

Zabbix - Documentation Complète

🕒 Date de création	@20 septembre 2024 10:58
🏷️ Étiquettes	Zabbix

Zabbix Server est une solution open-source de surveillance informatique qui permet de suivre en temps réel la performance des serveurs, réseaux et applications. Il collecte et analyse les données des hôtes surveillés, envoie des alertes en cas de problème, et offre des tableaux de bord interactifs pour visualiser l'état des systèmes. Adapté à des infrastructures de toutes tailles, Zabbix Server est un outil fiable pour garantir la disponibilité et la performance des ressources IT.

[Objectif](#)

[Prérequis](#)

[Installation de Zabbix Server](#)

[Installation du dépôt Zabbix](#)

[Installation de Zabbix Server, Frontend, Agent](#)

[Création de la base de donnée initiale](#)

[Téléchargement et secure-installation de MariaDB \(FACULTATIF\)](#)

[Configuration de la base de donnée Zabbix](#)

[Configuration du frontend PHP de Zabbix avec Nginx](#)

[Démarrage du serveur Zabbix et Agent](#)

[Ajouter l'entrée DNS de votre serveur Zabbix dans OPNSense](#)

[Zabbix Agent 2](#)

[Objectif](#)

[Prérequis](#)

[Installation de Zabbix Agent 2](#)

[Installation du dépôt Zabbix](#)

[Installation de Zabbix Agent 2](#)

[Configuration de Zabbix Agent 2](#)

[Démarrage de votre Zabbix Agent](#)

[Installation Zabbix Agent windows](#)

[Objectif](#)

[Prérequis](#)

[Téléchargement de Zabbix Agent](#)

[Installation et Configuration de Zabbix Agent](#)

[Install Agent SNMP](#)

[Prérequis](#)

[Installation de SNMP sur le Serveur Zabbix](#)

[Installation de SNMPD sur votre machine Debian 12](#)

[Démarrage de SNMPD](#)

[Configuration de SNMPD](#)

[Ajout de votre VM via SNMP](#)

[Mise en place scénario de suivi Web](#)

[Prérequis](#)

[Création d'un Scénario Web](#)

[Création d'une étape](#)

[Création du Scénario](#)

[Envoi automatique de mail](#)

[Prérequis](#)

[Configuration des types de médias pour l'envoi des alertes par e-mail](#)

[Assigner vos Types de Média à un utilisateur](#)
[Automatisation du type de média utilisé par sévérité des alertes](#)
[Faire un test d'envoi de mail par sévérité](#)

Objectif

- Créer une VM Zabbix Server + Accès interface Web

Prérequis

VM Debian

- Pour les prérequis, tout dépend du nombre d'items* que vous mettrez dans votre Zabbix

Taille	Nombre d'items	CPU/vCPU	Mémoire
Petit	<1000 items	2vCPU	8Gb
Moyen	<10 000 items	4vCPU	16Gb
Grand	<100 000 items	16vCPU	64Gb

Dans Zabbix, un **item est un élément de surveillance qui collecte des données à partir d'une source spécifique, comme un serveur, un appareil réseau ou un service. Un item définit ce que vous voulez surveiller (par exemple, l'utilisation du processeur, la quantité de mémoire libre, l'état d'un service réseau, etc.).*

Installation de Zabbix Server

Pour installer Zabbix Server, nous allons suivre la documentation officielle de Zabbix :

<https://www.zabbix.com/fr/download>

L'avantage de cette documentation est qu'elle s'adapte en fonction de vos besoins, versions, ...

Dans notre cas, nous allons installer la version 7.0 LTS de Zabbix, sur Debian 12, avec comme BDD MySQL et Nginx comme Serveur Web

VERSION DE ZABBIX	OS DISTRIBUTION	VERSION DU SYSTÈME D'EXPLOITATION	ZABBIX COMPONENT	BASE DE DONNÉES ²	SERVEUR WEB
7.0 LTS	Alma Linux	12 (Bookworm)	Server, Frontend, Agent	MySQL	Apache
6.4	Amazon Linux	11 (Bullseye)	Proxy	PostgreSQL	Nginx
6.0 LTS	CentOS	10 (Buster)	Agent		
5.0 LTS	Debian		Agent 2		
	Debian (arm64)				

Installation du dépôt Zabbix

Dans un premier temps, il va falloir installer le dépôt (repository) Zabbix, celui-ci permettra d'obtenir les paquets spécifiques à Zabbix et pouvoir mettre à jour Zabbix via le gestionnaire de paquets APT

Téléchargement du fichier du dépôt Zabbix

```
# wget https://repo.zabbix.com/zabbix/7.0/debian/pool/main/z/zabbix-release/zabbix-release_7.0-2+debian12_all.deb
```

Installation du paquet du dépôt Zabbix sur notre système + Ajout de l'URL du dépôt à la liste des sources de paquets ([voir source.list](#))

```
# dpkg -i zabbix-release_7.0-2+debian12_all.deb
```

Mise à jour de la BDD des paquets disponibles

```
# apt update
```

Installation de Zabbix Server, Frontend, Agent

Installation des dépendances nécessaires (Zabbix Server, Frontend, Agent, Nginx)

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

Création de la base de donnée initiale

Cette étape va permettre de configurer une base de données, et un utilisateur (MySQL) pour que Zabbix puisse stocker et gérer les données de surveillance.

