DOCUMENTATION

ANS INFORMATIQUE

ANS
INFORMATIQUE

SUPERVISISER

UN PARC INFORMATIQUE

A L'AIDE
D'UN OUTIL DE

SUPERVIVION

TEL QUE

ZABBIX

7.0

ZABBIX

ANS INFORMATIQUE

SOMMAIRE

ANS INFORMATIQUE

TELECHARGER, INSTALLER ET FAIRE LES PREMIERES CONFIGURATIONS DE ZABBIX

-

AJOUTER UN HOTE

Avec le protocole SNMP

Avec un agent ZABBIX

CREER UN GROUPE DE MODELES

CREER UN GROUPE D'HOTES

TELECHARGER, INSTALLER ET METTRE EN PLACE UN TEMPLATE

FAIRE REMONTER DES INFORMATIONS POUR EMETTRE DES ALERTES AVEC DES DECLENCHEURS PAR NIVEAU DE SEVERITE (Exemple avec remontée de certificats Windows Server 2022)

Déploiement du fichier de configuration de l'agent Zabbix via GPO (AD)

Dépôt des scripts de récupération de données sur le serveur Zabbix

Mise en place de Zabbix

INTRODUCTION

Qu'est-ce qu'un superviseur de parc informatique ?

Un superviseur de parc informatique tel que Zabbix correspond à un outil permettant de surveiller l'activité d'une ou plusieurs infrastructures (routeurs, switchs, serveurs, BDD, ...) en temps réel.
Ces superviseurs permettent également d'installer des alertes ayant pour objectif de prévenir d'un incident via des notifications mails ou SMS.

Qu'est-ce que Zabbix et comment fonctionne-t-il ?

Zabbix est un superviseur de parc informatique open-source.
Son fonctionnement repose sur l'utilisation d'agents installés sur des machines supervisées et de protocoles de collectes de données tel que le SNMP, permettant une analyse proactive des performances.

Comment fonctionne-t-il ?

Pour fonctionner efficacement, Zabbix utilise des agents ou des protocoles comme SNMP afin de collecter des métriques sur les serveurs, réseaux et applications. Cette collecte repose sur des OID (Object Identifier) qui identifient précisément les informations à récupérer. Les données ainsi obtenues sont ensuite stockées dans une base de données avant d'être intégrées dans une interface intuitive et facilement compréhensible.

À partir de ces données, Zabbix permet également de générer des alertes grâce à des déclencheurs intégrés aux templates. Ces derniers peuvent être issus de la communauté ou créés sur mesure, facilitant ainsi la supervision et la réactivité face aux anomalies.

Qu'est-ce que le protocole SNMP et comment fonctionne-t-il ?

Le protocole SNMP (Simple Network Management Protocol) est utilisé pour la supervision exclusivement. Il fonctionne grâce à une architecture comprenant un gestionnaire SNMP installés sur les appareils surveillés, et une base MIB qui stocke les métriques disponibles.
Le gestionnaire envoie des requêtes aux agents via UDP (port 161), et ces derniers répondent avec les informations demandées. SNMP permet également l'envoie d'alertes en cas d'anomalies détectée sur un équipement.

NOUVEAUTES DE ZABBIX 7.0

Quelles améliorations ont été apportées aux performances et à la productivité ?

Zabbix 7.0 LTS apporte plusieurs améliorations en matière de performance :

- Surveillance Web Synthétique :
Supervision avancée des sites et applications web avec captures d'écran et analyse des performances.

- Équilibrage de charge et haute disponibilité du Proxy Zabbix :
Gestion automatique des proxys pour une meilleure évolutivité.

- Optimisation de la collecte des données :
Interrogation asynchrone permettant jusqu'à 1000 vérifications simultanées par processus.

- Contrôle centralisé des délais de collecte :
Configuration des délais directement via l'interface graphique ou l'API.

- Amélioration de la découverte réseau :
Détection plus rapide des équipements et services.

- Prise en charge de l'authentification multi-facteurs (MFA) :
Sécurité renforcée pour l'accès des utilisateurs.

- Nouveaux widgets de visualisation :
Ajout de graphes, jauges et tableaux dynamiques pour une meilleure lisibilité des métriques.

- Supervision de l'état de Zabbix lui-même :
Identification proactive des éventuels problèmes internes.

- Séparation des processus critiques :
Amélioration de la stabilité et de la fiabilité du système.

- Intégration avec des applications tierces :
Notifications vers Slack, MS Teams, Telegram, etc.

Quelles sont les nouveaux modèles pré-intégrés (templates) disponibles ?

Zabbix 7.0 LTS introduit une belle collection de nouveaux modèles pré-intégrés pour simplifier la supervision de services cloud, d'infrastructures réseau et d'applications :

- Google Cloud Platform :
Surveille les ressources et services utilisés sur GCP, comme les VM, le stockage ou les bases de données.

- Microsoft Azure Cost Management:
Suit les coûts et la consommation de ressources sur Azure pour mieux gérer le budget cloud.

- Microsoft Azure Cosmos DB for MongoDB:
Contrôle les performances et la disponibilité de la base Cosmos DB compatible MongoDB.

- Amazon ECS (Elastic Container Service):
Observe l'état des conteneurs et des services déployés sur ECS.

- AWS ELB Application Load Balancer:
Vérifie la santé et les performances des répartiteurs de charge applicatifs AWS.

- Oracle Cloud Infrastructure:
Supervise les ressources cloud Oracle comme les instances, le stockage ou le réseau.

- Microsoft SQL (agent 2 et ODBC) :
Surveille les bases SQL Server via l'agent Zabbix ou une connexion ODBC.

- Checkpoint Quantum Security Gateway:
Suit l'état et les alertes de sécurité des pares-feux CheckPoint.

- Nextcloud:
Contrôle l'état de santé et les performances d'un serveur Nextcloud.

- Fortinet FortiGate:
Surveille les équipements de sécurité FortiGate (trafic, sessions, alertes).

- HPE iLO :
Supervise les serveurs HPE via leur interface de gestion iLO (température, alimentation, etc.).

- Cisco SD-WAN:
Observe les performances et la connectivité des réseaux définis par logiciel Cisco.

- HashiCorp Nomad:
Suit l'état des tâches et des nœuds dans un cluster Nomad.

- PostgreSQL via ODBC :
Surveille les bases PostgreSQL via une connexion ODBC.

- OpenStack Nova:
Contrôle les instances et ressources gérées par le composant Nova d'OpenStack.

- Acronis Cyber Protect Cloud:
Vérifie les sauvegardes, la sécurité et les alertes dans la plateforme Acronis.

- YugabyteDB:
Surveille les performances et la disponibilité de la base de données distribuée YugabyteDB.

Comment Zabbix renforce-t-il la sécurité avec l'authentification à deux facteurs (A2F) et d'autres fonctionnalités ?

Afin de garantir la sécurité des accès à sa plateforme, Zabbix intègre des mécanismes avancés d'authentification. Parmi eux, l'authentification à deux facteurs (A2F) joue un rôle clé : elle impose à l'utilisateur de confirmer son identité à l'aide d'un mot de passe classique, complété par un code temporaire généré via une application mobile (comme Google Authenticator). Cette double vérification rend les accès non autorisés beaucoup plus difficiles, même en cas de compromission du mot de passe.

Zabbix propose également l'intégration avec Duo Universal Prompt, une solution de sécurité moderne qui adapte le mode d'authentification au contexte : notification push, biométrie, géolocalisation, etc. Ce système renforce la sécurité tout en maintenant une expérience utilisateur fluide.

D'autres dispositifs complètent cette approche :

- Des connexions chiffrées via HTTPS, protégeant les échanges de données ;
- Une gestion des droits strictement basée sur les rôles et le principe du moindre privilège ;
- Des protections intégrées contre les attaques fréquentes sur les interfaces web, telles que le clickjacking ou l'injection de code malveillant.

En somme, Zabbix adopte une stratégie de défense en profondeur, combinant technologie, bonnes pratiques et outils de cybersécurité pour assurer une protection robuste de ses systèmes et de ses utilisateurs.

COMPRENDRE LES NOTIONS PRINCIPALES DE ZABBIX

Qu'est-ce qu'un hôte ?

Un hôte dans Zabbix représente un équipement ou un service à surveiller : serveur, switch, machine virtuelle, application, etc. C'est l'unité de base sur laquelle on applique la supervision.

Qu'est-ce qu'un modèle (Template) ?

Un modèle est un ensemble préconfiguré d'éléments, de déclencheurs, de graphiques et de règles. Il permet d'appliquer rapidement une configuration standard à plusieurs hôtes similaires, ce qui facilite la gestion et la cohérence.

Qu'est-ce qu'un groupe d'hôtes ?

Un groupe d'hôtes dans Zabbix est une collection logique de machines ou d'équipements que l'on regroupe pour faciliter leur supervision, leur gestion et l'attribution des droits d'accès.

Qu'est-ce qu'un groupe de modèles ?

Un groupe de modèles est un ensemble structuré de modèles de supervision (templates) permettant d'organiser et de réutiliser efficacement des configurations prêtes à l'emploi dans différents contextes

Qu'est-ce qu'un déclencheur ?

Un déclencheur (trigger) est une règle logique qui analyse les données collectées. Il génère une alerte si une condition est remplie (ex. : CPU > 90 % pendant 5 minutes). Il permet donc de détecter les incidents.

Qu'est-ce qu'une règle de découverte ?

Une règle de découverte automatise la détection d'hôtes ou de services sur un réseau. Elle permet à Zabbix d'ajouter dynamiquement des équipements à surveiller, selon des critères définis (plage IP, ports, services actifs, etc.).

Qu'est-ce qu'un élément ?

Un élément (item) est une donnée spécifique collectée sur un hôte, comme l'utilisation CPU, l'espace disque, ou l'état d'un service. C'est la brique de base de la supervision.

Qu’est-ce qu’un OID ?

Un OID (Object Identifier) est un identifiant utilisé dans le protocole SNMP pour accéder à une information précise sur un équipement réseau. Zabbix s’en sert pour interroger des périphériques comme des routeurs ou des imprimantes.

Qu’est-ce qu’un agent Zabbix ?

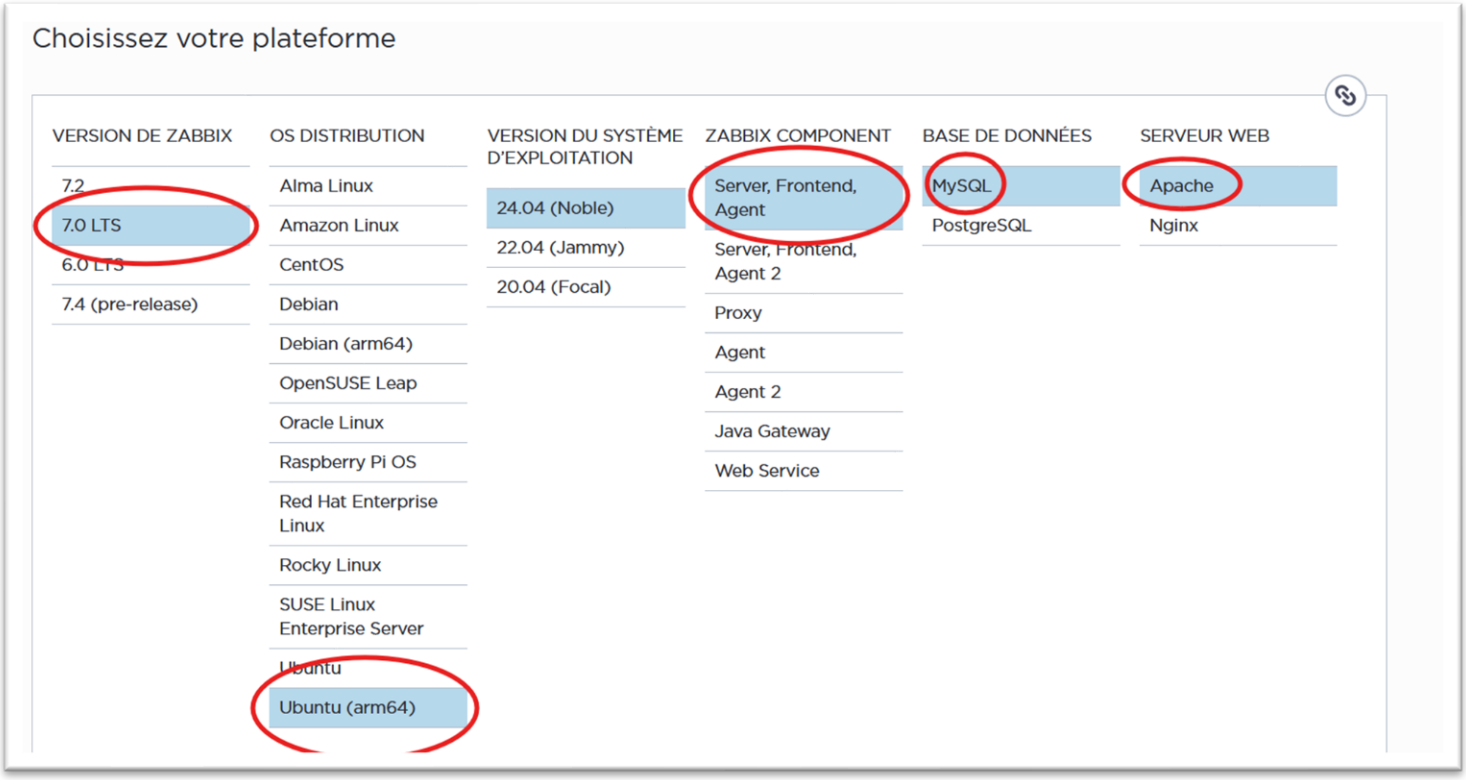
L’agent Zabbix est un petit programme installé sur un hôte. Il collecte des données système (CPU, mémoire, processus, etc.) et les envoie au serveur Zabbix. Il permet une supervision fine et détaillée.

UTILISER ZABBIX ET LE METTRE EN PLACE

Télécharger, installer et faire les premières configurations

Sur la machine ou vous allez mettre en place Zabbix, rendez-vous sur le site de Zabbix puis dans l'onglet Download : https://www.zabbix.com/fr/download

Sélectionnez ensuite les bonnes informations correspondant à votre contexte :



EXPLICATION : On choisit la version 7.0 car il s'agit de la version dite Stable la plus récente. L'OS sélectionné est au choix mais il est préférable de choisir un OS de type en version serveur sans interface graphique pour se mettre en conditions réelles. A propos de la version de Zabbix on choisit la version Server Frontend, Agent (*Possibilité de choisir le mode Server Frontend, Agent 2 mais nécessité d'adapté lors du téléchargement d'un agent sous une machine qui doit être surveillée en prenant un agent de type 2*). Pour la base de données, on choisira MySQL qui est une version connue et pour le serveur Web c'est au choix en fonction des connaissances de chacun. Dans notre cas on choisira Apache.

-

Pour l'installation de ce package, il suffira de suivre **DANS LES DETAILS** les indications qui suivent *(Différentes de la capture d'écran en fonction des options choisis précédemment)* :

a. Become root user

Start new shell session with root privileges.

```
$ sudo -s
```

b. Install Zabbix repository Documentation

```
# wget https://repo.zabbix.com/zabbix/7.0/ubuntu-arm64/pool/main/z/zabbix-release/zabbix-release_latest_7.0+ubuntu24.04_all.deb
# dpkg -i zabbix-release_latest_7.0+ubuntu24.04_all.deb
# apt update
```

c. Install Zabbix server, frontend, agent

```
# apt install zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf zabbix-sql-scripts zabbix-agent
```

d. Create initial database Documentation

Make sure you have database server up and running.

Run the following on your database host.

```
# mysql -uroot -p
password
mysql> create database zabbix character set utf8mb4 collate utf8mb4_bin;
mysql> create user zabbix@localhost identified by 'password';
mysql> grant all privileges on zabbix.* to zabbix@localhost;
mysql> set global log_bin_trust_function_creators = 1;
mysql> quit;
```

On Zabbix server host import initial schema and data. You will be prompted to enter your newly created password.

```
# zcat /usr/share/zabbix-sql-scripts/mysql/server.sql.gz | mysql --default-character-set=utf8mb4 -uzabbix -p zabbix
```

Disable log_bin_trust_function_creators option after importing database schema.

```
# mysql -uroot -p
password
mysql> set global log_bin_trust_function_creators = 0;
mysql> quit;
```

e. Configure the database for Zabbix server

Edit file /etc/zabbix/zabbix_server.conf

```
DBPassword=password
```

f. Start Zabbix server and agent processes

Start Zabbix server and agent processes and make it start at system boot.

```
# systemctl restart zabbix-server zabbix-agent apache2
# systemctl enable zabbix-server zabbix-agent apache2
```

g. Open Zabbix UI web page

The default URL for Zabbix UI when using Apache web server is http://host/zabbix

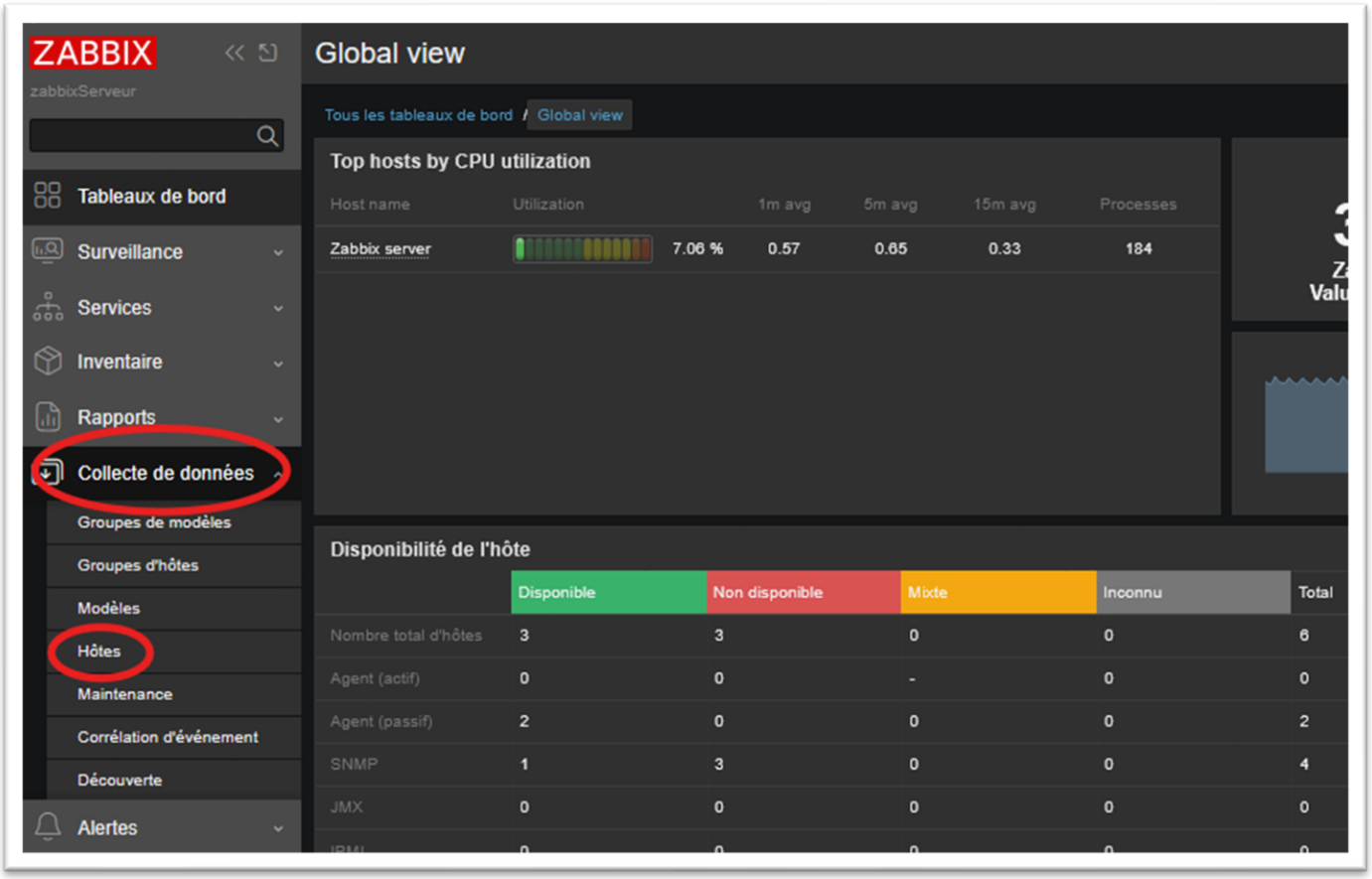
Une fois l'installation effectuée, vous pourrez accéder à l'interface de Zabbix via son adresse IP dans un navigateur Web en entrant
<IP>/zabbix
Puis connectez-vous grâce aux identifiants par défaut suivant :
Identifiant : Admin
MDP : zabbix

Il est évident que vous pourrez tout à fait ajouter des identifiants personnalisés avec la section **Utilisateurs de Zabbix une fois connecté.**

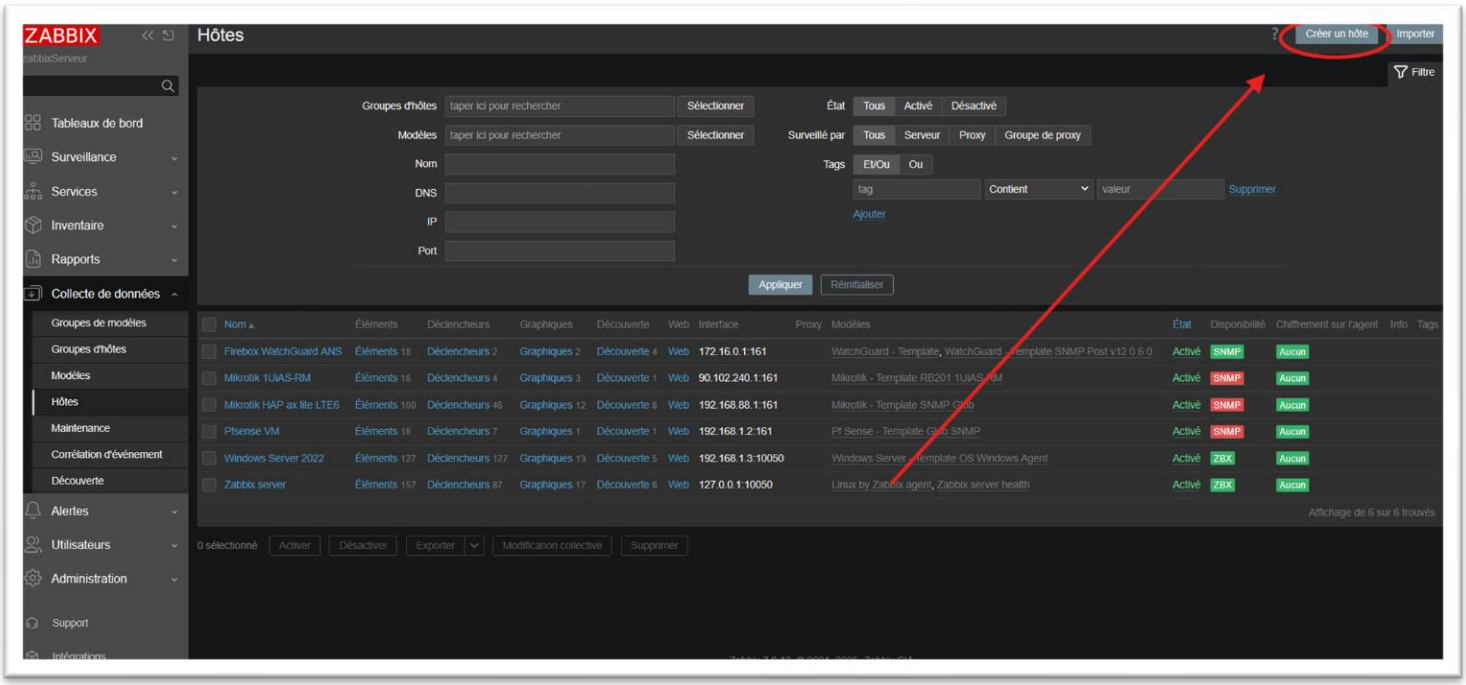
PS : A noter que si vous souhaitez accéder à l'interface Web de votre Zabbix depuis un réseau extérieur à votre réseau LAN, vous devrez mettre en place une redirection de port sur votre routeur/firewall.

