

Uptime 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
 - Statut
 - Résultat
 - Résultat Long
- Métriques
 - Définition
 - Exemple
- 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 **Uptime by WinRM** va vérifier la date du dernier redémarrage de la machine supervisée.

Il y a 2 modes de fonctionnement :

1. S'il est inférieur au seuil minimum, le statut passera en **CRITIQUE** (*1h par défaut*),
 - Cela permet d'être notifié qu'un redémarrage vient d'avoir lieu.
2. S'il est supérieur à l'un des seuils maximum, le statut passera en **CRITIQUE / ATTENTION** .
 - Ce paramétrage informe si un serveur n'a pas été redémarré depuis trop longtemps.
 - Cette 2 option peut-être désactivée.

Statut	Nom de check	Résultat	Résultat Long
	Uptime by WinRM	 Uptime is 2 hours 3 minutes 2 seconds	-

Paramétrage

Le check utilise la ligne de commande suivante :

```
$WINDOWS-BY-WINRM__SHINKEN__PLUGINS$/$/check_windows_health_by_winrm_rust --check check_uptime
--hostname "$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__UPTIME__CRIT$"
-l "$_HOSTWINDOWS_BY_WINRM__UPTIME__HIGH-WARN$, $_HOSTWINDOWS_BY_WINRM__UPTIME__HIGH-CRIT$"
```

Données utilisées provenant des modèles

Données communes pour les checks des modèles

Nom	Modifiable sur	Valeur par défaut	Description
WINDOWS_BY_WINRM__AUTHMET HOD	l'Hôte (<i>Onglet Données</i>)	ntlm	Méthode d'authentification utilisé. Valeurs possibles : basic, ntlm
WINDOWS_BY_WINRM__DOMAINP ASSWORD	l'Hôte (<i>Onglet Données</i>)	Ch4nge_Th1s_P4s sw0rd	Mot de passe de l'utilisateur de supervision
WINDOWS_BY_WINRM__DOMAINU SER	l'Hôte (<i>Onglet Données</i>)	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 (<i>Onglet Données</i>)	5985	Port de connexion au serveur WinRM de l'hôte à superviser.
WINDOWS_BY_WINRM__TIMEOUT	l'Hôte (<i>Onglet Données</i>)	20	Temps maximum sans réponse d'une requête WinRM pour que la sonde renvoi un statut <i>INCONNU</i> .

Données spécifiques pour ce check

Nom	Modifiable sur	Unité	Défaut	Description
WINDOWS_BY_WINRM__UPTIME__ CRIT	l'Hôte (<i>Onglet Données</i>)	secondes	3600	Temps écoulé depuis le dernier redémarrage en secondes en dessous duquel le check passe en CRITIQUE . (<i>Pour savoir qu' un redémarrage vient d'avoir lieu</i>)
WINDOWS_BY_WINRM__UPTIME__ HIGH-CRIT	l'Hôte (<i>Onglet Données</i>)	secondes	0 (<i>inactif</i>)	Temps écoulé depuis le dernier redémarrage en secondes au-dessus duquel le check passe en CRITIQUE . Une valeur à 0 permet de ne pas activer cette vérification. (<i>Pour vérifier que cela ne fait pas trop longtemps que la machine n'a pas été redémarrée</i>)

WINDOWS_BY_WINRM__UPTIME__ HIGH-WARN	l'Hôte (Onglet Données)	secondes	0 (<i>inactif</i>)	Temps écoulé depuis le dernier redémarrage en secondes au-dessus duquel le check passe en ATTENTION . Une valeur à 0 permet de ne pas activer cette vérification. (Pour vérifier que cela ne fait pas trop longtemps que la machine n'a pas été redémarrée)
---	------------------------------	----------	----------------------	--

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 (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)	--	USERPLUGINDIR/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
	Uptime by WinRM	 Uptime is 2 hours 3 minutes 2 seconds	-

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_UPTIME_CRIT`
 - `WINDOWS_BY_WINRM_UPTIME_HIGH-WARN`
 - `WINDOWS_BY_WINRM_UPTIME_HIGH-CRIT`
- 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.

