Adame BENYOUB

PAPPE NAGIOSXI

Nagios® XI™

Session 2025

BTS SIO SISR

Sommaire

Installation et configuration de Nagios XI

On commence par mettre à jour le serveur en utilisant ces commandes :

```
root@NagiosXi:~# apt update
```

```
root@NagiosXi:~# apt upgrade
```

```
root@NagiosXi:~# apt update
```

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

Créer un répertoire.

```
root@NagiosXi:~# mkdir /opt/nagios
```

Nous rentrons dans le dossier que nous venons de créer.

```
root@NagiosXi:~# cd /opt/nagios/
```

On télécharge Nagios XI.

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

On décompresse l'archive.

```
root@NagiosXi:/opt/nagios# tar -xvzf xi-latest.tar.gz
```

On peut voir le dossier « nagiosxi ».

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

Entrer dans le répertoire « nagiosxi ».

```
root@NagiosXi:/opt/nagios# cd nagiosxi
```

Nous lançons le script d'installation.

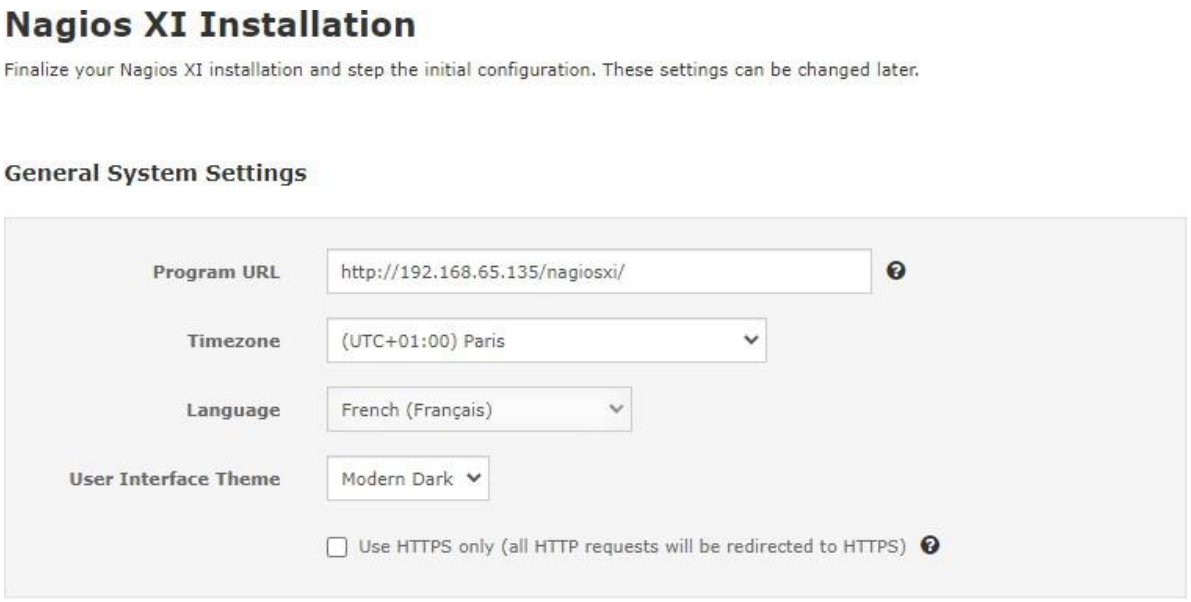
```
root@NagiosXi:/opt/nagios/nagiosxi# ./fullinstall
```

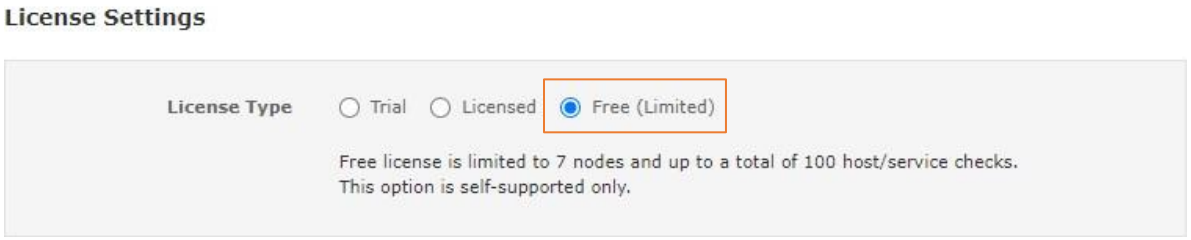
Entrer « Y » pour continuer l'installation.

```
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
```

