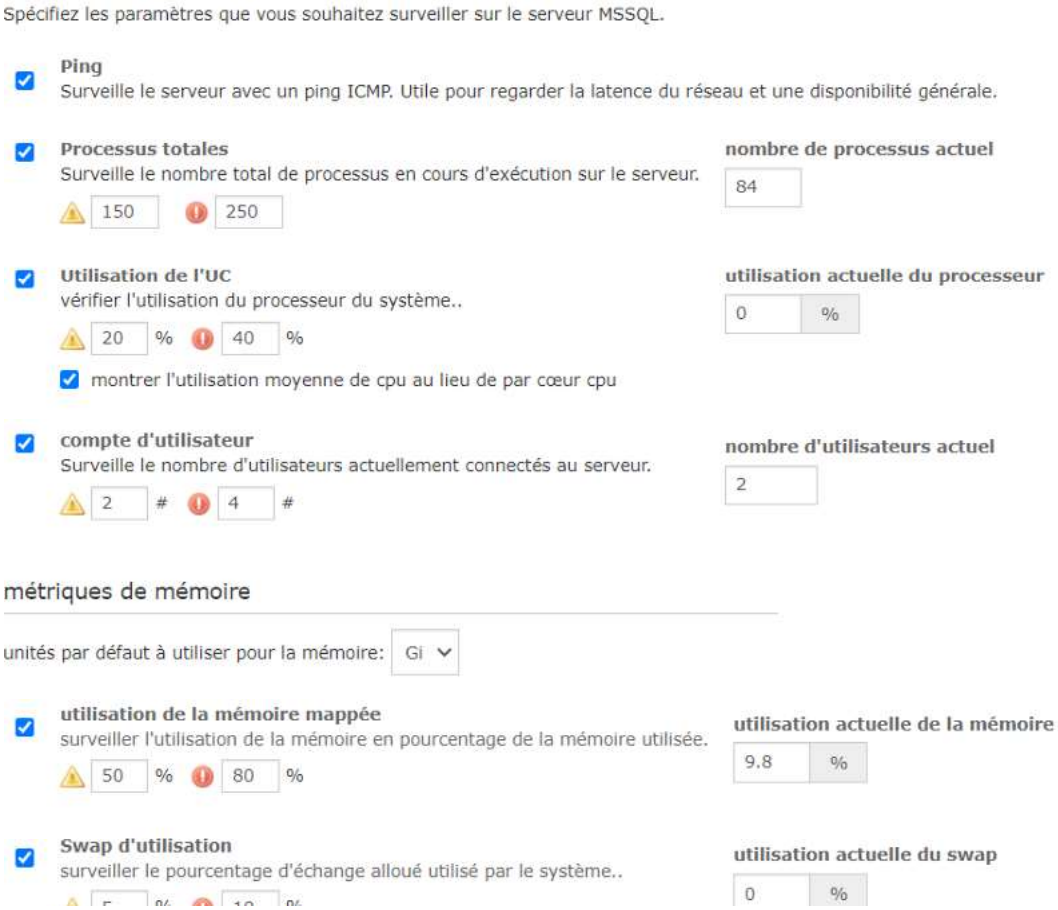
Pour ajouter le serveur Debian à superviser dans Nagios XI, accédez à l'interface d'administration de Nagios. Ensuite, rendez-vous dans le menu "Configurer", puis sélectionnez "Assistants de configuration" pour commencer l'ajout du nouvel hôte.

Chercher puis cliquez ensuite sur « Linux Serveur »

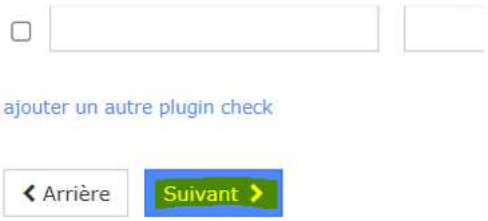
Il faut maintenant entrer les parametre suivant :

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

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



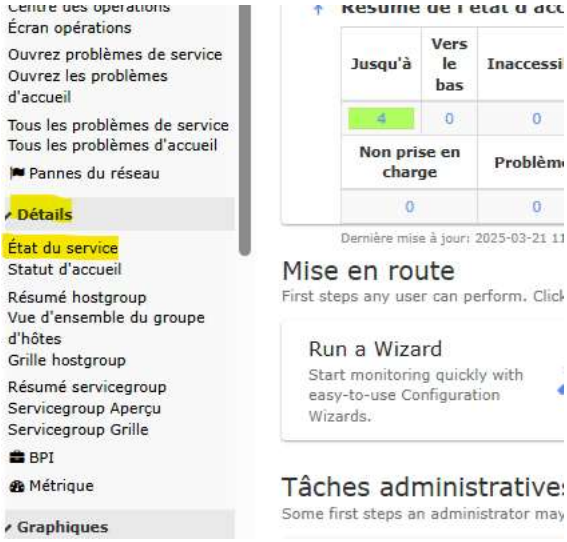
Puis cliquer sur « Suivant ».



