

CONFIGURER DES ACTIONS AVEC ZABBIX 7



SOMMAIRE

1. L'ALERTING C'EST QUOI ?
2. LA MISE EN PLACE DES ALERTES AVEC ZABBIX 7.0
 - a. Configuration d'un compte de messagerie
 - b. Test de l'envoi d'une notification par mail
 - c. Configuration d'une action de déclencheur
 - d. Vérifier le bon fonctionnement de l'alerting en simulant une panne dans l'infrastructure
 - e. Vérifier le retour à l'état normal (réception des notifications)

© tutos-info.fr - 07/2024



DIFFICULTE



UTILISATION COMMERCIALE INTERDITE

1 – L'ALERTING C'EST QUOI ?

ZABBIX est une solution open source très puissante qui permet d'auditer et de monitorer une infra complète (voir tutoriel « Installer et configurer Zabbix »). Dans ce tutoriel, nous allons étudier les actions « d'alerting » offertes par Zabbix 7.0.

En matière de sécurité, on distingue des différences entre un **événement**, une **alerte** et un **incident** de sécurité. Quel est le rôle respectif de chacun dans la sécurité informatique ? Comment bien utiliser les événements de sécurité, les alertes et les incidents dans le cadre de sa sécurité opérationnelle ?

Une alerte de sécurité est une notification produite par un outil de surveillance ou un système de détection. **L'alerte se produit** lorsqu'un événement susceptible de **révéler une activité malveillante ou une violation de sécurité** a été identifié. Les alertes de sécurité sont généralement générées à la suite d'une analyse automatisée des événements de sécurité. Une intervention humaine permet d'évaluer leur gravité et de confirmer ou non leur caractère malveillant.

Un événement de sécurité est une **action rapportée par un système de surveillance**. Les événements de sécurité ne représentent pas nécessairement une menace pour la sécurité informatique. Une analyse plus approfondie est nécessaire pour le déterminer.

On parle **d'incident de sécurité lorsque des dommages sont causés (ou susceptibles d'être causés) à un système d'information, que des données et/ou des systèmes sont compromis**. La violation de sécurité est identifiée et confirmée. Un incident de sécurité appelle une réponse rapide permettant de le contenir, de comprendre la situation et d'y remédier afin d'en limiter les dommages (potentiels ou avérés).

L'importance de la détection précoce des événements

Les outils de gestion des événements de sécurité offrent une visibilité complète sur l'activité d'un système d'information. Ils permettent ainsi d'être informé en temps réel des événements qui s'y déroulent, et de détecter de manière précoce les événements qui sortent des schémas habituels. Cette détection précoce offre justement une plus grande réactivité face aux menaces.

Réaction aux alertes et prévention des attaques

Bien configurées, les alertes attirent l'attention des équipes chargées de la sécurité opérationnelle, les invitant à réagir rapidement et à investiguer. **Objectif** : prendre les mesures nécessaires pour protéger le SI d'une violation de sécurité et éviter la survenue d'un incident de sécurité majeur.

Gestion des incidents pour minimiser les impacts

Une fois l'incident de sécurité confirmé, différentes mesures permettent d'éviter sa propagation et d'en minimiser les impacts : qualifier l'incident, isoler les systèmes ou les machines infectés le cas échéant, etc. La méthodologie relative à la gestion des incidents de sécurité comporte également une phase de RETEX destinée à faire le point sur la crise passée et à capitaliser dessus afin d'éviter la survenue de nouveaux incidents.

Exemples d'événements de sécurité

- **Anomalies de trafic sur le réseau** : augmentation inhabituelle du volume du trafic, par exemple.

- **Activités inhabituelles et suspectes liées au comportement des utilisateurs** : tentatives et échecs répétés d'authentification, changements de privilèges, tentatives d'accès non autorisés à des ressources, etc.

Exemples d'alertes de sécurité

Certains outils de détection sont en mesure de repérer un nombre élevé d'échecs de tentatives d'authentification sur une courte période. Cette information se transforme en alerte de sécurité car elle signale une possible **tentative d'attaque par force brute**. Si les équipes chargées de la sécurité parviennent à identifier l'adresse IP à partir de laquelle la tentative d'attaque a été lancée, elles peuvent par exemple la bloquer.