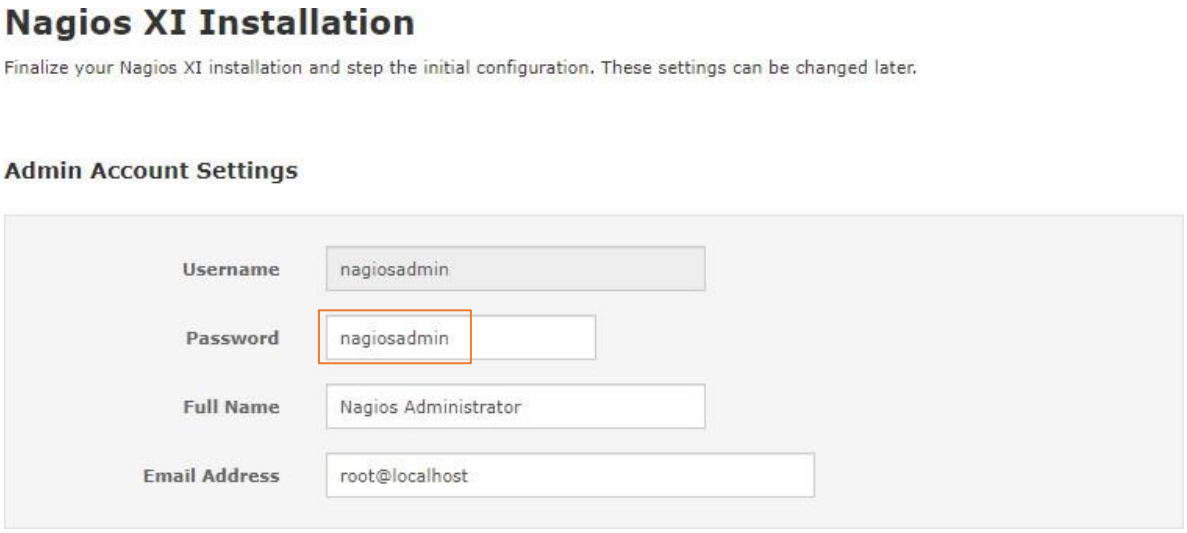
Voici l'installation terminé, on peut voir l'URL pour accéder à l'interface web de Nagios XI.

Voici les paramètres à entrer :

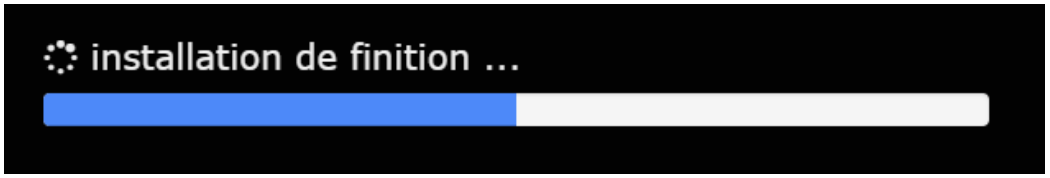




Ici nous définissons les paramètres de compte administrateur. Le mot de passe sera « nagiosadmin ».