“Téléchargement et secure-installation de MariaDB” est facultatif mais recommandé pour sécuriser davantage votre base de donnée

Téléchargement et secure-installation de MariaDB (FACULTATIF)

Téléchargement de MariaDB-Server

```
# apt install mariadb-server
```

Installation de MariaDB avec `mariadb-secure-installation`, qui permet de configurer des paramètres de sécurité comme la suppression des utilisateurs anonymes, la désactivation de la connexion root à distance, et la définition d'un mot de passe root.

```
# mariadb-secure-installation
```

```
# Change the root password? [Y/n] y
```

Changer le mot de passe root (Recommandé)

```
# Remove anonymous users? [Y/n] y
```

Supprimer les utilisateurs anonymes (Recommandé)

```
# Disallow root login remotely? [Y/n] y
```

Empêcher les connexion à distance pour l'utilisateur root (Recommandé)

```
# Remove test database and access to it? [Y/n] y
```

Supprimer la bdd de test par défaut (Recommandé)

```
# Reload privilege tables now? [Y/n] y
```

Recharge les privilèges maintenant (Oui)

Se connecter à votre base de donnée mysql avec l'utilisateur root

```
# mysql -uroot -p
```

Configuration de la base de donnée

```
# mysql> create database zabbix_pei character set utf8mb4 collate utf8mb4_bin;
```

Création d'une BDD "zabbix_pei" avec comme jeu de caractères utf8mb4

```
# mysql> create user zabbix@localhost identified by 'password';
```

Création de l'utilisateur "zabbix" + Définition du mot de passe ("password" à modifier)

```
# mysql> grant all privileges on zabbix.* to zabbix@localhost;
```

Attribution de toutes les privilèges à l'utilisateur "zabbix" sur "zabbix_pei"

```
# mysql> set global log_bin_trust_function_creators = 1;
```

Permet à des utilisateurs non administrateurs de créer et utiliser des fonctions stockées

```
# mysql> quit;
```

Quitter la session MySQL

Une fois votre base de donnée configurée, il va falloir importer le schéma de Zabbix initial dans notre base de donnée

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

Décompresse le contenu du fichier "server.sql.gz" | Envoi vers la base de donnée

Une fois le contenu envoyé vers la base de donnée, nous pouvons désactiver `log_bin_trust_function_creators` activé précédemment.

```
# mysql -uroot -p
```

Connection à la BDD

```
password
```

```
# mysql>
```

```
set global log_bin_trust_function_creators = 0;
```

Interdit à des utilisateurs non administrateurs de créer et utiliser des fonctions stockées

```
# mysql> quit;
```

Quitter la session MySQL

Configuration de la base de donnée Zabbix

Une fois la base de donnée correctement installée, il va maintenant falloir la configurer pour la rendre fonctionnelle avec notre environnement.

Toute la configuration de la database va se faire via le fichier de configuration `zabbix_server.conf` présent dans `/etc/zabbix/(zabbix_server.conf)`

Après avoir ouvert le fichier de configuration avec un éditeur de texte (vim, nano, ...), vous devrez modifier le mot de passe de votre base de donnée

Mot de passe de la base de donnée

Remplacez "password" par le mot de passe de votre BDD, puis décommentez la ligne en supprimant le #

```
# DBPassword="password"
```

Configuration du frontend PHP de Zabbix avec Nginx

Dernière étape : Modifier le fichier de configuration `nginx.conf` présent dans le répertoire `/etc/zabbix/nginx.conf`

Définition du port sur lequel Nginx écoutera les requêtes HTTP

Une fois dans le fichier de configuration, cherchez

```
# listen 8080;  
# server_name example.com;
```

Décommentez les deux lignes,

Pour server_name, remplacez example.com par le nom DNS de votre serveur Zabbix

Attention : Si à la fin de l'installation vous ne parvenez pas à accéder à l'interface Web de votre Serveur Zabbix, modifiez le port d'écoute (listen) sur 80

```
listen 80;
```

Démarrage du serveur Zabbix et Agent

L'installation est terminée, il ne vous reste plus qu'à démarrer votre serveur Zabbix et faire en sorte qu'il "start at boot" (Démarré en même temps que votre machine)

Démarrage de votre Zabbix Server

```
sudo systemctl restart zabbix-server zabbix-agent nginx php8.2-fpm
```

Activation du start at boot

```
sudo systemctl enable zabbix-server zabbix-agent nginx php8.2-fpm
```

Ajouter l'entrée DNS de votre serveur Zabbix dans OPNSense

Une fois l'installation terminée, il ne vous reste plus qu'à ajouter une entrée DNS pour votre Serveur Zabbix dans votre OPNSense.

Pour cela, nous allons utiliser Unbound DNS, un résolveur DNS intégré à OPNSense et accessible dans l'onglet

Services → UnboundDNS → Overrides

Une fois dans le bon onglet, il ne vous reste plus qu'à cliquer sur le + situé en haut à droite en renseignant les informations nécessaires.

Edit Host Override	
Enabled	<input checked="" type="checkbox"/>
Host	zabbix
Domain	pei.sio.lan
Type	A (IPv4 address)
IP address	10.31.30.99
Description	Zabbix

Vous pouvez vous désormais vous connecter à votre Zabbix en tapant le nom DNS de votre serveur, renseigné dans `server_name` dans votre fichier de configuration nginx.

Zabbix Agent 2

Zabbix Agent est un composant essentiel de la solution de surveillance Zabbix, chargé de collecter des données sur les performances des systèmes surveillés. Il envoie ces données au serveur Zabbix pour analyse, permettant de surveiller des éléments tels que la charge CPU, l'utilisation de la mémoire, ou l'état des services.

Objectif

- Installation de Zabbix Agent 2 sur une machine debian pour permettre sa connexion sur notre Serveur Zabbix

Prérequis

- Serveur Zabbix
- VM Debian

Installation de Zabbix Agent 2

Pour installer Zabbix Agent 2, nous allons suivre la documentation officielle de Zabbix : <https://www.zabbix.com/fr/download>

L'avantage de cette documentation est qu'elle s'adapte en fonction de vos besoins, versions, ...

