

Stats Kernel by WinRM

Sommaire

Contexte

Paramétrage

- Données utilisées provenant des modèles
 - Données communes pour les checks des modèles
 - Les données communes pour certain checks
 - Données spécifiques pour ce check
 - Données DFE (Duplicate Foreach)

Données utilisées provenant du check

- Données globales
- Propriétés de l'hôte

Résultat

Exemple

Interprétation des données

- Statut
- Résultat
- Résultat Long

Métriques

Définition



Exemple

Erreurs et pré-requis

- Erreurs de configuration du poller shinken (spécifique à certains checks)
 - POLLER - BAD STATE – Permission denied
- Erreurs de connexion (communes à tous les checks)
 - UNKNOWN – Transport error : failed to send request: request timed out
 - UNKNOWN – Transport error : sent request failed: connection refused
 - UNKNOWN – Transport error : sent request failed: host is not reachable
 - UNKNOWN – Transport error : sent request failed: DNS resolution failed
 - UNKNOWN – Transport error : failed to build request: given uri is invalid
 - UNKNOWN – Authentication NTLM failed : NTLM is not supported by the server
 - UNKNOWN – Authentication NTLM failed : Unauthorized
 - UNKNOWN – Authentication Basic failed : Basic is not supported by the server
 - UNKNOWN – Authentication Basic failed : Unauthorized
- Erreurs de configuration de l'hôte à supervisor (communes à tous les checks)
 - UNKNOWN – Response fault error: Code: s:Sender, Subcode: w:AccessDenied, Reason: Access is denied.
 - MONITORED HOST - BAD STATE – Command execution Failed. Permission denied.
 - UNKNOWN – Command execution Failed. [...] Provider failure

Contexte

Le check **Stats Kernel by WinRM** va récupérer les statistiques de votre kernel afin d'en générer des métriques.

Statut	Nom de check	Résultat	Résultat Long
	Stats Kernel by WinRM	 Kernel statistics collected as metrics. • Averages calculated over 5 minutes 1 second	-

Paramétrage

Le check utilise la ligne de commande suivante :

```
$WINDOWS-BY-WINRM__SHINKEN__PLUGINS__DIR$/check_windows_health_by_winrm_rust --check check_stats_kernel  
--hostname "$HOSTADDRESS$"  
--port "$_HOSTWINDOWS_BY_WINRM__PORT$"  
--username "$_HOSTWINDOWS_BY_WINRM__DOMAINUSER$"  
--password "$_HOSTWINDOWS_BY_WINRM__DOMAINPASSWORD$"  
--auth_method "$_HOSTWINDOWS_BY_WINRM__AUTHMETHOD$"  
--timeout "$_HOSTWINDOWS_BY_WINRM__TIMEOUT$"  
--shared_winrm_tmp_wf "$_HOSTWINDOWS_BY_WINRM__POLLER-SHARED-WORKING-FOLDER"
```

Données utilisées provenant des modèles

Données communes pour les checks des modèles

Nom	Modifiable sur	Valeur par défaut	Description
WINDOWS_BY_WINRM__AUTHMETHOD	l'Hôte (Onglet Données)	ntlm	Méthode d'authentification utilisé. Valeurs possibles : basic, ntlm
WINDOWS_BY_WINRM__DOMAINPASSWORD	l'Hôte (Onglet Données)	Change_Th1s_P4ssw0rd	Mot de passe de l'utilisateur de supervision
WINDOWS_BY_WINRM__DOMAINUSER	l'Hôte (Onglet Données)	shinken_user	Nom complet de l'utilisateur de supervision utilisé pour exécuter des commandes à distance. Voici quelques exemples : <ul style="list-style-type: none"> mon_utilisateur mon_domaine\mon_utilisateur mon_utilisateur@mon_domaine
WINDOWS_BY_WINRM__PORT	l'Hôte (Onglet Données)	5985	Port de connexion au serveur WinRM de l'hôte à superviser.
WINDOWS_BY_WINRM__TIMEOUT	l'Hôte (Onglet Données)	20	Temps maximum sans réponse d'une requête WinRM pour que la sonde renvoi un statut INCONNU .