	Critical	Warning
Minimum UPTIME (0 for inactive)	< 3600 s <code>WINDOWS_BY_WINRM_UPTIME_CRIT</code>	--
Maximum UPTIME (0 for inactive)	> 0 s <code>WINDOWS_BY_WINRM_UPTIME_HIGH-CRIT</code>	> 0 s <code>WINDOWS_BY_WINRM_UPTIME_HIGH-WARN</code>

Situation	Statut	Exemple								
Le serveur a été redémarré il y a moins de WINDOWS_BY_WINRM_UPTIME_CRIT secondes	CRITIQUE	<table><tr><th>Statut</th><th>Nom de check</th><th>Résultat</th><th>Résultat Long</th></tr><tr><td></td><td>Uptime by WinRM</td><td>CRITICAL Uptime is less than threshold 1 hour (Up since 35 seconds).</td><td>-</td></tr></table>	Statut	Nom de check	Résultat	Résultat Long		Uptime by WinRM	CRITICAL Uptime is less than threshold 1 hour (Up since 35 seconds).	-
Statut	Nom de check	Résultat	Résultat Long							
	Uptime by WinRM	CRITICAL Uptime is less than threshold 1 hour (Up since 35 seconds).	-							
Le serveur n'a pas été redémarré depuis plus que la valeur de WINDOWS_BY_WINRM_UPTIME_HIGH-CRIT secondes. WINDOWS_BY_WINRM_UPTIME_HIGH-CRIT doit être différent de 0.	CRITIQUE	<table><tr><th>Statut</th><th>Nom de check</th><th>Résultat</th><th>Résultat Long</th></tr><tr><td></td><td>Uptime by WinRM</td><td>CRITICAL Uptime is more than 1 hour 5 minutes (Up since 2 hours 4 minutes 58 seconds).</td><td>-</td></tr></table>	Statut	Nom de check	Résultat	Résultat Long		Uptime by WinRM	CRITICAL Uptime is more than 1 hour 5 minutes (Up since 2 hours 4 minutes 58 seconds).	-
Statut	Nom de check	Résultat	Résultat Long							
	Uptime by WinRM	CRITICAL Uptime is more than 1 hour 5 minutes (Up since 2 hours 4 minutes 58 seconds).	-							
Le serveur n'a pas été redémarré depuis plus que la valeur de WINDOWS_BY_WINRM_UPTIME_HIGH-WARN secondes. WINDOWS_BY_WINRM_UPTIME_HIGH-WARN doit être différent de 0.	ATTENTION	<table><tr><th>Statut</th><th>Nom de check</th><th>Résultat</th><th>Résultat Long</th></tr><tr><td></td><td>Uptime by WinRM</td><td>WARNING Uptime is more than 1 hour 1 minute 40 seconds (Up since 2 hours 6 minutes 4 seconds).</td><td>-</td></tr></table>	Statut	Nom de check	Résultat	Résultat Long		Uptime by WinRM	WARNING Uptime is more than 1 hour 1 minute 40 seconds (Up since 2 hours 6 minutes 4 seconds).	-
Statut	Nom de check	Résultat	Résultat Long							
	Uptime by WinRM	WARNING Uptime is more than 1 hour 1 minute 40 seconds (Up since 2 hours 6 minutes 4 seconds).	-							

Résultat

Affiche le temps depuis lequel la machine supervisée est allumée.

Résultat Long

Pas de résultat long.

Métriques

Définition

Nom de la métrique	Unité	Description	Seuil d'avertissement	Seuil critique
--------------------	-------	-------------	-----------------------	----------------

uptime_in_days	jours	Temps depuis le dernier démarrage	WINDOWS_BY_WINRM_UPTIME_HIGH-WARN	WINDOWS_BY_WINRM_UPTIME_HIGH-CRIT WINDOWS_BY_WINRM_UPTIME_CRIT
----------------	-------	-----------------------------------	-----------------------------------	---

Exemple

Métriques :

Métrique	Valeur	Seuil d'avertissement	Seuil critique
uptime_in_days	0.03d		

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 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 [Ntlm].	Authentication Basic failed : Basic is not supported by the server. Supported by server : -

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 denied.	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.