Ajouter un hôte

Place à des choses plus intéressantes, mettons en place notre 1er hôte à surveiller sur Zabbix. Pour ce faire accéder au menu **Collecte de données** puis **Hôtes**.



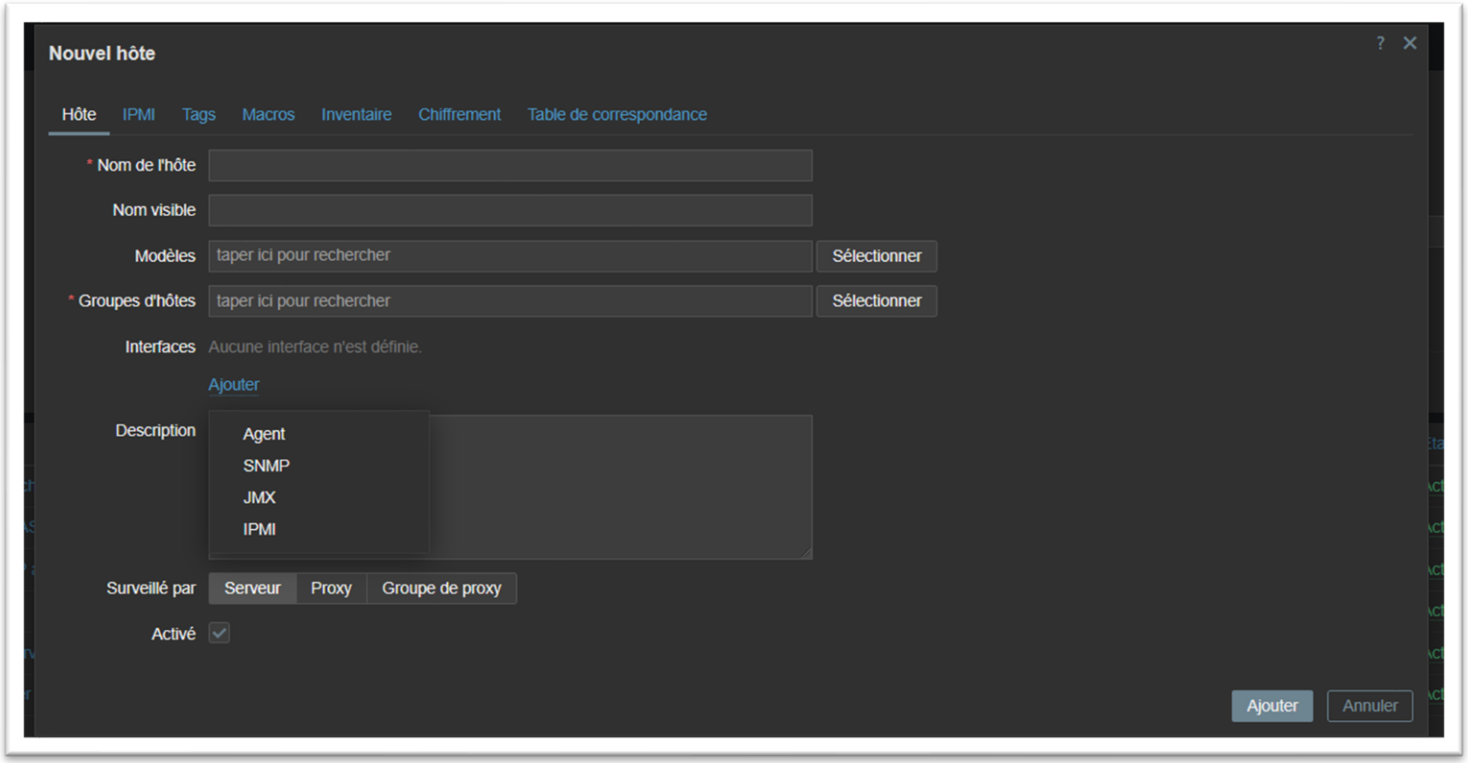
Cliquez ensuite sur **Créer un hôte** :



Puis remplissez les champs suivants de la manière indiquée :

- Nom de l'hôte : Entrez un nom qui vous permettra d'identifier votre hôte
- Nom visible : Ce champ se remplira automatiquement lorsque vous rentrerez le nom de l'hôte
- Modèles : On laissera ce champ vide pour l'instant et l'étudierons lors de la mise en place d'un Template
- Groupes d'hôtes : Au sein de ce champ vous devrez sélectionner un groupe dans lequel sera classé votre hôte (***Attention*** *: Les groupes d'hôtes par défaut ne correspondent peut-être pas à vos attentes, par défaut sélectionnez donc un groupe et on créera d'autres groupes plus significatifs par la suite.*)
- Interface (**Ajouter**) : C'est ici que l'on va ajouter l'adresse IP de notre hôte. Ici on a 4 choix d'ajout d'interface :
  - Via **SNMP**
  - Via un **AGENT ZABBIX**
  - Via **JMX**
  - Via **IPMI**

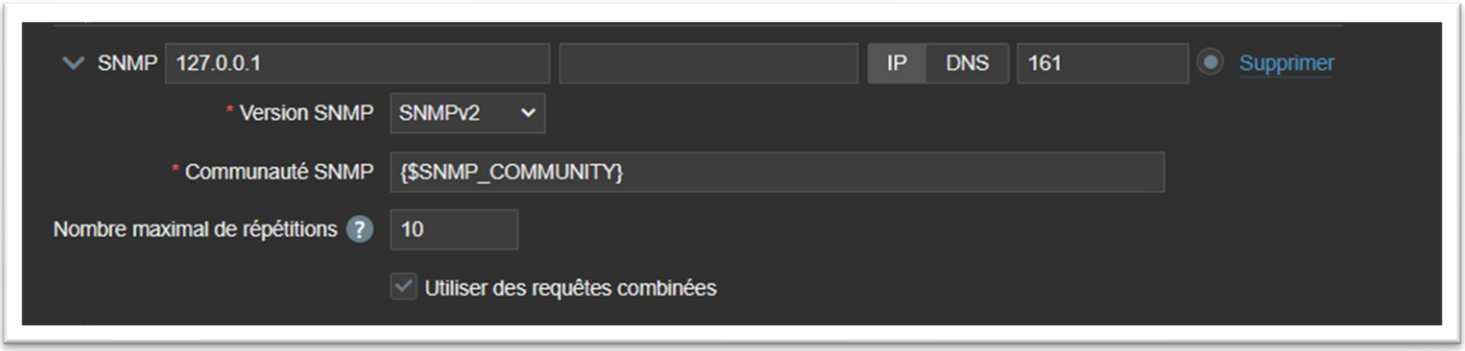
Parmi ces options, seul les 2 premières vont être employées.



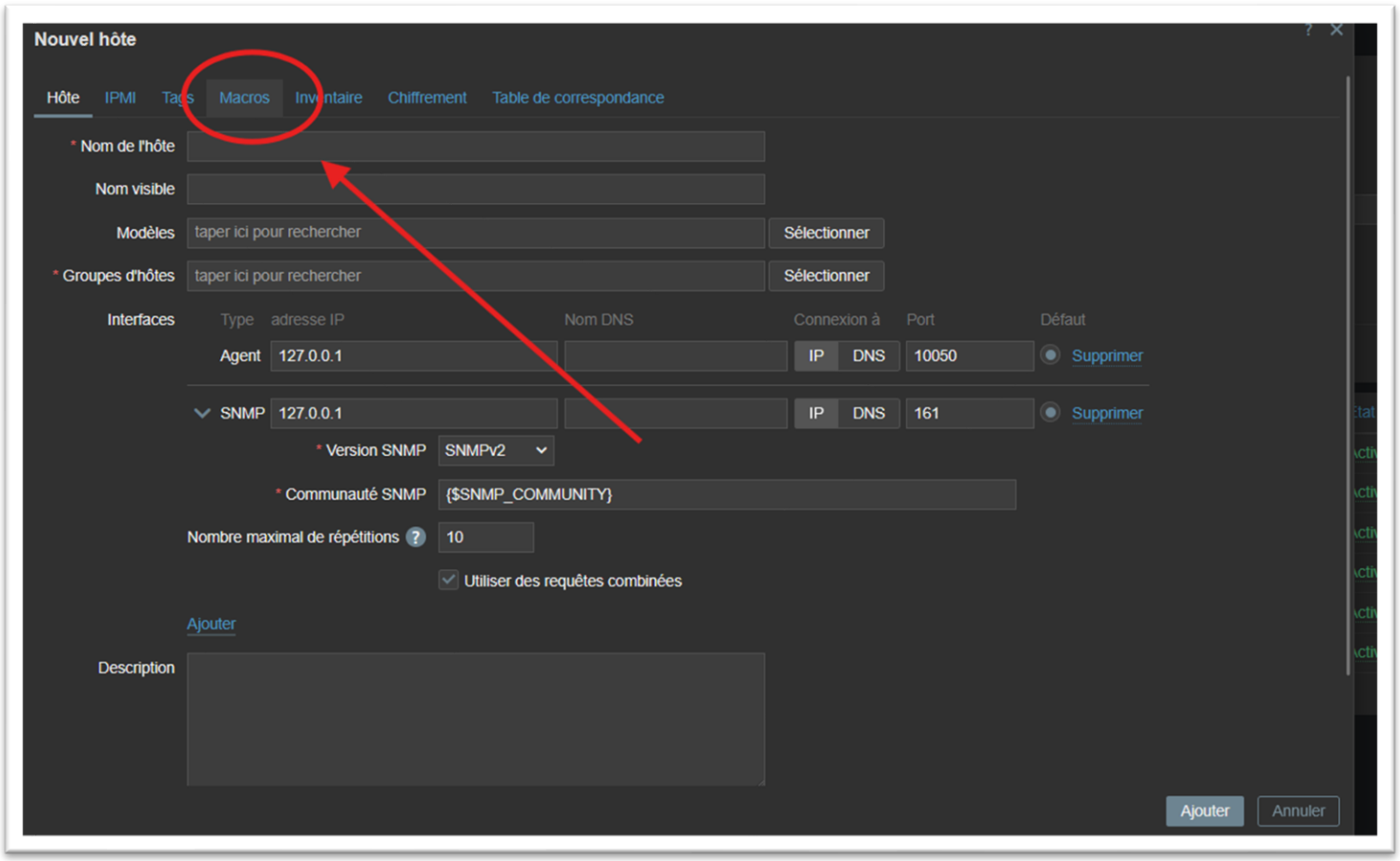
Avec le protocole SNMP

Commençons avec le protocole SNMP. Afin de configurer le SNNP vous allez avoir besoin de connaitre la Communauté SNMP (*Une communauté SNMP est un groupe de périphériques réseau partageant une même chaîne d'accès, utilisée comme mot de passe, permettant de surveiller et gérer ces équipements via le protocole SNMP*) de l'appareil SNMP. De plus connaitre la version de SNMP utilisée sur l'appareil à surveiller est crucial.

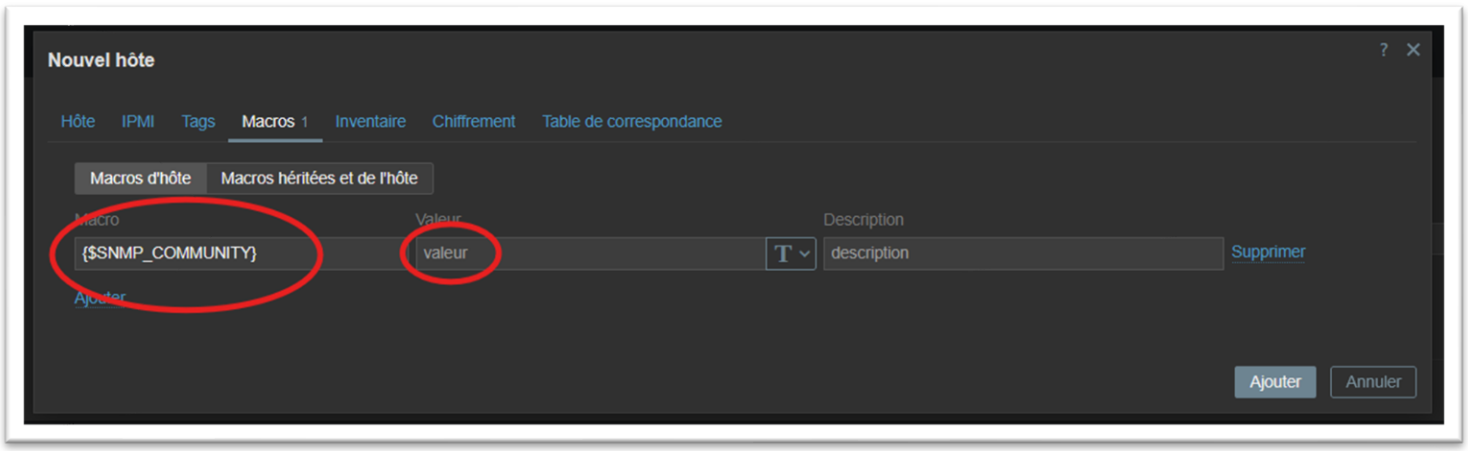
PS : N'oubliez pas d'activer le protocole SNMP sur la machine cible.



Une fois que vous avez réussi à collecter ces deux éléments renseigner dans le champ **Version SNMP** la version de SNMP utilisé.
Concernant la communauté SNMP utilisée, se rendre dans l'onglet **Macros**.



Une fois dans cet onglet remplissez la case de gauche comme ci-dessous puis la case du milieu avec le nom de la communauté SNMP utilisée par l'appareil à surveiller :

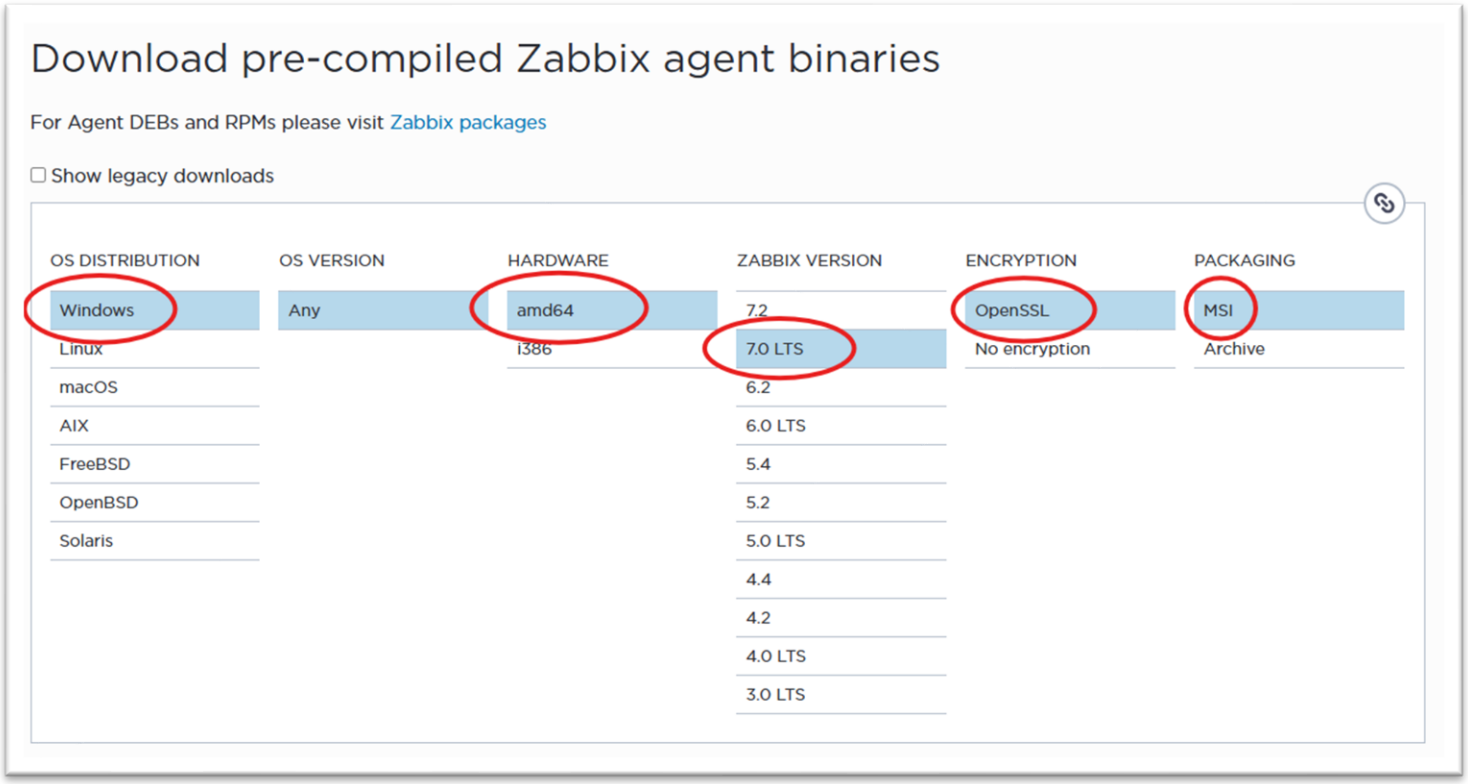


Vous pourrez ensuite valider vos modifications en cliquant sur **Ajouter** en bas à droite de la fenêtre.

Avec un agent Zabbix

Afin de mettre en place la surveillance d'un hôte à l'aide d'un agent Zabbix, munissez-vous du poste cible et rendez-vous dans la section d'installation des

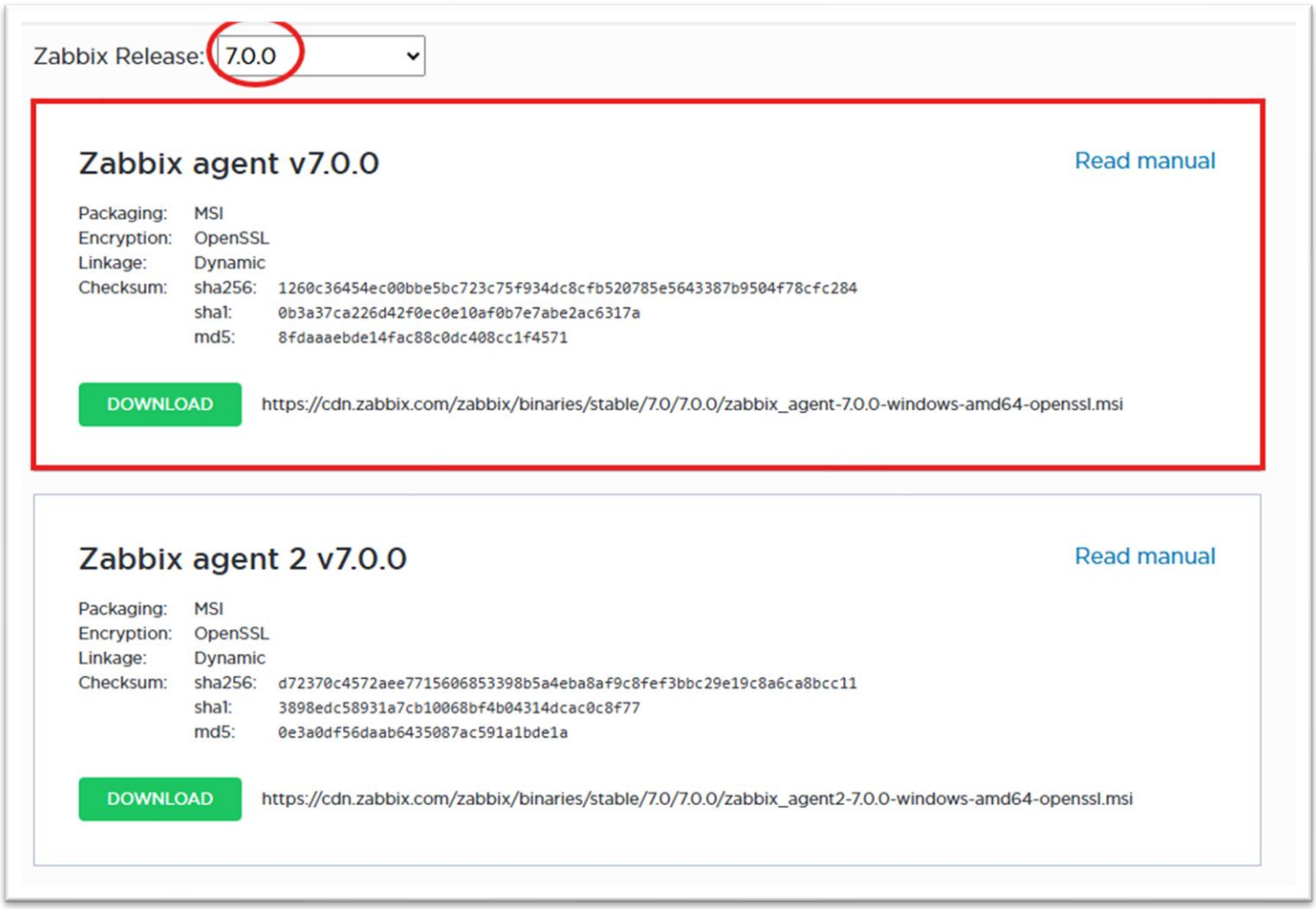
agents Zabbix sur le site de Zabbix (*ou au lien suivant :* [*https://www.zabbix.com/download_agents*](https://www.zabbix.com/download_agents)).