Les données communes pour certain checks

Pour les checks suivants :

- Network Interfaces by WinRM
- Stats Disks by WinRM
- Stats Kernel by WinRM

Nom	Modifiable sur	Unité	Défaut	Description
WINDOWS_BY_WINRM__WORKING-FOLDER-BASE-PATH	l'Hôte (Onglet Données)	--	/tmp	Chemin absolu où sera créé le dossier WINDOWS_BY_WINRM__WORKING-FOLDER-TMP-DIRNAME .
WINDOWS_BY_WINRM__WORKING-FOLDER-TMP-DIRNAME	l'Hôte (Onglet Données)	--	shinken	Nom de dossier temporaire où seront stockés les fichiers temporaires générés par les sondes. Ne peut contenir uniquement des caractères alphanumériques, slash, antislash, espace, guillemet simple et double, tiret et tiret du bas.

Données spécifiques pour ce check

Pas de données spécifiques pour ce check

Données DFE (Duplicate Foreach)

Pas de données DFE pour ce check

Données utilisées provenant du check

Pas de données provenant du check pour ce modèle

Données globales

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



USERPLUGINS DIR	Non modifiable <i>(Sauf Admin Shinken)</i>	--	/var/lib/shinken/libexec	/var/lib/shinken/libexec	Chemin absolu contenant les sondes installés par Shinken
WINDOWS-BY- WINRM__SHIN KEN__VENDOR	Non modifiable <i>(Sauf Admin Shinken)</i>	--	shinken-additional-packs	shinken-additional-packs	Dossier fournit par shinken
WINDOWS-BY- WINRM__SHIN KEN__PACKNA ME	Non modifiable <i>(Sauf Admin Shinken)</i>	--	windows-by-WinRM__shinken	windows-by- WinRM__shinken	Dossier contenant les sondes
WINDOWS-BY- WINRM__SHIN KEN__PLUGIN SDIR	Non modifiable <i>(Sauf Admin Shinken)</i>	--	USERPLUGINS/DIR/WINDOWS-BY- WINRM__SHINKEN__VENDOR /WINDOWS-BY- WINRM__SHINKEN__PACKNAME	/var/lib/shinken-user /libexec/shinken-additional- packs/windows-by- WinRM__shinken	Chemin absolu du dossier contenant les sondes du pack windows-by-WinRM__shinken (<i>n on modifiable</i>)

Propriétés de l'hôte

Nom	Modifiable sur	Unité	Défaut	Valeur par défaut	Description
HOSTADDRESS	l'Hôte <i>(Onglet Général)</i>	--	Nom de l'hôte	Nom de l'hôte	Adresse de l'hôte

Résultat

Exemple

Statut	Nom de check	Résultat	Résultat Long
	Stats Kernel by WinRM	 Kernel statistics collected as metrics. • Averages calculated over 5 minutes 1 second	-

Interprétation des données







Statut

- Il peut prendre 2 valeurs **OK** / **INCONNU**
 - Voici un tableau récapitulatif du statut attendu suivant le retour de sonde :



Le check calcule des moyennes par rapports aux mesures de ses dernières exécutions. Alors, l'intervalle d'exécution du check va affecter la période sur laquelle ces moyennes sont calculées.

- Un intervalle d'exécution rapide donnera des moyennes plus volatiles, où il sera plus facile d'observer des pics.
- Un intervalle d'exécution lent donnera des moyennes plus lissées.

Situation	Statut	Exemple								
<ul style="list-style-type: none"> • Les mesures des disques ont bien été stockés dans les métriques. 	OK	<table border="1"> <thead> <tr> <th>Statut</th> <th>Nom de check</th> <th>Résultat</th> <th>Résultat Long</th> </tr> </thead> <tbody> <tr> <td></td> <td>Stats Kernel by WinRM</td> <td> Kernel statistics collected as metrics. • Averages calculated over 5 minutes 1 second</td> <td>-</td> </tr> </tbody> </table>	Statut	Nom de check	Résultat	Résultat Long		Stats Kernel by WinRM	 Kernel statistics collected as metrics. • Averages calculated over 5 minutes 1 second	-
Statut	Nom de check	Résultat	Résultat Long							
	Stats Kernel by WinRM	 Kernel statistics collected as metrics. • Averages calculated over 5 minutes 1 second	-							

<ul style="list-style-type: none"> Les moyenne n'a pas pu être calculé. Aucune mesure n'a été trouvée. 	INCON NU	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 10%;">Statut</th> <th style="width: 20%;">Nom de check</th> <th style="width: 50%;">Résultat</th> <th style="width: 20%;">Résultat Long</th> </tr> </thead> <tbody> <tr> <td style="text-align: center;"></td> <td>Stats Kernel by WinRM</td> <td>UNKNOWN Data from the previous executions could not be found • The next run will produce interpretable data.</td> <td style="text-align: center;">-</td> </tr> </tbody> </table>	Statut	Nom de check	Résultat	Résultat Long		Stats Kernel by WinRM	UNKNOWN Data from the previous executions could not be found • The next run will produce interpretable data.	-
Statut	Nom de check	Résultat	Résultat Long							
	Stats Kernel by WinRM	UNKNOWN Data from the previous executions could not be found • The next run will produce interpretable data.	-							

Résultat

Le résultat contient un message indiquant le statut du check.

