FICHE PROCEDURE

CONFIGURATION ZABBIX — SUPERVISION DE SECURITE ET DETECTION D'INTRUSIONS

Auteur: CHADHOULI EL-Anrif

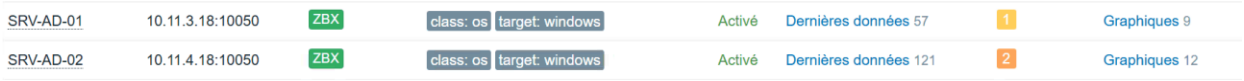
Dossier BTS SIO SISR — Supervision des échecs de connexion Windows via Event ID 4625

CONTEXTE ET OBJECTIF

Cette procédure permet de configurer Zabbix afin de surveiller les échecs de connexion Windows sur un contrôleur de domaine et de remonter immédiatement une alerte de sécurité lorsqu'un Event ID 4625 est détecté.

Le principe est le suivant: l'agent Zabbix installé sur SRV-AD-01 lit localement les journaux Windows puis envoie l'information au serveur Zabbix en mode actif. Le serveur Zabbix centralise ensuite l'événement, déclenche une alerte et l'affiche sur le tableau de bord.

Élément	Valeur
Serveur Zabbix	10.11.3.19 — Debian 12
Cible supervisée	SRV-AD-01 — 10.11.3.18 — Windows Server 2025
Événement surveillé	Security Event ID 4625
Mode agent	Actif



PRE-REQUIS

- Accès administrateur à SRV-AD-01.
- Accès administrateur à l'interface Web Zabbix.
- Agent Zabbix installé sur SRV-AD-01.
- Connectivité réseau fonctionnelle entre SRV-AD-01 et 10.11.3.19 sur le port Zabbix.
- Heure système synchronisée sur le serveur et sur le poste Windows pour éviter les incohérences de logs.

CONFIGURATION DE L'AGENT ZABBIX SUR WINDOWS

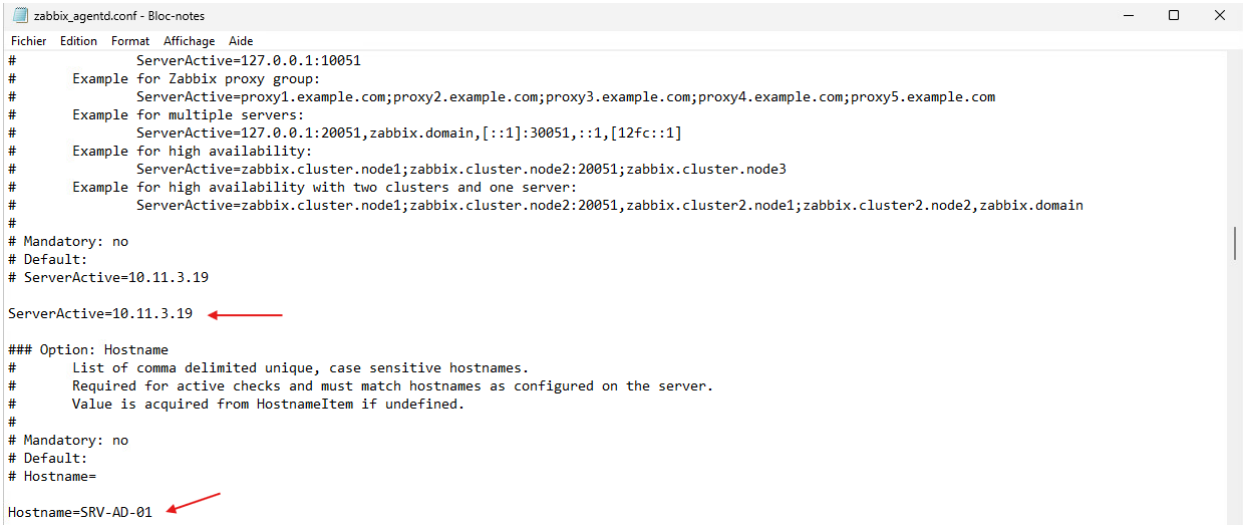
1. Modifier le fichier de configuration

Le mode actif est obligatoire dans ce cas, car l'agent doit pousser lui-même les données vers le serveur Zabbix. Cela évite de dépendre d'une interrogation passive et permet de remonter plus proprement les événements du journal Security.

