

Service de supervision Nagios XI



Table des matières

Contexte StadiumCompany	2
Cahier des charges Stadiumcompany.....	4
Mission 8	4
Solution :	6
Projet	6
Objectif du projet.....	6
Mise en place du serveur de supervision Nagios XI	7
Configuration de base du serveur.....	7
Installation du service NagiosXI	7
Supervision du réseau	11
SNMP.....	11
Windows.....	11
Linux	15
NCPA.....	18
Windows.....	18
Linux	22
Autodiscovery.....	26
Conclusion.....	29

Contexte StadiumCompany

StadiumCompany gère un grand stade et avait initialement mis en place un réseau de communication avancé lors de la construction. Cependant, au fil du temps, l'entreprise a ajouté de nouveaux équipements et augmenté les connexions sans tenir compte de ses objectifs commerciaux à long terme ni de la conception de son infrastructure réseau. Cela a conduit à des problèmes de bande passante et de gestion du trafic, limitant la capacité de la société à offrir des services de qualité.

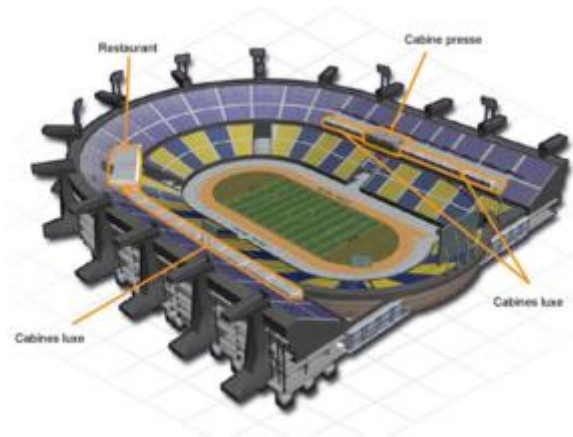


Maintenant, la direction de StadiumCompany souhaite améliorer la satisfaction de ses clients en introduisant de nouvelles technologies et en permettant l'organisation de concerts, mais le réseau actuel ne le permet pas. Sachant qu'elle ne possède pas l'expertise nécessaire en matière de réseau, la direction a décidé de faire appel à des consultants réseau pour concevoir, gérer et mettre en œuvre ce projet en trois phases.

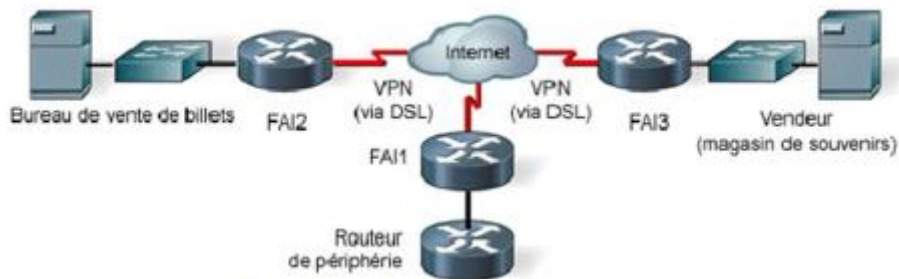
La première phase consiste à planifier le projet et à préparer une conception réseau de haut niveau. Pour cela, StadiumCompany a engagé NetworkingCompany, une société spécialisée en conception de réseaux, qui a interrogé le personnel du stade pour comprendre l'organisation et les installations.



StadiumCompany emploie 170 personnes à temps plein, dont 35 dirigeants et responsables, ainsi que 135 employés. Ils ont également recours à environ 80 intérimaires pour des événements spéciaux. Tous les employés, à l'exception des préposés au terrain et des gardiens, utilisent des PC et des téléphones connectés à un PABX vocal numérique.



Le stade propose des installations pour deux équipes sportives, une équipe visiteuse, un restaurant de luxe et un fournisseur de concessions. Il dispose également de deux sites distants, une billetterie en centre-ville et une boutique de souvenirs, connectés via DSL à un FAI local.



Le stade est construit sur deux niveaux, avec des locaux techniques reliés par des câbles à fibre optique en raison de sa grande taille. Les équipes sportives ont leurs bureaux et installations, tandis que le restaurant de luxe loue également des bureaux auprès de StadiumCompany

En résumé, StadiumCompany souhaite moderniser son réseau pour répondre aux besoins actuels et futurs, et a fait appel à des experts pour le guider à travers ce processus de mise à niveau.

Cahier des charges Stadiumcompany

Le Cahier des Charges de StadiumCompany révèle votre intégration au sein de la division Systèmes d'Information (SI) de l'entreprise pour cette année. Votre mission centrale consistera à assumer la responsabilité de l'administration des systèmes et des réseaux informatiques.

StadiumCompany se compose de plusieurs sites distincts, chacun ayant un rôle spécifique :

1. Site 1 : Stade - Ce site est le cœur de l'entreprise, abritant l'hébergement informatique, le siège social et le centre administratif. Il est le pivot autour duquel s'articulent toutes les opérations et activités de l'entreprise.

2. Site 2 : Billetterie - Ce site est dédié à la gestion des ventes de billets, un élément essentiel pour les événements sportifs et les spectacles organisés au stade.

3. Site 3 : Magasin - Ce site est spécialement conçu pour la vente d'articles souvenirs, offrant aux fans et aux visiteurs la possibilité d'acheter des produits liés à l'équipe ou aux événements.

Le Cahier des Charges insiste sur la nécessité de documenter les différentes solutions retenues pour le projet en fonction de leur niveau de complexité. Cette approche méthodique garantira que chaque aspect de l'infrastructure informatique soit clairement spécifié et que les procédures soient consignées de manière exhaustive. Cela s'inscrit dans la vision globale adoptée par StadiumCompany pour assurer une gestion efficace et cohérente de ses ressources informatiques.

Votre rôle au sein de cette mission sera d'une importance cruciale, car vous devrez contribuer à façonner et à maintenir l'infrastructure technologique qui soutient les opérations de l'entreprise et qui permet de répondre aux défis uniques posés par chaque site.

Mission 8 : Mise en Place d'un Système de Supervision Open Source

Contexte : StadiumCompany recherche l'implémentation et la configuration d'une solution Open Source pour la supervision à distance des différents éléments actifs de son infrastructure systèmes et réseaux au stade, avec la gestion des alertes.

Plan de Travail : Le principal objectif du projet est de sélectionner et mettre en place une solution de surveillance des serveurs, routeurs, commutateurs, etc., qui réponde aux critères suivants :

1. **Coûts Minimaux** : Rechercher une solution open source qui limite au maximum les coûts financiers associés.
2. **Collecte d'Informations** : Mettre en place un système de collecte d'informations permettant la détection des pannes, la surveillance de la disponibilité des serveurs (Windows, Linux), des routeurs, des commutateurs, des états des imprimantes réseau, et de leurs services.
3. **Monitoring Avancé** : Configurer des fonctionnalités avancées de monitoring, telles que la surveillance de la charge CPU, de l'espace disque, de la mémoire disponible, des entrées/sorties, des processus en cours d'exécution, du taux de paquets perdus, du temps de parcours moyen, des informations d'état SNMP, du trafic réseau, de la bande passante consommée, etc.
4. **Monitoring des Services** : Surveiller les services essentiels tels que DNS, DHCP, HTTP, SMTP, POP, IMAP, FTP, etc.

5. **Gestion des Alertes** : Mettre en place un système de gestion des alertes qui notifie automatiquement par e-mail ou SMS en cas de problème ou de défaillance d'un élément du réseau.
6. **Rapports Mensuels** : Générer des rapports mensuels sur le fonctionnement des serveurs, y compris les statistiques de disponibilité et de performance.
7. **Création de Graphes** : Créer des graphiques et une cartographie du réseau pour une visualisation claire de l'infrastructure supervisée.
8. **Interface Utilisateur Conviviale** : Mettre à disposition une interface utilisateur graphique conviviale pour permettre aux utilisateurs d'interagir avec le logiciel de supervision.

Cette mission vise à garantir la surveillance proactive de l'infrastructure informatique du stade, à améliorer la réactivité en cas de problèmes, et à fournir des données exploitables pour une gestion optimale des systèmes et des réseaux. La solution open source sélectionnée doit être efficace, économique et répondre aux besoins spécifiques de StadiumCompany.

