

Service \$KEY\$ State 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
 - Résultat
 - Résultat Long
- Métriques
- Erreurs et pré-requis
 - Erreurs de configuration de l'hôte supervisé (spécifique à ce check)
 - MONITORED HOST - BAD STATE - Access denied
 - Résolution
 - MONITORED HOST - BAD STATE - Service "." does not exist as an installed service.
 - 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 **Service [\$KEY\$] State by WinRM** permet de vérifier le status d'un service Windows. Il permet ainsi de s'assurer que les services supervisés sont bien dans l'état attendu.

Le check utilise une donnée **Duplicate Foreach** qui permet de générer automatiquement le check pour chaque service à superviser.

Statut	Nom de check	Résultat	Résultat Long
	Service [win] State by WinRM	 Service 'WinRM' in expected state (Running).	-

Paramétrage

```
$WINDOWS-BY-WINRM__SHINKEN__PLUGINS__DIR$/check_windows_health_by_winrm_rust --check check_service_state
--hostname "$HOSTADDRESS$"
--port "$_HOSTWINDOWS_BY_WINRM__PORT$"
--username "$_HOSTWINDOWS_BY_WINRM__DOMAINUSERS$"
--password "$_HOSTWINDOWS_BY_WINRM__DOMAINPASSWORD$"
--auth_method "$_HOSTWINDOWS_BY_WINRM__AUTHMETHOD$"
--timeout "$_HOSTWINDOWS_BY_WINRM__TIMEOUT$"
-n "$ARG1$"
-e "$ARG2$"
```

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 (Onglet Données)	ntlm	Méthode d'authentification utilisé. Valeurs possibles : basic, ntlm
WINDOWS_BY_WINRM__DOMAINP ASSWORD	l'Hôte (Onglet Données)	Ch4nge_Th1s_P4s sw0rd	Mot de passe de l'utilisateur de supervision
WINDOWS_BY_WINRM__DOMAINU SER	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 <i>INCONNU</i> .

Données spécifiques pour ce check

Aucune données spécifique pour ce check.

Données DFE (Duplicate Foreach)

Donnée	Description	Exemple
WINDOWS_BY_WINRM__SERVICE-STATE__SERVICE-TO-CHECK	Définit une paire KEY\$(VALUE)\$. • KEY correspond au nom du service à superviser. • VALUE correspond à l'état attendu du service à superviser. ◦ Les valeurs possibles sont : ▪ Stopped ▪ Start Pending ▪ Stop Pending ▪ Running ▪ Continue Pending ▪ Pause Pending ▪ Paused	WinRM\$(Running)\$

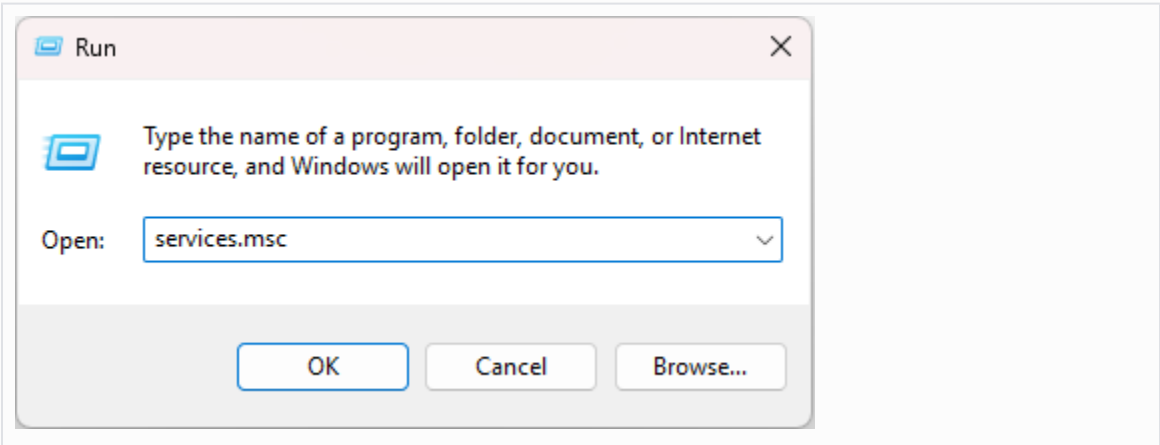
- [Dupliquer des checks en fonction d'une liste de valeurs présentes dans la Donnée d'un hôte \(duplicate_foreach\)](#)

Modifier les données accrochées à l'hôte affectera l'ensemble des checks dupliqués.
Afin de paramétrer individuellement chaque checks, il est possible de surcharger les données des checks.

