

# Procédure d'installation et mise en place d'un agent





# SOMMAIRE PROCEDURE

03

Prérequis

10

Installation de Zabbix

07

Installation de l'agent Zabbix

12

Ajout d'un équipement réseau à Zabbix avec SNMP

14

Supervision de Proxmox avec un agent Zabbix



## Prérequis

Pour la **mise en place de la solution** de supervision, l'environnement technique repose sur une infrastructure virtualisée à l'aide de **Proxmox**, sur lequel est déployée une machine virtuelle **Ubuntu** dédiée à la supervision. Cette VM interagit avec les équipements réseau suivants : un switch Cisco Catalyst 2960, un routeur Cisco de la série 4300, un pare-feu PfSense, ainsi qu'avec **l'ensemble de mon infrastructure**. Ces éléments permettent de simuler un environnement réseau d'entreprise réaliste à superviser.

Dans ce projet, **Zabbix** et **Grafana** sont installés conjointement. Zabbix se charge de la collecte et de l'analyse des données de supervision, tandis que Grafana permet une visualisation dynamique et personnalisée des métriques sous forme de tableaux de bord. Cette association constitue une solution complète et intuitive, facilitant le suivi des performances du réseau et des systèmes supervisés.

L'installation de Zabbix est réalisée à l'aide de **Docker**, ce qui permet une mise en place rapide, modulaire et facile à maintenir. Pour cela, je me suis appuyé sur la documentation disponible sur le dépôt GitHub suivant :

[GitHub - akmalovaa/zabbix-docker: zabbix nginx postgresql grafana docker compose](https://github.com/akmalovaa/zabbix-docker) , qui propose un déploiement clé en main de Zabbix avec NGINX, PostgreSQL et Grafana via Docker Compose.

 Note : Avant de commencer, il est essentiel d'avoir installé Docker et Docker Compose sur la machine virtuelle Ubuntu.



## Installation de Zabbix

Après l'installation de Docker et Docker Compose sur la machine virtuelle Ubuntu, **on commence** par cloner le dépôt GitHub contenant la configuration nécessaire au déploiement de Zabbix et Grafana, à l'aide de la commande :  
**git clone https://github.com/akmalovaa/zabbix-docker.git.**

Une fois le dépôt récupéré, on **se déplace** dans le répertoire du projet avec:  
**cd zabbix-docker**, puis on vérifie la présence des fichiers nécessaires à l'aide de la commande **ls**. Ensuite, **on lance les conteneurs Docker** définis dans le fichier **docker-compose.yml** à l'aide de la commande **docker compose up -d**, ce qui permet de démarrer tous les services en arrière-plan. Cette étape déploie automatiquement les composants essentiels tels que le serveur Zabbix, l'interface web, la base de données PostgreSQL, NGINX, ainsi que Grafana.

```
tactical@Zabbix:~$ su - root
Mot de passe :
root@Zabbix:~# git clone https://github.com/akmalovaa/zabbix-docker.git
Clonage dans 'zabbix-docker'...
remote: Enumerating objects: 127, done.
remote: Counting objects: 100% (70/70), done.
remote: Compressing objects: 100% (39/39), done.
remote: Total 127 (delta 40), reused 49 (delta 31), pack-reused 57 (from 1)
réception d'objets: 100% (127/127), 1.28 Mio | 18.24 Mio/s, fait.
Résolution des deltas: 100% (46/46), fait.
root@Zabbix:~# cd
root@Zabbix:~# ls
snap zabbix-docker
root@Zabbix:~# cd zabbix-docker
root@Zabbix:~/zabbix-docker# ls
compose.yaml db dump.sh db restore.sh grafana README.md
root@Zabbix:~/zabbix-docker# docker compose up -d
+] Running 42/42
✓ zabbix-server Pulled
✓ d608445de803 Pull complete
✓ af5b1f7ab5ab Pull complete
✓ bd282510aa05 Pull complete
✓ cea24a08cd12 Pull complete
✓ 45ac8d26e686 Pull complete
✓ 962a15e87eb3 Pull complete
✓ zabbix-agent Pulled
✓ 5a7813e071bf Pull complete
✓ 80efccc1ad8f Pull complete
```

