Stats CPU by WinRM

Sommaire

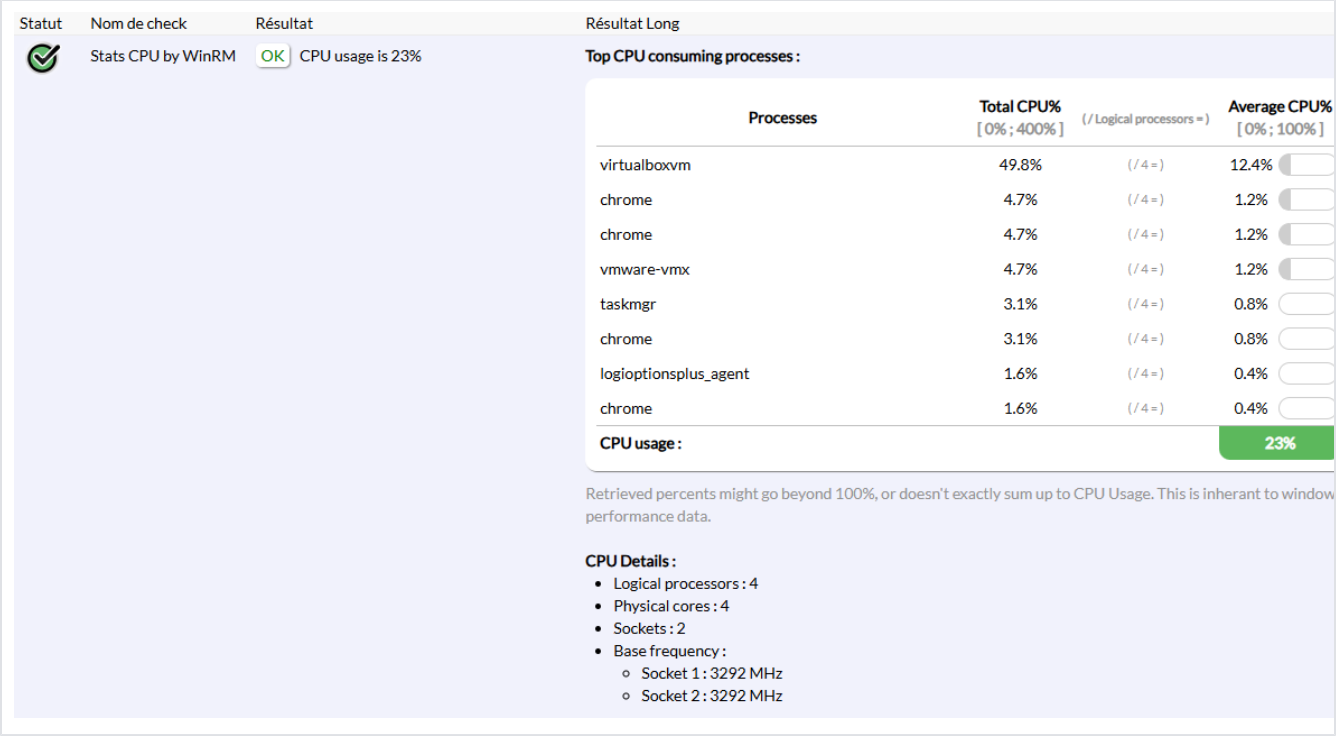
Contexte

Le check Stats CPU by WinRM va utiliser des commandes à travers le serveur WinRM pour rechercher des informations sur le CPU, tel que le nombre de cœurs, la fréquence, le pourcentage d'utilisation du processeur au cours de la dernière seconde et pour finir, si l'utilisation du processeur est trop importante, les **X processus** consommant le plus de CPU (*X étant la donnée CPU_MAX_PROCESS modifiable dans la configuration*), perm ettant de voir quels processus sont les plus consommateurs.