Solution :

Nagios XI est une application de supervision de réseau libre sous licence GPL (General Public Licence), fonctionnant avec le système d'exploitation linux. Cette caractéristique va dans le sens du système d'exploitation choisi auparavant : Debian, qui est une version de linux. Il a pour fonction la surveillance des hôtes et services spécifiés, alertant

Cette polyvalence permet d'utiliser Nagios dans différentes entreprises, quelque soit la topologie du réseau, et la nature des systèmes d'exploitation utilisés. Ce logiciel est composé de trois parties :

1. Le moteur de l'application (manager), qui gère et ordonne les supervisions des différents équipements,
2. Les plugins qui servent d'intermédiaire entre l'hôte, chez qui l'on souhaite récupérer des informations, et le moteur de Nagios. Il faut noter que pour accéder à une certaine ressource sur un hôte, il faut installer les plugins (check snmp) sur le système d'exploitation (linux) de Nagios, et installer l'agent SNMP correspondant sur le système d'exploitation de l'hôte en question (PC, Serveur). Dans le cadre de mon projet, les hôtes étant des switchs, il suffit d'activer le protocole SNMP au niveau du switch, et de créer une communauté afin que les plugins communiquent avec le switch.
3. L'interface web, qui permet d'avoir une vue d'ensemble de l'état des machines du parc informatique supervisé, et qui permet ainsi d'intervenir le plus rapidement possible en ciblant précisément la panne

Projet

Objectif du projet

L'objectif du projet est de mettre en place un service de supervision qui permettra de surveiller le matériel du réseau de très près, cela permettra de prévenir des pannes matérielles et de pouvoir intervenir au plus vite sur ces pannes

Mise en place du serveur de supervision Nagios XI

Configuration de base du serveur

On renomme notre machine : `hostnamectl set-hostname nagiosxi`

On met une adresse IP fixe : `nano /etc/network/interfaces`

```
# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug ens32
iface ens32 inet static
address 172.20.0.40/24
gateway 172.20.0.1
```

On configure la fichier de résolution DNS : `nano /etc/resolv.conf`

```
domain stadiumcompany.com_
search stadiumcompany.com
nameserver 172.20.0.10
```

On teste la résolution DNS

```
root@nagiosxi:~# nslookup www.google.com
Server:      172.20.0.10
Address:     172.20.0.10#53

Non-authoritative answer:
Name:   www.google.com
Address: 142.250.178.132
Name:   www.google.com
Address: 2a00:1450:4007:819::2004
```

On met à jour notre machine : `apt update && apt upgrade -y`

Installation du service NagiosXI

On peut installer Nagios de deux façons :

Méthode rapide, installer via curl : `apt install curl`

`curl https://assets.nagios.com/downloads/nagiosxi/install.sh | sh`

Méthode manuelle

Création d'un répertoire tmp : `mkdir tmp`

Téléchargement du paquet dans le répertoire avec wget :

wget <http://assets.nagios.com/downloads/nagiosxi/xi-latest.tar.gz>

Décompression du fichier : `tar xzfv xi-latest.taz.gz`

Déplacement dans le répertoire nagiosxi : `cd nagiosxi/`

Puis lancement de la commande : `./fullinstall`

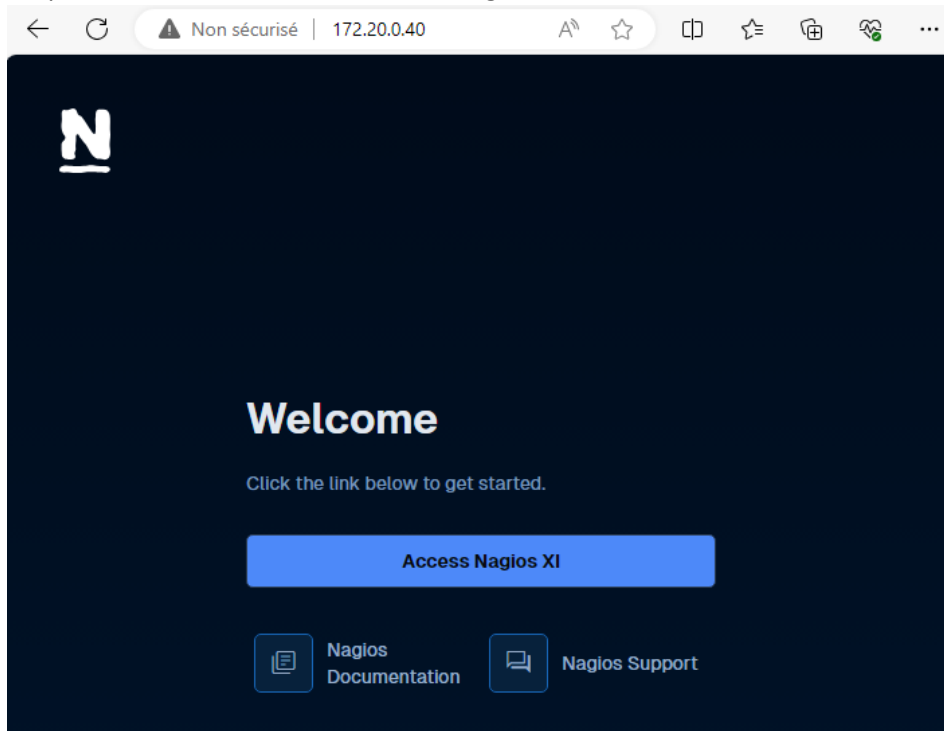
L'installation est terminée

```
Nagios XI Installation Complete!
-----

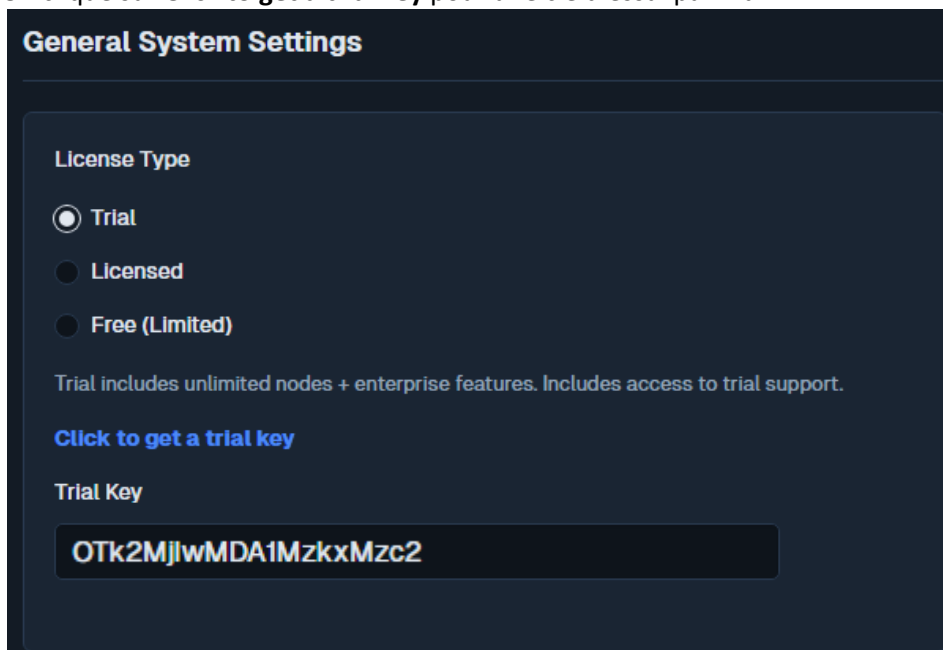
You can access the Nagios XI web interface by visiting:
  http://172.20.0.40/nagiosxi/

You have new mail in /var/mail/root
root@nagios:~#
```

On peut accéder à l'interface web de NagiosXI



On clique sur **Click to get a trial key** pour une clé d'essai par mail

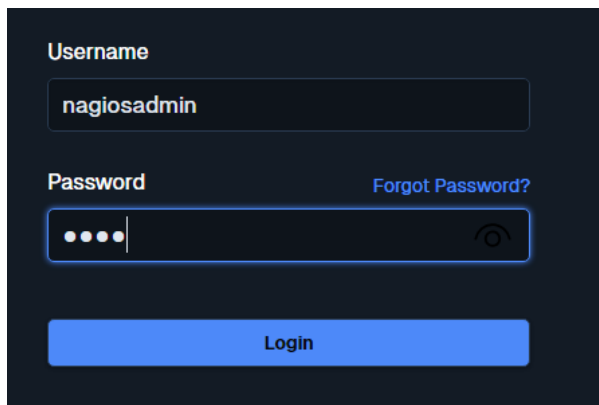


On définit les identifiants de connexion **admin**



A screenshot of the Nagios XI user creation form. It has a dark blue background with white text. The form contains four input fields: 'Username' with the value 'nagiosadmin', 'Password' with the value 'root', 'Full Name' with the value 'Nagios Administrator', and 'Email Address' with the value 'root@localhost'.

