Lab supervision Zabbix

BENNAT Walid

LAB 4 : Les Déclencheur

Les **déclencheurs (triggers)** dans **Zabbix** sont un élément **fondamental** du système de supervision.

Ils servent à **détecter et signaler les problèmes** à partir des **données collectées** par les **éléments (items)**.

Qu’est-ce qu’un déclencheur (trigger) ?

Un **déclencheur** est une **condition logique** appliquée aux **valeurs collectées** par un **item** (élément de surveillance).

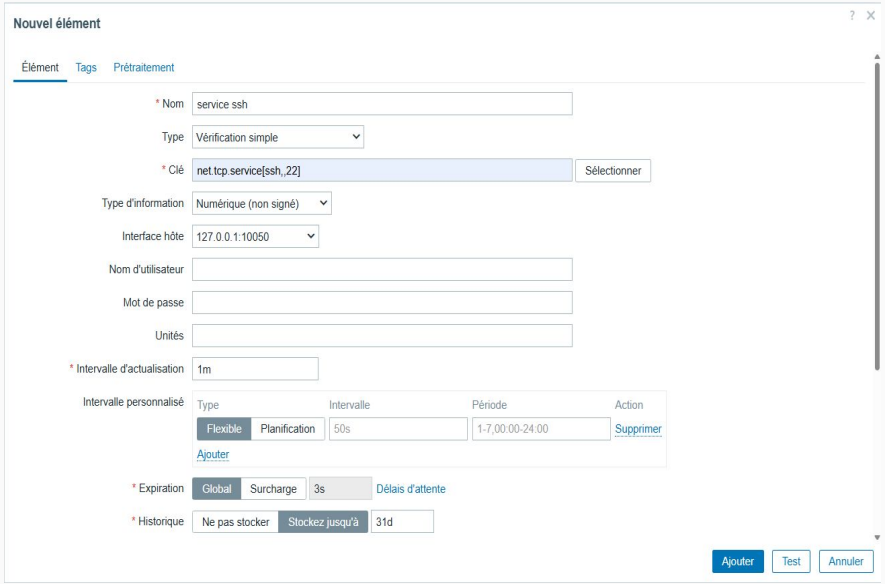
Exemple :

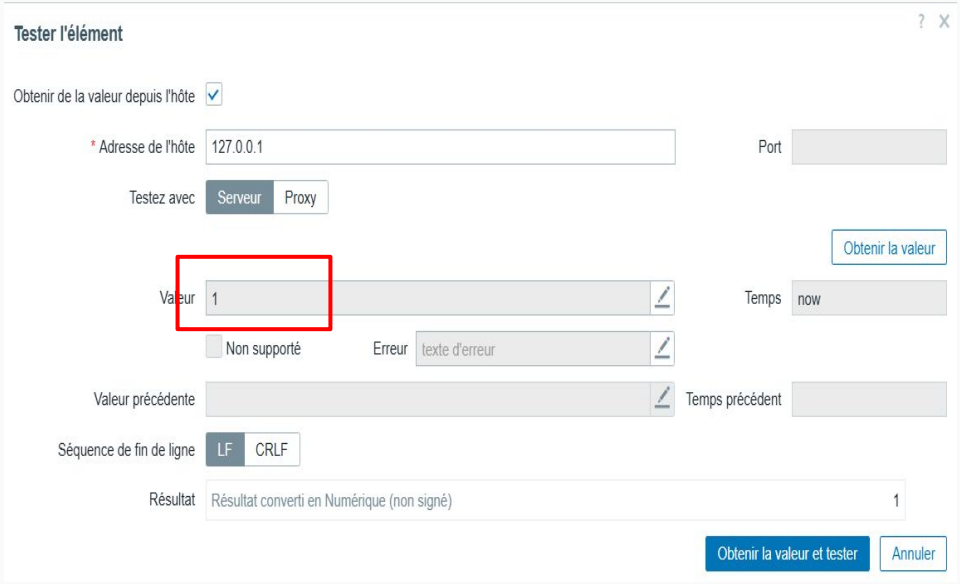
Si la charge CPU dépasse 90 % pendant 5 minutes → alors le déclencheur passe en **état de problème**.