Les processus sont accompagnés leur consommation CPU, ainsi que d'indicateurs en pourcentage ainsi qu'une jauge graphique pour facilement visualiser l'Average CPU % :

- Total CPU% : utilisation cumulée du temps CPU sur l'ensemble des processeurs logiques. Cette valeur peut aller jusqu'à 100% × nombre de processeurs logiques.
- Average CPU% : moyenne de consommation CPU par cœur logique. Calculée ainsi : Average CPU% = Total CPU% / nombre de processeurs logiques. Elle correspond à la valeur affichée dans le Gestionnaire des tâches de Windows

La somme des mesures individuelles de l'Average CPU% de chaque processus peuvent différer de CPU usage, car ces mesures ne peuvent pas être prises à un seul instant T. Comme ces mesures sont volatiles, on peut alors parfois observer des différences.



Statut	Nom de check	Résultat	Résultat Long
✓	Stats CPU by WinRM	OK CPU usage is 23%	**Top CPU consuming processes :**

Processes	Total CPU% [0% ; 400%]	(/ Logical processors =)	Average CPU% [0% ; 100%]
virtualboxvm	49.8%	(/ 4 =)	12.4%
chrome	4.7%	(/ 4 =)	1.2%
chrome	4.7%	(/ 4 =)	1.2%
vmware-vmx	4.7%	(/ 4 =)	1.2%
taskmgr	3.1%	(/ 4 =)	0.8%
chrome	3.1%	(/ 4 =)	0.8%
logioptionsplus_agent	1.6%	(/ 4 =)	0.4%
chrome	1.6%	(/ 4 =)	0.4%
CPU usage :			23%

Retrieved percents might go beyond 100%, or doesn't exactly sum up to CPU Usage. This is inherant to window performance data.

CPU Details :

- Logical processors : 4
- Physical cores : 4
- Sockets : 2
- Base frequency :
  - Socket 1 : 3292 MHz
  - Socket 2 : 3292 MHz

Paramétrage

```
$WINDOWS-BY-WINRM__SHINKEN__PLUGINSDIR$/check_windows_health_by_winrm_rust --check check_stats_cpu
    --hostname "$HOSTADDRESS$"
    --port "$_HOSTWINDOWS_BY_WINRM__PORT$"
    --username "$_HOSTWINDOWS_BY_WINRM__DOMAINUSER$"
    --password "$_HOSTWINDOWS_BY_WINRM__DOMAINPASSWORD$"
    --auth_method "$_HOSTWINDOWS_BY_WINRM__AUTHMETHOD$"
    --timeout "$_HOSTWINDOWS_BY_WINRM__TIMEOUT$"
    -c "$_HOSTWINDOWS_BY_WINRM__STATS-CPU__CRIT$"
    -w "$_HOSTWINDOWS_BY_WINRM__STATS-CPU__WARN$"
    -m "$_HOSTWINDOWS_BY_WINRM__STATS-CPU__MAX-PROCESS$"
```

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

Donnée	Modifiable sur	Unité	Valeur par défaut	Description
WINDOWS_BY_WINRM__STATS-CPU__CRIT	l'Hôte *(Onglet Données)*	%	*90*	Définit le pourcentage d'utilisation du processeur à partir duquel le check passe en ***CRITIQUE***.
WINDOWS_BY_WINRM__STATS-CPU__WARN	l'Hôte *(Onglet Données)*	%	*80*	Définit le pourcentage d'utilisation du processeur à partir duquel le check passe en ***ATTENTION***.
WINDOWS_BY_WINRM__STATS-CPU__MAX-PROCESS	l'Hôte *(Onglet Données)*	--	*10*	Définit le nombre de processus alarmant à afficher au maximum.

Afin de récupérer le pourcentage d'utilisation du CPU au cours d'une seconde, le check attendra au moins une seconde, lui permettant de calculer le pourcentage au niveau de celle-ci.