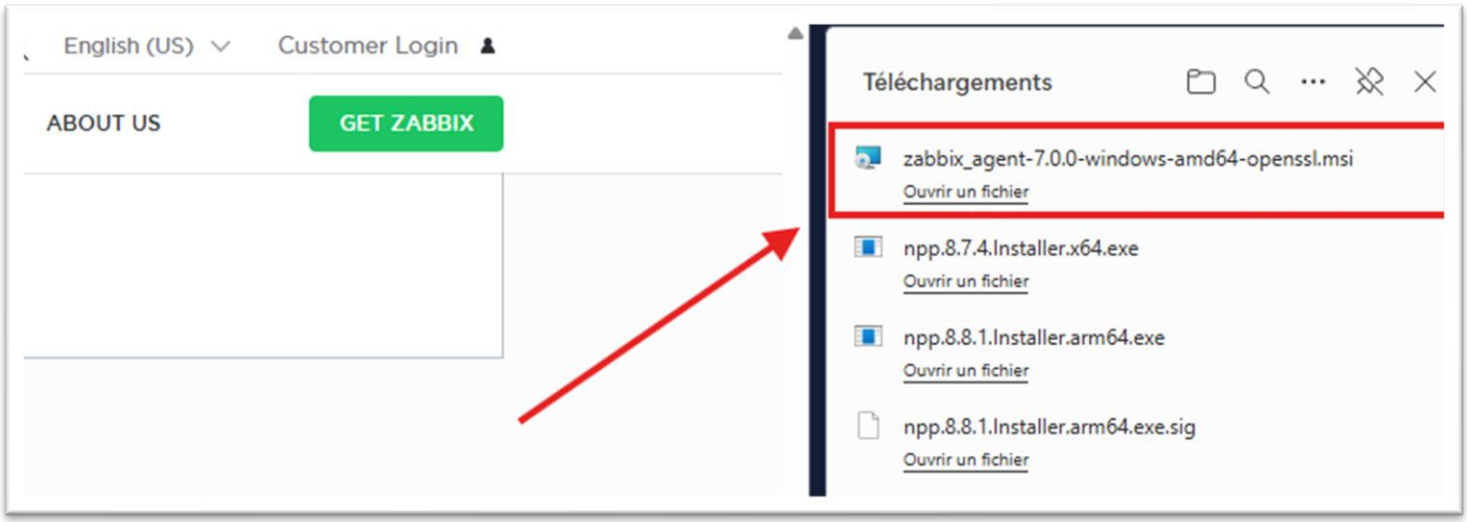
Sélectionnez le système d'exploitation de la machine détenteur de l'agent. Choisissez la version de matériel correspondant. Prenez la bonne version de Zabbix (*dans le cas présent la 7.0*). Choisissez l'option d'encryption pour plus de sécurité. Enfin prenez le packaging de type MSI.

-

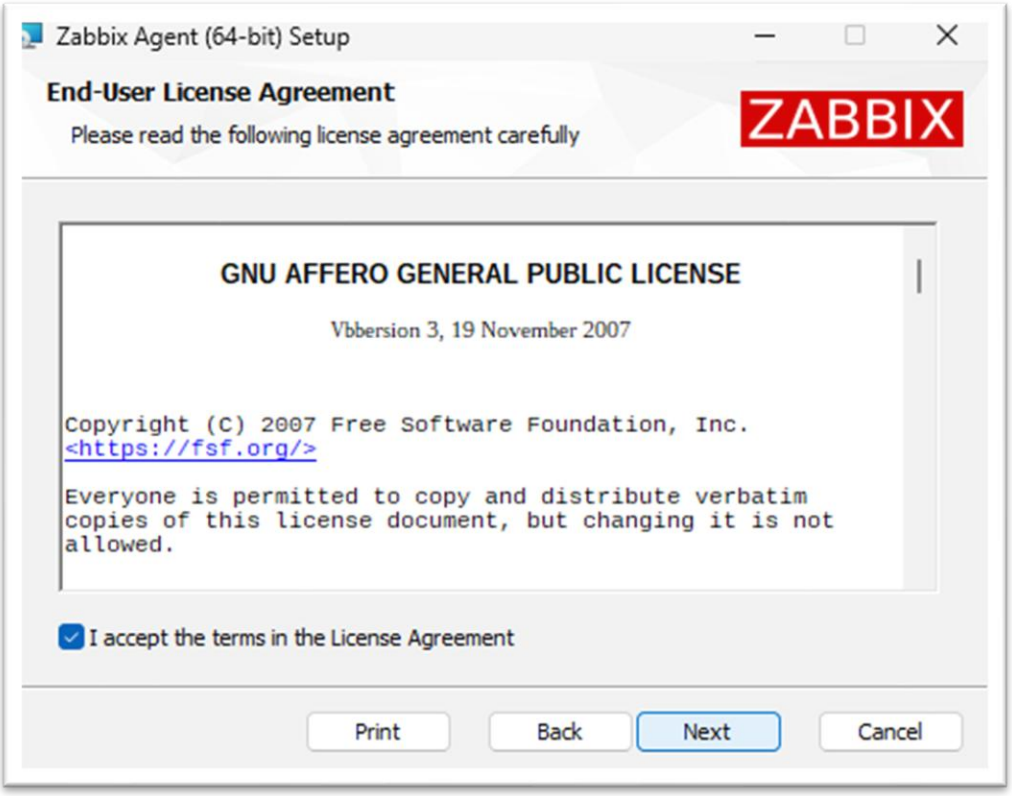
Maintenant place au téléchargement de l'agent. N'oubliez pas de mettre la bonne version de Zabbix puis télécharger un agent de type '*1*' :

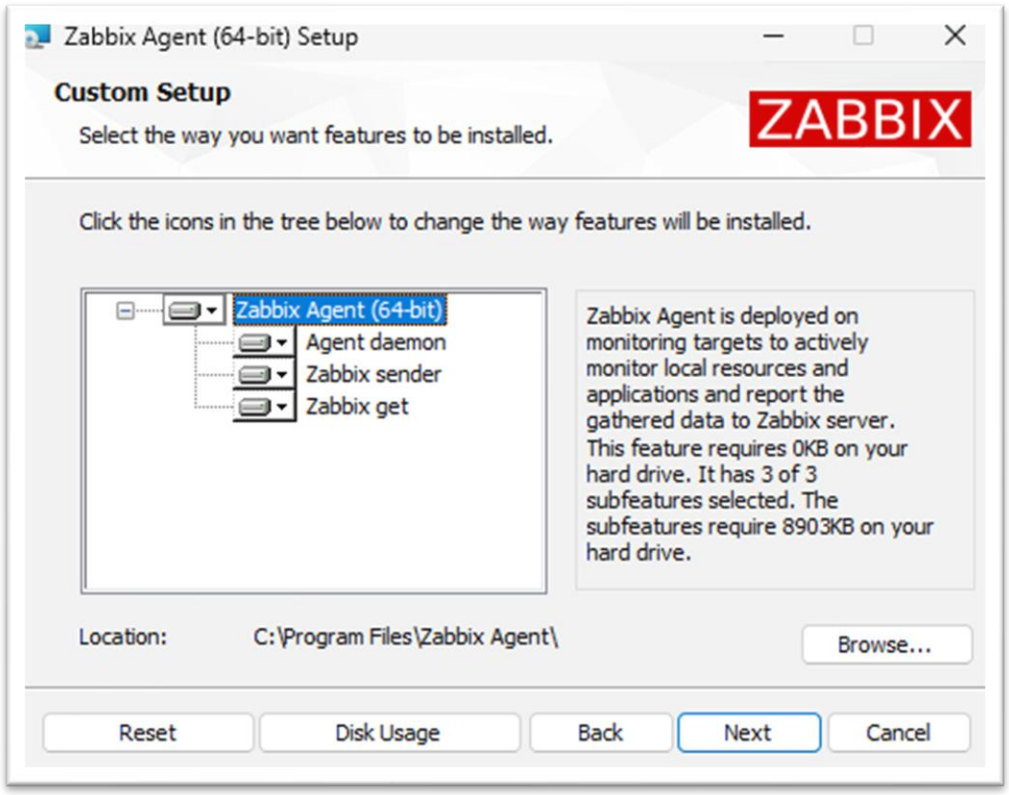


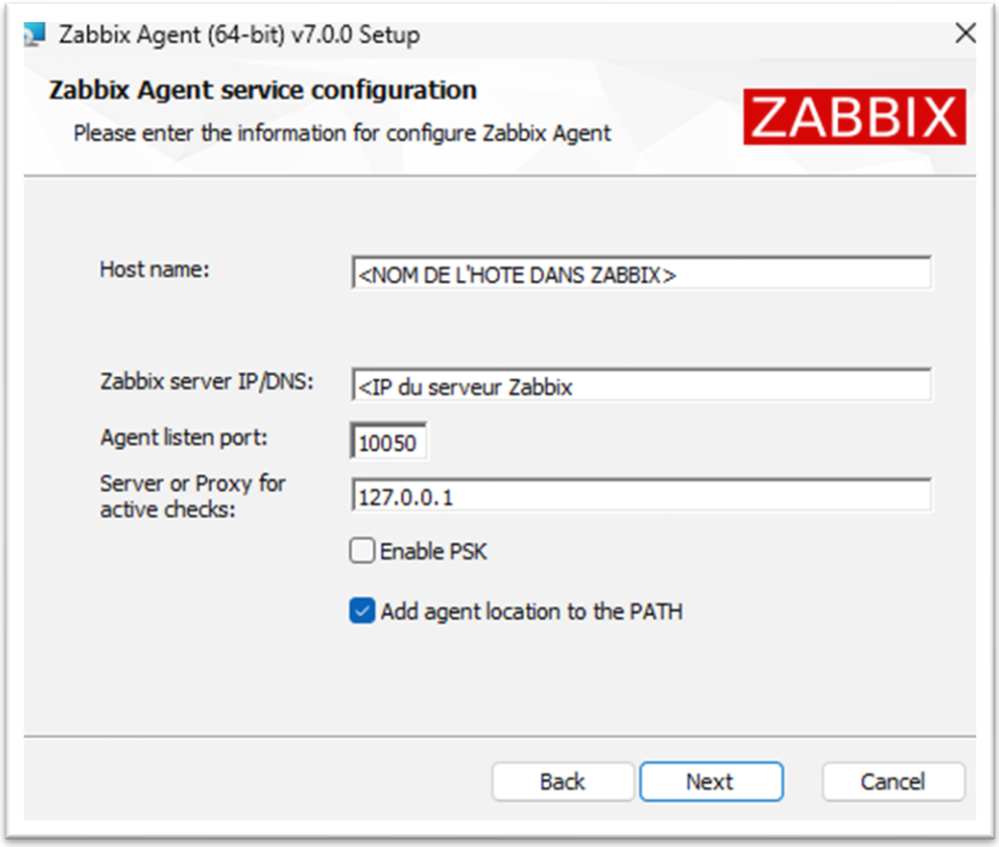
Cliquez ainsi sur **Download** puis téléchargez le fichier une fois installer.

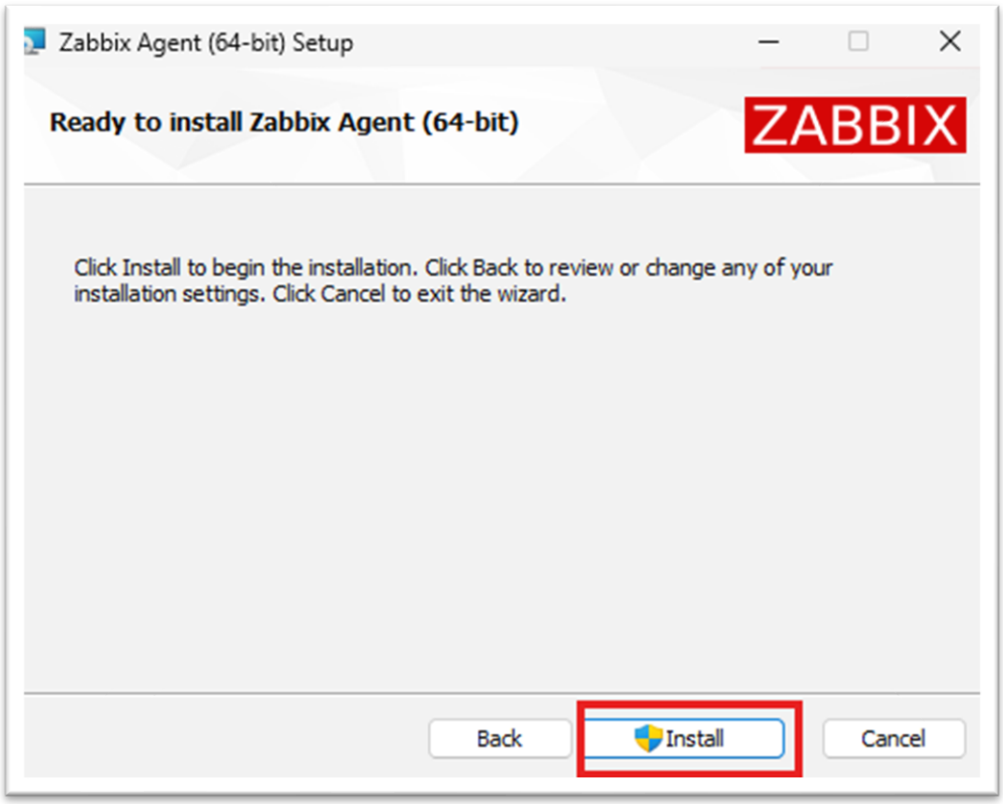



Zabbix Agent (64-bit) Setup
ZABBIX
The Enterprise-class Monitoring Solution for Everyone
www.zabbix.com
Welcome to the Zabbix Agent (64-bit) Setup Wizard
The Setup Wizard will install Zabbix Agent (64-bit) on your computer. Click Next to continue or Cancel to exit the Setup Wizard.
Back
Next
Cancel


Zabbix Agent (64-bit) Setup
End-User License Agreement
Please read the following license agreement carefully
ZABBIX
GNU AFFERO GENERAL PUBLIC LICENSE
Vbbersion 3, 19 November 2007
Copyright (C) 2007 Free Software Foundation, Inc.
<https://fsf.org/>
Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.
I accept the terms in the License Agreement
Print
Back
Next
Cancel


Zabbix Agent (64-bit) Setup
Custom Setup
Select the way you want features to be installed.
ZABBIX
Click the icons in the tree below to change the way features will be installed.
Zabbix Agent (64-bit)
Agent daemon
Zabbix sender
Zabbix get
Zabbix Agent is deployed on monitoring targets to actively monitor local resources and applications and report the gathered data to Zabbix server. This feature requires 0KB on your hard drive. It has 3 of 3 subfeatures selected. The subfeatures require 8903KB on your hard drive.
Location:
C:\Program Files\Zabbix Agent\
Browse...
Reset
Disk Usage
Back
Next
Cancel

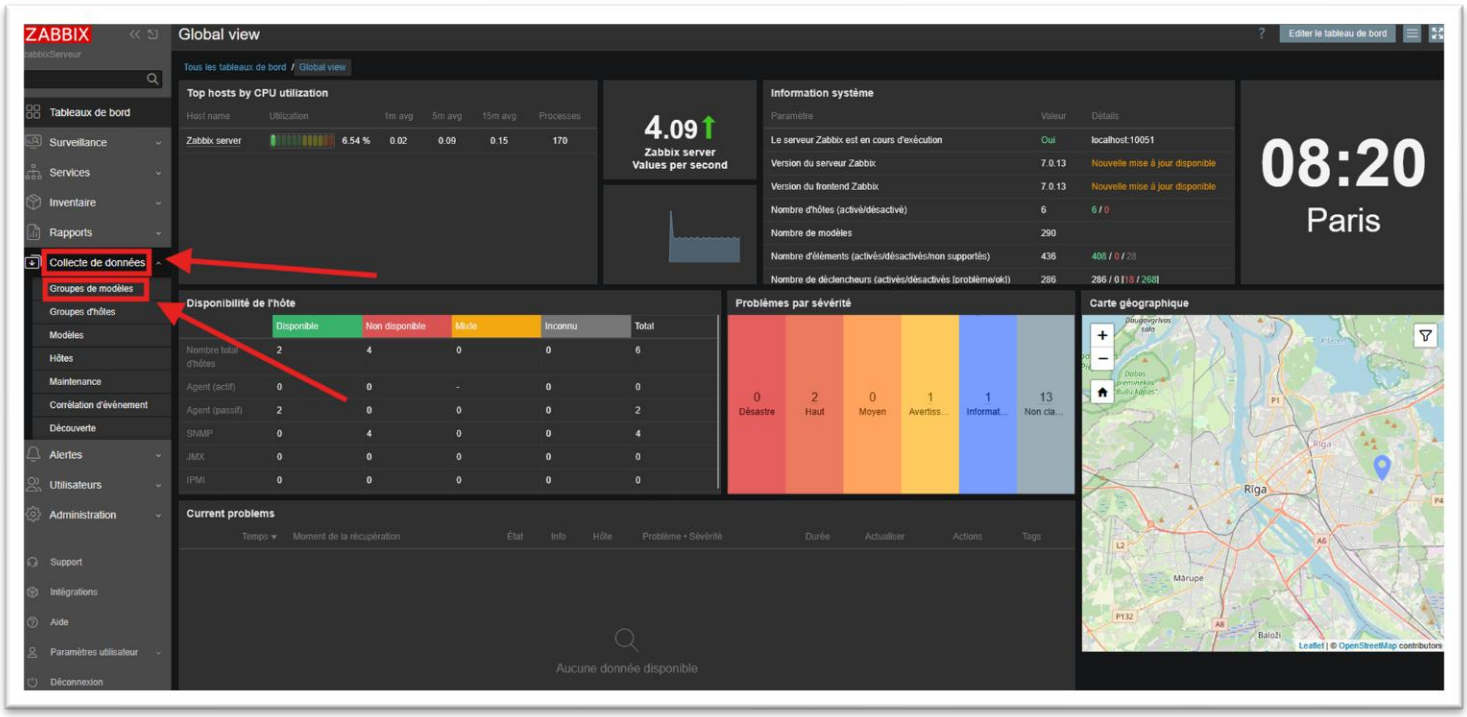

Zabbix Agent (64-bit) v7.0.0 Setup
Zabbix Agent service configuration
Please enter the information for configure Zabbix Agent
ZABBIX
Host name:
<NOM DE L'HOTE DANS ZABBIX>
Zabbix server IP/DNS:
<IP du serveur Zabbix
Agent listen port:
10050
Server or Proxy for active checks:
127.0.0.1
Enable PSK
Add agent location to the PATH
Back
Next
Cancel



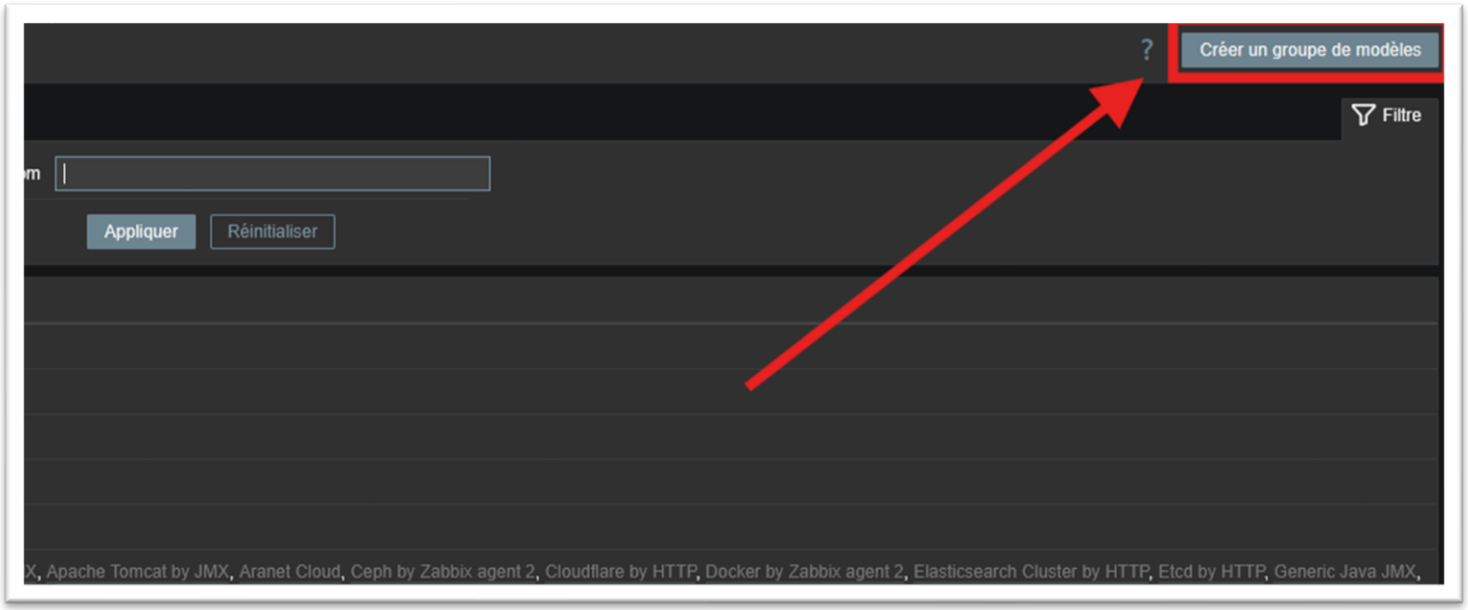
Enfin, une fois l'installation effectuée, de retour sur Zabbix, vous n'avez plus qu'à entrer l'IP de l'hôte dans le champ IP de l'agent de l'hôte. Puis ajoutez votre hôte.

