

# Migration MMapV1 vers Wired Tiger

## Contexte

Le modèle de check "EventLogSystem" vérifie la quantité d'événements présents dans le journal des événements Windows du système.

## Exemple


### Exemple de résultat

? Unknown Attachment

## Données et métriques

### Données

Donnée	Description	Valeur par défaut
_WINDOWS_EVENT_LOG_WARN	Définis la quantité d'événements présents dans le journal des événements Windows des applications à partir duquel le check passe en avertissement	1
_WINDOWS_EVENT_LOG_CRIT	Définis la quantité d'événements présents dans le journal des événements Windows des applications à partir duquel le check passe en critique	2
_WINDOWS_EVENT_LOG_TIMEOUT	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, qui est de 60 secondes.	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`. Voir Temps maximum d'exécution d'un check ( voir [Editer un check](#) ).

### Métriques

Nom de la métrique	Description
Event_Count	Nombres d'évènements contenus dans les events logs du système

## Fonctionnement

Le check utilise la commande `check_windows_eventlogs`, ainsi que le script `check_wmi_plus`.

```
$PLUGINS_DIR/check_wmi_plus.pl -H "$HOSTADDRESS$" -u "$HOSTDOMAINUSER$" -p "$HOSTDOMAINPASSWORD$" -m checkeventlog -a "$ARG1$" -o 2 -3 1 -w "$HOSTWINDOWS_EVENT_LOG_WARN$" -c "$HOSTWINDOWS_EVENT_LOG_CRIT$" -t "$HOSTWINDOWS_EVENT_LOG_TIMEOUT$" --inidir=$WMI_INI_DIR$ --security-mechanisms=$HOSTWINDOWS_SECURITY_MECHANISMS$
```

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