On se connecte avec les identifiants définis avant



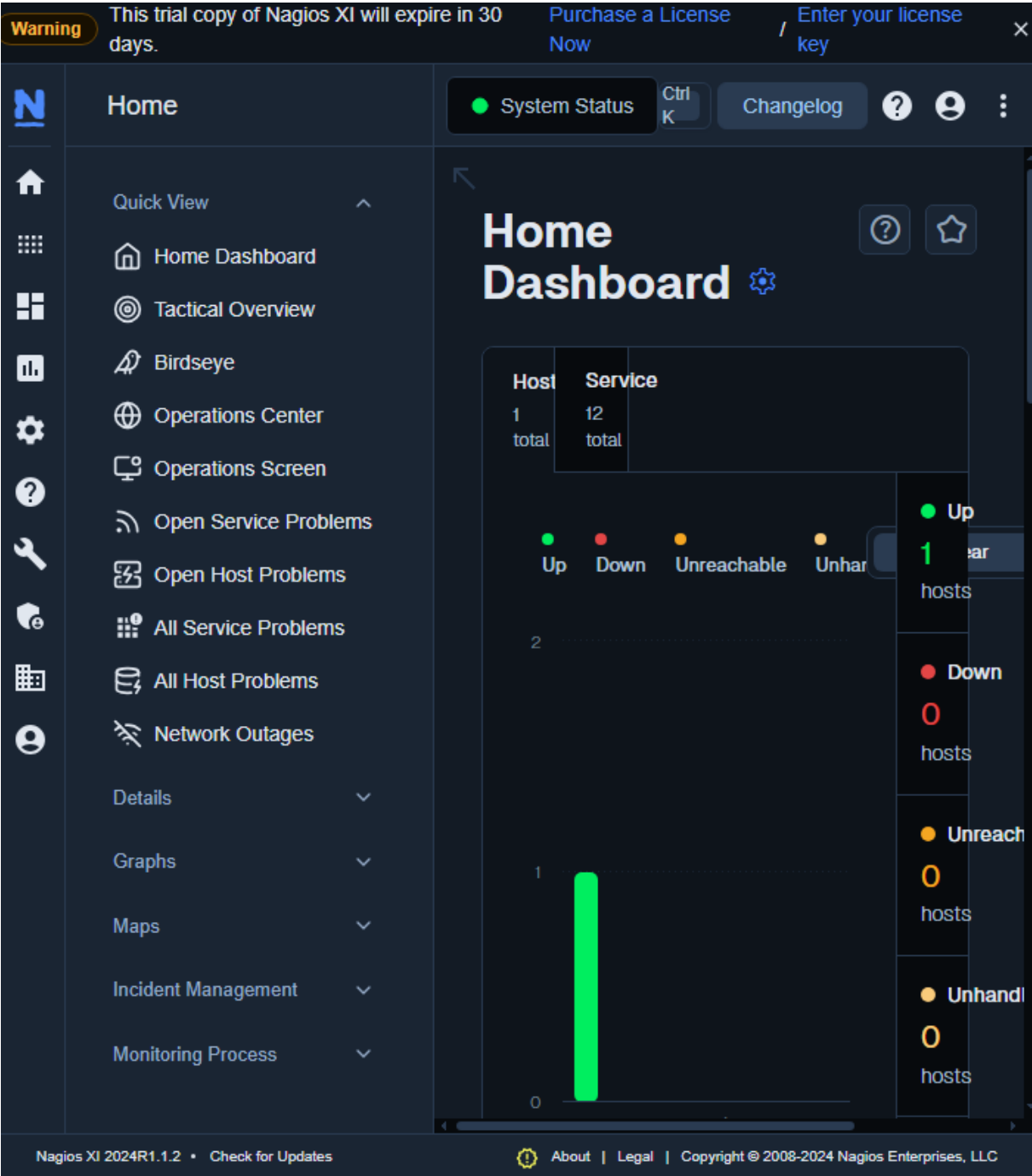
A screenshot of the Nagios XI login page. It has a dark blue background with white text. There are two input fields: 'Username' with the value 'nagiosadmin' and 'Password' which is masked with dots. To the right of the password field is a link that says 'Forgot Password?'. Below the password field is a blue button labeled 'Login'.

On accepte le **contrat de licence**



A screenshot of the Nagios XI License Agreement page. It has a dark blue background with white text. The title 'License Agreement' is at the top. Below it is a warning: 'You must agree to the Nagios Software License Terms and Conditions before continuing using this software.' The main content is a scrollable text area containing the 'Nagios Software License Terms and Conditions'. At the bottom, there is a checkbox with a checkmark and the text 'I have read, understood, and agree to be bound by the terms of the license above.' Below this is a blue button labeled 'Submit'.

