

NATHAN GABRIELE

# **AP\_SUPERVISION\_ZABBIX**

---

# Sommaire

Introduction .....	1
Schéma Réseau.....	2
Tableau d'adressage .....	2
Définition .....	3
Création de la machine Serveur.....	4
Installation de Zabbix.....	14
Installation du serveur Zabbix sur notre Ubuntu Server .....	16
Téléchargement et installation de Zabbix Server .....	18
Page du setup.php .....	22
Création d'un certificat SSL dans apache 2 .....	30
Création des groupes d'hôtes .....	37
Authentification et LDAP .....	40
Règle de découverte .....	42
Vérifications et application de la règle de découverte .....	43
Tableau de bord Zabbix.....	50
Découverte et Configuration .....	51
Installation de l'agent Zabbix .....	73
Windows.....	73
Installation sur Linux.....	79
Via les repositories Zabbix (linux) .....	84
Conclusion.....	88
Webographie.....	89

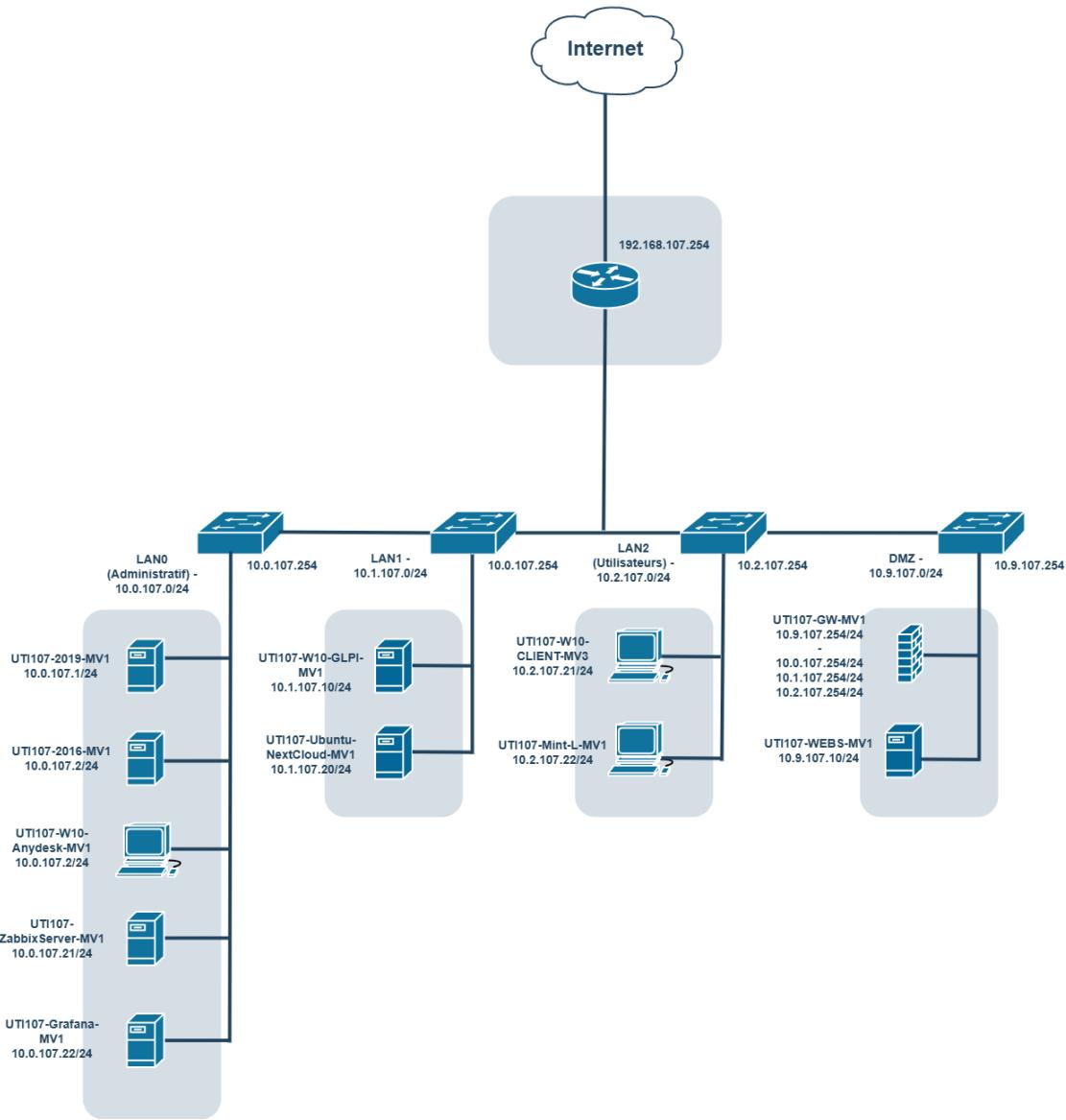
## Introduction

Dans cet atelier, nous allons étudier **Zabbix**, une solution open-source de supervision informatique qui permet de surveiller en temps réel la disponibilité, les performances et la santé des systèmes et des applications. Grâce à son architecture client-serveur, Zabbix collecte des données depuis des agents installés sur les hôtes et permet d'analyser ces informations pour détecter des anomalies, générer des alertes et assurer une gestion proactive des infrastructures.

Nous aborderons les bases de Zabbix, telles que la configuration des hôtes, la création d'éléments de données et la mise en place de déclencheurs pour surveiller des paramètres spécifiques. Nous verrons également comment configurer des alertes et notifications afin d'être informé immédiatement en cas de problème, ainsi que les outils de visualisation de Zabbix, comme les graphiques et tableaux de bord, pour suivre en temps réel l'état de vos ressources.

L'objectif de cet atelier est de vous fournir les compétences nécessaires pour déployer et administrer une instance Zabbix, de façon à garantir la disponibilité et les performances de vos systèmes, tout en vous permettant de réagir rapidement aux incidents grâce à des alertes configurées de manière optimale.

## Schéma Réseau



## Tableau d'adressage

	Adresse IP	Passerelle par défaut	DNS
UTI107-ZabbixServer-MV1	10.0.107.21	10.0.107.254	10.0.107.1 1.1.1.1
UTI107-2019-MV1	10.0.107.1	10.0.107.254	10.0.107.1 1.1.1.1
UTI107-W10-CLIENT-MV3	10.2.107.21	10.2.107.254	10.0.107.1 1.1.1.1
UTI107-WebS-MV1	10.9.107.10	10.9.107.254	10.0.107.1 172.31.1.4, 172.31.1.6

## Définition

Qu'est-ce qu'un superviseur ?

La supervision des serveurs consiste à surveiller l'activité des serveurs (physiques ou virtuels) pour assurer leur bon fonctionnement. Ces serveurs, qui répondent aux demandes des utilisateurs et autres systèmes, doivent être maintenus pour éviter les problèmes, d'autant plus qu'un serveur peut gérer de nombreuses requêtes simultanément. Ce suivi est essentiel dans une infrastructure IT, notamment en raison de la diversité des types de serveurs (web, messagerie, bases de données, etc.).

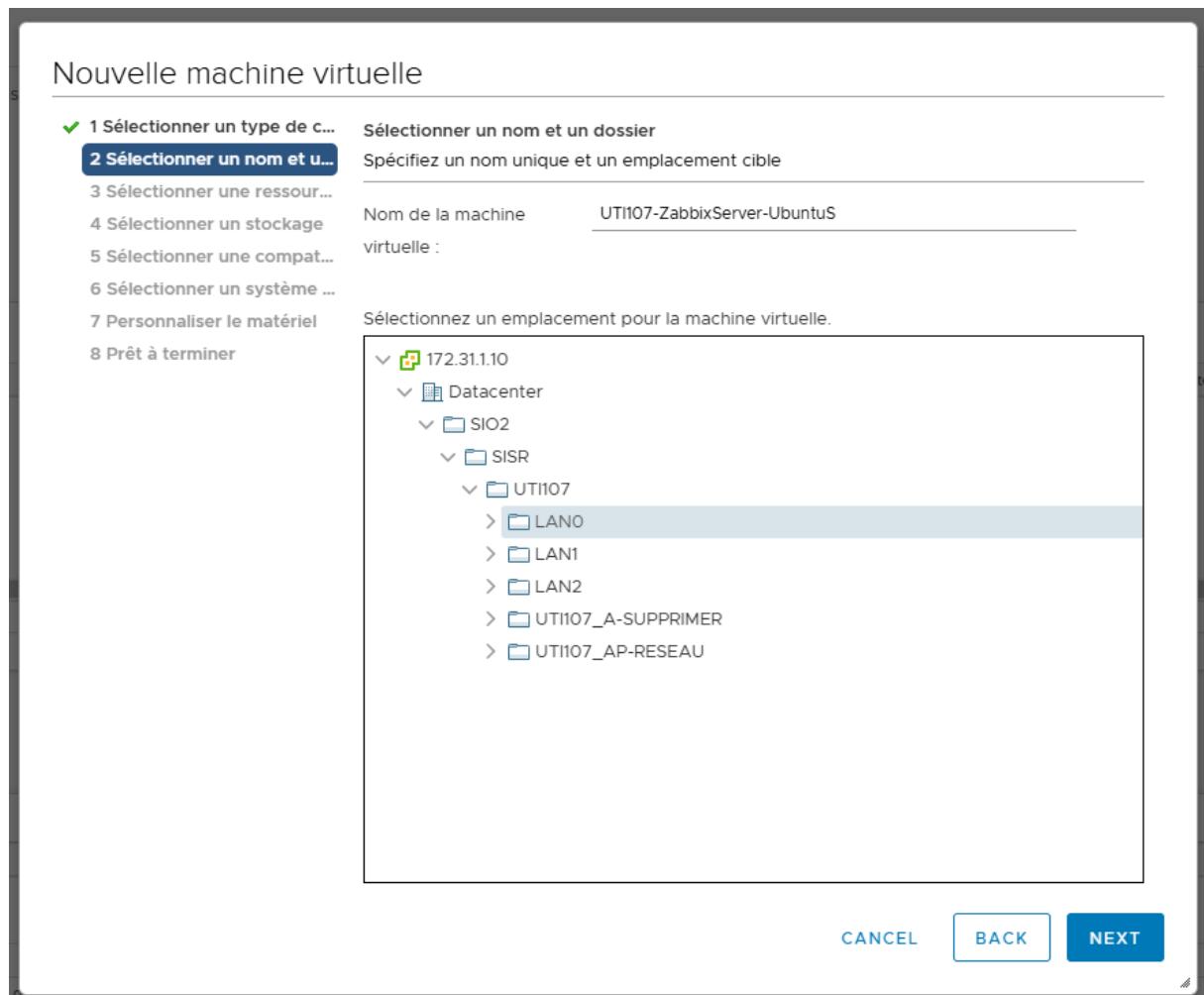
Le terme « supervision des serveurs » est complexe en raison de la très grande variété des serveurs qui existent. Un serveur web peut être une machine physique, mais il est de plus en plus souvent un serveur virtuel hébergé sur une machine physique partagée par des dizaines de clients, chacun exécutant son propre système de serveur de façon indépendante. Les serveurs de messagerie, les serveurs d'impression et les serveurs de base de données ne sont que quelques exemples de serveurs physiques ou logiciels.

Pourquoi est-ce que le superviseur est important ?

La supervision des serveurs est cruciale pour assurer la fiabilité des services IT. Elle permet de détecter les problèmes de performances, de prévenir les interruptions, et d'éviter les pertes de données, tout en garantissant une expérience utilisateur fluide. Elle fournit des données en temps réel et historiques pour évaluer l'état des serveurs et prédire les risques potentiels (comme le manque d'espace disque). Sans cette surveillance, les risques de perte de clients ou de corruption de données augmentent considérablement.

## Création de la machine Serveur

Premièrement, nous avons défini le **nom de la machine virtuelle** comme UTI107-ZabbixServer-UbuntuS-MV1, ce qui permet de l'identifier clairement parmi d'autres VM. Le choix de l'emplacement dans la structure de dossiers (LAN0 sous UTI107) garantit que la machine est associée à la bonne organisation réseau et administrative. Ce choix est justifié pour une meilleure gestion et allocation des ressources, en particulier dans des environnements virtualisés partagés où chaque projet ou service est segmenté.



Nous avons sélectionné le **système d'exploitation invité** comme étant **Linux** avec la version spécifique **Ubuntu Linux (64 bits)**. Ce choix est basé sur les besoins du serveur (héberger Zabbix, une solution de supervision). Ubuntu est privilégié pour sa stabilité, sa compatibilité avec Zabbix et son support à long terme (LTS). La spécification exacte garantit également que le matériel virtuel est optimisé pour ce système.

## Nouvelle machine virtuelle

- ✓ 1 Sélectionner un type de c...
- ✓ 2 Sélectionner un nom et u...
- ✓ 3 Sélectionner une ressour...
- ✓ 4 Sélectionner un stockage
- ✓ 5 Sélectionner une compat...

### 6 Sélectionner un système ...

7 Personnaliser le matériel

8 Prêt à terminer

#### Sélectionner un système d'exploitation invité

Choisissez le système d'exploitation invité qui sera installé sur la machine virtuelle

L'identification du système d'exploitation invité permet à l'assistant de fournir les valeurs par défaut appropriées pour l'installation du système d'exploitation.

Famille de SE invités :

Version du SE invité :

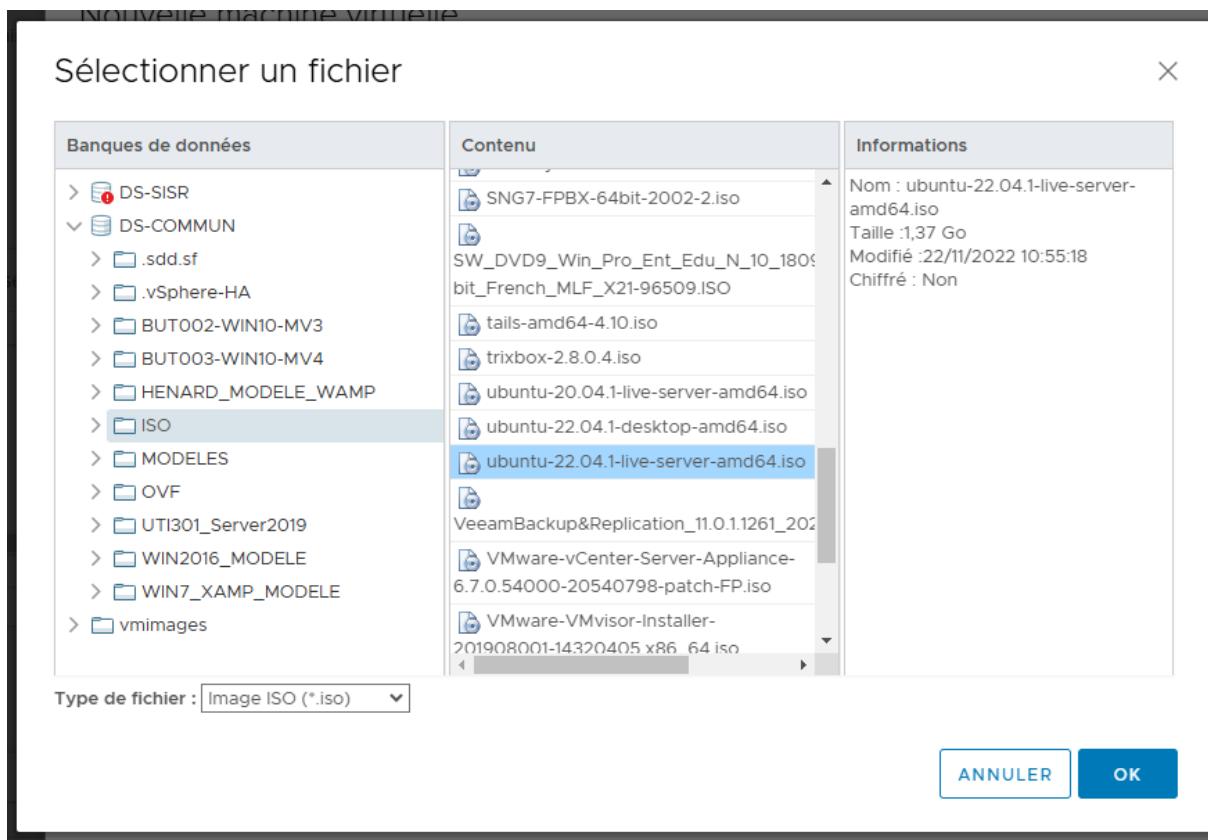
Compatibilité : ESXi 6.7 et versions ultérieures (VM version 14)

[CANCEL](#)

[BACK](#)

[NEXT](#)

Le fichier ISO que nous allons utiliser est **ubuntu-22.04-live-server-amd64.iso**, situé dans le répertoire partagé DS-SISR. Ce choix est stratégique car Ubuntu 22.04 LTS offre des fonctionnalités modernes, une sécurité renforcée et une compatibilité avec les outils de supervision comme Zabbix. L'ISO est stocké dans une banque de données commune, ce qui facilite son utilisation par d'autres projets ou installations.



Mettre le disque en provisionnement dynamique, 100 Go de stockage et 8Go de mémoire vive et ce dernier sera dans le réseau d'administration.

Les paramètres matériels de la machine virtuelle incluent :

- **CPU** : 1 vCPU, suffisant pour les charges de travail initiales du serveur Zabbix.
  - **Mémoire** : 4 Go, adapté aux besoins d'un serveur de supervision.
  - **Disque dur** : 50 Go, offrant un espace suffisant pour le système, les journaux et la base de données.
  - **Réseau** : Connecté au réseau SISR-DMZ-1079 pour isoler le serveur dans un environnement sécurisé.
  - **Lecteur CD/DVD** : Monté sur le fichier ISO sélectionné pour permettre l'installation du système.
- Ces choix garantissent un équilibre entre la performance et l'économie des ressources dans un environnement partagé.

## Nouvelle machine virtuelle

- ✓ 1 Sélectionner un type de c...
- ✓ 2 Sélectionner un nom et u...
- ✓ 3 Sélectionner une ressour...
- ✓ 4 Sélectionner un stockage
- ✓ 5 Sélectionner une compat...
- ✓ 6 Sélectionner un système ...

### Personnaliser le matériel

Configurez le matériel de la machine virtuelle

Matériel virtuel      Options VM

AJOUTER UN PÉRIPHÉRIQUE

#### 7 Personnaliser le matériel

8 Prêt à terminer

> CPU		1	▼	
> Mémoire *	4		▼	Go ▼
> Nouveau disque dur *	50		▼	Go ▼
> Nouveau contrôleur SCSI *	LSI Logic Parallel			
> Nouveau réseau *	SISR-DMZ-1079	▼	<input checked="" type="checkbox"/> Connecter...	
> Nouveau lecteur CD/DVD *		▼	<input checked="" type="checkbox"/> Fichier ISO banque de donn	▼ Connecter...
> Carte vidéo *	Spécifier les paramètres personnalisés	▼		
Pérophérique VMCI	Pérophérique sur le bus PCI de la machine virtuelle fournissant la prise en charge pour	▼		

Compatibilité : ESXi 6.7 et versions ultérieures (VM version 14)

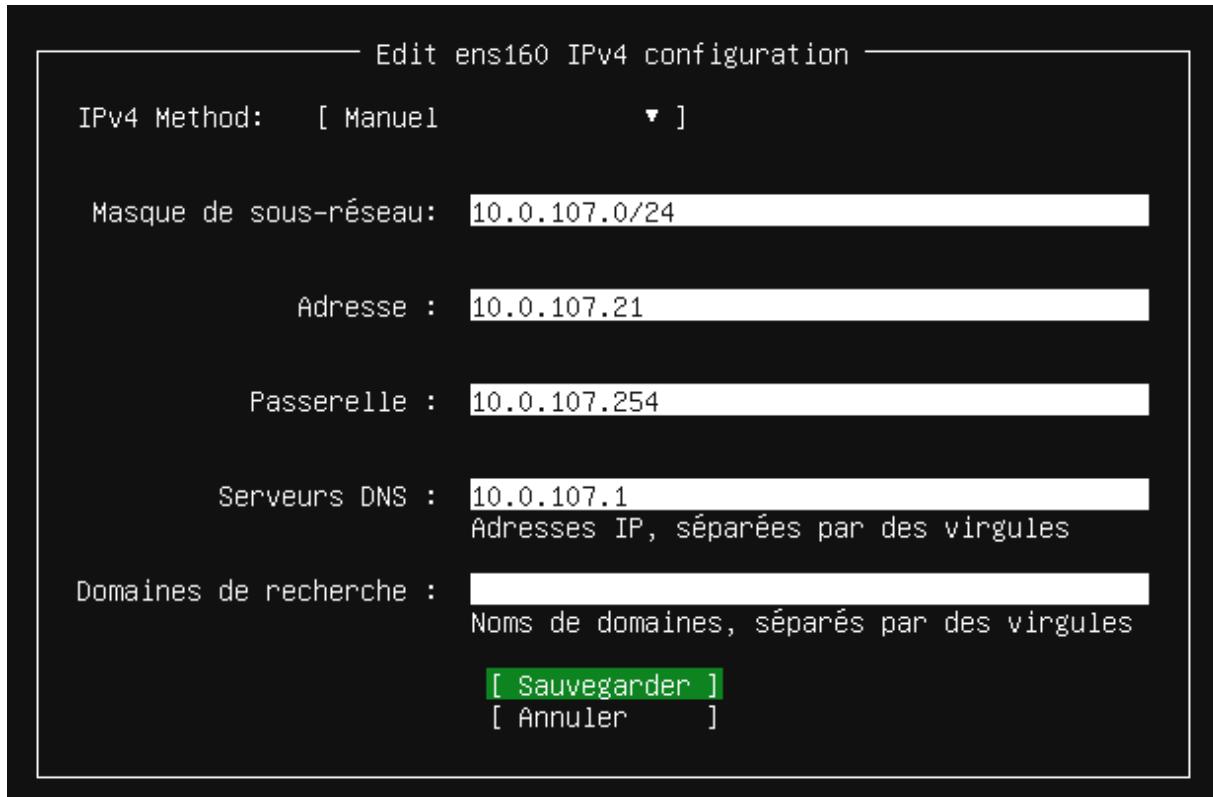
CANCEL

BACK

NEXT

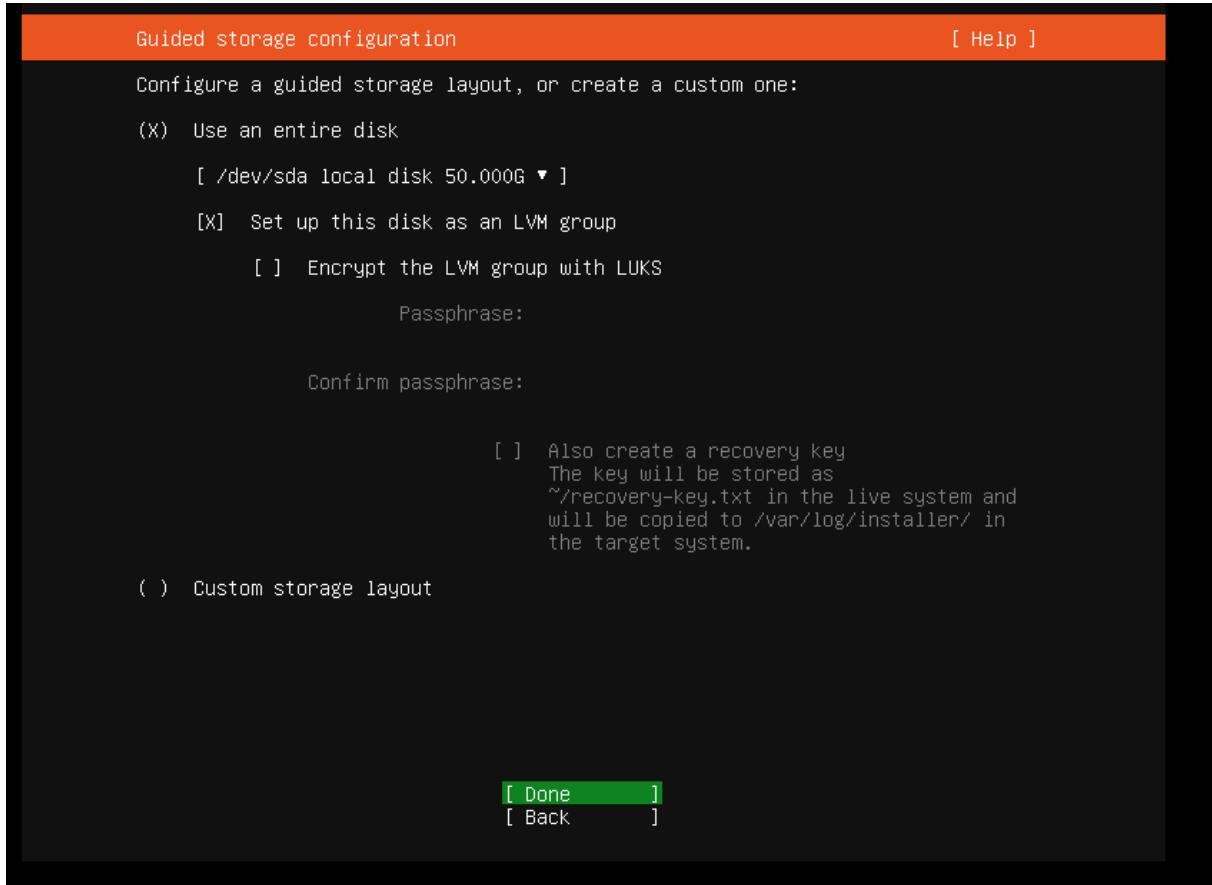
Le réseau sur la machine UTI107-ZabbixServer-UbuntuS-MV1 a été configuré manuellement avec les paramètres suivants :

- Adresse IP** : 10.0.107.21 dans le LAN1 (statique pour une identification stable sur le réseau).
- Masque de sous-réseau** : 255.255.255.0 ou /24, typique pour un réseau local.
- Passerelle** : 10.0.107.254, permettant l'accès extérieur au sous-réseau.
- Serveur DNS** : 10.0.107.1, pour la résolution des noms de domaine. Cette configuration garantit une connectivité stable et une intégration dans le réseau local, tout en respectant les bonnes pratiques d'adressage IP.

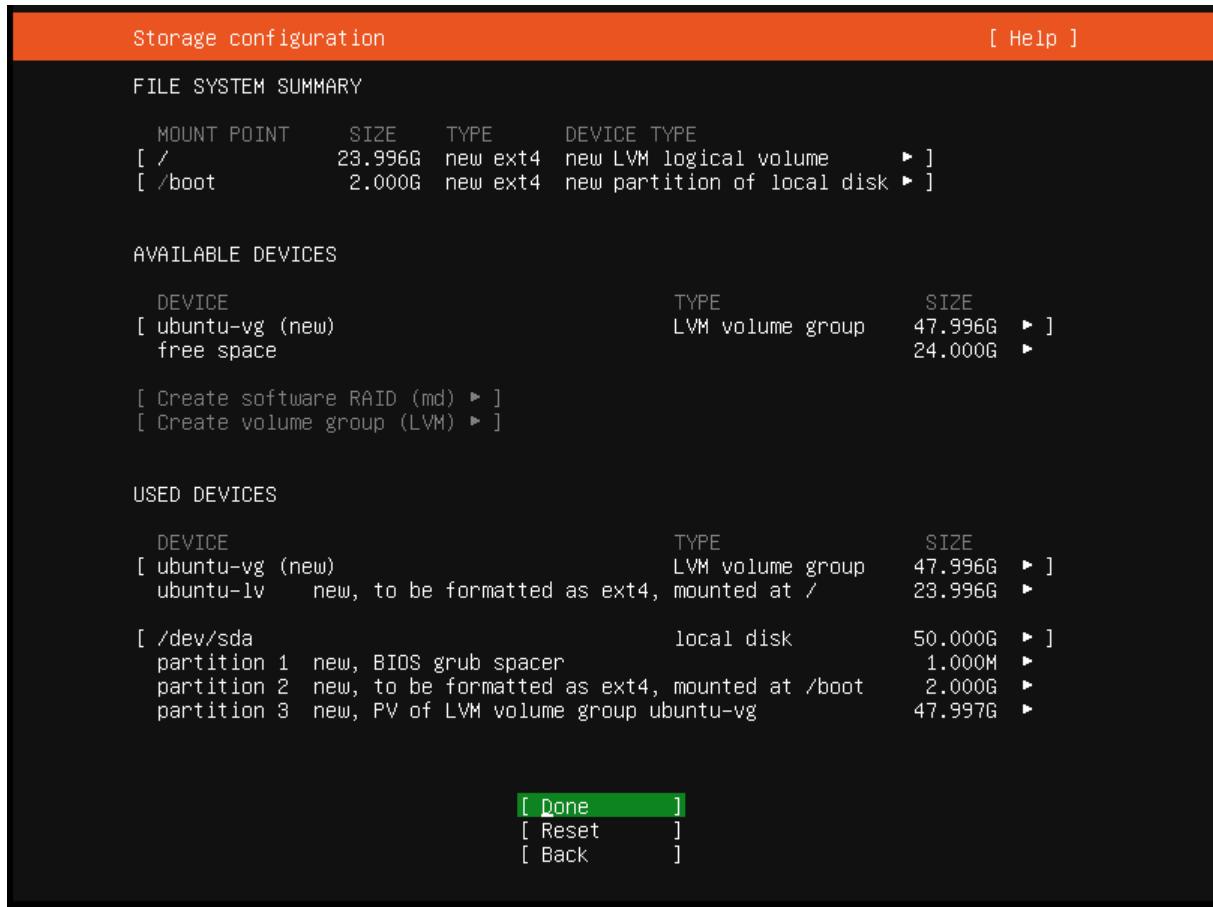


L'étape de configuration du stockage présente une approche guidée où l'intégralité du disque disponible, /dev/sda, est utilisée. Cette méthode standardise le partitionnement pour garantir une configuration fonctionnelle sans intervention complexe. L'activation de LVM permet une gestion dynamique des volumes, utile si des ajustements de stockage sont nécessaires après l'installation. L'encryptage avec LUKS, bien que proposé, n'a pas été sélectionné pour éviter des

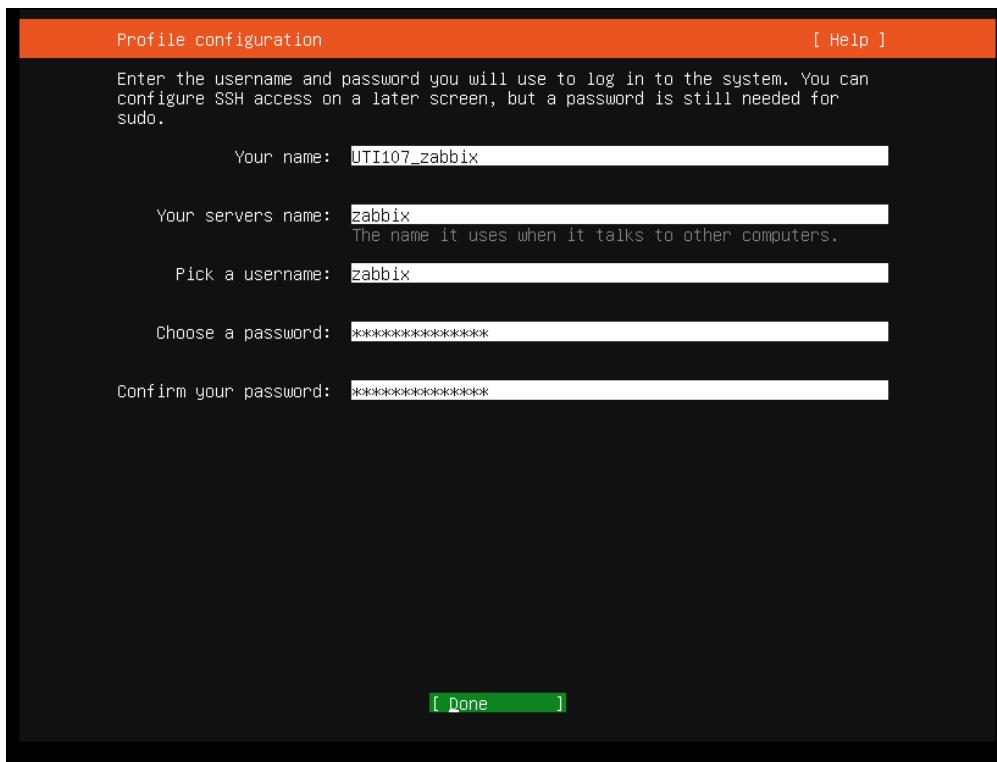
étapes supplémentaires ou une surcharge de performances dans ce contexte précis.