- Ouvrir le fichier zabbix_agentd.conf sur SRV-AD-01.
- Renseigner ou vérifier les paramètres suivants:

```
ServerActive=10.11.3.19
Hostname=SRV-AD-01
```

- Vérifier que le service démarre automatiquement avec Windows.



2. Redémarrer le service

Après modification du fichier, il faut redémarrer le service pour que l'agent charge la nouvelle configuration. Sans redémarrage, Zabbix peut continuer à utiliser l'ancienne configuration en mémoire.

- Ouvrir services.msc sur SRV-AD-01.
- Rechercher le service Zabbix Agent.
- Cliquer sur Redémarrer.
- Vérifier que l'état du service est En cours d'exécution.

CREATION DE L'ITEM ZABBIX

3. Créer l'item de collecte

L'item sert à lire automatiquement les événements d'échec de connexion dans le journal Security de Windows. Le code 4625 correspond à un échec d'authentification, ce qui en fait un indicateur utile pour détecter des tentatives de mot de passe erroné ou de bruteforce.

- Ouvrir l'interface Web Zabbix.
- Aller dans Configuration > Hosts > SRV-AD-01 > Items.
- Cliquer sur Create item.

Paramètre	Valeur
Nom	Audit - Echec de connexion (Event ID 4625)
Type	Zabbix agent (active)
Key	eventlog[Security,,,,4625]
Type d'information	Log

- Enregistrer l'item.
- Vérifier qu'il est actif et qu'il commence à remonter des données.

CREATION DU TRIGGER D'ALERTE

4. Créer le déclencheur

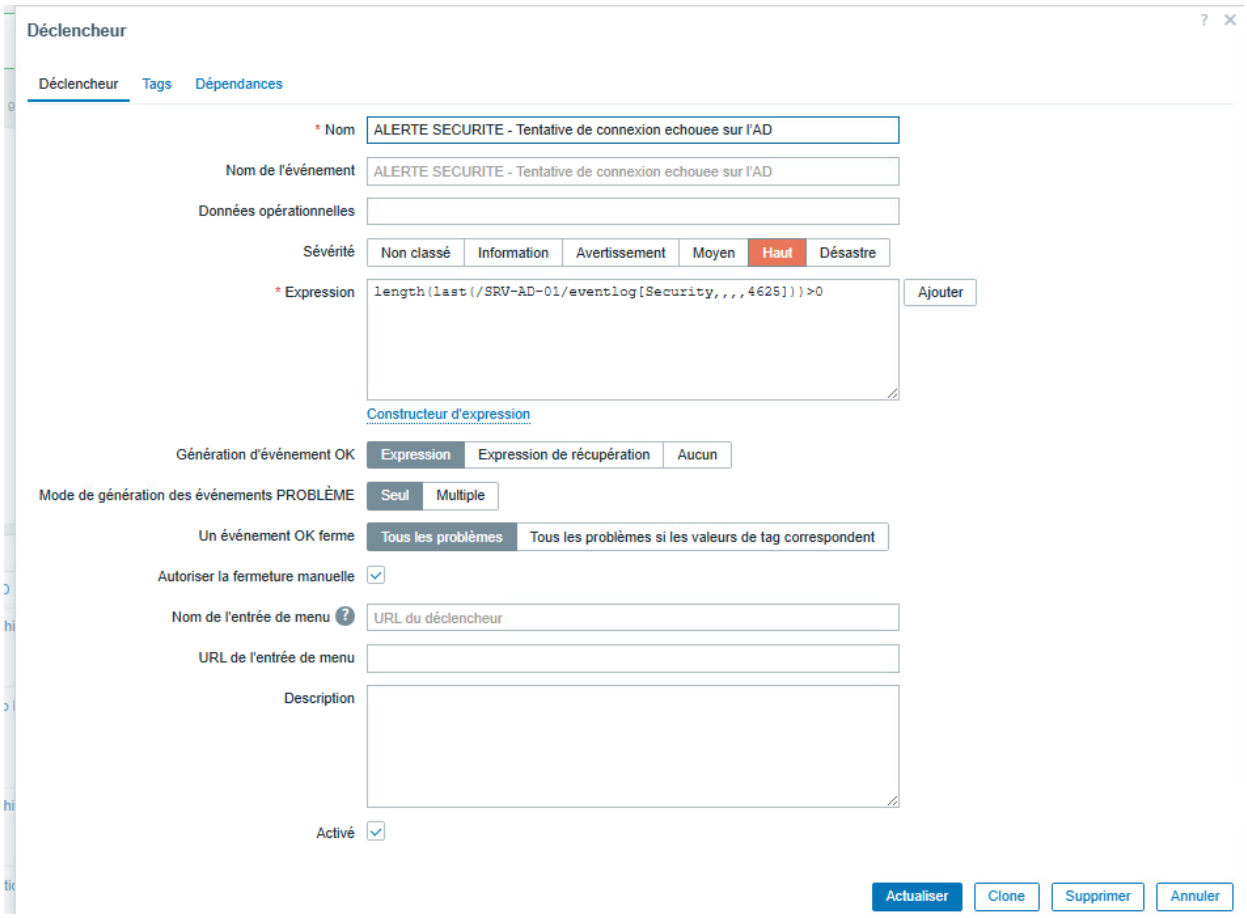
Le trigger transforme la remontée de l'événement en alerte visible immédiatement dans Zabbix. La sévérité High est adaptée car un Event ID 4625 répété peut signaler une tentative d'attaque par mot de passe ou une mauvaise configuration du compte.