## 2. Restauration de la base de données :

Une fois les conteneurs lancés, on procède à la restauration de la base de données, si cela est nécessaire. Pour cela, on commence par rendre le script db\_restore.sh exécutable en modifiant ses permissions à l'aide de la commande suivante :

**chmod +x ./db\_restore.sh**

Une fois cela effectué, on exécute le script en utilisant la commande :

**./db\_restore.sh**

Ce script permet de réinitialiser ou de restaurer la base de données de Zabbix, selon la configuration du dépôt.

```
root@Zabbix:~/zabbix-docker# chmod +x ./db_restore.sh
root@Zabbix:~/zabbix-docker# ./db_restore.sh
no such service: db
cat: pgdump.sql: Aucun fichier ou dossier de ce nom
unknown shorthand flag: 'U' in -U

Usage: docker [OPTIONS] COMMAND [ARG...]

Run 'docker --help' for more information
[+] Running 6/6
✓ Container grafana           Removed
✓ Container zabbix-agent      Removed
✓ Container frontend          Removed
✓ Container server            Removed
✓ Container postgres          Removed
✓ Network zabbix-docker_network-zabbix Removed
```

Enfin, pour vérifier que les conteneurs sont correctement lancés et fonctionnent, on utilise la commande suivante :

**docker ps**

Cette commande permet de lister tous les conteneurs actifs, ce qui assure que tous les services nécessaires, tels que le serveur Zabbix, l'interface web, la base de données et Grafana, sont bien opérationnels.

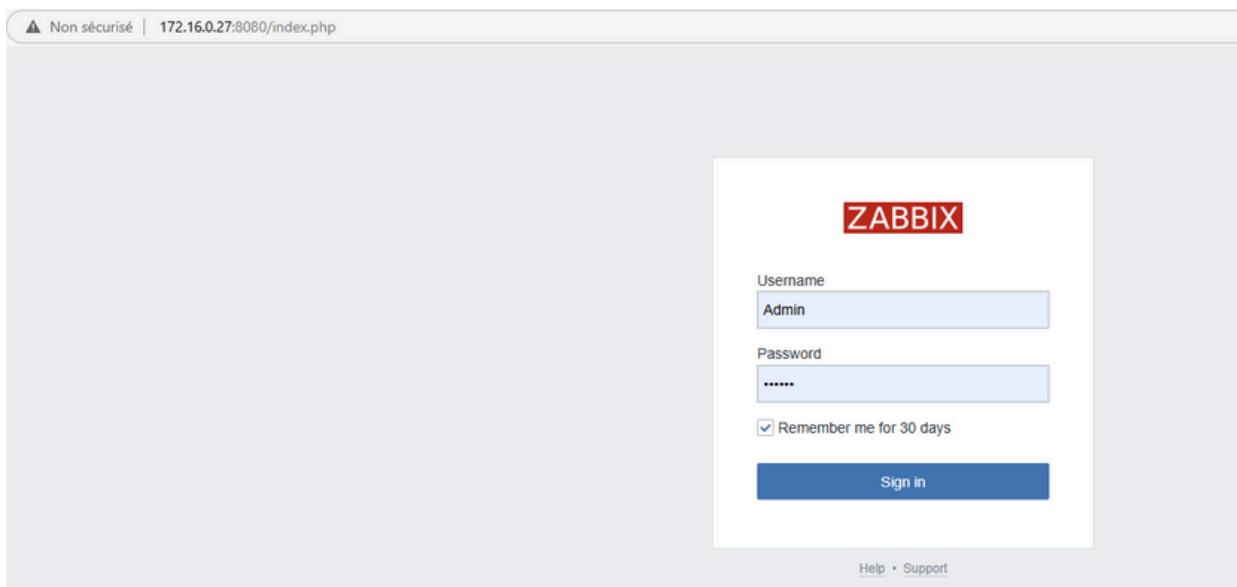
CONTAINER ID	IMAGE	NAMES	COMMAND	CREATED	STATUS
89262951ab86	grafana/grafana:11.6.0	grafana	"/run.sh"	2 minutes ago	Up 2 minutes
683ce273fdcb	zabbix/zabbix-web-nginx-pgsql:ubuntu-7.2-latest	frontend	"docker-entrypoint.sh"	2 minutes ago	Up 2 minutes (health)
3->8443/tcp, [::]:8443->8443/tcp	zabbix/zabbix-agent2:ubuntu-7.2-latest	zabbix-agent	"/usr/bin/docker-ent..."	2 minutes ago	Up 2 minutes
a50c7511a960	zabbix/zabbix-server-pgsql:ubuntu-7.2-latest	server	"/usr/bin/docker-ent..."	2 minutes ago	Up 2 minutes
b1ce3c17bac6	postgres:16-alpine	postgres	"docker-entrypoint.s..."	2 minutes ago	Up 2 minutes
561b5d8e7888					

