PROCÉDURE TECHNIQUE · BTS SIO SISR

Installer Zabbix 7.0 LTS sur Debian 13 (Apache, MariaDB, Agent 2)

Mettre en service un serveur de supervision Zabbix avec son interface web, sa base MariaDB et la supervision de la machine elle-même.

Auteur	Plot 1
Contexte	TP réalisé en équipe — Plot 1, domaine ngrange.local
Version	2.0 — novembre 2026
Environnement	Debian 13 · Zabbix 7.0.32 LTS · Apache 2 · MariaDB · PHP 8.4 · Zabbix Agent 2
Durée estimée	30 à 45 min

Identifiants d'accès — Plot 1

Machine / service	Adresse	Identifiant	Mot de passe
SRV-ZABBIX (SSH)	192.168.21.4	`sio2`	`Azerty13.`
Base MariaDB	localhost / zabbix	`zabbix`	`Azerty13.`
Zabbix (web)	http://192.168.21.4/zabbix/	`Admin`	`zabbix (par défaut, à remplacer)`

Sommaire

1. Objectif
2. Architecture et prérequis
3. Installation et configuration
4. Vérification
5. Dépannage
6. Sécurité et bonnes pratiques
7. Aide-mémoire : utiliser Zabbix au quotidien

1. Objectif

Zabbix est une plateforme libre de supervision : elle collecte des métriques (CPU, mémoire, disques, services), déclenche des alertes et les affiche dans un tableau de bord. Cette procédure installe, sur une VM Debian 13 nommée **SRV-ZABBIX**, le serveur Zabbix 7.0 LTS, son interface web (Apache + PHP), sa base de données MariaDB et l'agent Zabbix Agent 2, qui permet au serveur de se superviser lui-même.

2. Architecture et prérequis

Élément	Valeur
Machine	VM **SRV-ZABBIX** (VMID 204, SRV-ZABBIX.ngrange.local), Debian 13, accès Internet, compte avec `sudo`
Adresse IP	`192.168.21.4` (LAN 192.168.21.0/24, passerelle 192.168.21.254, DNS 192.168.21.1 puis 192.168.21.2) ; vérifier avec `hostname -I`
Zabbix	7.0.32 LTS (serveur et frontend)
Services	Apache 2, MariaDB, PHP 8.4 (fourni par Debian 13), Zabbix Agent 2
Base de données	Base `zabbix` (utf8mb4, collation `utf8mb4_bin`), utilisateur `zabbix@localhost`
Ports	80/TCP (interface web), 10051/TCP (serveur Zabbix, écoute des agents actifs), 10050/TCP (agent)
Accès web	`http://192.168.21.4/zabbix/`

> **Captures**
> Les captures proviennent du TP réalisé en équipe : les adresses et noms visibles peuvent différer ; les valeurs à utiliser sont celles du texte (Plot 1).

> **À savoir**
> Remplacer tous les textes entre chevrons par des valeurs réelles et uniques. Aucun mot de passe réel n'apparaît dans ce document.

3. Installation et configuration

1 Préparer le système et installer Apache et MariaDB

Mettre le système à jour, puis installer le serveur web et la base de données qui hébergeront Zabbix.

```
sudo apt update
sudo apt full-upgrade -y
sudo apt install -y wget apache2 mariadb-server
sudo systemctl enable --now apache2 mariadb
```

Sécuriser MariaDB (suppression des comptes anonymes et de la base de test, root distant interdit) :

```
sudo mariadb-secure-installation
```

2 Ajouter le dépôt officiel Zabbix 7.0

Les paquets Zabbix de la distribution sont plus anciens : le dépôt officiel fournit la branche 7.0 LTS. Le paquet `zabbix-release` déclare le dépôt et sa clé de signature.

```
cd /tmp
REPO=https://repo.zabbix.com/zabbix/7.0/debian/pool/main/z/zabbix-release
wget "$REPO/zabbix-release_7.0-5+debian13_all.deb" -O zabbix-release.deb
sudo dpkg -i zabbix-release.deb
sudo apt update
```

> **Numéro de paquet**
>
> Le suffixe « 7.0-5 » est celui du TP ; s'il n'existe plus, consulter `https://repo.zabbix.com/zabbix/7.0/debian/pool/main/z/zabbix-release/` pour le nom en vigueur.

