Event Log System by WMI - Modèle windows-by-WMI__ntlmv2

Sommaire

Contexte

Le modèle de check "**Event Log System by WMI**" vérifie la quantité d'événements présents dans le journal des événements Windows du système.

Statut	Nom de check	Résultat	Résultat Long
	Event Log System by WMI	OK - 0 event(s) of Severity Level: "Error,Warning", were recorded in the last 1 hours from the system Event Log.	-

Paramétrage

Le check utilise la ligne de commande suivante :

```
$PLUGINSDIR$/check_wmi_plus.pl -H "$HOSTADDRESS$" -u "$_HOSTDOMAINUSER$" -p "$_HOSTDOMAINPASSWORD$" -m
checkeventlog -a "$ARG1$"
 -o 2 -3 1 -w "$_HOSTWINDOWS_EVENT_LOG_WARN$" -c "$_HOSTWINDOWS_EVENT_LOG_CRIT$" -t
"$_HOSTWINDOWS_EVENT_LOG_TIMEOUT$"
 --inidir=$WMI_INI_DIR$ --security-mechanisms=$_HOSTWINDOWS_SECURITY_MECANISMS$ --nokeepstate --extrawmicarg
"--option=client ntlmv2 auth=Yes"
```

Données utilisées provenant du modèle

Données communes pour les checks du modèle

Nom	Modifiable sur	Défaut	Valeur par défaut à l'installation de Shinken	Description
DOMAINUSERSHORT	l'Hôte *(Onglet Données)*	$DOMAINUSERSHORT$	**shinken_user**	Nom d'utilisateur utilisé, sans le domaine
DOMAINPASSWORD	l'Hôte *(Onglet Données)*	$DOMAINPASSWORD$	**superpassword**	Mot de passe de l'utilisateur

`DOMAIN`	l'Hôte *(Onglet Données)*	$DOMAIN$	**MYDOMAIN**	Nom du domaine Active Directory du compte. Si vide, alors c'est le domaine du serveur qui sera utilisé, ou un compte local s'il n'est pas dans un domaine Active Directory.
`DOMAIN USER`	l'Hôte *(Onglet Données)*	$_HOSTDOMAIN$\\$_HOSTDOMAINUSERSHORT$	**MYDOMAIN\\shinken_user**	Nom complet utilisé pour se connecter, il faut par défaut DOMAINE\DOMAINUSERSHORT. • À n'utiliser que si vous ne souhaitez pas utiliser les variables DOMAINUSERSHORT et DOMAIN, et que votre connexion se fait sur un autre format que Domaine /utilisateur.
`WINDOWS_SECURITY_MECANISMS`	l'Hôte *(Onglet Données)*	integrity	**integrity**	Niveau de sécurité utilisé pour se connecter sur le serveur Windows : • **integrity** : (*par défaut*) valeur de sécurité élevée • **connect**: valeur de sécurité faible, qui sera **bloquée** sur les serveurs Windows à partir de **mi-2022** (*voir la page l'article de microsoft sur le sujet*), à partir des serveurs Windows 2008. ◦ Cette valeur ne doit être utilisée que sur de vieux serveurs qui ne gèrent pas les connexions au niveau *integrity*.

Données spécifiques pour ce check

Nom	Modifiable sur	Unité	Défaut	Valeur par défaut à l'installation de Shinken	Description
`WINDOWS_EVENT_LOG_WARN`	l'Hôte *(Onglet Données)*	-	1	**1**	Définis la quantité d'événements présents dans le journal des événements Windows à partir duquel le check passe en avertissement
`WINDOWS_EVENT_LOG_CRIT`	l'Hôte *(Onglet Données)*	-	60	**2**	Définis la quantité d'événements présents dans le journal des événements Windows à partir duquel le check passe en critique
`WINDOWS_EVENT_LOG_TIMEOUT`	l'Hôte *(Onglet Données)*	seconde	60	**60**	Cette donnée spécifie le nombre de secondes au-delà duquel la commande est interrompue. Certaines requêtes et un réseau avec une latence élevée peuvent nécessiter une augmentation de la valeur par défaut. Si le temps dépasse 60 secondes, il faut modifier la propriété "temps maximum d'exécution d'un check" pour qu'elle surpasse cette valeur (*voir la page* La surcharge des propriétés pour un check)

Les données DFE (Duplicate Foreach)

Pas de données DFE pour ce check.

Données utilisées provenant du check

Pas de données spécifiques pour ce check.

Données globales

Nom	Modifiable sur	Unité	Défaut	Valeur par défaut à l'installation de Shinken	Description
`PLUGINS DIR`	Non modifiable *(Sauf Admin Shinken)*	--	/var/lib/shinken/libexec	**/var/lib/shinken/libexec**	Chemin absolu du dossier contenant la sonde (*non modifiable*)

Nom	Modifiable sur	Unité	Défaut	Valeur par défaut à l'installation de Shinken	Description
HOSTADDRESS	l'Hôte *(Onglet Général)*	---	Nom de l'hôte	**Nom de l'hôte**	Adresse de l'hôte

Résultat

Exemple

Statut	Nom de check	Résultat	Résultat Long
	Event Log System by WMI	OK - 0 event(s) of Severity Level: "Error,Warning", were recorded in the last 1 hours from the system Event Log.	-

Interprétation

Statut

Il peut prendre quatre valeurs ***OK***/ ***CRITIQUE***/ ***ATTENTION*** / ***INCONNU***.

- Le statut va dépendre du retour de sonde et de la configuration spécifique du check pour les données suivantes :
  - *WINDOWS_EVENT_LOG_CRIT*,
  - *WINDOWS_EVENT_LOG_WARN*,
  - *WINDOWS_EVENT_LOG_TIMEOUT*
- Voici un tableau récapitulatif du statut attendu suivant le retour de sonde :

Situation	*Statut*
En fonction du nombre d'événements présents dans le journal : • Si c'est **supérieur** à WINDOWS_EVENT_LOG_CRIT (*par défaut : **2***)	***CRITIQUE***
En fonction du nombre d'événements présents dans le journal : • Si c'est **supérieur** à WINDOWS_EVENT_LOG_WARN (*par défaut : **1***)	***ATTENTION***
Si la sonde n'a pas eu de réponse avant le temps maximum • Si **supérieur** à WINDOWS_EVENT_LOG_TIMEOUT (*par défaut : **60s***)	***INCONNU***

Résultat

Renvoi au format texte :

- le nombre d'éléments avec une sévérité "Error" ou "Warning"

Résultat Long

Pas de résultat long pour ce check.

Métriques

Nom	Unité	Description
Event_Count	-	Nombre d'évènements contenus dans le journal des événements Windows du système