Files Matching KEY EXIST by WinRM

Sommaire

Contexte

Le check **File Matching [KEY] EXIST by WinRM** permet de vérifier la présence de fichiers dans un répertoire, en fonction d'un filtre spécifique ou d'une liste de nom de fichiers.

Paramétrage

Le check utilise la ligne de commande suivante :

```
$WINDOWS-BY-WINRM__SHINKEN__PLUGINSDIR$/check_windows_health_by_winrm_rust --check check_files_matching
          --hostname "$HOSTADDRESS$"
          --port "$_HOSTWINDOWS_BY_WINRM__PORT$"
          --username "$_HOSTWINDOWS_BY_WINRM__DOMAINUSER$"
          --password "$_HOSTWINDOWS_BY_WINRM__DOMAINPASSWORD$"
          --auth_method "$_HOSTWINDOWS_BY_WINRM__AUTHMETHOD$"
          --timeout "$_HOSTWINDOWS_BY_WINRM__TIMEOUT$"

          --path "$ARG1$"
          --filter "$ARG2$"

          --recursive "$ARG3$"
          --include_hidden "$ARG4$"

          --kind "exist"
```

Données utilisées provenant du modèle

Données communes pour les checks du modèle

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

Aucune donnée spécifique — ce check ne dispose pas de seuils configurables.

Les données DFE (Duplicate Foreach)

Nom	Modifiable sur	Valeur par défaut	Description	Exemple

<table>
<tr>
<td>WINDOWS_BY_WINRM__FILES-MATCHING-EXIST</td>
<td>l'Hôte

(Onglet Données)</td>
<td>--</td>
<td>
<table>
<tr><th>Valeur</th><th>Explication</th><th>Exemple</th></tr>
<tr><td>KEY</td><td>Nom utilisé pour garantir l'unicité des checks DFE générés.</td><td>LOGS</td></tr>
<tr><td>$ARG1$</td><td>Répertoire principal à analyser.</td><td>C:\shinken</td></tr>
<tr><td>$ARG2$</td><td>Filtre à appliquer sur ce répertoire. Il peut prendre deux formes différentes :
un pattern
une liste de noms de fichiers</td><td>*.log
[fichier1.log,fichier2.log] ou fichier1.log;fichier2.log</td></tr>
<tr><td>$ARG3$</td><td>Active ou désactive la recherche récursive dans le répertoire principal. Il peut accepter 2 types de données :
un booléen
un nombre entier</td><td>true/false
Note : À "true", le check analysera le répertoire et tous ses dossiers jusqu'à la profondeur maximale.
3 (Le check analysera le répertoire et ses dossiers à une profondeur maximale de 3).</td></tr>
<tr><td>$ARG4$</td><td>Active ou désactive la prise en compte des fichiers cachés.</td><td>true/false</td></tr>
</table>
</td>
<td>
Mode pattern :
<pre>LOGS$(C:\shinken)$(*.log)$$(10)$$(20)$$(MB)$$(true)$$(true)$</pre>
Mode liste :
<pre>LOGS$(C:\shinken)$([fichier1.log,fichier2.log])$$(10)$$(20)$$(MB)$$(true)$$(true)$</pre>
</td>
</tr>
</table>

Si aucune valeur n'est renseignée pour un **$ARGn$** sur un check, la valeur définie sur la donnée associée dont il hérite est utilisée à la place. Cette donnée peut à son tour avoir sa propre valeur par défaut.

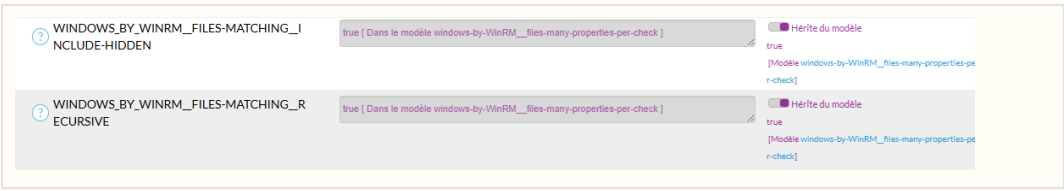
Tous les checks DFE générés à partir du modèle Modèle windows-by-WinRM__files-one-property-per-check héritent de ses valeurs par défaut. Cela implique que :