3 Installer les composants Zabbix

Serveur (support MySQL/MariaDB), interface PHP, configuration Apache, scripts SQL du schéma et agent.

```
sudo apt install -y zabbix-server-mysql zabbix-frontend-php
sudo apt install -y zabbix-apache-conf zabbix-sql-scripts
sudo apt install -y zabbix-agent2
zabbix_server --version | head -n 1
```

> **Contrôle**
>
> La dernière commande doit afficher une version 7.0.x.

4 Créer la base et le compte SQL dédié

Zabbix exige la collation `utf8mb4_bin` (sensibilité à la casse). Le compte `zabbix` n'a de droits que sur la base `zabbix`. Le paramètre `log_bin_trust_function_creators` est activé le temps de l'import, car le schéma crée des triggers et fonctions alors que la journalisation binaire est active.

```
sudo mariadb

CREATE DATABASE zabbix CHARACTER SET utf8mb4 COLLATE utf8mb4_bin;
CREATE USER 'zabbix'@'localhost'
  IDENTIFIED BY 'Azerty13.';
GRANT ALL PRIVILEGES ON zabbix.* TO 'zabbix'@'localhost';
SET GLOBAL log_bin_trust_function_creators = 1;
FLUSH PRIVILEGES;
EXIT;
```

> **Mot de passe**
>
> `Azerty13.` est le mot de passe commun du laboratoire Plot 1 ; en production, utiliser un secret fort et unique. Ne jamais utiliser le compte root MariaDB dans Zabbix.

5 Importer le schéma et rétablir le paramètre MariaDB

Importer le schéma initial fourni par Zabbix, contrôler la version de schéma, puis désactiver à nouveau l'option temporaire (elle abaisse la sécurité si elle reste active).

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

mysql -uzabbix -p zabbix -e "SELECT mandatory,optional FROM dbversion;"

sudo mariadb -e "SET GLOBAL log_bin_trust_function_creators = 0;"
```

L'import dure plusieurs minutes sur une petite VM ; la requête `dbversion` doit renvoyer une ligne (valeurs numériques).

6 Configurer le serveur Zabbix et PHP

Le serveur doit connaître les paramètres de la base. Éditer `/etc/zabbix/zabbix_server.conf` :

```
DBHost=localhost
DBName=zabbix
DBUser=zabbix
DBPassword=Azerty13.
```

Fixer le fuseau horaire PHP dans `/etc/php/8.4/apache2/php.ini` (le fichier `/etc/zabbix/apache.conf` installé par `zabbix-apache-conf` contient aussi une directive `php_value date.timezone` qu'on peut adapter à la place) :

```
date.timezone = Europe/Paris
```

> **Protéger le fichier**
>
> Il contient le mot de passe SQL : vérifier qu'il n'est pas lisible par tous (`ls -l /etc/zabbix/zabbix_server.conf` , propriétaire root:zabbix, mode 640).

7 Démarrer et activer les services

```
sudo systemctl restart zabbix-server zabbix-agent2 apache2
sudo systemctl enable zabbix-server zabbix-agent2 apache2
systemctl is-active zabbix-server zabbix-agent2 apache2
hostname -I
```

> **Résultat attendu**
>
> Trois lignes « active ». L'interface répond sur `http://192.168.21.4/zabbix/` .

8 Terminer l'assistant web

Ouvrir `http://192.168.21.4/zabbix/`, choisir la langue, valider la page des prérequis, puis saisir uniquement les valeurs suivantes :

Champ	Valeur
Type de base	MySQL
Hôte de base	localhost
Port	0 (port par défaut)
Base	zabbix
Utilisateur SQL	zabbix
Mot de passe	Le secret SQL créé à l'étape 4
Serveur Zabbix	localhost, port 10051
Fuseau horaire	Europe/Paris

Première connexion : identifiant `Admin` (avec une majuscule), mot de passe initial `zabbix` (valeur par défaut publique de Zabbix, à changer aussitôt).

9 Sécuriser le compte administrateur

- Changer immédiatement le mot de passe du compte `Admin` (Utilisateurs, Utilisateurs, Admin).
- Créer ensuite un compte administrateur nominatif.

4. Vérification