Les alertes de sécurité sont également susceptibles de prévenir de **tentatives d'intrusion**. Les éléments associés à l'alerte et l'analyse réalisée permettent d'aiguiller les équipes sur les mesures à prendre : blocage de l'adresse IP à l'origine de la tentative d'intrusion, désactivation des ports réseau inutilisés, meilleure configuration des pare-feu, renforcement de la gestion des accès et des privilèges, etc.

Le **rançongiciel** est un **exemple typique d'incident de sécurité**, qu'il est possible de découper en 4 grandes phases :

1. Reconnaissance de la cible afin de comprendre son écosystème, à partir d'informations disponibles publiquement, de fuites de données, etc.
2. Accès initial : obtention d'identifiants de connexion, par exemple via des emails de phishing, puis diffusion d'un logiciel malveillant (loader).
3. Exploitation, avec escalade de privilèges et déplacement latéral. L'objectif de cette phase est d'obtenir davantage de droits et d'étendre son emprise sur le réseau de l'organisation ciblée.
4. Impact : chiffrement des données, diffusion d'une demande de rançon.

2 – LA MISE EN PLACE DES ALERTES AVEC ZABBIX 7.0

CONFIGURATION D'UNE ADRESSE DE MESSAGERIE POUR L'ALERTING

On commence, ici, par la configuration d'une boîte mail afin que Zabbix nous avertisse en cas de problème dans l'infra.

Pour notre tutoriel, nous allons utiliser une adresse de type Office 365 (tutoriel de laboratoire). En production il sera possible, bien entendu, de configurer un mail professionnel adapté et différent.

Attention, pour la réalisation de cette partie, il faudra vous munir des identifiants de connexion du compte mail à ajouter.

Pour cela, depuis l'interface web de Zabbix :

- Cliquez, dans le volet de gauche, sur « **Alertes** » - « **Types de média** »
- Dans la liste affichée, cliquez sur « **Office365** » afin d'indiquer les paramètres de votre compte mail Office 365 :



- Saisissez un nom (« SERVEUR ZABBIX » par exemple) et saisissez les paramètres de votre compte de messagerie (ici Office 365), **sans oublier de cliquer la case « Activé »**, puis cliquez « **Actualiser** » :

✓ Type de média mis à jour

Le compte apparaît dans la liste :

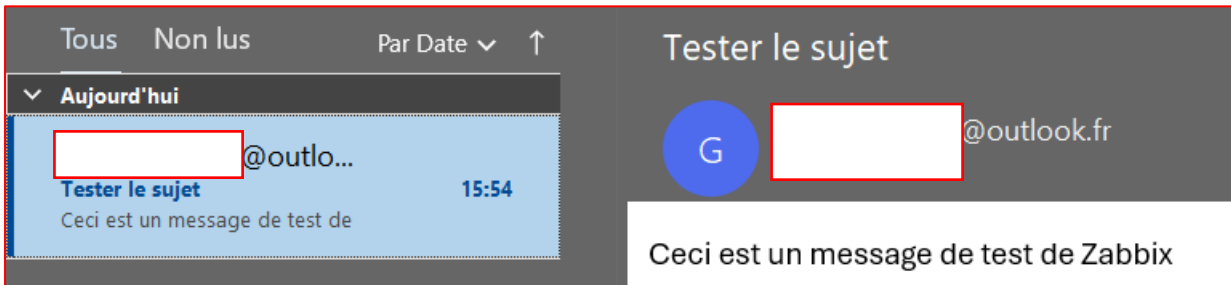
Alertes	Types de média	Scripts	Utilisateurs
<input type="checkbox"/>	Telegram	Webhook	Désactivé
<input type="checkbox"/>	TOPdesk	Webhook	Désactivé
<input type="checkbox"/>	VictorOps	Webhook	Désactivé
<input type="checkbox"/>	ZABBIX SERVEUR	Courriel	Activé

CONFIGURATION DE LA LIVRAISON DES NOTIFICATIONS

On teste la configuration du compte mail pour s’assurer que les notifications par mail fonctionnent. Pour cela :

