Connection Failed by WinRM

Sommaire

Les tentatives d'intrusion pour corruption ou vol de données ne doivent pas être sous-estimées dans le cadre de votre supervision de vos postes et serveurs Linux. Ce check a donc été conçu pour vous permettre de garder le maximum de vigilance sur les échecs de connexion sur votre parc.

Le check **Connection Failed by WinRM** va vérifier vos logs dans un laps de temps donné (*24h par défaut, modifiable dans les données*) et vous donner le nombre total de tentatives de connexions échouées, et un tableau comportant une ligne par trio IP-Host-Interface (*dans le cas d'une connexion réseau*) ou couple Host-Interface (*dans le cas d'une connexion locale sans adresse IP*).

- Vous obtiendrez alors le nombre de tentatives au cas par cas, la date de la première et de la dernière tentative, et les informations précédemment énoncées.
  - Le tableau est classé par le nombre total de tentatives de connexion pour le trio IP-Host-Interface ou Host-Interface.
- Deux seuils configurables permettent de déterminer quand le check passe en **ATTENTION** , puis en **CRITIQUE** .

Statut	Nom de check	Résultat	Résultat Long
	Connection Failed by WinRM	OK There are no failed connection attempts in the last 24 hours.	-

Paramétrage

Le check utilise la ligne de commande suivante :

```
$WINDOWS-BY-WINRM__SHINKEN__PLUGINSDIR$/check_windows_health_by_winrm_rust --check check_connection_failed
    --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 "$_HOSTWINDOWS_BY_WINRM__CONNECTION-FAILED__WARN$"
    -c "$_HOSTWINDOWS_BY_WINRM__CONNECTION-FAILED__CRIT$"
    --time "$_HOSTWINDOWS_BY_WINRM__CONNECTION-FAILED__TIME-LIMIT$"
    --interfaces-allowed "$_HOSTWINDOWS_BY_WINRM__CONNECTION-FAILED__INTERFACES-ALLOWED$"
```

Données utilisées provenant du modèle

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__CONNECTION-FAILED__WARN`	l'Hôte *(Onglet Données)*	--	*5*	Définit le nombre de connexions échouées à partir duquel le check passe en **ATTENTION** .
`WINDOWS_BY_WINRM__CONNECTION-FAILED__CRIT`	l'Hôte *(Onglet Données)*	--	*10*	Définit le nombre de connexions échouées à partir duquel le check passe en **CRITIQUE** .

`WINDOWS_BY_WINRM__CONNECTION-FAILED__TIME-LIMIT`	l'Hôte *(Onglet Données)*	heures	*24*	Les **X dernières heures** de logs lus pour identifier les connexions échouées.
`WINDOWS_BY_WINRM__CONNECTION-FAILED__LOGON-TYPES`	l'Hôte *(Onglet Données)*		*ALL*	Filtres des **types de connexion (LogonType)** à prendre en compte dans le check, séparés par des virgules. Les types de connexion pris en compte doivent **correspondre à au moins un des filtres** fournis (basés sur le nom du *LogonType*). • **Network** prendra en compte les connexions de type **Network** • **Interactive** prendra en compte uniquement les connexions **locales interactives** • **RemoteInteractive** prendra en compte les connexions **RDP / Terminal Services** • **Service,Batch** prendra en compte les échecs liés aux **services** et **tâches planifiées** La valeur ***ALL*** peut être utilisée afin de **prendre en compte tous les types de connexion** définis.

Voici la liste des **types de connexion (LogonType)** que le check peut superviser :

Logon Type	Logon Title	Description
2	Interactive	A user logged on to this computer.
3	Network	A user or computer logged on to this computer from the network.
4	Batch	Batch logon type is used by batch servers, where processes may be executing on behalf of a user without their direct intervention.
5	Service	A service was started by the Service Control Manager.
7	Unlock	This workstation was unlocked.
8	NetworkCleartext	A user logged on to this computer from the network. The user's password was passed to the authentication package in its unhashed form. The built-in authentication packages all hash credentials before sending them across the network. The credentials do not traverse the network in plaintext (also called cleartext).
9	NewCredentials	A caller cloned its current token and specified new credentials for outbound connections. The new logon session has the same local identity, but uses different credentials for other network connections.
10	RemoteInteractive	A user logged on to this computer remotely using Terminal Services or Remote Desktop.
11	CachedInteractive	A user logged on to this computer with network credentials that were stored locally on the computer. The domain controller was not contacted to verify the credentials.