Dans notre cas, nous allons installer la version 7.0 LTS de Zabbix, sur Debian 12, avec comme BDD MySQL et Nginx comme Serveur Web

VERSION DE ZABBIX	OS DISTRIBUTION	VERSION DU SYSTÈME D'EXPLOITATION	ZABBIX COMPONENT	BASE DE DONNÉES	SERVEUR WEB
7.0 LTS	Alma Linux	12 (Bookworm)	Server, Frontend, Agent	---	---
6.4	Amazon Linux	11 (Bullseye)	Proxy		
6.0 LTS	CentOS	10 (Buster)	Agent		
5.0 LTS	Debian		Agent 2		
	Debian (arm64)		Java Gateway		
	OpenSUSE Leap		Web Service		

Installation du dépôt Zabbix

Dans un premier temps, il va falloir installer le dépôt (repository) Zabbix, celui-ci permettra d'obtenir les paquets spécifiques à Zabbix et pouvoir mettre à jour Zabbix via le gestionnaire de paquets APT

Téléchargement du fichier du dépôt Zabbix

```
# wget https://repo.zabbix.com/zabbix/7.0/debian/pool/main/z/zabbix-release/zabbix-release_7.0-2+debian12_all.deb
```

Installation du paquet du dépôt Zabbix sur notre système + Ajout de l'URL du dépôt à la liste des sources de paquets ([voir source.list](#))

```
# dpkg -i zabbix-release_7.0-2+debian12_all.deb
```

Mise à jour de la BDD des paquets disponibles

```
# apt update
```

Installation de Zabbix Agent 2

Téléchargement des paquets de Zabbix Agent 2

```
# apt install zabbix-agent2 zabbix-agent2-plugin-*
```

Configuration de Zabbix Agent 2

Une fois votre Zabbix Agent 2 installé, il va falloir le configurer.

Le fichier de configuration qui va nous intéresser se nomme `zabbix_agent2.conf` et se trouve généralement dans `/etc/zabbix/zabbix_agent2.conf`

Une fois votre fichier ouvert avec un éditeur de texte (vim, nano, ...), au minimum 3 éléments seront à modifier : Server, ServerActive, et Hostname

Server="ip de votre Zabbix Server"

Permet de définir l'adresse ip du serveur Zabbix qui supervisera cet agent

ServerActive="ip de votre Zabbix Server"

Permet de définir le serveur pour l'envoi de données de l'agent vers le serveur

Hostname="Nom de la VM sur laquelle Agent 2 est installé"

Le nom d'hôte qui sera utilisé pour identifier cet agent dans l'interface Zabbix.

Démarrage de votre Zabbix Agent

L'installation est terminée, il ne vous reste plus qu'à redémarrer votre Zabbix Agent, pour appliquer les modifications faites sur le fichier de configuration, et faire en sorte qu'il "start at boot" (Démarre en même temps que votre machine)

Redémarrage de votre Zabbix Server

```
sudo systemctl restart zabbix-agent2
```

Activation du start at boot

```
sudo systemctl enable zabbix-agent2
```

Installation Zabbix Agent windows

Zabbix Agent est un composant essentiel de la solution de surveillance Zabbix, chargé de collecter des données sur les performances des systèmes surveillés. Il envoie ces données au serveur Zabbix pour analyse, permettant de surveiller des éléments tels que la charge CPU, l'utilisation de la mémoire, ou l'état des services.

Objectif

- Installation de Zabbix Agent 2 sur une machine debian pour permettre sa connexion sur notre Serveur Zabbix

Prérequis

- VM Windows 10 / 11 / Serveur
- Connexion internet

Téléchargement de Zabbix Agent

Pour télécharger et installer Zabbix Agent sur une machine Windows, rendez-vous sur le [site de téléchargement de Zabbix](#). Dans le menu en haut de la page, sélectionnez **"Zabbix Agents"**.

Une fois sur la page, choisissez votre système d'exploitation (Windows) ainsi que les autres options proposées, selon vos besoins. Sélectionnez la version qui correspond le mieux à votre configuration.

Dans notre cas, voici la configuration que nous allons utiliser :

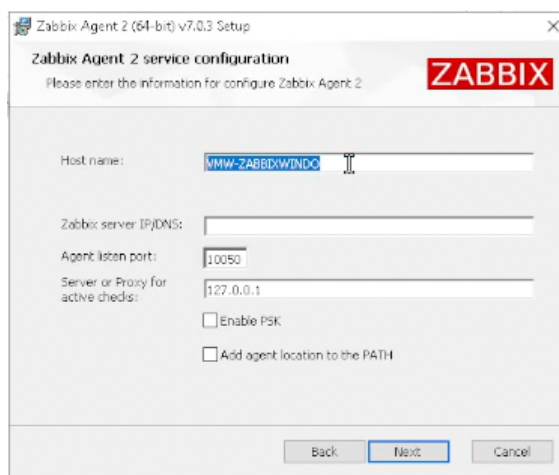
OS DISTRIBUTION	VERSION DU SYSTÈME D'EXPLOITATION	MATÉRIEL	VERSION DE ZABBIX	CHIFFREMENT	FORMAT
Windows	Any	amd64	7.0 LTS	OpenSSL	MSI
Linux		i386	6.4	No encryption	Archive
macOS			6.2		
AIX			6.0 LTS		

Au moment de télécharger l'exécutable, veillez à bien télécharger "Zabbix Agent 2".

Installation et Configuration de Zabbix Agent

Une fois votre fichier téléchargé, vous pouvez commencer l'installation en l'ouvrant simplement. Pour cela, double-cliquez sur le fichier exécutable.