LAB 4 : Les Déclencheur

Déclencheur SSH

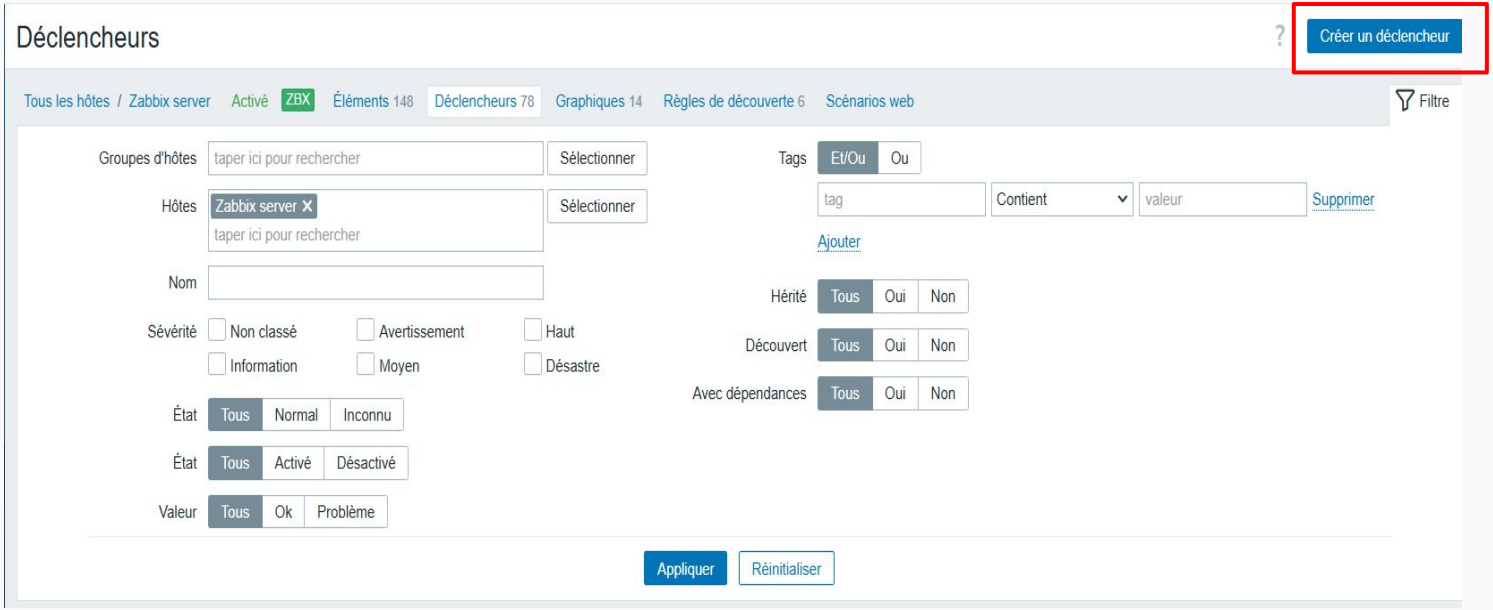
Étape 1 : Si aucun élément SSH n’a encore été créé, il faut en ajouter un.