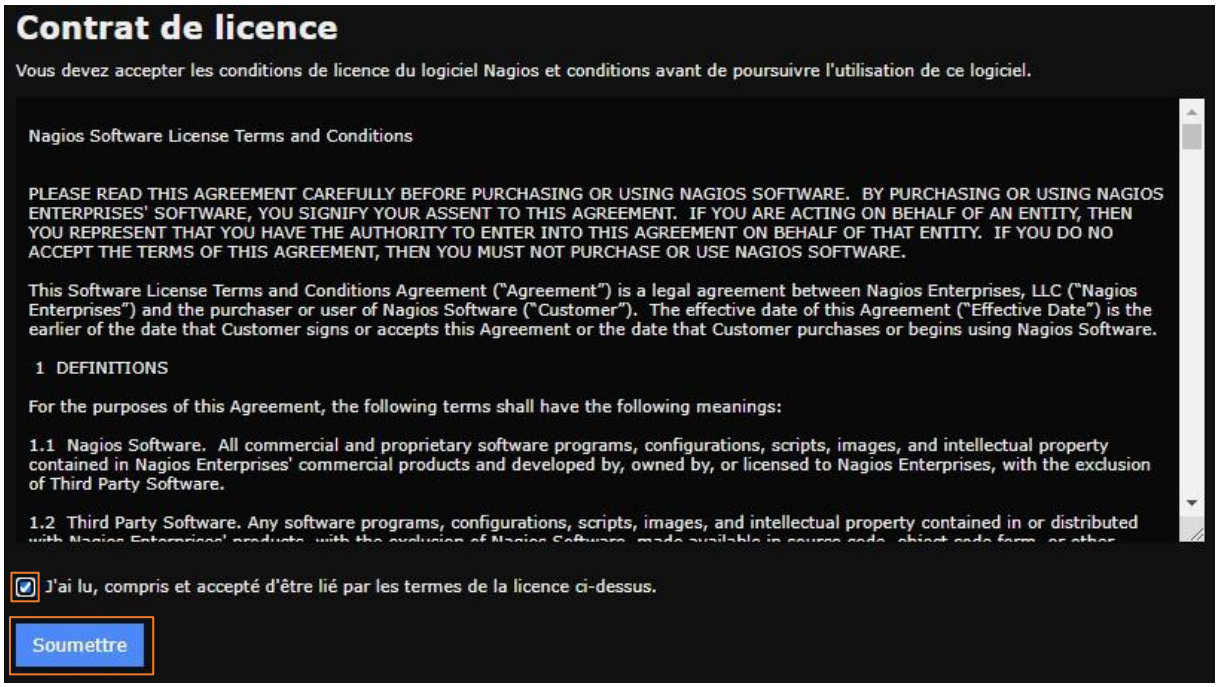


L'installation est en cours :