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

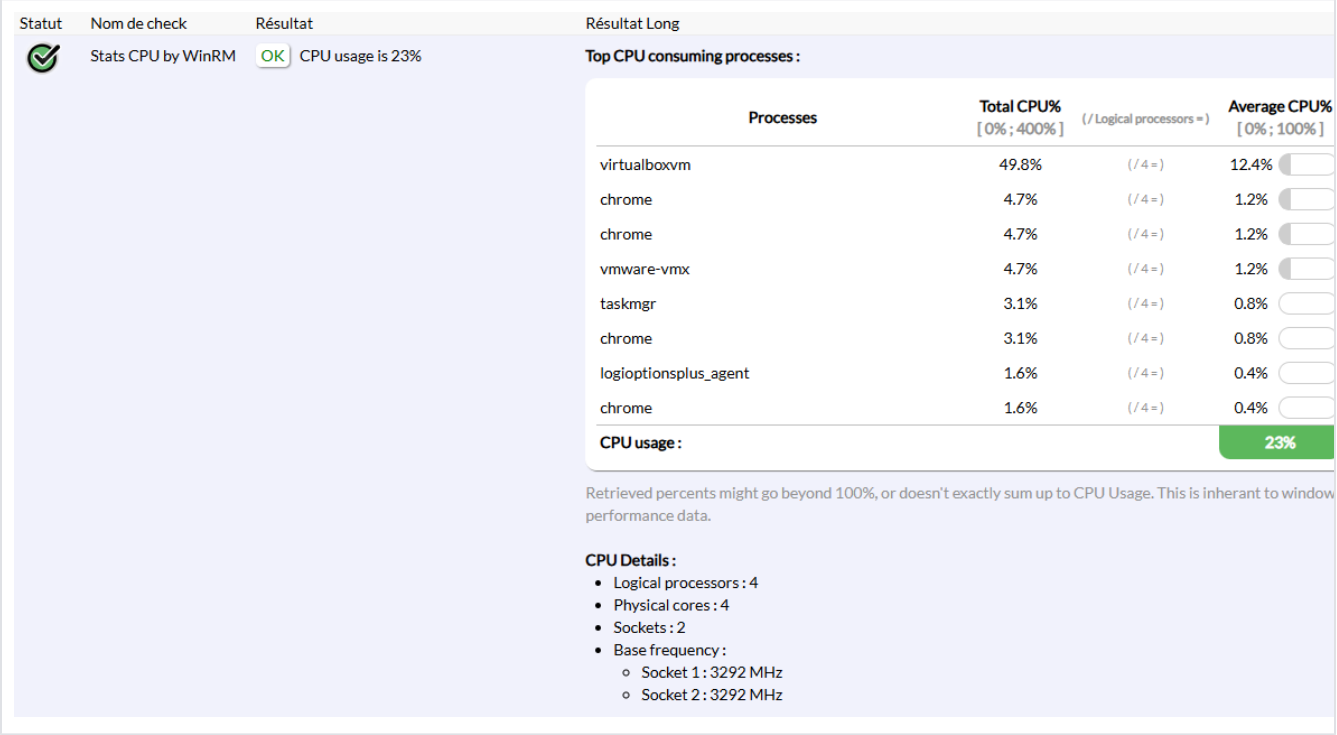
WINDOWS-BY-WINRM__SHINKEN__PACKNAME	Non modifiable *(Sauf Admin Shinken)*	--	windows-by-WinRM__shinken	**windows-by-WinRM__shinken**	Dossier contenant les sondes
WINDOWS-BY-WINRM__SHINKEN__PLUGINSDIR	Non modifiable *(Sauf Admin Shinken)*	--	USERPLUGINSDIR/WINDOWS-BY-WINRM__SHINKEN__VENDOR/WINDOWS-BY-WINRM__SHINKEN__PACKNAME	**/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