Créer un groupe de modèles

La création d'un groupe de modèles est aussi simple que la création d'un dossier dans lequel on place des fichiers.
Pour se faire il suffit de se rendre dans la section **Collecte de données** puis Groupe de modèles :



Sélectionnez ensuite **Créer un groupe de modèle** :

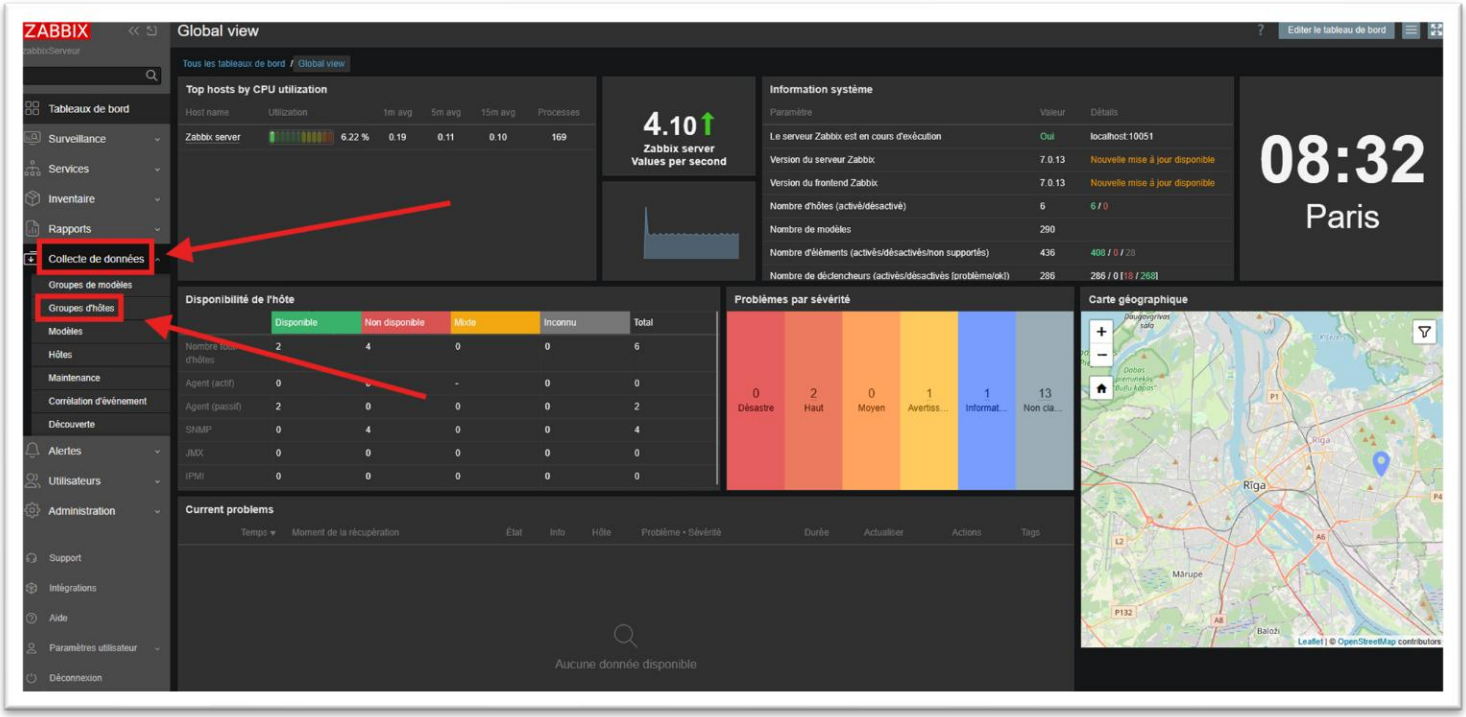


Entrez ensuite le nom du groupe de modèle, par exemple WatchGuard :

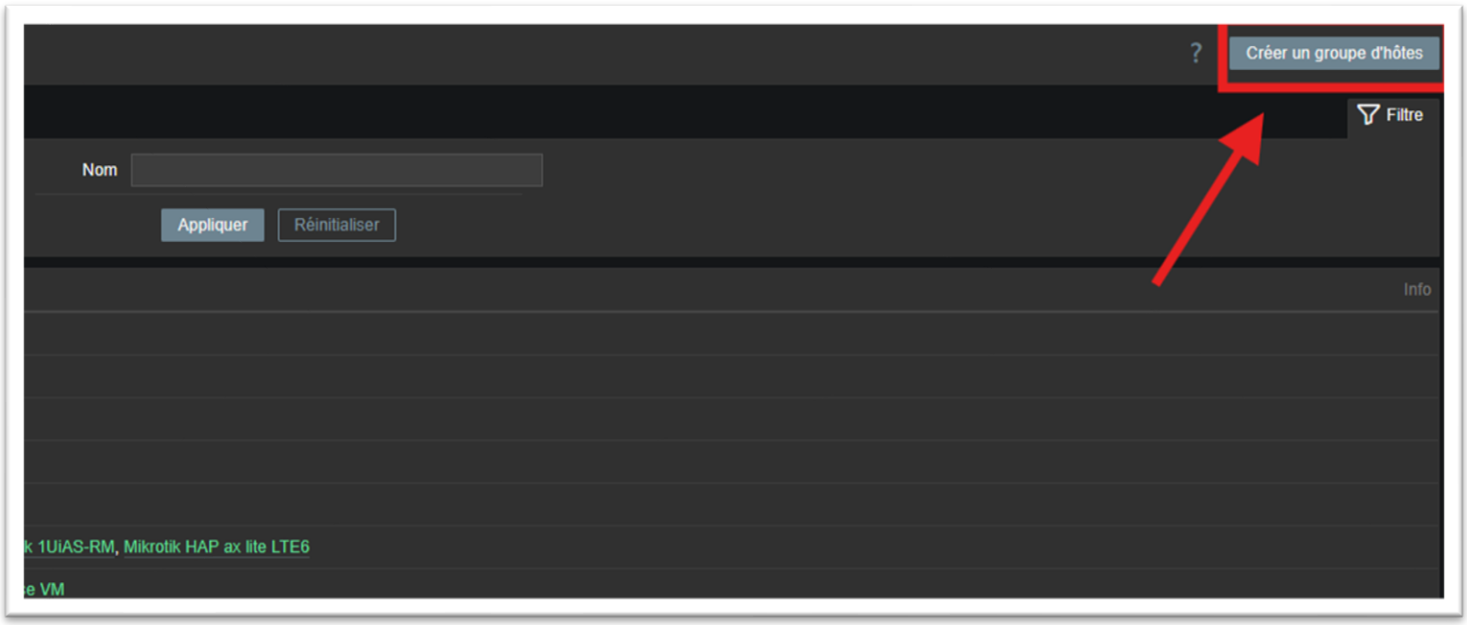
Ensuite plus qu'à ajouter le groupe et il apparaitra dans le tableau.

Créer un groupe d'hôtes

Démarche similaire à celle des groupes de modèles. Rendez-vous dans la section **Collecte de données** puis dans **Groupes d'hôtes**.



Puis **Créer un groupe d'hôtes** :



Puis entrez le nom du groupe d'hôtes, par exemple WatchGuard :

Enfin ajouter le groupe d'hôtes. Il apparaitra dans le tableau.

Télécharger, Installer et mettre en place un Template

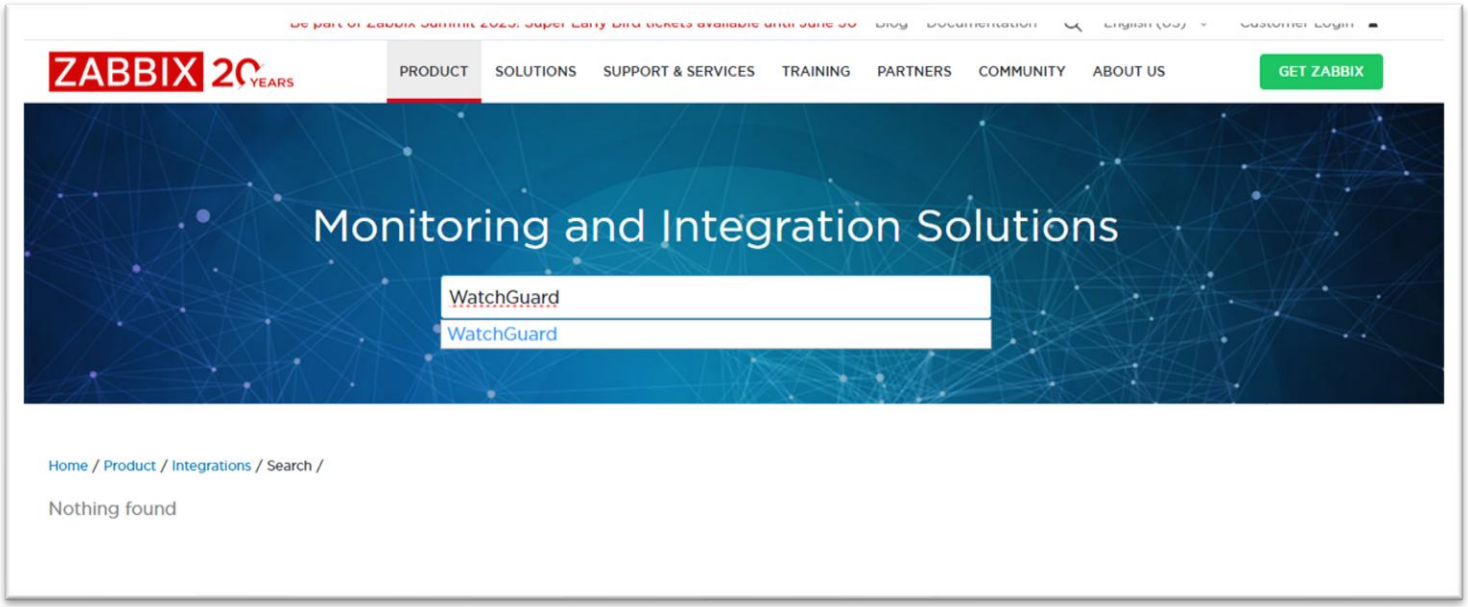
Avant toute chose, il est nécessaire de comprendre qu'un Template n'est pas toujours compatible avec un hôte ou avec une version de Zabbix.
Les Template dit non communautaires proposé par Zabbix lui-même (sur son site ou pré-intégré à la version) sont généralement complétement compatible avec les machines qui y sont indiquées.
Mais les templates communautaires provenant généralement des plateformes communautaires tel que GitHub sont eux plus susceptible de manquer de compatibilité avec certains appareils.

Néanmoins ces deux types de templates ont un point commun, ils sont tous les deux répertoriés sur le site de Zabbix nous évitant ainsi d'aller chercher sur de multiples sites.

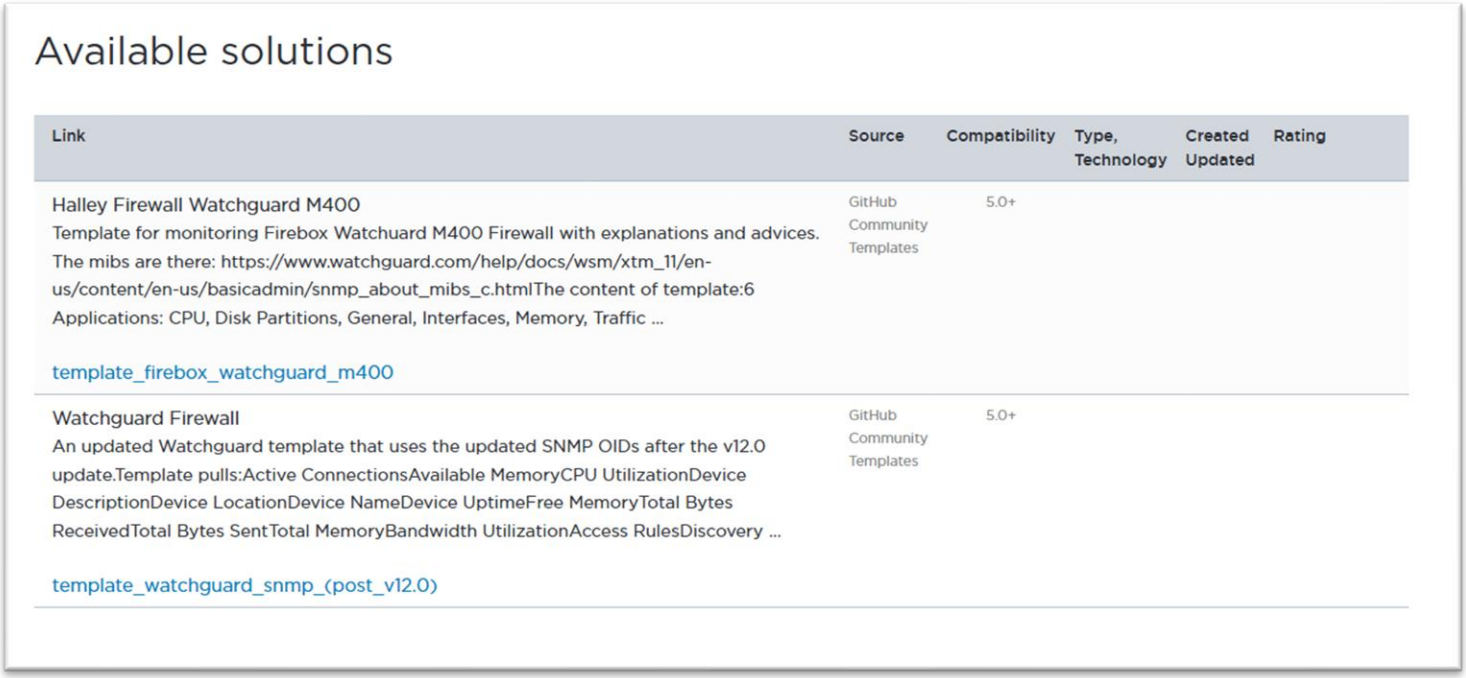
-

Afin de télécharger un template rendez-vous dans la section intégration du site de Zabbix au lien suivant : https://www.zabbix.com/integrations

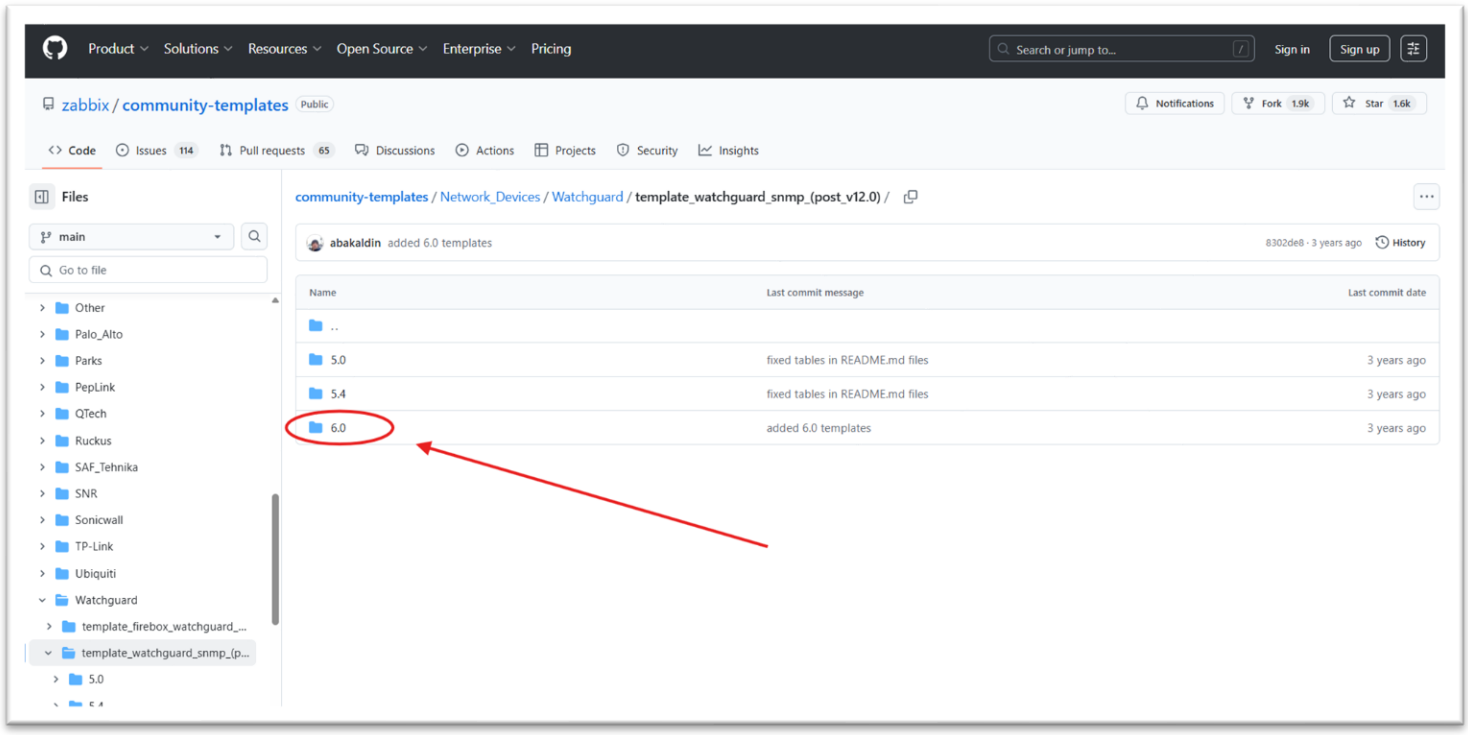
Puis entrez le nom de la marque de la machine (*tout au long de l'explication on prendra en exemple les Firebox de WatchGuard*) :

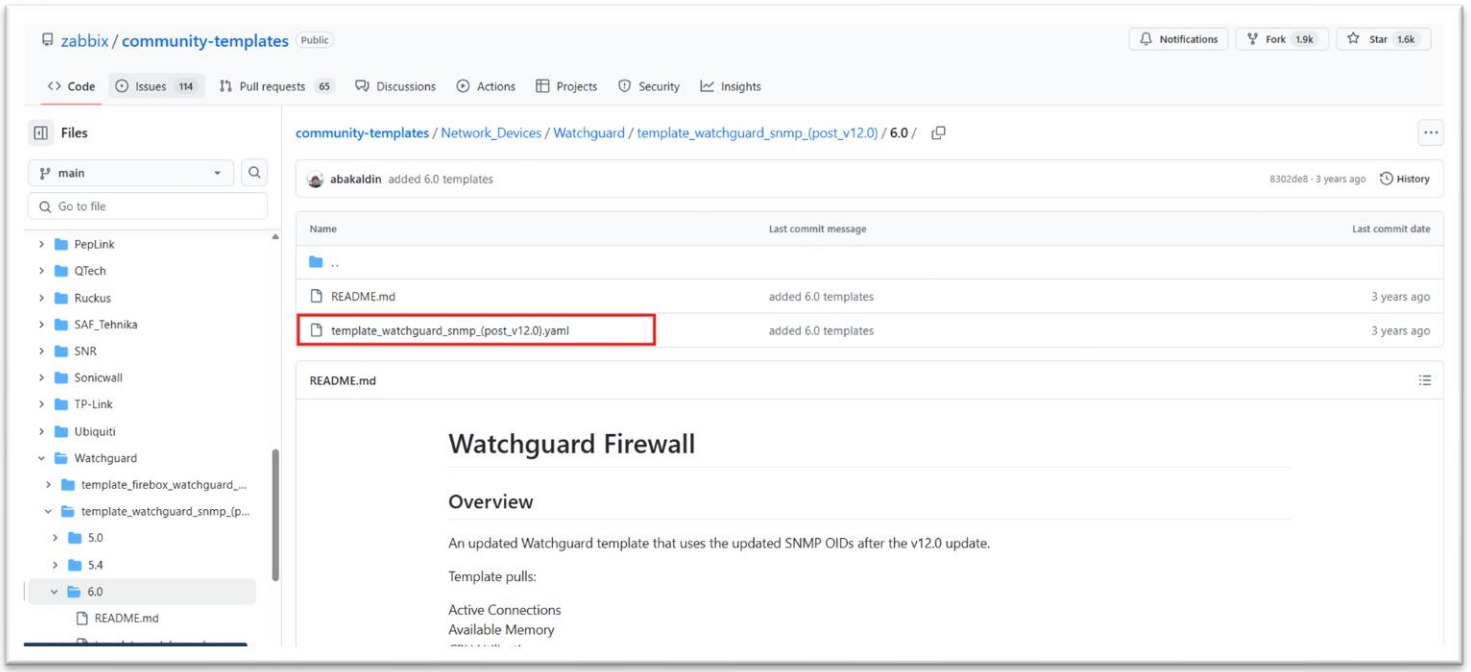


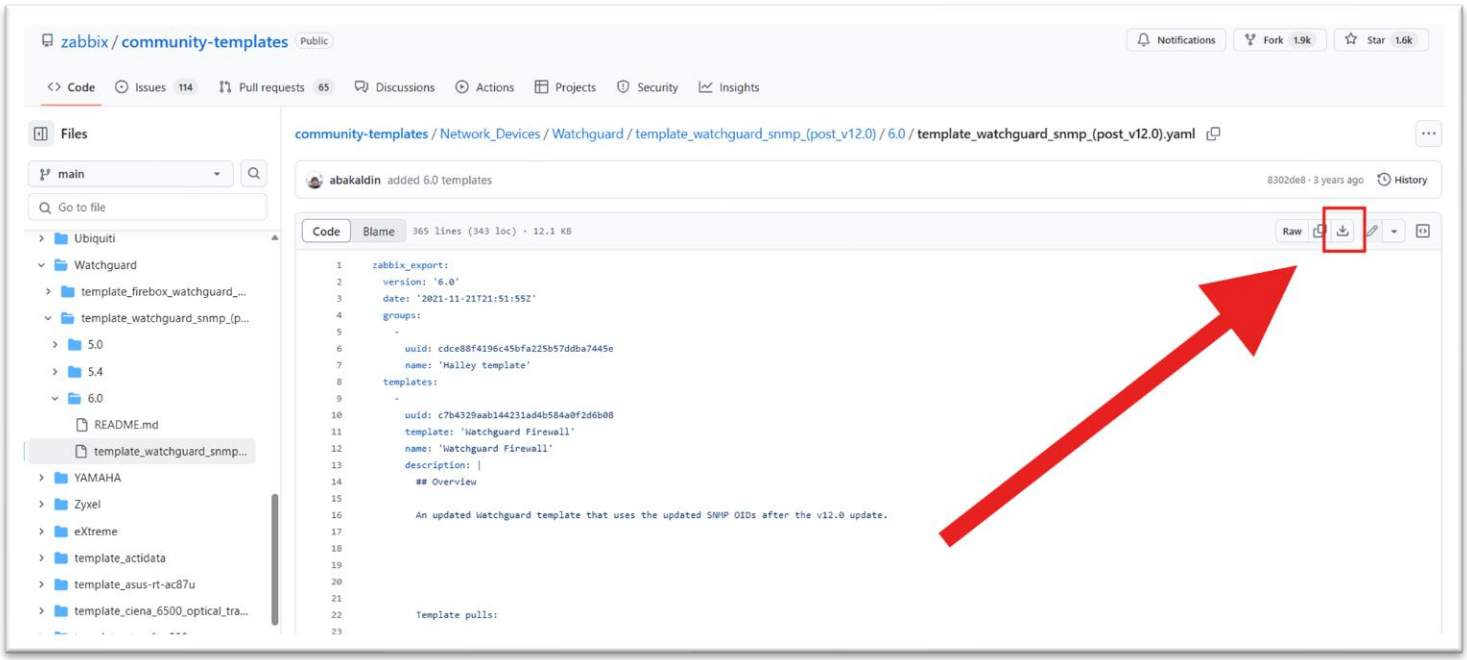
Puis faire **Entrer** :