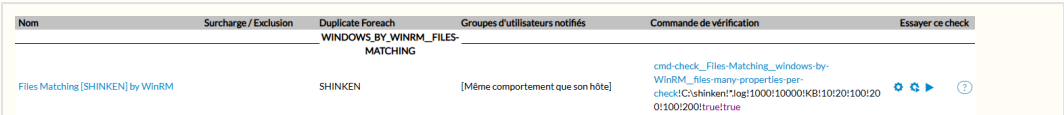
- **Effet global** : tant que **$ARGn$** n'est pas renseigné sur une instance, celle-ci lit la variable hôte définie par le modèle. Si plusieurs instances laissent **$ARGn$** vide, elles partagent toutes la même valeur. Modifier la variable hôte (ou la valeur par défaut du modèle) se répercute donc sur **toutes** les instances qui n'ont pas renseigné **$ARGn$**.
- **Comportement spécifique à une instance** : la seule façon de donner à une instance un comportement différent est de renseigner explicitement le **$ARGn$** concerné sur cette instance.

Exemple — **$ARG12$** et **$ARG13$** (fichiers cachés et récursivité) du check *Files Matching [KEY] by WinRM* :

1. Si ils ne sont pas renseignés sur l'instance, le modèle utilise les variables hôtes **WINDOWS_BY_WINRM__FILES-MATCHING__RECURSIVE** et **WINDOWS_BY_WINRM__FILES-MATCHING__INCLUDE-HIDDEN**.

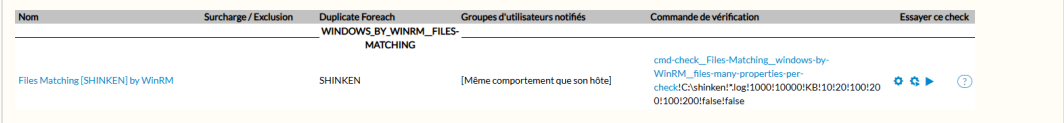
2. Si ces variables ne pas sont pas définies, elles prendront leur propre valeur par défaut, **true**.





La coloration ici, indique que les valeurs par défauts sont utilisés

3. Si plusieurs instances ne déclarent pas **$ARG12$** et **$ARG13$,** les 2 utiliseront les même données.
4. Conséquence : plusieurs instances générées sans **$ARG12$** et **$ARG13$** utiliseront toutes **true**. Pour qu'une instance particulière utilise **false**, il faut renseigner **$ARG12$** et **$ARG13$** sur cette instance ; modifier **WINDOWS_BY_WINRM__FILES-MATCHING__RECURSIVE** et **WINDOWS_BY_WINRM__FILES-MATCHING__INCLUDE-HIDDEN** à **false** fe rait basculer toutes les instances sans surcharge à **false**.



Données utilisées provenant du check

Pas de données provenant du check

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

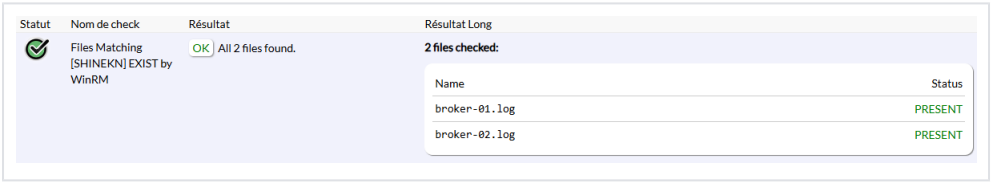
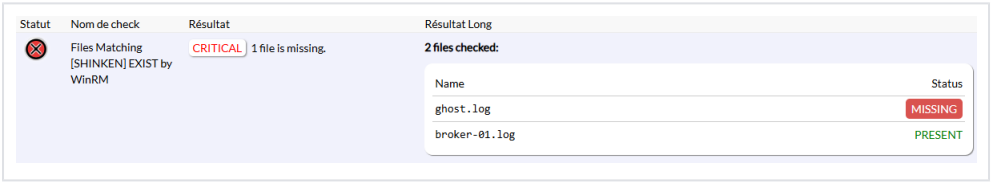
Statut	Nom de check	Résultat	Résultat Long
	Files Matching [SHINKEN] EXIST by WinRM	OK 5 file(s) found matching 'Pattern: '*.log'' in 'C:\shinken'.	-