- Dans l'hôte SRV-AD-01, ouvrir l'onglet Triggers.
- Cliquer sur Create trigger.

Paramètre	Valeur
Nom de l'alerte	ALERTE SECURITE - Tentative de connexion echouee sur l'AD
Sévérité	High
Expression	length(last(/SRV-AD-01/eventlog[Security,,,,4625]))>0
Allow manual close	Activé

- Valider l'expression et enregistrer le trigger.

L’option Allow manual close est utile pour permettre à l’administrateur de clôturer manuellement l’incident après analyse.



TESTS ET VALIDATION

5. Cahier de recette

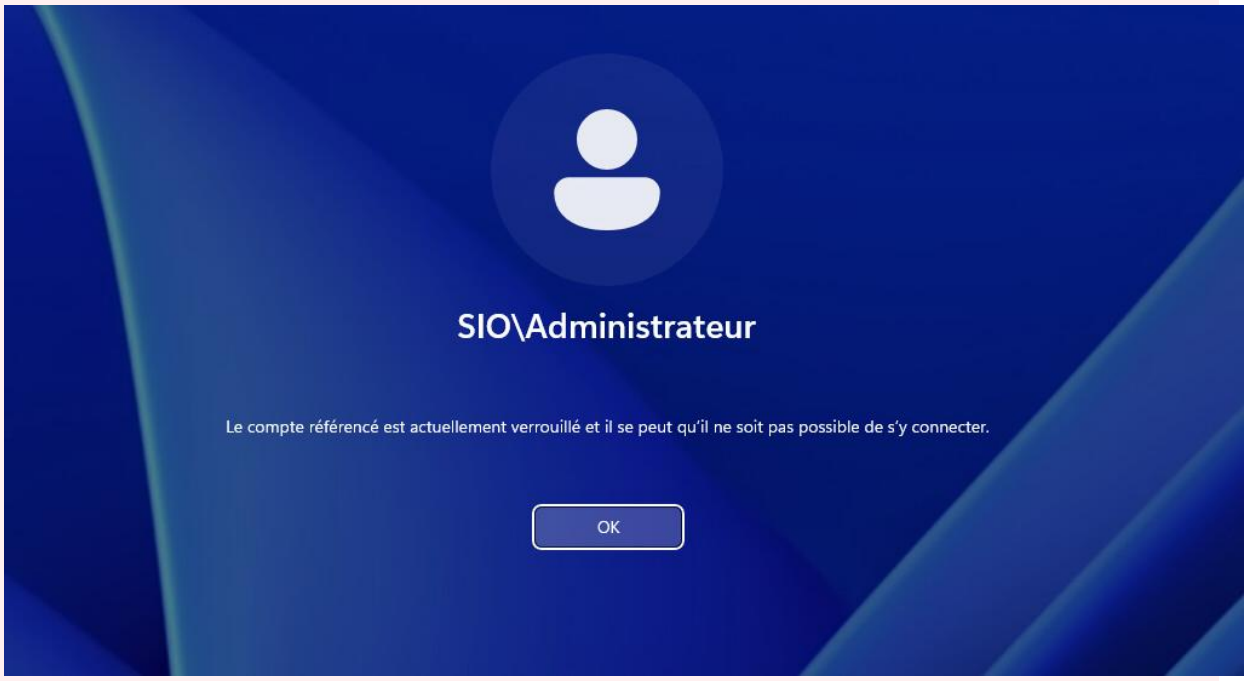
Le test consiste à provoquer volontairement des échecs de connexion pour vérifier que Zabbix détecte bien l’événement et déclenche l’alerte sans délai important.