On a accès à l’interface web de NagiosXI

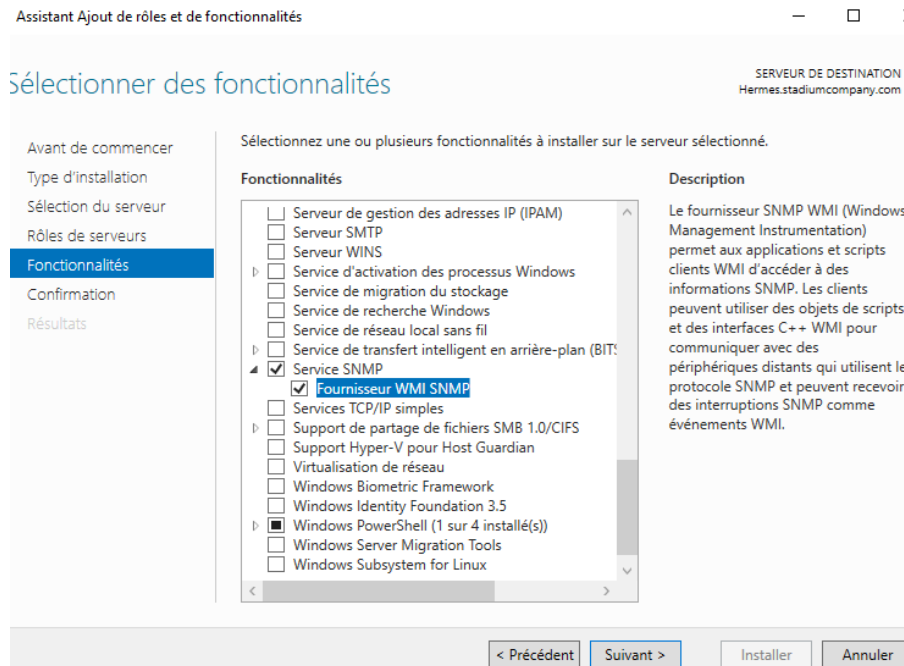


Supervision du réseau

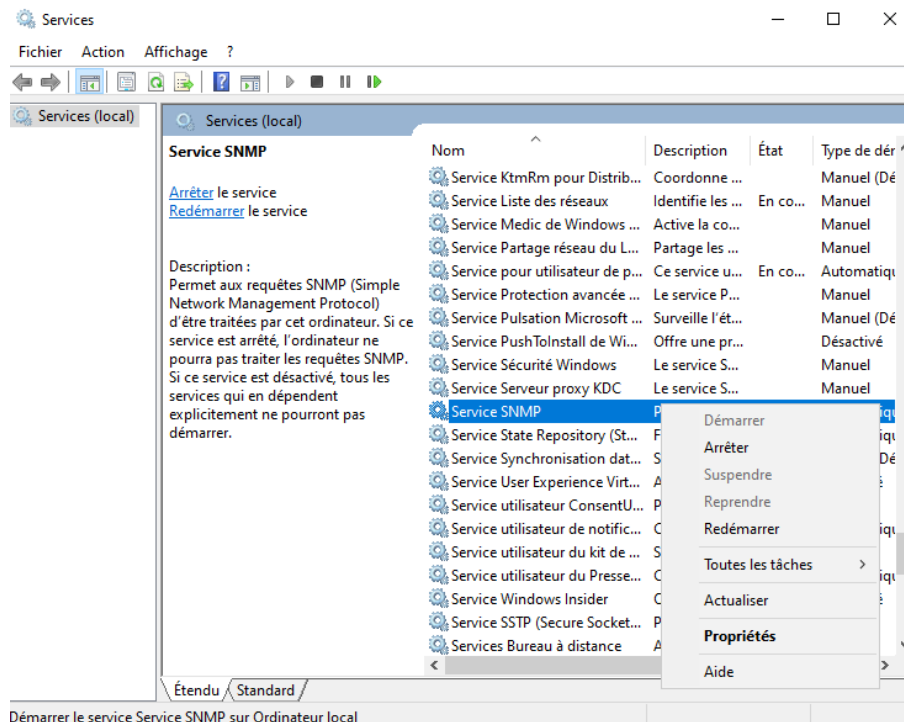
SNMP

Windows

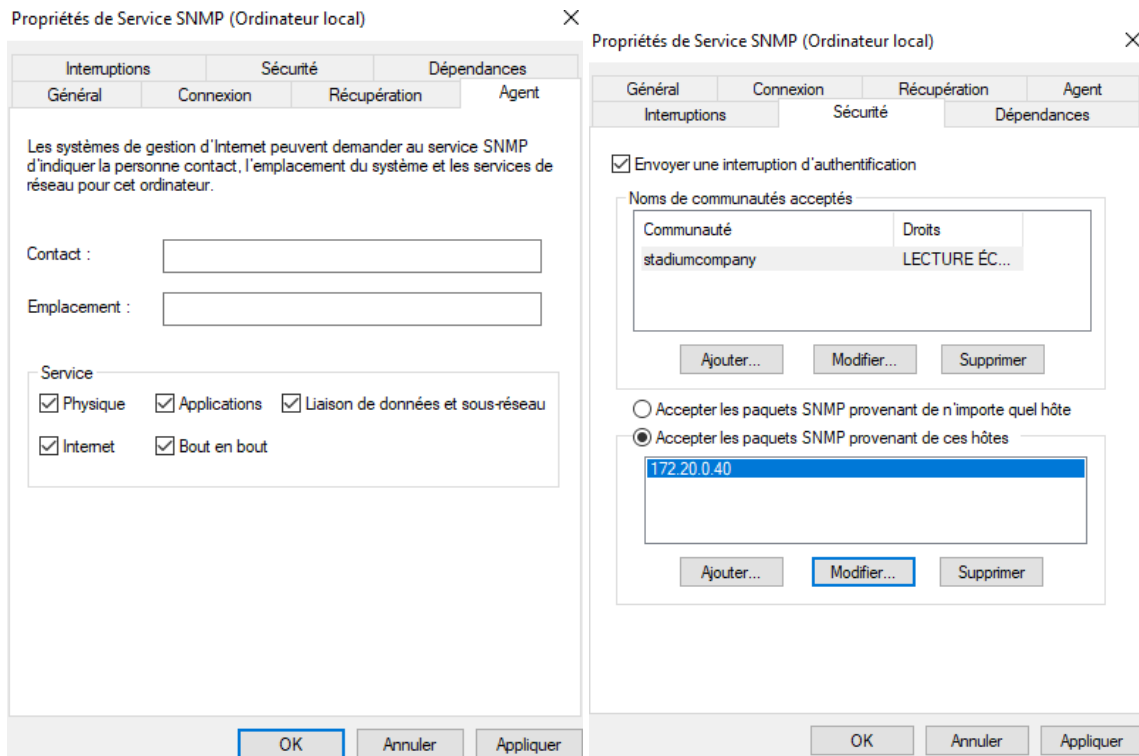
Pour la supervision SNMP Windows, il faut installer le service **SNMP** sur notre machine Windows



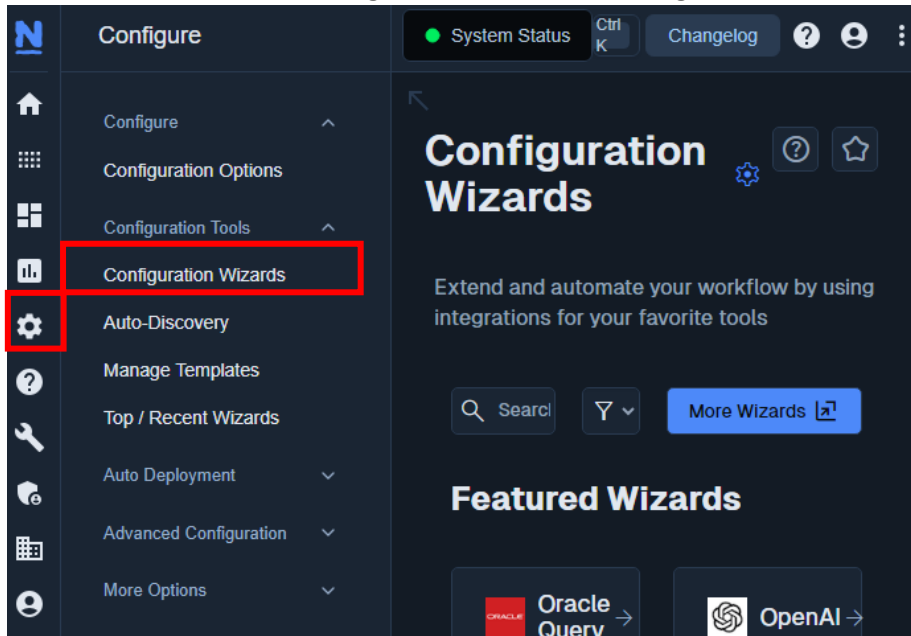
On va ensuite dans **Services** pour changer les propriétés du **service SNMP**



On change les valeurs dans **Agent** et **Sécurité** et on applique



On retourne sur l'**interface NagiosXI** et on va dans **Configure Wizards**



On cherche **Windows SNMP** et on rentre les informations de la machine (IP, SNMP)

Configuration Wizards

Extend and automate your workflow by using integrations for your favorite tools

No Filter

More Wizards

Wizards

Linux SNMP
Monitor a Linux workstation or server using SNMP.

SNMP
Monitor a device, service, or application using SNMP.

SNMP Trap
Monitor SNMP Traps.

SNMP Walk
Scan an SNMP-enabled device for elements to monitor.

Windows SNMP
Monitor a Microsoft® Windows workstation or server using SNMP.

Windows SNMP Configuration Wizard

Step 1

Windows Machine Information

* IP Address ⓘ

* Operating System

SNMP Settings

Specify the settings used to monitor the Windows machine via SNMP

* SNMP Version ⓘ


* SNMP Port ⓘ

SNMP Version Settings

* SNMP Community ⓘ


Next >


Nagios a retrouvé le nom de la machine (hermes) et on sélectionne les éléments à superviser
On choisit aussi le temps de réponse vers le serveur NagiosXI et on peut terminer la configuration



Windows SNMP Configuration Wizard

Step 2





Windows Machine Details

IP Address:

172.20.0.10

Host Name: ⓘ

Hermes.stadiumcompany.com

Server Metrics

Specify which services you would like to monitor for the Windows machine

☒ Ping ⓘ

▲

80

%

●

90

%

☒ CPU ⓘ

▲

80

%

●

90

%

☒ Physical Memory Usage ⓘ

▲

80

%

●

90

%

☒ Virtual Memory Usage ⓘ

▲

5

%


●

10

%


☒ Disk Usage ⓘ


The wizard will populate detected drives automatically. To add more drives select a new drive from the dropdown list.



Windows SNMP Configuration Wizard

Step 3





Monitoring Settings

Define basic parameters that determine how the host and service(s) should be monitored.

Under normal circumstances:

Monitor the host and service(s) every

15

 minutes

When a potential problem is first detected:

Re-check the host and service(s) every

1

 minutes up to

5

 times before sending a notification

< Back

Next >

Finish with Defaults

Cancel

Pour vérifier la remontée, on va dans **View** puis **Service Detail**

The screenshot displays the Nagios XI interface. On the left sidebar, the 'Service Detail' link under the 'Host Detail' section is highlighted with a red box. The main content area shows the 'Service Status' page for 'all services'. It features two summary cards:

- Host Status Summary**: Shows 2 Up (green), 0 Down (red), 0 Unreachable (yellow), and 0 Pending (grey). Problems are 0, and All hosts are 2.
- Service Status Summary**: Shows 13 OK (green), 0 Warning (yellow), 0 Unknown (orange), and 0 Critical (red). Pending services are 5, Problems are 0, Unhandled Problems are 0, and All services are 18.

Both summaries were last updated on 2024-05-06 13:44:47. Below these is a table listing individual service checks with columns for Host, Service, Status, Duration, Attempt, Last Check, and Status Information.