Interprétation

Statut

- Il peut prendre trois valeurs ***OK*** / ***CRITIQUE*** / ***INCONNU*** .
  - Ce check ne dispose pas de seuils configurables. Le statut dépend uniquement de la présence ou de l'absence des fichiers attendus.
  - Voici un tableau récapitulatif du statut attendu suivant le retour de sonde :

Situation	*Statut*	*Exemple*
• **Mode pattern** — au moins un fichier correspondant au filtre est présent dans le répertoire	***OK***	

▪ **Mode pattern** — aucun fichier correspondant au filtre dans le répertoire ciblé	***CRITIQUE***	
• **Mode liste** — tous les fichiers attendus sont présents	***OK***	
▪ **Mode liste** — au moins un fichier attendu est absent du répertoire ciblé	***CRITIQUE***	

Résultat

Une seule ligne, le format dépend du mode de filtre :

Mode pattern :

- **OK** : N fichier(s) trouvé(s) correspondant à '' dans ''.
- **CRITIQUE** (0 fichier) : Aucun fichier trouvé correspondant à '<filtre>' dans '<chemin>'.

Mode liste :

- **OK** (tous trouvés) : Les N fichier(s) sont tous présent(s).
- **CRITIQUE** (1 manquant) : N fichier(s) manquant(s).

Résultat Long

En **mode pattern**, aucun résultat long n'est émis.

En **mode liste** ($ARG2$ sous la forme **[fichier1.log, fichier2.log, ...]**), le résultat long est toujours émis. Il présente un tableau listant chaque fichier attendu avec son statut : **PRESENT** ou **MISSING**.

Métriques

Aucune métrique émise par ce check.

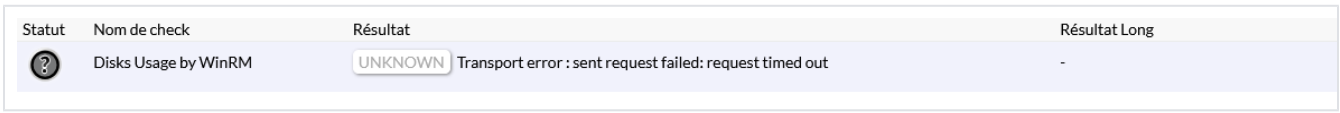
Erreurs et pré-requis

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.



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 :