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

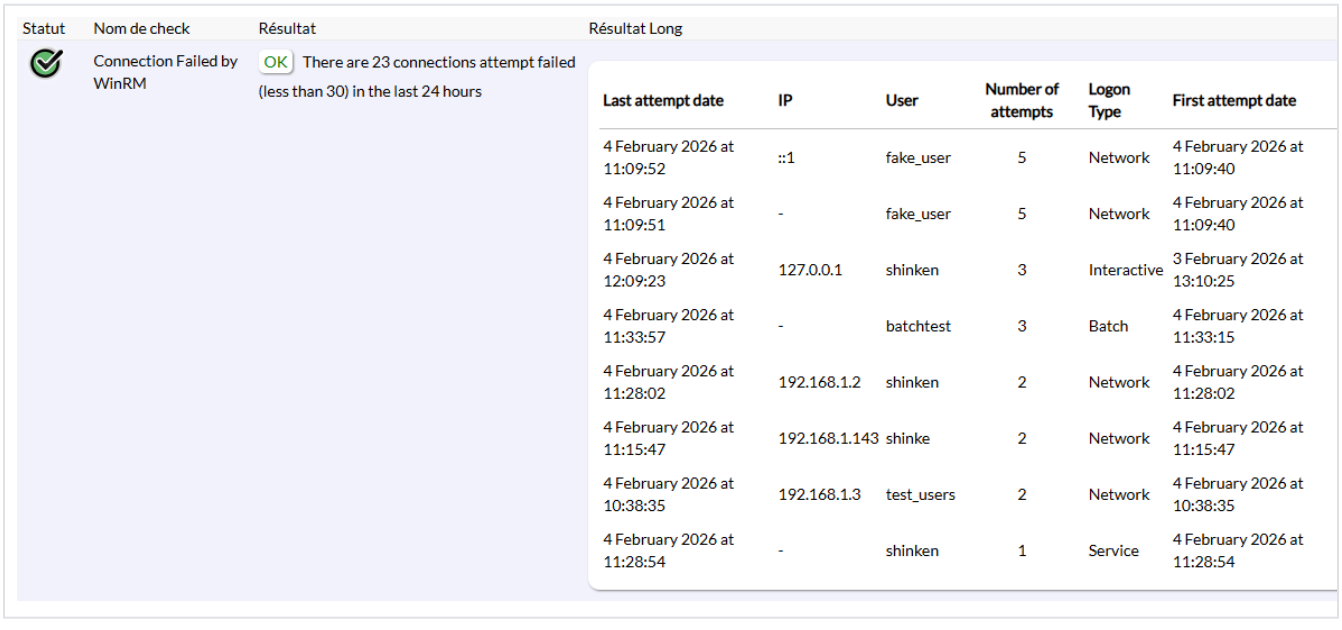
USERPLUGINSDIR	Non modifiable *(Sauf Admin Shinken)*	--	/var/lib/shinken/libexec	**/var/lib/shinken/libexec**	Chemin absolu contenant les sondes installés par Shinken
WINDOWS-BY-WINRM__SHINKEN__VENDOR	Non modifiable *(Sauf Admin Shinken)*	--	shinken-additional-packs	**shinken-additional-packs**	Dossier 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
	Connection Failed by WinRM	OK There are 23 connections attempt failed (less than 30) in the last 24 hours

Résultat Long

Last attempt date	IP	User	Number of attempts	Logon Type	First attempt date
4 February 2026 at 11:09:52	::1	fake_user	5	Network	4 February 2026 at 11:09:40
4 February 2026 at 11:09:51	-	fake_user	5	Network	4 February 2026 at 11:09:40
4 February 2026 at 12:09:23	127.0.0.1	shinken	3	Interactive	3 February 2026 at 13:10:25
4 February 2026 at 11:33:57	-	batchtest	3	Batch	4 February 2026 at 11:33:15
4 February 2026 at 11:28:02	192.168.1.2	shinken	2	Network	4 February 2026 at 11:28:02
4 February 2026 at 11:15:47	192.168.1.143	shinke	2	Network	4 February 2026 at 11:15:47
4 February 2026 at 10:38:35	192.168.1.3	test_users	2	Network	4 February 2026 at 10:38:35
4 February 2026 at 11:28:54	-	shinken	1	Service	4 February 2026 at 11:28:54