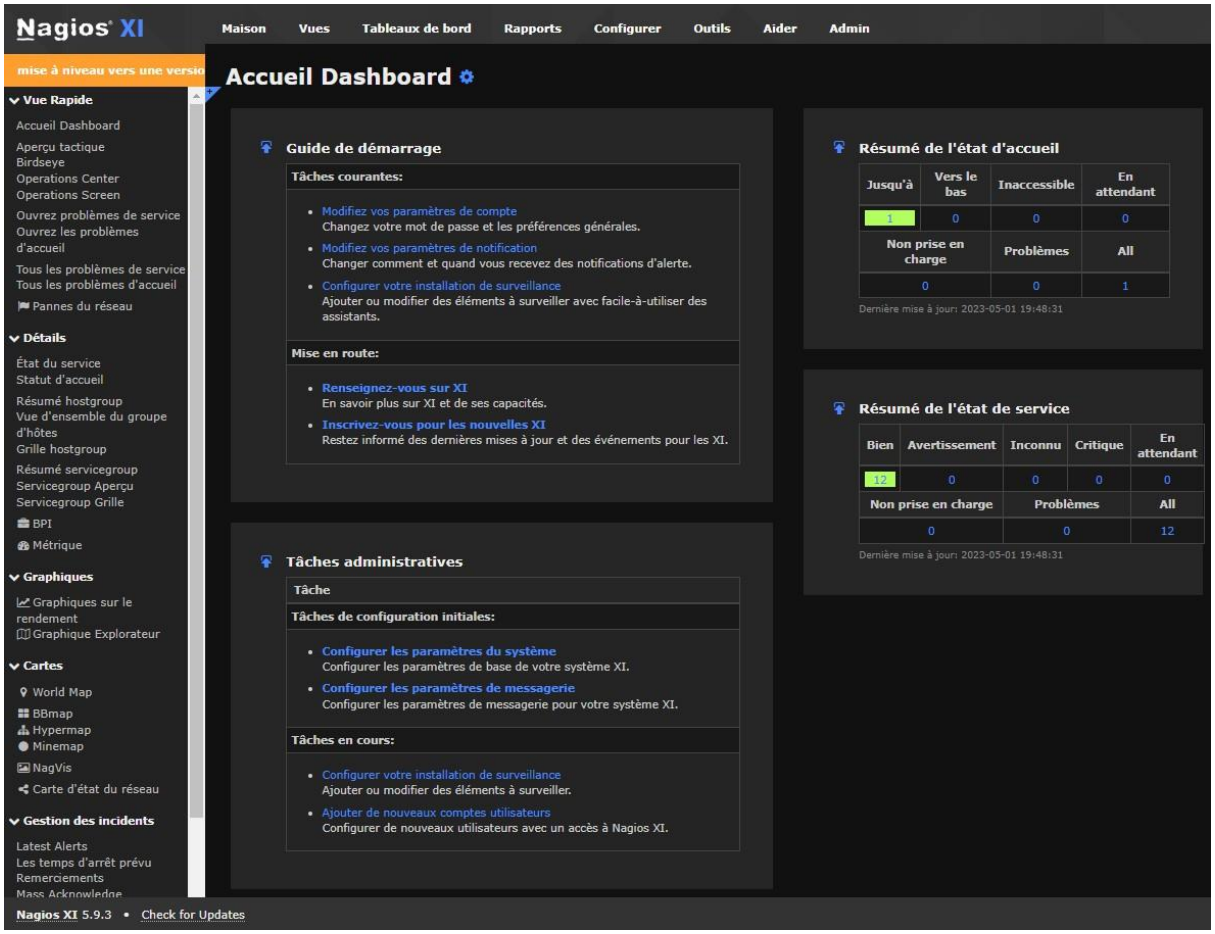


Cliquer sur « Se connecter à Nagios xi » pour être rediriger vers la page d'administration

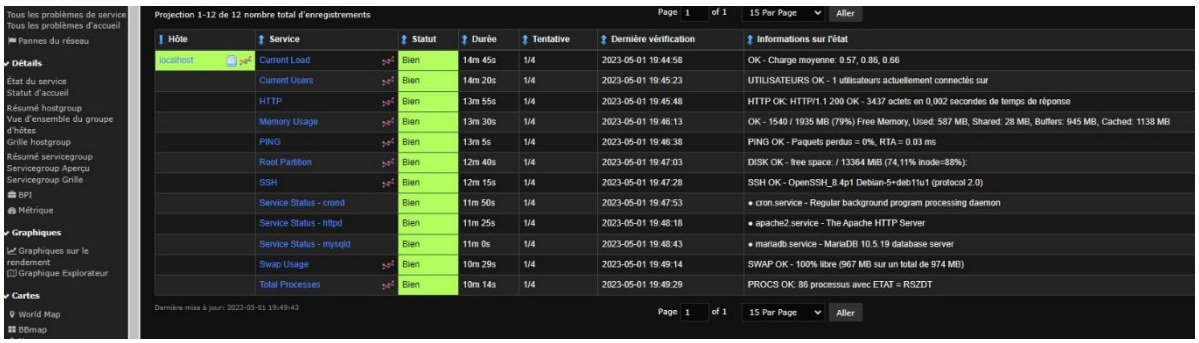
On accepte le contrat de licence :



Nous voici désormais connecté à notre Nagios XI fonctionnel.



En cliquant sur « Détails » puis « Etat du service » on peut voir l'état de service du serveur Nagios
(localhost).



Supervision Debian

J’ai décidé de superviser ma machine GLPI pour suivre la machine et en cas de problème, intervenir rapidement sur celle-ci.

Prérequis (sur la machine Debian à superviser)

Nous mettons à jour Debian et nous installons les paquets : ssh, gnupg, et gnupg2 :

```
root@glpi:~# apt update
```

```
root@glpi:~# apt upgrade_
```

```
root@glpi:~# apt install ssh_
```

```
root@glpi:~# apt install gnupg
```

```
root@glpi:~# apt install gnupg2
```

