

Adame BENYOUB



PAPPE NAGIOSXI

Nagios[®]
XI[™]



Session 2025

BTS SIO SISR

Sommaire

Introduction.....	2
Contexte	2
Installation et configuration de Nagios XI	2
Supervision Debian.....	7
Prérequis (sur la machine Debian à superviser)	7
Installation de NCPA (sur la machine Debian à superviser)	7
Ajout du serveur Debian	8
Installation et configuration de l'agent Nagios XI	12
Fail2Ban.....	13
Introduction.....	13
Installation.....	14
Les Jails.....	16

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.

```
Nagios XI Installation Complete!
```

```
-----
```

```
You can access the Nagios XI web interface by visiting:
```

```
http://votreadresseip/nagiosxi/
```

Voici les paramètres à entrer :

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://192.168.65.135/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) ?		

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.			

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

Nagios XI Installation

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

Admin Account Settings

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

L'installation est en cours :



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

Mot de passe

[se connecter à nagios xi >](#)

On accepte le contrat de licence :

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](#)

Nous voici désormais connecté à notre Nagios XI fonctionnel.

Accueil Dashboard

Guide de démarrage

Tâches courantes:

- Modifiez vos paramètres de compte
- Modifiez vos paramètres de notification
- Configurez votre installation de surveillance

Mise en route:

- Renseignez-vous sur XI
- Inscrivez-vous pour les nouvelles XI

Tâches administratives

Tâche

Tâches de configuration initiales:

- Configurez les paramètres du système
- Configurez les paramètres de messagerie

Tâches en cours:

- Configurez votre installation de surveillance
- Ajoutez de nouveaux comptes utilisateurs

Résumé de l'état d'accueil

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

Dernière mise à jour: 2023-05-01 19:48:31

Résumé de l'état de service

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

Dernière mise à jour: 2023-05-01 19:48:31

Nagios XI 5.9.3 • Check for Updates

En cliquant sur « Détails » puis « Etat du service » on peut voir l'état de service du 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
Bbmap
Hypermap
Minemap
NagVis
Carte d'état du réseau

Gestion des incidents

Latest Alerts
Les temps d'arrêt prévu
Remerciements
Mass Acknowledge

Projection 1-12 de 12 nombre total d'enregistrements

Hôte	Service	Statut	Durée	Tentative	Dernière vérification	Informations sur l'état
localhost	Current Load	Bien	14m 45s	1/4	2023-05-01 19:44:58	OK - Charge moyenne: 0.57, 0.86, 0.66
	Current Users	Bien	14m 20s	1/4	2023-05-01 19:45:23	UTILISATEURS OK - 1 utilisateurs actuellement connectés sur
	HTTP	Bien	13m 55s	1/4	2023-05-01 19:45:48	HTTP OK: HTTP/1.1 200 OK - 3437 octets en 0,002 secondes de temps de réponse
	Memory Usage	Bien	13m 30s	1/4	2023-05-01 19:46:13	OK - 1540 / 1935 MB (79%) Free Memory, Used: 587 MB, Shared: 28 MB, Buffers: 945 MB, Cached: 1138 MB
	PING	Bien	13m 5s	1/4	2023-05-01 19:46:38	PING OK - Paquets perdus = 0%, RTA = 0.03 ms
	Root Partition	Bien	12m 40s	1/4	2023-05-01 19:47:03	DISK OK - free space / 13364 MB (74,11% inuse=88%):
	SSH	Bien	12m 15s	1/4	2023-05-01 19:47:28	SSH OK - OpenSSH_8.4p1 Debian-5-deb11u1 (protocol 2.0)
	Service Status - cron	Bien	11m 50s	1/4	2023-05-01 19:47:53	• cron.service - Regular background program processing daemon
	Service Status - httpd	Bien	11m 25s	1/4	2023-05-01 19:48:18	• apache2.service - The Apache HTTP Server
	Service Status - mysqld	Bien	11m 0s	1/4	2023-05-01 19:48:43	• mariadb.service - MariaDB 10.5.19 database server
	Swap Usage	Bien	10m 29s	1/4	2023-05-01 19:49:14	SWAP OK - 100% libre (967 MB sur un total de 974 MB)
	Total Processes	Bien	10m 14s	1/4	2023-05-01 19:49:29	PROCS OK: 86 processus avec ETAT = RSZDT

Dernière mise à jour: 2023-05-01 19:49:42

Page 1 of 1 15 Per Page Aller

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 :

```
# deb cdrom:[Debian GNU/Linux 11.5.0 _Bullseye_ - Official amd64 NETINST 20220910-10:38]/ bullseye >
#deb cdrom:[Debian GNU/Linux 11.5.0 _Bullseye_ - Official amd64 NETINST 20220910-10:38]/ bullseye m
deb http://deb.debian.org/debian/ bullseye main
deb-src http://deb.debian.org/debian/ bullseye main

deb http://security.debian.org/debian-security bullseye-security main
deb-src http://security.debian.org/debian-security bullseye-security main

# bullseye-updates, to get updates before a point release is made;
# see https://www.debian.org/doc/manuals/debian-reference/ch02.en.html#updates_and_backports
deb http://deb.debian.org/debian/ bullseye-updates main
deb-src http://deb.debian.org/debian/ bullseye-updates main

# This system was installed using small removable media
# (e.g. netinst, live or single CD). The matching "deb cdrom"
# entries were disabled at the end of the installation process.
# For information about how to configure apt package sources,
# see the sources.list(5) manual.
deb https://repo.nagios.com/deb/buster /_
```