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

Nous avons fini la configuration.

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



Nous constatons que la machine est bien présente.

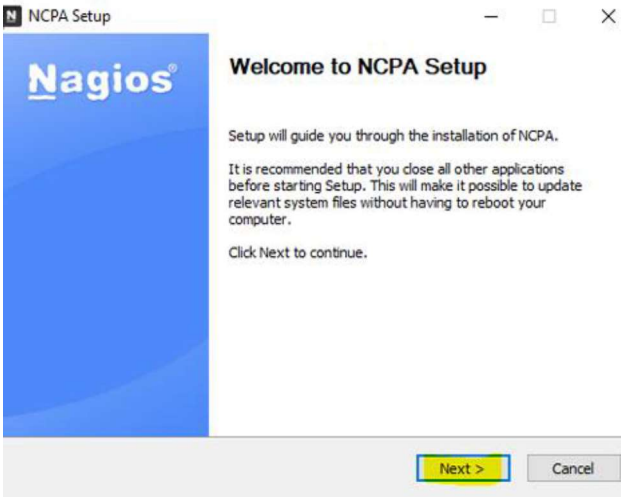
Hôte	Service	Statut	Durée	Tentative	Dernière vérification	Informations sur l'état
172.16.1.4	CPU Usage	Bien	2d 23h 2m 58s	1/5	2025-03-21 11:23:52	OK: Percent was 0.00 %
	Disk Usage on /	Bien	2d 23h 2m 36s	1/5	2025-03-21 11:24:11	OK: Used disk space was 6.00 % (Used: 2.72 GiB, Free: 42.79 GiB, Total: 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/systemd-sysusers.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

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.

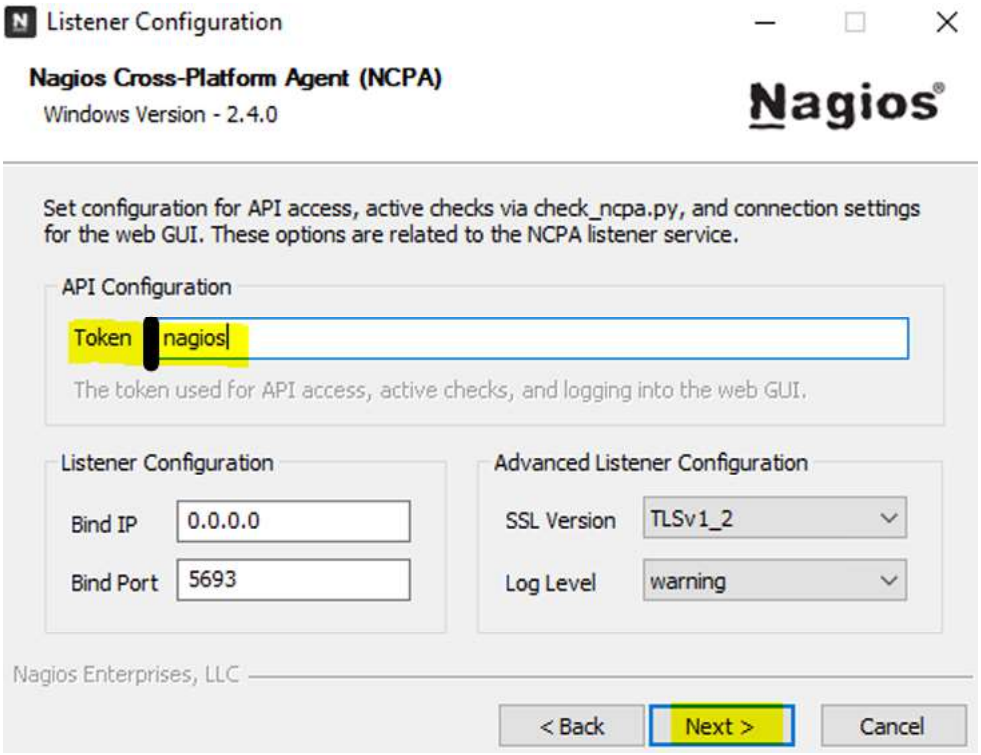
Bien choisir celui-ci.

