

Lab supervision Zabbix

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.

Nouvel élément

Élément Tags Prétraitement

* Nom service ssh

Type Vérification simple

* Clé net.tcp.service[ssh,22] Sélectionner

Type d'information Numérique (non signé)

Interface hôte 127.0.0.1:10050

Nom d'utilisateur

Mot de passe

Unités

* Intervalle d'actualisation 1m

Intervalle personnalisé

Type	Intervalle	Période	Action
Flexible	Planification	50s	1-7:00:00-24:00

Ajouter Supprimer

* Expiration Global Surcharge 3s Délais d'attente

* Historique Ne pas stocker Stockez jusqu'à 31d

Ajouter Test Annuler

Tester l'élément

Obtenir de la valeur depuis l'hôte

* Adresse de l'hôte 127.0.0.1 Port

Testez avec Serveur Proxy

Obtenir la valeur

Valeur Temps now

Non supporté Erreur texte d'erreur

Valeur précédente Temps précédent

Séquence de fin de ligne LF CRLF

Résultat Résultat converti en Numérique (non signé) 1

Obtenir la valeur et tester Annuler

LAB 4 : Les Déclencheur

Créer un déclencheur

Déclencheurs

Tous les hôtes / Zabbix server Activé ZBX Éléments 148 Déclencheurs 78 Graphiques 14 Règles de découverte 6 Scénarios web ? Filtre

Groupes d'hôtes Sélectionner

Hôtes Zabbix server Sélectionner

Nom

Sévérité Non classé Avertissement Haut
 Information Moyen Désastre

État Tous Normal Inconnu

État Tous Activé Désactivé

Valeur Tous Ok Problème

Tags Et/Ou Ou
tag Contient valeur Supprimer Ajouter

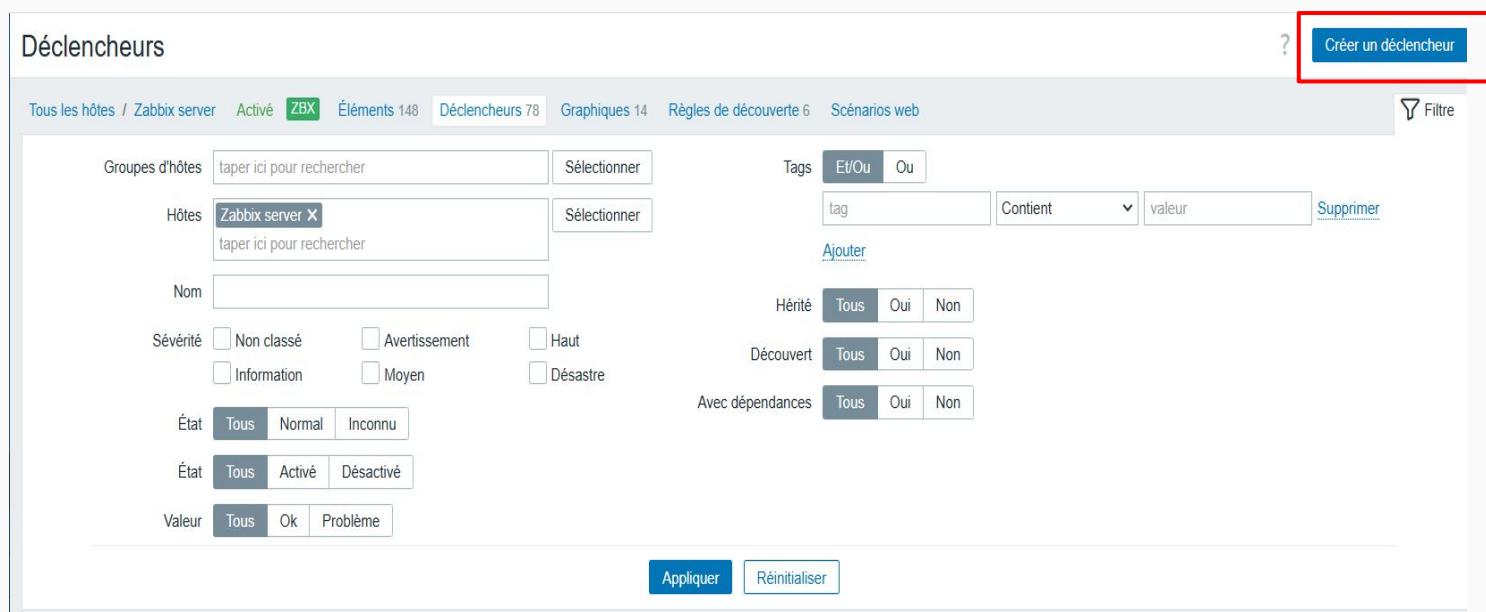
Hérité Tous Oui Non

Découvert Tous Oui Non

Avec dépendances Tous Oui Non

Créer un déclencheur

Appliquer Réinitialiser



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.

