Modèle windows-by-WMI__ntlmv2

Sommaire

Contexte

Le modèle **windows-by-WMI__ntlmv2** permet de superviser des hôtes sur lesquels est installé le système d'exploitation Windows en forçant l'usage de la méthode d'authentification ntlmv2.

- Il donne, entre autres, des informations sur les statistiques d'interface réseau, l'utilisation du matériel (*CPU, mémoire, disques...*), ainsi que les services et le temps depuis le dernier redémarrage.

Si le besoin de modifier certains éléments (*commandes, checks ou modèles d'hôtes*) se présente, il faut lire la page Les bonnes pratiques d'utilisation d'un pack livré par Shinken).

Sommaire des checks

Nom	Description
`Services by WMI`	Vérifie le nombre de services Windows en erreur d'un système d'exploitation Windows. (*voir la page* Services by WMI - Modèle windows-by-WMI__ntlmv2)
`Event Log System by WMI`	Vérifie la quantité d'événements présents dans le journal des événements Windows du système. (*voir la page* Event Log System by WMI - Modèle windows-by-WMI__ntlmv2)
`Memory by WMI`	Vérifie l'utilisation de la mémoire RAM de la machine. (*voir la page* Memory by WMI - Modèle windows-by-WMI__ntlmv2)
`Network Interface by WMI`	Renvoie le statut et utilisation des différentes interfaces réseaux du système d'exploitation. (*voir la page* Network Interface by WMI - Modèle windows-by-WMI__ntlmv2)
`Network Interface by WMI`	Effectue une mesure sur le temps passé depuis le démarrage d'une machine Windows. (*voir la page* Reboot by WMI - Modèle windows-by-WMI__ntlmv2)
`Swap by WMI`	Analyse les statistiques d'utilisation des fichiers de pages mémoire d'un système d'exploitation Windows. (*voir la page* Swap by WMI - Modèle windows-by-WMI__ntlmv2)

`CPU by WMI`	renvoie les statistiques d'utilisation des processeurs du système d'exploitation Windows. (*voir la page* Cpu by WMI - Modèle windows-by-WMI__ntlmv2)
`Disks by WMI`	Analyse les statistiques d'utilisation des disques d'un système d'exploitation Windows. (*voir la page* Disks by WMI - Modèle windows-by-WMI__ntlmv2)
`Event Log Application by WMI`	Vérifie la quantité d'événements présents dans le journal des événements Windows des applications. (*voir la page* Event Log Application by WMI - Modèle windows-by-WMI__ntlmv2)

Les données

Les données communes pour tous les checks

Nom	Modifiable sur	Défaut	Valeur par défaut à l'installation de Shinken	Description
`DOMAINUSERSHORT`	l'Hôte *(Onglet Données)*	$DOMAINUSERSHORT$	**shinken_user**	Nom d'utilisateur utilisé, sans le domaine
`DOMAINPASSWORD`	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.
`DOMAINUSER`	l'Hôte *(Onglet Données)*	$_HOSTDOMAIN$\\$_HOSTDOMAINUSERSHORT$	**MYDOMAIN\\shinken_user**	Nom complet utilisé pour se connecter, il faut par défaut DOMAINE\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_MECANISMS`	l'Hôte *(Onglet Données)*	integrity	**integrity**	Niveau de sécurité utilisé pour se connecter sur le serveur Windows : • **integrity** : (*par défaut*) 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 *integrity*.

Les données spécifiques

Pour le check "Services by WMI - Modèle windows-by-WMI__ntlmv2"

Nom	Modifiable sur	Unité	Défaut	Valeur par défaut à l'installation de Shinken	Description

`WINDOWS_EXCLUDED_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)**	Permets d'exclure des services du test.
`WINDOWS_AUTO_SERVICES_WARN`	l'Hôte *(Onglet Données)*	-	0	**0**	Nombre minimum de services en erreur à partir duquel le check passe en avertissement.
`WINDOWS_AUTO_SERVICES_CRIT`	l'Hôte *(Onglet Données)*	-	1	**1**	Nombre minimum de services en erreur à partir duquel le check passe en critique.
`WINDOWS_EXCLUDED_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)

Pour le check "Event Log System by WMI - Modèle windows-by-WMI__ntlmv2"

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. 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)

Pour le check "Memory by WMI - Modèle windows-by-WMI__ntlmv2"

Nom	Modifiable sur	Unité	Défaut	Valeur par défaut à l'installation de Shinken	Description
WINDOWS_ALL_MEM_WARN	l'Hôte *(Onglet Données)*	%	80	**80**	Il définit le pourcentage d'utilisation de la mémoire à partir duquel le check passe en avertissement.
WINDOWS_ALL_MEM_CRIT	l'Hôte *(Onglet Données)*	%	90	**90**	Il définit le pourcentage d'utilisation de la mémoire à partir duquel le check passe en critique.
WINDOWS_ALL_MEM_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)

Pour le check "Network Interface by WMI - Modèle windows-by-WMI__ntlmv2"

Nom	Modifiable sur	Unité	Défaut	Valeur par défaut à l'installation de Shinken	Description
WINDOWS_NETWORK_INTERFACE	l'Hôte *(Onglet Données)*	-	*	*	Nom de l'interface réseau à superviser.
WINDOWS_NETWORK_INTERFACE_DELAY	l'Hôte *(Onglet Données)*	seconde	2	**2**	Les métriques se terminant par "PerSec" représentent des moyennes calculées sur une période définie. La donnée _WINDOWS_NETWORK_INTERFACE_DELAY détermine la période sur laquelle cette moyenne est calculée. Pour cette raison, plus le délai est long et plus la valeur de la métrique est significative.

