Institution des Chartreux Documentation

Documentation

FAUBLADIER--ANETTE Alexandre, ANTHOARD

Thomas, ROMERA Baptiste

02/04/2025

Table des matières

[Introduction 1](#_Toc194504143)

[Installation de Zabbix 1](#_Toc194504144)

[Fonctionnement et prérequis 1](#_Toc194504145)

[Ajout d’utilisateurs 2](#_Toc194504146)

[Superviser des clients 5](#_Toc194504147)

[Client Agent 5](#_Toc194504148)

[Client SNMP 6](#_Toc194504149)

[Ajout des alertes 9](#_Toc194504150)

[Résultat attendu 10](#_Toc194504151)

# Introduction

Pour notre solution de supervision, nous avons opté pour l’installation de Zabbix. Zabbix est un logiciel de supervision local et open source, ce qui nous offre la possibilité d’ajuster et de personnaliser son serveur de virtualisation selon nos besoins. Nous avons décidé de ne pas l’installer dans un conteneur Docker, préférant suivre les recommandations du site officiel pour une installation optimale.

# Installation de Zabbix

Pour l’installation de la solution, nous avons choisi d’héberger le serveur Zabbix sur un système Ubuntu 24. Pour obtenir le logiciel, nous avons suivi les instructions fournies par le constructeur afin d’installer Zabbix 7.2. Une fois la solution implémentée et opérationnelle, nous avons pu accéder à l’interface via l’adresse : « 172.16.10.13/zabbix ». Afin d’améliorer la navigation, nous avons également configuré un DNS permettant d’accéder à l’interface via : « zabbix.networks.local/zabbix».

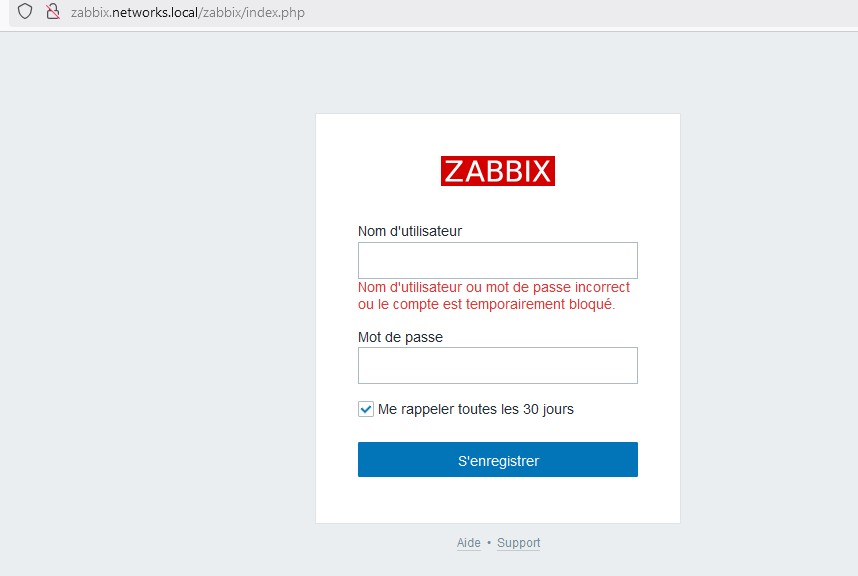


Figure 1 – Interface de connexion de Zabbix

# Fonctionnement et prérequis

Pour utiliser Zabbix et commencer à superviser les postes clients, il est nécessaire d’installer des agents sur ces derniers. L’agent Zabbix a pour rôle d’envoyer des informations concernant les machines au serveur principal, garantissant ainsi une remontée d’informations complète et fiable. Pour l’installation des agents, nous avons suivi les étapes détaillées sur le site officiel. Ces agents sont déployés sur les machines clientes que nous souhaitons superviser, notamment notre machine Vault, notre base de données (BDD), notre Active Directory (AD), et d’autres systèmes essentiels.