### 3.Accès à l'interface web

Une fois tous les conteneurs en cours d'exécution, on peut accéder aux interfaces web de Zabbix et Grafana via un navigateur.

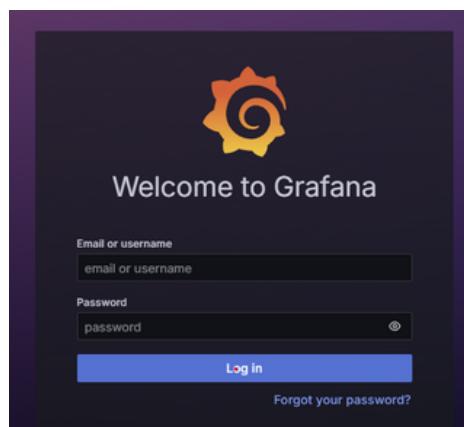
Par défaut, les ports utilisés pour l'accès sont configurés dans le fichier **docker-compose.yml**. Dans le cas de cette installation, Zabbix est accessible à l'adresse <http://172.16.0.27:8080>, tandis que Grafana est disponible via <http://172.16.0.27:3000>. Lors de la première connexion à Zabbix, l'interface demande les identifiants suivants par défaut :

- Nom d'utilisateur : Admin
- Mot de passe : zabbix



Pour Grafana, les identifiants initiaux sont généralement :

- Nom d'utilisateur : admin
- Mot de passe : admin



# Installation de l'agent Zabbix

## 1. Installation d'un agent sur une machine cliente

Sur une machine de test sous Windows, on installe l'agent Zabbix en téléchargeant le fichier .msi depuis le site officiel : [https://www.zabbix.com/download\\_agents](https://www.zabbix.com/download_agents). Ce fichier permet une installation rapide de l'agent, nécessaire pour remonter les données vers le serveur de supervision.

Zabbix Release: 7.2.5

**Zabbix agent v7.2.5** Read manual

Packaging: MSI  
Encryption: OpenSSL  
Linkage: Dynamic  
Checksum:  
sha256: 1dc08f9af06789aace989eee4d82a63353b4939cb7b79e4e6c22851fd060039f  
sha1: adfb8388c2626e588c95a00633a7f36cf45a675db  
md5: 7c614bd1ec4ab33d31349011b75fdbc1