L'installateur se lancera automatiquement. Vous n'avez qu'à cliquer sur **"Suivant"** jusqu'à arriver à la page de configuration.



Pour faire fonctionner correctement l'Agent Zabbix sur une machine Windows, trois informations essentielles doivent être renseignées.

Tout d'abord, le **"Host name"**, qui correspond au nom de votre machine Windows. Ce nom est utilisé pour identifier l'ordinateur au sein du réseau Zabbix. Pour le trouver, accédez aux paramètres de votre PC, puis allez dans l'onglet **"À propos"** situé dans la section **"Système"**. Le nom de l'appareil y sera indiqué.

Ensuite, l'option **"Zabbix server IP/DNS"** permet à l'Agent de se connecter au serveur Zabbix. Vous devez entrer ici l'adresse IP ou le nom DNS de votre serveur Zabbix. Cela permettra à l'Agent d'identifier et de communiquer avec le serveur central.

Enfin, l'option **"Server or Proxy for active checks"** correspond au paramètre **"ServerActive"** utilisé sur les systèmes Debian. Ici aussi, vous devez renseigner l'adresse IP ou le nom DNS de votre serveur Zabbix, car ce paramètre détermine où l'Agent envoie les résultats des vérifications actives (les données collectées sans demande explicite du serveur).

Une fois ces trois informations correctement renseignées, vous pouvez terminer l'installation. Votre Agent Zabbix est maintenant prêt à fonctionner et à communiquer avec le serveur pour surveiller votre machine.

Install Agent SNMP

Le SNMP (Simple Network Management Protocol) est un protocole de gestion réseau qui permet de surveiller et contrôler des équipements comme des routeurs ou serveurs. Il fonctionne via des managers et agents pour collecter des données et envoyer des commandes. Les versions récentes, comme SNMPv3, offrent plus de sécurité avec l'authentification et le chiffrement. Utilisé avec des outils comme **Zabbix**, il collecte des données sur les performances et l'état des systèmes pour une supervision en temps réel.

Prérequis

CLI Serveur Zabbix | SSH Recommandé

- Vlan 3130 : Ressources
- IP : 10.31.30.99
- DNS : zabbix.pei.sio.lan

VM Debian 12 | SSH Recommandé

- **Prérequis matériel**

Au minimum : 1 vCPU

Au minimum : 2Go RAM

Au minimum : 5Go de stockage

- **Connexion réseau**

Vlan 3130 : Ressources

IP Statique : 10.31.30.99

DNS : zabbixsnmp.pei.sio.lan

Installation de SNMP sur le Serveur Zabbix

Pour connecter un appareil en SNMP sur votre Serveur Zabbix, il va tout d'abord falloir installer SNMP sur celui-ci

Mise à jour des paquets + Installation de SNMP

```
# apt update
# apt install snmp
```

Installation de SNMPD sur votre machine Debian 12

Pour connecter une machine via SNMP sur votre Zabbix, vous devrez tout d'abord installer SNMPD.

SNMPd est le "daemon" **SNMP** qui fonctionne sur un système Linux ou Unix. C'est un service qui permet à un appareil d'être surveillé via le protocole SNMP.

Mise à jour des paquets + Installation de SNMPD

```
# apt update
# apt install snmpd
```

Démarrage de SNMPD

L'installation est terminée, il ne reste plus qu'à démarrer votre serveur Zabbix et à s'assurer qu'il se lance automatiquement au démarrage de la machine.

Démarrage de snmpd

```
sudo systemctl start snmpd
```

Activation du start at boot

```
sudo systemctl enable snmpd
```

Configuration de SNMPD

Une fois SNMPD démarré, vous pouvez passer à sa configuration.

Avant cela, il est important de récupérer le nom de votre machine, ce que vous pouvez faire en utilisant la commande `hostname -f`.

Configuration de SNMPD via l'éditeur de texte "vim"

```
# vim /etc/snmp/snmpd.conf
```

18. sysLocation Sitting on the Dock of the Bay

19. Me <me@example.org>

Dans la ligne 18, remplacez "Sitting on the Dock of the Bay" par votre localisation

Dans la ligne 19, remplacez Me <me@example.org> par une adresse mail

23. sysServices 72

Commentez la ligne

39. master agentx

Commentez la ligne

49. agentaddress 127.0.0.1,[::1]

Commentez la ligne, puis ajoutez la ligne ci-dessous

agentaddress upd:161,upd6[::1]:161

63. view systemonly included .1.3.6.1.2.1.1

64. view systemonly included .1.3.6.1.2.1.25.1

Commentez les ligne

71. rocommunity public default -V systemonly

72. rocommunity6 public default -V systemonly

Commentez les lignes, puis ajoutez la ligne ci-dessous

73. rocommunity hg.ttc.local

86. rouser authPrivUser authpriv -V systemonly

89. includeDir /etc/snmp/snmpd.conf.d

Commentez les lignes

Une fois toutes les modifications effectués, vous pouvez sauvegarder et quitter le fichier de configuration.