Résultat Long

Pas de résultat long.

Métriques

Définition

Nom de la métrique	Unité	Description	Seuil d'avertissement	Seuil critique
pgfault_by_s	pgfault/s	Moyenne du nombre d'erreurs de page (<i>mineures et majeures</i>) par seconde. Calculé sur l'intervalle des deux dernières exécutions.	--	--
hardfault_by_s	hardfault/s	Moyenne du nombre d'erreurs de page majeur par seconde. Calculé sur l'intervalle des deux dernières exécutions.	--	--
softfault_by_s	softfault/s	Moyenne du nombre d'erreurs de page mineur par seconde. Calculé sur l'intervalle des deux dernières exécutions.		
ctxt_by_s	ctxt/s	Moyenne du nombre de changements de contexte. Calculé sur l'intervalle des deux dernières exécutions.	--	--
total_processes	processes	Nombre total de processus à l'instant T.	--	--
intr_by_s	intr/s	Moyenne du nombre d'interruptions processeur par seconde. Calculé sur l'intervalle des deux dernières exécutions.	--	--

Exemple

Métriques :

Métrique	Valeur	Seuil d'avertissement	Seuil critique
pgfault_by_s	23442.60pgfaults/s		
hardfault_by_s	989.28hardfaults/s		
softfault_by_s	22453.32softfaults/s		
ctxt_by_s	19873.97ctxt/s		
total_processes	359.00processes		
intr_by_s	13510.18intr/s		

Erreurs et pré-requis

Erreurs de configuration du poller shinken (spécifique à certains checks)

POLLER - BAD STATE – Permission denied

Le *poller* qui exécutera les checks nécessite un droit d'écriture et de lecture dans le répertoire décrit par **WINDOWS_BY_WINRM_POLLER-SHARED-WORKING-FOLDER-BASE-PATH/WINDOWS_BY_WINRM_POLLER-SHARED-WORKING-FOLDER-TMP-DIRNAME**, par défaut **/tmp/shinken**.

Vous pouvez obtenir les erreurs suivantes :

Statut	Nom de check	Résultat	Résultat Long
	Stats Disks by WinRM	POLLER - BAD STATE Failed to create sample storage : • Error creating the temporary working folder '/tmp/shinken/windows-by-WinRM_shinken'. Got error Permission denied (os error 13)	-

Statut	Nom de check	Résultat	Résultat Long
	Stats Disks by WinRM	POLLER - BAD STATE Failed to compute average : <ul style="list-style-type: none"> error when opening in read write mode sample 'C:' (at /tmp/shinken/windows-by-WinRM_shinken/stats_disks_by_winrm_rust_192.168.1.34_5985_C.tmp), Got 'Permission denied (os error 13)' Operation might be needed on the Poller 	-

Résolution



Remarque

Cette série de commandes ne peut être effectuée qu'en ayant les droits root.

Donc en étant connecté au compte root ou en ayant fait la commande "su" au préalable.



Remarque

Les instructions suivantes sont à exécuter sur le ou les pollers shinken.

Utilisation

```
shinken_tmp_dirname="shinken"
mkdir --parents /tmp/$shinken_tmp_dirname
chown -R root:shinken /tmp/$shinken_tmp_dirname
chmod -R g+rxw /tmp/$shinken_tmp_dirname
```

Explication

- La commande **mkdir --parents /tmp/\$shinken_tmp_dirname** crée un récursivement un répertoire.
- La commande **chown -R root:shinken /tmp/\$shinken_tmp_dirname** modifie le groupe du dossier **/tmp/shinken**.
 - Cela garantit que des droits peuvent être appliqués au groupe shinken sur ce dossier.
- La commande **chmod -R g+rxw /tmp/\$shinken_tmp_dirname** applique immédiatement les droits nécessaires au dossier **/tmp/shinken** pour le groupe **shinken**.
 - Les droits de lecture, d'écriture et d'exécution sont ajoutés au dossier. Cela permet aux sondes de créer et lire des fichiers dans le dossier **/tmp/shinken**.