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

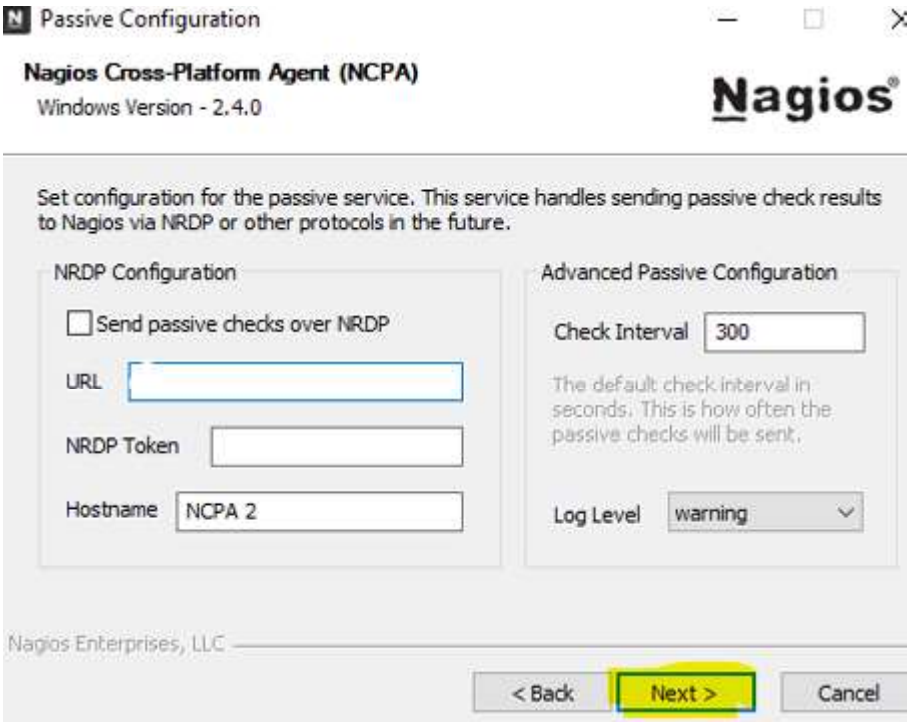


Puis accepter les conditions :

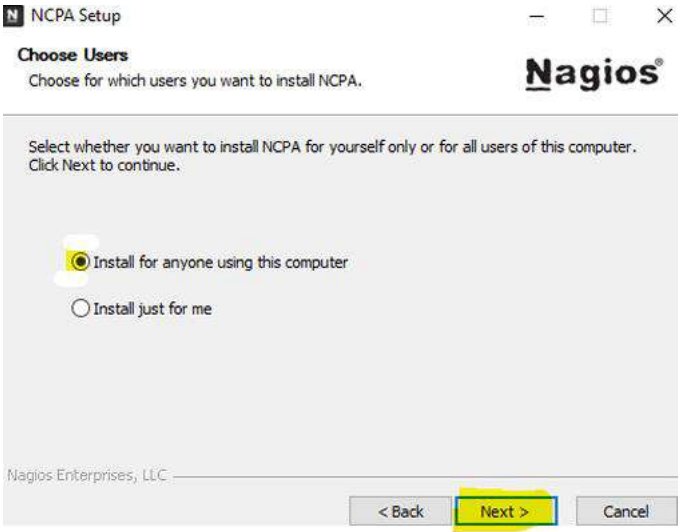
Ajouter un Token, et cliquer sur Next :



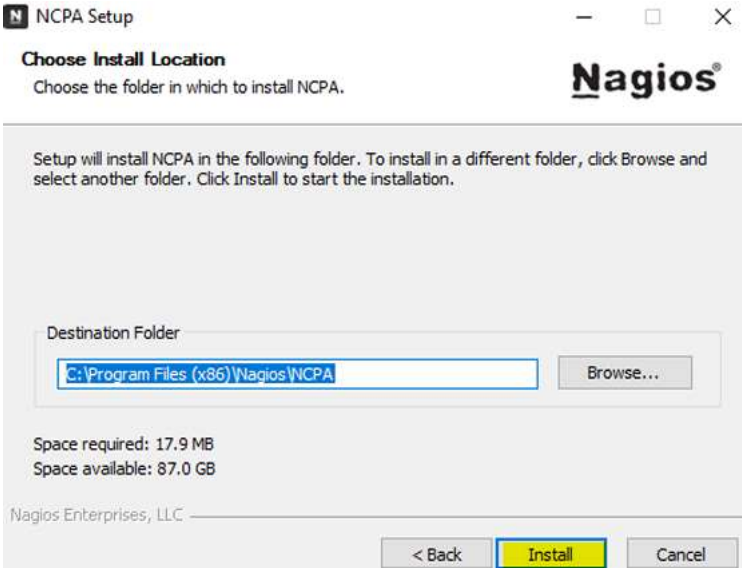
Ensuite passer cette étape avec Next :



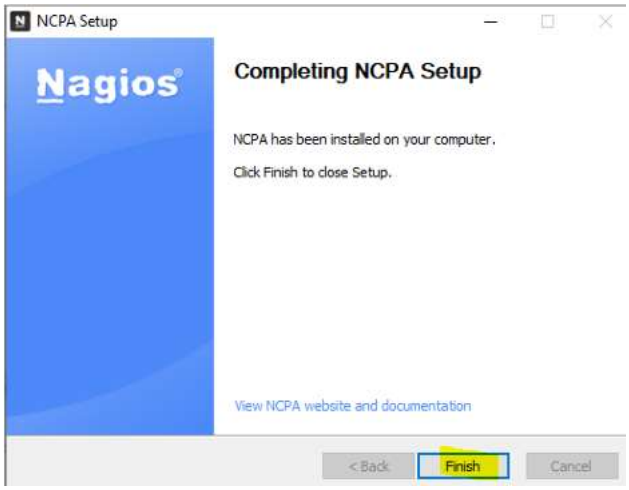
Cocher la case Install, puis cliquer sur Next :