Redémarrage de "snmpd" afin d'appliquer les modifications effectuées

```
# systemctl restart snmpd
```

Ajout de votre VM via SNMP

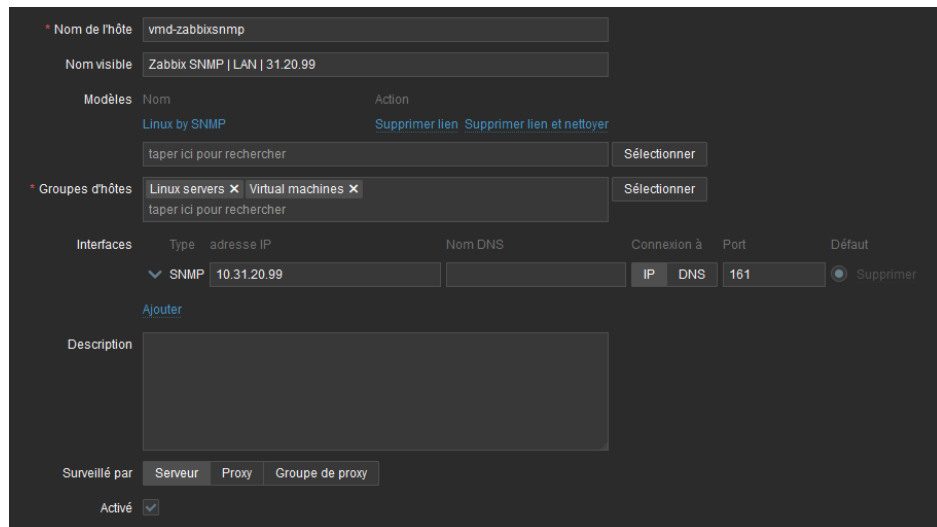
Enfin, pour ajouter votre machine virtuelle, comme pour un Agent, allez dans

Collecte de données → Hôtes.

Lorsque vous créez un nouvel hôte, sélectionnez bien "Linux by SNMP" dans la section **Modèles**.

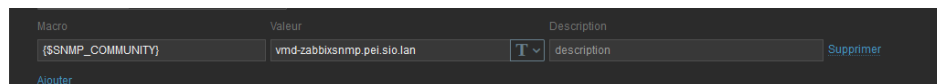
Concernant l'interface, en choisissant **SNMP**, vous pourrez, tout comme pour l'Agent, entrer l'IP de votre VM. Cependant, une étape supplémentaire est nécessaire.

Pour finaliser l'ajout de votre hôte, copiez `{${SNMP_COMMUNITY}}`, puis rendez-vous dans l'onglet **Macro**.



The screenshot shows the Zabbix host configuration page for an SNMP host. The 'Nom de l'hôte' is 'vmd-zabbixsnmp' and the 'Nom visible' is 'Zabbix SNMP | LAN | 31.20.99'. Under 'Modèles', 'Linux by SNMP' is selected. The 'Groupes d'hôtes' section shows 'Linux servers' and 'Virtual machines' selected. In the 'Interfaces' table, the 'SNMP' interface is configured with IP '10.31.20.99', connection type 'IP', and port '161'. The 'Description' field is empty. At the bottom, 'Surveillé par' is set to 'Serveur' and 'Activé' is checked.

Ajoutez une nouvelle macro avec comme Macro : `{${SNMP_COMMUNITY}}`, et comme valeur, le nom de votre machine (`hostname -f`)



The screenshot shows the Zabbix macro configuration page. A new macro is being added with the name `{${SNMP_COMMUNITY}}` and the value `vmd-zabbixsnmp.pei.sio.lan`. The 'Description' field contains the text 'description'. There is a 'Supprimer' button and an 'Ajouter' button at the bottom.

Votre machine sera correctement ajoutée à votre Zabbix.

Contrairement à Zabbix Agent, où la disponibilité est confirmée par l'icône **ZBX**, ici, le message de confirmation ou non de la disponibilité sera **SNMP**

Mise en place scénario de suivi Web

En complément, Zabbix permet également le suivi des sites web en surveillant leur disponibilité, performance et temps de réponse. Grâce à des scénarios de monitoring, il peut détecter les pannes et alerter en cas de problème, garantissant ainsi la qualité des services en ligne.

Prérequis

- Serveur Zabbix

- Vlan 3130 : Ressources
- IP : 10.31.30.99
- DNS : zabbix.pei.sio.lan

Hôte Zabbix

- Zabbix Server
- Vlan 3130 : Ressources
- IP : 10.31.30.99

Site Web à monitorer

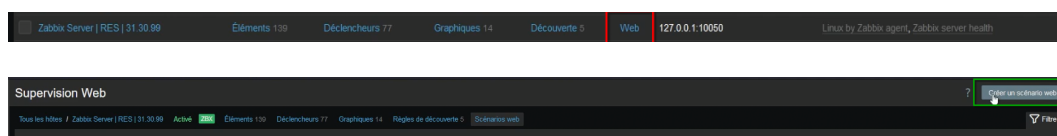
- <https://www.greenitsolutions.fr/>

Création d'un Scénario Web

Pour créer un scénario web, vous devez d'abord choisir quel hôte sera responsable de la surveillance. Lorsque vous ajoutez un élément de monitoring dans la section "Web" d'un hôte sur Zabbix, cet hôte devient responsable de surveiller le site web que vous souhaitez suivre.

Dans ce cas, nous allons sélectionner notre serveur Zabbix.

Une fois l'hôte choisi, allez dans la section "Web", puis cliquez sur "Créer un scénario Web" en haut à droite (Zabbix version 7.0 LTS).



Création d'une étape

Une fois l'interface de création ouvert, vous aller dans un premier temps vous rendre dans "**Étapes**" pour créer une étape*.

**Les étapes servent à simuler des interactions utilisateurs avec le site. Chaque étape correspond à une action précise que Zabbix va exécuter pour vérifier le comportement du site à différents points d'interaction.*

Dans l'étape que vous allez créer, vous allez renseigner :

Nom du site : GreenITSolutions

Nom du site que Zabbix va vérifier (Le nom ne sera pas utilisé par Zabbix, il sert seulement à vous repérer)

URL à visiter : <https://www.greenitsolutions.fr/>

L'adresse exacte que Zabbix doit vérifier (par exemple, la page d'accueil ou une page spécifique du site).