- Cliquez le lien bleu « **Test** » situé à droite du compte mail précédemment configuré ; une fenêtre s’affiche, complétez-la avec une adresse de destinataire :

- Cliquez le bouton « **Test** » ; si vos paramètres ont été correctement configurés, vous recevrez un mail de test et le message suivant :



CONFIGURATION DU COMPTE MAIL DE L'ADMINISTRATEUR ZABBIX

Maintenant que le compte mail est configuré et testé, on l'enregistre dans le compte administrateur de Zabbix. Bien entendu, vous pouvez créer un nouvel utilisateur avec des droits d'administration si vous ne souhaitez pas utiliser le compte d'administrateur par défaut.

- Cliquez, dans le volet de gauche de l'interface web de Zabbix, sur « **Utilisateurs** » - « **Utilisateurs** »
- Cliquez sur l'utilisateur « **Admin** » (utilisateur administrateur créé par défaut) :

<input type="checkbox"/>	Nom d'utilisateur ▲	Prénom	Nom de famille	Rôle utilisateur	Groupes	Est connecté ?	Connexion	Accès à l'interface	Accès API	Mode debug	État	Provisionné
<input type="checkbox"/>	Admin	Zabbix	Administrator	Super admin role	Internal, Zabbix administrators	Oui (26/06/2024 14:40:01)	Ok	Interne	Activé	Désactivé	Activé	
<input type="checkbox"/>	guest			Guest role	Disabled, Guests, Internal	Non	Ok	Interne	Désactivé	Désactivé	Désactivé	

- Cliquez, dans le haut de la fenêtre, sur « **Média** »
- Cliquez le lien bleu « **Ajouter** », complétez la fenêtre et cliquez « **Actualiser** » :

Média ✕

Type

* Envoyer à [Supprimer](#)

[Ajouter](#)

* Lorsque actif

Utiliser si sévérité

- Non classé
- Information
- Avertissement
- Moyen
- Haut
- Désastre

Activé

- Cliquez « **Actualiser** » pour valider les paramètres d'envoi de courriels :

Utilisateurs

Utilisateur Média 1 Permissions

Média	Type	Envoyer à	Lorsque actif	Utiliser si sévérité	État	Action
	*ZABBIX	<input type="text" value=""/> @ik.me	1-7,00:00-24:00	N I A M H D	Activé	Édition Supprimer
Ajouter						

Actualiser Supprimer Annuler

Utilisateur mis à jour

CONFIGURATION D'UNE ACTION DE DECLENCHEUR AVEC NOTIFICATION PAR MAIL

Nous allons configurer une « **action** » Zabbix dite de « **déclencheur** » qui permettra d'être notifié en cas de problème. Pour cela, depuis l'interface web de Zabbix, effectuez les manipulations suivantes :

- Cliquez sur « **Alertes** » - « **Actions** » et « **Actions de déclencheur** » :

Alertes

Actions

Types de média

Scripts

Utilisateurs

Actions de déclencheur

Actions des services

Actions de découverte

Actions d'enregistrement automatique

Actions internes

- Cliquez, en haut à droite de la fenêtre affichée, sur « **Créer une action** »
- Saisissez un nom pour l'action :

Action

Action Opérations 1

* Nom ALERTE ARRET HOTE

- Cliquez le lien « **Ajouter** » de la rubrique « **Conditions** » afin de définir des actions de déclenchement ; une fenêtre s'affiche :

Nouvelle condition

Type Déclencheur

Opérateur égal n'est pas égal

Source du déclencheur Hôte Modèle

* Déclencheurs taper ici pour rechercher Sélectionner

Ajouter Annuler

- Sélectionner les déclencheurs en cliquant le bouton « **Sélectionner** »
- Cliquez à nouveau « **Sélectionner** » pour choisir les hôtes à surveiller :

Déclencheurs

Hôte

- Choisissez le groupe d'hôtes à inclure. Ici, nous choisissons « **Virtual machines** » car nous avons affecté les machines virtuelles Windows 11 initiales dans ce groupe d'hôte (cela peut être modifié) :