```
systemctl status zabbix-server zabbix-agent2 apache2 --no-pager
sudo tail -n 20 /var/log/zabbix/zabbix_server.log
sudo ss -tlnp | grep -E ':(80|10050|10051)\b'
curl -sI http://127.0.0.1/zabbix/ | head -n 1
```

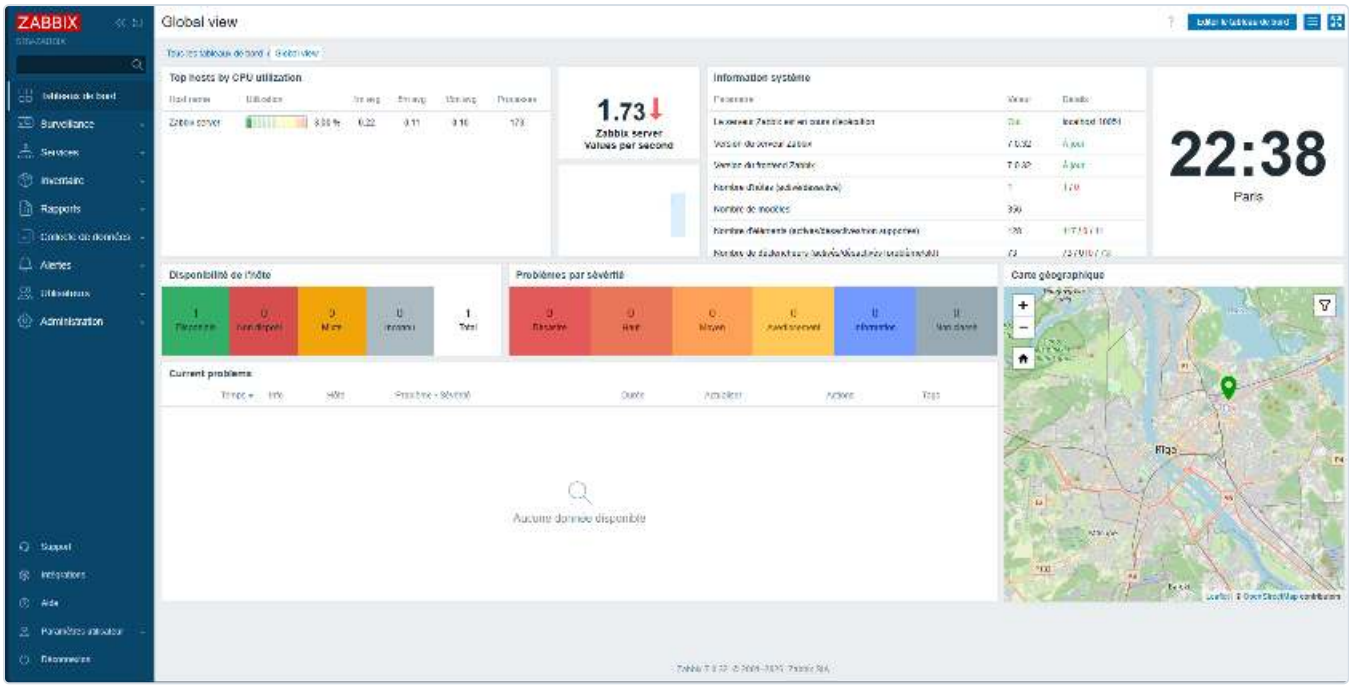

Figure 1 – Tableau de bord « Global view » : serveur en cours d'exécution, version 7.0.32 à jour pour le serveur et le frontend, 1 hôte disponible

Contrôle	Résultat attendu
Serveur	« Le serveur Zabbix est en cours d'exécution : Oui » (localhost:10051)
Version	Serveur et frontend en 7.0.32, mention « À jour »
Agent	Zabbix agent 2 actif ; l'hôte « Zabbix server » apparaît comme disponible
Journal	Aucune erreur de connexion à la base dans `zabbix_server.log`
Sécurité	Mot de passe Admin changé, secret SQL non exposé

Résultat attendu

Le tableau de bord s'affiche avec des données de l'hôte « Zabbix server » (CPU, processus) : la chaîne agent, serveur, base et interface fonctionne.

5. Dépannage

Symptôme	Cause probable	Solution
Assistant : « Cannot connect to the database »	Mot de passe, utilisateur ou base incorrects	Tester `mysql -uzabbix -p zabbix` ; corriger les valeurs de l'assistant
Import SQL en erreur sur les triggers	`log_bin_trust_function_creators` non activé	Le passer à 1 (étape 4), relancer l'import sur une base recréée vide
Prérequis PHP en échec (fuseau horaire)	`date.timezone` absent	Renseigner la directive (étape 6) puis `systemctl restart apache2`
« Zabbix server is not running » dans l'interface	Service arrêté ou mauvais `DBPassword`	`journalctl -u zabbix-server` et `/var/log/zabbix/zabbix_server.log` ; corriger puis redémarrer