Code d'état requis : 200

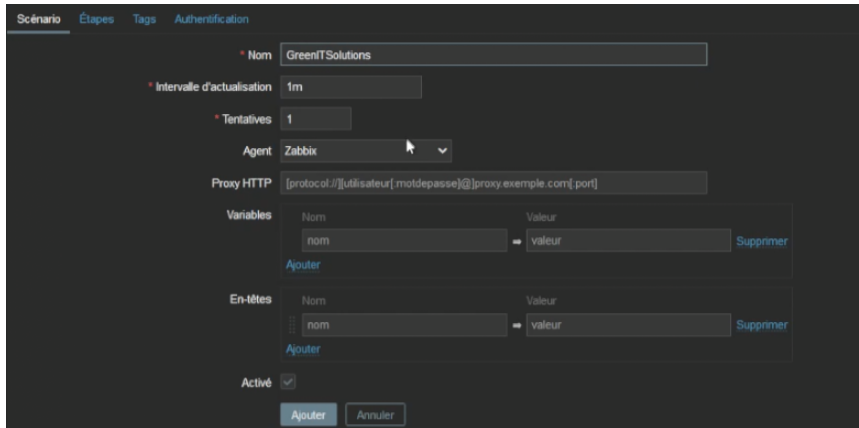
Le "code d'état" dans le cadre d'une requête web fait référence aux codes d'état HTTP, qui sont des réponses standard fournies par un serveur web pour indiquer le résultat d'une requête.

200 – Succès : La requête a été reçue, comprise et traitée avec succès.

Création du Scénario

Une fois votre étape créée, vous pouvez revenir dans l'onglet principal "Scénario" et y entrer le nom de votre scénario web.

Après avoir renseigné l'étape et le nom de votre scénario, il vous suffit de cliquer sur "Ajouter" pour finaliser l'ajout.

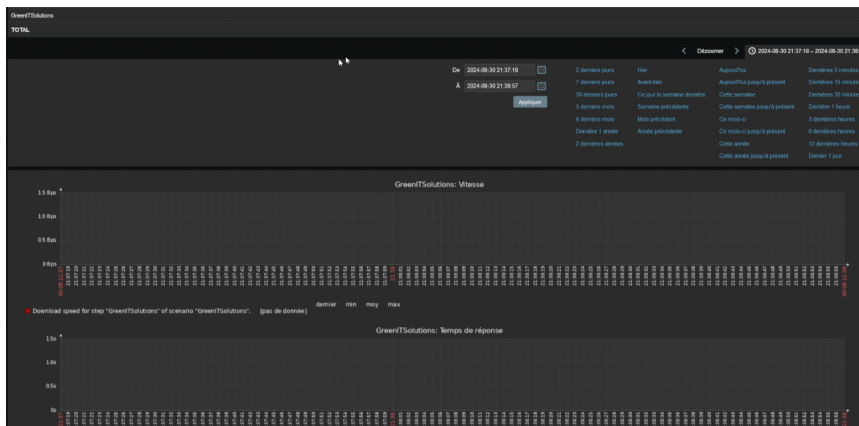


Votre scénario a été créé avec succès. Pour vérifier l'état du site ajouté, allez dans **Surveillance → Hôtes**.

Dans cet onglet, vous verrez tous les hôtes que vous avez ajoutés, et vous aurez la possibilité de cliquer sur l'onglet **"Web"** de l'hôte choisi pour la surveillance.



Vous verrez alors votre site, il ne vous reste plus qu'à cliquer sur celui-ci pour y voir l'interface de surveillance.



Envoi automatique de mail

Zabbix intègre une fonctionnalité d'envoi de mails pour alerter les administrateurs en cas de problèmes détectés lors de la surveillance. Cette fonctionnalité est particulièrement utile pour être informé immédiatement lorsqu'un site web, un service ou une infrastructure rencontre une panne ou une dégradation de performance.

Prérequis

Serveur Zabbix

- Vlan 3130 : Ressources
- IP : 10.31.30.99
- DNS : zabbix.pei.sio.lan

Un serveur SMTP pour l'envoi d'e-mails (par exemple, Gmail, un serveur interne, etc.)

La messagerie utilisée doit obligatoirement avoir la fonctionnalité A2F ainsi que la possibilité de créer des mot de passes d'Applications

Adresses email prêtes à recevoir les notifications

pei.btssio@gmx.com

pei.btssio@gmail.com

Utilisateur Zabbix

sioadmin

Configuration des types de médias pour l'envoi des alertes par e-mail

Pour que Zabbix puisse envoyer des notifications par e-mail, vous devez configurer un "type de média", qui représente le canal de communication utilisé pour l'envoi des alertes.

Dans le menu principal de Zabbix, rendez-vous dans la section Alertes, puis cliquez sur Types de média. Vous y verrez une liste des types de médias déjà configurés.

Si vous utilisez Gmail, vous pouvez simplement ouvrir le type de média existant "Gmail", le cloner, puis modifier les informations selon vos besoins.

Nom du type de média : Gmail_Alerting

Le nom du type de média utilisé pour envoyer des notifications via email dans Zabbix.

Type : Courriel

Sélectionnez le type de média pour les alertes. Dans ce cas, il s'agit de l'option "Courriel".

Fournisseur de messagerie : Gmail

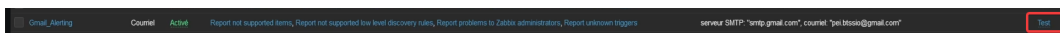
Courriel : pei.btssio@gmail.com

L'adresse email utilisée pour envoyer les alertes aux utilisateurs.

Mot de passe : *****

Mot de passe application généré via Gmail

Une fois votre média créé, il apparaîtra dans la liste comme **"Activé"**. Après activation, vous pouvez cliquer sur **"Test"** à droite de la ligne correspondante pour envoyer un e-mail de test, afin de vérifier que la connexion entre Zabbix et votre messagerie fonctionne correctement.