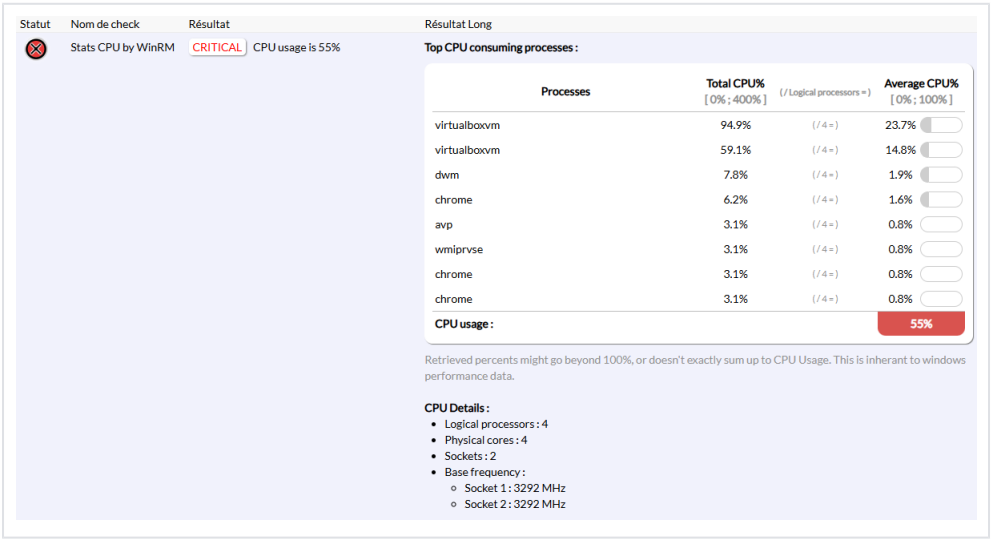
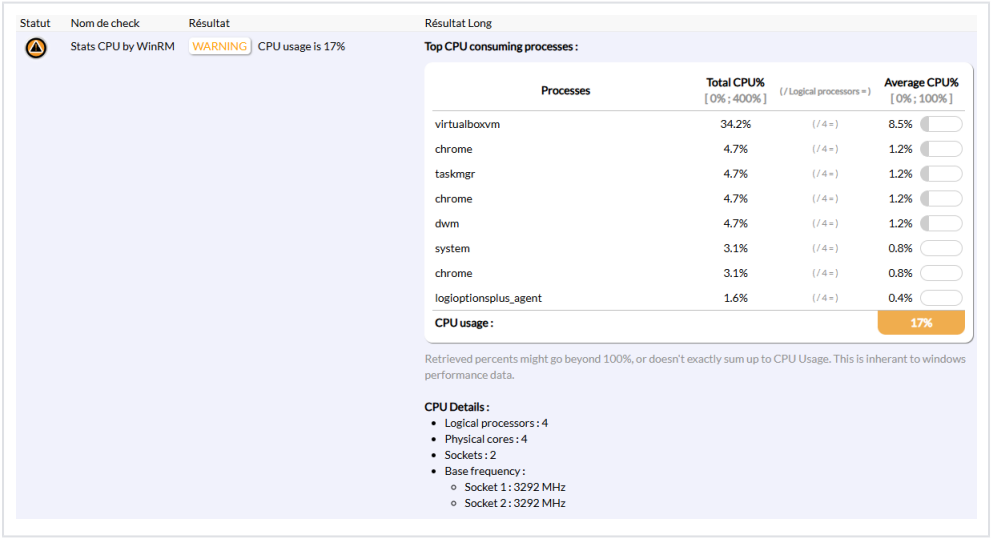
Interprétation

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_BY_WINRM__STATS-CPU__CRIT**
  - **WINDOWS_BY_WINRM__STATS-CPU__WARN**
- Voici un tableau récapitulatif du statut attendu suivant le retour de sonde :

Le texte de 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__STATS-CPU__CRIT**	***CRITIQUE***	
• Les charges dépassent la valeur de **WINDOWS_BY_WINRM__STATS-CPU__WARN.**	***ATTENTION***	

Résultat

Le résultat contient un message indiquant le statut ainsi que l'utilisation du CPU en pourcentage, valeur correspondant à la métrique **cpu_all_usage**.

Résultat Long

Le résultat long contient un tableau qui liste les **X processus** les plus consommateurs (*le **X** correspond à la donnée WINDOWS_BY_WINRM__STATS-CPU__MAX-PROCESS*). La mesure d'utilisation CPU est donnée avec Total CPU% et Average CPU%.

