

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 "$_HOSTWINDOWS_AUTO_SERVICES_CRIT$" --indir=$WMI_INI_DIR$ --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 USERSH ORT	l'Hôte (Onglet Données)	\$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)	\$_HOSTDOMAIN\$\\\$_HOSTDOMAIN\USER\$	MYDOMAIN\shinken_user	Nom complet utilisé pour se connecter, il faut par défaut DOMAIN\DOMAINUSERSHORT. 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.
WINDOWS_SECURITY_MECHANISMS	l'Hôte (Onglet Données)	integrity	integrity	Niveau de sécurité utilisé pour se connecter sur le serveur Windows : 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. - 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_EXCLUDE_AUTO_SERVICES	l'Hôte (Onglet Données)	-	Service Google Update \ (gupdate\) Remote Registry Software Protection Windows Biometric Service Microsoft Edge Update Service (edgeupdate)15	Service Google Update \ (gupdate\) Remote Registry Software Protection Windows Biometric Service Microsoft Edge Update Service (edgeupdate)	Permet d'exclure des services du test.
WINDOWS_AUTOSERVICE_WARN	l'Hôte (Onglet Données)	seconde	0	0	Nombre minimum de services en erreur à partir duquel le check passe en avertissement.
WINDOWS_AUTOSERVICE_CRIT	l'Hôte (Onglet Données)	seconde	1	1	Nombre minimum de services en erreur à partir duquel le check passe en critique.
WINDOWS_EXCLUDE_AUTO_TIMEOUT	l'Hôte (Onglet Données)	seconde	15	15	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.  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)

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
	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 : Si c'est supérieur à WINDOWS_AUTO_SERVICES_CRIT (<i>par défaut: 90%</i>)	CRITIQUE
En fonction du nombre de services qui ne fonctionnent pas : Si c'est supérieur à WINDOWS_AUTO_SERVICES_WARN (<i>par défaut: 80%</i>)	ATTENTION
Si la sonde n'a pas eu de réponse avant le temps maximum Si supérieur à WINDOWS_EXCLUDED_AUTO_TIMEOUT (<i>par défaut: 15 s</i>)	INCONNU

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.