Erreurs du pack windows-by-WinRM__shinken

Sommaire

Contexte

Vous retrouverez dans cette page les erreurs fréquentes liées à une mauvaise configuration, authentification ou problèmes de connexion.

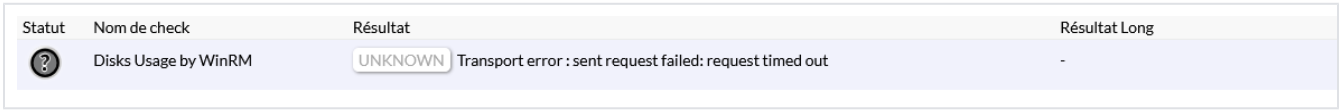
Les Erreurs

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 :

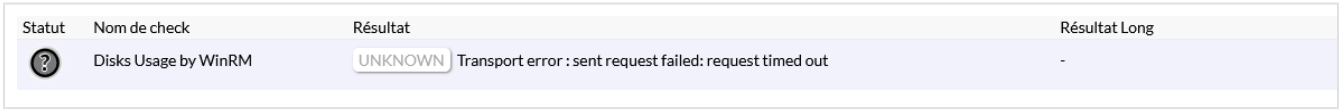
```
# Redémarrer le service WinRM :
Restart-Service WinRM

# 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.

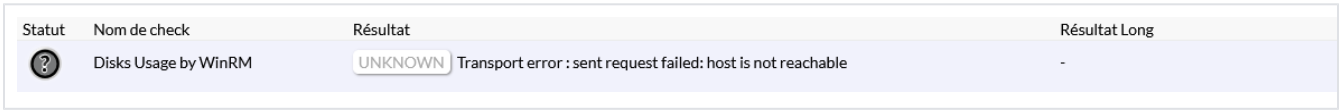
- Il se peut que vôte service WinRM ne soit pas lancé
- ou que votre pare-feu ne soit pas configuré.



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

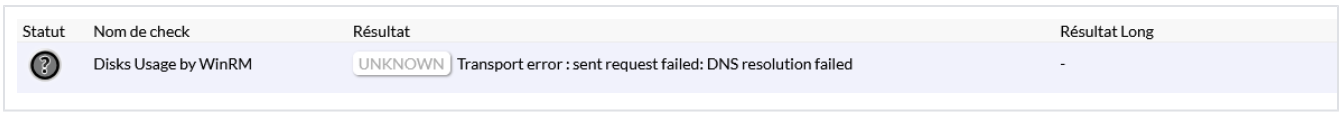
L'hôte n'a pas pu recevoir la requête. Vérifiez votre réseau, routeur, pare-feu et nom d'hôte.



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

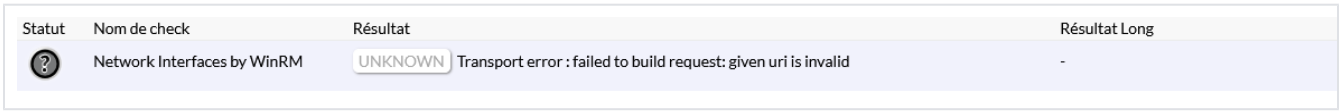
Le nom de l'hôte n'a pas pu être résolu. Vérifiez que l'adresse renseignée est correcte et que le serveur DNS est accessible.



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

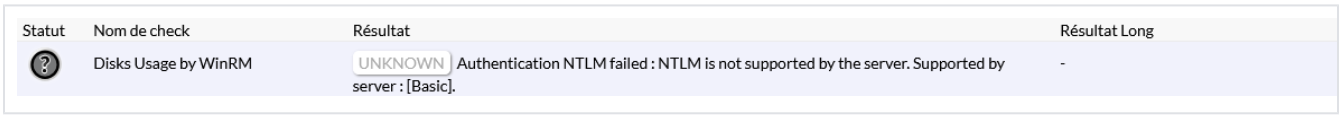
Le nom de l'hôte n'est pas une URI valide. Vérifiez que l'adresse renseignée est correcte.



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.

Ntp Sync by WinRM

MONITORED HOST - BAD STATE – Windows Time service is not running. Please start the w32time service

Le service de temps **W32Time** n'est pas allumé.

Statut	Nom de check	Résultat	Résultat Long
	Ntp Sync by WinRM	MONITORED HOST - BAD STATE Windows Time service is not running. Please start the w32time service. Couldn't fetch NTP synchronization data as Windows Time Service is down.	-

La commande ci-dessous permet de le rallumer :

```
# Redémarrer le service WinRM :
Restart-Service W32Time
```

Il est aussi possible de le configurer pour se lancer automatiquement au démarrage :

