Processes Memory by WinRM

Sommaire

- Contexte
- Paramétrage
  - Données utilisées provenant des modèles
    - Données communes pour les checks des modèles
    - 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
- Erreurs et pré-requis
  - 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 superviser (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 **Processes Memory by WinRM** va vérifier l'utilisation de la mémoire RAM WSS (*Working Set Size*) de chaque processus et vous alerter dans le cas où ces derniers dépasseraient un certain seuil.

- Les seuils sont modifiables dans les données.
- Dans le cas où vous atteignez le seuil ***CRITIQUE*** , le check vous alertera aussi des processus dépassant seulement le seuil ***WARNING*** .

Statut	Nom de check	Résultat	Résultat Long
	Processes Memory by WinRM	OK No process uses more than 50% of your memory.	-

Paramétrage

Le check utilise la ligne de commande suivante :

```
$WINDOWS-BY-WINRM__SHINKEN__PLUGINSDIR$/check_windows_health_by_winrm_rust --check check_processes_memory
 --hostname "$HOSTADDRESS$"
 --port "$_HOSTWINDOWS_BY_WINRM__PORT$"
 --username "$_HOSTWINDOWS_BY_WINRM__DOMAINUSER$"
 --password "$_HOSTWINDOWS_BY_WINRM__DOMAINPASSWORD$"
 --auth_method "$_HOSTWINDOWS_BY_WINRM__AUTHMETHOD$"
 --timeout "$_HOSTWINDOWS_BY_WINRM__TIMEOUT$"
 -w "$_HOSTWINDOWS_BY_WINRM__PROCESSES-MEMORY__WARN$"
 -c "$_HOSTWINDOWS_BY_WINRM__PROCESSES-MEMORY__CRIT$"
 -U "$_HOSTWINDOWS_BY_WINRM__PROCESSES-MEMORY__UNIT$"
```

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)*	Ch4nge_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 : ▪ 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***.

Données spécifiques pour ce check

Nom	Modifiable sur	Unité	Valeur par défaut	Description
`WINDOWS_BY_WINRM__PROCESSES-MEMORY__CRIT`	l'Hôte *(Onglet Données)*	%	60	Définit l'utilisation RAM à partir de laquelle le check passe en **CRITIQUE** (% ou MB selon la donnée unit).
`WINDOWS_BY_WINRM__PROCESSES-MEMORY__WARN`	l'Hôte *(Onglet Données)*	%	50	Définit l'utilisation RAM à partir de laquelle le check passe en **ATTENTION** (% ou MB selon la donnée unit).
`WINDOWS_BY_WINRM__PROCESSES-MEMORY__UNIT`	l'Hôte *(Onglet Données)*	-	%	Définit l'unité utilisée pour le check (appliquée aussi sur le critique et warning) . Valeurs possibles : • **MB** • **%**

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
`USERPLUGINSDIR`	Non modifiable *(Sauf Admin Shinken)*	--	/var/lib/shinken/libexec	**/var/lib/shinken/libexec**	Chemin absolu contenant les sondes installés par Shinken
`WINDOWS-BY-WINRM__SHINKEN__VENDOR`	Non modifiable *(Sauf Admin Shinken)*	--	shinken-additional-packs	**shinken-additional-packs**	Dossier fournit par shinken
`WINDOWS-BY-WINRM__SHINKEN__PACKNAME`	Non modifiable *(Sauf Admin Shinken)*	--	windows-by-WinRM__shinken	**windows-by-WinRM__shinken**	Dossier contenant les sondes
`WINDOWS-BY-WINRM__SHINKEN__PLUGINSDIR`	Non modifiable *(Sauf Admin Shinken)*	--	`USERPLUGINSDIR/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** (*non modifiable*)

Propriétés de l'hôte

Nom	Modifiable sur	Unité	Défaut	Valeur par défaut	Description
`HOSTADDRESS`	l'Hôte *(Onglet Général)*	--	Nom de l'hôte	**Nom de l'hôte**	Adresse de l'hôte