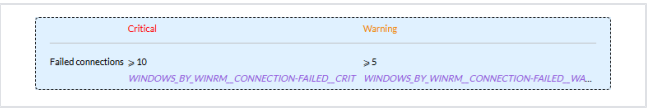
Interprétation des données

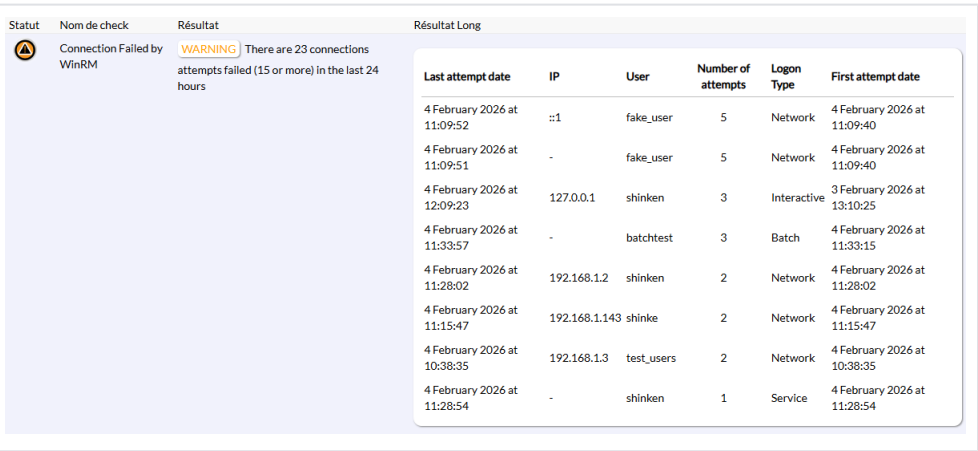
Statut

- Le statut peut prendre 4 valeurs différentes : ***OK*** / ***ATTENTION*** / ***CRITIQUE*** / ***INCONNU*** .

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

- Le statut va dépendre du retour de sonde et de la configuration spécifique du check pour les données suivantes :
  - **WINDOWS_BY_WINRM__CONNECTION-FAILED__CRIT**
  - **WINDOWS_BY_WINRM__CONNECTION-FAILED__WARN**



Situation	*Statut*	*Exemple*
• Les nombre de tentatives de connections échoués est supérieur ou égal à **WINDOWS_BY_WINRM__CONNECTION-FAILED__CRIT**.	***CRITIQUE***	
• Les nombre de tentatives de connections échoués est supérieur ou égal à **WINDOWS_BY_WINRM__CONNECTION-FAILED__WARN**.	***ATTENTION***	

Résultat

Le résultat contient un message indiquant le statut ainsi que le nombre de connexions échouées dépassant le seuil ***CRITIQUE*** ou d' ***ATTENTION*** .

Résultat long

Le résultat long contient un tableau classé par le nombre total de tentatives de connexion pour le trio IP-Host-Interface ou Host-Interface.

Métriques

Définition

Nom de la métrique	Unité	Description	Seuil d'avertissement	Seuil critique
total	--	Nombre de connexions échouées	**WINDOWS_BY_WINRM__CONNECTION-FAILED__WARN**	**WINDOWS_BY_WINRM__CONNECTION-FAILED__CRIT**

Exemple

Métriques :

Métrique	Valeur	Seuil d'avertissement	Seuil critique
total	12.00	5.00	10.00

Erreurs et pré-requis

Connection Failed by WinRM

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

Le check n'a pas pu accéder au **journal de sécurité Windows (Security Event Log)** lors de l'exécution distante de la commande PowerShell.