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 :

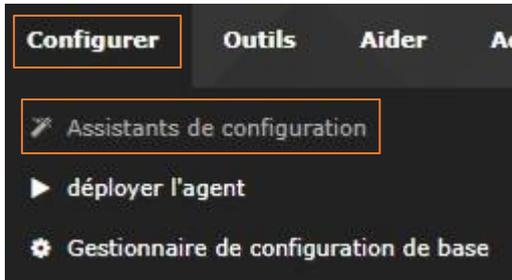
```
[api]  
  
#  
# The token that will be used to log into the basic web GUI (API browser, graphs, top charts, etc)  
# and to authenticate requests to the API and requests through check_ncpa.py  
#  
community_string = nagios
```

Nous redémarrons ensuite le service NCPA

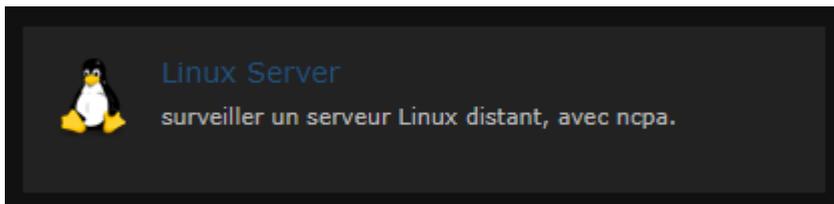
```
root@glpi:~# service ncpa_listener restart_
```

Ajout du serveur Debian

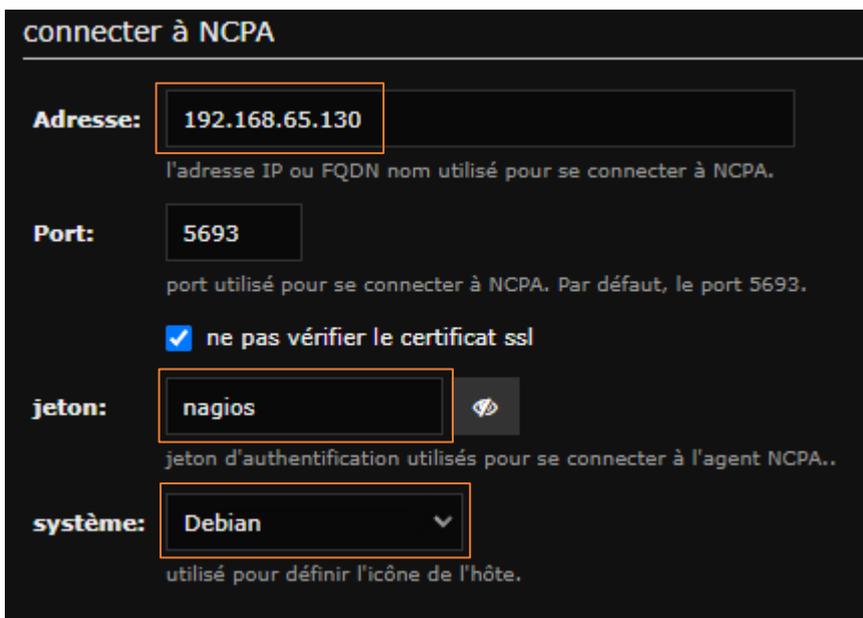
Nous allons désormais ajouter le serveur Debian précédemment configuré au serveur Nagios XI, pour cela, se diriger sur l'interface d'administration de Nagios XI puis cliquer sur « Configurer » et « Assistants de configuration »



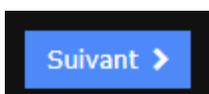
Cliquer ensuite sur « Linux Serveur »



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

A screenshot of the 'connecter à NCPA' (connect to NCPA) form. The form fields are as follows: 'Adresse:' (Address) with the value '192.168.65.130'; 'Port:' (Port) with the value '5693'; a checked checkbox for 'ne pas vérifier le certificat ssl' (do not verify the ssl certificate); 'jeton:' (token) with the value 'nagios'; and 'système:' (system) with a dropdown menu set to 'Debian'. Each field is highlighted with an orange box. Below each field is a small explanatory text.

On clique ensuite sur « Suivant »



On peut ensuite sélectionner les paramètres désirés :

métriques système

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** 126
▲ 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** 1
▲ 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** 25.6 %
▲ 50 % ⓘ 80 %
- Swap d'utilisation**
surveiller le pourcentage d'échange alloué utilisé par le système.. **utilisation actuelle du swap** 0 %
▲ 5 % ⓘ 10 %

les métriques de disque

spécifier les disques du l'alerte et pourcentages critiques pour la capacité du disque.

disque / montage	Statut actuel	seuils
<input checked="" type="checkbox"/> \	6.2 % ⓘ	▲ 70 % ⓘ 90 %
<input checked="" type="checkbox"/> \sys\fs\cgroup	0 % ⓘ	▲ 70 % ⓘ 90 %

Et on clique ensuite sur « Suivant »



On définit ensuite les paramètres de surveillance et on clique 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.

La configuration est terminée

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 192.168.65.130](#)
- [Voir les photos récentes de configuration](#)

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 connaître :

- `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.