- Verrouiller la session Windows sur SRV-AD-01.
- Saisir volontairement 3 mots de passe erronés sur l’écran de connexion.
- Constater l’apparition de l’événement 4625 dans le journal Security.
- Vérifier la remontée immédiate de l’alerte rouge sur le Dashboard Zabbix.
- Contrôler que le trigger passe en état Problem.

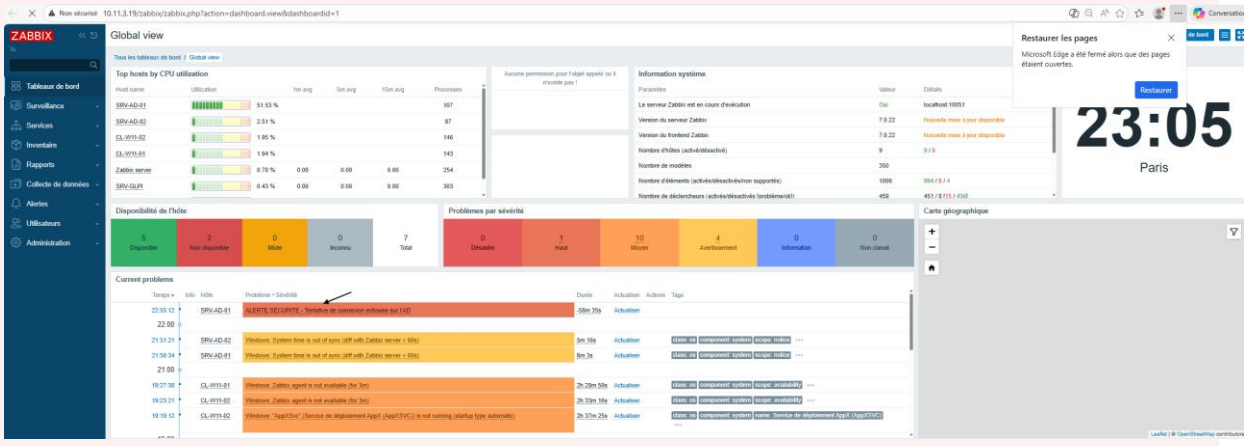
Test	Résultat attendu
3 échecs de connexion Windows	Événement Security 4625 détecté
Remontée Zabbix	Alerte rouge de sévérité High

Acquittement manuel	Possible via Allow manual close

Écran de verrouillage Windows avec 3 mots de passe erronés saisis



Dashboard Zabbix affichant l'alerte rouge liée à l'Event ID 4625



EXPLICATION TECHNIQUE

En mode actif, l'agent Zabbix n'attend pas que le serveur vienne l'interroger. Il collecte localement les événements et envoie les résultats vers 10.11.3.19. Cette méthode est particulièrement adaptée à la supervision de sécurité, car elle limite les problèmes liés aux filtres Windows, aux ports entrants et aux latences d'interrogation.

Le journal Security de Windows contient les événements de sécurité sensibles. L'Event ID 4625 correspond à un échec de connexion. En le surveillant, on peut repérer rapidement une erreur de mot de passe répétée, un compte verrouillé ou une tentative d'accès non autorisée.

Le trigger utilisé est volontairement simple : dès qu'un 4625 apparaît, l'alerte passe à l'état Problem. Dans un environnement de production plus avancé, il serait possible d'ajouter des seuils, un filtrage par compte ou une condition temporelle pour réduire les faux positifs.

POINTS DE CONTROLE FINAUX

- L'agent Zabbix est bien configuré en mode actif sur SRV-AD-01.
- L'item eventlog[Security,,,,4625] remonte les échecs de connexion.
- Le trigger High se déclenche dès la détection d'un événement 4625.
- Le dashboard Zabbix affiche une alerte rouge exploitable pour la supervision de sécurité.