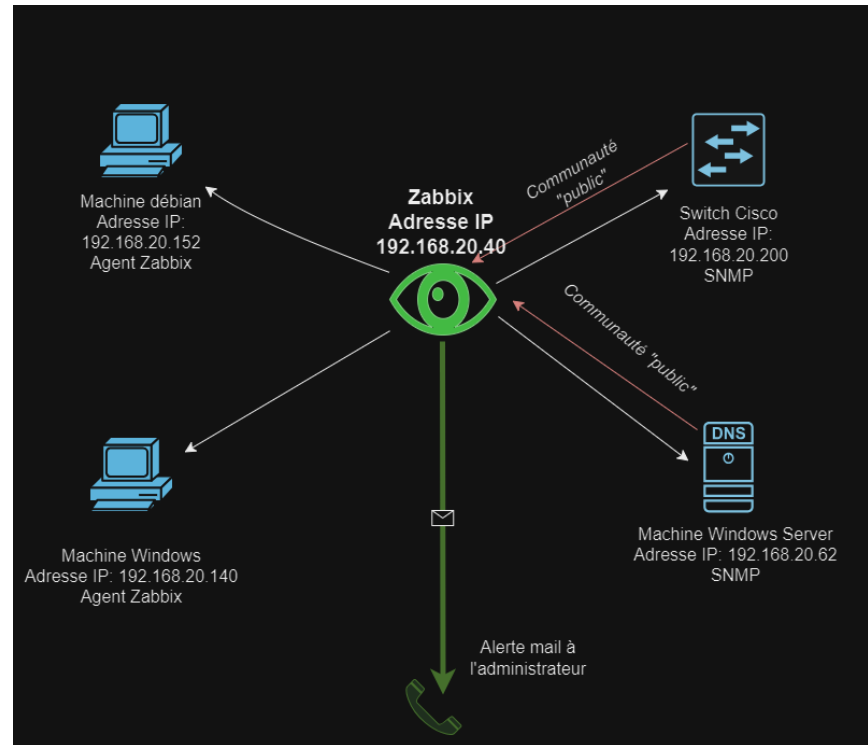




TP-Supervision

THOMAS GRZESINSKI

Schéma du contexte



ZABBIX

Zabbix est un logiciel libre permettant de surveiller l'état de divers réseau, serveurs et autres matériels réseau et produisant des graphiques dynamiques de consommation des ressources.

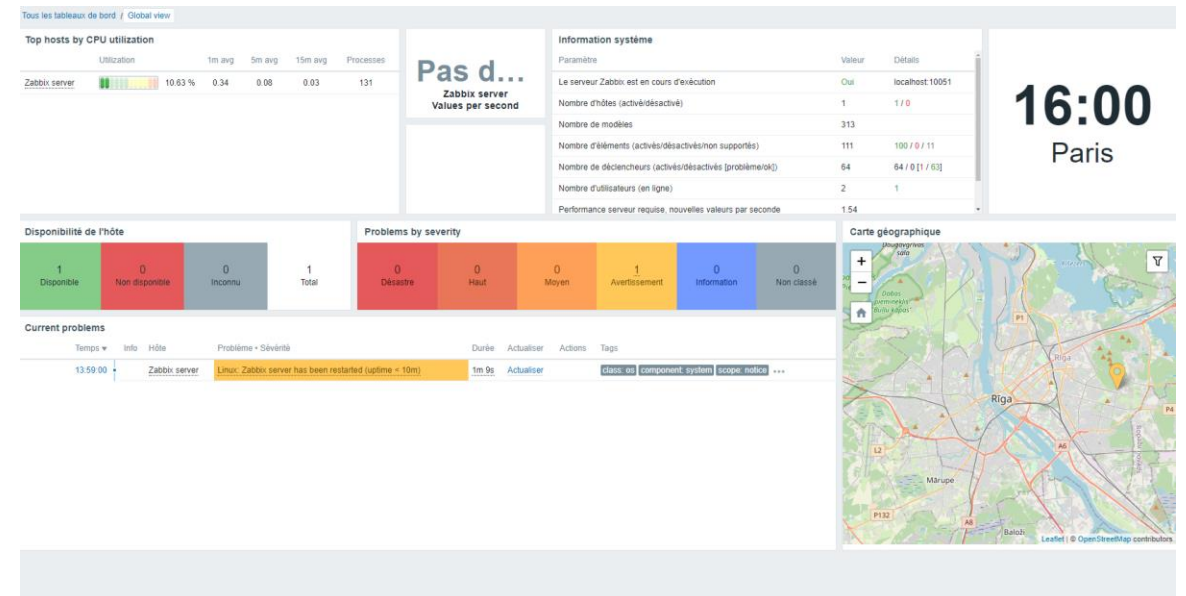
Pour installer Zabbix il est préférable de suivre ce tuto [TUTO-ZABBIX](#)