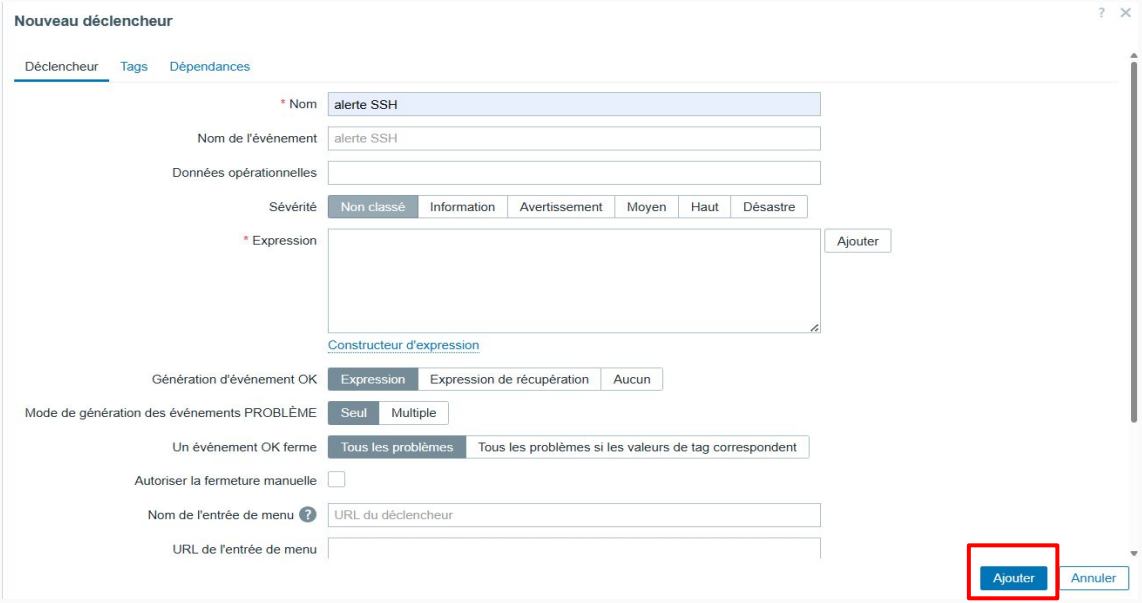
LAB 4 : Les Déclencheur

Créer un déclencheur

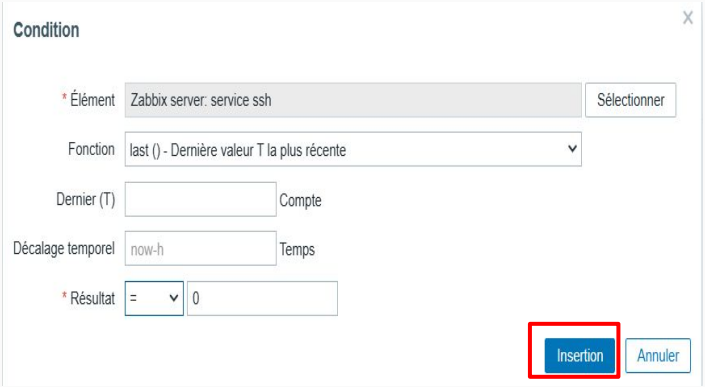


LAB 4 : Les Déclencheur

On doit maintenant ajouter une expression qui utilisera l'élément SSH déjà créé afin de l'intégrer dans notre élément de calcul.