Nouveau déclencheur

Déclencheur Tags Dépendances

* Nom alerte SSH

Nom de l'événement alerte SSH

Données opérationnelles

Sévérité Non classé Information Avertissement Moyen Haut Désastre

* Expression

Ajouter

Constructeur d'expression

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

Ajouter Annuler

ajouter et insérer une expression

Condition

* Élément Zabbix server: service ssh Sélectionner

Fonction last() - Dernière valeur T la plus récente

Dernier (T) Compte

Décalage temporel now-h Temps

* Résultat = 0

Insertion Annuler

The screenshot illustrates the configuration of a new trigger named "alerte SSH". In the main window, the "Expression" field is empty and has an "Ajouter" button. A modal window titled "ajouter et insérer une expression" is open, showing a "Condition" section with fields for element, function, time range, and result. The "Insertion" button in the modal is highlighted with a red box, indicating the next step is to insert the condition into the trigger's expression.

LAB 4 : Les Déclencheur

Déclencheur
créé avec
succès

Déclencheurs

Tous les hôtes / Zabbix server Activé ZBX Éléments 148 Déclencheurs 79 Graphiques 14 Règles de découverte 6 Scénarios web

Filtre

Groupes d'hôtes : taper ici pour rechercher Sélectionner Tags : Et/Ou Ou

Hôtes : Zabbix server X Sélectionner tag Contient valeur Supprimer

taper ici pour rechercher

Nom : Ajouter

Sévérité : Non classé Avertissement Haut Hérité : Tous Oui Non

Information Moyen Désastre Découvert : Tous Oui Non

Moyen Désastre Avec dépendances : Tous Oui Non

État : Tous Normal Inconnu

État : Tous Activé Désactivé

Valeur : Tous Ok Problème

Appliquer Réinitialiser

Sévérité	Valeur	Nom ▲	Données opérationnelles	Expression	État	Info	Tags
<input type="checkbox"/> Haut	OK	alerte SSH		last(/Zabbix server/net.tcp.service[ssh,,22])=0	Activé		

LAB 4 : Les Déclencheur

Maintenant on va stopper SSH avec: sudo systemctl stop ssh

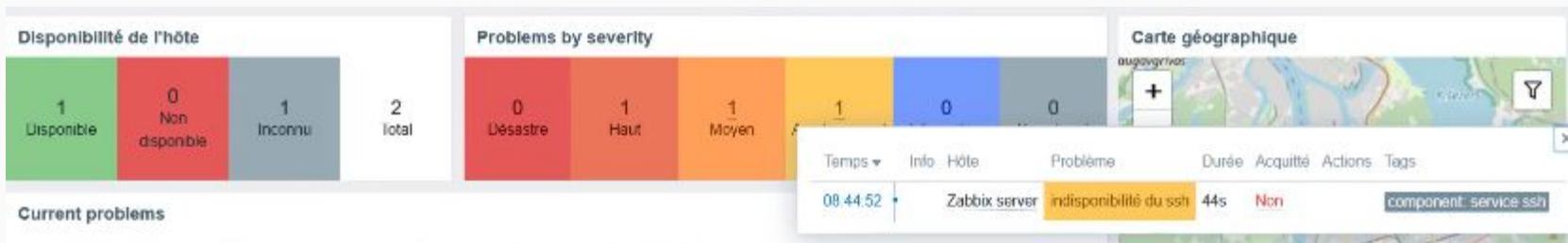
```
walidadmin@walid:~$ sudo systemctl stop ssh
[sudo] Mot de passe de walidadmin :
Stopping 'ssh.service', but its triggering units are still active:
ssh.socket
```

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: enabled)
  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:syste m.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.av g(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

Déclencheur

Nom : Interface ens33 état

Nom de l'événement : Interface ens33 état

Données opérationnelles :

Sévérité : Haut

* Expression : `last(/Zabbix server vfs.file.contents["/sys/class/net/ens33/operstate"])=0`

Génération d'événement OK : Expression

Mode de génération des événements PROBLÈME : Seul

Un événement OK ferme : Tous les problèmes

Autoriser la fermeture manuelle :

Nom de l'entrée de menu : URL du déclencheur

URL de l'entrée de menu :

Actualiser | Clone | Supprimer | Annuler

Éléments

Hôte	Zabbix server	Sélectionner		
Interface ens33: Inbound packets discarded	net.if.in["ens33",dropped]	Agent Zabbix	Numérique (non signé)	Activé
Interface ens33: Inbound packets with errors	net.if.in["ens33",errors]	Agent Zabbix	Numérique (non signé)	Activé
Interface ens33: Interface type	vfs.file.contents["/sys/class/net/ens33/type"]	Agent Zabbix	Numérique (non signé)	Activé
Interface ens33: Operational status	vfs.file.contents["/sys/class/net/ens33/oper"]	Agent Zabbix	Numérique (non signé)	Activé
Interface ens33: Outbound packets discarded	net.if.out["ens33",dropped]	Agent Zabbix	Numérique (non signé)	Activé
Interface ens33: Outbound packets with errors	net.if.out["ens33",errors]	Agent Zabbix	Numérique (non signé)	Activé
Interface ens33: Speed	vfs.file.contents["/sys/class/net/ens33/speed"]	Agent Zabbix	Numérique (non signé)	Activé
Interrupts per second	system.cpu.intr	Agent Zabbix	Numérique (flottant)	Activé
LLD queue	zabbix[lld_queue]	Zabbix interne	Numérique (non signé)	Activé
Load average (1m avg)	system.cpu.load[all,avg1]	Agent Zabbix	Numérique (flottant)	Activé
Load average (5m avg)	system.cpu.load[all,avg5]	Agent Zabbix	Numérique (flottant)	Activé

Annuler

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