Si vous souhaitez ajouter une messagerie différente de Gmail, vous devrez cloner le type de média existant "Email" pour l'adapter à votre nouveau service de messagerie.

Nom du type de média : **GMX_Alerting**

Le nom du type de média utilisé pour envoyer des notifications via email dans Zabbix.

Type : **Courriel**

Sélectionnez le type de média pour les alertes. Dans ce cas, il s'agit de l'option "Courriel".

Serveur SMTP : mail.gmx.com

Le serveur SMTP utilisé pour envoyer les emails. Si vous utilisez Gmail, l'adresse sera `mail.gmx.com`. Pour d'autres serveurs SMTP, remplacez par l'adresse correspondante.

Port SMTP : **465**

Le port du serveur SMTP. Le port 465 est utilisé pour une connexion sécurisée via StartTLS. Si vous utilisez SSL, le port peut être 587.

Courriel : pei.btssio@gmail.com

L'adresse email utilisée pour envoyer les alertes aux utilisateurs.

Sécurité de la connexion : SSL/TLS

Authentification : Nom d'utilisateur et mot de passe

Nom d'utilisateur : pei.btssio@gmx.com

Mot de passe : *****

Mot de passe application généré par GMX

Nouveau type de média

Type de média Modèles de messages Options

* Nom GMX_Alerting

Type Courriel

Fournisseur de messagerie Generic SMTP

* serveur SMTP mail.gmx.com

Port du serveur SMTP 485

* Courriel pei.btssio@gmx.com

SMTP helo

Sécurité de la connexion Aucun STARTTLS SSL/TLS

Vérifier le pair SSL

Vérifier l'hôte SSL

Authentification Aucun Nom d'utilisateur et mot de passe

Nom d'utilisateur pei.btssio@gmx.com

Mot de passe *****

Format du message HTML Texte brut

Description

Activé

Ajouter Annuler

Tout comme pour Gmail, une fois que votre type de média est créé et activé, vous pourrez le tester pour vérifier que la connexion entre Zabbix et votre messagerie fonctionne correctement.

Assigner vos Types de Média à un utilisateur

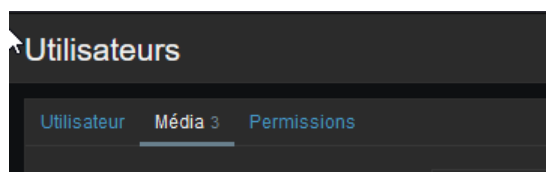
Une fois que vos types de média ont été créés, il est nécessaire de les assigner à un utilisateur. Assigner un type de média à un utilisateur dans Zabbix permet de définir comment et par quel canal cet utilisateur recevra des notifications lors d'un événement de surveillance (comme une alerte). Cela garantit que les alertes seront envoyées via des canaux spécifiques (email, SMS, Slack, etc.) selon la configuration du type de média et les préférences de l'utilisateur.

Pour assigner un type de média à un utilisateur, allez dans :

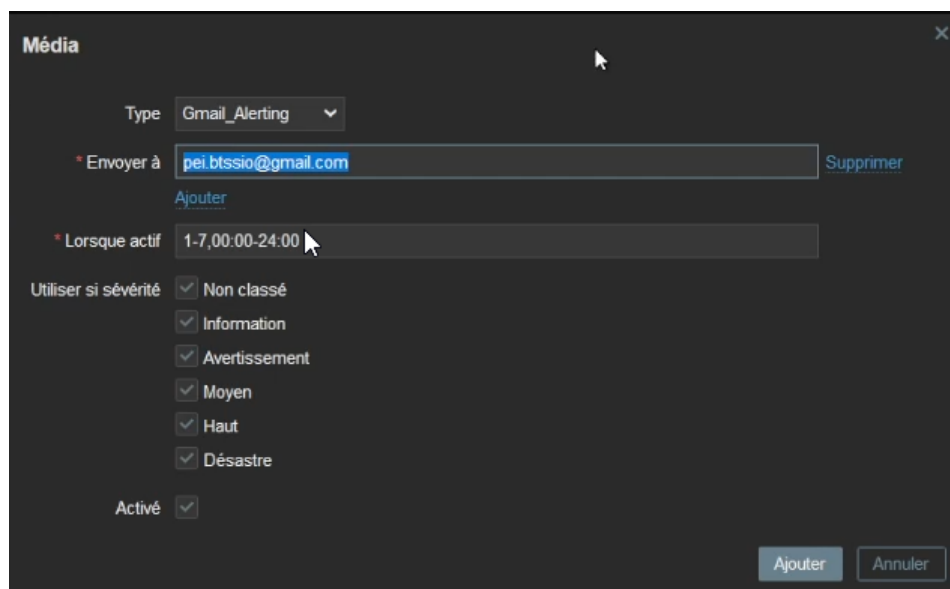
Utilisateurs → Utilisateurs

C'est ici que vous retrouverez les utilisateurs créés précédemment.

Pour lui assigner un type de média, cliquez sur l'utilisateur, puis accédez à l'onglet "Média" pour ajouter un nouveau média.



Dans l'interface d'ajout du média, il vous suffit de sélectionner le type de média que vous avez créé précédemment, puis de renseigner l'adresse email à laquelle les notifications seront envoyées.



