

Compte-rendu

Contexte :

La société Amine nous a demandé d'intervenir afin de mettre en place un système de surveillance sur le réseau. Ce réseau contiendra un LAN avec un routeur.

Nous pourrons le configurer afin d'avoir plusieurs fonctionnalités comme laisser l'accès au SSH ou au RDP. Le système de surveillance est Zabbix et il va nous permettre de surveiller tous les appareils présents sur notre réseau.

Sommaire:

- 1 - Installation de Zabbix et configuration du serveur Windows 2019
- 2 - Configuration de Pfsense, Ubuntu serveur et Windows server
- 3 - Configuration de Zabbix

Prérequis :

- Un routeur Pfsense
- Serveur Ubuntu 22.04 LTS
- Serveur Windows 2019

Explication :

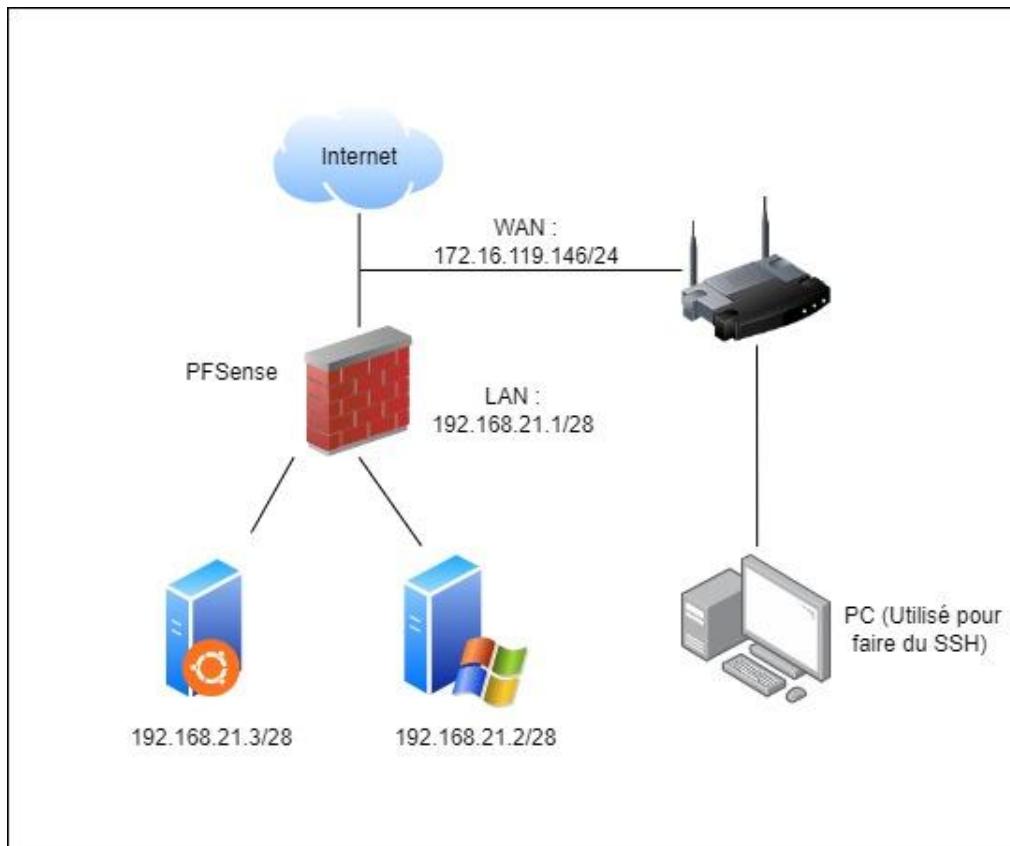
Tout d'abord, nous allons installer Zabbix sur un serveur Ubuntu en version 22.04.

Ensuite, nous allons installer Windows 2019 pour un serveur avec une configuration de la carte réseau.

Puis, on installera un routeur Pfsense avec une configuration pour le sous-réseaux et la création d'une règle pour laisser passer le SSH si jamais on veut configurer le serveur Ubuntu.

Enfin, nous allons configurer Zabbix avec la possibilité d'ajouter des fonctionnalités pour être alerté lorsqu'il y a un problème sur le réseau.