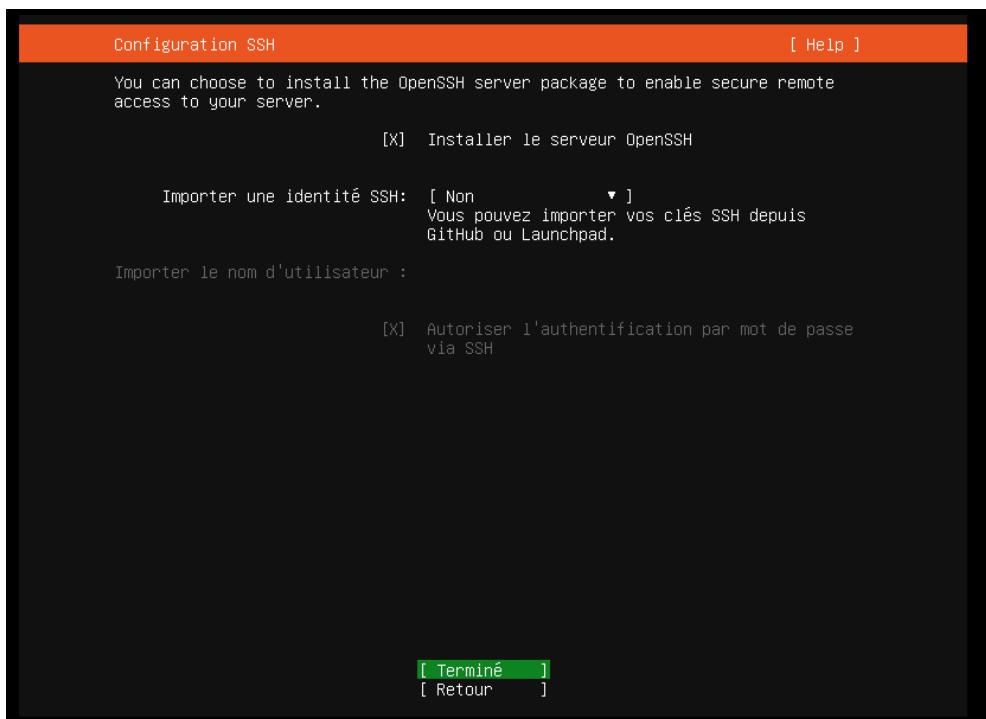
Le récapitulatif de la configuration du stockage affiche la répartition automatique des partitions. Une partition de 2 Go est dédiée à /boot, nécessaire pour les fichiers du chargeur de démarrage GRUB, et un volume principal de 24 Go est alloué à la racine (/), où le système d'exploitation et ses fichiers seront installés. Ces partitions sont logiquement organisées via LVM, permettant des redimensionnements futurs si la charge ou les besoins évoluent.



L'écran de configuration du profil demande les informations de base pour identifier et sécuriser le serveur. Le nom de la machine est défini comme UTI107\_zabbix, facilitant son identification sur le réseau. Un utilisateur nommé zabbix est configuré, avec un mot de passe sécurisé, pour gérer le serveur avec des droits d'administrateur. Cette étape garantit une configuration initiale adaptée à l'exploitation du serveur.



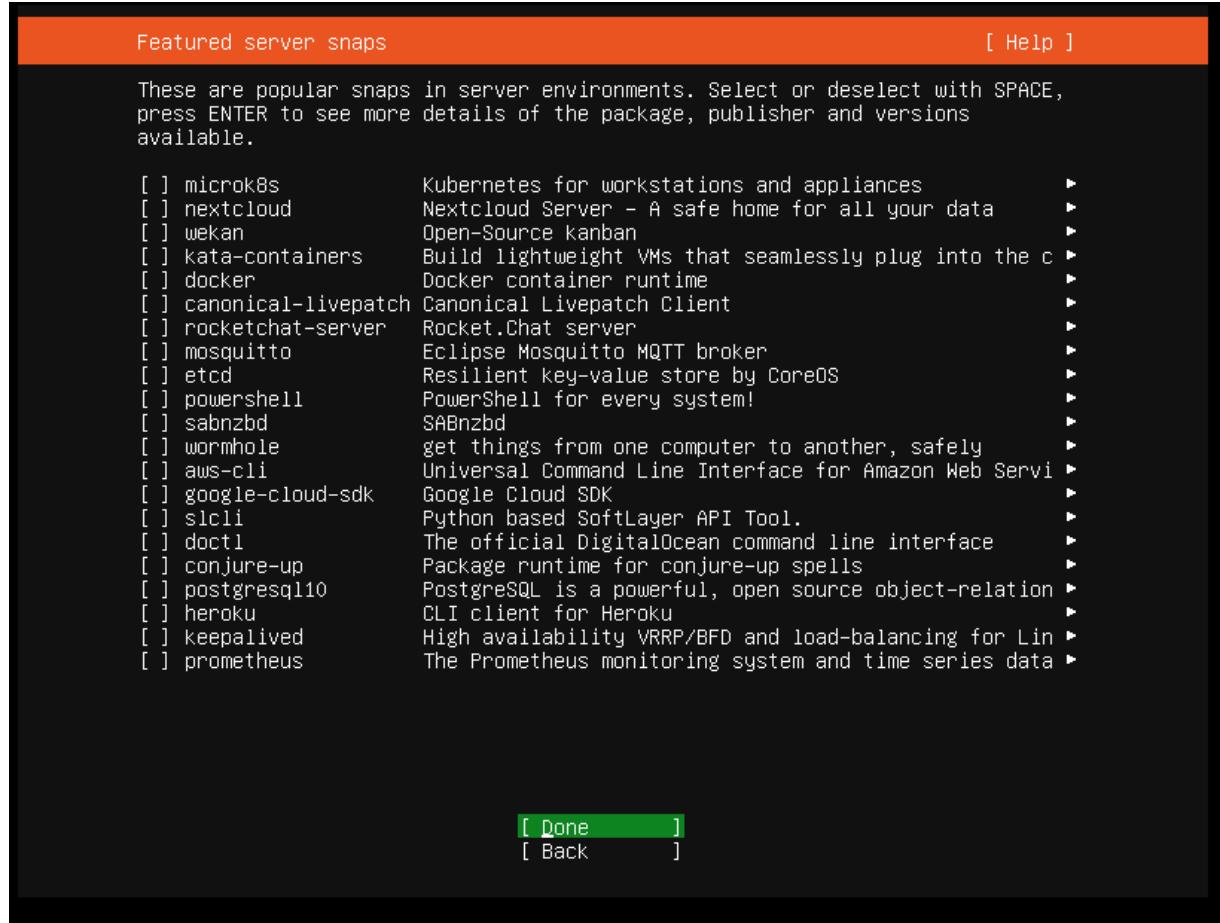
la configuration de SSH, l'installation du serveur OpenSSH est activée pour permettre l'accès distant sécurisé au système. Cette fonctionnalité est essentielle pour administrer le serveur sans avoir un accès physique direct. L'authentification par mot de passe est autorisée, ce qui simplifie l'accès dans des environnements contrôlés ou de test, tout en laissant la possibilité de renforcer la sécurité avec des clés SSH si nécessaire.



L'écran suivant propose l'installation de différents logiciels sous forme de *snaps*, comme Docker, Prometheus ou encore GRUB. Aucun logiciel supplémentaire n'est sélectionné à ce stade, indiquant une préférence pour une installation minimalistre, réduisant les dépendances inutiles et laissant le choix d'ajouter ultérieurement des composants en fonction des besoins spécifiques

du

projet.



Lors de l'installation, le processus détaille les étapes, telles que l'installation des paquets système, la configuration de GRUB pour le démarrage, et la mise en place des configurations réseau. Cela assure que tous les composants nécessaires sont bien installés et prêts à être utilisés. L'utilisateur peut ainsi suivre l'avancement, garantissant que le système est configuré correctement et sans erreur.

```
Installing system [ Help ]  
  
curtin command install  
configuring installed system  
running 'curtin curthooks'  
curtin command curthooks  
configuring apt configuring apt  
installing missing packages  
Installing packages on target system: ['grub-pc']  
configuring iscsi service  
configuring raid (mdadm) service  
configuring NVMe over TCP  
installing kernel  
setting up swap  
apply networking config  
writing etc/fstab  
configuring multipath  
updating packages on target system  
configuring pollinate user-agent on target  
configuring kernel crash dumps settings  
updating initramfs configuration  
configuring target system bootloader  
installing grub to target devices  
copying metadata from /cdrom  
final system configuration  
calculating extra packages to install  
installing openssh-server  
retrieving openssh-server  
curtin command system-install  
unpacking openssh-server /  
curtin command system-install \  
  
[ View full log ]
```

la phase de démontage des supports d'installation et de finalisation du système confirme que l'installation s'est déroulée correctement. Un message demande de retirer le média d'installation, tel qu'un fichier ISO, pour éviter un redémarrage accidentel sur le support initial.

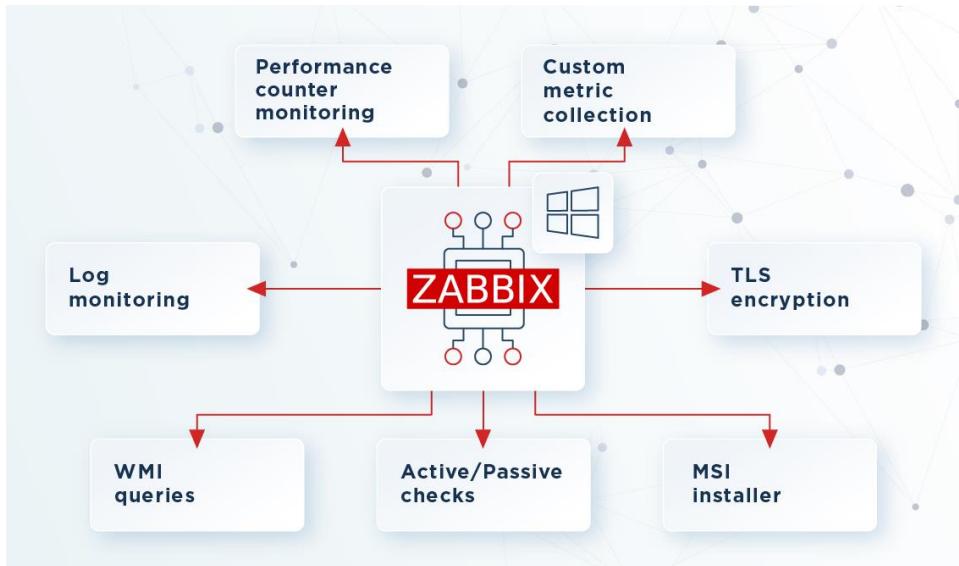
Cette finalisation prépare le système à démarrer normalement et à être opérationnel.

```
[FAILED] Failed unmounting /cdrom.
[ OK ] Unmounted /media/filesystem.
[ OK ] Unmounted /media/minimal.
[ OK ] Unmounted /rofs.
[ OK ] Unmounted Mount unit for core20, revision 1587.
[ OK ] Unmounted /tmp/tmpfqri7xqj/ubuntu-server-minimal.ubuntu-server.squashfs.dir.
[ OK ] Unmounted /tmp/tmpfqri7xqj/ubuntu-server-minimal.squashfs.dir.
[ OK ] Unmounted /media/full.
[ OK ] Unmounted Mount unit for lxd, revision 22923.
[ OK ] Unmounted Mount unit for snapd, revision 16292.
[ OK ] Unmounted /run/credentials/systemd-sysusers.service.
[ OK ] Unmounted /run/snapd/ns/lxd.mnt.
Unmounting /run/snapd/ns...
[ OK ] Unmounted /run/snapd/ns.
[ OK ] Unmounted Mount unit for subiquity, revision 3698.
[ OK ] Unmounted /target/boot.
Unmounting /target...
[ OK ] Unmounted /tmp/tmpfqri7xqj/root.dir.
Unmounting /tmp...
[ OK ] Unmounted /tmp.
[ OK ] Stopped target Swap.
[ OK ] Unmounted /target.
[ OK ] Stopped target Preparation for Local File Systems.
[ OK ] Reached target Unmount All Filesystems.
Stopping Monitoring of LVM2 mirrors,...c. using dmeventd or progress polling...
Stopping Device-Mapper Multipath Device Controller...
[ OK ] Stopped Create Static Device Nodes in /dev.
[ OK ] Stopped Create System Users.
[ OK ] Stopped Device-Mapper Multipath Device Controller.
[ OK ] Stopped Remount Root and Kernel File Systems.
[ OK ] Stopped Monitoring of LVM2 mirrors, ...etc. using dmeventd or progress polling.
[ OK ] Reached target System Shutdown.
Starting Shuts down the "live" preinstalled system cleanly...
Please remove the installation medium, then press ENTER:
Unmounting /cdrom...
[FAILED] Failed unmounting /cdrom.
```

## Installation de Zabbix

Mais qu'est-ce que Zabbix ?

Zabbix est un logiciel qui supervise de nombreux paramètres réseaux ainsi que la santé et l'intégrité des serveurs. Zabbix utilise un mécanisme de notification flexible qui permet aux utilisateurs de configurer une base d'alerte e-mail pour pratiquement tous les événements. Cela permet une réponse rapide aux problèmes serveurs. Zabbix offre un excellent reporting et des fonctionnalités de visualisation de données basées sur les données stockées.



À quoi ressemble le flux de données ?

L'agent Zabbix collecte les données qui nous intéressent, par exemple l'utilisation actuelle du processeur, la RAM, le flux de données sur le réseau, la charge de la base de données et l'efficacité des services individuels (par exemple, HTTP, SSH, FTP).

Il envoie ensuite les informations collectées au serveur principal, en les formulant dans des tableaux ou des graphiques clairs et faciles à lire.

Les données sont conservées dans des bases de données relationnelles (MySQL, Oracle ou PostgreSQL) et sont accessibles via une interface Web intuitive.

### Les principales fonctionnalités de Zabbix

Zabbix propose une série de fonctionnalités qui optimisent la supervision des serveurs et réseaux, en fournissant une visibilité centralisée et une gestion simplifiée.

- **Surveillance et compatibilité :**
  - Découverte automatique des serveurs et périphériques réseau
  - Interface web centralisée pour gérer la supervision
  - Compatibilité avec de nombreux systèmes (Linux, Solaris, Windows, etc.)
- **Agents et options de surveillance :**
  - Mécanismes de "polling" et "trapping" pour un suivi flexible
  - Surveillance avec ou sans agent
  - Authentification d'agent sécurisée pour une communication fiable
- **Gestion et alertes :**

- Notifications par e-mail sur les événements prédéfinis
- Permissions utilisateurs configurables
- Visualisation de haut niveau et journal d'audit pour un suivi détaillé

Ces fonctionnalités font de Zabbix un outil robuste, centralisé et capable d'alerter les équipes en temps réel.

### **Avantages de Zabbix**

Les nombreux avantages de Zabbix en font une solution de choix pour les entreprises recherchant une supervision performante et économique.

- **Solution open source et économique :**
  - Zabbix est gratuit et à faible coût d'entretien
  - Installation simple et faible courbe d'apprentissage
- **Efficacité et centralisation :**
  - Agents optimisés pour UNIX et Windows
  - Base de données centralisée pour le stockage des données de supervision
- **Fonctionnalités avancées :**
  - Support SNMP (v1 et v2)
  - Visualisation des capacités et procédure de nettoyage intégrée

En résumé, Zabbix combine flexibilité, efficacité et un faible coût de possession, ce qui en fait un choix prisé pour surveiller les infrastructures IT.

### *Installation du serveur Zabbix sur notre Ubuntu Server*

Dans un premier temps, nous allons configurer les paramètres nécessaires pour l'installation de Zabbix. La version sélectionnée est **Zabbix 7.0 LTS**, car il s'agit de la version stable avec un support à long terme, garantissant fiabilité et mises à jour prolongées. Le choix de **Ubuntu 22.04 LTS (Jammy)** comme système d'exploitation est justifié par sa compatibilité avec Zabbix 7.0 et ses fonctionnalités modernes tout en restant stable. Côté composants, l'utilisateur sélectionne le serveur, le frontend et l'agent Zabbix, couvrant ainsi l'ensemble des besoins pour une surveillance complète : le serveur gère la collecte et le stockage des données, le frontend offre une interface web pour visualiser les métriques, et l'agent collecte les données sur les hôtes surveillés.

VERSION DE ZABBIX	OS DISTRIBUTION	VERSION DU SYSTÈME D'EXPLOITATION	ZABBIX COMPONENT	BASE DE DONNÉES	SERVEUR WEB
7.0 LTS	Alma Linux	24.04 (Noble)	Server, Frontend, Agent	MySQL	Apache
6.4	Amazon Linux	22.04 (Jammy)	Proxy	PostgreSQL	Nginx
6.0 LTS	CentOS	20.04 (Focal)	Agent		
5.0 LTS	Debian	18.04 (Bionic)	Agent 2		
7.2 (pre-release)	Debian (arm64)	16.04 (Xenial)	Java Gateway		
	OpenSUSE Leap		Web Service		
	Oracle Linux				
	Raspberry Pi OS				
	Red Hat Enterprise Linux				
	Rocky Linux				
	SUSE Linux Enterprise Server				
	Ubuntu				
	Ubuntu (arm64)				

Pour la base de données, **MySQL** est choisie. Ce choix est souvent préféré en raison de sa popularité, de sa facilité de configuration et de son intégration transparente avec Zabbix. MySQL offre également des performances solides pour gérer des volumes de données importants, tout en restant accessible pour les administrateurs moins expérimentés. Enfin, **Apache** est configuré comme serveur web, une solution classique et éprouvée, offrant compatibilité et simplicité dans la gestion de l'interface frontend.

L'accès terminal à une machine installée avec Ubuntu Server 22.04 LTS. Le login serverzabbix et les métriques affichées confirment que le serveur est correctement configuré et opérationnel. Les ressources système montrent une utilisation faible, avec seulement **14,5% de stockage utilisé sur 47.93 Go**, confirmant que le serveur est prêt pour Zabbix sans surcharge initiale. L'adresse IP (10.0.107.21) est affichée, indiquant que la machine est correctement connectée au réseau et accessible pour l'administration.

```
Ubuntu 22.04.1 LTS zabbixserver tty1
zabbixserver login: serverzabbix
Password:
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-124-generic x86_64)

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

 System information as of lun. 04 nov. 2024 15:02:18 UTC

 System load: 0.08447265625 Processes: 198
 Usage of /: 14.5% of 47.93GB Users logged in: 0
 Memory usage: 3% IPv4 address for ens160: 10.0.107.21
 Swap usage: 0%

103 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

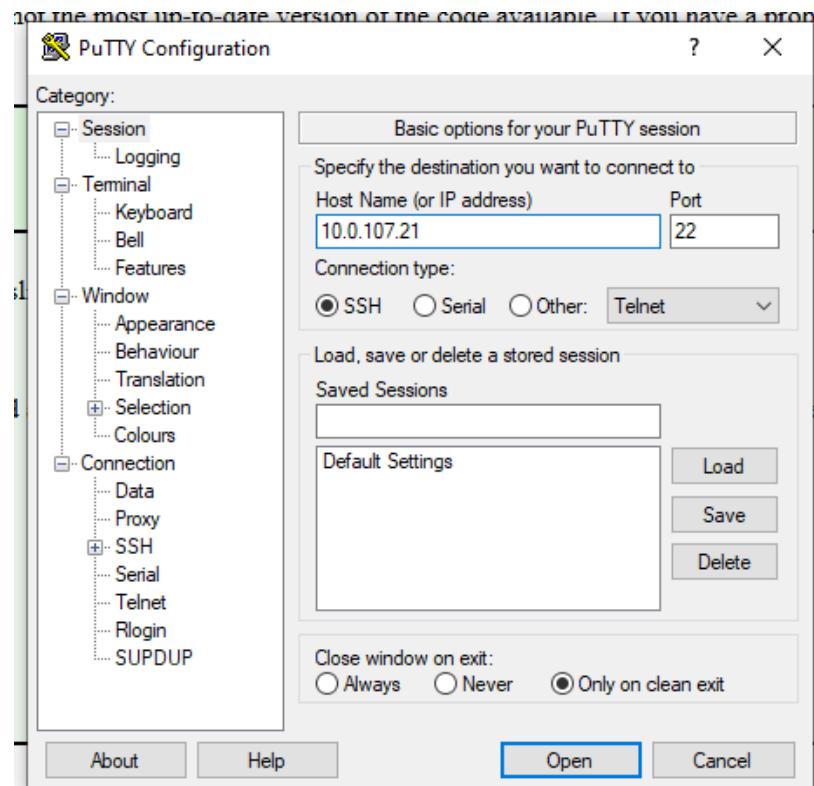
serverzabbix@zabbixserver:~$
```

On peut commencer la procédure d'installation de Zabbix Packages sur notre Ubuntu Server.

## Téléchargement et installation de Zabbix Server

Pour permettre le copier-coller et une prise en main plus rapide, nous utilisons **PuTTY** pour nous connecter au serveur Zabbix via SSH. Nous saisissons l'adresse IP de notre serveur, 10.0.107.21, ainsi que le port par défaut, **22**, qui correspond au protocole SSH activé précédemment.

Nous sélectionnons **SSH** comme type de connexion pour garantir un chiffrement sécurisé des échanges entre notre machine et le serveur. Cette configuration simple avec PuTTY nous permet d'administrer efficacement le serveur Zabbix depuis un poste Windows, en restant dans un environnement rapide et convivial.



Dorénavant pour installer, il faut appliquer les commandes ci-dessous.

- Become root user

Start new shell session with root privileges.

```
$ sudo -s
```

- Install Zabbix repository

[Documentation](#)

```
# wget https://repo.zabbix.com/zabbix/7.0/ubuntu/pool/main/z/zabbix-release/zabbix-release_latest+ubuntu22.04_all.deb
# dpkg -i zabbix-release_latest+ubuntu22.04_all.deb
# apt update
```

- Install Zabbix server, frontend, agent

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

- Installer MySQL

Avant d'exécuter ses commandes, installer mysql.

Installation du serveur MySQL pour gérer la base de données de Zabbix :

```
# apt install mysql-server
```

S'assurer que le service MySQL est actif :

```
# systemctl start mysql  
# systemctl enable mysql
```

e. Créer la base de données initiale

Se connecter à MySQL avec les priviléges root :

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

Saisir le mot de passe de l'utilisateur root.

Exécuter les commandes SQL dans MySQL :

```
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;
```

Importer les scripts SQL pour initialiser la base de données :

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

Réinitialiser la configuration MySQL :

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

Puis exécuter dans MySQL :

```
mysql> set global log_bin_trust_function_creators = 0;  
mysql> quit;
```

## f. Configurer la base de données pour Zabbix

Configuration du mot de passe dans **/etc/zabbix/zabbix\_server.conf**

Nous avons édité le fichier de configuration principal de Zabbix Server pour y définir le mot de passe utilisé par le serveur pour accéder à la base de données MySQL. Cela est indispensable pour établir une connexion sécurisée et valide entre le serveur Zabbix et la base de données, en spécifiant **DBPassword=zabbix**.

modifier le fichier : /etc/zabbix/zabbix\_server.conf = nano /etc/zabbix\_server.conf

DBPassword=zabbix

```
root@zabbixserver:/home/serverzabbix
GNU nano 6.2                                     /etc/zabbix/zabbix_server.conf
### Option: DBPassword
#      Database password.
#      Comment this line if no password is used.
#
# Mandatory: no
# Default:
DBPassword=zabbix

### Option: DBSocket
#      Path to MySQL socket.
#
# Mandatory: no
# Default:
# DBSocket=

### Option: DBPort
#      Database port when not using local socket.
#
# Mandatory: no
# Range: 1024-65535
# Default:
# DBPort=
```

g. Démarrer les processus du serveur et de l'agent Zabbix

Nous avons redémarré les services nécessaires avec la commande :

```
# systemctl restart zabbix-server zabbix-agent apache2
# systemctl enable zabbix-server zabbix-agent apache2
root@zabbixserver:/home/serverzabbix# systemctl restart zabbix-server zabbix-agent apache2
root@zabbixserver:/home/serverzabbix# systemctl enable zabbix-server zabbix-agent apache2
Synchronizing state of zabbix-server.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable zabbix-server
Synchronizing state of zabbix-agent.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable zabbix-agent
Synchronizing state of apache2.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable apache2
root@zabbixserver:/home/serverzabbix#
```

Ensuite, nous avons activé ces services pour qu'ils démarrent automatiquement au prochain redémarrage grâce à :

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

### Vérification de l'état du service Zabbix Agent

La commande `systemctl status zabbix-agent` a permis de vérifier que le service est actif et fonctionne correctement. Ce diagnostic est essentiel pour s'assurer que l'agent est prêt à collecter et transmettre les métriques au serveur Zabbix.

```

zabbix@zabbix:~$ sudo systemctl status zabbix-agent
[sudo] password for zabbix:
● zabbix-agent.service - Zabbix Agent
  Loaded: loaded (/lib/systemd/system/zabbix-agent.service; enabled; vendor preset: enabled)
  Active: active (running) since Wed 2024-11-27 15:13:59 UTC; 1 day 7h ago
    Main PID: 109450 (zabbix_agentd)
      Tasks: 13 (limit: 4564)
     Memory: 15.6M
        CPU: 8min 53.038s
      CGroup: /system.slice/zabbix-agent.service
          ├ 109450 /usr/sbin/zabbix_agentd -c /etc/zabbix/zabbix_agentd.conf
          ├ 109451 "/usr/sbin/zabbix_agentd: collector [idle 1 sec]" ...
          ├ 109452 "/usr/sbin/zabbix_agentd: listener #1 [waiting for connection]"
          ├ 109453 "/usr/sbin/zabbix_agentd: listener #2 [waiting for connection]"
          ├ 109454 "/usr/sbin/zabbix_agentd: listener #3 [waiting for connection]"
          ├ 109455 "/usr/sbin/zabbix_agentd: listener #4 [waiting for connection]"
          ├ 109456 "/usr/sbin/zabbix_agentd: listener #5 [waiting for connection]"
          ├ 109457 "/usr/sbin/zabbix_agentd: listener #6 [waiting for connection]"
          ├ 109458 "/usr/sbin/zabbix_agentd: listener #7 [waiting for connection]"
          ├ 109459 "/usr/sbin/zabbix_agentd: listener #8 [waiting for connection]"
          ├ 109460 "/usr/sbin/zabbix_agentd: listener #9 [waiting for connection]"
          ├ 109461 "/usr/sbin/zabbix_agentd: listener #10 [waiting for connection]"
          └ 109462 "/usr/sbin/zabbix_agentd: active checks #1 [idle 1 sec]" ...

```

## Vérification de l'état du service Zabbix Agent

La commande `systemctl status apache2` a permis de vérifier que le service est actif et fonctionne correctement. Cela nous permettra de nous connecter à l'interface Zabbix.

```

serverzabbix@zabbixserver:~$ sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
  Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
  Active: active (running) since Thu 2024-11-07 08:05:08 UTC; 9min ago
    Docs: https://httpd.apache.org/docs/2.4/
  Process: 857 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
 Main PID: 949 (apache2)
   Tasks: 11 (limit: 9396)
  Memory: 97.7M
     CPU: 5.812s
    CGroup: /system.slice/apache2.service
        ├ 949 /usr/sbin/apache2 -k start
        ├ 1056 /usr/sbin/apache2 -k start
        ├ 1057 /usr/sbin/apache2 -k start
        ├ 1058 /usr/sbin/apache2 -k start
        ├ 1059 /usr/sbin/apache2 -k start
        ├ 1271 /usr/sbin/apache2 -k start
        ├ 1274 /usr/sbin/apache2 -k start
        ├ 1288 /usr/sbin/apache2 -k start
        ├ 1289 /usr/sbin/apache2 -k start
        └ 1290 /usr/sbin/apache2 -k start
        1291 /usr/sbin/apache2 -k start

nov. 07 08:05:08 zabbixserver systemd[1]: Starting The Apache HTTP Server...
nov. 07 08:05:08 zabbixserver apachectl[874]: AH00558: apache2: Could not reliably determine the ser...
nov. 07 08:05:08 zabbixserver systemd[1]: Started The Apache HTTP Server.

serverzabbix@zabbixserver:~$ 

```

## Page du setup.php

Dans cette étape, nous accédons au processus de configuration initiale du frontend Zabbix via l'URL `http://10.0.107.21/zabbix/setup.php`. Cette adresse pointe directement vers le script de configuration pour lancer l'installation et la mise en place de Zabbix après avoir configuré et démarré le serveur.

Sur cet écran d'accueil, nous avons la possibilité de choisir la langue par défaut pour l'interface de configuration, ici configurée en français (fr\_FR) pour simplifier la prise en main pour un utilisateur francophone. Cette page est également une introduction au processus d'installation divisé en plusieurs étapes : vérification des prérequis, configuration de la connexion à la base de données, définition des paramètres du serveur, récapitulatif des configurations, et enfin, l'installation proprement dite.

L'accès à cette URL spécifique est nécessaire car elle déclenche la séquence de configuration, permettant à Zabbix de s'assurer que les éléments essentiels sont correctement paramétrés avant de rendre le serveur pleinement opérationnel. Ce point d'entrée garantit que toutes les étapes suivantes, telles que les connexions à la base de données et les configurations système, s'effectueront dans un ordre logique et sans erreurs.



Lors de cette étape, Zabbix vérifie si les composants nécessaires (PHP, MySQL, etc.) sont installés et configurés selon ses exigences minimales. Les éléments vérifiés incluent la version de PHP, les limites de mémoire (memory\_limit), les tailles maximales d'upload et de post (upload\_max\_filesize et post\_max\_size), et la compatibilité avec MySQL. Tous les éléments sont marqués comme "OK", indiquant que le serveur est prêt à continuer. Cette vérification garantit que l'environnement est optimal pour une installation sans erreur, ce qui est essentiel pour assurer une performance stable.

## Vérification des prérequis

Bienvenue

Vérification des prérequis

Configurer la connexion à la base de données

Paramètres

Résumé pré-installation

Installer

		Valeur actuelle	Requis
	Version de PHP	8.1.2-1ubuntu2.19	8.0.0 <span>OK</span>
	Option PHP "memory_limit"	128M	128M <span>OK</span>
	Option PHP "post_max_size"	16M	16M <span>OK</span>
	Option PHP "upload_max_filesize"	2M	2M <span>OK</span>
	Option PHP "max_execution_time"	300	300 <span>OK</span>
	Option PHP "max_input_time"	300	300 <span>OK</span>
	support de bases de données par PHP	MySQL	<span>OK</span>
	bcmath pour PHP	actif	<span>OK</span>
	mbstring pour PHP	actif	<span>OK</span>
	Option PHP "mbstring.func_overload"	inatif	inatif <span>OK</span>

[Retour](#)[Prochaine étape](#)

Ici, nous avons configuré les paramètres de connexion à la base de données. Les informations saisies incluent :

- **Type de base de données** : MySQL, choisi pour sa compatibilité et ses performances avec Zabbix.
- **Hôte de la base de données** : localhost, car la base est hébergée localement sur le même serveur.
- **Nom de la base de données** : zabbix, précédemment créé lors de l'installation.
- **Utilisateur et mot de passe** : Définis pour sécuriser l'accès à la base tout en maintenant une liaison fiable avec Zabbix Server.

Ce choix permet à Zabbix de gérer ses données dans une base sécurisée et accessible rapidement, tout en isolant les accès avec un compte dédié.



## Configurer la connexion à la base de données

Veuillez créer la base de données manuellement et configurer les paramètres de connexion. Appuyez sur le bouton "Prochaine étape" quand c'est fait.