Automatisation du type de média utilisé par sévérité des alertes

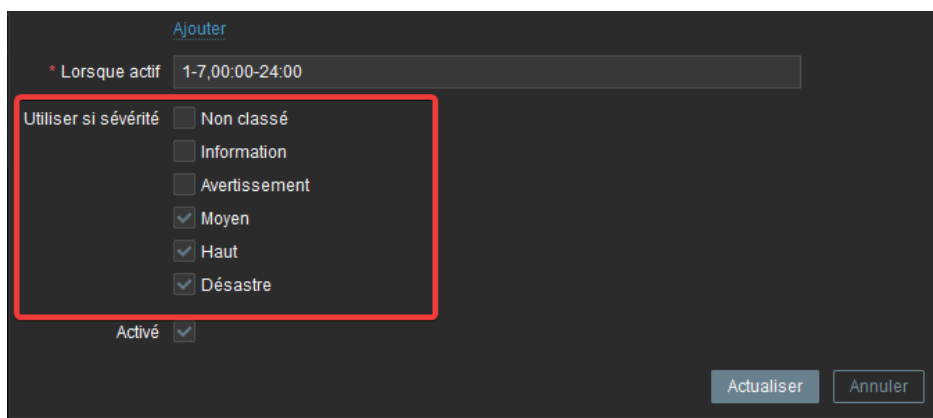
Sur Zabbix, vous pouvez automatiser le type de média utilisé en fonction de la sévérité des alertes.

Zabbix propose 6 niveaux de sévérité :

- **Non classé** : Événement sans niveau de gravité attribué.
- **Information** : Événement non critique, informatif seulement.
- **Avertissement** : Risque potentiel, nécessite une attention mais pas encore critique.
- **Moyen** : Problème modéré, pourrait nécessiter une intervention.
- **Haut** : Problème sérieux, doit être traité rapidement.
- **Désastre** : Incident critique, urgence absolue, impact majeur sur le système.

Pour automatiser le type de média utilisé, vous pouvez spécifier, lors de l'assignation du type de média à un utilisateur, quelles sévérités d'alerte seront envoyées à une adresse spécifique.

Dans cet exemple, nous avons configuré l'adresse GMX pour recevoir uniquement les alertes de niveau **Non classé**, **Information**, et **Avertissement**, tandis que les alertes de sévérité supérieure sont envoyées à l'adresse Gmail.



Faire un test d'envoi de mail par sévérité

Une fois vos types de média créés, il ne vous reste plus qu'à vérifier si l'envoi automatique de mails fonctionne correctement.

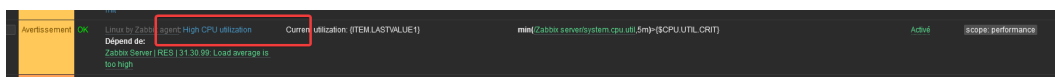
Pour ce faire, nous allons déclencher une alerte manuellement afin de voir si le mail est bien envoyé. Si vous avez configuré plusieurs boîtes mail en fonction de la sévérité, cela vous permettra également de vérifier si l'alerte est envoyée à la bonne messagerie en fonction du niveau de sévérité.

Pour déclencher une alerte manuellement, rendez-vous dans :

Collecte de données → Hôtes

Une fois la liste de vos hôtes affichée, cliquez sur "**Déclencheurs**" à côté d'un hôte où l'agent est disponible (indiqué par un ZBX vert).

Dans les déclencheurs de votre agent, vous pourrez créer un déclencheur personnalisé pour provoquer une alerte. Dans notre exemple, nous allons simuler une utilisation anormale du CPU en sélectionnant l'alerte "**High CPU utilization**".



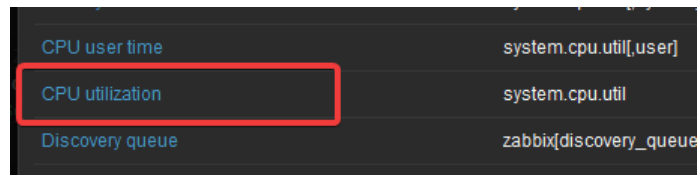
Une fois dessus, nous allons la Cloner pour en créer une nouvelle, et la personnaliser comme nous le voulons.

Nom : Nom de votre déclencheur, pensez bien à la renommer pour pouvoir l'identifier et la supprimer plus facilement après

Sévérité : Sévérité de votre alerte, peut être utile de modifier dans le cas où vous souhaitez tester vos envoi de mail par sévérité.

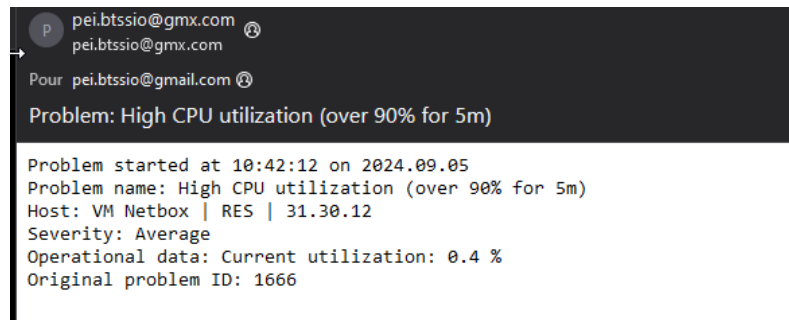
Expression : Pour simuler une utilisation anormale du CPU, supprimez la ligne déjà existante, puis cliquez sur "Ajouter".

Dans un premier temps, choisissez un "Element" parmi la liste. Ici, nous allons prendre "CPU utilization"



Vous pouvez ensuite modifier le résultat en le changeant le = par un < et y insérer la valeur **100**.

Une fois votre déclencheur créé, rendez-vous sur votre tableau de bord pour vérifier que l'alerte a bien été déclenchée. Ensuite, consultez votre messagerie pour vous assurer que vous avez bien reçu l'email correspondant à l'alerte.



Si vous souhaitez ajouter une messagerie différente de Gmail, vous devrez cloner le type de média existant "Email" pour l'adapter à votre nouveau service de messagerie.