Il est nécessaire d'adapter la variable **shinken_tmp_dirname** si vous avez modifié l'un des deux variables suivantes :

- WINDOWS_BY_WINRM_POLLER-SHARED-WORKING-FOLDER-BASE-PATH**
- WINDOWS_BY_WINRM_POLLER-SHARED-WORKING-FOLDER-TMP-DIRNAME**

Erreurs de connexion (communes à tous les checks)

UNKNOWN – Transport error : failed to send request: request timed out

L'hôte supervisé a mis trop de temps à répondre à la requête.



Note : ce problème peut également provenir d'un mauvais port configuré, d'un port fermé sur l'hôte supervisé, ou si le service WinRM est stoppé sur l'hôte supervisé.

Statut	Nom de check	Résultat	Résultat Long
	Disks Usage by WinRM	UNKNOWN Transport error : sent request failed: request timed out	-

Résolution :

La commande ci dessous permet de voir l'état du service WinRM :

```
Get-Service WinRM
```


Il est possible de le démarrer ou de le configurer pour se lancer automatiquement avec les commandes suivantes :

```
# Redémarrer le service WinRM :  
Restart-Service WinRM  
  
# Configurer le démarrage automatique  
Set-Service -Name WinRM -StartupType Automatic
```

UNKNOWN – Transport error : sent request failed: connection refused


L'hôte à refusé la connexion ; ou bien son pare-feu.

- Il se peut que votre service WinRM ne soit pas lancé
- ou que votre pare-feu ne soit pas configuré.

Statut	Nom de check	Résultat	Résultat Long
	Disks Usage by WinRM	UNKNOWN	Transport error : sent request failed: request timed out


UNKNOWN – Transport error : sent request failed: host is not reachable

L'hôte n'a pas pu recevoir la requête. Vérifiez votre réseau, routeur, pare-feu et nom d'hôte.

Statut	Nom de check	Résultat	Résultat Long
	Disks Usage by WinRM	UNKNOWN	Transport error : sent request failed: host is not reachable


UNKNOWN – Transport error : sent request failed: DNS resolution failed

Le nom de l'hôte n'a pas pu être résolu. Vérifiez que l'adresse renseignée est correcte et que le serveur DNS est accessible.

Statut	Nom de check	Résultat	Résultat Long
	Disks Usage by WinRM	UNKNOWN	Transport error : sent request failed: DNS resolution failed


UNKNOWN – Transport error : failed to build request: given uri is invalid

Le nom de l'hôte n'est pas une URI valide. Vérifiez que l'adresse renseignée est correcte.

Statut	Nom de check	Résultat	Résultat Long
	Network Interfaces by WinRM	UNKNOWN	Transport error : failed to build request: given uri is invalid

UNKNOWN – Authentication NTLM failed : NTLM is not supported by the server

NTLM n'est pas activé sur l'hôte à superviser.

Statut	Nom de check	Résultat	Résultat Long
	Disks Usage by WinRM	UNKNOWN	Authentication NTLM failed : NTLM is not supported by the server. Supported by server : [Basic].

Résolution :

Vous pouvez :

- Activer NTLM sur l'hôte supervisé avec la commande suivante :

```
winrm set winrm/config/service/auth '@{Negotiate="true"}'
```

- Choisir un autre mode d'authentification, en modifiant la donnée "WINDOWS_BY_WINRM__AUTHMETHOD"


UNKNOWN – Authentication NTLM failed : Unauthorized

La connexion NTLM n'a pas été autorisée. Les raisons possibles sont :

- Le couple utilisateur / mot de passe n'est pas valide
- L'utilisateur n'existe pas
- Winrm n'a pas été configuré avec la commande :

```
winrm quickconfig
```

- L'utilisateur n'appartient pas aux groupes nécessaires aux permissions WinRM


Statut	Nom de check	Résultat	Résultat Long
	Disks Usage by WinRM	UNKNOWN	Authentication NTLM failed : Unauthorized.

Résolution :

Il faut s'assurer d'avoir correctement appliqué les configurations décrites dans les sections "Configuration de WinRM" et "Configuration de l'utilisateur" (Voir la page [Configuration du Windows supervisé pour le pack windows-by-WinRM__shinken](#)).

UNKNOWN – Authentication Basic failed : Basic is not supported by the server

L'authentification basic n'est pas activé sur l'hôte à superviser.