Hôte « Zabbix server » indisponible	Agent 2 arrêté ou `Server=` incorrect	`systemctl status zabbix-agent2` ; vérifier `/etc/zabbix/zabbix_agent2.conf` (Server=127.0.0.1)
404 sur /zabbix	Configuration Apache Zabbix non chargée	Vérifier le paquet `zabbix-apache-conf` et `systemctl restart apache2`

6. Sécurité et bonnes pratiques

- Changer le mot de passe par défaut `Admin` / `zabbix` dès la première connexion et travailler avec des comptes nominatifs.
- Ne pas exposer l'interface sur Internet sans HTTPS (certificat reconnu) et sans filtrage réseau (pare-feu limitant 80/443 et 10051 aux réseaux utiles).
- Compte SQL dédié, limité à la base `zabbix` ; ne jamais utiliser root MariaDB ; ne jamais montrer le mot de passe SQL dans une capture.
- Rétablir `log_bin_trust_function_creators = 0` après l'import (étape 5).
- Sauvegarder régulièrement la base (`mariadb-dump --single-transaction zabbix`) et le dossier `/etc/zabbix` .
- Installer régulièrement les mises à jour Zabbix et Debian (`apt update && apt upgrade`) ; suivre le cycle de vie de la branche 7.0 LTS.

7. Aide-mémoire : utiliser Zabbix au quotidien

Chemins de menu de l'interface française de Zabbix 7.0 LTS (menu latéral : Tableaux de bord, Surveillance, Services, Inventaire, Rapports, Collecte de données, Alertes, Utilisateurs, Administration). Si un intitulé diffère, utiliser le champ de recherche du menu.

7.1 Installer l'agent sur la machine à superviser

1 Agent Linux (Debian/Ubuntu)

Ajouter le dépôt Zabbix 7.0 adapté à la distribution (étape 2), puis :