L'identifiant et le mot de passe par défaut de Zabbix est : Admin et zabbix

Interface Zabbix

Au démarrage l'interface de Zabbix ressemble a ceci:

Sur cette interface nous pouvons y configurer des hôtes à monitorer, voir les problèmes liés aux machines sur le réseau via le tableau de disponibilité de l'hôte.



Configuration d'un agent Zabbix sur un débian

Nous allons maintenant configurer un agent Zabbix sur notre machine débian.

L'agent Zabbix est déployé sur une cible de surveillance pour surveiller activement les ressources et applications locales(disques durs, mémoire, statistiques du processeur...)

Sur la machine débian a monitorer il faut donc:

- Installer l'agent *apt install zabbix-agent*
- Aller dans le fichier conf *nano /etc/zabbix/zabbix_agentd.conf*
- Mettre l'adresse IP du Zabbix pour que notre machine zabbix puisse récupérer les paquets de notre hôte `Server=192.168.20.40_`

Configuration d'un agent Zabbix sur un débian

- Ensuite redémarrer l'agent avec la commande `systemctl zabbix-agent restart`

Retourner sur l'interface Zabbix

Dessus vous devez:

- Aller dans collecte des données -> hôtes

- Créer un hôte

- Dessus il faudra la nommer , mettre son adresse IP et comme modèles le Zabbix agent

- Si tout est configuré correctement la disponibilité de votre agent devrait être verte et il remontera des données

Pour voir les données remontées aller dans « Surveillance » -> dernières données

The screenshot shows the 'Hôte' (Host) configuration page in Zabbix. The 'Nom de l'hôte' (Host name) is 'DEBthomasg'. The 'Nom visible' (Visible name) is also 'DEBthomasg'. The 'Modèles' (Templates) field is set to 'Zabbix agent'. The 'Groupes d'hôtes' (Host groups) field is set to 'Virtual machines'. The 'Interfaces' table has one entry: 'Agent' with IP '192.168.20.152', connection type 'IP', and port '10050'. The 'Description' field is empty. The 'Surveillance via le proxy' (Monitor via proxy) dropdown is set to '(pas de proxy)'. The 'Activé' (Enabled) checkbox is checked. At the bottom, there are buttons for 'Actualiser', 'Clone', 'Clone complet', 'Supprimer', and 'Annuler'.

The screenshot shows the 'Surveillance' (Monitoring) page in Zabbix. The breadcrumb trail is 'Éléments 4 > Déclencheurs 2 > Graphiques 1 > Découverte > Web > 192.168.20.152:10050 > Zabbix agent'. The host 'DEBthomasg' is shown with a green status indicator and the label 'Actif'. The 'ZBX' and 'Aucun' labels are visible. Below, there is a table with columns for 'Nom', 'Statut', 'Dernière mise à jour', 'Prochain', and 'Type'. The table contains two rows of data for the host 'DEBthomasg'.