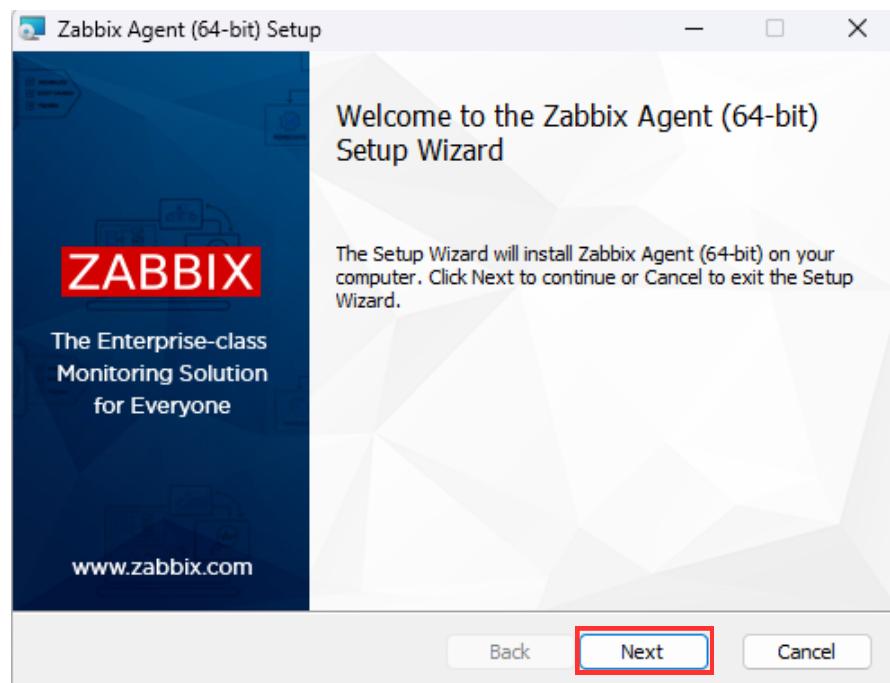
**DOWNLOAD** [https://cdn.zabbix.com/zabbix/binaries/stable/7.2/7.2.5/zabbix\\_agent-7.2.5-windows-amd64-openssl.msi](https://cdn.zabbix.com/zabbix/binaries/stable/7.2/7.2.5/zabbix_agent-7.2.5-windows-amd64-openssl.msi)

**Zabbix agent 2 v7.2.5** Read manual

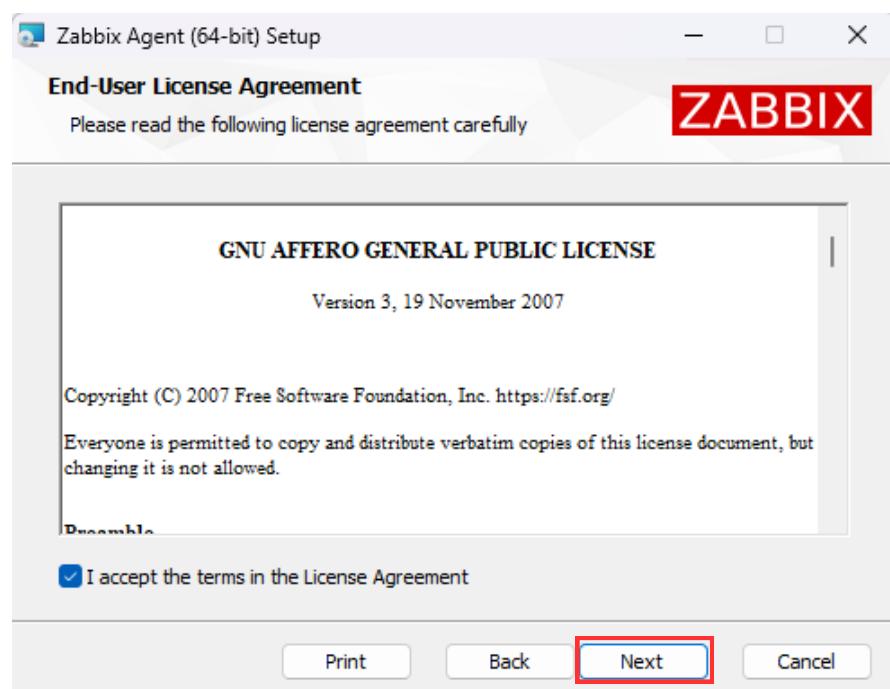
Packaging: MSI  
Encryption: OpenSSL  
Linkage: Dynamic  
Checksum:  
sha256: 2454647b372d2dbf8cb3b04a702266f1fae8c33a603ee8be93ecf82caabb5c  
sha1: 5206c42f49794f9a17397d0bee69c3607141bdcc  
md5: 7fc1f82edalca0f7101e1c87c4cfa63d