Groupes d'hôtes

Nom

[Discovered hosts](#)

[Linux servers](#)

Virtual machines

[Zabbix servers](#)

- Sélectionner la machine souhaitée (« win11 » par exemple) :

Hôtes

Groupe d'hôtes

Nom

win11

win11-2

- Choisissez, ensuite, les conditions de déclenchement souhaitées dans la liste. Ici, nous avons sélectionné **des conditions avec une sévérité moyenne** (alerte de non-fonctionnement) mais également **des conditions de type « avertissement »** (redémarrage de l'hôte) :

Déclencheurs

Hôte

<input type="checkbox"/>	mscorsvc (Microsoft Defender Service de base) is not running	Moyen	Activé
<input type="checkbox"/>	"mpssvc" (Pare-feu Windows Defender) is not running	Moyen	Activé
<input type="checkbox"/>	"nsi" (Service Interface du magasin réseau) is not running	Moyen	Activé
<input type="checkbox"/>	"PcaSvc" (Service de l'Assistant Compatibilité des programmes) is not running	Moyen	Activé
<input checked="" type="checkbox"/>	"Power" (Alimentation) is not running	Moyen	Activé

Déclencheurs

Hôte

<input type="checkbox"/>	"wscsvc" (Centre de sécurité) is not running	Moyen	Activé
<input type="checkbox"/>	"WSearch" (Windows Search) is not running	Moyen	Activé
<input checked="" type="checkbox"/>	"Zabbix Agent" (Zabbix Agent) is not running	Moyen	Activé
<input type="checkbox"/>	0 C:: Disk is overloaded Dépend de 0 C:: Disk read request responses are too high 0 C:: Disk write request responses are too high	Avertissement	Activé
<input type="checkbox"/>	0 C:: Disk read request responses are too high	Avertissement	Activé
<input type="checkbox"/>	0 C:: Disk write request responses are too high	Avertissement	Activé
<input checked="" type="checkbox"/>	Active checks are not available	Haut	Activé

Déclencheurs

Hôte

Dépend de
High memory utilization

<input checked="" type="checkbox"/>	Host has been restarted	Avertissement	Activé
-------------------------------------	-------------------------	---------------	--------

- Cliquez le bouton « **Sélectionner** » pour valider les conditions retenues pour l'alerting :

Nouvelle condition

Type

Opérateur

Source du déclencheur

* Déclencheurs

- win11: "Power" (Alimentation) is not running x
- win11: "Zabbix Agent" (Zabbix Agent) is not... x
- win11: Active checks are not available x
- win11: Host has been restarted x

taper ici pour rechercher

- Cliquez « **Ajouter** » et « **Actualiser** » pour valider vos choix ; vous obtenez ceci :