Bienvenue

Vérification des prérequis

Type de base de données

Configurer la connexion à la base de données

Hôte base de données

Paramètres

Port de la base de données  0 - utiliser le port par défaut

Résumé pré-installation

Nom de la base de données

Installer

Stocker les informations d'identification dans

Utilisateur

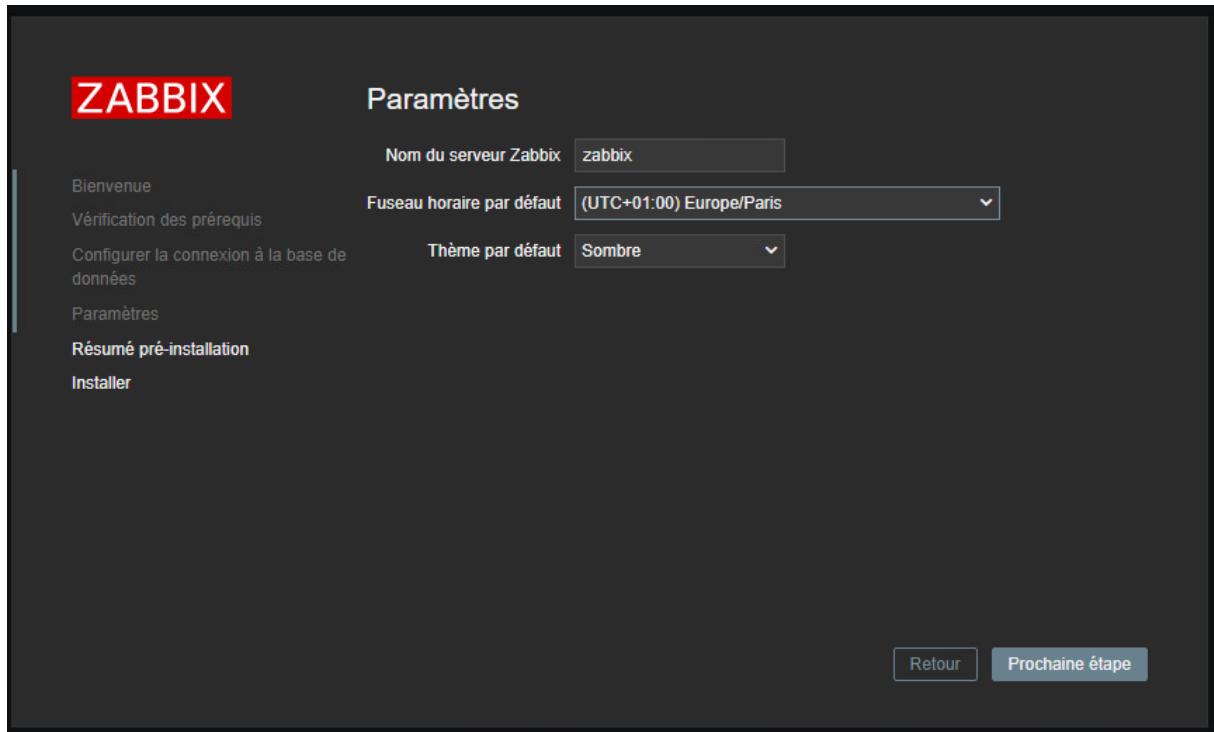
Mot de passe

Chiffrement TLS de la base de données La connexion ne sera pas chiffrée car elle utilise un fichier socket (sous Unix) ou de la mémoire partagée (Windows).

Cette étape concerne les paramètres généraux du serveur Zabbix :

- **Nom du serveur** : Nous avons défini zabbix, ce qui permet de facilement identifier cette instance dans une infrastructure où plusieurs serveurs Zabbix pourraient exister.
- **Fuseau horaire** : Europe/Paris, aligné avec notre localisation, pour garantir la cohérence des données temporelles dans les rapports et alertes.
- **Thème par défaut** : Le thème sombre a été choisi pour améliorer la lisibilité et réduire la fatigue visuelle des administrateurs qui consultent régulièrement l'interface.

Ces paramètres sont cruciaux pour personnaliser l'interface en fonction de l'environnement et des besoins des utilisateurs.



Ici, dans cette partie, un récapitulatif des configurations effectuées est affiché. Cela inclut :

- **Type et nom de la base de données.**
- **Serveur et utilisateur associés à la base.**
- **Nom du serveur Zabbix et autres paramètres.**

Cette vérification finale est indispensable pour valider que toutes les informations saisies sont correctes avant de lancer l'installation. Cela évite d'éventuelles erreurs liées à des configurations incorrectes.

**ZABBIX**

## Résumé pré-installation

Veuillez vérifier les paramètres de configuration. Si tout est correct, appuyez sur le bouton "Prochaine étape" ; sinon, le bouton "Retour" pour changer les paramètres.

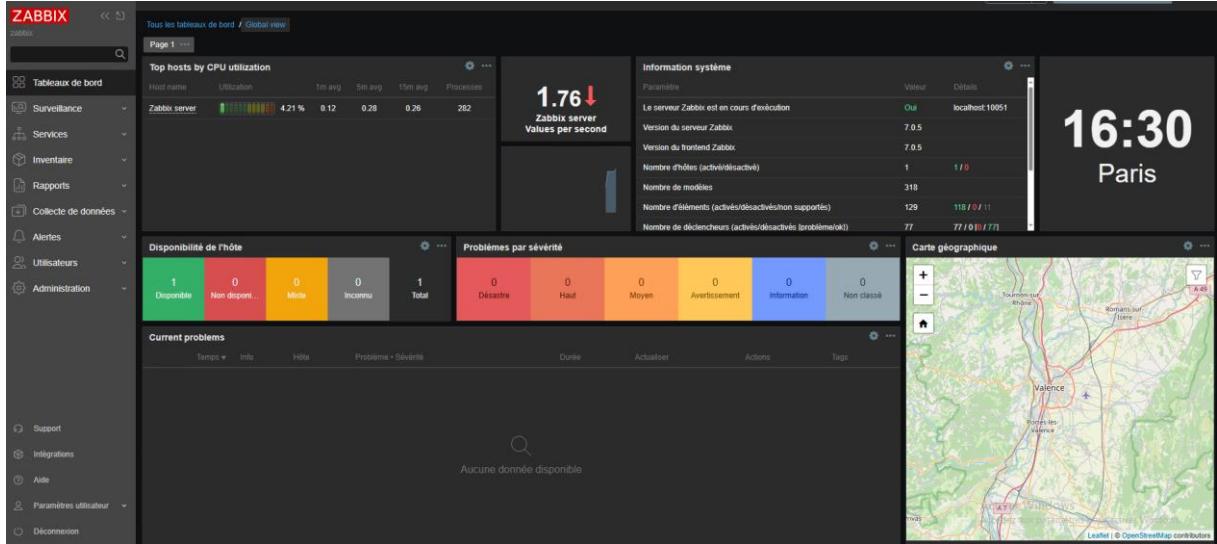
Bienvenue	Type de base de données	MySQL
Vérification des prérequis	Serveur base de données	localhost
Configurer la connexion à la base de données	Port de la base de données	défaut
Paramètres	Nom de la base de données	zabbix
Résumé pré-installation	Utilisateur base de données	zabbix
Installer	Mot de passe utilisateur de la base de données	*****
	Chiffrement TLS de la base de données	false
	Nom du serveur Zabbix	zabbix

[Retour](#) [Prochaine étape](#)

Après l'installation, nous accédons à l'interface de connexion. Par défaut, l'identifiant Admin et son mot de passe initial sont utilisés. Cela permet de s'assurer que l'installation a réussi et que l'interface est fonctionnelle. Une fois connectés, nous pouvons modifier les paramètres de sécurité (changer le mot de passe d'Admin) et commencer à configurer le serveur pour la surveillance.



Le tableau de bord Zabbix affiche ici les principales métriques du serveur, telles que l'utilisation CPU, les informations système, et une carte géographique pour visualiser les hôtes surveillés. Cette configuration est conçue pour offrir une interface visuelle claire et efficace permettant une surveillance en temps réel des performances et des incidents, favorisant ainsi une gestion proactive des systèmes.



Lors de la création d'un nouvel hôte DNS, nous avons configuré le nom "zabbix", le FQDN complet "zabbix.DOMAD107.peda" et son adresse IP associée. L'activation de l'enregistrement PTR garantit que la résolution DNS inverse est opérationnelle. Ce choix est essentiel pour permettre une gestion fluide des hôtes au sein du réseau et éviter tout problème de compatibilité ou de recherche.

**Nouvel hôte**

Nom (utilise le domaine parent si ce champ est vide) :

Nom de domaine pleinement qualifié (FQDN) :

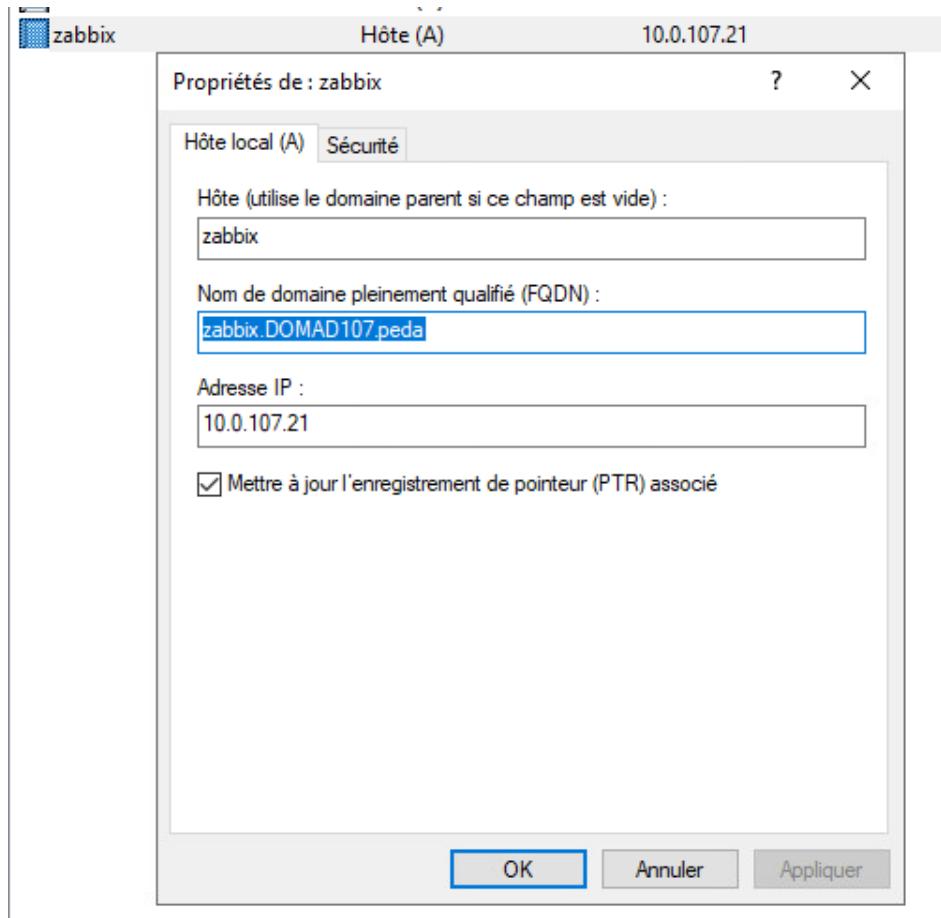
Adresse IP :

Créer un pointeur d'enregistrement PTR associé

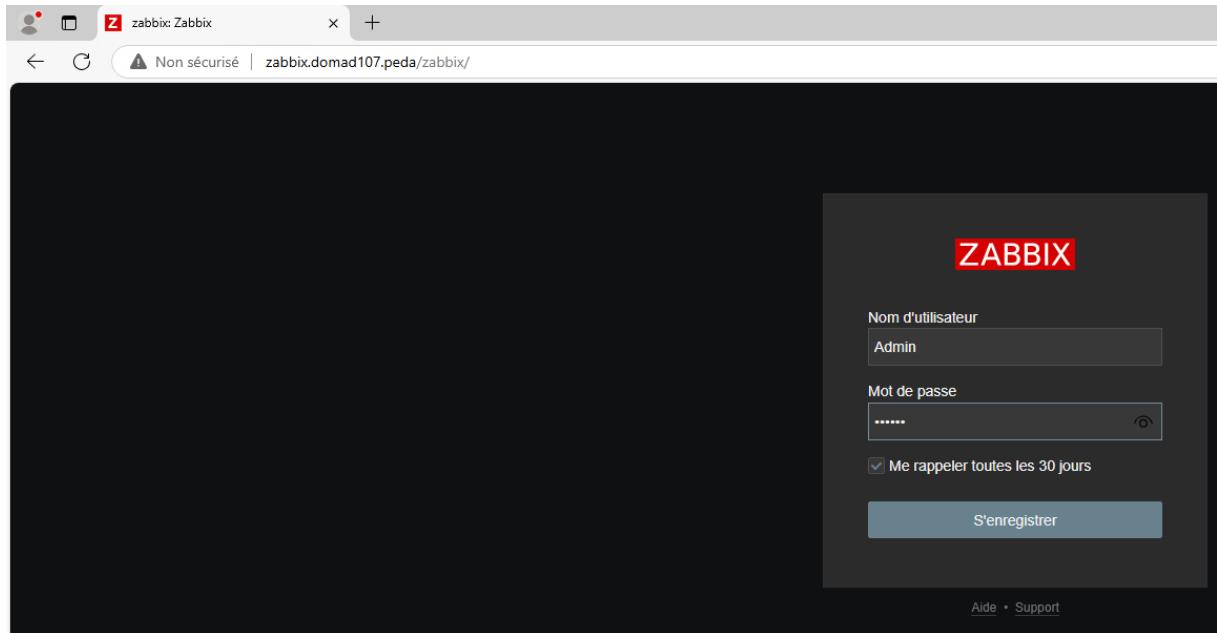
Autoriser tout utilisateur identifié à mettre à jour les enregistrements DNS avec le même nom de propriétaire

**Ajouter un hôte** **Annuler**

Une fois l'hôte configuré, les propriétés sont vérifiées dans l'interface DNS. L'adresse IP et le FQDN sont confirmés, et la case permettant la mise à jour des enregistrements PTR reste cochée. Cela garantit que toute modification future sera automatiquement synchronisée, minimisant ainsi les erreurs potentielles dans les résolutions DNS.



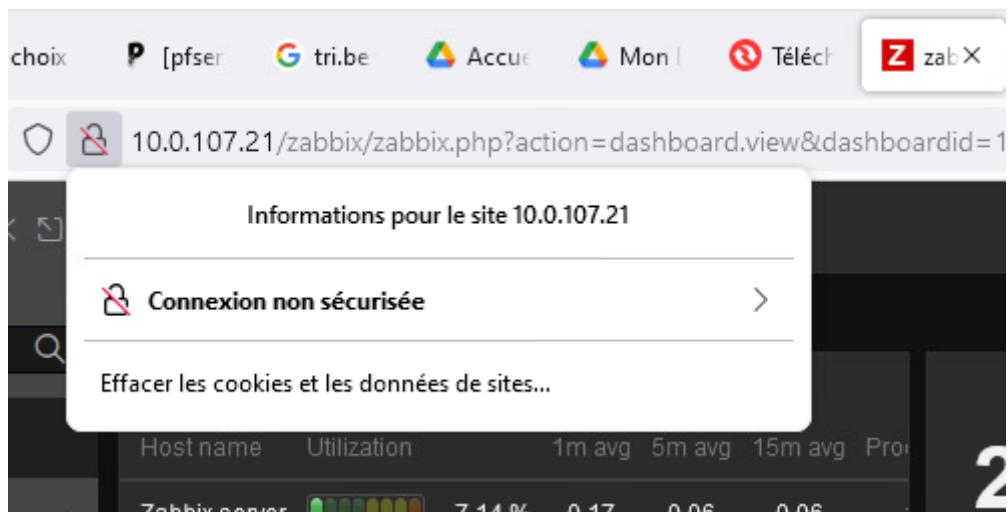
L'accès à l'interface frontend de Zabbix via "zabbix.domad107.peda" est une pratique standard permettant une meilleure gestion des accès. Utiliser un nom de domaine, plutôt qu'une adresse IP brute, facilite l'accès pour les administrateurs et rend l'interface plus professionnelle. Toutefois, l'absence de certificat SSL à ce stade entraîne l'affichage d'une alerte "non sécurisé", soulignant la nécessité de sécuriser le serveur.



Pour renforcer la sécurité des communications, un certificat SSL a été configuré et activé via Apache. Ce processus chiffre les échanges entre les utilisateurs et le serveur, protégeant ainsi les données contre les interceptions. Cette étape est primordiale pour garantir un environnement sécurisé et conforme aux meilleures pratiques en matière de cybersécurité, surtout lorsque des informations sensibles comme des identifiants de connexion sont en jeu.

### Création d'un certificat SSL dans apache 2

Pour vérifier l'état de la connexion au serveur Zabbix, nous utilisons un navigateur comme Mozilla Firefox ou Google Chrome. Le navigateur signale ici une connexion non sécurisée, car le protocole HTTP est utilisé sans certificat SSL valide. Ce manque de configuration SSL expose des risques importants en matière de cybersécurité, notamment l'interception de données sensibles transmises entre le client et le serveur (attaque de type man-in-the-middle). Cela souligne l'importance de mettre en place un certificat SSL et de basculer vers HTTPS pour garantir la confidentialité et l'intégrité des communications.



Nous activons le module SSL d'Apache avec la commande a2enmod ssl, suivie par l'activation de la configuration par défaut avec a2ensite default-ssl. Cela permet de préparer le serveur à utiliser le protocole HTTPS. Ensuite, nous redémarrons le service Apache avec systemctl restart apache2 pour appliquer les modifications. Cette étape est essentielle pour sécuriser les connexions entre le serveur et les clients en cryptant les communications.

```
root@zabbix:/home/zabbix# a2enmod ssl
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create
elf-signed certificates.
To activate the new configuration, you need to run:
  systemctl restart apache2
root@zabbix:/home/zabbix# a2ensite default-ssl
Enabling site default-ssl.
To activate the new configuration, you need to run:
  systemctl reload apache2
root@zabbix:/home/zabbix# service apache2
Usage: apache2 {start|stop|graceful-stop|restart|reload|force-reload}
root@zabbix:/home/zabbix# service apache2 reload
root@zabbix:/home/zabbix#
```

Après avoir activé le module SSL et la configuration par défaut, nous exécutons service apache2 reload pour recharger Apache et appliquer les changements sans interrompre les connexions en cours. Cela garantit que les modifications liées au SSL sont prises en compte immédiatement.

```
root@zabbix:/home/zabbix# service apache2 reload
```

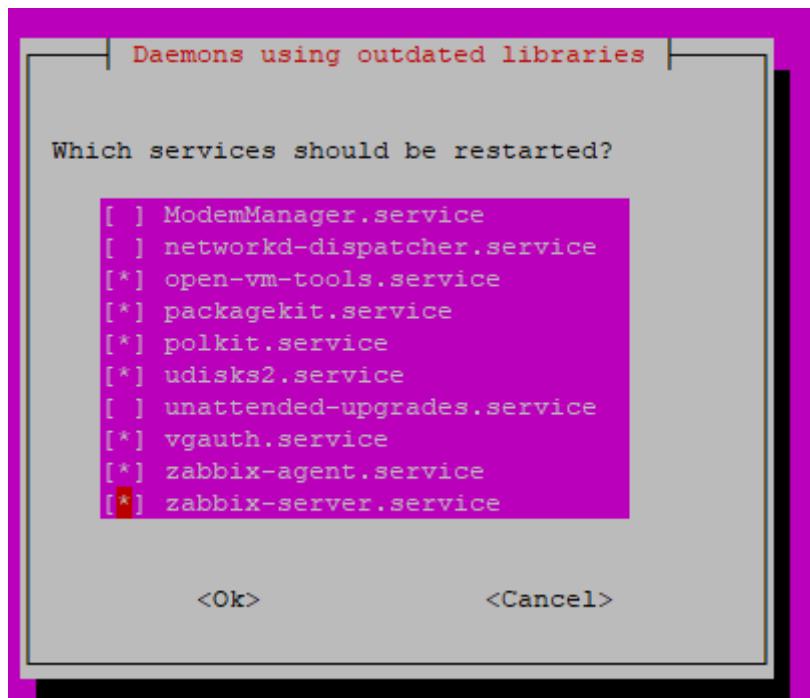
Nous installons les outils NSS avec sudo apt install libnss3-tools. Ces outils sont nécessaires pour générer et gérer des certificats SSL localement, particulièrement dans des environnements de développement ou de tests.

```
root@zabbix:/home/zabbix/mkcert# sudo apt install libnss3-tools
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
libnss3-tools est déjà la version la plus récente (2:3.98-0ubuntu0.22.04.2).
0 mis à jour, 0 nouvellement installés, 0 à enlever et 115 non mis à jour.
root@zabbix:/home/zabbix/mkcert#
```

Nous clonons le projet mkcert à partir de GitHub en exécutant git clone <https://github.com/FiloSottile/mkcert> puis nous naviguons dans le répertoire avec cd mkcert. Cet outil est choisi pour simplifier la génération de certificats SSL auto-signés, car il est facile à configurer et s'intègre bien avec les systèmes modernes.

```
root@zabbix:/home/zabbix/mkcert# git clone https://github.com/FiloSottile/mkcert && cd mkcert
Cloning into 'mkcert'...
remote: Enumerating objects: 775, done.
remote: Counting objects: 100% (307/307), done.
remote: Compressing objects: 100% (87/87), done.
remote: Total 775 (delta 236), reused 221 (delta 220), pack-reused 468 (from 1)
Receiving objects: 100% (775/775), 1.79 MiB | 8.28 MiB/s, done.
Resolving deltas: 100% (374/374), done.
```

Cette étape permet de redémarrer les services affectés par une mise à jour des bibliothèques. Nous sélectionnons les services essentiels comme zabbix-agent et zabbix-server pour appliquer les mises à jour et garantir leur bon fonctionnement. Cela évite que ces services utilisent d'anciennes versions des bibliothèques en mémoire. Après sélection, nous validons avec "OK" pour assurer la stabilité du système.



Nous compilons mkcert en utilisant Go avec la commande go build -ldflags "-X main.Version=\$(git describe --tags)". Cette étape assure que l'outil est correctement configuré et prêt à être utilisé. Si des dépendances manquent, comme indiqué dans la capture, elles peuvent être ajoutées en utilisant les outils fournis par Go.

```
^Croot@zabbix:/home/zabbix/mkcert/mkcert# 
root@zabbix:/home/zabbix/mkcert/mkcert# go build -ldflags "-X main.Version=$(git describe --tags)"
go: golang.org/x/net@v0.0.0-20220421235706-1dlef9303861 requires
    golang.org/x/sys@v0.0.0-20211216021012-1d35b9e2eb4e: missing go.sum entry; to add it:
        go mod download golang.org/x/sys
root@zabbix:/home/zabbix/mkcert/mkcert# 
```

Nous générerons un certificat SSL en exécutant mkcert zabbix.DOMAD107.peda. Cette commande crée un certificat et une clé privée pour sécuriser le domaine spécifié. Le certificat est sauvegardé dans des fichiers .pem, comme mentionné dans la sortie de la commande. Ces certificats seront utilisés par Apache pour activer les connexions sécurisées.

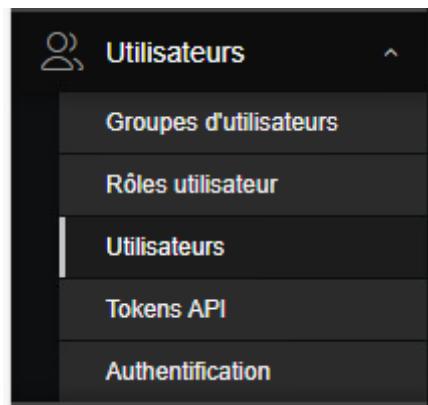
```
root@zabbix:/home/zabbix/mkcert/mkcert# mkcert "zabbix.DOMAD107.peda"
Created a new local CA 🌐
Note: the local CA is not installed in the system trust store.
Run "mkcert -install" for certificates to be trusted automatically ✅

Created a new certificate valid for the following names 🌐
- "zabbix.DOMAD107.peda"

The certificate is at "./zabbix.DOMAD107.peda.pem" and the key at "./zabbix.DOMAD107.peda-key.pem" ✅
It will expire on 27 February 2027 🕰️

root@zabbix:/home/zabbix/mkcert/mkcert# 
```

Le menu "Utilisateurs" offre un accès direct à la gestion des comptes, des groupes et des rôles. Il permet de définir les permissions des utilisateurs, par exemple en assignant des rôles comme "Super admin" pour une gestion complète ou "Guest" pour un accès restreint. Cette étape est fondamentale pour sécuriser l'interface et limiter les actions aux personnes autorisées.



La liste des utilisateurs configurés présente des informations essentielles : rôles, groupes associés et statut de connexion. On remarque ici que l'utilisateur "Admin" est actif avec des droits complets, tandis que "Guest" a des permissions limitées. Cette vue facilite le suivi des sessions actives et garantit une administration centralisée.

Nom d'utilisateur	Prénom	Nom de famille	Rôle utilisateur	Groupes	Est connecté ?	Connexion	Accès à l'interface	Accès API	Mode debug	État
Admin	Zabbix	Administrator	Super admin role	Internal, Zabbix administrators	Oui (18/11/2024 17:05:29)	Ok	Interne	Activé	Désactivé	Activé
guest			Guest role	Disabled, Guests, Internal	Non	Ok	Interne	Désactivé	Désactivé	Désactivé

Créer un utilisateur dédié dans Zabbix est une étape cruciale pour garantir la sécurité et une gestion efficace des accès. Dans un environnement critique, il est essentiel que chaque utilisateur dispose de droits strictement adaptés à ses responsabilités. Cela minimise les risques de modifications non intentionnelles ou malveillantes et assure un suivi précis des actions via les journaux d'audit. La création d'un utilisateur avec des permissions bien définies permet également d'assurer une gestion centralisée et cohérente, essentielle dans un système comme Zabbix.



### 1. Saisie des informations de base

Lors de la création d'un utilisateur, nous renseignons le **Nom d'utilisateur**, le **Prénom** et le **Nom de famille**. Ces informations permettent d'identifier chaque utilisateur de manière claire et unique dans le système. Une identification précise est essentielle pour maintenir la traçabilité et une gestion structurée.

### 2. Attribution des groupes

Nous associons l'utilisateur au groupe **Zabbix administrators** en le sélectionnant dans le champ **Groupes**. Cette étape est essentielle pour lui attribuer les droits nécessaires à l'administration du système. En segmentant les permissions par groupe, nous garantissons que chaque utilisateur n'a accès qu'aux fonctionnalités pertinentes, ce qui limite les risques d'accès non autorisé.

### 3. Définition du mot de passe

Un mot de passe robuste est défini et confirmé pour sécuriser l'accès. Cette configuration protège l'interface Zabbix contre des intrusions, garantissant que seuls les utilisateurs autorisés peuvent se connecter. Utiliser des mots de passe forts est une bonne pratique de sécurité, surtout dans des environnements critiques.

### 4. Personnalisation des préférences utilisateur

Les préférences sont configurées pour répondre aux besoins de l'utilisateur :

- La **Langue** est définie sur Français, garantissant une interface compréhensible.
- Le **Fuseau horaire** est réglé sur (UTC+01:00 Europe/Paris), assurant une synchronisation correcte des données et des alertes avec la localisation de l'utilisateur.

- Le **Thème sombre** est choisi pour un confort visuel optimal, particulièrement utile dans des environnements de faible luminosité.

**Utilisateurs**

Utilisateur Média Permissions

\* Nom d'utilisateur: Reeth92SIO  
 Prénom: Reeth92  
 Nom de famille: Reeth  
 Groupes: Zabbix administrators

\* Mot de passe:

\* Mot de passe (une autre fois):

Le mot de passe n'est pas obligatoire pour le type d'authentification non interne.

Langue: Français (fr\_FR)

Fuseau horaire: (UTC+01:00) Europe/Paris

Thème: Sombre

Connexion automatique:

Auto-déconnexion:  15m

\* Rafraîchir: 30s

\* Lignes par page: 50

URL (après connexion):

Dans l'interface utilisateur de Zabbix, nous avons configuré les permissions d'accès pour un nouvel utilisateur. Le rôle "Admin role" a été sélectionné, ce qui accorde des droits avancés sur toutes les sections critiques, notamment les tableaux de bord, la collecte de données, les alertes, et les services. Cette configuration garantit que cet utilisateur peut superviser et intervenir sur des éléments essentiels, tout en respectant une organisation claire des responsabilités. L'attribution de permissions spécifiques, comme l'accès en lecture-écriture aux services, vise à maintenir un contrôle précis sur les fonctionnalités critiques.

Nous avons associé l'utilisateur au groupe "Zabbix administrators". Ce choix, réalisé via un menu déroulant, permet de regrouper les utilisateurs ayant des responsabilités similaires. Cela simplifie la gestion des permissions en appliquant des paramètres prédéfinis à tous les membres d'un même groupe. Cette méthode est particulièrement utile dans les environnements complexes où plusieurs administrateurs doivent collaborer.

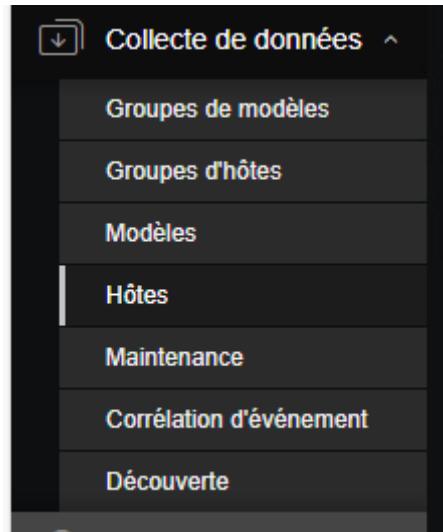
Une fois toutes les configurations terminées, l'utilisateur est ajouté au système. La liste des utilisateurs affiche désormais les informations principales, telles que le groupe, le rôle, et l'état de connexion. La vérification de ces paramètres garantit que l'utilisateur est correctement configuré avant d'accéder à l'interface. La présence de l'utilisateur dans la liste avec un statut "Actif" confirme que la création a été effectuée avec succès.

## 5. Finalisation de la création

Pour enregistrer les paramètres, nous cliquons sur le bouton **Ajouter**. L'utilisateur est ainsi créé et devient immédiatement opérationnel, avec les permissions et configurations définies. Cette étape garantit que l'accès est conforme aux politiques de sécurité et que l'utilisateur peut interagir avec les fonctionnalités de Zabbix.

### Création des groupes d'hôtes

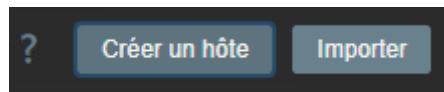
Dans le menu "Collecte de données", nous configurons les paramètres de surveillance, comme les groupes d'hôtes ou les modèles. Cette section est clé pour organiser les données à surveiller et adapter la supervision selon le contexte. Par exemple, on peut créer des modèles spécifiques pour des environnements réseau complexes.



Le tableau des hôtes affiche une vue détaillée des entités surveillées, incluant l'état, la disponibilité et les interfaces. Ici, l'hôte "Zabbix server" est configuré avec le modèle "Linux by Zabbix agent" et est opérationnel. Cette configuration garantit que les métriques sont correctement collectées et analysées pour une supervision optimale.

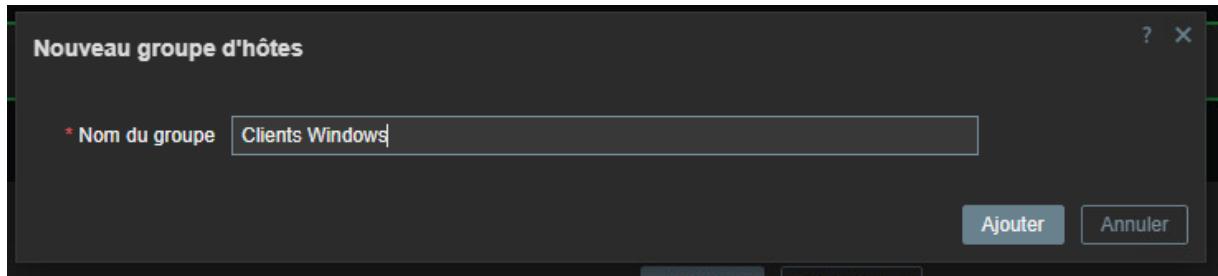
Cette organisation structurée améliore la sécurité, la surveillance et l'efficacité de la gestion dans Zabbix. Chaque étape a son importance pour assurer une supervision fiable et personnalisée.

La première capture montre l'interface permettant de gérer les hôtes, avec les boutons **Créer un hôte** et **Importer**. Pour ajouter un nouvel hôte à surveiller, il faut cliquer sur le bouton "Créer un hôte". Cette étape est essentielle pour inclure de nouvelles machines ou serveurs dans la gestion Zabbix. L'option "Importer" permet de configurer plusieurs hôtes rapidement via un fichier de configuration.