Continuer avec Install :



Enfin, cliquer sur finish :

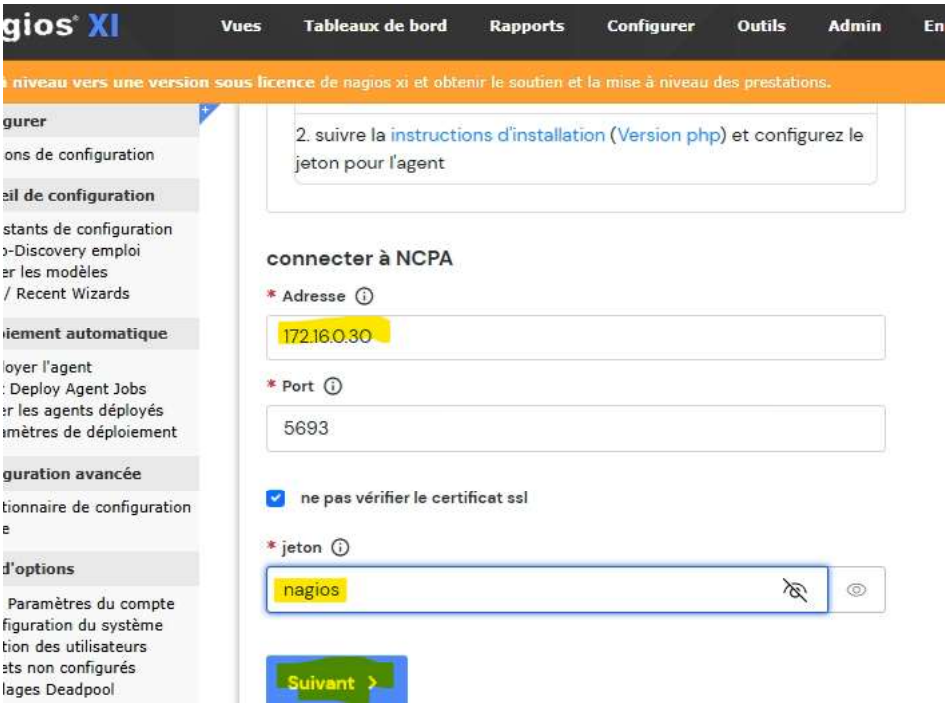


Ajout du serveur Windows (AD) sur NAGIOS XI

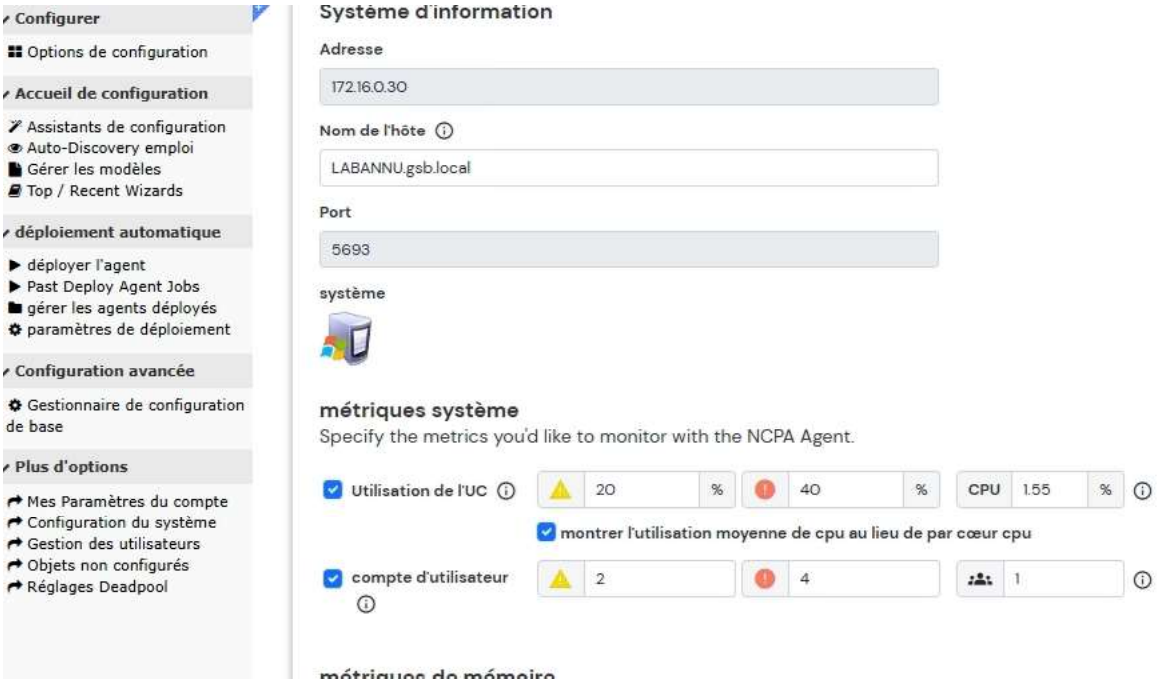
Pour ajouter le serveur Windows à superviser dans Nagios XI, accédez à l'interface d'administration de Nagios. Ensuite, rendez-vous dans le menu "Configurer", puis sélectionnez "Assistants de configuration" pour commencer l'ajout du nouvel hôte.