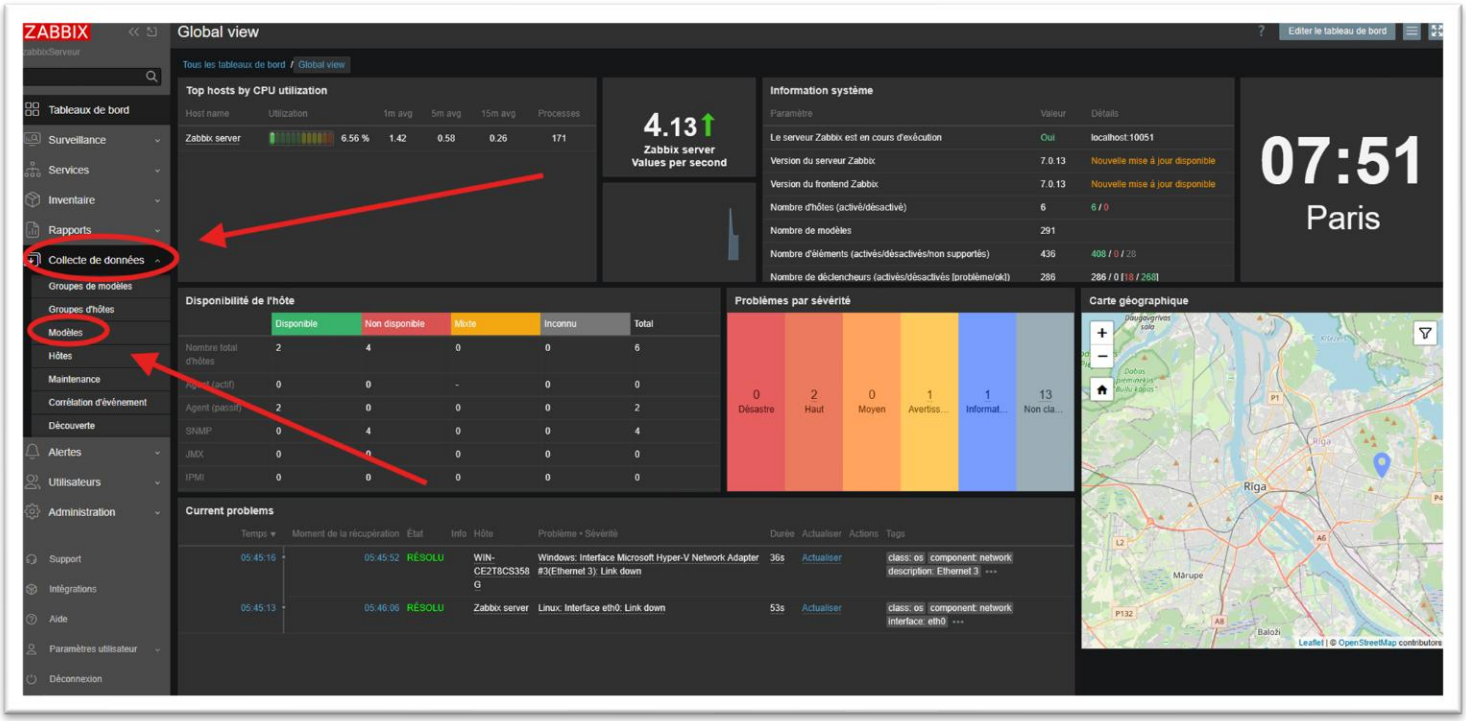
Ici on sélectionnera la version post_v12.0 car il s'agit d'une version utilisant le SNMP. On clique alors sur le lien en bleu.
Dans le cas présent, il s'agit d'un template communautaire donc on va être rediriger vers GitHub.


Product
Solutions
Resources
Open Source
Enterprise
Pricing
Search or jump to...
Sign in
Sign up
zabbix / community-templates
Public
Notifications
Fork 1.9k
Star 1.6k
Code
Issues 114
Pull requests 65
Discussions
Actions
Projects
Security
Insights
Files
main
Go to file
Other
Palo_Alto
Parks
PepLink
QTech
Ruckus
SAF_Tehnika
SNR
Sonicwall
TP-Link
Ubiquiti
Watchguard
template_firebox_watchguard_...
template_watchguard_snmp_(p...
5.0
community-templates / Network_Devices / Watchguard / template_watchguard_snmp_(post_v12.0) /
abakaldin added 6.0 templates
8302de8 · 3 years ago
History
Name
Last commit message
Last commit date
..
5.0
fixed tables in README.md files
3 years ago
5.4
fixed tables in README.md files
3 years ago
6.0
added 6.0 templates
3 years ago

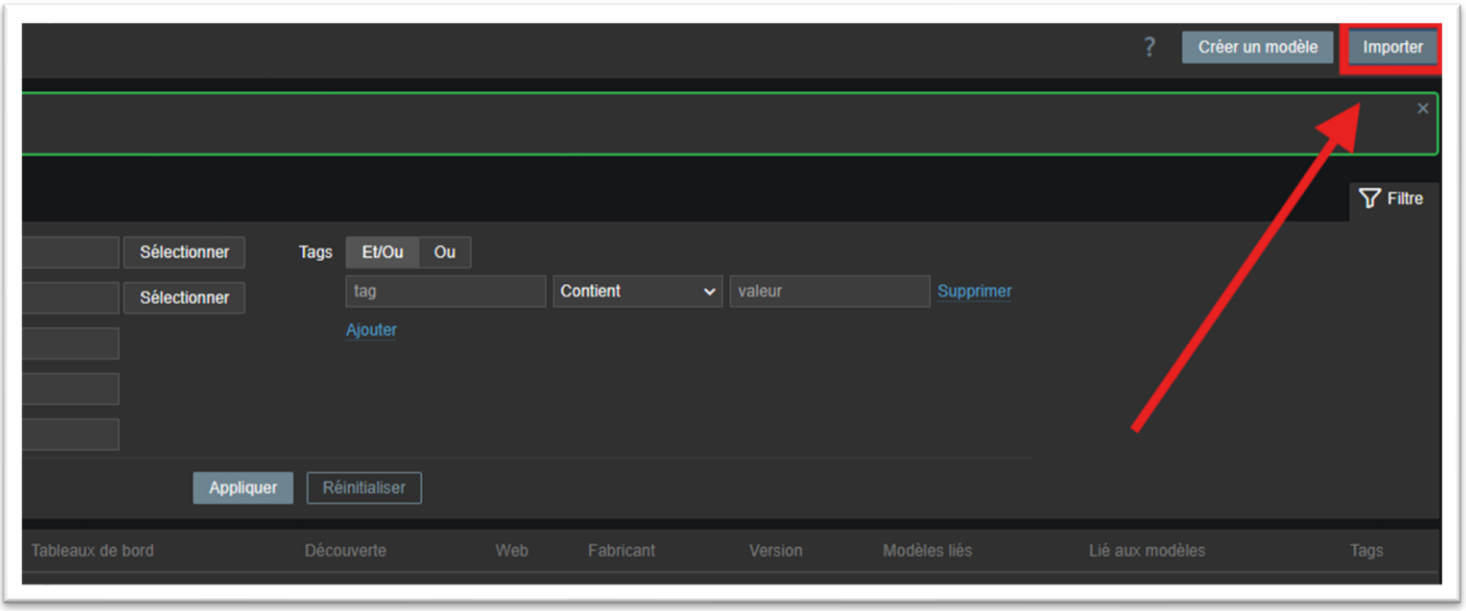

zabbix / community-templates
Public
Notifications
Fork 1.9k
Star 1.6k
Code
Issues 114
Pull requests 65
Discussions
Actions
Projects
Security
Insights
Files
main
Go to file
PepLink
QTech
Ruckus
SAF_Tehnika
SNR
Sonicwall
TP-Link
Ubiquiti
Watchguard
template_firebox_watchguard_...
template_watchguard_snmp_(p...
5.0
5.4
6.0
README.md
community-templates / Network_Devices / Watchguard / template_watchguard_snmp_(post_v12.0) / 6.0 /
abakaldin added 6.0 templates
8302de8 · 3 years ago
History
Name
Last commit message
Last commit date
..
README.md
added 6.0 templates
3 years ago
template_watchguard_snmp_(post_v12.0).yaml
added 6.0 templates
3 years ago
README.md
Watchguard Firewall
Overview
An updated Watchguard template that uses the updated SNMP OIDs after the v12.0 update.
Template pulls:
Active Connections
Available Memory



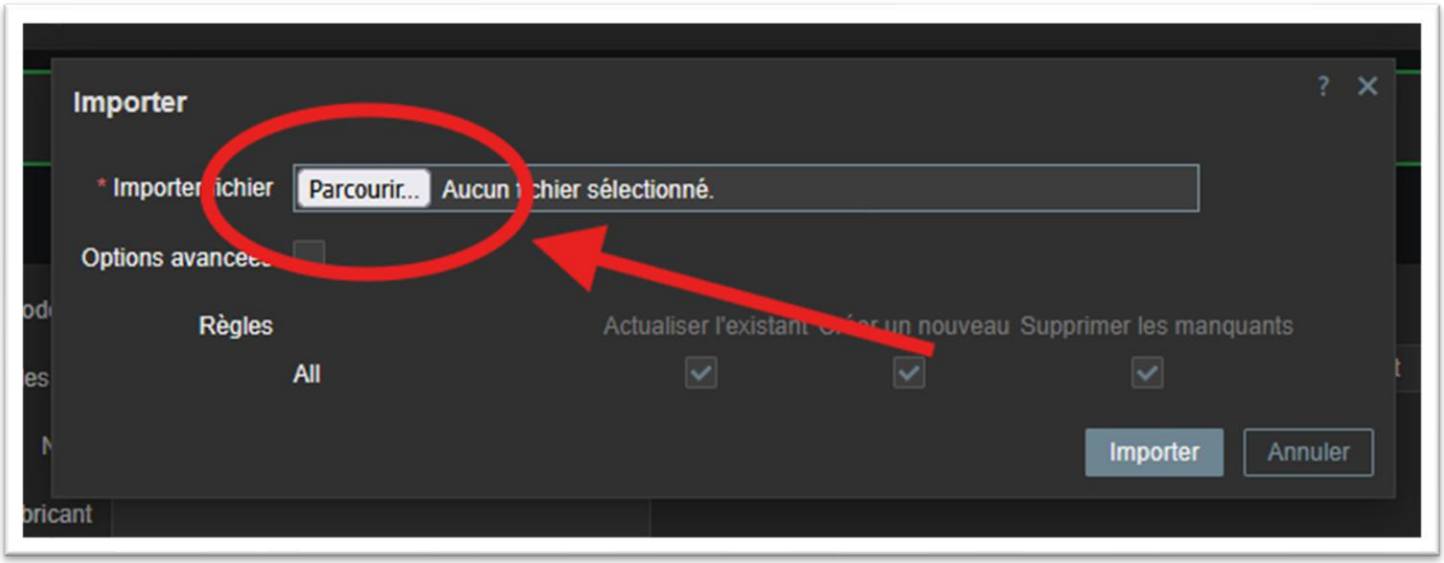
Ensuite, reste à importer notre Template dans Zabbix. Pour se faire se rendre dans la section **Collecte de données** puis dans **Modèles** :



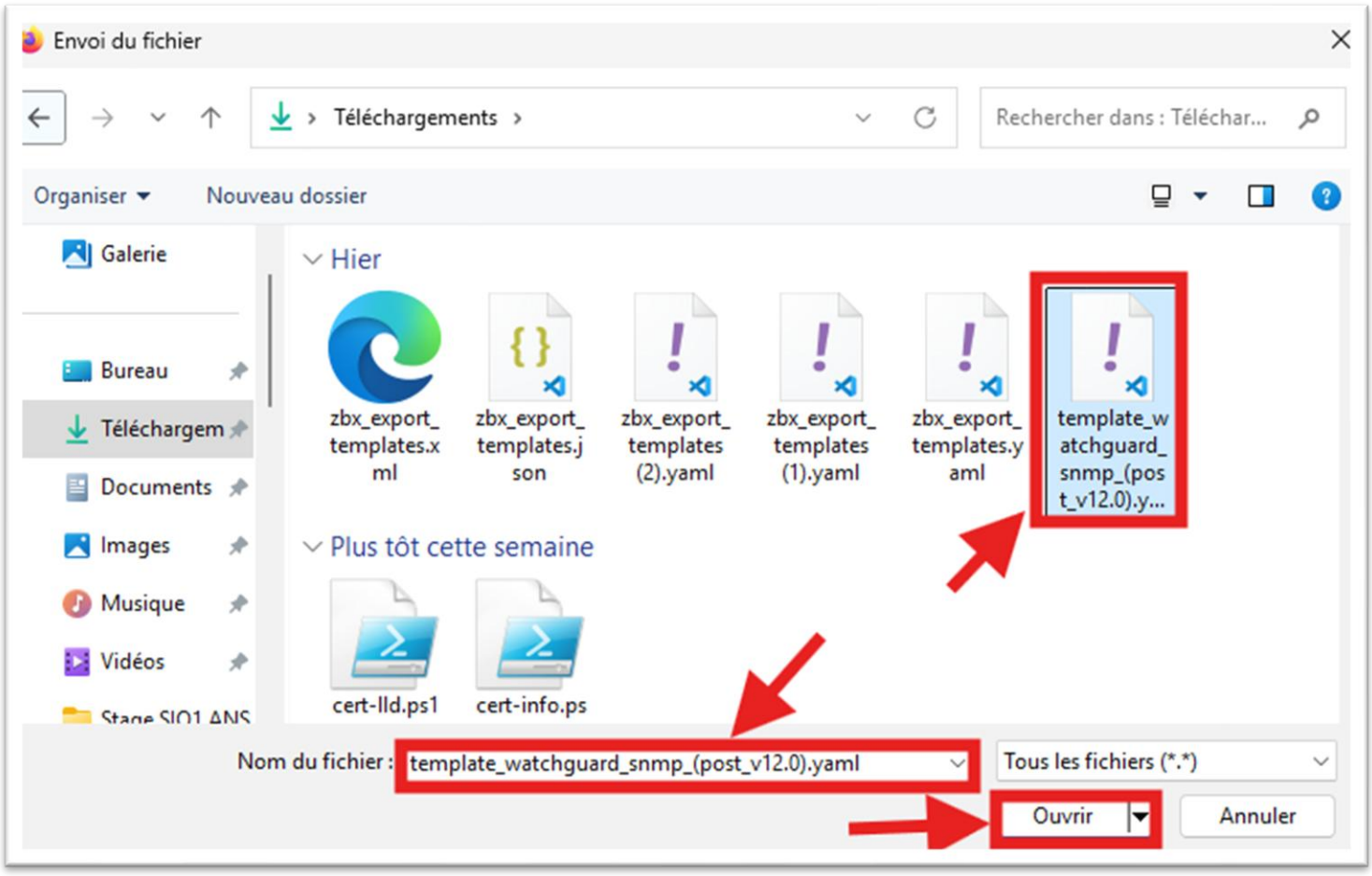
Puis cliquez sur **Importer** :



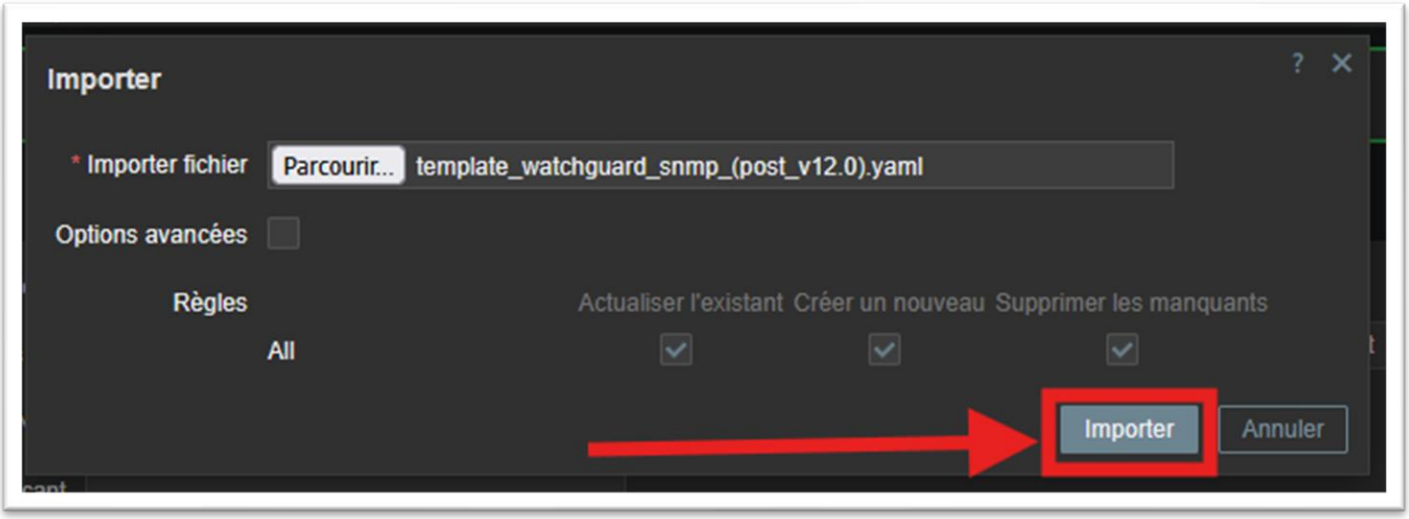
Puis **Parcourir** les fichiers de votre poste pour retrouver votre fichier de Template.



Sélectionnez votre Template :

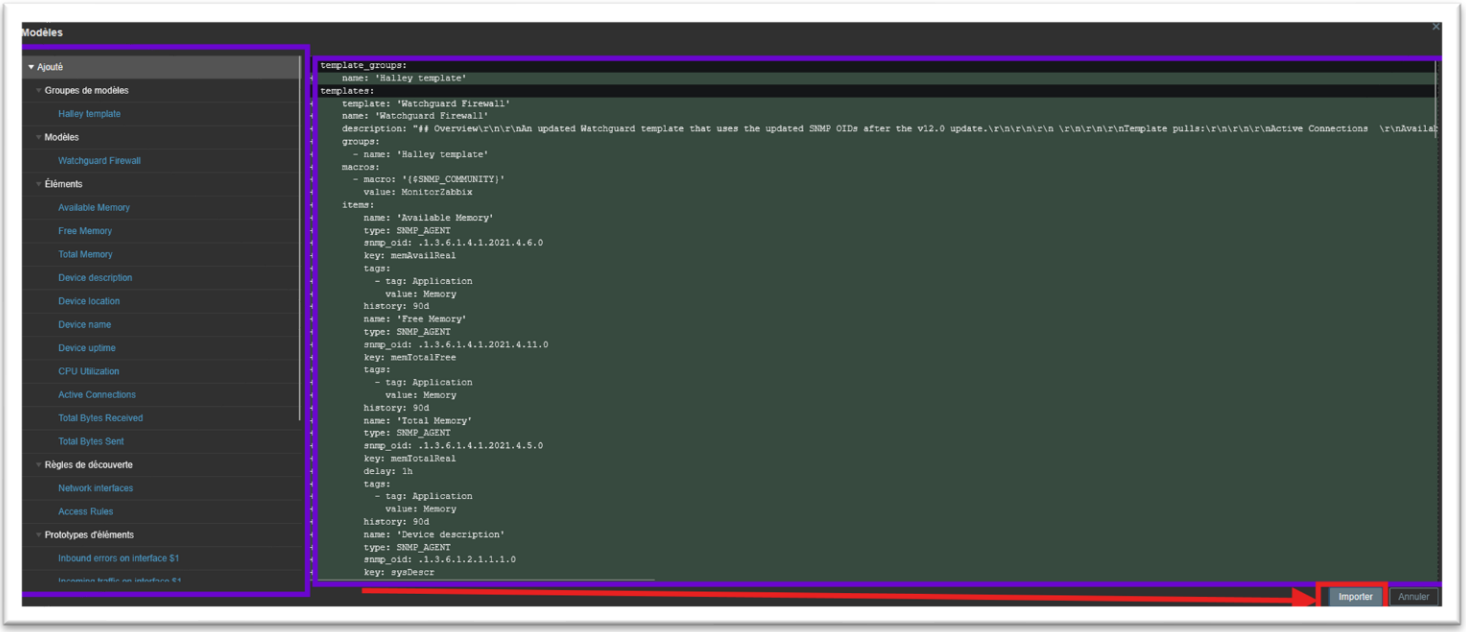


Cliquez ensuite sur **Importer** :

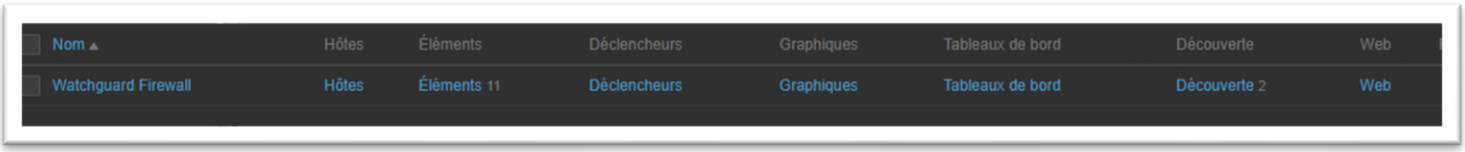


Ensuite apparaitra sur la gauche de la pop-up le résumé des éléments présents dans le Template. Sur la droite sera affiché le code du Template. Cliquez ici sur **Importer** de nouveau afin d'importer le Template.

