

# Event Log System by WMI - Modèle windows-by-WMI\_\_ntlmv2

## 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
    - Statut
    - Résultat
    - Résultat Long
- Métriques

## 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=$_HOSTWINDOWS_SECURITY_MECHANISMS$ --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                                |
|-------------------------|-------------------------------------|-------------------------|-----------------------------------------------|--------------------------------------------|
| DOMAIN<br>USERSH<br>ORT | l'Hôte<br><br>( Onglet<br>Données ) | \$DOMAINUS<br>ERSHORT\$ | shinken_user                                  | Nom d'utilisateur utilisé, sans le domaine |
| DOMAIN<br>PASSWO<br>RD  | l'Hôte<br><br>( Onglet<br>Données ) | \$DOMAINPAS<br>SWORD\$  | superpassword                                 | Mot de passe de l'utilisateur              |

|                             |                              |                                            |                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------------------|------------------------------|--------------------------------------------|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DOMAIN                      | l'Hôte<br>( 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<br>( Onglet Données ) | \$_HOSTDOMAIN\$\\\$_HOSTDOMAIN\USERSHORT\$ | MYDOMAIN\shinken_user | Nom complet utilisé pour se connecter, il faut par défaut DOMAIN\DOMAINUSERSHORT.<br><ul style="list-style-type: none"><li>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.</li></ul>                                                                                                                                                                                                                                                                                                 |
| WINDOWS_SECURITY_MECHANISMS | l'Hôte<br>( Onglet Données ) | integrity                                  | integrity             | Niveau de sécurité utilisé pour se connecter sur le serveur Windows :<br><ul style="list-style-type: none"><li><b>integrity</b> : ( <i>par défaut</i> ) valeur de sécurité élevée</li><li><b>connect</b>: valeur de sécurité faible, qui sera <b>bloquée</b> sur les serveurs Windows à partir de <b>mi-2022</b> ( voir la page <a href="#">l'article de microsoft sur le sujet</a> ), à partir des serveurs Windows 2008.<ul style="list-style-type: none"><li>Cette valeur ne doit être utilisée que sur de vieux serveurs qui ne gèrent pas les connexions au niveau <i>integrity</i>.</li></ul></li></ul> |

## 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<br>( 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<br>( 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<br>( 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.<br><div> Si le temps dépasse 60 secondes, il faut modifier la propriété "temps maximum d'exécution d'un check" pour qu'elle dépasse cette valeur ( voir la page <a href="#">La surcharge des propriétés pour un check</a> )</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<br>( Sauf Admin Shinken ) | --    | /var/lib/shinken/libexec | /var/lib/shinken/libexec                      | Chemin absolu du dossier contenant la sonde ( <i>non modifiable</i> ) |

| Nom         | Modifiable sur               | Unité | Défaut        | Valeur par défaut à l'installation de Shinken | Description       |
|-------------|------------------------------|-------|---------------|-----------------------------------------------|-------------------|
| HOSTADDRESS | l'Hôte<br>( 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 : <ul style="list-style-type: none"> <li>Si c'est <b>supérieur</b> à WINDOWS_EVENT_LOG_CRIT ( <i>par défaut : 2</i> )</li> </ul> | <b>CRITIQUE</b>  |
| En fonction du nombre d'événements présents dans le journal : <ul style="list-style-type: none"> <li>Si c'est <b>supérieur</b> à WINDOWS_EVENT_LOG_WARN ( <i>par défaut : 1</i> )</li> </ul> | <b>ATTENTION</b> |
| Si la sonde n'a pas eu de réponse avant le temps maximum <ul style="list-style-type: none"> <li>Si <b>supérieur</b> à WINDOWS_EVENT_LOG_TIMEOUT ( <i>par défaut : 60s</i> )</li> </ul>       | <b>INCONNU</b>   |

### 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 |