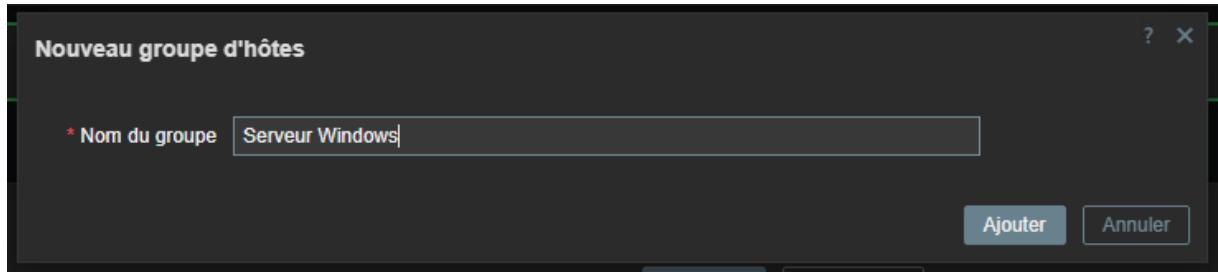


Dans la deuxième capture, la section **Collecte de données** est ouverte, montrant les options disponibles, comme **Groupes de modèles**, **Groupes d'hôtes**, etc. Nous sélectionnons "Groupes d'hôtes" pour organiser les hôtes selon leur type ou rôle. Cette hiérarchisation améliore la gestion et facilite le ciblage spécifique lors de la surveillance ou du dépannage.

Une nouvelle fenêtre s'ouvre pour créer un groupe appelé **Clients Windows**. Nommer un groupe en fonction du type d'hôtes permet de structurer les ressources surveillées, facilitant l'identification et la configuration de règles adaptées. Cela répond également aux besoins d'une gestion granulaire et spécifique des hôtes.



De la même manière, un autre groupe est créé pour les **Serveurs Windows**. Cette distinction est cruciale pour appliquer des modèles de surveillance spécifiques (par exemple, une stratégie différente pour serveurs et postes de travail). Une bonne segmentation réduit les risques d'erreur et garantit une surveillance optimisée.



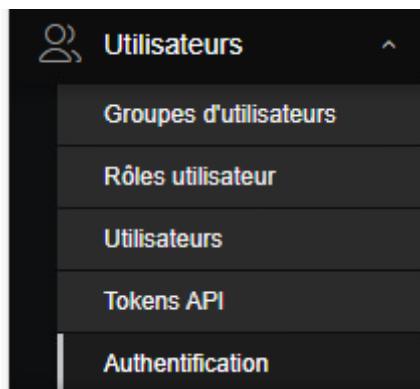
La dernière capture illustre la liste complète des groupes d'hôtes, incluant ceux créés précédemment comme **Clients Windows** et **Serveurs Windows**. Cette vue fournit un aperçu global, montrant quels groupes contiennent des hôtes actifs et simplifiant la navigation. Les groupes préexistants comme **Linux Servers** ou **Databases** sont également visibles, soulignant l'importance d'une classification cohérente pour une gestion efficace.

Group	Host	Status
Clients Windows	UT107-AdminW10	Active
Serveur Windows	SRV1-DC107	Active
Zabbix servers	Zabbix server	Active

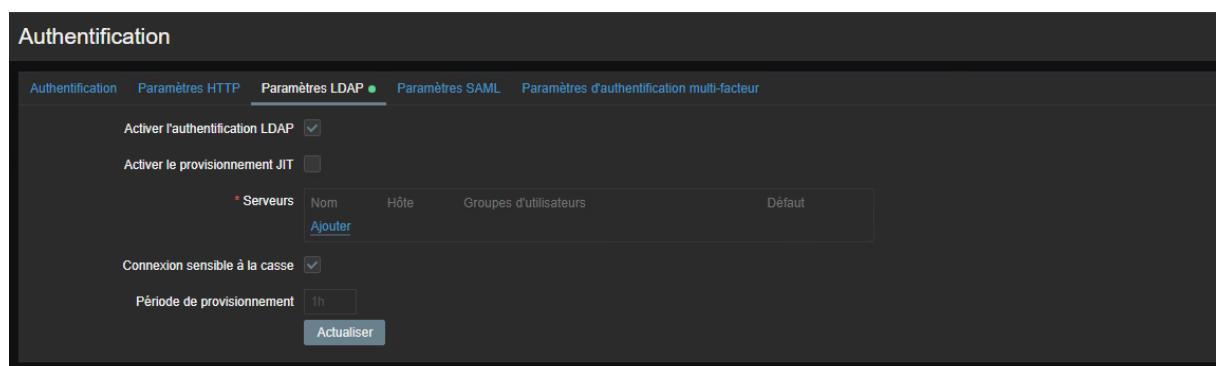
Avantages de ce choix :

- **Une Organisation structurée** : Les groupes d'hôtes permettent de gérer facilement un grand nombre de machines. Par exemple, un groupe "Clients Windows" peut recevoir des modèles spécifiques pour surveiller les performances des postes de travail.
- **Clarté et flexibilité** : Classer les hôtes en groupes évite le désordre, particulièrement dans les environnements complexes avec de nombreuses entités à surveiller.
- **Évolutivité** : Avec une structure modulaire comme celle-ci, il est possible d'ajouter de nouveaux groupes ou hôtes sans désorganiser l'ensemble.

## Authentification et LDAP



Dans la section **Paramètres LDAP**, l'option "Activer l'authentification LDAP" est cochée pour démarrer la configuration. Cette étape prépare Zabbix à communiquer avec un serveur LDAP pour valider les connexions utilisateur. Cela offre une gestion centralisée des identités, réduisant ainsi la nécessité de gérer des comptes localement.



Un nouveau serveur est ajouté en cliquant sur **Ajouter** sous l'onglet des serveurs. Nous précisons l'adresse du serveur LDAP, ici **ldap://10.0.107.1**, ainsi que le nom de l'hôte. Aucune association de groupe d'utilisateurs n'est définie pour cette configuration spécifique. Cette étape est cruciale pour établir la connexion entre Zabbix et l'annuaire LDAP afin de synchroniser les identités.

Nouveau serveur LDAP

* Nom	Idap://10.0.107.1
* Hôte	Idap
* Port	389
* DN de base	dc=DOMAD107,dc=peda
* Attribut recherché	sAMAccountName
DN de lien	Idap@DOMAD107.peda
Mot de passe de lien	*****
Description	
<input type="checkbox"/> Configurer le provisionnement JIT	
<b>Configuration avancée</b>	
<input type="button" value="Ajouter"/> <input type="button" value="Test"/> <input type="button" value="Annuler"/>	

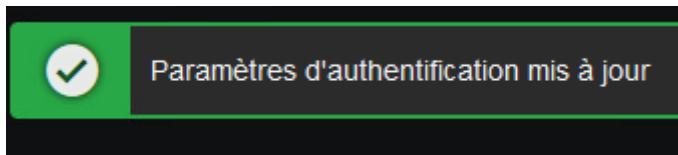
L'option "Connexion sensible à la casse" est activée pour garantir que les noms d'utilisateur soient traités avec exactitude, en respectant les majuscules et minuscules. La période de provisionnement est configurée sur 1 heure, ce qui signifie que les informations d'authentification seront actualisées automatiquement à intervalles réguliers. Ces réglages améliorent la précision et la fluidité des connexions utilisateur.

Authentification

Authentification	Paramètres HTTP	Paramètres LDAP	Paramètres SAML	Paramètres d'authentification multi-facteur															
Activer l'authentification LDAP <input checked="" type="checkbox"/>																			
Activer le provisionnement JIT <input type="checkbox"/>																			
<table border="1"> <thead> <tr> <th>* Serveurs</th> <th>Nom</th> <th>Hôte</th> <th>Groupes d'utilisateurs</th> <th>Défaut</th> </tr> </thead> <tbody> <tr> <td></td> <td>Idap://10.0.107.1</td> <td>Idap</td> <td>0</td> <td><input checked="" type="radio"/></td> </tr> <tr> <td></td> <td><a href="#">Ajouter</a></td> <td></td> <td></td> <td><a href="#">Supprimer</a></td> </tr> </tbody> </table>					* Serveurs	Nom	Hôte	Groupes d'utilisateurs	Défaut		Idap://10.0.107.1	Idap	0	<input checked="" type="radio"/>		<a href="#">Ajouter</a>			<a href="#">Supprimer</a>
* Serveurs	Nom	Hôte	Groupes d'utilisateurs	Défaut															
	Idap://10.0.107.1	Idap	0	<input checked="" type="radio"/>															
	<a href="#">Ajouter</a>			<a href="#">Supprimer</a>															
Connexion sensible à la casse <input checked="" type="checkbox"/>																			
Période de provisionnement <input type="text" value="1h"/>	<input type="button" value="Actualiser"/>																		

Après avoir configuré le serveur et validé les réglages, la notification « Paramètres d'authentification mis à jour » confirme que l'opération est réussie. Cette étape de validation garantit que les modifications sont prises en compte par le système et prêtes à être utilisées. La

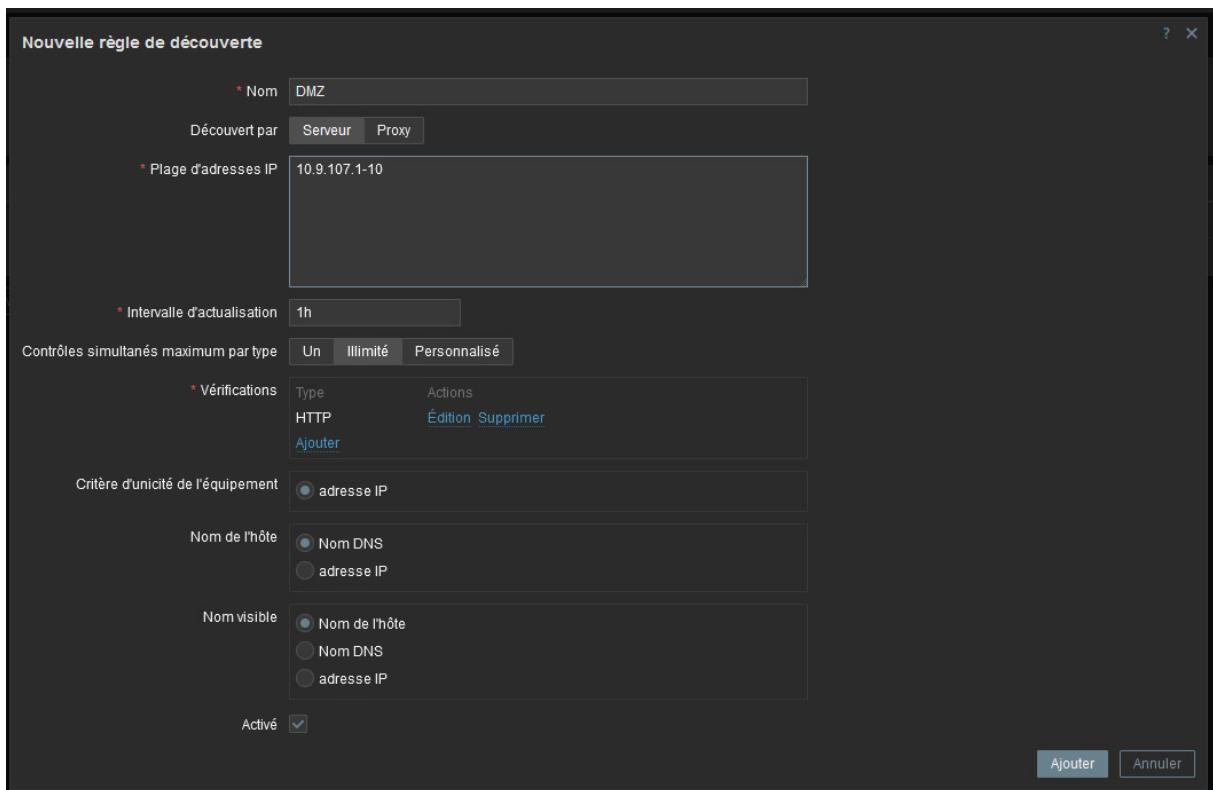
période de provisionnement, ici définie à 1 heure, permet d'automatiser la synchronisation des données utilisateur, ce qui est pratique pour maintenir l'actualisation.



Elle garantit que les utilisateurs peuvent désormais s'authentifier via LDAP, centralisant ainsi leur gestion des accès.

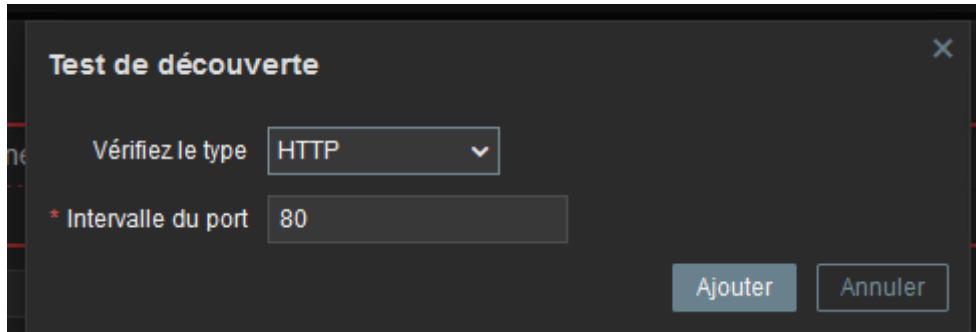
### Règle de découverte

Lors de la création de la règle de découverte, elle a été nommée "DMZ" pour représenter clairement la zone concernée. Une plage d'adresses IP spécifique, allant de 10.9.107.1 à 10, a été définie afin de cibler les équipements situés dans la zone démilitarisée (DMZ) du réseau. L'intervalle d'actualisation a été configuré sur une heure, ce qui garantit que Zabbix recherche périodiquement de nouveaux hôtes dans cette plage IP tout en minimisant la charge sur le réseau. Cette étape permet de restreindre la portée de la découverte aux seules ressources pertinentes de la DMZ, optimisant ainsi les performances.

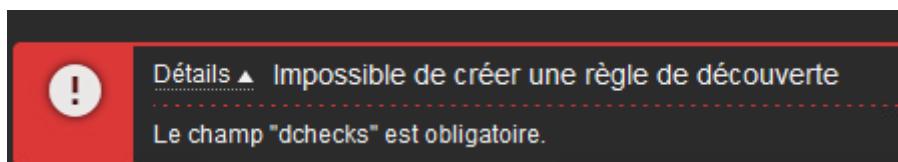


Une vérification HTTP a été spécifiée pour contrôler la disponibilité des équipements dans la plage IP définie. Cette vérification, configurée pour interroger le port 80, est idéale pour vérifier la réponse des services web, souvent utilisés dans des environnements de type DMZ. Le choix du protocole HTTP permet d'assurer qu'un service critique, comme un serveur ou une

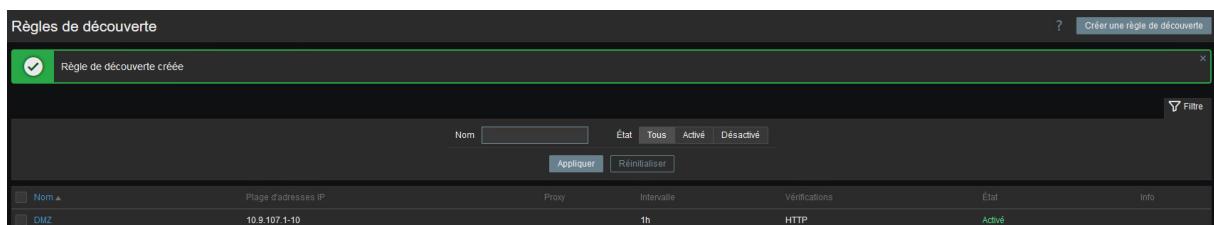
application web, est bien opérationnel. Ce paramètre est essentiel pour surveiller les hôtes clés tout en réduisant les tests inutiles sur d'autres services.



Lors de la première tentative de création de la règle, une erreur a été signalée, indiquant que le champ "dchecks" (vérifications) était obligatoire. Cela a mis en lumière une configuration incomplète où la vérification n'avait pas été correctement associée à la règle. Elle souligne fortement l'importance de vérifier la cohérence des paramètres avant de valider une règle, car une configuration incorrecte peut entraîner une inefficacité de la découverte.

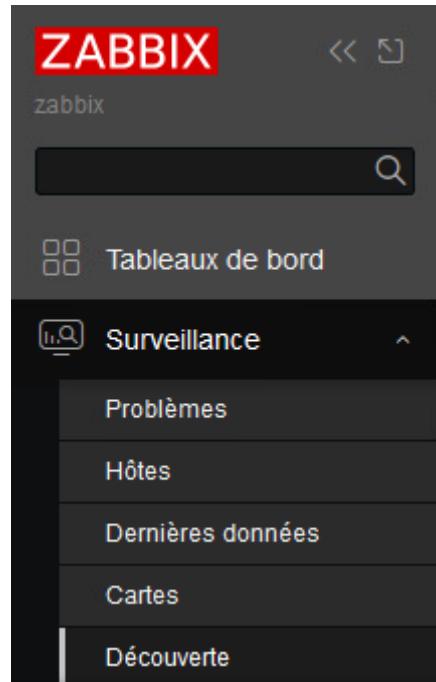


Après correction des paramètres, la règle a été validée et créée avec succès. Une confirmation verte affichée dans l'interface indique que la règle est active et prête à fonctionner. Les paramètres finaux incluent une plage IP définie, un intervalle d'actualisation de 1 heure, et une vérification HTTP active. Cette réussite confirme que le système est prêt à automatiser la découverte des hôtes dans la DMZ, assurant une surveillance continue et efficace des ressources réseau.

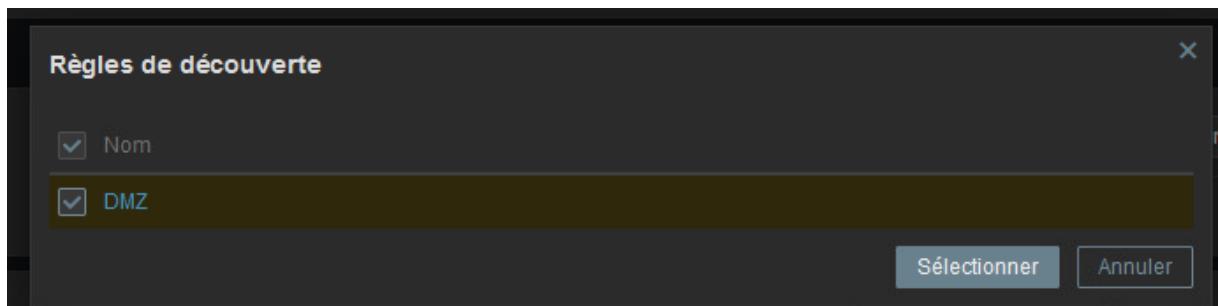


### Vérifications et application de la règle de découverte

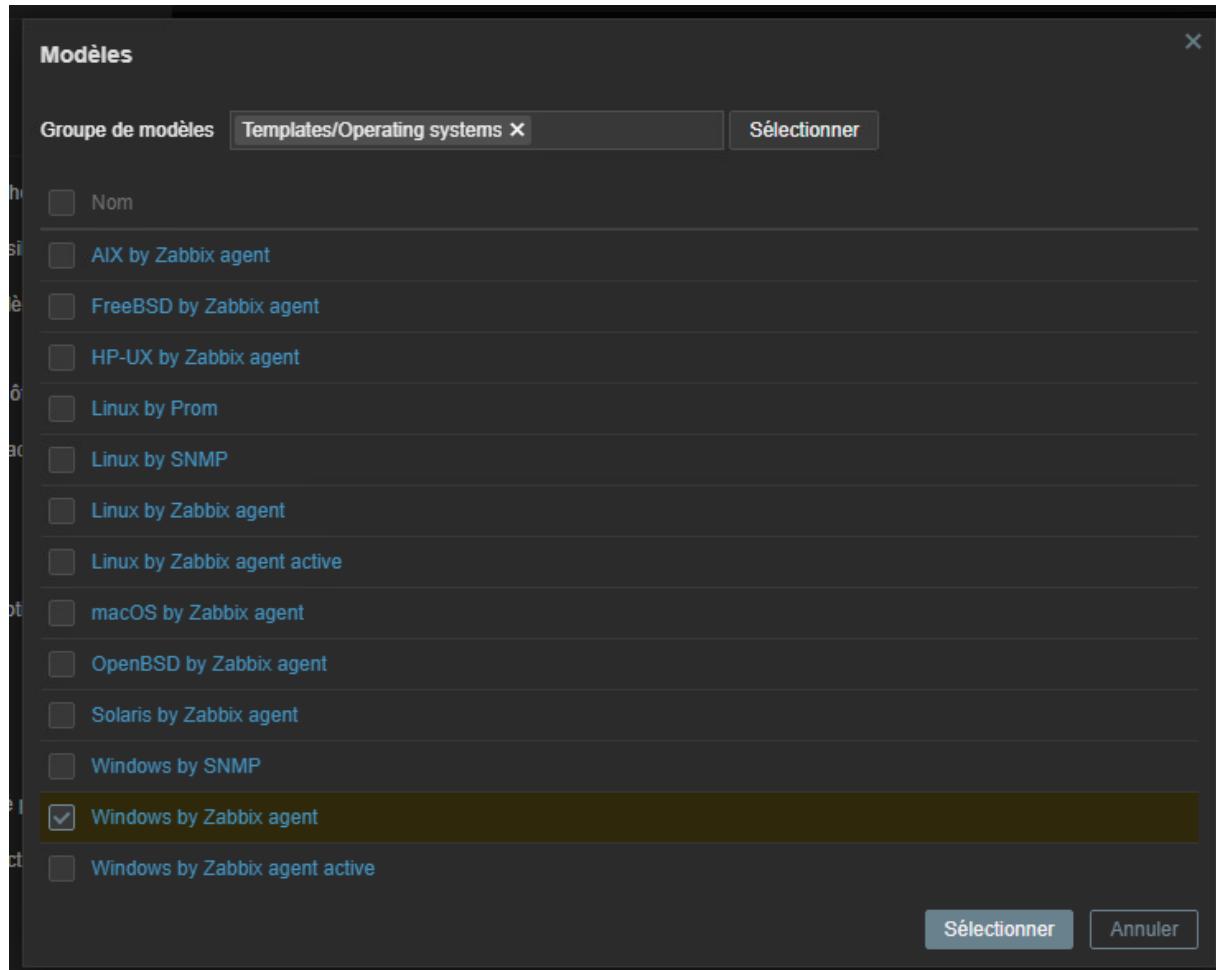
Le menu "Surveillance" de Zabbix est affiché, offrant plusieurs fonctionnalités telles que "Problèmes", "Hôtes", "Dernières données" ou encore "Découverte". Ce panneau permet de naviguer parmi les éléments de surveillance critiques, d'identifier les incidents en temps réel et de gérer les équipements surveillés. Il constitue un point de départ essentiel pour toute opération de diagnostic ou d'analyse dans Zabbix.



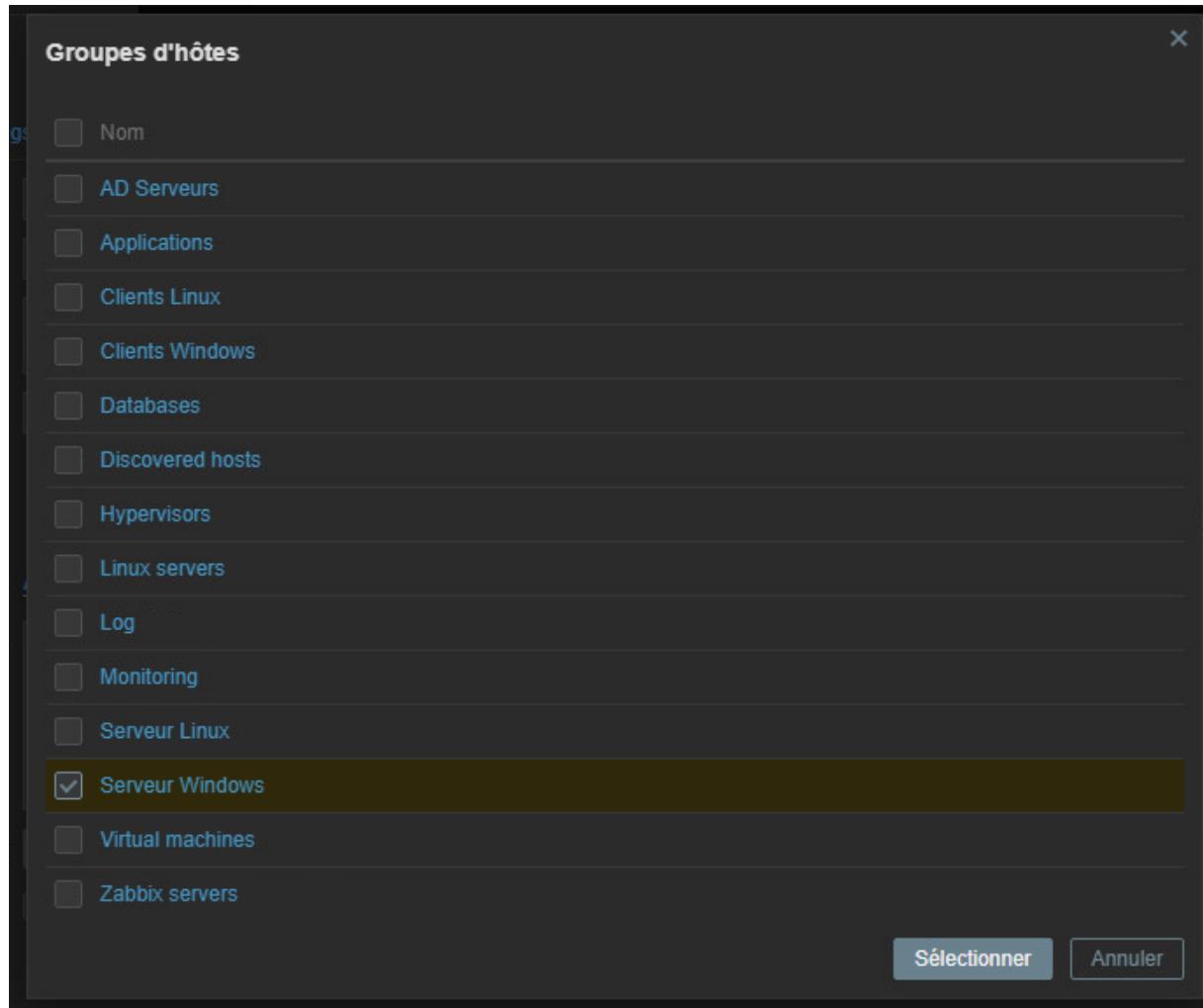
Cette capture illustre le choix de la règle de découverte "DMZ" dans la liste des règles disponibles. La sélection d'une règle existante permet d'automatiser l'identification des équipements au sein de la plage d'adresses IP configurée. Cette étape optimise la découverte des ressources et réduit les tâches manuelles associées à leur ajout.



Le modèle "Windows by Zabbix agent" est choisi pour l'hôte. Ce template inclut une configuration standardisée pour surveiller les systèmes d'exploitation Windows. Il fournit des éléments comme des métriques de performances, des déclencheurs d'alerte, et des graphiques, permettant ainsi une surveillance exhaustive des serveurs ou postes Windows.



Le groupe d'hôtes "Serveur Windows" est assigné à l'hôte. Cela facilite l'organisation des équipements en fonction de leur rôle ou type, en l'occurrence les serveurs sous Windows. Les groupes permettent également d'appliquer des configurations globales, comme des permissions ou des actions automatiques, à l'ensemble des hôtes qui leur sont associés.



Un nouvel hôte nommé "SRV1-DC107" est configuré. Les informations essentielles, telles que l'adresse IP (10.0.107.1), le port par défaut de l'agent (10050), et le modèle "Windows by Zabbix agent" sont définies. L'association au groupe "Serveur Windows" assure une catégorisation efficace pour ce serveur. Ces configurations permettent à Zabbix de collecter les données d'état et de performances de cet équipement.

Nouvel hôte

Hôte    IPMI    Tags    Macros    Inventaire    Chiffrement    Table de correspondance

\* Nom de l'hôte: SRV1-DC107

Nom visible: SRV1-DC107

Modèles: Windows by Zabbix agent

\* Groupes d'hôtes: Serveur Windows

Interfaces

Type	adresse IP	Nom DNS	Connexion à	Port	Défaut
Agent	10.0.107.1		IP	DNS	10050

Description:

Surveillé par:

Activé:

L'hôte "UTI107-AdminW10", représentant un poste de travail Windows, est configuré. L'adresse IP (10.0.107.10) et le port par défaut sont définis, et le modèle ainsi que le groupe "Clients Windows" sont assignés. Cette configuration individualisée pour les postes clients garantit une segmentation claire entre les différents types d'équipements dans le système de supervision.

Nouvel hôte

Hôte    IPMI    Tags    Macros    Inventaire    Chiffrement    Table de correspondance

\* Nom de l'hôte: UTI107-AdminW10

Nom visible: UTI107-AdminW10

Modèles: Windows by Zabbix agent

\* Groupes d'hôtes: Clients Windows

Interfaces

Type	adresse IP	Nom DNS	Connexion à	Port	Défaut
Agent	10.0.107.10		IP	DNS	10050

Description:

Surveillé par:

Activé:

Un test de connectivité est réalisé via la commande ping pour l'adresse IP 10.9.107.10. Les résultats confirment que l'hôte est accessible sur le réseau, sans perte de paquets. Cette étape

est indispensable pour valider que Zabbix peut établir une communication avec le dispositif avant d'entamer la collecte des données.

```
root@zabbix:/etc# ping 10.9.107.10
PING 10.9.107.10 (10.9.107.10) 56(84) bytes of data.
64 bytes from 10.9.107.10: icmp_seq=1 ttl=63 time=0.678 ms
64 bytes from 10.9.107.10: icmp_seq=2 ttl=63 time=0.791 ms
64 bytes from 10.9.107.10: icmp_seq=3 ttl=63 time=0.754 ms
64 bytes from 10.9.107.10: icmp_seq=4 ttl=63 time=0.627 ms
64 bytes from 10.9.107.10: icmp_seq=5 ttl=63 time=0.605 ms
^X64 bytes from 10.9.107.10: icmp_seq=6 ttl=63 time=0.757 ms
--- 10.9.107.10 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5077ms
rtt min/avg/max/mdev = 0.605/0.702/0.791/0.069 ms
root@zabbix:/etc#
```

Cette vue synthétise les informations sur les hôtes supervisés, leurs interfaces et leur disponibilité. L'état "actif" de l'hôte "SRV1-DC107" indique une surveillance opérationnelle, avec des données collectées en temps réel pour une analyse continue.

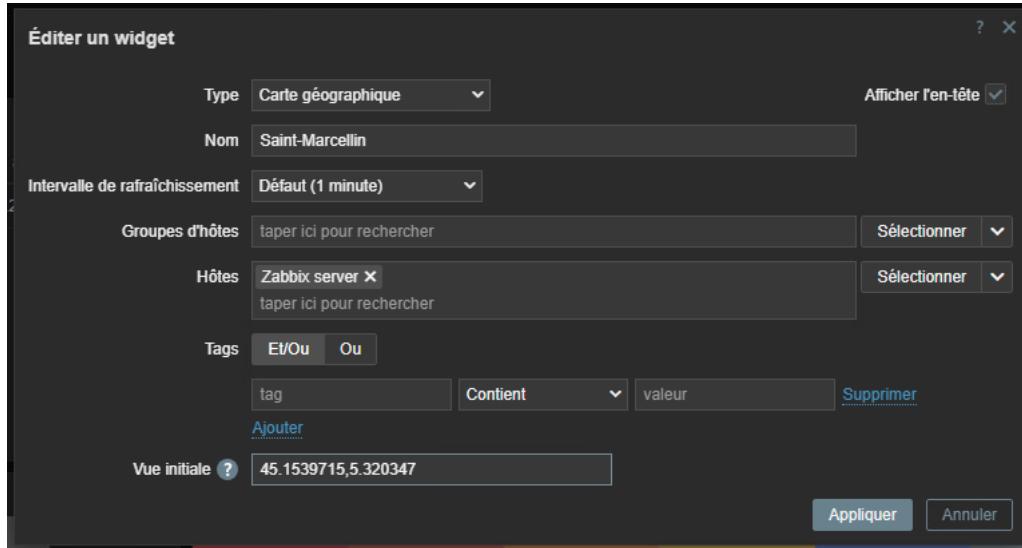
Nom	Interface	Disponibilité	Tags	État	Dernières données	Problèmes	Graphiques	Tableaux de bord	Web
SRV1-DC107	10.0.107.1:1050	<span style="background-color: green; color: white;">ZBX</span>	class: os target: windows	Activé	Dernières données 156	<span style="color: orange;">!</span>	Graphiques 32	Tableaux de bord 3	Web

La première illustration présente deux graphiques clés relatifs aux performances du disque "C:" sur l'hôte "SRV1-DC107". Le graphique supérieur analyse les longueurs moyennes des files d'attente des opérations de lecture et d'écriture, un indicateur critique pour mesurer la congestion du disque. Le graphique inférieur, quant à lui, fournit des données sur les temps moyens d'attente des requêtes de lecture et d'écriture, permettant de détecter d'éventuels goulets d'étranglement dans les entrées/sorties. Ces visualisations offrent une analyse détaillée et indispensable à l'optimisation des performances du stockage.