Schéma de la mission :



Tutoriel :

1- Installation de Zabbix et configuration du serveur Windows 2019

```
serverlinux@serverlinux:~$ sudo apt-get install apache2 libapache2-mod-php mariadb-server php php-mbstring php-gd php-xml php-bcmath php-ldap php-mysql unzip curl gnupg2 -y
```

Tout d'abord, on installe LAMP serveur pour le serveur HTTP.

```
serverlinux@serverlinux:~$ sudo nano /etc/php/8.1/apache2/php.ini
```

On configure le fichier configuration de php en changeant les paramètres pour notre serveur web.

```
memory_limit 256M
upload_max_filesize 16M
post_max_size 16M
max_execution_time 300
max_input_time 300
max_input_vars 10000
```

```
date.timezone = Europe/France
```

```
serverlinux@serverlinux:~$ systemctl restart apache2
```

On redémarre notre service apache2

```
serverlinux@serverlinux:~$ sudo mysql
```

On se connecte à la base de données MYSQL pour créer une base de données pour zabbix puis un utilisateur.

```
MariaDB [(none)]> CREATE DATABASE zabbixdb character set utf8 collate utf8_bin;  
Query OK, 1 row affected (0.004 sec)  
  
MariaDB [(none)]> CREATE USER 'zabbixuser'@'localhost' IDENTIFIED BY 'password';  
Query OK, 0 rows affected (0.007 sec)  
  
MariaDB [(none)]> GRANT ALL PRIVILEGES ON zabbixdb.* TO 'zabbixuser'@'localhost'  
  WITH GRANT OPTION;  
Query OK, 0 rows affected (0.002 sec)  
  
MariaDB [(none)]> FLUSH PRIVILEGES;  
Query OK, 0 rows affected (0.003 sec)  
  
MariaDB [(none)]> exit;
```

On vient d'accorder les priviléges à notre utilisateur "zabbixuser".

```
serverlinux@serverlinux:~$ sudo wget https://repo.zabbix.com/zabbix/6.2/ubuntu/pool/main/z/zabbix-release/zabbix-release_6.2-2%2Bubuntu22.04_all.deb
```

```
serverlinux@serverlinux:~$ sudo dpkg -i zabbix-release_6.2-2+ubuntu22.04_all.deb
```

```
serverlinux@serverlinux:~$ sudo apt update
```

On installe maintenant zabbix qui n'est disponible dans les repo d'ubuntu donc on l'installe à partir du site officiel.

```
serverlinux@serverlinux:~$ sudo apt install zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf zabbix-sql-scripts zabbix-agent
```

On fait de même pour avoir Zabbix server.

```
serverlinux@serverlinux:~$ systemctl start zabbix-server
```

```
serverlinux@serverlinux:~$ systemctl enable zabbix-server
```

On active maintenant le serveur Zabbix.

```
serverlinux@serverlinux:~$ sudo nano /etc/zabbix/zabbix_server.conf
```

```
DBUser=zabbix

### Option: DBPassword
#       Database password.
#       Comment this line if no password is used.
#
# Mandatory: no
# Default:
DBPassword=password
```

On configure le fichier de configuration de zabbix serveur pour mettre un mot de passe à notre utilisateur.

```
serverlinux@serverlinux:~$ sudo systemctl restart zabbix-server zabbix-agent apache2
```

```
serverlinux@serverlinux:~$ systemctl enable zabbix-server zabbix-agent apache2
```

On active maintenant zabbix server.

2- Configuration du routeur PfSense,ubuntu serveur et Windows server 2019

```
pfSense 2.5.2-RELEASE amd64 Fri Jul 02 15:33:00 EDT 2021
Bootup complete

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

VMware Virtual Machine - Netgate Device ID: dc74eef0bccd9054eb14

*** Welcome to pfSense 2.5.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 172.16.119.146/24
LAN (lan)      -> em1      -> v4: 192.168.21.1/28

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults 13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell

Enter an option: [zone: udp_inpcb] kern.ipc.maxsockets limit reached
arprequest: cannot find matching address
```

On sait qu'on à notre réseau en 192.168.21.0/28 donc on met notre pfSense sur notre première adresse.

SSH:

Firewall / NAT / Port Forward / Edit

Edit Redirect Entry

Disabled	<input type="checkbox"/> Disable this rule			
No RDR (NOT)	<input type="checkbox"/> Disable redirection for traffic matching this rule This option is rarely needed. Don't use this without thorough knowledge of the implications.			
Interface	WAN			
Choose which interface this rule applies to. In most cases "WAN" is specified.				
Address Family	IPv4			
Select the Internet Protocol version this rule applies to.				
Protocol	TCP			
Choose which protocol this rule should match. In most cases "TCP" is specified.				
Source	Display Advanced			
Destination	<input type="checkbox"/> Invert match.	WAN address	/	Address/mask
Destination port range	From port	40000	To port	40000
Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only				

Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.

