

Institution des Chartreux

Documentation supervision

Documentation PPE

FAUBLADIER--ANETTE Alexandre, ANTHOARD
Thomas, MONTEIRO Matéo, ROMERA Baptiste
24/05/2025

Table des matières

Introduction.....	1
Installation de Zabbix.....	1
Fonctionnement et prérequis.....	1
Ajout d'utilisateurs.....	2
Superviser des clients.....	5
Client Agent.....	5
Client SNMP.....	6
Ajout des alertes.....	9
Résultat attendu.....	10
Grafana.....	10
Installation de Grafana.....	10
Configuration de Grafana et prérequis.....	11

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 ».

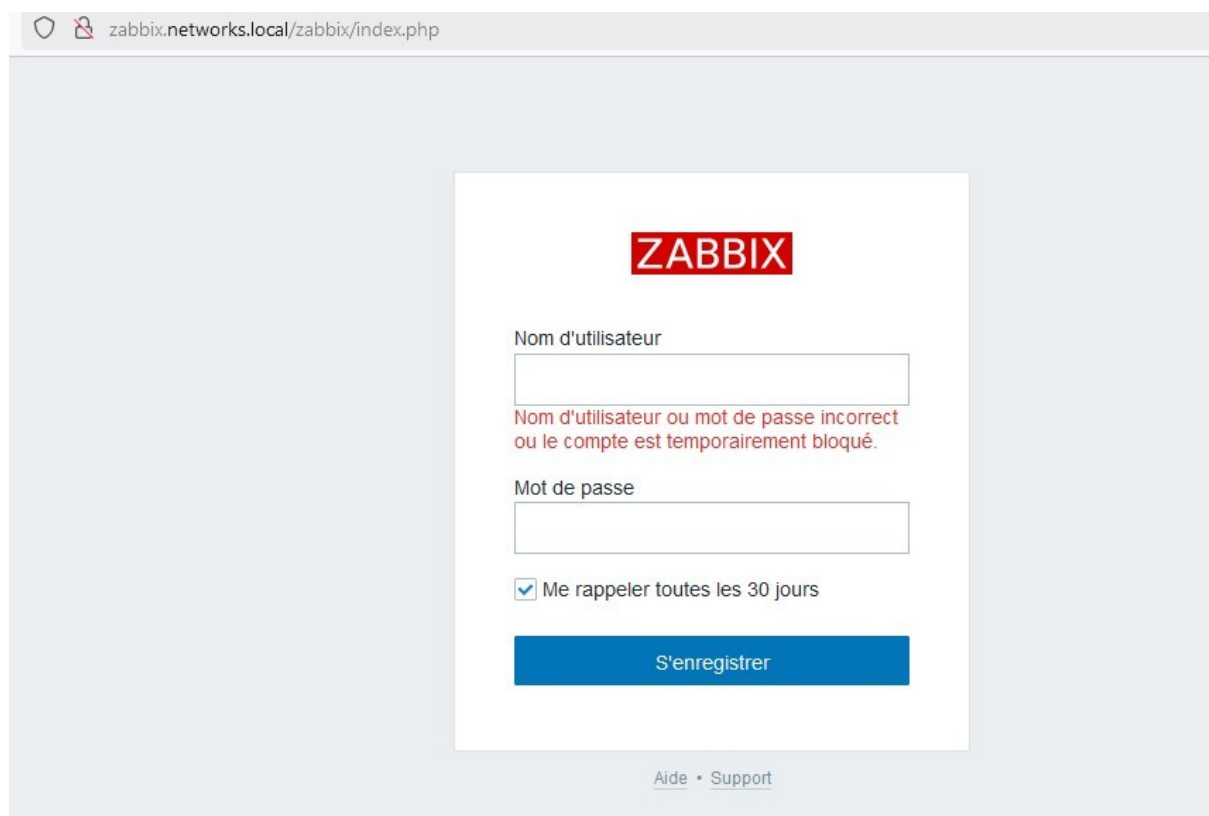
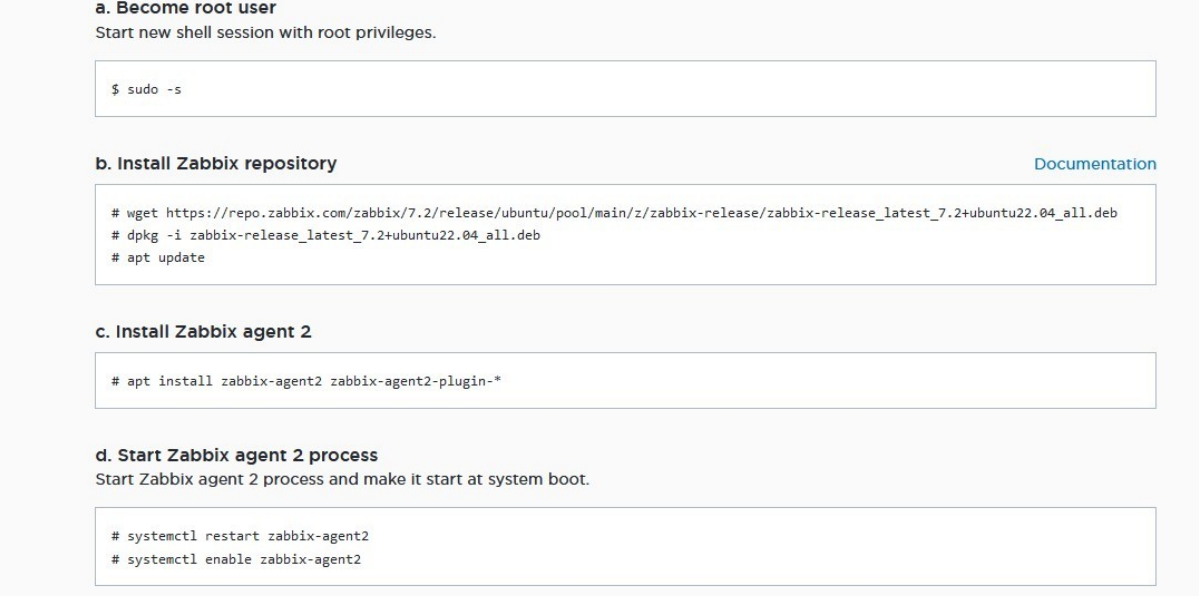