**DOWNLOAD** [https://cdn.zabbix.com/zabbix/binaries/stable/7.2/7.2.5/zabbix\\_agent2-7.2.5-windows-amd64-openssl.msi](https://cdn.zabbix.com/zabbix/binaries/stable/7.2/7.2.5/zabbix_agent2-7.2.5-windows-amd64-openssl.msi)

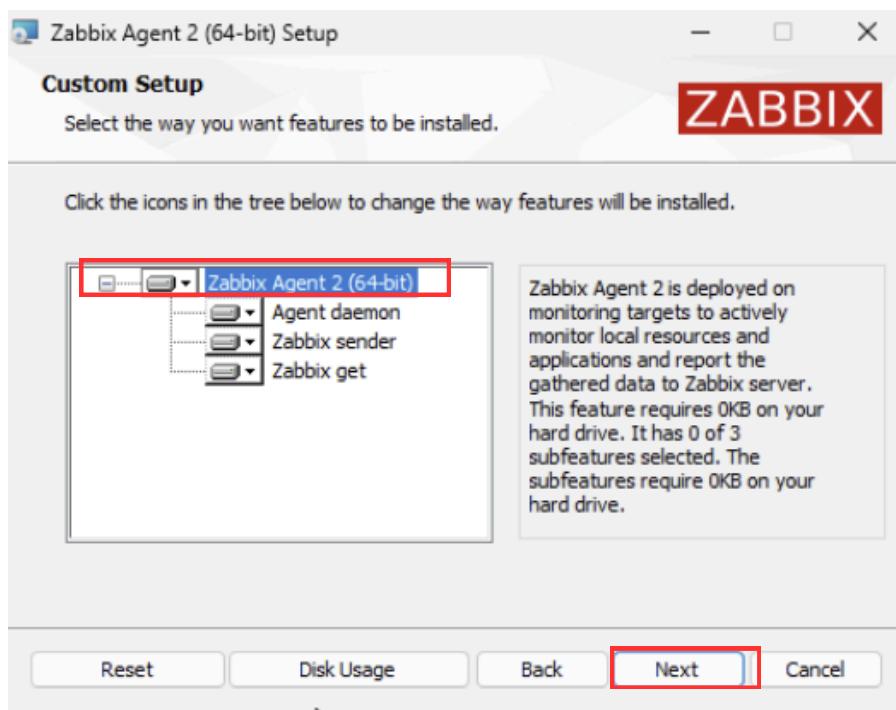
Exécuter ensuite le fichier téléchargé pour lancer l'installation.



Cliquez ensuite sur "Next" pour passer à l'étape suivante.