Choisissez ensuite Windows Server :

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

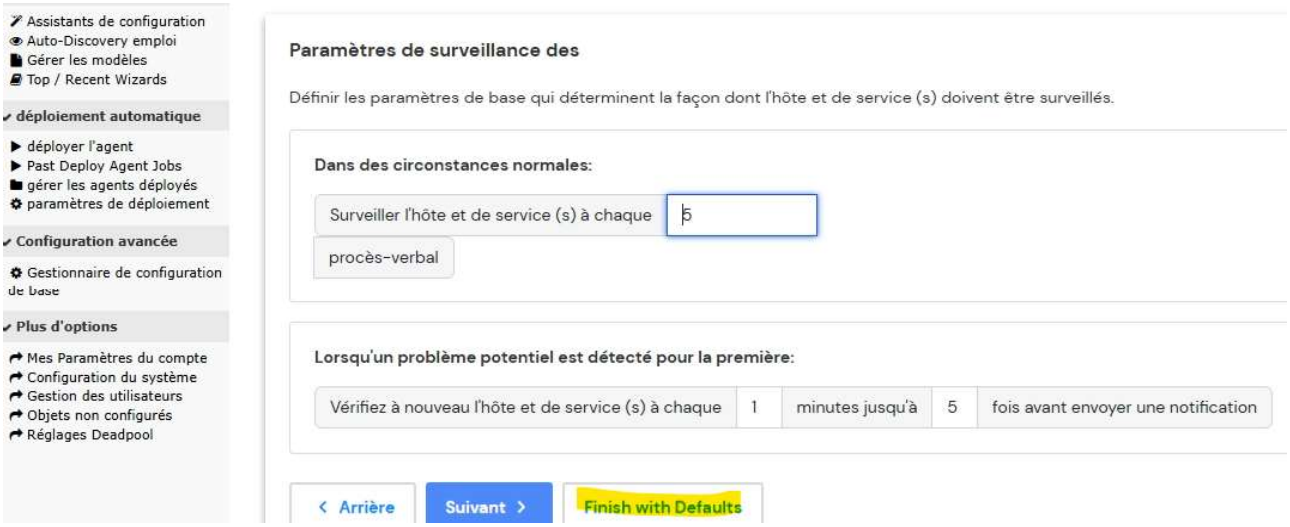


Maintenant à vous de choisir les paramètres que vous voulez configurer :

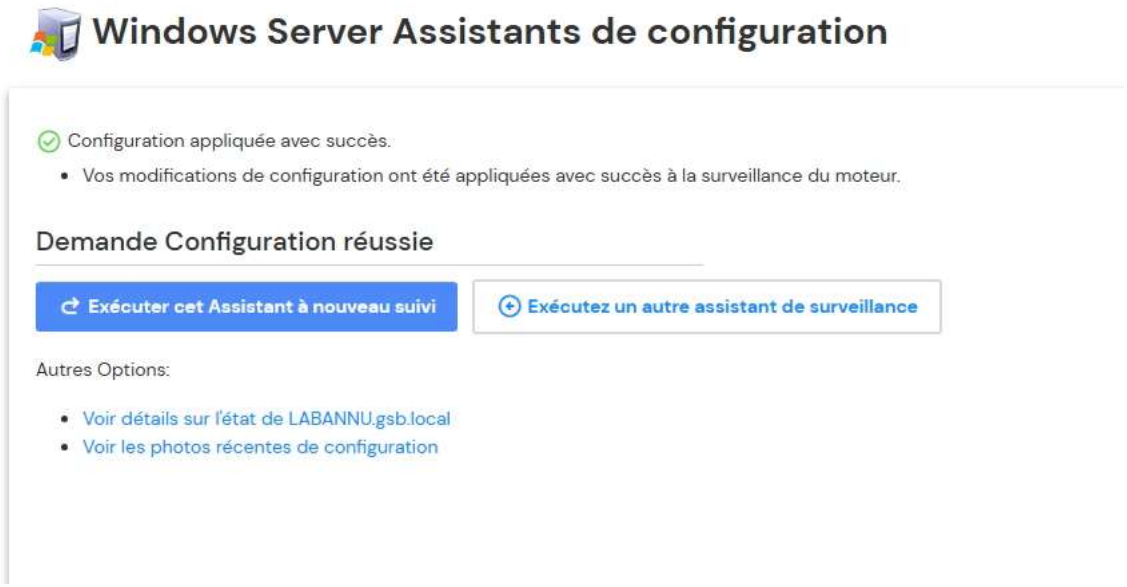


Puis cliquer sur suivant :