```
sudo apt install -y zabbix-agent2
sudo nano /etc/zabbix/zabbix_agent2.conf
#   Server=192.168.21.4          # contrôles passifs : serveur autorisé
#   ServerActive=192.168.21.4    # contrôles actifs
#   Hostname=<NOM_EXACT_DE_L_HOTE>      # doit être identique au nom saisi dans
l'interface
sudo systemctl enable --now zabbix-agent2
sudo systemctl status zabbix-agent2 --no-pager
```

Ouvrir le port 10050/TCP vers le serveur si un pare-feu est actif (par exemple `sudo ufw allow from 192.168.21.4 to any port 10050 proto tcp`).

2 Agent Windows

Télécharger le MSI « Zabbix agent 2 » 7.0 sur la page de téléchargements officielle, puis :

```
msiexec /i zabbix_agent2-7.0.<X>-windows-amd64-openssl.msi /qn SERVER=192.168.21.4
SERVERACTIVE=192.168.21.4 HOSTNAME=<NOM_EXACT_DE_L_HOTE>
```

- L'assistant graphique demande les mêmes trois valeurs. Fichier : `C:\Program Files\Zabbix Agent 2\zabbix_agent2.conf` ; service Windows « Zabbix Agent 2 » (redémarrer après modification).
- Autoriser le port 10050/TCP entrant dans le pare-feu Windows depuis le serveur.
- Hôtes du Plot 1 à superviser : SRV-AD1EX `192.168.21.1`, SRV-AD2 `192.168.21.2`, SRV-GLPI `192.168.21.3`, SRV-ARTICA `192.168.21.5` (agent), pfSense `192.168.21.254` (SNMP, voir 7.4) ; `Hostname` = nom exact saisi dans l'interface (par exemple `SRV-AD1EX`).

7.2 Ajouter un hôte, groupe d'hôtes et template

1 Collecte de données › Groupes d'hôtes › Créer un groupe d'hôtes

- Saisir un nom (par exemple « Serveurs Linux »). Les groupes servent à regrouper les hôtes et à attribuer les droits aux utilisateurs.

2 **Collecte de données › Hôtes › Créer un hôte**

- **Nom d'hôte** : exactement la valeur `Hostname` de l'agent ; **Modèles** : *Linux by Zabbix agent* ou *Windows by Zabbix agent* ; **Groupes d'hôtes** : au moins un ; **Interfaces** › Ajouter › Agent : IP (ou DNS) et port 10050 ; **Activé** coché. Cliquer sur « Ajouter ».
- Pour lier un template à un hôte existant : Collecte de données › Hôtes › [hôte] › champ **Modèles** › Sélectionner › Mettre à jour. Pour plusieurs hôtes : cocher les hôtes puis « Mise à jour en masse ». Les modèles disponibles sont listés dans Collecte de données › Modèles.
- Vérifier : Surveillance › Hôtes ; l'icône **ZBX** doit passer au vert sous 1 à 2 minutes.

7.3 Créer un item et un déclencheur

1 **Collecte de données › Hôtes › [hôte] › Éléments › Créer un élément**

- Champs : **Nom**, **Type** (Agent Zabbix), **Clé** (par exemple `system.cpu.load[all,avg1]`), **Type d'information** (numérique à virgule flottante), **Unités**, **Intervalle de mise à jour** (par exemple 1m), **Période de conservation de l'historique**.
- Tester une clé depuis le serveur : `zabbix_get -s 192.168.21.1 -k system.cpu.load[all,avg1]` (paquet `zabbix-get`), ou sur l'hôte : `sudo zabbix_agent2 -t system.cpu.load[all,avg1]`.

2 **Collecte de données › Hôtes › [hôte] › Déclencheurs › Créer un déclencheur**

- Champs : **Nom**, **Sévérité** (Information à Désastre), **Expression**, par exemple : `avg(/NOM_HOTE/system.cpu.load[all,avg1],5m)>2` (syntaxe Zabbix 6.0/7.0 ; utiliser le bouton « Ajouter » de l'éditeur d'expression).
- Le problème apparaît dans Surveillance › Problèmes tant que l'expression est vraie.

7.4 Superviser par SNMP (switch, pfSense)

1 **Activer SNMP sur l'équipement, puis créer l'hôte**

- Sur l'équipement : activer SNMP v2c (ou v3) et définir une communauté en lecture seule `<COMMUNAUTE_SNMP>` (jamais « public »). Sur pfSense : Services › SNMP.
- Zabbix : Collecte de données › Hôtes › Créer un hôte › Interfaces › Ajouter › **SNMP** : IP, port 161, version SNMPv2 (ou SNMPv3 avec ses paramètres), **Communauté** (par exemple via la macro `{$SNMP_COMMUNITY}` de l'hôte).
- Modèles : *Network Generic Device by SNMP* (switch générique) ou le modèle du constructeur ; *PFSense by SNMP* pour pfSense (vérifier leur présence dans Collecte de données › Modèles).
- Tester depuis le serveur : `snmpwalk -v2c -c <COMMUNAUTE_SNMP> 192.168.21.254 1.3.6.1.2.1.1.1.0` (paquet `snmp`). L'icône **SNMP** de l'hôte doit passer au vert.

7.5 Dashboards et graphiques

1 **Tableaux de bord › Créer un tableau de bord**

- Nommer, cliquer sur « Ajouter un widget » (Graphique, Problèmes, Carte, Horloge, etc.), choisir hôtes et éléments puis enregistrer. Bouton « Éditer le tableau de bord » en haut à droite pour modifier.