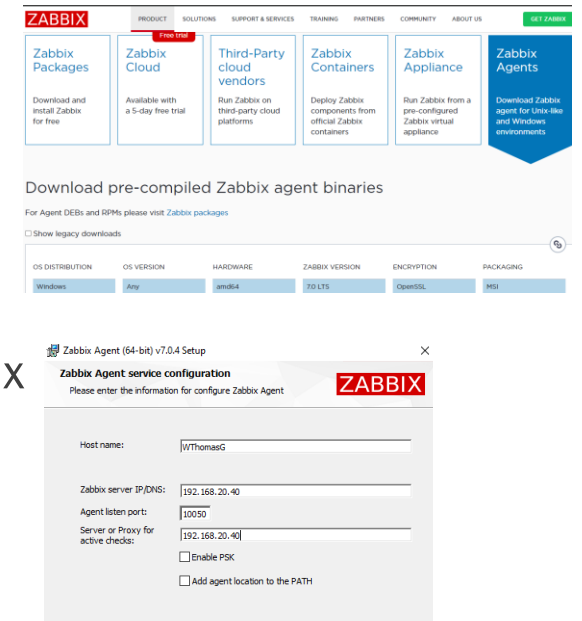
Configuration d'un agent Zabbix sur Windows

Sur Windows, la mise en place d'un agent est un peu plus simple.

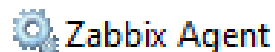
En effet aller sur le site internet de Zabbix et installer l'agent pour un Windows

URL: [Zabbix agents](https://zabbix.com/agents)

Une fois l'agent installer, lancer l'agent et configuré l'adresse IP de votre Zabbix



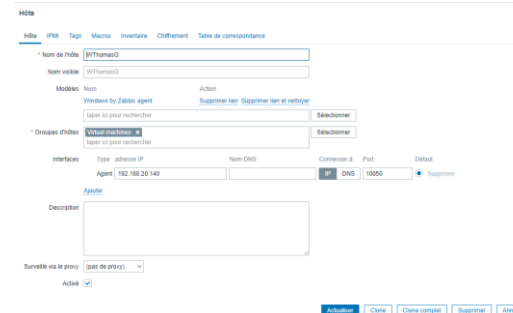
Vérifier l'installation de l'agent en allant dans la console Windows (W+R) et regarder si l'agent est bien installé



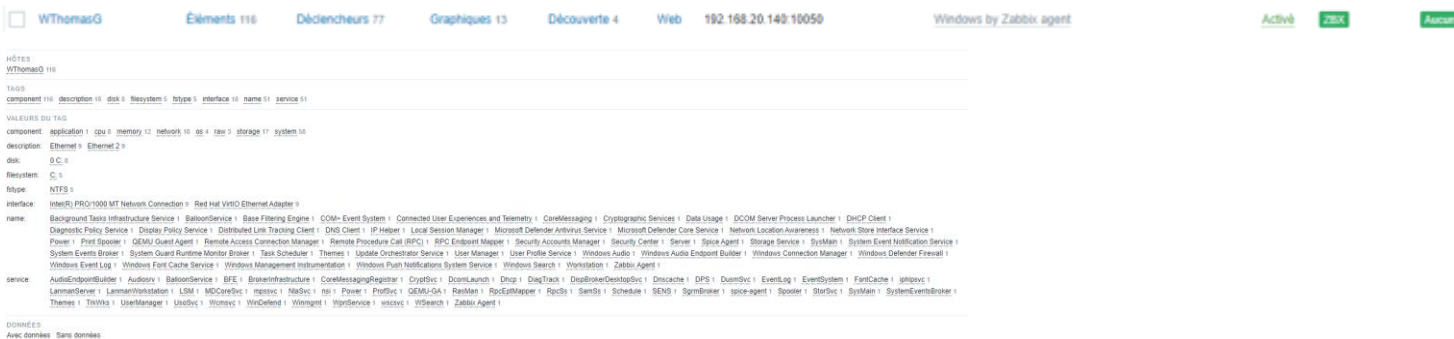
Provides sys... En co... Automatique (débu... Système local