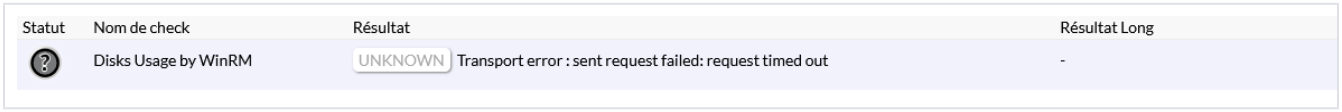
```
# Redémarrer le service WinRM :
Restart-Service WinRM

# 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.

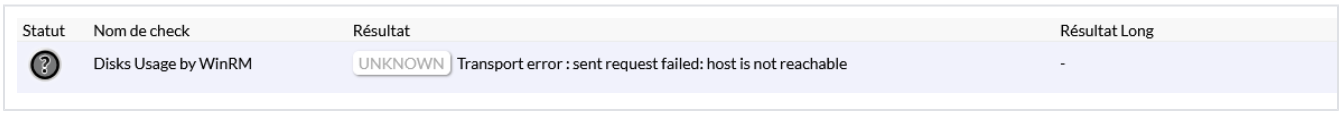
- Il se peut que vôte service WinRM ne soit pas lancé
- ou que votre pare-feu ne soit pas configuré.



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

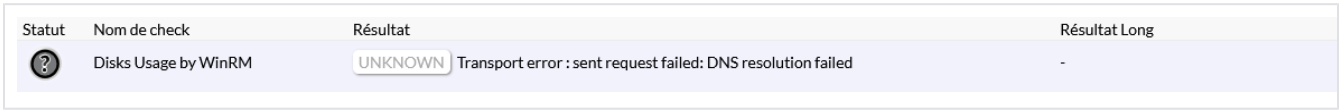
L'hôte n'a pas pu recevoir la requête. Vérifiez votre réseau, routeur, pare-feu et nom d'hôte.



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

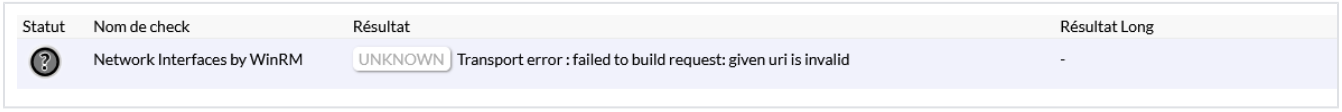
Le nom de l'hôte n'a pas pu être résolu. Vérifiez que l'adresse renseignée est correcte et que le serveur DNS est accessible.



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

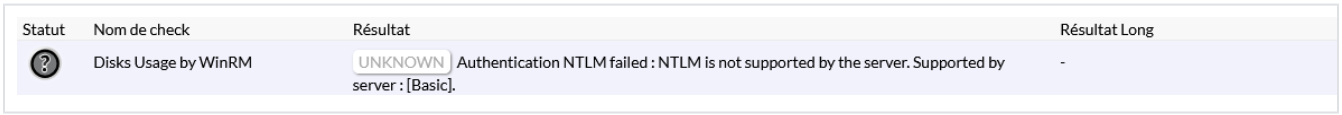
Le nom de l'hôte n'est pas une URI valide. Vérifiez que l'adresse renseignée est correcte.



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**"

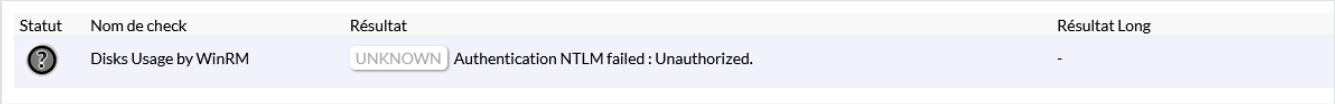
UNKNOWN – Authentication NTLM failed : Unauthorized

La connexion NTLM n'a pas été 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
- Le mot de passe du compte de supervision a expiré, ou un changement est imposé à la prochaine ouverture de session.



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 de WinRM et du compte de supervision sur une seule machine Windows pour le pack windows-by-WinRM__shinken*).

Si la configuration WinRM est correcte, penchez pour une expiration du mot de passe ou un changement imposé.

Sur l'hôte supervisé, en session administrateur, exécuter :

```
Get-WinEvent -FilterHashtable @{LogName='Security'; Id=4625} -MaxEvents 20 |
      ForEach-Object {
        $p = $_.Properties
        "{0}  account={1,-20} status=0x{2:X8} substatus=0x{3:X8}" -f `
            $_.TimeCreated, $p[5].Value, $p[7].Value, $p[9].Value
      }
```

Repérer les lignes portant le nom du compte de supervision, puis interpréter :

Status	Sub Status	Cause
0xC000006D	0xC000006A	Mot de passe incorrect
0xC000006D	0xC0000064	Le compte n'existe pas
0xC000006E	0xC0000071	Mot de passe EXPIRÉ
0xC0000224	0x00000000	Changement de mot de passe imposé a la prochaine ouverture de session
0xC000015B	0x00000000	Le compte n'a pas le droit « Accéder à cet ordinateur depuis le réseau »
0xC0000234	0x00000000	Compte verrouillé
0xC000006E	0xC0000072	Compte désactivé
0xC0000193	0x00000000	Compte expiré (le compte lui-même, pas son mot de passe)
0xC0000133	0x00000000	Horloges désynchronisées entre l'hôte et le contrôleur de domaine
0xC0000225	0x00000000	Anomalie Windows connue, sans conséquence (à ignorer)

ATTENTION : les deux codes doivent être lus ensemble

La cause n'est pas portée par le même champ selon les cas : il faut relever le **Status** et le **Sub Status**, et faire correspondre la paire complète au tableau ci-dessus.

Si la cause est une **expiration** ou un **changement imposé** :

- Réinitialisez le mot de passe du compte de supervision
- Reportez le nouveau mot de passe dans les données de vos modèles hôtes sur le synchronizer.
- Ensuite vous pouvez désactiver l'expiration pour le compte de supervision. (*Voir page Configuration du Windows supervisé dans un Domaine (Active Directory) pour le pack windows-by-WinRM__shinken ou la page Configuration du Windows supervisé pour le pack windows-by-WinRM__shinken selon votre configuration*)

Si le code est **0xC000015B** :

La configuration de l'hôte est incomplète : le compte existe et son mot de passe est valide, mais il n'a pas le droit d'ouverture de session sur cette machine. Rejouez **Configure-Host.ps1** en workgroup, ou vérifiez l'application des GPO en domaine.

Si le code est **0xC0000133** :

Vérifiez la synchronisation horaire de l'hôte supervisé. Le check Ntp Sync by WinRM du pack surveille précisément ce point.

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
```