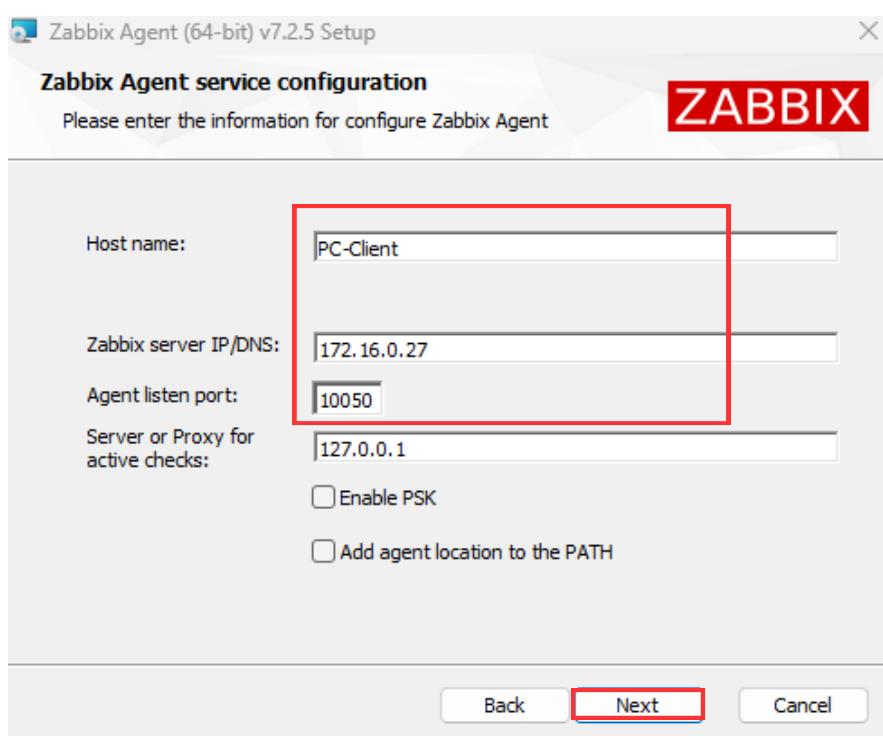


Sélectionner l'option par défaut "Zabbix Agent 2", puis cliquer sur "Next" pour continuer.

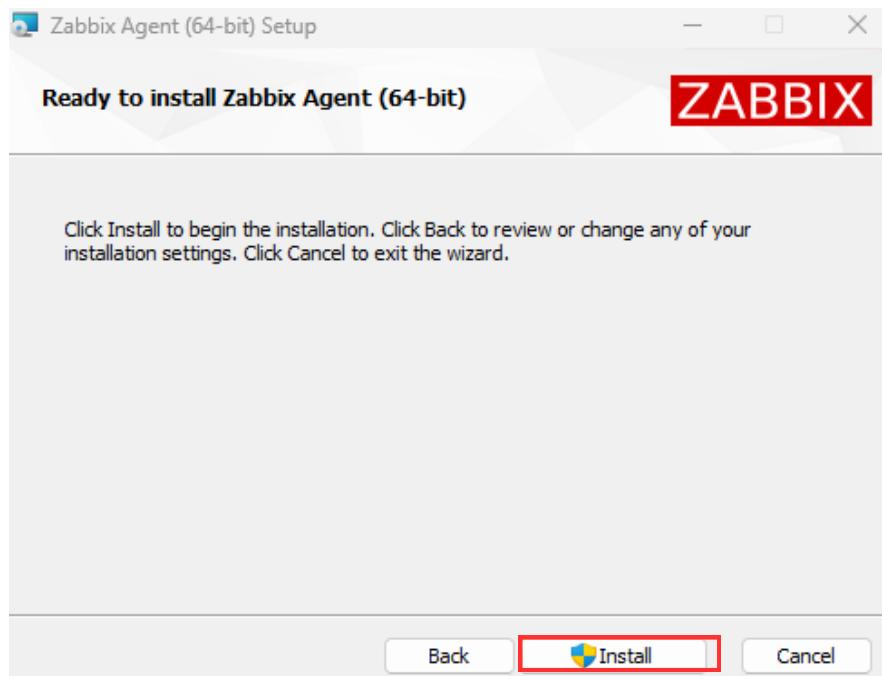


Renseigner ensuite les informations demandées :

- Hostname : entrer le nom de la machine à superviser (dans notre cas : PC-Client)
- Zabbix Server IP : saisir l'adresse IP du serveur Zabbix
- Port : laisser le port par défaut (10050)
- Server or Proxy : laisser cette option par défaut si l'agent est en communication directe avec le serveur (ce qui est généralement le cas)