Configuration d'un agent Zabbix sur Windows

Retourner sur votre interface Zabbix configurer votre hôte Windows, en y mettant son adresse IP et comme modèles « Windows by Zabbix agent »



De la même manière que Debian si l'agent est bien configuré sa disponibilité devrait être verte et il devrait remonter des données dans la surveillance de Zabbix



Configuration d'un SNMP sur un Windows Server

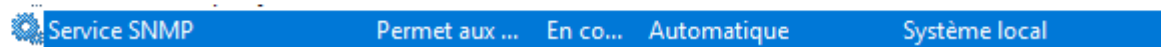
On voudrait cette fois ci, configurer un SNMP sur un Windows server pour pouvoir le monitorer a distance

SNMP: Simple Network Management Protocol, en français « protocole simple de gestion de réseau », est un protocole de communication qui permet aux administrateurs réseau de gérer les équipements du réseau, de superviser et de diagnostiquer des problèmes réseaux et matériels à distance.

Pour faire ceci on doit donc aller dans le gestionnaire du serveur Windows et ajouter le service SNMP

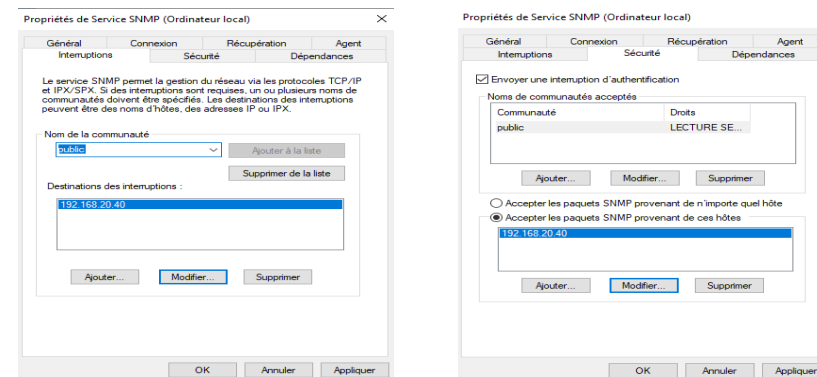
▸ Service SNMP (Installé)

Une fois ceci fait aller dans la console du serveur (W+R) et entrer services, rechercher « Services SNMP »



Configuration d'un SNMP sur un Windows Server

Double cliquer dessus et dans interruption et sécurité ajouté comme nom de communauté « public » et la destination l'adresse IP du Zabbix



Une communauté SNMP regroupe des périphériques et des systèmes de gestion. Seuls les membres de la même communauté peuvent échanger des messages SNMP, et un périphérique ou un système peut appartenir à plusieurs communautés.

La communauté par défaut est donc « public »

Redémarrer le service une fois que tout est configuré

Supervision d'un switch cisco

Configuration:

- Tout d'abord il vous faudra connecter votre switch a votre pc en mode console pour pouvoir le configurer
- On va configurer une interface réseau sur un VLAN pour qu'il puisse être lisible sur le réseau

```
Switch(config-if)#interface vlan 1
Switch(config-if)#ip address 192.168.20.220 255.255.255.0
Switch(config-if)#no sh
```

- On active les traps SNMP avec la commande snmp-server enable traps
- On choisit la destination de notre serveur et la communauté
- On sauvegarde avec un write memory

```
Switch(config)#snmp-server host 192.168.20.90 public
```

Supervision d'un switch Cisco

Sur l'interface Zabbix nous allons configurer un hôte pour le switch Cisco. Il faut donc attribuer son adresse IP, on choisira comme modèle le Cisco IO by SNMP. Ceci dépendra de votre switch Cisco.