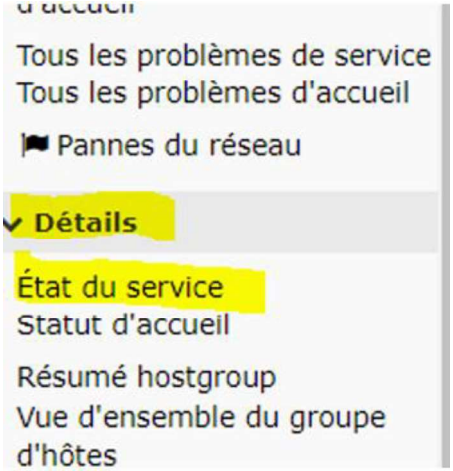
Vous pouvez maintenant cliquer sur le bouton “Finish with default” :



La configuration est terminée :



Si vous souhaitez verifier si la machine est bien présente :



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 wa
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(

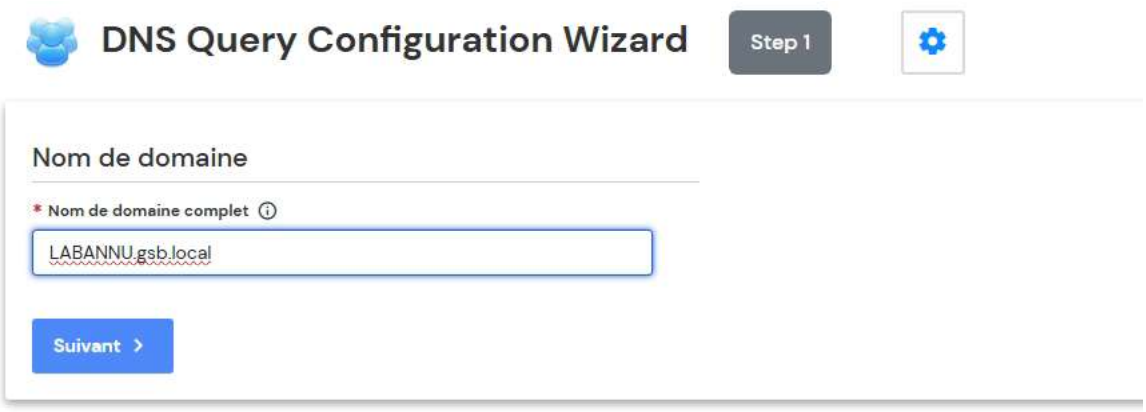
Supervision du DNS

Nous allons maintenant superviser le DNS

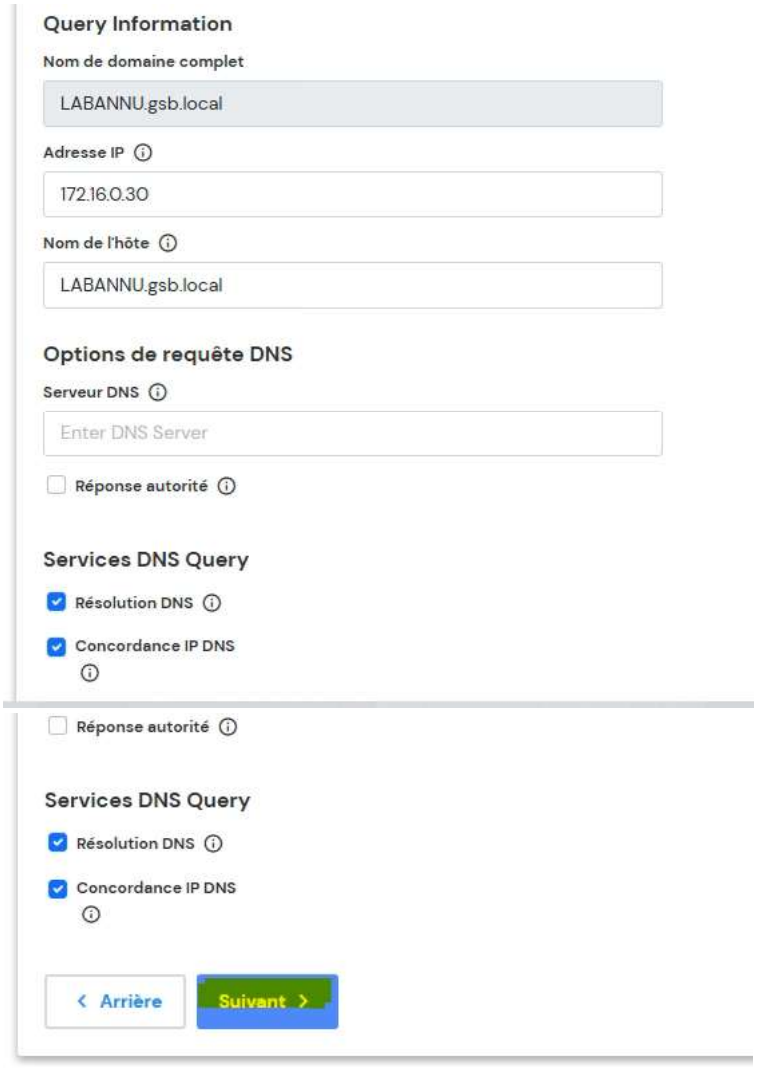
Pour cela se rendre dans “Configurer” puis sur “Assistants de configurations” :