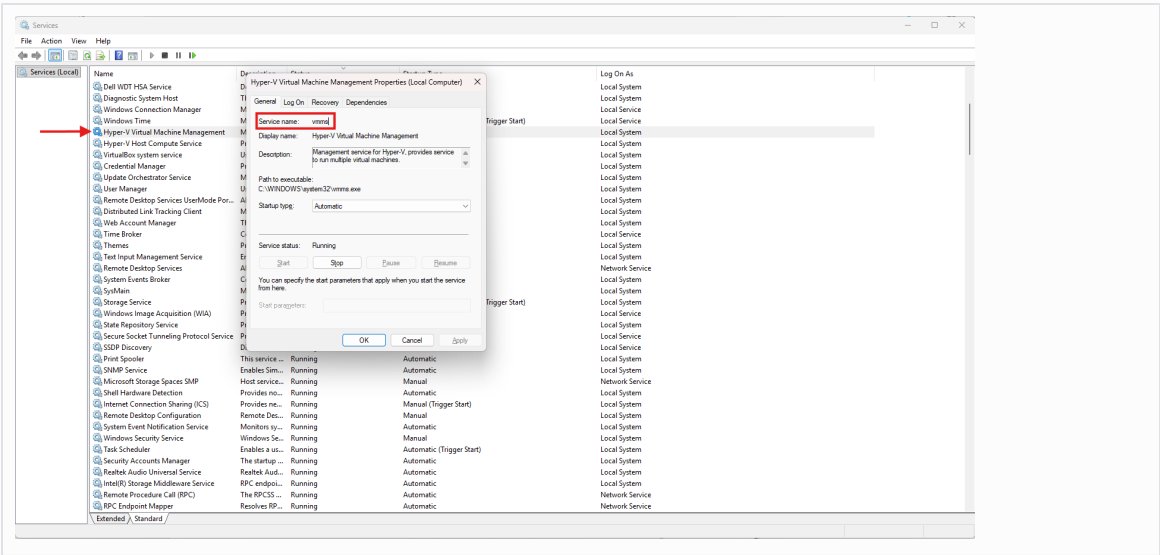
- [La surcharge des propriétés pour un check](#)

i En cas de difficulté pour identifier les services à superviser, il est possible de rechercher leur noms depuis l'application services.msc. Les services ont un nom unique, et un nom d'affichage. Les étapes ci-dessous expliquent comment récupérer le nom unique, qui est utilisé pour configurer le check.

- Ouvrir la fenêtre d'exécution avec le raccourcis "Windows" + "R"
- Rentrer "services.msc" puis cliquer sur OK.



- Une nouvelle fenêtre s'affiche avec l'ensemble des services supervisable sur votre machine.
- Recherche le service voulu parmi la liste
- Une fois trouvé, cliquer droit dessus, puis "propriétés"
- Le nom de service unique apparait en première propriété de l'onglet Général



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__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)	--	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 (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
	Service [win] State by WinRM	 Service 'WinRM' in expected state (Running).	-

Interprétation

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

Situation	Statut	Exemple								
Le service est dans l' état attendu défini par la variable WINDOWS_BY_WINRM__SERVICE-STATE__SERVICE-TO-CHECK . (\$VALUE 2\$)	OK	<table><tr><th>Statut</th><th>Nom de check</th><th>Résultat</th><th>Résultat Long</th></tr><tr><td></td><td>Service [win] State by WinRM</td><td>OK Service 'WinRM' in expected state (Running).</td><td>-</td></tr></table>	Statut	Nom de check	Résultat	Résultat Long		Service [win] State by WinRM	OK Service 'WinRM' in expected state (Running).	-
Statut	Nom de check	Résultat	Résultat Long							
	Service [win] State by WinRM	OK Service 'WinRM' in expected state (Running).	-							
Le service n'est pas dans l'état attendu défini par la variable WINDOWS_BY_WINRM__SERVICE-STATE__SERVICE-TO-CHECK . (\$VALUE 2\$)	CRITIQUE	<table><tr><th>Statut</th><th>Nom de check</th><th>Résultat</th><th>Résultat Long</th></tr><tr><td></td><td>Service [Time] State by WinRM</td><td>CRITICAL Unexpected state for service 'w32time'. Service state is 'Running' but expected 'Stopped'.</td><td>-</td></tr></table>	Statut	Nom de check	Résultat	Résultat Long		Service [Time] State by WinRM	CRITICAL Unexpected state for service 'w32time'. Service state is 'Running' but expected 'Stopped'.	-
Statut	Nom de check	Résultat	Résultat Long							
	Service [Time] State by WinRM	CRITICAL Unexpected state for service 'w32time'. Service state is 'Running' but expected 'Stopped'.	-							

Résultat

Le résultat contient un message indiquant le statut du check.

Résultat Long

Pas de résultat long.

Métriques

Aucune métrique n'est renvoyée pour ce check.

Erreurs et pré-requis

Erreurs de configuration de l'hôte supervisé (spécifique à ce check)

MONITORED HOST - BAD STATE - Access denied

L'utilisateur de supervision ne dispose pas des droits nécessaires pour interroger l'état du service cible.

Statut	Nom de check	Résultat	Résultat Long
	Service [win] State by WinRM	MONITORED HOST - BAD STATE Access denied querying "WinRM" service status. Please read the check documentation to grant privilege.	-

Résolution

 La résolution de ce problème doit se faire en mode **Administrateur** sur un terminal PowerShell.

L'utilisateur de supervision doit avoir accès en lecture au service supervisé.

Dans le pack sont livrés des scripts permettant l'opération : [Configuration du Windows supervisé pour le pack windows-by-WinRM__shinken](#)

MONITORED HOST - BAD STATE - Service "..." does not exist as an installed service.

Le service n'a pas été trouvé sur le système cible.

Statut	Nom de check	Résultat	Résultat Long
	Service [fake_service] State by WinRM	UNKNOWN Service "FakeService" does not exist as an installed service. - Search service to monitor with the following command: <code>(Get-Service).Name</code> - Then update DFE variable "WINDOWS_BY_WINRM_SERVICES-STATE_SERVICES-TO-CHECK"	-

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 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'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.