Statut	Nom de check	Résultat	Résultat Long
?	Connection Failed by WinRM	MONITORED HOST - BAD STATE Command execution Failed. Permission denied. STDERR : Get-WinEvent : Could not retrieve information about the Security log. Error: Attempted to perform an unauthorized operation.. At line:1 char:347 + ...);$events = Get-WinEvent @{ LogName='Security'; Id=4625; StartTime=$S ... + ~~~~~~ + CategoryInfo : NotSpecified: (:) [Get-WinEvent], Exception + FullyQualifiedErrorId : LogInfoUnavailable,Microsoft.PowerShell.Commands.GetWinEventCommand	-

L'accès au journal **Security** est **restreint par Windows** et nécessite des **droits spécifiques**.
Si l'utilisateur de supervision utilisé par le check ne dispose pas des permissions nécessaires, Windows retourne l'erreur suivante.
Résolution

Attribuer au compte de supervision les droits nécessaires pour la lecture du journal **Security** :

- en l'ajoutant au groupe **Lecteurs des journaux d'événements** (ou **Event Log Readers**)
- et en lui accordant explicitement l'accès en lecture au journal Security (méthode utilisée par le script de configuration d'un hôte fourni dans le pack)

Pour les environnements **Active Directory**, vérifier que le script **Set-EventLogSecurity.ps1** est bien **déployé via une GPO** et correctement **rattaché aux UO concernées**.

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 :

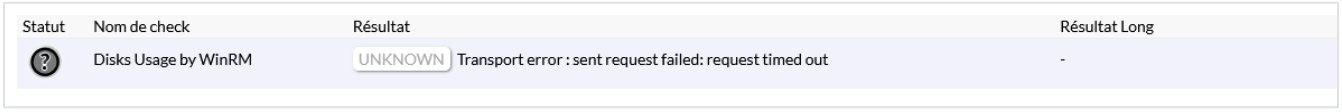
```
# Redémarrer le service WinRM :
Restart-Service WinRM

# 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.

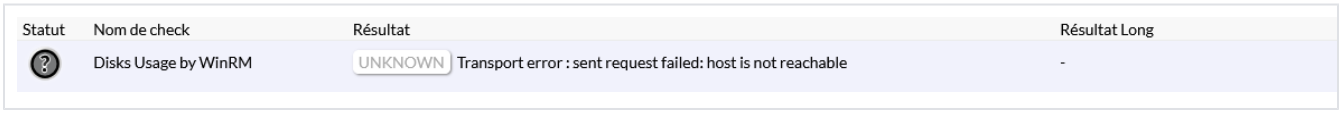
- Il se peut que vôte service WinRM ne soit pas lancé
- ou que votre pare-feu ne soit pas configuré.



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

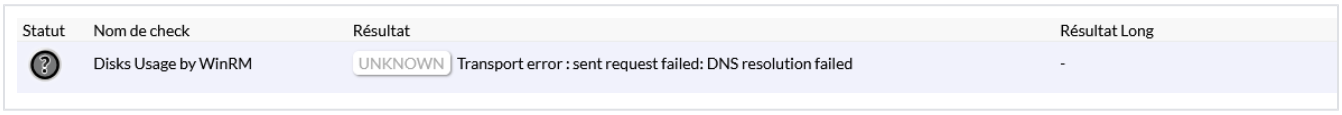
L'hôte n'a pas pu recevoir la requête. Vérifiez votre réseau, routeur, pare-feu et nom d'hôte.



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

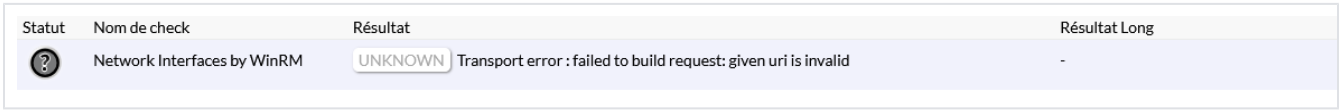
Le nom de l'hôte n'a pas pu être résolu. Vérifiez que l'adresse renseignée est correcte et que le serveur DNS est accessible.



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

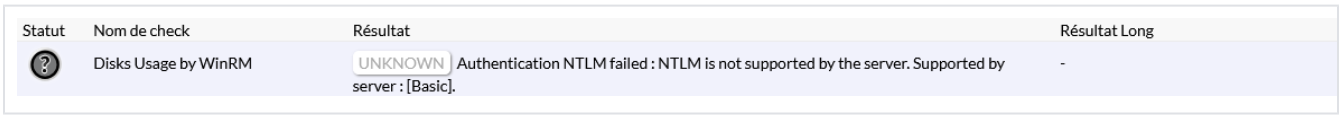
Le nom de l'hôte n'est pas une URI valide. Vérifiez que l'adresse renseignée est correcte.



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.