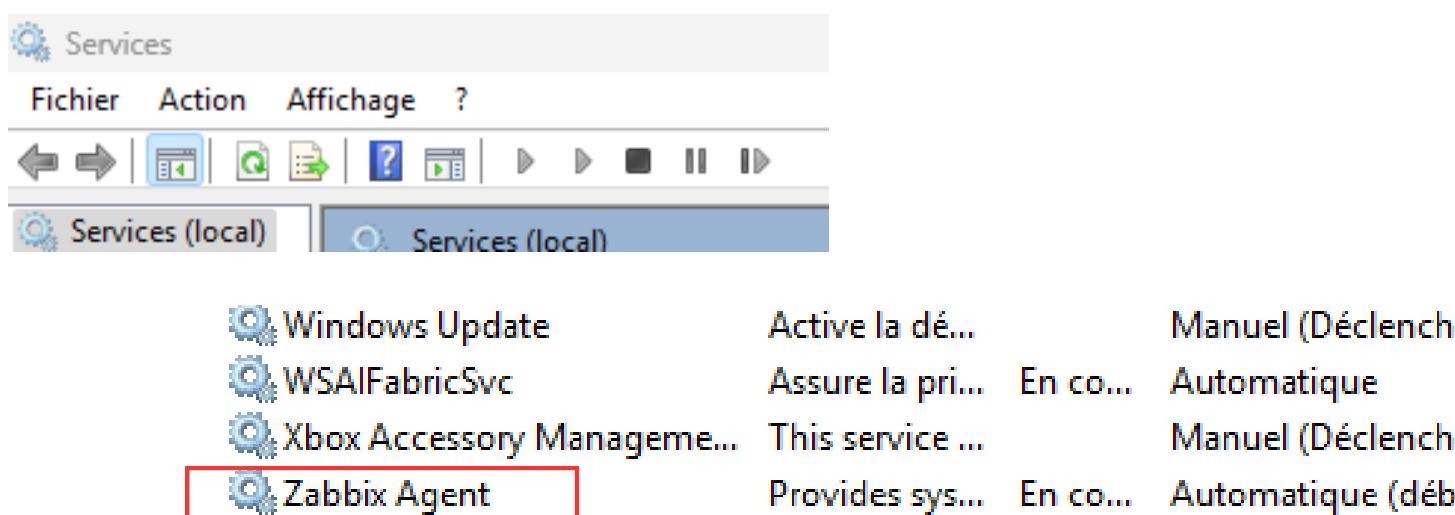


Cliquer sur "Install" pour lancer l'installation.



Une fois l'installation terminée, il est recommandé de vérifier dans les services Windows que l'agent Zabbix a bien été installé et qu'il fonctionne correctement.

Le service doit apparaître sous le nom "Zabbix Agent" ou "Zabbix Agent 2", avec le statut "En cours d'exécution".



Retourner ensuite sur l'interface web de Zabbix pour créer un nouvel hôte. Dans la section Configuration > Hosts, cliquer sur "Create host", puis ajouter le PC client sur lequel l'agent vient d'être installé. Renseigner le nom de l'hôte, le groupe (ex. : "Clients"), et l'adresse IP de la machine :

Host

Host IPMI Tags Macros Inventory Encryption Value mapping

\* Host name: PC-Client

Visible name: PC-Client

Templates: Windows by Zabbix agent Actions: Unlink Unlink and clear

type here to search Select

\* Host groups: Virtual machines X Actions: Select

type here to search

Interfaces Type IP address DNS name Connect to Port Default

Agent: 172.16.0.55 [ ] IP DNS 10050 [ ] Remove

Add

Description:

Monitored by: Server Proxy Proxy group

Enabled:

Update Clone Delete Cancel

Une fois toutes les informations renseignées, cliquer sur "Add" pour enregistrer l'hôte. Après quelques instants, les premières données devraient commencer à remonter automatiquement si la configuration est correcte.

Et voilà, vous venez d'ajouter un hôte à Zabbix en installant un agent via le fichier .exe.