Host ↓	Service ↓	Status ↓	Duration ↓	Attempt ↓	Last Check ↓	Status Information ↓
Hermes.stadiumcompany.com >🔍 📄	CPU Usage	OK	N/A	1/5	2024-05-06 13:44:44	2 CPU, average load 19.0% < 80% : OK
	Drive C: Disk Usage	Pending	N/A	1/5	N/A	Service check is pending... Check is scheduled for 2024-05-06 13:45:18

Linux

On installe le service SNMP : `apt install snmpd snmp -y`

On efface le contenu du fichier de configuration SNMP : `echo "" > /etc/snmp/snmpd.conf`

Et on l'édite de cette manière : `nano /etc/snmp/snmpd.conf`

```
GNU nano 5.4 /etc/snmp/snmpd.conf *
sysLocation stadiumcompany
sysContact root <root@stadiumcompany.com>

#Snmpecoute toutes les adresses IPv4 du serveur
agentaddress udp:161,udp6:[::1]:161

#nom de communauté pour l'accès par le réseau
rocommunity stadiumcompany default_
```

On redémarre le service : `service snmpd restart`

On vérifie son bon fonctionnement

```
root@glpi:~# service snmpd status
• snmpd.service - Simple Network Management Protocol (SNMP) Daemon.
  Loaded: loaded (/lib/systemd/system/snmpd.service; enabled; vendor preset: enabled)
  Active: active (running) since Mon 2024-05-06 15:53:53 CEST; 6s ago
  Process: 8922 ExecStartPre=/bin/mkdir -p /var/run/agentx (code=exited, status=0/SUCCESS)
  Main PID: 8923 (snmpd)
  Tasks: 1 (limit: 2280)
  Memory: 4.7M
  CPU: 21ms
  CGroup: /system.slice/snmpd.service
          └─8923 /usr/sbin/snmpd -LDw -u Debian-snmp -g Debian-snmp -I -smux mteTrigger mte

mai 06 15:53:53 glpi systemd[1]: snmpd.service: Succeeded.
mai 06 15:53:53 glpi systemd[1]: Stopped Simple Network Management Protocol (SNMP) Daemon..
mai 06 15:53:53 glpi systemd[1]: Starting Simple Network Management Protocol (SNMP) Daemon....
mai 06 15:53:53 glpi systemd[1]: Started Simple Network Management Protocol (SNMP) Daemon..
lines 1-15/15 (END)
```

On peut vérifier le service SNMP avec : `snmpwalk -v1 -c stadiumcompany 172.20.0.30`

```
.1.5.4
iso.3.6.1.2.1.88.1.4.3.1.1.6.95.115.110.109.112.100.95.109.116.101.84.114.105.103.103.101.114.7
105.108.117.114.101 = OID: iso.3.6.1.2.1.88.2.0.4
iso.3.6.1.2.1.88.1.4.3.1.1.6.95.115.110.109.112.100.95.109.116.101.84.114.105.103.103.101.114.7
108.108.105.110.103 = OID: iso.3.6.1.2.1.88.2.0.3
iso.3.6.1.2.1.88.1.4.3.1.1.6.95.115.110.109.112.100.95.109.116.101.84.114.105.103.103.101.114.7
.114.101.100 = OID: iso.3.6.1.2.1.88.2.0.1
iso.3.6.1.2.1.88.1.4.3.1.1.6.95.115.110.109.112.100.95.109.116.101.84.114.105.103.103.101.114.7
.115.105.110.103 = OID: iso.3.6.1.2.1.88.2.0.2
iso.3.6.1.2.1.88.1.4.3.1.2.6.95.115.110.109.112.100.95.108.105.110.107.68.111.119.110 = STRING
mpd"
iso.3.6.1.2.1.88.1.4.3.1.2.6.95.115.110.109.112.100.95.108.105.110.107.85.112 = STRING: "_snmpd
iso.3.6.1.2.1.88.1.4.3.1.2.6.95.115.110.109.112.100.95.109.116.101.84.114.105.103.103.101.114.7
105.108.117.114.101 = STRING: "_snmpd"
iso.3.6.1.2.1.88.1.4.3.1.2.6.95.115.110.109.112.100.95.109.116.101.84.114.105.103.103.101.114.7
108.108.105.110.103 = STRING: "_snmpd"
iso.3.6.1.2.1.88.1.4.3.1.2.6.95.115.110.109.112.100.95.109.116.101.84.114.105.103.103.101.114.7
.114.101.100 = STRING: "_snmpd"
iso.3.6.1.2.1.88.1.4.3.1.2.6.95.115.110.109.112.100.95.109.116.101.84.114.105.103.103.101.114.7
.115.105.110.103 = STRING: "_snmpd"
iso.3.6.1.2.1.88.1.4.3.1.3.6.95.115.110.109.112.100.95.108.105.110.107.68.111.119.110 = STRING
nkUpDown"
iso.3.6.1.2.1.88.1.4.3.1.3.6.95.115.110.109.112.100.95.108.105.110.107.85.112 = STRING: "_link
"
iso.3.6.1.2.1.88.1.4.3.1.3.6.95.115.110.109.112.100.95.109.116.101.84.114.105.103.103.101.114.7
105.108.117.114.101 = STRING: "_triggerFail"
iso.3.6.1.2.1.88.1.4.3.1.3.6.95.115.110.109.112.100.95.109.116.101.84.114.105.103.103.101.114.7
108.108.105.110.103 = STRING: "_triggerFire"
iso.3.6.1.2.1.88.1.4.3.1.3.6.95.115.110.109.112.100.95.109.116.101.84.114.105.103.103.101.114.7
.114.101.100 = STRING: "_triggerFire"
iso.3.6.1.2.1.88.1.4.3.1.3.6.95.115.110.109.112.100.95.109.116.101.84.114.105.103.103.101.114.7
.115.105.110.103 = STRING: "_triggerFire"
iso.3.6.1.2.1.92.1.1.1.0 = Gauge32: 1000
iso.3.6.1.2.1.92.1.1.2.0 = Gauge32: 1440
iso.3.6.1.2.1.92.1.2.1.0 = Counter32: 0
iso.3.6.1.2.1.92.1.2.2.0 = Counter32: 0
```


On procède à la même manipulation que **Windows mais avec Linux**


Configuration Wizards


Extend and automate your workflow by using integrations for your favorite tools


No Filter

More Wizards

Wizards

 **Linux SNMP** →
Monitor a Linux workstation or server using SNMP.

 **SNMP** →
Monitor a device, service, or application using SNMP.

 **Linux SNMP Configuration Wizard**

Step 1

Linux Machine Information

* IP Address ⓘ

172.20.0.30

SNMP Settings

Specify the settings used to monitor the Linux machine via SNMP.

* SNMP Version ⓘ

2c

* SNMP Port ⓘ


161

SNMP Version Settings

* SNMP Community ⓘ


stadiumcompany

Next >



Linux SNMP Configuration Wizard

Step 2



Linux Machine Details

IP Address

172.20.0.30

Host Name ⓘ

172.20.0.30

Server Metrics

Specify which services you would like to monitor for the Linux machine.

☒ CHECKED ⓘ

☒ CPU ⓘ



80

%



90


%

☒ Physical Memory Usage ⓘ



80

%



90


%

☒ Swap Usage ⓘ



5


%



10


%


☒ Disk Usage ⓘ



Linux SNMP Configuration Wizard

Step 3





Monitoring Settings

Define basic parameters that determine how the host and service(s) should be monitored.

Under normal circumstances:

Monitor the host and service(s) every

5

minutes

When a potential problem is first detected:

Re-check the host and service(s) every

1

minutes up to

5





times before sending a notification

< Back

Next >

Finish with Defaults

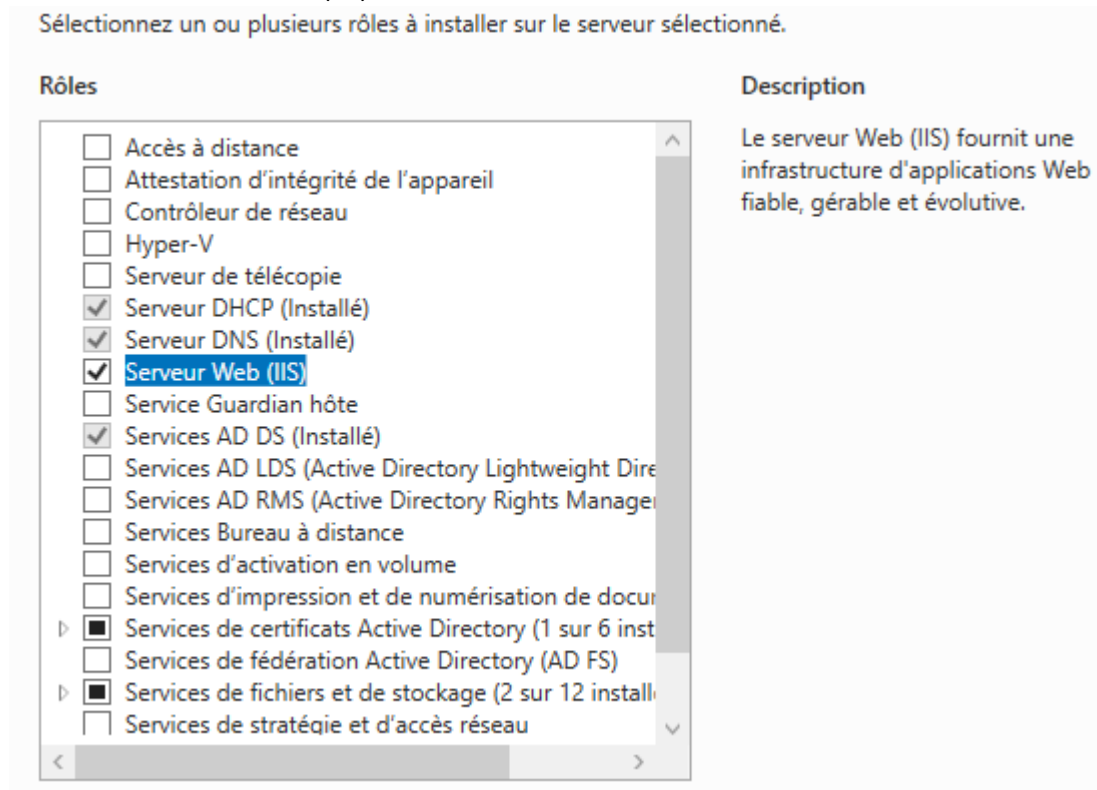
Cancel

Host ↓	Service ↓	Status ↓	Duration ↓	Attempt ↓	Last Check ↓	Status Information ↓
<div><div></div>172.20.0.30</div>	<div> CPU Usage</div>	<div><div></div>Pending</div>	<div><div></div>N/A</div>	<div>1/5</div>	<div>N/A</div>	Service check is pending... Check is scheduled for 2024-05-06 14:00:22
	<div> Memory Usage</div>	<div><div></div>Pending</div>	<div><div></div>N/A</div>	<div>1/5</div>	<div>N/A</div>	Service check is pending... Check is scheduled for 2024-05-06 14:01:03
	<div> Ping</div>	<div><div></div>Pending</div>	<div><div></div>N/A</div>	<div>1/5</div>	<div>N/A</div>	Service check is pending... Check is scheduled for 2024-05-06 14:01:44
	<div> Swap Usage</div>	<div><div></div>Pending</div>	<div><div></div>N/A</div>	<div>1/5</div>	<div>N/A</div>	Service check is pending... Check is scheduled for 2024-05-06 14:02:25

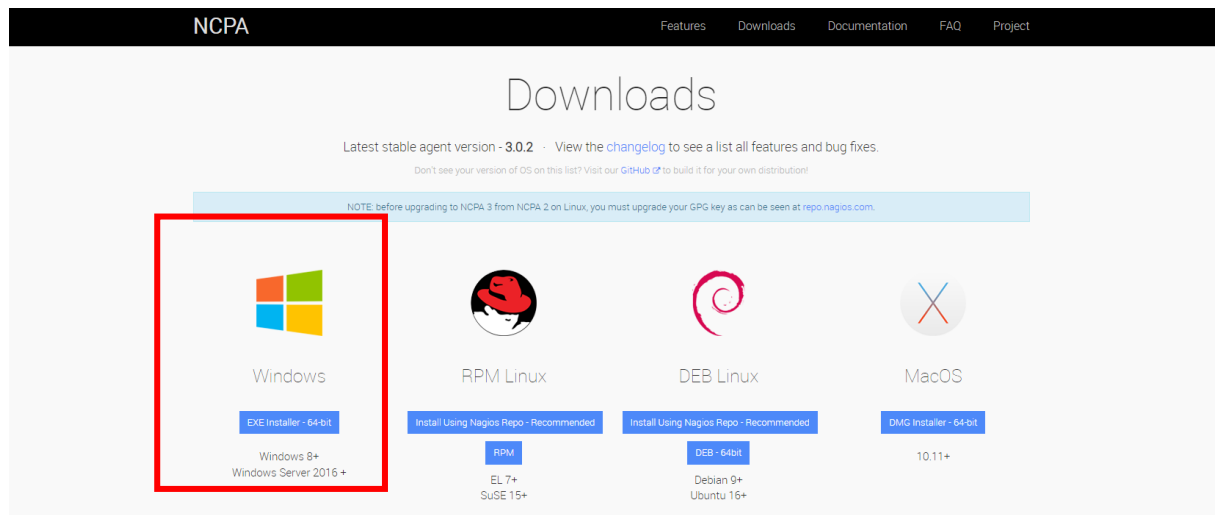
NCPA

Windows

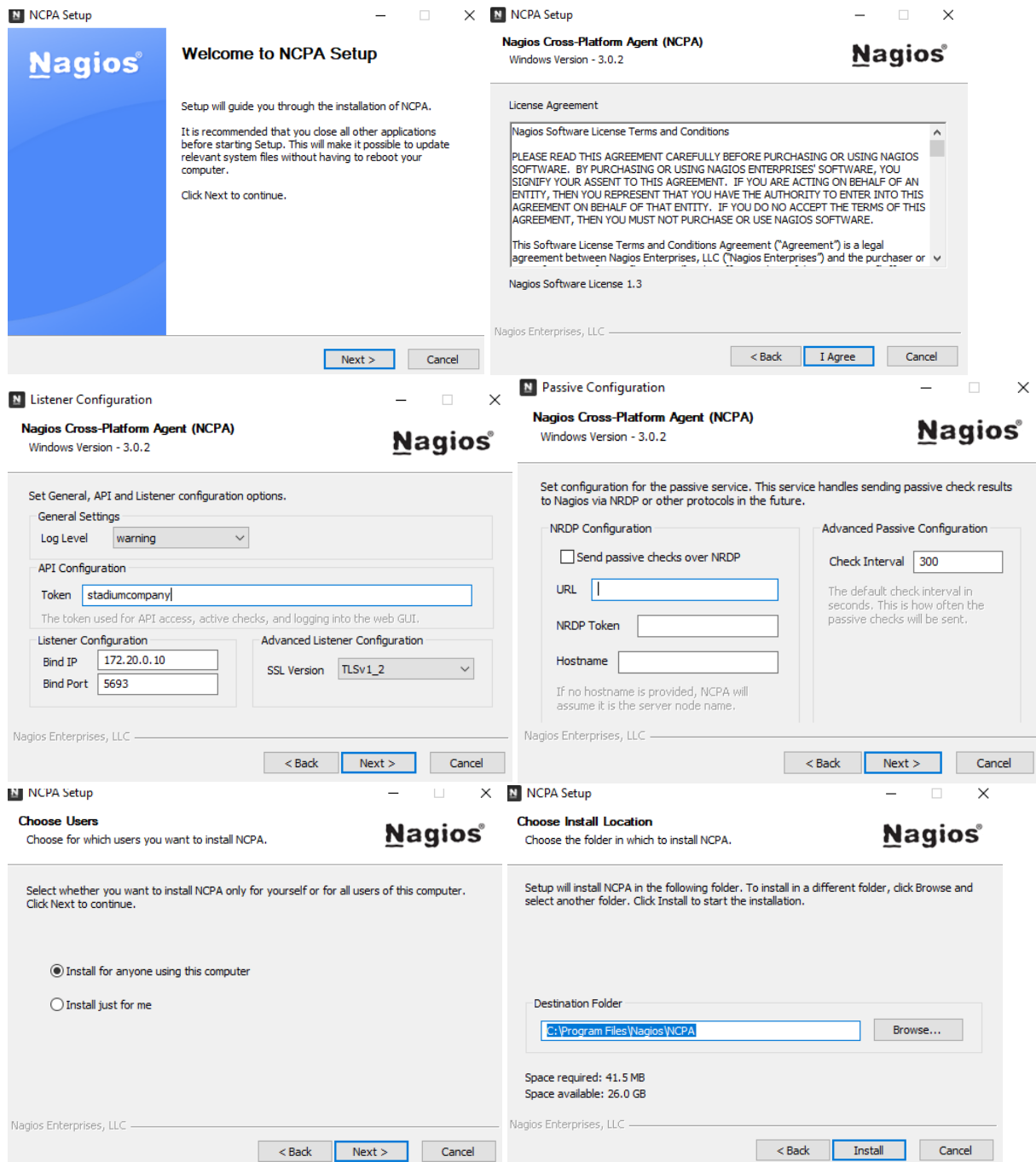
On installe le service Web (IIS)



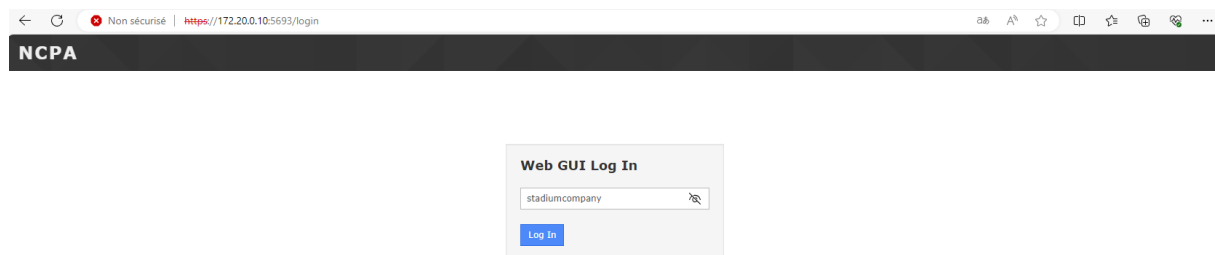
On installe ensuite l'agent NCPA (<https://www.nagios.org/ncpa/#downloads>)





On exécute le fichier puis va configurer



On peut accéder au service NCPA avec l'adresse (<https://172.20.0.10:5693>)



On lance ensuite la recherche **NCPA Windows** sur Nagios

 **Windows Server** 

Monitor a Microsoft® Windows 2008, 2012, 2016, or 2019 server with NCPA.