Puis choisir DNS :

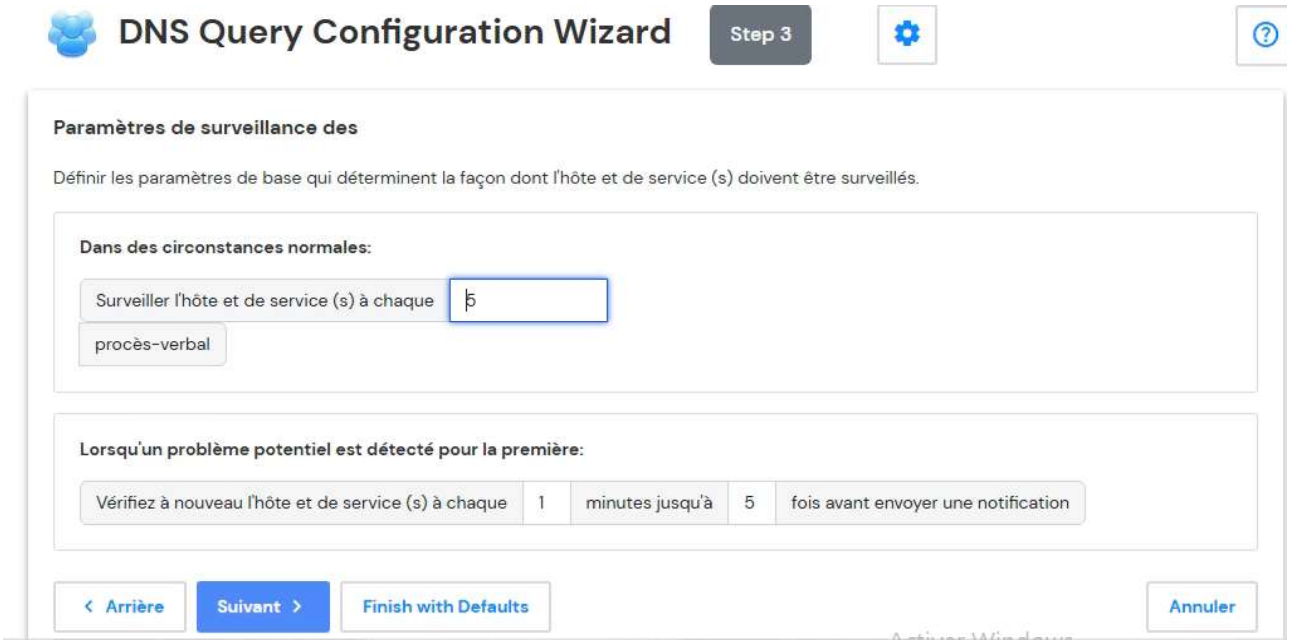
Maintenant entre le nom de domaine du contrôleur de domaine, puis cliquer sur suivant :



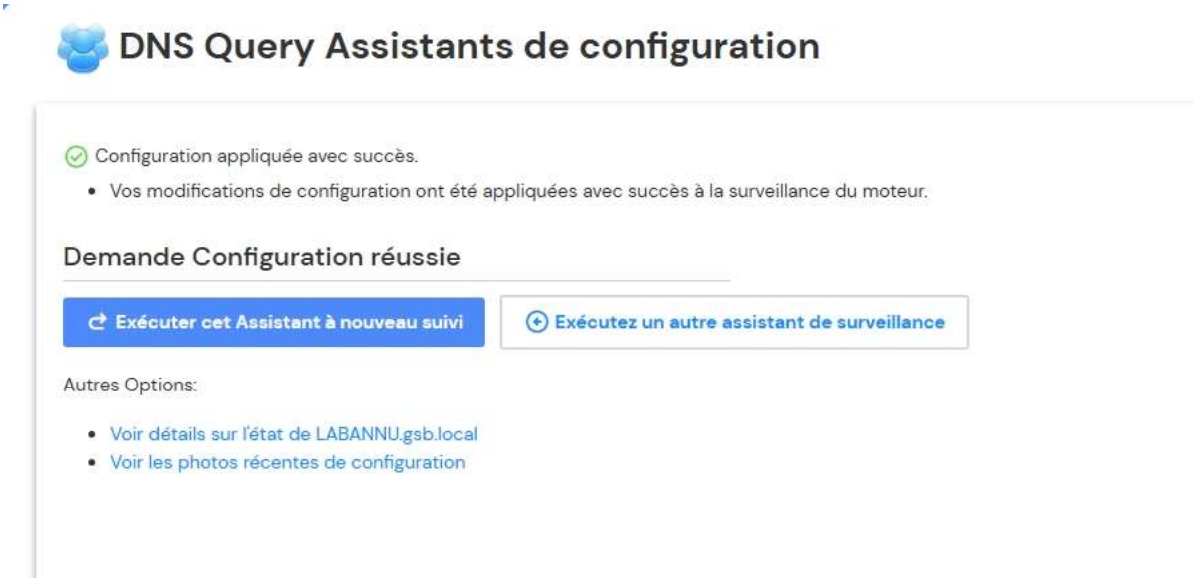
Verifier si tout est correct puis cliquer sur suivant :