The screenshot shows the Zabbix 'Hôte' configuration page. The 'Nom de l'hôte' field is set to 'Cisco'. The 'Modèles' section has 'Cisco IOS by SNMP' selected. The 'Groupes d'hôtes' section has 'Hyperviseurs' selected. In the 'Interfaces' section, an interface is configured with 'Type' set to 'SNMP', 'adresse IP' set to '192.168.20.220', 'Connexion à' set to 'IP', and 'Port' set to '161'. The 'Version SNMP' is set to 'SNMPv2' and the 'Communauté SNMP' is set to '{SNMP_COMMUNITY}'. The 'Nombre maximal de répétitions' is set to '10' and the checkbox 'Utiliser des requêtes combinées' is checked.

On rajoutera en plus une « Macros », les macros sont des variables, identifiées par une syntaxe spécifique. Les macros se résolvent en une valeur spécifique en fonction du contexte.

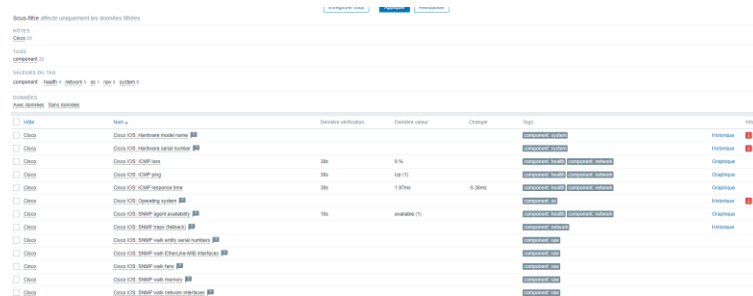
On ajoutera donc la macro `{$COMMUNITY}` et en valeur public, vu qu'on a attribué celle-ci sur le switch

The screenshot shows the Zabbix 'Macros d'hôte' configuration page. A macro is being added with the name '{\$COMMUNITY}', the value 'public', and the description 'description'. The 'Ajouter' button is visible. Below the macro configuration, a table shows the host configuration: 'Cisco' with IP '192.168.20.220:161', model 'SNMP', and target 'class: network target: cisco target: cisco-ios'. The status is 'Activé' and the last data received is 'Dernières données 23'. The page also includes navigation links for 'Problems', 'Graphiques', 'Tableaux de bord 1', and 'Web'.

Supervision d'un switch Cisco

La même chose, pour voir si votre supervision est opérationnelle. Aller dans Surveillance -> dernières données.

Et si tout est correctement configuré alors votre serveur devrait remonter des données



The screenshot shows a monitoring interface with a table of data points. The table has columns for 'Nom', 'Dernière valeur', 'Dernière unité', 'Change', and 'Type'. The data points are listed as follows:

Nom	Dernière valeur	Dernière unité	Change	Type
Check IOS Hardware modules				Intégrité
Check IOS Hardware boot counter				Intégrité
Check IOS CPU use	3%	%		Graphique
Check IOS CPU avg	14 (1)			Graphique
Check IOS CPU response time	3%	1.87ms	-0.3ms	Graphique
Check IOS Operating system				Intégrité
Check IOS SNMP agent availability	OK	available (1)		Graphique
Check IOS SNMP trap delivery				Intégrité
Check IOS SNMP walk with valid community				Intégrité
Check IOS SNMP walk Ethernet MIB statistics				Intégrité
Check IOS SNMP walk tcp				Intégrité
Check IOS SNMP walk memory				Intégrité
Check IOS SNMP walk network interfaces				Intégrité

Supervision

Voici le résumer des trois hôtes que l'on a supervise.