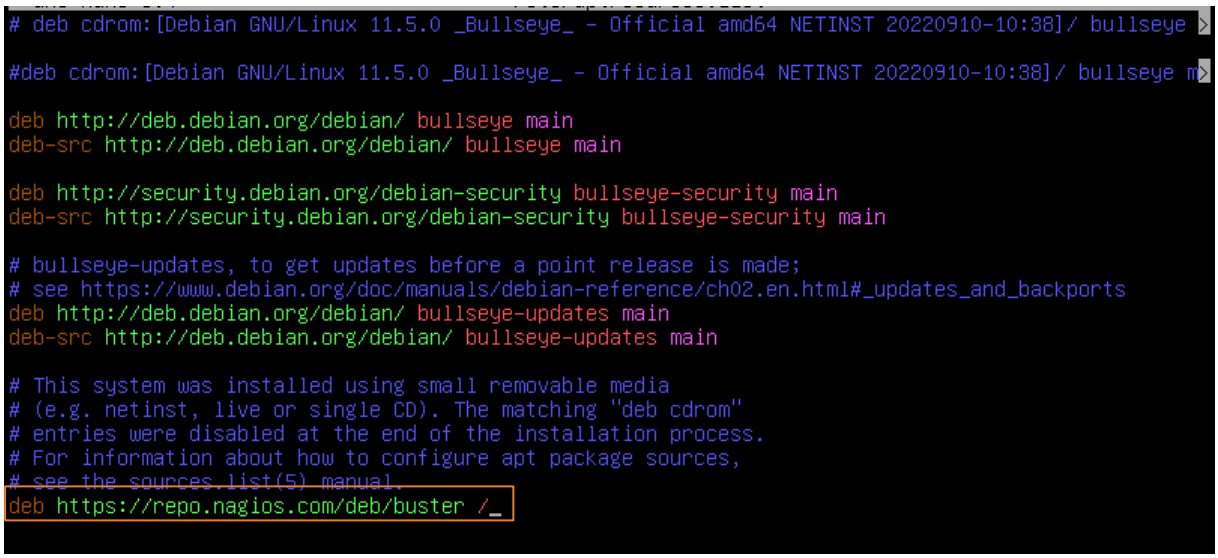
Installation de NCPA (sur la machine Debian à superviser)

NCPA est l’agent qui va être installé sur la Debian à superviser afin de remonter les informations au serveur Nagios XI

On va ajouter le dépôt dans le fichier sources.list de la machine Debian :

```
root@glpi:~# nano /etc/apt/sources.list
```

On ajoute la ligne « deb https://repo.nagios.com/deb/buster / » à la fin du fichier :



On ajoute ensuite la clé publique

```
root@glpi:~# wget -qO - https://repo.nagios.com/GPG-KEY-NAGIOS-V2 | apt-key add -
Warning: apt-key is deprecated. Manage keyring files in trusted.gpg.d instead (see apt-key(8)).
OK
```

On installe ensuite le paquet :

```
root@glpi:~# apt install apt-transport-https_
```

Puis on met à jour le serveur

```
root@glpi:~# apt update_
```

Nous installons NCPA

```
root@glpi:~# apt install ncpa_
```

Nous devons ensuite modifier le token qui se trouve dans le fichier /usr/local/ncpa/etc/ncpa.cfg

```
root@glpi:~# nano /usr/local/ncpa/etc/ncpa.cfg_
```

Dans la partie « [api] » on rentre :

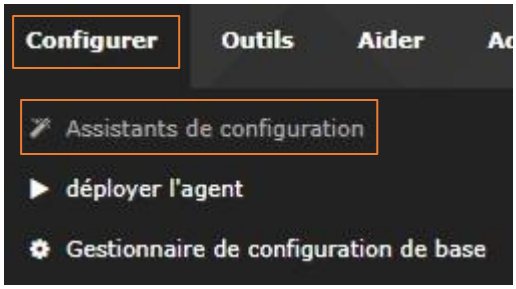
```
[api]

#
# The token that will be used to log into the basic web GUI (API browser, graphs, top charts, etc)
# and to authenticate requests to the API and requests through check_ncpa.py
#
community_string = nagios
```

Nous redémarrons ensuite le service NCPA

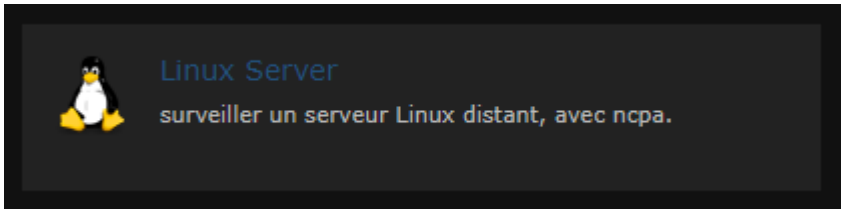
```
root@glpi:~# service ncpa_listener restart_
```