Redirect target IP	<input type="button" value="Single host"/> Type	<input type="text" value="192.168.21.3"/> Address
Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12 for IPv4 In case of IPv6 addresses, it must be from the same "scope", i.e. it is not possible to redirect from link-local addresses scope (fe80:*) to local scope (::1)		
Redirect target port	<input type="button" value="SSH"/> Port	<input type="button" value="Custom"/> Custom
Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically). This is usually identical to the "From port" above.		
Description	<input type="text" value="ssh du serveur ubuntu vers pc externe"/> A description may be entered here for administrative reference (not parsed).	
No XMLRPC Sync	<input type="checkbox"/> Do not automatically sync to other CARP members This prevents the rule on Master from automatically syncing to other CARP members. This does NOT prevent the rule from being overwritten on Slave.	
NAT reflection	<input type="button" value="Use system default"/>	
Filter rule association	<input type="button" value="Pass"/>	

Rule Information

Created 10/9/22 01:25:37 by admin@192.168.21.2 (Local Database)

Updated 10/9/22 01:31:28 by admin@192.168.21.2 (Local Database)

 Save

On crée une règle de redirection de port pour permettre l'accès depuis l'extérieur avec internet afin de se connecter en ssh avec un port personnalisé (pour une sécurité).

Le port par défaut du ssh est 22 mais on le customise en 40000.

Une requête envoyée sur l'adresse IP WAN du pfSense, sur le port 40000 sera automatiquement redirigée vers l'adresse IP 192.168.21.3 sur le port 22

```
amine@amine-Vector-GP66-12UGS:~$ ssh serverlinux@192.168.1.70 -p 40000
serverlinux@192.168.1.70's password:
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-48-generic x86_64)

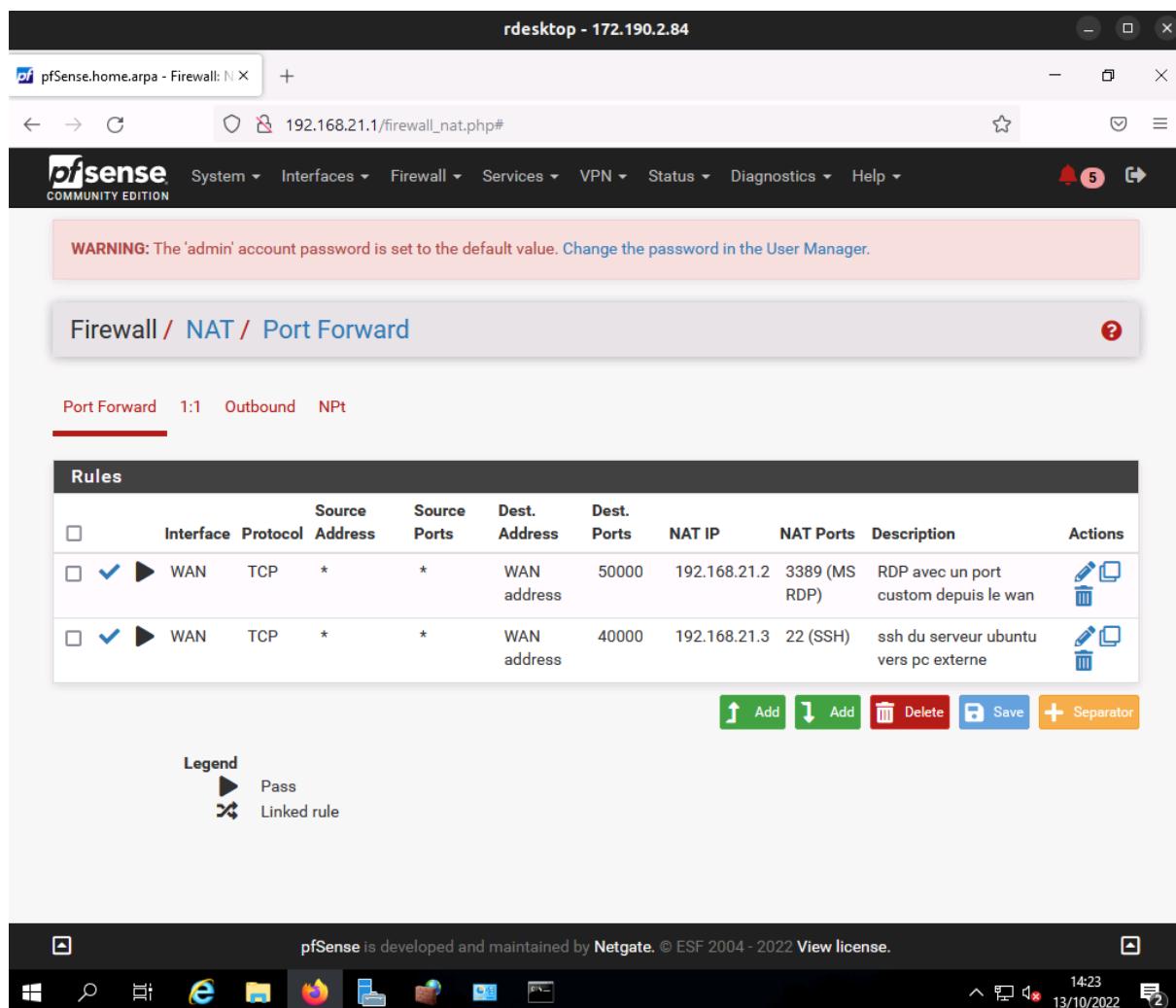
 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

 System information as of dim. 09 oct. 2022 01:41:21 UTC

 System load:  0.154296875      Processes:           280
 Usage of /:   47.9% of 13.67GB  Users logged in:      1
```