Le serveur Zabbix se supervise automatiquement

Nom ▲	Interface	Disponibilité	Tags	État	Dernières données	Problèmes	Graphiques	Tableaux de bord	Web
Cisco	192.168.20.220:161	SNMP	class: network target: cisco target: cisco-ios	Activé	Dernières données 23	Problèmes	Graphiques	Tableaux de bord 1	Web
DEBthomasg	192.168.20.152:10050	ZBX	class: software target: zabbix-agent	Activé	Dernières données 4	Problèmes	Graphiques 1	Tableaux de bord 1	Web
WServerThomasG	192.168.20.62:161	SNMP	class: os target: windows	Activé	Dernières données 77	1	Graphiques 10	Tableaux de bord 3	Web
WThomasG	192.168.20.140:10050	ZBX	class: os target: windows	Activé	Dernières données 116	2 1	Graphiques 13	Tableaux de bord 3	Web
Zabbix server	127.0.0.1:10050	ZBX	class: os class: software target: linux ...	Activé	Dernières données 129	Problèmes	Graphiques 25	Tableaux de bord 5	Web

Affichage de 5 sur 5 trouvés

Automatisation détection d'anomalie

Zabbix propose plusieurs possibilités et différentes fonctions lorsque nous supervisons les machines.

Mais on a aussi la possibilité de créer des alertes automatiques pour nous prévenir en cas de problèmes sur l'une de nos machines

Configuration:

- Aller dans vos hôtes , sur l'une des machines cliquer sur déclencheurs
- Créer un déclencheur

The screenshot shows the Zabbix trigger configuration page. The 'Déclencheur' tab is active. The configuration includes:

- Nom:** Agent hors ligne
- Nom de l'événement:** Agent hors ligne
- Données opérationnelles:** (empty)
- Sévérité:** Non classé, Information, Avertissement, Moyen, Haut (selected), Désastre
- * Expression:** last(/DEShomng/agent.hostname)=0
- Génération d'événement OK:** Expression, Expression de récupération, Aucun
- Mode de génération des événements PROBLÈME:** Seul, Multiple
- Un événement OK ferme:** Tous les problèmes, Tous les problèmes si les valeurs de tag correspondent
- Autoriser la fermeture manuelle:**
- Nom de l'entrée de menu:** URL du déclencheur
- URL de l'entrée de menu:** (empty)
- Description:** Prévenir quand l'agent est hors ligne
- Activé:**

Buttons at the bottom: Acheter, Clone, Supprimer, Annuler.

Automatisation détection d'anomalie

- Donner un nom a ce déclencheur
- Son niveau de sévérité si l'évènement est grave ou non
- Ecrivez un script (expression) qui permet de définir la cause de l'évènement. Nous ici on a décidé de recevoir un mail quand la machine sera éteinte ou hors ligne
- Aller ensuite dans « Alertes -> Actions -> Actions de déclencheurs
- Créer une action ou vous lui donnerez un nom
- Ajouter lui une condition (ajout de notre déclencheur)

Déclencheur Tags Dépendances

* Nom Agent hors ligne

Nom de l'évènement Agent hors ligne

Données opérationnelles

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

* Expression last (/DEBthomaag/agent.hostname)=0 [Ajouter](#)

[Constructeur d'expression](#)

Génération d'évènement OK Expression Expression de récupération Aucun

Mode de génération des événements PROBLÈME Seul Multiple

Un évènement OK ferme Tous les problèmes Tous les problèmes si les valeurs de tag correspondent

Autoriser la fermeture manuelle

Nom de l'entrée de menu URL du déclencheur

URL de l'entrée de menu

Description Prévenir quand l'agent est hors ligne

Activé

[Actualiser](#) [Clone](#) [Supprimer](#) [Annuler](#)

Action

Opérations :

* Durée de l'escale d'opération par défaut 1h

Opérations

Étapes	Détails	Déterminer dans	Durée	Action
1	Envoyer le message aux utilisateurs: Admin (Zabbix-Administrateur) via Email	Immédiatement	Début	Éditer Supprimer

Opérations de récupération

Étapes	Détails	Action
	Envoyer le message aux utilisateurs: Admin (Zabbix-Administrateur) via Email	Éditer Supprimer

Opérations de mise à jour

Étapes	Détails	Action

Interrompre les opérations en cas de problèmes simplifiés

Suspendre les opérations des problèmes supprimés

Notifier les escalades annulées

* Au moins une opération doit exister

[Actualiser](#) [Clone](#) [Supprimer](#) [Annuler](#)