`WINDOWS_NETWORK_INTERFACE_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)

Pour le check "Reboot by WMI - Modèle windows-by-WMI__ntlmv2"

Nom	Modifiable sur	Unité	Défaut	Valeur par défaut à l'installation de Shinken	Description
`WINDOWS_REBOOT_WARN`	l'Hôte *(Onglet Données)*	minute	15	**15**	Temps en dessous duquel le check passe en avertissement.
`WINDOWS_REBOOT_CRIT`	l'Hôte *(Onglet Données)*	minute	5	**5**	Temps en dessous duquel le check passe en critique.
`WINDOWS_REBOOT_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)

Pour le check "Swap by WMI - Modèle windows-by-WMI__ntlmv2"

Nom	Modifiable sur	Unité	Défaut	Valeur par défaut à l'installation de Shinken	Description
`WINDOWS_SWAP_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)

Pour le check "Cpu by WMI - Modèle windows-by-WMI__ntlmv2"Services by WMI - Modèle windows-by-WMI__ntlmv2

Nom	Modifiable sur	Unité	Défaut	Valeur par défaut à l'installation de Shinken	Description

_WINDOWS_ALL_CPU_WARN	l'Hôte *(Onglet Données)*	%	80	**80**	Il définit le pourcentage d'utilisation des processeurs à partir duquel le check passe en avertissement.
_WINDOWS_ALL_CPU_CRIT	l'Hôte *(Onglet Données)*	%	90	**90**	Il définit le pourcentage d'utilisation des processeurs à partir duquel le check passe en critique.
_WINDOWS_ALL_CPU_DELAY	l'Hôte *(Onglet Données)*	seconde	2	**2**	Les métriques se terminant par "PerSec" représentent des moyennes calculées sur une période définie. La donnée _WINDOWS_ALL_CPU_DELAY détermine la période sur laquelle cette moyenne est calculée. Pour cette raison, plus le délai est long et plus la valeur de la métrique est significative.
_WINDOWS_ALL_CPU_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)

Pour le check "Disks by WMI - Modèle windows-by-WMI__ntlmv2"

Nom	Modifiable sur	Unité	Défaut	Valeur par défaut à l'installation de Shinken	Description
WINDOWS_DISK_WARN	l'Hôte *(Onglet Données)*	-	80	**80**	Il définit le pourcentage d'utilisation de l'espace disque à partir duquel le check passe en avertissement.
WINDOWS_DISK_CRIT	l'Hôte *(Onglet Données)*	-	90	**90**	Il définit le pourcentage d'utilisation de l'espace disque à partir duquel le check passe en critique.
WINDOWS_DISK_TIMEOUT	l'Hôte *(Onglet Données)*	secondes	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)

Pour le check "Event Log Application by WMI - Modèle windows-by-WMI__ntlmv2"

Nom	Modifiable sur	Unité	Défaut	Valeur par défaut à l'installation de Shinken	Description
`WINDOWS_EVENT_LOG_WARN`	l'Hôte *(Onglet Données)*	-	1	**1**	Nombre minimum d'événements présents dans le journal des événements Windows des applications en erreur à partir duquel le check passe en avertissement.
`WINDOWS_EVENT_LOG_CRIT`	l'Hôte *(Onglet Données)*	-	2	**2**	Nombre minimum d'événements présents dans le journal des événements Windows des applications en erreur à partir duquel le check passe en critique.
`WINDOWS_EVENT_LOG_TIMEOUT`	l'Hôte *(Onglet Données)*	secondes	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. 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)

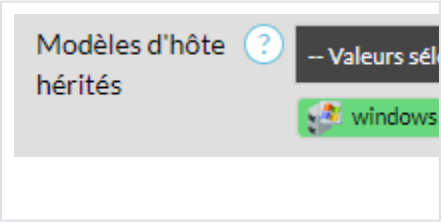
Pas de données DFE pour ce modèle

Comment appliquer un modèle d'hôte à un hôte

Application du modèle via l'interface de Configuration

Dans l'interface de Configuration :

- créer ou éditer un hôte (*voir la page Editer un Hôte*),
- ajouter le modèle **"windows"** dans la propriété "**Modèles d'hôte hérités**" à l'aide du menu déroulant.



Application du modèle via un collecteur d'import de fichiers au format .cfg

Dans votre fichier de définition de vos éléments à importer via votre collecteur :

- créer ou éditer la définition de votre hôte,
- ajouter la valeur **"windows"** (*selon vos besoins*), dans la propriété "**use**",
- importer le contenu du fichier via un collecteur de type "cfg-file-import" (*voir la page Collecteur de type (cfg-file-import) - Import depuis des fichiers au format .cfg*).

```
define host {
    host_name   mon_hôte_windows
    use         windows
}
```