On remarque qu'on réussit bien à se connecter en SSH avec le port 40000 qui est redirigé.

RDP :

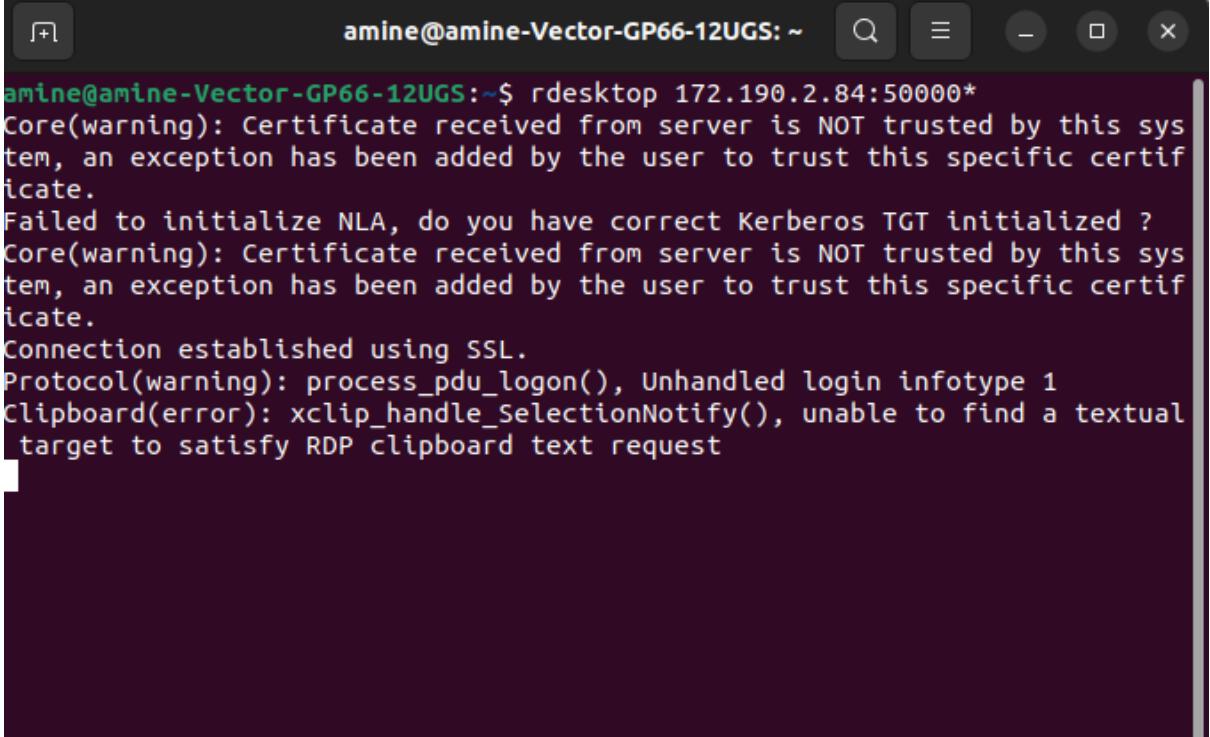


The screenshot shows a Windows desktop environment with a browser window titled 'rdesktop - 172.190.2.84' displaying the pfSense firewall configuration. The URL in the address bar is '192.168.21.1/firewall_nat.php#'. The pfSense navigation bar includes 'System', 'Interfaces', 'Firewall', 'Services', 'VPN', 'Status', 'Diagnostics', 'Help', and a notification bell with 5 alerts. A red warning box at the top states: 'WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.' The main content area is titled 'Firewall / NAT / Port Forward' and shows the 'Port Forward' tab selected. The table lists two port forwarding rules:

Index	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
1	TCP	*	*	WAN address	50000	192.168.21.2	3389 (MS RDP)	RDP avec un port custom depuis le wan	 
2	TCP	*	*	WAN address	40000	192.168.21.3	22 (SSH)	ssh du serveur ubuntu vers pc externe	 

At the bottom of the pfSense interface, there is a legend:  Pass and  Linked rule. The taskbar at the bottom of the screen shows various application icons and the system tray.