Figure 1 – Interface de connexion de Zabbix

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.



The image shows a terminal window with four sections of commands for installing Zabbix agent 2. Section 'a' shows becoming root with 'sudo -s'. Section 'b' shows installing the Zabbix repository with 'wget', 'dpkg', and 'apt update'. Section 'c' shows installing 'zabbix-agent2' and its plugins. Section 'd' shows restarting and enabling the 'zabbix-agent2' service with 'systemctl'.

```
a. Become root user
Start new shell session with root privileges.

$ sudo -s

b. Install Zabbix repository
Documentation

# wget https://repo.zabbix.com/zabbix/7.2/release/ubuntu/pool/main/z/zabbix-release/zabbix-release_latest_7.2+ubuntu22.04_all.deb
# dpkg -i zabbix-release_latest_7.2+ubuntu22.04_all.deb
# apt update

c. Install Zabbix agent 2

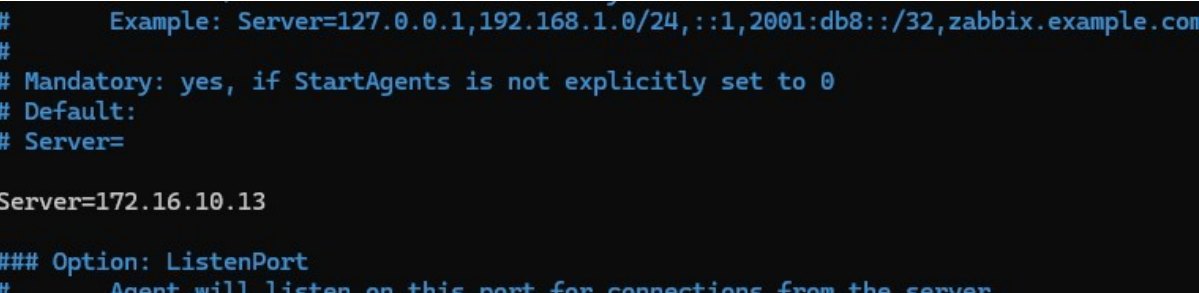
# apt install zabbix-agent2 zabbix-agent2-plugin-*

d. Start Zabbix agent 2 process
Start Zabbix agent 2 process and make it start at system boot.

# systemctl restart zabbix-agent2
# systemctl enable zabbix-agent2
```

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.



The image shows a snippet of the Zabbix client configuration file. It includes a comment with an example server address, a mandatory setting for 'StartAgents', and a configuration for 'Server=172.16.10.13'. It also shows the 'ListenPort' option with a comment explaining its function.

```
# 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=172.16.10.13
### Option: ListenPort
# Agent will listen on this port for connections from the server.
```

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 ».