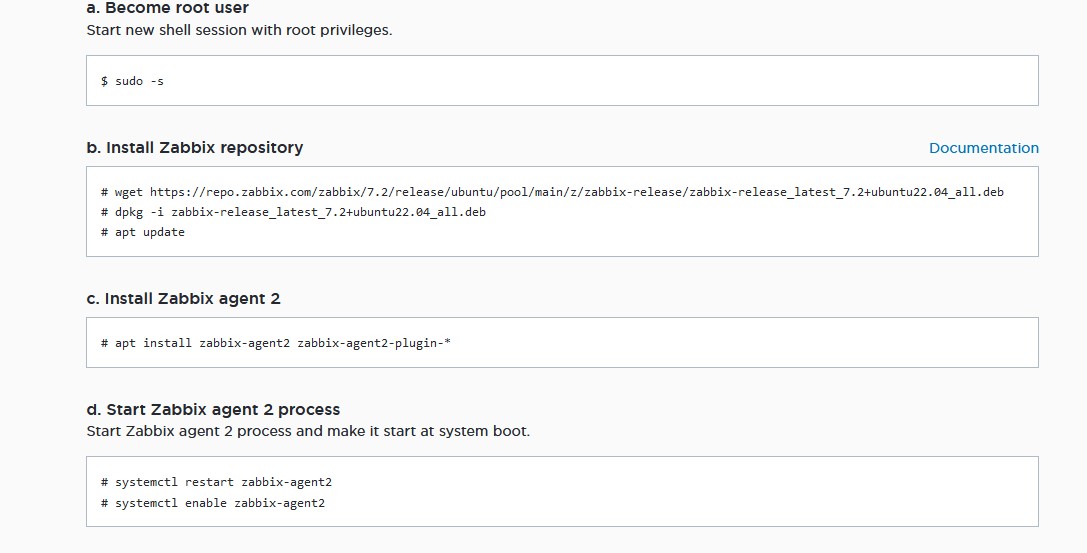


Figure 2 – Procédure d’installation de l’agent Zabbix

Une fois l’agent installé, il est nécessaire de modifier son fichier de configuration pour spécifier l’adresse IP du serveur Zabbix. Une fois cette étape réalisée, nous pouvons créer l’hôte correspondant sur le serveur Zabbix, ce qui permet de recevoir les informations transmises par les agents.



Figure 3 – Réglages du fichier de configuration du client Zabbix.

# Ajout d’utilisateurs

Concernant les utilisateurs, nous allons ajouter un utilisateur pour les alertes et un autre pour Grafana. Ces deux comptes seront utilisables par toute personne disposant du mot de passe associé, mais dans notre cas, ils seront réservés à des services. Dans un premier temps, les deux comptes devront disposer des permissions « Super-admin » sur le serveur Zabbix, leur permettant d’accéder aux services nécessaires, d’envoyer et d’exporter des données par e-mail, ainsi que de permettre la connexion d’un autre utilisateur depuis un logiciel tiers.

Pour créer ces deux comptes, nous devons nous rendre dans « Utilisateurs » → « Utilisateurs » → « Créer un utilisateur ».

Une image contenant texte, capture d’écran, logiciel, Logiciel multimédia

Le contenu généré par l’IA peut être incorrect.

Une image contenant texte, capture d’écran, logiciel, Logiciel multimédia

Le contenu généré par l’IA peut être incorrect.

Une image contenant texte, capture d’écran, logiciel, Logiciel multimédia

Le contenu généré par l’IA peut être incorrect.

Figure X à X – Paramètres et configuration de l’utilisateur « Alertes »

Concernant l’utilisateur « Alertes », il doit impérativement avoir les droits « Super-admin », car c’est la seule façon d’autoriser l’envoi de mails depuis le serveur Zabbix. De plus, il doit obligatoirement disposer d’une adresse e-mail renseignée dans l’onglet Média).

Une image contenant texte, capture d’écran, logiciel, Logiciel multimédia

Le contenu généré par l’IA peut être incorrect.

Figure X – Configuration de l’utilisateur « Grafana »



Figure X – Utilisateur « Grafana » et « Alerte »

# Superviser des clients

## Client Agent

Pour superviser notre infrastructure, il est nécessaire d’installer des agents sur les serveurs clients. Une fois l’agent installé sur la machine, nous redirigeons les informations de cet agent vers le serveur de supervision.