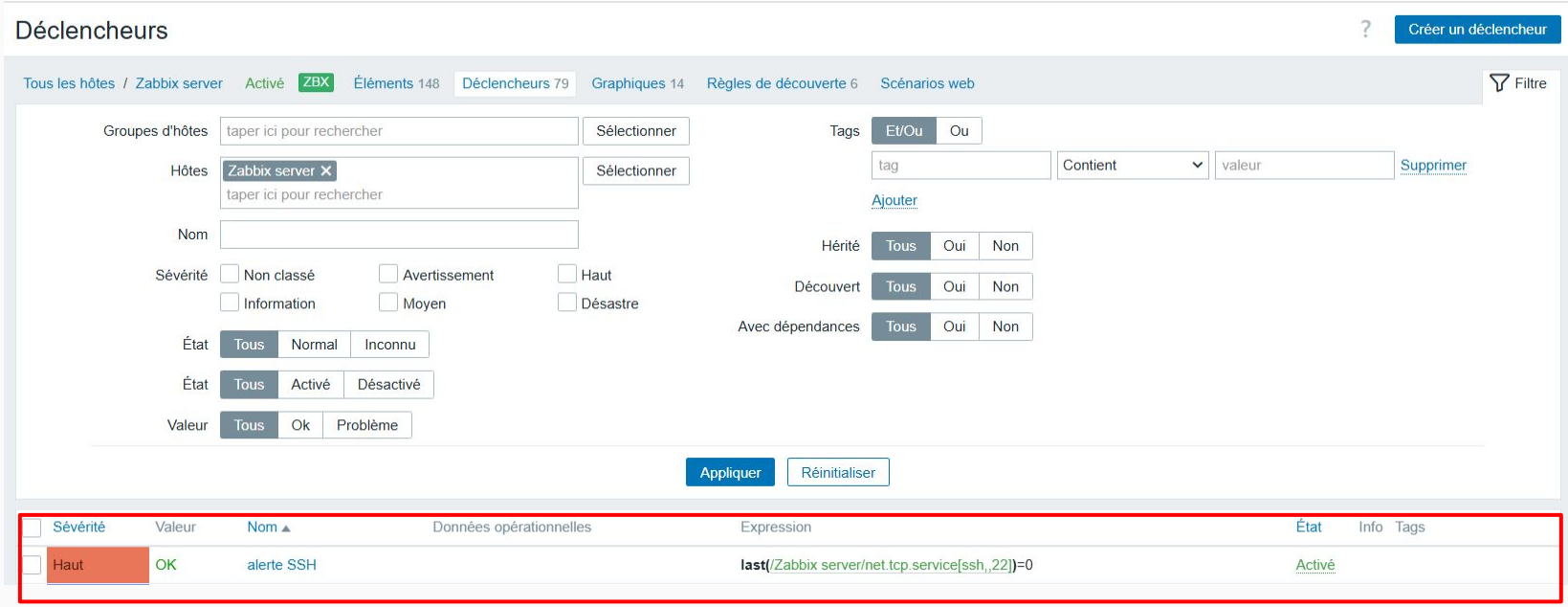


ajouter et insérer une expression



LAB 4 : Les Déclencheur

Déclencheur créé avec succès



LAB 4 : Les Déclencheur

Maintenant on va stopper SSH avec: sudo systemctl stop ssh

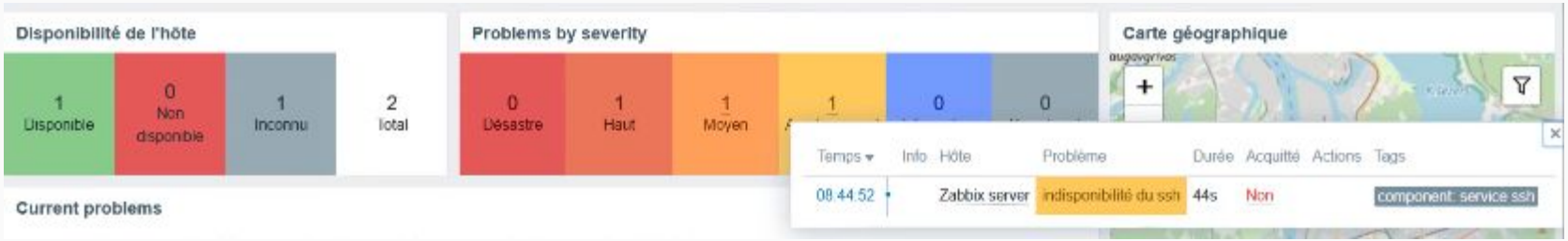
```
walidadmin@walid:~$ sudo systemctl stop ssh
[sudo] Mot de passe de walidadmin :
Stopping 'ssh.service', but its triggering units are still active:
ssh.socket
```

On peut vérifier avec: sudo systemctl status ssh

```
walidadmin@walid:~$ sudo systemctl status ssh
○ ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; preset: enab>
     Active: inactive (dead) since Mon 2025-11-03 17:17:03 CET; 10s ago
   Duration: 6h 54min 33.088s
TriggeredBy: ● ssh.socket
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 1258 ExecStart=/usr/sbin/sshd -D $SSHD_OPTS (code=exited, status=0>
   Main PID: 1258 (code=exited, status=0/SUCCESS)
        CPU: 1.062s
```