Métriques

Définition

Nom de la métrique	Unité	Description	Seuil d'avertissement	Seuil critique
cpu_all_usage	%	Retourne le pourcentage de temps CPU actif au cours de la dernière seconde (*Correspond au % afficher dans le résultat du check*).	**WINDOWS_BY_WINRM__STATS-CPU__WARN**	**WINDOWS_BY_WINRM__STATS-CPU__CRIT**
cpu_(NUMERO_CPU)**_usr**	%	Retourne le pourcentage de temps CPU utilisé par les processus en **espace utilisateur** au cours de la dernière seconde.	--	--

cpu_(NUMERO_CPU)**_priv**	%	Retourne le pourcentage de temps CPU utilisé par les processus en **mode noyau** au cours de la dernière seconde.	--	--
cpu_(NUMERO_CPU)**_idle**	%	Retourne le pourcentage de temps CPU **inactif** au cours de la dernière seconde.	--	--
cpu_(NUMERO_CPU)**_irq**	%	Retourne le pourcentage de temps CPU consacré au traitement des **interruptions matérielles** (périphériques physiques) au cours de la dernière seconde.	--	--
cpu_(NUMERO_CPU)**_dpc**	%	Retourne le pourcentage de temps CPU utilisé par les **DPC** (*Deferred Procedure Calls*) — routines différées généralement utilisées par les pilotes pour finaliser le traitement d' interruptions au cours de la dernière seconde.	--	--

Toutes les métriques contenant le mot **(** NUMERO_CPU **)** dans le tableau ci-dessus seront dupliquées en fonction du nombre de processeurs logique présents sur le serveur supervisé.

Exemple (*pour 2 CPUs*) :

- cpu_00_usr
- cpu_00_priv
- ...
- cpu_01_usr
- cpu_01_priv
- ...

Exemple

Métriques :

Métrique	Valeur	Seuil d'avertissement	Seuil critique
cpu_all_usage	85.60%	80.00	90.00
cpu_all_usr	49.04%		
cpu_all_priv	36.19%		
cpu_all_idle	10.76%		
cpu_all_irq	2.34%		
cpu_all_dpc	1.17%		
cpu_00_usr	40.48%		
cpu_00_priv	45.15%		
cpu_00_idle	9.34%		
cpu_00_irq	3.11%		
cpu_00_dpc	4.67%		
cpu_01_usr	42.03%		
cpu_01_priv	40.48%		
cpu_01_idle	10.94%		
cpu_01_irq	3.11%		
cpu_01_dpc	0.00%		
cpu_02_usr	56.04%		
cpu_02_priv	28.02%		
cpu_02_idle	12.34%		
cpu_02_irq	0.00%		
cpu_02_dpc	0.00%		
cpu_03_usr	57.60%		
cpu_03_priv	31.14%		
cpu_03_idle	10.40%		
cpu_03_irq	3.11%		
cpu_03_dpc	0.00%		

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	-

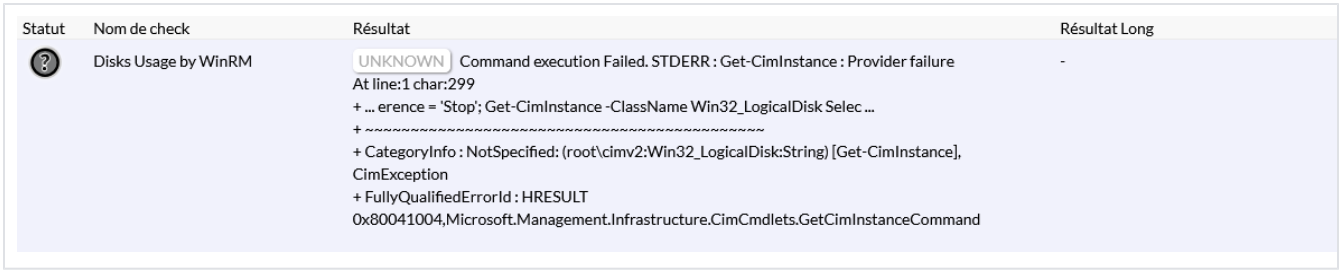
Résolution :

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.