Automatisation détection d'anomalie

- Avant d'actualiser aller dans opérations
- Faites en sorte que votre Admin reçoit un message lorsque la machine est hors connexion
- Pour configurer le mail de votre Admin aller dans utilisateurs et ajouter lui son adresse mail ou son numéro de téléphone :

Média	Type	Envoyer à	Lorsque actif	Utiliser si sévérité	État	Action
	Email	thomas.grzesinski2@gmail.com	1-7,00:00-24:00	N I A M H D	Activé	Édition Supprimer
	SMS	06 52 53 67 12	1-7,00:00-24:00	N I A M H D	Désactivé	Édition Supprimer
	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: taper ici pour rechercher

Envoyer aux utilisateurs: Admin (Zabbix Administrator) taper ici pour rechercher

Envoyer uniquement à: Email

Message personnalisé:

Sujet: ATTENTION !!!!

Message: La machine débian ne répond plus

Étiquette	Norm	Action
Ajouter		

Automatisation détection d'anomalie Notification mail

Mais pour recevoir cette anomalie vous devez donc configurer un serveur SSMTP sur votre Zabbix.

Configuration:

- Avant vous devez sur votre adresse mail activer la vérification en deux étapes
- Une fois ceci fait vous devez configurer un mot de passe d'application nommer le donc smtp

- Un mot de passe sera d'application sera donc généré

Nom de l'appli
smtp

ahmb zeoi yxmf wqbb

Automatisation détection d'anomalie Notification mail

- Maintenant sur votre machine Zabbix vous allez installer un serveur smtp avec la commande `apt install smtp`
- Ouvrir le fichier de configuration du serveur `nano /etc/ssmtp/ssmtp.conf`
- Configurer votre adresse mail dans le root
- Le mailhub sera donc le smtp sur port 465
- Activer l'authentification du User qui est votre adresse mail et son password qui est le password d'applications que l'on a généré précédemment

```
GNU nano 7.2 /etc/ssmtp/ssmtp.conf
#
# Config file for sSMTP sendmail.
#
# The person who gets all mail for userids < 1000
# Make this empty to disable rewriting.
root=thomas.grzesinski@gmail.com

# The place where the mail goes. The actual machine name is required no
# MX records are consulted. Commonly mailhosts are named mail.domain.com
mailhub=smtp.gmail.com:465

# Where will the mail seem to come from?
#rewriteDomain=

# The full hostname
#hostname=debian12

# Are users allowed to set their own From: address?
# YES - Allow the user to specify their own From: address
# NO - Use the system generated From: address
FromLineOverride=YES
AuthUser=thomas.grzesinski@gmail.com
AuthPass=ahmbzeoiyxmfuqbb
useTLS=YES
```

Automatisation détection d'anomalie Notification mail

- Sauvegarder et ensuite lancer un message test sur votre mail

```
root@debian12:~# echo "Test de la messagerie du serveur Zabbix" | ssmtp thomas.grzesinski2@gmail.com
```

Si tout fonctionne correctement alors vous devrez recevoir votre message dans votre boîte mail



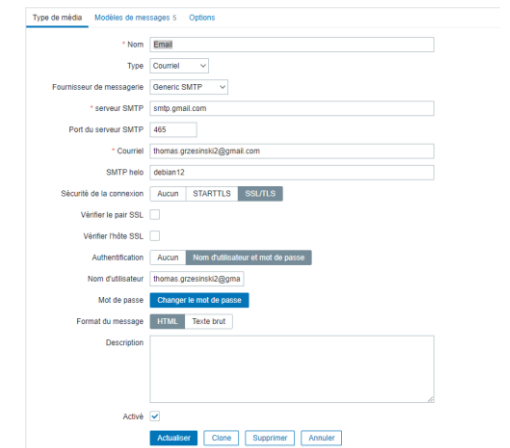
root <thomas.grzesinski2@gmail.com>

14:48 (il y a 0 minute)