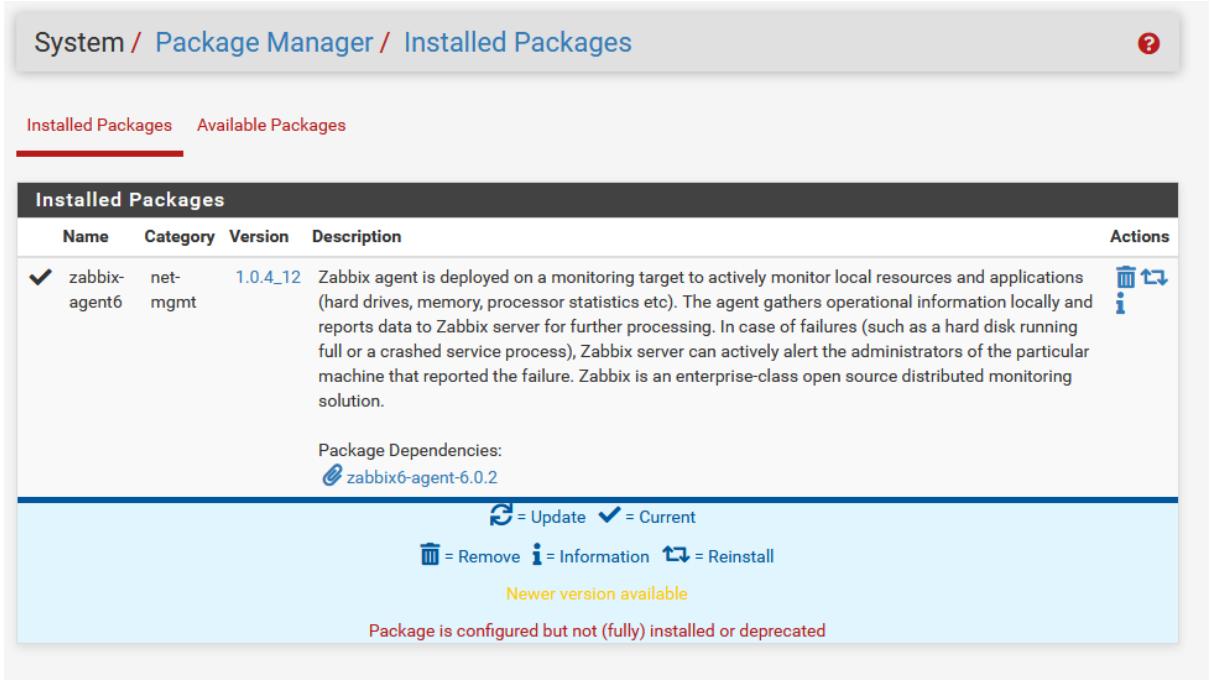
On configure la redirection de port pour le RDP avec le port personnalisé en 50000 (on peut voir que je suis déjà connecté en RDP pour un test).



```
amine@amine-Vector-GP66-12UGS:~$ rdesktop 172.190.2.84:50000*
Core(warning): Certificate received from server is NOT trusted by this system, an exception has been added by the user to trust this specific certificate.
Failed to initialize NLA, do you have correct Kerberos TGT initialized ?
Core(warning): Certificate received from server is NOT trusted by this system, an exception has been added by the user to trust this specific certificate.
Connection established using SSL.
Protocol(warning): process_pdu_logon(), Unhandled login infotype 1
Clipboard(error): xclip_handle_SelectionNotify(), unable to find a textual target to satisfy RDP clipboard text request
```

On installe rdesktop pour pouvoir accéder à distance à notre serveur Windows 2019, on rentre l'adresse ip de notre serveur et on met le port personnalisé qu'on a choisi.

AGENT ZABBIX :



Name	Category	Version	Description	Actions
zabbix-agent6	net-mgmt	1.0.4_12	Zabbix agent is deployed on a monitoring target to actively monitor local resources and applications (hard drives, memory, processor statistics etc). The agent gathers operational information locally and reports data to Zabbix server for further processing. In case of failures (such as a hard disk running full or a crashed service process), Zabbix server can actively alert the administrators of the particular machine that reported the failure. Zabbix is an enterprise-class open source distributed monitoring solution.	  