```
# Configurer le démarrage automatique
Set-Service -Name W32Time -StartupType Automatic
```

MONITORED HOST - BAD STATE – No external time server source is configured.

La machine Windows supervisé n'a aucune source NTP externe configuré. Son unique référence de temps est sa propre horloge.

Statut	Nom de check	Résultat	Résultat Long
?	Ntp Sync by WinRM	MONITORED HOST - BAD STATE No external time server source is configured. Configured source is 'Local CMOS Clock'. The server considers itself as the time reference instead of being synchronized to an external NTP server, making this check unapplicable.	-

Résolution 1 :

Si ce comportement était attendu, alors il est possible de désactiver le check **NTP Sync by WinRM** sur cette machine.
Résolution 2 :

Il est possible de configurer sa machine Windows avec de nouvelles sources externes NTP. Pour cela :

Ouvrir un PowerShell en administrateur.

Clic-droit sur PowerShell Exécuter en tant qu'administrateur
Définir un nouveau serveur NTP

Remplacer le serveur par celui de votre choix (exemple : `pool.ntp.org` ou `time.windows.com`).

```
w32tm /config /manualpeerlist:"time.windows.com" /syncfromflags:manual /reliable:yes /update
```

Redémarrer le service de temps Windows

```
Restart-Service w32time
```

Forcer une synchronisation (optionnel)

```
w32tm /resync
```

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**.

Services Matching [KEY] by WinRM

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: (Get-Service).Name • Then update DFE variable "WINDOWS_BY_WINRM__SERVICES-STATE__SERVICES-TO-CHECK"	-

Erreurs de configuration du poller shinken

Erreurs communes à certains checks

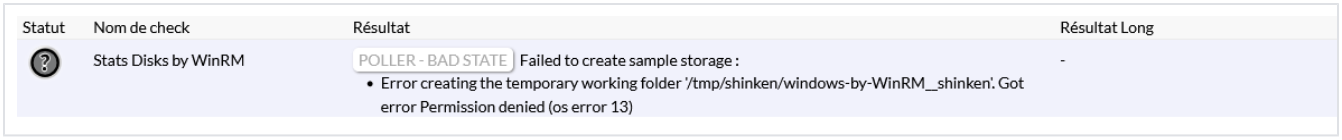
POLLER - BAD STATE – Permission denied

Les checks concernés sont :

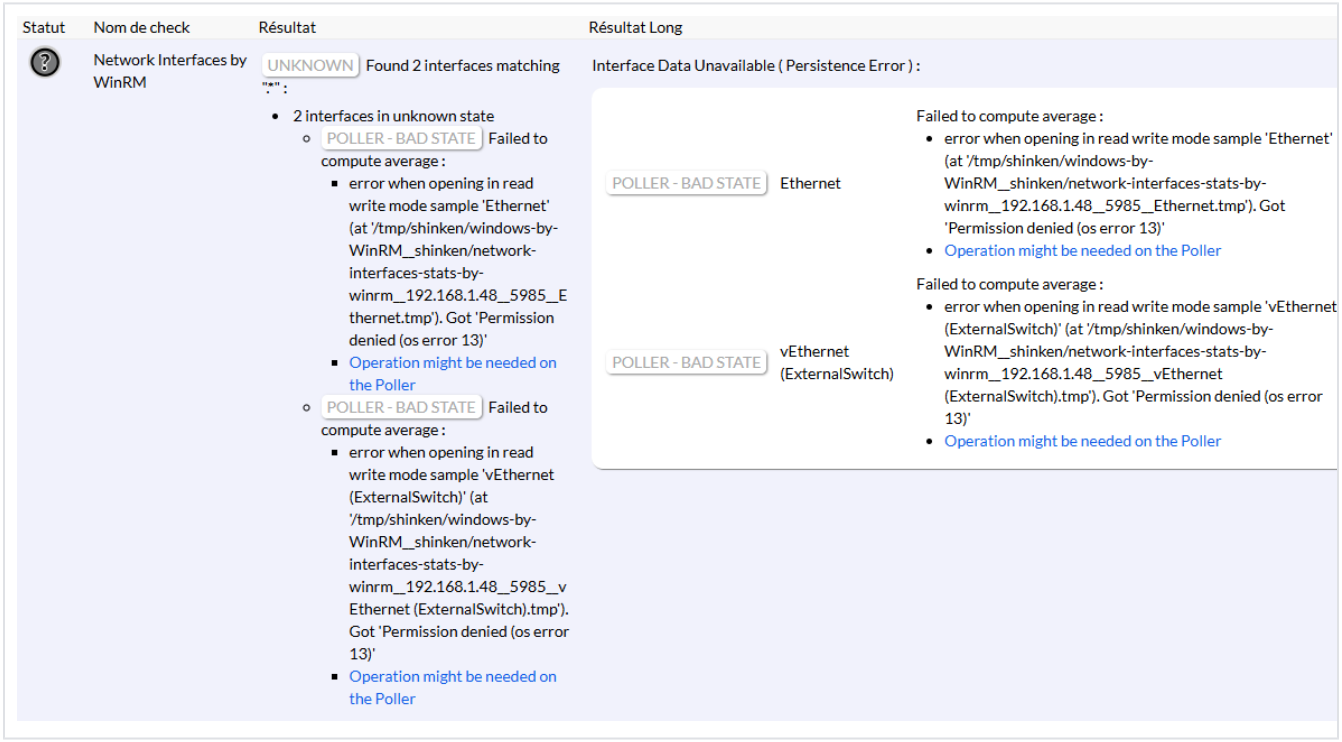
- **Network Interfaces by WinRM**
- **Stats Disks by WinRM**

Le *poller* qui exécutera les checks nécessite un droit d'écriture et de lecture dans le répertoire décrit par **WINDOWS_BY_WINRM__POLLER-SHARED-WORKING-FOLDER-BASE-PATH/WINDOWS_BY_WINRM__POLLER-SHARED-WORKING-FOLDER-TMP-DIRNAME**, par défaut **/tmp /shinken .**

Vous pouvez obtenir les erreurs suivantes :



Statut	Nom de check	Résultat	Résultat Long
?	Stats Disks by WinRM	POLLER - BAD STATE Failed to create sample storage : • Error creating the temporary working folder '/tmp/shinken/windows-by-WinRM_shinken'. Got error Permission denied (os error 13)	-



Statut	Nom de check	Résultat	Résultat Long
?	Network Interfaces by WinRM	UNKNOWN Found 2 interfaces matching "*" : • 2 interfaces in unknown state ◦ POLLER - BAD STATE Failed to compute average : ▪ error when opening in read write mode sample 'Ethernet' (at '/tmp/shinken/windows-by-WinRM_shinken/network-interfaces-stats-by-winrm_192.168.1.48_5985_Ethernet.tmp'). Got 'Permission denied (os error 13)' ▪ Operation might be needed on the Poller ◦ POLLER - BAD STATE Failed to compute average : ▪ error when opening in read write mode sample 'vEthernet (ExternalSwitch)' (at '/tmp/shinken/windows-by-WinRM_shinken/network-interfaces-stats-by-winrm_192.168.1.48_5985_vEthernet (ExternalSwitch).tmp'). Got 'Permission denied (os error 13)' ▪ Operation might be needed on the Poller	Interface Data Unavailable (Persistence Error) : POLLER - BAD STATE Ethernet Failed to compute average : • error when opening in read write mode sample 'Ethernet' (at '/tmp/shinken/windows-by-WinRM_shinken/network-interfaces-stats-by-winrm_192.168.1.48_5985_Ethernet.tmp'). Got 'Permission denied (os error 13)' • Operation might be needed on the Poller POLLER - BAD STATE vEthernet (ExternalSwitch) Failed to compute average : • error when opening in read write mode sample 'vEthernet (ExternalSwitch)' (at '/tmp/shinken/windows-by-WinRM_shinken/network-interfaces-stats-by-winrm_192.168.1.48_5985_vEthernet (ExternalSwitch).tmp'). Got 'Permission denied (os error 13)' • Operation might be needed on the Poller

Résolution

> **Remarque**
>
> Cette série de commandes ne peut être effectuée qu'en ayant les droits root.
>
> Donc en étant connecté au compte root ou en ayant fait la commande "su" au préalable.

> Les instructions suivantes sont à exécuter sur vos pollers

Utilisation