Après avoir modifié le fichier de configuration situé à «

/etc/zabbix/zabbix\_agentd.conf » pour indiquer l’adresse IP du serveur Zabbix,

nous pouvons procéder à l’ajout de l’hôte sur le serveur Zabbix

.



Figure 4 – Ajout d’un nouveau client

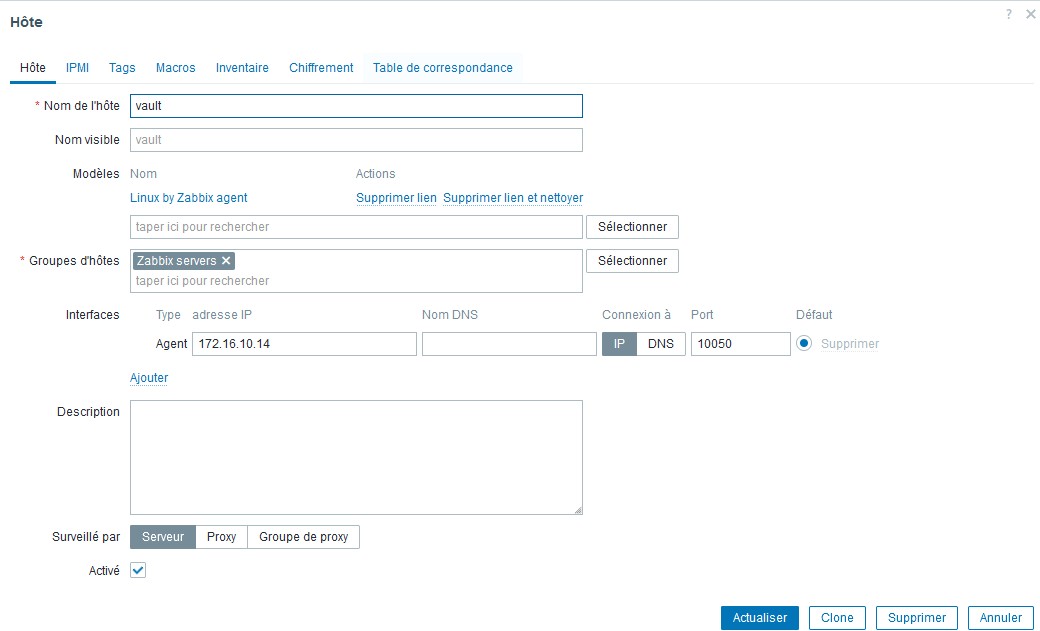


Figure 5 – Complétion des informations dans le serveur Zabbix

## Client SNMP

Pour répondre à notre besoin de supervision, nous avons décidé de connecter nos éléments d’interconnexion, tels que nos switches, à notre logiciel de supervision. Pour ce faire, ces éléments seront intégrés via le protocole SNMP sur Zabbix. Sur l’hôte correspondant, il est nécessaire de configurer l’utilisation du SNMP à la place des agents. Lors de la création d’un nouvel hôte dans l’interface Zabbix, il suffit de sélectionner « SNMP » dans la section dédiée aux interfaces. Ensuite, il faudra renseigner les informations spécifiques à votre switch.

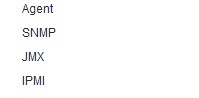


Figure 6 – Choix de l’interface de l’agent

Dans notre cas, nous souhaitons superviser notre switch. Pour cela, une fois l’hôte créé dans Zabbix, nous devons activer le protocole SNMPv2 sur le switch, car il est plus simple à mettre en œuvre. Une fois connectés à l’interface de gestion du switch, nous nous rendons dans la section dédiée au SNMP pour procéder à son activation.

