cockpit
IT Service Manager

Supervision - Configuration du contrôle "Observateur d'événements Windows"

Document FAQ

Table des matières

Introduction

I. Objectif

- Présenter le fonctionnement et le paramétrage du contrôle « Windows - Observateur d'événements ».

II. Pré-requis

- Le contrôle fonctionne avec une connexion WinRM à l'équipement, pas avec une connexion WMI.

III. Alertes de configuration

- La connexion au système d'exploitation ne fonctionne pas ou n'est pas de type WinRM.

Principes

Les différents éléments du contrôle se comportent comme des filtres, de la même manière que les filtres de l'observateur d'événements Windows.

Exemple :

Check-specific parameters			
Check period:	○ Since the last check	◉ In the last 60 minutes	
Files (separator: ";"):	System;Application		
Sources (separator: ";"):	Service Control Manager		
Keywords:	AuditSuccess, EventLogClassic		
Level:	☑ Warning	☑ Error	☑ Critical
	☑ Information	☐ Verbose	
Event ID (separator: ";"):	10120;7036		
User:			
Category (separator: ";"):	◉ Include all categories		
	○ Include all categories whose message contains at least one of the search terms		
	○ Include all categories whose message does not contain any of the search terms		
Description (separator: ";"):	◉ Include all descriptions		
	○ Include all descriptions whose message contains at least one of the search terms		
	○ Include all descriptions whose message does not contain any of the search terms		
Alert threshold:	Alert if the number of messages matching the criteria on the period is greater than 0		

Dans l'exemple ci-dessus, le contrôle suit la logique suivante :

- La recherche s'effectue dans les fichiers « Application » et « System ».
- Parmi les messages collectés de ces 2 fichiers, seuls ceux ayant la source « Service Control Manager » sont conservés.
- Parmi les messages restants, sont gardés ceux possédant les mots-clés « AuditSuccess » ou « EventLogClassic ».
- Enfin seuls les messages correspondant aux IDs 10120 ou 7036 sont conservés.

> Important : Il est donc nécessaire de bien définir la recherche car il est techniquement possible de paramétrer un contrôle « incohérent » dans le sens où les éléments que l'on recherche ne peuvent être trouvés.

Paramétrage du contrôle

I. Paramètres génériques

- Disponibilité équipement : Non
- Statut inversé : Non
- Graphique : Non
- Double seuil : Non
- Disponibilité dans les rapports : Oui (Disponibilité / Supervision)

II. Paramètres spécifiques

A. Période de contrôle

Deux périodes de contrôle peuvent être sélectionnés.

1. Depuis le dernier contrôle

Principe :

- À Chaque exécution, le contrôle vérifie les événements depuis l'exécution précédente.
- Note : Si le contrôle s'exécute de 09h à 18h, à l'exécution de 09h, le contrôle collectera les événements survenus de 18h la veille à 09h.

Fonctionnement :

- Première exécution automatique : Lors de la toute première exécution du contrôle, le contenu du fichier n'est pas contrôlé, le contrôle mémorise sa position dans le fichier.

> Note : Avant cette première exécution automatique, la commande « Exécuter » n'apparaît pas dans le menu d'actions du contrôle.

- Exécutions automatiques suivantes : Les exécutions suivantes (même en cas de désactivation / activation du contrôle) le contrôle vérifie le contenu apparu depuis l'exécution précédente du contrôle. À la fin de la vérification, la position dans le fichier est mémorisée.
- Exécution manuelle : Lors de l'exécution manuelle, la vérification se fait sur le contenu apparu depuis le dernier contrôle automatique exécuté. Les exécutions manuelles n'impactent pas les collectes des exécutions automatiques du contrôle.

2. Au cours des 'XX' dernières minutes

- Le contrôle recherche les événements sur la période indiquée à partir de l'heure d'exécution du contrôle.
- Ajuster le planning d'exécution du contrôle en fonction de la période renseignée pour qu'il n'y ait pas de « trous » dans la supervision.