- Consultation rapide : Surveillance › Hôtes › [hôte] › Graphiques ou Dernières données ; Surveillance › Problèmes pour les alertes en cours.

7.6 Alertes par courriel

1 **Alertes › Types de média › E-mail**

- Renseigner **Serveur SMTP**, **Port**, **Sécurité de connexion**, **Authentification** (utilisateur, mot de passe `<MOT_DE_PASSE>`), **E-mail expéditeur**. Utiliser le bouton « Tester » du type de média.

2 **Utilisateurs › Utilisateurs › [utilisateur] › onglet Média › Ajouter**

- Type : E-mail, destinataire, périodes d'envoi et sévérités acceptées.

3 **Alertes › Actions › Actions de déclencheur › Créer une action**

- **Conditions** (par exemple groupe d'hôtes, sévérité ≥ Haut) ; onglet **Opérations** › Ajouter : envoyer un message à un utilisateur ou groupe via E-mail. Ajouter si besoin une opération de récupération. Historique : Rapports › Journal d'actions.

7.7 Maintenance

1 **Collecte de données › Maintenance › Créer une période de maintenance**

- Nom, **Type de maintenance** (avec ou sans collecte de données), période active, **Périodes** (une fois, quotidienne, etc.), **Hôtes** ou groupes concernés. Pendant la maintenance, les alertes sont supprimées.

7.8 Découverte réseau

1 **Collecte de données › Découverte › Créer une règle de découverte**

- **Plage IP** (par exemple `192.168.21.1-254`), **Intervalle**, **Vérifications** (Agent Zabbix avec une clé comme `system.uname`, ou SNMP).

2 **Alertes › Actions › Actions de découverte › Créer une action**

- Condition sur la règle de découverte, opérations « Ajouter un hôte », « Ajouter aux groupes d'hôtes » et « Lier au modèle ». Résultats : Surveillance › Découverte.

7.9 Utilisateurs et rôles

1 **Utilisateurs › Groupes d'utilisateurs, Rôles, Utilisateurs**

- Groupes d'utilisateurs : définir les **droits sur les groupes d'hôtes** (lecture, lecture-écriture, refus).
- Rôles : type **Utilisateur**, **Admin** ou **Super admin** et accès aux modules de l'interface.
- Utilisateurs › Créer un utilisateur : **Nom d'utilisateur**, **Groupes**, mot de passe `<MOT_DE_PASSE>`, **Rôle**. Un compte sans groupe ne voit aucun hôte.

7.10 Un hôte est rouge (ZBX indisponible) : que vérifier ?

Survoler l'icône rouge dans Surveillance › Hôtes : le message d'erreur indique souvent la cause. Puis dérouler :

Contrôle	Commande / action
Agent démarré ?	`systemctl status zabbix-agent2` (Windows : service « Zabbix Agent 2 »)
Port ouvert ?	Depuis le serveur : `nc -zv 192.168.21.1 10050` ; sur l'hôte : `ss -tlnp | grep 10050` ; vérifier le pare-feu
Réponse de l'agent ?	`zabbix_get -s 192.168.21.1 -k agent.ping` doit renvoyer 1
`Server=` correct ?	Doit contenir l'IP du serveur Zabbix (celle vue par l'agent) ; redémarrer l'agent après modification
`Hostname=` correct ?	Identique, à la casse près, au nom d'hôte dans l'interface (indispensable pour les contrôles actifs)
Interface de l'hôte	IP/DNS et port 10050 corrects dans la fiche de l'hôte
Journaux	`/var/log/zabbix/zabbix_agent2.log` sur l'hôte ; `/var/log/zabbix/zabbix_server.log` sur le serveur

> **Astuce**
> Après modification d'un fichier de configuration du serveur, redémarrer le service ; pour recharger le cache de configuration sans coupure : `sudo zabbix_server -R config_cache_reload` .

7.11 Raccourcis et emplacements utiles

Élément	Valeur
Interface web	`http://192.168.21.4/zabbix/`
Config serveur	`/etc/zabbix/zabbix_server.conf`
Config agent 2	`/etc/zabbix/zabbix_agent2.conf` (Windows : `C:\Program Files\Zabbix Agent 2\`)
Config web / PHP	`/etc/zabbix/apache.conf`, `/etc/zabbix/web/zabbix.conf.php`, `/etc/php/8.4/apache2/php.ini`
Logs	`/var/log/zabbix/zabbix_server.log`, `zabbix_agent2.log`, `/var/log/apache2/error.log`
Services	`sudo systemctl restart zabbix-server zabbix-agent2 apache2`
Ports	80 (web), 10051 (serveur), 10050 (agent), 161/UDP (SNMP)
Outils de test	`zabbix_get`, `zabbix_agent2 -t <clé>`, `snmpwalk`
Cache de configuration	`sudo zabbix_server -R config_cache_reload`

Sources : documentation officielle Zabbix 7.0 (zabbix.com/documentation/7.0/en/manual) · cycle de vie des versions (zabbix.com/life_cycle_and_release_policy.html) · dépôt Debian (repo.zabbix.com/zabbix/7.0/debian/) · Procédure rédigée à partir d'un TP réalisé en équipe.