Utilisateurs

Utilisateur
Média 1
Permissions

* Nom d'utilisateur
Alertes

Prénom

Nom de famille

Groupes
Zabbix administrators X
Sélectionner

Mot de passe
Changer le mot de passe

Langue
Valeur système par défaut

Fuseau horaire
Valeur système par défaut: (UTC+02:00) Europe/Paris

Thème
Valeur système par défaut

Connexion automatique
☐

Auto-déconnexion
☐ 15m

* Rafraîchir
30s

* Lignes par page
50

URL (après connexion)

Actualiser
Supprimer
Annuler

Type	Envoyer à	Lorsque actif	Utiliser si sévérité	État	Actions
Gmail	a.faubladier@eleve.leschartreux.net	1-7,00:00-24:00	N I A M H D	Activé	Édition Supprimer
Ajouter					
Actualiser Supprimer Annuler					

Utilisateurs

Utilisateur
Média 1
Permissions

Rôle
Super admin role X
Sélectionner

Type d'utilisateur
Super administrateur

Permissions

Groupe	Type	Permissions
Tous les groupes	Hôtes	Lecture-écriture
Tous les groupes	Modèles	Lecture-écriture

Les permissions ne peuvent être assignées qu'aux groupes d'utilisateurs.

Accès aux éléments de l'interface utilisateur

Tableaux de bord

Dashboards

Surveillance

Problèmes
Hôtes
Dernières données
Cartes
Découverte

Services

Services
SLA
Rapport SLA

Inventaire

Aperçu
Hôtes

Rapports

Information système
Rapports planifiés
Rapport de disponibilité
Top 100 des déclencheurs
Journal d'audit
Journal des actions
Notifications

Collecte de données

Groupes de modèles
Groupes d'hôtes
Modèles
Hôtes
Maintenance
Corrélation d'événement
Découverte

Alertes

Actions de déclencheur
Actions des services
Actions de découverte
Actions d'enregistrement automatique
Actions internes
Types de média
Scripts

Utilisateurs

Groupes d'utilisateurs
Rôles utilisateur
Utilisateurs
Tokens API
Authentification

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).

Utilisateurs

Utilisateur

Média

Permissions

* Nom d'utilisateur

Grafana

Prénom

Grafana User

Nom de famille

Groupe

Zabbix administrators X

taper ici pour rechercher

Sélectionner

Mot de passe

Changer le mot de passe

Langue

Valeur système par défaut

Fuseau horaire

Valeur système par défaut: (UTC+02:00) Europe/Paris

Thème

Valeur système par défaut

Connexion automatique

Auto-déconnexion

15m

* Rafraîchir

30s

* Lignes par page

50

URL (après connexion)

Actualiser

Supprimer

Annuler

Figure X – Configuration de l'utilisateur « Grafana »

<input type="checkbox"/>	Alertes	Super admin	role	Non	Ok	Valeur système par défaut	Activé	Désactivé	Activé
<input type="checkbox"/>	Grafana	Grafana User	Super admin	Oui (02/04/2025 16:12:15)	Ok	Valeur système par défaut	Activé	Désactivé	Activé

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

Hôtes Créer un hôte

Nom

État

Groupes d'hôtes

Tags

IP

DNS

Port

Ajouter

Afficher les hôtes en maintenance ☒ Afficher les problèmes supprimés ☐

Sévérité ☐ Non classé ☐ Avertissement ☐ Haut ☐ Information ☐ Moyen ☐ Désastre

Figure 4 – Ajout d'un nouveau client

Hôte ? ×

Hôte IPMI Tags Macros Inventaire Chiffrement Table de correspondance

* Nom de l'hôte

Nom visible

Modèles Nom Actions

[Linux by Zabbix agent](#) [Supprimer lien](#) [Supprimer lien et nettoyer](#)

* Groupes d'hôtes

Interfaces	Type	adresse IP	Nom DNS	Connexion à	Port	Défaut
Agent		<input type="text" value="172.16.10.14"/>	<input type="text"/>	<input checked="" type="radio"/> IP <input type="radio"/> DNS	<input type="text" value="10050"/>	<input checked="" type="radio"/> Supprimer

[Ajouter](#)

Description

Surveillé par

Activé ☒

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.

Agent
SNMP
JMX
IPMI

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.