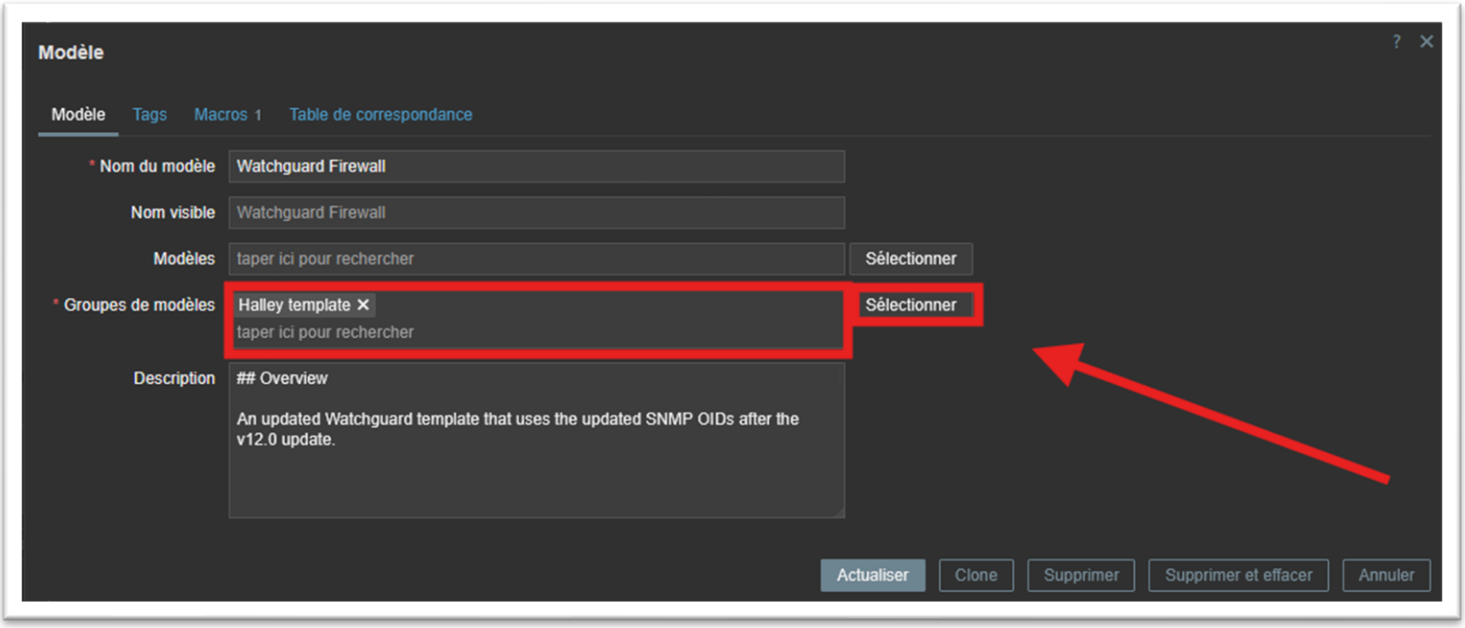
PS : Prêtez bien attention à ce que le Template n'existe pas déjà ou que certains éléments ne soit pas déjà présent dans d'autres Template, cela pourrait empêcher Zabbix d'importer le Template en vous renvoyant une erreur.



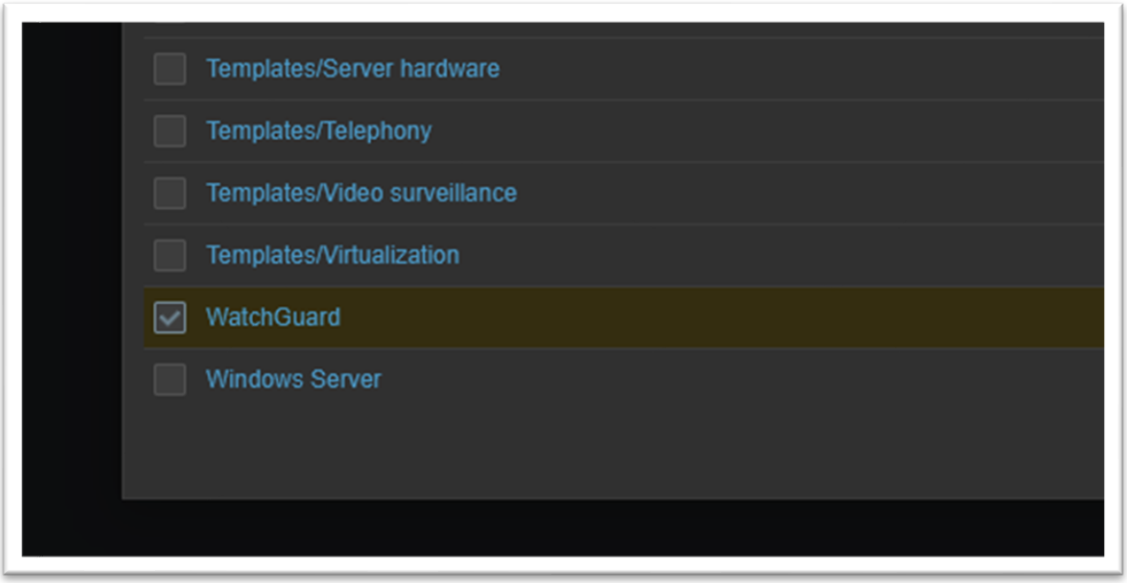
Une fois importé le Template sera affiché dans le tableau à l'écran :

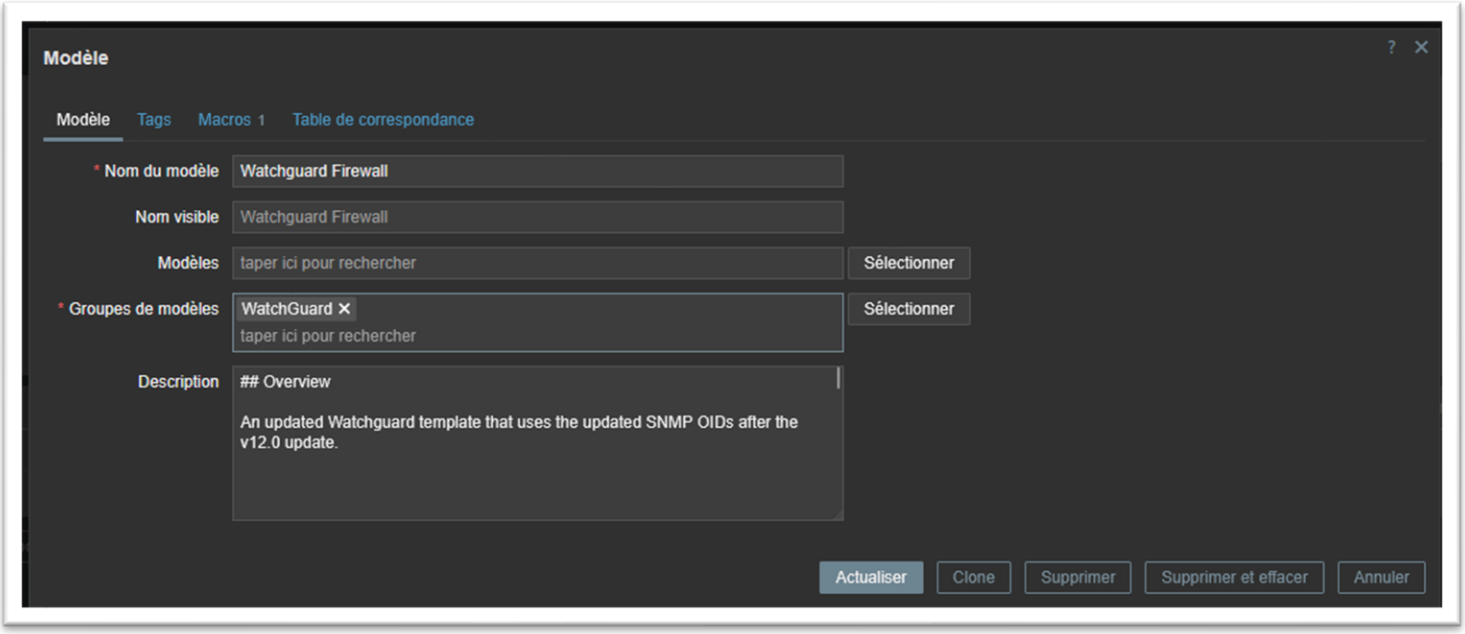


Maintenant on va devoir associer un emplacement dans un groupe de modèles au modèle (Template) que l'on vient d'importer. Pour se faire cliquez sur le nom du Template. Dans la fenêtre pop-up qui s'ouvre cliquez sur **Sélectionner** pour sélectionner un nouveau groupe de modèle :

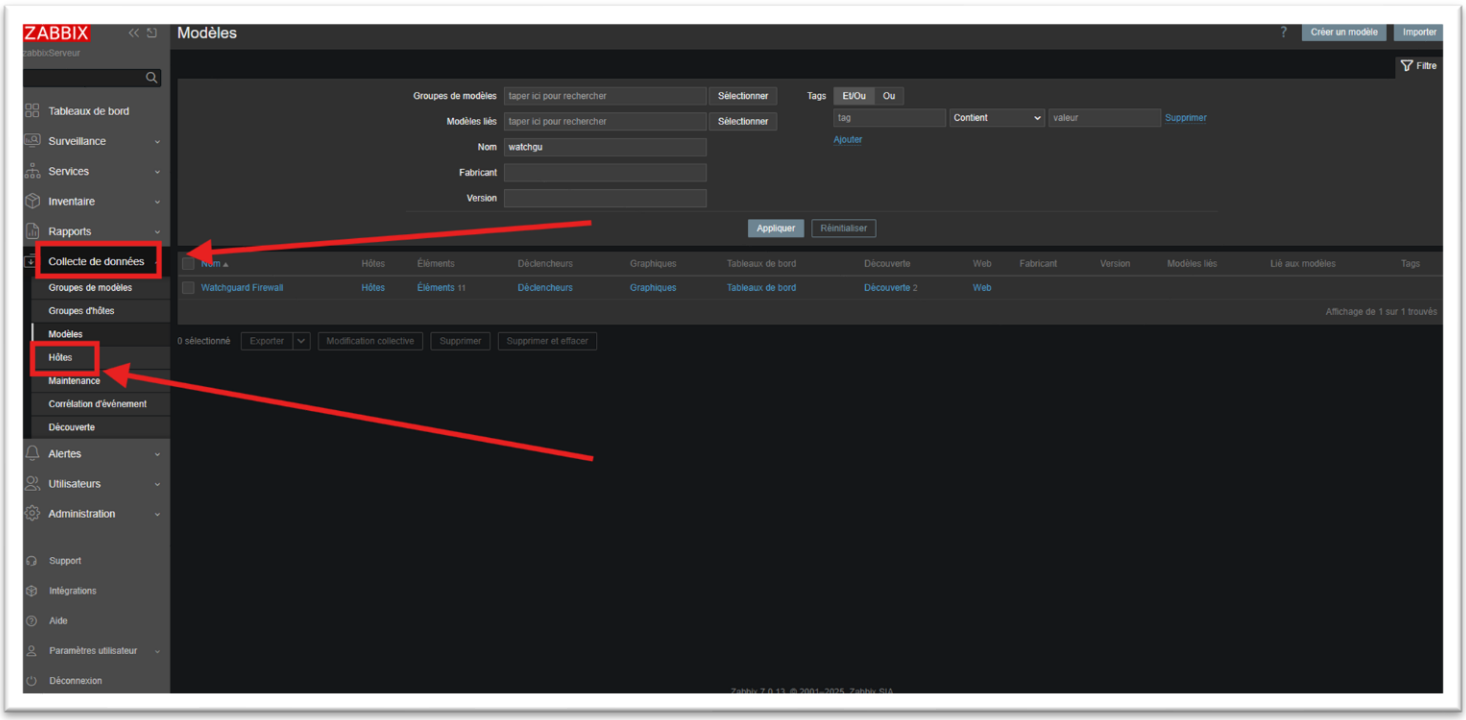


Ici si vous avez suivit toutes les étapes de cette documentation/procédure, vous devriez voir apparaitre le groupe de modèle créer auparavant (WatchGuard). Si cela vous convient sélectionnez ce groupe de modèle et retirez celui attribué par défaut.

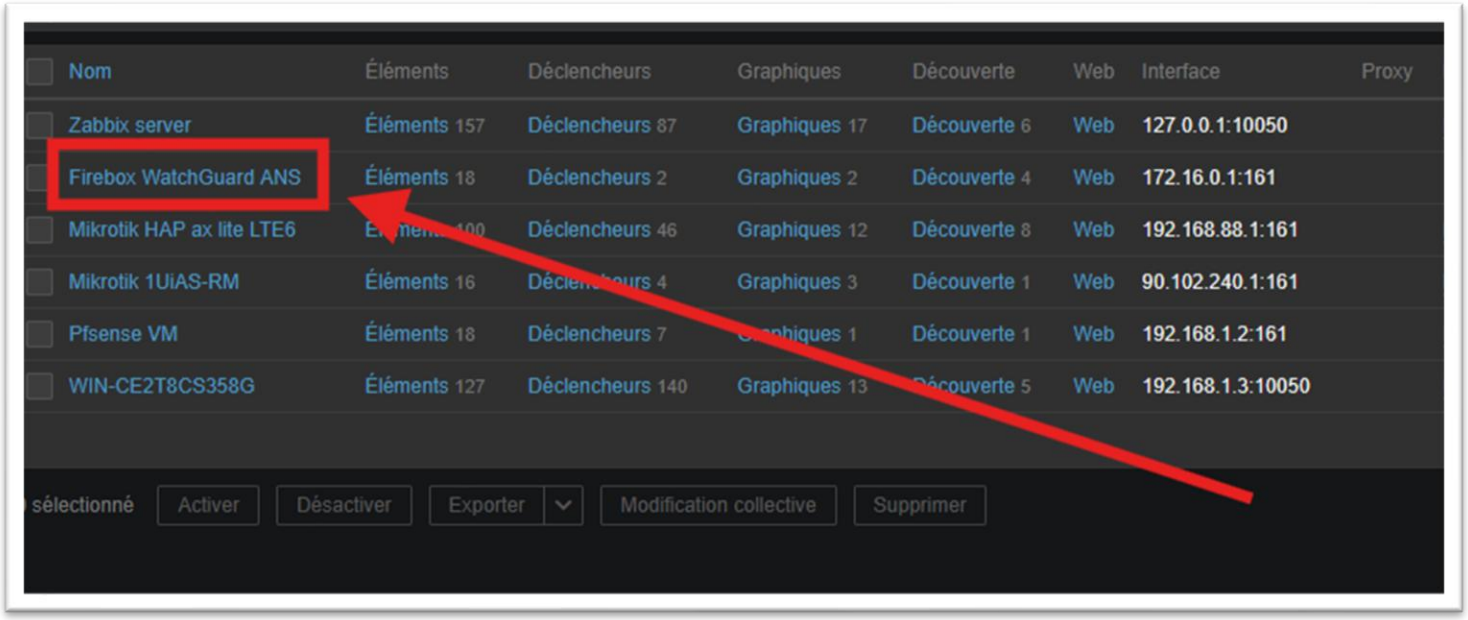




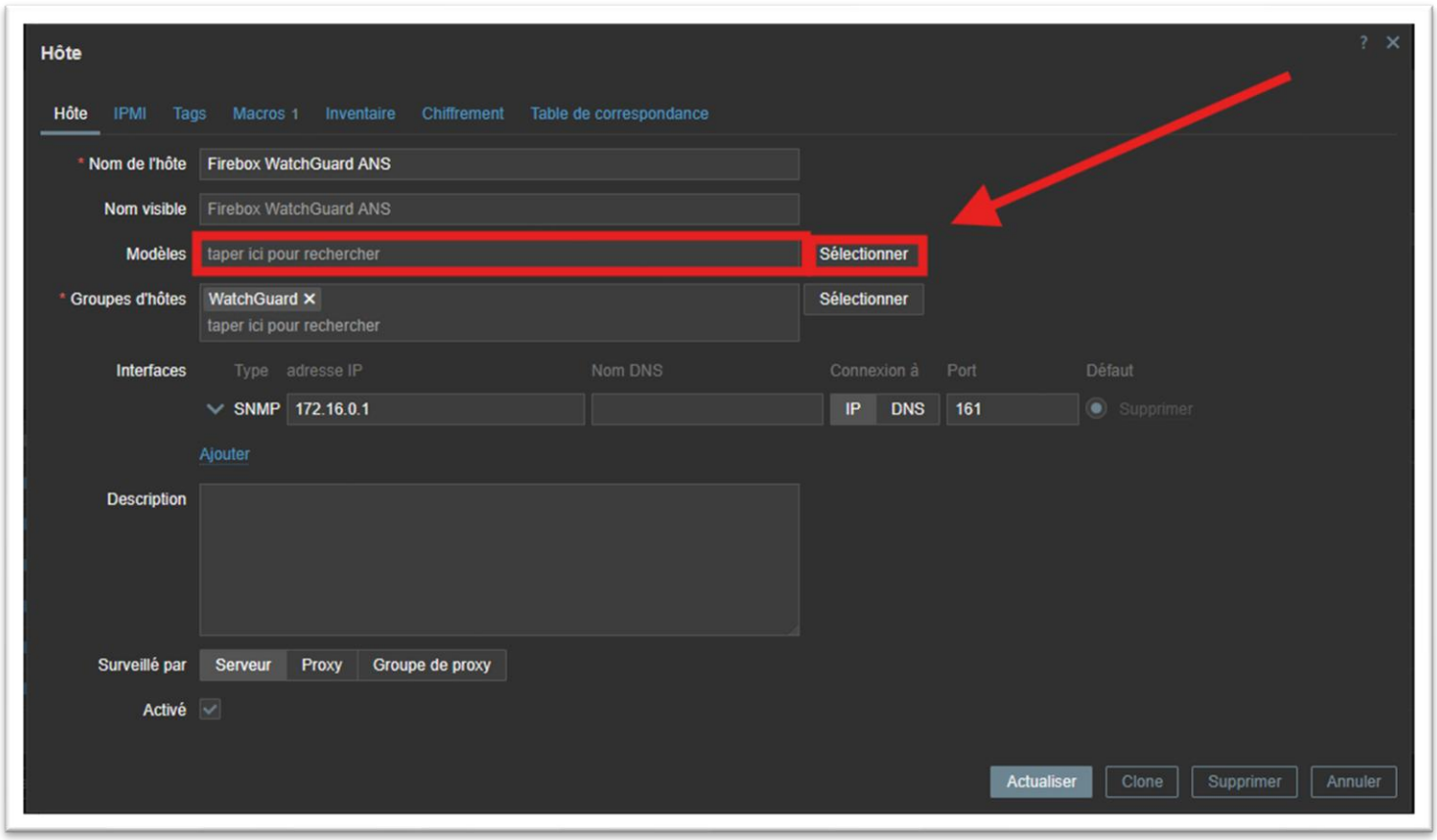
Maintenant pour pouvoir faire remonter nos données et pouvoir faire du reporting, nous allons devoir associer ce Template à un hôte. Pour ce faire nous allons aller sélectionner notre hôte dans **Collecte de données** puis dans **Hôtes** :



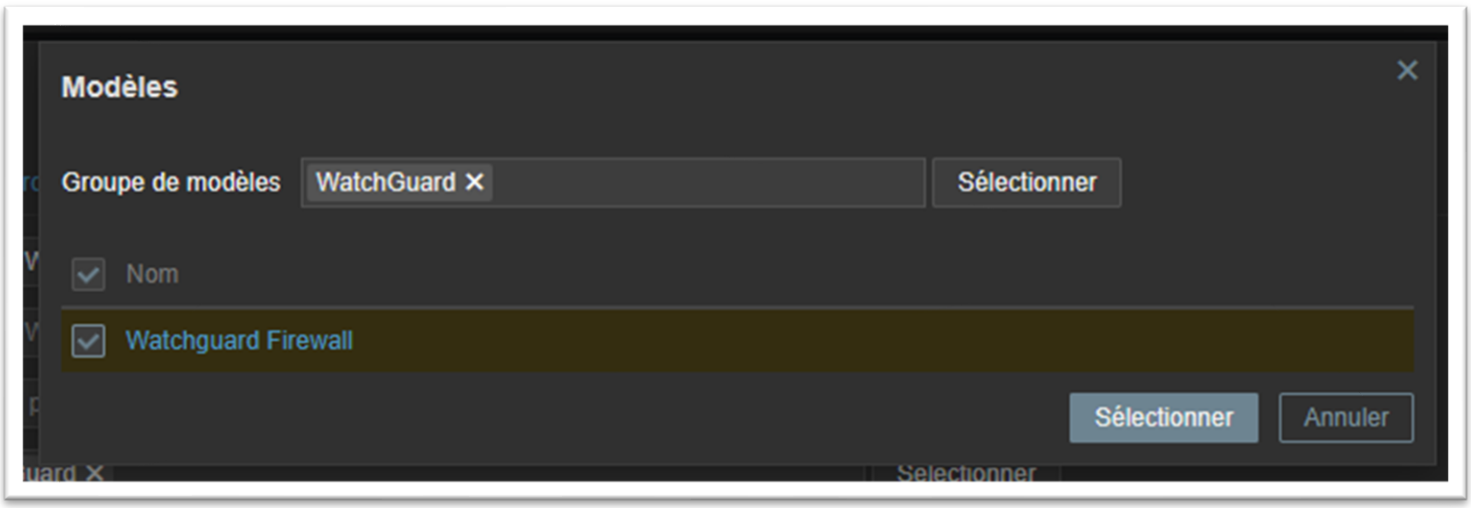
Cliquez sur l'hôte souhaité.