B. Fichiers et Sources

1. Principes

- Au moins un des deux champs « Fichiers » et « Sources » doit être renseignés :
  - Le champ « Fichiers » est renseigné, le champ « Source » peut-être vide.
  - Le champ « Sources » est renseigné, le champ « Fichiers » peut-être vide.
- Quand les champs « Fichiers » et « Sources » sont renseignés, les recherches sont croisées :
  - Je cherche les événements du fichier « Application » uniquement :

  - Je cherche les événements ayant la source « Windows Error Reporting » dans le fichier « Application » :

  - Je cherche les événements ayant la source « Windows Error Reporting » dans les fichiers « System » et « Application » :

  - Je cherche les événements ayant la source « Windows Error Reporting » dans tous les fichiers :

2. Fichiers

- Renseigner les fichiers où la recherche doit s'effectuer.
- Si le champ est vide, la recherche s'effectue sur tous les fichiers, de la même manière que si on avait sélectionné tous les fichiers.
- Le bouton « Sélectionner » permet d'afficher les fichiers de logs de l'équipement et le nombre d'entrées pour chaque fichier. Les fichiers de logs « System » (Application, System, etc.) sont affichés en début de liste.
- Il est possible de renseigner plusieurs fichiers, mais cela peut alourdir l'exécution du contrôle et solliciter l'équipement supervisé.

> Important 1 : Il est important de tester l'exécution du contrôle quand on effectue la re-cherche sur plusieurs fichiers afin de voir si le contrôle tombe en timeout.
> Important 2 : Prêter attention aux noms des fichiers, en cas d'erreur le contrôle ne trouve pas d'événements et peut donc remonter un succès alors que le contrôle cherche des éléments qu'il ne peut trouver.

3. Sources

- Renseigner les sources que le contrôle doit rechercher.
- Si le champ est vide, le contrôle recherche toutes les sources.
- Le bouton « Sélectionner » permet d'afficher les sources reconnues par l'équipement.

> Les sources que l'on relève dans l'observateur d'événement Windows n'apparaissent pas toujours au même format que dans le contrôle, exemple :
> - Dans l'observateur d'événements Windows : « MSDTC 2 »
> - Dans la liste de choix du contrôle « Microsoft-Windows-MSDTC 2 »
> Il est important de vérifier l'orthographe de la source lors du paramétrage du contrôle, si elle n'est pas correcte, le contrôle peut remonter un succès alors que le contrôle cherche des sources qui n'existent pas.

C. Mots-clés

- Aucun mot-clé n'est sélectionné par défaut, la recherche prend alors en compte les événements quelque soit leur mot-clé.
- Sélectionner un ou plusieurs mots-clés pour rechercher précisément les événements possédant ces mots-clés, dans ce cas les événements n'ayant pas ces mots sont exclus.
- La liste des mots-clés correspond aux mots-clés que l'on trouve dans le filtre de l'observateur des événements Windows.

D. Niveaux

- Au moins un niveau doit être sélectionné.

E. ID de l'événement

- Le champ est vide par défaut, la recherche prend alors en compte les événements quelque soit leur ID.
- Renseigner un ou plusieurs IDs pour rechercher précisément les événements possédant ces IDs, dans ce cas les événements ne possédant pas ces IDs sont exclus.

F. Utilisateur

- Aucun utilisateur n'est renseigné par défaut, la recherche prend alors en compte les événements quelque soit leur utilisateur.

- Renseigner un utilisateur (un seul utilisateur peut être renseigné) pour rechercher précisément les événements appartenant à cet utilisateur.
- L'utilisateur peut être local ou de domaine (domain\user).

> Vérifier l'existence et l'orthographe de l'utilisateur, en cas d'erreur le contrôle ne remontera pas d'événements et sera donc en succès.

G. Catégorie

- Permet de rechercher des termes sur le champ « Task Category » des événements.
- Il est possible d'inclure ou d'exclure les événements ayant les termes recherchés.

H. Description

- Permet de rechercher des termes dans la description des événements.
- Il est possible d'inclure ou d'exclure les événements ayant les termes recherchés.

> Les messages ne sont pas intégralement remontés, seuls les 50 premiers caractères de la première ligne du message sont collectés, essentiellement pour des soucis de performance. Si le filtre recherche des éléments du message au-delà des 50 premiers caractères, les termes et donc les messages ne seront pas trouvés.

I. Seuil d'alerte

- Alerte si le nombre de messages trouvés est inférieur ou supérieur au seuil.
- La valeur du seuil peut être comprise entre 0 et 999.

Fin du document