Ajout du serveur Debian

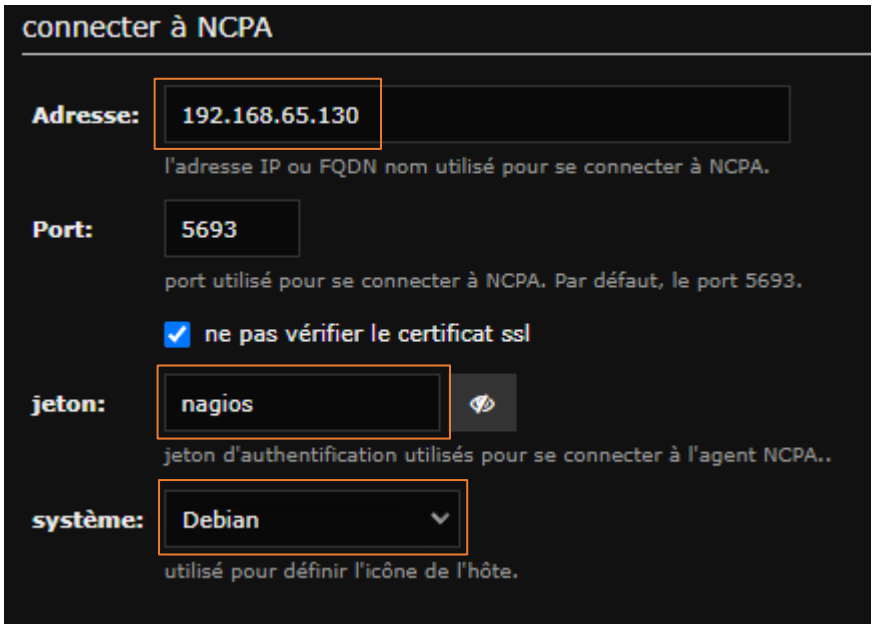
Nous allons désormais ajouter le serveur Debian précédemment configuré au serveur Nagios XI, pour cela, se diriger sur l'interface d'administration de Nagios XI puis cliquer sur « Configurer » et
« Assistants de configuration »



Cliquer ensuite sur « Linux Serveur »



On entre ensuite les paramètres nécessaires, dont l'IP, le jeton et le système.



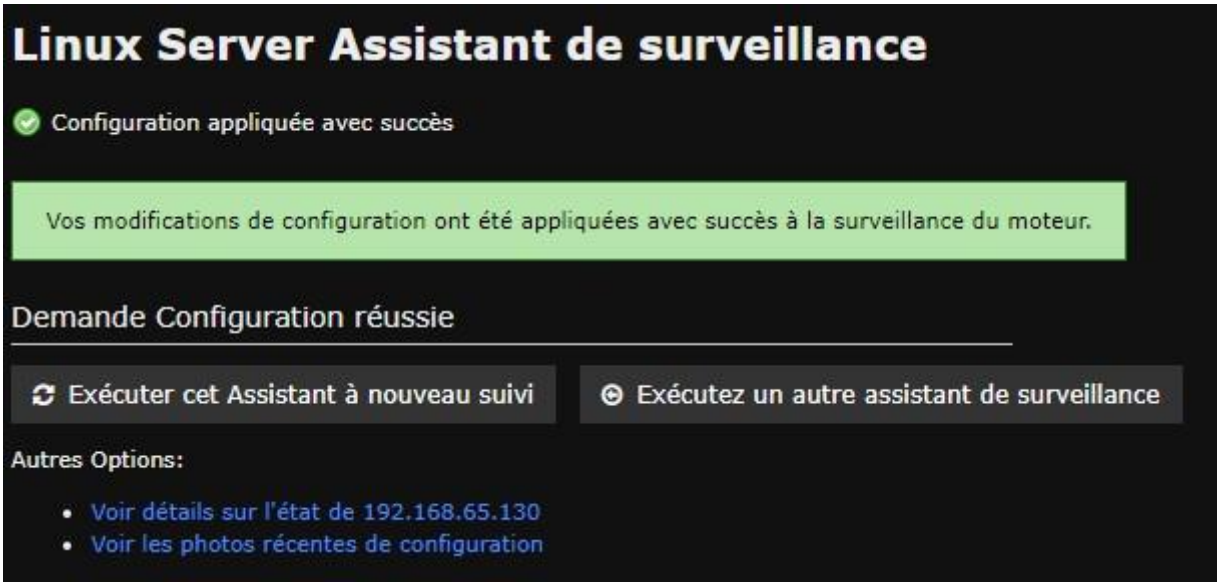
On clique ensuite sur « Suivant »

On peut ensuite sélectionner les paramètres désirés :

Et on clique ensuite sur « Suivant »

On définit ensuite les paramètres de surveillance et on clique sur « Terminer »