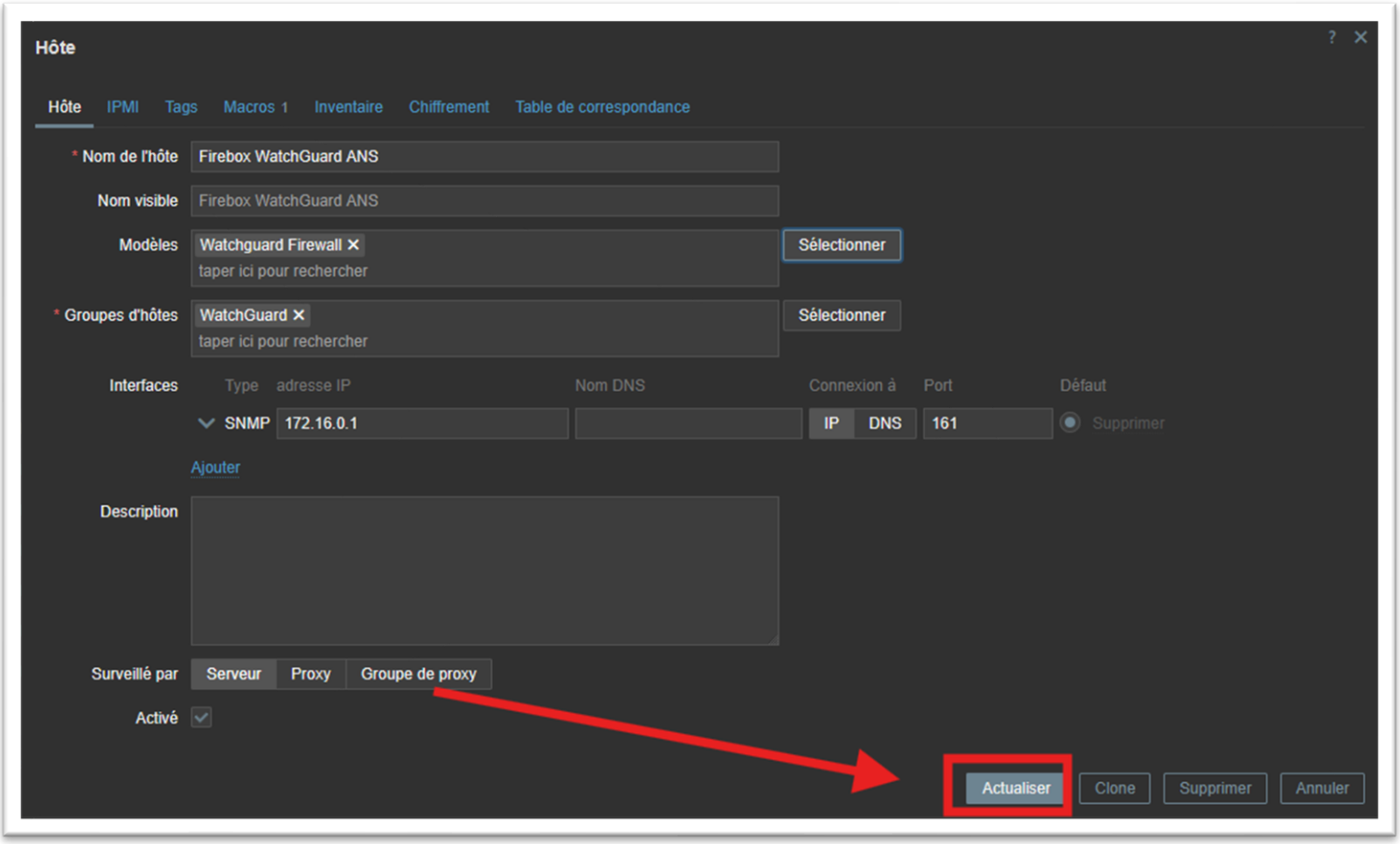
Cliquez sur **Sélectionner** pour sélectionner un modèle :



Entrez le groupe de modèles puis sélectionner le modèle proposé :



Puis cliquez sur sélectionner pour attribuer le Template et cliquez sur **Actualiser** pour attribuer les modifications sur l'hôte :



Pour accéder aux données remontées accédez à la section **Surveillance** puis **Dernières données**.

Faire remonter des informations pour émettre des alertes avec des déclencheurs par niveau de sévérité (Exemple avec remonté de certificats Windows Server 2022)

Passons aux choses sérieuses, voyons maintenant comment faire une remontée d'informations personnalisées. Dans le cas présent, on va essayer de faire remonter des certificats sur Zabbix depuis des machines distantes surveillées.

-

Dans un premier temps, nous allons devoir déployer le fichier de configuration des agents Zabbix avec les informations nécessaires à la mise en place de la remontée des certificats. Il est donc évident que vous devez avoir un hôte sur lequel est présent un agent et qui est déjà créer et configurer dans Zabbix (*pour cela se référer plus haut*).

-

PS : Avant de déployer le fichier de configuration de l'agent Zabbix, il est nécessaire de vérifier que les fichiers de configuration actuels ne possèdent pas d'informations supplémentaires à l'élément importé qui pourraient être écrasées.

Déploiement du fichier de configuration de l'agent Zabbix via GPO (AD)

Au sein de ce fichier de configuration on aura :

- Le DNS/IP du serveur Zabbix :

```
Server=supervision.ansinformatique.com
```

- L'activation des commandes à distance :

```
AllowKey=system.run[*]
EnableRemoteCommands=1
```

- L'ajout des paramètres d'accès à un fichier par système de clé :

```
UserParameter=cert.discovery,powershell -ExecutionPolicy Bypass -NoProfile -File "C:\Scripts\cert-lld.ps1"
UserParameter=cert.info[*],powershell -ExecutionPolicy Bypass -NoProfile -File "C:\Scripts\cert-info.ps1" -Thumbprint "$1"
```

Ce fichier de configuration se nomme **zabbix_agentd.conf**

Dépôt des scripts de récupération de données sur le serveur Zabbix

Comme on le remarque dans les lignes **UserParameter** insérées dans le fichier de configuration de l'agent Zabbix, deux scripts sont utilisés et exécutés. Voici ci-dessous le code de chacun de ces scripts :

-

cert-info.ps1

```
param(
   [string]$Thumbprint
)

$severityLevels = @{
   "Desastre" = 6
   "Haut" = 5
   "Moyen" = 4
   "Avertissement" = 3
   "Information" = 2
   "Non classee" = 1
}

$stores = @(
   "Cert:\LocalMachine\My",
   "Cert:\LocalMachine\CA",
   "Cert:\LocalMachine\Root",
   "Cert:\LocalMachine\AuthRoot",
   "Cert:\LocalMachine\TrustedPublisher"
)

$now = Get-Date

$certFound = $null
foreach ($store in $stores) {
   $cert = Get-ChildItem -Path $store -ErrorAction SilentlyContinue | Where-Object { $_.Thumbprint -eq $Thumbprint }
   if ($cert) {
      $certFound = $cert
      break
```

```
    }
}

if (-not $certFound) {
    Write-Output "{}"
    exit 0
}

$daysLeft = ($certFound.NotAfter - $now).Days

if ($daysLeft -le 0) {
    $severity = "Desastre"
} elseif ($daysLeft -le 7) {
    $severity = "Haut"
} elseif ($daysLeft -le 14) {
    $severity = "Moyen"
} elseif ($daysLeft -le 21) {
$severity = "Avertissement"
} else {
    $severity = "Non classee"
}

$result = [PSCustomObject]@{
    NomCertificat   = $certFound.FriendlyName
    DateExpiration  = $certFound.NotAfter.ToString("yyyy-MM-dd HH:mm:ss")
    JoursRestants   = $daysLeft
    Severite        = $severity
    NiveauSeverite  = $severityLevels[$severity]
    Empreinte       = $certFound.Thumbprint
}

$result | ConvertTo-Json -Depth 5
exit 0
```

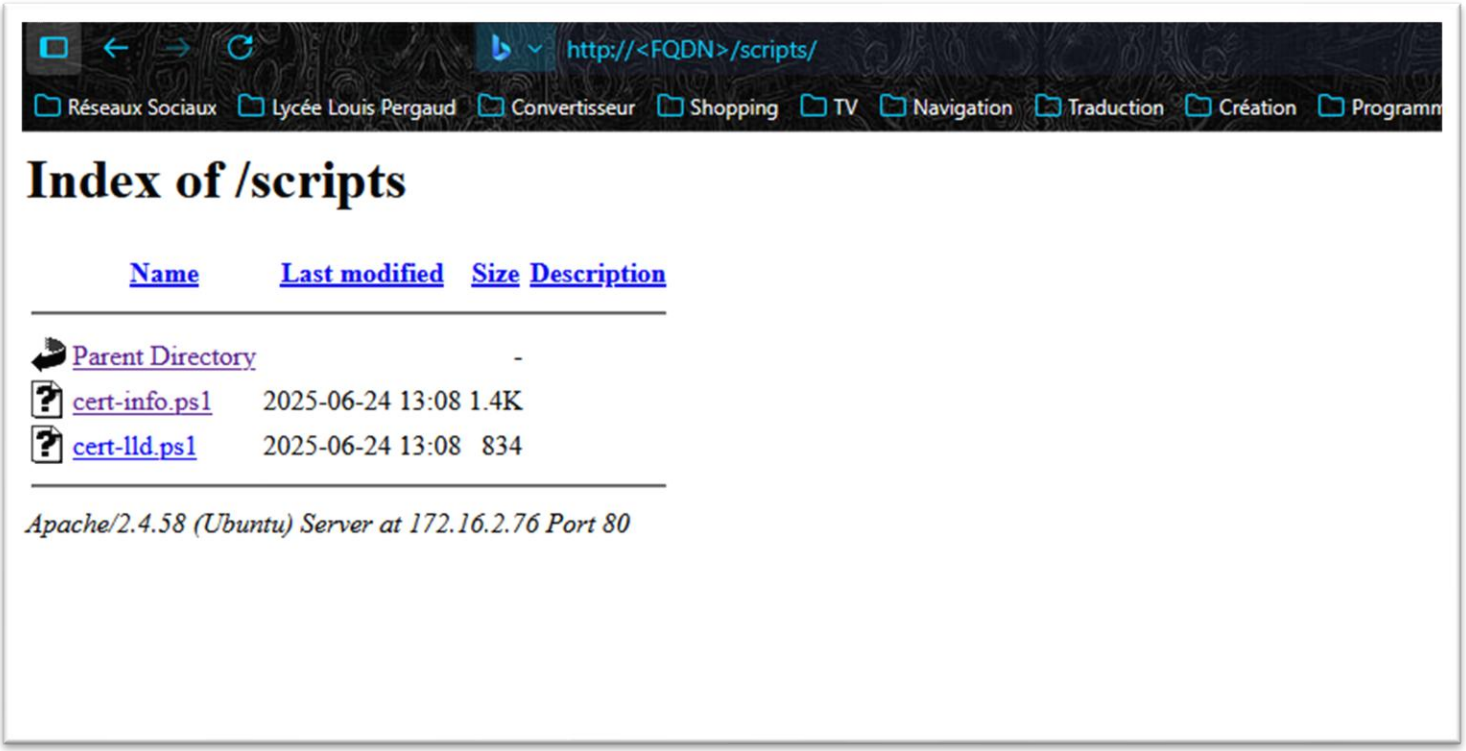
cert-lld.ps1

```
$MaxDaysExpiration = 30
$stores = @(
    "Cert:\LocalMachine\My",
    "Cert:\LocalMachine\CA",
    "Cert:\LocalMachine\Root",
    "Cert:\LocalMachine\AuthRoot",
    "Cert:\LocalMachine\TrustedPublisher"
)

$now = Get-Date
$threshold = $now.AddDays($MaxDaysExpiration)

$lld = @()

foreach ($store in $stores) {
```

```
    $certs = Get-ChildItem -Path $store -ErrorAction SilentlyContinue
    foreach ($cert in $certs) {
        if ($cert.NotAfter -le $threshold -and $cert.NotAfter -ge $now) {
            $lld += @{
                "{#CERTNAME}"     = $cert.FriendlyName
                "{#THUMBPRINT}"   = $cert.Thumbprint
                "{#CERTEXPIRATE}" = $cert.NotAfter.ToString("yyyy-MM-dd
HH:mm:ss")
            }
        }
    }
}

$output = @{ data = $lld }
$output | ConvertTo-Json -Depth 5
exit 0
```

-

Ces deux scripts seront placés sur le serveur Zabbix à l'emplacement ou s'ouvre le serveur Web *(/var/www/html)*.
On y créera un dossier qui se nommera **scripts** dans lequel on placera nos deux scripts. Ce qui donnera l'arborescence suivante :



Pour se faire se rendre sur votre serveur Linux, accédez au dossier avec :

cd /var/www/html

Créer le dossier :

mkdir scripts

Puis vos fichiers :

nano cert-info.ps1
<Entrez votre code>

Enregistrez et fermez le fichier avec Ctrl + S puis Ctrl + X
Attribuez les droits au fichier pour ne pas permettre l'exécution avec :
chmod -x <nom fichier>

Faire la même démarche pour l'autre fichier

Mise en place de Zabbix

De retour sur Zabbix, une fois les fichiers déposés, il faut configurer Zabbix pour qu'il accède aux fichiers, les exécutent et puisse récupérer les informations nécessaires et recherchées.

-

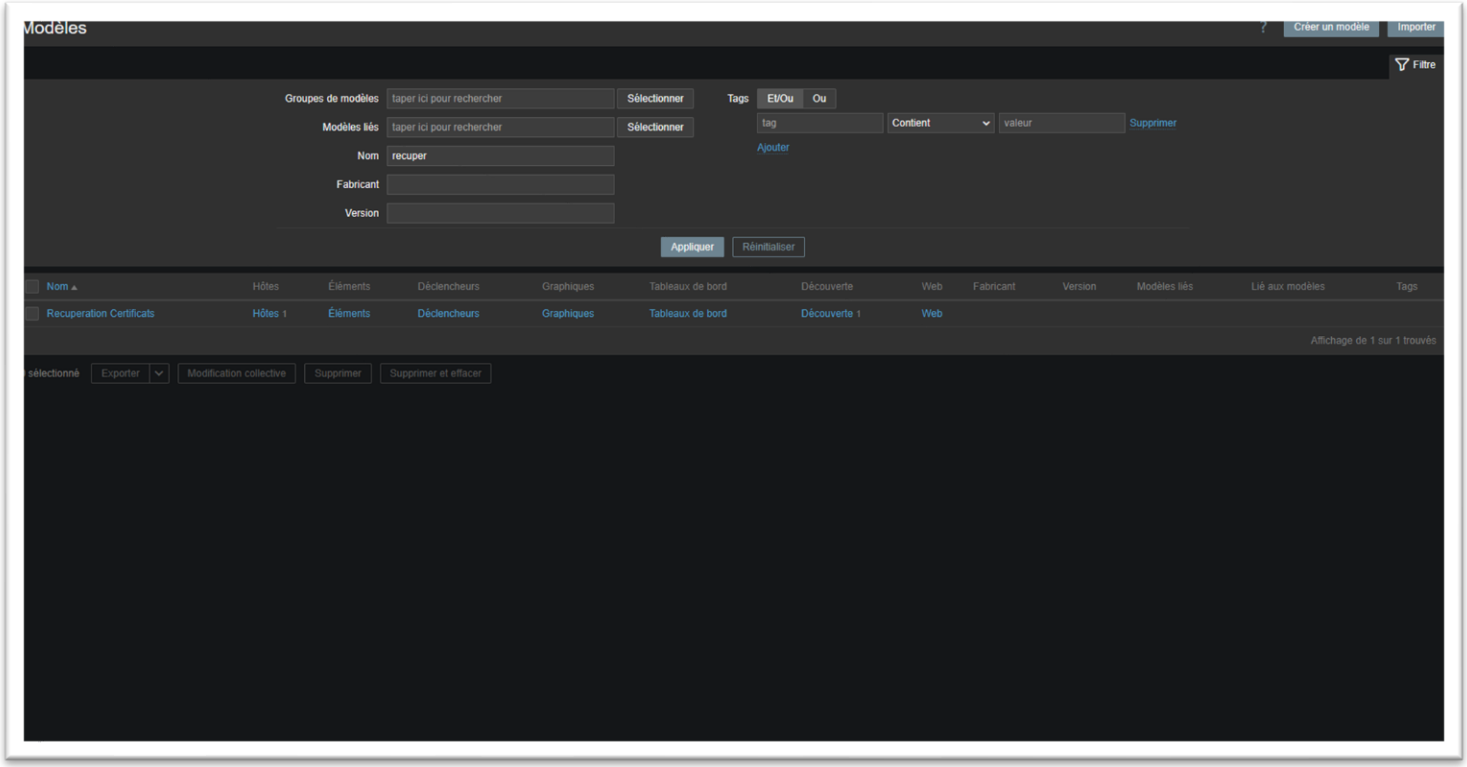
Tout d'abord, il va être nécessaire de créer un groupe de modèles **Recuperation des certificats** (*voir procédure plus haut*).

-

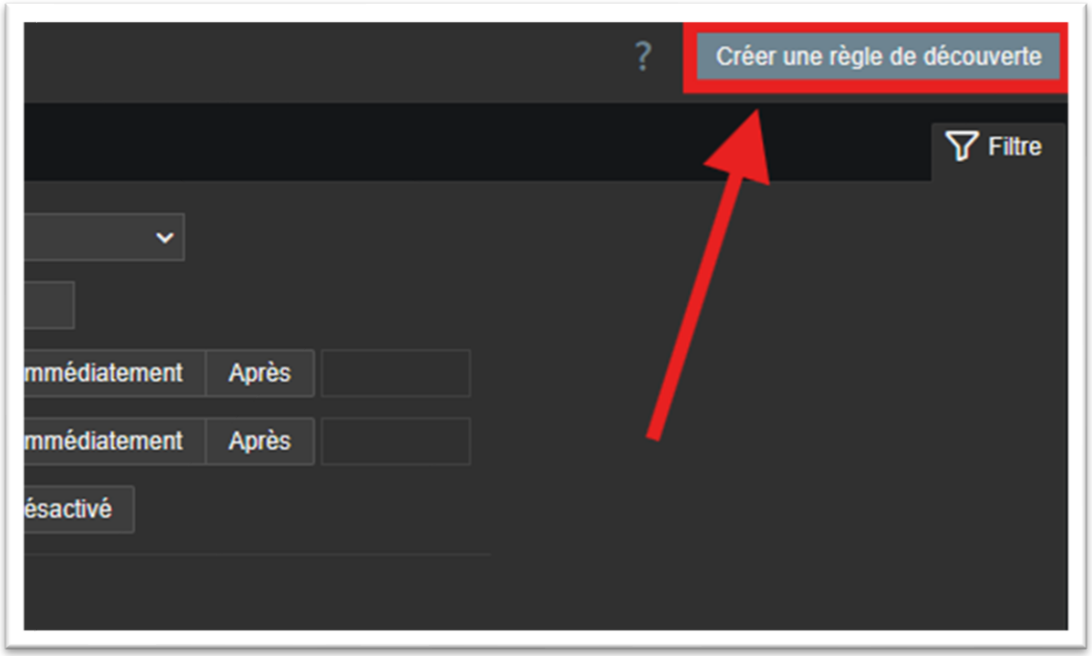
Ensuite, nous allons devoir créer un modèle **Recuperation des certificats** (*voir procédure plus haut*).

-

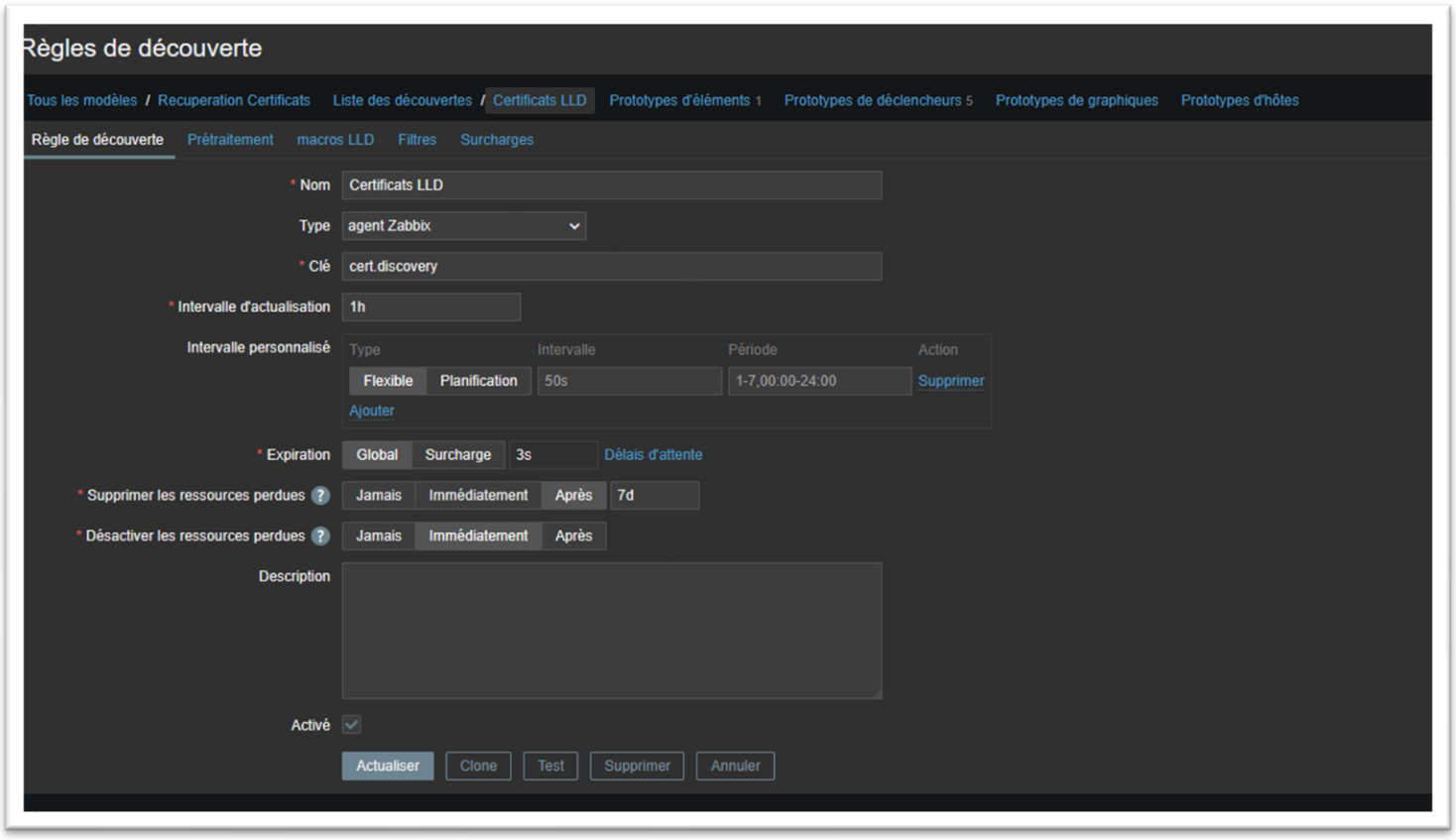
Une fois que l'on a ajouté tout cela, il va falloir configurer la récupération des données.



