


# Services 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 **"Services by WMI"** vérifie le nombre de services Windows en erreur d'un système d'exploitation Windows.

| Statut  | Nom de check    | Résultat   | Résultat Long |
|---|-----------------|--|---------------|
|  | Services by WMI | OK - Found 63 Services(s), 63 OK and 0 with problems (4 excluded). | -             |

## Paramétrage

Le check utilise la ligne de commande suivante :

```
$PLUGINSDIR$/check_wmi_plus.pl -H "$HOSTADDRESS$" -u "$_HOSTDOMAINUSER$" -p "$_HOSTDOMAINPASSWORD$" -m  
checkservice -a Auto  
-o "$_HOSTWINDOWS_EXCLUDED_AUTO_SERVICES$" -w "$_HOSTWINDOWS_AUTO_SERVICES_WARN$" -c  
"$_HOSTWINDOWS_AUTO_SERVICES_CRIT$" --inidir=$WMI_INI_DIR$ --security-mechanisms=$_HOSTWINDOWS_SECURITY_MECHANISMS$ --nokeepstate  
-t "$_HOSTWINDOWS_AUTO_SERVICES_TIMEOUT$" --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><i>( Onglet<br/>Données )</i> | \$DOMAINUS<br>ERSHORT\$ | <b>shinken_user</b>                           | Nom d'utilisateur utilisé, sans le domaine |
| DOMAIN<br>PASSWO<br>RD  | l'Hôte<br><i>( Onglet<br/>Données )</i> | \$DOMAINPAS<br>SWORD\$  | <b>superpassword</b>                          | 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\USER\$ | MYDOMAIN\shinken_user | Nom complet utilisé pour se connecter, il faut par défaut DOMAIN\DOMAINUSERSHORT.<br><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>   |
| WINDO<br>S_SECU<br>RITY<br>_MECAN<br>ISMS | l'Hôte<br>( Onglet Données ) | integrity                            | integrity             | Niveau de sécurité utilisé pour se connecter sur le serveur Windows :<br><br><ul style="list-style-type: none"> <li><b>integrity</b> : ( par défaut ) 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  |
|--|------------------------------|---------|--|---|--|
| WINDO<br>WS_EX<br>CLUDE<br>D_AUT<br>O_SER<br>VICES | l'Hôte<br>( Onglet Données ) | -       | Service Google Update \ (gupdate) Remote Registry Software Protection Windows Biometric Service Microsoft Edge Update Service (edgeupdate)15 | <b>Service Google Update \ (gupdate) Remote Registry Software Protection Windows Biometric Service Microsoft Edge Update Service (edgeupdate)</b> | Permet d'exclure des services du test.   |
| WINDO<br>WS_AU<br>TO_SE<br>RVICE<br>S_WARN         | l'Hôte<br>( Onglet Données ) | seconde | 0  | <b>0</b>  | Nombre minimum de services en erreur à partir duquel le check passe en avertissement.  |
| WINDO<br>WS_AU<br>TO_SE<br>RVICE<br>S_CRIT         | l'Hôte<br>( Onglet Données ) | seconde | 1  | <b>1</b>  | Nombre minimum de services en erreur à partir duquel le check passe en critique.   |
| WINDO<br>WS_EX<br>CLUDE<br>D_AUT<br>O_TIM<br>EOUT  | l'Hôte<br>( Onglet Données ) | seconde | 15   | <b>15</b>   | 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><br><div style="border: 1px solid gray; 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 <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<br>DIR | Non modifiable<br>( Sauf Admin<br>Shinken ) | --    | /var/lib/shinken<br>/libexec | <b>/var/lib/shinken/libexec</b>               | 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 | <b>Nom de l'hôte</b>                          | Adresse de l'hôte |

## Résultat

### Exemple

| Statut  | Nom de check    | Résultat   | Résultat Long |
|---|-----------------|--|---------------|
|  | Services by WMI | OK - Found 63 Services(s), 63 OK and 0 with problems (4 excluded). | -             |

## 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\_AUTO\_SERVICES\_CRIT,
  - WINDOWS\_AUTO\_SERVICES\_WARN,
  - WINDOWS\_EXCLUDED\_AUTO\_TIMEOUT
- Voici un tableau récapitulatif du statut attendu suivant le retour de sonde :

| Situation  | Statut           |
|--|------------------|
| En fonction du nombre de services qui ne fonctionnent pas : <ul style="list-style-type: none"><li>Si c'est <b>supérieur</b> à <b>WINDOWS_AUTO_SERVICES_CRIT</b> ( <i>par défaut: 90%</i> )</li></ul> | <b>CRITIQUE</b>  |
| En fonction du nombre de services qui ne fonctionnent pas : <ul style="list-style-type: none"><li>Si c'est <b>supérieur</b> à <b>WINDOWS_AUTO_SERVICES_WARN</b> ( <i>par défaut: 80%</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 <b>WINDOWS_EXCLUDED_AUTO_TIMEOUT</b> ( <i>par défaut: 15 s</i> )</li></ul>      | <b>INCONNU</b>   |

## Résultat

Renvoi au format texte :

- le nombre de services trouvé
- le nombre OK
- le nombre avec des problèmes
- le nombre exclu ( *optionnel* )

## Résultat Long

*pas de résultat long pour ce check.*

## Métriques

| Nom                         | Unités | Description                      |
|-----------------------------|--------|----------------------------------|
| Excluded_Service_Count      | -      | Quantité de services exclus.     |
| Service_Count_OK_State      | -      | Quantité de services en état OK. |
| Service_Count_Problem_State | -      | Quantité de services en erreur.  |
| Total_Service_Count         | -      | Quantité de services totaux.     |