La configuration est terminée



En retournant sur la page d'accueil on clique sur « Etat de service »

On peut désormais voir la machine que nous venons d'ajouter en plus de la machine Nagios XI

Hôte	Service	Statut	Durée	Tentative	Dernière vérification	Informations sur l'état
192.168.65.130	CPU Usage	Bien	1m 14s	1/5	2023-05-21 01:57:16	OK: Percent was 0.00 %
	Disk Usage on /	Bien	N/A	1/5	2023-05-21 01:56:31	OK: Used disk space was 6.20 % (Used: 2.82 GiB, Free: 42.68 GiB, Total: 47.97 GiB)
	Disk Usage on /sys/fs/bpf	Bien	N/A	1/5	2023-05-21 01:56:35	OK: Used disk space was 0.00 % (Used: 0.00 GiB, Free: 0.00 GiB, Total: 0.00 GiB)
	Disk Usage on /sys/fs/cgroup	Bien	N/A	1/5	2023-05-21 01:56:42	OK: Used disk space was 0.00 % (Used: 0.00 GiB, Free: 0.00 GiB, Total: 0.00 GiB)
	Memory Usage	Bien	N/A	1/5	2023-05-21 01:56:52	OK: Memory usage was 25.60 % (Available: 1.41 GiB, Total: 1.90 GiB, Free: 0.48 GiB, Used: 0.32 GiB)
	Ping	Bien	N/A	1/5	2023-05-21 01:56:49	OK - 192.168.65.130 rta 0,174ms lost 0%
	Swap Usage	Bien	N/A	1/5	2023-05-21 01:56:45	OK: Swap usage was 0.00 % (Used: 0.00 GiB, Free: 0.95 GiB, Total: 0.95 GiB)
	Total Processes	Bien	N/A	1/5	2023-05-21 01:56:55	OK: Process count was 126
	User Count	Bien	N/A	1/5	2023-05-21 01:56:59	OK: Count was 1 users
	ens33 Bandwidth - Inbound	Bien	N/A	1/5	2023-05-21 01:57:02	OK: Bytes_recv was 0 MB/s
	ens33 Bandwidth - Outbound	Bien	N/A	1/5	2023-05-21 01:57:06	OK: Bytes_sent was 0 MB/s
localhost	Current Load	Bien	19d 6h 22m 32s	1/4	2023-05-21 01:52:38	OK - Charge moyenne: 0.01, 0.03, 0.11
	Current Users	Bien	19d 6h 22m 7s	1/4	2023-05-21 01:53:03	UTILISATEURS OK - 1 utilisateurs actuellement connectés sur
	HTTP	Bien	19d 6h 21m 42s	1/4	2023-05-21 01:53:28	HTTP OK: HTTP/1.1 200 OK - 3437 octets en 0,000 secondes de temps de réponse
	Memory Usage	Bien	19d 6h 21m 17s	1/4	2023-05-21 01:53:53	OK - 2041 / 1935 MB (105%) Free Memory, Used: 624 MB, Shared: 35 MB, Buffers: 394 MB, Cached: 1125 MB

Introduction

Le service Fail2ban va permettre de protéger un serveur Linux des attaques de brute-force automatiquement en surveillant les logs. Dès que les conditions sont réunies (nombres de tentative dans un intervalle de temps), l'adresse IP suspecte est bannie durant un temps déterminé. Le ban est réalisé à l'aide du système de pare-feu iptables.

Cet article traite de l'installation ainsi que la configuration de fail2ban sur une Debian 12. Le service SSHD servira d'exemple. Des commandes pour interagir avec le service fail2ban sont également présentées.

Sous Debian 12, le paquet rsyslog n'est plus installé par défaut. Celui-ci est nécessaire au bon fonctionnement sans modification de la configuration de fail2ban. Cependant, il est tout de même préférable de configurer celui-ci pour fonctionner avec systemd.

Installation

Fail2ban est présent dans les dépôts de Debian

```
sudo apt install -y fail2ban
```

Si `iptables` n'est pas installé, le faire :

```
sudo apt install -y iptables
```

Créer les fichiers de configuration adéquat en se basant sur ceux présents :

```
sudo cp /etc/fail2ban/jail.{conf,local}
```

Editer le fichier `jail.local` :

```
sudo vi /etc/fail2ban/jail.local
```

Installer le paquet rsyslog

```
sudo apt install -y rsyslog
```

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

```
backend = systemd
```

Il y a 3 directives importantes à connaitre :

- bantime : La durée de ban d'une adresse IP.