Package Dependencies:
 zabbix6-agent-6.0.2

 = Update  = Current
 = Remove  = Information  = Reinstall

Newer version available

Package is configured but not (fully) installed or deprecated

On installe l'agent zabbix pour notre routeur pour qu'il remonte sur notre serveur zabbix.

Package / Services: Zabbix Agent 6 / Agent

Agent

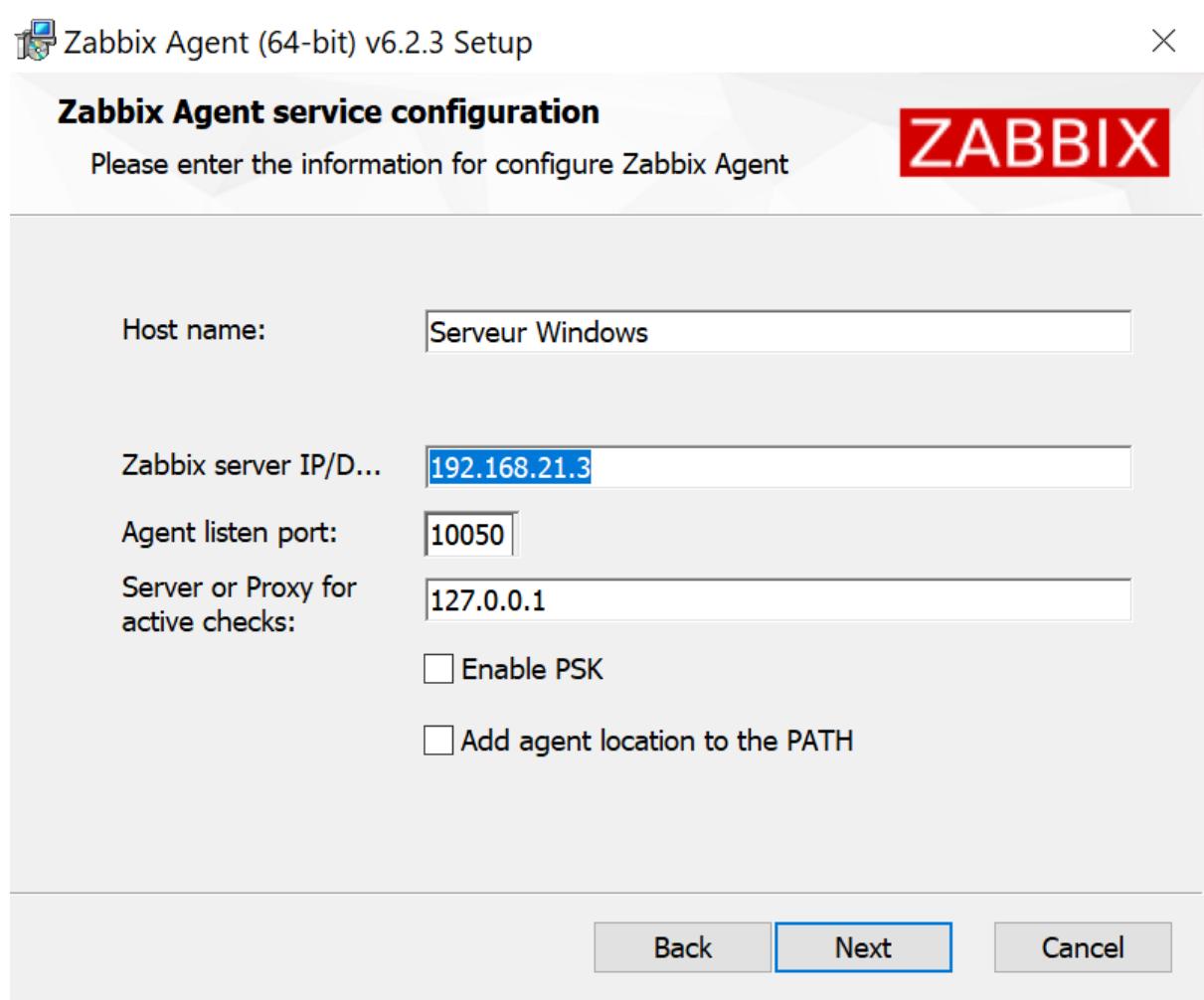
Zabbix Agent Settings

Enable	<input checked="" type="checkbox"/> Enable Zabbix Agent service.
Server	192.168.21.3
List of comma delimited IP addresses (or hostnames) of ZABBIX servers.	
Server Active	192.168.21.3
List of comma delimited IP:port (or hostname:port) pairs of Zabbix servers for active checks.	
Hostname	RouteurPFSENSE
Unique, case sensitive hostname. Required for active checks and must match hostname as configured on the Zabbix server.	
Listen IP	0.0.0.0
Comma-separated list of IP addresses for connections from the server. (Default: 0.0.0.0 - all IPv4 interfaces)	
Listen Port	10050
Listen port for connections from the server. (Default: 10050)	
Refresh Active Checks	120