## Ajout d'un équipement réseau à Zabbix avec SNMP

Activer SNMP v2c sur le switch ou routeur

Pour permettre à Zabbix de superviser l'équipement, activer SNMP en exécutant la commande suivante en mode configuration :

**snmp-server community public RO**

```
SW1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)#snmp-server community public RO
SW1(config)#exit
SW1#wr
Building configuration...
[OK]
```

*Tester la communication SNMP avec snmpwalk :*

Depuis la console du serveur Zabbix, utilisez la commande suivante pour vérifier que le routeur répond bien aux requêtes SNMP :

**snmpwalk -v2c -c public 192.168.0.100**

```
tactical@Zabbix:~$ snmpwalk -v2c -c public 192.168.0.100
iso.3.6.1.2.1.1.1.0 = STRING: "Cisco IOS Software, C2960X Software (C2960X-UNIVE
RSALK9-M), Version 15.2(4)E8, RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2019 by Cisco Systems, Inc.
Compiled Fri 15-Mar-19 10:55 by prod_rel_team"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.9.1.1208
iso.3.6.1.2.1.1.3.0 = Timeticks: (10164663) 1 day, 4:14:06.63
iso.3.6.1.2.1.1.4.0 = ""
iso.3.6.1.2.1.1.5.0 = STRING: "SW1.assumer-ssh"
iso.3.6.1.2.1.1.6.0 = ""
iso.3.6.1.2.1.1.7.0 = INTEGER: 6
```

Une fois la vérification SNMP effectuée, vous pouvez ajouter l'équipement sur Zabbix :

New host

Host IPMI Tags Macros Inventory Encryption Value mapping

\* Host name: Switch1  
Visible name: Switch1  
Templates: Cisco IOS by SNMP

\* Host groups: Equipements

Interfaces

Type	IP address	DNS name	Connect to	Port	Default
SNMP	192.168.0.100		IP	161	<input checked="" type="radio"/> Remove
* SNMP version: SNMPv2					
* SNMP community: public					
Max repetition count: 10 <input type="checkbox"/> Use combined requests					

Add Description:

Monitored by:

Enabled:

L'agent a été bien ajouté sur Zabbix :

Switch1	192.168.0.100:161	SNMP	class: network target: cisco target: cisco-ios
Zabbix server	zabbix-agent:10050	ZBX	class: os class: software target: linux ...

## Supervision de Proxmox avec un agent Zabbix

Avant d'installer l'agent Zabbix, commencez par mettre à jour les paquets du serveur avec la commande suivante : apt update

Une fois la mise à jour terminée, installez l'agent Zabbix en exécutant la commande suivante : apt install zabbix-agent2

```
root@assurmer:~# apt install zabbix-agent2
```

Une fois l'installation terminée, éditer le fichier de configuration de l'agent : sudo nano /etc/zabbix/zabbix\_agent2.conf

Modifier les lignes suivantes : Server=172.16.0.27

ServerActive=172.16.0.27

ListenPort=10050

Hostname=nom exact de la vm

```
ServerActive=172.16.0.27
### Option: Hostname
#           List of comma delimited hostnames
#           Required for active monitoring
#           Value is acquired from /etc/hostname
#
# Mandatory: no
# Default:
# Hostname=
#
Hostname=srvproxmox
### Option: ListenPort
#           Agent will listen on this port
#           Mandatory: no
#           Range: 1024-32767
#           Default:
ListenPort=10050
```

Redémarrer le service Zabbix Agent 2 et l'activer automatiquement au démarrage :

```
root@assurmer:~# nano /etc/zabbix/zabbix_agent2.conf
root@assurmer:~# systemctl restart zabbix-agent2
root@assurmer:~# systemctl enable zabbix-agent2
Synchronizing state of zabbix-agent2.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable zabbix-agent2
root@assurmer:~#
```

Ensuite, comme mentionné précédemment, ajoutez le serveur Proxmox en tant qu'hôte dans Zabbix en remplissant les informations nécessaires (nom, groupe, adresse IP, etc.). Une fois cela fait, l'hôte sera ajouté et la supervision pourra commencer.

Et voilà, la procédure est terminée !