```
shinken_tmp_dirname="shinken"
mkdir --parents /tmp/$shinken_tmp_dirname
chown -R root:shinken /tmp/$shinken_tmp_dirname
chmod -R g+rwx /tmp/$shinken_tmp_dirname
```

Explication

1. La commande **mkdir --parents /tmp/$shinken_tmp_dirname** crée un récursivement un répertoire.

2. La commande **chown -R root:shinken /tmp/$shinken_tmp_dirname** modifie le groupe du dossier **/tmp/shinken**.

   - Cela garantit que des droits peuvent être appliqués au groupe shinken sur ce dossier.

3. La commande **chmod -R g+rwx /tmp/$shinken_tmp_dirname** applique immédiatement les droits nécessaires au dossier **/tmp/shinken** pour le groupe **shinken**.

- Les droits de lecture, d'écriture et d'exécution sont ajoutés au dossier. Cela permet aux sondes de créer et lire des fichiers dans le dossier **/tmp/shinken**.

Il est nécessaire d'adapter la variable **shinken_tmp_dirname** si vous avez modifié l'un des deux variables suivantes :

- **WINDOWS_BY_WINRM__POLLER-SHARED-WORKING-FOLDER-BASE-PATH**
- **WINDOWS_BY_WINRM__POLLER-SHARED-WORKING-FOLDER-TMP-DIRNAME**