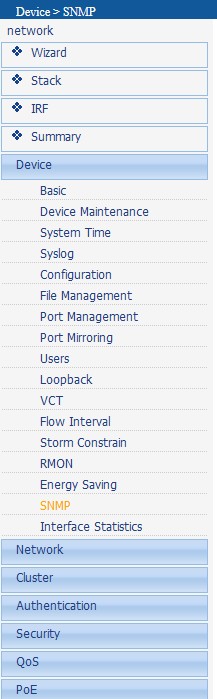


Figure 7 – Interface du switch SNMP

Une fois dans l’interface de gestion SNMP du switch, nous sélectionnons le protocole SNMPv2. Ensuite, nous créons une « communauté », qui sert à définir un groupe d’appareils pouvant échanger des données via SNMP.



Figure 8 – Interface d’activation des différents protocole SNMP

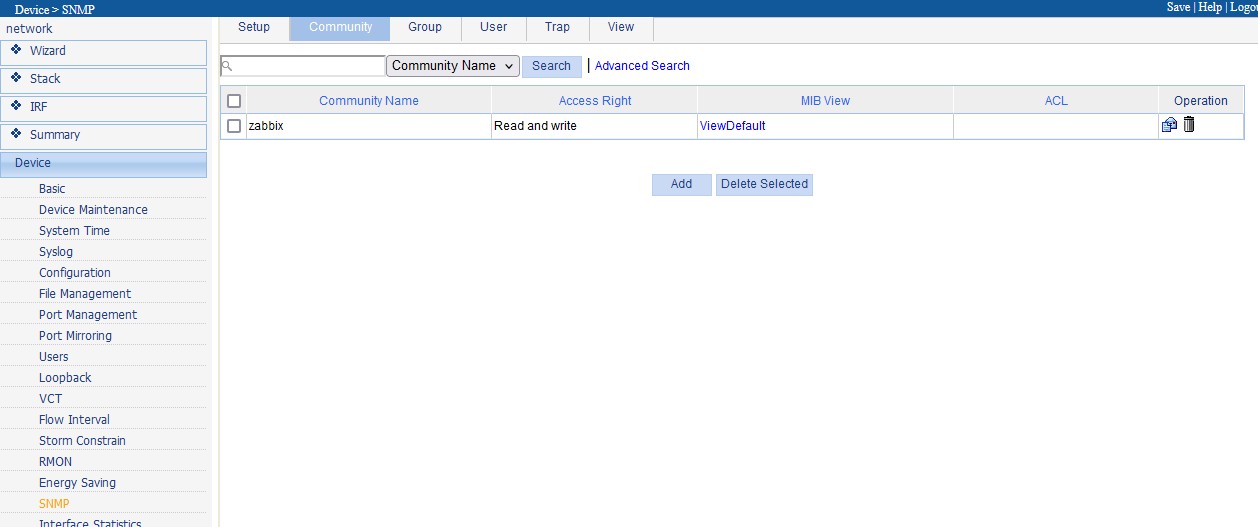


Figure 9 – Interface de configuration de la communauté

Après avoir créé la communauté sur le switch et configuré ses autorisations en « read-write », nous remplissons les informations relatives au protocole SNMP dans Zabbix pour établir la connexion avec l’hôte.