Setup NCPA

The agent should be installed before running this wizard

1. Download the latest version of NCPA for the system you would like to monitor
2. Follow the [installation instructions \(PDF version\)](#) and configure the token for the agent

Connect to NCPA

* Address ⓘ



172.20.0.10

* Port ⓘ

5693

☒ Do not verify SSL certificate

* Token ⓘ

.....  

Next >

Host Information

Address

172.20.0.10


Host Name ⓘ

Hermes.stadiumcompany.com

Port

5693

System



System Metrics

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

☒ CPU Usage ⓘ

▲

20

%

●

40

%

CPU

24.2

%

ⓘ

☒ Show average CPU usage instead of per cpu core

☒ User Count ⓘ

▲

2

%

●

4


%

👤

1

ⓘ

Memory Metrics



Windows Server Configuration Wizard

Step 3

⚙️

?

Monitoring Settings

Define basic parameters that determine how the host and service(s) should be monitored.

Under normal circumstances:

Monitor the host and service(s) every

5

 minutes

When a potential problem is first detected:

Re-check the host and service(s) every

1

 minutes up to

5

 times before sending a notification

< Back

Next >

Finish with Defaults

Cancel

On va dans **Service Detail** pour vérifier la remontée

Showing 1-15 of 20 total records

<< < Page 1 / 2 15 Per Page Go > >>

Search...

Host ↓	Service ↓	Status ↓	Duration ↓	Attempt ↓	Last Check ↓	Status Information ↓
● Hermes.stadiumcompany.com 📄	CPU Usage	● Pending ⓘ N/A	1/5	N/A		Service check is pending... Check is scheduled for 2024-05-06 14:22:17
	Disk Usage on C:/	● Pending ⓘ N/A	1/5	N/A		Service check is pending... Check is scheduled for 2024-05-06 14:22:47
	Disk Usage on D:/	● Pending ⓘ N/A	1/5	N/A		Service check is pending... Check is scheduled for 2024-05-06 14:23:17

Linux

Sur Linux, on installe aussi un serveur Web (apache2) puis le service NCPA (<https://www.nagios.org/ncpa/#downloads>)



`apt-get install apt-transport-https`

On ajoute le dépôt Linux dans le chemin `/etc/apt/sources.list.d/nagios.list` :

`echo "deb https://repo.nagios.com/deb/bullseye/" >> /etc/apt/sources.list.d/nagios.list`

On ajoute la clé publique de NagiosGPG : `apt install gnupg`

`wget -qO - https://repo.nagios.com/GPG-KEY-NAGIOS-V3 | apt-key add -`
`apt update`

On installe le module NCPA : `apt-get install NCPA -y`

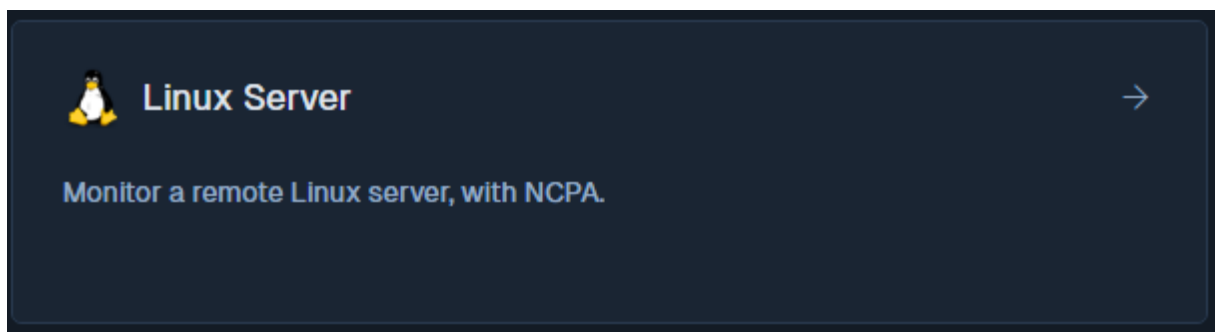
On ouvre le fichier de configuration : `nano /usr/local/ncpa/etc/ncpa.cfg`

On modifie la partie `[api]` : `community_string = stadiumcompany`

```
[api]
#
# The token that will be used to log
# and to authenticate requests to the
#
community_string = stadiumcompany_
```

On redémarre le service : `/etc/init.d/ncpa restart` puis `/etc/init.d/ncpa status`

On procède à la même remontée que Windows



1. Download the latest version of [NCPA](#) for the system you would like to monitor

2. Follow the [installation instructions \(PDF version\)](#) and configure the token for the agent

Connect to NCPA

* Address ⓘ

172.20.0.30

* Port ⓘ

5693

☒ Do not verify SSL certificate

* Token ⓘ

Show

.....



* System ⓘ

Debian



Next >

Host Information

Address

172.20.0.30


Host Name ⓘ

glpi.stadiumcompany.com

Port

5693

System






System Metrics




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

☒ Ping ⓘ

☒ Total Processes ⓘ




	150	%		250	%		129	ⓘ
--	-----	---	--	-----	---	--	-----	---

☒ CPU Usage ⓘ


	20	%		40	%		CPU 0	% ⓘ
---	----	---	---	----	---	---	-------	-----

☒ Show average CPU usage instead of per cpu core

☒ User Count ⓘ

	2	%		4	%		1	ⓘ
---	---	---	---	---	---	---	---	---

Linux Server Configuration Wizard

Step 3 

ⓘ

Monitoring Settings

Define basic parameters that determine how the host and service(s) should be monitored.

Under normal circumstances:

Monitor the host and service(s) every minutes

When a potential problem is first detected:

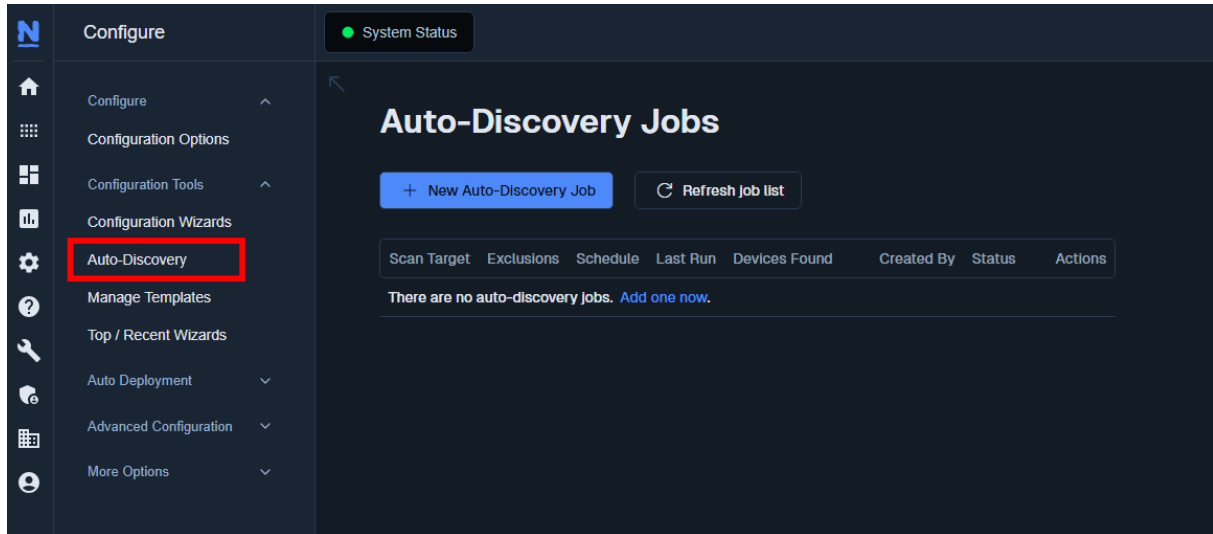
Re-check the host and service(s) every minutes up to times before sending a notification