LAB 4 : Les Déclencheur

Résultat finale



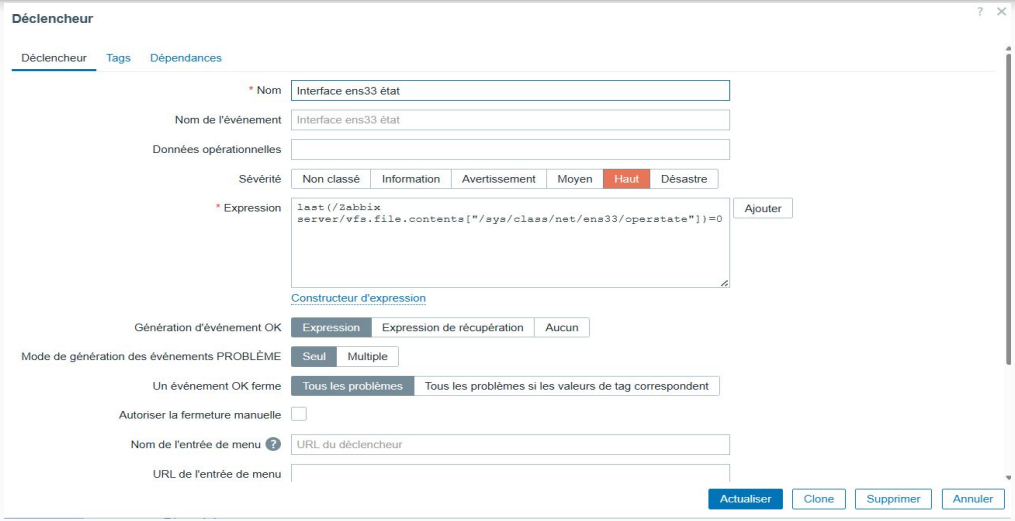
LAB 4 : Les Déclencheur

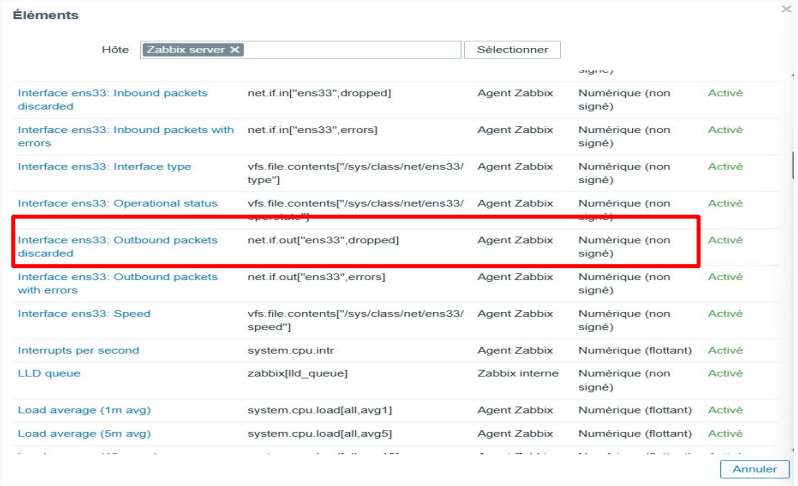
Exemple de déclencheur

N°	Objectif du déclencheur	Expression (exemple)	Gravité	Description / Action
1	Charge CPU trop élevée	{Serveur1:system.cpu.load.avg(5m)}>5	Average	La charge CPU moyenne dépasse 5 sur 5 min. Vérifie les processus consommateurs.
2	Utilisation mémoire trop élevée	{Serveur1:vm.memory.util.avg(5m)}>85	High	La mémoire utilisée dépasse 85 % sur 5 min. Risque de lenteur ou de crash.
3	Espace disque faible (partition /)	{Serveur1:vfs.fs.size[/,pfree].last()}<15	High	L'espace libre sur / est inférieur à 15 %. Supprime ou archive les fichiers inutiles.

LAB 4 : Les Déclencheur

Déclencheur pour interface ens33





Sévérité	Valeur	Nom ▲	Données opérationnelles	Expression	État	Info	Tags
Haut	OK	alerte SSH		**last**(/Zabbix server/net.tcp.service[ssh,,22])=0	Activé		
Haut	OK	Interface ens33 état		**last**(/Zabbix server/vfs.file.contents["/sys/class/net/ens33/operstate"])=2	Activé		

LAB 4 : Les Déclencheur

Déclencheur pour interface ens33

Consultez le lien officiel de Zabbix afin de mieux comprendre la syntaxe et l'utilisation des expressions de déclencheurs.

https://www.zabbix.com/documentation/5.2/en/manual/config/triggers/expression

LAB 4 : Les Déclencheur

Faux positifs

Un **faux positif**

Une alerte déclenchée par erreur — le système croit qu'un service, un équipement ou une ressource est en panne, mais ce n'est pas le cas.

Panne réseau momentanée

- Zabbix ne reçoit plus de réponse d'un hôte pendant quelques secondes (perte de paquets ou latence réseau).
- Il déclenche une alerte *"Host unreachable"*, mais le serveur n'était pas réellement en panne.
  → L'hôte fonctionne normalement : **faux positif**.

LAB 4 : Les Déclencheur

Faux positifs

Un **faux positif**

Seuils trop stricts

- Tu configures une alarme CPU > 80 %.
- Le CPU passe brièvement à 81 % pendant 5 secondes.
- Zabbix envoie une alerte, mais ce pic est normal et sans impact réel.
  → **Faux positif**, car le seuil n'est pas représentatif d'un vrai problème.