Action

Action Opérations 2

* Nom

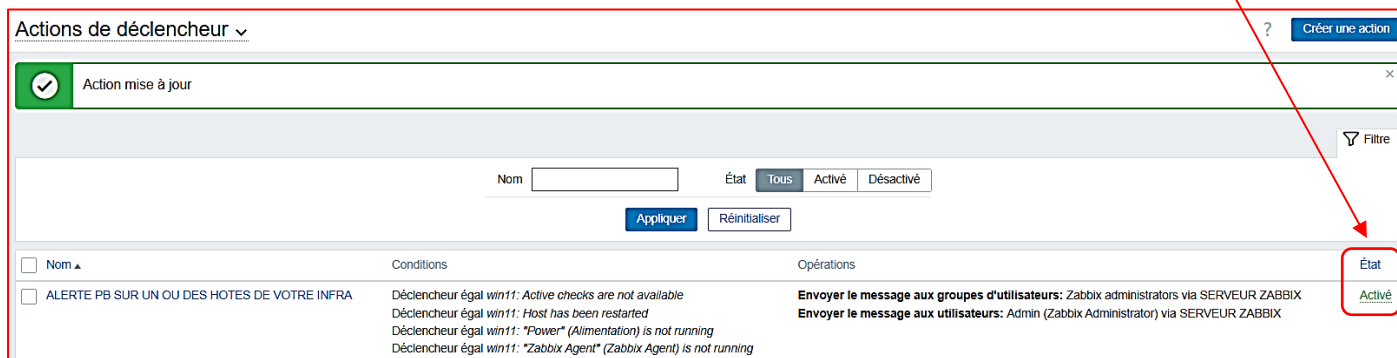
Type de calcul A or B or C or D

Conditions	Etiquette	Nom	Action
A		Déclencheur égal win11: Host has been restarted	Supprimer
B		Déclencheur égal win11: "Power" (Alimentation) is not running	Supprimer
C		Déclencheur égal win11: "Zabbix Agent" (Zabbix Agent) is not running	Supprimer
D		Déclencheur égal win11: Active checks are not available	Supprimer

Activé

* Au moins une opération doit exister.

Votre action de déclenchement est maintenant activée (l'état de l'action s'affiche en mode « **Activé** » sur le côté droit de la fenêtre) :



Actions de déclencheur ▾ ? Créer une action

✓ Action mise à jour

Filter

Nom État Tous Activé Désactivé

Appliquer Réinitialiser

<input type="checkbox"/> Nom ▲	Conditions	Opérations	État
<input type="checkbox"/> ALERTE PB SUR UN OU DES HOTES DE VOTRE INFRA	Déclencheur égal win11: Active checks are not available Déclencheur égal win11: Host has been restarted Déclencheur égal win11: "Power" (Alimentation) is not running Déclencheur égal win11: "Zabbix Agent" (Zabbix Agent) is not running	Envoyer le message aux groupes d'utilisateurs: Zabbix administrators via SERVEUR ZABBIX Envoyer le message aux utilisateurs: Admin (Zabbix Administrator) via SERVEUR ZABBIX	Activé

TEST D'ALERTING AVEC SIMULATION D'UNE PANNE

Afin de vérifier si l'alerting fonctionne bien (réception d'un mail de notification), nous allons simuler une panne en arrêtant la machine Windows 11. Patientez quelques minutes de manière à ce que Zabbix détecte le problème (agent inactif).

- Ouvrez votre boîte mail et relevez votre courrier ; un mail d'alerte a été réceptionné et vous informe que la machine « win11 » pose un souci car son état est en mode « **not available** » avec une sévérité haute (« **high** ») :

Problem started at 16:58:32 on 2024.06.26
Problem name: Active checks are not available
Host: win11
Severity: High
Operational data: Current state: not available (2)
Original problem ID: 220

Si vous ne rallumez pas la machine immédiatement et que vous patientez, vous recevrez d'autres mails de notification comme celui-ci qui nous informe que Zabbix n'a pas reçu de réponse des agents depuis plus de 10 minutes :

Problem started at 17:12:51 on 2024.06.26
Problem name: More than 100 items having missing data for more than 10 minutes
Host: Zabbix server
Severity: Warning
Operational data: 216
Original problem ID: 223

- Rallumez la machine Windows 11 qui était défectueuse pour simuler la réparation de cette dernière et patientez quelques minutes.

Un mail de notification est reçu quelques minutes plus tard et confirme le rétablissement de la situation :

```
Problem has been resolved at 16:36:57 on 2024.06.26
Problem name: Host has been restarted (uptime < 10m)
Problem duration: 7m 58s
Host: win11
Severity: Warning
Original problem ID: 215
```

Un autre mail indique le problème a été résolu :

```
Problem has been resolved at 16:29:32 on 2024.06.26
Problem name: Active checks are not available
Problem duration: 5m 0s
Host: win11
Severity: High
Original problem ID: 213
```

De nombreuses autres possibilités d'actions sont possibles. Il n'est pas possible de toutes les exposer ici. Nous vous invitons à les tester afin de mesurer toute la puissance de Zabbix !

Fichiers et commandes Zabbix utiles

Fichier de configuration de l'agent Zabbix :

/etc/zabbix/zabbix_agentd.conf

Fichier de configuration du serveur Zabbix :

/etc/zabbix/zabbix_server.conf

Relancer l'agent Zabbix sur Debian :

systemctl restart zabbix-agent

Vérifier le statut du serveur Zabbix sur Debian :

systemctl status zabbix-server