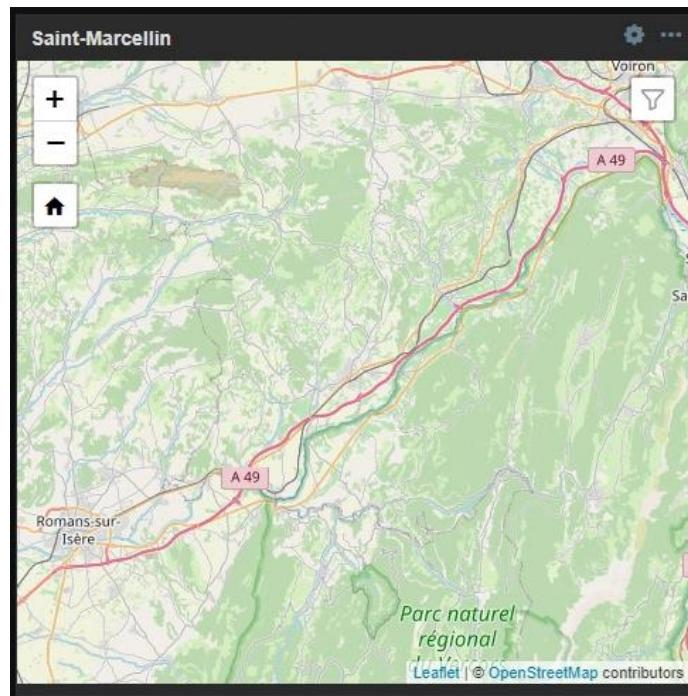


Maintenant nous allons éditer le widget de type "Carte géographique" intégré au tableau de bord Zabbix. Ce widget est configuré pour représenter visuellement les données géolocalisées de

l'hôte "Zabbix server". Les coordonnées fournies (45.1539715, 5.320347) définissent le point de vue initial de la carte, correspondant à Saint-Marcellin. L'intervalle de rafraîchissement, défini à une minute, assure une mise à jour continue des informations. Ce type de widget est particulièrement pertinent pour les infrastructures réparties géographiquement, offrant une représentation visuelle précise et une identification rapide des anomalies.



Après la configuration précédemment effectuée, la carte affiche le point géographique sélectionné, représentant Saint-Marcellin et ses environs. Cette représentation visuelle permet d'identifier rapidement la localisation des ressources surveillées. Elle est idéale pour un monitoring en temps réel des hôtes, dans le contexte d'une infrastructure répartie, en fournissant une vue claire et intuitive sur les emplacements clés.



## Tableau de bord Zabbix

Mais qu'est-ce qu'un tableau de bord sur un outil de monitoring ?

Un **tableau de bord sur Zabbix** est un ensemble d'éléments graphiques configurés pour afficher des informations de surveillance en temps réel. Zabbix collecte des données sur les performances, la disponibilité et l'état des systèmes et équipements à surveiller, comme la charge CPU, la mémoire, l'utilisation du disque ou encore les métriques réseau. Dans l'interface web de Zabbix, les utilisateurs peuvent créer des **tableaux de bord personnalisés** en ajoutant des widgets tels que des graphiques, des diagrammes, des cartes, ou des tableaux de données. Chaque widget peut être configuré pour afficher des métriques spécifiques en fonction des **hôtes** (par exemple, un serveur, un routeur, une application) et des **items** (comme la température d'un serveur ou le taux de transfert réseau). L'objectif est de donner une vue d'ensemble de l'infrastructure, permettant aux administrateurs de surveiller rapidement les performances et de réagir aux alertes. Ce tableau de bord peut aussi afficher des **triggers**, qui indiquent si des seuils critiques sont atteints et déclenchent des alertes.

Un **tableau de bord sur Grafana**, quant à lui, est principalement utilisé pour la **visualisation avancée des données**. Grafana se connecte à différentes sources de données, comme **Prometheus**, **InfluxDB**, ou **Zabbix**, pour collecter des métriques et les afficher sous forme de visualisations interactives et dynamiques. Les utilisateurs peuvent créer des **panneaux de visualisation** qui affichent des graphiques, des diagrammes circulaires, des histogrammes, des cartes de chaleur et d'autres types de données visuelles. Grafana permet une grande personnalisation de ces visualisations, offrant ainsi une flexibilité dans la manière de présenter les données en fonction des besoins spécifiques de l'utilisateur. Par exemple, un panneau peut afficher la **charge du serveur** sur plusieurs jours, tandis qu'un autre peut fournir une vue instantanée des **taux de transfert**. Grafana permet aussi de configurer des **alertes** basées sur les données visualisées, afin de notifier les utilisateurs lorsque des conditions critiques sont détectées, mais c'est dans la présentation visuelle et l'interactivité des données qu'il excelle.

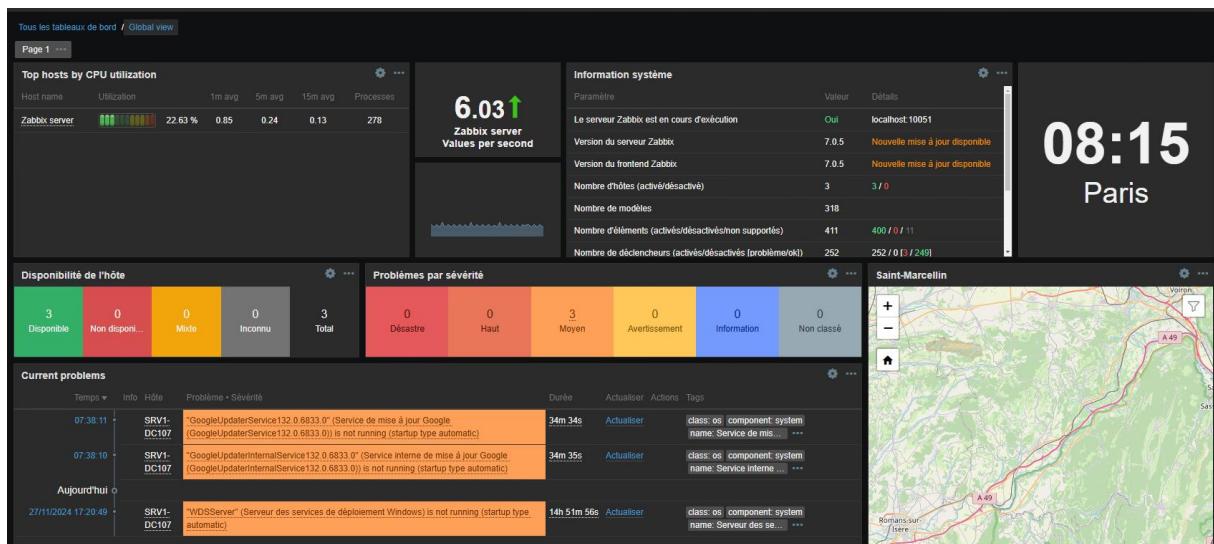
Zabbix et Grafana sont tous deux utilisés pour créer des **tableaux de bord** permettant de suivre les performances des systèmes informatiques, mais leur approche diffère. Zabbix offre une **solution tout-en-un** de surveillance, avec des alertes et des graphiques intégrés dans la plateforme, idéal pour une surveillance centralisée et une gestion des alertes. En revanche, Grafana est davantage axé sur la **visualisation avancée** et la personnalisation des données, et il est souvent utilisé comme un outil complémentaire aux systèmes de collecte de données, y compris Zabbix. Grafana permet aux utilisateurs de créer des **dashboards interactifs** et détaillés en utilisant des données provenant de plusieurs sources différentes, ce qui le rend particulièrement adapté pour une analyse approfondie et des visualisations interactives des données collectées en temps réel.

## Découverte et Configuration

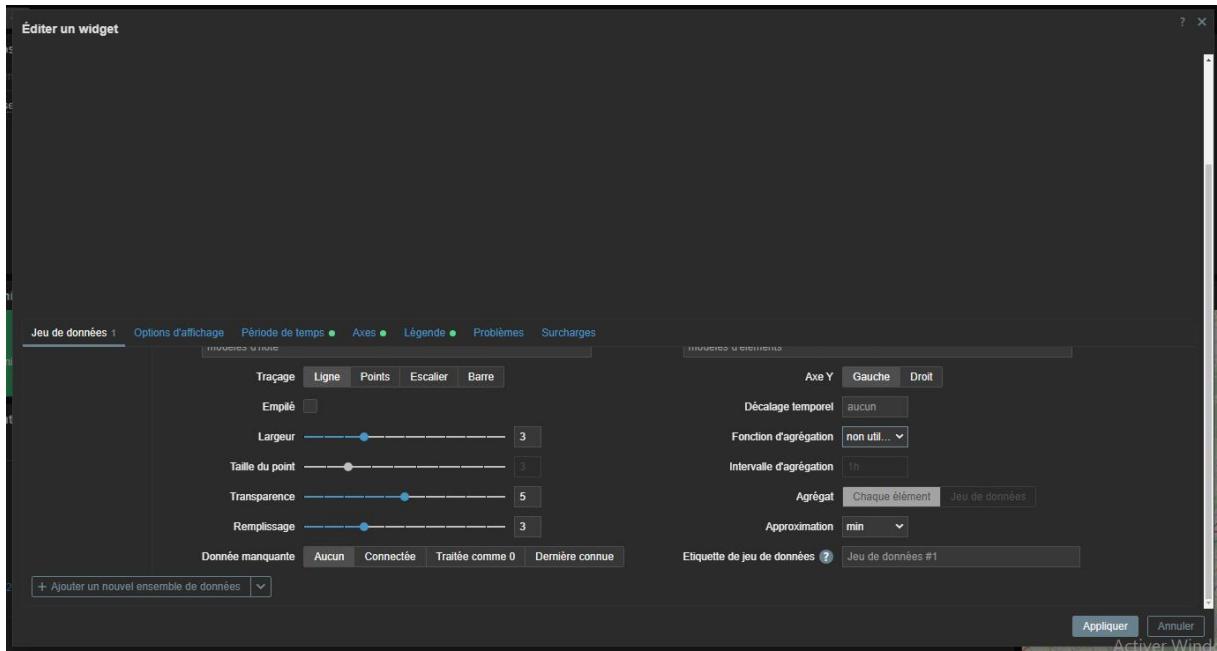
Le tableau de bord Zabbix présenté ici intègre des indicateurs clés pour une supervision en temps réel des systèmes. En haut à gauche, l'utilisation du CPU par hôte est affichée, avec des données précises sur la charge, comme celle du serveur Zabbix à 22,6 %. Cette vue permet une évaluation rapide des performances des hôtes supervisés. À droite, une section d'informations système compile des données essentielles telles que la version de Zabbix, le nombre d'hôtes actifs et les déclencheurs enregistrés, offrant une vue globale de l'état du système.

La partie centrale est consacrée à la classification des problèmes par gravité, facilitant leur hiérarchisation et la prise de décision rapide. Les sections "Disponibilité de l'hôte" et "Problèmes actuels" listent des informations précises sur les incidents détectés, comme des services non démarrés sur des machines spécifiques, accompagnés de minutages précis pour un suivi rigoureux. Ces alertes incluent également des options pour actualiser les données et confirmer si les problèmes sont résolus.

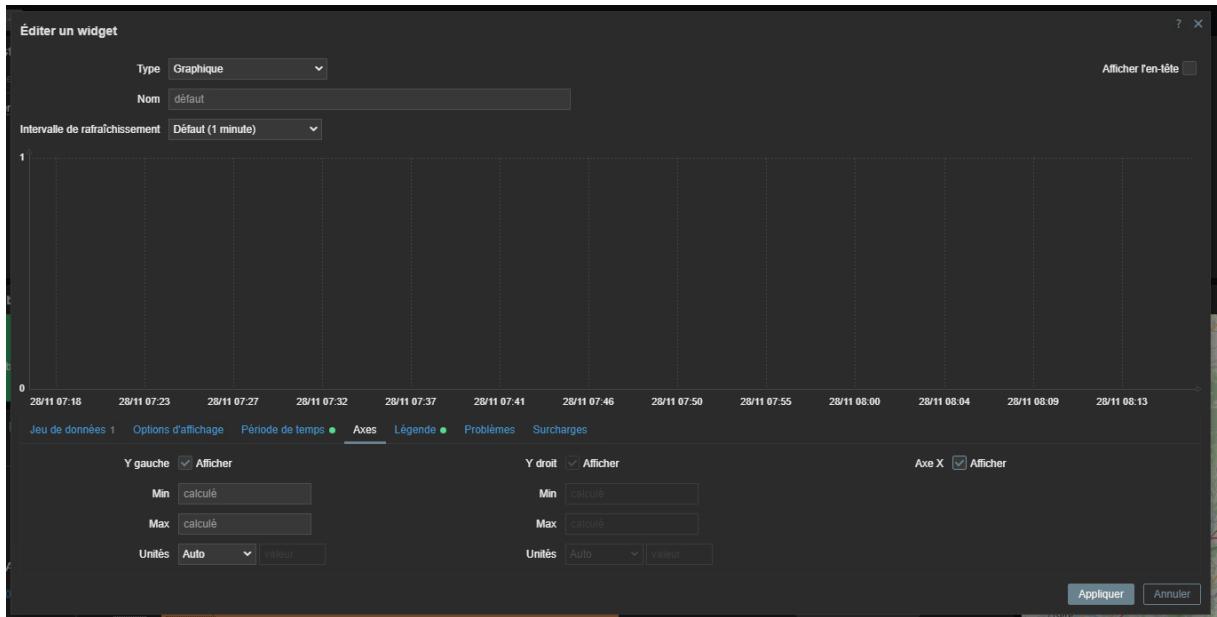
Sur la droite, une carte géographique enrichit l'expérience utilisateur en affichant les localisations des équipements ou des incidents supervisés, ici centrée sur Saint-Marcellin. Cette intégration permet de contextualiser les informations de manière visuelle, particulièrement utile dans des infrastructures distribuées. Cette organisation des widgets favorise une gestion claire et efficace des infrastructures, tout en mettant en avant les priorités.



L'interface permet de personnaliser un widget graphique avec plusieurs options. Les paramètres incluent le tracé (ligne, points, escalier, ou barre), la largeur et la transparence. Ces ajustements visent à améliorer la lisibilité et à fournir une visualisation adaptée des données collectées. Les réglages comme l'agrégation ou la gestion des données manquantes sont essentiels pour assurer une précision dans l'interprétation des données affichées, même en cas d'anomalies de collecte.



Une autre interface est dédiée au paramétrage des axes du graphique. Les limites des axes (min et max) peuvent être calculées automatiquement ou définies manuellement. Ce paramètre est indispensable pour éviter des représentations écrasées ou disproportionnées, garantissant ainsi une meilleure visibilité des variations significatives. L'ajout des unités, comme les bits ou pourcentages, rend les données plus compréhensibles pour les utilisateurs.

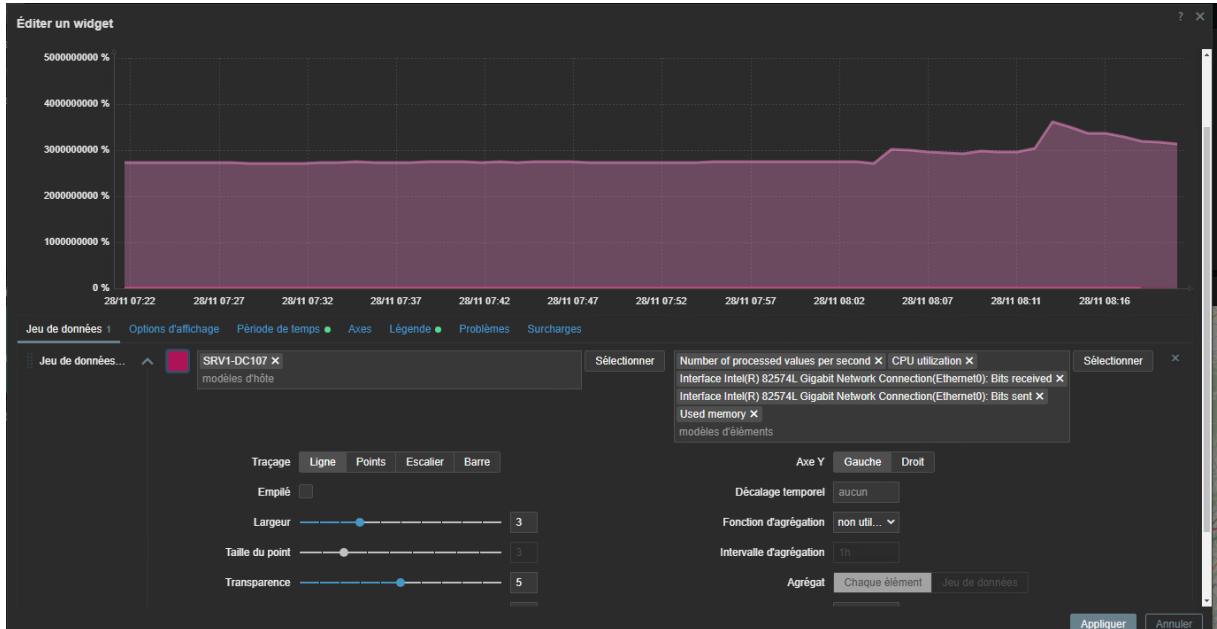


Une liste des éléments de données associés à l'hôte "SRV1-DC107" est affichée pour permettre le choix des métriques spécifiques à inclure dans le graphique. Ici, des paramètres tels que "Bits received" et "Bits sent" sur une interface réseau sont sélectionnés. Ces choix sont adaptés pour surveiller l'activité réseau, un indicateur clé pour évaluer la performance et

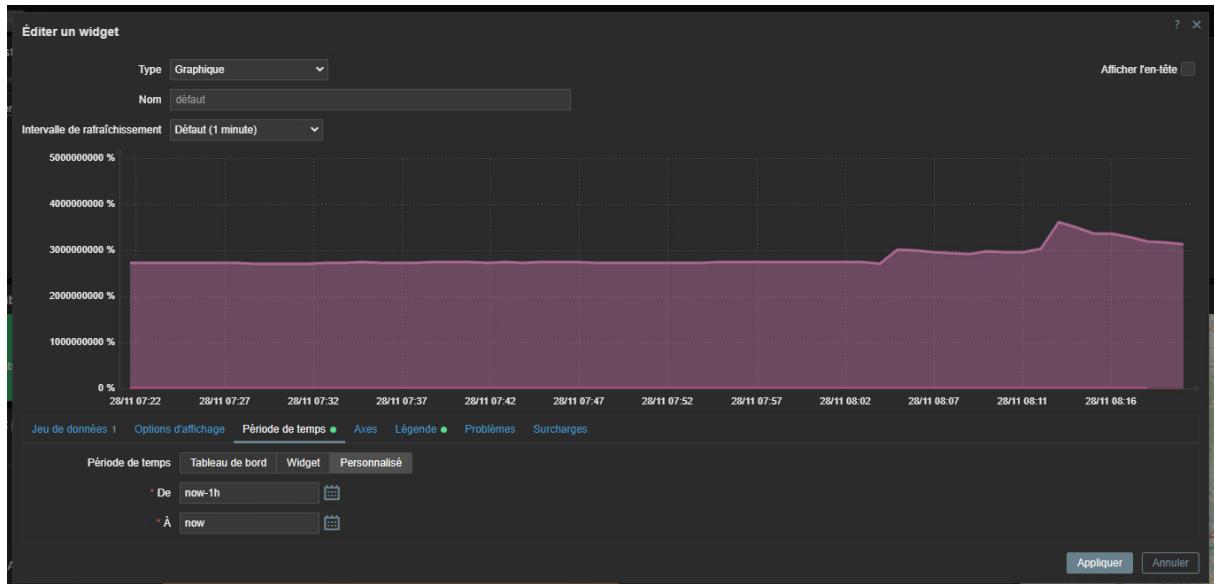
déTECTER DES PROBLÈMES DE BANDE PASSANTE. LA DISPOsITIVITÉ DES ÉLÉMENTS EN "ACTIF" INDIQUE QUE LES DONNÉES SONT PRÊTES À ÊTRE COLLECTÉES.

Éléments				
Hôte	SRV1-DC107 X	Sélectionner		
FS [Deploy(G:)]: Space: Total	vfs.fs.dependent.size[G:,total]	Élément dépendant	Numérique (non signé)	Activé
FS [Deploy(G:)]: Space: Used	vfs.fs.dependent.size[G:,used]	Élément dépendant	Numérique (non signé)	Activé
FS [Deploy(G:)]: Space: Used, in %	vfs.fs.dependent.size[G:,pused]	Élément dépendant	Numérique (flottant)	Activé
<input checked="" type="checkbox"/> Interface Intel(R) 82574L Gigabit Network Connection(Ethernet0): Bits received	net.if.in["346F93F3-0D90-4774-A126-141922F1 12F4"]	agent Zabbix	Numérique (non signé)	Activé
<input checked="" type="checkbox"/> Interface Intel(R) 82574L Gigabit Network Connection(Ethernet0): Bits sent	net.if.out["346F93F3-0D90-4774-A126-141922F1 11F4"]	agent Zabbix	Numérique (non signé)	Activé

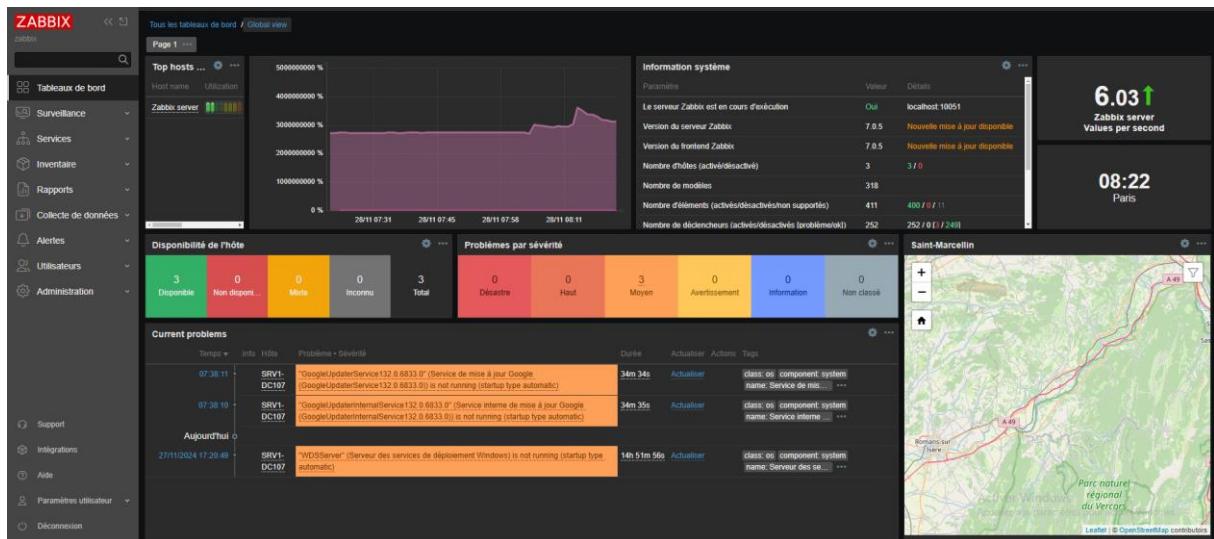
Le premier écran présente les réglages d'un widget de type graphique dans Zabbix. Plusieurs éléments de données, tels que l'utilisation du processeur, la mémoire utilisée et les bits réseau reçus/envoyés, ont été sélectionnés pour leur pertinence dans le suivi des performances de l'hôte "SRV1-DC107". Les options de visualisation incluent le tracé sous forme de ligne, des points ajustables et une transparence configurable pour une meilleure lisibilité des courbes. Ces réglages permettent de représenter les données clés de manière claire et précise, facilitant l'analyse des tendances.



La deuxième interface permet de configurer la période d'affichage des données sur le graphique. La plage temporelle est définie de "now-1h" à "now", ce qui offre une vue en temps réel des performances du système sur la dernière heure. Les paramètres des axes Y et X sont également ajustables, avec la possibilité d'utiliser des échelles automatiques ou personnalisées selon les besoins. Cela permet de contextualiser les données et de zoomer sur des intervalles spécifiques pour une analyse approfondie.



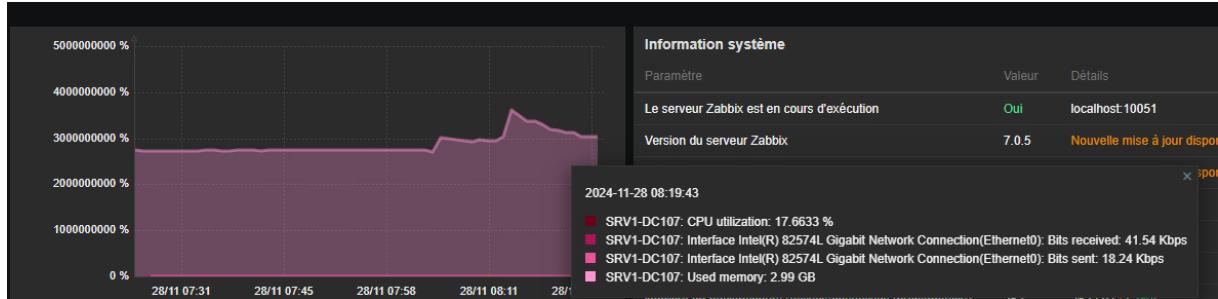
Le graphique précédemment configuré est intégré au tableau de bord et offre une visualisation claire des données de performance critiques. Il représente l'utilisation du processeur, la mémoire consommée, ainsi que les bits réseau reçus et envoyés par l'hôte "SRV1-DC107". Ce graphique est actualisé régulièrement, conformément à l'intervalle de rafraîchissement défini, garantissant une mise à jour en temps réel.



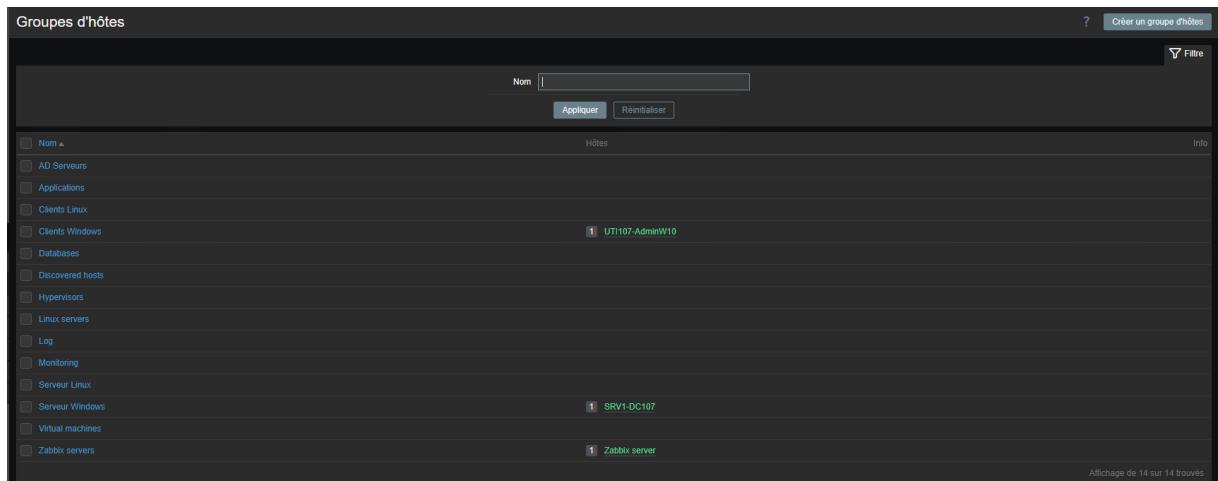
Le graphique affiche des détails clés liés aux performances de l'hôte "SRV1-DC107". Les informations incluent une utilisation CPU à 17,66 %, la quantité de données reçues sur l'interface réseau Ethernet0 (41,54 Kbps), les données envoyées (18,24 Kbps) et l'utilisation mémoire de 2,99 Go. Ces indicateurs permettent une analyse rapide des ressources consommées, utile pour détecter des surcharges ou des goulots d'étranglement.

L'inclusion de ces métriques précises dans un graphique favorise une prise de décision informée en cas d'anomalie. Par exemple, une hausse anormale de l'utilisation du processeur ou du

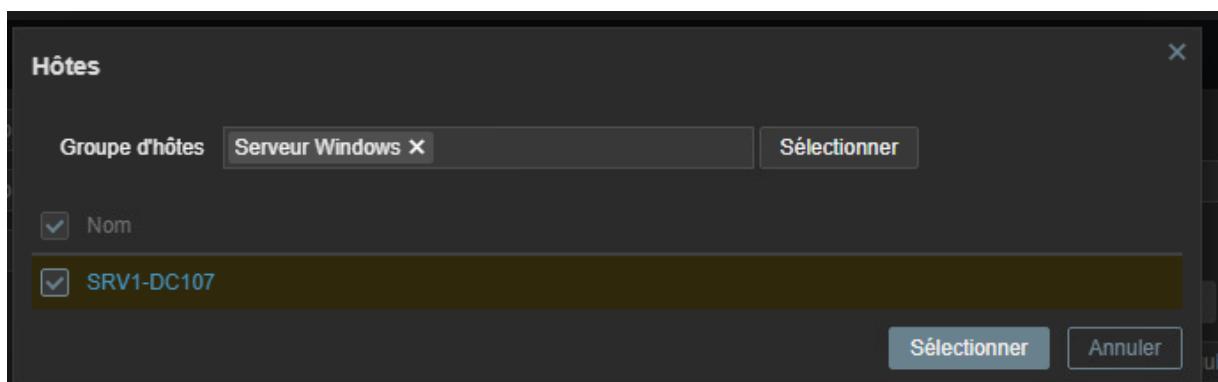
réseau pourrait indiquer un problème nécessitant une attention immédiate. Ce choix technique vise à améliorer la supervision proactive et à minimiser les temps de réponse face aux incidents.



La vue des groupes d'hôtes offre une organisation claire des équipements supervisés, regroupés par catégories spécifiques telles que "Serveur Windows" ou "Clients Linux". Cette classification facilite la gestion des infrastructures, en permettant d'appliquer des configurations ou des modèles adaptés à chaque groupe. Une telle organisation optimise le suivi et l'analyse des performances selon des critères ciblés.



L'association de l'hôte "SRV1-DC107" au groupe "Serveur Windows" garantit une gestion cohérente et centralisée. En rattachant cet hôte à un groupe, toutes les configurations et politiques appliquées à ce dernier sont automatiquement propagées, ce qui réduit les erreurs et simplifie les tâches administratives.



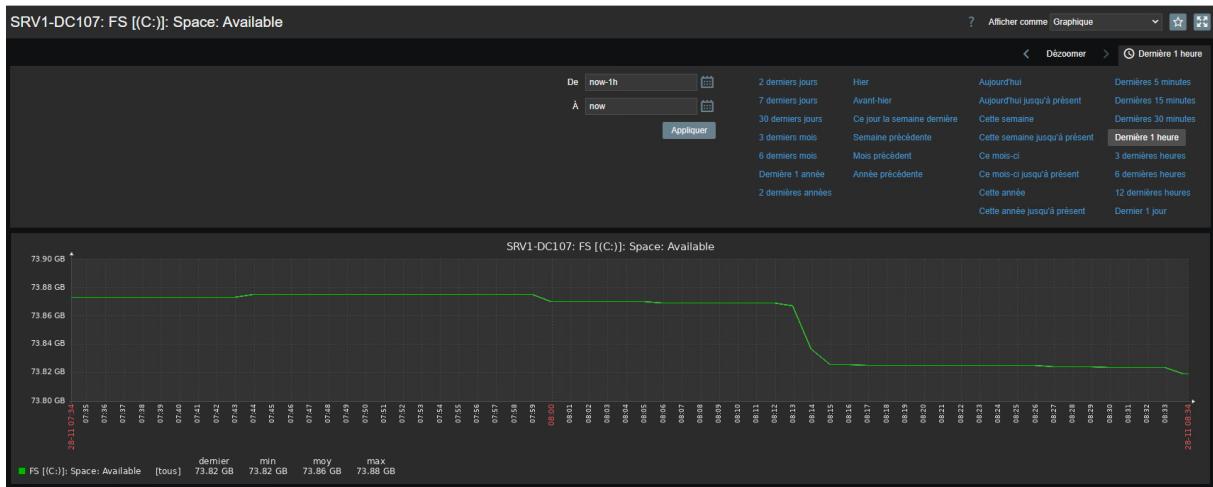
Les dernières données collectées pour un hôte sont accessibles dans une vue détaillée, affichant des métriques comme l'utilisation réseau ou l'espace disque. Ces informations permettent de surveiller en temps réel l'état de l'équipement et de détecter rapidement d'éventuelles anomalies ou tendances anormales.