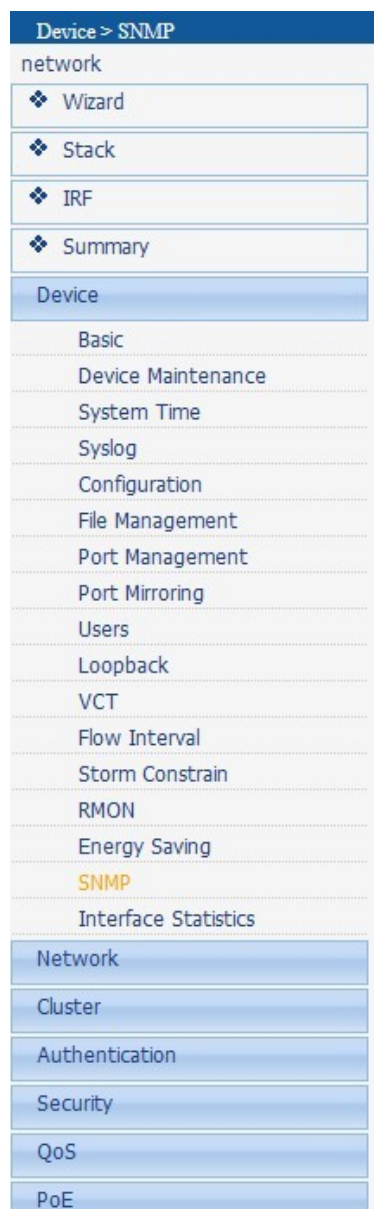


Figure 7 – Interface du switch SNMP

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.

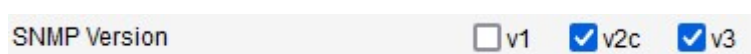


Figure 8 – Interface d'activation des différents protocole SNMP

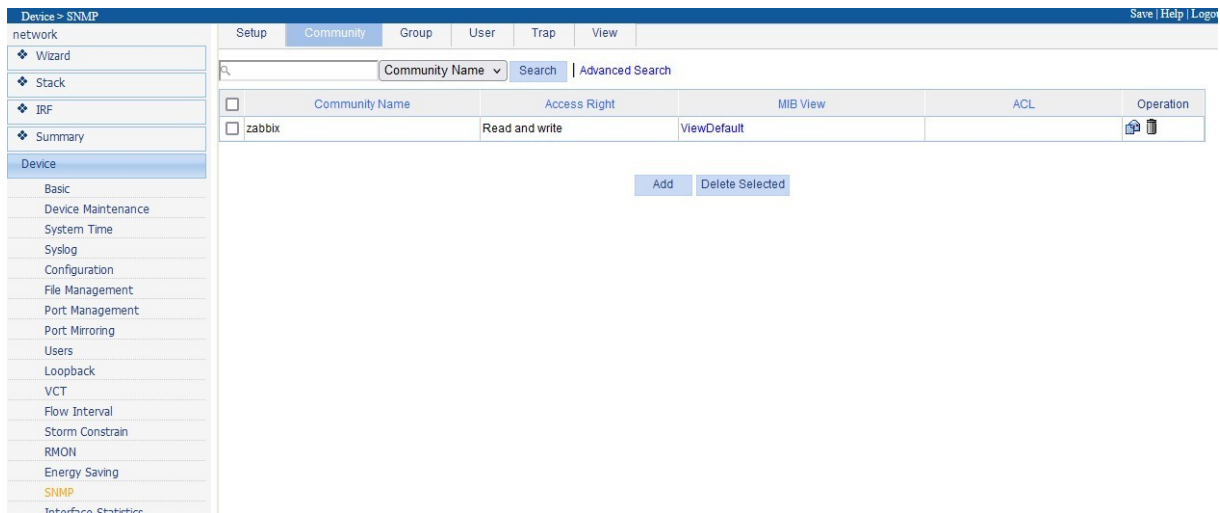


Figure 9 – Interface de configuration de la communauté

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.

Hôte

Nom de l'hôte: switch

Nom visible: switch

Modèles: Linux by SNMP

Groupes d'hôtes: Zabbix servers

Interfaces:

Type	adresse IP	Nom DNS	Connexion à	Port	Défaut
SNMP	172.16.10.10		IP	DNS	161

* Version SNMP: SNMPv2

* Communauté SNMP: zabbix

Nombre maximal de répétitions: 10

☒ Utiliser des requêtes combinées

Description:

Surveillé par: ☒ Actif

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.

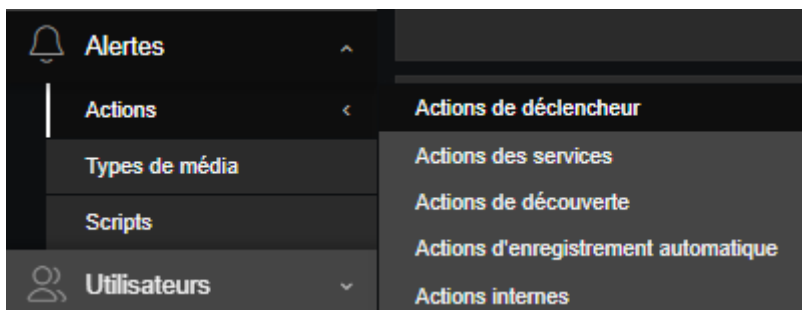


Figure X – Ajout d'un déclencheur

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).