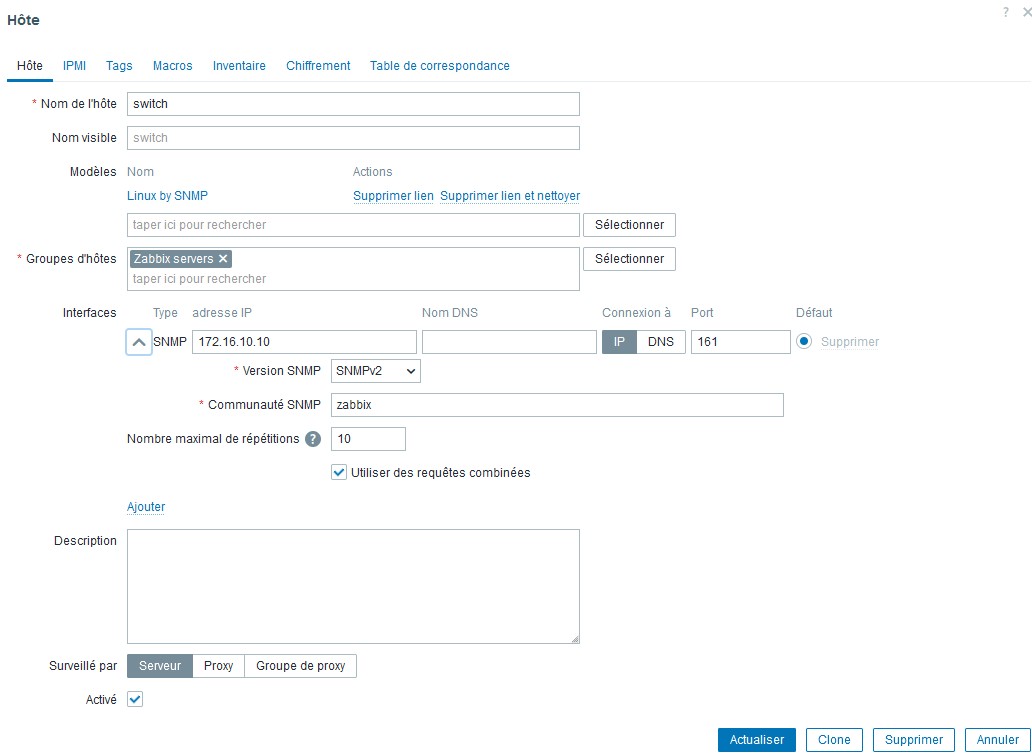


Figure 10 – Complétion des informations dans le logiciel

Une fois les informations renseignées et l’hôte créé, la collecte des données devrait s’effectuer automatiquement. En théorie, nous devrions obtenir le résultat attendu, avec les informations du switch remontant correctement dans l’interface de supervision :

Figure 11 – Résultat de la connexion au logiciel

# Ajout des alertes

Dans Zabbix, il est possible d’ajouter des alertes sur des « Déclencheurs ». Pour ce faire, nous allons nous rendre dans : « Alertes » → « Actions » → « Actions de déclencheur ». C’est ici que nous allons pouvoir configurer nos déclencheurs.

Une image contenant texte, capture d’écran, Police

Le contenu généré par l’IA peut être incorrect.

Figure X – Ajout d’un déclencheur

Une fois sur l’interface, nous allons pouvoir commencer la création d’une action en cliquant sur « Créer une action ». Nous allons ensuite renseigner le nom de l’action ainsi que la condition. Cette condition est très importante, car c’est le déclencheur que nous allons sélectionner à ce moment-là qui sera utilisé comme base pour notre action. Par exemple, si un serveur fonctionne de manière trop intense ou subit une surcharge soudaine, un déclencheur s’active. C’est lors de la création de l’action que nous définissons comment elle doit réagir en cas d’activation de ce déclencheur. Nous allons ensuite paramétrer l’onglet « Opérations » pour indiquer à notre action qui elle doit prévenir. Dans notre cas, nous avons préalablement créé un utilisateur disposant des permissions nécessaires ainsi que d’un média, lui permettant d’envoyer des mails. (Dans notre exemple, si le serveur WDS-MDT ne répond pas via l’agent Zabbix, une alerte sera envoyée à l’utilisateur « Alerte » défini précédemment).

Une image contenant texte, logiciel, Logiciel multimédia, capture d’écran

Le contenu généré par l’IA peut être incorrect.

Une image contenant capture d’écran, texte, logiciel, Logiciel multimédia

Le contenu généré par l’IA peut être incorrect.

Figure X à X – Création d’une alerte

La dernière étape consiste à créer un « Type de média » contenant les informations de connexion de notre serveur mail. Une fois cela fait, chaque fois que le déclencheur s’activera, un courriel sera envoyé à l’utilisateur « Alerte », permettant ainsi la notification par mail.



Figure X – Type de média « Gmail » créer

# Résultat attendu

Les résultats attendus après avoir connecté tous les éléments que Zabbix pouvait prendre en compte, tels que les postes clients et les éléments d’interconnexion (comme le switch), sont maintenant en place. Pour ce faire, nous avons utilisé les agents Zabbix pour superviser les postes clients et le protocole SNMP pour surveiller notre switch.