The screenshot shows the Zabbix interface with the following details:

- Left sidebar:** Navigation menu with options like Tableaux de bord, Surveillance, Problèmes, Hôtes, Dernières données, Cartes, Découverte, Services, Inventaire, Rapports, Collecte de données, Alertes, Utilisateurs, Administration, Support, Intégrations, Aide, Paramètres utilisateur, and Déconnexion.
- Top bar:** Title 'Dernières données', search bar, and various buttons for filtering and applying tags.
- Host Selection:** 'Groupes d'hôtes' and 'Hôtes' dropdowns, with 'SRV1-DC107 X' selected.
- Tags:** A section for applying tags, with 'Nom' and 'Tags' fields.
- Metrics and Services:** A large table showing various metrics and their values, including disk usage (e.g., 0 C: 8.10 2.8 3.1 4.6), system services (e.g., Intel(R) 82574L Gigabit Network Connection), and network interfaces (e.g., Intel(R) 82574L Gigabit Network Connection (Ethernet0)).
- Bottom:** Buttons for 'Enregistrer sous', 'Appliquer', and 'Réinitialiser'.

Le graphique représentant les "Bits reçus" via l'interface réseau Ethernet met en lumière l'activité réseau de l'hôte. Ce type de visualisation est indispensable pour identifier des problèmes comme des congestions ou des interruptions réseau. De même, le graphique relatif à l'espace disque disponible offre une vision claire de l'évolution du stockage. Une diminution notable pourrait indiquer une saturation imminente ou des fichiers inutiles nécessitant une suppression.





La configuration des types de média dans Zabbix est un point crucial pour la gestion des alertes. La liste des médias disponibles, incluant des options comme le courriel ou les webhooks, garantit que les notifications sont acheminées par des canaux adaptés. Cela assure une réactivité accrue face aux incidents.

Types de média						
Nom		Etat	Tous	Activé	Désactivé	
				<a href="#">Appliquer</a>	<a href="#">Réinitialiser</a>	
Brevis.our	Webhook	Désactivé	4	Report not supported items, Report not supported low level discovery rules, Report problems to Zabbix administrators, Report unknown triggers		
Discord	Webhook	Désactivé	4	Report not supported items, Report not supported low level discovery rules, Report problems to Zabbix administrators, Report unknown triggers		
Email	Courriel	Désactivé	4	Report not supported items, Report not supported low level discovery rules, Report problems to Zabbix administrators, Report unknown triggers		
Email (HTML)	Courriel	Désactivé	4	Report not supported items, Report not supported low level discovery rules, Report problems to Zabbix administrators, Report unknown triggers		
Event-Driven Ansible	Webhook	Désactivé	4	Report not supported items, Report not supported low level discovery rules, Report problems to Zabbix administrators, Report unknown triggers		
Express.ms	Webhook	Désactivé	4	Report not supported items, Report not supported low level discovery rules, Report problems to Zabbix administrators, Report unknown triggers		
Github	Webhook	Désactivé	4	Report not supported items, Report not supported low level discovery rules, Report problems to Zabbix administrators, Report unknown triggers		
GLPI	Webhook	Désactivé	4	Report not supported items, Report not supported low level discovery rules, Report problems to Zabbix administrators, Report unknown triggers		
Email	Courriel	Désactivé	4	Report not supported items, Report not supported low level discovery rules, Report problems to Zabbix administrators, Report unknown triggers		
Gmail relay	Courriel	Désactivé	4	Report not supported items, Report not supported low level discovery rules, Report problems to Zabbix administrators, Report unknown triggers		
iAlert	Webhook	Désactivé	4	Report not supported items, Report not supported low level discovery rules, Report problems to Zabbix administrators, Report unknown triggers		
iTop	Webhook	Désactivé	4	Report not supported items, Report not supported low level discovery rules, Report problems to Zabbix administrators, Report unknown triggers		
Jira	Webhook	Désactivé	4	Report not supported items, Report not supported low level discovery rules, Report problems to Zabbix administrators, Report unknown triggers		

Lors de la configuration d'un type de média pour l'envoi de courriels, l'utilisation d'un serveur SMTP sécurisé, comme Gmail, garantit la fiabilité des notifications tout en respectant les standards de sécurité. Les paramètres tels que le chiffrement et l'authentification renforcent la confidentialité et la protection des données transmises.

Type de média

Type de média Modèles de messages 5 Options

\* Nom Email

Type Courriel

Fournisseur de messagerie Generic SMTP

\* serveur SMTP smtp.gmail.com

Port du serveur SMTP 465

\* Courriel nathanhyperespace@gmail.com

SMTP helo gmail.com

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 nhyperespace@gmail.com

Mot de passe

Format du message HTML Texte brut

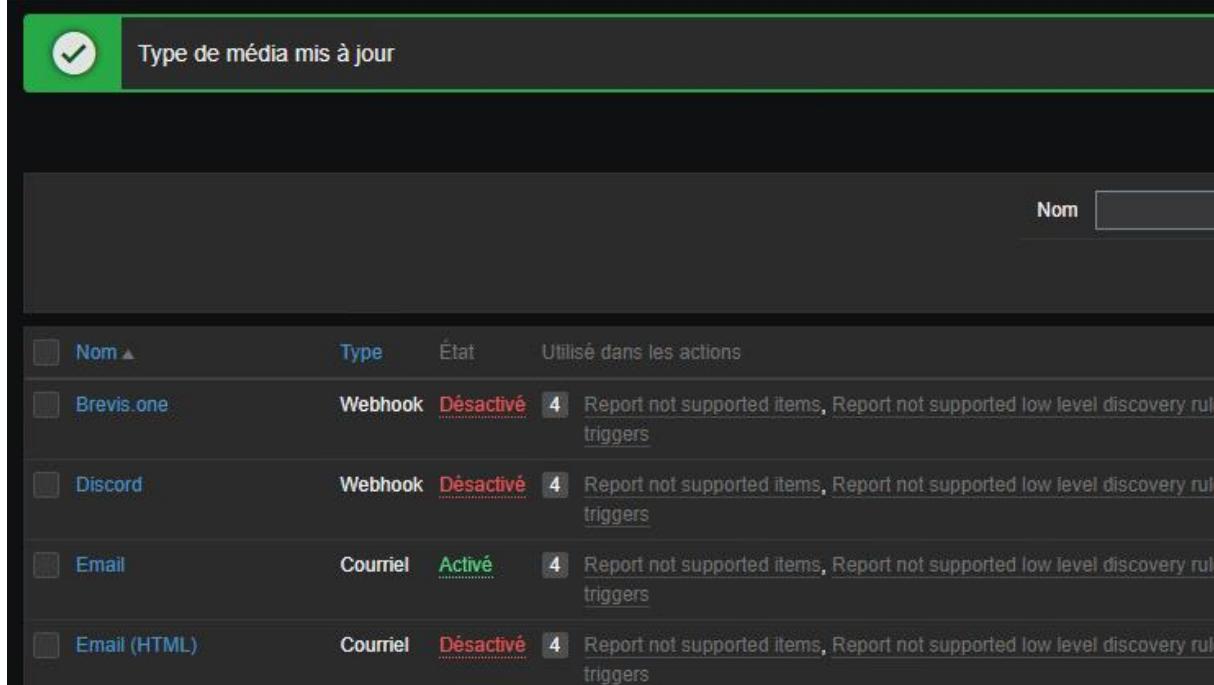
Description

Actualiser Clone Supprimer Annuler

La validation confirmant que le type de média a été mis à jour indique que la configuration du système est correctement enregistrée. Cela garantit que les notifications par le média spécifié seront opérationnelles sans erreur. Dans ce cas, le type de média "Email" est activé, ce qui signifie que les alertes pourront être envoyées directement par courriel.

L'activation de ce média est essentielle pour une supervision efficace, car les courriels offrent un canal de communication fiable et instantané pour informer les administrateurs de tout incident critique. Le statut "Actif" pour le média "Email" assure que les configurations associées, comme les modèles de messages, fonctionneront sans restriction, renforçant ainsi la réactivité face aux problèmes.

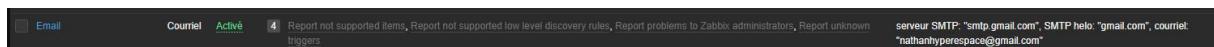
## Types de média



Nom	Type	État	Utilisé dans les actions
Brevis.one	Webhook	Désactivé	4 Report not supported items, Report not supported low level discovery rules, Report problems to Zabbix administrators, Report unknown triggers
Discord	Webhook	Désactivé	4 Report not supported items, Report not supported low level discovery rules, Report problems to Zabbix administrators, Report unknown triggers
Email	Courriel	Activé	4 Report not supported items, Report not supported low level discovery rules, Report problems to Zabbix administrators, Report unknown triggers
Email (HTML)	Courriel	Désactivé	4 Report not supported items, Report not supported low level discovery rules, Report problems to Zabbix administrators, Report unknown triggers

Le média "Email" est configuré comme actif, validant la disponibilité du canal pour l'envoi d'alertes critiques. L'adresse "nathanhyperespace@gmail.com" et le serveur SMTP "smtp.gmail.com" avec son hélo SMTP assurent une configuration fonctionnelle.

Le statut "Actif" garantit une transmission instantanée des notifications, optimisant la réactivité des administrateurs face aux incidents. La validation technique confirme une configuration robuste et prête à l'emploi pour la supervision efficace.



serveur SMTP: "smtp.gmail.com", SMTP helo: "gmail.com", courriel: "nathanhyperespace@gmail.com"

Une notification de validation confirme la mise à jour du type de média, rendant les alertes par courriel immédiatement opérationnelles. Cette confirmation est essentielle pour garantir que la configuration est correcte et fonctionnelle. Les modèles de messages associés permettent de personnaliser les notifications selon leur nature (problème, récupération, découverte). Cela rend les alertes plus explicites et directement exploitables par les administrateurs.

Type de média

Type de média Modèles de messages 5 Options

Modèles de messages	Type de message	Modèle	Actions
Problème	Problem started at {EVENT.TIME} on {EVENT.D...	Édition Supprimer	
Récupération de problème	Problem has been resolved at {EVENT.RECOV...	Édition Supprimer	
Mise à jour du problème	{USER.FULLNAME} {EVENT.UPDATE.ACTION...}	Édition Supprimer	
Découverte	Discovery rule: {DISCOVERY.RULE.NAME} Dev...	Édition Supprimer	
Enregistrement automatique	Host name: {HOST.HOST} Host IP: {HOST.IP} A...	Édition Supprimer	
<a href="#">Ajouter</a>			

Actualiser Clone Supprimer Annuler

Les options avancées liées aux médias, comme la gestion du nombre de tentatives ou des intervalles entre celles-ci, assurent une transmission fiable des messages même en cas de perturbations temporaires des services de messagerie. Ces réglages renforcent la robustesse et la fiabilité du système de supervision.

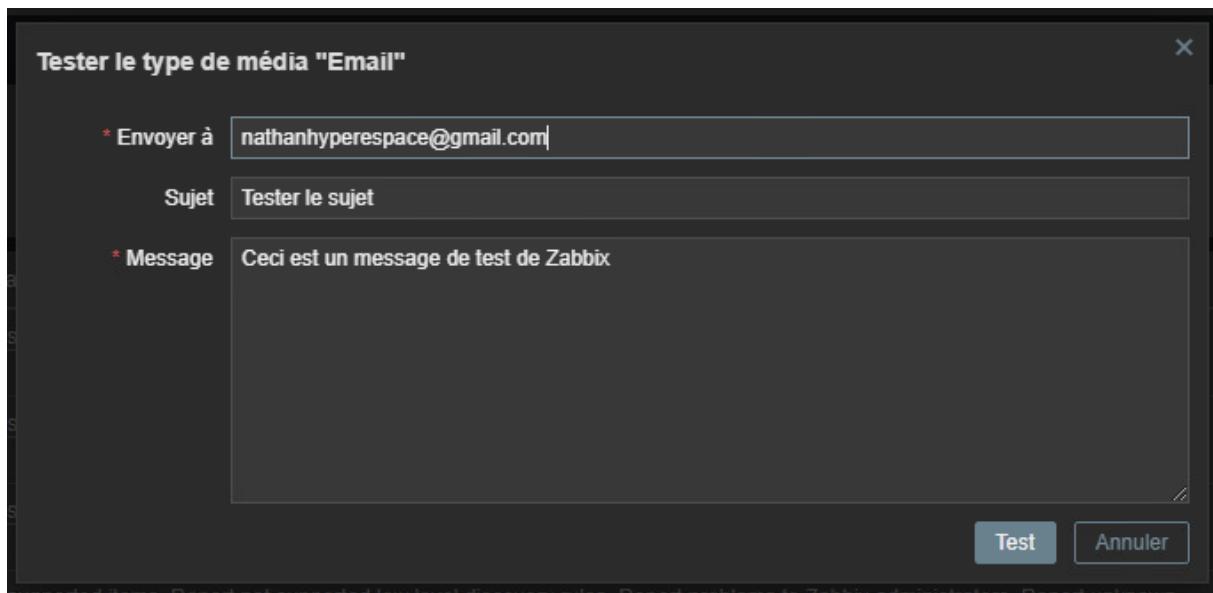
Type de média

Type de média Modèles de messages 5 Options

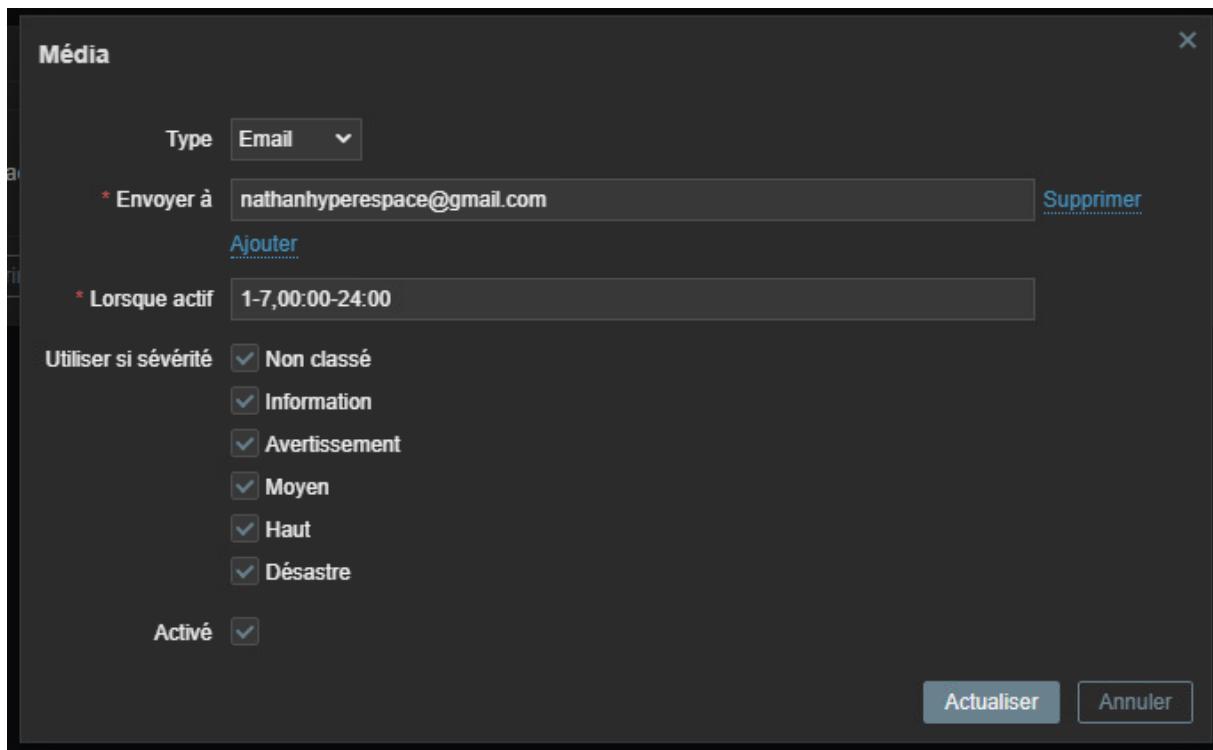
Sessions concurrentes	Un	Illimité	Personnalisé
* Tentatives	3		
* Intervalle entre tentatives	10s		

Actualiser Clone Supprimer Annuler

Le test du média "Email" vérifie la capacité d'envoi de messages via le serveur SMTP en renseignant une adresse de destination, un sujet, et un contenu de message. Cette étape garantit que les alertes peuvent être transmises efficacement et détecte rapidement les problèmes de configuration, notamment au niveau de la connectivité ou des paramètres SMTP.



La configuration du média "Email" précise l'adresse de réception, les plages horaires d'activation et les niveaux de gravité des alertes. Ces paramètres assurent une communication optimisée en filtrant les alertes selon leur priorité. L'activation explicite confirme que ce canal est prêt à être utilisé pour transmettre des notifications importantes.



L'association du média configuré à un utilisateur permet une personnalisation des notifications en fonction des responsabilités. En attribuant des paramètres spécifiques, comme des plages horaires et des seuils de gravité, la gestion des alertes devient plus ciblée et efficace, améliorant la réactivité face aux incidents critiques.

Utilisateurs

Utilisateur Média 1 Permissions

Média Type Envoyer à Lorsque actif Utiliser si严重性 État Action  
Email nathanhyperespace@gmail.com 1-7,00:00-24:00 **N I A M H D** Activé Édition Supprimer  
Ajouter

Actualiser Supprimer Annuler

L'affichage des utilisateurs met en évidence leur rôle et leurs permissions au sein du système. Chaque utilisateur est lié à un groupe précis et possède des droits adaptés à ses responsabilités. Par exemple, l'utilisateur "Admin" est doté d'un rôle de super administrateur, lui conférant un accès complet à toutes les fonctionnalités. Cette organisation assure un contrôle d'accès rigoureux et une séparation claire des tâches, essentielle pour une administration sécurisée et efficace.

Utilisateurs

Créer un utilisateur Filtre

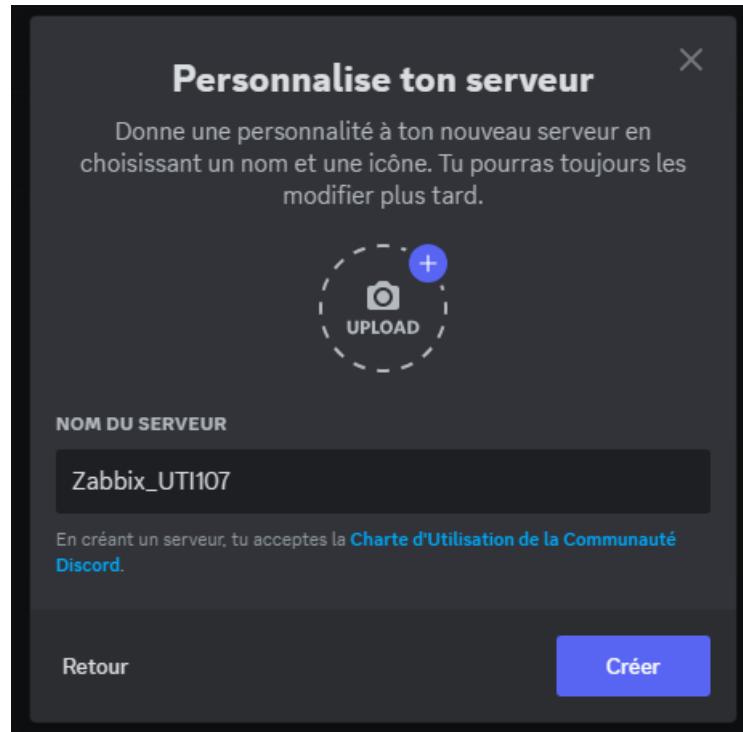
Nom d'utilisateur Rôles utilisateur Groupes d'utilisateur

Appliquer Réinitialiser

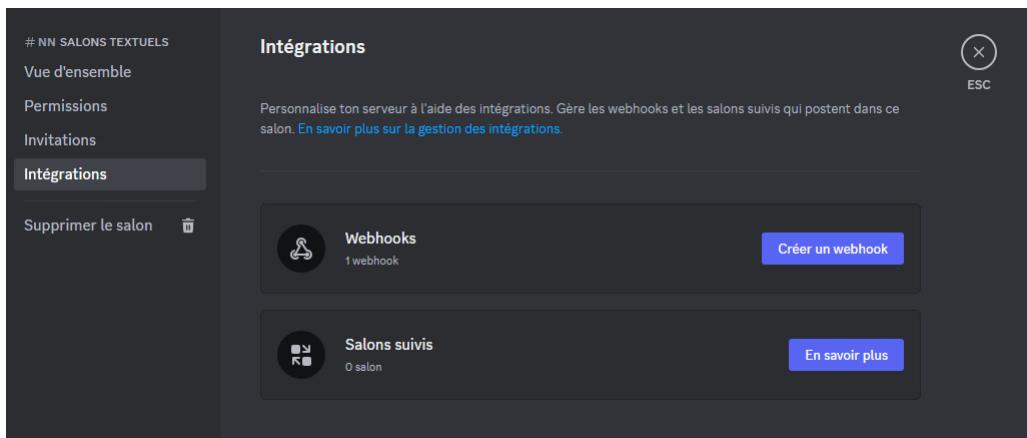
Nom d'utilisateur	Prénom	Nom de famille	Rôle utilisateur	Groupes	Est connecté ?	Connexion	Accès à l'interface	Accès API	Mode debug	État	Provisionné	Info
Admin	Zabbix	Administrator	Super admin role	Internal, Zabbix administrators	Oui (28/11/2024 09:00:27)	Ok	Interne	Activé	Désactivé	Activé		
guest			Guest role	Disabled, Guests, Internal	Non	Ok	Interne	Désactivé	Désactivé	Désactivé		
Reeth92SIO	Reeth92	Reeth	Admin role	Zabbix administrators	Non	Ok	Valeur système par défaut	Activé	Désactivé	Activé		

Affichage de 3 sur 3 trouvés

La configuration du serveur "Zabbix\_UTI107" permet de centraliser les notifications et alertes. En choisissant un nom personnalisé et une icône dédiée, l'infrastructure gagne en clarté et en distinction. Cette étape est cruciale pour faciliter l'identification et le suivi des alertes émises par ce serveur. Cela permet une meilleure organisation dans des environnements supervisant plusieurs instances.



La configuration des intégrations montre une connectivité flexible entre Zabbix et Discord. Le webhook intitulé "Zabbix Alerter", associé à un salon spécifique, établit un lien direct entre les alertes système et la plateforme de communication. Ce choix garantit une transmission en temps réel des informations critiques aux équipes, augmentant ainsi leur réactivité et leur coordination.



L'intégration des webhooks dans Discord, comme vu avec "Zabbix Alerter", simplifie la diffusion des alertes aux membres de l'équipe. En associant un webhook à un salon spécifique, les notifications sont diffusées immédiatement, permettant un suivi collaboratif des incidents. Ce mécanisme réduit le délai de réaction face aux problèmes critiques et améliore la coordination au sein des équipes.

POSTE SUR #NN

Zabbix Alerter

Crée le 28 nov. 2024 par reeth92

NOM

Zabbix Alerter

SALON

#nn

Supprimer

Copier l'URL du webhook

Suppression de webhook

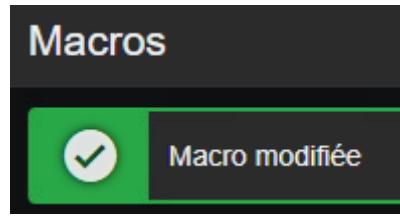
Le menu "Macros" dans la partie Administration de Zabbix centralise la gestion des variables globales ou spécifiques aux hôtes, simplifiant les configurations répétitives.

Administration

- Général
- Journal d'audit
- Nettoyage
- Groupes de proxy
- Proxys
- Macros
- File d'attente

Les macros définies, telles que celles pour la communauté SNMP ou l'URL de Zabbix, illustrent une approche standardisée et automatisée de la configuration. Ces macros facilitent la personnalisation des modèles et des processus, permettant un gain de temps significatif dans les déploiements. Leur modification, confirmée par le système, garantit la prise en compte des paramètres mis à jour.

Macro	Valeur	Description	Supprimer
{\$SNMP_COMMUNITY}	NetMgmt@2024	T description	Supprimer
{\$ZABBIX_URL}	https://zabbix.lan	T description	Supprimer
<a href="#">Ajouter</a>			
<a href="#">Actualiser</a>			



La configuration du type de média « Discord » repose sur l'utilisation d'un webhook, où chaque paramètre, tel que l'alerte ou le sujet, est défini pour permettre une intégration fluide avec la plateforme Discord. Le champ « discord\_endpoint » pointe directement vers l'URL de l'API, garantissant un envoi précis des notifications vers le salon approprié.

**Type de média**

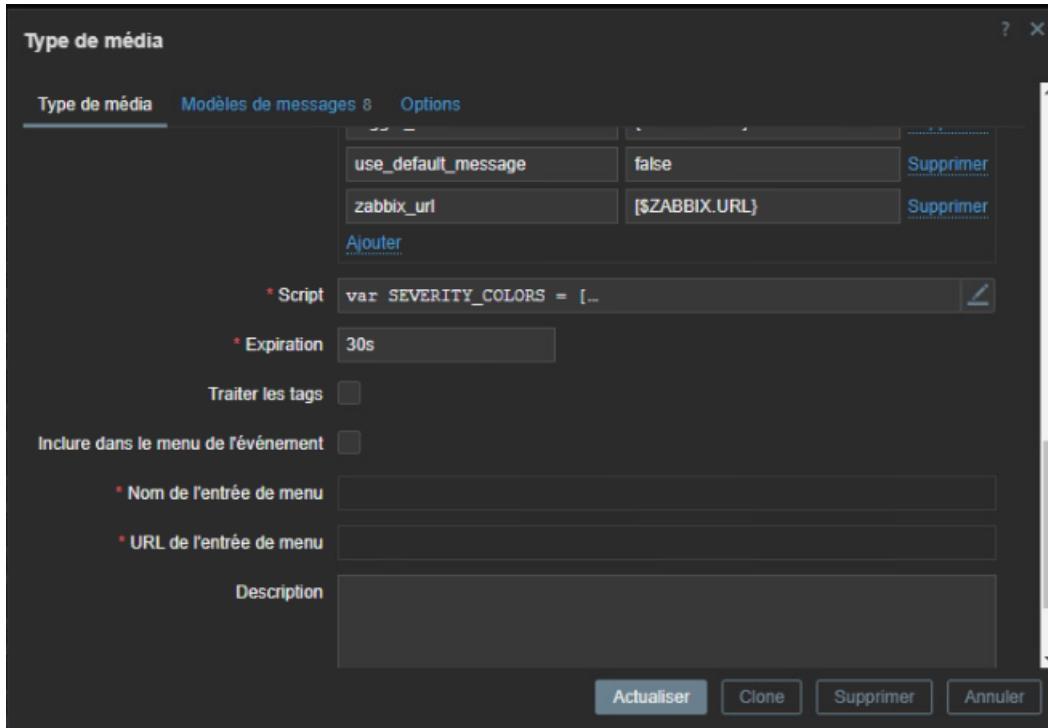
Type de média Modèles de messages 8 Options

Paramètres	Nom	Valeur	Action
	alert_message	{ALERT.MESSAGE}	Supprimer
alert_subject	{ALERT.SUBJECT}	Supprimer	
discord_endpoint	https://discord.com/api/webhooks	Supprimer	
event_date	{EVENT.DATE}	Supprimer	
event_id	{EVENT.ID}	Supprimer	
event_name	{EVENT.NAME}	Supprimer	
event_nseverity	{EVENT.NSEVERITY}	Supprimer	
event_opdata	{EVENT.OPDATA}	Supprimer	
event_recovery_date	{EVENT.RECOVERY.DATE}	Supprimer	
event_recovery_time	{EVENT.RECOVERY.TIME}	Supprimer	
event_severity	{EVENT.SEVERITY}	Supprimer	
event_source	{EVENT.SOURCE}	Supprimer	
event_tags	{EVENT.TAGS}	Supprimer	
event_time	{EVENT.TIME}	Supprimer	
event_update_action	{EVENT.UPDATE.ACTION}	Supprimer	
event_update_date	{EVENT.UPDATE.DATE}	Supprimer	
event_update_message	{EVENT.UPDATE.MESSAGE}	Supprimer	

Actualiser Clone Supprimer Annuler

Un script dédié est intégré à cette configuration avec une expiration programmée à 30 secondes. Ce délai contrôle la durée de vie des alertes afin d'éviter des notifications périmées ou non

pertinentes. Ce réglage est particulièrement utile pour améliorer la fluidité et la réactivité du système.

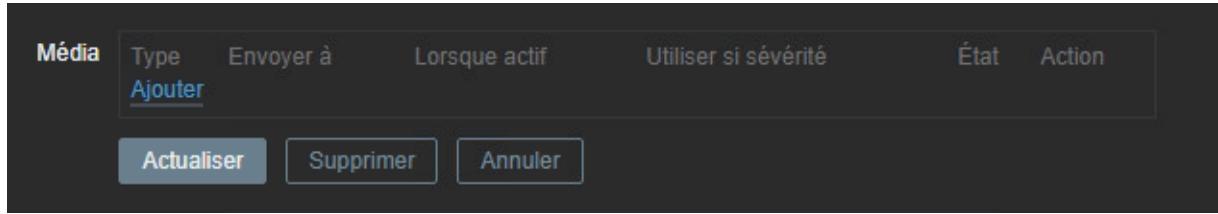


Le tableau général synthétise l'état des médias configurés, mettant en avant que Discord est activé, contrairement à d'autres médias désactivés. Cette vue permet une vérification rapide du bon fonctionnement des canaux de notification en cours d'utilisation, confirmant que Discord est opérationnel.

Nom	Type	État	Utilisé dans les actions
Brevis.one	Webhook	Désactivé	<a href="#">Report not supported items, Report not supported low level discovery rules, Report problems to Zabbix administrators, Report triggers</a>
Discord	Webhook	Activé	<a href="#">Report not supported items, Report not supported low level discovery rules, Report problems to Zabbix administrators, Report triggers</a>
Email	Courriel	Activé	<a href="#">Report not supported items, Report not supported low level discovery rules, Report problems to Zabbix administrators, Report triggers</a>

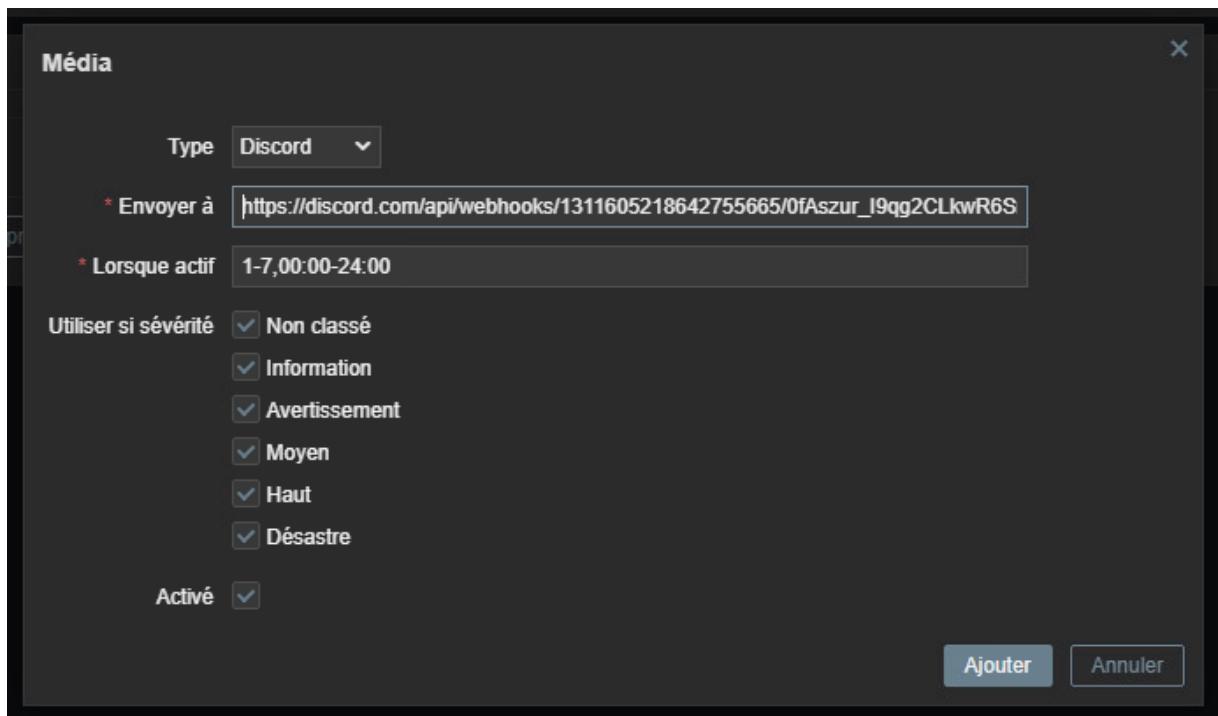
[Ajouter](#)

L'ajout du média se fait via une interface simplifiée où les paramètres critiques, comme l'URL du webhook et les niveaux de gravité, sont soigneusement renseignés. Cette étape assure que chaque événement est traité avec la priorité qu'il mérite.



