


EventLogSystem - 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
 - Statut
 - Résultat
 - Résultat Long
- Métriques

Contexte

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

| Statut | Nom de check | Résultat | Résultat Long |
|--|----------------|--|--|
|  | EventLogSystem | OK - 1 event(s) of Severity Level: "Error,Warning", were recorded in the last 1 hours from the system Event Log. (List is on next line. Fields shown are - Logfile:TimeGenerated:EventId:EventCode :SeverityLevel:Type:SourceName:Message) | System:20230602121114.017422-000:5781:5781:Warning:NETLOGON:Dynamic registration or deletion of one or more DNS records associated with DNS domain 'SHINKEN.local' failed. These records are used by other computers to locate this server as a domain controller (if the specified domain is an Active Directory domain) or as an LDAP server (if the specified domain is an application partition). Possible causes of failure include: - TCP/IP properties of the network connections of this computer contain wrong IP address(es) of the preferred and alternate DNS servers - Specified preferred and alternate DNS servers are not running - DNS server(s) primary for the records to be registered is not running - Preferred or alternate DNS servers are configured with wrong root hints - Parent DNS zone contains incorrect delegation to the child zone authoritative for the DNS records that failed registration USER ACTION Fix possible misconfiguration(s) specified above and initiate registration or deletion of DNS records by running 'nltest.exe /dsregdns' from the command prompt on the domain controller or by restarting Net Logon service on the domain controller. |

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 USERSHORT ORT | l'Hôte <i>(Onglet Données)</i> | \$DOMAINUSERSHORT\$ | shinken_user | Nom d'utilisateur utilisé, sans le domaine |

| | | | | |
|------------------------------------|---------------------------------|---|-----------------------------------|--|
| DOMAIN PASSWORD | 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) | \$_HOSTDOMAINS\$\ \$_HOSTDOMAINUSERSH ORT\$ | MYDOMAIN\shinken _user | Nom complet utilisé pour se connecter, il faut par défaut DOMAIN\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_SECURITY _MECANISMS | l'Hôte (Onglet Données) | integrity | integrity | Niveau de sécurité utilisé pour se connecter sur le serveur Windows : <ul style="list-style-type: none"> integrity : (<i>par défaut</i>) 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 | 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. <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 (<i>non modifiable</i>) |

| 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 |
|---|----------------|---|---|
|  | EventLogSystem | OK - 1 event(s) of Severity Level: "Error;Warning", were recorded in the last 1 hours from the system Event Log. (List is on next line. Fields shown are - Logfile:TimeGenerated:EventId:EventCode :SeverityLevel:Type:SourceName:Message) | System:20230602121114.017422-000:5781:5781:Warning:NETLOGON:Dynamic registration or deletion of one or more DNS records associated with DNS domain 'SHINKEN.local' failed. These records are used by other computers to locate this server as a domain controller (if the specified domain is an Active Directory domain) or as an LDAP server (if the specified domain is an application partition). Possible causes of failure include: - TCP/IP properties of the network connections of this computer contain wrong IP address(es) of the preferred and alternate DNS servers - Specified preferred and alternate DNS servers are not running - DNS server(s) primary for the records to be registered is not running - Preferred or alternate DNS servers are configured with wrong root hints - Parent DNS zone contains incorrect delegation to the child zone authoritative for the DNS records that failed registration USER ACTION Fix possible misconfiguration(s) specified above and initiate registration or deletion of DNS records by running 'nltest.exe /dsregdns' from the command prompt on the domain controller or restarting Net Logon service on the domain controller. |

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"> Si c'est supérieur à WINDOWS_EVENT_LOG_CRIT (<i>par défaut : 2</i>) | CRITIQUE |
| En fonction du nombre d'événements présents dans le journal : <ul style="list-style-type: none"> Si c'est supérieur à WINDOWS_EVENT_LOG_WARN (<i>par défaut : 1</i>) | ATTENTION |
| Si la sonde n'a pas eu de réponse avant le temps maximum <ul style="list-style-type: none"> Si supérieur à WINDOWS_EVENT_LOG_TIMEOUT (<i>par défaut : 60s</i>) | 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 |