Résultat

Exemple

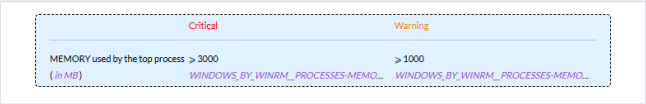
Statut	Nom de check	Résultat	Résultat Long
	Processes Memory by WinRM	OK No process uses more than 50% of your memory.	-

Interprétation des données

Statut

- Le statut peut prendre 4 valeurs différentes : ***OK*** / ***ATTENTION*** / ***CRITIQUE*** / ***INCONNU*** .
  - Le statut va dépendre du retour de sonde et de la configuration spécifique du check pour les données suivantes :
    - **WINDOWS_BY_WINRM__PROCESSES-MEMORY__CRIT**
    - **WINDOWS_BY_WINRM__PROCESSES-MEMORY__WARN**

La colonne "Affichage des seuils" montre les paramètres utilisés et leur valeur définie sur l'équipement supervisé.



Situation	*Statut*	*Exemple*

• Les charges dépassent la valeur de **WINDOWS_BY_WINRM__PROCESSES-MEMORY__CRIT**	***CRITIQUE***	Statut: Processes Memory by WinRM Nom de check: Processes Memory by WinRM Résultat: CRITICAL 1 process uses more than 20% of your memory. Résultat Long: **Top 1 consuming processes :** PID 15188 Name vmmem Used Memory % (MB) 21.0 % 3429 MB Combined usage : 21.0 % → 3429 MB of your total memory (16302 MB) Used memory is called WorkingSet in Windows. It represents the total amount of memory in bytes that a process is using, including both private and shared memory.
• Les charges dépassent la valeur de **WINDOWS_BY_WINRM__PROCESSES-MEMORY__CRIT** et **WINDOWS_BY_WINRM__PROCESSES-MEMORY__WARN**	***CRITIQUE***	Statut: Processes Memory by WinRM Nom de check: Processes Memory by WinRM Résultat: CRITICAL 2 processes use more than 2000MB of your memory. WARNING 1 process uses more than 1000MB of your memory. Résultat Long: **Top 3 consuming processes :** PID Name Used Memory MB (%) 15188 vmmem 3237 MB 19.9 % 16736 VirtualBoxVM 2941 MB 18.0 % 18788 chrome 1364 MB 8.4 % Combined usage : 7542 MB → 46.3 % of your total memory (16302 MB) Used memory is called WorkingSet in Windows. It represents the total amount of memory in bytes that a process is using, including both private and shared memory.
• Les charges dépassent la valeur de **WINDOWS_BY_WINRM__PROCESSES-MEMORY__CRIT**	***ATTENTION***	Statut: Processes Memory by WinRM Nom de check: Processes Memory by WinRM Résultat: WARNING 2 processes use more than 10% of your memory. Résultat Long: **Top 2 consuming processes :** PID Name Used Memory % (MB) 15188 vmmem 21.0 % 3427 MB 16736 VirtualBoxVM 17.6 % 2876 MB Combined usage : 38.7 % → 6302 MB of your total memory (16302 MB) Used memory is called WorkingSet in Windows. It represents the total amount of memory in bytes that a process is using, including both private and shared memory.

Résultat

Le résultat contient un message indiquant le statut ainsi que le nombre de processus dont la consommation RAM dépasse le seuil ***CRITIQUE*** ou d' ***ATTENTION*** .

Résultat long

Le résultat long contient 2 tableaux :

- Un tableau qui indique les processus ayant dépassé le seuil de ***CRITIQUE*** .
- Un tableau qui indique les processus ayant dépassé le seuil d' ***ATTENTION*** .

Les tableaux n ' apparaissent que si des processus ont dépassé les seuils , dans le cas contraire , les tableaux n'apparaîtront pas .

Métriques

Aucune métrique n'est renvoyée pour ce check

Erreurs et pré-requis

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 connection ; ou bien son pare-feu.

- Il se peut que vôte 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 autorisé. 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 autorisé. 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'éxécution 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 éxécuter 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, necessaire 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 necessaire 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.