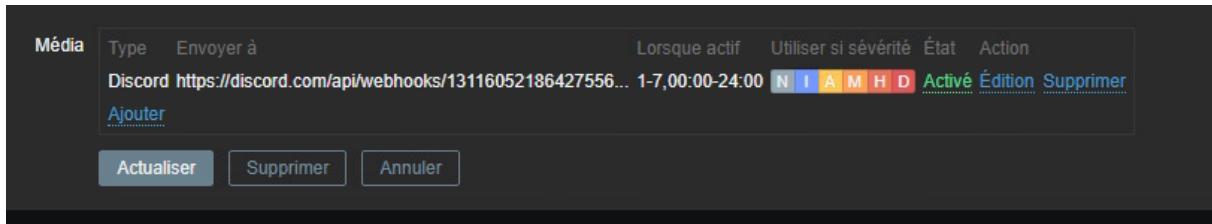
Le détail de l'envoi à Discord montre une configuration adaptée à une disponibilité permanente, paramétrée pour fonctionner 24 heures sur 24, 7 jours sur 7. Les niveaux de sévérité cochés incluent toutes les catégories, des informations aux désastres, assurant ainsi qu'aucune alerte ne soit négligée.

L'onglet des paramètres utilisateur met en évidence l'association entre le média Discord et les plages horaires définies, prouvant que les notifications suivent un schéma clair et sont actives sans interruption. Cela garantit une disponibilité constante pour les notifications importantes.



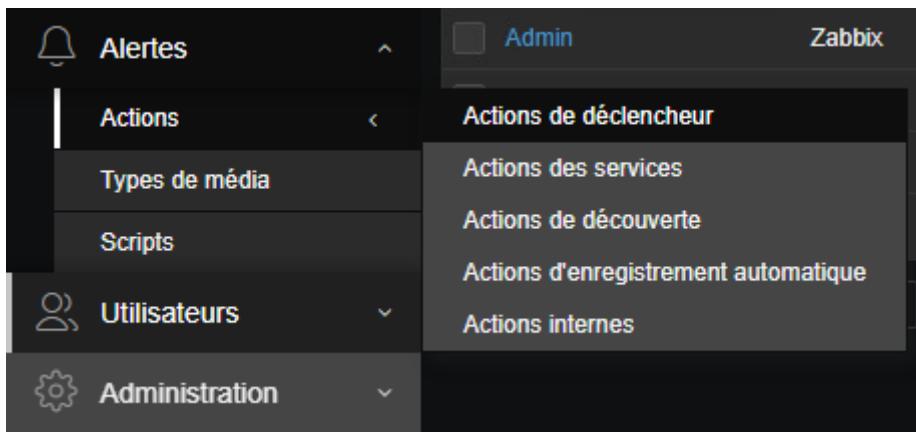
La confirmation finale des paramètres montre une configuration cohérente et robuste, avec un webhook actif prêt à recevoir et traiter les alertes de Zabbix de manière efficace et en temps réel. Cela offre une garantie de communication fiable entre la plateforme de supervision et les administrateurs via Discord.

Enfin, le menu média affiche les options comme « Ajouter », permettant d'intégrer de nouveaux médias ou de mettre à jour les configurations existantes. Ces fonctionnalités facilitent la gestion des intégrations et permettent des ajustements rapides en fonction des besoins évolutifs.



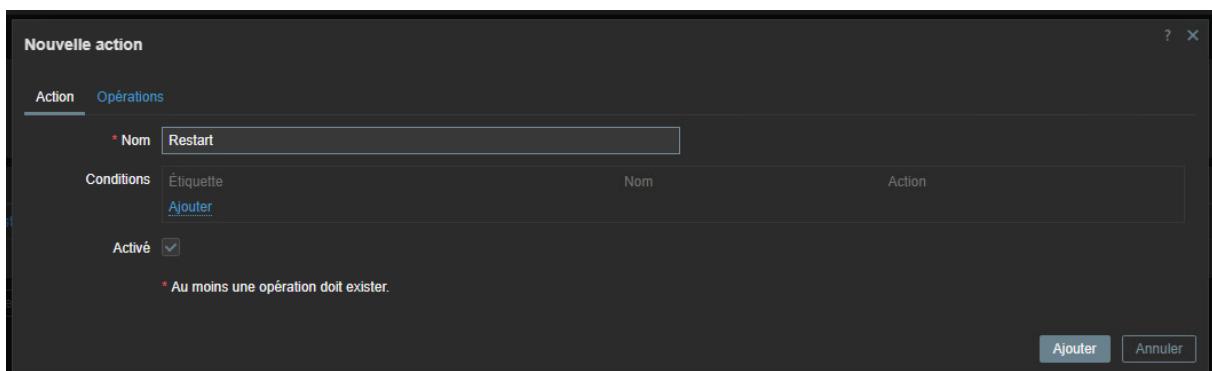
The screenshot shows a table with columns: Type, Envoyer à, Lorsque actif, Utiliser si sévérité, État, and Action. There is one row for 'Discord' with the URL <https://discord.com/api/webhooks/13116052186427556...>. The 'Action' column shows buttons for 'Edition' (highlighted in blue) and 'Supprimer'. Below the table are buttons for 'Actualiser', 'Supprimer', and 'Annuler'.

Le menu "Actions" a été utilisé pour accéder aux options disponibles, incluant les déclencheurs, actions internes et actions automatiques. Cela permet de choisir le contexte adapté pour automatiser les réponses ou alerter les administrateurs en fonction des événements identifiés dans le système.



The screenshot shows the Zabbix navigation menu with the 'Actions' section expanded. The sub-options listed are: Actions de déclencheur, Actions des services, Actions de découverte, Actions d'enregistrement automatique, and Actions internes.

Une action intitulée "Restart" a été définie, activée pour répondre automatiquement à un événement spécifique. Le nom donné reflète l'intention de l'action, ici redémarrer un service ou un système ciblé en cas de problème. Les conditions associées précisent les déclencheurs liés à cette action.



The screenshot shows the 'Nouvelle action' (New Action) dialog. The 'Action' tab is selected. The 'Nom' (Name) field contains 'Restart'. The 'Conditions' section shows 'Ajouter' (Add) selected. The 'Activé' (Active) checkbox is checked. A note at the bottom states: 'Au moins une opération doit exister.' (At least one operation must exist). At the bottom right are buttons for 'Ajouter' (Add) and 'Annuler' (Cancel).

La liste des déclencheurs permet de spécifier des événements critiques. Par exemple, le déclencheur "Zabbix server has been restarted" a été choisi pour détecter et réagir aux

redémarrages inattendus du serveur Zabbix. Ces déclencheurs sont essentiels pour cibler des problèmes précis tout en évitant des alertes excessives.

<input type="checkbox"/> Utilization of trigger housekeeper processes is high	Moyen	Activé
<input type="checkbox"/> Utilization of unreachable poller processes is high	Moyen	Activé
<input type="checkbox"/> Utilization of vmware collector processes is high	Moyen	Inconnu
<input type="checkbox"/> Version has changed	Information	Activé
<input type="checkbox"/> Zabbix agent is not available	Moyen	Activé
<input checked="" type="checkbox"/> Zabbix server has been restarted	Avertissement	Activé
<input type="checkbox"/> Zabbix value cache working in low memory mode	Haut	Activé

Sélectionner Annuler

Une condition a été ajoutée pour associer l'action "Restart" uniquement au déclencheur sélectionné. Ce paramètre garantit que l'action s'exécute uniquement lorsque le déclencheur correspondant est activé, réduisant ainsi le risque d'opérations inutiles.

Déclencheurs

Hôte: Zabbix server X Sélectionner

<input type="checkbox"/>	Utilization of preprocessing manager processes is high	Moyen	Activé
<input type="checkbox"/>	Utilization of preprocessing worker processes is high	Moyen	Activé
<input type="checkbox"/>	Utilization of proxy group manager processes is high	Moyen	Activé
<input type="checkbox"/>	Utilization of proxy poller processes is high	Moyen	Activé
<input type="checkbox"/>	Utilization of report manager processes is high	Moyen	Inconnu
<input type="checkbox"/>	Utilization of report writer processes is high	Moyen	Inconnu
<input type="checkbox"/>	Utilization of self-monitoring processes is high	Moyen	Activé
<input type="checkbox"/>	Utilization of service manager processes is high	Moyen	Activé
<input type="checkbox"/>	Utilization of snmp poller processes is high	Moyen	Activé
<input type="checkbox"/>	Utilization of snmp trapper processes is high	Moyen	Inconnu
<input type="checkbox"/>	Utilization of task manager processes is high	Moyen	Activé
<input type="checkbox"/>	Utilization of timer processes is high	Moyen	Activé
<input type="checkbox"/>	Utilization of trapper processes is high	Moyen	Activé
<input type="checkbox"/>	Utilization of trigger housekeeper processes is high	Moyen	Activé
<input type="checkbox"/>	Utilization of unreachable poller processes is high	Moyen	Activé
<input type="checkbox"/>	Utilization of vmware collector processes is high	Moyen	Inconnu
<input type="checkbox"/>	Version has changed	Information	Activé
<input type="checkbox"/>	Zabbix agent is not available	Moyen	Activé
<input checked="" type="checkbox"/>	Zabbix server has been restarted	Avertissement	Activé
<input type="checkbox"/>	Zabbix value cache working in low memory mode	Haut	Activé

Sélectionner Annuler

La liste des problèmes en cours montre les incidents non résolus, tels que "WDS Server not running". Cela permet de surveiller l'état des systèmes et de valider l'efficacité des déclencheurs et des actions configurées.

Current problems

Temps	Info	Hôte	Problème • Sévérité	Durée	Actualiser	Actions	Tags
27/11/2024 17:20:49		SRV1-DC107	"WDS Server" (Serveur des services de déploiement Windows) is not running. (startup type automatic)	1j 5h 14m	Actualiser		class: os component: system name: Serveur des se... ...

### Nouvelle condition

Type: Déclencheur

Opérateur: égal

Source du déclencheur: Hôte

\* Déclencheurs: Zabbix server: Zabbix server has been rest...

Sélectionner

Ajouter Annuler

### Nouvelle action

Action Opérations

\* Nom: Restart

Conditions

Étiquette	Nom	Action	Supprimer
A	Déclencheur égal Zabbix server: Zabbix server has been restarted		

Activé:

\* Au moins une opération doit exister.

Ajouter Annuler

### Nouvelle action

Action Opérations

Action Opérations

\* Durée de l'étape d'opération par défaut: 1h

Opérations

Étapes	Détails	Démarrer dans	Durée	Action

Ajouter

### Détails de l'opération

Opération Envoi message

Étapes 1 - 1 (0 - indéfiniment)

Durée de l'étape 0 (0 - utiliser les paramètres par défaut de l'action)

\* Au moins un utilisateur ou un groupe d'utilisateurs doit être sélectionné.

Envoyer aux groupes d'utilisateurs

Envoyer aux utilisateurs    
taper ici pour rechercher

Envoyer uniquement à

Message personnalisé

Conditions

Étiquette	Nom	Action
Ajouter		

### Nouvelle action

Action Opérations 1

\* Durée de l'étape d'opération par défaut 1h

Opérations

Étapes	Détails	Démarrer dans	Durée	Action
1	Envoyer le message aux utilisateurs: Reeth92SIO (Reeth92 Reeth) via Discord	Immédiatement	Défaut	<input type="button" value="Édition"/> <input type="button" value="Supprimer"/>
<input type="button" value="Ajouter"/>				

Opérations de récupération

Détails	Action
<input type="button" value="Ajouter"/>	

Opérations de mise à jour

Détails	Action
<input type="button" value="Ajouter"/>	

Interrompre les opérations en cas de problèmes symptomatiques

Suspendre les opérations des problèmes supprimés

Notifier les escalades annulées

\* Au moins une opération doit exister.

Actions de déclencheur

Action ajoutée

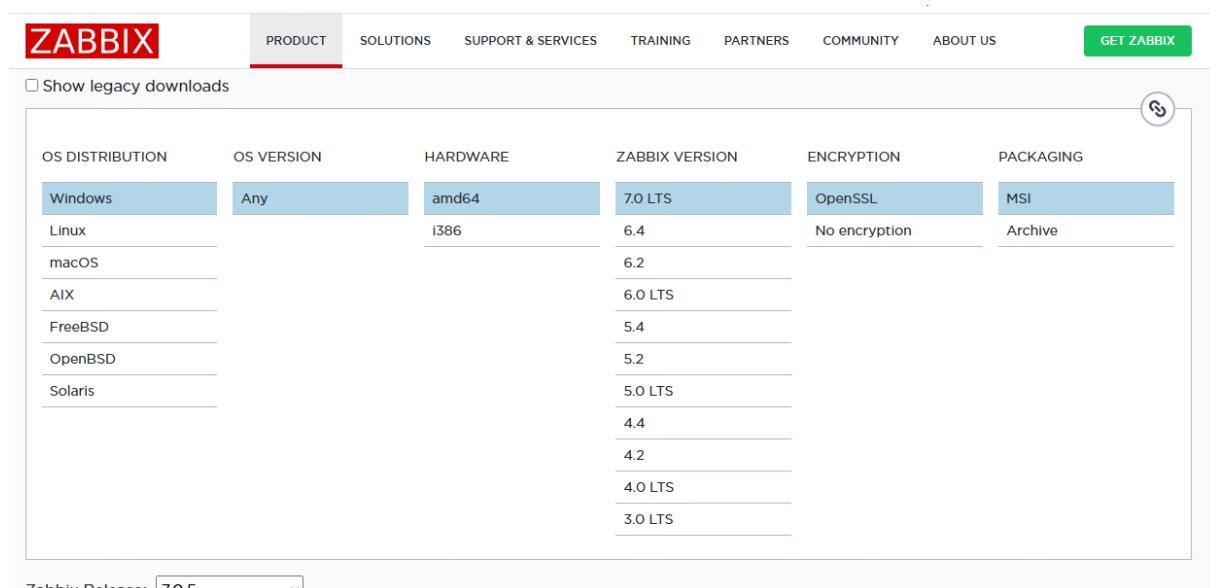
Conditions	Opérations	État
<input type="checkbox"/> Nom	<input type="text"/>	<input type="button" value="Tous"/> <input type="button" value="Activé"/> <input type="button" value="Désactivé"/>
<input type="checkbox"/> Report problems to Zabbix administrators	Envoyer le message aux groupes d'utilisateurs: Zabbix administrators via tous les médias	Désactivé
<input type="checkbox"/> Restart	Envoyer le message aux utilisateurs: Reeth92SIO (Reeth92 Reeth) via Discord	Activé

Affichage de 2 sur 2 trouvés

## Installation de l'agent Zabbix

### Windows

Premièrement, sur le site de l'éditeur, les paramètres nécessaires que nous avons choisi au téléchargement de l'agent Zabbix ont été configurés pour un environnement Windows avec un processeur amd64. La version 7.0 LTS a été choisie en raison de sa fiabilité et de son support à long terme, particulièrement adapté aux systèmes critiques. L'utilisation du chiffrement OpenSSL garantit la sécurité des échanges entre l'agent et le serveur, tandis que le format MSI simplifie l'installation sur des postes Windows, ce qui favorise une mise en œuvre rapide.



The screenshot shows the Zabbix download page. The 'PRODUCT' tab is selected. A table lists download options for Windows, Any OS version, amd64 hardware, and 7.0 LTS Zabbix version. The table includes columns for OS distribution, OS version, hardware, Zabbix version, encryption, and packaging. The 'Windows' row is highlighted in blue.

OS DISTRIBUTION	OS VERSION	HARDWARE	ZABBIX VERSION	ENCRYPTION	PACKAGING
Windows	Any	amd64	7.0 LTS	OpenSSL	MSI
Linux		i386	6.4	No encryption	Archive
macOS			6.2		
AIX			6.0 LTS		
FreeBSD			5.4		
OpenBSD			5.2		
Solaris			5.0 LTS		
			4.4		
			4.2		
			4.0 LTS		
			3.0 LTS		

Les checksums (SHA256, SHA1 et MD5) fournissent un moyen fiable de confirmer l'intégrité du fichier, réduisant ainsi les risques liés à des fichiers corrompus ou malveillants. Le lien direct vers le téléchargement hébergé sur le site officiel de Zabbix assure une source authentique et sécurisée, renforçant la confiance des administrateurs dans le processus de déploiement. La clarté des informations présentées facilite la prise en main et garantit une installation sans incident.

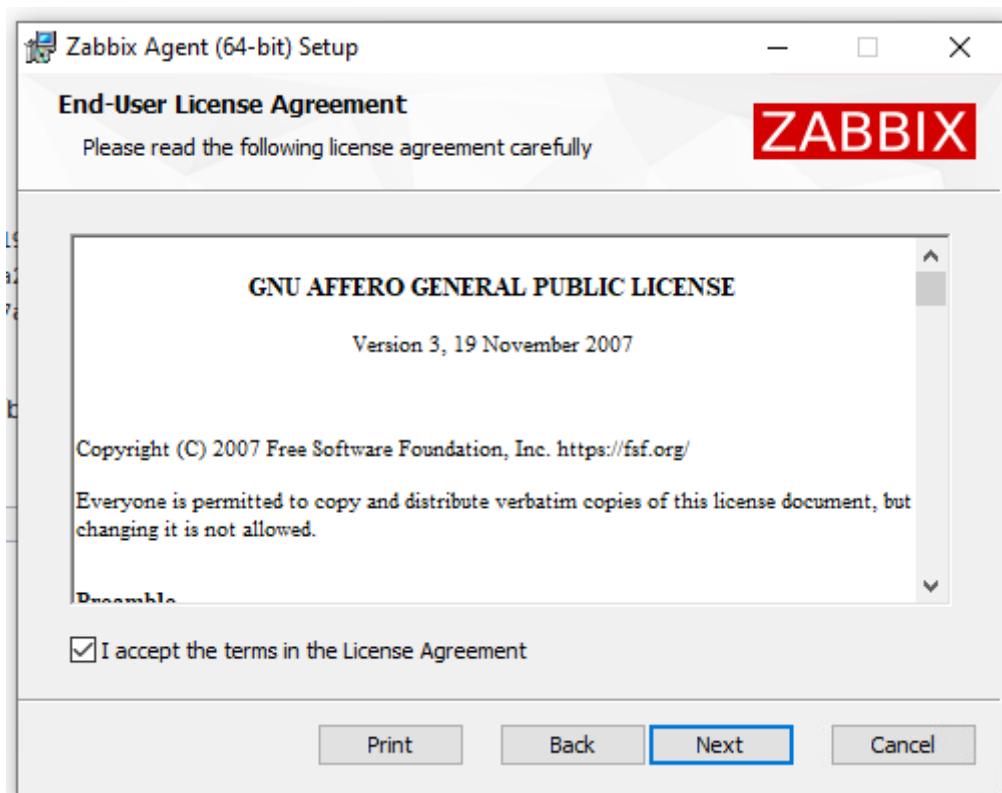
**Zabbix agent v7.0.5**

Packaging: MSI  
Encryption: OpenSSL  
Linkage: Dynamic  
Checksum: sha256: 1d5a1e93626091b89546b6cb00197fe0569ce77cc062691604d10d24203a2d30  
shal: 238f36d2d4b2ccbec09f88273da2278a8783dc64  
md5: f3cac46e40150ac95e05e615f37a2db8

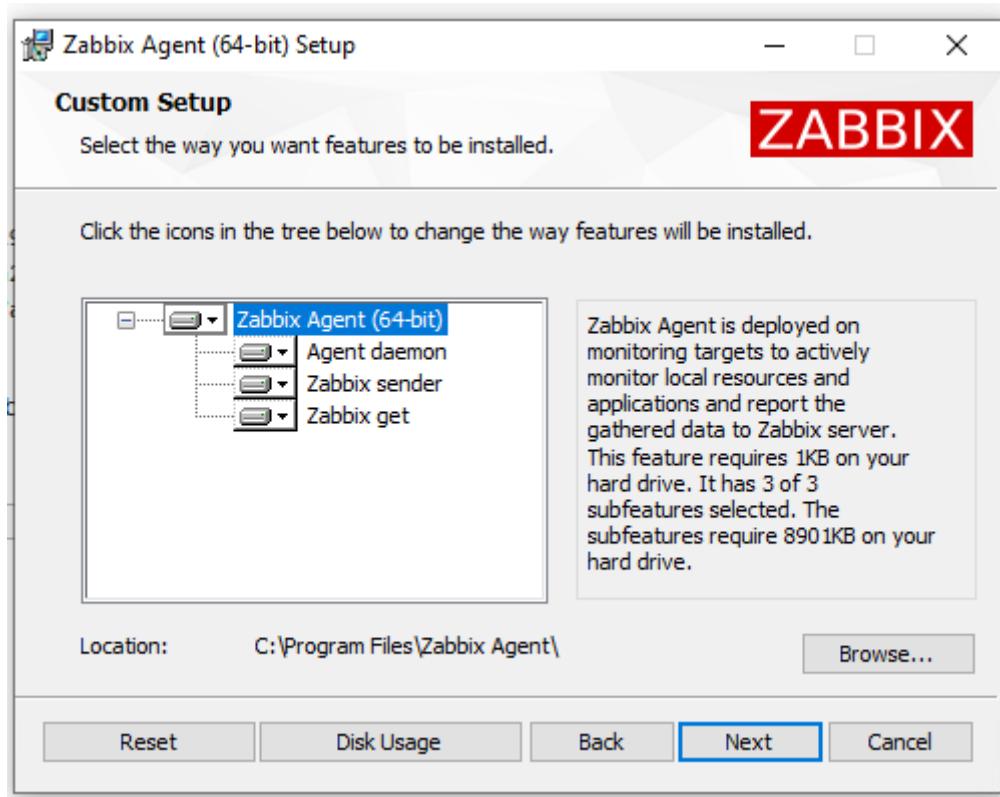
**DOWNLOAD** [https://cdn.zabbix.com/zabbix/binaries/stable/7.0/7.0.5/zabbix\\_agent-7.0.5-windows-amd64-openssl.msi](https://cdn.zabbix.com/zabbix/binaries/stable/7.0/7.0.5/zabbix_agent-7.0.5-windows-amd64-openssl.msi)

**Read manual**

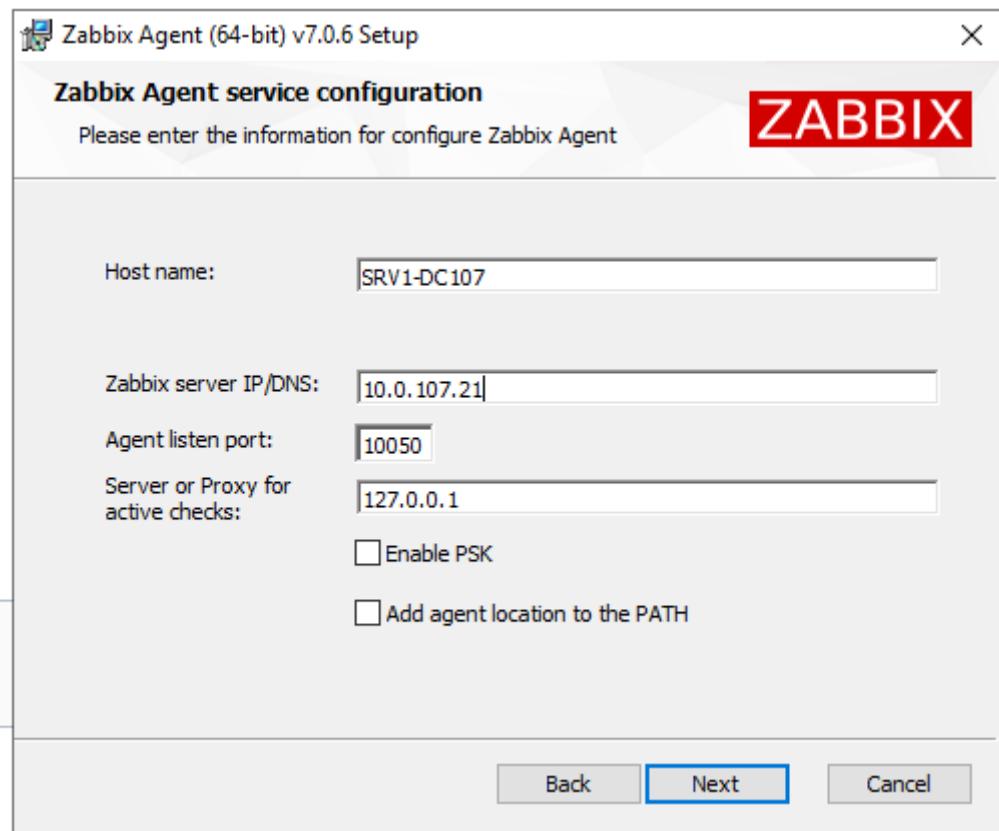
La présentation de la licence GNU Affero General Public License montre l'engagement envers un logiciel libre et redistribuable. L'utilisateur doit accepter les termes pour poursuivre, soulignant l'importance des aspects légaux dans les logiciels.



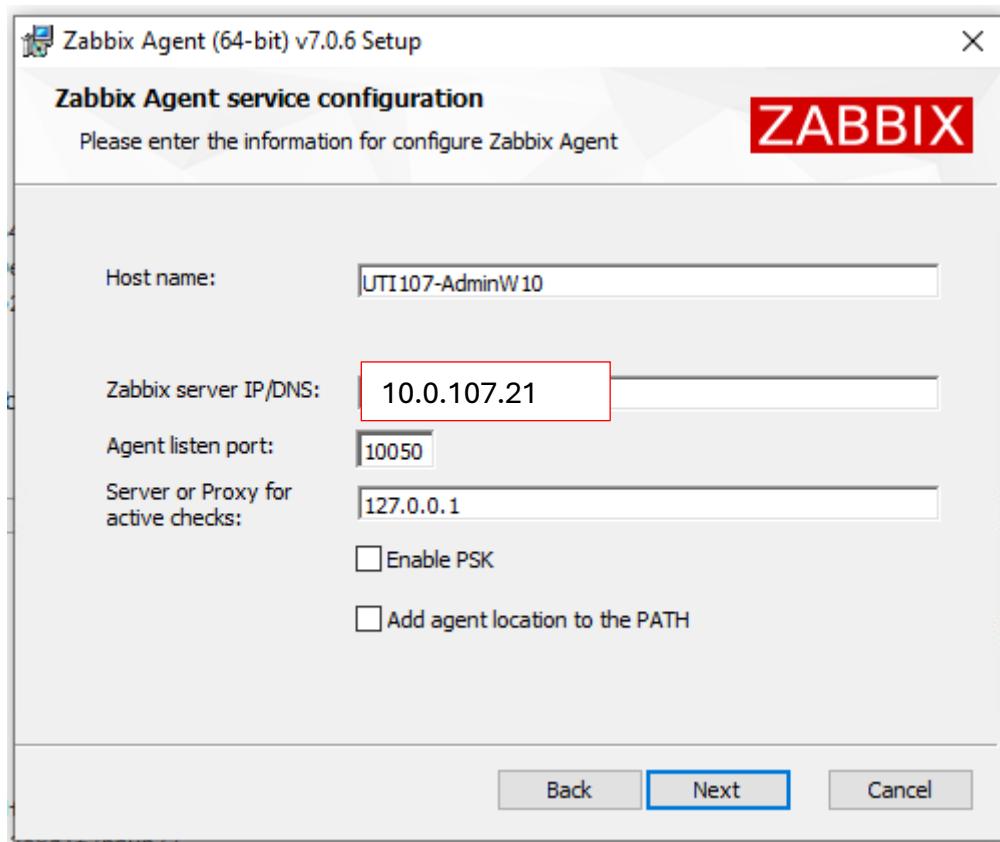
Les composants comme "Agent daemon", "Zabbix sender" et "Zabbix get" sont sélectionnés pour une installation complète. Cela garantit une fonctionnalité totale pour la surveillance et la communication avec le serveur Zabbix.



Les champs tels que le nom d'hôte, l'adresse IP/DNS du serveur Zabbix, le port d'écoute (10050) et les adresses de proxy actif sont renseignés pour établir une connexion efficace entre l'agent et le serveur. Ces réglages sont fondamentaux pour garantir une communication fluide.



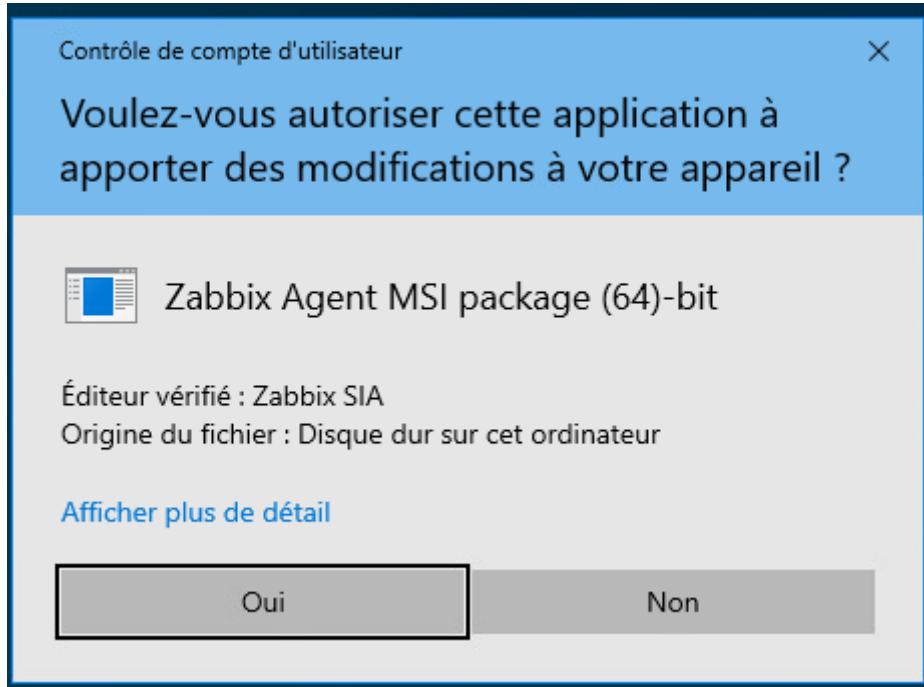
Un autre hôte, nommé UTI107-AdminW10, est configuré avec des paramètres similaires, ce qui démontre la flexibilité et la possibilité de gérer plusieurs agents sur différents systèmes.