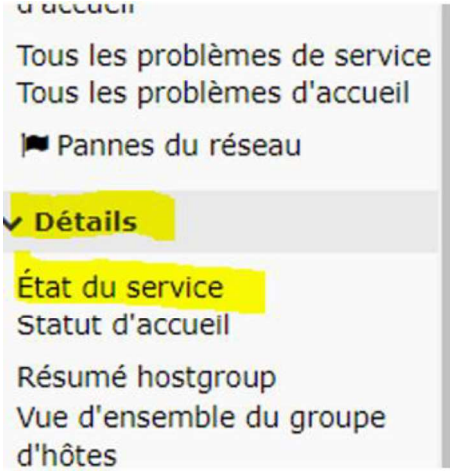
Pour finir cliquer sur “Suivant” :



La configuration est maintenant terminée :



Nous allons maintenant verifier s'il est bien présent :



	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@mouslim:~# apt install fail2ban -y
```

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

```
root@mouslim:~# systemctl status fail2ban
● fail2ban.service - Fail2Ban Service
     Loaded: loaded (/lib/systemd/system/fail2ban.service; enabled; vendor pres>
     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 mouslim systemd[1]: Starting Fail2Ban Service...
mars 04 16:49:26 mouslim systemd[1]: Started Fail2Ban Service.
mars 04 16:49:26 mouslim fail2ban-server[696]: Server ready
lines 1-14/14 (END)
```

- Maintenant démarre-le :

```
root@mouslim:~# systemctl start fail2ban
root@mouslim:~# systemctl enable fail2ban
Synchronizing state of fail2ban.service with SysV service script with /lib/syste
md/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@mouslim:~# 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@mouslim:~# 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 :

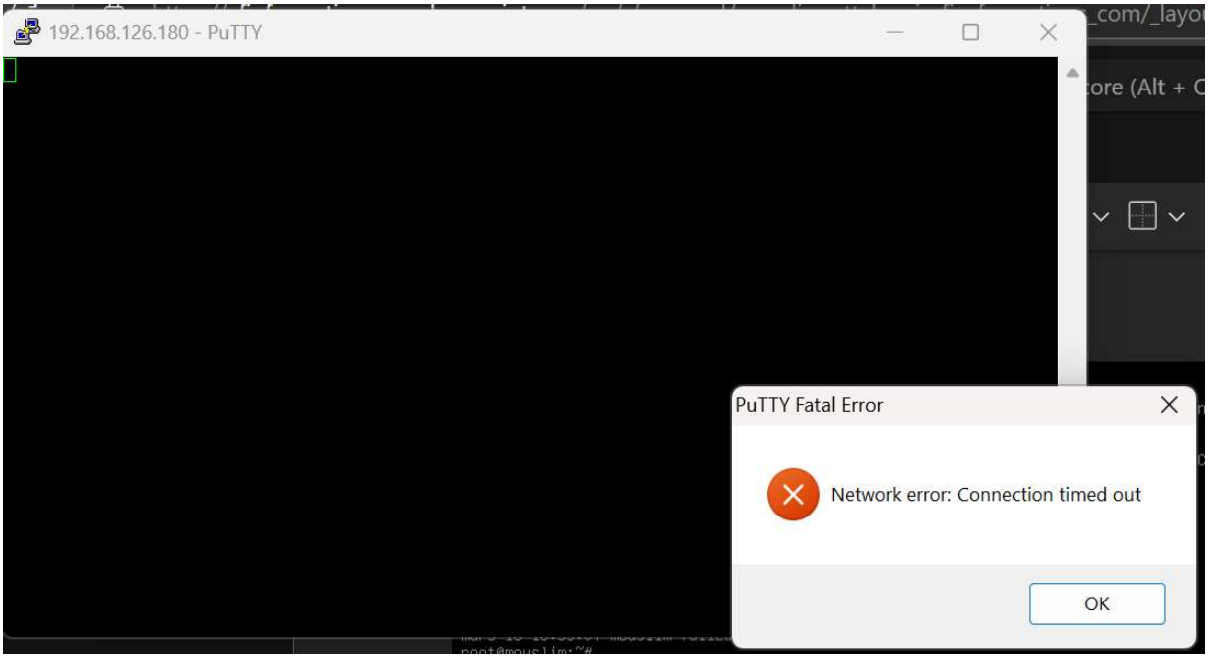
```
root@nagios:~# systemctl restrat fail2ban
```

- Nous allons vérifier si tout fonctionne bien :

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

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.