Statut	Nom de check	Résultat	Résultat Long
	Disks Usage by WinRM	UNKNOWN	Authentication Basic failed : Basic is not supported by the server. Supported by server : [Ntlm].

Résolution :

Vous pouvez :

- Activer Basic sur l'hôte supervisé avec la commande suivante, et autoriser les communications non chiffrées :

```
winrm set winrm/config/service/auth '@{Basic="true"}'  
winrm set winrm/config/service '@{AllowUnencrypted="true"}'
```

- Choisir un autre mode d'authentification, en modifiant la donnée "WINDOWS_BY_WINRM__AUTHMETHOD"


UNKNOWN – Authentication Basic failed : Unauthorized

La connexion basic n'a pas été autorisée. Les raisons possibles sont :

- Le couple utilisateur / mot de passe n'est pas valide
- L'utilisateur n'existe pas
- Winrm n'a pas été configuré avec la commande :

```
winrm quickconfig
```

- L'utilisateur n'appartient pas aux groupes nécessaires aux permissions WinRM

Statut	Nom de check	Résultat	Résultat Long
	Disks Usage by WinRM	UNKNOWN	Authentication Basic failed : Unauthorized.

Résolution :

Il faut s'assurer d'avoir correctement appliqué les configurations décrites dans les sections "Configuration de WinRM" et "Configuration de l'utilisateur" (Voir la page [Configuration du Windows supervisé pour le pack windows-by-WinRM__shinken](#)).

Erreurs de configuration de l'hôte à superviser (communes à tous les checks)

UNKNOWN – Response fault error: Code: s:Sender, Subcode: w:AccessDenied, Reason: Access is denied.

L'utilisateur utilisé n'a pas accès à l'exécution de commandes à distances.

Statut	Nom de check	Résultat	Résultat Long
	Disks Usage by WinRM	UNKNOWN	Response fault error: Code: s:Sender, Subcode: w:AccessDenied, Reason: Access is denied.

Résolution :

Il est important de donner les accès "Read" et "Invoke" à l'utilisateur de supervision afin qu'il puisse lire des ressources et exécuter des commandes sur l'hôte supervisé.

Il faut s'assurer d'avoir correctement appliqué la configuration décrite dans la section "Permissions WinRM pour l'utilisateur" (Voir la page [Configuration du Windows supervisé pour le pack windows-by-WinRM__shinken](#)).

MONITORED HOST - BAD STATE – Command execution Failed. Permission denied.

L'utilisateur utilisé n'a pas accès aux objets CIM, nécessaire à la supervision de la machine.

Statut	Nom de check	Résultat	Résultat Long
	Disks Usage by WinRM	MONITORED HOST - BAD STATE	Command execution Failed. Permission denied. STDERR : Get-CimInstance : Access denied At line:1 char:299 + ... erence = 'Stop'; Get-CimInstance -ClassName Win32_LogicalDisk Selec ... + ~~~~~ + CategoryInfo : PermissionDenied: (root\cimv2:Win32_LogicalDisk:String) [Get-CimInstance], CimException + FullyQualifiedErrorId : HRESULT 0x80041003,Microsoft.Management.Infrastructure.CimCmdlets.GetCimInstanceCommand

Résolution :

Il est nécessaire de donner les accès à distance aux objets CIMv2 et StandardCimv2.

Il faut s'assurer d'avoir correctement appliqué la configuration décrite dans la section "Autorisation aux objets CIM" (Voir la page [Configuration du Windows supervisé pour le pack windows-by-WinRM__shinken](#)).

UNKNOWN – Command execution Failed. [...] Provider failure

L'utilisateur utilisé n'a pas accès aux objets CIM. Les permissions sont en cours d'application.

Statut	Nom de check	Résultat	Résultat Long
	Disks Usage by WinRM	UNKNOWN	Command execution Failed. STDERR : Get-CimInstance : Provider failure At line:1 char:299 + ... erence = 'Stop'; Get-CimInstance -ClassName Win32_LogicalDisk Selec ... + ~~~~~ + CategoryInfo : NotSpecified: (root\cimv2:Win32_LogicalDisk:String) [Get-CimInstance], CimException + FullyQualifiedErrorId : HRESULT 0x80041004,Microsoft.Management.Infrastructure.CimCmdlets.GetCimInstanceCommand

Résolution :

L'erreur survient après la modification des droits aux objets CIM de l'utilisateur. Il suffit d'attendre ou de redémarrer la machine afin que les permissions s'actualisent.