Par défaut si aucun suffixe n'est spécifié, la durée est exprimée en secondes. Pour un ban permanent, indiquer un nombre négatif.

- findtime : La durée pour comptabiliser le nombre de tentatives maximales (maxretry) avant de déclencher un ban.
- maxretry : Le nombre de tentative durant la période indiquée dans findtime avant de ban une ip.

Exemple :

```
bantime  = 1d
findtime  = 10m
maxretry = 5
```

Si 5 échecs d'authentification sont détectés dans un intervalle de 10 minutes, l'adresse IP sera ban pendant 24h.

Pour être notifié par email, modifier la ligne commençant par action :

```
action = %(action_mw)s
```

Modifier l'adresse de destinataire et d'expéditeur :

```
destemail = admin@linuxize.com
sender = root@linuxize.com
```

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

```
sudo systemctl restart fail2ban.service
```

Vérification :

```
systemctl status fail2ban.service
```

Les jails

Fail2ban utilise un concept de jails (prisons). Une jail décrit un service et comprend des notions de filtres ainsi que d'action. Lorsque les données sont écrites dans les logs,fail2ban va compter les patterns recherchés du service à surveiller pour y appliquer une action quand ça match.

Fail2ban est fournit avec plusieurs jails pour différents services. Une jail peut être définie manuellement.

- Pour activer une jail, il faut ajouter la directive enabled = true juste après le titre.
- Exemple pour le service sshd (toujours dans le fichier jail.local) :

```
- [sshd]
- enabled  = true
- maxretry  = 3
- findtime  = 1d
- bantime  = 4w
```

```
ignoreip  = 127.0.0.1/8 192.168.1.0/24
```

- Les adresses IP 127.x.x.x et 192.168.1.x sont en liste blanche.
- Toutes autres adresses IP sera ban, en cas de 3 échecs d'authentification au service ssh dans un laps de temps de 24h, pour une durée de 4 semaines.

Pour résumer

Installation avec backend systemd

```
sudo apt install -y fail2ban iptables
sudo cp /etc/fail2ban/jail.{conf,local}
sudo sed -i 's/backend = auto/backend = systemd/' /etc/fail2ban/jail.local
sudo systemctl restart fail2ban.service
systemctl status fail2ban.service
sleep 2
sudo fail2ban-client status sshd
```

Installation avec service rsyslog

```
sudo apt install -y fail2ban iptables rsyslog
sudo cp /etc/fail2ban/jail.{conf,local}
sudo systemctl restart fail2ban.service
systemctl status fail2ban.service
sleep 2
sudo fail2ban-client status sshd
```

Fail2ban client

Fail2ban est fournit avec un outil en ligne de commande : `fail2ban-client`. Celui va permettre d'interagir avec le service fail2ban.

Pour voir toutes les options disponibles :

```
fail2ban-client -h
```

Voici quelques exemples :

- Connaitre le status du service :

```
sudo fail2ban-client status
```

- Vérifier le status de la jail sshd :

```
sudo fail2ban-client status sshd
```

- Unban une adresse IP :

```
sudo fail2ban-client set sshd unbanip 11.22.33.44
```

- Ban une adresse IP :

```
sudo fail2ban-client set sshd banip 11.22.33.44
```

Conclusion

L'intégration de **GLPI** avec **NCPA** et **Fail2Ban** permet de renforcer la gestion et la sécurité du parc informatique. **NCPA** facilite la supervision en offrant une collecte efficace des métriques système et réseau, améliorant ainsi la réactivité face aux incidents. De son côté, **Fail2Ban** protège l'infrastructure en bloquant automatiquement les tentatives d'accès malveillantes, réduisant les risques d'intrusion.

Cette combinaison d'outils assure une meilleure visibilité sur l'état des équipements et une sécurité renforcée, tout en optimisant la gestion des incidents. L'automatisation des tâches de surveillance et de protection permet non seulement de gagner en efficacité mais aussi de garantir un environnement informatique plus stable et sécurisé.

En conclusion, ce projet démontre l'importance d'une approche proactive et centralisée pour la gestion et la sécurisation des infrastructures IT, en s'appuyant sur des outils open-source performants et complémentaires.