À cci : moi ▾

Test de la messagerie du serveur Zabbix

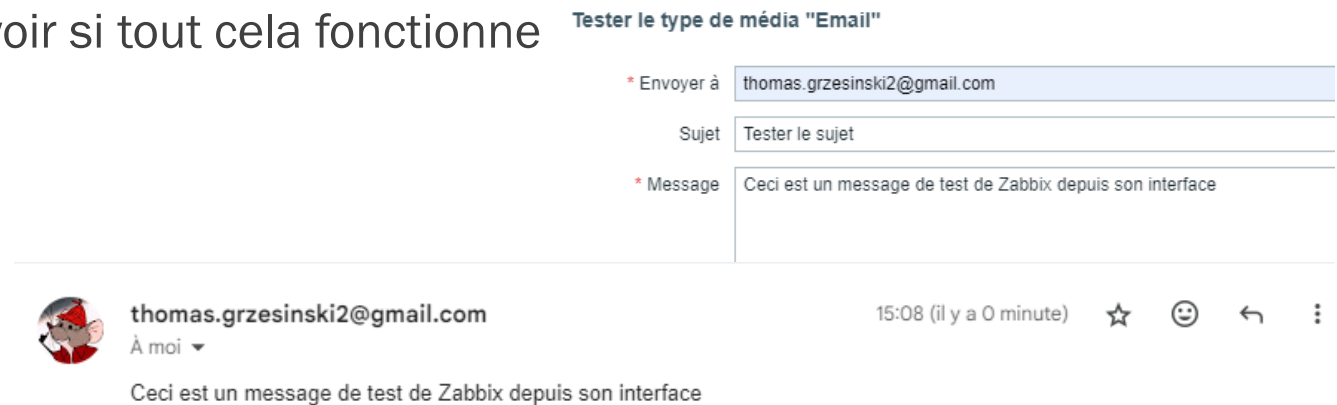
- Sur votre interface Zabbix vous devez donc configurer le type de média de cette manière:



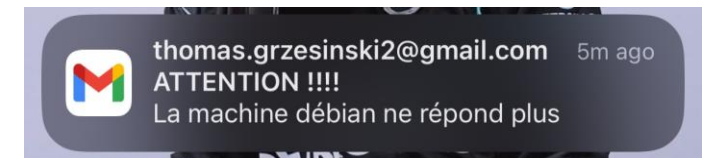
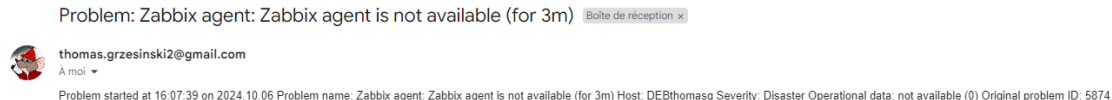
The screenshot shows the Zabbix media configuration interface. It includes fields for Name (Email), Type (Courriel), Message provider (Generic SMTP), SMTP server (smtp.gmail.com), Port (465), Email (thomas.grzesinski2@gmail.com), and SMTP helo (debian12). There are also checkboxes for connection security (STARTTLS, SSL/TLS), SSL verification, and authentication (None, Username and password). The authentication fields are filled with 'thomas.grzesinski2@gmail.com' for the username and a password field with a 'Change password' button. The message format is set to HTML. At the bottom, there are buttons for 'Actualiser', 'Cloner', 'Supprimer', and 'Annuler'.

Automatisation détection d'anomalie Notification mail

- Lancer un test a votre adresse mail pour voir si tout cela fonctionne



- A partir de maintenant vous allez donc recevoir des mails automatisés si votre machine ne répond plus



Source aide au tp

Source installation de Zabbix: [Tuto](#)

Source agent Zabbix Debian: [Tuto](#)

Source SNMP Windows Server: [Tuto](#)

Source SNMP Cisco: [Tuto](#)

Source création d'alerte et automatisation: [Tuto](#)