TLS-RELATED Parameters

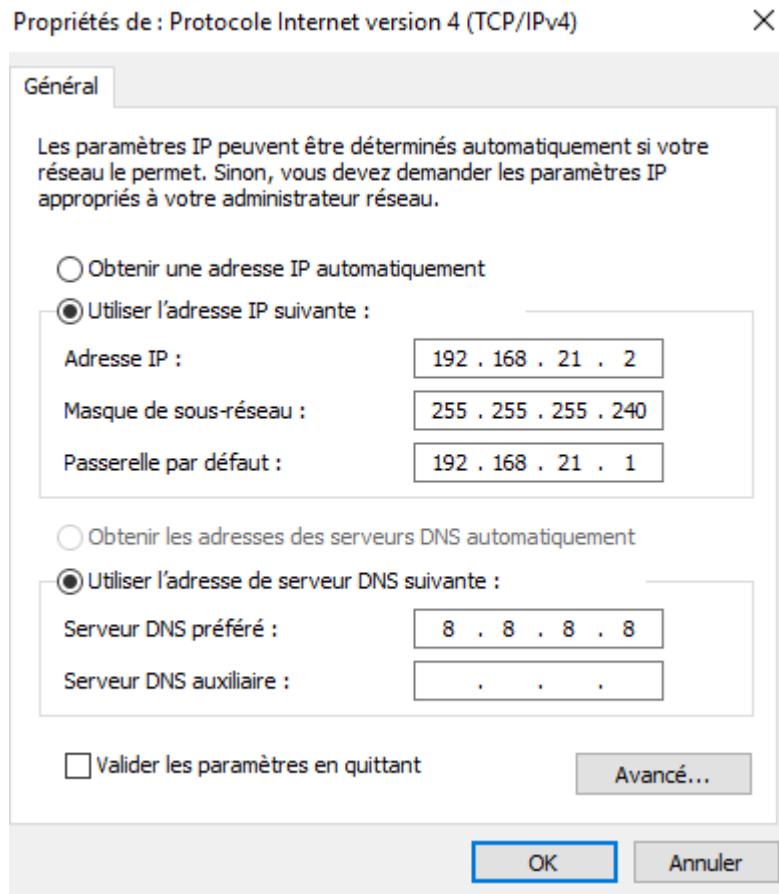
TLS Connect	unencrypted
How the agent should connect to server or proxy. Used for active checks. Only one value can be specified: unencrypted - connect without encryption psk - connect using TLS and a pre-shared key cert - connect using TLS and a certificate	
TLS Accept	unencrypted
What incoming connections to accept. Multiple values can be specified: unencrypted - connect without encryption psk - connect using TLS and a pre-shared key cert - connect using TLS and a certificate	
TLS CA	none
Top-level CA certificate for peer certificate verification.	
TLS CA System	<input type="checkbox"/> Use the CA certificate list from the operating system. This option overrides prior option.
TLS CRL	none
List of revoked certificates.	
TLS Cert	none
Agent certificate.	
TLS PSK Identity	

On active maintenant l'agent en renseignant l'ip de notre serveur zabbix.



On fait de même sur notre serveur Windows.

CONFIGURATION IP :