La ligne Server=10.0.107.21 est ajoutée pour spécifier l'adresse IP du serveur Zabbix. Cette méthode offre une alternative manuelle utile pour les environnements nécessitant une personnalisation supplémentaire.

```
File Edit Selection View ... ← → Search [Administrator] Manage Learn More
Restricted Mode is intended for safe code browsing. Trust this window to enable all features.
zabbix_agentd.conf •
C: > Program Files > Zabbix Agent > zabbix_agentd.conf
96
97     ### Option: Server
98     # List of comma delimited IP addresses, optionally in CIDR notation, or DNS names of Zabbix servers
99     # Incoming connections will be accepted only from the hosts listed here.
100    # If IPv6 support is enabled then '127.0.0.1', '::127.0.0.1', '::ffff:127.0.0.1' are treated equivalently
101    # '0.0.0.0/0' can be used to allow any IPv4 address.
102    # Example: Server=127.0.0.1,192.168.1.0/24,::1,2001:db8::/32,zabbix.domain
103    #
104    # Mandatory: yes, if StartAgents is not explicitly set to 0
105    # Default:
106    # Server=
107
108    Server=10.0.107.21
109
110   ### Option: ListenPort
111   # Agent will listen on this port for connections from the server.
112   #
113   # Mandatory: no
114   # Range: 1024-32767
115   # Default:
116   # ListenPort=10050
117
118
119   ### Option: ListenIP
120   # List of comma delimited IP addresses that the agent should listen on.
121   # First IP address is sent to Zabbix server if connecting to it to retrieve list of active checks
122   #
123   # Mandatory: no
124   # Default:
125   # ListenIP=0.0.0.0
126
127
128   ### Option: StartAgents
```

La demande de confirmation sous Windows garantit la sécurité en exigeant une validation avant l'installation. L'éditeur « Zabbix SIA » identifié renforce la confiance quant à l'origine du fichier.



### Installation sur Linux

Nous sélectionnons les versions correspondantes pour installer Zabbix Agent sur Ubuntu, en choisissant l'architecture, la version LTS pour sa stabilité, et un format adapté comme le paquet archive pour une intégration fluide dans l'environnement Linux.

Show legacy downloads 

OS DISTRIBUTION	OS VERSION	HARDWARE	ZABBIX VERSION	ENCRYPTION	PACKAGING
Windows	4.12	ppc64le	6.0 LTS	No encryption	Archive
Linux	3.0		5.4		
macOS	2.6		5.0 LTS		
AIX	2.4		4.0 LTS		
FreeBSD					
OpenBSD					
Solaris					

```
tar -xvf zabbix_agent-6.0.3-linux-4.12-ppc64le-static.tar.gz
```

L'extraction de l'archive Zabbix, réalisée à l'aide de la commande tar -xvf, permet de décompresser les fichiers nécessaires au fonctionnement de l'agent dans le répertoire de travail. Cette opération garantit une organisation claire des composants, incluant les exécutables et les fichiers de configuration indispensables, comme zabbix\_agentd.conf. Ce choix permet une inspection préalable avant le déploiement.

```
serveur-web@serveurweb-virtual-machine:~$ tar -xvf zabbix_agent-6.0.3-linux-4.12-ppc64le-static.tar.gz
zabbix_agent-6.0.3-linux-4.12-ppc64le-static/
zabbix_agent-6.0.3-linux-4.12-ppc64le-static/usr/
zabbix_agent-6.0.3-linux-4.12-ppc64le-static/usr/sbin/
zabbix_agent-6.0.3-linux-4.12-ppc64le-static/usr/sbin/zabbix_agentd
zabbix_agent-6.0.3-linux-4.12-ppc64le-static/usr/bin/
zabbix_agent-6.0.3-linux-4.12-ppc64le-static/usr/bin/zabbix_get
zabbix_agent-6.0.3-linux-4.12-ppc64le-static/usr/bin/zabbix_sender
zabbix_agent-6.0.3-linux-4.12-ppc64le-static/usr/share/
zabbix_agent-6.0.3-linux-4.12-ppc64le-static/usr/share/man/
zabbix_agent-6.0.3-linux-4.12-ppc64le-static/usr/share/man/man1/
zabbix_agent-6.0.3-linux-4.12-ppc64le-static/usr/share/man/man1/zabbix_get.1
zabbix_agent-6.0.3-linux-4.12-ppc64le-static/usr/share/man/man1/zabbix_sender.1
zabbix_agent-6.0.3-linux-4.12-ppc64le-static/usr/share/man/man8/
zabbix_agent-6.0.3-linux-4.12-ppc64le-static/usr/share/man/man8/zabbix_agentd.8
zabbix_agent-6.0.3-linux-4.12-ppc64le-static/etc/
zabbix_agent-6.0.3-linux-4.12-ppc64le-static/etc/zabbix/zabbix_agentd.conf.d/
zabbix_agent-6.0.3-linux-4.12-ppc64le-static/etc/zabbix/zabbix_agentd.conf
```

Ensuite, le déplacement du répertoire décompressé vers /usr/local/zabbix avec la commande mv offre un emplacement centralisé pour l'exécution de l'agent. L'adoption de ce chemin standard facilite la gestion à long terme et simplifie les mises à jour ou l'intégration avec d'autres services. Ces actions assurent une structure propre et conforme aux pratiques recommandées.

```
sudo mv zabbix_agent-6.0.3-linux-4.12-ppc64le-static /usr/local/zabbix
```

```
cd /usr/local/zabbix
```

```
serveur-web@serveurweb-virtual-machine:~$ sudo mv zabbix_agent-6.0.3-linux-4.12-ppc64le-static /usr/local/zabbix
serveur-web@serveurweb-virtual-machine:~$ cd /usr/local/zabbix
serveur-web@serveurweb-virtual-machine:/usr/local/zabbix$ s
```

```
sudo nano /usr/local/zabbix/zabbix_agentd.conf
```

```
serveur-web@serveurweb-virtual-machine:/usr/local/zabbix$ sudo nano /usr/local/zabbix/zabbix_agentd.conf
```

L'édition du fichier de configuration zabbix\_agentd.conf permet de définir les paramètres essentiels pour le fonctionnement de l'agent Zabbix. La commande utilisée dans le terminal lance l'éditeur de texte nano pour modifier ce fichier directement dans le répertoire d'installation. L'option Server est définie avec l'adresse IP du serveur Zabbix (10.0.107.21), garantissant une communication avec le système central.

```
Server=ZABBIX_SERVER_IP
```

```
ListenPort=10050
```

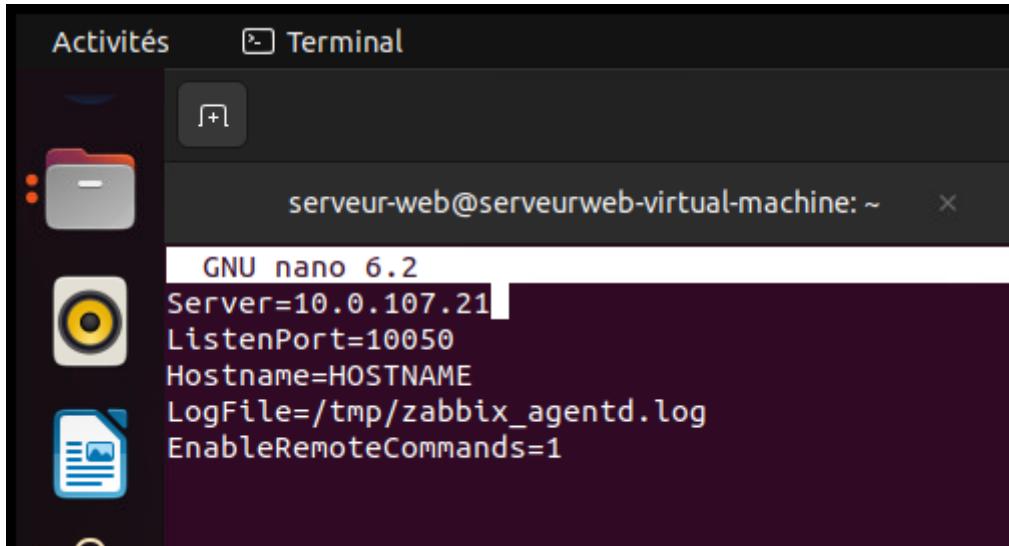
```
Hostname=HOSTNAME
```

```
LogFile=/tmp/zabbix_agentd.log
```

```
EnableRemoteCommands=1
```

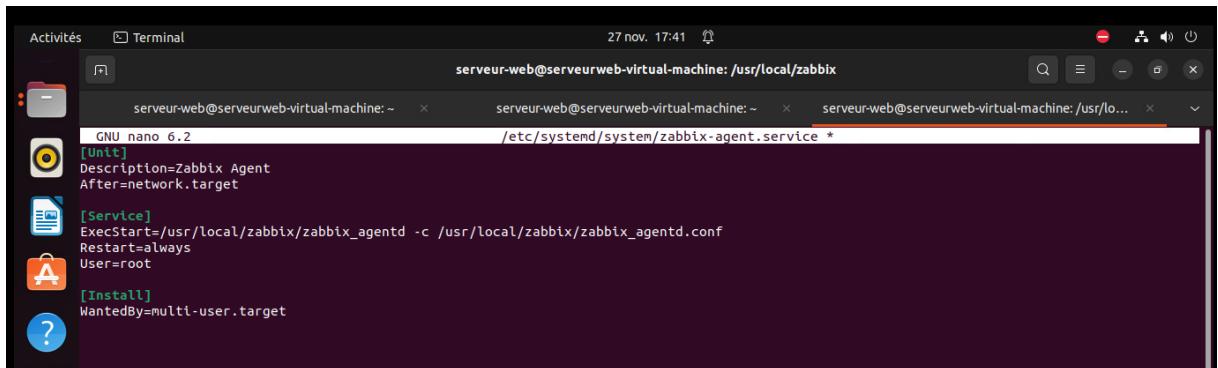
Le contenu du fichier montre des réglages comme le port d'écoute ListenPort=10050, qui est standard pour les agents Zabbix. Le champ Hostname permet d'identifier clairement la machine dans l'interface du serveur. Le chemin vers le fichier de log est spécifié avecLogFile=/tmp/zabbix\_agentd.log pour faciliter le suivi des événements. Enfin, l'activation de la

commande à distance avec `EnableRemoteCommands=1` permet au serveur d'exécuter des tâches directement sur l'agent, ce qui améliore la gestion et l'automatisation des opérations.



```
GNU nano 6.2
Server=10.0.107.21
ListenPort=10050
Hostname=HOSTNAME
LogFile=/tmp/zabbix_agentd.log
EnableRemoteCommands=1
```

```
./zabbix_agentd -c /usr/local/zabbix/zabbix_agentd.conf
```



```
[Unit]
Description=Zabbix Agent
After=network.target

[Service]
ExecStart=/usr/local/zabbix/zabbix_agentd -c /usr/local/zabbix/zabbix_agentd.conf
Restart=always
User=root

[Install]
WantedBy=multi-user.target
```

La commande `sudo nano /etc/systemd/system/zabbix-agent.service` permet de créer ou modifier un fichier de service `systemd` pour gérer l'agent Zabbix. Voici une analyse technique et justifiée du contenu du fichier de service configuré :

```
sudo nano /etc/systemd/system/zabbix-agent.service
```

```
[Unit]
Description=Zabbix Agent
After=network.target

[Service]
```

```
ExecStart=/usr/local/zabbix/zabbix_agentd -c /usr/local/zabbix/zabbix_agentd.conf
Restart=always
User=root

[Install]
WantedBy=multi-user.target
```

Si on analyse le contenu précédent :

#### [Unit]

- Description=Zabbix Agent : Fournit une brève description pour identifier clairement le service, ici l'agent Zabbix.
- After=network.target : Garantit que le service ne démarre qu'après que les services réseau nécessaires sont opérationnels. Cette dépendance est cruciale pour l'agent qui communique avec le serveur Zabbix.

#### [Service]

- ExecStart=/usr/local/zabbix/zabbix\_agentd -c /usr/local/zabbix/zabbix\_agentd.conf : Spécifie la commande à exécuter pour démarrer l'agent, en utilisant explicitement le chemin vers le fichier de configuration.
- Restart=always : Configure un redémarrage automatique en cas d'échec du service. Cette directive améliore la résilience et la disponibilité.
- User=root : Définit que le service s'exécute avec les priviléges de l'utilisateur root, garantissant un accès complet aux ressources nécessaires pour le fonctionnement de l'agent.

#### [Install]

- WantedBy=multi-user.target : Permet au service d'être activé pour le mode multi-utilisateur, correspondant à un état standard pour les systèmes Linux en production.

La configuration assure une exécution stable et efficace de l'agent Zabbix, ce qui est essentiel dans des environnements où une supervision en temps réel est indispensable. En définissant des dépendances réseau et des commandes claires, elle garantit une intégration fluide dans l'écosystème système.

La directive `Restart=always` renforce la résilience en redémarrant automatiquement le service en cas de défaillance. Cette redondance est particulièrement importante pour maintenir une continuité des opérations et éviter les interruptions dans la surveillance.

Placer le fichier dans le répertoire `/etc/systemd/system/` permet de le reconnaître comme une unité personnalisée. Cette séparation des configurations standard et spécifiques améliore la gestion des services, offrant une flexibilité accrue pour les administrateurs système.

```
sudo systemctl daemon-reload
sudo systemctl enable zabbix-agent
sudo systemctl start zabbix-agent

sudo systemctl status zabbix-agent
```

Après avoir défini et enregistré la configuration de l'agent Zabbix dans le fichier de service `systemd`, il est nécessaire de recharger le démon `systemd` avec la commande `sudo systemctl daemon-reload`. Cela permet au système d'actualiser sa liste de services et de prendre en compte le fichier nouvellement ajouté. Ce choix garantit que le service personnalisé est correctement détecté et prêt à être activé.

La commande `sudo systemctl enable zabbix-agent` active le démarrage automatique de l'agent Zabbix au démarrage du système. Cela est essentiel pour assurer la continuité du monitoring, même après un redémarrage. Cette option renforce la fiabilité du service en s'assurant qu'il est opérationnel sans intervention manuelle.

L'exécution de `sudo systemctl start zabbix-agent` initialise l'agent Zabbix, activant ainsi la communication entre l'agent et le serveur central. Cette commande est cruciale pour démarrer effectivement le processus de surveillance configuré.

Enfin, `sudo systemctl status zabbix-agent` permet de vérifier que le service a bien démarré et fonctionne comme prévu. L'affichage des journaux et de l'état actuel donne un aperçu des éventuelles erreurs ou des confirmations de bon fonctionnement, facilitant le diagnostic en cas de problème. Ces commandes successives garantissent une mise en place robuste et fiable du service de surveillance.

## Via les repositories Zabbix (linux)

```
ifconfig
```

```
sudo apt update && sudo apt upgrade -y
```

L'accès au dépôt officiel de Zabbix permet de récupérer des paquets fiables et adaptés aux différentes versions d'Ubuntu, garantissant une compatibilité avec l'environnement cible. La sélection des fichiers, comme les versions spécifiques pour Ubuntu 22.04, est facilitée grâce à une organisation claire des paquets, ce qui réduit les risques d'erreurs liées à des incompatibilités.



## ZABBIX Zabbix Official Repository

Zabbix Official Repository provides installation packages for Red Hat Enterprise Linux, CentOS, Oracle Linux, Ubuntu, Debian, SUSE Linux Enterprise Server and even Raspbian.

These packages are created and officially supported by Zabbix SIA.

Installation instructions are available in [Zabbix download](#) page and [Zabbix documentation](#).

If you have any problems or suggestions, please report an issue on [Zabbix Bug Tracking System](#).

If you want to get professional support, installation or upgrade service, please see our [Zabbix technical support service](#) page.

### Index of /zabbix/7.0/ubuntu/pool/main/z/zabbix-release/

..		
<a href="#">zabbix-release_7.0-1+ubuntu16.04.dsc</a>	03-Jun-2024 05:57	1542
<a href="#">zabbix-release_7.0-1+ubuntu16.04.tar.gz</a>	03-Jun-2024 05:57	5987
<a href="#">zabbix-release_7.0-1+ubuntu16.04_all.deb</a>	03-Jun-2024 05:57	5926
<a href="#">zabbix-release_7.0-1+ubuntu18.04.dsc</a>	03-Jun-2024 05:57	1542
<a href="#">zabbix-release_7.0-1+ubuntu18.04.tar.gz</a>	03-Jun-2024 05:57	5962
<a href="#">zabbix-release_7.0-1+ubuntu18.04_all.deb</a>	03-Jun-2024 05:57	6012
<a href="#">zabbix-release_7.0-1+ubuntu20.04.dsc</a>	03-Jun-2024 05:57	1542
<a href="#">zabbix-release_7.0-1+ubuntu20.04.tar.gz</a>	03-Jun-2024 05:57	5958
<a href="#">zabbix-release_7.0-1+ubuntu20.04_all.deb</a>	03-Jun-2024 05:57	6012
<a href="#">zabbix-release_latest+ubuntu16.04_all.deb</a>		
<a href="#">zabbix-release_latest+ubuntu18.04_all.deb</a>		
<a href="#">zabbix-release_latest+ubuntu20.04_all.deb</a>		
<a href="#">zabbix-release_latest+ubuntu22.04_all.deb</a>		
<a href="#">zabbix-release_latest+ubuntu24.04_all.deb</a>		

Le téléchargement du fichier zabbix-release avec la commande wget est une méthode simple et efficace, particulièrement adaptée aux environnements de serveur où les interfaces graphiques ne sont pas disponibles. Une fois le fichier téléchargé, une vérification rapide avec la commande ls confirme sa présence dans le répertoire de travail, assurant que l'installation peut se poursuivre sans problème.

```
serveur-web@serveurweb-virtual-machine: ~ $ wget https://repo.zabbix.com/zabbix/7.0/ubuntu/pool/main/z/zabbix-release/zabbix-release_latest+ubuntu22.04_all.deb
--2024-11-28 22:55:19-- https://repo.zabbix.com/zabbix/7.0/ubuntu/pool/main/z/zabbix-release/zabbix-release_latest+ubuntu22.04_all.deb
Résolution de repo.zabbix.com (repo.zabbix.com)... 178.128.6.101, 2604:a880:2:d0::2062:d001
Connexion à repo.zabbix.com (repo.zabbix.com)|178.128.6.101|:443... connecté.
requête HTTP transmise, en attente de la réponse... 200 OK
Taille : 8288 (8,1K) [application/octet-stream]
Enregistre : 'zabbix-release_latest+ubuntu22.04_all.deb'

zabbix-release_latest+ubuntu22.04_all.deb 100%[=====] 8,09K --.-KB/s   0s

2024-11-28 22:55:19 (92,7 MB/s) - 'zabbix-release_latest+ubuntu22.04_all.deb' enregistré [8288/8288]
```

La commande « ls » confirme la présence du fichier zabbix-release\_latest+ubuntu22.04\_all.deb, essentiel pour configurer les dépôts officiels de Zabbix sur un système Ubuntu 22.04. Ce fichier .deb contient les informations nécessaires pour ajouter le dépôt Zabbix et assurer la compatibilité des mises à jour et des installations futures. Sa vérification garantit que l'installation peut continuer sans interruption ou erreur.

```
serveur-web@serveurweb-virtual-machine: $ ls
2024   elementor           Musique      theplus-addons  wp-settings.php
Backup  essential-addons-elementor  Public       Vidéos       zabbix_agent-6.8.3-linux-4.12-ppc64le-static.tar.gz
Bureau  Images             snap        wpforms      zabbix-release_latest+ubuntu22.04_all.deb
Documents Modèles          Téléchargements  wpo
```

L'installation du fichier .deb à l'aide de sudo dpkg -i intègre automatiquement le dépôt Zabbix dans le système de gestion de paquets d'Ubuntu. Cette configuration simplifie les mises à jour et la gestion des paquets à l'avenir.

```
serveur-web@serveurweb-virtual-machine:~$ sudo dpkg -i zabbix-release_latest+ubuntu22.04_all.deb
Sélection du paquet zabbix-release précédemment désélectionné.
(Lecture de la base de données... 209068 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de zabbix-release_latest+ubuntu22.04_all.deb ...
Dépaquetage de zabbix-release (1:7.0-2+ubuntu22.04) ...
Paramétrage de zabbix-release (1:7.0-2+ubuntu22.04) ...
```

Ensuite, la commande sudo apt update synchronise le gestionnaire de paquets avec les nouveaux dépôts, garantissant que toutes les versions récentes des paquets nécessaires sont disponibles.

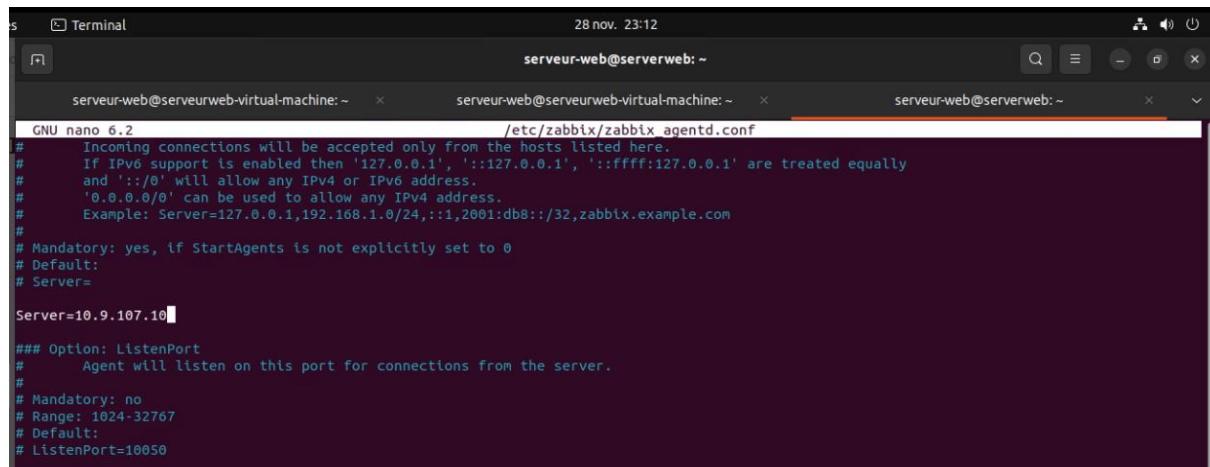
```
serveur-web@serveurweb-virtual-machine: $ sudo apt update
Atteint :1 http://fr.archive.ubuntu.com/ubuntu jammy InRelease
Atteint :2 http://fr.archive.ubuntu.com/ubuntu jammy-updates InRelease
Atteint :3 http://security.ubuntu.com/ubuntu jammy-security InRelease
Atteint :4 http://fr.archive.ubuntu.com/ubuntu jammy-backports InRelease
Réception de :5 https://repo.zabbix.com/zabbix-tools/debian-ubuntu jammy InRelease [2 473 B]
Réception de :6 https://repo.zabbix.com/zabbix/7.0/ubuntu jammy InRelease [3 220 B]
Réception de :7 https://repo.zabbix.com/zabbix-tools/debian-ubuntu jammy/main Sources [960 B]
Réception de :8 https://repo.zabbix.com/zabbix-tools/debian-ubuntu jammy/main all Packages [657 B]
Réception de :9 https://repo.zabbix.com/zabbix/7.0/ubuntu jammy/main Sources [12,0 kB]
Réception de :10 https://repo.zabbix.com/zabbix/7.0/ubuntu jammy/main amd64 Packages [22,6 kB]
Réception de :11 https://repo.zabbix.com/zabbix/7.0/ubuntu jammy/main all Packages [4 951 B]
46,8 ko réceptionnés en 2s (29,2 ko/s)
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Tous les paquets sont à jour.
N: Le fichier configuré « main/binary-i386/Packages » ne sera pas pris en compte car le dépôt « https://repo.zabbix.com/zabbix/7.0/ubuntu jammy InRelease » ne prend pas en charge l'architecture « i386 »
serveur-web@serveurweb-virtual-machine: $
```

Pour installer l'agent Zabbix, la commande “sudo apt install zabbix-agent -y” est utilisée. Ce choix permet de gérer facilement les dépendances requises par l'agent et de s'assurer que l'installation est complète et fonctionnelle. Une fois installé, le fichier de configuration de l'agent, zabbix\_agentd.conf, est modifié via l'éditeur de texte nano pour définir l'adresse IP ou le nom DNS du serveur Zabbix. Ces paramètres sont cruciaux pour établir une connexion entre l'agent et le serveur.

```
serveur-web@serveurweb-virtual-machine: ~ $ sudo apt install zabbix-agent -y
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets suivants ont été installés automatiquement et ne sont plus nécessaires :
  libflashrom1 libftdi1-2 liblvm13
Veuillez utiliser « sudo apt autoremove » pour les supprimer.
Les paquets supplémentaires suivants seront installés :
  libmodbus5
Les NOUVEAUX paquets suivants seront installés :
  libmodbus5 zabbix-agent
0 mis à jour, 2 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 317 ko dans les archives.
Après cette opération, 926 ko d'espace disque supplémentaires seront utilisés.
Réception de :1 http://fr.archive.ubuntu.com/ubuntu jammy/universe amd64 libmodbus5 amd64 3.1.6-2 [23,5 kB]
Réception de :2 https://repo.zabbix.com/zabbix/7.0/ubuntu jammy/main amd64 zabbix-agent amd64 1:7.0.6-1+ubuntu22.04 [293 kB]
317 ko réceptionnés en 1s (235 ko/s)
Sélection du paquet libmodbus5:amd64 précédemment désélectionné.
(Lecture de la base de données... 209077 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../libmodbus5_3.1.6-2_amd64.deb ...
Dépaquetage de libmodbus5:amd64 (3.1.6-2) ...
Sélection du paquet zabbix-agent précédemment désélectionné.
Préparation du dépaquetage de .../zabbix-agent_1%3a7.0.6-1+ubuntu22.04_amd64.deb ...
Dépaquetage de zabbix-agent (1:7.0.6-1+ubuntu22.04) ...
Progression : [ 33%] [#####
.....
```

Pour installer l'agent Zabbix, la commande `sudo apt install zabbix-agent` est utilisée. Ce choix permet de gérer facilement les dépendances requises par l'agent et de s'assurer que l'installation est complète et fonctionnelle. Une fois installé, le fichier de configuration de l'agent, `zabbix_agentd.conf`, est modifié via l'éditeur de texte nano pour définir l'adresse IP ou le nom DNS du serveur Zabbix. Ces paramètres sont cruciaux pour établir une connexion entre l'agent et le serveur.

Server=10.9.107.10



```
serveur-web@serveurweb-virtual-machine: ~ 28 nov. 23:12
serveur-web@serverweb: ~
serveur-web@serverweb: ~

GNU nano 6.2 /etc/zabbix/zabbix_agentd.conf
# Incoming connections will be accepted only from the hosts listed here.
# If IPv6 support is enabled then '127.0.0.1', '::127.0.0.1', '::ffff:127.0.0.1' are treated equally
# and '::/0' will allow any IPv4 or IPv6 address.
# '0.0.0.0/0' can be used to allow any IPv4 address.
# Example: Server=127.0.0.1,192.168.1.0/24,::1,2001:db8::/32,zabbix.example.com
#
# Mandatory: yes, if StartAgents is not explicitly set to 0
# Default:
# Server=

Server=10.9.107.10

### Option: ListenPort
#       Agent will listen on this port for connections from the server.
#
# Mandatory: no
# Range: 1024-32767
# Default:
# ListenPort=10050
```

Enfin, la configuration des vérifications actives via le paramètre `ServerActive=Adresse IP` du serveur web (`ServerActive=10.9.107.10`) permet à l'agent d'envoyer activement des données au serveur Zabbix. Cette fonctionnalité est essentielle pour les environnements où la proactivité et la rapidité de communication sont des exigences clés. Toutes ces étapes assurent une installation optimisée et un fonctionnement fluide de l'agent Zabbix sur un système Ubuntu.

```
#           If port is not specified, default port is used.
#           IPv6 addresses must be enclosed in square brackets if port for the
#           If port is not specified, square brackets for IPv6 addresses are
#           If this parameter is not specified, active checks are disabled.
#           Example: ServerActive=127.0.0.1:20051,zabbix.domain,[::1]:30051,:
#
# Mandatory: no
# Default:
# ServerActive=

ServerActive=10.9.107.10

### Option: Hostname
#           Unique, case sensitive hostname.
#           Required for active checks and must match hostname as configured
#           Value is acquired from HostnameItem if undefined.
#
# Mandatory: no
# Default:
Hostname=serverweb

### Option: HostnameItem
#           Item used for generating Hostname if it is undefined. Ignored if
#           Does not support UserParameters or aliases.
#
# Mandatory: no
# Default:
# HostnameItem=system.hostname

### Option: HostMetadata
```

## Conclusion

Cet atelier sur Zabbix a été une véritable immersion dans l'univers de la supervision et de la gestion des infrastructures. La mise en place initiale du serveur Zabbix et de ses agents s'est révélée complexe, notamment en raison de la configuration des dépendances et des ajustements réseau. Ces défis techniques m'ont permis de consolider mes connaissances en administration système et en gestion des services réseau.

La création et la configuration des hôtes ainsi que des éléments de surveillance ont exigé beaucoup de rigueur pour garantir une collecte de données fiable et utile. J'ai appris à concevoir des déclencheurs précis pour identifier les anomalies et à structurer des tableaux de bord efficaces pour centraliser et visualiser les informations essentielles sur les performances des systèmes.

La mise en place de notifications et d'alertes m'a confronté à d'autres difficultés, notamment dans le choix et l'intégration des canaux de communication et dans la définition de seuils adaptés. Cet apprentissage m'a sensibilisé à l'importance d'un paramétrage équilibré pour éviter une surcharge d'alertes tout en garantissant une bonne réactivité face aux incidents.

Pour Conclure, cet atelier m'a permis d'acquérir une vision plus claire et une meilleure maîtrise des outils de supervision comme Zabbix. Les difficultés rencontrées ont été enrichissantes, car elles m'ont aidé à développer des compétences pratiques et à adopter une démarche méthodique dans la gestion et le suivi des systèmes.

## Webographie

**Qu'est-ce qu'un serveur de monitoring – Splunk :** [https://www.splunk.com/fr\\_fr/data-insider/what-is-server-monitoring.html](https://www.splunk.com/fr_fr/data-insider/what-is-server-monitoring.html)

**Zabbix Download – Zabbix :**  
[https://www.zabbix.com/fr/download?zabbix=7.0&os\\_distribution=ubuntu\\_arm64&os\\_version=22.04&components=server\\_frontend\\_agent&db=pgsql&ws=apache](https://www.zabbix.com/fr/download?zabbix=7.0&os_distribution=ubuntu_arm64&os_version=22.04&components=server_frontend_agent&db=pgsql&ws=apache)

**Comment fonctionne le système de surveillance Zabbix ? – Bluffy (en anglais) :**  
<https://blurify.com/blog/video-surveillance-the-control-and-safety-thanks-to-zabbix/#:~:text=The%20Zabbix%20agent%20collects%20the,to%2Dread%20tables%20or%20charts.>

**Télécharger Putty – Putty :** <https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html>

**Templates Discord :**  
[https://git.zabbix.com/projects/ZBX/repos/zabbix/browse/templates/media/discord/media\\_discord.yaml](https://git.zabbix.com/projects/ZBX/repos/zabbix/browse/templates/media/discord/media_discord.yaml)

**Documentation officielle de Zabbix :**  
<https://www.zabbix.com/documentation>  
Ce site contient des informations complètes sur l'installation, la configuration et la gestion de Zabbix.

**Téléchargement de Zabbix :**  
<https://www.zabbix.com/fr/download>  
Fournit les fichiers nécessaires pour installer Zabbix sur différents systèmes.

**Tutoriels Linux pour Zabbix :**  
<https://linuxhint.com/install-zabbix-server-ubuntu/>  
Guide détaillé pour l'installation et la configuration de Zabbix sur Ubuntu.

**Qu'est-ce qu'un serveur de monitoring (Splunk) :**  
[https://www.splunk.com/fr\\_fr/data-insider/what-is-server-monitoring.html](https://www.splunk.com/fr_fr/data-insider/what-is-server-monitoring.html)  
Ce lien offre une introduction générale aux concepts de monitoring des serveurs.

**Support officiel Zabbix :**  
<https://support.zabbix.com/>  
Idéal pour signaler des problèmes ou poser des questions techniques.

**Tutoriels en français sur Zabbix par Xavki :** <https://xavki.blog/zabbix-tutoriels-francais/>

**Tutoriel d'installation et de configuration de Zabbix sur Ubuntu 20.04 :**  
<https://www.digitalocean.com/community/tutorials/how-to-install-and-configure-zabbix-to-securely-monitor-remote-servers-on-ubuntu-20-04-fr>

Communauté Francophone de la Supervision Libre : <https://wiki.monitoring-fr.org/zabbix/start.html>

Tutoriel vidéo : "Comment surveiller son réseau informatique avec Zabbix" :  
[https://www.youtube.com/watch?v=3lc\\_EEbJhAU](https://www.youtube.com/watch?v=3lc_EEbJhAU)