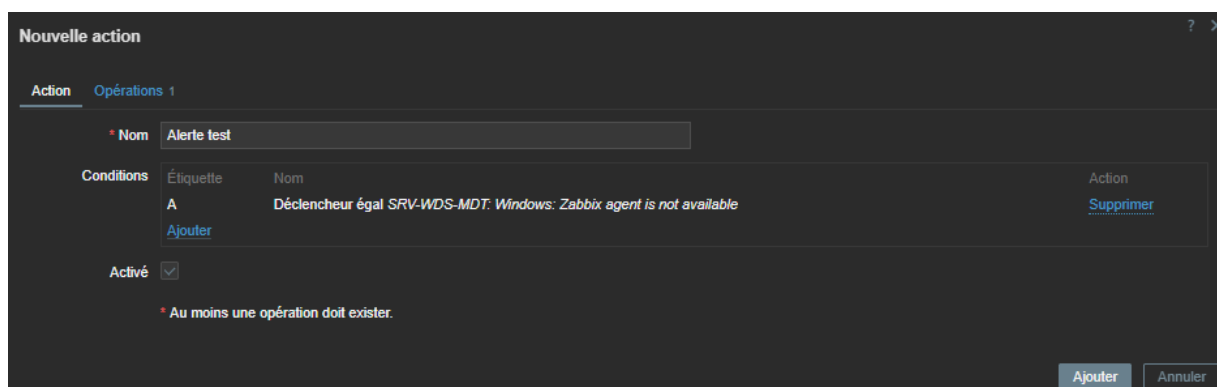


Figure X à X – Création d’une alerte

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.

Grafana

Installation de Grafana

Pour faciliter la lecture des données reçues de Zabbix, nous avons mis en place un second outil sur la même machine. Grafana permet de simplifier l’affichage et le traitement des données, facilitant ainsi l’analyse de l’état de santé des serveurs.

Nous avons choisi ce logiciel pour sa simplicité d’installation, son confort visuel pour la lecture des données, mais aussi pour sa compatibilité avec notre outil de supervision Zabbix. Grafana joue ici uniquement le rôle de surcouche, affichant les données remontées par les agents Zabbix préalablement installés sur les machines cibles ou via des remontées SNMP.

Configuration de Grafana et prérequis

Dans un premier temps, nous allons pouvoir créer un utilisateur sur l'outil de supervision, dédié uniquement aux connexions de Grafana. Ce compte permettra à Grafana de récupérer les données de Zabbix en s'y connectant. Il est impératif que ce compte dispose des permissions de type superadministrateur:

The screenshot shows the 'User' tab in the Grafana administration interface. The form contains the following fields and values:

- * Alias:** grafana
- Name:** (empty)
- Last Name:** (empty)
- * Groups:** Zabbix administrators (selected from a dropdown menu with a search bar 'type here to search' and a 'Select' button)
- * Password:** (masked with dots)
- * Password (once again):** (masked with dots)
- Language:** English (en_GB) (dropdown menu)
- Theme:** System default (dropdown menu)
- Auto-login:** ☐
- Auto-logout:** ☐ 15m
- * Refresh:** 30s
- * Rows per page:** 50
- URL (after login):** (empty)

Figure X – Création du user Grafana

Ensuite, sur Grafana, nous allons installer le plugin « Zabbix », qui permettra à ce dernier d'accéder aux données récupérées et stockées par Zabbix.



Figure X – Installation du plugin Zabbix sur Grafana

Une fois les informations de connexion renseignées, Grafana nous permet d'accéder aux données de Zabbix. Cela nous donne la possibilité d'afficher ces informations dans un tableau de bord Grafana, plus lisible et moderne que l'interface native de l'outil de supervision.

Une fois la connexion établie, nous pouvons commencer la création du tableau de bord. Celui-ci nous permettra d'afficher les éléments suivants :

- Disponibilité des agents
- Utilisation du CPU
- Mémoire RAM disponible
- Espace disque disponible
- Variation de l'utilisation des CPU des machines

Après avoir configuré et implémenté les graphiques ainsi que les données que nous souhaitons visualiser, nous obtenons le résultat suivant :



Figure X – Intégration et création du Dashboard Grafana