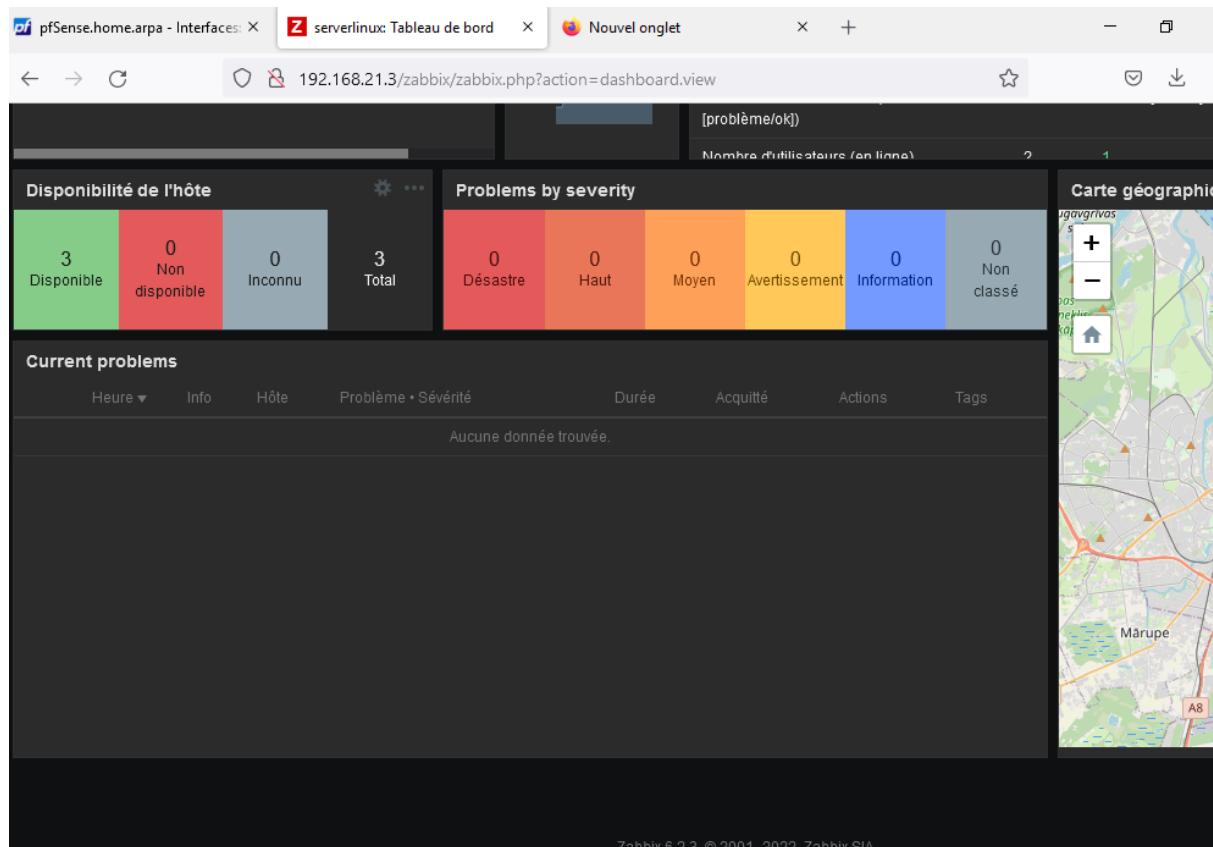


On met l'ip du serveur windows 2019 en 192.168.21.2/28 avec le routeur Pfsense en passerelle, notre DNS sera 8.8.8.8 pour avoir accès à internet.

```
GNU nano 6.2                               /etc/netplan/00-installer-config.yaml
# This is the network config written by 'subiquity'
network:
  ethernets:
    ens33:
      dhcp4: false
      addresses: [192.168.21.3/28]
      gateway4: 192.168.21.1
      nameservers:
        addresses: [8.8.8.8]
  version: 2
```

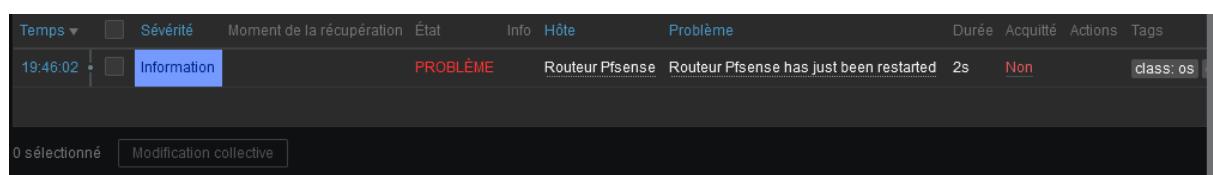
On met ensuite notre Ubuntu server en 192.168.21.3/28 avec l'ip de notre PFsense en passerelle, notre DNS sera 8.8.8.8 pour avoir accès à internet.

3- Configuration de Zabbix



On ajoute nos trois hôtes donc le serveur Ubuntu qui contient Zabbix, notre serveur Windows 2019 et notre routeur PFSense (nos trois hôtes sont bien présent)

4- Test de la surveillance Zabbix



On vient de redémarrer le serveur Pfsense pour tester si un problème va être détecté et remonter sur le serveur Zabbix et on remarque qu'il apparaît bien.

Conclusion :

On a bien rempli la mission qui est de mettre en place un système de monitoring (surveillance) sur notre réseau pour avoir des notifications et alertes en temps réel. Ce réseau interne aura accès à internet. On pourra accéder à nos appareils à distance depuis l'extérieur grâce à des règles ssh qu'on a configurées sur notre routeur PFsense. Cela permettra de pouvoir gérer notre serveur Ubuntu. Bien évidemment, il faut ajouter tous les hôtes pour pouvoir recevoir des alertes et vérifier s'il y a des problèmes critiques (grâce à notre tableau de bord configurable).