< Back **Next >** Finish with Defaults Cancel

<div><div>●</div> glplstadiumcompany.com</div>	<div><div></div><div></div></div>	CPU Usage	<div><div>●</div> Pending</div>	<div><div>🕒</div> N/A</div>	1/5	N/A	Service check is pending... Check is scheduled for 2024-05-06 14:59:52
		Disk Usage on /	<div><div>●</div> Pending</div>	<div><div>🕒</div> N/A</div>	1/5	N/A	Service check is pending... Check is scheduled for 2024-05-06 15:00:17
		Disk Usage on /home	<div><div>●</div> Pending</div>	<div><div>🕒</div> N/A</div>	1/5	N/A	Service check is pending... Check is scheduled for 2024-05-06 15:00:42
		Disk Usage on /sys/fs/bpf	<div><div>●</div> Pending</div>	<div><div>🕒</div> N/A</div>	1/5	N/A	Service check is pending... Check is scheduled for 2024-05-06 15:01:07
		Disk Usage on /sys/fs/cgroup	<div><div>●</div> Pending</div>	<div><div>🕒</div> N/A</div>	1/5	N/A	Service check is pending... Check is scheduled for 2024-05-06 15:01:32
		Disk Usage on /tmp	<div><div>●</div> Pending</div>	<div><div>🕒</div> N/A</div>	1/5	N/A	Service check is pending... Check is scheduled for 2024-05-06 15:01:57
		Disk Usage on /var	<div><div>●</div> Pending</div>	<div><div>🕒</div> N/A</div>	1/5	N/A	Service check is pending... Check is scheduled for 2024-05-06 15:02:22

Autodiscovery

On va **Auto-Discovery**, on crée un **New Auto-Discovery Job**



On renseigne le réseau (172.20.0.0) qu'il va analyser

The screenshot shows the 'New Auto-Discovery Job' configuration form. The title 'New Auto-Discovery Job' is at the top. Below it is a subtitle: 'Use this form to configure an auto-discovery job.' The form is divided into sections: 'Auto-Discovery Setup', 'Scan Target', 'Exclude IPs', 'Schedule', and 'Advanced Options'. In the 'Scan Target' section, the text '172.20.0/24' is entered in the input field. Below this is a hint: 'Enter an network address and netmask to define the IP ranges to scan.' In the 'Exclude IPs' section, there is an empty input field and a hint: 'An optional comma-separated list of IP addresses and/or network addresses to exclude from the scan.' In the 'Schedule' section, 'One Time' is selected in a dropdown menu, with a hint: 'Specify the schedule you would like this job to be run.' In the 'Advanced Options' section, 'OS Detection' is set to 'On' in a dropdown menu.

Il retrouve les 5 machines du réseau (hermes, glpi, zimbra, pfsense et nagios)

Auto-Discovery Jobs

✔ Auto-discovery job started.

+ New Auto-Discovery Job

↻ Refresh Job list

Scan Target	Exclusions	Schedule	Last Run	Devices Found	Created By	Status	Actions
172.20.0.0/24	-	Once	2024-05-06 15:14:05	5 New / 5 Total	nagiosadmin	Finished	

Discovered Items

The hosts below were discovered during the auto-discovery scan. hosts identified as linux servers with ssh available and no agent already deployed have been pre-selected for agent deployment.

Show discovered services

<input type="checkbox"/>	Address	Host Name	Type	Device/Operating System [Accuracy] ⓘ	Mac Vendor	Agent Deployed ⓘ	Status
<input type="checkbox"/>	172.20.0.1	172.20.0.1	Unknown		VMware	No	New
<input type="checkbox"/>	172.20.0.10	Hermes.stadiumcompany.com	Windows Server	Microsoft Windows Server 2016 [93%]	VMware	No	New
<input type="checkbox"/>	172.20.0.20	172.20.0.20	Linux Server	Linux 2.6.32 [96%]	VMware	No	New
<input checked="" type="checkbox"/>	172.20.0.30	glpi.stadiumcompany.com	Linux Server	Linux 2.6.32 [96%]	VMware	No	New
<input type="checkbox"/>	172.20.0.40	172.20.0.40	Linux Server	Linux 2.6.32 [100%]		No	New

Deploy Agents to Selected Hosts

On va ensuite dans **Configuration Wizards** pour chercher **Auto-discovery** et on procède de la même manière que Windows et Linux, on peut sélectionner quelles machines à remonter

Auto-Discovery

Monitor servers, devices, and services found by auto-discovery jobs.

Auto-Discovery Configuration Wizard

Step 1

Auto-Discovery Jobs

Configure a new Auto-Discovery Job in [Auto-Discovery](#)

Auto-Discovery Job

* Job ⓘ

Scan of 172.20.0.0/24 @ 2024-05-06 15:12:36 - Found 5 New / 5 Total

* Show ⓘ

New Hosts

* Default Services ⓘ

Common

* Host Addresses ⓘ

IP Addresses

Next >


Auto-Discovery Configuration Wizard

Step 2

Scan Results


The hosts and services below were discovered during the auto-discovery scan. Select the hosts and services you would like to monitor.


<input checked="" type="checkbox"/>	Address	Type	OS	Status	Host Name	Services			
						<input type="checkbox"/> Service Name	Service	Port	Protocol
<input checked="" type="checkbox"/>	172.20.0.1	Unknown		New	pfsense.stadiumcompany.com				
						<input type="checkbox"/> TCP Port 53 - domain	domain	53	TCP
						<input checked="" type="checkbox"/> HTTPS	https	443	TCP
						<input type="checkbox"/> TCP Port 2121 - lprop	lprop	2121	TCP
<input checked="" type="checkbox"/>	172.20.0.10	Windows Server	Microsoft Windows Server 2016	New	Hermes.stadiumcompany.com				
						<input type="checkbox"/> TCP Port 53 - domain	domain	53	TCP
						<input type="checkbox"/> TCP Port 88 - kerberos	kerberos	88	TCP
						<input type="checkbox"/> TCP Port 135 - epmap	epmap	135	TCP
						<input checked="" type="checkbox"/> NetBIOS	netbios-ssn	139	TCP



Auto-Discovery Configuration Wizard

Step 3





Monitoring Settings

Define basic parameters that determine how the host and service(s) should be monitored.

Under normal circumstances:

Monitor the host and service(s) every

5

minutes

When a potential problem is first detected:

Re-check the host and service(s) every

1

minutes up to

5

times before sending a notification

< Back

Next >

Finish with Defaults

Cancel

On peut voir la remontée des machines du réseau (172.20.0.0)

Host ↓	Service ↓	Status ↓	Duration ↓	Attempt ↓	Last Check ↓	Status Information ↓
172.20.0.20	HTTPS	Ok	N/A	1/5	2024-05-06 15:24:22	HTTP OK - HTTP/1.1 200 OK - 12812 bytes in 0.170 second response time
	IMAP	Ok	N/A	1/5	2024-05-06 15:25:16	IMAP OK - 0.003 second response time on 172.20.0.20 port 143 [* OK IMAP4rev1 proxy server ready]
	IMAP SSL	Pending	N/A	1/5	N/A	Service check is pending... Check is scheduled for 2024-05-06 15:26:20
	LDAP	Pending	N/A	1/5	N/A	Service check is pending... Check is scheduled for 2024-05-06 15:27:13
	POP3	Pending	N/A	1/5	N/A	Service check is pending... Check is scheduled for 2024-05-06 15:28:06
	Ping	Pending	N/A	1/5	N/A	Service check is pending... Check is scheduled for 2024-05-06 15:27:32
Hermes.stadiumcompany.com	SMTP	Ok	N/A	1/5	2024-05-06 15:24:37	SMTP OK - 0.007 sec. de temps de réponse
	LDAP	Ok	N/A	1/5	2024-05-06 15:25:25	TCP OK - 0.001 second response time on 172.20.0.10 port 389
	NetBIOS	Pending	N/A	1/5	N/A	Service check is pending... Check is scheduled for 2024-05-06 15:26:29
glpi.stadiumcompany.com	Ping	Pending	N/A	1/5	N/A	Service check is pending... Check is scheduled for 2024-05-06 15:27:22
	HTTP	Pending	N/A	1/5	N/A	Service check is pending... Check is scheduled for 2024-05-06 15:28:15
	HTTPS	Pending	N/A	1/5	N/A	Service check is pending... Check is scheduled for 2024-05-06 15:28:36
localhost	Ping	Ok	N/A	1/5	2024-05-06 15:24:45	OK - 172.20.0.30 rta 0.668ms lost 0%
	Current Load	Ok	1h 20m 7s	1/4	2024-05-06 15:25:10	OK - Charge moyenne: 1.99, 1.39, 1.31
	Current Users	Ok	1h 19m 42s	1/4	2024-05-06 15:20:47	UTILISATEURS OK - 1 utilisateurs actuellement connectés sur

Last Updated: 2024-05-06 15:25:29

<<

<

Page 1 / 3

15 Per Page

Go

>

>>

Conclusion

La mise en place d'un service de supervision permet au service informatique de surveiller quasiment en temps réel les informations sur les machines du réseau, permettant ainsi de prévenir toute panne et de redémarrer ces serveurs très rapidement