Ici cliquez sur **Découverte** sur la ligne du modèle puis **Créer une règle de découverte** :



Remplissez les champs comme ci-dessous :



On retrouve le type **agent Zabbix** pour dire que l'on va sonder via un agent Zabbix. Mais on retrouve également la clé **cert.discovery** pour aller exécuter le programme qui à été téléchargé depuis le serveur Zabbix. Cela va donc permettre de faire la « découverte » des certificats grâce à un script PowerShell.

-

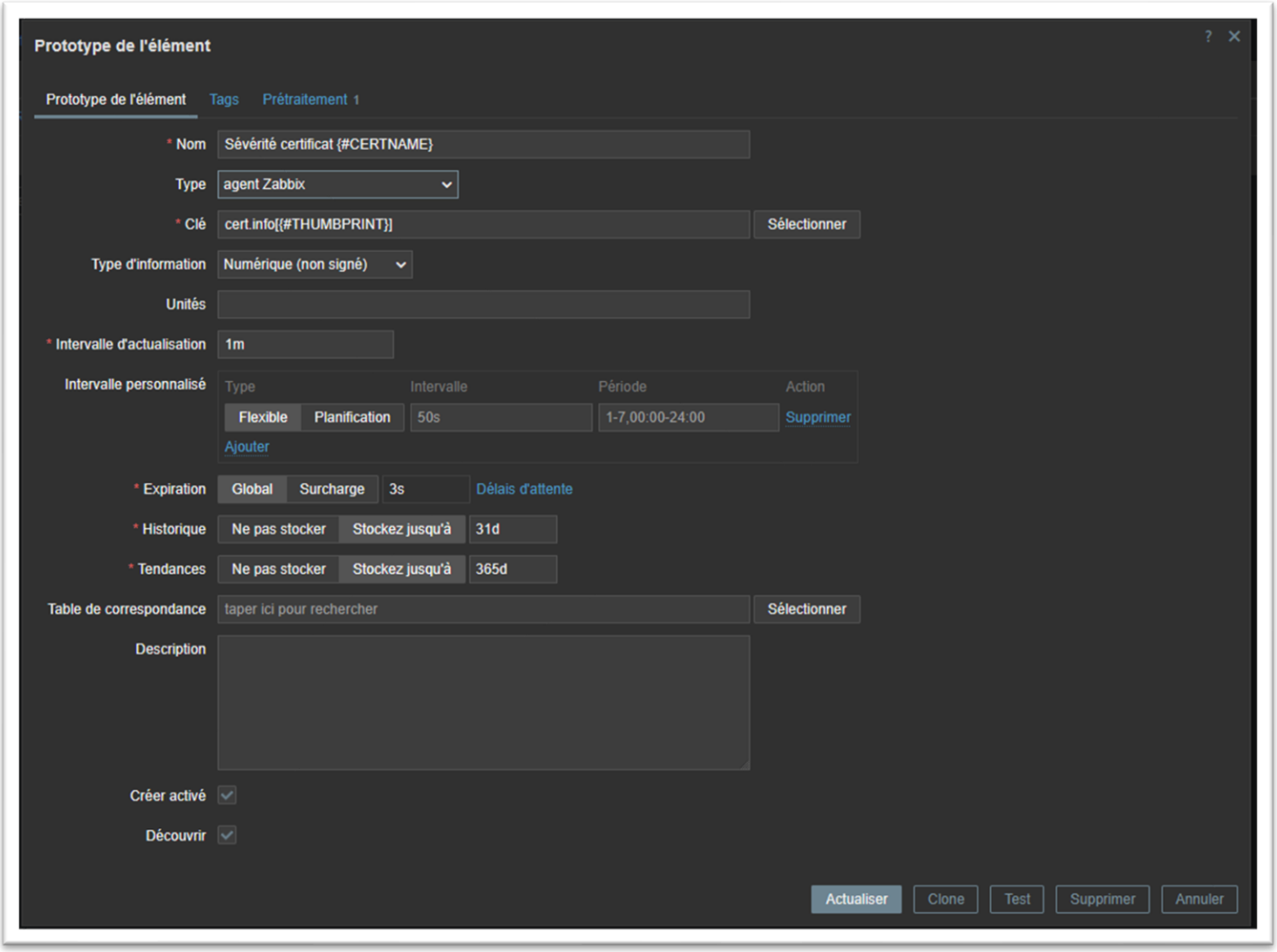
Maintenant on va récupérer les niveaux de sévérité des certificats, pour cela on va utiliser un **prototype d'élément** (*Un prototype d'élément Zabbix est un modèle de collecte de données utilisé dans les règles de découverte automatique (LLD). Il permet de générer dynamiquement des éléments de surveillance pour chaque ressource détectée, comme un système de fichiers ou une interface réseau.*).

-

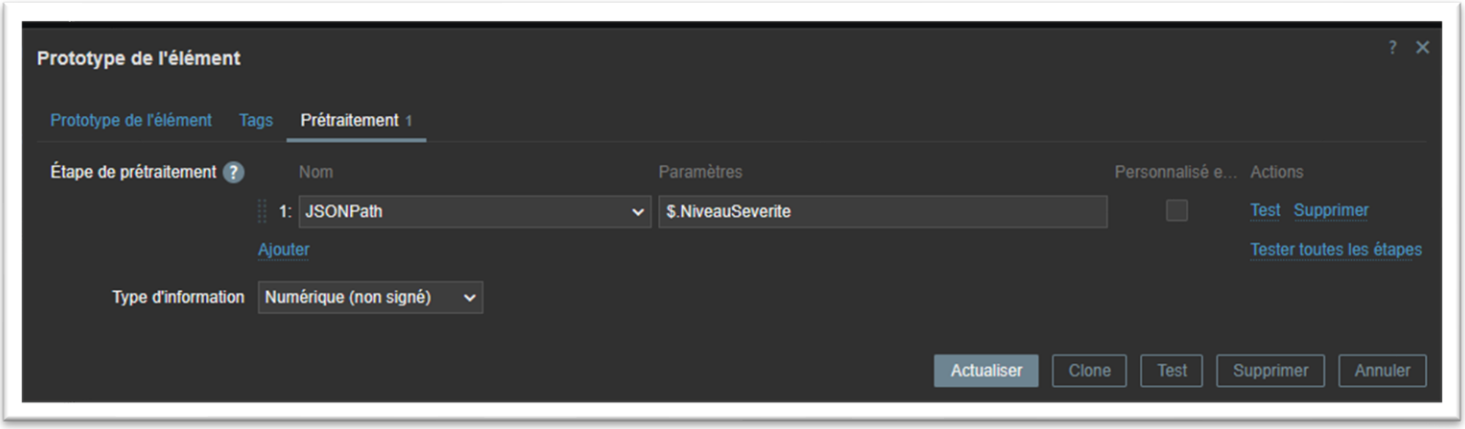
Se rendre ainsi dans la section **Prototype d'éléments** située en haut de la fenêtre.

-

Cliquez ensuite sur **Créer un prototype d'éléments** en haut à droite et remplir les champs de la manière suivante :



On ajoutera également un prétraitement (*Le prétraitement dans Zabbix est un mécanisme qui permet de transformer les données collectées avant leur enregistrement. Il sert à nettoyer, convertir ou enrichir les valeurs brutes pour les rendre exploitables.*) dans la section **Prétraitement** :



-

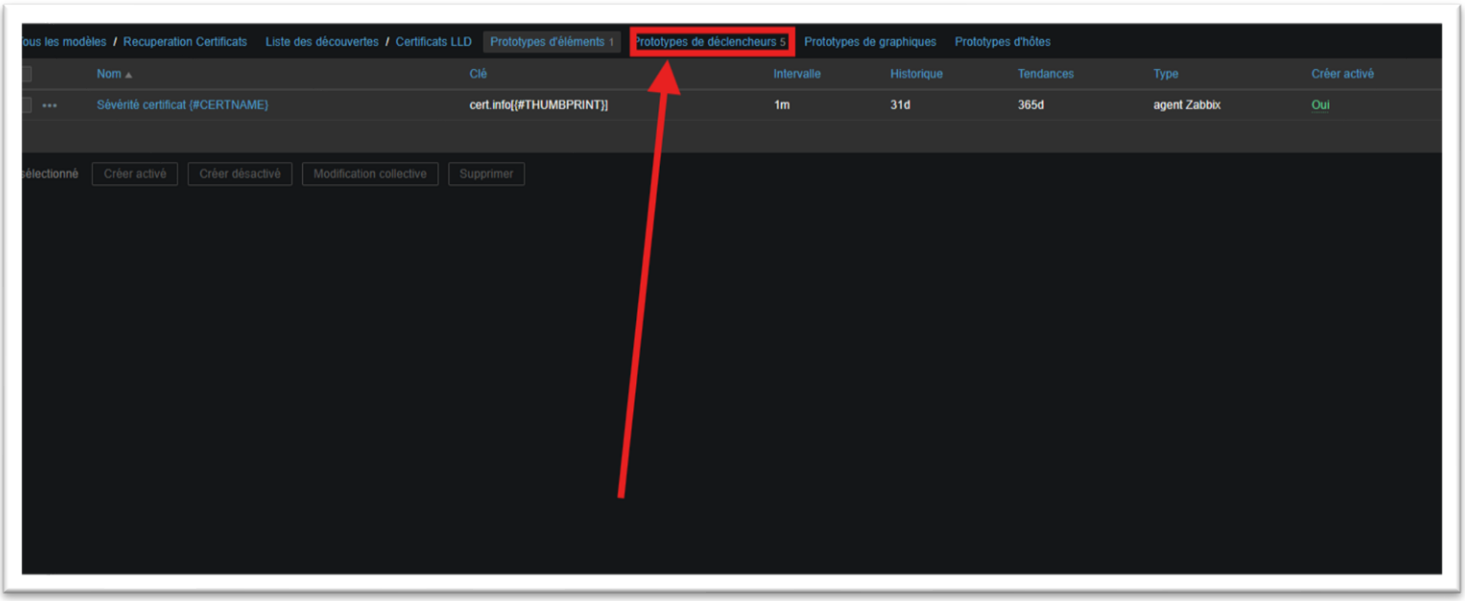
Cliquez ensuite sur **Ajouter/Actualiser** pour mettre à jour les modifications.

-

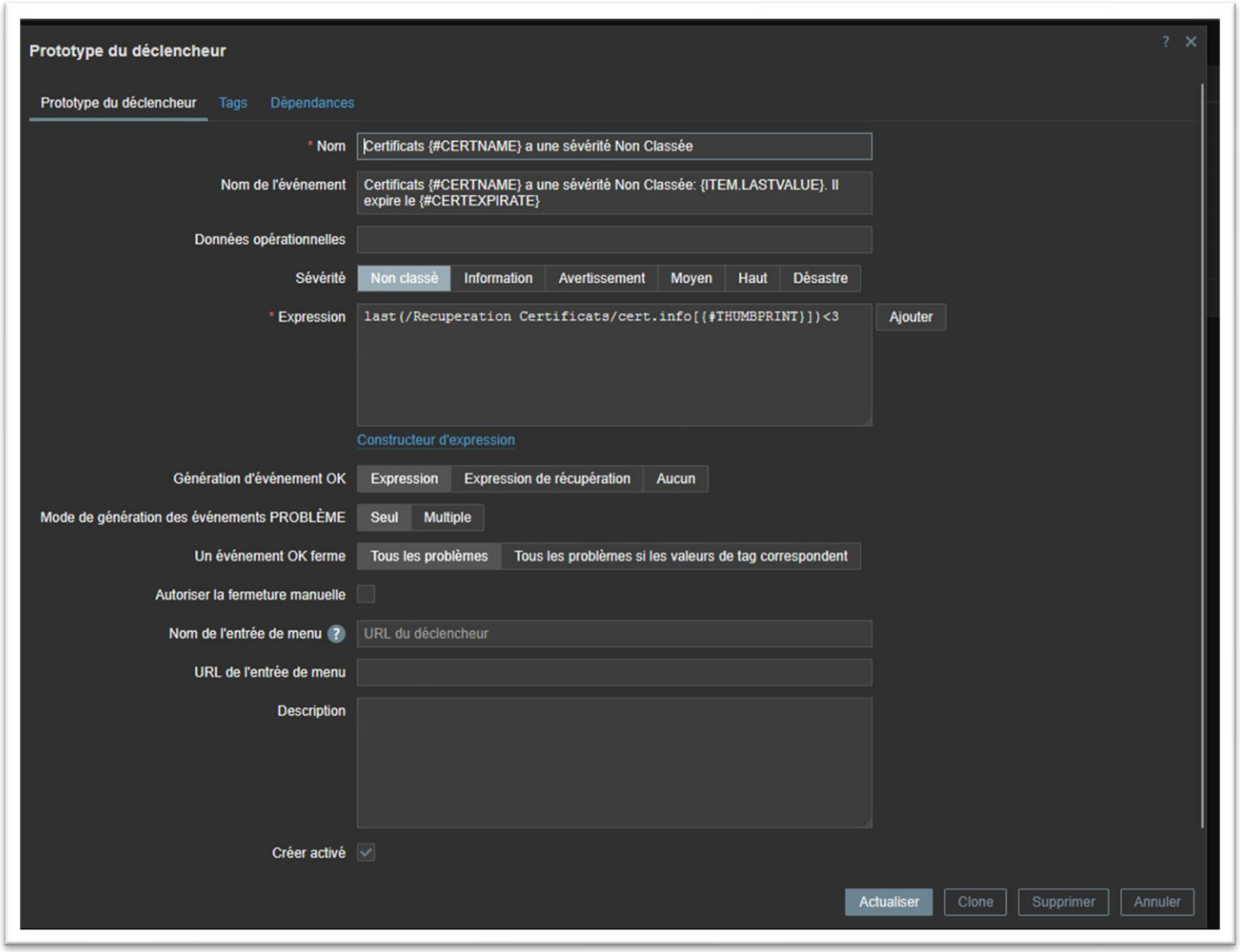
Place maintenant aux prototypes déclencheurs. Ces prototypes déclencheurs vont ainsi permettent de mettre en place les alertes sur le Dashboard de Zabbix.

-

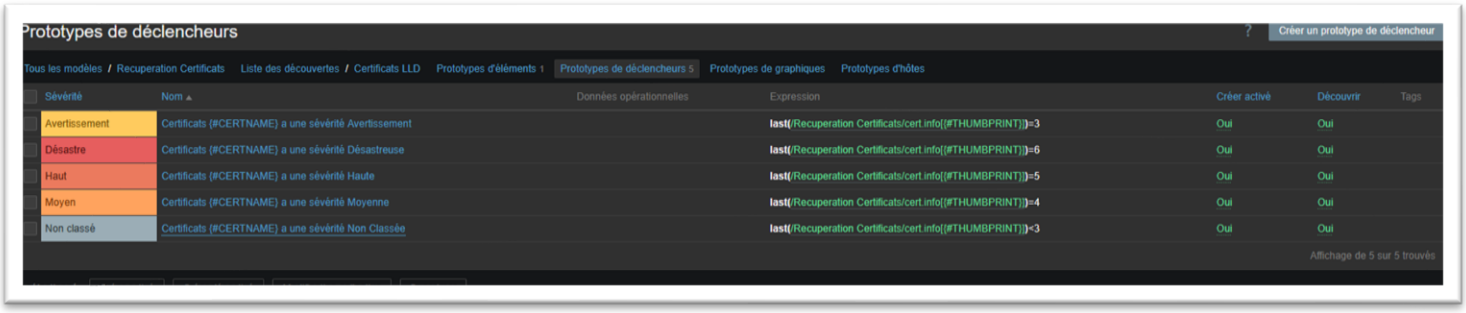
Rendez-vous dans la section **Prototype de déclencheurs**.



Puis cliquez sur **Créer un prototype de déclencheur**. Puis remplir de la façon suivante en adaptant pour chaque sévérité :



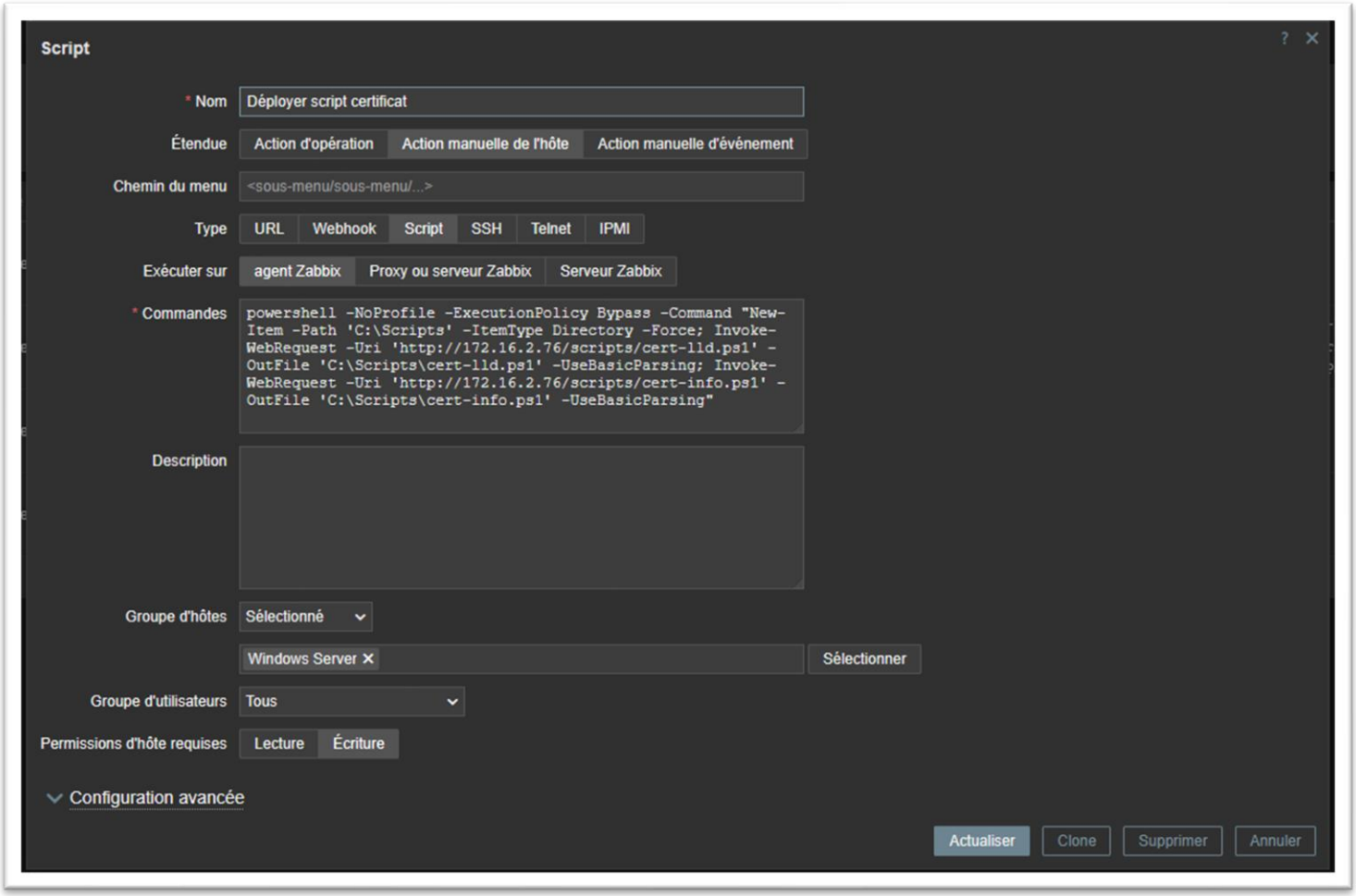
Jusqu'à obtenir ceci :



Enfin mettons en place le script de déploiement qui va télécharger les fichiers sur le serveur.

-

Pour cela se rendre dans **Alertes** puis **Scripts** puis **Créer un script**. Puis remplir les champs comme ci-dessous :


Script
* Nom
Déployer script certificat
Étendue
Action d'opération
Action manuelle de l'hôte
Action manuelle d'événement
Chemin du menu
<sous-menu/sous-menu/...>
Type
URL
Webhook
Script
SSH
Telnet
IPMI
Exécuter sur
agent Zabbix
Proxy ou serveur Zabbix
Serveur Zabbix
* Commandes
powershell -NoProfile -ExecutionPolicy Bypass -Command "New-Item -Path 'C:\Scripts' -ItemType Directory -Force; Invoke-WebRequest -Uri 'http://172.16.2.76/scripts/cert-lld.ps1' -OutFile 'C:\Scripts\cert-lld.ps1' -UseBasicParsing; Invoke-WebRequest -Uri 'http://172.16.2.76/scripts/cert-info.ps1' -OutFile 'C:\Scripts\cert-info.ps1' -UseBasicParsing"
Description
Groupe d'hôtes
Sélectionné
Windows Server
Sélectionner
Groupe d'utilisateurs
Tous
Permissions d'hôte requises
Lecture
Écriture
Configuration avancée
Actualiser
Clone
Supprimer
Annuler