- Le mot de passe du compte de supervision a expiré, ou un changement est imposé à la prochaine ouverture de session.
- 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 de WinRM et du compte de supervision sur une seule machine Windows pour le pack windows-by-WinRM__shinken*).

Si la configuration WinRM est correcte, penchez pour une expiration du mot de passe ou un changement imposé.

Sur l'hôte supervisé, en session administrateur, exécuter :

```
Get-WinEvent -FilterHashtable @{LogName='Security'; Id=4625} -MaxEvents 20 |
      ForEach-Object {
        $p = $_.Properties
        "{0}  account={1,-20} status=0x{2:X8} substatus=0x{3:X8}" -f `
            $_.TimeCreated, $p[5].Value, $p[7].Value, $p[9].Value
      }
```

Repérer les lignes portant le nom du compte de supervision, puis interpréter :

Status	Sub Status	Cause
0xC000006D	0xC000006A	Mot de passe incorrect
0xC000006D	0xC0000064	Le compte n'existe pas
0xC000006E	0xC0000071	Mot de passe EXPIRÉ
0xC0000224	0x00000000	Changement de mot de passe imposé a la prochaine ouverture de session
0xC000015B	0x00000000	Le compte n'a pas le droit « Accéder à cet ordinateur depuis le réseau »
0xC0000234	0x00000000	Compte verrouillé
0xC000006E	0xC0000072	Compte désactivé
0xC0000193	0x00000000	Compte expiré (le compte lui-même, pas son mot de passe)
0xC0000133	0x00000000	Horloges désynchronisées entre l'hôte et le contrôleur de domaine
0xC0000225	0x00000000	Anomalie Windows connue, sans conséquence (à ignorer)

ATTENTION : les deux codes doivent être lus ensemble

La cause n'est pas portée par le même champ selon les cas : il faut relever le **Status** et le **Sub Status**, et faire correspondre la paire complète au tableau ci-dessus.

Si la cause est une **expiration** ou un **changement imposé** :

- Pour reinitialiser le mot de passe du compte et / ou désactiver l'expiration du mot de passe pour le compte de supervision. (*Voir page Configuration du Windows supervisé dans un Domaine (Active Directory) pour le pack windows-by-WinRM__shinken ou la page Configuration du Windows supervisé pour le pack windows-by-WinRM__shinken selon votre configuration*)
- Reportez le nouveau mot de passe dans les données de vos modèles hôtes sur le synchronizer.

Si le code est **0xC000015B** :

La configuration de l'hôte est incomplète : le compte existe et son mot de passe est valide, mais il n'a pas le droit d'ouverture de session sur cette machine. Rejouez **Configure-Host.ps1** en workgroup, ou vérifiez l'application des GPO en domaine.

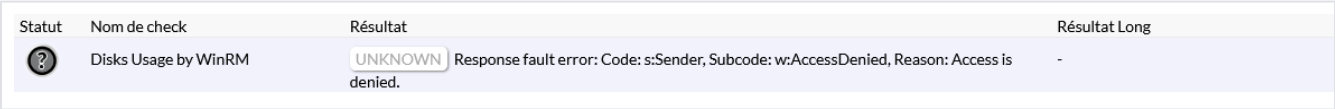
Si le code est **0xC0000133** :

Vérifiez la synchronisation horaire de l'hôte supervisé. Le check Ntp Sync by WinRM du pack surveille précisément ce point.

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.



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 de WinRM et du compte de supervision sur une seule machine Windows 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 de WinRM et du compte de supervision sur une seule machine Windows 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.