


EventLogApplication - Modèle windows

Sommaire

- Contexte
- Paramétrage
 - Données utilisées provenant du modèle
 - Données communes pour les checks du modèle
 - Données spécifiques pour ce check
 - Les données DFE (Duplicate Foreach)
 - Données utilisées provenant du check
 - Données globales
- Résultat
 - Exemple
 - Interprétation des données
- Métriques

Contexte

Le check "EventLogApplication" vérifie la quantité d'événements présents dans le journal des événements Windows des applications.

Statut	Nom de check	Résultat	Résultat Long
	EventLogApplication	OK - 0 event(s) of Severity Level: "Error,Warning", were recorded in the last 1 hours from the application 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=$_HOSTWINDOWS_SECURITY_MECHANISMS$ --nokeepstate
```

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
DOMAIN USERSH ORT	l'Hôte (Onglet Données)	\$DOMAINUS ERSHORT\$	shinken_user	Nom d'utilisateur utilisé, sans le domaine
DOMAIN PASSWO RD	l'Hôte (Onglet Données)	\$DOMAINPAS SWORD\$	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)	\$_HOSTDOM AIN\$\\ \$_HOSTDOM AINUSERSH ORT\$	MYDOMAIN\shinken _user	Nom complet utilisé pour se connecter, il faut par défaut DOMAINE\DOMAINUSERSHORT. <ul style="list-style-type: none"> 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.
WINDOW S_SECU RITY _MECAN ISMS	l'Hôte (Onglet Données)	integrity	integrity	Niveau de sécurité utilisé pour se connecter sur le serveur Windows : <ul style="list-style-type: none"> 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. <ul style="list-style-type: none"> Cette valeur ne doit être utilisée que sur de vieux serveurs qui ne gèrent pas les connexions au niveau <i>integrity</i>.

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	Nombre minimum d'événements présents dans le journal des événements Windows en erreur à partir duquel le check passe en avertissement.
_WINDOWS_EVENT_LOG_CRITICAL	l'Hôte (Onglet Données)	-	2	2	Nombre minimum d'événements présents dans le journal des événements Windows en erreur à partir duquel le check passe en critique.
_WINDOWS_EVENT_LOG_TIMEOUT	l'Hôte (Onglet Données)	secondes	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. <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  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) </div>

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)


- Propriétés de l'hôte

Nom	Modifiable sur	Unité	Défaut	Valeur par défaut à l'installation de Shinken	Description
-----	----------------	-------	--------	---	-------------

HOSTADDRESS	l'Hôte (Onglet Général)		Nom de l'hôte		Adresse de l'hôte
-------------	------------------------------	--	---------------	--	-------------------

Résultat

Exemple

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

Interprétation des données

- Statut : Le statut peut prendre quatre valeurs (*OK* / *WARNING* / *CRITICAL* / *UNKNOWN*).
- Résultat : Renvoi les métriques au format texte.
- Résultat Long : *pas de résultat long pour ce check.*

Métriques

Nom	Unités	Description
Event_Count	-	Nombre d'évènements contenus dans le journal des événements Windows des applications.