

Les modules du Synchronizer

Contexte

Le modèle de check EventLogSystem, dédié au modèle Windows (propriété "Attaché sur les modèles d'hôte" mise à "windows"), il vérifie la quantités d'événements présents dans le journal des événements Windows du système, il utilise la commande **check_windows_eventlogs** avec un Argument "system"

Exemple

Exemple de commande

```
$PLUGINS_DIR$/check_wmi_plus.pl -H "$HOSTADDRESS$" -u "$_HOSTDOMAINUSER$" -p "$_HOSTDOMAINPASSWORD$" -m checkeventlog -a "$ARG1$" -o 2 -3 1 -w "$_HOSTWINDOWS_EVENT_LOG_WARN$" -c "$_HOSTWINDOWS_EVENT_LOG_CRIT$" --inidir=$WMI_INI_DIR$ --security-mechanisms=$_HOSTWINDOWS_SECURITY_MECHANISMS$
```

Note : **\$ARG1\$** sera donc remplacé par **system** lors de l'exécution de la commande

Exemple de résultat

? Unknown Attachment

Données et métriques

Données

Donnée	Description	Valeur par défaut
_WINDOWS_EVENT_LOG_WARN	Définit le pourcentage d'utilisation du processeur à partir duquel le check passe en critique	90
_WINDOWS_EVENT_LOG_CRIT	Définit le pourcentage d'utilisation du processeur à partir duquel le check passe en avertissement	80
_WINDOWS_EVENT_LOG_TIMEOUT	Définit le temps d'attente de la commande avant de timeout en seconde	60



Si le temps de `_WINDOWS_EVENT_LOG_TIMEOUT` dépasse les 60 secondes, le check devra être surchargé pour passer le "temps maximum d'exécution d'un check" à la valeur défini dans le `_WINDOWS_EVENT_LOG_TIMEOUT`

Métriques

Nom de la métrique	Description
Event_Count	Nombres d'évènements contenue dans les events logs application